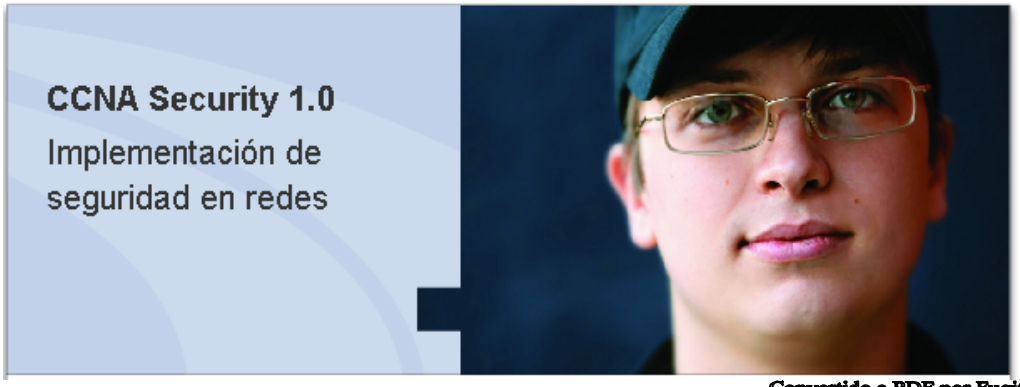


Convertido a PDF por Fugitivo
Aportes por Custodia Lacrimarum

INTRODUCCION

Mensaje a los estudiantes.

Bienvenido
Bienvenido al curso CCNA Security. El objetivo de este curso es desarrollar un entendimiento detallado de los principios de seguridad en redes y de las herramientas y configuraciones disponibles. Este material del curso en línea lo ayudará a desarrollar las aptitudes necesarias para diseñar y soportar la seguridad en redes.

Más que solo información
Este ambiente de aprendizaje asistido por PC es una parte importante de la experiencia total del curso para estudiantes e instructores de Networking Academy. El material en línea de este curso está diseñado para ser utilizado en combinación con otras herramientas y actividades didácticas. Por ejemplo,

presentaciones en clase, debates y práctica con su instructor
prácticas de laboratorio que usan equipos de redes dentro del aula de Networking Academy
evaluaciones en línea y un libro de calificaciones para cotejar
la herramienta de simulación Packet Tracer.

Una comunidad global
Cuando participa en Networking Academy, se suma a una comunidad mundial conectada por tecnologías y objetivos en común. En el programa, participan escuelas, institutos de enseñanza superior, universidades y otras entidades de más de 160 países. Para ver la comunidad de Networking Academy mundial visite http://www.academynetspace.com.

El material de este curso incluye una amplia gama de tecnologías que facilitan la forma de trabajar, vivir, jugar y aprender de las personas, comunicándose mediante voz, vídeo y otros datos. La red e Internet afectan a las personas de distintas maneras en las distintas partes del mundo. Si bien hemos trabajado con instructores de todo el mundo para crear este material, es importante que trabaje con su instructor y compañeros para que el material de este curso se aplique a su situación local.

Manténgase comunicado
Este material de instrucción en línea, como el resto de las herramientas del curso, son parte de algo más grande: la Networking Academy. Podrá encontrar el portal del administrador, instructor y estudiante del programa en http://www.cisco.com/web/learning/netacad/index.html. Allí obtendrá acceso a las demás herramientas del programa, como el servidor de evaluación y el libro de calificaciones del alumno, así como también a actualizaciones informativas y otros enlaces relevantes.

Mind Wide Open™
Un objetivo importante en la educación es enriquecer al estudiante (a usted), ampliando lo que sabe y puede hacer. Sin embargo, es importante comprender que el material de instrucción y el instructor sólo pueden facilitarle el proceso. Es usted quien debe asumir el compromiso de incorporar nuevas aptitudes. A continuación encontrará algunas sugerencias que lo ayudarán a aprender y crecer:

1. Tome notas. Los profesionales del campo de networking generalmente tienen diarios de ingeniería en donde anotan las cosas que observan y aprenden. La toma de notas es importante como ayuda para mejorar su comprensión con el pasar del tiempo.

2. Reflexione. El curso proporciona información que le permitirá cambiar lo que sabe y lo que puede hacer. A medida que vaya avanzando en el curso, pregúntese qué cosas tienen sentido y cuáles no. Haga preguntas cuando algo resulte confuso. Intente averiguar más sobre los temas que le interesan. Si no está seguro por qué se enseña algo, pregúntele a su instructor o a un amigo. Piense cómo se complementan las distintas partes del curso.

3. Practique. Creemos que practicar es tan importante para el e-learning que le dimos un nombre especial. Lo llamamos e-Doing. Es muy importante que realice las actividades del material de instrucción en línea y que también realice las actividades del Packet Tracer y las prácticas de laboratorio.

4. Practique nuevamente. ¿Alguna vez pensó que sabía cómo hacer algo y luego, cuando llegó el momento de demostrarlo en una prueba o en el trabajo, descubrió que en realidad no había aprendido bien cómo hacerlo? Como cuando se aprende cualquier nueva habilidad, como un deporte, un juego o un idioma, aprender una aptitud profesional requiere paciencia y mucha práctica antes de que pueda decir que realmente la ha aprendido. El material de instrucción en línea de este curso le brinda oportunidades para practicar mucho distintas aptitudes. Aprovéchelas al máximo. También puede trabajar con su instructor para ampliar el Packet Tracer y otras herramientas para práctica adicional según sea necesario.

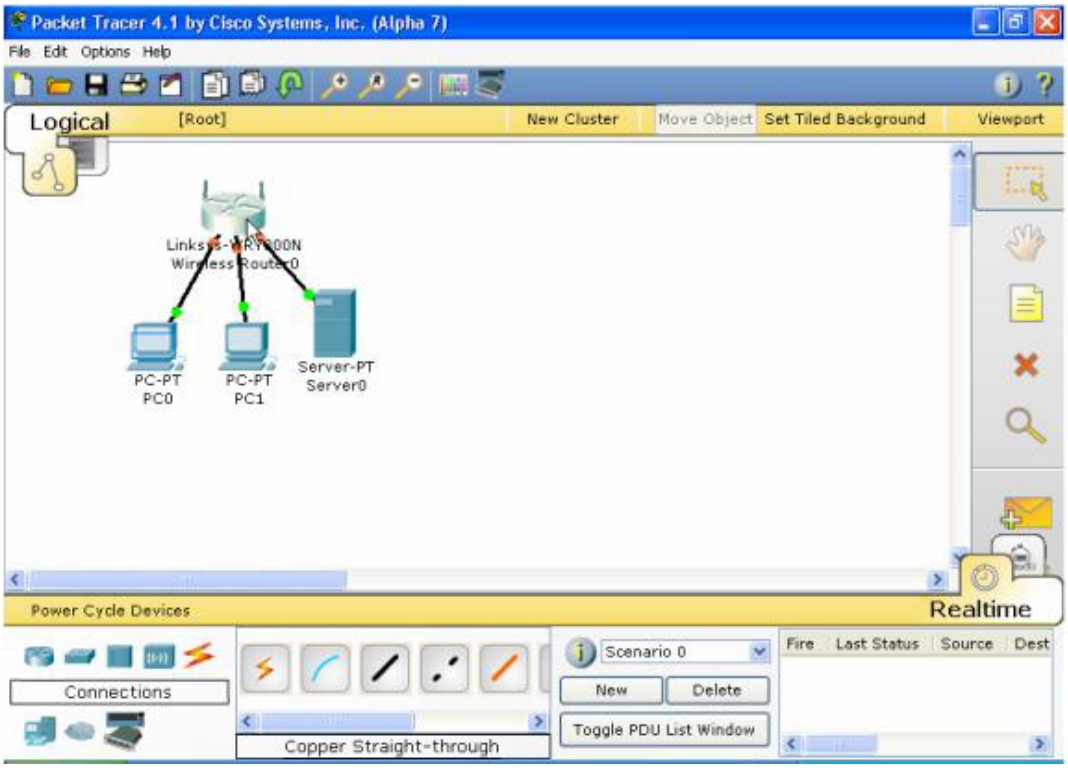
5. Enseñe. Generalmente, enseñarle a un amigo o colega es una buena forma de reforzar su propio aprendizaje. Para enseñar bien, deberá completar los detalles que puede haber pasado por alto en la primera lectura. Las conversaciones sobre el material del curso con compañeros, colegas y el instructor pueden ayudarlo a fijar los conocimientos de los conceptos de networking.

6. Realice cambios a medida que avanza. El curso está diseñado para proporcionar comentarios mediante actividades y cuestionarios interactivos, el sistema de evaluación en línea y a través de interacciones estructuradas con su instructor. Puede utilizar estos comentarios para entender mejor cuáles son sus fortalezas y debilidades. Si existe un área en la que tiene problemas, concéntrese en estudiar o practicar más esa área. Solicite comentarios adicionales a su instructor y a otros estudiantes.

Explore el mundo de networking
Esta versión del curso incluye una herramienta especial llamada Packet Tracer. El Packet Tracer es una herramienta de aprendizaje de networking que admite una amplia gama de simulaciones físicas y lógicas. También ofrece herramientas de visualización para ayudar a entender los componentes internos de una red.

Las actividades preelaboradas de Packet Tracer consisten en simulaciones de red, juegos, actividades y desafíos que brindan una amplia gama de experiencias de aprendizaje.

Cree sus propios mundos
También puede usar el Packet Tracer para crear sus propios experimentos y situaciones de red. Esperamos que, con el tiempo, utilice Packet Tracer no sólo para realizar las actividades desarrolladas previamente, sino también para convertirse en autor, explorador e investigador.



Una vez que complete este curso satisfactoriamente, podrá:

- Describir las amenazas de seguridad que las infraestructuras de red modernas afrontan.
- Asegurar los routers Cisco.
- Implementar AAA en routers Cisco utilizando bases de datos de router locales y servidores externos.
- Mitigar amenazas a redes y routers Cisco utilizando ACLs.
- Implementar reportes y administración de redes seguros.
- Mitigar ataques comunes de capa 2.
- Implementar el grupo de características de firewall de IOS de Cisco.
- Implementar el grupo de características de IPS de IOS de Cisco.
- Implementar VPNs de IPsec sitio a sitio.

CAPITULO 1 Amenazas modernas a la seguridad de las redes.

1.0 Introducción al capitulo

1.0.1 Introducción al capitulo

La seguridad de las redes es ahora una parte integral de las redes informáticas. Incluye protocolos, tecnologías, dispositivos, herramientas y técnicas que aseguran los datos y reducen las amenazas. Las soluciones de seguridad en redes surgieron en los años 1960 pero no se convirtieron en un conjunto exhaustivo de soluciones para redes modernas hasta el principio del nuevo milenio.

La mayor motivación de la seguridad en redes es el esfuerzo por mantenerse un paso más adelante de los hackers malintencionados. Del mismo modo que los médicos intentan prevenir nuevas enfermedades tratando problemas existentes, los profesionales de la seguridad en redes intentan prevenir ataques minimizando los efectos de los ataques en tiempo real. La continuidad de los negocios es otro factor impulsor de la seguridad en redes.

Se han creado organizaciones de seguridad en redes para establecer comunidades formales de profesionales de la seguridad en redes. Estas organizaciones establecen estándares, fomentan la colaboración y proveen oportunidades de desarrollo para los profesionales de la seguridad. Es importante que los profesionales de la seguridad en redes estén al tanto de los recursos provistos por estas organizaciones.

La complejidad de la seguridad en redes dificulta dominar todo lo que ésta abarca. Varias organizaciones han creado dominios que subdividen el mundo de la seguridad en redes en pedazos más fácilmente manejables. Esta división facilita a los profesionales

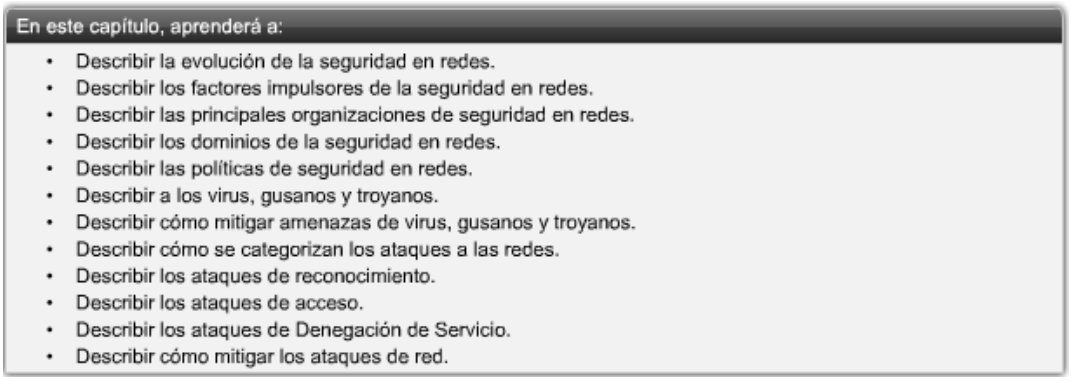
concentrarse en áreas más precisas de especialización en su educación, investigación y trabajo.

Las políticas de seguridad en redes son creadas por empresas y organizaciones gubernamentales para proveer un marco para que los empleados sigan en su trabajo diario. Los profesionales de la seguridad en redes de nivel administrativo son responsables de crear y mantener la política de seguridad de red. Todas las prácticas de seguridad en redes están relacionadas con y guiadas por la política de seguridad en redes.

Tal como la seguridad en redes está compuesta de dominios, los ataques a las redes son clasificados para hacer más fácil el aprender de ellos y abordarlos apropiadamente. Los virus, los gusanos y los troyanos son tipos específicos de ataques a las redes. Más generalmente, los ataques a las redes se clasifican como de reconocimiento, de acceso o de Denegación de Servicio.

Mitigar los ataques a las redes es el trabajo del profesional de seguridad en redes. En este capítulo, el alumno dominará la teoría subyacente de la seguridad en redes, cuya comprensión es necesaria antes de profundizar en una práctica de seguridad en redes. Aquí se presentan los métodos de mitigación de ataques de red, y el resto del curso comprende la implementación de estos métodos.

Una práctica de laboratorio para el capítulo, Herramientas de auditoría de seguridad e investigación de ataques de red, guiará al alumno en cuanto a herramientas de auditoría de seguridad e investigación de ataques de red. La práctica de laboratorio se encuentra en el manual de laboratorio en Academy Connection en [cisco.netacad.net.](cisco.netacad.net)



1.1 Principios fundamentales de una red segura.

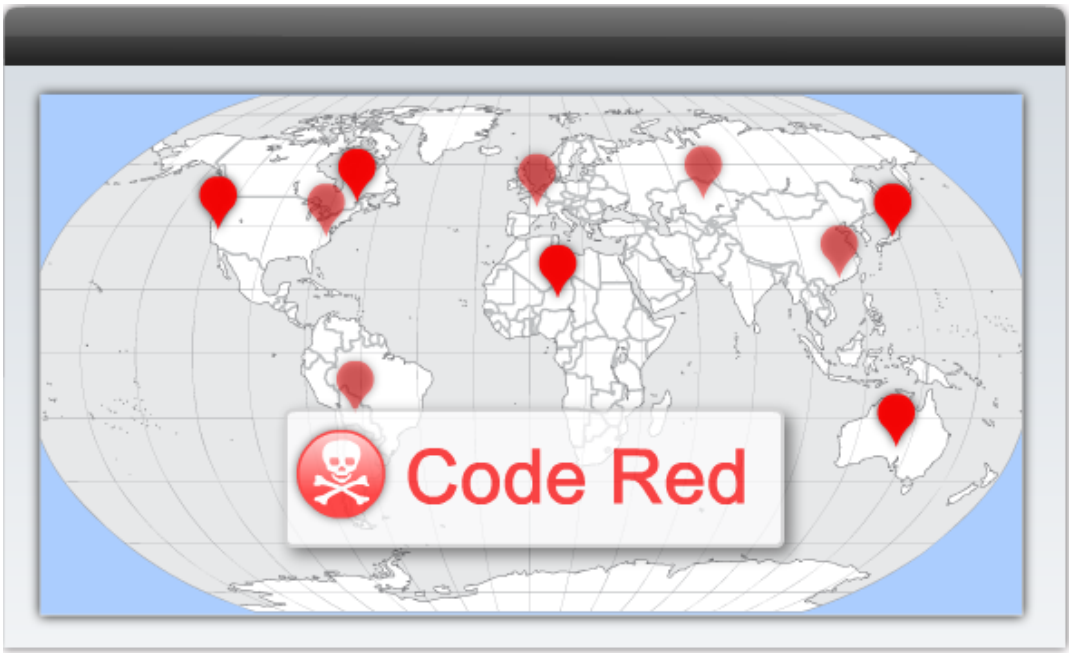
1.1.1 Evolución de la seguridad en redes.

En julio de 2001, el gusano Code Red atacó servidores web globalmente, infectando a más de 350.000 hosts. El gusano no solo interrumpió el acceso a los servidores infectados, sino que también afectó las redes locales que alojaban los servidores, volviéndolas muy lentas o inutilizables. El gusano Code Red causó una Denegación de Servicio (DoS) a millones de usuarios.

Si los profesionales de seguridad en redes responsables de los servidores infectados por el gusano hubieran desarrollado e implementado una política de seguridad, se habrían aplicado parches de seguridad a tiempo. El gusano Code Red habría sido detenido y solo ameritaría una nota al pie en la historia de la seguridad en redes.

La seguridad en redes está directamente relacionada con la continuidad de los negocios de una organización. Una brecha en la seguridad de la red puede afectar al e-comercio, causar la pérdida de datos, amenazar la privacidad de las personas (con potenciales consecuencias legales), y comprometer la integridad de la información. Estas vulnerabilidades pueden resultar en pérdidas de ingresos para las compañías, robo de propiedad intelectual, demandas e incluso puede amenazar la seguridad pública.

Mantener una red segura garantiza la seguridad de los usuarios de la red y protege los intereses comerciales. Esto requiere vigilancia de parte de los profesionales de seguridad en redes de la organización, quienes deberán estar constantemente al tanto de las nuevas y evolucionadas amenazas y ataques a las redes, así como también de las vulnerabilidades de los dispositivos y aplicaciones. Esta información se utiliza para adaptar, desarrollar e implementar técnicas de mitigación. Sin embargo, la seguridad de la red es, en última instancia, responsabilidad de todos los que la usan. Por esta razón, es trabajo del profesional de seguridad en redes asegurarse de que todos los usuarios reciban capacitación sobre concientización en seguridad. Mantener la red segura y protegida ofrece un ambiente de trabajo más estable y funcional para todos.

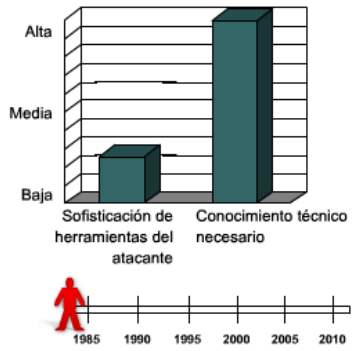


"La necesidad es la madre de todos los inventos". Este dicho se aplica perfectamente a la seguridad en redes. Cuando surgió Internet, los intereses comerciales eran insignificantes. La gran mayoría de los usuarios eran expertos en investigación y desarrollo. Los primeros usuarios raramente se involucraban en actividades que pudieran dañar a los otros usuarios. Internet no era un ambiente seguro porque no necesitaba serlo.

En el comienzo, el propósito de las redes era conectar a la gente y a sus máquinas a través medios de comunicación. El trabajo de un técnico de redes era conectar dispositivos para mejorar la habilidad de las personas de comunicar información e ideas. Los primeros usuarios de Internet no pasaban mucho tiempo pensando si sus actividades en línea podían amenazar la seguridad de su red o de sus propios datos.

Cuando los primeros virus se desataron y tomó lugar el primer ataque de DoS, el mundo cambió para los profesionales de redes. Para satisfacer las necesidades de los usuarios, los profesionales de redes aprendieron técnicas para asegurar a sus redes. El objetivo primordial de los profesionales de redes evolucionó de diseñar, construir y hacer crecer redes a asegurar redes existentes.

Hoy en día, Internet es una red muy diferente a la que era en sus comienzos en los años 1960. El trabajo de un profesional de redes incluye asegurarse de que el personal apropiado esté muy versado en herramientas, procesos, técnicas, protocolos y tecnologías de seguridad en redes. Es crítico que los profesionales de seguridad en redes mantengan una paranoia saludable para manejar la colección de amenazas a las redes en constante evolución.

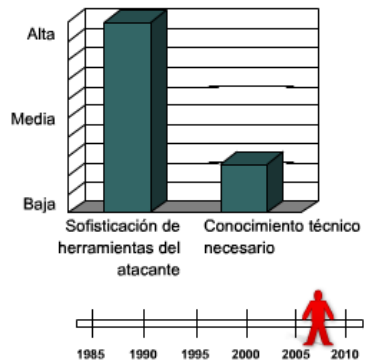


Arrastre al atacante sobre la linea de tiempo.

Linea de tiempo:

- 1978 - Primer Spam en ARPAnet
- 1988 - Virus Morris de Internet
- 1999 - Virus Melissa de correo electronico
- 2000 - Ataque DoS Mafiaboy, gusano Love Bug, cracker de contraseñas L0phtCrack
- 2001 - Ataque de DoS Code Red
- 2004 - Botnet golpea los sistemas militares de EEUU
- 2007 - Storm botnet, filtrado de datos de tarjeta de crédito TJX
- 2008 - Fraude de acciones Société Générale

Las amenazas se vuelven cada vez más sofisticadas a medida que disminuye la necesidad de conocimiento técnico de los atacantes para implementar ataques.



Arrastre al atacante sobre la linea de tiempo.

Linea de tiempo:

- 1978 - Primer Spam en ARPAnet
- 1988 - Virus Morris de Internet
- 1999 - Virus Melissa de correo electronico
- 2000 - Ataque DoS Mafiaboy, gusano Love Bug, cracker de contraseñas L0phtCrack
- 2001 - Ataque de DoS Code Red
- 2004 - Botnet golpea los sistemas militares de EEUU
- 2007 - Storm botnet, filtrado de datos de tarjeta de crédito TJX
- 2008 - Fraude de acciones Société Générale

Las amenazas se vuelven cada vez más sofisticadas a medida que disminuye la necesidad de conocimiento técnico de los atacantes para implementar ataques.

A medida que la seguridad en redes se convirtió en una parte integral de las operaciones diarias, fueron surgiendo dispositivos dedicados a funciones particulares de la seguridad en redes.

Una de las primeras herramientas de seguridad de redes fue el sistema de detección de intrusos (IDS), desarrollado por SRI International en 1984. Un IDS provee detección en tiempo real de ciertos tipos de ataques mientras están en progreso. Esta detección permite a los profesionales de redes mitigar más rápidamente el impacto negativo de estos ataques en los dispositivos de red y los usuarios. A fines de los años 1990, el sistema o sensor de prevención de intrusos (IPS) comenzó a reemplazar a la solución IDS. Los dispositivos IPS permiten detectar actividad maliciosa y tiene la habilidad de bloquear el ataque automáticamente en tiempo real.

Además de las soluciones IPS e IDS, se desarrollaron los firewalls para prevenir que tráfico no deseado ingresara a ciertas áreas señaladas dentro de una red, proporcionando seguridad de perímetro. En 1988, Digital Equipment Corporation (DEC) creó el primer firewall de red en la forma de un filtro de paquetes. Estos primeros firewalls inspeccionaban los paquetes para verificar que se correspondieran con conjuntos de reglas predefinidas, con la opción de forwardearlos o descartarlos. Los firewalls de filtrado de paquetes inspeccionan cada paquete aisladamente sin examinar si es parte de una conexión existente. En 1989, AT&T Bell Laboratories desarrolló el primer firewall de estados (stateful). Como los firewalls de filtrado de paquetes, los firewalls de estados utilizan reglas predefinidas para permitir o denegar tráfico. A diferencia de los firewalls de filtrado de paquetes, los firewalls de estados hacen seguimiento de las conexiones establecidas y determinan si un paquete pertenece a un flujo de datos existente, ofreciendo mayor seguridad y procesamiento más rápido.

Los firewalls originales eran prestaciones de software agregadas a dispositivos de red existentes, como routers. Con el tiempo, varias empresas desarrollaron firewalls dedicados o autónomos, que permiten a los routers y switches liberar la memoria y el procesador de la intensiva actividad de filtrar paquetes. Para las organizaciones que no requieren un firewall dedicado, los routers modernos, como el Router de Servicios Integrados Cisco (ISR), pueden ser utilizados como sofisticados firewalls de estados.

Además de encargarse de amenazas que provienen de afuera de la red, los profesionales de redes deben también estar preparados para amenazas que provengan desde adentro de la misma. Las amenazas internas, ya sean intencionales o accidentales, pueden causar aún más daño que las amenazas externas, por el acceso directo y conocimiento de la red y datos corporativos. A pesar de este hecho, el desarrollo de herramientas y técnicas para mitigar amenazas internas ha tardado más de 20 años luego de la introducción de herramientas y técnicas para mitigar amenazas externas.

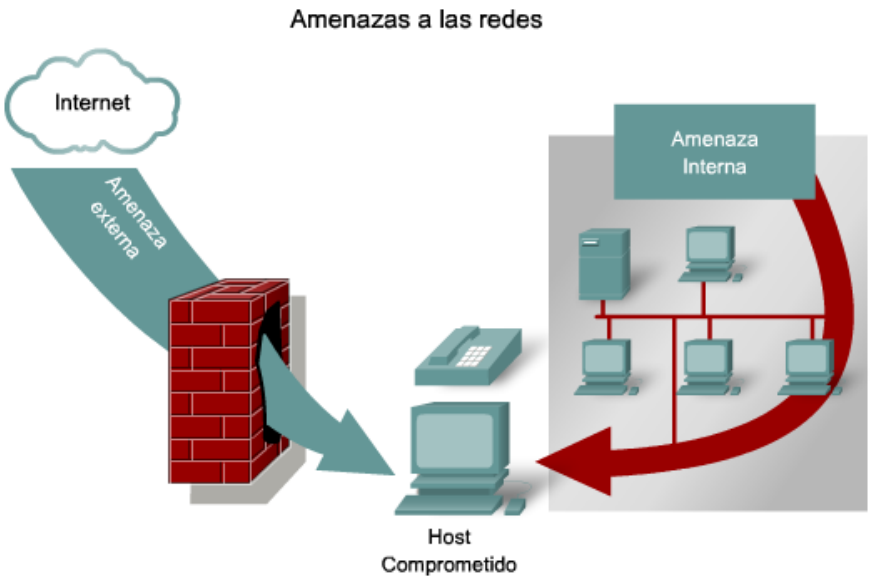
Un caso común de una amenaza que se origina desde dentro de una red es el de un empleado descontento con ciertas habilidades técnicas y voluntad de hacer daño. La mayoría de las amenazas desde dentro de la red revelan los protocolos y tecnologías utilizados en la red de área local (LAN) o la infraestructura switcheada. Estas amenazas internas caen, básicamente, en dos categorías: falsificación y DoS.

Los ataques de falsificación son ataques en los que un dispositivo intenta hacerse pasar por otro falsificando datos. Por ejemplo, la falsificación de direcciones MAC ocurre

cuando una computadora envia paquetes de datos cuya dirección MAC corresponde a otra computadora que no es la propia. Como éste, existen otros tipos de ataques de falsificación.

Los ataques de DoS hacen que los recursos de una computadora no estén disponibles para los usuarios a los que estaban destinados. Los hackers usan varios métodos para lanzar ataques de DoS.

Como profesional de seguridad en redes, es importante entender los métodos diseñados específicamente para apuntar a estos tipos de amenazas y asegurar la seguridad de la LAN.



Amenazas a la red | Evolución de la seguridad de LAN

Haga clic en cada botón para ver el contenido asociado.

Año	1998	2000	2003
Tecnología de seguridad	Mitigación de ataques de spoofing de direcciones MAC Mitigación de ataques de desbordamiento de tabla de direcciones Mitigación de tormentas LAN	Mitigación de falsificación de bridge raíz Mitigación de ataques VLAN	Mitigación de ataques de falsificación ARP

Amenazas a la red | Evolución de la seguridad de LAN

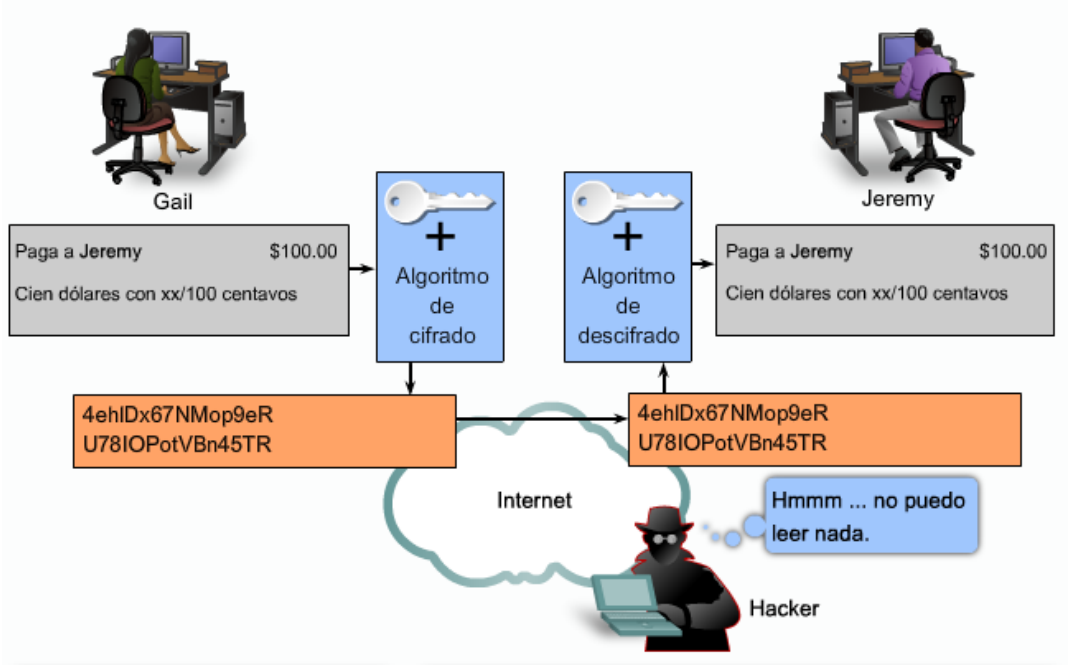
Haga clic en cada botón para ver el contenido asociado.

Además de prevenir y denegar tráfico malicioso, la seguridad en redes también requiere que los datos se mantengan protegidos. La criptografía, el estudio y práctica de ocultar información, es ampliamente utilizada en la seguridad de redes moderna. Hoy en día, cada tipo de comunicación de red tiene un protocolo o tecnología correspondiente, diseñado para ocultar esa comunicación de cualquier otro que no sea el usuario al que está destinada.

Los datos inalámbricos pueden ser cifrados (ocultados) utilizando varias aplicaciones de criptografía. Se puede cifrar una conversación entre dos usuarios de teléfonos IP y también pueden ocultarse con criptografía los archivos de una computadora. Estos son solo algunos ejemplos. La criptografía puede ser utilizada en casi cualquier comunicación de datos. De hecho, la tedencia apunta a que todas las comunicaciones sean cifradas.

La criptografía asegura la confidencialidad de los datos, que es uno de los tres componentes de la seguridad de la información: confidencialidad, integridad y disponibilidad. La seguridad de la información comprende la protección de la información y de los sistemas de información de acceso, uso, revelación, interrupción, modificación o destrucción no autorizados.

El cifrado provee confidencialidad al ocultar los datos en texto plano. La integridad de los datos, es decir, el hecho de que los datos sean preservados sin alteraciones durante una operación, se mantiene a través del uso de mecanismos de hashing. La disponibilidad, que es la accesibilidad a los datos, está garantizada por los mecanismos de network hardening y sistemas de resguardo de datos.



1.1.2 Impulsores de la seguridad en redes

La palabra hackers tiene una variedad de significados. Para muchos, significa programadores de Internet que intentan ganar acceso no autorizado a dispositivos en Internet. También se usa para referirse a individuos que corren programas para prevenir o reducir la velocidad del acceso a las redes por parte de un gran número de usuarios, o corromper o eliminar los datos de los servidores. Pero para otros, el término hacker tiene una interpretación positiva como un profesional de redes que utiliza habilidades de programación de Internet sofisticadas para asegurarse de que las redes no sean vulnerables a ataques. Bueno o malo, el hacking es una fuerza impulsora de la seguridad en redes.

Desde una perspectiva de negocios, es importante minimizar los efectos de los hackers con malas intenciones. Los negocios pierden productividad cuando la red es lenta o no responde. Las ganancias se ven impactadas por la pérdida y la corrupción de datos.

El trabajo del profesional de seguridad en redes es el de estar siempre un paso más adelante que los hackers tomando capacitaciones, participando en organizaciones de seguridad, suscribiéndose a canales web (feeds) en tiempo real sobre amenazas y visitando sitios web de seguridad diariamente. El profesional de seguridad en redes también debe tener acceso a herramientas de seguridad, protocolos, técnicas y tecnologías de última generación. Los profesionales de la seguridad en redes tienen que tener muchas de las cualidades que se buscan en el personal de policía: deben mantenerse al tanto de actividades maliciosas y tener las habilidades y herramientas para minimizar o eliminar las amenazas asociadas con esas actividades.

El hacking tiene el efecto accidental de poner a los profesionales de la seguridad en redes al frente en cuanto a posibilidades de empleo y remuneración. Sin embargo, en relación con otras profesiones tecnológicas, la seguridad en redes tiene la curva de aprendizaje más empinada y la mayor demanda de participación constante en desarrollo profesional.



El hacking comenzó en la década de 1960 con el phone freaking, o phreaking, que se refiere al hecho de usar varias frecuencias de radio para manipular los sistemas de teléfono. El phreaking comenzó cuando AT&T comenzó a incluir conmutadores automáticos en sus sistemas telefónicos. Los conmutadores telefónicos de AT&T utilizaban muchos tonos, o marcación por tonos, para indicar diferentes funciones, como el marcado y la terminación de una llamada. Algunos clientes de AT&T se percataron de que, imitando un tono usando un silbato, podían explotar los conmutadores telefónicos para efectuar llamadas a larga distancia gratuitas.

A medida que los sistemas de comunicación evolucionaron, los métodos de hacking los fueron siguiendo. El wardialing se popularizó en la década de 1980 con el uso de modems de computadora. Los programas de wardialing escaneaban automáticamente los números telefónicos de un área, marcando cada uno en búsqueda de computadoras, sistemas de tablón de anuncios (bulletin board systems) y máquinas de fax. Cuando se encontraba un número de teléfono, se usaban programas de cracking de contraseñas para acceder.

El wardriving comenzó en la década de 1990 y es popular aun hoy. Con el wardriving, los usuarios acceden sin autorización a las redes por medio de access points inalámbricos. Esto se logra en usando un medio de transporte y una computadora o PDA con acceso inalámbrico. Los programas de password cracking se usan para identificarse, si es necesario, e incluso hay software para descifrar el esquema de cifrado requerido para asociarse al access point.

Otras amenazas han evolucionado desde los años 1960, incluyendo herramientas de escaneo como Nmap y SATAN, así como herramientas de hacking de administración de sistemas remotos como Back Orifice. Los profesionales de la seguridad en redes deben estar familiarizados con todas estas herramientas.

Diariamente, se transfieren billones de dólares a través de Internet, y el sustento de millones depende del comercio en Internet. Por esta razón, las leyes criminales existen para proteger a los individuos y a los bienes de las empresas. Hay numerosos casos de individuos que han tenido que enfrentarse al sistema judicial a causa de estas leyes.

El primer virus por correo electrónico, el virus Melissa, fue escrito por David Smith de Aberdeen, New Jersey. Este virus resultó en overflows de memoria en servidores de mail de Internet. David Smith fue sentenciado a 20 meses de prisión federal y una multa de 5000 dólares.

Robert Morris creó el primer gusano de Internet con 99 líneas de código. Cuando salió el gusano Morris, 10% de los sistemas de Internet se detuvieron. Robert Morris fue acusado y recibió tres años de libertad condicional, 400 horas de trabajos comunitarios y una multa de 10000 dólares.

Uno de los hackers de Internet más famosos, Kevin Mitnick, fue a prisión por cuatro años por hackear cuentas de tarjetas de crédito a principios de los años 1990.

Sea el ataque vía spam, un virus, DoS o simplemente una entrada forzosa a una cuenta, cuando la creatividad de los hackers es utilizada para fines maliciosos, generalmente

acaban en prisión, pagando grandes multas y perdiendo acceso al mismo ambiente que veneran.



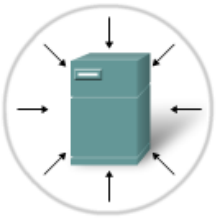
Primer Virus



Primer Gusano



Primer Spam



Primer Ataque DoS

Virus Melissa por correo electrónico – Marzo, 1999 (Debajo se muestra el correo electrónico distribuido.)

From: ******
Subject: Important Message From ******
To: (50 names from alias list)

Here is that document you asked for ... don't show anyone else ;-)

Attachment: LIST.DOC

Haga clic sobre las imágenes para ver información sobre el primer virus, gusano, spam y ataque de DoS.



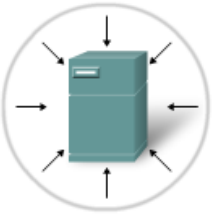
Primer Virus



Primer Gusano



Primer Spam



Primer Ataque DoS

El gusano Morris de Internet

Todos los eventos que siguen ocurrieron en la noche del 2 de noviembre de 1988.
6:00 PM - Aproximadamente a esta hora se lanza el gusano.
8:49 PM - El gusano infecta una VAX 8600 en la Universidad de Utah (cs.utah.edu).
9:09 PM - El gusano inicia el primero de sus ataques para infectar a otras comptadoras a partir de la VAX.
9:21 PM - El promedio de carga del sistema llega a 5. (El promedio de carga mide cuánto está trabajando el sistema. A las 9:30 de la noche, el promedio de carga de la VAX generalmente era 1. Cualquier promedio de carga más alto que 5 causa demoras en el procesamiento de datos.)
9:41 PM - El promedio de carga llega a 7.

Haga clic sobre las imágenes para ver información sobre el primer virus, gusano, spam y ataque de DoS.



Primer spam de ARPAnet – 1978 (Debajo se muestra el mensaje de spam distribuido por ARPAnet.)

To: Everyone
From:
Subject: Presentation Today

DIGITAL WILL BE GIVING A PRODUCT PRESENTATION OF THE NEWEST MEMBERS OF THE DECSYSTEM-20 FAMILY; THE DECSYSTEM-2020, 2020T, 2060, AND 2060T. THE DECSYSTEM-20 FAMILY OF COMPUTERS HAS EVOLVED FROM THE TENEX OPERATING SYSTEM AND THE DECSYSTEM-10 COMPUTER ARCHITECTURE. BOTH THE DECSYSTEM-2060T AND 2020T OFFER FULL ARPANET SUPPORT UNDER THE TOPS-20 OPERATING SYSTEM. THE

Haga clic sobre las imágenes para ver información sobre el primer virus, gusano, spam y ataque de DoS.



Ataque DoS Mafiaboy – Febrero de 2000 (Debajo se muestra un artículo describiendo la sentencia de mafiaboy poco tiempo después de que se detuvo el ataque de DoS.)

'Mafiaboy' Sentenced to 8 Months
Wired News Report 09.13.01

"Mafiaboy," the Canadian teenager who launched a denial of service attack that paralyzed many of the Internet's major sites for one week in February 2000, will be spending the next eight months in a youth detention center.

Judge Gilles Ouellet, who presided over the trial in Quebec's Youth Court, handed down the ruling on

Haga clic sobre las imágenes para ver información sobre el primer virus, gusano, spam y ataque de DoS.

Como resultado de los exploits de los hackers, la sofisticación de sus herramientas y la legislación gubernamental, las soluciones de seguridad se desarrollaron rápidamente en los años 1990. A fines de esa década se habían desarrollado muchas soluciones sofisticadas para la seguridad de las redes para que las organizaciones desplegaran estratégicamente en sus redes. Con estas soluciones llegaron nuevas oportunidades de trabajo y mejor compensación en el campo de la seguridad en redes.

Los ingresos anuales del profesional de la seguridad en redes están entre los mejores de las carreras profesionales en tecnologías por la profundidad y amplitud de conocimientos requeridos. Los profesionales de la seguridad en redes deben actualizar constanteente sus habilidades para mantenerse por encima de las últimas amenazas. El desafío de ganar y mantener el conocimiento necesario generalmente se traduce en una escasez de profesionales de la seguridad en redes.

Los profesionales de la seguridad en redes son responsables de mantener la seguridad de los datos de una organización y garantizar la integridad y confidencialidad de la información. Un profesional de la seguridad en redes puede ser responsable de montar firewalls y sistemas de prevención de intrusos, así como también de asegurar el cifrado de los datos de la compañía. Implementar esquemas de autenticación dentro de una empresa también es una tarea importante. El trabajo implica mantener historiales detallados de actividad sospechosa en la red para usarla para reprender y procesar infractores. Como un profesional de la seguridad en redes, también es importante mantener una familiaridad con las organizaciones de seguridad en redes. Estas organizaciones generalmente tienen la información más actualizada sobre amenazas y vulnerabilidades.



Ingeniero de seguridad en redes



Analista de seguridad de la información



Especialista de seguridad en redes



Administrador de seguridad en redes



Arquitecto de seguridad en redes



Ingeniero de sistemas

1.1.3 Organizaciones de seguridad en redes.

Los profesionales de la seguridad en redes deben colaborar con colegas profesionales más frecuentemente que en la mayoría de las otras profesiones. Esto incluye asistir a workshops y conferencias que generalmente están asociadas con, patrocinadas u organizadas por organizaciones tecnológicas locales, nacionales o internacionales.

Tres de las organizaciones de seguridad en redes mejor establecidas son:

SysAdmin, Audit, Network, Security (SANS) Institute
Computer Emergency Response Team (CERT)

International Information Systems Security Certification Consortium ((ISC)2 se dice "I-S-C-squared" en inglés)

Existen varias otras organizaciones de seguridad en redes que también son importantes para los profesionales de la seguridad en redes. InfoSysSec es una organización de seguridad en redes que aloja un portal de novedades de seguridad, proporcionando las últimas novedades en cuanto a alertas, exploits y vulnerabilidades. La Mitre Corporation mantiene una lista de las vulnerabilidades y exposiciones comunes (CVE), utilizada por organizaciones de seguridad de redes de gran prestigio. FIRST es una organización de seguridad que reúne una variedad de equipos de respuesta a incidentes de seguridad de organizaciones gubernamentales, comerciales y educativas, para fomentar la cooperación y coordinación en el intercambio de información, la prevención de incidentes y la rápida reacción. Finalmente, el Center for Internet Security (CIS) es un emprendimiento sin fines de lucro que desarrolla puntos de referencia en la configuración de la seguridad a través de consensos globales para reducir el riesgo de interrupciones en los negocios y el comercio electrónico.



SANS se estableció en 1989 como una organización cooperativa de investigación y educación. El objetivo de SANS es la capacitación y certificación en seguridad de la información. SANS desarrolla documentos de investigación sobre varios aspectos de la seguridad de la información.

Un gran rango de individuos, desde auditores y administradores de red hasta directores de seguridad de la información comparten lecciones aprendidas y soluciones a varios desafíos. En el núcleo de SANS están los practicantes de la seguridad en varias organizaciones globales, desde empresas hasta universidades, trabajando juntos para ayudar a toda la comunidad de la seguridad de la información.

Los recursos de SANS son mayormente accesibles bajo solicitud. Esto incluye el popular Internet Storm Center, el sistema de advertencias tempranas de Internet; NewsBites, la publicación semanal de noticias; @RISK, la publicación semanal de vulnerabilidades; alertas de seguridad inmediatas y más de 1200 papers de investigación original que han ganado premios.

SANS desarrolla cursos de seguridad que pueden ser tomados para prepararse para la Certificación Global de Seguridad de la Información (Global Information Assurance Certification - GIAC) en auditoría, administración, operaciones, asuntos legales, administración de seguridad y seguridad de software. GIAC certifica las habilidades de los profesionales de la seguridad, que van desde la seguridad de la información de nivel de entrada hasta áreas de avanzada como auditoría, detección de intrusos, manejo de incidentes, firewalls y protección de perímetro, peritaje de datos, técnicas de hacking, seguridad de sistemas operativos UNIX y Windows y codificación de aplicaciones y software segura.



El CERT es parte del Software Engineering Institute (SEI) en Carnegie Mellon University, financiado por el gobierno de los Estados Unidos. El CERT fue creado para trabajar con la comunidad de Internet para detectar y resolver incidentes de seguridad en las computadoras. El gusano Morris motivó la formación del CERT bajo la directiva de la Defense Advanced Research Projects Agency (DARPA). El CERT Coordination Center (CERT/CC) tiene por objetivo coordinar la comunicación entre los expertos durante emergencias de seguridad para ayudar a prevenir futuros accidentes.

El CERT responde a incidentes de seguridad serios y analiza las vulnerabilidades de los productos. El CERT trabaja para administrar los cambios relacionados con técnicas progresivas de intrusión y con las dificultades en detectar ataques y atrapar a los atacantes. El CERT desarrolla y pomueve el uso de prácticas de administración de sistemas y tecnologías apropiadas para resistir ataques en sistemas en red, para limitar el daño y para garantizar la continuidad de los servicios.

El CERT se ocupa de cinco áreas: aseguramiento del software, sistemas seguros, seguridad en las organizaciones, respuesta coordinada y educación y capacitación.

El CERT difunde información publicando artículos, reportes técnicos y de investigación y papers en una variedad de temas de seguridad. El CERT trabaja con los medios de noticias para crear conciencia sobre los riesgos de Internet y los pasos que los usuarios pueden tomar para protegerse. El CERT trabaja on otras organizaciones tecnológicas importantes como FIRST e IETF, para incrementar el compromiso con la seguridad y la robustez. EL CERT también aconseja a las organizaciones del gobierno de los Estados Unidos, como el National Threat Assessment Center, el National Security Council, y el Homeland Security Council.



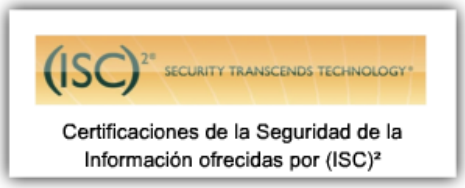
(ISC)2 provee productos y servicios educativos independientes del proveedor en más de 135 países. Su membresía incluye 60000 profesionales certificados de la industria en todo el mundo.

La misión de (ISC)2 es hacer del cibermundo un lugar seguro elevando la seguridad de la información al dominio público y soportando y desarrollando profesionales de la seguridad de la información en todo el mundo.

(ISC)2 desarrolla el (ISC)2 Common Body of Knowledge (CBK). El CBK define los estándares globales de la industria, sirviendo como un marco común de términos y principios sobre los cuales están basadas las credenciales (ISC)2. El CBK permite a los profesionales de todo el mundo discutir, debatir y resolver temas pertinentes al campo.

(ISC)2 es reconocido universalmente por sus cuatro certificaciones de seguridad de la información, incluyendo una de las certificaciones más populares en la profesión de seguridad en redes, el Certified Information Systems Security Professional (CISSP). Estas credenciales ayudan a garantizar que los empleadores con empleados certificados mantengan la seguridad de los activos e infraestructuras de información.

(ISC)2 promueve la excelencia al manejar amenazas de seguridad a través de sus programas de capacitación y certificación. Como miembros, las personas tienen acceso a oportunidades de socialización e información actual de la industria únicas a esta red de profesionales certificados de la seguridad de la información.

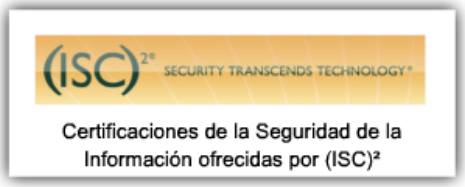


Systems Security Certified Practitioner (SSCP)

Certification and Accreditation Professional (CAP)

Certified Secure Software Lifecycle Professional (CSSLP)

Certified Information Systems Security Professional (CISSP)



Systems Security Certified Practitioner (SSCP)

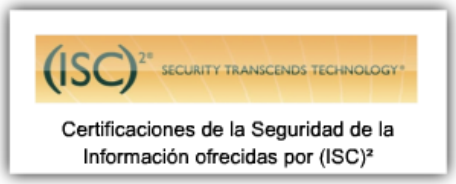
Certification and Accreditation Professional (CAP)

Certified Secure Software Lifecycle Professional (CSSLP)

Certified Information Systems Security Professional (CISSP)

Systems Security Certified Practitioner (SSCP)

Solo está disponible para candidatos calificados que suscriban al código de ética de (ISC)² y pasen el examen de certificación SSCP basado en el SSCP Common Body of Knowledge (CBK) relevante. Los candidatos también deben poder probar por lo menos un año de experiencia en uno de los siete dominios que comprenden la certificación SSCP:



Systems Security Certified Practitioner (SSCP)

Certification and Accreditation Professional (CAP)

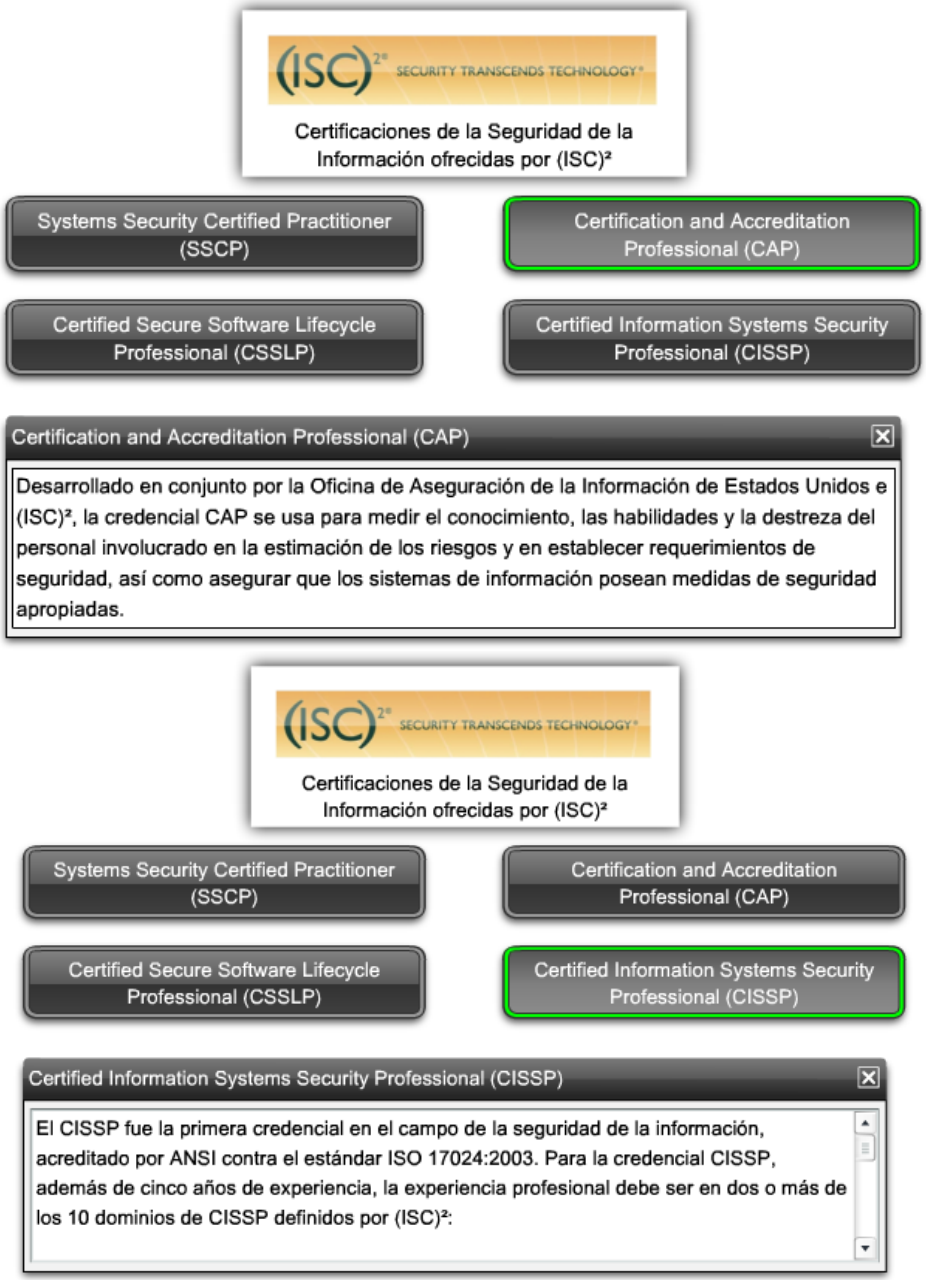
Certified Secure Software Lifecycle Professional (CSSLP)

Certified Information Systems Security Professional (CISSP)

Certified Secure Software Lifecycle Professional (CSSLP)

La certificación más reciente de (ISC)², es la única certificación en la industria que asegura que la seguridad está siendo considerada en todo el ciclo de vida del software. Se enfoca en siete dominios:

- Conceptos de software seguro



Además de los sitios web de las organizaciones de seguridad, una de las herramientas más útiles para los profesionales de la seguridad en redes es la de los feeds Really Simple Syndication (RSS).

RSS es una familia de formatos basados en XML utilizados para publicar información frecuentemente actualizada, como entradas de blogs, noticias, audio y video. RSS utiliza un formato estandarizado. Un canal RSS incluye texto completo o resumido y metadatos, como fechas de publicación y autorías.

RSS beneficia a los profesionales que deseen suscribirse a actualizaciones que lleguen en tiempo y forma de sitios web particulares o agregar canales de varios sitios a un solo lugar. Los canales RSS pueden ser leidos utilizando un lector RSS basado en web,

típicamente incrustado en un navegador web. El software del lector RSS revisa regularmente los canales a los que el usuario está suscripto, buscando nuevas actualizaciones, y provee una interfaz para monitorear y leer los canales. Al utilizar RSS, el profesional de la seguridad en redes puede adquirir información actualizada diariamente y juntar información de amenazas en tiempo real para repasar en cualquier otro momento.

Por ejemplo, la página web US-CERT Current Activity es un resumen actualizado regularmente que incluye los tipos de incidentes de seguridad más frecuentes y de mayor impacto que se reportan al US-CERT. Se encuentra disponible un canal RSS de solo texto en http://www.us-cert.gov/current/index.rdf. Este canal reporta a toda hora del día o la noche, con información relacionada con consejos de seguridad, estafas por correo electrónico, vulnerabilidades en el resguardo de datos, malware que se propaga a través de redes sociales y otras amenazas potenciales.



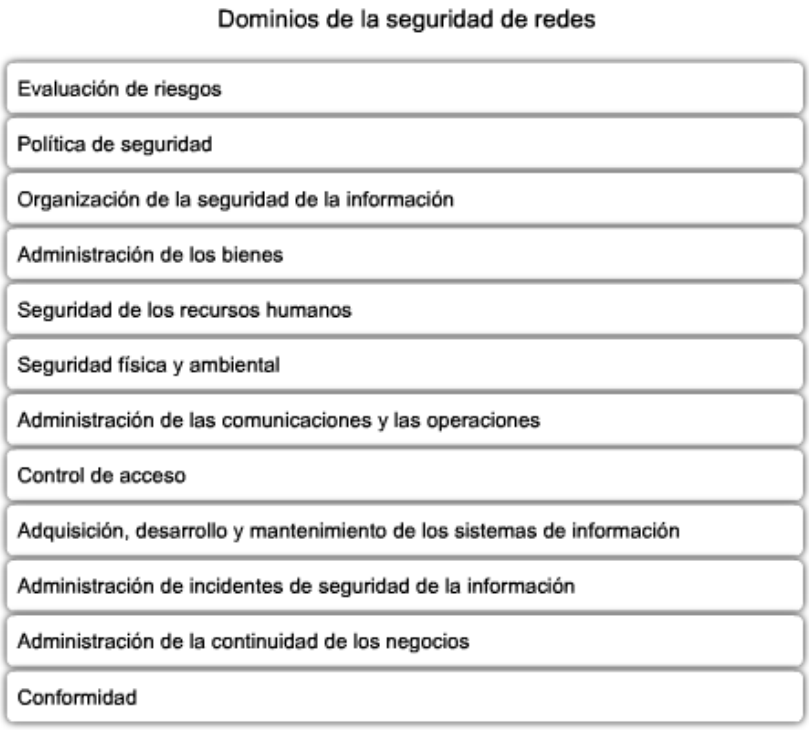
1.1.4 Dominios de la seguridad en redes

Es vital que los profesionales de la seguridad en redes entiendan los motivos de la misma y se familiaricen con las organizaciones dedicadas a ésta. También es importante entender los varios dominios de la seguridad en redes. Los dominios proveen un marco organizado para facilitar el aprendizaje sobre la seguridad en redes.

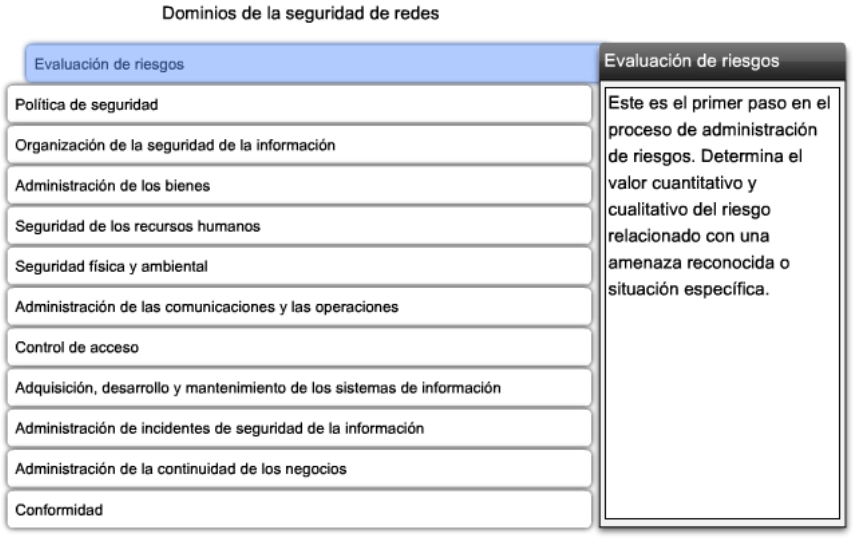
Existen 12 dominios de seguridad en redes especificados por la International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC). Descriptos por ISO/IEC 27002, estos 12 dominios sirven para organizar a alto nivel el vasto reino de la información bajo el paraguas de la seguridad en redes. Estos

dominios tienen algunos paralelismos significativos con los dominios definidos por la certificación CISSP.

Los 12 dominios están diseñados para servir como base común para desarrollar los estándares de seguridad en las organizaciones y las práctidas de admiinistración de seguridad efectiva, así como también para ayudar a construir una confianza en las actividades que toman lugar dentro de la organización.



Pase el cursor por encima de cada dominio de seguridad de la red para más información.



Pase el cursor por encima de cada dominio de seguridad de la red para más información.

Dominios de la seguridad de redes

- Evaluación de riesgos
- Política de seguridad
- Organización de la seguridad de la información
- Administración de los bienes
- Seguridad de los recursos humanos
- Seguridad física y ambiental
- Administración de las comunicaciones y las operaciones
- Control de acceso
- Adquisición, desarrollo y mantenimiento de los sistemas de información
- Administración de incidentes de seguridad de la información
- Administración de la continuidad de los negocios
- Conformidad

Política de seguridad

Es un documento que trata las restricciones y comportamientos de los miembros de una organización y generalmente especifica cómo se puede acceder a los datos y quién puede acceder a qué datos.

Pase el cursor por encima de cada dominio de seguridad de la red para más información.

Dominios de la seguridad de redes

- Evaluación de riesgos
- Política de seguridad
- Organización de la seguridad de la información
- Administración de los bienes
- Seguridad de los recursos humanos
- Seguridad física y ambiental
- Administración de las comunicaciones y las operaciones
- Control de acceso
- Adquisición, desarrollo y mantenimiento de los sistemas de información
- Administración de incidentes de seguridad de la información
- Administración de la continuidad de los negocios
- Conformidad

Organización de la seguridad de la información

Este es el modelo de gobierno establecido por una organización para la seguridad de la información.

Pase el cursor por encima de cada dominio de seguridad de la red para más información.

Dominios de la seguridad de redes

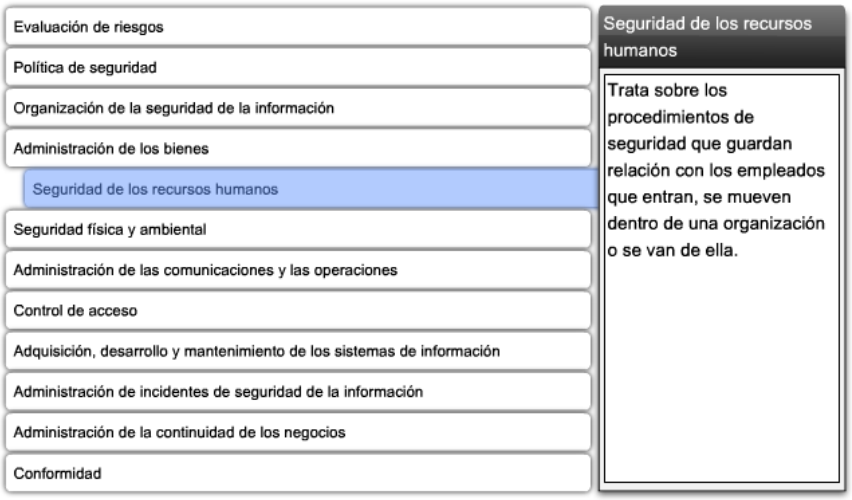
- Evaluación de riesgos
- Política de seguridad
- Organización de la seguridad de la información
- Administración de los bienes
- Seguridad de los recursos humanos
- Seguridad física y ambiental
- Administración de las comunicaciones y las operaciones
- Control de acceso
- Adquisición, desarrollo y mantenimiento de los sistemas de información
- Administración de incidentes de seguridad de la información
- Administración de la continuidad de los negocios
- Conformidad

Administración de bienes

Es un inventario y esquema de clasificación para los bienes de información.

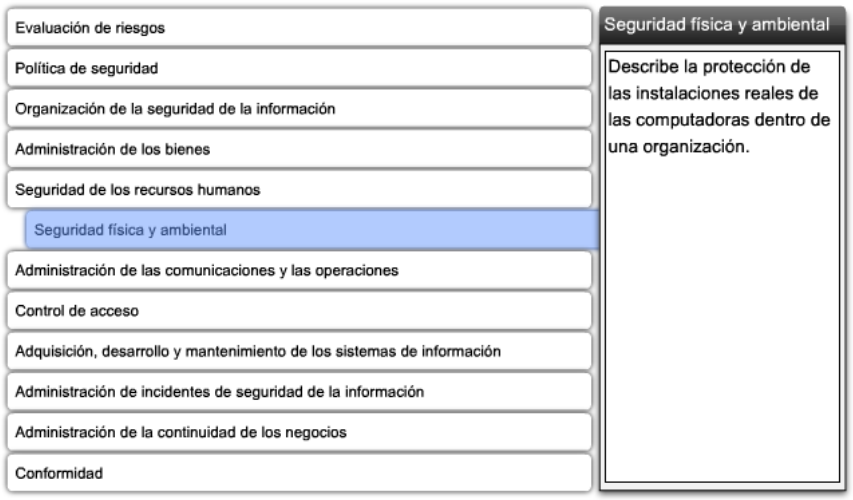
Pase el cursor por encima de cada dominio de seguridad de la red para más información.

Dominios de la seguridad de redes



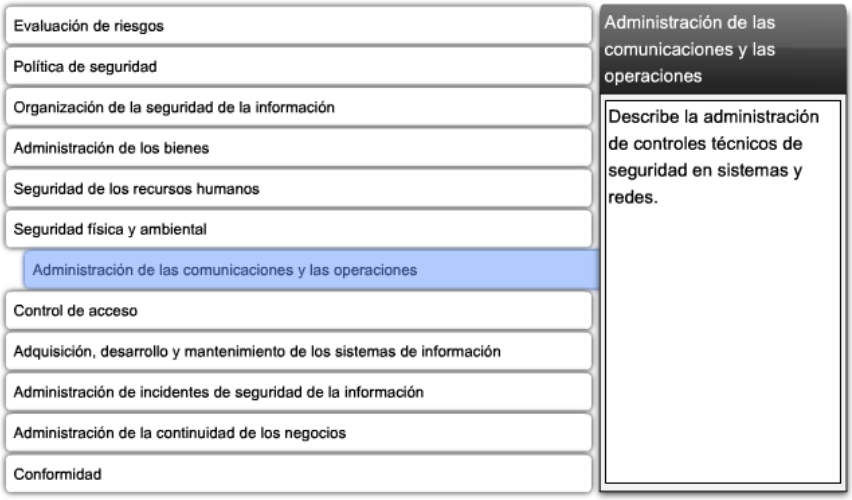
Pase el cursor por encima de cada dominio de seguridad de la red para más información.

Dominios de la seguridad de redes



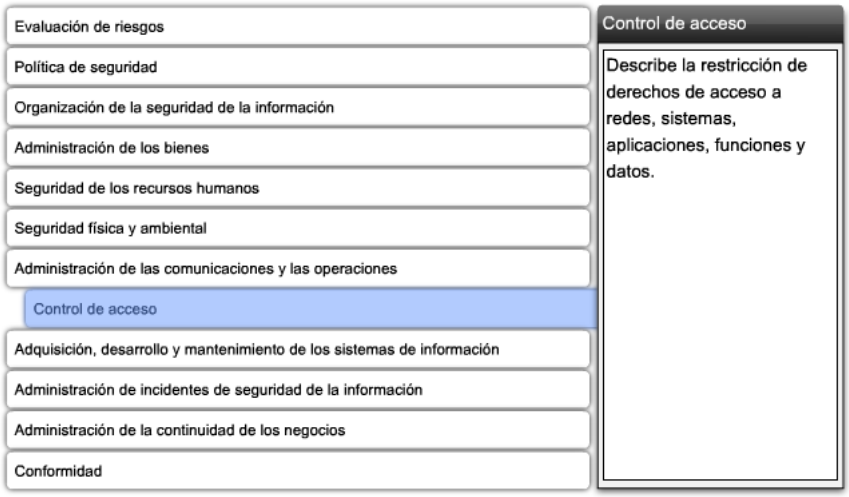
Pase el cursor por encima de cada dominio de seguridad de la red para más información.

Dominios de la seguridad de redes



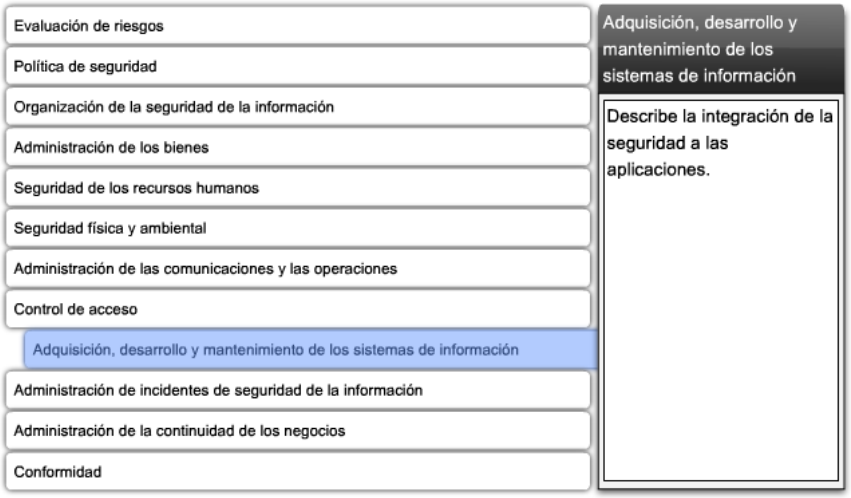
Pase el cursor por encima de cada dominio de seguridad de la red para más información.

Dominios de la seguridad de redes



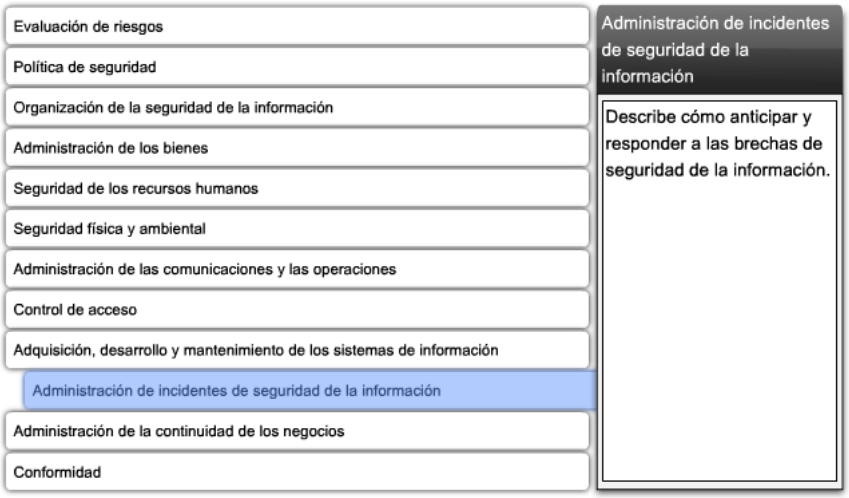
Pase el cursor por encima de cada dominio de seguridad de la red para más información.

Dominios de la seguridad de redes

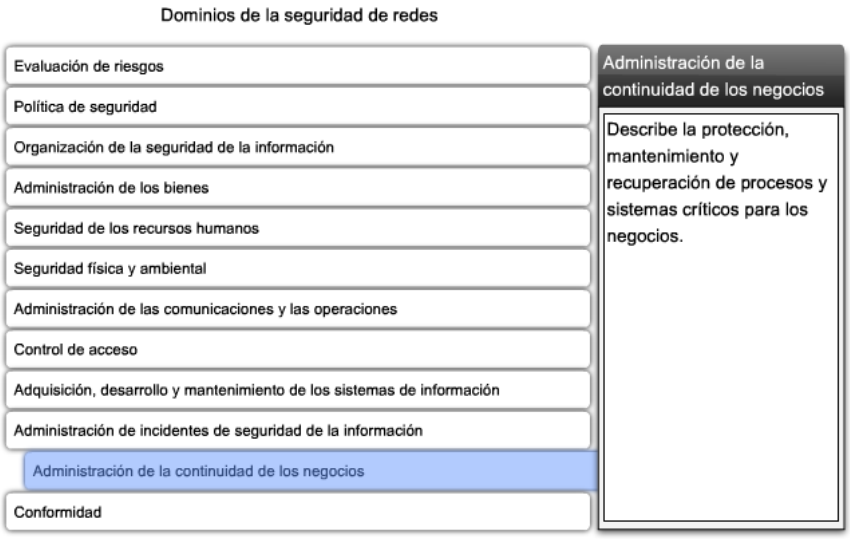


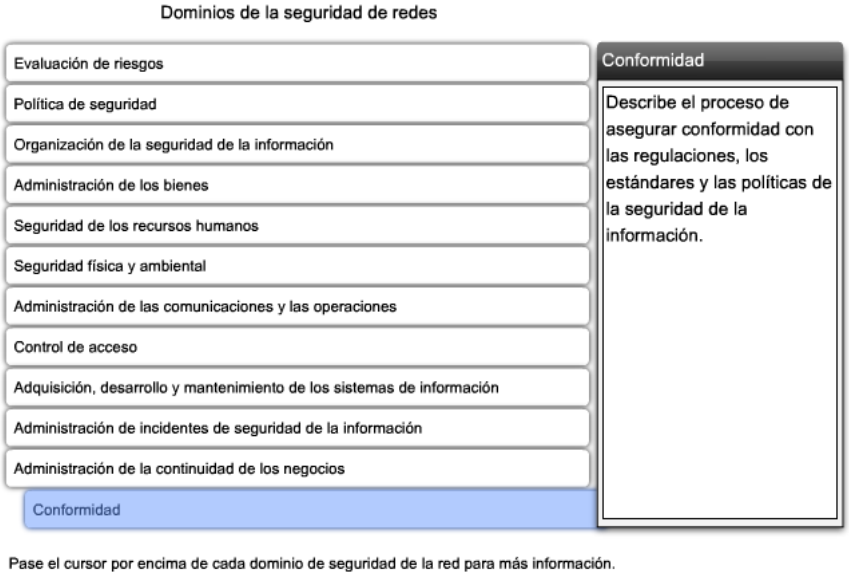
Pase el cursor por encima de cada dominio de seguridad de la red para más información.

Dominios de la seguridad de redes



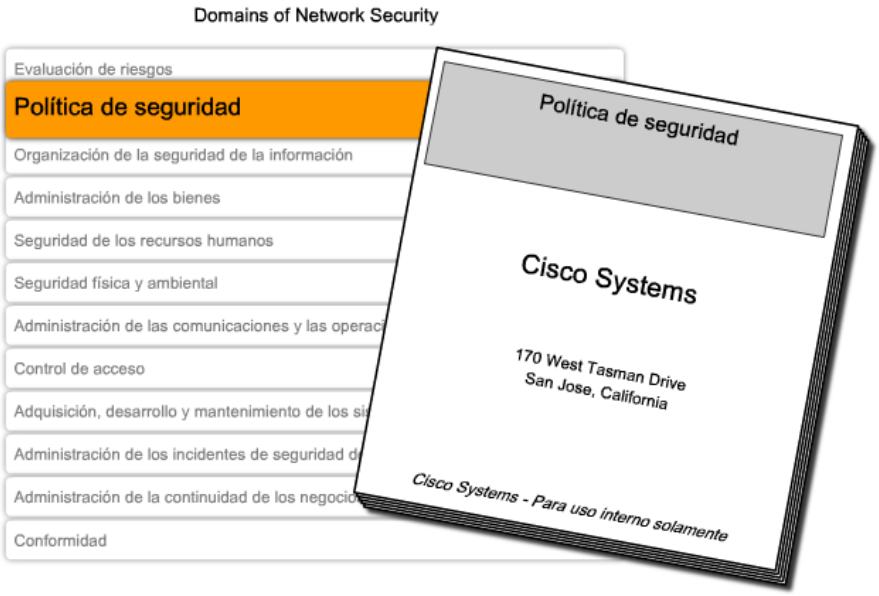
Pase el cursor por encima de cada dominio de seguridad de la red para más información.





Los 12 dominios de la seguridad en redes proveen una separación conveniente para los elementos de la seguridad en redes. Aunque no es importante memorizarlos, es importante estar al tanto de su existencia y declaración formal de parte de la ISO. Estos 12 dominios sirven como referencia útil para avanzar en el trabajo como profesional de la seguridad en redes.

Uno de los dominios más importantes es el de las políticas de seguridad. Una política de seguridad es una declaración formal de las reglas a las cuales deberán atender las personas que tienen acceso a los bienes tecnológicos y de información de una organización. La conceptualización, el desarrollo y la aplicación de una política de seguridad tienen un rol significativo en mantener a la organización segura. Es responsabilidad del profesional de la seguridad en redes hacer cumplir las políticas de seguridad en todos los aspectos de las operaciones de negocios en la organización.



1.1.5 Políticas de seguridad en redes

La política de seguridad en redes es un documento amplio diseñado para ser claramente aplicable a las operaciones de una organización. La política se utiliza para asistir en el diseño de la red, transmitir principios de seguridad y facilitar el despliegue de la red.

La política de seguridad en redes traza las reglas de acceso a la red, determina cómo se harán cumplir las políticas y describe la arquitectura básica del ambiente básico de seguridad de la información de la empresa. El documento generalmente consta de varias páginas. Por su amplitud de cobertura e impacto, generalmente es un comité el que lo compila. Es un documento complejo que está diseñado para gobernar temas como acceso a los datos, navegación en la web, uso de las contraseñas, criptografía y adjuntos de correo electrónico.

Una política de seguridad deberá mantener a los usuarios malintencionados lejos y tener control sobre usuarios potencialmente peligrosos. Antes de crear una política debe entenderse qué servicios están disponibles a cuáles usuarios. La política de seguridad de red establece una jerarquía de permisos de acceso y da a los empleados solo el acceso mínimo necesario para realizar sus tareas.

La política de seguridad de la red establece cuáles bienes deben ser protegidos y da pautas sobre cómo deben ser protegidos. Esto será luego usado para determinar los dispositivos de seguridad y las estrategias y procedimientos de mitigación que deberán ser implementados en la red.



Una Red Autodefensiva de Cisco (Cisco Self-Defending Network - SDN) utiliza la red para identificar, prevenir y adaptarse a las amenazas. A diferencia de estrategias de solución puntuales, en las cuales se compran los productos individualmente sin considereación de cuáles productos trabajan mejor juntos, un enfoque basado en la red es un enfoque estratégico que está a la altura de los desafíos actuales y evoluciona para cubrir las nuevas necesidades de seguridad.

Un SDN de Cisco comienza con una plataforma fuerte, segura y flexible sobre la cual se construye la solución de seguridad. Una topología SDN de Cisco incluye un Administrador de Seguridad de Cisco (Cisco Security Manager), un Sistema de Respuesta, Análisis y Monitoreo (Monitoring, Analysis, and Response System - MARS), uno o más IPS, uno o más firewalls, varios routers y concentradores VPN. Algunos de estos pueden aparecer como blades en un switch Catalyst 6500 o como módulos en un Router de Servicios Integrados (Integrated Services Router - ISR), quizás incluso como software instalado en servidores o como dispositivos autónomos.

El Portfolio de Seguridad Integrado de Cisco ha sido diseñado para satisfacer los requerimientos y diversos modelos de despliegue de cualquier red y cualquier ambiente. Hay muchos productos disponibles para atender a estas necesidades.

Red Autodefensiva de Cisco

Servicios:

Visibilidad y protección 360º:
Proporciona una defensa de la red global y proactiva

Control simplificado:
Seguimiento de política y manejo de amenazas en toda la red

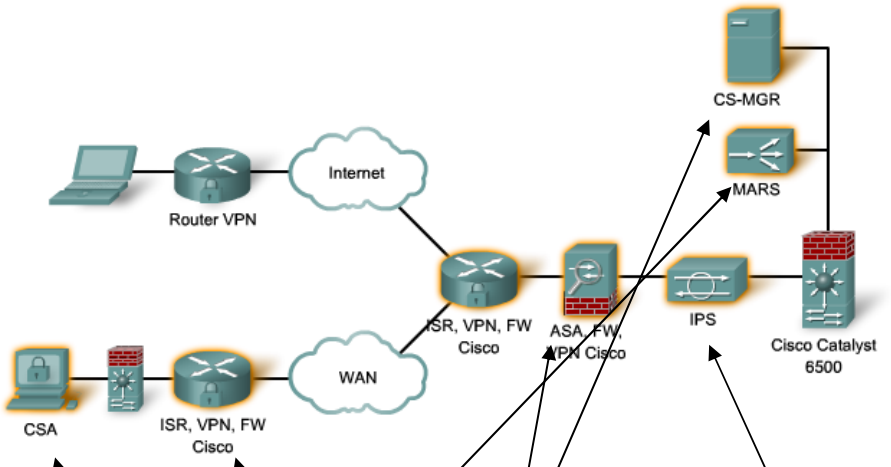
Elasticidad de los negocios:
Asegura las operaciones de la empresa



Servicios | Topología

Haga clic en los botones para ver el contenido asociado.

Red Autodefensiva de Cisco



Servicios | Topología

Pase el cursor sobre los íconos resaltados para ver más información.

CSA	ISR, VPN, FW de Cisco	ASA, FW, VPN Cisco	IPS
El dispositivo NAC de Cisco y el Agente de Seguridad de Cisco proveen seguridad de punto final.	El firewall IOS de Cisco y el software VPN proporcionan uso de la red privada, control de acceso y filtrado.	El software de firewall IOS de Cisco y las Cisco Adaptive Security Appliances filtran el tráfico.	El IPS Cisco provee inspección de tráfico y mitigación de amenazas.

MARS	CS-MGR
El Sistema de Respuesta, Análisis y Monitoreo de Seguridad de Cisco (MARS) provee manejo de las amenazas.	El Administrador de Seguridad de Cisco provee administración basada en la política.

La mayoría de los clientes no adopta todos los componentes del SDN de Cisco de una sola vez. Por esta razón el SDN de Cisco proporciona productos que pueden ser desplegados independientemente y soluciones que pueden enlazar estos productos entre ellos a medida que aumenta la confianza en cada producto y subsistema.

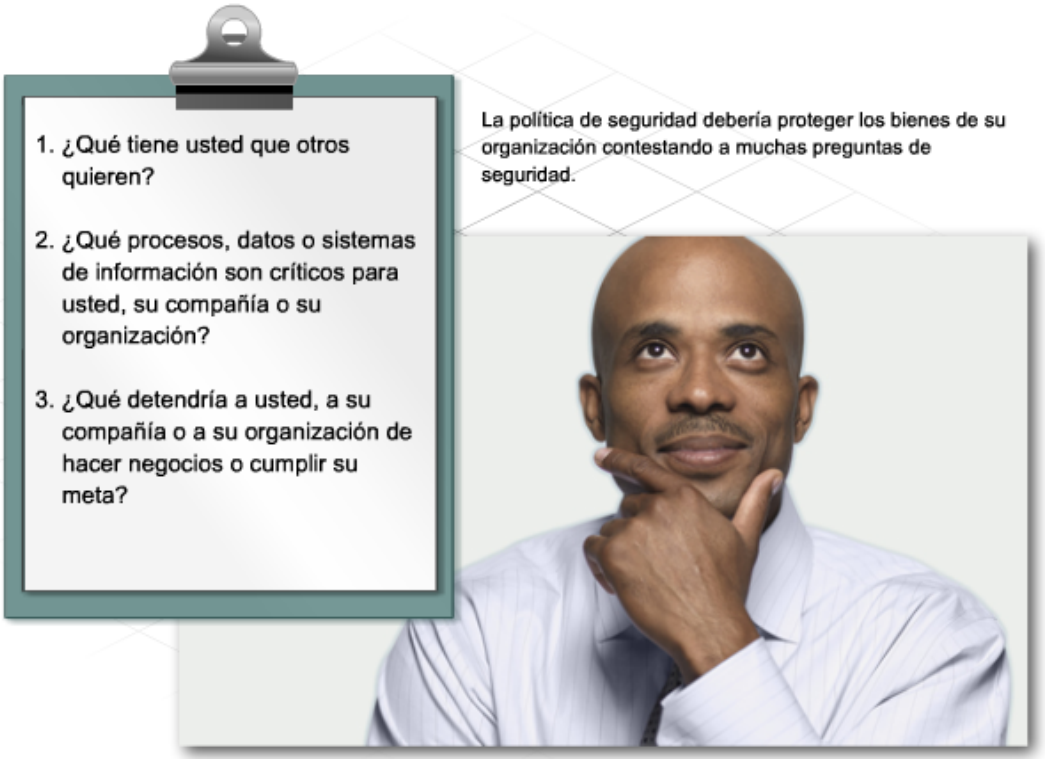
Los elementos de un enfoque de SDN de Cisco pueden integrarse a una política de seguridad de redes. Al potenciar el enfoque SDN de Cisco creando y enmendando la política de seguridad, puede contribuirse a crear una estructura jerárquica en el documento.



Aunque la política de seguridad debería ser exhaustiva, también debe ser lo suficientemente suscinta como para ser utilizable por los profesionales de la tecnología en la organización.

Uno de los pasos más importantes al crear una política es el de indentificar los bienes críticos. Estos pueden incluir bases de datos, aplicaciones vitales, información de clientes y empleados, información comercial clasificada, discos compartidos, servidores de correo electrónico y servidores web.

La política de seguridad es un conjunto de objetivos para la compañía, reglas de comportamiento para los usuarios y administradores y requerimientos para sistemas y la administración que asegure colectivamente la seguridad de los sistemas informáticos y la red de una organización. Es un "documento vivo" en el sentido de que el documento nunca está terminado y continuamente se actualiza a medida que cambian los requerimientos de tecnología, negocios y empleados.



1.2. Virus, gusanos y troyanos

1.2.1 Virus

Las principales vulnerabilidades de las computadoras de los usuarios finales son los ataques de virus, gusanos y troyanos:

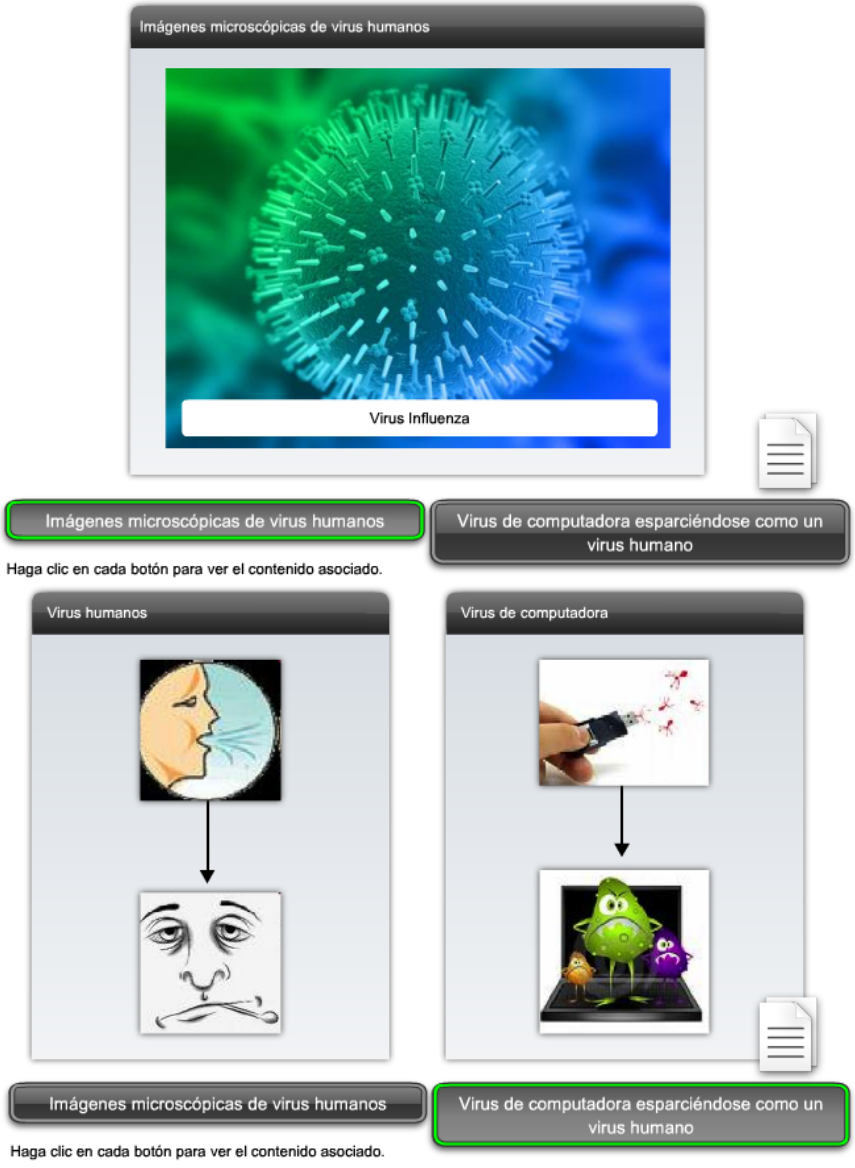
Un virus es un software malicioso que se adjunta a otro programa para ejecutar una función indeseada específica en una computadora.
Un gusano ejecuta código arbitrario e instala copias de sí mismo en la memoria de la computadora infectada, que luego infecta a otros hosts.
Un troyano es una aplicación escrita para parecerse a otra cosa. Cuando se descarga y ejecuta un troyano, ataca a la computadora del usuario final desde dentro.

Tradicionalmente, el término virus se refiere a un organismo infeccioso que requiere de una célula huésped para crecer y multiplicarse. Un estudiande de la Universidad de California del Sur llamado Frederick Cohen sugirió el término "virus de computadora" en 1983. Un virus de computadora, al que llamaremos virus en el resto de este curso, es un programa que puede copiarse a sí mismo e infectar una computadora sin el conocimiento del usuario.

Un virus es código malicioso que se adjunta a archivos ejecutables o programas legítimos. La mayoría de los virus requiere una activación de parte del usuario final y puede permanecer inactivo por largos períodos de tiempo y luego activarse en una fecha u hora específica. Un virus simple puede instalarse en la primera línea de código en un archivo ejecutable. Una vez activado, el virus puede buscar en el disco otros ejecutables para infectar todos los archivos que aún no hayan sido infectados. Los virus pueden ser inofensivos, como aquellos que muestran una imagen en la pantalla, pero también

pueden ser destructivos, como aquellos que modifican o eliminan los archivos del disco rígido. Los virus también pueden ser programados para mutar con el propósito de evitar su detección.

En años anteriores, los virus generalmente eran diseminados a través de floppy disks y módems. Hoy en día, la mayoría de los virus se pasan a través de pendrives, CDs, DVDs, redes compartidas o correo electrónico. Los virus por correo electrónico son actualmente el tipo más común de virus.



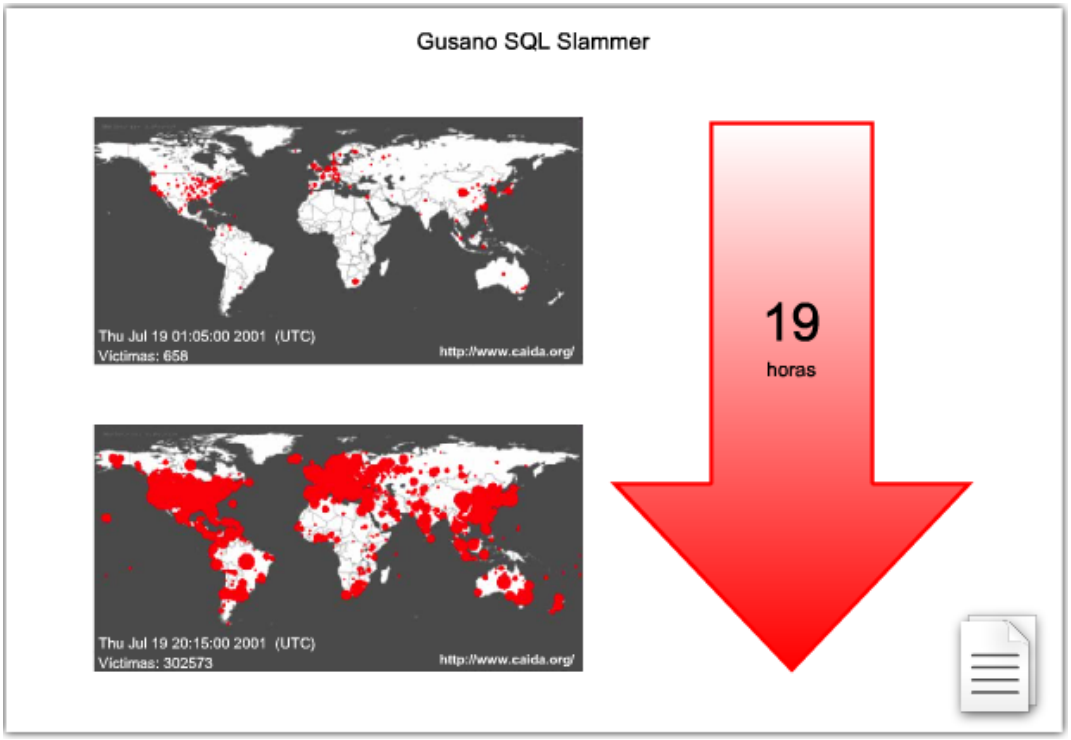
1.2.2 Gusanos

Gusanos

Los gusanos son un tipo de código hostil particularmente peligroso. Se multiplican explotando vulnerabilidades en las redes independientemente. Los gusanos generalmente hacen que las redes operen más lentamente.

Mientras que los virus requieren un programa huésped para ejecutarse, los gusanos pueden ejecutarse solos. No requieren la participación del usuario y pueden diseminarse muy rápidamente en la red.

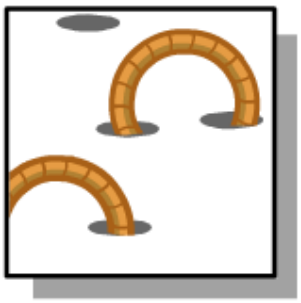
Los gusanos son responsables de algunos de los ataques más devastadores de Internet. Por ejemplo, el SQL Slammer Worm de enero de 2003 hizo que el tráfico global de Internet fuera más lento como resultado de un ataque de Denegación de Servicio. Más de 250,000 hosts fueron afectados en los primeros 30 minutos. El gusano explotó una vulnerabilidad de desbordamiento de buffer en el servidor SQL de Microsoft. Se había lanzado un parche para esta vulnerabilidad a mediados de 2002, por lo que los servidores que fueron afectados eran aquellos que no habían descargado la actualización que contenía el parche. Este es un buen ejemplo de por qué es tan importante que la política de seguridad de la organización exija actualizaciones y parches oportunos para los sistemas operativos y aplicaciones.



A pesar de las técnicas de mitigación que han surgido en los últimos años, los gusanos han continuado en su evolución gracias a Internet, y todavía representan una amenaza. Aunque los gusanos se han vuelto sofisticados con el tiempo, todavía tienden a estar basados en la explotación de vulnerabilidades en las aplicaciones de software. La mayoría de los ataques de gusanos tiene tres componentes principales:

Una vulnerabilidad habilitante - Los gusanos se instalan utilizando un mecanismo de explotación (adjunto de correo electrónico, archivo ejecutable, troyano) en un sistema vulnerable.
Sistema de propagación- Luego de acceder a un dispositivo, el gusano se mmultiplica y localiza nuevos objetivos.
Carga - Cualquier código malicioso que resulta en alguna acción. La mayoría de las veces esto se usa para crear una puerta trasera en el host infectado.

Los gusanos son programas autocontenidos que atacan a un sistema para explotar una vulnerabilidad conocida. Luego de una explotación exitosa, el gusano se copia del host atacante al sistema recientemente explotado y el ciclo vuelve a comenzar.



Componentes de los gusanos

- Vulnerabilidad habilitante
- Mecanismos de propagación
- Carga

Al explorar los principales ataques de gusanos y virus de los últimos 20 años se vuelve evidente que las varias fases de los métodos de ataque empleados por los hackers son en general similares. Hay cinco fases básicas de ataque, ya sea un virus o un gusano el que se contagie.

Fase de exploración - Se identifican los objetivos vulnerables. Se buscan computadoras que puedan ser explotadas. Se usan escaneos de ping de Protocolo de Mensajes de Control de Internet (Internet Control Message Protocol - ICMP) para hacer mapas de la red. Luego la aplicación escanea e identifica sistemas operativos y software vulnerable. Los hackers pueden obtener contraseñas utilizando ingenería social, ataques de diccionario, ataques de fuera bruta o sniffing de redes.
Fase de penetración - Se transfiere código de explotación al objetivo vulnerable. Se busca ejecutar el código de explotación a través de un vector de ataque como un desbordamiento de buffer, vulnerabilidades de ActiveX o Interfaz de Entrada Común (Common Gateway Interface - CGI) o un virus de correo electrónico.
Fase de persistencia - Luego de que el ataque haya sido exitosamente lanzado en la memoria, el código trata de persistir en el sistema víctima. El objetivo es asegurar que el código atacante esté ejecutándose y disponible al atacante incluso si el sistema se reinicia. Esto se logra modificando archivos del sistema, efectuando cambios en el registro e instalando nuevo código.
Fase de propagación - El atacante intenta extender el ataque a otros objetivos buscando máquinas vecinas vulnerables. Los vectores de propagación incluyen mandar copias del

ataque por correo electrónico a otros sistemas, subir archivos a otros sistemas utilizando servicios de FTP o de compartición de archivos, conexiones web activas y transferencias de archivos a través del Internet Relay Chat (IRC).
Fase de paralización - Se hace daño real al sistema. Se pueden borar archivos, el sistema puede colapsar, se puede robar información y se pueden lanzar ataques distribuidos de DoS (DDoS).

Las cinco fases básicas de ataque permiten a los expertos de seguridad describir a los virus y gusanos convenientemente de acuerdo a su mecanismo de implementación particular para cada fase. Esto facilita la categorización de los virus y los gusanos.

Los virus y los gusanos son dos métodos de ataque. Otro método es el troyano, que impulsa a los virus o gusanos con el elemento agregado de hacerse pasar por un programa benigno.

Virus y gusanos – Comparación de explotaciones (~20 años)

	Morris 1988	Love Bug 2000	Code Red 2001	Slammer 2003	MyDoom 2004	Zotob 2005	MS RPC DNS 0day 2007
Exploración	Escanea por finger	N/A	Escanea por IIS	N/A	N/A	Escanea por servicios de directorio MS	Escanea por solicitud Mapper de punto final
Penetración	Causa desbordamiento de buffer en fingerd	Llega como adjunto de correo electrónico	Causa desbordamiento de buffer en IIS	Causa desbordamiento de buffer en SQL y MSDE	Llega como adjunto de correo electrónico	Causa desbordamiento de buffer en el servicio UPnP	Causa desbordamiento de buffer en el servicio RPC
Persistencia	Ejecuta un script para descargar código	Crea ejecutables y edita el registro	Ejecuta un script para descargar código	N/A	Crea ejecutables y edita el registro	Crea ejecutables y edita el registro, descarga código	Ejecuta su payload para descargar código
Propagación	Busca direcciones y se extiende a nuevas víctimas	Abre la libreta de direcciones y se envía por correo electrónico a nuevas víctimas	Elige nuevas direcciones y se extiende a nuevas víctimas	Elige nuevas direcciones y se extiende a nuevas víctimas	Abre la libreta de direcciones y se envía por correo electrónico a nuevas víctimas	Inicia servicios FTP y TFTP, busca direcciones y se extiende a nuevas víctimas	Busca direcciones y se extiende a nuevas víctimas
Paralización	Engendra muchos procesos que hacen al sistema más lento	El gusano se disemina	Engendra muchos hilos que hacen al sistema más lento	Genera muchos paquetes, lo cual hace a la red más lenta	El gusano se disemina	Elimina claves y archivos del registro y termina procesos	El gusano se disemina

1.2.3 Troyanos

Troyano

El término troyano proviene de la mitología griega. Los guerreros griegos ofrecieron al pueblo de Troya (troyanos) un caballo gigante hueco como regalo. Los troyanos llevaron el caballo gigante adentro de su ciudad amurallada, sin sosechar que éste contenía muchos guerreros griegos. Durante la noche, cuando la mayoría de los troyanos dormía, los guerreros salieron del caballo y tomaron la ciudad.

Un troyano, en el mundo de la computación, es malware que realiza operaciones maliciosas bajo el disfraz de una función deseada. Un virus o gusano puede llevar consigo un troyano. Los troyanos contienen código malicioso oculto que explota los privilegios del usuario que lo ejecuta. Los juegos suelen llevar un troyano adjunto.

Cuando el juego se está ejecutando, funciona, pero, en segundo plano, el troyano ha sido instalado en el sistema del usuario y continúa ejecutándose luego de que el juego ha sido cerrado.

El concepto de troyano es flexible. Puede causar daño inmediato, proveer acceso remoto al sistema (una puerta trasera), o llevar a cabo acciones instruídas remotamente, como "envíame el archivo de la contraseña una vez por semana".

Los troyanos personalizados, como aquellos que tienen un objetivo específico, son difíciles de detectar.

Los troyanos generalmente se clasifican de acuerdo al daño que causan o la manera en que violan el sistema:

Troyanos de acceso remoto (permiten el acceso remoto no autorizado)
Troyano de envío de datos (provee al atacante de datos sensibles como contraseñas)
Troyano destructivo (corrompe o elimina archivos)
Troyano proxy (la computadora del usuario funciona como un servidor proxy)
Troyano FTP (abre el puerto 21)
Troyano inhabilitador de software de seguridad (detiene el funcionamiento de programas antivirus y/o firewalls)
Troyano de denegación de servicio (reduce la velocidad o detiene la actividad en la red)



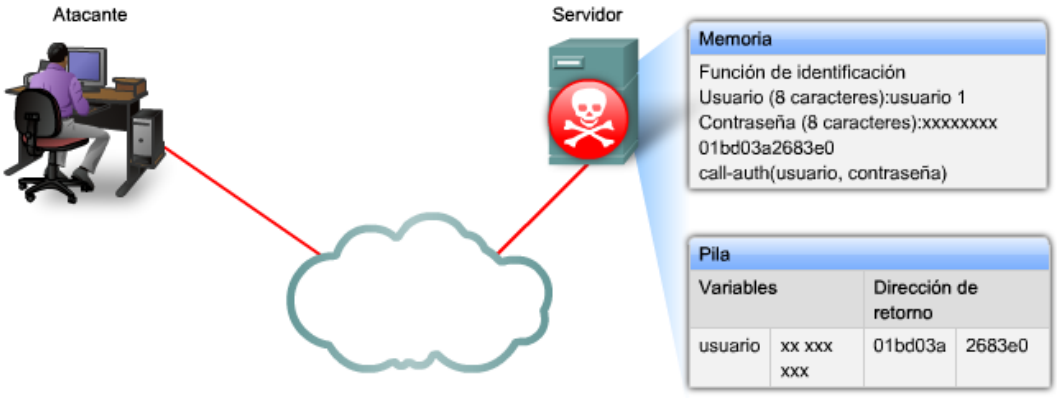
1.2.4 Mitigación de virus, gusanos y troyanos

La mayoría de las vulnerabilidades descubiertas en el software tienen relación con el desbordamiento del buffer. Un buffer es un área de la memoria alocada utilizada por los procesos para almacenar datos temporariamente. Un desbordamiento en el buffer ocurre cuando un buffer de longitud fija llena su capacidad y un proceso intenta almacenar datos más allá de ese límite máximo. Esto puede dar por resultado que los datos extra sobreescriban localizaciones de memoria adyacntes o causen otros comportamientos inesperados. Los desbordamientos de buffer son generalmente el conducto principal a

través del cual los virus, gusanos y troyanos hacen daño. De hecho, hay informes que sugieren que un tercio de las vulnerabilidades de software identificadas por el CERT están relacionadas con desbordamientos de buffer.

Los virus y troyanos tienden a aprovecharse de los desbordamientos de buffer de root locales. Un desbordamiento de buffer de root es un desbordamiento de buffer que busca obtener privilegios de root en un sistema. Los desbordamientos de buffer de root locales requieren que el sistema o usuario final efectúe algún tipo de acción. Un desbordamiento de buffer de root local se inicia típicamente cuando un usuario abre un adjunto de un correo electrónico, visita un sitio web o intercambia un archivo a través de mensajería instantánea.

Los gusanos como SQL Slammer y Code Red explotan los desbordamientos de buffer de root locales. Los desbordamientos de buffer de root remotos son similares a los desbordamientos de buffer de root locales, con la diferencia de que no se requiere intervención de usuario final o sistema.



Los virus, gusanos y troyanos pueden causar serios problemas a las redes y sistemas finales. Los administradores de red tiene varias maneras de mitigar estos ataques. Nótese que las técnicas de mitigación generalmente se consideran en la comunidad de seguridad como contramedidas.

El principal recurso para la mitigación de ataques de virus y troyanos es el software antivirus. El software antivirus ayuda a prevenir a los hosts de ser infectados y diseminar código malicioso. Requiere mucho más tiempo limpiar computadoras infectadas que mantener al software antivirus y a las definiciones de virus actualizados en las mismas máquinas.

El software antivirus es el producto de seguridad más ampliamente desplegado en el mercado de hoy en día. Muchas compañías que crean software antivirus, como Symantec, Computer Associates, McAfee y Trend Micro han estado en el negocio de detectar y eliminar virus por más de una década. Muchas empresas e instituciones educativas compran licencias al por mayor para sus usuarios. Los usuarios pueden identificarse en un sitio con su cuenta y descargar el software antivirus en sus computadoras de escritorio, notebooks o servidores.

Los productos antivirus tienen opciones de automatización de actualizaciones para que las nuevas definiciones de virus y actualizaciones de software puedan ser descargadas automáticamente o a petición. Esta práctica es el requisito más esencial para mantener una red libre de virus y debería ser formalizada en una política de seguridad de red.

Los productos antivirus son basados en host. Estos productos son instalados en las computadoras y los servidores para detectar y eliminar virus. Sin embargo, no pueden detener a los virus de entrar a la red, por lo que el profesional de la seguridad en redes debe mantenerse al tanto de los virus principales y de las actualizaciones en cuanto a virus emergentes.



Los gusanos dependen más de la red que los virus. La mitigación de gusanos requiere diligencia y coordinación de parte de los profesioales de la seguridad en redes. La respuesta a una infección de un gusano puede separarse en cuatro fases: contención, inoculación, cuarentena y tratamiento.

La fase de contención consiste en limitar la difusión de la infección del gusano de áreas de la red que ya están infectadas. Esto requiere compartimentización y segmentación de la red para hacer más lento o detener al gusano y prevenir que los hosts actualmente infectados infecten a otros sistemas. La contención requiere el uso de ACLs tanto entrantes como salientes en los routers y firewalls de los puntos de control de la red.

La fase de inoculación corre en paralelo o subsecuente a la fase de contención. Durante la fase de inoculación todos los sistemas no infectados reciben un parche del vendedor apropiado para la vulnerabilidad. El proceso de inoculación priva aún más a los gusanos de objetivos disponibles. Un escáner de red puede ayudar a identificar hosts potencialmente vulnerables. El ambiente móvil prevaleciente en las redes modernas postula desafíos significativos. Es común que las laptops se saquen del ambiente de red

segura y se conecten a ambientes potencialmente inseguros, tales como las redes caseras. Sin parches apropiados en el sistema, una laptop puede ser infectada por un gusano o virus y traerlo al ambiente seguro de la red de la organización donde puede infectar otros sistemas.

La fase de cuarentena incluye el rastreo y la identificación de máquinas infectada dentro de las áreas contenidas y su desconexión, bloqueo o eliminación. Esto aisla estos sistemas apropiadamente para la fase de tratamiento.

Durante la fase de tratamiento, los sistemas activamente infectados son desinfectados del gusano. Esto puede significar terminar el proceso del gusano, eliminar archivos modificados o configuraciones del sistema que el gusano haya introducido e instalar un parche para la vulnerabilidad que el gusano usaba para explotar el sistema. En casos más severos, esto puede requerir la reinstalación completa del sistema para asegurarse de que el gusano y sus productos derivados sean removidos.

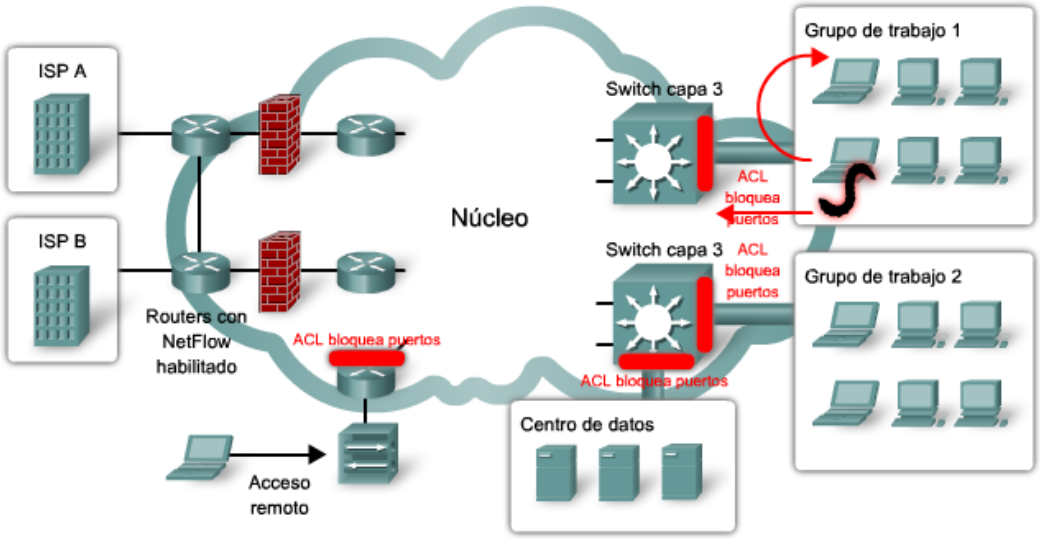


En el caso del gusano SQL Slammer, el tráfico malicioso fue detectado en el puerto UDP 1434. Este puerto normalmente debería ser bloqueado por un firewall en el perímetro. Sin embargo, la mayoría de las infecciones entra por una puerta trasera y no pasa por el firewall; por lo tanto, para prevenir la diseminación de este gusano sería necesario bloquear este puerto en todos los dispositivos de la red interna.

En algunos casos, el puerto a través del cual se disemina el gusano puede ser crítico para la operación de negocios. Por ejemplo, cuando se propagaba el SQL Slammer, algunas organizaciones no podían bloquear el puerto UDP 1434 porque era necesario para acceder al servidor SQL para transacciones de negocios legítimas. En una situación como esa deben considerarse alternativas.

Si se conocen los dispositivos de red que usan el servicio del puerto afectado, se puede permitir acceso selectivo. Por ejemplo, si solo un pequeño número de clientes utiliza el

servidor SQL, una opción podría ser abrir el puerto UDP 1434 solo a dispositivos críticos. No se garantiza que el acceso selectivo resuelva el problema, pero ciertamente disminuye la probabilidad de una infección.



Una opción integradora para mitigar ls efectos de los virus, gusanos y troyanos es un sistema de prevención de intrusos basado en el host (host-based intrusion prevention system - HIPS).

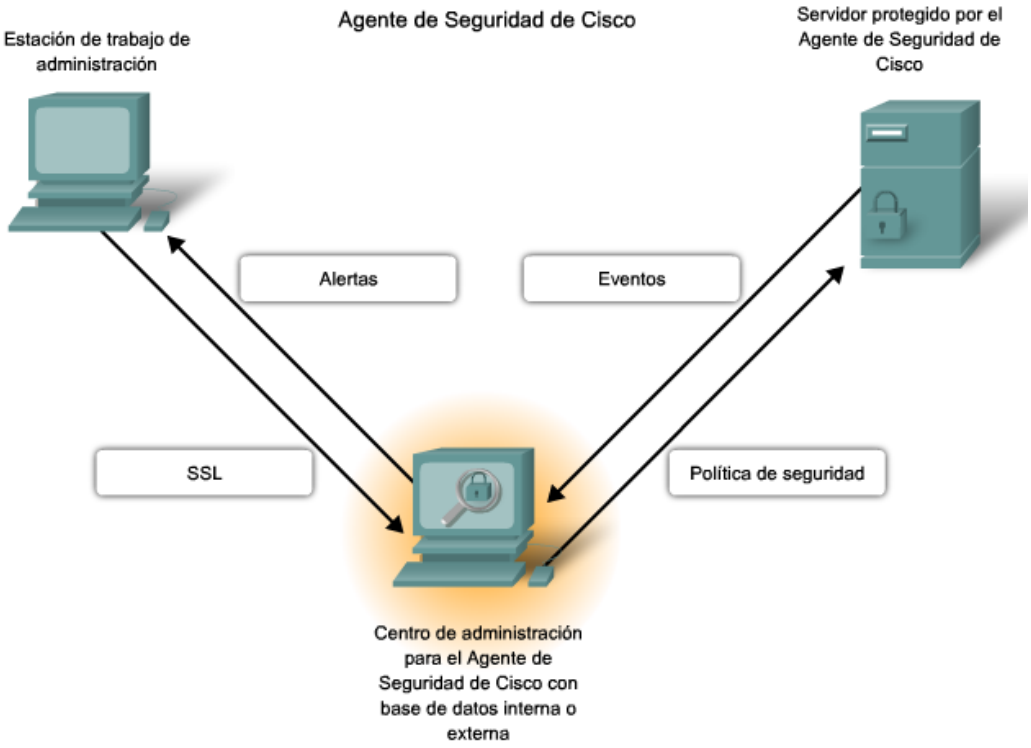
El Agente de Seguridad de Cisco (Cisco Security Agent - CSA) es un sistema de prevención de intrusos basado en el host que pueden ser integrado con software antivirus de varios vendedores. El CSA protege al sistema operativo de amenazas en la red. El CSA proporciona una solución más integradora y centralizada que no depende de que los usuarios finales vigilen las actualizaciones del software antivirus y usen firewalls basados en el host.

Otra solución para mitigar las amenazas es el Control de Admisión a la Red de Cisco (Cisco Network Admission Control - NAC). La aplicación NAC de Cisco es una solución llave-en-mano para controlar el acceso a la red. Solo admite hosts que se hayan identificado y cuya seguridad haya sido examinada y aprobada para la red. Esta solución es particularmente útil para orgaizaciones con redes de tamaño medio que necesitan un seguimiento del sistema operativo, parches de antivirus y actualizaciones de vulnerabilidades simplificado e integrado. La aplicación NAC de Cisco no necesita ser parte de una red Cisco para funcionar.

El Sistema de Respuesta, Análisis y Monitoreo (MARS) proporciona monitoreo de seguridad para dispositivos de seguridad de red y aplicaciones de host creadas por Cisco y otros proveedores. MARS efectúa recomendaciones precisas para remoción de amenazas, incluyendo la habilidad de visualizar el camino de la amenaza e identificar la fuente de la amenaza con gráficos topológicos detallados que simplifican la respuesta de seguridad.

Los virus, gusanos y troyanos pueden hacer lentas a las redes o detenerlas completamente y corromper o destruir datos. Hay opciones de hardware y software

disponibles para mitigar estas amenazas. Los profesionales de la seguridad en redes deben estar constantemente alerta. No es suficiente con reaccionar a las amenazas. Un buen profesional de la seguridad en redes examina toda la red en busca de vulnerabilidades y las arregla antes de que tome lugar un ataque.



1.3 Metodologías de ataque

1.3.1 Ataques de reconocimiento

Hay varios tipos diferentes de ataques de red que no son virus, gusanos o troyanos. Para mitigar los ataques, es útil tener a los varios tipos de ataques categorizados. Al categorizar los ataques de red es posible abordar tipos de ataques en lugar de ataques individuales. No hay un estándar sobre cómo categorizar los ataques de red. El método utilizado en este curso clasifica los ataques en tres categorías principales.

Ataques de reconocimiento

Los ataques de reconocimiento consisten en el descubrimiento y mapeo de sistemas, servicios o vulnerabilidades sin autorización. Los ataques de reconocimiento muchas veces emplean el uso de sniffers de paquetes y escáners de puertos, los cuales están ampliamente disponibles para su descarga gratuita en Internet. El reconocimiento es análogo a un ladrón vigilando un vecindario en busca de casas vulnerables para robar, como una residencia sin ocupantes o una casa con puertas o ventanas fáciles de abrir.

Ataques de acceso

Los ataques de acceso explotan vulnerabilidades conocidas en servicios de autenticación, FTP y web para ganar acceso a cuentas web, bases de datos confidenciales y otra información sensible. Un ataque de acceso puede efectuarse de varias maneras. Un ataque de acceso generalmente emplea un ataque de diccionario para adivinar las contraseñas del sistema. También hay diccionarios especializados para diferentes idiomas.

Ataques de Denegación de Servicio

Los ataques de Denegación de Servicio envían un número extremadamente grande de solicitudes en una red o Internet. Estas solicitudes excesivas hacen que la calidad de funcionamiento del dispositivo víctima sea inferior. Como consecuencia, el dispositivo atacado no está disponible para acceso y uso legítimo. Al ejecutar explotaciones o combinaciones de explotaciones, los ataques de DoS desaceleran o colapsan aplicaciones y procesos.

Ataques de reconocimiento

El reconocimiento también se conoce como recolección de información y, en la mayoría de los casos, precede un ataque de acceso o de DoS. En un ataque de reconocimiento, el intruso malicioso típicamente comienza por llevar a cabo un barrido de ping en la red objetivo para determinar qué direcciones IP están siendo utilizadas. El intruso entonces determina qué servicios o puertos están disponibles en las direcciones IP activas. Nmap es la aplicación más popular para escanear puertos. A partir de la información de puertos obtenida, el intruso interroga al puerto para determinar el tipo y la versión de la aplicación y el sistema operativo que está corriendo sobre el host objetivo. En muchos casos, los intrusos buscan servicios vulnerables que puedan ser explotados luego, cuando hay menos probabilidad de ser atrapados.

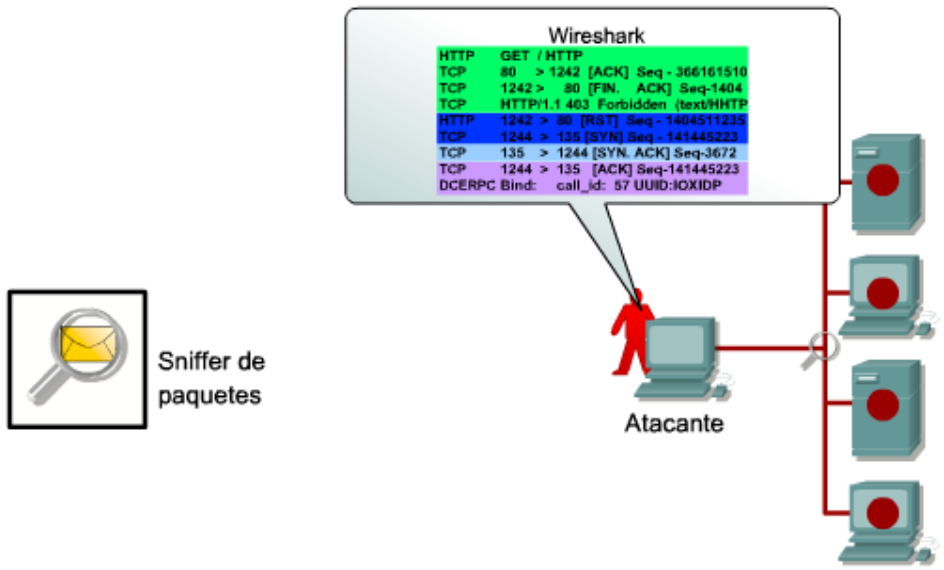
Los ataques de reconocimiento utilizan varias herramientas para ganar acceso a una red:

Sniffers de paquetes
Barridos de ping
Escaneo de puertos
Búsquedas de información en Internet

Un sniffer de paquetes es una aplicación de software que utiliza una tarjeta de red en modo promiscuo para capturar todos los paquetes de red que se transmitan a través de una LAN. El modo promiscuo es un modo mediante el cual la tarjeta de red envía todos los paquetes que se reciben a una aplicación para procesarlos. Algunas aplicaciones de red distribuyen paquetes de red en texto plano sin cifrar. Como los paquetes de red no están cifrados, pueden ser entendidos por cualquier aplicación que pueda levantarlos de la red y procesarlos.

Los sniffers de paquetes solo funcionan en el mismo dominio de colosión que la red bajo ataque, salvo que el atacante tenga acceso a los switches intermedios.

Hay numerosos sniffers de paquetes disponibles, tanto freeware como shareware. Estos no requieren que el usuario tenga entendimiento de los protocolos que operan detrás.



Haga clic sobre el ícono de Sniffer de paquetes para ver el ataque.

Cuando se usan como herramientas legítimas, las aplicaciones de barrido de ping y escaneo de puertos efectúan una serie de pruebas en los hosts y dispositivos para identificar servicios vulnerables. La información se recolecta examinando el direccionamiento IP y datos de puerto o banner de los puertos TCP y UDP. Un atacante usa barridos de ping y escaneos de puerto para adquirir información para comprometer el sistema.

El barrido de ping es una técnica de escaneo de redes básica que determina qué rango de direcciones IP corresponde a los hosts activos. Un solo ping indica si un host específico existe en la red. El barrido de ping consiste en solicitudes de eco ICMP enviadas a varios hosts. Si una dirección dada está activa, la dirección devuelve una respuesta de eco ICMP. Los barridos de ping están entre los métodos más viejos y lentos utilizados para escanear una red.

Cada servicio de un host está asociado con un número de puerto bien conocido. El escaneo de puertos es un escaneo de un rango de números de puerto TCP o UDP en un host para detectar servicios abiertos. Consiste en el envío de un mensaje a cada puerto de un host. La respuesta recibida indica si el puerto es utilizado.

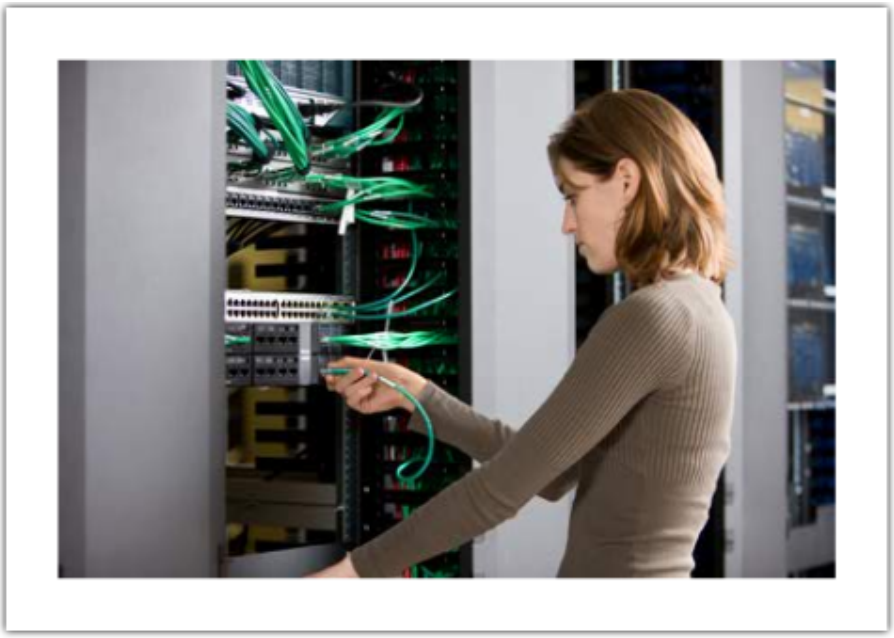
Las búsquedas de información en Internet pueden revelar información sobre quién es el dueño de un dominio particular y qué direcciones han sido asignadas a ese dominio. También pueden revelar quién es el dueño de una dirección de IP particular y qué dominio está asociado con la dirección.

Los barridos de ping sobre direcciones reveladas por búsquedas de información en Internet pueden dar una imagen de los hosts activos en un ambiente en particular. Luego de que se ha generado esa lista, las herramientas de escaneo de puertos pueden pasar por

todos los puertos bien conocidos para proporcionar una lista completa de todos los servicios que están corriendo en los hosts que el barrido de ping descubrió. Los hackers pueden entonces examinar las características de las aplicaciones activas, de donde pueden extraer información específica útil para un hacker cuya intención es comprometer ese servicio.

Es necesario tener en consideración que los ataques de reconocimiento son generalmente precursores a ataques posteriores con la intención de ganar acceso no autorizado a una red o interrumpir el funcionamiento de la misma. Un profesional de la seguridad en redes puede detectar un ataque de reconocimiento en proceso mediante alarmas que se disparan cuando ciertos parámetros se exceden, por ejemplo, las solicitudes ICMP por segundo. Un ISR de Cisco soporta la tecnología de seguridad que permite que estas alarmas se disparen. Esto está disponible por medio de funcionalidad de prevención de intrusos basada en la red soportada por las imágenes IOS de seguridad de Cisco que corren sobre los ISRs.

Los sistemas de prevención de intrusos basados en host y los sistemas independientes de detección de intrusos basados en red también pueden ser utilizados para notificar un ataque de reconocimiento en proceso.



1.3.2 Ataques de acceso

Ataques de acceso

Los hackers utilizan los ataques de acceso en las redes o sistemas por tres razones: para obtener datos, para ganar acceso y para escalar privilegios de acceso.

Los ataques de acceso generalmente emplean ataques de contraseña para adivinar las contraseñas del sistema. Los ataques de contraseña pueden ser implementados utilizando varios métodos, incluyendo ataques de fuerza bruta, programas troyanos, falsificación de IPs y sniffers de paquetes. Sin embargo, la mayoría de los ataques es

por fuerza bruta, es decir, repetidos intentos basados en un diccionario incorporado para identificar una cuenta de usuario o contraseña.

Un ataque de fuerza bruta generalmente se lleva a cabo usando un programa que corre a través de la red e intenta ingresar a un recurso compartido, como un servidor. Luego de que un atacante gana acceso a un recurso, tiene los mismos derechos que el usuario cuya cuenta comprometió. Si esta cuenta tiene suficientes privilegios, el atacante puede crear una puerta trasera para acceso futuro sin preocuparse por cambios de contraseña o de estado en relación a la cuenta de usuario comprometida.

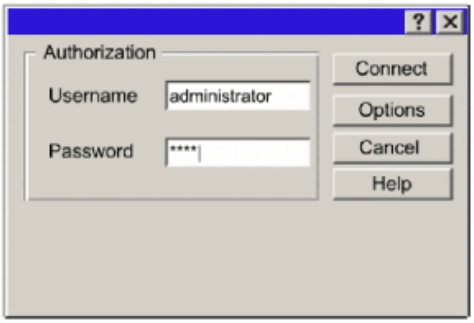
A modo de ejemplo, un usuario puede ejecutar la aplicación L0phtCrack, o LC5, para efectuar un ataque de fuerza bruta para obtener una contraseña de un servidor Windows. Cuando se obtiene la contraseña, el atacante puede instalar un keylogger, que envía una copia de todas las pulsaciones de teclas a un destino deseado. También se puede instalar un troyano que envíe una copia de todos los paquetes enviados y recibidos por el objetivo a un destino particular, permitiendo así el monitoreo del tráfico desde y hacia ese servidor.

Hay cinco tipos de ataques de acceso:

Ataques de contraseña - El atacante intenta adivinar las contraseñas del sistema. Un ejemplo común es un ataque de diccionario.
Explotación de la confianza - El atacante usa privilegios otorgados a un sistema en una forma no autorizada, posiblemente causando que el objetivo se vea comprometido.
Redirección de puerto - Se usa un sistema ya comprometido como punto de partida para ataques contra otros objetivos. Se instala una herramienta de instrusión en el sistema comprometido para redirección de sesiones.
Ataque Man in the Middle - El atacante se ubica en el medio de una comunicación entre dos entidades legítimas para leer o modificar los datos que pasan entre las dos partes. Un ataque Man in the Middle popular involucra a una laptop actuando como un punto de acceso no autorizado (rogue access point) para capturar y copiar todo el tráfico de red de un usuario objetivo. Frecuentemente el usuario está en un lugar público conectado a un punto de acceso inalámbrico.
Desbordamiento de buffer - El programa escribe datos más allá de la memoria de buffer alocada. Los desbordamientos de buffer surgen generalmente como consecuencia de un error en un programa C o C++. Un resultado del desbordamiento es que los datos válidos se sobreescriben o explotan para permitir la ejecución de código malicioso.

Los atacantes pueden implementar ataques de contraseña utilizando varios métodos diferentes:

- Ataques de fuerza bruta
- Programas troyanos
- Sniffers de paquetes



Ataque de contraseña | Explotación de confianza | Redirección de puertos | Man in the middle | Desbordamiento de buffer

Haga clic sobre cada botón para ver el contenido asociado.

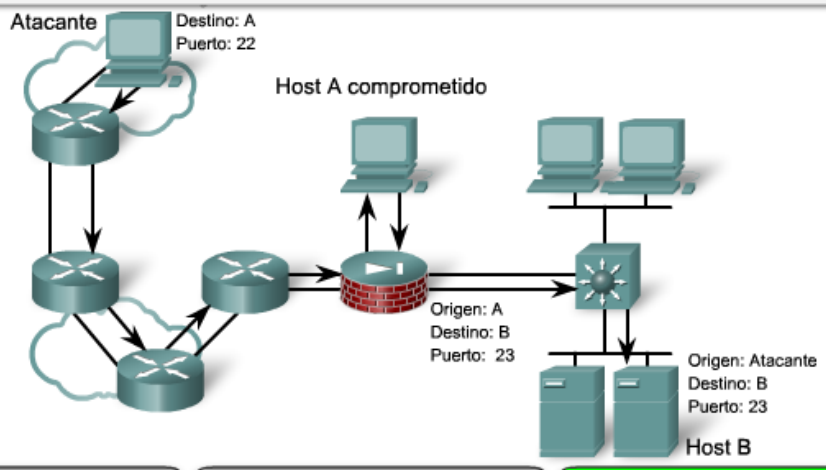
Sistema operativo de la red	Modelos de confianza
Windows	Directorio activo del dominio (Active Directory - AD)
Linux y UNIX	Network File System (NFS) Network Information Service Plus (NIS+)



Ataque de contraseña | Explotación de confianza | Redirección de puertos | Man in the middle | Desbordamiento de buffer

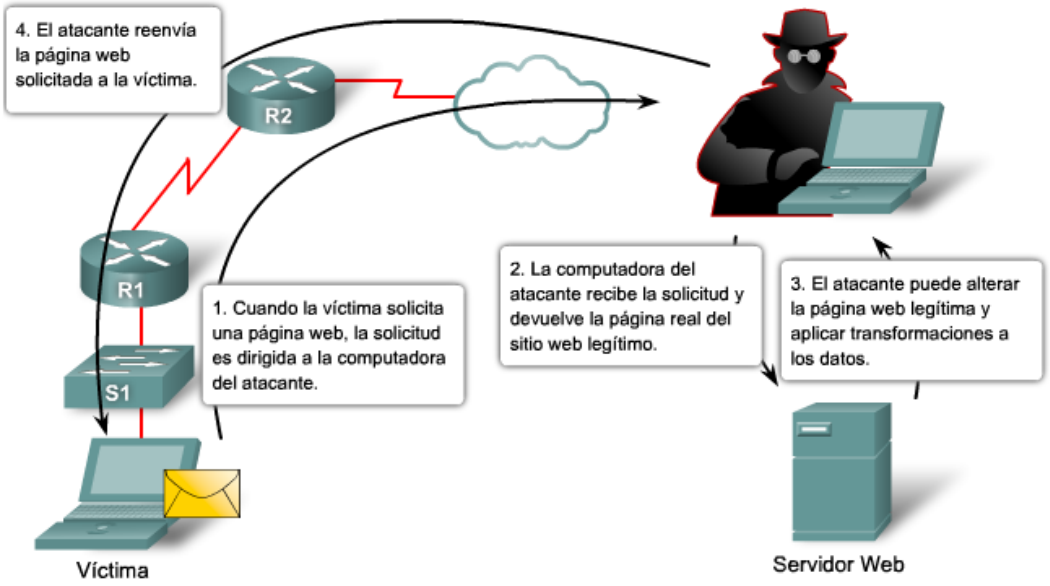
Haga clic sobre cada botón para ver el contenido asociado.

La redirección de puertos es un tipo de ataque de explotación de confianza que usa un host comprometido para pasar tráfico que en cualquier otro caso sería descartado a través de un firewall. Se mitiga principalmente a través del uso de modelos de confianza apropiados. El software antivirus y un IDS basado en host pueden ayudar a detectar y prevenir a un atacante de instalar utilidades de redirección de puertos en el host.



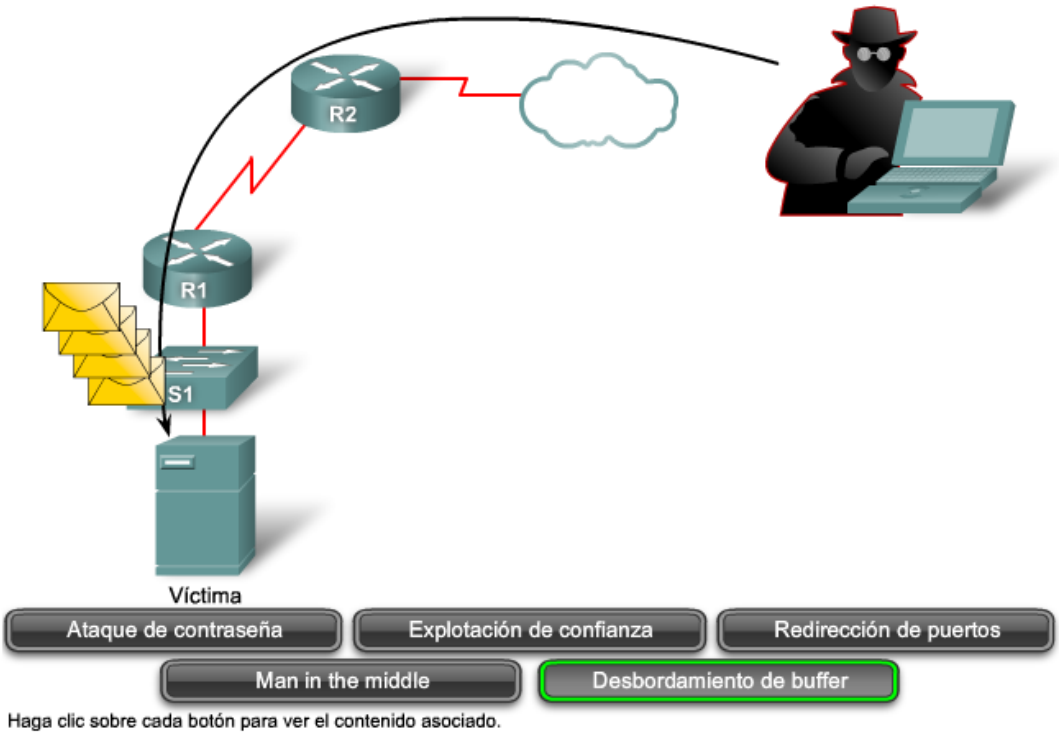
Ataque de contraseña | Explotación de confianza | Redirección de puertos | Man in the middle | Desbordamiento de buffer

Haga clic sobre cada botón para ver el contenido asociado.



Ataque de contraseña | Explotación de confianza | Redirección de puertos | Man in the middle | Desbordamiento de buffer

Haga clic sobre cada botón para ver el contenido asociado.

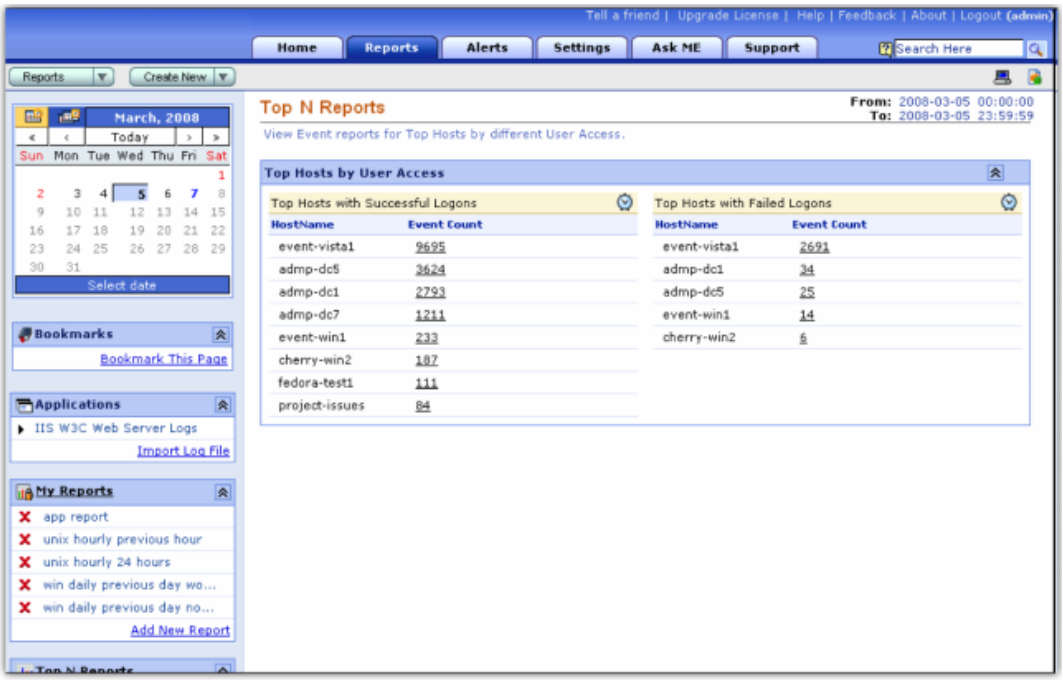


Los ataques de acceso en general pueden ser detectados revisando los registros, el uso del ancho de banda y la carga de los procesos.

La política de seguridad de la red debería especificar que los registros se mantienen formalmente para todos los servidores y dispositivos de la red. Al revisar los registros, el personal de seguridad puede determinar si ha ocurrido un número inusual de intentos fallidos de autenticación. Los paquetes de software como el Motor de Análisis de Eventos o el Servidor de Control de Acceso Seguro de Cisco (Cisco Secure Access Control Server - CSACS) mantienen información relativa a los intentos fallidos de autenticación en dispositivos de red. Los servidores UNIX y Windows también mantienen un registro de los intentos fallidos de autenticación. Los routers y dispositivos firewall de Cisco pueden ser configurados para prevenir intentos de autenticación de una fuente particular por un tiempo dado luego de un número preestablecido de fallos en un período específico de tiempo.

Los ataques Man in the Middle generalmente consisten en la replicación de datos. Un índice de un ataque como éste es una cantidad inusual de actividad en la red y uso del ancho de banda, como lo puede indicar algún software de monitoreo de red.

Asimismo, un ataque de acceso que tenga como resultado un sistema comprometido probablemente será delatado por la lentitud de la actividad, producto de ataques de desbordamiento de buffer en proceso, como indicado por las cargas de proceso activas visibles en un sistema Windows o UNIX.



1.3.3Ataques de denegación de servicio

Ataques de Denegación de Servicio

El ataque de DoS es un ataque de red que resulta en algún tipo de interrupción en el servicio a los usuarios, dispositivos o aplicaciones. Muchos mecanismos pueden generar un ataque de DoS. El método más simple es generar grandes cantidades de lo que simula ser tráfico de red válido. Este tipo de ataque de DoS satura la red para que el tráfico de usuario válido no pueda pasar.

El ataque de DoS se aprovecha del hecho de que los sistemas objetivo como los servidores deben mantener información de estado. Las aplicaciones pueden depender de los tamaños de buffer esperados y el contenido específico de los paquetes de red. Un ataque de DoS puede explotar esto enviando tamaños de paquetes o valores de datos que no son esperados por la aplicación receptora.

Hay dos razones principales por las cuales puede ocurrir un ataque de DoS:

Un host o aplicación no puede manejar una condición esperada, como datos de entrada formateados maliciosamente, una interacción inesperada entre componentes del sistema, o un simple agotamiento de los recursos.
Una red, host o aplicación es incapaz de manejar una cantidad enorme de datos, haciendo que el sistema colapse o se vuelva extremadamente lento.

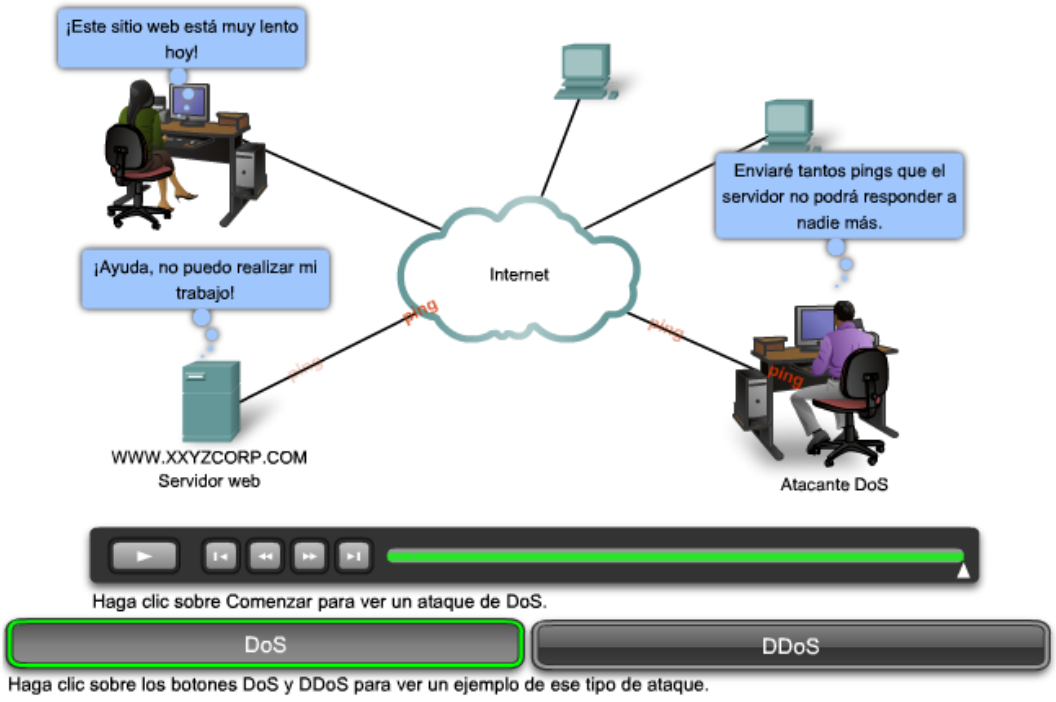
Los ataques de DoS intentan comprometer la disponibilidad de una red, un host o una aplicación. Se los considera un riesgo importante porque pueden interrumpir fácilmente un proceso de negocios y causar pérdidas significativas. Estos ataques son relativamente sencillos de llevar a cabo, incluso por un atacante inexperto.

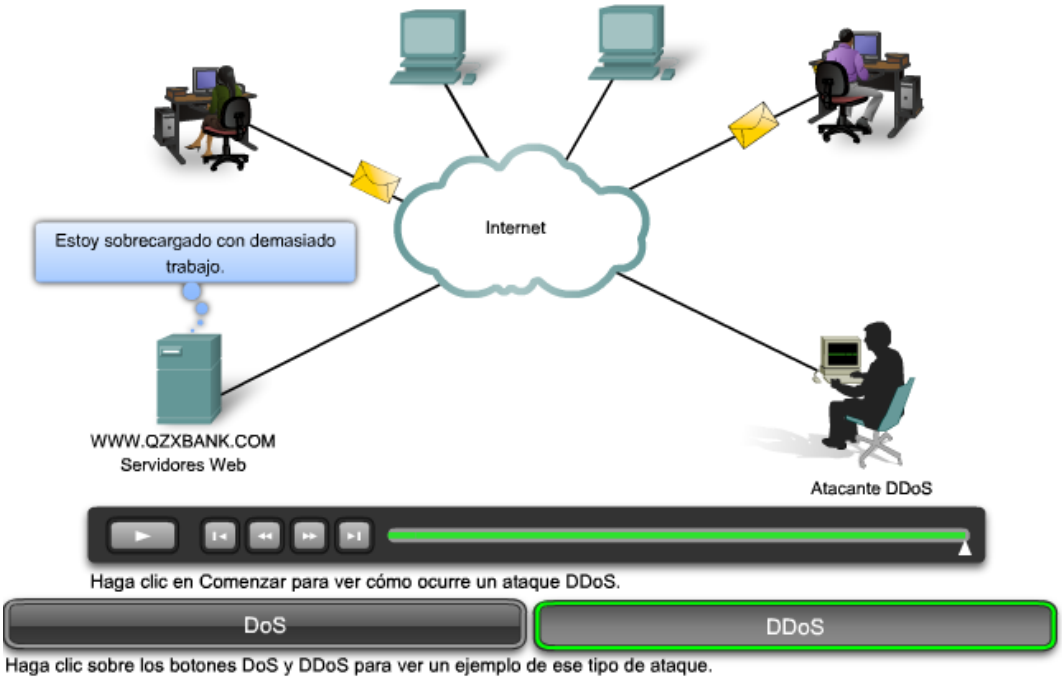
Un ejemplo de ataque de DoS es el envío de un paquete malicioso. Un paquete malicioso es un paquete cuyo formato es inapropiado, diseñado para hacer que el dispositivo receptor procese el paquete de manera inapropiada. El paquete malicioso hace que el dispositivo receptor colapse o funcione muy lentamente. Este ataque puede hacer que todas las comunicaciones desde y hacia el dispositivo se interrumpan.

En otro ejemplo, un atacante envía una seguidilla de paquetes continuos que colman el ancho de banda de enlaces de red disponible. En la mayoría de los casos, es imposible diferenciar entre el atacante y el tráfico legítimo para rastrear un ataque rápidamente hasta su fuente. Si muchos sistemas en el núcleo de Internet están comprometidos, el atacante puede aprovecharse de un ancho de banda prácticamente ilimitado para desatar tormentas de paquetes hacia objetivos deseados.

Un ataque Distribuido de Denegación de Servicio (DDoS) es similar en intención al ataque de DoS, excepto en que el ataque DDoS se origina en varias fuentes coordinadas. Además de aumentar la cantidad de tráfico en la red originado en múltiples atacantes distribuidos, un ataque DDoS también presenta el desafío de requerir que la defensa de la red identifique y detenga a cada atacante distribuido.

Como ejemplo, un ataque DDoS podría proceder como sigue. Un hacker escanea buscando sistemas accesibles. Luego de que el hacker accede a varios sistemas "handler", el hacker instala software zombie en ellos. Los zombies luego escanean e infectan a sistemas agente. Cuando el hacker accede a los sistemas agentes, el hacker carga software de ataque por control remoto para que lleve a cabo el ataque DDoS.





Será útil detallar tres ataques de DoS comunes para entender mejor cómo funcionan.

El ping de la muerte

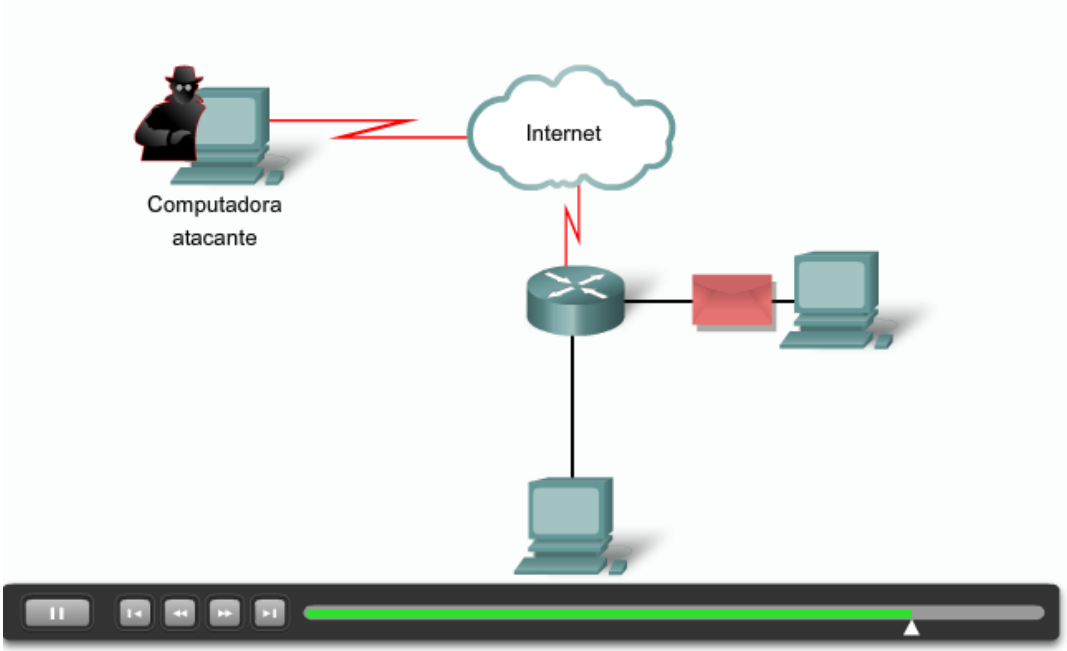
En un ataque de ping de la muerte, un hacker envía una solicitud de eco en un paquete IP más grande que el tamaño de paquete máximo de 65535 bytes. Enviar un ping de este tamaño puede colapsar la computadora objetivo. Una variante de este ataque es colapsar el sistema enviando fragmentos ICMP, que llenen los buffers de reensamblado de paquetes en el objetivo.

Ataque Smurf

En un ataque smurf, el atacante envía un gran número de solicitudes ICMP a direcciones broadcast, todos con direcciones de origen falsificadas de la misma red que la víctima. Si el dispositivo de ruteo que envía el tráfico a esas direcciones de broadcast reenvía los broadcast, todos los host de la red destino enviarán respuestas ICMP, multiplicando el tráfico por el número de hosts en las redes. En una red broadcast multiacceso, cientos de máquinas podrían responder a cada paquete.

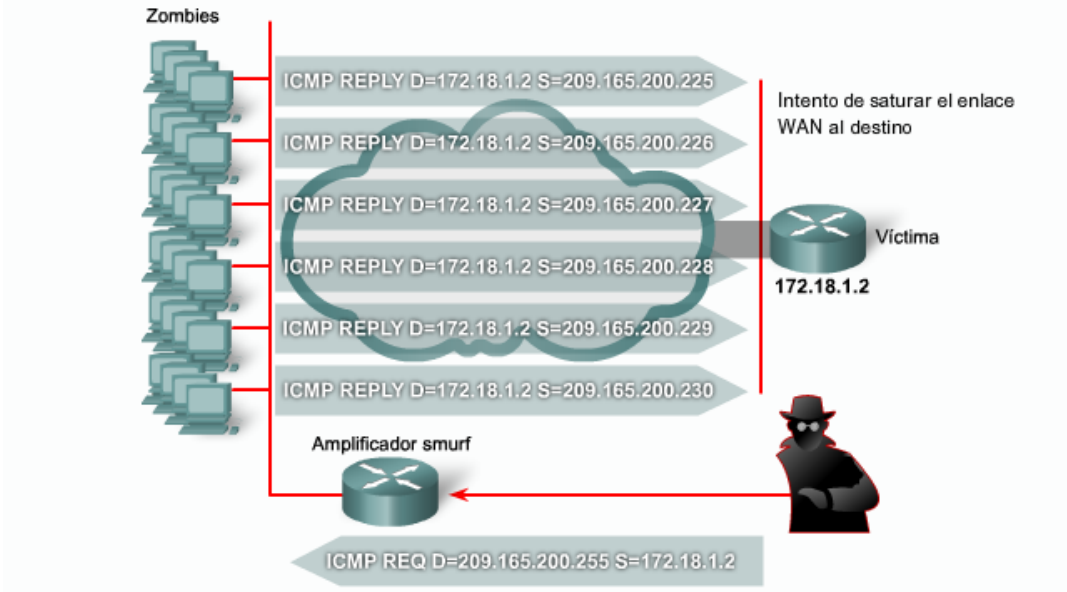
Inundación TCP/SYN

En un ataque de inundación TCP/SYN, se envía una inundación de paquetes SYN TCP, generalmente con una dirección de origen falsa. Cada paquete se maneja como una solicitud de conexión, causando que el servidor genere una conexión a medio abrir devolviendo un paquete SYN-ACK TCP y esperando un paquete de respuesta de la dirección del remitente. Sin embargo, como la dirección del remitente es falsa, la respuesta nunca llega. Estas conexiones a medio abrir saturan el número de conexiones disponibles que el servidor puede atender, haciendo que no pueda responder a solicitudes legítimas hasta luego de que el ataque haya finalizado.



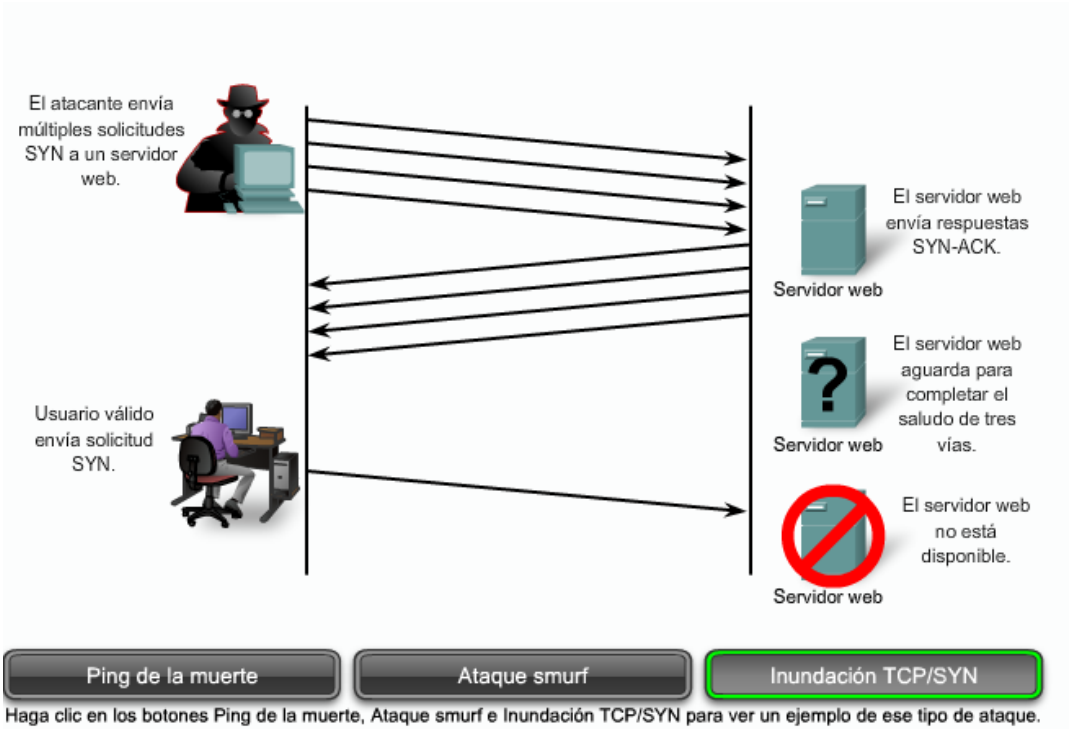
Ping de la muerte | Ataque smurf | Inundación TCP/SYN

Haga clic en los botones Ping de la muerte, Ataque smurf e Inundación TCP/SYN para ver un ejemplo de ese tipo de ataque.



Ping de la muerte | Ataque smurf | Inundación TCP/SYN

Haga clic en los botones Ping de la muerte, Ataque smurf e Inundación TCP/SYN para ver un ejemplo de ese tipo de ataque.



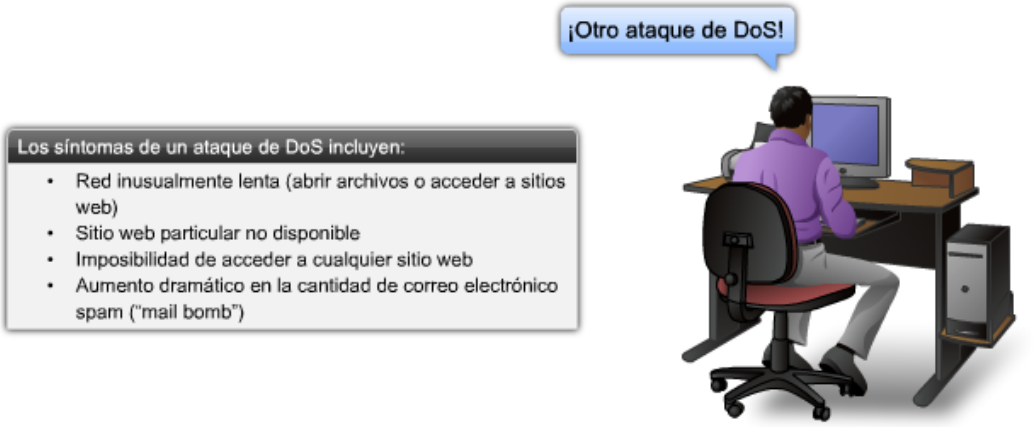
La inundación TCP/SYN, el ping de la muerte y los ataques smurf demuestran cuán devastante puede ser un ataque de DoS. Hasta la fecha, cientos de ataques de DoS han sido documentados. Hay cinco maneras básicas en las que los ataques de DoS pueden hacer daño:

Consumo de los recursos, como ancho de banda, espacio en el disco o tiempo de procesador
Modificación de la información de configuración, como la información de ruteo
Modificación de la información de estado, como el reinicio de las sesiones TCP
Modificación de los componentes físicos de la red
Obstrucción de las comunicaciones entre la víctima y otros.

Generalmente no es difícil determinar si está ocurriendo un ataque de DoS. Un gran número de quejas sobre no poder acceder a los recursos es un primer indicio de un ataque de DoS. Para minimizar el número de ataques, un paquete de software de utilización de red debería estar corriendo todo el tiempo. Esto también debe ser requerido por la política de seguridad de la red. Un gráfico de utilización de la red que muestre actividad inusual puede indicar un ataque de DoS.

Es necesario tener en consideración que los ataques de DoS pueden ser una parte de un ataque mayor. Los ataques de DoS pueden acarrear problemas en los segmentos de la red de las computadoras bajo ataque. Por ejemplo, la capacidad de paquetes por segundo de un router entre Internet y una LAN puede ser excedido por el ataque, comprometiendo no solo el sistema objetivo sino también toda la red. Si el ataque es llevado a cabo en una escala suficientemente grande, regiones geográficas enteras de conectividad a Internet podrían ser comprometidas.

No todos los fallos de servicios, incluso aquellos que son resultado de actividades maliciosas, son necesariamente ataques de DoS. De cualquier modo, los ataques de DoS están entre los tipos más peligrosos de ataques, y es crítico que el profesional de la seguridad en redes actúe rápidamente para mitigar los efectos de tales ataques.



1.3.4 Mitigación de ataques de red

Hay un gran número de ataques de red, metodologías de ataques de red y categorizaciones de ataques de red. La pregunta importante es "¿Cómo puedo mitigar los ataques de red?".

El tipo de ataque, como especificado por la categorización que distingue entre ataques de reconocimiento, de acceso o de DoS, determina la manera de mitigar una amenaza a una red.



Los ataques de reconocimiento pueden ser mitigados de varias maneras.

Utilizar una autenticación fuerte es una primera opción para la defensa contra sniffers de paquetes. La autenticación fuerte es un método de identificar a los usuarios que no puede ser fácilmente burlados. Una contraseña de una sola vez (One-Time Password - OTP) es una forma de autenticación fuerte. Las OTPs utilizan una autenticación de dos factores. La autenticación de dos factores combina algo que uno ya tiene, como una tarjeta de token, con algo que uno conoce, como un PIN. Los cajeros automáticos (Automated teller machines - ATMs) utilizan la autenticación de dos factores.

El cifrado también es efectivo en la mitigación de ataques de sniffers de paquetes. Si el tráfico está cifrado, es prácticamente irrelevante si un sniffer de paquetes está siendo utilizado, ya que los datos capturados no son legibles.

El software antisniffer y las herramientas de hardware detectan cambios en el tiempo de respuesta de los hosts para determiar si los hosts están procesando más tráfico del que sus propias cargas de tráfico indicaría. Aunque esto no elimina completamente la amenaza, puede reducir el número de ocurrencias de la amenaza como parte de un sistema englobador de mitigación.

Una infraestructura switcheada es la norma hoy en día, lo cual dificulta la captura de datos que no sean los del dominio de colisión inmediato, que probablemente contenga solo un host. Una infraestructura switcheada no elimina la amenaza de los sniffers de paquetes, pero puede reducir enormemente la efectividad del sniffer.

Es imposible mitigar el escaneo de puertos. Sin embargo, el uso de un IPS y un firewall puede limitar la información que puede ser descubierta con un escáner de puerto, y los barridos de ping pueden ser detenidos si se deshabilitan el eco y la respuesta al eco ICMP en los routers de borde. Sin embargo, cuando estos servicios se deshabilitan, los datos de diagnóstico de la red se pierden. Además, los escaneos de puerto pueden correr sin barridos de ping enteros. Los escaneos simplemente toman más tiempo porque las direcciones IP sin actividad también son escaneadas.

Los IPS basados en red y los basados en host pueden notificar al administrador cuando está tomando lugar un ataque de reconocimiento. Esta advertencia permite al administrador prepararse mejor para el ataque o notificar al ISP sobre el lugar desde donde se está lanzando el reconocimiento.



Las técnicas de mitigación de ataques de reconocimiento disponibles incluyen:

- Implementar autenticación para asegurar el acceso apropiado.
- Usar cifrado para inutilizar los ataques de sniffer de paquetes.
- Usar de herramientas antisniffer para detectar ataques de sniffer de paquetes.
- Implementar una infraestructura switcheada.
- Usar un firewall e IPS.

También hay varias técnicas disponibles para mitigar los ataques de acceso.

Un número sorprendente de ataques de acceso se lleva a cabo a través de simples averiguaciones de contraseñas o ataques de diccionario de fuerza bruta contra las contraseñas. El uso de protocolos de autenticación cifrados o de hash, en conjunción con una política de contraseñas fuerte, reduce enormemente la probabilidad de ataques de acceso exitosos. Hay prácticas específicas que ayudan a asegurar una política de contraseñas fuerte:

Deshabilitar cuentas luego de un número específico de autenticaciones fallidas. Esta práctica ayuda a prevenir los intentos de contraseña continuos.
No usar contraseñas en texto plano. Usar o una contraseña de una sola vez (OTP) o una contraseña cifrada.
Usar contraseñas fuertes. Las contraseñas fuertes tienen por lo menos seis caracteres y contienen letras mayúsculas y minúsculas, números y caracteres especiales.

El principio de confianza mínima también debería diseñarse e implementarse en la estructura de red. Esto significa que los sistemas no deberían usarse entre ellos innecesariamente. Por ejemplo, si una organización tiene un servidor utilizado por dispositivos no confiables, como servidores web, el dispositivo confiable (servidor) no debería confiar en dispositivos no confiables (servidores web) incondicionalmente.

La criptografía es un componente crítico de una red segura moderna. Se recomienda utilizar cifrado para el acceso remoto a una red. Además, el tráfico del protocolo de ruteo también debería estar cifrado. Cuanto más cifrado esté el tráfico, menos oportunidad tendrán los hackers de interceptar datos con ataques Man in the Middle.



Las técnicas de mitigación de ataques de acceso disponibles incluyen:

- Seguridad de contraseñas fuerte
- Principios de confianza mínima
- Criptografía
- Parches de sistema operativo y aplicaciones

Las empresas con presencia de alto perfil en Internet deberían planear con anticipación cómo responder a ataques potenciales de DoS. Históricamente, muchos ataques de DoS tenían como fuente direcciones de origen falsificadas. Este tipo de ataque puede ser truncado usando tecnologías antifalsificación (antispoofing) en routers y firewalls de perímetro. Hoy en día, muchos ataques de DoS son ataques distribuidos de DoS

llevados a cabo por hosts comprometidos en varias redes. Mitigar los ataques DDoS requiere diagnóstico y planeamiento cuidadoso, así como también cooperación de los ISP.

Los elementos más importantes para mitigar los ataques de DoS son los firewalls y los IPS. Se recomiendan fuertemente los IPS tanto basados en host como basados en red.

Los routers y switches Cisco soportan algunas tecnologías antifalsificación como seguridad de puerto, snooping de DHCP, IP Source Guard, inspección de ARP dinámico y ACLs.

Por último, aunque la Calidad de Servicio (Quality of Service - QoS) no ha sido diseñada como una tecnología de seguridad, una de sus aplicaciones, la implementación de políticas de tráfico (traffic policing), puede ser utilizada para limitar el tráfico ingresante de cualquier cliente dado en un router de borde. Esto limita el impacto que puede tener una sola fuente sobre el uso del ancho de banda de ingreso.



Los principales medios para mitigar ataques de DoS incluyen:

- IPS y firewalls (ASAs e ISRs Cisco)
- Tecnologías antifalsificación
- Calidad de servicio - traffic policing

Defender su red de ataques requiere vigilancia y educación constantes. Hay 10 buenas prácticas que representan la mejor aseguración de su red.

1. Mantener parches actualizados, instalándolos cada semana o día si fuera posible, para prevenir los ataques de desbordamiento de buffer y la escalada de privilegios.

2. Cerrar los puertos innecesarios y deshabilitar los servicios no utilizados.

3. Utilizar contraseñas fuertes y cambiarlas seguido.

4. Controlar el acceso físico a los sistemas.

5. Evitar ingresos innecesarios en páginas web. Algunas páginas web permiten a sus usuarios ingresar nombre de usuario y contraseñas. Un hacker puede ingresar algo más que solo un nombre de usuario. Por ejemplo, ingresar "jdoe; rm -rf /" puede permitir a un atacante remover el archivo del sistema raíz de un servidor UNIX. Los programadores deben limitar la cantidad de caracteres de ingreso y no aceptar caracteres como | ; < >.

6. Realizar copias de resguardo y probar los archivos resguardados regularmente.

7. Educar a los empleados en cuanto a los riesgos de la ingeniería social y desarrollar estrategias para validar las entidades a través del teléfono, del correo electrónico y en persona.

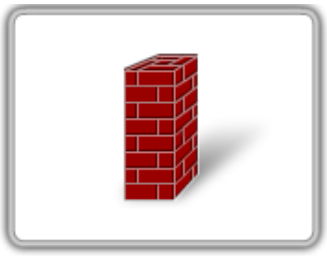
8. Cifrar y poner una contraseña a datos sensibles.

9. Implementar hardware y software de seguridad como firewalls, IPSs, dispositivos de red privada virtual (virtual private network - VPN), software antivirus y filtrado de contenidos.

10. Desarrollar una política de seguridad escrita para la compañía.

Estos métodos son tan solo un punto de partida para una gestión de seguridad robusta. La organizaciones deben estar siempre alerta para defenderse de amenazas en constante evolución.

Al usar estos métodos probados para asegurar una red y aplicar el conocimiento ganado en este capítulo, el alumno está preparado para comenzar a desplegar soluciones de seguridad en redes. Una de las primeras consideraciones del despliegue tiene que ver con la seguridad en el acceso a dispositivos de red.


Firewall


Controlar el acceso físico


Parches y actualizaciones

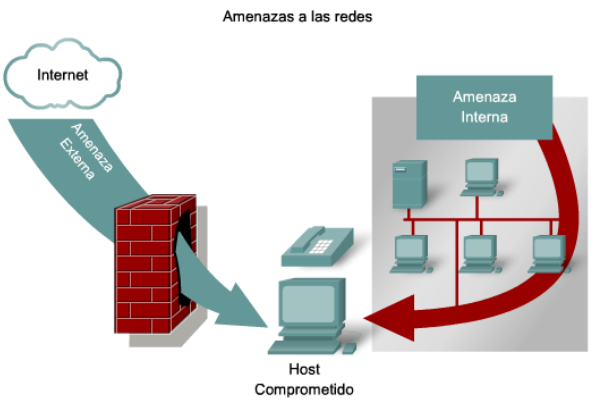


Desarrollar una política de seguridad


Proteger con contraseña los datos sensibles


Antivirus

1.4.1 Resumen del capitulo



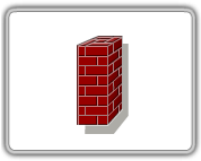
- La seguridad de las redes ha evolucionado en los últimos 40 años desde las primeras medidas que eran originalmente implementadas en ARPAnet.
- El trabajo malicioso de los hackers y la necesidad de mantener las operaciones de negocios empujan la labor de la seguridad en redes.
- Las organizaciones de la seguridad en redes proveen un foro para que los profesionales colaboren y mejoren sus habilidades.
- La seguridad en redes consiste en varios dominios que permiten a los profesionales especializarse y estructuran el mundo de la seguridad en redes.
- Las políticas de seguridad en redes proveen un

Haga clic sobre lo botones para información resumida.

- El virus es un software malicioso que se adjunta a otro programa para ejecutar acciones no deseadas en un sistema final.
- El gusano ejecuta código arbitrario e instala copias de sí mismo en la memoria de una computadora infectada, que luego infecta a otros hosts.
- Un troyano es una aplicación escrita para parecerse a otra cosa. Cuando un troyano se descarga y abre, ataca a la computadora del usuario final desde dentro.
- Hay herramientas específicas disponibles para mitigar los efectos de los virus, gusanos y troyanos.



Haga clic sobre lo botones para información resumida.


Firewall


Controlar el acceso físico


Parches y actualizaciones



Desarrollar una política de seguridad


Proteger con contraseña los datos sensibles


Antivirus

- Los ataques de reconocimiento consisten en el descubrimiento y mapeo no autorizado de sistemas, servicios y vulnerabilidades.
- Los ataques de acceso explotan vulnerabilidades conocidas en servicios de autenticación, de FTP y web para ganar acceso a cuentas web, bases de datos confidenciales y otra información sensible.
- Los ataques de DoS envían un número extremadamente grande de solicitudes sobre la red o Internet. Estas solicitudes excesivas sobrecargan el dispositivo objetivo, degradando el rendimiento.
- Los ataques de reconocimiento, acceso y DoS son mitigados con técnicas, dispositivos y tecnologías específicas.

Haga clic sobre lo botones para información resumida.

CAPITULO 2 SEGURIDAD DE LOS DISPOSITIVOS DE RED

2.0 Introducción al capitulo

2.0.1 Introducción al capitulo

La seguridad el tráfico que sale de la red y escrutar el tráfico ingresante son aspectos críticos de la seguridad en redes. La seguridad del router de borde, que se conecta con la red externa, es un primer paso importante al asegurar la red.

El hardening de dispositivos es una tarea esencial que nunca debe ser pasada por alto. Significa implementar métodos probados para asegurar el router físicamente y proteger el acceso administrativo utilizando la interfaz de línea de comandos (command-line interface - CLI) del IOS Cisco así como también el Administrador de Routers y Dispositivos de Seguridad de Cisco (Cisco Router and Security Device Manager - SDM). Algunos de estos métodos comprenden la seguridad del acceso administrativo, incluyendo mantener contraseñas, configurar funciones de identificación virtual mejoradas e implementar Secure Shell (SSH). Como no todo el personal de la tecnología de la información debería tener el mismo nivel de acceso a los dispositivos de infraestuctura, definir roles administrativos de acceso es otro aspecto importante de la seguridad los dispositivos de infraestructura.

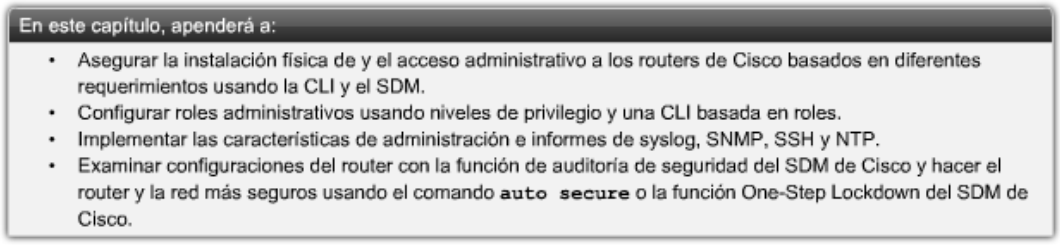
La seguridad de las funciones de administración y reportes del IOS de los dispositivos de Cisco también es importante. Las prácticas recomendadas para asegurar el syslog, utilizando el Protocolo de Administración de Redes Simple (Simple Network Management Protocol - SNMP), y configurando el Protocolo de Tiempo de Red (Network Time Protocol - NTP) son examinadas.

Muchos servicios del router están habilitados por defecto. Muchas de estas funciones están habilitadas por razones históricas pero ya no son necesarias. Este capítulo discute algunos de estos servicios y examina las configuraciones de router con la función de Auditoría de Seguridad del Cisco SDM. Este capítulo también examina la función one-step lockdown del Cisco SDM y el comando auto secure, que puede ser utilizado para automatizar las tareas de hardening de dispositivos.

La práctica de laboratorio del capítulo, Seguridad del router para acceso administrativo, es una práctica muy englobadora que presenta la oportunidad de practicar el amplio rango de funciones de seguridad presentadas en este capítulo. El laboratorio presenta los diferentes medios de asegurar el acceso administrativo a un router, incluyendo las buenas prácticas de contraseñas, una configuración de banner apropiada, funciones de identificación mejoradas y SSH. La función de acceso a la CLI basada en roles se basa en la creación de vistas como manera de proveer diferentes niveles de acceso a los routers. La función de Configuración Resistente del IOS de Cisco permite asegurar las imágenes de router y los archivos de configuración. Syslog y SNMP se utilizan para informes de administración. AutoSecure de Cisco es una herramienta automatizada para asegurar los routers Cisco utilizando la CLI. La función de Auditoría de Seguridad de SDI provee funcionalidades similares a AutoSecure. El laboratorio está en el manual de laboratorio en Academy Connection en **cisco.netacad.net.**

La actividad de Packet Tracer Configurar los Routers Cisco para Syslog, NTP y SSH, proporciona a los alumnos prácticas adicionales para implementar las tecnologías

presentadas en este capítulo. En particular, los alumnos configurarán con NTP, syslog, registro de mensajes con marca de tiempo, cuentas de usuario locales, conectividad SSH exclusiva y pares de claves RSA para servidores SSH. También se explora el uso del acceso del cliente SSH desde una PC Windows y desde un router Cisco. Las actividades de Packet Tracer para CCNA Security están disponibles en Academy Connection en cisco.netacad.net.



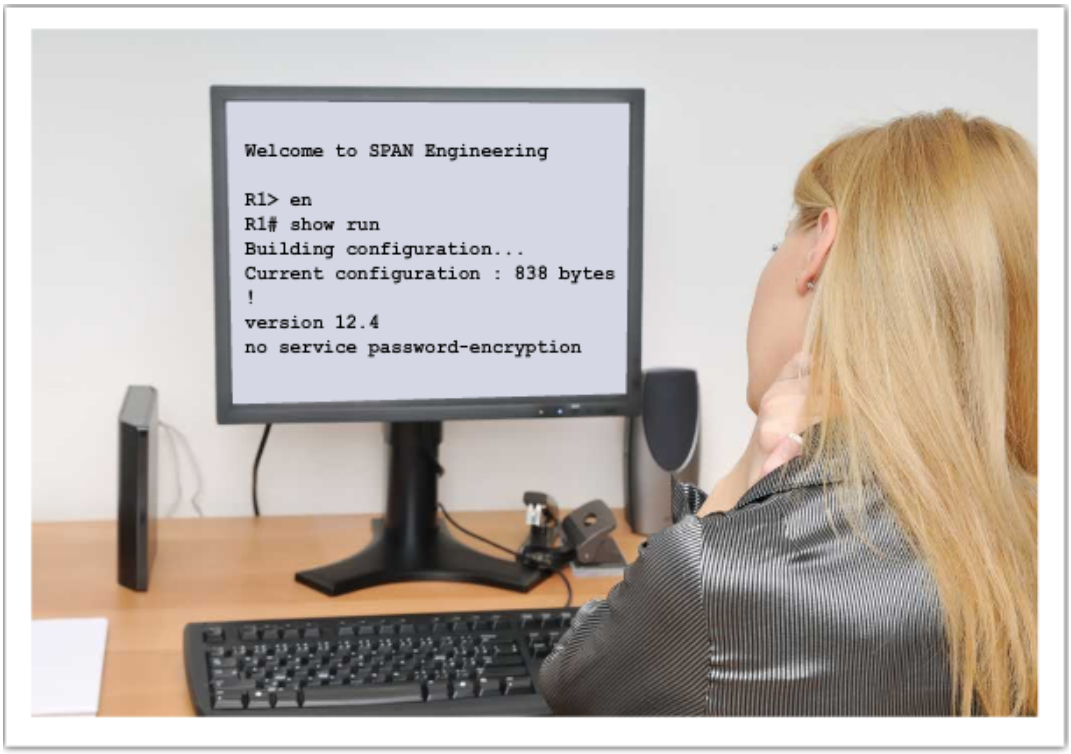
2.1.1 Seguridad del router de borde

La seguridad la infraestructura de la red es crítica para la seguridad de toda la red. La infraestructura de la red incluye routers, switches, servidores, estaciones de trabajo y otros dispositivos.

Considere un empleado descontento mirando casualmente por sobre el hombro del administrador de la red mientras el administrador se está identificando en el router de borde. Esto se conoce como shoulder surfing y es una manera sorprendentemente fácil para un atacante de ganar acceso no autorizado.

Si un atacante obtiene acceso a un router, la seguridad y la administración de toda la red pueden ser comprometidas, dejando a los servidores y las estaciones de trabajo bajo riesgo. Es crítico que las políticas y controles de seguridad apropiados puedan ser implementados para prevenir el acceso no autorizado a todos los dispositivos de la infraestructura. Aunque todos los dispositivos de una infraestructura están en riesgo, los routers generalmente son el objetivo principal para los atacantes de redes. Esto ocurre porque los routers actúan como la policía del tránsito, dirigiendo el tráfico hacia, desde y entre redes.

El router de borde es el último router entre la red interna y una red de confianza como Internet. Todo el tráfico a Internet de una organización pasa por este router de borde; por lo tanto, generalmente funciona como la primera y última línea de defensa de una red. A través del filtrado inicial y final, el router de borde ayuda a asegurar el perímetro de una red protegida. También es responsable de implementar las acciones de seguridad que están basadas en las políticas de seguridad de la organización. Por estas razones, es imperativo asegurar los routers de la red.



La implementación del router de borde varía en función del tamaño de la organización y la complejidad del diseño de red requerido. Las implementaciones de router pueden incluir un solo router protegiendo toda una red interna o un router como la primera línea de defensa en un enfoque de defensa profunda.

Enfoque de un solo router

En el enfoque de un solo router, un solo router conecta la red protegida, o LAN interna a Internet. Todas las políticas de seguridad están configuradas en este dispositivo. Generalmente se utiliza este esquema en implementaciones de sitios pequeños como sitios de sucursales y SOHO. En las redes más pequeñas, las funciones de seguridad requeridas pueden ser soportadas por ISRs sin comprometer el rendimiento del router.

Enfoque de defensa profunda

El enfoque de defensa profunda es más seguro que el de un solo router. En este enfoque, el router de borde actúa como la primera línea de defensa y se lo conoce como screening router. Envía al firewall todas las conexiones dirigidas a la LAN interna.

La segunda línea de defensa es el firewall. El firewall básicamente retoma donde dejó el router y realiza filtrado adicional. Provee control de acceso adicional ya que monitorea el estado de las conexiones, actuando como un dispositivo de control.

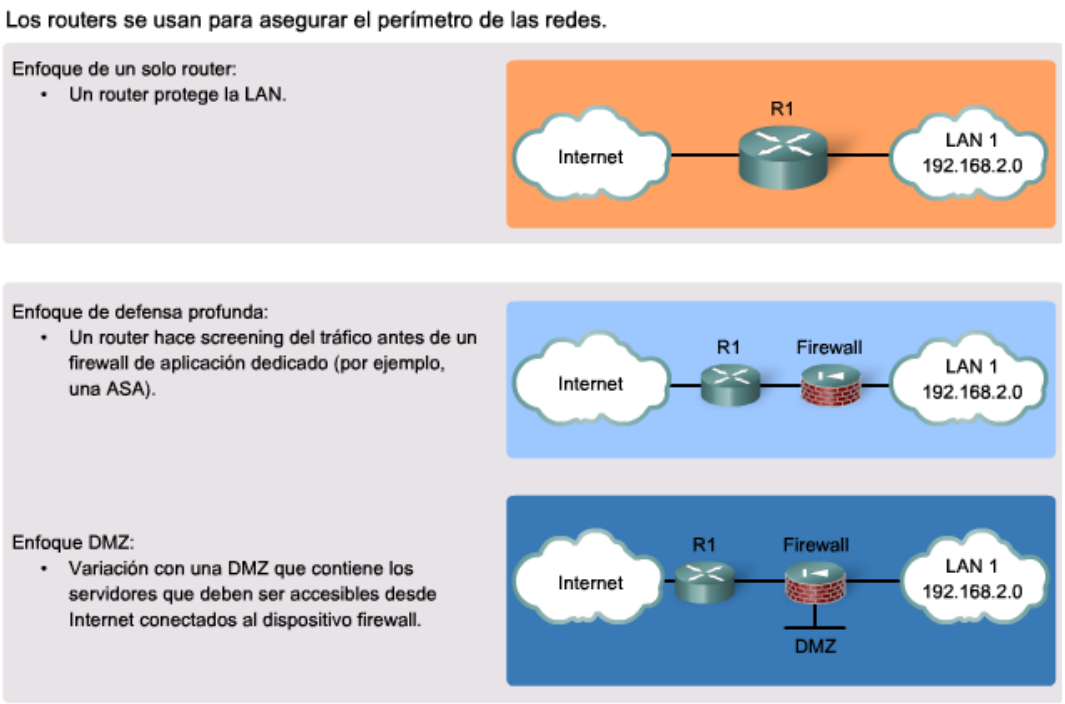
El router de borde tiene un conjunto de reglas que especifican qué tráfico permitir y qué tráfico denegar. Por defecto, el firewall deniega la iniciación de conexiones desde las redes externas (no confiables) para la red interna (confiable). Sin embargo, permite a los usuarios internos conectarse a las redes no confiables y permite que las respuestas vuelvan a través del firewall. También puede realizar autenticación de usuario (proxy de

autenticación) par que los usuarios tengan que estar autenticados para ganar acceso a los recursos de la red.

Enfoque DMZ

Una variante del enfoque de defensa profunda es ofrecer un área intermedia llamada zona desmilitarizada (demilitarized zone - DMZ). La DMZ puede ser utilizada para los servidores que tienen que ser accesibles desde Internet o alguna otra red externa. La DMZ puede ser establecida entre dos routers, con un router interno conectado a la red protegida y un router externo conectado a la red no protegida, o ser simplemente un puerto adicional de un solo router. El firewall, ubicado entre las redes protegida y no protegida, se instala para permitir las conexiones requeridas (por ejemplo, HTTP) de las redes externas (no confiables) a los servidores públicos en la DMZ. EL firewall sirve como protección primaria para todos los dispositivos en la DMZ. En el enfoque DMZ, el router provee protección filtrando algún tráfico, pero deja la mayoría de la protección a cargo del firewall.

(El foco de este curso está en las opciones de seguridad de ISR, incluyendo explicaciones sobre cómo configurar estas opciones. Con respecto a las Cisco Adaptive Security Appliance (ASA), la discusión se limita a implementar diseños. Para configuración de dispositivos ASA, véase **www.cisco.com**.)



Asegurar el router de borde es un primer paso crítico en la seguridad de la red. Si hay otros routers internos, también deben estar configurados con seguridad. Deben mantenerse tres áreas de seguridad de routers.

Seguridad física

Proveer seguridad física para los routers:

Ubicar el router y los dispositivos físicos que se conectan a él en un cuarto bajo llave que sea accesible solo para personal autorizado, esté libre de interferencia magnética o electrostática y tenga un sistema contra incendios y controles de temperatura y humedad.
Instalar un sistema de alimentación ininterrumpida (uninterruptible power supply - UPS) y mantener los componentes de repuesto disponibles. Esto reduce la posibilidad de un ataques de DoS a causa de pérdida de electricidad en el edificio.

Seguridad de los Sistemas Operativos

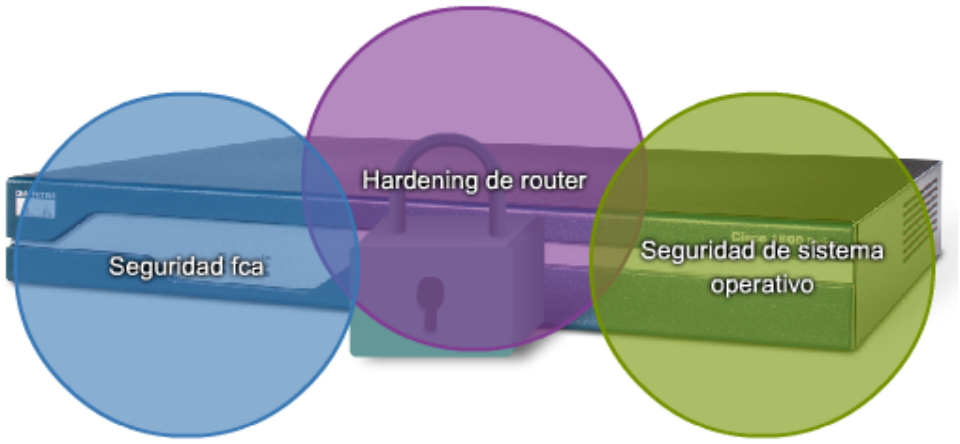
Seguridad de las funciones y rendimiento de los sistemas operativos del router:

Configurar el router con la máxima cantidad de memoria posible. La disponibilidad de la memoria puede ayudar a proteger la red de ataques de DoS, mientras que soporta el máximo rango de dispositivos de seguridad.
Usar la última versión estable del sistema operativo que cumpla los requerimientos de la red. Las funciones de seguridad de un sistema operativo evolucionan con el tiempo. Tenga en cuenta que la última versión de un sistema operativo puede no ser la versión más estable disponible.
Mantenga una copia segura de resguardo de la imagen del sistema operativo y el archivo de configuración del router.

Hardening del router

Elimine potenciales abusos de puertos y servicios no utilizados:

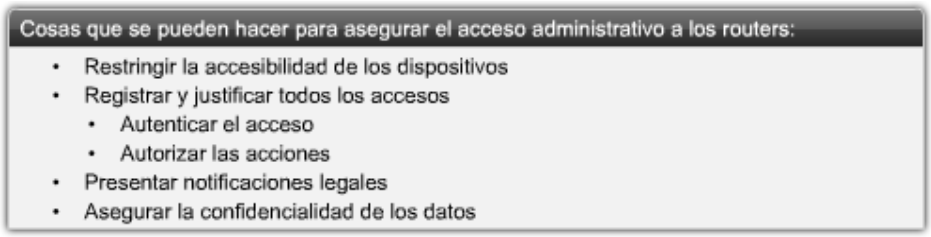
Asegure el control administrativo. Asegúrese de que solo personal autorizado tenga acceso y su nivel de acceso sea controlado.
Deshabilite puertos e interfaces no utilizadas. Reduzca la cantidad de maneras por las que puede accederse a un dispositivo.
Deshabilitar servicios innecesarios. Como muchas computadoras, el router tiene servicios habilitados por defecto. Algunos de estos servicios son innecesarios y pueden ser utilizados por un atacante para reunir información o para efectuar explotaciones.



El acceso administrativo es un requerimiento para la administración del router; por lo tanto, asegurar el acceso admiistrativo es una tarea extremadamente importante. Si una persona no autorizada ganara acceso administrativo a un router, esa persona podría alterar parámetros de enrutamiento, deshabilitar funciones de enrutamiento o descubrir y ganar acceso a otros sistemas en la red.

Se requieren muchas tareas importantes para asegurar el acceso administrativo a un dispositivo de una infraestructura:

Restringir la accesibilidad de los dispositivos - Limitar los puertos administrativos, restringir los comunicadores permitidos y restringir los métodos de acceso permitidos.
Registrar y justificar todos los accesos - Para propósitos de auditoría, registrar a todos los que acceden al dispositivo, incluyendo lo que ocurra durante el acceso y cuándo ocurre.
Acceso autenticado - Asegurarse de que el acceso sea otorgado solo a usuarios, grupos y servicios autenticados. Limitar el número de intentos de ingreso fallidos y el tiempo entre intentos.
Autorizar las acciones - Restringir las acciones y vistas permitidas a un usuario, grupo o servicio particular.
Presentar notificaciones legales - Mostrar una notificación legal, desarrollada en conjunto con el consejo legal de la empresa, para sesiones interactivas.
Asegurar la confidencialidad de los datos - Proteger los datos sensibles almacenados localmente de ser vistos o copiados. Considerar la vulnerabilidad de los datos en tránsito sobre un canal de comunicación expuestos a sniffing, secuestros de sesión y ataques man in the middle (MITM).



Hay dos maneras de acceder a un dispositivo para propósitos administrativos: local y remotamente.

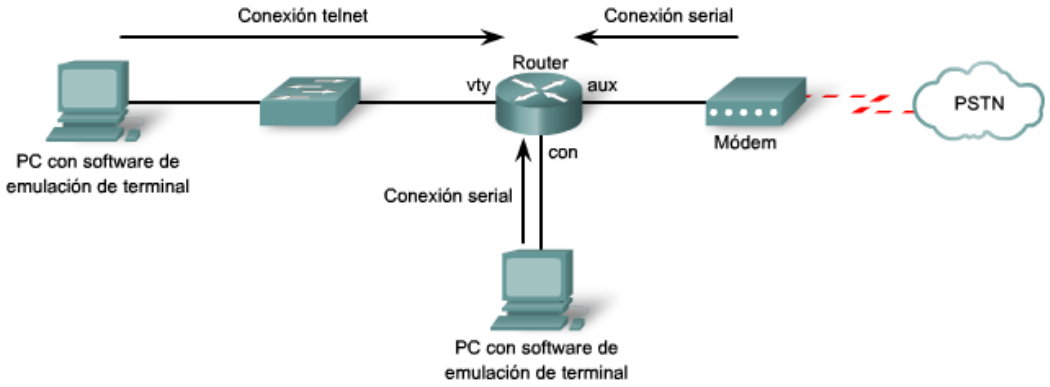
Todos los dispositivos de la infraestructura de la red puede ser accedidos localmente. El acceso local a un router usualmente requiere una conexión directa a un puerto de consola en el router de Cisco utilizando una computadora que esté ejecutando software de emulación de terminal.

Algunos dispositivos de red pueden ser accedidos remotamente. El acceso remoto típicamente requiere permitir conexiones Telnet, Secure Shell (SSH), HTTP, HTTPS o Simple Network Management Protocol (SNMP) al router desde una computadora. Esta computadora puede estar en la misma subred o en una diferente. Algunos protocolos de acceso remoto envían al router los datos en texto plano, incluyendo nombres de usuario y contraseñas. Si un atacante logra reunir tráfico de red mientras un administrador está autenticado remotamente a un router, el atacante podrá capturar las contraseñas o información de configuración del router.

Por esta razón, se prefiere permitir solo acceso local al router. Sin embargo, el acceso remoto puede ser necesario de cualquier forma. Cuando se accede a la red remotamente, deben tomarse algunas precauciones:

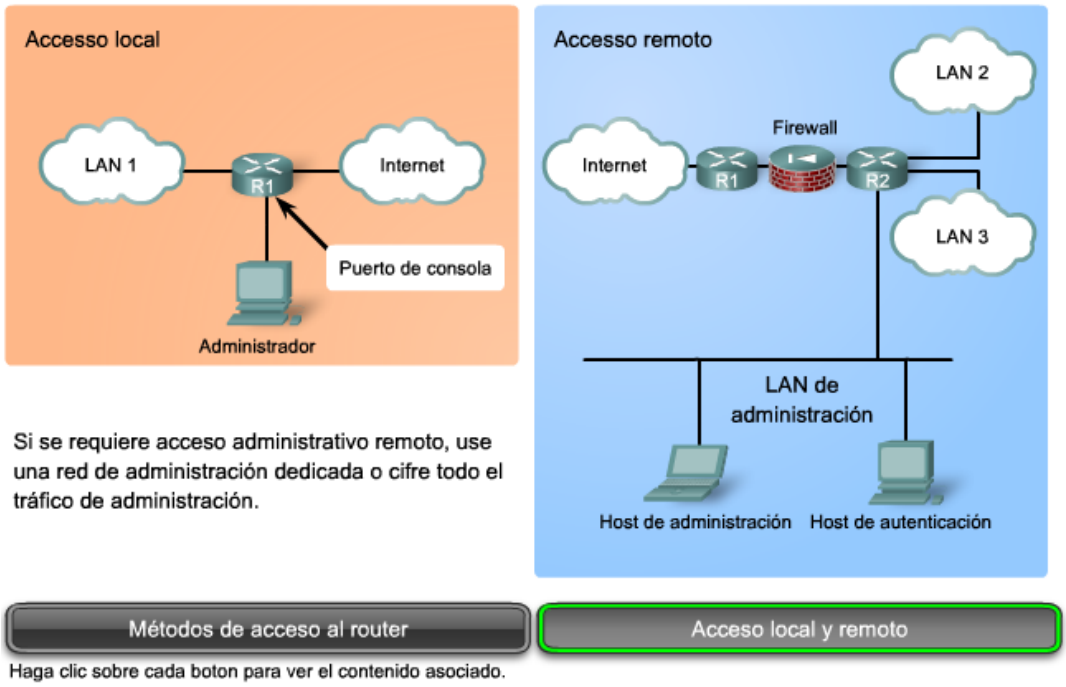
Cifrar todo el tráfico entre la computadora del administrador y el router. Por ejemplo, en lugar de usar Telnet, usar SSH. O en lugar de usar HTTP, usar HTTPS.
Establecer una red de administración dedicada. La red de administración deberá incluir solo hosts de administración identificados y conexiones a una interfaz dedicada en el router.
Configurar un filtro de paquetes para permitir que solo los hosts de administración identificados y protocolos de preferencia accedan al router. Por ejemplo, permitir solo solicitudes SSH de la dirección IP del host de administración para iniciar una conexión a los routers en la red.

Estas precauciones son valiosas, pero no protegen enteramente a la red. Otras líneas de defensa deben ser implementadas también. Una de las más básicas e importantes es el uso de una contraseña segura.



Métodos de acceso al router | Acceso local y remoto

Haga clic sobre cada boton para ver el contenido asociado.



2.1.2 Configuración de un acceso administrativo seguro

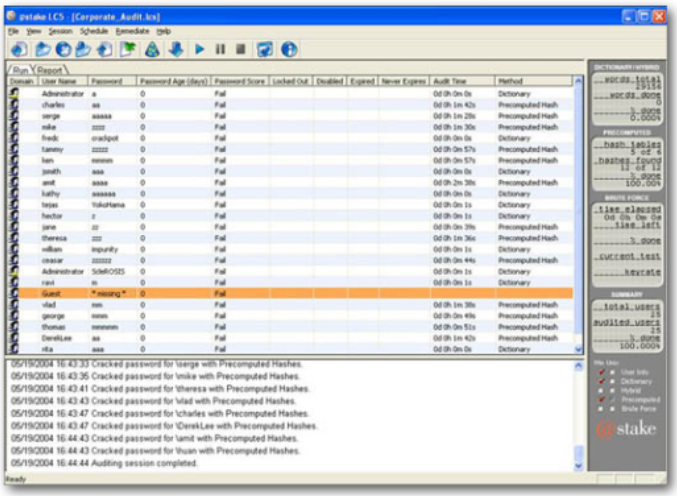
Los atacantes usan varios métodos de descubrimiento de contraseñas administrativas. Pueden hacer shoulder surfing, intentar adivinar las contraseñas basándose en la información personal del usuario, o hacer sniffing de los paquetes TFTP que contienen archivos de configuración en texto plano. Los atacantes también pueden usar herramientas como L0phtCrack y Cain & Abel para efectuar ataques de fuerza bruta para adivinar las contraseñas.

Para proteger bienes como routers y switches, siga estos consejos comunes para elegir contraseñas fuertes. Estos consejos han sido diseñados para hacer que las contraseñas sean menos fácilmente descubiertas por medio de herramientas de cracking y de adivinación inteligente:

Utilice una contraseña de 10 o más caracteres de longitud. Cuanto más larga, mejor.
Haga a su contraseña compleja. Incluya una mezcla de letras mayúsculas y minúsculas, símbolos y espacios.
Evite contraseñas basadas en repeticiones, palabras de diccionario, secuencias de letras o números, nombres de usuario, nombres de mascotas o parientes, información biográfica (como cumpleaños, número de pasaporte o documento, nombres de ancestros) u otros tipos de información fácilmente identificable.
Escriba la contraseña deliberadamente mal, realizando algunos reemplazos de letras. Por ejemplo, Smith = Smyth = 5mYth o Security = 5ecur1ty.
Cambie las contraseñas seguido. Si una contraseña está comprometida sin su conocimiento, la ventana de oportunidad para que el ataque la use será limitada.
No escriba las contraseñas en papel o las deje en lugares obvios como el escritorio o el monitor.

En los routers Cisco y muchos otros sistemas, los espacios antes de la contraseña son ignorados, no así los espacios dentro de la contraseña. Por lo tanto, un método para crear una contraseña fuerte es utilizar la barra espaciadora en la contraseña y crear una frase compuesta de varias palabras. Esto se denomina frase de acceso. La frase de acceso es generalmente más fácil de recordar que una simple contraseña. También es más larga y más difícil de adivinar.

Los administradores deben asegurarse de que se usen contraseñas fuertes en toda la red. Una manera de lograr esto es usando las mismas herramientas de ataques de fuerza bruta y cracking que usaría un atacante para verificar la solidez de las contraseñas.



Ataque de fuerza bruta | Contraseñas fuertes y débiles

Haga clic sobre los botones para ver el contenido asociado.

Contraseña débil	Por qué es débil
secret	Contraseña simple de diccionario.
smith	Nombre de soltera de la madre.
toyota	Marca de auto.
bob1967	Nombre y fecha de nacimiento del usuario.
Blueleaf23	Palabras y números simples.

Contraseña fuerte	Por qué es fuerte
b67n42d39c	Combina caracteres alfanuméricos.
12^h u4@1p7	Combina caracteres alfanuméricos, símbolos e incluye un espacio.

Ataque de fuerza bruta | Contraseñas fuertes y débiles

Haga clic sobre los botones para ver el contenido asociado.

Muchos puertos de acceso requieren contraseñas en un router Cisco, incluyendo el puerto de consola, el puerto auxiliar y las conexiones de terminal virtual. La administración de las contraseñas en una red grande debería mantenerse por medio de un servidor de autenticación central TACACS+ o RADIUS como el Servidor de Control de Acceso Seguro de Cisco (ACS). Todos los routers deben ser configurados con las contraseñas de usuario y de EXEC privilegiado. También se recomienda el uso de una base de datos de nombres de usuario local como copia de resguardo si el acceso a un servidor de autenticación, autorización y registro de auditoría (authentication, authorization, and accounting - AAA) se encuentra comprometido. El uso de una contraseña y la asignación de niveles de privilegios son maneras simples de proporcionar control de acceso terminal en una red. Deben establecerse contraseñas para el modo de acceso EXEC privilegiado y líneas individuales como las líneas de consola y auxiliar.

Contraseña enable secret

El comando de configuración enable secret contraseña restringe el acceso al modo EXEC privilegiado. La contraseña enable secret siempre está dispersa (hashed) dentro de la configuración del router usando un algoritmo Message Digest 5 (MD5). Si la contraseña enable secret se pierde o se olvida, debe ser reemplazada utilizando el procedimiento de recuperación de contraseñas de los routers Cisco.

línea de consola

Por defecto, el puerto de línea de consola no requiere una contraseña para el acceso administrativo de la consola; sin embargo, siempre debe ser configurado con una contraseña a nivel de línea de puerto de consola. Use el comando line console 0 seguido de los subcomandos login y password para solicitar el ingreso y establecer una contraseña de ingreso en la línea de consola.

líneas de terminal virtual

Por defecto, los routers de Cisco soportan hasta cinco sesiones simultáneas de terminal virtual vty (Telnet o SSH). En el router, los puertos vty se numeran del 0 al 4. Use el comando line vty 0 4 seguido por los subcomandos login y password para solicitar ingreso y establecer una contraseña de ingreso a las sesiones Telnet entrantes.

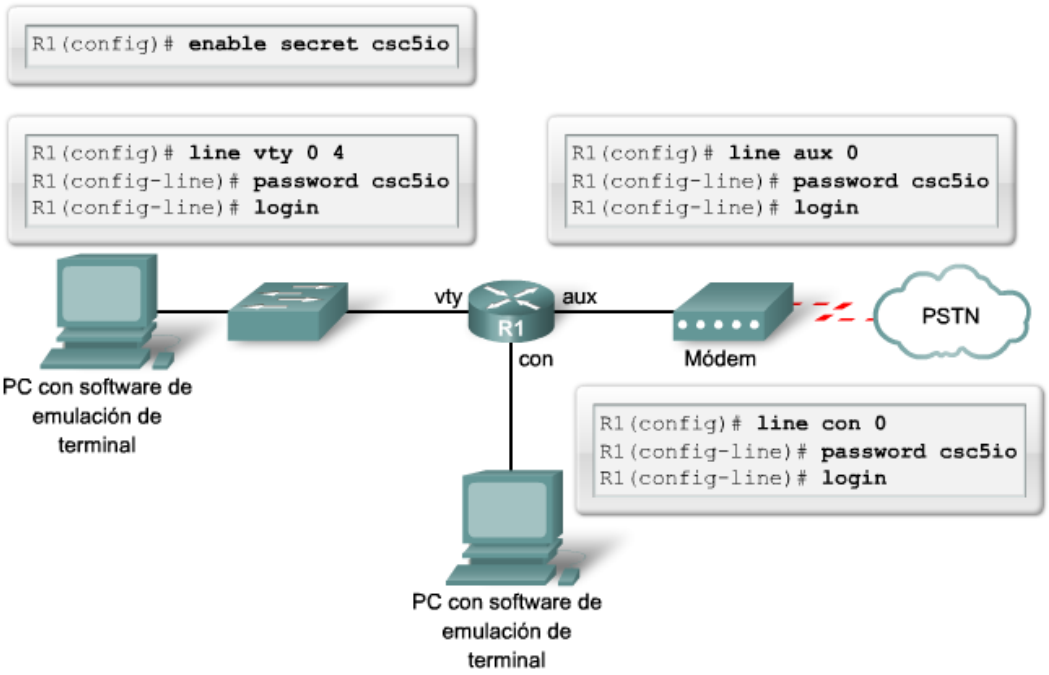
línea auxiliar

Por defecto, los puertos auxiliares del router no requieren una contraseña para acceso administrativo remoto. Los administradores algunas veces usan este puerto para configurar y monitorear remotamente el router usando una conexión de módem dialup.

Para acceder a la línea auxiliar, use el comando line aux 0. Use los subcomandos login y password para solicitar ingreso y establecer una contraseña de ingreso a las conexiones entrantes.

Por defecto, con excepción de la contraseña enable secret, todas las contraseñas de router de Cisco están almacenadas en texto plano dentro de la configuración del router. Estas contraseñas pueden ser visualizadas con el comando show running-config. Los

sniffers también pueden ver estas contraseñas si los archivos de configuración de servidor TFTP atraviesan una conexión no asegurada de intranet o Internet. Si un intruso gana acceso al servidor TFTP donde están almacenados los archivos de configuración del router, podrá obtener estas contraseñas.



Para aumentar la seguridad de las contraseñas, debe configurarse lo siguiente:

Establecer longitudes mínimas de contraseñas.
Deshabilitar conexiones no utilizadas.
Cifrar todas las contraseñas en el archivo de configuración.

Longitud de caracteres mínima

A partir de la Release 12.3(1) del IOS de Cisco, los administradores pueden especificar la longitud de caracteres mínima para todas las contraseñas de routers con un valor de 0 a 16 caracteres usando el comando de configuración global security passwords min-length longitud. Se recomienda fuertemente establecer la longitud mínima de la contraseña en 10 caracteres, para eliminar contraseñas comunes que resultan cortas y prevalecen en la mayoría de las redes, como "lab" y "cisco".

Este comando afecta las contraseñas de usuario, las enable secret y las de línea que se creen luego de que el comando sea ejecutado. Las contraseñas de router ya existentes no son afectadas. Cualquier intento de crear una nueva contraseña que contenga menos caracteres que la longitud especificada fallará y se mostrará un mensaje de error similar al siguiente:

Password too short - must be at least 10 characters. Password configuration failed.

Deshabilitar conexiones no utilizadas

Por defecto la interfaz administrativa permanece activa y autenticada por 10 minutos luego de la última actividad de la sesión. Luego de eso, la sesión caduca y se cierra.

Si un administrador está lejos de la terminal mientras la conexión de la consola permanece activa, una atacante tendrá hasta 10 minutos para ganar acceso privilegiado. Se recomienda, por lo tanto, que estos relojes sean ajustados para limitar la cantidad de tiempo a un máximo de dos a tres minutos. Estos relojes pueden ser ajustados usando el comando exec-timeout modo de configuración de línea para cada uno de los tipos de línea utilizado.

También es posible deshabilitar el proceso exec para una línea específica, como el puerto auxiliar, usando el comando no exec dentro del modo de configuración del línea. Este comando permite solo conexiones salientes en la línea. El comando no exec permite deshabilitar el proceso EXEC para conexiones que pueden intentar enviar datos no solicitados al router.

Cifrar todas las contraseñas

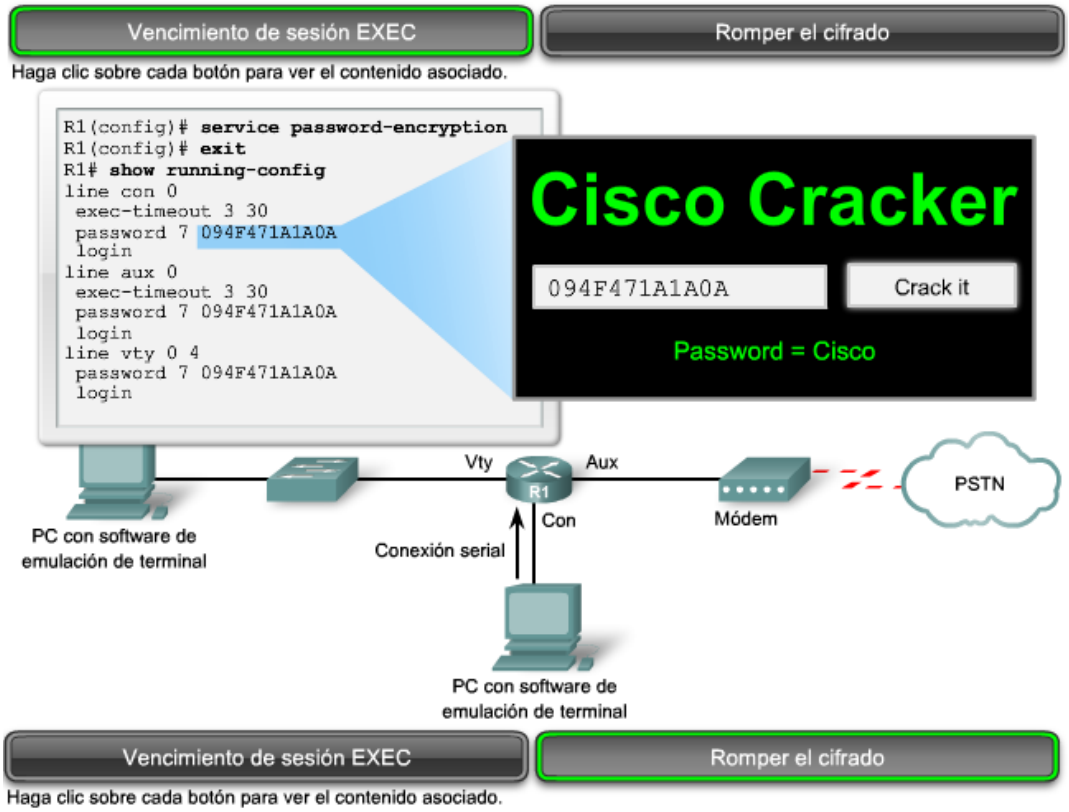
Por defecto, algunas contraseñas se muestran en texto plano, o sea, sin cifrar, en la configuración del software IOS de Cisco. Con excepción de la contraseña enable secret, todas las otras contraseñas en texto plano en el archivo de configuración pueden ser cifradas con el comando service password-encryption. Este comando dispersa contraseñas en texto plano actuales y futuras en el archivo de configuración a un texto cifrado. Para detener el proceso de cifrado de las contraseñas, use la forma no del comando. Solo las contraseñas creadas luego de que se emita el comando no serán no cifradas. Las contraseñas ya existentes que estén cifradas permanecerán de esa manera.

El comando service password-encryption es útil principalmente para evitar que individuos no autorizados puedan ver contraseñas en el archivo de configuración. El algoritmo utilizado por el comando service password-encryption es simple y fácilmente reversible por alguien que tenga acceso al texto cifrado y una aplicación de cracking de contraseñas. Por esta razón, el comando no deberá ser utilizado con la intención de proteger los archivos de configuración contra ataques serios.

El comando enable secret es mucho más seguro, ya que cifra la contraseña utilizando MD5, un algoritmo mucho más fuerte.

```
router(config-line)#
exec-timeout minutes [seconds]
```

Parámetro	Descripción
minutes	Este entero especifica el número de minutos sin actividad antes de que la sesión expire.
seconds	(Opcional) Este entero especifica el intervalo de tiempo adicional en segundos .



Otra función de seguridad disponible es la autenticación. Los routers de Cisco mantienen una lista de nombres de usuario y contraseñas en una base de datos local en el router para realizar autenticación local. Hay dos métodos para configurar nombres de usuario de cuentas locales.

username nombre password contraseña

username nombre secret contraseña

El comando username secret es más seguro porque usa el algoritmo más fuerte, MD5, para dispersar las claves. MD5 es un algoritmo mucho mejor que el tipo 7 estándar utilizado por el comando service password-encryption. La capa agregada de protección que proporciona MD5 es útil en ambientes en los que la contraseña atraviesa la red o es

almacenada en un servidor TFTP. Tenga en consideración que al configurar una combinación de nombre de usuario y contraseña deben seguirse las restricciones de longitud de contraseña. Use el comando login local en la configuración de linea para habilitar la base de datos local para autenticación.

Todos los ejemplos restantes en este capítulo usan la configuración username secret en lugar de username password.

```
router(config)#
username name secret {[0] password | 5 encrypted-secret}
```

Parámetro	Descripción
name	Este parámetro especifica el nombre de usuario.
0	(Opcional) Esta opción indica que la contraseña en texto plano deberá ser dispersa por el router usando MD5.
password	Este parámetro es la contraseña en texto plano que será dispersa usando MD5.
5	Este parámetro indica que la contraseña encrypted-secret ha sido dispersa usando MD5.
encrypted-secret	Este parámetro representa la contraseña encrypted-secret MD5 que se encuentra almacenada como contraseña de usuario cifrada.

Comando username | Configuración ejemplo

Haga clic en cada botón para ver el contenido asociado.

```
R1(config)# service password-encryption
R1(config)# username JR-ADMIN password letmein
% Password too short - must be at least 10 characters. Password
configuration failed
R1(config)# username JR-ADMIN password cisco12345
R1(config)# username ADMIN secret cisco54321
R1(config)# line con 0
R1(config-line)# login local
```

```
R1# show run | include username
username JR-ADMIN password 7 060506324F41584B564347
username ADMIN secret 5 $1$G3oQ$hEvsd5iz76WJuSJvtzs8I0
R1#
```

```
R1 con0 is now available

Press RETURN to get started.

User Access Verification

Username: ADMIN
Password:
R1>
```

Comando username | Configuración ejemplo

Haga clic en cada botón para ver el contenido asociado.

2.1.3 Configuracion de seguridad mejorada para autenticación virtual

Asignar contraseñas y autenticación local no evita que un dispositivo pueda ser objetivo de un ataque. Los ataques de DoS inundan los dispositivos con tantas solicitudes de conexión que el dispositivo puede no proveer un servicio normal de autenticación para los administradores legítimos del sistema. El ataque de diccionario, usado para conseguir acceso administrativo a un sistema, inunda al dispositivo con cientos de combinaciones de usuario y contraseña. El resultado final es muy parecido al del ataque de DoS, ya que el dispositivo no puede procesar las solicitudes de usuarios legítimos. La red necesita tener sistemas para detectar y ayudar a prevenir estos ataques.

Habilitando un perfil de detección, el dispositivo de red puede ser configurado para reaccionar a repetidos intentos de ingreso fallidos con un rechazo a las solicitudes de conexión subsiguientes (login blocking). Este bloqueo puede ser configurado para un período de tiempo que se denomina período silencioso (quiet period). Durante un período silencioso se permiten los intentos de conexión legítimos por medio de la configuración de una lista de control de acceso (access control list - ACL) con las direcciones asociadas con los administradores de sistemas.

La función de identificación mejorada del IOS Cisco proporciona más seguridad para los dispositivos IOS al crear una conexión virtual como Telnet, SSH o HTTP, ya que hace más lentos los ataques de diccionario y detiene los ataques de DoS. Para configurar mejor la seguridad de las conexiones de ingreso virtuales, el proceso de autenticación deberá ser configurado con parámetros específicos:

Retardos entre intentos de ingreso sucesivos
Cierre de sesión si se sospechan ataques de DoS
Generación de mensajes de registro del sistema para detección de sesiones

Estas mejoras no se aplican a las conexiones de consola. Se asume que solo el personal autorizado tendrá acceso físico a los dispositivos.



Se dispone de los siguientes comandos para configurar un dispositivo IOS de Cisco para que soporte las funciones de ingreso mejoradas.

Router# configure terminal

Router(config)# login block-for segundos attempts intentos within segundos

Router(config)# login quiet-mode access-class {acl-nombre | acl-número}

Router(config)# login delay segundos

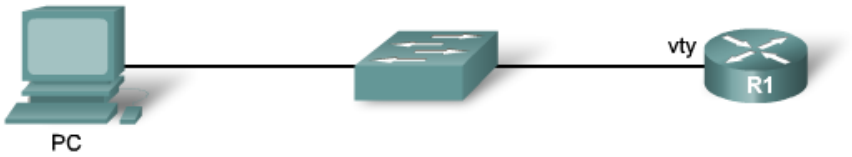
Router(config)# login on-failure log [every login]

Router(config)# login on-success log [every login]

La autenticación en las líneas vty debe ser configurada para usar una combinación de nombre de usuario y contraseña. Si se configuran las líneas para usar solo una contraseña, no se habilitarán las funciones de ingreso mejoradas.

¿Qué hace cada comando?

```
R1# configure terminal
R1(config)# username ADMIN secret cisco54321
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# exit
R1(config)# login block-for 15 attempts 5 within 60
R1(config)# ip access-list standard PERMIT-ADMIN
R1(config-std-nacl)# remark Permit only Administrative hosts
R1(config-std-nacl)# permit 192.168.10.10
R1(config-std-nacl)# permit 192.168.11.10
R1(config-std-nacl)# exit
R1(config)# login quiet-mode access-class PERMIT-ADMIN
R1(config)# login delay 10
R1(config)# login on-success log
R1(config)# login on-failure log
R1(config)# exit
```



Por defecto, todas las funciones de ingreso mejoradas están deshabilitadas. Use el comando login block-for para habilitarlas.

La función login block-for monitorea la actividad de inicio de sesión en el dispositivo y opera en dos modos:

Modo normal (de vigilancia) - El router cuenta la cantidad de intentos de ingreso fallidos dentro de una cantidad de tiempo determinada.

Modo silencioso (período silencioso) - Si el número de ingresos fallidos sobrepasa el umbral configurado, todos los intentos de ingreso de Telnet, SSH y HTTP serán denegados.

Cuando se habilita el modo silencioso, no se permite ningún intento de ingreso, incluso el acceso administrativo válido. Sin embargo, este comportamiento puede esquivarse para proporcionar acceso a los hosts críticos en todo momento mediante el uso de una ACL. La ACL debe ser creada e identificada usando el comando login quiet-mode access-class.

Por defecto, los dispositivos IOS de Cisco pueden aceptar conexiones, como Telnet, SSH y HTTP, tan rápidamente como pueden éstas ser procesadas. Esto hace a los dispositivos susceptibles a herramientas de ataque de diccionario como Cain o L0phtCrack, que son capaces de ejecutar miles de intentos de contraseña por segundo. El comando login block-for invoca un retraso de un segundo entre intentos de ingreso. El atacante tendrá que esperar un segundo antes de probar con otra contraseña.

Este tiempo de retraso puede modificarse mediante el comando login delay. El comando login delay introduce un retraso uniforme entre intentos sucesivos de ingreso. El retraso ocurre en todos los intentos de ingreso, tanto fallidos como exitosos.

Los comandos login block-for, login quiet-mode access-class y login delay ayudan a bloquear los intentos de ingreso fallidos por un período de tiempo limitado, pero no pueden evitar que el atacante intente nuevamente. ¿Cómo puede un administrador saber cuándo alguien intenta ganar acceso a la red adivinando la contraseña?

En este ejemplo se deshabilitará el inicio de sesión por 120 segundos (2 minutos) si ocurren más de 5 ingresos fallidos en un período de 60 segundos.

```
R1(config)# login block-for 120 attempts 5 within 60
```

- Este comando debe ser emitido antes que cualquier otro comando **login**. Este comando puede ayudar a proporcionar detección y prevención de DoS.

login block-for | login quiet-mode | login delay

Haga clic en los botones para ver los comandos. Pase sobre las partes resaltadas del comando para más información.

Este ejemplo muestra una configuración que invoca una ACL denominada PERMIT-ADMIN. Los hosts que concuerden con las sentencias de PERMIT-ADMIN están exentos del modo silencioso.

```
R1(config)# ip access-list standard PERMIT-ADMIN
R1(config-std-nacl)# remark Permit only Administrative hosts
R1(config-std-nacl)# permit 192.168.10.10
R1(config-std-nacl)# permit 192.168.11.10
R1(config-std-nacl)# exit
R1(config)# login quiet-mode access-class PERMIT-ADMIN
```

- Los comandos especifican una ACL aplicada al router cuando cambia al modo silencioso e identifica hosts exentos del tiempo de fallos del modo silencioso.
- Si no se configuran, todas las solicitudes de inicio de sesión serán denegadas durante el modo silencioso.

login block-for | login quiet-mode | login delay

Haga clic en los botones para ver los comandos. Pase sobre las partes resaltadas del comando para más información.

El ejemplo configura un retraso de 3 segundos entre intentos de ingreso sucesivos.

```
R1(config)# login delay 3
```

- Ayuda a mitigar ataques de diccionario
- Este es un comando opcional. Si no se configura, se instituirá el retraso por defecto de un segundo luego de que se configure el comando **login block-for**.

login block-for | login quiet-mode | login delay

Haga clic en los botones para ver los comandos. Pase sobre las partes resaltadas del comando para más información.

El comando auto secure habilita el registro de mensajes para intentos fallidos de ingreso. El registro de intentos de ingreso exitosos no está habilitado por defecto.

Estos comandos pueden ser utilizados para mantener un registro del número de intentos de ingreso exitosos y fallidos.

login on-failure log [every login] genera registros para las solicitudes de ingreso fallidas.

login on-success log [every login] genera mensajes en el registro para las solicitudes de ingreso exitosas.

El número de intentos de ingreso antes de que se genere un mensaje puede especificarse mediante el parámetro [every login]. El valor por defecto es 1. El rángo válido va de 1 a 65,535.

Como alternativa, el comando security authentication failure rate tasa umbral log genera un mensaje en el registro cuando se excede la tasa de fallos de inicio de sesión.

Para verificar que el comando login block-for esté configurado y el modo en el que está el router, use el comando show login. El router puede estar en modo normal o silencioso, dependiendo de si se ha excedido el umbral de intentos de ingreso.

El comando show login failures muestra más información en relación a los intentos fallidos, como la dirección IP de la que se originó el intento de ingreso fallido.

```
R1(config)# login on-success log [every login]
R1(config)# login on-failure log [every login]
R1(config)# exit
```

Comandos log | show login Modo normal | Ataque Ejemplo | show login Modo silencioso | show login failures

Haga clic en cada botón y pase sobre el texto resaltado para más información.

En este ejemplo se configuró el comando **`login block-for`** para bloquear el ingreso de hosts por 120 segundos si más de 5 solicitudes fallan dentro de un período de 60 segundos.

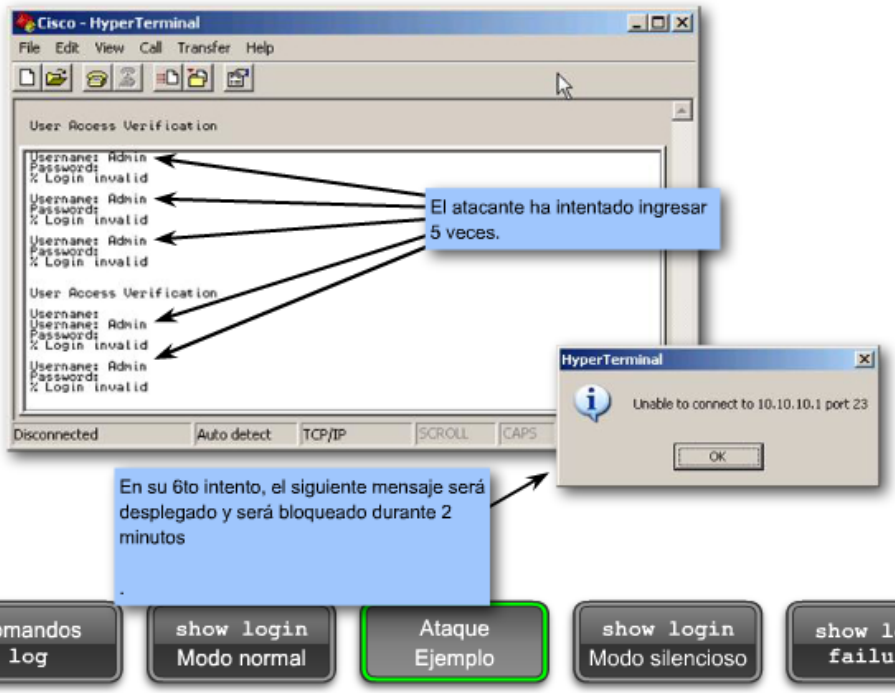
```
R1# show login
     A login delay of 10 seconds is applied.
     Quiet-Mode access list PERMIT-ADMIN is applied.

     Router enabled to watch for login Attacks.
     If more than 5 login failures occur in 60 seconds or less,
     logins will be disabled for 120 seconds.

     Router presently in Normal-Mode.
     Current Watch Window
         Time remaining: 5 seconds.
         Login failures for current window: 4.
     Total login failures: 4.
```

Comandos log | show login Modo normal | Ataque Ejemplo | show login Modo silencioso | show login failures

Haga clic en cada botón y pase sobre el texto resaltado para más información.



Comandos log | show login Modo normal | Ataque Ejemplo | show login Modo silencioso | show login failures

Haga clic en cada botón y pase sobre el texto resaltado para más información.

```
R1#
*Dec 10 15:38:54.455: %SEC_LOGIN-1-QUIET_MODE_ON: Still timeleft for
watching failures is 12 secs, [user: admin] [Source: 10.10.10.10]
[localport: 23] [Reason: Login Authentication Failed - BadUser] [ACL:
PERMIT-ADMIN] at 15:38:54 UTC Wed Dec 10 2008
R1# show login
     A login delay of 3 seconds is applied.
     Quiet-Mode access list PERMIT-ADMIN is applied.

     Router enabled to watch for login Attacks.
     If more than 5 login failures occur in 60 seconds or less,
     logins will be disabled for 120 seconds.

     Router presently in Quiet-Mode.
     Will remain in Quiet-Mode for 105 seconds.
     Restricted logins filtered by applied ACL PERMIT-ADMIN.
R1#
```

Comandos log | show login Modo normal | Ataque Ejemplo | show login Modo silencioso | show login failures

Haga clic en cada botón y pase sobre el texto resaltado para más información.

```
R1# show login failures
Total failed logins: 22
Detailed information about last 50 failures

Username        SourceIPAddr    lPort Count TimeStamp
admin           1.1.2.1         23    5     15:38:54 UTC Wed Dec 10 2008
Admin           10.10.10.10     23    13    15:58:43 UTC Wed Dec 10 2008
admin           10.10.10.10     23    3     15:57:14 UTC Wed Dec 10 2008
cisco           10.10.10.10     23    1     15:57:21 UTC Wed Dec 10 2008

R1#
```

Comandos log | show login Modo normal | Ataque Ejemplo | show login Modo silencioso | show login failures

Haga clic en cada botón y pase sobre el texto resaltado para más información.

Use mensajes banner para presentar una notificación legal a los potenciales intrusos para informarles que no son bienvenidos en esa red. Los banners son muy importantes para la red desde una perspectiva legal. Ha habido casos en que los intrusos han ganado en la corte porque no se toparon con mensajes de advertencia apropiados al acceder a redes enrutadas. Además de advertir a intrusos potenciales, los banners también pueden ser utilizados para informar a administradores remotos de las restricciones de uso.

La elección del contenido de los mensajes banner es importante y debe ser revisada por un asesor legal antes de colocarse en routers de red. Nunca use la palabra "bienvenido" o algún otro saludo familiar que puede ser sacado de contexto o entendido como una invitación para usar la red.

Los banners están deshabilitados por defecto y deben ser habilitados explícitamente. Use el comando banner desde el modo de configuración global para especificar mensajes apropiados.

banner {exec | incoming | login | motd | slip-ppp} d message d

Los tokens son opcionales y pueden ser utilizados en la sección del mensaje del comando banner:

$(hostname) - Muestra el nombre de host del router.

$(domain) - Muestra el nombre de dominio del router.

$(line) - Muestra los números de línea vty o tty (asíncrona).

$(line-desc) - Muestra la descripción de la línea.

Tenga cuidado al colocar esta información en el router, ya que provee más información a un potencial intruso.

También se puede usar el SDM de Cisco para configurar mensajes de banner.



Parámetros del comando | Banner ejemplo

Haga clic en cada botón y pase sobre el texto resaltado para más información.



Parámetros del comando | Banner ejemplo

Haga clic en cada botón y pase sobre el texto resaltado para más información.

2.1.4 Configuración de SSH

Al permitir el acceso administrativo remoto, también es importante considerar las implicancias de seguridad al enviar información a través de la red. Tradicionalmente, el acceso remoto en los routers era configurado usando Telnet sobre el puerto 23 de TCP. Sin embargo, Telnet fue desarrollado cuando la seguridad no era un problema, por lo tanto, todo el tráfico de Telnet se envía en texto plano. Al usar este protocolo, los datos críticos, como configuraciones del router, son de fácil acceso para los atacantes. Los hackers pueden capturar paquetes reenviados por la computadora de un administrador usando un analizador de protocolos como Wireshark. Si el atacante captura el flujo Telnet inicial, podrá aprender el nombre de usuario y la contraseña del administrador.

Sin embargo, el acceso remoto puede ahorrarle tiempo y dinero a una organización a la hora de hacer cambios necesarios en la configuración. Entonces, ¿cómo puede establecerse una conexión de acceso remoto segura para administrar dispositivos IOS de Cisco?

SSH ha reemplazado a Telnet como práctica recomendada para proveer administración de router remota con conexiones que soportan confidencialidad e integridad de la sesión. Provee una funcionalidad similar a una conexión Telnet de salida, con la excepción de que la conexión está cifrada y opera en el puerto 22. Con autenticación y cifrado, SSH permite comunicaciones seguras sobre una red no segura.

Deben completarse cuatro pasos antes de configurar un router para el protocolo SSH:

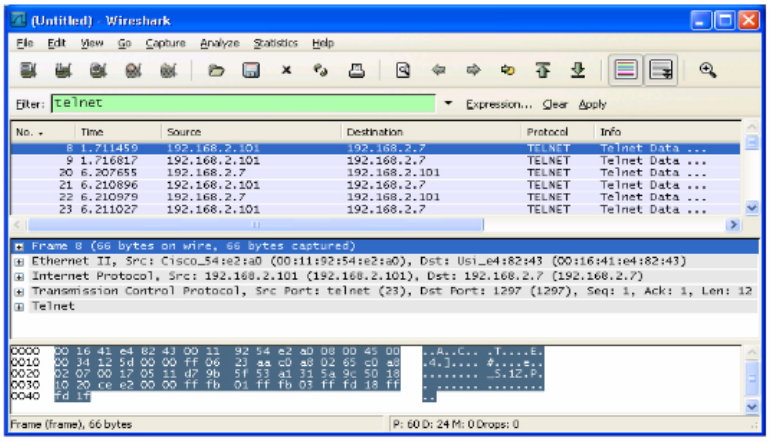
Paso 1. Asegurarse de que los routers destino estén ejecutando una imagen del IOS de Cisco release 12.1(1)T o posterior, para que soporten SSH. Solo las imágenes criptográficas del IOS de Cisco que contienen el grupo de funciones IPsec soportan SSH. Específicamente, las imágenes criptográficas del IOS de Cisco 12.1 o la posterior IPsec DES o el Triple Data Encryption Standard (3DES) soportan SSH. Estas imágenes

generalmente tienen el ID k8 o k9 en su nombre de imagen. Por ejemplo, c1841-advipservicesk9-mz.124-10b.bin es una imagen que soporta SSH.

Paso 2. Asegurarse de que cada uno de los routers destino tenga un nombre de host único.

Paso 3. Asegurarse de que cada router destino esté usando el nombre de dominio correcto para la red.

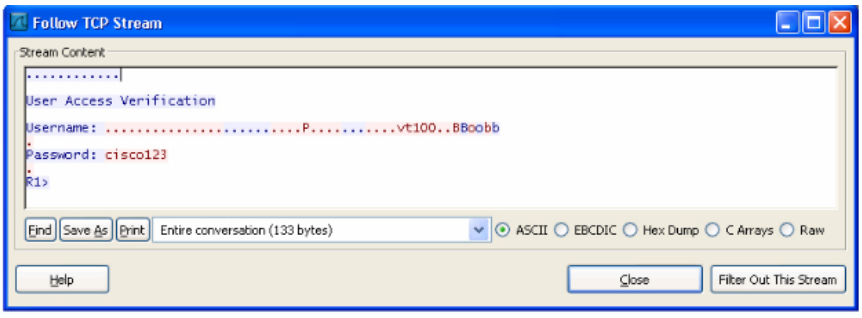
Paso 4. Asegurarse de que los routers destino estén configurados para autenticación local o servicios AAA para autenticación de usuario y contraseña. Esto es obligatorio para una conexión SSH de router a router.



Hay un atacante usando Wireshark para capturar paquetes en una subred local. El atacante está particularmente interesado en el flujo Telnet TCP y nota que la dirección IP del administrador (192.168.2.7) ha iniciado una sesión Telnet a un dispositivo.

Captura Telnet de Wireshark | Contraseña capturada | Captura SSH de Wireshark | Contraseña cifrada

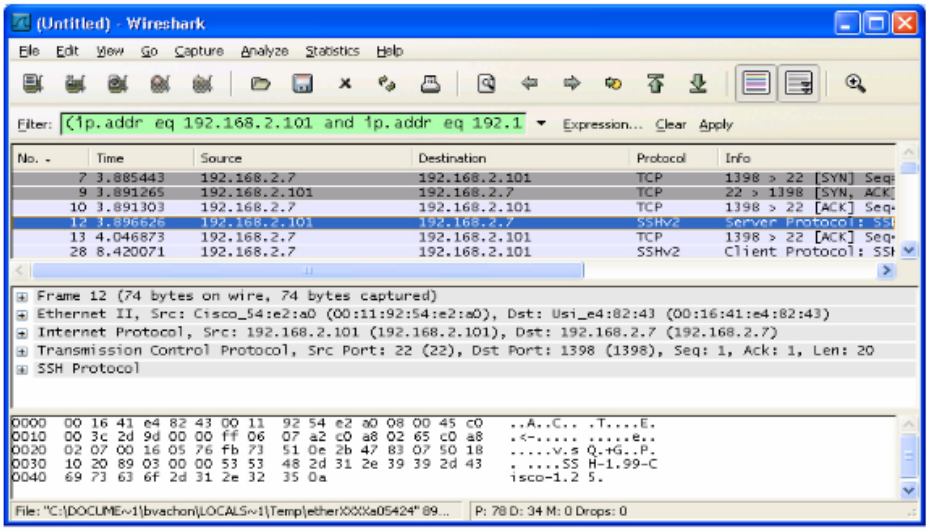
Haga clic sobre cada botón para ver el contenido asociado.



Siguiendo el flujo Telnet, el atacante ha capturado el nombre de usuario del administrador (Bob) y su contraseña (cisco123).

Captura Telnet de Wireshark | Contraseña capturada | Captura SSH de Wireshark | Contraseña cifrada

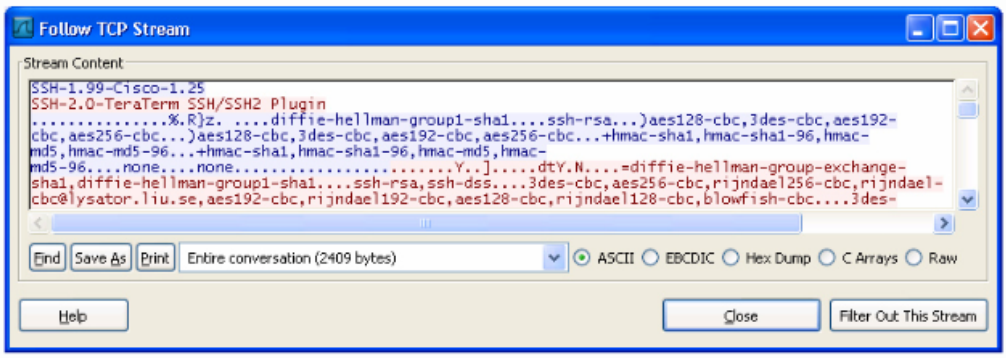
Haga clic sobre cada botón para ver el contenido asociado.



Cuando el administrador usa SSH, el atacante ya no ve los paquetes Telnet y debe filtrar por la dirección IP del administrador en su lugar.

Captura Telnet de Wireshark | Contraseña capturada | Captura SSH de Wireshark | Contraseña cifrada

Haga clic sobre cada botón para ver el contenido asociado.



Cuando sigue el flujo de datos, el atacante solo ve paquetes TCP y SSH, que revelan información cifrada inservible.

Captura Telnet de Wireshark | Contraseña capturada | Captura SSH de Wireshark | Contraseña cifrada

Haga clic sobre cada botón para ver el contenido asociado.

Usando la CLI, hay cuatro pasos para configurar un router Cisco para que soporte SSH:

Paso 1. Si el router tiene un nombre de host único, configure el nombre de dominio IP de la red usando el comando ip domain-name nombre-dominio en el modo de configuración global.

Paso 2. Deben generarse las claves secretas de una sola vía para que un router cifre el tráfico SSH. Estas claves se denominan claves asimétricas. El software IOS de Cisco usa el algoritmo Rivest, Shamir, and Adleman (RSA) para generar claves. Para crear la clave RSA, use el comando crypto key generate rsa general-keys módulo modulus-size en el modo de configuración global. El módulo determina el tamaño de la clave RSA y puede ser configurado de 360 bits a 2048 bits. Cuanto más grande sea el módulo, más segura será la clave RSA. Sin embargo, las claves con valores de módulo grandes toman más tiempo para ser generadas y para cifrarse y descifrarse. La longitud mínima de clave módulo recomendada es de 1024 bits.

Para verificar el SSH y mostrar las claves generadas, use el comando show crypto key mypubkey rsa en modo EXEC privilegiado. Si hay pares de claves existentes, se recomienda que sean sobreescritos usando el comando crypto key zeroize rsa.

Paso 3. Asegúrese de que haya una entrada de nombre de usuario válida en la base de datos local. Si no la hay, cree una usando el comando username nombre secret contraseña.

Paso 4. Habilite sesiones SSH vty de entrada usando los comandos de línea vty login local y transport input ssh.

SSH se habilita automáticamente luego de que se generan las claves RSA. Puede accederse al servicio SSH del router usando software de cliente SSH.




```
R1# conf t
R1(config)# ip domain-name span.com
R1(config)# crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.span.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

R1(config)#
*Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)# username Bob secret cisco
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exit
```

Paso 1: Configurar el nombre de dominio IP
Paso 2: Generar claves secretas de una sola vía
Paso 3: Verificar o crear una entrada en la base de datos local
Paso 4: Habilitar sesiones SSH VTY de entrada

Comandos SSH opcionales

Opcionalmente, pueden usarse comandos SSH para configurar lo siguiente:

Versión SSH
Período de vencimiento de sesión SSH
Número de reintentos de autenticación

Los routers Cisco soportan dos versiones de SSH: SSH version 1 (SSHv1) y SSH version 2 (SSHv2), la versión más nueva y segura. SSHv2 proporciona mejor seguridad usando el intercambio de claves Diffie-Hellman y el código de autenticación de mensajes (message authentication code - MAC) de fuerte revisión de integridad.

El IOS de Cisco Release 12.1(1)T y posteriores soportan SSHv1. El IOS de Cisco Release 12.3(4)T y posteriores operan en modo de compatibilidad y soportan tanto SSHv1 como SSHv2. Para cambiar del modo de compatibilidad a una versión específica, use el comando de configuración global ip ssh version {1 | 2}.

El intervalo de tiempo que el router espera para que responda el cliente SSH durante la fase de negociación SSH puede ser configurado usando el comando ip ssh time-out segundos en el modo de configuración global. El intervalo por defecto es de 120 segundos. Cuando se inicia la sesión EXEC, se aplica el tiempo de vencimiento estándar de exec configurado para vty.

Por defecto, el usuario tiene tres intentos para ingresar antes de ser desconectado. Para configurar un número diferente de intentos consecutivos SSH, use el comando ip ssh authentication-retries entero en el modo de configuración global.

Para verificar las configuraciones de comandos SSH opcionales, use el comando show ip ssh.

Luego de que SSH haya sido configurado, el cliente SSH deberá conectarse a un router con SSH habilitado.




```
R1# show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
R1#
R1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# ip ssh version 2
R1(config)# ip ssh time-out 60
R1(config)# ip ssh authentication-retries 2
R1(config)# ^Z
R1#
R1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 60 secs; Authentication retries: 2
R1#
```

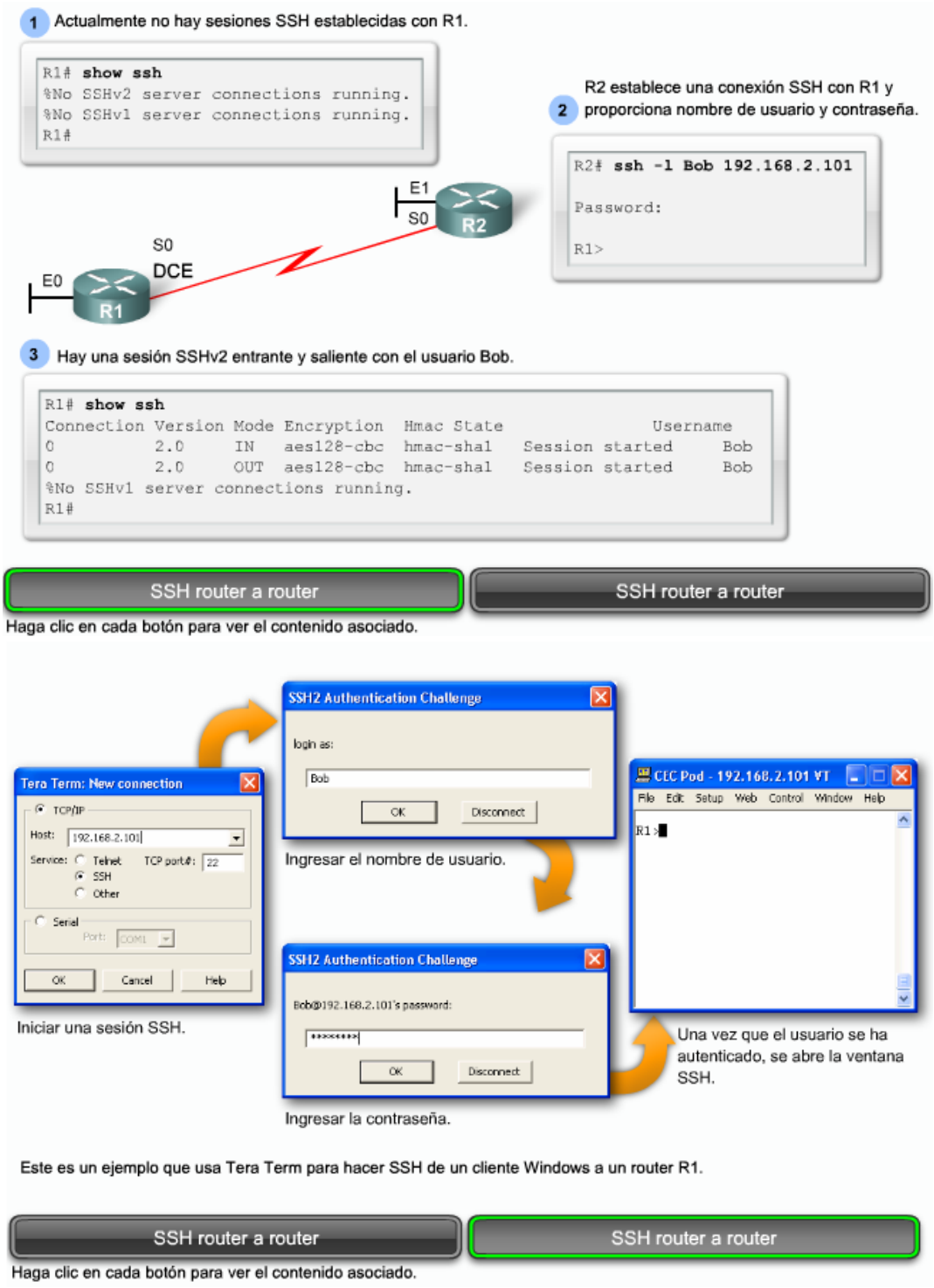
Hay dos maneras de conectarse a un router con SSH habilitado:

Conectarse mediante un router Cisco con SSH habilitado usando el comando de modo privilegiado EXEC ssh.
Conectarse usando un cliente SSH público y disponible comercialmente ejecutándose en un host. Algunos ejemplos de estos clientes son PuTTY, OpenSSH, and TeraTerm.

Los routers de Cisco son capaces de actuar como el servidor SSH y como un cliente SSH para conectarse a otro dispositivo que tenga SSH habilitado. Por defecto, ambas de estas funciones están habilitadas en el router cuando se habilita SSH. Como servidor, el router puede aceptar conexiones de cliente SSH. Como cliente, el router puede hacer SSH con otro router que tenga SSH habilitado.

El procedimiento para conectarse a un router Cisco varía en relación con la aplicación del cliente SSH. Generalmente, el cliente SSH inicia una conexión SSH al router, luego el servicio SSH del router pide el nombre de usuario con la contraseña correcta. Si la autenticación es exitosa, el router puede ser administrado como si el administrador estuviera usando una sesión Telnet estándar.

Utilice el comando show ssh para verificar el estado de las conexiones cliente.



El SDM de Cisco puede ser usado para configurar un demonio SSH en un router. Para ver la configuración actual de las claves SSH, vaya a Configure > Additional Tasks > Router Access > SSH. La configuración de las claves SSH tiene dos opciones de estado.

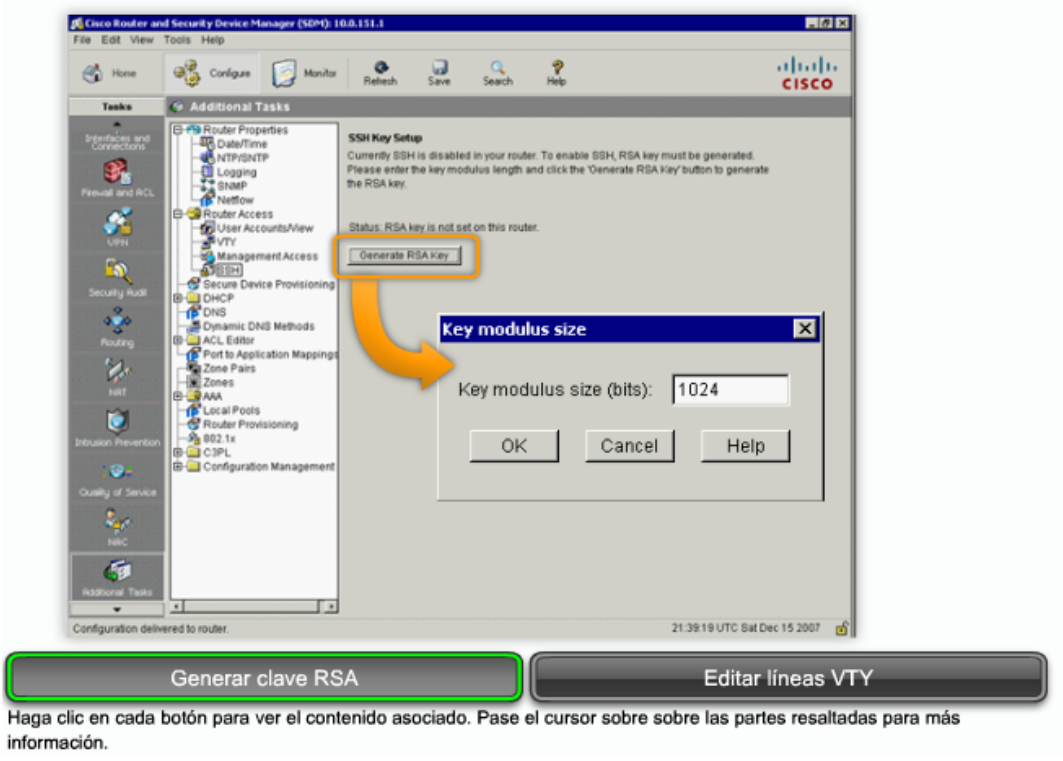
RSA key is not set on this router - Esta notificación aparece si no hay una clave criptográfica configurada para el dispositivo. Si no hay clave configurada, ingrese un tamaño de módulo y genere la clave.

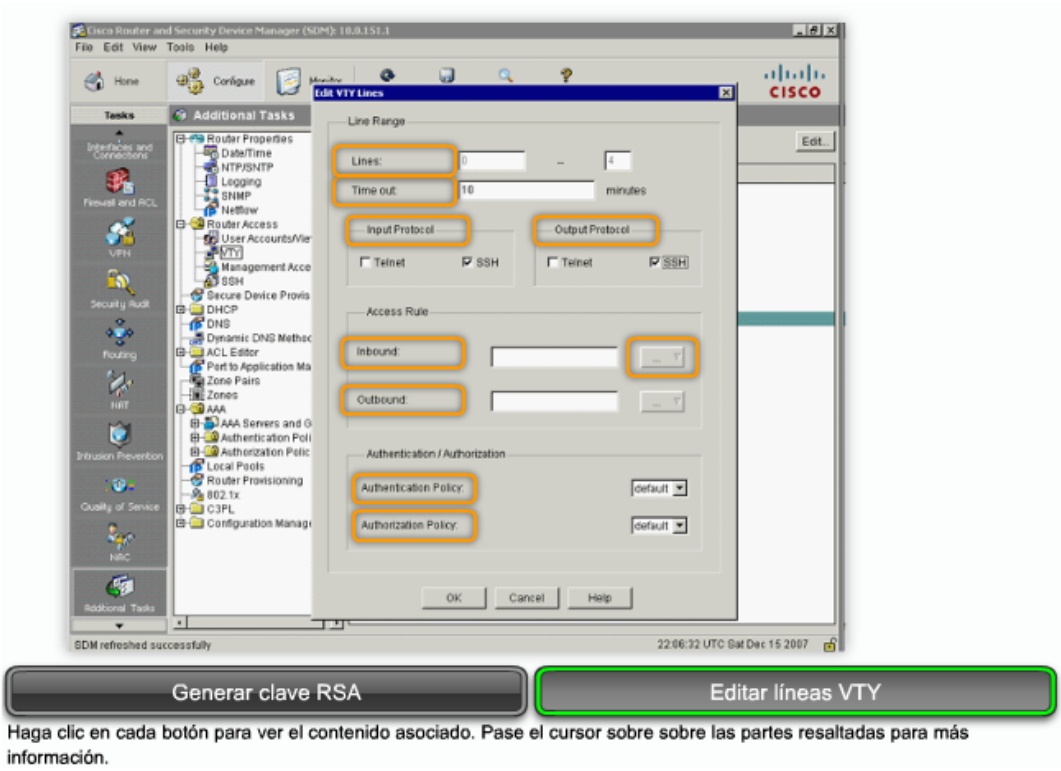
RSA key is set on this router - Esta notificación aparece si se ha generado una clave criptográfica, en cuyo caso SSH está habilitado en el router.

El archivo de configuración que viene por defecto con un router Cisco con SDM habilitado automáticamente habilita acceso Telnet y SSH desde la interfaz LAN y genera una clave RSA.

El botón Generate RSA configura una clave criptográfica si no hay una en existencia. Aparece luego la ventana de diálogo Key Modulus Size. Si el valor de módulo debe estar entre 512 y 1024, ingrese un valor entero que sea múltiplo de 64. Si el valor debe ser mayor a 1024, ingrese 1536 o 2048. Si se ingresa un valor mayor a 512, la generación de las claves puede tomar un minuto o más.

Luego de que se ha habilitado SSH en el router, deben configurarse las líneas vty para soportar SSH. Vaya a Configure > Additional Tasks > Router Access > VTY. Se desplegará la ventana VTY Lines con las configuraciones vty del router. Haga clic sobre el botón Edit para configurar los parámetros vty.





2.2 Asignación de roles administrativos

2.2.1 Configuración de niveles de privilegios

Aunque es importante que el administrador de sistemas pueda conectarse a un dispositivo y administrarlo con seguridad, deben agregarse más configuraciones para mantener segura a la red. Por ejemplo, ¿debe proporcionarse acceso sin restricciones a todos los empleados de una empresa? La respuesta a esta pregunta generalmente es no. La mayoría de los empleados de una empresa solo requiere acceso a áreas específicas de la red. ¿Habrá que dar acceso sin restricciones a todos los empleados del departamento de Informática? Tenga en consideración que las grandes organizaciones tienen muchos empleados en diferentes tipos de trabajos agrupados dentro del departamento de Informática. Por ejemplo, hay empleados con el título de Jefe de Servicios Informáticos (CIO), Operador de Seguridad, Administrador de Redes, Ingeniero WAN, Administrador LAN, Administrador de Software, Soporte Técnico y otros. No todos los trabajos requieren los mismos privilegios de acceso a los dispositivos de la infraestructura.

Tomemos este ejemplo: un administrador de red se va de vacaciones y, como precaución, le da las contraseñas de modo privilegiado EXEC de todos los dispositivos de la infraestructura a otro administrador de red a su cargo. Algunos días después, el administrador curioso accidentalmente deshabilita toda la red de la empresa. Este escenario no es tan poco común, ya que demasiado seguido se asegura a los los routers solo con las contraseñas de modo privilegiado EXEC. Cualquiera que tenga conocimiento de esta contraseña tiene acceso sin restricciones a todo el router.

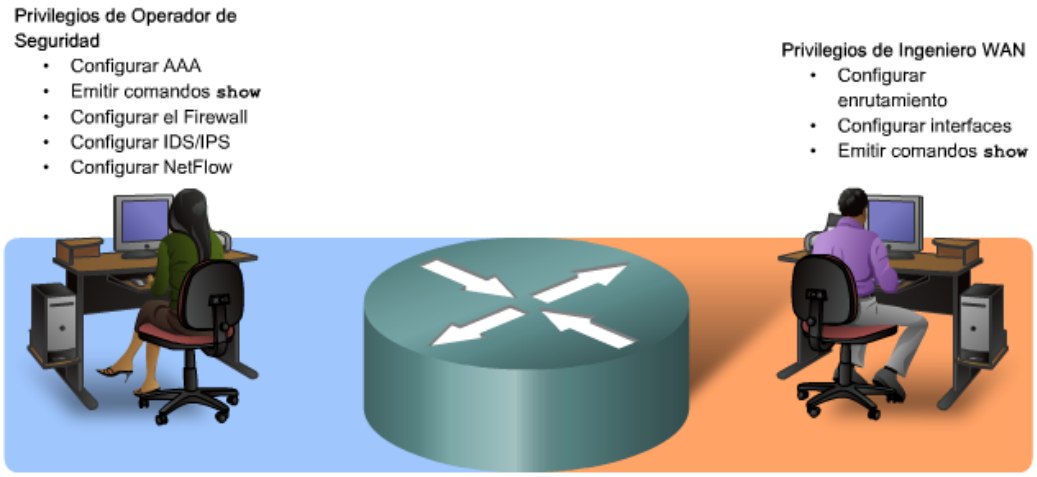
El siguiente paso para el administrador de sistemas que quiere asegurar la red es configurar niveles de privilegio. Los niveles de privilegio determinan a quién le será

permitido conectarse al dispositivo y qué podrá hacer una vez que se conecte. La CLI del software IOS de Cisco tiene dos niveles de acceso a los comandos.

El modo de usuario EXEC (nivel 1 de privilegios) - Proporciona los privilegios más básicos al usuario del modo EXEC y le permite solo comandos de nivel de usuario con el promptrouter>.
El modo EXEC privilegiado (nivel 15 de privilegios) - Incluye todos los comandos de nivel enable con el prompt router# .

Aunque estos dos niveles proporcionan control, algunas veces se necesita un nivel de control más preciso.

El software IOS de Cisco tiene dos métodos para proveer acceso a la infraestructura: nivel de privilegios y CLI basada en roles.



Asignación de niveles de privilegios

A partir de la Release 10.3 del IOS de Cisco, los routers Cisco le permiten al administrador configurar múltiples niveles de privilegios. Esto es especialmente útil en un ambiente de help desk (soporte) donde ciertos administradores deben estar habilitados para configurar y monitorear todas las parets del router (nivel 15) y otros administradores solo deben monitorear, pero no configurar, el router (niveles personalizados 2 a 14). Hay 16 niveles de privilegios en total. Los niveles 0, 1 y 15 tienen configuración predeterminada.

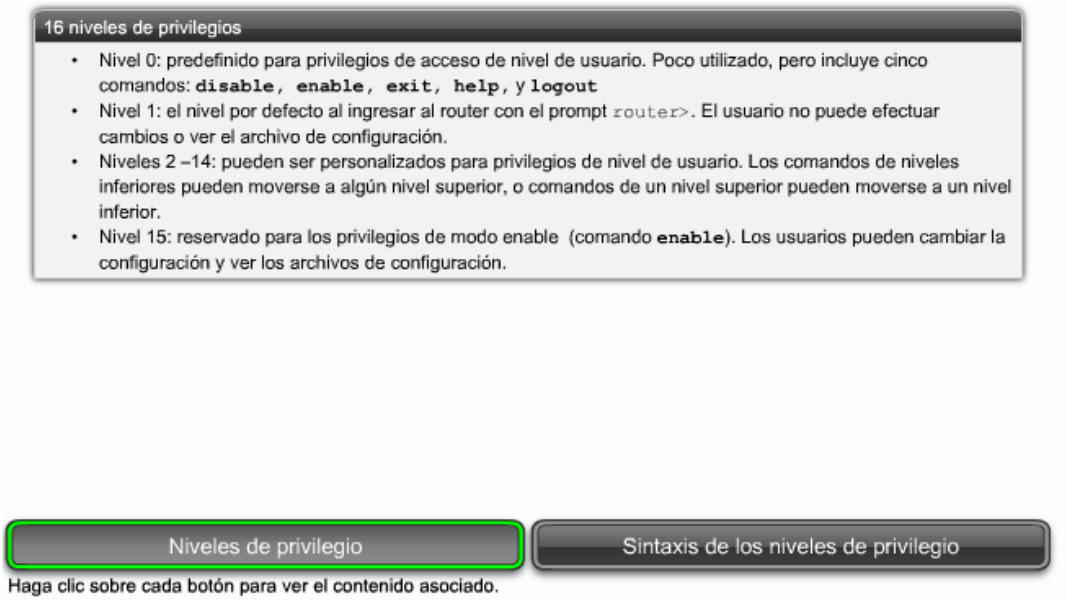
Un administrador puede definir múltiples niveles de privilegios personalizados y asignar diferentes comandos a cada nivel. Cuanto más alto el nivel de privilegios, más acceso al router tiene el usuario. Los comandos disponibles en niveles de privilegios más bajos también son ejecutables a niveles más altos, porque cada nivel de privilegios incluye los privilegios de todos los otros niveles inferiores. Por ejemplo, un usuario autorizado para el nivel de privilegios 10 tiene acceso a comandos permitidos en los niveles 0 a 10 (si también están definidos). Un usuario de nivel 10 no puede acceder a

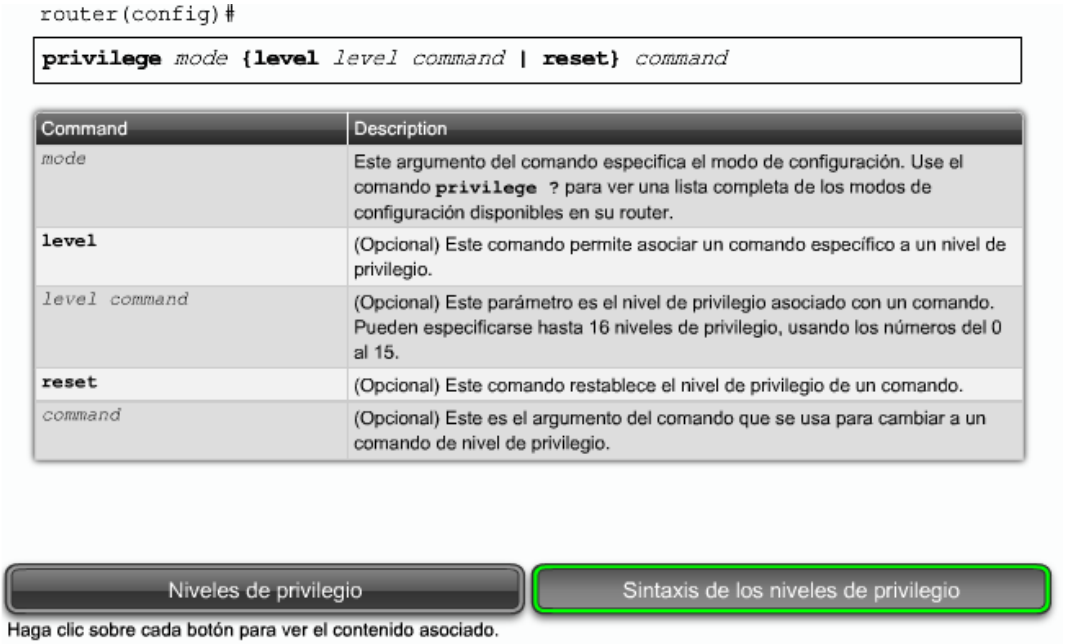
los comandos otorgados al nivel de privilegios 11 (o mayor). Un usuario autorizado para privilegios de nivel 15 puede ejecutar todos los comandos de IOS de Cisco.

Para asignar comandos a un nivel de privilegios personalizado, utilice el comando privilege del modo de configuración global.

Router(config)# privilege modo {level nivel de comando | reset} comando

Es importante tener en cuenta que asignar un comando con múltiples palabras clave, como show ip route, a un nivel específico de privilegios asigna automáticamente a todos los comandos asociados con las primeras palabras claves al nivel de privilegios específico. Por ejemplo, tanto el comando show como el comando show ip serán asignados automáticamente al nivel de privilegios al que show ip route fue asignado. Esto es necesario porque el comando show ip route no puede ser ejecutado si no se tiene acceso a los comandos show y show ip. Los subcomandos que siguen a show ip route también se asignan al mismo nivel de privilegios. Asignar el comando show ip route permite al usuario emitir todos los comandos show, como show version.





Deben configurarse niveles de privilegios para autenticación. Hay dos métodos para asignar contraseñas a los diferentes niveles:

Para el nivel privilegiado usando el comando de configuración global enable secret level contraseña del nivel.
Para un usuario que tiene acceso a un nivel de privilegios específico, usando el comando de configuración global username nombre privilege nivel secret contraseña.

Por ejemplo, un administrador puede asignar cuatro niveles de acceso a los dispositivos dentro de una organización:

Una cuenta USER (nivel 1, que no incluya ping)
Una cuenta SUPPORT (todo el acceso al nivel 1, más el comando ping)
Una cuenta JR-ADMIN (acceso a los niveles 1 a 5, más el comando reload)
Una cuenta ADMIN (acceso sin restricciones)

Implementar niveles de privilegio varía dependiendo de la estructura de la organización y las diferentes funciones que requieran acceso a los dispositivos de la infraestructura.

En el caso de USER, que requiere acceso de nivel 1 por defecto (Router>), no se definen niveles de privilegio personalizados. Esto es causado porque el modo de usuario por defecto es equivalente al nivel 1.

Se puede asignar un nivel de acceso mayor a la cuenta SUPPORT, como nivel 5. El nivel 5 automáticamente hereda los comandos de los niveles 1 a 4, además de comandos adicionales que pueden asignarse. Tenga en consideración que cuando se asigna un comando a un nivel específico, el acceso a ese comando se quita de todos los niveles inferiores. Por ejemplo, para asignar el comando ping al nivel 5, use la siguiente secuencia de comandos.

privilege exec level 5 ping

La cuenta USUARIO (nivel 1) ya no tiene acceso al comando ping, porque el usuario debe tener acceso al nivel 5 o mayor para realizar la función ping.

Para asignar una contraseña al nivel 5, ingrese el siguiente comando.

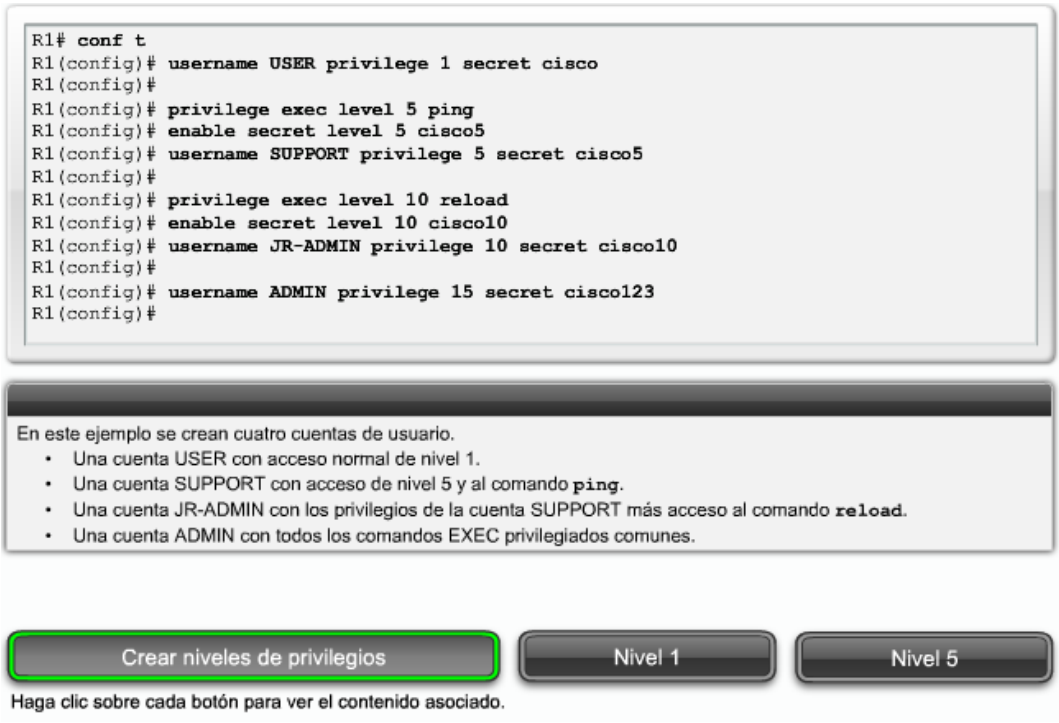
enable secret level 5 cisco5

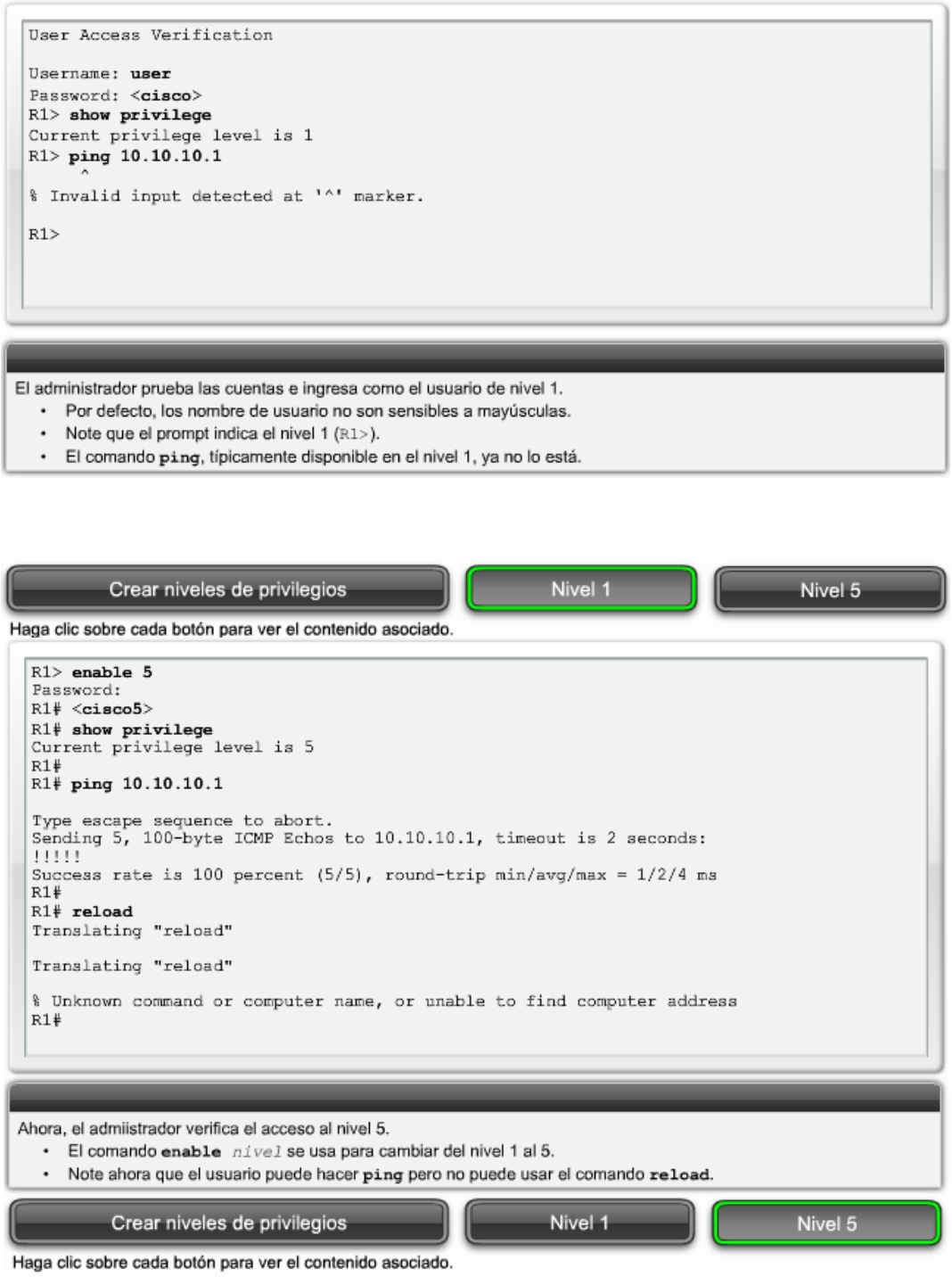
Para acceder al nivel 5, debe usarse la contraseña cisco5.

Para asignar un nombre de usuario específico al nivel 5, ingrese el siguiente comando.

username support privilege 5 secret cisco5

Solo los usuarios que ingresen bajo el nombre support podrán acceder al nivel 5, que también hereda los privilegios del nivel 1.





La cuenta JR-ADMIN requiere acceso a todos los comandos de los niveles 1 y 5, así como también al comando reload. Debe asignarse a esta cuenta un nivel de acceso más alto, como nivel 10. El nivel 10 automáticamente heredará todos los comandos de los niveles inferiores.

Para asignar el nivel 10 al comando reload de modo EXEC privilegiado, use la siguiente secuencia de comandos.

privilege exec level 10 reload

username jr-admin privilege 10 secret cisco10

enable secret level 10 cisco10

Al emitir estos comandos, el comando reload solo está disponible para los usuarios de nivel de acceso 10 o mayor. Se otorga acceso al nivel de privilegios 10 al nombre de usuario jr-admin junto con todos los comandos asociados, incluyendo aquellos comandos asignados a niveles de privilegios inferiores. Para acceder al nivel 10 de privilegios, se requiere la contraseña cisco10.

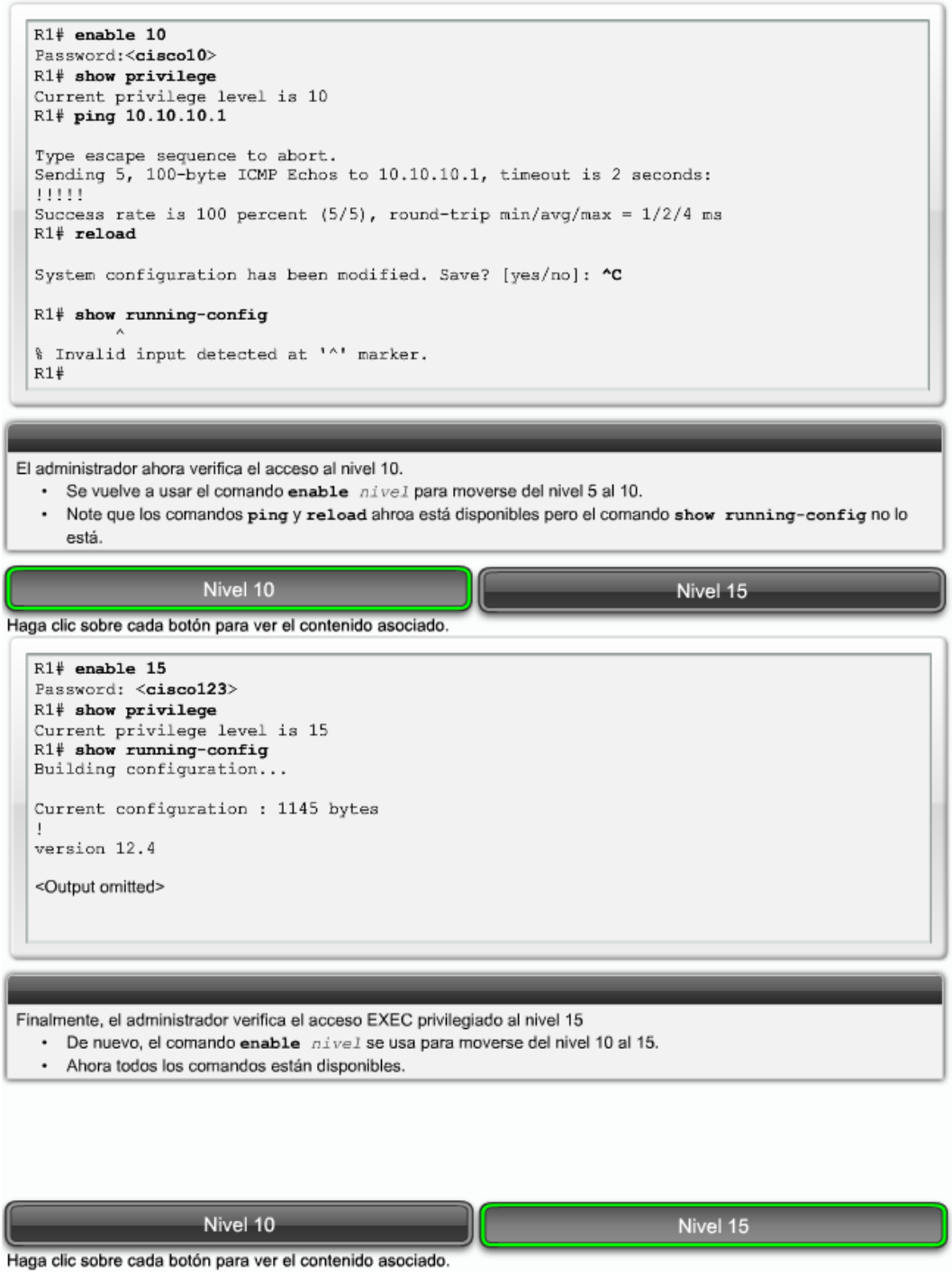
Puede asignarse a una cuenta ADMIN el nivel de acceso 15 para el modo EXEC privilegiado. En esta instancia, no deberán definirse comandos personalizados. Puede asignarse una contraseña personalizada usando el comando enable secret level 15 cisco123, sin embargo, ésta no sobreescribe la contraseña enable secret, que también debe ser utilizada para acceder al nivel 15. Use el comando username admin privilege 15 secret cisco15 para asignar nivel 15 de acceso al usuario ADMIN con la contraseña cisco15.

Tenga en consideración que cuando asigna nombres de usuario a niveles de privilegio, las palabras clave privilege y secret no son intercambiables. Por ejemplo, el comando username USER secret cisco privilege 1 no asigna nivel de acceso 1 a la cuenta USER. En su lugar, crea una cuenta con la contraseña "cisco privilege 1".

Para acceder a niveles de privilegio establecidos, ingrese el comando enable nivel desde el modo de usuario e ingrese la contraseña que fue asignada al nivel de privilegio personalizado. Use el mismo comando para moverse de un nivel inferior a un nivel superior.

Para moverse del nivel 1 al nivel 5, use el comando enable 5 en el prompt EXEC.
Para moverse al nivel 10, use el comando enable 10 con la contraseña correcta.
Para moverse del nivel 10 al nivel 15, use el comando enable. Si no se especifica ningún nivel de privilegio, se asume el nivel 15.

Algunas veces es fácil que un usuario olvide qué nivel de acceso tiene actualmente. Use el comando show privilege para mostrar y confirmar el nivel de privilegio actual. Recuerde que los niveles de privilegio superiores automáticamente heredan los accesos a los comandos de los niveles inferiores.



Aunque asignar niveles de privilegios otorga algo de flexibilidad, algunas organizaciones pueden no hallar este sistema adecuado, por las siguientes limitaciones:

No hay control de acceso a interfaces, puertos, interfaces lógicas y ranuras específicas en un router.
Los comandos disponibles en niveles inferiores de privilegios siempre son ejecutables en niveles superiores.

Los comandos específicamente asociados a un nivel de privilegios superior nunca están disponibles para usuarios de niveles de privilegio inferiores.
Asignar un comando con múltiples palabras clave a un nivel específico de privilegios también asigna todos los comandos asociados con las primeras palabras clave del mismo nivel de privilegios. Un ejemplo es el comando show ip route.

Sin embargo, la mayor limitación es que si un administrador necesita crear una cuenta que tenga acceso a la mayoría de, aunque no todos, los comandos, deben configurarse sentencias privilege exec para cada comando que debe ser ejecutado en un nivel de privilegios inferior al 15. Este puede ser un proceso bastante tedioso.

¿Cómo pueden superarse las limitaciones de asignar niveles de privilegios?



2.2.2 Configuración de acceso a la CLI basado en roles

CLI basada en roles

Para proporcionar mayor flexibilidad que la que otorgan los niveles de privilegios, Cisco introdujo la función de Acceso a la CLI Basado en Roles en la Release 12.3(11)T del IOS. Esta función provee acceso más granular, ya que controla específicamente cuáles comandos están disponibles para roles específicos. El acceso a la CLI basado en roles permite al administrador de la red crear diferentes vistas de las configuraciones del router para diferentes usuarios. Cada vista define los comandos CLI a los que cada usuario tiene acceso.

Seguridad

El acceso a la CLI basado en roles mejora la seguridad del dispositivo, ya que define el grupo de comandos de la CLI que es accesible para un usuario particular. Además, los administradores pueden controlar el acceso del usuario a puertos, interfaces lógicas y

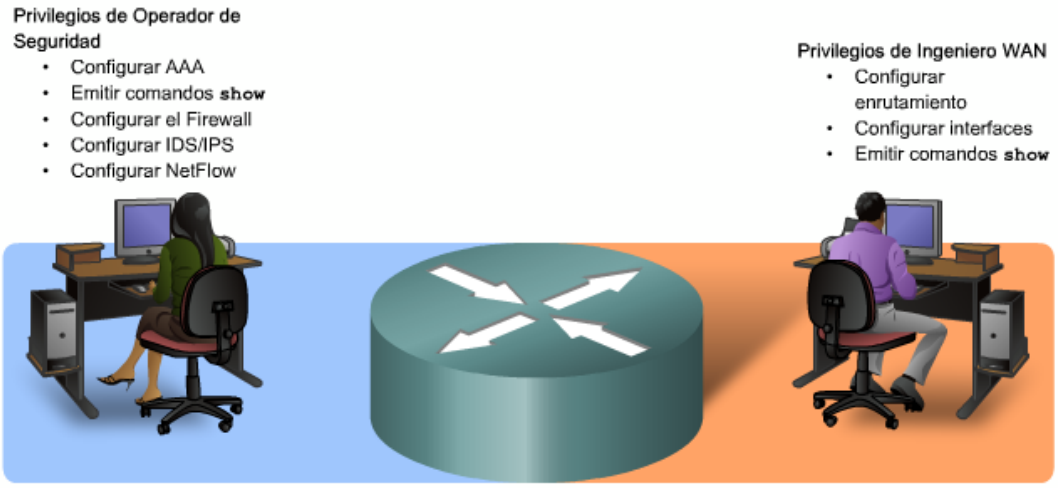
ranuras específicas en un router. Esto detiene al usuario de cambiar la configuración o recolectar información a la que no debería tener acceso.

Disponibilidad

El acceso a la CLI basado en roles imposibilita la ejecución no intencional de comandos de CLI por parte de personal no autorizado, lo que podría dar resultados no deseados. Esto minimiza el período de inactividad.

Eficiencia operativa

Los usuarios solo ven los comandos de la CLI que son aplicables a los puertos y la CLI a los que tienen acceso; por lo tanto, el router parece menos complejo y los comandos son de más fácil identificación cuando se usa la función de ayuda en el dispositivo.



La CLI basada en roles proporciona tres tipos de vistas:

Vista de root
Vista CLI
Supervista

Cada vista dictamina qué comandos están disponibles.

Vista de root

Para configurar cualquier vista en el sistema, el administrador debe estar en la vista de root. La vista de root tiene los mismos privilegios de acceso que un usuario con nivel 15 de privilegios. Sin embargo, una vista de root no es lo mismo que un usuario de nivel 15. Solo un usuario de vista de root puede configurar una nueva vista y agregar o remover comandos de las vistas existentes.

Vista de CLI

Puede asociarse un grupo específico de comandos a una vista CLI. A diferencia de los niveles de privilegios, la vista CLI no tiene jerarquías de comandos y, por lo tanto, no hay vistas superiores o inferiores. Deben asignarse todos los comandos asociados con cada vista, y las vistas no heredan comandos de otras vistas. Adicionalmente, los mismos comandos pueden ser utilizados en varias vistas.

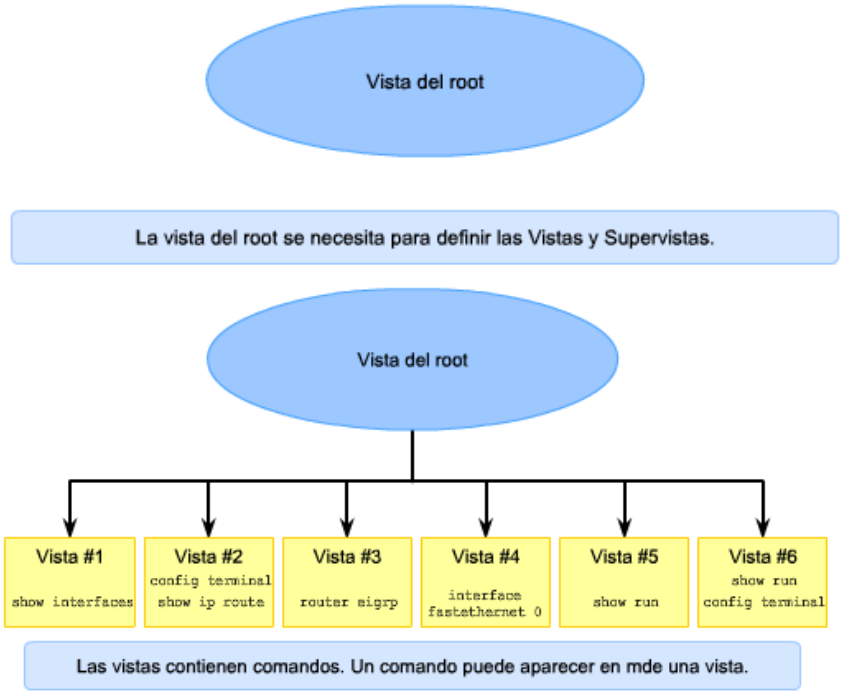
Supervista

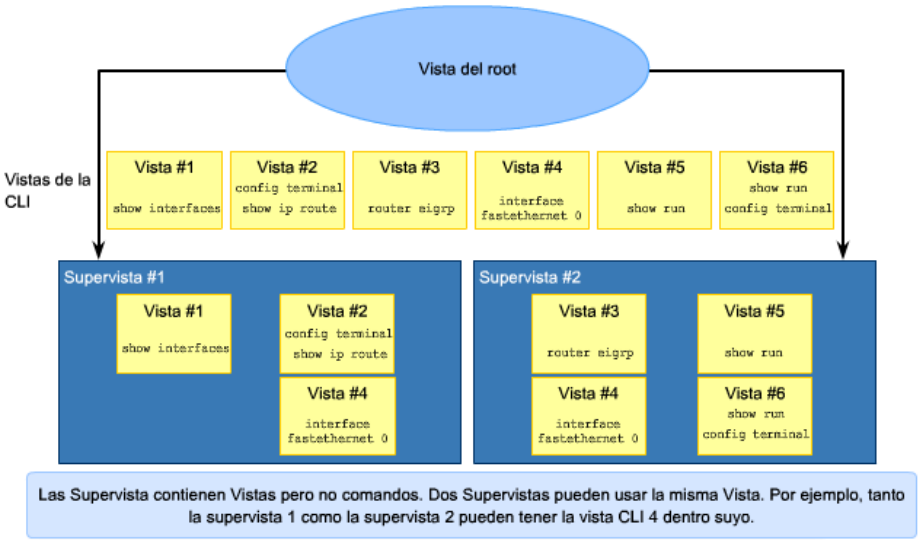
La supervista consiste en una o más vistas CLI. Los administradores pueden definir qué comandos son aceptados y qué información de configuración es visible. Las supervistas permiten al administrador de redes asignar a los usuarios y grupos de usuarios múltiples vistas CLI de una sola vez, en lugar de tener que asignar una sola vista CLI por usuario con todos los comandos asociados a esa única vista CLI.

Las supervistas tienen las siguientes características:

Una sola vista CLI puede ser compartida entre varias supervistas.
No pueden configurarse comandos para una supervista. El administrador debe agregar comandos a la vista CLI y luego agregar esa vista CLI a la supervista.
Los usuarios que están autenticados en una supervista pueden acceder a todos los comandos que están configurados para cualquiera de las vistas CLI que son parte de la supervista.
Cada supervista tiene una contraseña que se usa para moverse entre supervistas o de una vista CLI a una supervista.

Eliminar una supervista no elimina las vistas CLI asociadas. Las vistas CLI permanecen disponibles para ser asignadas a otra supervista.





Antes de que un administrador pueda crear una vista, debe habilitarse AAA con el comando aaa new-model o SDM de Cisco.

Para configurar y editar las vistas, el administrador debe ingresar a la vista de root usando el comando de EXEC privilegiado enable view . Tambien puede usarse el comando enable view root. Ingrese la contraseña enable secret cuando se la pida.

Hay cinco pasos para crear y administrar una vista específica.

Paso 1. Habilitar AAA con el comando de configuración global aaa new-model. Salga e ingrese a la vista de root con el comando enable view.

Paso 2. Cree una vista usando el comando parser view nombre-vista. Esto habilita el modo de configuración de la vista. Excluyendo la vista de root, hay un límite máximo de 15 vistas en total.

Paso 3. Asigne una contraseña secret a la vista usando el comando secret contraseña-cifrada.

Paso 4. Asigne comandos a la vista seleccionada usando el comando commands parser-mode {include | include-exclusive | exclude} [all] [interface nombre-interfaz | comando] en el modo de configuración de vista.

Paso 5. Salga del modo de configuración de la vista emitiendo el comando exit.

```
router#
enable [view [view-name]]
```

- El comando se usa para ingresar a la vista CLI. Ingrese la raíz del nombre de una vista. Si no se especifica un nombre, se asume root.
- Recuerde que el comando **aaa new-model** debe ser configurado antes de entrar a la vista.

Parámetro	Descripción
view	Ingresa a la vista de root si no se ha especificado un nombre de vista, lo que habilita al administrador para configurar las vistas CLI. Se requiere la palabra clave de la vista para configurar una vista CLI.
view-name	(Opcional) Ingresa o deja una vista CLI específica. Esta palabra clave puede usarse para moverse de una vista CLI a otra.

Paso 1 | Pasos 2 y 3 | Paso 4 | Configuración ejemplo | Configuración actual

Haga clic sobre cada botón para ver el contenido asociado.

```
router(config)#
parser view view-name
```

- Crea una vista e ingresa al modo de configuración de la vista.

```
router(config-view)#
secret encrypted-password
```

- Establece una contraseña para proteger el acceso a la vista.
- La contraseña debe ser creada inmediatamente después de crear una vista, si no es así, se mostrará un mensaje de error.

Paso 1 | Pasos 2 y 3 | Paso 4 | Configuración ejemplo | Configuración actual

Haga clic sobre cada botón para ver el contenido asociado.

```
router(config-view)#
```

commands *parser-mode* **{include | include-exclusive | exclude} [all]**
[interface *interface-name* **|** *command***]**

- Agrega comandos o interfaces a una vista.

Comando	Descripción
commands	Agrega comandos o interfaces a una vista.
parser-mode	Modo en el que existe el comando especificado, por ejemplo el modo EXEC.
include	Agrega un comando o una interfaz a la vista y permite que el mismo comando o interfaz se agregue a otras vistas.
include-exclusive	Agrega un comando o una interfaz a la vista y excluye el mismo comando o interfaz de las otras vistas.
exclude	Excluye un comando o una interfaz de la vista.
all	Una "wildcard" que permite a todos los comandos de un modo de configuración específico que empiezan con al misma palabra clave en cada subinterfaz de una interfaz específica ser parte de la vista.
interface *interface-name*	Interfaz agregada a la vista.
command	Comando agregado a la vista.

Paso 1 | Pasos 2 y 3 | Paso 4 | Configuración ejemplo | Configuración actual

Haga clic sobre cada botón para ver el contenido asociado.

```
R1(config)# parser view SHOWVIEW
*Mar  1 09:54:54.873: %PARSER-6-VIEW_CREATED: view 'SHOWVIEW' successfully created.
R1(config-view)# secret cisco
R1(config-view)# commands exec include show
R1(config-view)# exit
R1(config)# parser view VERIFYVIEW
*Mar  1 09:55:24.813: %PARSER-6-VIEW_CREATED: view 'VERIFYVIEW' successfully created.
R1(config-view)# commands exec include ping
% Password not set for the view VERIFYVIEW
R1(config-view)# secret cisco5
R1(config-view)# commands exec include ping
R1(config-view)# exit
R1(config)# parser view REBOOTVIEW
R1(config-view)#
*Mar  1 09:55:52.297: %PARSER-6-VIEW_CREATED: view 'REBOOTVIEW' successfully created.
R1(config-view)# secret cisco10
R1(config-view)# commands exec include reload
R1(config-view)# exit
R1(config)#
```

Paso 1 | Pasos 2 y 3 | Paso 4 | Configuración ejemplo | Configuración actual

Haga clic sobre cada botón para ver el contenido asociado.

```
R1# show running-config

<output omitted>

parser view SHOWVIEW
 secret 5 $1$GL2J$8njLecwTaLAc0UuWo1/Fv0
 commands exec include show
!
parser view VERIFYVIEW
 secret 5 $1$d08J$1zOYSI4WainGxkn0Hu71P1
 commands exec include ping
!
parser view REBOOTVIEW
 secret 5 $1$L71Z$1Jtn5IhP43fVE7SVoF1pt.
 commands exec include reload
!
```

Paso 1 | Pasos 2 y 3 | Paso 4 | Configuración ejemplo | Configuración actual

Haga clic sobre cada botón para ver el contenido asociado.

Los pasos para configurar una supervista son esencialmente los mismos que para configurar una vista CLI, excepto que en lugar de usar el comando commands para asignar comandos, debe usarse el comando view nombre-vista para asignar vistas. El administrador debe estar en la vista de root para configurar una supervista. Para confirmar que se está usando la vista de root, use el comando enable view o el comando enable view root. Ingrese la contraseña enable secret cuando se la solicite.

Hay cuatro pasos para crear y administrar una supervista.

Paso 1. Cree una vista usando el comando parser view nombre-vista superview e ingrese al modo de configuración de supervista.

Paso 2. Asigne una contraseña secret a la vista usando el comando secret contraseña-cifrada.

Paso 3. Asigne una vista existente usando el comando view nombre-vista en el modo de configuración de vista.

Paso 4. Salga del modo de configuración de supervista emitiendo el comando exit.

Puede asignarse más de una vista a una supervista, y las vistas pueden ser compartidas por más de una supervista.

Para acceder a las vistas existentes, ingrese el comando enable view nombre-vista en el modo de usuario e ingrese la contraseña que se asignó a la vista personalizada. Use el mismo comando para moverse de una vista a la otra.

```
router(config)#
parser view view-name superview
```

- Appending the keyword **superview** to the **parser view** Comando que crea una supervista e ingresa al modo de configuración de vista.

```
router(config-view)#
secret encrypted-password
```

- Establece una contraseña para proteger el acceso a la supervista.
- La contraseña debe ser creada inmediatamente después de crear una vista, si no es así, se mostrará un mensaje de error..

Pasos 1 y 2 | Paso 3 | Configuración de ejemplo | Configuración actual

Haga clic sobre cada botón para ver el contenido asociado.

```
router(config-view)#
view view-name
```

- Agrega una vista CLI a una supervista.
- Se pueden agregar múltiples vistas.
- Las supervistas pueden compartir vistas.

Pasos 1 y 2 | Paso 3 | Configuración de ejemplo | Configuración actual

Haga clic sobre cada botón para ver el contenido asociado.

```
R1(config)# parser view USER superviewv
* Mar  1 09:56:26.465 : %PARSER-6-SUPER_VIEW_CREATED: super view 'USER' successfully
created.
R1(config-view)# secret cisco
R1(config-view)# view SHOWVIEW
*Mar  1 09:56:33.469: %PARSER-6-SUPER_VIEW_EDIT_ADD: view SHOWVIEW added to superview
USER.
R1(config-view)# exit
R1(config)#
R1(config)# parser view SUPPORT superview
*Mar  1 09:57:33.825 : %PARSER-6-SUPER_VIEW_CREATED: super view 'SUPPORT'
successfully created.
R1(config-view)# secret cisco1
R1(config-view)# view SHOWVIEW
*Mar  1 09:57:45.469: %PARSER-6-SUPER_VIEW_EDIT_ADD: view SHOWVIEW added to superview
SUPPORT.
R1(config-view)# view VERIFYVIEW
*Mar  1 09:57:57.077: %PARSER-6-SUPER_VIEW_EDIT_ADD: view VERIFYVIEW added to
superview SUPPORT.
R1(config-view)#exit
R1(config)#
```

Pasos 1 y 2 | Paso 3 | Configuración de ejemplo | Configuración actual

Haga clic sobre cada botón para ver el contenido asociado.

```
R1# show running-config

<output omitted>

!
parser view SUPPORT superview
 secret 5 $1$Vp1O$BBB1N68Z2ekr/aLHledts.
 view SHOWVIEW
 view VERIFYVIEW
!
parser view USER superview
 secret 5 $1$E4k5$ukHyfYP7dHOC48N8pxm4s/
 view SHOWVIEW
!
parser view JR-ADMIN superview
 secret 5 $1$8kx2$rbAe/ji220OmQ1yw.568g0
 view SHOWVIEW
 view VERIFYVIEW
 view REBOOTVIEW
!
```

Pasos 1 y 2 | Paso 3 | Configuración de ejemplo | Configuración actual

Haga clic sobre cada botón para ver el contenido asociado.

Para verificar una vista, use el comando enable view. Ingrese el nombre de la vista para verificar y proporcione la contraseña para ingresar a la vista. Use el comando de signo de pregunta (?) para verificar que los comandos disponibles en la vista sean los correctos.

Desde la vista de root, use el comando show parser view all para ver un resumen de todas las vistas.

```
R1# enable view USER
Password:
*Mar  1 09:59:46.197: %PARSER-6-VIEW_SWITCH: successfully set to view 'USER'.

R1# ?
Exec commands:
  enable  Turn on privileged commands
  exit    Exit from the EXEC
  show    Show running system information

R1#
R1# show ?
  flash:   display information about flash: file system
  version  System hardware and software status

R1#
```

Verificar USER | Verificar SUPPORT | Verificar JR-ADMIN | Verificar todas

Haga clic sobre cada botón para ver el contenido asociado.

```
R1# enable view SUPPORT
Password:
*Mar  1 10:00:11.353: %PARSER-6-VIEW_SWITCH: successfully set to view 'SUPPORT'.

R1# ?
Exec commands:
  enable  Turn on privileged commands
  exit    Exit from the EXEC
  ping    Send echo messages
  show    Show running system information

R1#
```

Verificar USER | Verificar SUPPORT | Verificar JR-ADMIN | Verificar todas

Haga clic sobre cada botón para ver el contenido asociado.

```
R1# enable view JR-ADMIN
Password:
*Mar  1 10:00:28.365: %PARSER-6-VIEW_SWITCH: successfully set to view 'JR-ADMIN'.

R1# ?
Exec commands:
  enable  Turn on privileged commands
  exit    Exit from the EXEC
  ping    Send echo messages
  reload  Halt and perform a cold restart
  show    Show running system information

R1#
```



Haga clic sobre cada botón para ver el contenido asociado.

```
R1# show parser view
No view is active ! Currently in Privilege Level Context
R1#
R1# enable view
Password:
*Mar  1 10:38:56.233: %PARSER-6-VIEW_SWITCH: successfully set to view 'root'.
R1#
R1# show parser view
Current view is 'root'
R1#
R1# show parser view all
Views/SuperViews Present in System:
 SHOWVIEW
 VERIFYVIEW
 REBOOTVIEW
 SUPPORT *
 USER *
 JR-ADMIN *
 ADMIN *
-------(*) represent superview-------
R1#
```



Haga clic sobre cada botón para ver el contenido asociado.

2.3 Monitoreo y administración de dispositivos

2.3.1 Seguridad de los archivos de configuración y la imagen IOS de cisco

Si un atacante obtuviera acceso a un router, podría hacer muchas cosas. Por ejemplo, podría alterar el flujo del tráfico, cambiar las configuraciones e incluso borrar el archivo de configuración de inicio y la imagen del IOS de Cisco. Si la configuración o la imagen del IOS se borran, el operador quizás nunca recupere una copia archivada para restaurar el router. El proceso de recuperación debe, entonces, tomar lugar en cada router afectado, agregándose al período de inactividad total de la red.

La función de configuración resistente (Resilient Configuration) del IOS de Cisco permite una recuperación más rápida si alguien reformatea la memoria flash o borra el archivo de configuración de inicio en la NVRAM. Esta función permite al router soportar intentos maliciosos de borrar los archivos, asegurando la imagen del router y manteniendo una copia segura de la configuración actual.

Cuando se asegura una imagen IOS de Cisco, la función de configuración resistente deniega todas las solicitudes para copiarla, modificarla o eliminarla. La copia segura de la configuración de inicio se almacena en la flash junto con la imagen segura del IOS. Este conjunto de los archivos de configuración actual y la imagen del IOS de Cisco se conoce como el conjunto de arranque (bootset).

La función de configuración resistente del IOS de Cisco solo está disponible para sistemas que soporten una interfaz flash Advanced Technology Attachment (ATA) PCMCIA. La imagen del IOS de Cisco y configuración actual de respaldo en el dispositivo de almacenamiento externo están ocultas, por lo que los archivos no se incluyen en ningún listado de directorios del disco.

Hay dos comandos de configuración global disponibles para configurar las funciones de configuración resistente del IOS de Cisco: secure boot-image y secure boot-config.



Un hacker puede borrar un router comprometido.

Cisco IOS Resilient Configuration facts

- El archivo de configuración en el grupo de arranque primario es una copia de la configuración actual que estaba en el router cuando se habilitó la función.
- La función asegura el grupo de archivos más pequeño posible para preservar el espacio de almacenamiento. No se requiere espacio extra para asegurar el archivo primario de imagen del IOS de Cisco.
- La función detecta automáticamente diferencias de versión de imagen o de configuración.
- Solo se usa almacenamiento local para asegurar archivos, eliminando desafíos de mantenimiento de escalabilidad que surjan a partir del almacenamiento de múltiples imágenes y configuraciones en servidores TFTP.
- La función puede ser deshabilitada solo a través de una sesión de consola.

El comando secure boot-image

El comando secure boot-image habilita la resistencia de la imagen del IOS de Cisco. Cuando se habilita por primera vez, se asegura la imagen actual del IOS de Cisco, al mismo tiempo que se crea una entrada en el registro. Esta función puede ser deshabilitada solo por medio de una sesión de consola usando la forma no del comando.

Este comando solo funciona adecuadamente cuando el sistema está configurado para ejecutar una imagen de un dispositivo de almacenamiento externo con una interfaz ATA. Adicionalmente, la imagen actual debe ser cargada desde un dispositivo de almacenamiento permanente para ser asegurada como primaria. Las imágenes que arrancan de la red, como un servidor TFTP, no pueden ser aseguradas.

La función de configuración resistente del IOS de Cisco detecta diferencias en la versión de la imagen. Si el router está configurado para arrancar con la función de resistencia del IOS de Cisco y se detecta una versión diferente del software IOS de Cisco, se muestra un mensaje similar al siguiente:

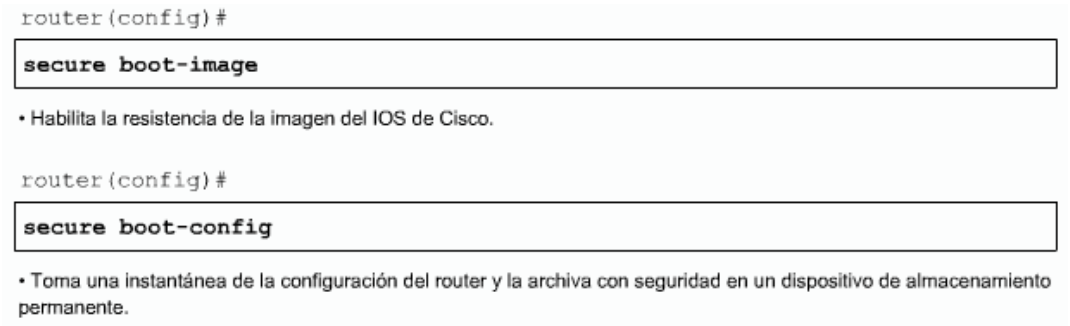
ios resilience: Archived image and configuration version 12.2 differs from running version 12.3

Para actualizar el archivo de imagen a la nueva imagen actual, reingrese el comando secure boot-image desde la consola. Se mostrará un mensaje en relación a la actualización de la imagen. La imagen vieja será liberada y visible en la salida del comando dir.

El comando secure boot-config

Para tomar una instantánea de la configuración actual del router y archivarla de manera segura en el dispositivo de almacenamiento permanente, use el comando secure boot-config en el modo de configuración global. Se mostrará un mensaje del registro en la consola notificando al usuario de que función de adaptabilidad de la configuración ha sido activada. El archivo de configuración está oculto y no puede ser visto o eliminado directamente desde el prompt de la CLI.

El escenario de actualización de la configuración es similar a una actualización de imagen. Esta función detecta una versión diferente de las configuraciones del IOS de Cisco y notifica al usuario de la diferencia de versiones. Puede ejecutarse el comando secure boot-config para actualizar el archivo de configuración a una nueva versión luego de que se han emitido nuevos comandos de configuración.



Los archivos de configuración asegurados no aparecen en la salida de un comando dir que se emite desde la CLI. Esto ocurre porque el sistema de archivos del IOS de Cisco no deja que los archivos asegurados sean enlistados. Ya que la imagen actual y los archivos de configuración actuales no son visibles a través del comando dir, use el comando show secure bootset para verificar la existencia del archivo. Este paso es

importante para verificar que la imagen del IOS de Cisco y los archivos de configuración hayan sido resguardados y asegurados apropiadamente.

Aunque el sistema de archivos del IOS de Cisco previene a estos archivos de ser vistos, el modo ROM monitor (ROMmon) no tiene tales restricciones y puede listar los archivos asegurados y arrancar desde ellos.

Hay cinco pasos para restaurar un conjunto de arranque primario de un archivo seguro luego de que el router ha sido manipulado (si se ha borrado la NVRAM o se ha formateado el disco):

Paso 1. Reiniciar el router usando el comando reload.

Paso 2. Desde el modo ROMmon, ingrese el comando dir para listar los contenidos del dispositivo que contiene el archivo asegurado de conjunto de arranque. Desde la CLI, el nombre del dispositivo puede hallarse en la salida del comando show secure bootset.

Paso 3. Arranque el router con la imagen del conjunto de arranque asegurada usando el comando boot con el nombre de archivo encontrado en el Paso 2. Cuando el router comprometido arranca, cambie al modo EXEC privilegiado y restaure la configuración.

Paso 4. Ingrese al modo de configuración global usando el comando conf t.

Paso 5. Restaure la configuración segura al nombre de archivo proporcionado usando el comando secure boot-config restore nombre-archivo.

```
router#
show secure bootset
```

• Verifica que la imagen del IOS de Cisco y los archivos de configuración hayan sido resguardados y asegurados apropiadamente.

```
Router# show secure bootset
IOS resilience router id FHK085031MD

IOS image resilience version 12.3 activated at 05:00:59 UTC Fri Feb 10 2006
Secure archive flash:c1841-advsecurityk9-mz.123-14.T1.bin type is image (elf) []
file size is 17533860 bytes, run size is 17699528 bytes
 Runnable image, entry point 0x8000F000, run from ram

IOS configuration resilience version 12.3 activated at 05:01:02 UTC Fri Feb 10 2
006
Secure archive flash:.runcfg-20060210-050102.ar type is config
configuration archive size 4014 bytes
```

Por si llegara a ocurrir que un router fuera comprometido o necesitara ser recuperado de una contraseña mal configurada, el administrador debe entender los procedimientos de recuperación de contraseñas. Por razones de seguridad, la recuperación de contraseñas requiere que el administrador tenga acceso físico al router a través de un cable de consola.

Recuperar la contraseña del router toma varios pasos.

Paso 1. Conectarse al puerto de consola.

Paso 2. Use el comando show version para ver y grabar el registro de configuración.

El registro de configuración es similar al BIOS de una computadora, en que controla el proceso de arranque. El registro de configuración, representado por un solo valor hexadecimal, le dice al router qué pasos específicos tomar cuando se enciende. Los registros de configuración tienen muchos usos, y la recuperación de contraseñas probablemente sea el más popular. Para ver y grabar el registro de configuración, use el comando show version.

R1> show version

<Output omitted>

Configuration register is 0x2102

El registro de configuración generalmente está puesto en 0x2102 o 0x102. Si ya no hay acceso al router (por una contraseña de ingreso o TACACS perdida) el administrador puede asumir con seguridad que el registro de configuración estará en 0x2102.

Paso 3. Use el interruptor para apagar y prender el router.

Paso 4. Emita la secuencia de break dentro de los 60 segundos de que el router ha sido apagado y prendido para que el router inicie en modo ROMmon.

Paso 5. Escriba confreg 0x2142 en el prompt rommon 1>.

Esto cambia el registro de configuración por defecto y causa que el router se saltee la configuración de inicio donde la contraseña enable password está almacenada.

Paso 6. Escriba reset en el prompt rommon 2>. El router volverá a iniciarse, pero ignorará la configuración guardada.

Paso 7. Escriba no como respuesta a todas las preguntas del setup, o presione Ctrl-C para saltearse el procedimiento de setup inicial.

Paso 8. Escriba enable en el prompt Router>. Esto pone al router en modo enable y le permite ver el prompt Router#.

Paso 9. Escriba copy startup-config running-config para copiar la NVRAM a la memoria. Tenga cuidado de no escribir copy running-config startup-config porque entonces la configuración inicial se borrará.

Paso 10. Escriba show running-config. En esta configuración, el comando shutdown aparece bajo todas las interfaces porque todas las interfaces están desactivadas. El administrador ahora puede ver las contraseñas (contraseñas enable password, enable

secret, vty y consola), ya sea en formado cifrado o no cifrado. Las contraseñas no cifradas pueden volver a ser usadas, pero las contraseñas cifradas necesitan que se cree una nueva contraseña en su lugar.

Paso 11. Ingrese a la configuración global e ingrese el comando enable secret para cambiar la contraseña enable secret. Por ejemplo

R1(config)# enable secret cisco

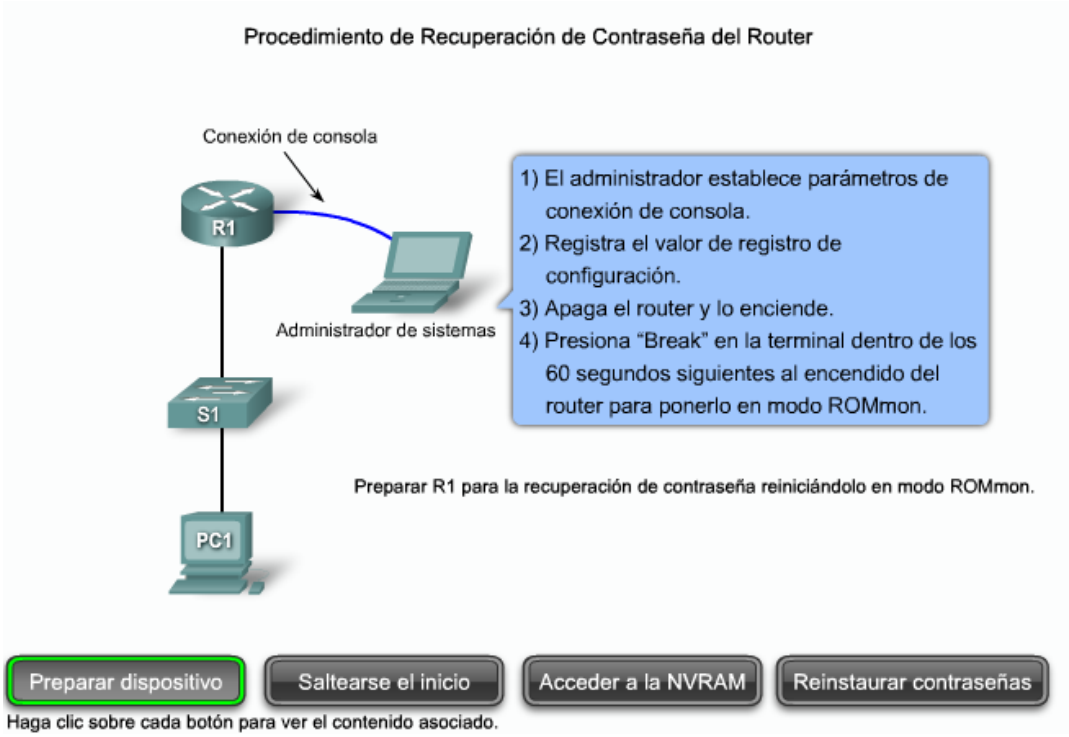
Paso 12. Emita el comando no shutdown en todas las interfaces que va a utilizar. Luego emita el comando show ip interface brief en el modo EXEC privilegiado para confirmar que la configuración de las interfaces es correcta. Todas las interfaces que serán usadas deberían mostrar "up up."

Paso 13. Desde el modo de configuración global, ingreseconfig-register configuration_register_setting. Se modificará el registro de configuración para mostrar el valor del paso 2 o 0x2102. Por ejemplo:

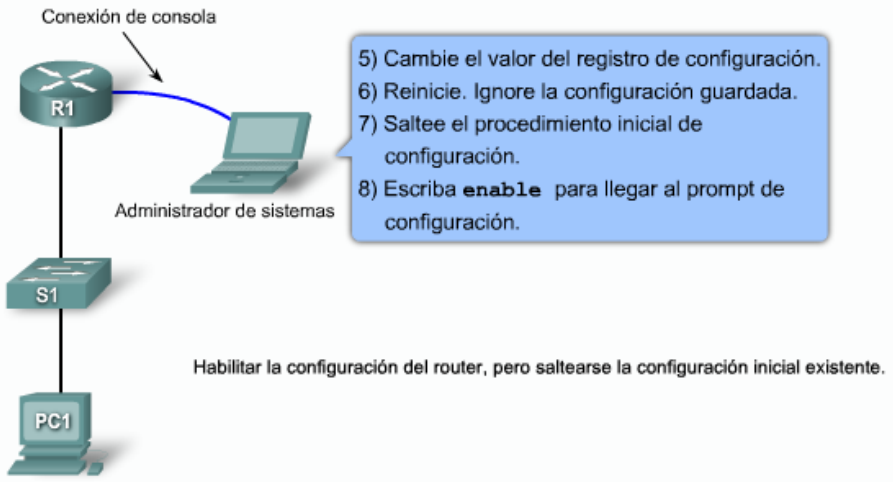
R1(config)# config-register 0x2102

Paso 14. Salve los cambios de configuración usando el comando copy running-config startup-config.

La recuperación de contraseña ha sido completada. Ingrese el comando show version para confirmar que el router vaya a usar el número de registro de configuración ingresado en el próximo arranque.



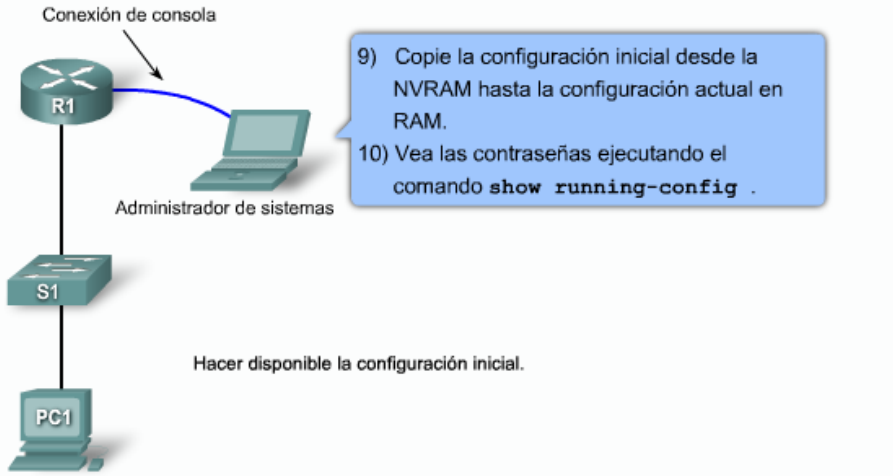
Procedimiento de Recuperación de Contraseña del Router



Preparar dispositivo | Saltearse el inicio | Acceder a la NVRAM | Reinstaurar contraseñas

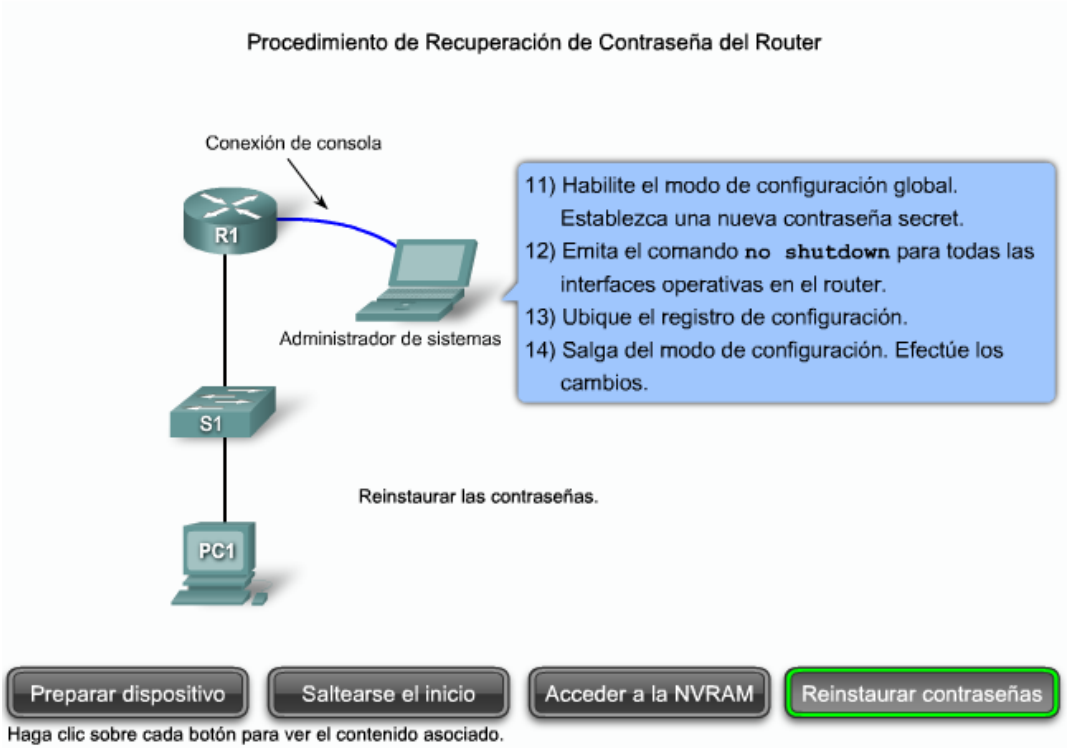
Haga clic sobre cada botón para ver el contenido asociado.

Procedimiento de Recuperación de Contraseña del Router



Preparar dispositivo | Saltearse el inicio | Acceder a la NVRAM | Reinstaurar contraseñas

Haga clic sobre cada botón para ver el contenido asociado.



Si alguien ganara acceso físico al router, podría tomar control del dispositivo a través del procedimiento de recuperación de contraseña. Este procedimiento, si se lo lleva a cabo correctamente, deja intacta la configuración del router. Si el atacante no efectúa grandes cambios, este tipo de ataque es difícil de detectar. Un atacante puede usar este método para descubrir la configuración del router y otra información pertinente sobre la red, como flujos de tráfico y restricciones de control de acceso.

El administrador puede mitigar esta brecha de seguridad potencial usando el comando de configuración global no service password-recovery. El comando no service password-recovery es un comando oculto del IOS de Cisco y no tiene argumentos o palabras clave. Si se configura un router con el comando no service password-recovery, se deshabilita el acceso al modo ROMmon.

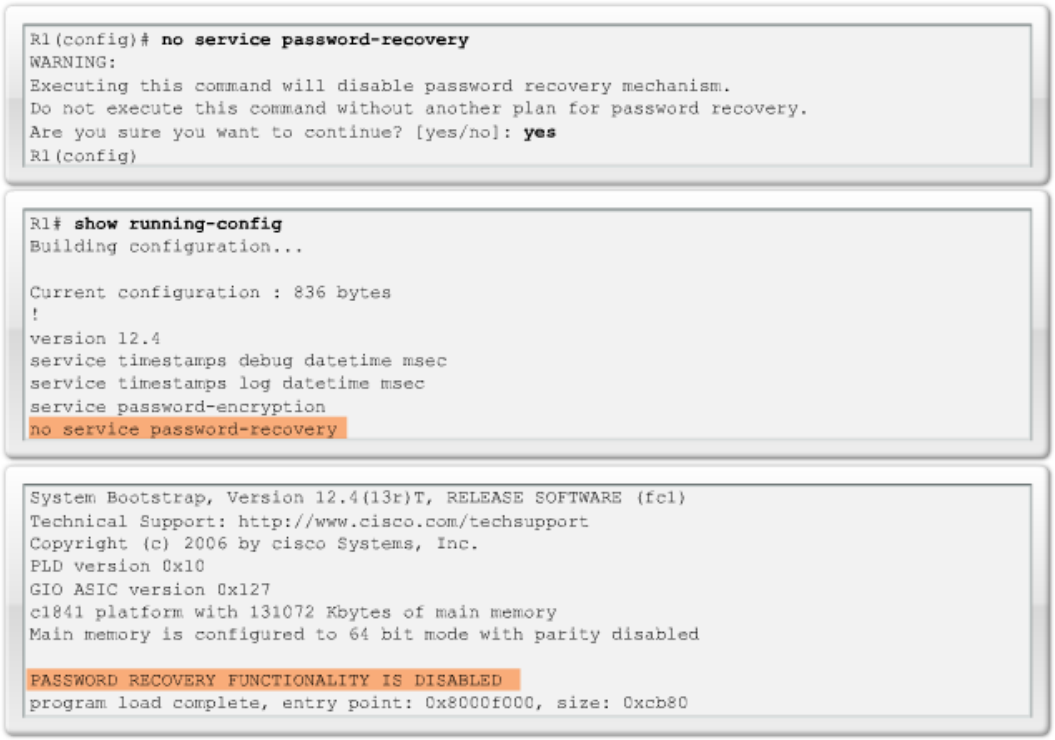
Cuando se ingresa el comando no service password-recovery, se muestra un mensaje de advertencia que debe ser aceptada para que la función se habilite.

El comando show running configuration muestra una sentencia no service password-recovery. Adicionalmente, cuando el router arranca, la secuencia de arranque inicial muestra un mensaje que dice "PASSWORD RECOVERY FUNCTIONALITY IS DISABLED" (la función de recuperación de contraseña está deshabilitada).

Para recuperar a un dispositivo luego de que se ingresa el comando no service password-recovery, debe emitir la secuencia break dentro de los cinco segundos luego de que la imagen se descomprima durante el arranque. Se le pedirá que confirme la acción de break. Luego de que se confirme la acción, se borra completamente la configuración de inicio, se habilita el procedimiento de recuperación de contraseña y el router se reinicia con la configuración por defecto de fábrica. Si no confirma la acción

de break, el router arranca normalmente con el comando no service password-recovery habilitado.

Una advertencia: si la memoria flash del router no contiene una imagen del IOS de Cisco válida por corrupción del archivo o eliminación, el comando ROMmon xmodem no puede ser usado para cargar una nueva imagen flash. Para reparar el router, el administrador debe obtener una nueva imagen del IOS de Cisco e un SIMM flash o una tarjeta PCMCIA card. Visite Cisco.com para más información en relación con el resguardo de imágenes flash.



2.3.2 Administración y reportes seguros

Los administradores de red deben administrar con seguridad todos los dispositivos y hosts en la red. En una red pequeña, administrar y monitorear los dispositivos de red es una operación sencilla. Sin embargo, en una empresa grande con cientos de dispositivos, monitorear, administrar y procesar los mensajes de registros puede ser un desafío.

Deben considerarse muchos factores al implementar una administración segura. Esto incluye administración de cambios en la configuración. Cuando una red está bajo ataque, es importante conocer el estado de dispositivos críticos de la red y cuándo ocurrieron las últimas modificaciones conocidas. La administración de cambios en la configuración también incluye temas como asegurarse de que la gente correcta tenga acceso cuado se adoptan nuevas metodologías de administración y cómo manejar herramientas y dispositivos que ya no se usan. Crear un plan para la administración de cambios debe ser parte de una política de seguridad englobadora; sin embargo,

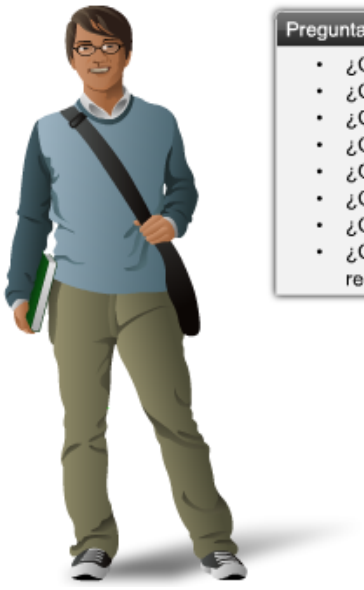
mínimamente, deben registrarse los cambios usando sistemas de autenticación sobre las configuración es de archivos y dispositivos que usen FTP o TFTP.

¿Se está siguiendo una política o un plan de administración de cambios? Estos temas deben ser establecidos y manejados con una política de administración de cambios.

El registro y el reporte de información automáticos de dispositivos identificados a hosts de administración también son consideraciones importantes. Estos registros e informes pueden incluir flujo de contenido, cambios de configuración y nuevas instalaciones de software, para nombrar algunos. Para identificar las prioridades de reporte y monitoreo, es importante tener datos de la administración y de los equipos de redes y seguridad. La política de seguridad también debería tener un rol importante a la hora de responder a qué información registrar y reportar.

Desde un punto de vista de reportes, la mayoría de los dispositivos de redes pueden enviar datos de syslog que pueden volverse invaluables en el momento de contrarestar problemas en la red o amenazas de seguridad. Se pueden enviar datos de cualquier dispositivo a un host de análisis de syslog para su revisión. Estos datos pueden ser revisados en tiempo real, bajo demanda y en informes programados. Hay varios niveles de registro para asegurar que la cantidad correcta de datos sea enviada, de acuerdo con el dispositivo que envía los datos. También es posible marcar los datos de registro del dispositivo dentro del software de análisis para permitir vistas granulares y reportes. Por ejemplo, durante un ataque, los datos de registro provistos por los switches de capa 2 no suelen ser tan interesantes como los datos provistos por el sistema de prevención de intrusos (IPS).

Muchas aplicaciones y protocolos, como SNMP, están disponibles para su uso en sistemas de administración de redes, con el propósito de monitorear y efectuar cambios en la configuración de los dispositivos de manera remota.



Preguntas syslog:

- ¿Cuáles son los registros más importantes?
- ¿Cómo se separan los mensajes importantes de las notificaciones de rutina?
- ¿Cómo se previene la manipulación de los registros?
- ¿Cómo se puede asegurar que las marcas de tiempo coincidan?
- ¿Qué datos del registro se necesitan en investigaciones criminales?
- ¿Cómo se maneja el volumen de mensajes?
- ¿Cómo se manejan todos los dispositivos?
- ¿Cómo se puede establecer cuándo ocurrieron los ataques o los fallos en la red?

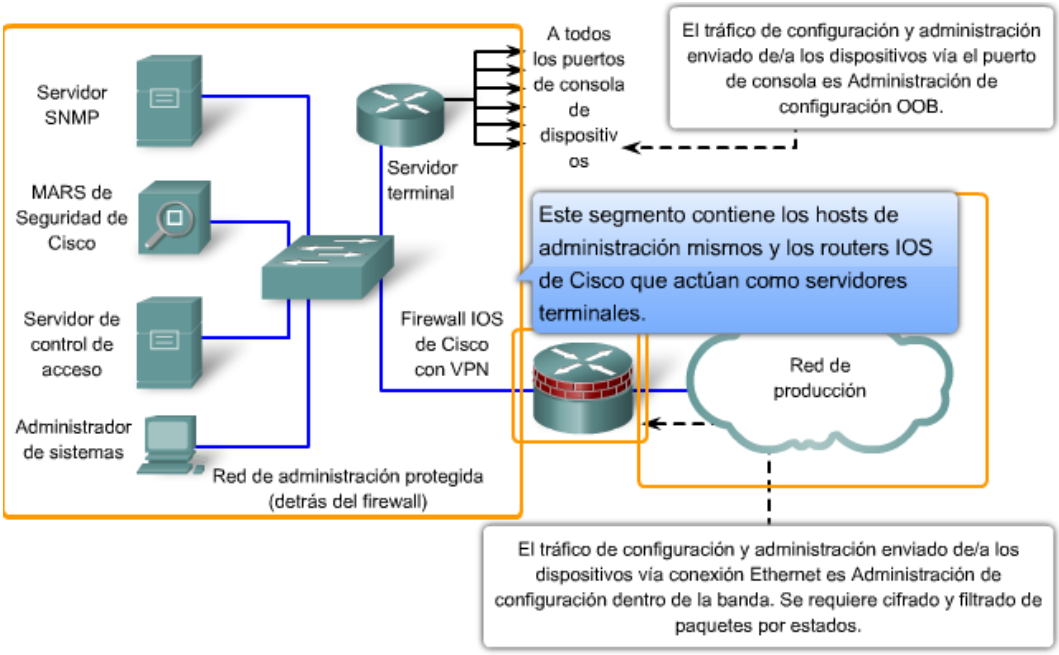
Cuando se registra y se administra información, el flujo de información entre los hosts de administración y los dispositivos administrados puede tomar uno de dos caminos:

Fuera de banda (out-of-band - OOB) - Flujos de información en una red de administración dedicada en los cuales no reside tráfico de producción.
En banda (in-band) - Flujos de información que atraviesan la red de producción de la empresa, Internet o ambos a través de canales de datos comunes.

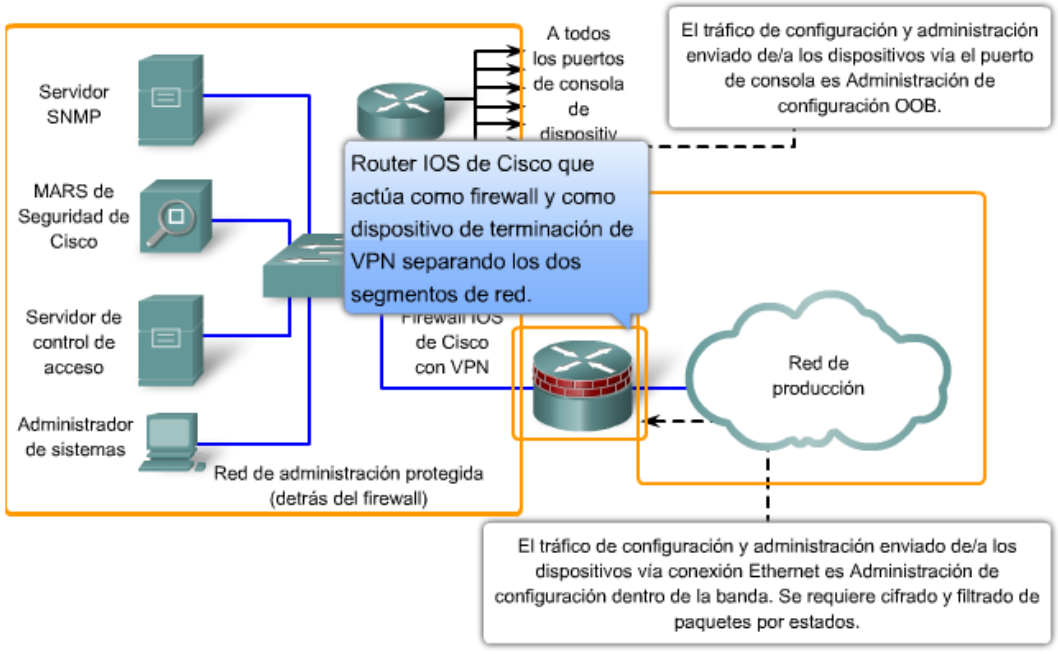
Por ejemplo, una red tiene dos segmentos de red separados por un router IOS de Cisco que actúa como un firewall y un dispositivo de terminación de red privada virtual (VPN). Un lado del firewall está conectado a todos los hosts de administración y a los routers IOS de Cisco que actúan como servidores terminales. Los servidores terminales ofrecen conexiones directas OOB a cualquier dispositivo que solicite administración en la red de producción. La mayoría de los dispositivos debería estar conectada a este segmento y configurarse usando administración OOB.

El otro lado del firewall se conecta con la red de producción en sí. La conexión a la red de producción solo es provista para el acceso selectivo a Internet proveniente de los hosts de administración, el tráfico de administración en banda limitado y el tráfico de administración cifrado proveniente de hosts predeterminados. La administración en banda ocurre solo cuando una aplicación de administración no usa OOB o cuando el dispositivo de Cisco que se administra no tiene suficientes interfaces físicas para soportar la conexión normal a la red de administración. Si un dispositivo debe contactar a un host de administración por medio del envío de datos a través de la red de producción, ese tráfico debería ser enviado de manera segura usando un túnel cifrado privado o un túnel VPN. El túnel deberá ser preconfigurado para permitir solo el tráfico requerido para administración y reportes de estos dispositivos. El túnel también deberá permanecer cerrado para que solo los hosts apropiados puedan iniciar y terminar túneles. El firewall del IOS de Cisco está configurado para permitir pasar información syslog al segmento de administración. Adicionalmente, se permiten Telnet, SSH y SNMP con la condición de que estos servicios sean iniciados por la red de administración.

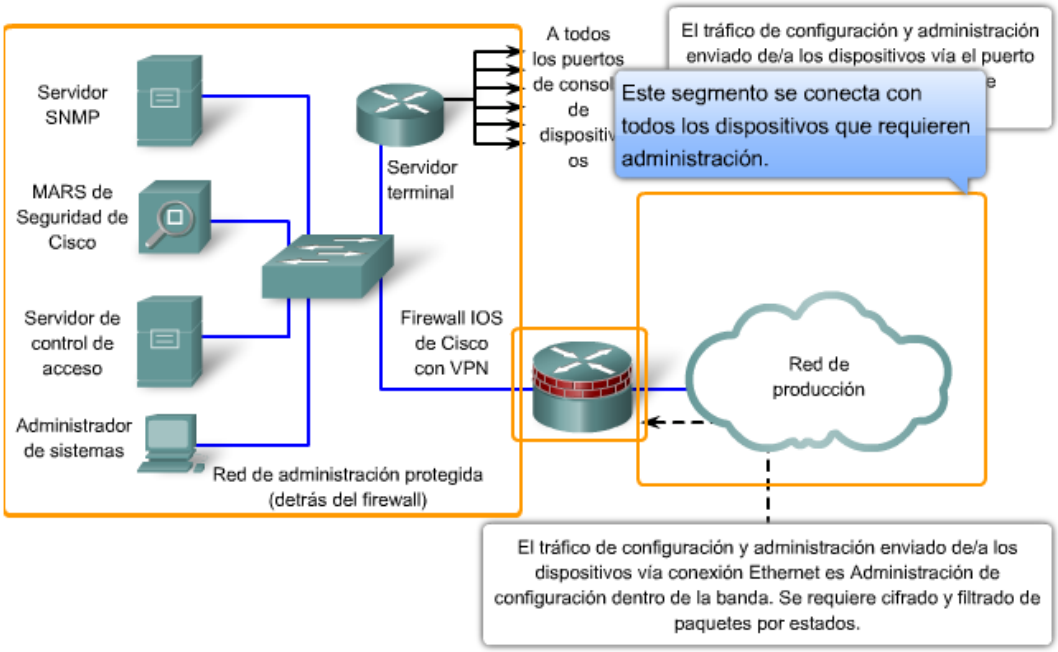
Como la red de administración tiene acceso adminstrativo a casi todas las áreas de la red, puede ser un objetivo muy atractivo para los hackers. El módulo de administración del firewall fue diseñado con muchas tecnologías hechas especialmente para mitigar tales riesgos. La principal amenaza es un hacker que intente ganar acceso a la red de administración en sí. Esto puede ser logrado a través de un host administrado comprometido al que el dispositivo de administración deba acceder. Para mitigar la amenaza de un dispositivo comprometido, debe implementarse un fuerte control de acceso en el firewall y en todos los otros dispositivos. Adicionalmente, los dispositivos de administración deben colocarse de manera tal que prevenga comunicación directa con otros hosts de la misma subred de administración, usando segmentos LAN o VLANs separados.



Pase por encima de las áreas resaltadas para mayor información.



Pase por encima de las áreas resaltadas para mayor información.



Pase por encima de las áreas resaltadas para mayor información.

Como regla general, para propósitos de seguridad, la administración OOB es apropiada para redes de empresas grandes. Sin embargo, no siempre es deseable. Muchas veces, la decisión depende del tipo de aplicaciones de administración que están corriendo y los protocolos que se están monitoreando, por ejemplo, una herramienta de administración que tiene el propósito de determinar la posibilidad de alcance de todos los dispositivos de una red. Considere una situación en la que dos switches principales están siendo administrados y monitoreados a través de una red OOB. Si un enlace crítico entre estos dos switches de administración falla en la red de producción, la aplicación que los monitorea puede nunca llegar a determinar que el enlace ha fallado para poder alertar al administrador. Esto ocurriría porque la red OOB hace que todos los dispositivos aparezcan como asociados a una sola red de administración OOB. La red de administración OOB no es afectada por el enlace caído. Con aplicaciones de administración como éstas, es preferible ejecutar la aplicación de administración en banda de manera segura.

La administración en banda también se recomienda en redes pequeñas, como forma de reducir los costos de la seguridad en la red. En tales arquitecturas, el tráfico de administración fluye en banda en todos los casos y se asegura en lo posible usando variantes seguras ante protocolos de administración inseguros (SSH en lugar de Telnet, por ejemplo). Otra opción es crear túneles seguros, usando protocolos como IPsec, para el tráfico de administración. Si el acceso de administración no es necesario constantemente, quizás se puedan hacer agujeros temporarios en el firewall con el exclusivo fin de realizar las funciones de administración. Esta técnica debe ser usada con precaución y todos los agujeros deben cerrarse inmediatamente después de completar las funciones de administración.

Finalmente, si se usan herramientas de administración remota con administración en banda, tenga cuidado con las vulnerabilidades de seguridad subyacentes en la herramienta de administración misma. Por ejemplo, los administradores de SNMP

generalmente están acostumbrados a resolver problemas y realizar tareas de configuración en la red. Sin embargo, SNMP debe ser tratado con el mayor cuidado, ya que el protocolo subyacente tiene su propio grupo de vulnerabilidades de seguridad.



Consejos de administración OOB
- Proporcione seguridad del más alto nivel y mitigue los riesgos de pasar protocolos de administración inseguros por la red de producción.

Consejos de administración dentro de la banda
- Aplíquela solo a los dispositivos que requieren administración o monitoreo.
- Use IPsec, SSH o SSL cuando sea posible.
- Pregúntese si el canal de administración necesita estar abierto permanentemente.

2.3.3 Uso de syslog para la seguridad en redes

La implementación de una herramienta de registro en el router es una parte importante de cualquier política de seguridad de redes. Los routers de Cisco pueden registrar información en relación a los cambios de configuración, violaciones de las ACL, el estado de las interfaces y muchos otros tipos de eventos. Los routers de Cisco pueden enviar mensajes de registro a muchos destinos diferentes. El router debería ser configurado para enviar mensajes de registro a uno o más de los siguientes destinos.

Consola - El registro de consola está habilitado por defecto. Los mensajes se registran a la consola y pueden ser visualizados cuando se modifica o se prueba el router usando software de emulación de terminal mientras se está conectado al puerto de consola del router.
Líneas de terminal - Las sesiones EXEC habilitadas pueden ser configuradas para recibir mensajes de registro en cualquiera de las líneas de terminal. Similar al registro de consola, este tipo de registro no se almacena en el router y, por lo tanto, solo es útil para el usuario en esa línea.

Registro de buffer - El registro de buffer es un poco más útil como herramienta de seguridad porque los mensajes quedan almacenados en la memoria del router por un cierto tiempo. Sin embargo, los eventos se limpian cada vez que el router se reinicia.
SNMP traps - Algunos umbrales pueden ser preconfigurados en los routers y otros dispositivos. Los eventos de los routers, como la superación de un umbral, pueden ser procesados por el router y reenviados como traps SNMP a un servidor SNMP externo. Las traps SNMP son una herramienta de registro de seguridad viable, pero requieren la configuración y mantenimiento de un sistema SNMP.
Syslog - Los routers Cisco pueden ser configurados para reenviar mensajes de registro a un servicio syslog externo. Este servicio puede residir en uno o muchos servidores o

estaciones de trabajo, incluyendo sistemas basados en UNIX o Microsoft Windows, o el dispositivo MARS de Seguridad de Cisco. Syslog es la herramienta de registro de mensajes más popular, ya que proporciona capacidades de almacenamiento de registro de largo plazo y una ubicación central para todos los mensajes del router.

Los mensajes de registro de los routers Cisco caen en uno de ocho niveles. Cuanto más bajo el número de nivel, mayor su severidad.

Los mensajes de registro de los routers Cisco contienen tres partes principales:

Marca de tiempo
Nombre y nivel de severidad del mensaje de registro
Texto del mensaje

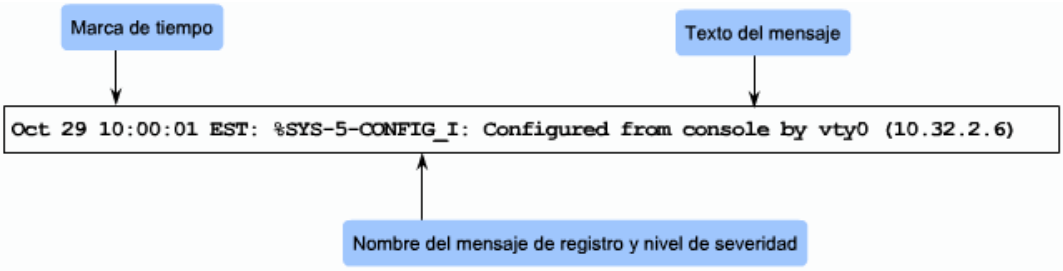


Nivel	Palabra clave	Descripción	Definición
0	emergencies	El sistema no se puede usar.	LOG_EMERG
1	alerts	Se requiere acción inmediata.	LOG_ALERT
2	critical	Existen condiciones críticas.	LOG_CRIT
3	errors	Existen condiciones de error.	LOG_ERR
4	warnings	Existen condiciones de advertencia.	LOG_WARNING
5	notification	Condiciones normales pero significativas.	LOG_NOTICE
6	informational	Mensajes solo informativos.	LOG_INFO
7	debugging	Mensajes de debugging.	LOG_DEBUG

Nivel syslog y nombre	Definición	Ejemplo
0 LOG_EMERG	Una condición de pánico que se envía por broadcast a todos los usuarios	El software IOS de Cisco no pudo cargarse
1 LOG_ALERT	Condición que requiere corrección inmediata, como una base de datos del sistema corrupta	Temperatura demasiado alta
2 LOG_CRIT	Condiciones críticas; por ejemplo, errores en el dispositivo	Imposible alocar memoria
3 LOG_ERR	Errores	Tamaño de memoria no válido
4 LOG_WARNING	Mensajes de advertencia	Falló la operación criptográfica
5 LOG_NOTICE	Condiciones sin errores que pueden requerir manejo especial	Cambio de estado de una interfaz, up o down
6 LOG_INFO	Mensajes informativos	Paquete denegado por una ACL
7 LOG_DEBUG	Mensajes que contienen información normalmente usada solo cuando se hace debugging en un programa	Tipo de paquete no válido

Niveles de severidad | Ejemplos | Mensaje de registro

Haga clic sobre cada botón para ver el contenido asociado.



El ejemplo muestra una entrada de un mensaje syslog de nivel 5, que indica que alguien ha configurado el router usando el puerto 0 vty.

Niveles de severidad | Ejemplos | Mensaje de registro

Haga clic sobre cada botón para ver el contenido asociado.

Syslog es el estándar para registrar eventos del sistema. Las implementaciones syslog contienen dos tipos de sistemas.

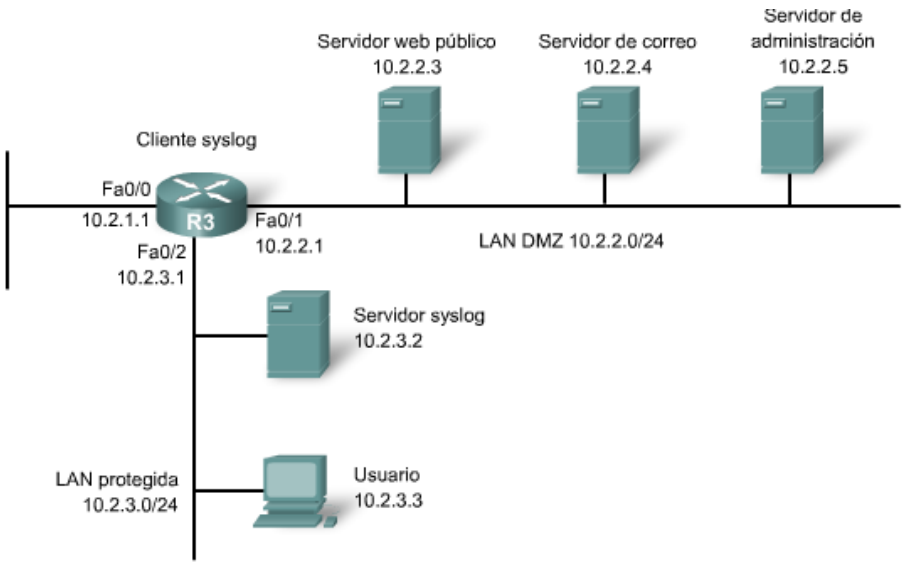
Servidores syslog - También conocidos como hosts de registro, estos sistemas aceptan y procesan mensajes de registro de clientes syslog.
Clientes syslog - Routers u otros tipos de equipamiento que generan y reenvían mensajes de registro a servidores syslog.

El protocolo syslog permite que se envíen mensajes de inicio de sesión desde un cliente syslog al servidor syslog. Aunque la habilidad de enviar registros a un servidor syslog

central es parte de una buena solución de seguridad, también puede ser parte de un problema potencial de seguridad. El problema más grande es la enormidad de la tarea de navegar toda la información resultante, correlacionar los eventos de varios dispositivos de red diferentes y servidores de aplicaciones, y realizar diferentes tipos de acciones basándose en una evaluación de vulnerabilidades que causaron el incidente.

El Sistema de Monitoreo, Análisis y Respuesta de Seguridad de Cisco (Security Monitoring, Analysis, and Response System - MARS) es un dispositivo de seguridad de Cisco que puede recibir y analizar mensajes syslog de varios dispositivos de red y hosts de Cisco y otras marcas. El MARS de seguridad de Cisco extiende la línea de productos de administración de seguridad para la iniciativa de la Red Autodefensiva de Cisco. El MARS de seguridad de Cisco es el primer dispositivo ideado para el propósito de la mitigación de amenazas de seguridad en tiempo real.

El MARS de seguridad de Cisco monitorea muchos tipos de tráfico de registros y reportes disponible en los productos de seguridad y red en la red de la empresa. El MARS de seguridad de Cisco combina todos estos datos de registros en una serie de sesiones que luego compara con una base de datos de reglas. Si las reglas indican que puede haber un problema, se dispara un incidente. Con el uso de este método, el administrador de la red puede hacer que el dispositivo MARS de seguridad de Cisco procese la mayoría de los datos de registro de los dispositivos de la red y enfocar los esfuerzos humanos en los problemas potenciales.



- El servidor syslog es un dispositivo que acepta y procesa los mensajes de registro de uno o más clientes syslog.
- El cliente syslog es un router o algún otro tipo de equipo que genera mensajes de registro y los reenvía a un servidor syslog.

Use los siguientes pasos para configurar el registro del sistema.

Paso 1. Establezca el host de registro de destino usando el comando logging host.

Paso 2. (Opcional) Establezca el nivel de severidad del registro (trap) usando el comando logging trap nivel.

Paso 3. Establezca la interfaz de origen usando el comando logging source-interface. Esto especifica que los paquetes syslog contienen la dirección IPv4 o IPv6 de una interfaz particular, sin importar cuál interfaz usa el paquete para salir del router.

Paso 4. Habilite el registro usando el comando logging on. Puede habilitar o deshabilitar el registro para estos destinos individualmente usando los comandos logging buffered, logging monitor y logging de configuración global. Sin embargo, si el comando logging on está deshabilitado, no se envían mensajes a estos destinos. Solo la consola recibe mensajes.

```
router(config)#
logging host [host-name | ip address]
```

Parámetro	Descripción
host-name	Nombre del host que quiere usar como servidor syslog.
ip-address	Dirección IP del host que quiere usar como servidor syslog.

Establecer host | Establecer nivel | Establecer interfaz | Habilitar registros | Configuración de ejemplo

Haga clic sobre cada botón para ver el contenido asociado.

```
router(config)#
logging trap level
```

Parámetro	Descripción
level	Limita el registro de mensajes a los servidores syslog un nivel específico y menores. Puede ingresar el número (0 a 7) o el nombre del nivel.

Establecer host | Establecer nivel | Establecer interfaz | Habilitar registros | Configuración de ejemplo

Haga clic sobre cada botón para ver el contenido asociado.

```
router(config)#
logging source-interface interface-type interface-number
```

Parámetro	Descripción
interface-type	Tipo de interfaz (por ejemplo, FastEthernet)
interface-number	Número de interfaz (por ejemplo, 0/1)

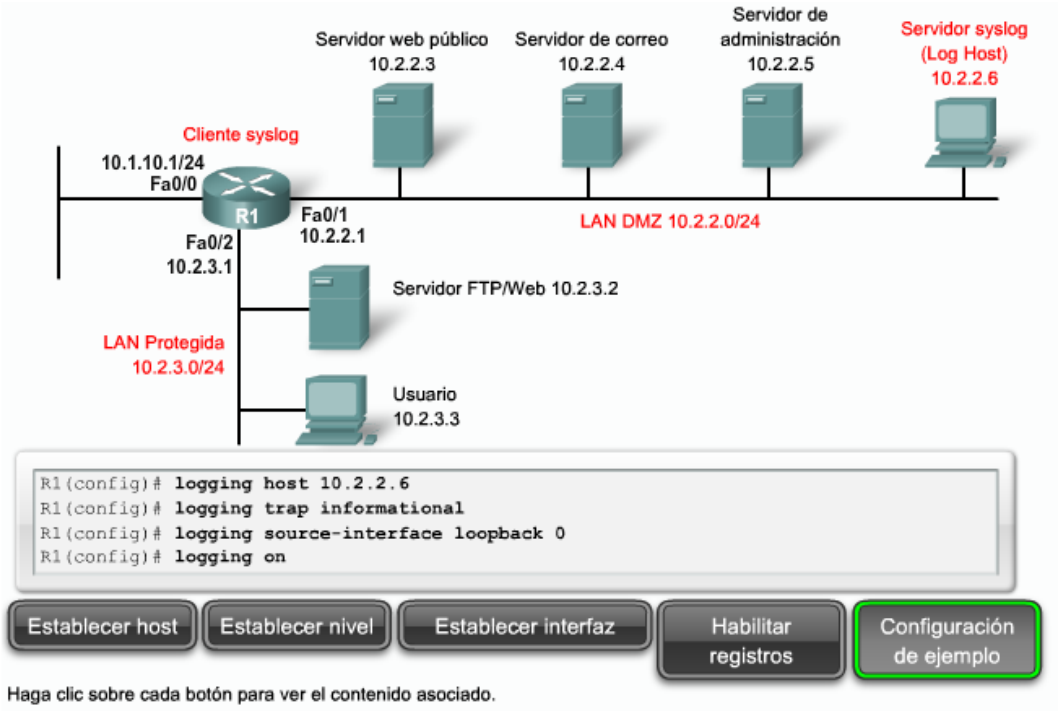
Establecer host | Establecer nivel | Establecer interfaz | Habilitar registros | Configuración de ejemplo

Haga clic sobre cada botón para ver el contenido asociado.

```
router(config)#
logging on
```

Establecer host | Establecer nivel | Establecer interfaz | Habilitar registros | Configuración de ejemplo

Haga clic sobre cada botón para ver el contenido asociado.



Para habilitar el registro de syslog en su router usando el Administrador de Dispositivos de Seguridad (Security Device Manager - SDM) y el Router Cisco, siga estos pasos.

Paso 1. Vaya a Configure > Additional Tasks > Router Properties > Logging.

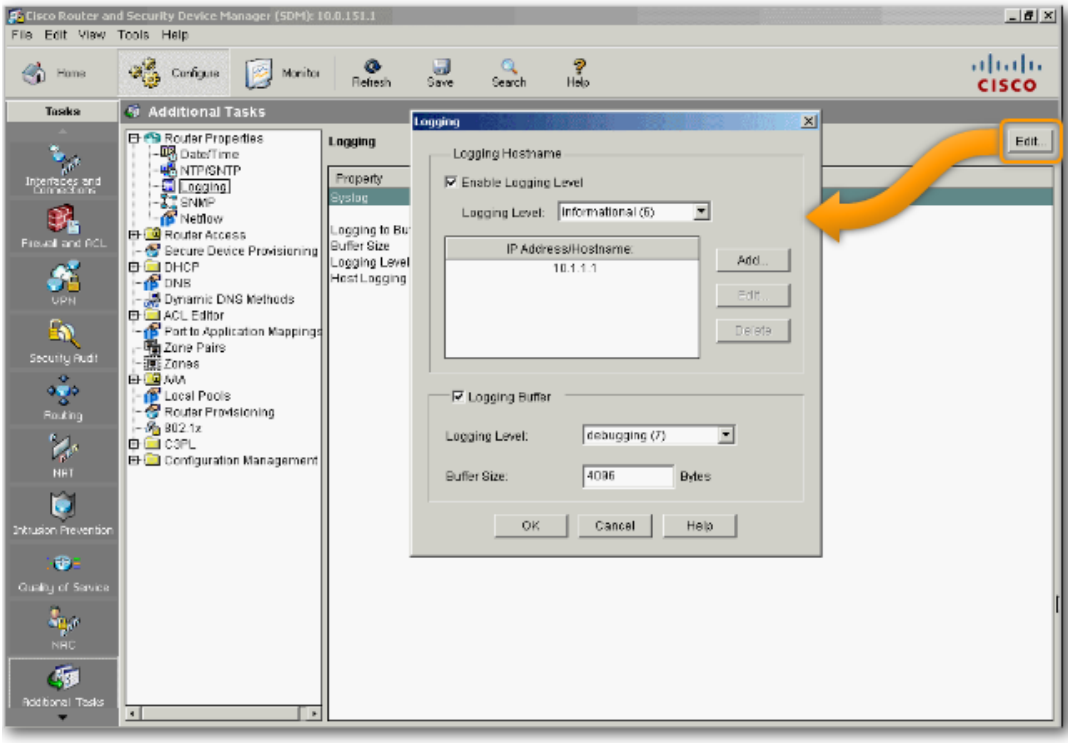
Paso 2. Desde el panel de registro, seleccione Edit.

Paso 3. En la ventana de registro, seleccione Enable Logging Level y vaya al nivel de registro desde la caja de Logging Level. Los mensajes serán registrados para el nivel seleccionado y los inferiores.

Paso 4. Haga clic en Add e ingrese una dirección IP de un host de registro en el campo IP Address/Hostname.

Paso 5. Haga clic sobre OK para volver a la caja de diálogo del registro.

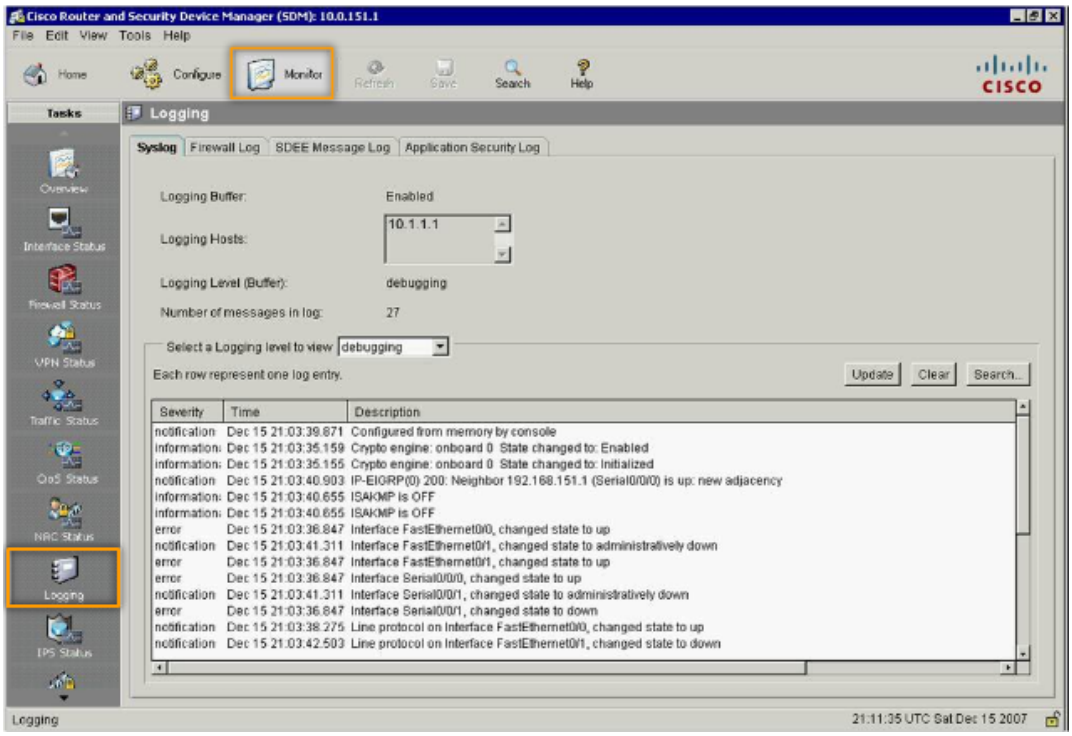
Paso 6. Haga clic en OK para aceptar los cambios y volver al panel de registro.



Los SDM de Cisco pueden ser usados para monitorear el registro eligiendo Monitor > Logging.

Desde la pestaña Syslog puede realizar las siguientes funciones:

Ver los hosts de registro a los cuales el router registra mensajes.
Elija el nivel de severidad mínimo para ver.
Monitorear los mensajes de syslog del router, actualizar la ventana para que muestre las entradas del registro más recientes y borrar todos los mensajes syslog del buffer del registro del router.



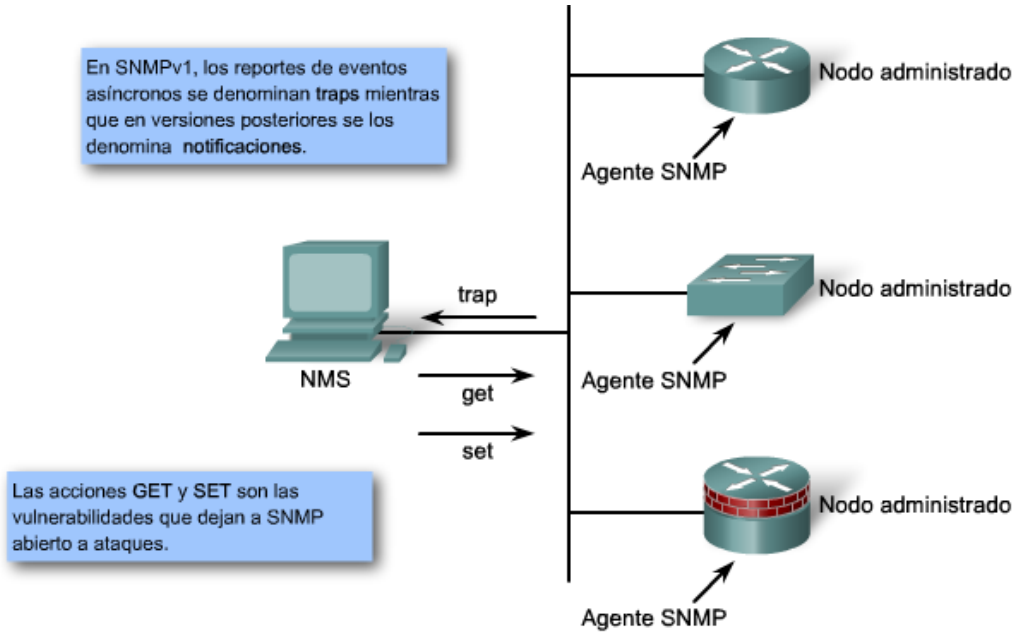
2.3.4 Uso de SNMP para la seguridad en redes

Otra herramienta común de monitoreo es SNMP. SNMP fue desarrollado para administrar nodos, como servidores, estaciones de trabajo, routers, switches, hubs y dispositivos de seguridad, en una red IP. SNMP es un protocolo de capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. SNMP es parte de la suite del protocolo TCP/IP. SNMP permite a los administradores de red administrar el rendimiento de la red, encontrar y resolver problemas en la red, y planear su crecimiento. Hay diferentes versiones de SNMP.

SNMP version 1 (SNMPv1) y SNMP version 2 (SNMPv2) están basadas en administradores (sistemas de administración de redes - network management systems [NMSs]), agentes (nodos administrados), y Bases de Información de Administración (Management Information Bases - MIBs). En cualquier configuración, por lo menos un administrador ejecuta software de administración SNMP. Los dispositivos de red que requieren administración, como los switches, routers, servidores y estaciones de trabajo, están equipados con un módulo de software de agente SNMP. El agente es responsable de proveer acceso a una MIB local de objetos que refleja los recursos y actividad en su nodo. Las MIBs almacenan datos sobre la operación del dispositivo y se espera que estén disponibles para usuarios remotos autenticados.

El administrador SNMP puede obtener (get) información del agente y cambiar (set) información en el agente. Los sets pueden cambiar variables de configuración en el dispositivo agente o iniciar acciones en los dispositivos. Una respuesta a un set indica la nueva configuración en el dispositivo. Por ejemplo, un set puede hacer que un router se reinicie o que envíe o reciba un archivo de configuración. Las traps SNMP permiten a un agente notificar a la estación de administración de eventos significativos mediante el

envíio de un mensaje SNMP no solicitado. La acción de los gets y sets conforma las vulnerabilidades que dejan a SNMP abierto a ataques.



Los agentes SNMP aceptan comandos y solicitudes de los sistemas de administración SNMP solo si esos sistemas tienen un community string correcto. Un community string SNMP es una cadena de texto que puede autenticar mensajes que pasan entre una estación de administración y un agente SNMP y permite acceso a la información en las MIBs. Los community strings se usan esencialmente para autenticación de solo contraseña en los mensajes entre el NMS y el agente.

Hay dos tipos de community strings.

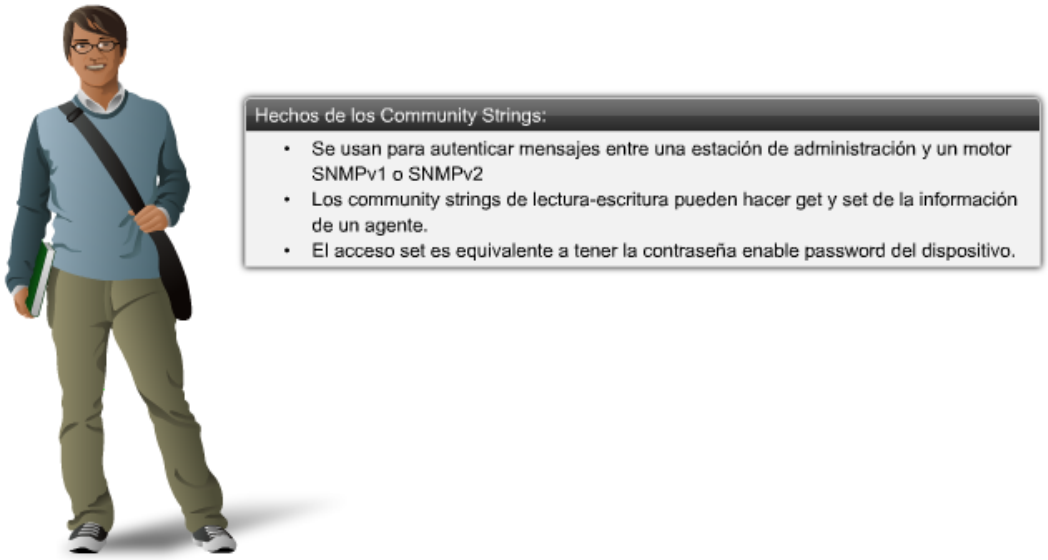
Community strings de solo lectura - Proporcionan acceso de solo lectura a todos los objetos en la MIB, excepto los community strings.
Community strings de lectura-escritura - Proporcionan acceso de lectura-escritura a todos los objetos en la MIB, excepto los community strings.

Si el administrador usa uno de los community strings de solo lectura correctos, puede hacer get o set de la información en el agente. En efecto, tener acceso set a un router es equivalente a tener la contraseña enable password del router.

Por defecto, la mayoría de los sistemas SNMP usa "public" como community string. Si usted configura su router agente SNMP para que use este community string tan comúnmente conocido, cualquiera que tenga un sistema SNMP podrá leer la MIB del router. Como las variables de la MIB de los routers pueden apuntar a tablas de enrutamiento y otras partes críticas de la configuración del router, es extremadamente importante que usted cree sus propios community strings SNMP personalizados. Sin embargo, incluso si se cambia el community string, los strings se envían en texto plano. Esta es una enorme vulnerabilidad en la arquitectura SNMPv1 y SNMPv2.

Si se usa una administración en banda, para reducir los riesgos de seguridad, la administración SNMP deberá configurarse para solo extraer información de los dispositivos en lugar de además permitirse insertar cambios "set" en los dispositivos. Para asegurar que la información de administración sea extraída, cada dispositivo deberá configurarse con un community string SNMP de solo lectura.

Mantener el tráfico SNMP en un segmento de administración permite al tráfico atravesar un segmento aislado cuando la información de administración se extrae de dispositivos y cuando los cambios de configuración se insertan en un dispositivo. Por lo tanto, si se usa una red OOB, es aceptable configurar un community string SNMP de lectura-escritura; sin embargo, tenga en consideración el aumento de riesgos de seguridad de un string en texto plano que permite modificaciones de las configuraciones de los dispositivos.

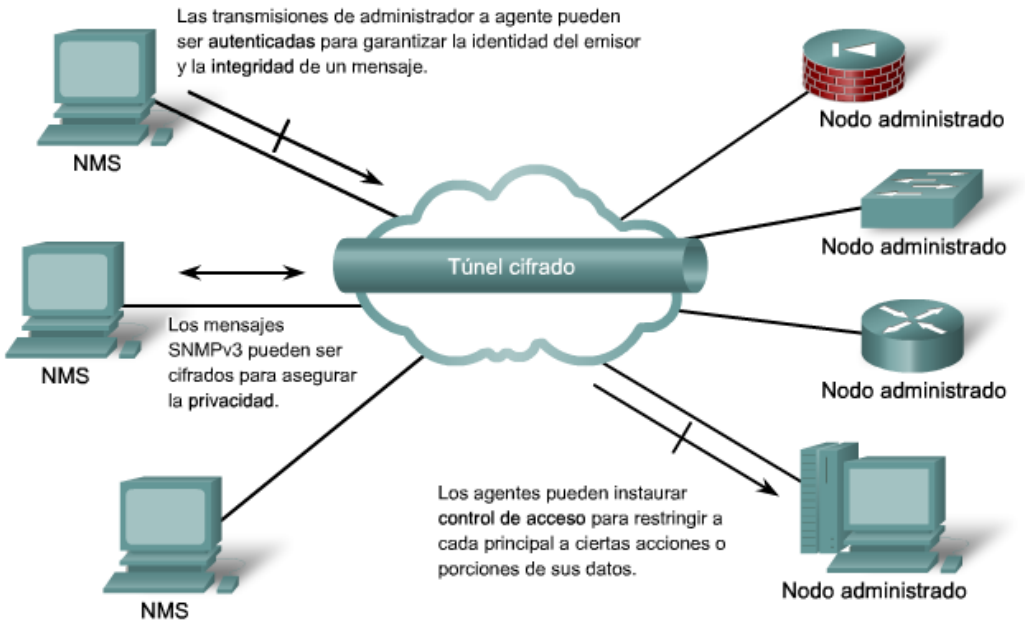


La versión actual de SNMPv3 resuelve las vulnerabilidades de las versiones anteriores incluyendo tres servicios importantes: autenticación, privacidad y control de acceso.

SNMPv3 es un protocolo interoperable basado en estándares para administración de redes. SNMPv3 usa una combinación de autenticación y cifrado de paquetes en la red para proporcionar acceso seguro a los dispositivos. SNMPv3 proporciona tres funciones de seguridad.

Integridad del mensaje - Asegura que el paquete no ha sido manipulado en su tránsito por la red.
Autenticación - Determina que el mensaje proviene de un origen válido.
Cifrado - Mezcla los contenidos de un paquete para evitar que pueda ser visualizado por una fuente no autorizada.

Aunque se recomienda usar SNMPv3 cuando sea posible por las funciones de seguridad agregadas, configurar SNMPv3 está más allá del alcance de este curso.



Al habilitar SNMP, es importante considerar el modelo y el nivel de seguridad. El modelo de seguridad es una estrategia de autenticación que se establece para un usuario y el grupo en el que el usuario reside. Actualmente, el software IOS de Cisco soporta tres modelos de seguridad: SNMPv1, SNMPv2 y SNMPv3. El nivel de seguridad es el nivel permitido de seguridad dentro de un modelo de seguridad. El nivel de seguridad es un tipo de algoritmo de seguridad que se emplea en cada paquete SNMP.

Hay tres niveles de seguridad.

noAuth - Autentica el paquete por medio de una comparación de strings en el nombre de usuario o community string.
auth - Autentica el paquete usando el Código de Autenticación de Mensaje Difuso (Hashed Message Authentication Code - HMAC) con el método MD5 o el método de Algoritmos de Difusión Seguros (Secure Hash Algorithms - SHA). RFC 2104, HMAC: Keyed-Hashing for Message Authentication describe el método HMAC.

priv - Autentica el paquete usando los algoritmos HMAC MD5 o HMAC SHA y cifra el paquete usando los algoritmos de Estándar de Cifrado de Datos (Data Encryption Standard - DES), DES Triple (3DES), o Estándar de Cifrado Avanzado (Advanced Encryption Standard - AES).

La combinación del modelo y el nivel determina el mecanismo de seguridad que se emplea cuando se maneja un paquete SNMP. Solo SNMPv3 soporta los niveles de seguridad auth y priv. Sin embargo, el SDM de Cisco no soporta la configuración de SNMPv3.

Para habilitar SNMPv1 y SNMPv2 usando un SDM de Cisco, siga los siguientes pasos:

Paso 1. Vaya a Configure > Additional Tasks > Router Properties > SNMP. Haga clic sobre Edit.

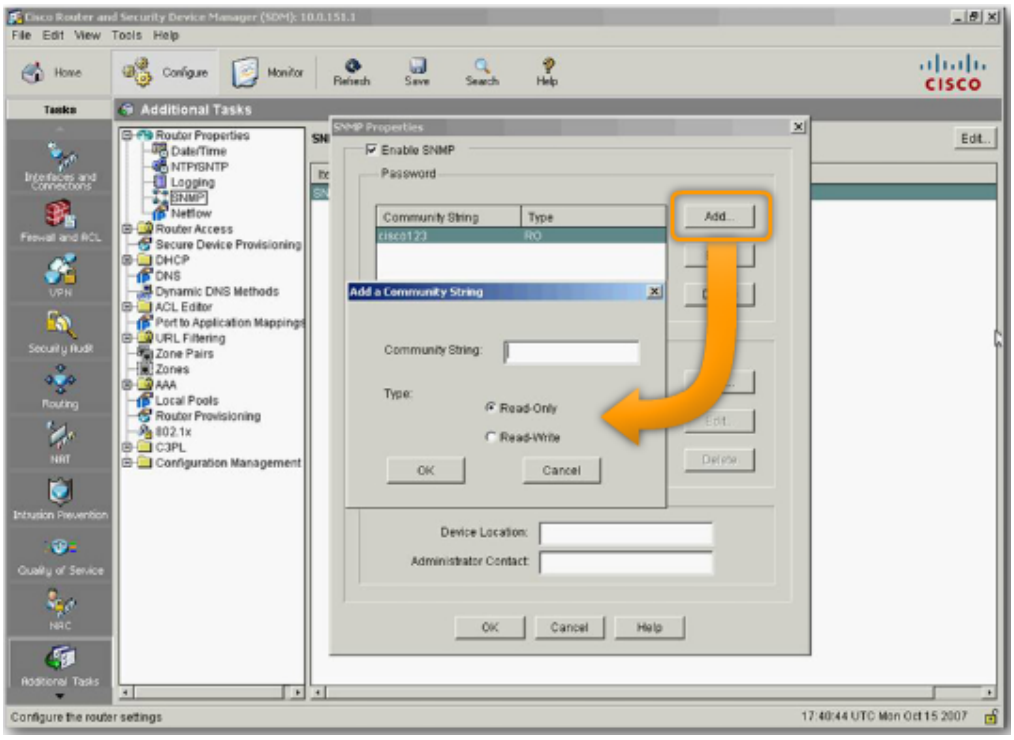
Paso 2. Desde la ventana SNMP Properties, seleccione Enable SNMP para habilitar el soporte de SNMP.

Establezca community strings e ingrese la información del administrador de traps desde la misma ventana de SNMP Properties que usó para habilitar el soporte.

Paso 3. En la ventana de SNMP Properties, haga clic sobre Add para crear nuevos community strings, haga clic sobre Edit para editar un community string existente, o haga clic sobre Delete para eliminar un community string.

Un comando ejemplo de la CLI que SDM generaría basándose en un community string de solo lectura cisco123 sería snmp-server community cisco123 ro.

ro - Asigna un community string de solo lectura.
rw - Asigna un community string de lectura-escritura.



El administrador puede también configurar dispositivos a los que el router envía traps. Estos dispositivos se conocen como receptores de traps. Los SDM de Cisco pueden ser usados para agregar, editar o borrar un receptor de traps.

Paso 1. Desde el panel SNMP en el SDM de Cisco, haga clic sobre Edit. Se mostrará la ventana SNMP Properties.

Paso 2. Para agregar un nuevo receptor de traps, haga clic sobre Add en la sección Trap Receiver de la ventana SNMP Properties. Se mostrará la ventana Add a Trap Receiver.

Paso 3. Ingrese la dirección IP o nombre de host del receptor de traps y la contraseña que se usará para conectarse a él. Típicamente, la dirección IP será la de la estación de

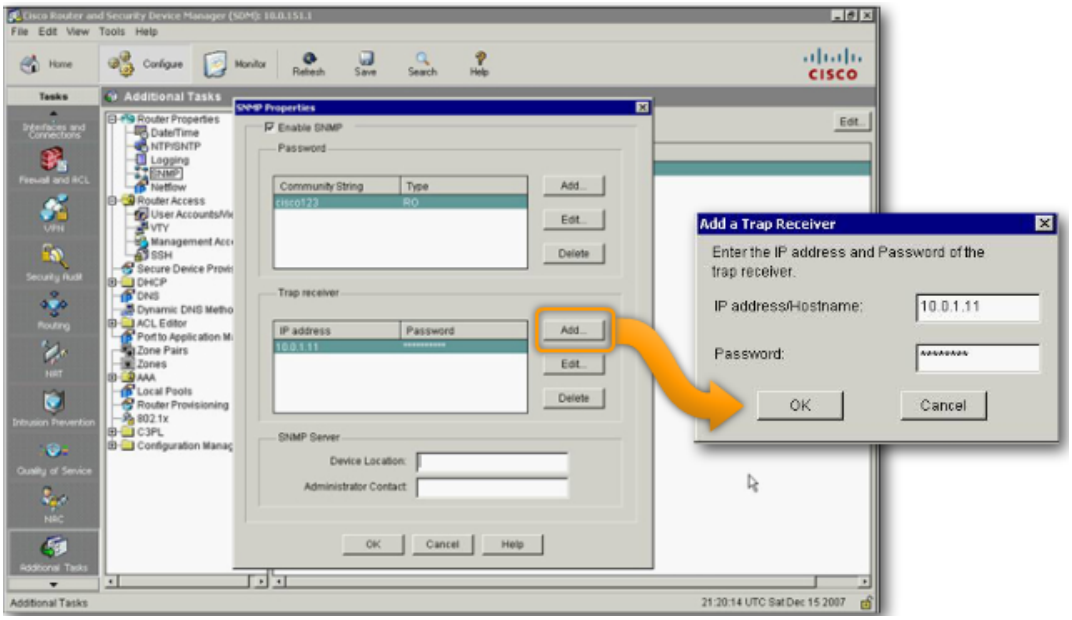
administración SNMP que monitorea su dominio. Verifique la dirección con el administrador del sitio si no está seguro.

Paso 4. Haga clic sobre OK para terminar de agregar el receptor de traps.

Paso 5. Para editar un receptor de traps existente, elija uno de la lista y haga clic sobre Edit. Para eliminar un receptor de traps existente, elija uno de la lista y haga clic sobre Delete.

Paso 6. Cuando la lista de receptores de traps esté completa, haga clic sobre OK para volver al panel de SNMP.

La ventana de SNMP Properties también contiene los campos SNMP Server Device Location field y SNMP Server Administrator Contact. Ambos campos son campos de texto que pueden ser usados para ingresar información descriptiva sobre la ubicación del servidor e información de contacto de la persona que administra el servidor SNMP. Estos campos no son obligatorios y no afectan la operación del router.



2.3.5 Uso de NTP

Muchos aspectos de la seguridad de una red, como los registros de seguridad, dependen de una fecha y marca de tiempo correcta y precisa. Cuando se lucha contra una amenaza, cada segundo importa, ya que es importante identificar el orden en que ocurrió un ataque específico. Para asegurarse de que los mensajes del registro estén sincronizados entre sí deben mantenerse los relojes de los hosts y los dispositivos de red sincronizados entre sí.

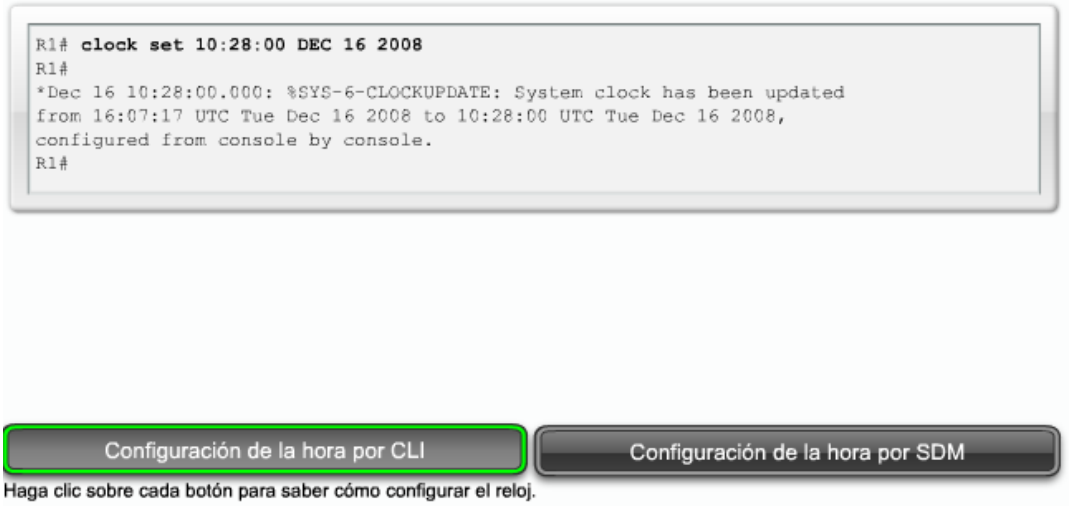
Típicamente, se pueden configurar la fecha y la hora en el router mediante dos métodos:

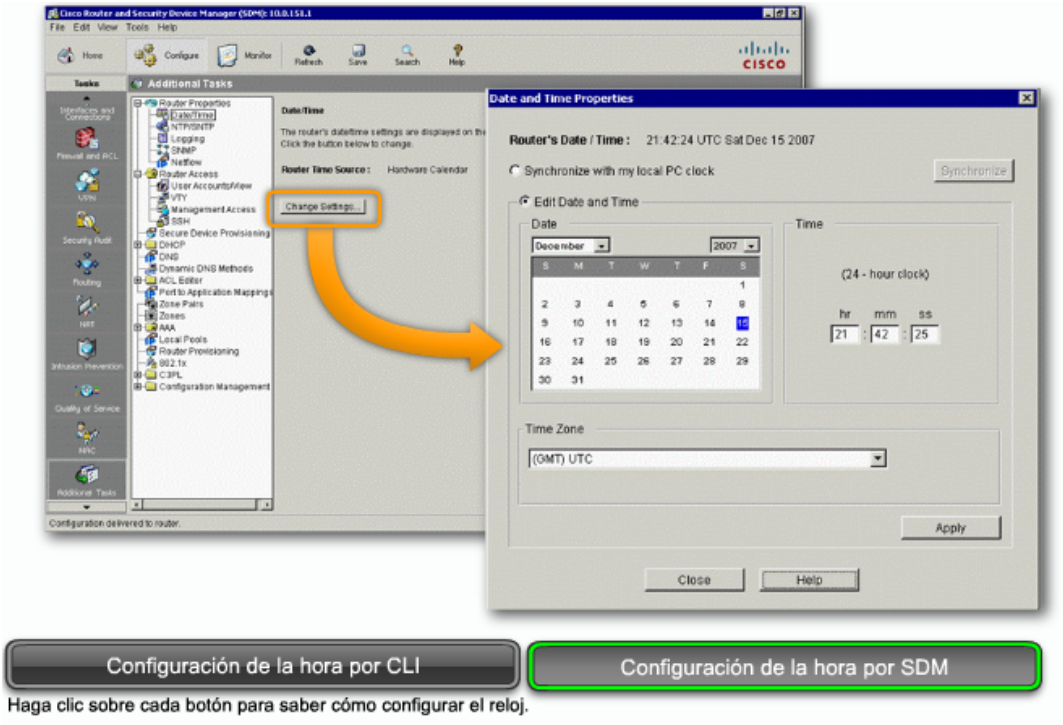
Editando la fecha y hora manualmente
Configurando el Protocolo de la Hora de la Red (Network Time Protocol - NTP)

Aunque el método manual funciona en el ambiente de una red pequeña, a medida que una red crece se vuelve difícil asegurarse de que todos los dispositivos de la infraestructura estén operando con la fecha sincronizada. Incluso en un ambiente de red pequeña, el método manual no es lo ideal. Si se reinicia un router, ¿De dónde sacará una fecha y marca de tiempo?

Una mejor solución es configurar NTP en la red. NTP permite a los routers de la red sincronizar sus configuraciones de tiempo con un servidor NTP. Un grupo de clientes NTP puede obtener información de fecha y hora de una sola fuente y tener configuraciones más consistentes. Cuando se implementa NTP en la red, puede configurarse para que se sincronice con un reloj privado o puede sincronizarse con un servidor NTP disponible públicamente en Internet.

NTP usa el puerto UDP 123 y está documentado en RFC 1305.





Al determinar si deberá usarse una sincronización con un reloj privado o un reloj público, es necesario poner los riesgos y los beneficios de ambos en una balanza.

Si se implementa un reloj privado, puede ser sincronizado al Coordinated Universal Time (UTC) vía satélite o radio. El administrador deberá asegurarse de que la fuente de tiempo sea válida y provenga de un sitio seguro; si no lo hiciera, puede introducir vulnerabilidades. Por ejemplo, un atacante puede lanzar un ataques de DoS enviando datos NTP falsos a través de Internet y hacia la red en un intento de cambiar los relojes en los dispositivos de red, posiblemente haciendo que los certificados digitales dejen de ser válidos. El atacante puede intentar confundir al administrador de red durante un ataque cambiando los valores de los relojes en los dispositivos de red. Esto dificultaría al administrador determinar el orden de los eventos syslog en múltiples dispositivos.

Extraer la hora de un reloj de Internet significa que se permitirán paquetes no seguros a través del firewall. Muchos servidores NTP en Internet no solicitan ninguna autenticación de sus pares; por lo tanto, el administrador de la red debe confiar en que el reloj mismo es confiable, válido y seguro.

Las comunicaciones (conocidas como asociaciones) entre máquinas que ejecutan NTP generalmente tienen una configuración estática. Se da a cada dispositivo la dirección IP de los masters NTP. Es posible obtener una fecha y hora precisa intercambiando mensajes NTP entre cada par de máquinas con una asociación. En una red configurada con NTP, se designan uno o más routers como master NTP (los encargados de mantener el reloj) usando el comando de configuración global ntp master.

Los clientes NTP contactan al master o escuchan mensajes del master para sincronizar sus relojes. Para contactar al master, use el comando ntp server dirección-servidor-ntp.

En un ambiente LAN, NTP puede ser configurado para usar mensajes de broadcast IP en lugar de usar el comando ntp broadcast client. Esta alternativa reduce la complejidad de la configuración ya que cada máquina puede ser configurada para enviar o recibir mensajes de broadcast. La precisión de la hora es marginalmente reducida porque el flujo de información tiene una sola vía.

```
Router(config)#
ntp master [stratum]
```

- Hace al sistema un servidor NTP autoritativo.
- El número de estrato es el número de saltos desde una fuente autoritativa como un reloj atómico.

```
Router(config)#
ntp server {ip-address | hostname} [version number] [key keyid]
[source interface] [prefer]
```

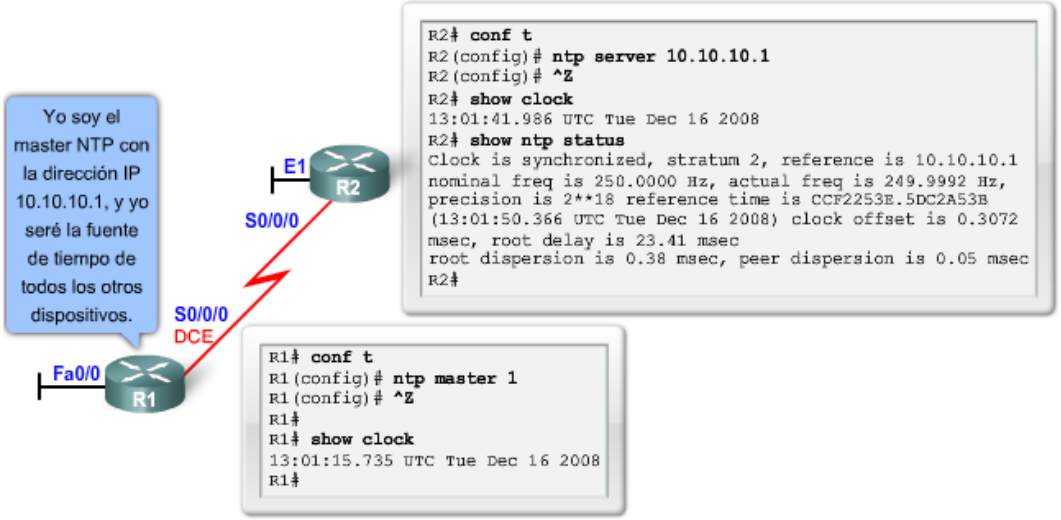
- Permite al reloj del software sincronizarse con un servidor NTP.

```
Router(config-if)#
ntp broadcast client
```

- Configura el dispositivo para recibir mensajes broadcast NTP en la interfaz.

Comandos NTP | Configuración NTP ejemplo

Haga clic sobre cada botón para ver el contenido asociado.



- R1 está configurado como master NTP.
- R2 está configurado como cliente NTP y ha sincronizado su reloj con R1.

Comandos NTP | Configuración NTP ejemplo

Haga clic sobre cada botón para ver el contenido asociado.

La hora que mantiene la máquina es un recurso crítico, por lo que las funciones de seguridad de NTP pueden ser usadas para evitar la configuración, accidental o maliciosa, de una hora incorrecta. Existen dos mecanismos de seguridad:

Esquema de restricciones basado en ACLs
Mecanismo de autenticación cifrado ofrecido por NTP versión 3 o posterior

NTP versión 3 (NTPv3) y posteriores soportan un mecanismo de autenticación criptográfico entre pares NTP. Este mecanismo de autenticación, en conjunto con las ACLs que especifican a qué dispositivos de red se les permite sincronizarse con otros dispositivos de red, puede ser usado para ayudar a mitigar tal ataque.

Para asegurar el tráfico NTP, se recomienda fuertemente la implementación de NTP versión 3 o posterior. Use los siguientes comandos en tanto el cliente NTP como el master NTP.

ntp authenticate

ntp authentication-key número-clave md5 valor-clave

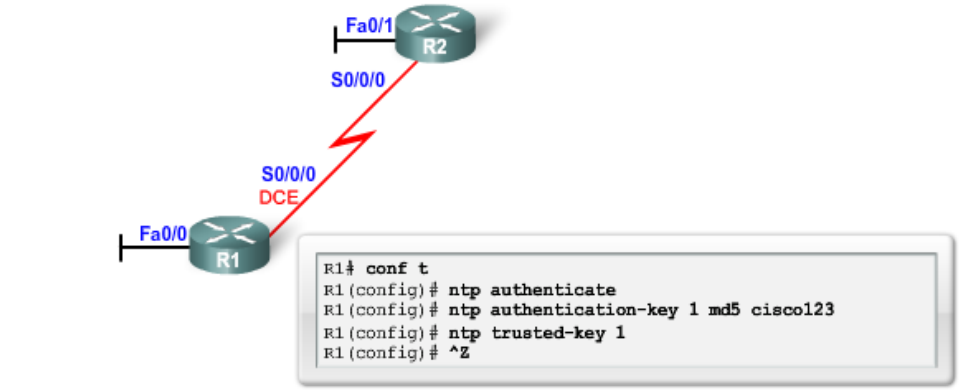
ntp trusted-key número-clave

La autenticación es para el beneficio del cliente para asegurar que esté obteniendo la hora de un servidor autenticado. Los clientes configurados sin autenticación también obtienen la hora del servidor. La diferencia está en que estos clientes no autentican al servidor como una fuente segura.

Use el comando show ntp associations detail para confirmar que el servidor sea una fuente autenticada.

Nota: el valor de la clave también puede configurarse como un argumento en el comando ntp server dirección-servidor-ntp.

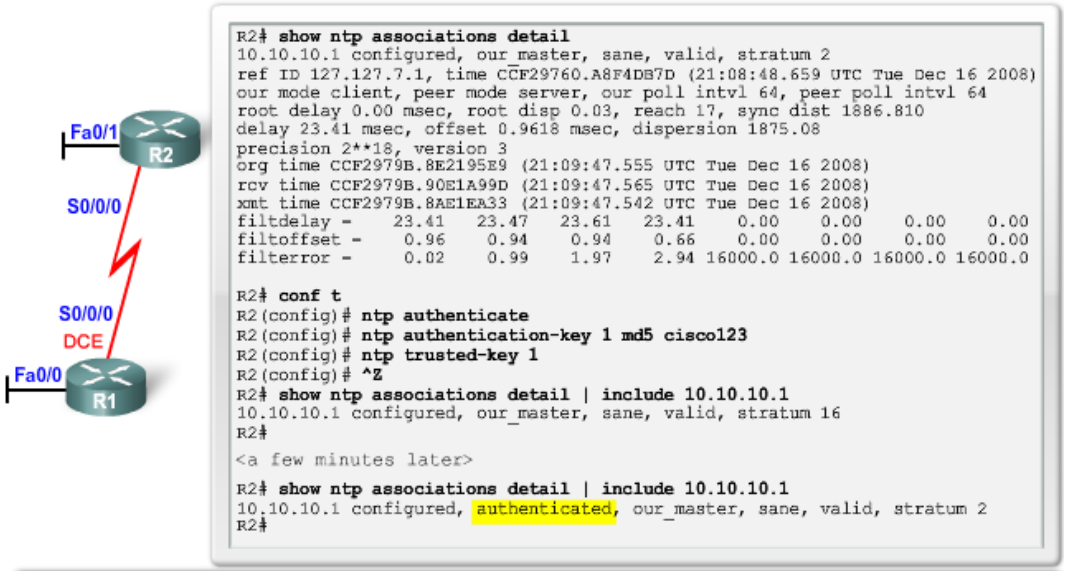




- R1 está configurado para autenticar clientes.
- Debe destacarse que la configuración permitirá a clientes no autenticados obtener la hora.

Comandos de seguridad NTP | Configuración NTP segura | Confirme la autenticación

Haga clic sobre cada botón para ver el contenido asociado.



- Note que la autenticación entre cliente y servidor puede tomar varios minutos.

Comandos de seguridad NTP | Configuración NTP segura | Confirme la autenticación

Haga clic sobre cada botón para ver el contenido asociado.

Los SDM de Cisco permiten al administrador de la red ver la información de servidor NTP configurada, agregar nueva información y editar o eliminar información existente.

Agregar un servidor NTP usando un SDM de Cisco toma siete pasos.

Paso 1. Vaya a Configure > Additional Tasks > Router Properties > NTP/SNTP. Aparecerá el panel de NTP, mostrando la información de todos los servidores NTP configurados.

Paso 2. Para agregar un nuevo servidor NTP, haga clic sobre Add. Aparecerá la ventana de Add NTP Server Details.

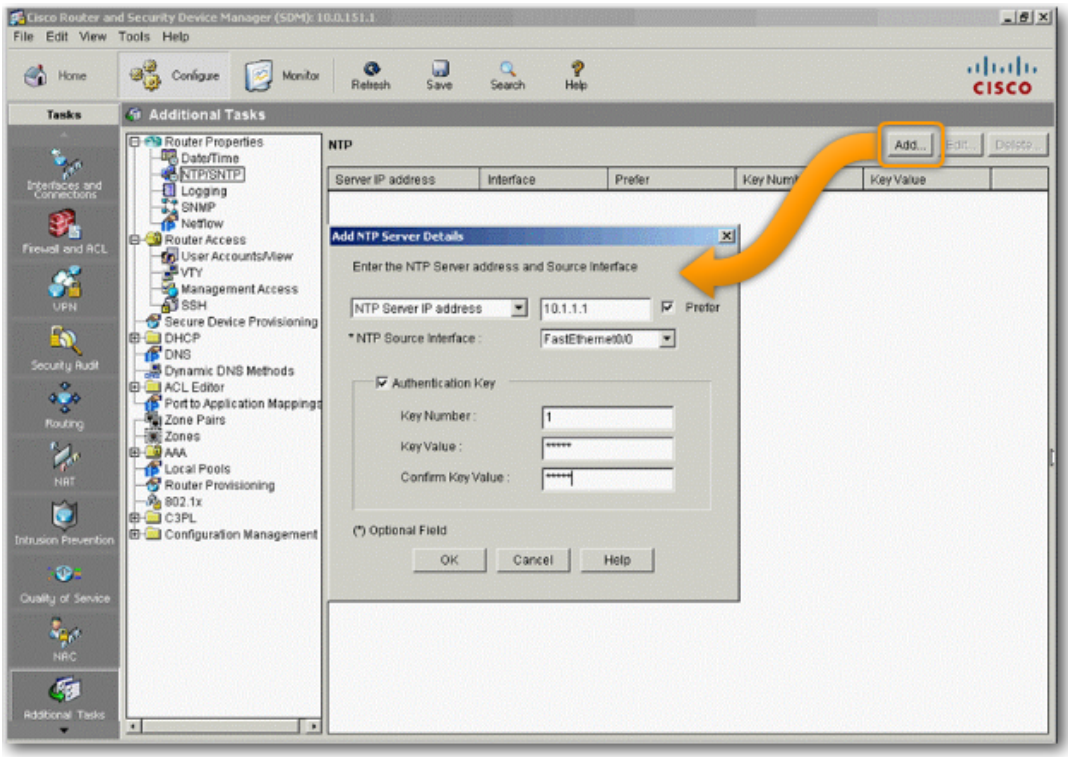
Paso 3. Agregue un servidor NTP por nombre si el router está configurado para usar un servidor DNS (Domain Name System) o por dirección IP si no. Para agregar un servidor NTP por dirección IP, ingrese la dirección IP en el campo contiguo a la opción NTP Server IP Address. Si la organización no tiene un servidor NTP, el administrador puede querer usar un servidor público, como uno de la lista de servidores disponible en http://support.ntp.org/bin/view/Servers/WebHome.

Paso 4. (Opcional) Desde la lista desplegable NTP Source Interface, elija la interfaz que usa el router para comunicarse con el servidor NTP. El campo de NTP Source Interface es opcional, y si se lo deja en blanco, los mensajes NTP serán enviados desde la interfaz más cercana al servidor NTP según la tabla de enrutamiento.

Paso 5. Seleccione Prefer si este servidor NTP ha sido designado como el servidor NTP preferido. Los servidores NTP preferidos son contactados antes que los no preferidos. Puede haber más de un servidor NTP preferido.

Paso 6. Si el servidor NTP usa autenticación, seleccione Authentication Key e ingrese el número de clave y su valor.

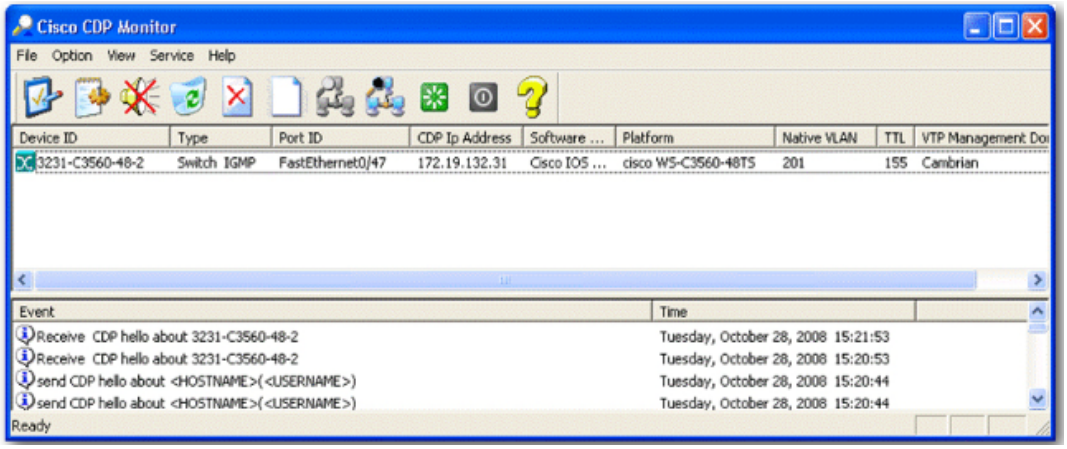
Paso 7. Haga clic sobre OK para terminar de agregar el servidor.



2.4.1 Auditorias de seguridad

Los routers de Cisco se despliegan inicialmente con muchos servicios habilitados por defecto. Esto es producto de la conveniencia y para simplificar el proceso de configuración requerido para tener el dispositivo plenamente operativo. Sin embargo, algunos de estos servicios pueden hacer que el dispositivo se vuelva vulnerable a ataques si no se habilita seguridad. Adicionalmente, los administradores pueden habilitar otros servicios en los routers Cisco que pueden exponer el dispositivo a riesgos significativos. Ambas situaciones deben tomarse en cuenta al asegurar la red.

Por ejemplo, el Protocolo de Descubrimiento de Cisco (Cisco Discovery Protocol - CDP) es un ejemplo de un servicio habilitado por defecto en los routers de Cisco. Se usa principalmente para obtener direcciones de protocolo de los dispositivos de Cisco circundantes y para descubrir las plataformas de esos dispositivos. Desafortunadamente, un atacante en la red puede usar CDP para descubrir dispositivos en la red local. Adicionalmente, los atacantes no necesitan tener dispositivos habilitados para CDP. Puede descargarse software como el CDP Monitor de Cisco, para obtener la información. El propósito de CDP es el de facilitar la tarea del administrador al descubrir y resolver problemas en otros dispositivos Cisco de la red. Sin embargo, por las implicancias de seguridad, el uso de CDP debe restringirse. Aunque es una herramienta extremadamente útil, no debería estar en toda la red. Los dispositivos de borde son un ejemplo de un dispositivo que no debe tener esta función hablitada.



Los atacantes seleccionan los servicios y protocolos que hacen más vulnerable a la red frente a acciones maliciosas.

Dependiendo de las necesidades de seguridad de la organización, muchos de estos servicios deberían estar deshabilitados o mínimamente restringidos en sus capacidades. Estas funciones van desde los protocolos propietarios de Cisco, como el Protocolo de Descubrimiento de Cisco (CDP), hasta protocolos globalmente disponibles como ICMP y otras herramientas de escaneo.

Algunas de las configuraciones por defecto en el software IOS de Cisco están ahí por razones históricas: cuando fueron elegidas eran necesarias pero probablemente serían diferentes si se eligieran nuevas opciones por defecto hoy en día. Otras configuraciones por defecto son aplicables para la mayoría de los sistemas pero pueden crear agujeros de

seguridad si es usan en dispositivos que forman parte de la defensa de perímetro de la red. Hay otras opciones por defecto que realmente son requeridas por los estándares, pero no son siempre deseables desde un punto de vista de seguridad.

Muchas prácticas ayudan a certificar que un dispositivo sea seguro.

Deshabilitar los servicios e interfaces innecesarios.
Deshabilitar y restringir los servicios de administración comúnmente configurados, como SNMP.
Deshabilitar servicios de sonda y escaneo, como ICMP.
Asegurar la seguridad del acceso terminal.
Deshabilitar el Protocolo de Resolución de Direcciones (Adress Resolution Protocol - ARP) gratuito y proxy.
Deshabilitar broadcasts dirigidos por IP.

Función	Defecto	Recomendación
Cisco Discovery Protocol (CDP)	Habilitado	Debe deshabilitarse globalmente o por interfaz si no se lo necesita.
Configuration autoloading	Deshabilitado	Debe permanecer deshabilitado cuando no está siendo usado por el router.
Servidor FTP	Deshabilitado	Debe deshabilitarse cuando no se necesita.
Servidor TFTP	Deshabilitado	Debe estar deshabilitado cuando no se necesita.
Servicio NTP (Network Time Protocol)	Deshabilitado	Debe permanecer deshabilitado cuando no se necesita.
Servicio de Packet assembler/disassembler (PAD)	Habilitado	Debe ser explícitamente deshabilitado cuando no se lo usa.
Servicios menores de TCP y User Datagram Protocol (UDP)	Habilitado en versiones 11.3 y posteriores	Deshabilite este servicio explícitamente.
Servicio MOP (Maintenance Operation Protocol)	Habilitado en la mayoría de las interfaces Ethernet	Debe ser explícitamente deshabilitado cuando no se usa.
Simple Network Management Protocol (SNMP)	Habilitado	Deshabilite este servicio cuando no se necesita.
Configuración y monitoreo HTTP o HTTPS	Setting is Cisco device dependent.	Deshabilite el servicio si no se necesita. Si este servicio se requiere, restrinja el acceso al servicio HTTP o HTTPS del router usando listas de control de acceso (ACLs).
Domain Name System (DNS)	Habilitado	Deshabilítelo cuando no se lo necesite. Si se necesita el servicio DNS lookup, asegúrese de configurar la dirección del servidor DNS explícitamente.
redirecciones ICMP (Internet Control Message Protocol)	Habilitado	Deshabilítelo cuando no se lo necesite.
Ruteo de origen IP	Habilitado	Deshabilite este servicio cuando no se necesite.
Servicio Finger	Habilitado	Deshabilite este servicio cuando no se necesite.
Notificación ICMP inalcanzable	Habilitado	Deshabilítelo en interfaces que se comunican con redes no confiables.
Respuesta a solicitud de máscara ICMP	Deshabilitado	Deshabilítelo en las interfaces que se comunican con redes no confiables.
Servicio de identificación IP	Habilitado	El servicio debe ser explícitamente deshabilitado.
TCP keepalives	Deshabilitado	Debe habilitarse globalmete para administrar las conexiones TCP y prevenir ciertos ataques de Denegación de Servicio (DoS). El servicio está habilitado en las versiones del software IOS de Cisco anteriores a la 12.0 y está deshabilitado en la 12.0 y posteriores. Deshabilite este servicio cuando no se necesite.
ARP gratuito (GARP)	Habilitado	Deshabilite los ARP gratuitos en todas las interfaces del router si el servicio no se necesita.
ARP proxy	Habilitado	Deshabilite este servicio en todas las interfaces excepto si el router está siendo utilizado como bridge en una LAN.

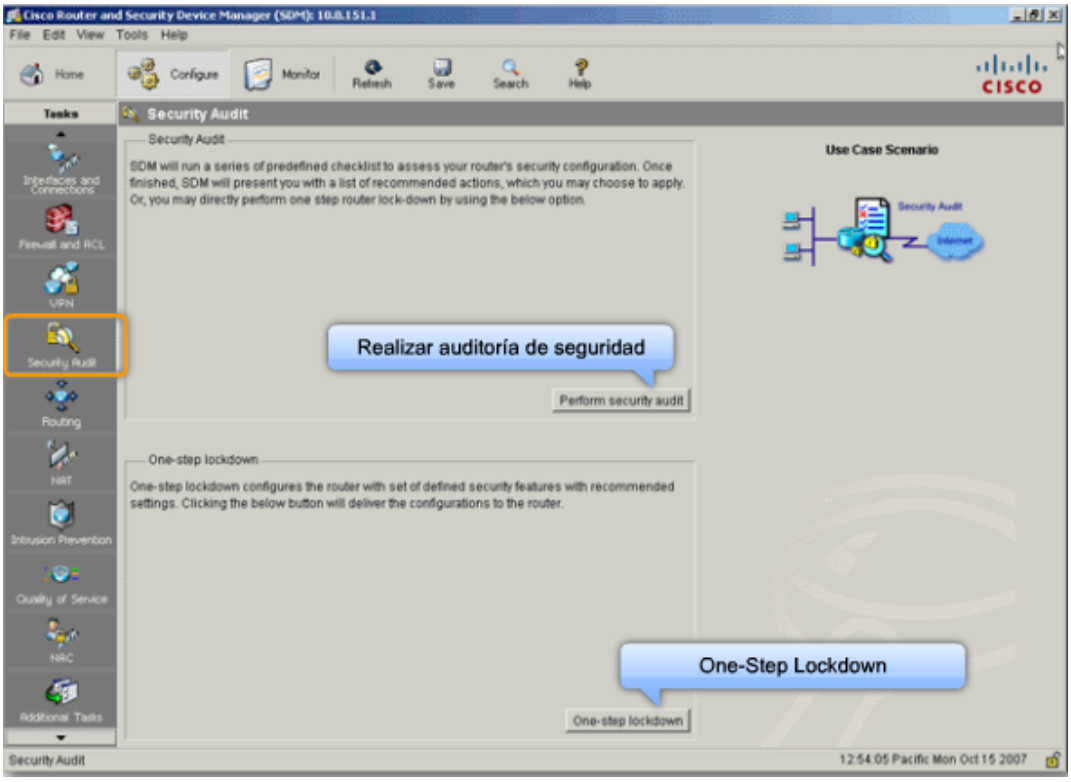
Para asegurar los dispositivos de red, los administradores deben determinar primero las vulnerabilidades existentes en la configuración actual. La mejor manera de lograrlo es usando una herramienta de auditoría de seguridad. La herramienta de auditoría de seguridad efectúa revisiones en el nivel de seguridad de las configuraciones comparándolas con configuraciones recomendadas y recolectando discrepancias. Luego de que se identifican las vulnerabilidades, los administradores de red deben modificar la configuración para reducir o eliminar las vulnerabilidades, asegurando el dispositivo y la red.

Tres herramientas de auditoría de seguridad son:

El asistente de Auditoría de Seguridad - una función de auditoría de seguridad proporcionada a través del SDM de Cisco. El asistente de Auditoría de Seguridad proporciona una lista de vulnerabilidades y luego permite al administrador elegir cuáles cambios en la configuración potencialmente relacionados con la seguridad implementarán en el router.

AutoSecure de Cisco - una función de auditoría de seguridad disponible a través de la CLI del IOS de CIsco. El comando autosecure inicia una auditoría de seguridad y luego permite cambios de configuración. Basándose en el modo seleccionado, los cambios de configuración pueden ser automáticos o requerir participación del administrador de la red.
One-Step Lockdown - una función de auditoría de seguridad proporcionada por el SDM de Cisco. La función One-Step Lockdown proporciona una lista de vulnerabilidades y luego efectúa los cambios de configuración recomendados para la seguridad automáticamente.

Tanto el asistente de Auditoría de Seguridad como One-Step Lockdown están basadas en la función Autosecure del IOS de Cisco.



Asistente de Auditoría de Seguridad

El asistente de Auditoría de Seguridad examina la configuración del router para determinar si existen problemas de seguridad potenciales en la configuración y luego muestra una pantalla que permite al administrador determinar cuáles de estos problemas de seguridad arreglar. En esta instancia, el asistente de Auditoría de Seguridad efectúa los cambios necesarios en la configuración del router para arreglar los problemas.

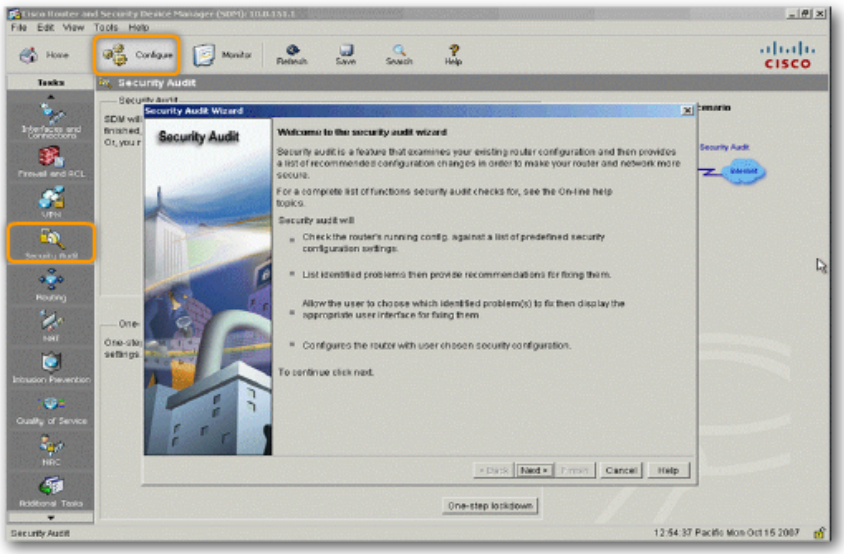
El asistente de Auditoría de Seguridad compara la configuración del router contra las configuraciones recomendadas y hace lo siguiente:

Apaga todos los servidores innecesarios.
Deshabilita los servicios innecesarios.
Aplica el firewall a las interfaces externas.
Deshabilita o hace hardening en SNMP.
Apaga las interfaces no utilizadas.
Verifica cuán fuertes son las contraseñas.
Instaura el uso de ACLs.

Cuando se inicia una auditoría de seguridad, el asistente de Auditoría de Seguridad debe saber qué interfaces del router conectar a la red interna y cuáles conectar a la parte externa de la red. El asistente de Auditoría de Seguridad luego examina la configuración del router para determinar si existen posibles problemas de seguridad. Luego muestra una pantalla que despliega todas las opciones de configuración examinadas y si la configuración actual del router pasa esos exámenes.

Cuando se completa la auditoría, el asistente de Auditoría de Seguridad identifica posibles vulnerabilidades en la configuración y proporciona una manera de corregir esos problemas. También le da al administrador la posibilidad de arreglar los problemas automáticamente, en cuyo caso determina los comandos de configuración necesarios. Se proporciona una descripción de los problemas específicos y una lista de los comandos del IOS de Cisco usados para corregir los problemas.

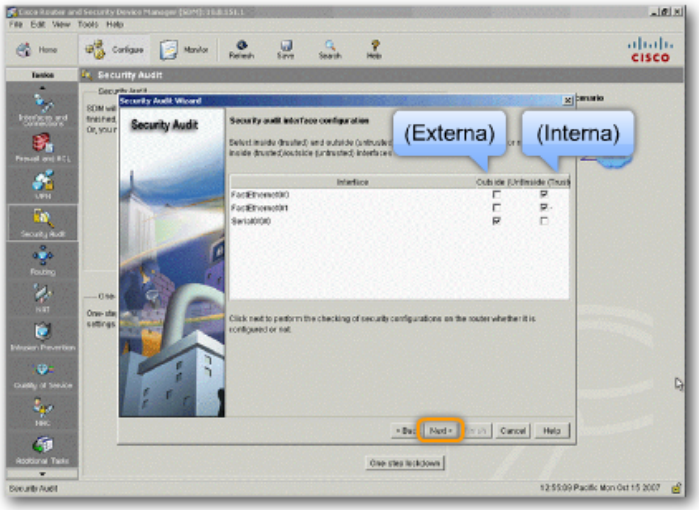
Antes de que se efectúe cualquier cambio en la configuración, una página de resumen muestra una lista de todos los cambios de configuración que el asistente de Auditoría de Seguridad está por hacer. El administrador debe hacer clic sobre Finish para enviar esas configuraciones al router.



Desde el SDM de Cisco SDM, vaya a **Configure > Security Audit**.

Pantalla de bienvenida | Identificación de interfaces | Vulnerabilidades identificadas | Arreglar problemas | Resumen

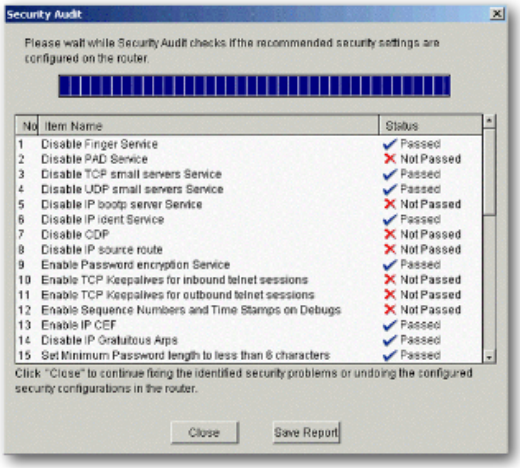
Haga clic sobre cada botón para ver el contenido asociado.



Para cada interfaz en la lista, haga clic sobre la caja Inside (Interna) o la caja Outside (Externa) para indicar adónde conecta la interfaz. Haga clic sobre **Next**.

Pantalla de bienvenida | Identificación de interfaces | Vulnerabilidades identificadas | Arreglar problemas | Resumen

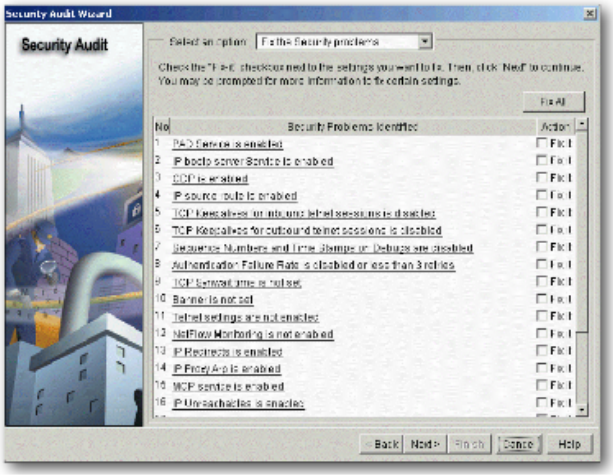
Haga clic sobre cada botón para ver el contenido asociado.



Aparece una ventana que muestra el progreso de la auditoría de seguridad, con una lista de todas las opciones de configuración examinadas y si la configuración actual pasó la prueba. Cuando finaliza la auditoría de seguridad, el administrador puede guardar el informe haciendo clic **Save Report**. Haga clic sobre **Close** para continuar arreglando los problemas de seguridad identificados o para deshacer las configuraciones de seguridad configuradas en el router.

Pantalla de bienvenida | Identificación de interfaces | Vulnerabilidades identificadas | Arreglar problemas | Resumen

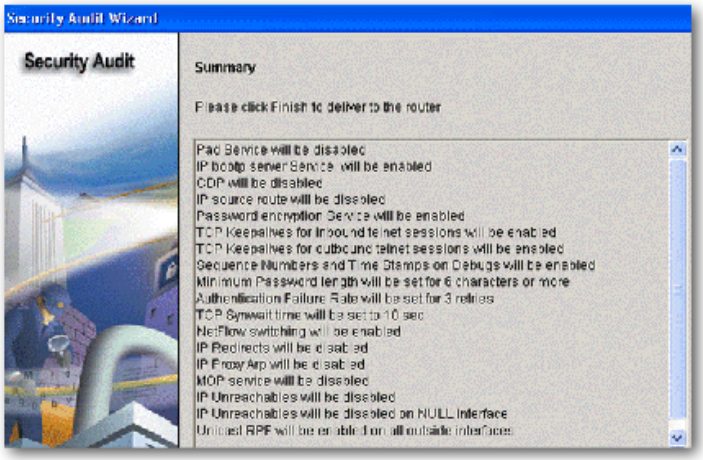
Haga clic sobre cada botón para ver el contenido asociado.



A continuación, la pantalla Security Audit Report Card muestra una lista de posibles problemas de seguridad con la opción de arreglar el problema. Haga clic sobre las cajas **Fix It** de los problemas que desea que el SDM de Cisco arregle. Para una descripción del problema y una lista de los comandos del IOS de Cisco que se agregarán a la configuración, haga clic en el enlace de la descripción problema.

Pantalla de bienvenida | Identificación de interfaces | Vulnerabilidades identificadas | Arreglar problemas | Resumen

Haga clic sobre cada botón para ver el contenido asociado.



Dependiendo de los problemas arreglados, el asistente de Auditoría de Seguridad puede mostrar una o más pantallas que requieran la participación del usuario para proceder con el arreglo. Una vez que se ha completado, la página de resumen del asistente muestra una lista de los cambios de configuración que hará la Auditoría de Seguridad. Haga clic sobre **Finish** para enviar los cambios al router.

Pantalla de bienvenida | Identificación de interfaces | Vulnerabilidades identificadas | Arreglar problemas | Resumen

Haga clic sobre cada botón para ver el contenido asociado.

2.4.2 Seguridad del router con AutoSecure

AutoSecure de Cisco

Lanzado con la versión 12.3 del IOS de Cisco, AutoSecure de Cisco es una función que se inicia desde la CLI y ejecuta un script. AutoSecure primero efectúa recomendaciones para arreglar vulnerabilidades de seguridad y luego modifica la configuración de seguridad del router.

AutoSecure puede asegurar las funciones del plano de administración y las funciones y servicios del plano de reenvíos de un router.

El plano de administración es la ruta lógica de todo el tráfico relacionado con la administración de una plataforma de enrutamiento. Se usa para controlar todas las otras funciones de enrutamiento y para administrar un dispositivo a través de su conexión con la red. Hay muchas funciones y servicios del plano de administración:

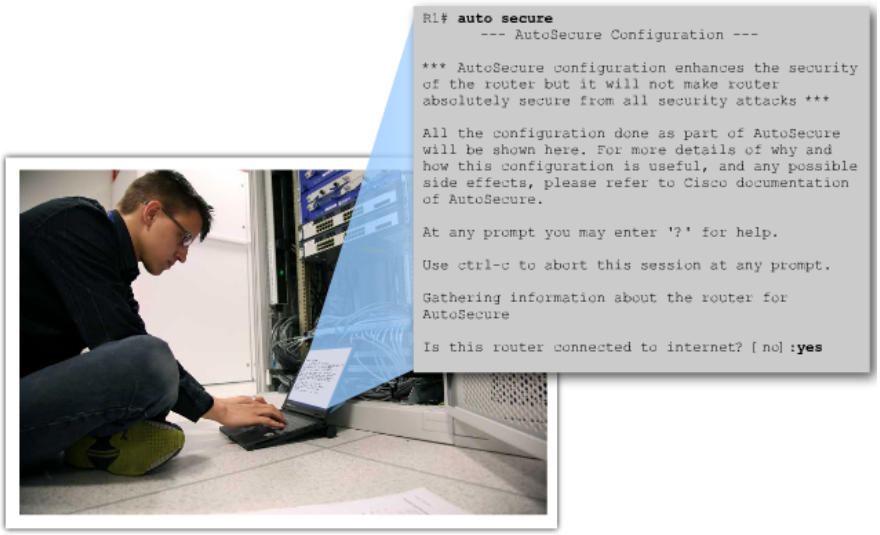
Pequeños servidores de BOOTP, CDP, FTP, TFTP, PAD, UDP y TCP, MOP, ICMP (redirecciones, respuestas a solicitudes de máscaras de red), enrutamiento de origen IP, Finger, cifrado de contraseñas, keepalives de TCP, ARP gratuito, ARP proxy y broadcast dirigidos seguros
Notificación legal a través de un banner
Contraseñas y funciones de autenticación seguras
NTP seguro
Acceso SSH seguro
Servicios de interceptación de TCP

El plano de reenvíos es responsable del reenvío de paquetes (o packet switching), que es el acto de recibir paquetes en las interfaces del router y enviarlos fuera de él a través de otras interfaces.

Hay tres servicios y funciones del plano de reenvíos:

Habilita Cisco Express Forwarding (CEF)
Habilita filtrado de tráfico con ACLs
Implementa inspección del firewall del IOS de Cisco para protocolos comunes

Generalmente se usa AutoSecure para proporcionar una política de seguridad básica en un router nuevo. Las funciones pueden ser alteradas posteriormente para soportar la política de seguridad de la organización.



Use el comando auto secure para habilitar la configuración de la función AutoSecure de Cisco. Esta configuración puede ser interactiva o no interactiva.

auto secure [no-interact]

En el modo interactivo, el router presenta opciones para habilitar o deshabilitar servicios y otras funciones de seguridad. Este es el modo por defecto, pero también puede ser configurado mediante el comando auto secure full.

El modo no interactivo es parecido a la función de auditoría de seguridad One-Step Lockdown del SDM, ya que ejecuta el comando AutoSecure de Cisco automáticamente con las configuraciones por defecto recomendadas por Cisco. Este modo se habilita con el modo de EXEC privilegiado auto secure no-interact.

El comando auto secure también puede ingresarse con palabras clave para configurar componentes específicos, como los planos de administración y de reenvíos.

router#

```
auto secure [no-interact | full] [forwarding | management]
[ntp | login | ssh | firewall | tcp-intercept]
```

```
R1# auto secure ?
  firewall       AutoSecure Firewall
  forwarding     Secure Forwarding Plane
  full           Interactive full session of AutoSecure
  login          AutoSecure Login
  management     Secure Management Plane
  no-interact    Non-interactive session of AutoSecure
  ntp            AutoSecure NTP
  ssh            AutoSecure SSH
  tcp-intercept  AutoSecure TCP Intercept
  <cr>

R1#
```

AutoSecure de Cisco | Parámetros

Haga clic sobre cada botón para ver el contenido asociado.

router#

```
auto secure [no-interact | full] [forwarding | management]
[ntp | login | ssh | firewall | tcp-intercept]
```

Parámetro	Descripción
no-interact	(Opcional) No se le mostrará una configuración interactiva al usuario. No se configurarán parámetros de diálogo interactivo, incluyendo nombres de usuario o contraseñas.
full	(Opcional) Se mostrarán preguntas interactivas. Es la configuración por defecto.
forwarding	(Opcional) Solo se asegurará el plano de reenvío.
management	(Opcional) Solo se asegurará el plano de administración.
ntp	(Opcional)Especifica la configuración de la función Network Time Protocol (NTP) en la interfaz de línea de comandos (CLI) de AutoSecure.
login	(Opcional) Especifica la configuración de la función Login en la CLI de AutoSecure.
ssh	(Opcional) Especifica la configuración de la función SSH en la CLI de AutoSecure.
firewall	(Opcional) Especifica la configuración de la función Firewall en la CLI de AutoSecure.
tcp-intercept	(Opcional) Especifica la configuración de la función TCP-Intercept en la CLI de AutoSecure.

AutoSecure de Cisco | Parámetros

Haga clic sobre cada botón para ver el contenido asociado.

Cuando se inicia el comando auto secure, se muestra un asistente que lleva al administrador a través de toda la configuración del dispositivo. Se requiere participación del usuario. Cuando se completa el asistente, se muestra la configuración actual con todos los cambios hechos a la configuración.

```
R1# auto secure
--- AutoSecure Configuration ---

*** AutoSecure configuration enhances the security of the router, but it will
not make it absolutely resistant to all security attacks ***

AutoSecure will modify the configuration of your device. All configuration
changes will be shown. For a detailed explanation of how the configuration
changes enhance security and any possible side effects, please refer to
Cisco.com for Autosecure documentation.
At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.

Gathering information about the router for AutoSecure

<continued>
```

- **auto secure** sin palabras clave va por defecto al modo interactivo.

Bienvenido | Identificar borde | Plano de administración | Banner

Contraseña | Interfaces seguras | Plano de reenvíos

Haga clic sobre cada botón para ver el contenido asociado.

```
Gathering information about the router for AutoSecure

Is this router connected to internet? [no]: yes
Enter the number of interfaces facing the internet [1]:

Interface              IP-Address      OK? Method Status                Protocol
FastEthernet0/0        192.168.10.1    YES manual up                    up
FastEthernet0/1        192.168.11.1    YES manual up                    up
FastEthernet0/1/0      unassigned      YES unset  up                    down
FastEthernet0/1/1      unassigned      YES unset  up                    down
FastEthernet0/1/2      unassigned      YES unset  up                    down
FastEthernet0/1/3      nassigned       YES unset  up                    down
Serial0/0/0            192.168.2.101   YES manual up                    up
Serial0/0/1            unassigned      YES manual administratively down down
Vlan1                  unassigned      YES manual up                    down
Enter the interface name that is facing the internet: Serial 0/0/0
Invalid interface name
```

- La interfaz externa se identifica para establecer el borde de la red.
- Los nombres de la interfaz deben ingresarse exactamente como se muestran en la salida del prompt.

Bienvenido | Identificar borde | Plano de administración | Banner

Contraseña | Interfaces seguras | Plano de reenvíos

Haga clic sobre cada botón para ver el contenido asociado.

```
Securing Management plane services...

Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol

Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
Disabling gratuitous arp

<continued>
```

- AutoSecure automáticamente deshabilita servicios innecesarios.

Bienvenido | Identificar borde | Plano de administración | Banner

Contraseña | Interfaces seguras | Plano de reenvíos

Haga clic sobre cada botón para ver el contenido asociado.

```
Here is a sample Security Banner to be shown at every access to device. Modify
it to suit your enterprise requirements.

Authorized Access only
  This system is the property of So-&-So-Enterprise.
  UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.
  You must have explicit permission to access this
  device. All activities performed on this device
  are logged. Any violations of access policy will result
  in disciplinary action.

Enter the security banner {Put the banner between k and k, where k is any
character}:
#
 *********     AUTHORIZED ACCESS ONLY ***********
    UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.
  You must have explicit permission to access this
  device. Any violations of access policy will result
  in disciplinary action.
#
<continued>
```

- AutoSecure pide un banner y muestra un ejemplo.

Bienvenido | Identificar borde | Plano de administración | Banner

Contraseña | Interfaces seguras | Plano de reenvíos

Haga clic sobre cada botón para ver el contenido asociado.

```
Enable secret is either not configured or is the same as enable password
Enter the new enable secret: cisco123
Confirm the enable secret : cisco123
Enter the new enable password: cisco1
% Password too short - must be at least 6 characters. Password configuration
failed
Enter the new enable password: cisco321
Confirm the enable password: cisco321
Configuring AAA local authentication
Configuring Console, Aux and VTY lines for local authentication, exec-timeout,
and transport
Securing device against Login Attacks
Configure the following parameters

Blocking Period when Login Attack detected: 120
Maximum Login failures with the device: 2
Maximum time period for crossing the failed login attempts: 60

Configure SSH server? [yes]: y

<continued>
```

- Se recolectan los parámetros de la seguridad de contraseñas y del comando **login block-for**.
- Se configura SSH.

Bienvenido | Identificar borde | Plano de administración | Banner

Contraseña | Interfaces seguras | Plano de reenvíos

Haga clic sobre cada botón para ver el contenido asociado.

```
Configuring interface specific AutoSecure services
Disabling the following ip services on all interfaces:

 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
Disabling mop on Ethernet interfaces

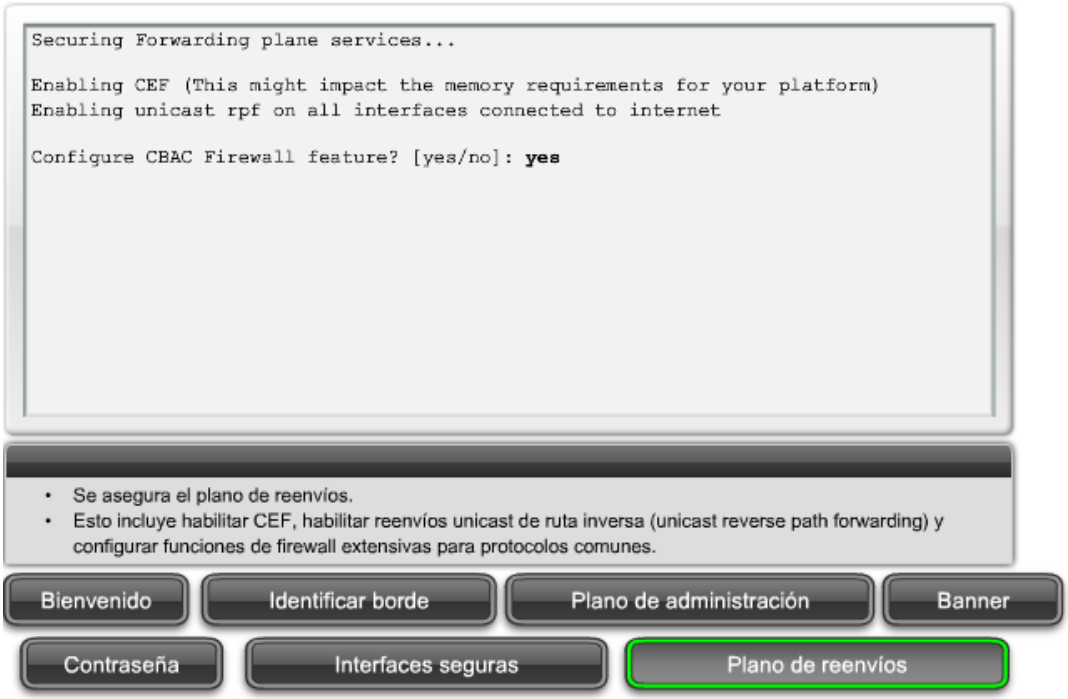
<continued>
```

- Se aplican comandos comunes de seguridad a todas las interfaces.
- Algunas funciones son específicas de la interfaz (ej. FastEthernet versus Serial).

Bienvenido | Identificar borde | Plano de administración | Banner

Contraseña | Interfaces seguras | Plano de reenvíos

Haga clic sobre cada botón para ver el contenido asociado.



2.4.3 Locking down a router using SDM

One-Step Lockdown de Cisco

One-step lockdown examina la configuración del router buscando problemas de seguridad potenciales y efectúa automáticamente los cambios necesarios a la configuración para corregirlos.

One-Step Lockdown de Cisco deshabilita:

Servicio de Finger
Servicio de PAD
Servicio de pequeños servidores TCP
Servicio de pequeños servidores UDP
Servicio de servidores BOOTP IP
Servicio de identificación de IPs
Cisco Discovery Protocol
Ruta de origen IP
GARPs IP
SNMP
Redirecciones IP
ARP proxy IP
Broadcast dirigido por IP
Servicio MOP
IPs inalcanzables
Respuesta de solicitud de máscara IP
IPs inalcanzables en interfaz nula

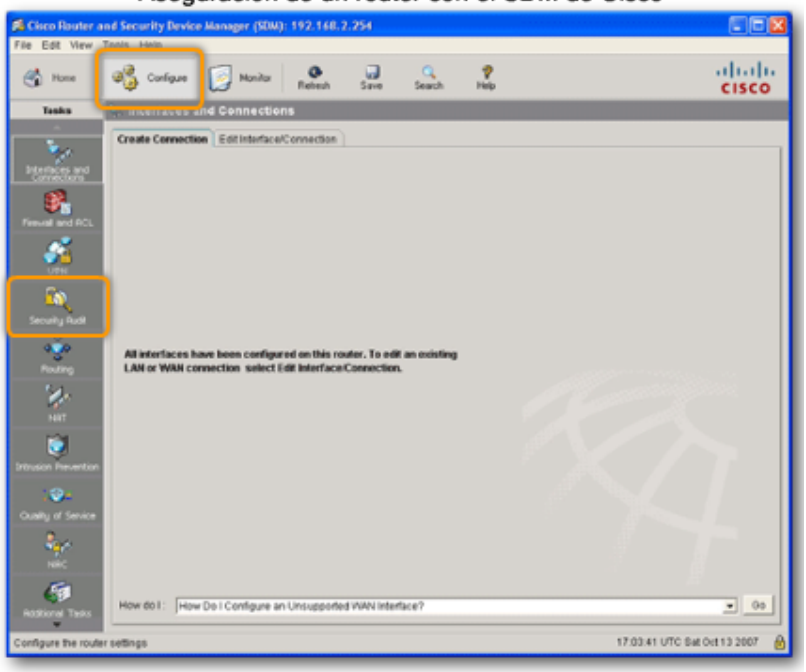
One-Step Lockdown de Cisco habilita:

Servicio de cifrado de contraseñas
Keepalives TCP para sesiones Telnet entrantes y salientes
Números de secuencia y marcas de tiempo en los debugs
Conmutación de IP Cisco Express Forwarding Enable NetFlow
Reverse Path Forwarding (RPF) Unicast en interfaces externas
Firewall en todas las interfaces externas
SSH para acceso al router
AAA

One-Step Lockdown de Cisco configura:

Longitud de contraseña mínima en seis caracteres
Tasa de fallos de autenticación a menos de tres intentos
Tiempo synwait TCP
Banner de notificaciones
Parámetros de inicio de sesión
Contraseña enable secret password
Scheduler interval
Scheduler allocate
Usuarios
Telnet
Clase de acceso al servicio de servidor HTTP
Clase de acceso en líneas vty

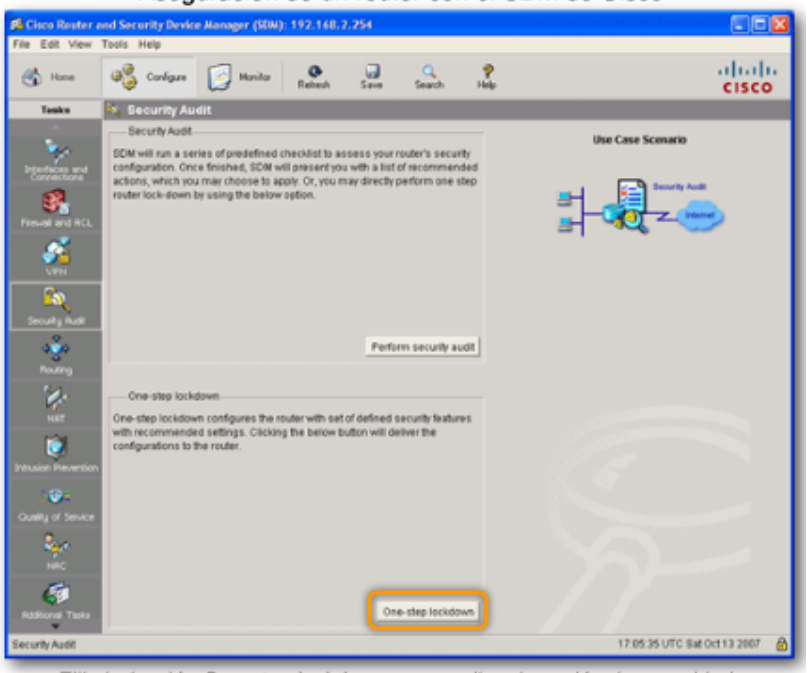
Aseguración de un router con el SDM de Cisco



Pasos: 1 2 3 4 5

Haga clic en los pasos para ver cómo completar el proceso One-Step Lockdown de Cisco.

Aseguración de un router con el SDM de Cisco

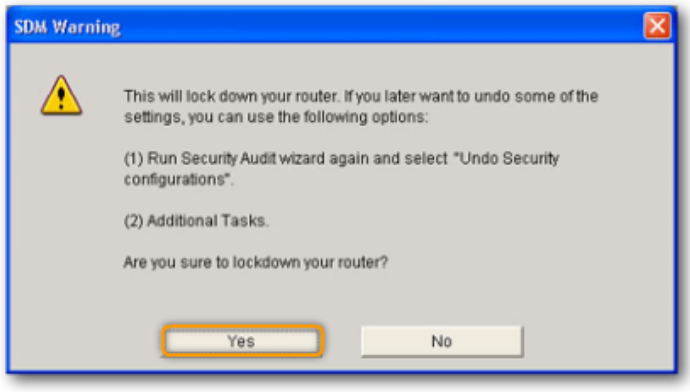


Elija la función **One-step lockdown** para realizar la acción de seguridad.

Pasos: 1 2 3 4 5

Haga clic en los pasos para ver cómo completar el proceso One-Step Lockdown de Cisco.

Aseguración de un router con el SDM de Cisco

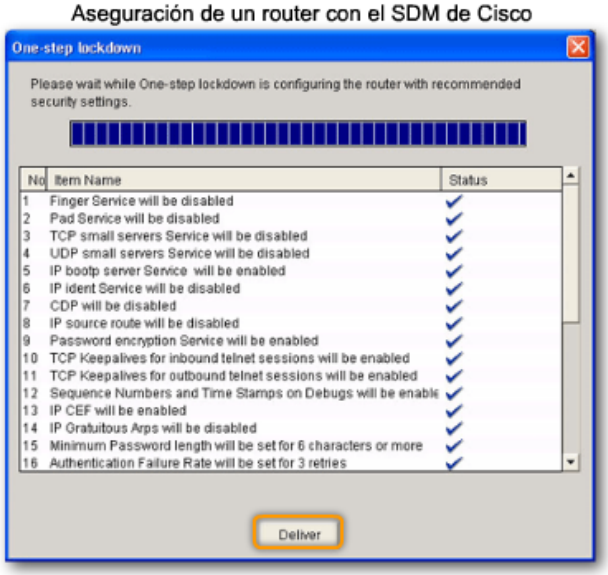


Asegúrese de hacer clic sobre **Yes** para continuar el proceso de auditoría de seguridad. Hacer clic en **No** cancelará la operación.

Pasos: 1 2 3 4 5

Haga clic en los pasos para ver cómo completar el proceso One-Step Lockdown de Cisco.

Aseguración de un router con el SDM de Cisco

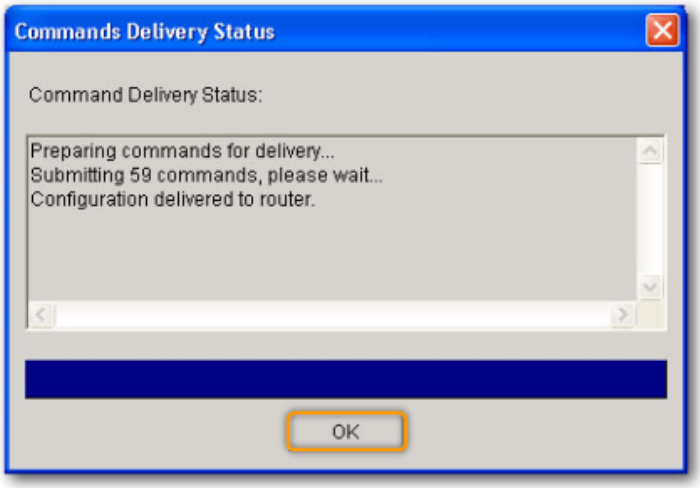


Una vez que se complete el proceso, SDM muestra una lista de configuraciones recomendadas. Haga clic sobre **Deliver** para enviar los cambios de configuración al router.

Pasos: 1 2 3 4 5

Haga clic en los pasos para ver cómo completar el proceso One-Step Lockdown de Cisco.

Aseguración de un router con el SDM de Cisco



La ventana Commands Delivery Status muestra el estado de envío de los comandos al router. Luego de que la configuración ha terminado de enviarse al router, haga clic sobre **OK**.

Pasos: 1 2 3 4 5

Haga clic en los pasos para ver cómo completar el proceso One-Step Lockdown de Cisco.

Decidir cuál función de lockdown automatizado usar, si AutoSecure o one-step lockdown de Auditoría de Seguridad SDM, es básicamente una cuestión de preferencias. Hay diferencias en cómo cada uno implementa las buenas prácticas de seguridad.

El SDM de Cisco no implementa todas las funciones que implementa AutoSecure de Cisco. A partir de la versión 2.4 del SDM de Cisco, las siguientes funciones de AutoSecure de Cisco ya no forman parte de one-step lockdown de SDM de Cisco:

Habilitar NTP - Basándose en el input, el AutoSecure de Cisco deshabilita NTP si no está siendo usado. Si no es así, NTP se configura con autenticación MD5. El SDM de Cisco no soporta la deshabilitación de NTP.
Configurar de AAA - Si el servicio AAA no está configurado, el AutoSecure de Cisco configura AAA local y pide la configuración de una base de datos de nombre de usuario y contraseña local al router. El SDM de Cisco no soporta configuración AAA.

Configurar de valores de Descarte de Paquetes Selectivo (Selective Packet Discard - SPD) - El SDM de Cisco no establece valores SPD.
Habilitar de interceptaciones TCP - El SDM de Cisco no habilita interceptaciones TCP.
Configurar de ACLs antifalsificación en las interfaces externas - AutoSecure de Cisco crea tres listas de acceso nombradas para prevenir las direcciones de origen de antifalsificación. El SDM de Cisco no configura estas ACLs.

Las siguientes funciones AutoSecure de Cisco son implementadas de manera diferente en el SDM de Cisco:

Habilitar SSH para acceso al router - El SDM de Cisco habilita y configura SSH en las imágenes IOS de Cisco que pueden tener el grupo de funciones IPSec; sin embargo, a diferencia de AutoSecure de Cisco, el SDM de Cisco no habilita Secure Copy Protocol (SCP) o deshabilita otros servicios de transferencia de archivos o de acceso, como FTP.

Deshabilitar SNMP - El SDM de Cisco deshabilita SNMP; sin embargo, a diferencia de AutoSecure de Cisco, el SDM de Cisco no provee una opción para configurar SNMPv3. La opción de SNMPv3 no está disponible en todos los routers.

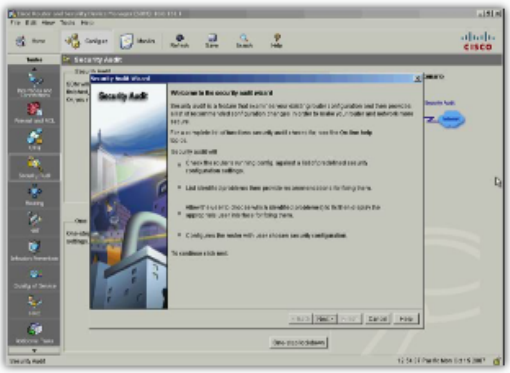
Sin importar cuál función automática elija, ésta debe ser usada como base y luego alterada para satisfacer las necesidades de la organización.

AutoSecure versus One-Step Lockdown de Auditoría de Seguridad de Cisco

```
R1# auto secure
--- AutoSecure Configuration ---

*** AutoSecure configuration enhances
the security of the router, but it
will not make it absolutely resistant
to all security attacks ***

AutoSecure will modify the
configuration of your device. All
configuration changes will be shown.
For a detailed explanation of how the
configuration changes enhance security
and any possible side effects, please
refer to Cisco.com for Autosecure
documentation.
```



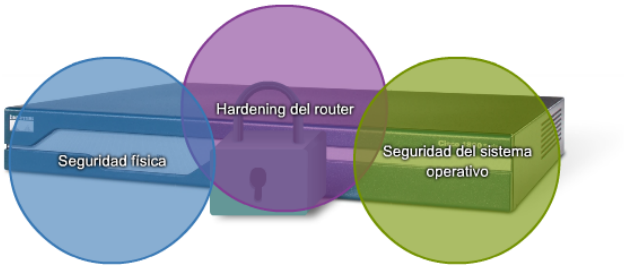
Además, AutoSecure de Cisco:

- Deshabilita NTP
- Configura AAA
- Establece valores SPD
- Habilita interceptaciones TCP
- Configura ACLs antifalsificación en las interfaces que se comunican con el exterior

SDM se diferencia en que:

- Deshabilita SNMP pero no configura SNMPv3 (varía con el router).
- Habilita y configura SSH con las imágenes del IOS de Cisco que lo soportan.
- No habilita Secure Copy Protocol (SCP); habilita FTP sin seguridad.

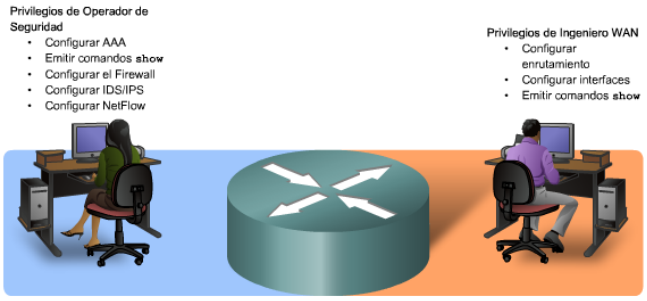
2.5.1 Resumen del capitulo



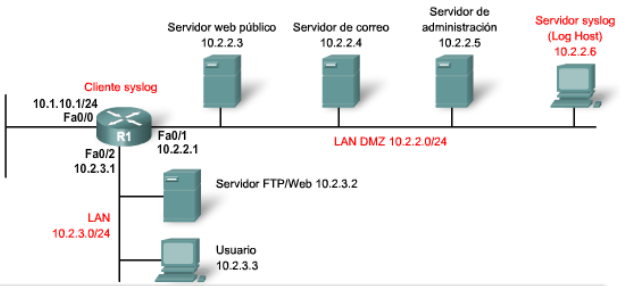
- Es crucial asegurar el perímetro de la red.
- Debe implementarse la aseguración del acceso administrativo en los dispositivos de la infraestructura.
- Implemente seguridad de inicio de sesión virtual avanzada para el acceso remoto a los dispositivos de la infraestructura.
- Use SSH en lugar de Telnet si es posible.



- Proporciona acceso a los dispositivos de infraestructura en base al nivel de privilegios.
- Implementa una CLI basada en roles para proporcionar acceso administrativo jerárquico.





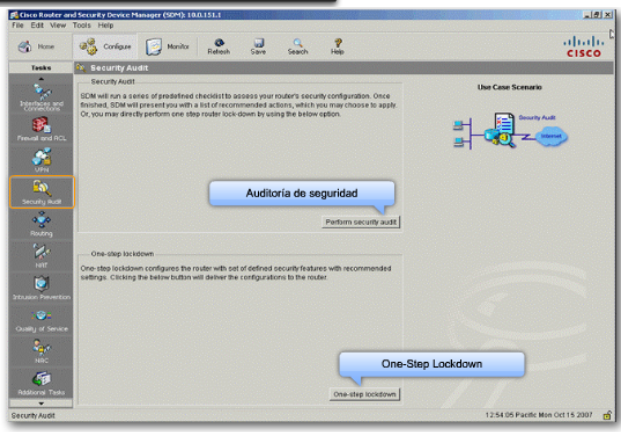



```
R1(config)# logging host 10.2.2.6
R1(config)# logging trap informational
R1(config)# logging source-interface loopback 0
R1(config)# logging on
```

- Asegure las imágenes del IOS de Cisco y los archivos de configuración usando la función de configuración resistente del IOS de Cisco.
- Identifique los factores para transmitir de manera segura datos relacionados con la administración de redes y los reportes de actividad del dispositivo.
- Implemente registros syslog logging para los dispositivos críticos a la infraestructura.
- Implemente reportes de administración SNMP.
- Configure una fuente de tiempo central usando NTP (Network Time Protocol - NTP).



- Identifique todos los servicios, interfaces y dispositivos de administración vulnerables a ataques de red.
- Realice auditorías de seguridad regularmente.
- Use la función one-step lockdown del SDM o el comando `auto secure` en los routers nuevos.





3 Autenticación, autorización y registro de auditoria

3.0 Introducción al capitulo

3.0.1 Introducción al capitulo

Debe diseñarse una red para controlar a quién se le permite conectarse a ella y qué se le permite hacer mientras está conectado. Estas especificaciones de diseño están identificadas en la política de seguridad de la red. La política especifica cómo los

administradores de red, usuarios corporativos, usuarios remotos, socios de negocios y clientes acceden a los recursos de la red. La política de seguridad de la red también puede demandar la implementación de un sistema de registro de auditoría que monitoree quién inicia sesión, cuándo y qué hace mientras está conectado.

La administración del acceso a la red mediante el uso de los comandos del modo de usuario o del modo privilegiado es un recurso limitado y no escala mucho. En cambio, el uso del protocolo de Autenticación, Autorización y Registro de Auditoría (Authentication, Authorization, and Accounting - AAA) proporciona el marco necesario para habilitar una seguridad de acceso escalable.

Los IOS de los routers Cisco pueden ser configurados para usar AAA para acceder a una base de datos local de usuario y contraseña. El uso de una base de datos local de usuario y contraseña proporciona mejor seguridad que una simple contraseña y es una solución de seguridad fácilmente implementable y relativamente barata. Los IOS de los routers Cisco también pueden ser configurados para usar AAA para acceder a un Servidor de Control de Acceso Seguro de Cisco (ACS). El uso de un ACS de Cisco es muy escalable porque todos los dispositivos de infraestructura acceden a un servidor central. La solución ACS segura de Cisco además es tolerante a fallas porque pueden configurarse varios servidores. La solución ACS segura de Cisco generalmente es implementada por grandes organizaciones.

La práctica de laboratorio del capítulo, Aseguración del acceso administrativo mediante el uso de AAA y RADIUS, permite a los estudiantes usar CLI y SDM para configurar y probar la autenticación local con y sin AAA. También se explora la autenticación centralizada usando AAA y RADIUS. El laboratorio está disponible en el manual de laboratorio en Academy Connection en cisco.netacad.net.

La actividad de Packet Tracer, Configuración de autenticación AAA en routers de Cisco, proporciona a los estudiantes práctica adicional en la implementación de las tecnologías presentadas en este capítulo. Los estudiantes aprenderán a configurar autenticación local con y sin AAA. Para la autenticación AAA basada en servidor se puede configurar TACACS+ y RADIUS. Las actividades de Packet Tracer para CCNA Security están disponibles en Academy Connection en cisco.netacad.net.

En este capítulo, aprenderá a:

- Explicar la función y operación del protocolo de autenticación, autorización y registro de auditoría(AAA).
- Configurar un router Cisco para realizar autenticación AAA con una base de datos local.
- Describir cómo configurar el ACS de Cisco para soportar AAA para routers con IOS Cisco.
- Configurar AAA basado en servidor.

3.1.1 Introducción AAA

Un intruso puede ganar acceso a equipamiento de red y servicios sensibles. Para ayudar a prevenir el acceso no deseado, el control de acceso es necesario. El control de acceso limita quién o qué puede usar recursos específicos así como servicios u opciones disponibles una vez que se otorga el acceso. Se pueden usar muchos tipos de métodos de autenticación en un dispositivo Cisco y cada método ofrece varios niveles de seguridad.

La forma más simple de autenticación son las contraseñas. Este método se configura usando una combinación de login y contraseña en la consola y líneas vty y puertos aux. Este método es el más sencillo de implementar pero también es el más débil y menos seguro. Los inicios de sesión de sólo contraseña son muy vulnerables a ataques de fuerza bruta. Adicionalmente, este método no ofrece registros de auditoría de ningún tipo. Cualquiera que tenga la contraseña puede ganar acceso al dispositivo y alterar la configuración.

Para ayudar a proporcionar registros de auditoría, puede implementarse la autenticación de base de datos local usando uno de los siguientes comandos:

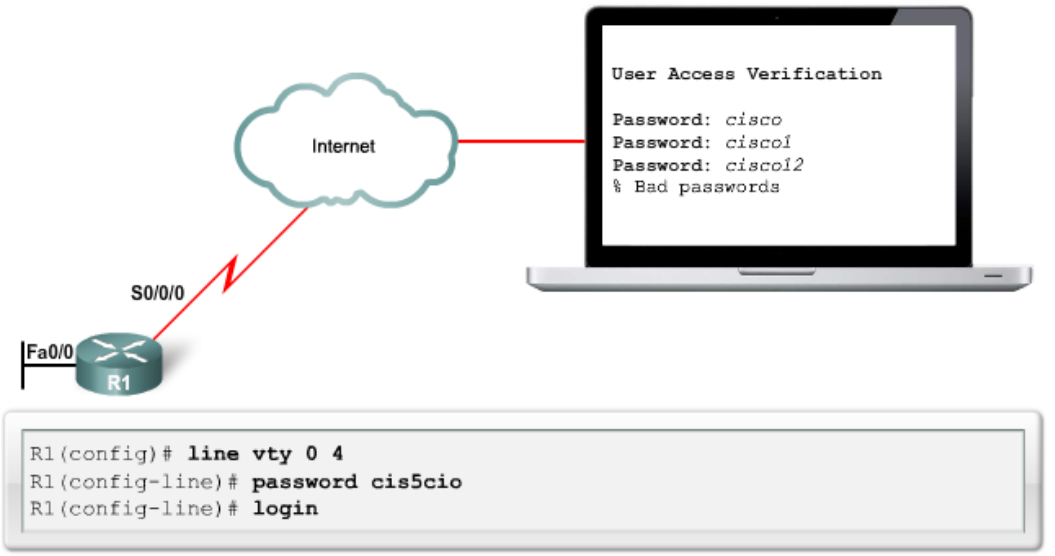
username nombre-usuario password contraseña

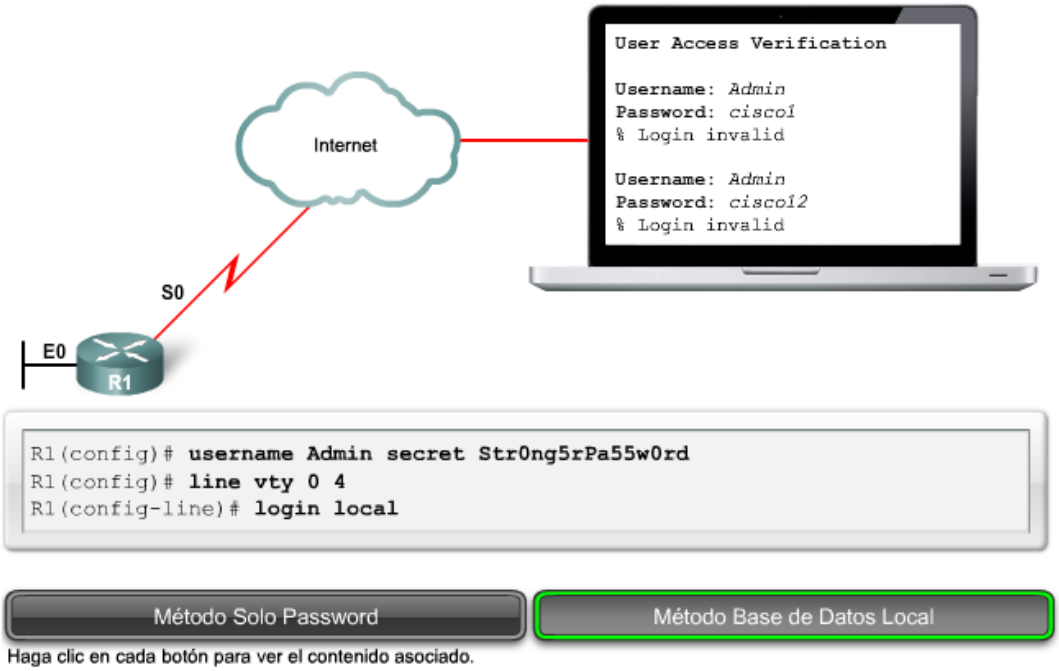
username nombre-usuario secret contraseña

Este método crea cuentas de usuario individuales en cada dispositivo con una contraseña específica asignada a cada usuario. El método de base de datos local proporciona seguridad adicional, ya que el atacante debe conocer tanto nombre de usuario como contraseña. También proporciona un mayor registro de auditoría, ya que se registra el nombre de usuario cada vez que el usuario inicia una sesión. Tenga en consideración que la combinación de comandos username password muestra la contraseña en texto plano en el archivos de configuración si el comando service password-encryption no ha sido emitido. Se recomienda especialmente la combinación username secret porque proporciona cifrado de tipo MD-5.

El método de base de datos local tiene algunas limitaciones. Las cuentas de usuario deben configurarse localmente en cada dispositivo. En una empresa grande que tiene múltiples routers y switches para administrar, puede tomar demasiado tiempo implementar y cambiar las bases de datos locales en cada dispositivo. Adicionalmente, la configuración de base de datos local no proporciona métodos de autenticación de resguardo. Por ejemplo, ¿qué pasaría si el administrador olvidara el nombre de usuario y contraseña de ese dispositivo? Sin métodos de autenticación disponibles, la recuperación de contraseñas es la única opción.

Una mejor solución es hacer que todos los dispositivos accedan a la misma base de datos de usuarios y contraseñas en un servidor central. Este capítulo explora los varios métodos de asegurar el acceso a las redes usando Autenticación, Autorización y Registro de Auditoría (AAA) para asegurar los routers Cisco.





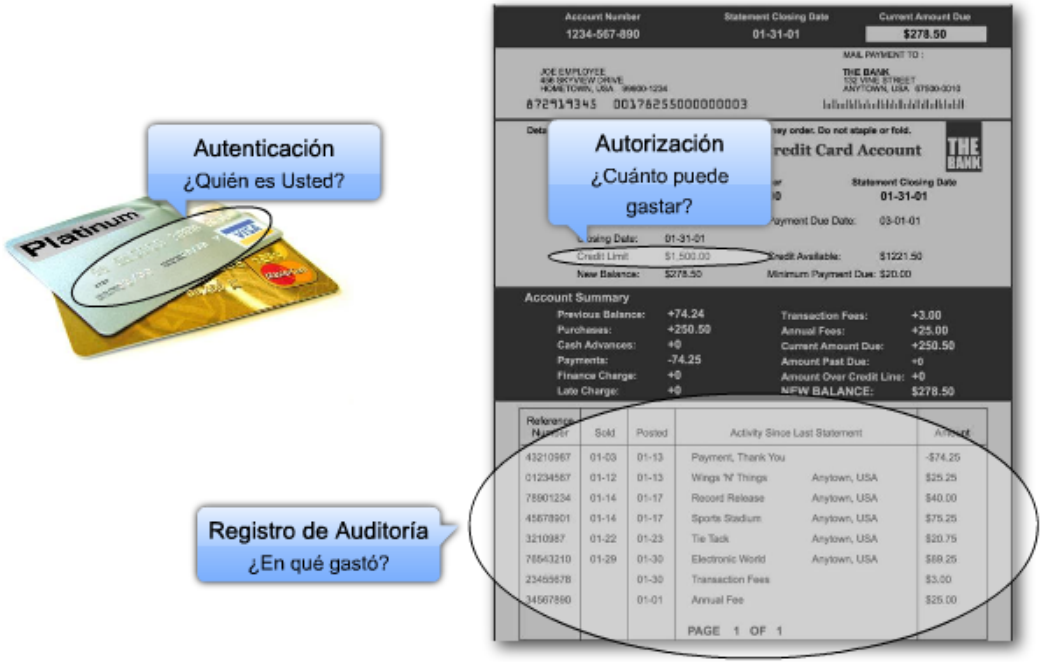
Los servicios de seguridad AAA proporcionan un marco inicial para montar control de acceso en un dispositivo de red. AAA es una manera de controlar a quién se le permite acceso a una red (autenticación) y qué pueden hacer mientras están allí (autorización), así como auditar qué acciones realizaron al acceder a la red (registro de auditoría). Otorga un mayor grado de escalabilidad que el que proporcionan los comandos de con, aux, vty y la autenticación EXEC privilegiada solos.

La seguridad AAA administrativa y de red tiene muchos componentes funcionales en el ambiente Cisco:

Autenticación - Los usuarios y administradores deben probar que son quienes dicen ser. La autenticación puede establecerse por medio de combinaciones de usuario y contraseña, preguntas de desafío y respuesta, tarjetas token y otros métodos. Por ejemplo: "Soy el usuario 'estudiante'. Conozco la contraseña para probar que soy el usuario 'estudiante'".

Autorización - Una vez que el usuario ha sido autenticado, los servicios de autorización determinan los recursos y operaciones a los que el usuario tiene acceso. Por ejemplo, "El usuario 'estudiante' puede acceder al host server XYZ sólo usando Telnet".
Registros de auditoría y auditabilidad - Los registros de auditoría registran lo que el usuario hace, incluyendo los recursos a los que accede, la cantidad de tiempo que se mantiene y cualquier cambio que se haga. El registro de auditoría monitorea el uso de los recursos. Un ejemplo es: "El usuario 'estudiante' accedió al host serverXYZ usando Telnet por 15 minutos".

Este concepto es similar al uso de una tarjeta de crédito. La tarjeta de crédito identifica al que puede usarla, determina cuánto puede gastar ese usuario y monitorea los ítems en los que el usuario gastó dinero.



3.1.2 Características de AAA

Autenticación AAA

Puede utilizarse AAA para autenticar usuarios para acceso administrativo o para acceso remoto a una red. Estos dos métodos de acceso usan diferentes modos para solicitar los servicios de AAA:

Modo carácter - El usuario envía una solicitud para establecer un proceso de modo EXEC con el router con fines administrativos.

Modo paquete - El usuario envía una solicitud para establecer una conexión con un dispositivo en la red a través del router.

A excepción de los comandos de registro de auditoría, todos los comandos AAA se aplican a ambos modos. Esta sección se concentra en asegurar el acceso de modo carácter. Para una red verdaderamente segura, también es importante configurar el router para acceso administrativo y acceso remoto a la red LAN seguros mediante el uso de los servicios AAA.

Cisco proporciona dos métodos comunes para implementar los servicios AAA.

Autenticación AAA local

AAA local usa una base de datos local para la autenticación. Este método almacena los nombres de usuario y sus correspondientes contraseñas localmente en el router Cisco, y los usuarios se autentican en la base de datos local. Esta base de datos es la misma que se requiere para establecer una CLI basada en roles. AAA local es ideal para redes pequeñas.

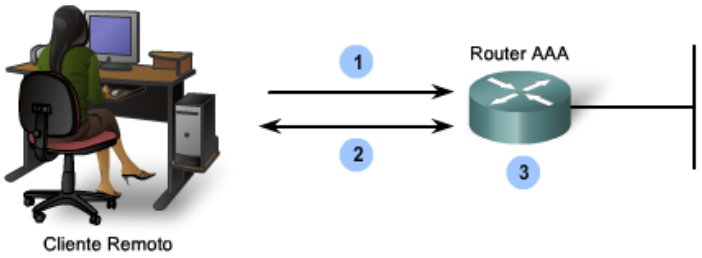
Autenticación AAA basada en servidor

El método basado en servidor usa un recurso externo de servidor de base de datos que utiliza los protocolos RADIUS o TACACS+. Los ejemplos incluyen el Servidor de Control de Acceso Seguro de Cisco (ACS) para Windows Server, el Cisco Secure ACS Solution Engine o Cisco Secure ACS Express. Si hay más de un router, AAA basado en servidor será la opción más apropiada.

Tipo de acceso	Modos	Puertos del Router	Comandos AAA comúnes
Acceso administrativo remoto	El modo carácter provee acceso de usuario y EXEC privilegiado.	consola, vty, aux y tty	Comandos **login**, **exec**, y **enable**
Acceso de red remota	El modo paquete provee acceso a recursos de red	Acceso Dial-up y VPN	Comandos **ppp** y **network**

Métodos de acceso | AAA Local | AAA Basado en servidor

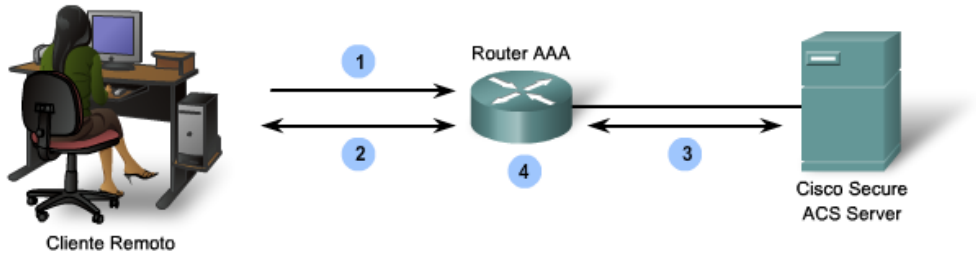
Haga clic en cada botón para ver el contenido asociado.



1. El cliente establece una conexión con el router.
2. El router AAA pide al usuario un nombre de usuario y una contraseña.
3. El router autentica el nombre de usuario y la contraseña usando la base de datos local y el usuario es autorizado a acceder a la red en base a la información en la base de datos local.

Métodos de acceso | AAA Local | AAA Basado en servidor

Haga clic en cada botón para ver el contenido asociado.



1. El cliente establece una conexión con el router.
2. El router AAA pide al usuario un nombre de usuario y una contraseña.
3. El router autentica el nombre de usuario y la contraseña usando el servidor AAA remoto.
4. El usuario es autorizado a acceder a la red en base a la información en el servidor AAA remoto.

Métodos de acceso | AAA Local | AAA Basado en servidor

Haga clic en cada botón para ver el contenido asociado.

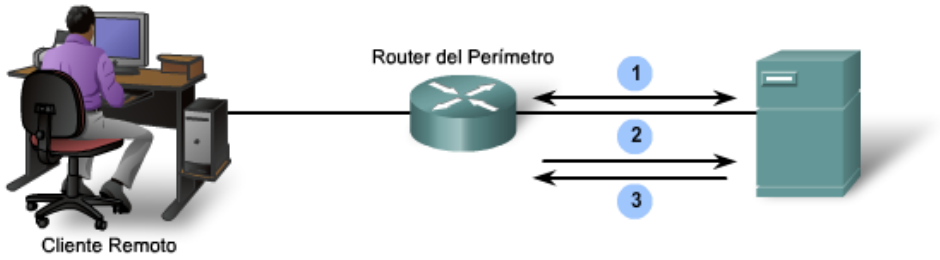
Autorización AAA

Una vez que los usuarios han ido autenticados exitosamente contra la fuente de datos AAA seleccionada (ya sea local o basada en servidor), se les autoriza el acceso a recursos específicos en la red. La autorización consiste básicamente en lo que un usuario puede y no puede hacer en la red luego de que es autenticado, parecido a cómo los niveles de privilegios y la CLI basada en roles les dan a los usuarios derechos y privilegios específicos a ciertos comandos en el router.

En general, la autorización se implementa usando una solución de AAA basada en servidor. La autorización usa un grupo de atributos creado que describe el acceso del usuario a la red. Estos atributos se comparan con la información contenida dentro de la

base de datos AAA y se determinan las restricciones para ese usuario, que son enviadas al router local donde el usuario está conectado.

La autorización, que se implementa inmediatamente después de que el usuario se autentica, es automática: no se requiere participación de parte del usuario luego de la autenticación.



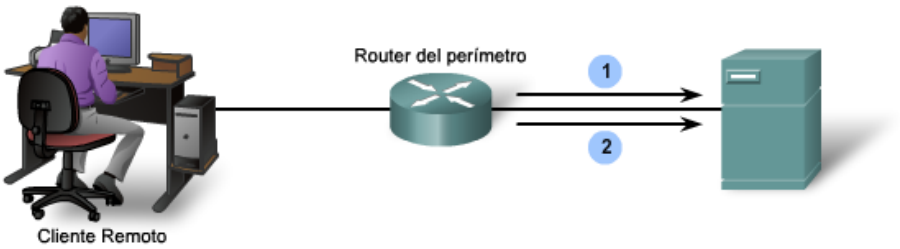
1. Cuando un usuario ha sido autenticado, una sesión es establecida con el servidor AAA.
2. El router solicita autorización para el servicio requerido del servidor AAA.
3. El servidor AAA retorna una PASA/FALLA para la autorización.

Registro de Auditoría AAA

El registro de auditoría recolecta y reporta datos de uso para que puedan ser empleados para auditorías o emisión de facturas. Los datos recolectados pueden incluir el inicio y fin de conexiones, comandos ejecutados, números de paquetes y número de bytes.

El registro de auditoría se implementa usando una solución AAA basada en servidor. Este servicio reporta estadísticas de uso al servidor ACS. Estas estadísticas pueden ser extraídas para crear reportes detallados sobre la configuración de la red.

Un uso popular de los registros de auditoría es su combinación con la autenticación AAA para la administración de dispositivos de internetworking por parte de los administradores. El registro de auditoría proporciona una mejor rendición que la que ofrece la autenticación. Los servidores AAA mantienen un registro detallado de absolutamente todo lo que hace el usuario una vez autenticado en el dispositivo. Esto incluye todos los comandos de configuración y EXEC emitidos por el usuario. El registro contiene varios campos de datos, incluyendo el nombre de usuario, la fecha y hora y el comando ingresado por el usuario. Esta información es útil al solucionar problemas en los dispositivos. También proporciona protección contra individuos malintencionados.



1. Cuando un usuario ha sido autenticado, el proceso de registro de auditoría de AAA genera un mensaje de comienzo para iniciar el proceso de registro de auditoría.
2. Cuando el usuario finaliza, un mensaje de fin es registrado y el proceso de registro de auditoría termina.

Pasos del registro de auditoría | Funciones del registro de auditoría AAA

Haga clic en cada botón para ver el contenido asociado.

Registro de auditoría de la red	El registro de auditoría de la red captura información para todas las sesiones del protocolo punto a punto (PPP), el protocolo de Internet de línea serial (SLIP) o el protocolo de acceso remoto de Apple (ARAP), incluyendo conteo de bytes y paquetes.
Registro de auditoría de la conexión	El registro de auditoría de la conexión captura información sobre las conexiones salientes desde el cliente AAA, como Telnet, transporte de area local (LAT), TN3270, paquetes assembler/disassembler (PAD) y rlogin.
Registro de Auditoría de EXEC	El registro de auditoría de EXEC captura información sobre las sesiones de terminal (user shells) de usuario EXEC en el servidor de acceso a la red, incluyendo nombre de usuario, tiempo de inicio y fin, dirección IP del servidor de acceso y (para usuario dial-in) el número de teléfono desde donde se originó la llamada.
Registro de Auditoría del sistema	El registro de auditoría del sistema captura información sobre todos los eventos a nivel de sistema (por ejemplo, cuando el sistema se reinicia o se activa o desactiva el registro de auditoría).
Registro de Auditoría de comandos	El registro de auditoría de comandos captura información sobre los comandos de shell de EXEC para un nivel de privilegios especificado que está siendo ejecutado en un servidor de acceso a la red. Cada registro de auditoría de comandos incluye una lista de los comandos ejecutados para un nivel de privilegios, asi como la fecha y hora en que cada comando fue ejecutado y el usuario que lo ejecutó.
Registro de Auditoría de recursos	La implementación de Cisco del registro de comandos de AAA captura registros "start" y "stop" para llamadas que han pasado la autenticación. La característica adicional de generar registros stop para llamadas que fallan al autenticarse como parte de la autenticación del usuario también está soportada. Tales registros son necesarios para usuarios que emplean registros de auditoría para administrar y monitorear sus redes.

Haga clic en cada botón para ver el contenido asociado.

3.2.1 Configuración de autenticación AAA local con CLI

La autenticación AAA local, también conocida como autenticación autocontenida, debe ser configurada en redes pequeñas que contengan uno o dos routers que provean acceso a un número limitado de usuarios. Este método usa los nombres de usuario y contraseñas locales almacenados en el router. El administrador de sistemas debe poblar la base de datos de seguridad local especificando perfiles de nombre de usuario y contraseña para cada usuario que pueda conectarse.

El método de autenticación AAA local es similar al uso del comando login local con una excepción: AAA proporciona además una manera de configurar métodos de autenticación de respaldo.

La configuración de los servicios AAA local para autenticar el acceso administrativo (acceso de modo carácter) requiere algunos pasos básicos.

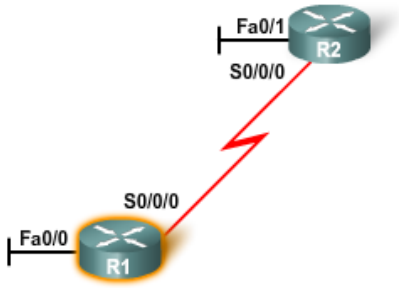
Paso 1. Agregar nombres de usuario y contraseñas a la base de datos local del router para los usuarios que requieren acceso administrativo al router.

Paso 2. Habilitar AAA globalmente en el router.

Paso 3. Configurar los parámetros AAA en el router.

Paso 4. Confirmar la configuración AAA y buscar posibles problemas.

```
R1# conf t
R1(config)# username JR-ADMIN secret Str0ngPa55w0rd
R1(config)# username ADMIN secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authentication login default local-case
R1(config)# aaa local authentication attempts max-fail 10
```



Haga clic en R1 para ver una muestra de configuración de Autenticación AAA Local.

Para habilitar AAA, use el comando de configuración global aaa new-model. Para deshabilitar AAA, use la forma no del comando.

Una vez habilitado AAA, para configurar la autenticación en los puertos vty, líneas asíncronas (tty), el puerto auxiliar o el de consola, defina una lista nombrada de los métodos de autenticación y luego aplíquela a las interfaces.

Para definir una lista nombrada de métodos de autenticación, use el comando aaa authentication login. Este comando requiere un nombre de lista y los métodos de autenticación. El nombre de la lista identifica la lista de métodos de autenticación activada cuando el usuario ingresa. La lista de métodos es una lista secuencial que describe los métodos de autenticación que se consultarán al momento de autenticar al usuario. Las listas de métodos permiten al administrador designar uno o más protocolos

de seguridad para la autenticación. El uso de más de un protocolo proporciona un sistema de autenticación de resguardo en caso de que falle el método inicial.

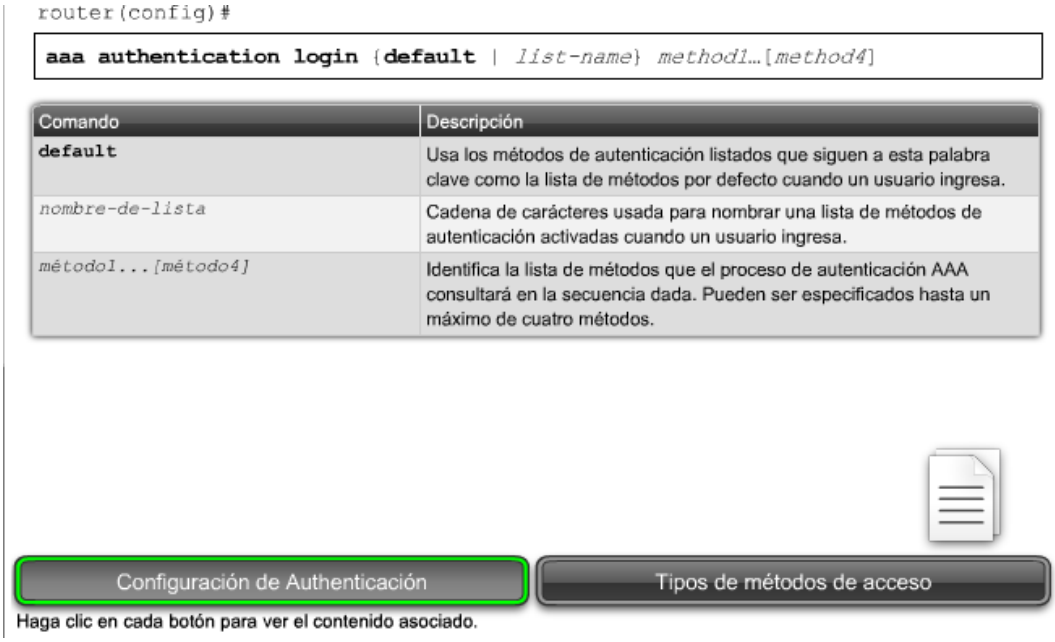
Pueden usarse muchas palabras clave para indicar el método. Para habilitar la autenticación local usando una base de datos local preconfigurada, use la palabra clave local o local-case. La diferencia entre ambas opciones es que local acepta e nombre de usuario no es sensible a mayúsculas y minúsculas, mientras que local-case sí. Para especificar que el usuario se puede autenticar usando la contraseña enable, use la palabra clave enable. Para asegurarse de que la autenticación sea exitosa incluso si todos los métodos devuelven errores, especifique none como el último método. Por motivos de seguridad, solo use none para probar la configuración AAA. No debe aplicarse nunca en una red en uso.

Por ejemplo, se puede configurar el método enable como mecanismo de apoyo si se olvidan el nombre de usuario o la contraseña.

aaa authentication login TELNET-ACCESS local enable

En este ejemplo, se crea una lista de autenticación llamada TELNET-ACCESS que requiere que los usuarios intenten primero autenticarse a la base de datos de usuario local en el router. Si ese intento devuelve un error, como que una base de datos local no está configurada, el usuario puede intentar autenticarse a través de la contraseña enable.

Se puede especificar un mínimo de un método y un máximo de cuatro métodos en una sola lista de métodos. Cuando un usuario intenta ingresar, se usa el primer método en la lista. El software del IOS de Cisco solo intenta efectuar la autenticación con el siguiente método en la lista cuando no hay respuesta u ocurre un error en el método anterior. Si el método de autenticación deniega acceso al usuario, el proceso de autenticación se detiene y no se permiten otros métodos de autenticación.



Palabra clave del Tipo de método de autenticación	Descripción
enable	Usa la contraseña de enable para la autenticación.
krb5	Usa Kerberos 5 para la autenticación.
krb5-telnet	Usa el protocolo de autenticación telnet Kerberos 5 cuando usa telnet para conectar al router.
line	Usa la contraseña de line para autenticación.
local	Usa la base de datos de usuarios local para la autenticación.
local-case	Usa la autenticación por nombre de usuario local sensible a mayúsculas.
none	No usa autenticación.
cache *nombre-del-grupo*	Usa un grupo servidor cache (cache server group) para la autenticación.
group radius	Usa la lista de todos los servidores RADIUS para la autenticación.
group tacacs+	Usa la lista de todos los servidores TACACS+ para la autenticación.
group *nombre-del-grupo*	Usa un subconjunto de servidores RADIUS o TACACS+ como fue definido por el comando **aaa group server radius** o **aaa group server tacacs+**.

Configuración de Authenticación | Tipos de métodos de acceso

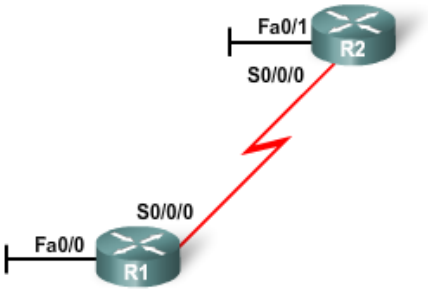
Haga clic en cada botón para ver el contenido asociado.

La lista de métodos definida debe ser aplicada a interfaces o líneas específicas. Para otorgar flexibilidad, se pueden aplicar diferentes listas de métodos a diferentes interfaces y líneas. Por ejemplo, un administrador puede aplicar una lista para Telnet y luego tener un método de ingreso diferente para la línea de comandos. Para habilitar un nombre de lista específico, use el comando aaa login authentication nombre-lista en el modo de configuración de línea.

La opción también sirve para configurar un nombre de lista por defecto. Cuando se habilita por primera vez AAA, se aplica la lista por defecto llamada "default" a todas las interfaces y líneas, pero no tiene métodos de autenticación definidos. Para asignar múltiples métodos de autenticación a la lista por defecto, use el comando aaa authentication login default método1... [método4].

Los métodos de autenticación en la lista default se usan por defecto en todas las líneas si no se crea una lista de métodos de autenticación personalizada. Si la interfaz o línea tiene aplicada una lista de métodos de autenticación diferente de la lista por defecto, esa lista será la usada. Si la lista default no está establecida y no hay ninguna otra lista, solo se controla la base de datos de usuarios local. Esto tiene el mismo efecto que el comando aaa authentication login default local. En la consola, el ingreso ocurre sin ningún control de autenticación si no está establecida la lista default.

Una vez que se aplica una lista de métodos de autenticación personalizada a la interfaz, es posible volver al método por defecto por medio del comando no aaa authentication login nombre-lista. Si no se ha definido la lista por defecto, la autenticación AAA no ocurrirá.




```
R1# conf t
R1(config)# username JR-ADMIN secret Str0ngPa55w0rd
R1(config)# username ADMIN secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authentication login default local-case enable
R1(config)# aaa authentication login TELNET-LOGIN local-case
R1(config)# line vty 0 4
R1(config-line)# login authentication TELNET-LOGIN
```

Se puede implementar seguridad adicional en la línea usando el comando aaa local authentication attempts max-fail número-intentos-fallidos en el modo de configuración global. Este comando asegura las cuentas de usuario AAA bloqueando las cuentas que tienen un número excesivo de intentos fallidos de ingreso. Para eliminar el número de intentos fallidos establecido, use la forma no del comando.

Para ver una lista de todos los usuarios bloqueados, use el comando show aaa local user lockout en el modo EXEC privilegiado. Use el comando clear aaa local user lockout {username nombre-usuario | all} en modo EXEC privilegiado para desbloquear a un usuario específico o para desbloquear a todos los usuarios bloqueados.

El comando aaa local authentication attempts max-fail difiere del comando login delay en la manera de manejar los intentos fallidos. El comando aaa local authentication attempts max-fail bloquea la cuenta del usuario si la autenticación falla. Esta cuenta permanece bloqueada hasta que un administrador la blanquee. El comando login delay introduce un retraso entre intentos de ingreso fallidos sin bloquear la cuenta.

Cuando un usuario ingresa a un router Cisco y utiliza AAA, se asigna un ID único a la sesión. Durante el tiempo que persista la sesión se recolectan varios atributos relacionados con esta, que son almacenados internamente dentro de la base de datos AAA. Estos atributos pueden incluir la dirección IP del usuario, el protocolo que se usa para acceder al router, como PPP o SLIP (Serial Line Internet Protocol), la velocidad de la conexión y el número de paquetes o bytes recibidos y trasmitidos.

Para ver los atributos recolectados en una sesión AAA, use el comando show aaa user {all | unique id} en el modo EXEC privilegiado. Este comando no proporciona información sobre todos los usuarios que ingresan a un dispositivo, sino sobre aquellos

que han sido autenticados o autorizados usando AAA o cuyas sesiones están siendo monitoreadas por el módulo de registro de auditoría de AAA.

Puede usarse el comando show aaa sessions para visualizar el ID único de una sesión.

```
router(config)#
aaa local authentication attempts max-fail [number-of-unsuccessful-attempts]
```

Comando	Descripción
número-de-intentos-fallidos	Número de intentos de autenticación fallidos antes de que se cierre la conexión y se bloquee la cuenta.

```
R1# show aaa local user lockout

                Local-user          Lock time
                JR-ADMIN            04:28:49 UTC Sat Dec 27 2008
```

Configurar Bloqueo | Ver sesiones AAA

Haga clic en cada botón para ver el contenido asociado.

```
R1# show aaa sessions
Total sessions since last reload: 4
Session Id: 1
   Unique Id: 175
   User Name: ADMIN
   IP Address: 192.168.1.10
   Idle Time: 0
   CT Call Handle: 0
```

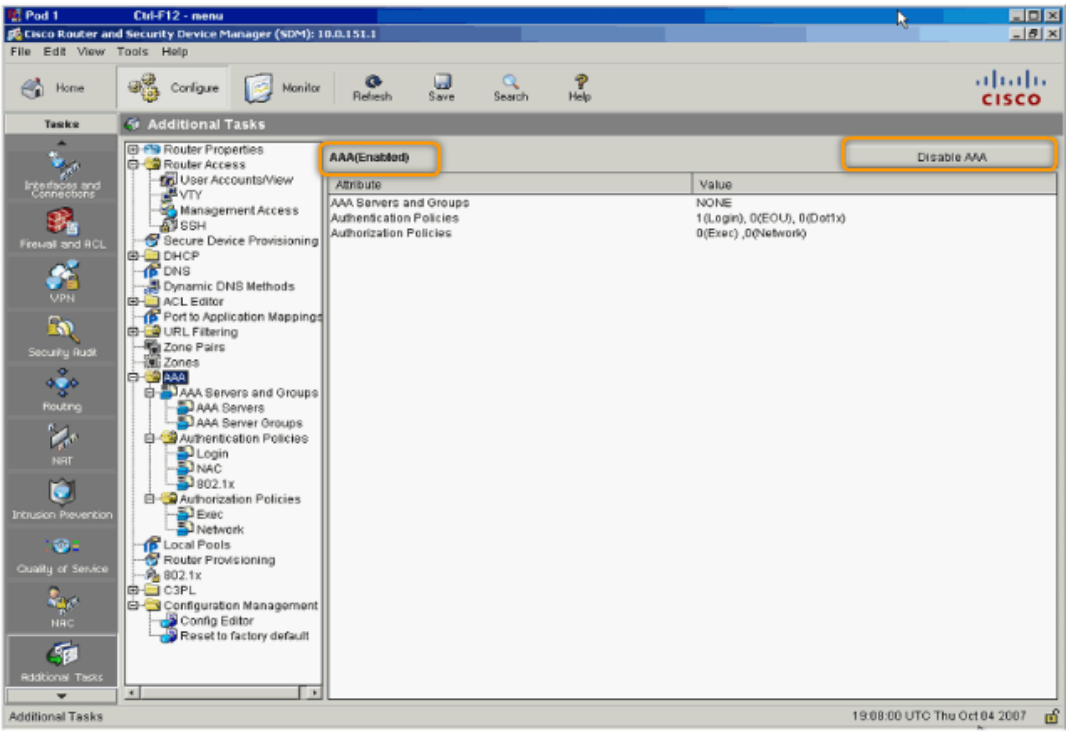
Configurar Bloqueo | Ver sesiones AAA

Haga clic en cada botón para ver el contenido asociado.

3.2.2 Configuracion de autenticación local con SDM

AAA está habilitado por defecto en el SDM de Cisco, pero es una buena idea confirmar que esté habilitado actualmente. Para verificar la configuración de AAA y para habilitar o deshabilitar AAA, vaya a Configure > Additional Tasks > AAA.

Si oprime el botón Disable AAA, el SDM de Cisco mostrará un mensaje que le comunicará que efectuará cambios de configuración para asegurar que se pueda acceder al router luego de que se deshabilite AAA.



La primera tarea al usar SDM para configurar los servicios AAA para autenticación local es crear usuarios:

Paso 1. Vaya a Configure > Additional Tasks > Router Access > User Accounts/View.

Paso 2. Haga clic en Add para añadir un usuario.

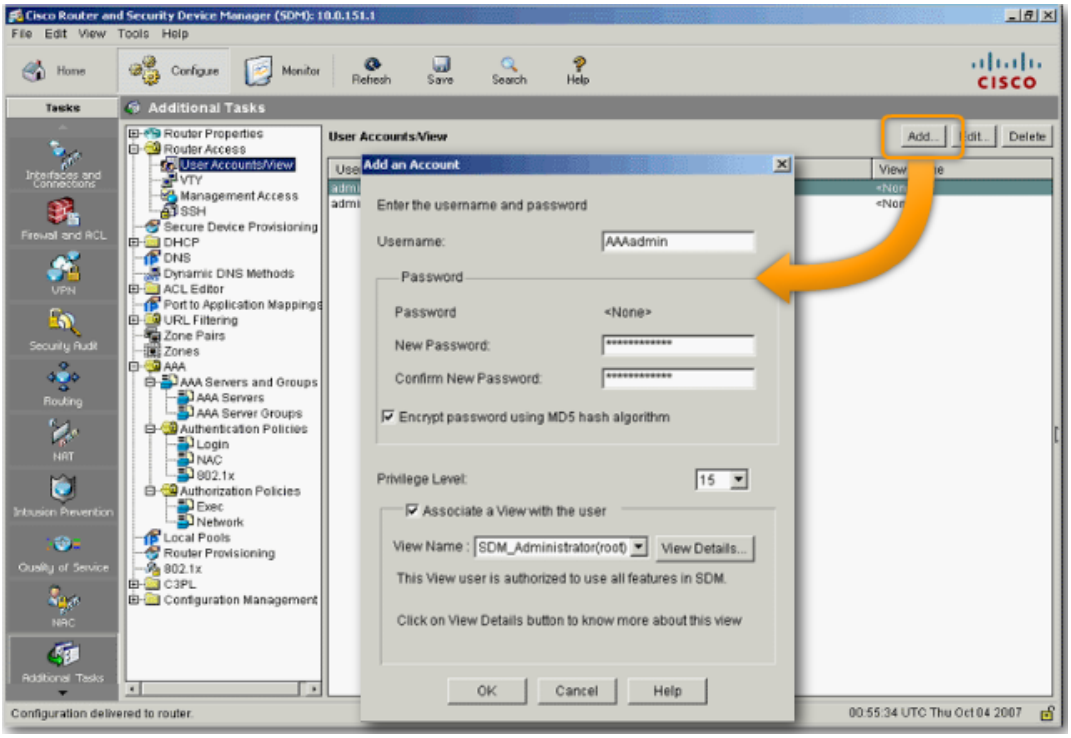
Paso 3. En la ventana Add an Account, ingrese el nombre de usuario y la contraseña en los campos apropiados para definir la cuenta de usuario.

Paso 4. En la lista desplegable elija 15 en caso de que no haya niveles de privilegios inferiores definidos.

Paso 5. Si se han definido las vistas, marque la casilla Associate a View with the User y elija una vista de la lista View Name asociada con el usuario.

Paso 6. Haga clic en OK.

El comando CLI generado por el SDM de Cisco es username AAAadmin privilege 15 secret 5 1f16u$uKOO6J/UnojZ0bCEzgnQi1 view root.



Para configurar la autenticación AAA, el administrador debe definir una lista de métodos de autenticación para el método por defecto o configurar una lista de métodos nombrada y aplicarla. Pueden crearse diferentes listas de métodos y aplicarse a diferentes interfaces o líneas.

Configure la lista de métodos por defecto para autenticación de ingreso usando la base de datos local:

Paso 1. Vaya a Configure > Additional Tasks > AAA > Authentication Policies > Login y haga clic enAdd.

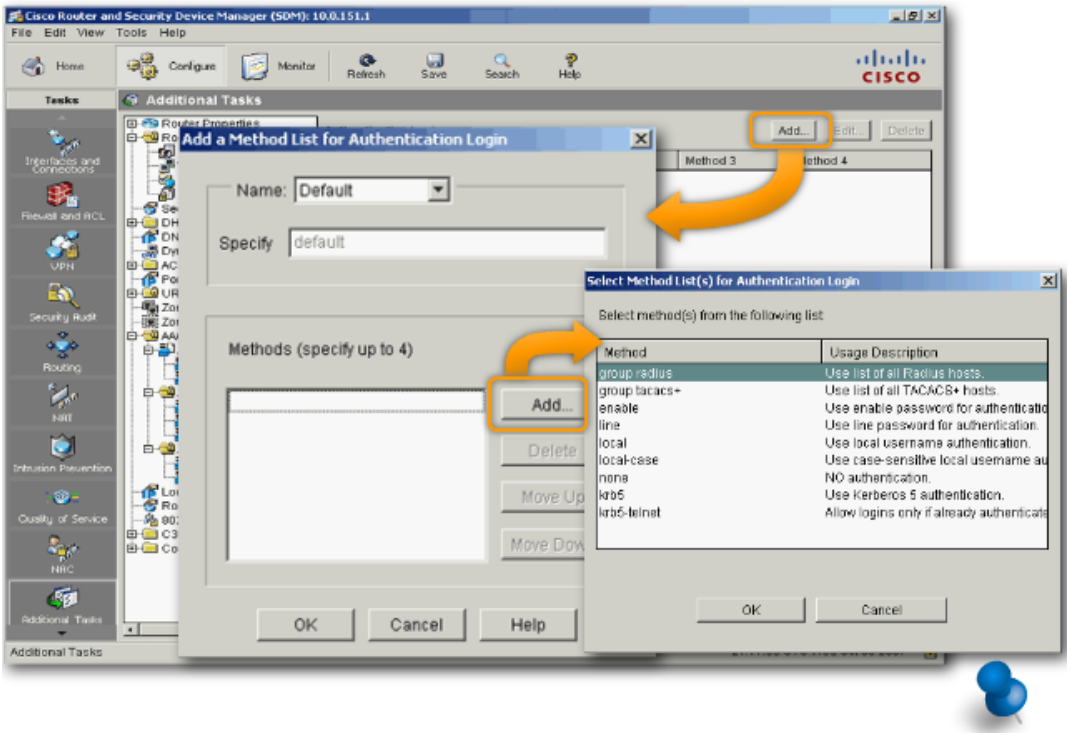
Paso 2. En la ventana Add a Method List for Authentication Login, verifique que la opción Default esté seleccionada en la lista desplegable Name.

Paso 3. Haga clic en Add.

Paso 4. En la ventana Select Method List(s) for Authentication Login, vaya a local en la lista de métodos.

Paso 5. Haga clic en OK.

El comando CLI generado por el SDM de Cisco es aaa authentication login default local.



3.2.3 Resolución de problemas de autenticación AAA local

El router Cisco tiene comandos de debugging que resultan útiles para la resolución de problemas en la autenticación. El comando debug aaa contiene muchas palabras clave que pueden ser usadas para este propósito. El comando debug aaa authentication es de un interés especial.

La mejor oportunidad para aprender a entender la salida de un proceso de debugging es cuando todo está funcionando con normalidad. Saber qué muestra la salida del debugging cuando todo está bien ayuda a identificar problemas cuando las cosas andan mal. Tenga precaución con el comando debug en un ambiente de producción, ya que estos comandos generan una carga significativa en los recursos del router y pueden afectar el comportamiento de la red.

```
R1# debug aaa ?
  accounting           Accounting
  administrative       Administrative
  api                  AAA api events
  attr                 AAA Attr Manager
  authentication       Authentication
  authorization        Authorization
  cache                Cache activities
  coa                  AAA CoA processing
  db                   AAA DB Manager
  dead-criteria        AAA Dead-Criteria Info
  id                   AAA Unique Id
  ipc                  AAA IPC
  mlist-ref-count      Method list reference counts
  mlist-state          Information about AAA method list state change and
                       notification
  per-user             Per-user attributes
  pod                  AAA POD processing
  protocol             AAA protocol processing
  server-ref-count     Server handle reference counts
  sg-ref-count         Server group handle reference counts
  sg-server-selection  Server Group Server Selection
  subsys               AAA Subsystem
  testing              Info. about AAA generated test packets
```

El comando debug aaa authentication es útil para la resolución de problemas en AAA. Para deshabilitar este comando use la forma no o la sentencia general undebug all.

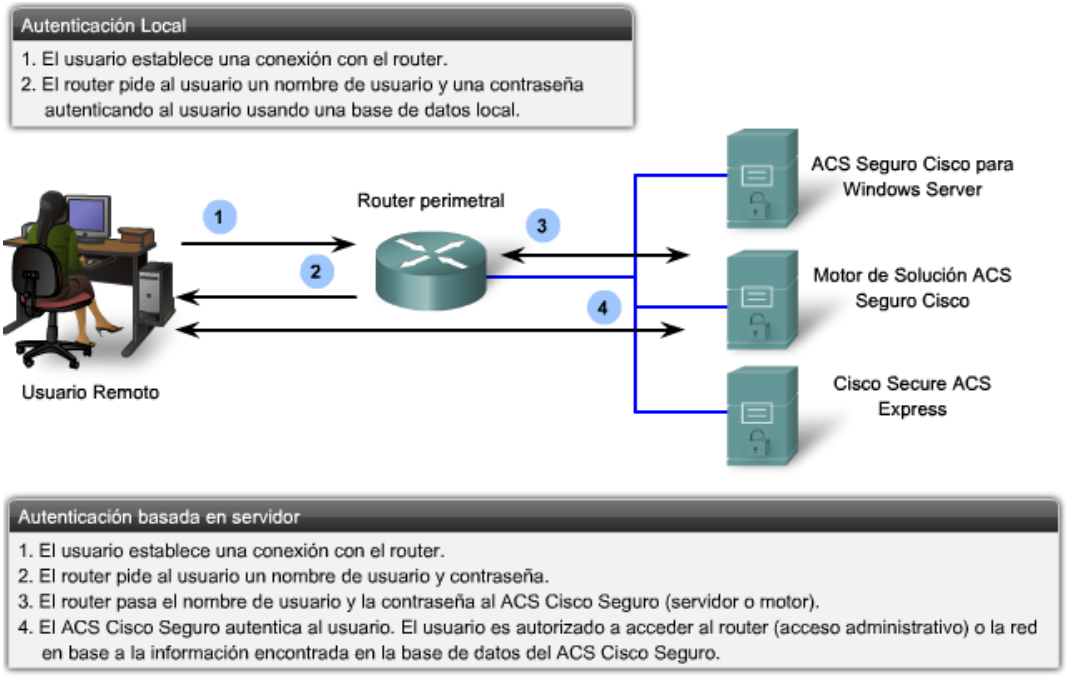
Busque específicamente los mensajes de estado GETUSER y GETPASS. El mensaje Method también es útil para identificar la lista de métodos a la que se está haciendo referencia.



3.3.1 Características de AAA basado en servidor

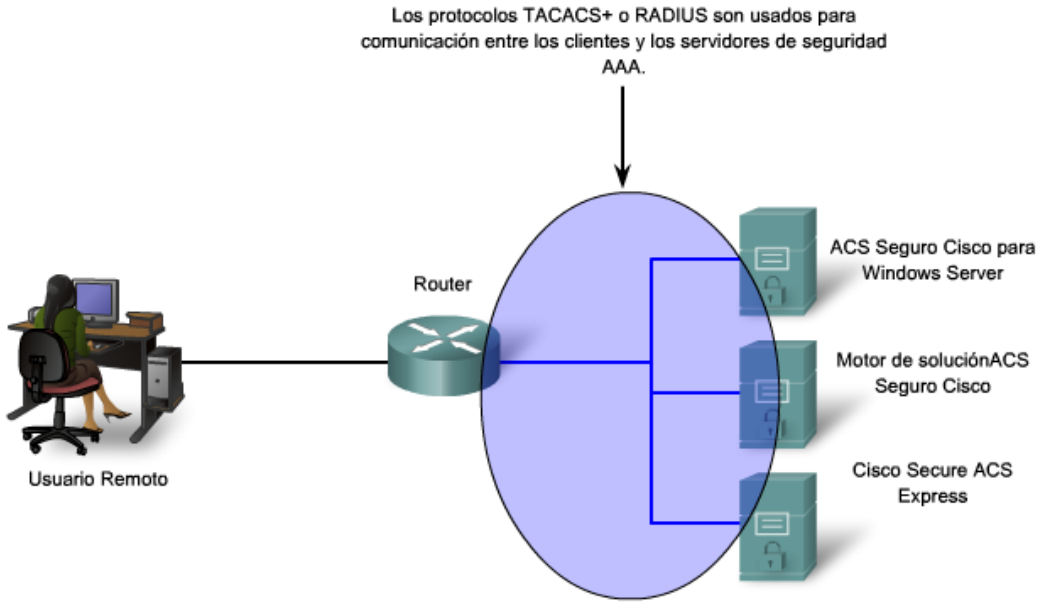
Las implementaciones de AAA local no son especialmente escalables. La mayoría de los entornos empresariales tienen más de un router Cisco con varios administradores y cientos o miles de usuarios que requieren acceso a la LAN de la empresa. Mantener bases de datos locales para cada router de Cisco en una red de tal tamaño no es factible.

Como solución a este desafío puede usarse uno o más servidores AAA, como los ACS Seguros de Cisco, para administrar las necesidades de acceso de los usuarios y administradores de toda la red de la empresa. Un ACS Cisco puede crear una base de datos de usuario y administrativa central a la que accedan todos los dispositivos de la red. También puede trabajar con bases de datos externas, incluyendo Active Directory y LDAP (Lightweight Directory Access Protocol). Estas bases de datos almacenan información de cuentas de usuario y contraseñas, permitiendo una administración centralizada de las cuentas de usuario.



La familia de productos de ACS de Cisco soporta tanto TACACS+ (Terminal Access Control Access Control Server Plus) como RADIUS (Remote Dial-in User Services), que son los dos protocolos predominantes usados por los dispositivos de seguridad, routers y switches de Cisco para la implementación de AAA.

Aunque ambos protocolos pueden ser usados para la comunicación entre clientes y servidores AAA, TACACS+ es considerado el más seguro entre ambos. Esto es porque todos los intercambios de TACACS+ son cifrados: RADIUS sólo cifra la contraseña de usuario. No cifra nombres de usuario, información del registro de auditoría o cualquier otra información que se transmita en el mensaje RADIUS.



3.3.2 Protocolos de comunicación de AAA basado en servidor

Tanto TACACS+ como RADIUS son protocolos de administración, pero cada uno soporta diferentes capacidades y funcionalidades. La elección de uno sobre otro depende de las necesidades de la organización. Por ejemplo, un ISP grande puede elegir RADIUS porque soporta un registro de auditoría detallado necesario para calcular lo que debe cobrarse al usuario. Una organización con varios grupos de usuarios puede seleccionar TACACS+ porque requiere la aplicación de políticas de autorización selectas por usuario y por grupo.

Es importante entender las varias diferencias entre los protocolos TACACS+ y RADIUS.

Los factores críticos de TACACS+ incluyen:

Es incompatible con TACACS y XTACACS
Separa la autenticación y la autorización
Cifra todas las comunicaciones
Usa el puerto TCP 49

Los factores críticos de RADIUS incluyen:

Usa servidores proxy RADIUS para escalabilidad
Combina la autenticación y la autorización RADIUS en un solo proceso
Cifra sólo la contraseña
Usa UDP
Soporta tecnologías de acceso remoto, 802.1X y SIP

Comparación TACACS+/RADIUS

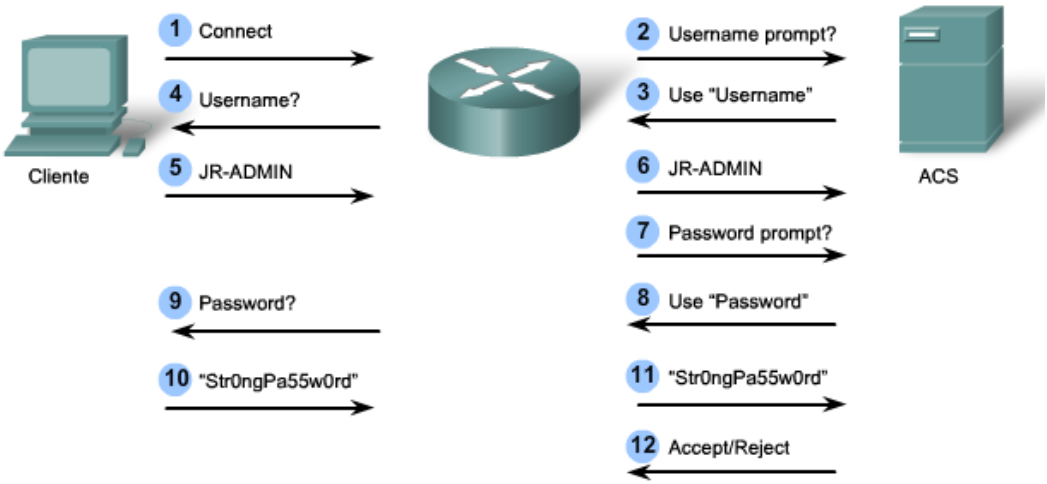
	TACACS+	RADIUS
Funcionalidad	Separa AAA de acuerdo a la arquitectura AAA, permitiendo modularidad en la implementación del servidor de seguridad	Combina autenticación y autorización pero separa el registro de auditoría, permitiendo menos flexibilidad en la implementación que TACACS+
Estándar	Mayormente soportado por Cisco	Estándar abierto/RFC
Protocolo de transporte	TCP	UDP
CHAP	Desafío bidireccional y respuesta como el usado en Challenge Handshake Authentication Protocol (CHAP)	Desafío unidireccional y respuesta desde el servidor de seguridad RADIUS hacia el cliente RADIUS
Soporte de Protocolo	Soporte Multiprotocolo	No ARA, no NetBEUI
Confidencialidad	Paquete completamente cifrado	Contraseña cifrada
Personalización	Provee autorización de comandos del router en base a usuarios y grupos	No tiene opciones para autorizar comandos del router en base a usuarios o grupos
Registro de Auditoría	Limitada	Extensiva

TACACS+ es una mejora de Cisco al protocolo TACACS original. A pesar de su nombre, TACACS+ es un protocolo enteramente nuevo que es incompatible con todas las versiones anteriores de TACACS. TACACS+ es soportado por la familia de routers

y servidores de acceso Cisco como parte de la versión de mantenimiento 10.3 del IOS de Cisco. Actualmente, Cisco está presentando TACACS+ a los grupos de trabajo de IETF y está contribuyendo a y adoptando los estándares de protocolo emergentes.

TACACS+ proporciona servicios AAA separados. Separar los servicios AAA proporciona flexibilidad en la implementación, ya que es posible usar TACACS+ para autorización y registros de auditoría mientras se usa otro método para la autenticación.

Las extensiones al protocolo TACACS+ proporcionan más tipos de códigos de solicitud y respuesta de autenticación que los que estaban en la especificación TACACS original. TACACS+ ofrece soporte multiprotocolo, como IP y AppleTalk. La operación normal de TACACS+ cifra todo el cuerpo del paquete para comunicaciones más seguras y usa el puerto TCP 49.



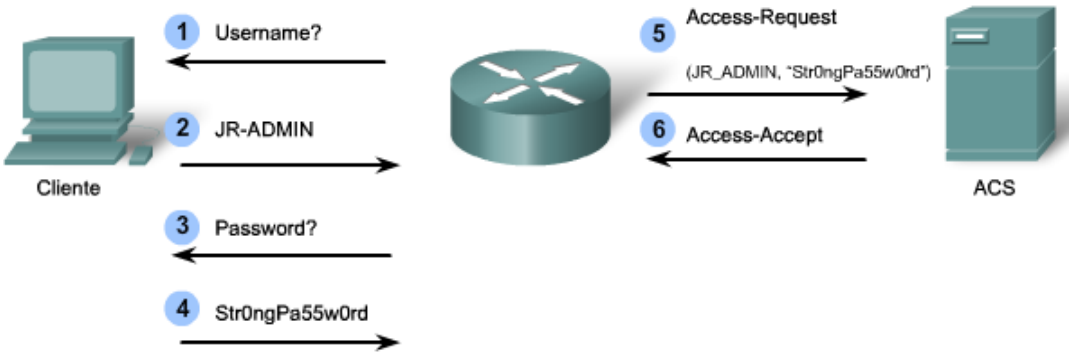
RADIUS, desarrollado por Livingston Enterprises, es un protocolo AAA abierto de estándar IETF con aplicaciones en acceso a las redes y movilidad IP. RADIUS trabaja tanto en situaciones locales y de roaming, y generalmente se usa para los registros de auditoría. Se lo define en los RFCs 2865, 2866, 2867 y 2868.

El protocolo RADIUS esconde las contraseñas durante la transmisión, incluso con el Protocolo de Autenticación de Contraseñas (Password Authentication Protocol - PAP), usando una operación bastante compleja que involucra la dispersión a través de Message Digest 5 (MD5) y una contraseña compartida. Sin embargo, el resto del paquete se envía en texto plano.

RADIUS combina autenticación y autorización en un solo proceso. Cuando el usuario se autentica, también está autorizado. RADIUS usa el puerto UDP 1645 o el 1812 para la autenticación y el puerto UDP 1646 o el 1813 para los registros de auditoría.

RADIUS es muy popular entre los proveedores de servicio VoIP. Pasa las credenciales de inicio de sesión de un nodo SIP (protocolo de inicio de sesión), como un teléfono de banda ancha, a un nodo SIP registrante usando autenticación digest, para luego enviarlas a un servidor RADIUS usando RADIUS. También es el protocolo utilizado por el estándar de seguridad 802.1X.

El protocolo DIAMETER es el reemplazo programado para RADIUS. DIAMETER usa un nuevo protocolo de transporte llamado Stream Control Transmission Protocol (SCTP) y TCP en lugar de UDP.



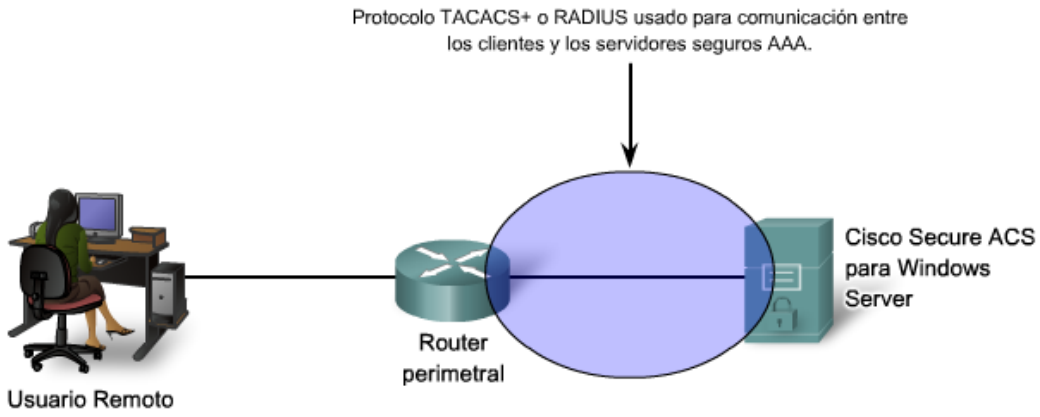
3.3.3 ACS seguro de Cisco

Hoy en día, existen muchos servidores de autenticación en el mercado: el servidor Steel-Belted RADIUS de Funk, el RADIUS Authentication Billing Manager de Livingston Enterprises, y los servidores RADIUS de server, Merit Networks son muy conocidos. Aunque estas son empresas de reputación con productos populares, carecen de la habilidad de combinar los protocolos TACACS+ y RADIUS en una sola solución. Afortunadamente el ACS Seguro de Cisco para Windows Server es una sola solución que ofrece AAA tanto para TACACS+ como para RADIUS.

El ACS Seguro de Cisco es un servidor de control de acceso altamente escalable y de alto rendimiento que puede ser usado para controlar el acceso y la configuración administrativos para todos los dispositivos de red en una red que soporta RADIUS o TACACS+ o ambos. El ACS Seguro de Cisco ofrece varios beneficios:

Extiende la seguridad de acceso al combinar la autenticación, el acceso del usuario y el acceso del administrador con control de políticas dentro de una solución de networking de identidad centralizada.

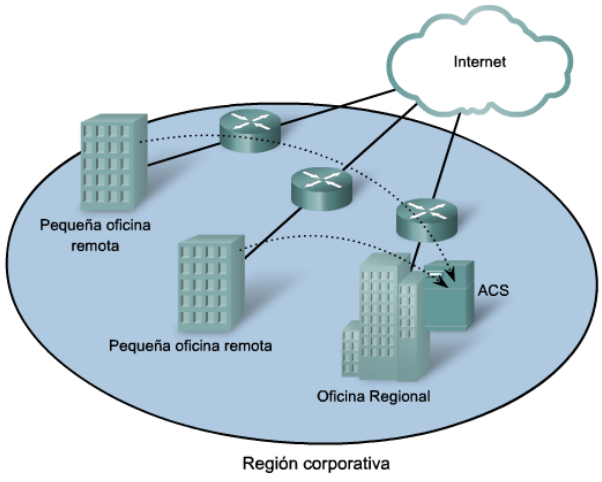
Permite mayor flexibilidad y movilidad, seguridad mejorada y ganancias en la productividad del usuario.
Aplica una política de seguridad uniforme para todos los usuarios, sin importar cómo acceden a la red.
Reduce la carga administrativa ya que escala el acceso administrativo y de usuario a la red.



El ACS Seguro de Cisco usa una base de datos central. Centraliza el control de todos los privilegios de usuario y los distribuye en los puntos de acceso de toda la red. El ACS Seguro de Cisco proporciona funciones de monitoreo y registro del comportamiento del usuario, conexiones de acceso y cambios de la configuración de los dispositivos. Esta función es extremadamente importante para las organizaciones que buscan atenerse a las varias reglas gubernamentales. El ACS Seguro de Cisco soporta una gran variedad de conexiones de acceso, incluyendo redes LAN cableadas e inalámbricas, dialup, banda ancha, contenido, almacenamiento, VoIP, firewalls y VPNs.

El ACS Seguro de Cisco soporta una gran variedad de conexiones de acceso, incluyendo redes LAN cableadas e inalámbricas, dialup, banda ancha, contenido, almacenamiento, VoIP, firewalls y VPNs proporciona una variedad de funciones avanzadas:

Monitoreo automático de servicio
Sincronización de la base de datos e importación de herramientas de despliegues de gran escala
Soporte de autenticación de usuario LDAP
Reporte de acceso administrativo y de usuario
Restricciones al acceso a la red basadas en criterios como la hora y el día de la semana
Perfiles de grupo de dispositivos y usuario



El ACS Seguro de Cisco es un componente importante de la arquitectura Identity Based Networking Services (IBNS) de Cisco. La IBNS de Cisco está basada en estándares de seguridad de puertos como IEEE 802.1X y Extensible Authentication Protocol (EAP) y extiende la seguridad desde el perímetro de la red a todos los puntos de conexión dentro de la LAN. Con esta nueva arquitectura, pueden desplegarse nuevas políticas de control, como cuotas por usuario, asignación de VLANs y ACLs (listas de control de acceso). Esto es posible gracias a las funciones extendidas de los switches y puntos de acceso inalámbricos de Cisco que los habilitan para consultar al ACS Seguro de Cisco a través del protocolo RADIUS.

El ACS Seguro de Cisco también es un componente importante del Control de Admisión a la Red de Cisco (NAC) de Cisco. El NAC de Cisco es una iniciativa industrial fomentada por Cisco. El NAC de Cisco usa la infraestructura de red para hacer cumplir la política de seguridad en todos los dispositivos que buscan acceso a los recursos de computación de la red. Esto limita el daño causado por virus y gusanos. Con el NAC de Cisco, los clientes pueden elegir permitir el acceso a la red solo a dispositivos de punto final confiables y que cumplan la política, restrigiendo el acceso de los dispositivos no confiables. NAC es parte de la iniciativa de Red Autodefensiva de Cisco (Cisco Self-Defending Network) y es la base de la habilitación de NAC en las redes de capa 2 y 3. Las fases futuras extienden la interoperación de la seguridad de red y de nodo para incluir funciones dinámicas de contención de inicidentes. Esta innovación permite a los elementos de sistemas que cumplen con la política reportar un mal uso que emane de sistemas infectados o malicioso durante un ataque. Los sistemas infectados pueden ser puestos en cuarentena del resto de la red dinámicamente para reducir significativamente la propagación de virus, gusanos y amenazas combinadas.



El ACS Seguro de Cisco tiene muchas funciones de alto rendimiento y escalabilidad:

Facilidad de uso - La interfaz de usuario basada en web simplifica y distribuye la configuración para perfiles de usuario, perfiles de grupo y configuración de ACS Seguro de Cisco.

Escalabilidad - El ACS Seguro de Cisco fue desarrollado con la capacidad de proporcionar soporte de servidores redundantes, bases de datos remotas y replicación de bases de datos y resguardo de datos a grandes redes.
Extensibilidad- El reenvió de autenticación LDAP soporta la autenticación de perfiles de usuario que se almacenan en directorios de marcas líderes de directorios, incluyendo Sun, Novell y Microsoft.
Administración - El soporte Microsoft Windows Active Directory consolida la administración Windows de nombre de usuario y contraseña y usa el Windows Performance Monitor para visualización de estadísticas en tiempo real.
Administración - Diferentes niveles de acceso para cada administrador del ACS Seguro de Cisco y la habilidad de agrupar dispositivos de red facilitan y flexibilizan el control del cumplimiento y cambios a la administración de la política de seguridad en todos los dispositivos de una red.
Flexibilidad del producto - Como el software IOS de Cisco tiene incorporado el soporte a AAA, el ACS Seguro de Cisco puede ser usado prácticamente en cualquier servidor de acceso a la red que sea vendido por Cisco (la versión del software IOS de Cisco debe soportar RADIUS o TACACS+). El ACS seguro de Cisco está disponible en tres opciones: Cisco Secure ACS Solution Engine, Cisco Secure ACS Express y Cisco Secure ACS para Windows.
Integración - La fuerte asociación con los routers IOS de Cisco y las soluciones VPN proporciona funciones como multichassis multilink PPP y autorización de comandos de software IOS de Cisco.
Soporte a terceros - El ACS Seguro de Cisco ofrece soporte de servidor token a cualquier empresa de contraseñas de una sola vez (one-time password - OTP) que proporcione una interfaz RADIUS que se atenga a las RFC, como RSA, PassGo, Secure Computing, ActiveCard, Vasco o CryptoCard.
Control - El ACS Seguro de Cisco proporciona cuotas dinámicas para restringir el acceso en base a la hora, el uso de la red, el número de sesiones iniciadas y el día de la semana.



El ACS Seguro de Cisco está disponible como software instalado en un Windows Server o en un servidor 1U asegurado y montable en rack, como el ACS Solution Engine o el ACS Express. Todos son ejemplos basados en servidor de cómo se proporcionan servicios AAA usando una base de datos de seguridad remota.

La opción de ACS Seguro de Cisco para Windows habilita los servicios AAA en un router para contactar un ACS Seguro de Cisco externo instalado en un sistema de servidor Windows para autenticación de usuario y administrador.

El Cisco Secure ACS Solution Engine es un dispositivo 1U montable en rack y asegurado con una licencia de ACS Seguro de Cisco preinstalada. Debe ser usado en grandes organizaciones en las que debe brindarse soporte a más de 350 usuarios. En comparación con el producto ACS Seguro de Cisco para Windows, Cisco Secure ACS Solution Engine reduce el costo total al eliminar la necesidad de instalar y mantener un servidor Microsoft Windows.

Cisco Secure ACS Express también es un dispositivo 1U montable en rack y asegurado que tiene una licencia de ACS Seguro de Cisco preinstalada. La diferencia es que la opción ACS Express está ideada para despliegues más pequeños, comerciales (de menos de 350 usuarios) y de oficinas secundarias o sucursales. ACS Express ofrece un grupo de funciones englobador pero simplificado, una GUI amigable con el usuario y un precio menor que permite a los administradores desplegar este producto en sutuaciones en las que Cisco Secure ACS para Windows Server o Cisco Secure ACS Solution Engine pueden no ser apropiados.

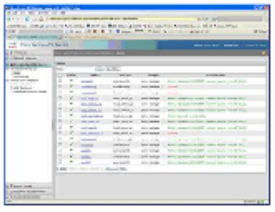
Aunque este capítulo se concentra en el despliegue de Cisco Secure ACS para Windows Server, los conceptos y funciones presentados también se encuentran disponibles en ACS Solution Engine y ACS Express.



Sistema Operativo ACS Seguro Cisco
- Windows 2000 Server con Service Pack 4
- Windows 2000 Advanced Server con Service Pack 4
- Windows Server 2003 Standard Edition
- Windows Server 2003 Enterprise Edition



Motor de solución Cisco Secure ACS
- Una plataforma dedicada altamente escalable que sirve como ACS de alto rendimiento.
- 1U, montada en un rack
- Preinstalada con software Windows con seguridad integrada, software ACS Seguro Cisco
- Soporta más de 350 usuarios



Cisco Secure ACS Express 5.0
- ACS de nivel de entrada con un conjunto de características limitadas
- Soporta hasta 50 dispositivos AAA y hasta 350 IDs usuario únicas en un período de 24 horas

3.3.4 Configuración del ACS seguro de Cisco

Antes de instalar el ACS Seguro de Cisco, es importante preparar el servidor. Deben considerarse los requerimientos de software del tercero, los requerimientos de red y puertos del servidor y los dispositivos AAA.

Requerimientos de software del tercero

Los productos de software mencionados en las notas de la versión son soportados para interoperabilidad por Cisco. Puede ser difícil obtener soporte para interoperabilidad con productos de software que no están mencionados en las notas de versión. La versión más reciente de las notas de versión del ACS Seguro de Cisco está disponible en Cisco.com.

Tenga en consideración que en la aplicación ACS Segura de Cisco, el cliente es un concentrador VPN, router, switch o firewall que usa los servicios de ese servidor.

Prerequisitos de red y puertos

La red debe cumplir ciertos requisitos específicos antes de que los administradores puedan comenzar a desplegar el ACS Seguro de Cisco:

Para un soporte completo de TACACS+ y RADIUS en los IOS de los dispositivos Cisco, los clientes AAA deben estar utilizando la versión 11.2 del IOS de Cisco o posterior.
Los dispositivos Cisco que no son clientes AAA del IOS de Cisco deben ser configurados con TACACS+, RADIUS o ambos.
Los clientes dial-in, VPN o inalámbricos deben poder conectarse a los clientes AAA aplicables.
La computadora que corre el ACS Seguro de Cisco debe poder alcanzar a todos los clientes AAA usando ping.
Los dispositivos gateway entre el ACS Seguro de Cisco y otros dispositivos en la red deben permitir la comunicación a través de los puertos necesarios para soportar la función o el protocolo aplicable.
Debe tenerse instalado un navegador web soportado en la computadora que ejecuta el ACS Seguro de Cisco. Para obtener la información más reciente sobre navegadores probados, vaya a las notas de versión del producto ACS Seguro de Cisco en Cisco.com.
Deben habilitarse todas las NICs en la computadora que ejecuta el ACS Seguro de Cisco. Si hay una tarjeta de red deshabilitada en la computadora que ejecuta el ACS Seguro de Cisco, la instalación del ACS Seguro de Cisco puede resultar lenta por retrasos causados por la Microsoft CryptoAPI.

Luego de haber instalado el ACS Seguro de Cisco exitosamente, debe realizarse una configuración inicial. La única manera de configurar un servidor ACS Seguro de Cisco es a través de una interfaz HTML.

Para acceder a la interfaz HTML del ACS Seguro de Cisco desde la computadora que está ejecutando el ACS Seguro de Cisco, use el ícono ACS Admin que aparece en el escritorio o ingrese la siguiente URL en un navegador web soportado: http://127.0.0.1:2002.

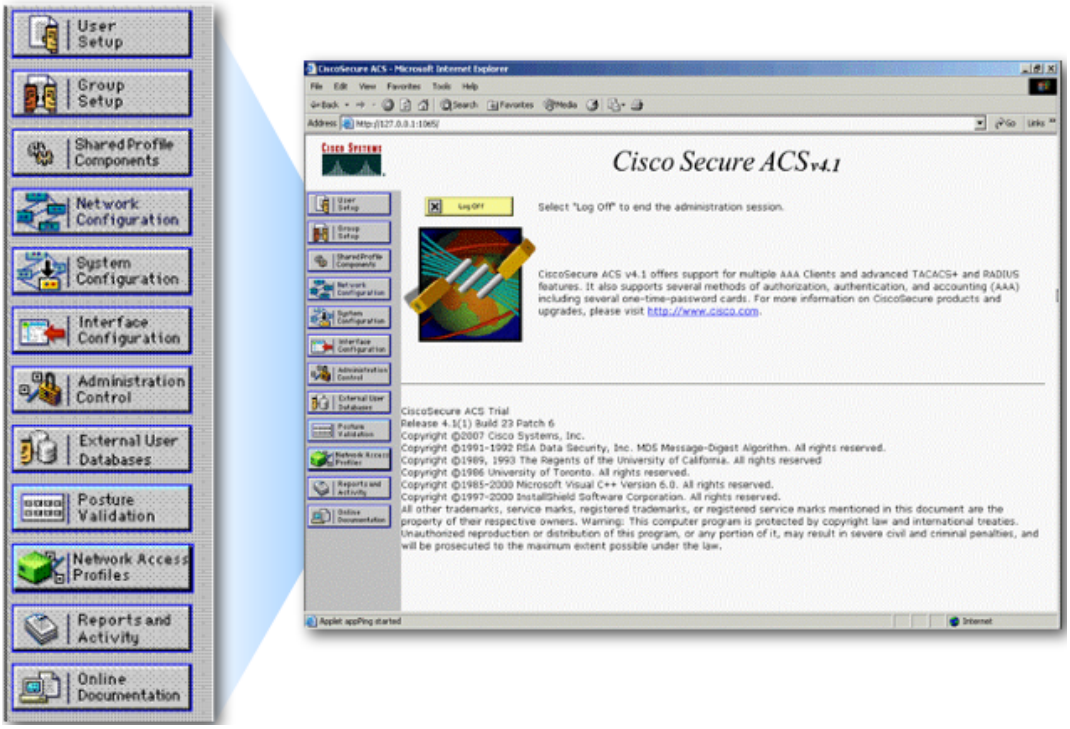
También puede accederse remotamente al ACS Seguro de Cisco luego de que se configura una cuenta de usuario administrador. Para acceder remotamente al ACS Seguro de Cisco, ingrese http://ip_address[hostname]:2002. Luego de la conexión inicial, se negocia un nuevo puerto dinámicamente.



La página de inicio del ACS Seguro de Cisco está dividida en marcos. Los botones de la barra de navegación representan áreas o funciones particulares que pueden ser configuradas:

Configuración de usuario
Configuración de grupo
Componentes de perfil compartido
Configuración de red
Configuración del sistema
Configuración de la interfaz
Control de administración
Bases de datos de usuarios externa
Validación de postura
Perfiles de acceso a la red
Reportes y actividad
Documentación en línea

Si no se muestran las opciones de RADIUS, debe añadirse el cliente AAA que usa el protocolo RADIUS. Adicionalmente, la configuración de interfaz es directamente afectada por los parámetros de la configuración de la red.



Antes de configurar un router, switch o firewall como cliente TACACS+ o RADIUS, el cliente AAA debe ser agregado al servidor y se deben especificar la dirección IP y la clave de cifrado. En la página de Configuración de Red (Network Configuration) se agregan, eliminan y modifican los clientes.

Para crear un cliente AAA, use la página de Configuración de Red:

Paso 1. Haga clic en Network Configuration en la barra de navegación. Aparecerá la página de Configuración de Red.

Paso 2. En la sección de clientes AAA, haga clic en Add Entry.

Paso 3. Ingrese el nombre de host del cliente en el campo AAA Client Hostname. Por ejemplo, ingrese el nombre del router que será el cliente AAA al servidor. En la aplicación ACS Segura de Cisco, el cliente es un router, switch, firewall o concentrador VPN que usa los servicios del servidor.

Paso 4. Ingrese la dirección IP en el campo AAA Client IP Address.

Paso 5. Ingrese la clave secreta que el cliente utiliza para el cifrado en el campo Shared Secret.

Paso 6. Elija el protocolo AAA apropiado de la lista desplegable Authenticate Using.

Paso 7. Complete los otros parámetros según se requiera.

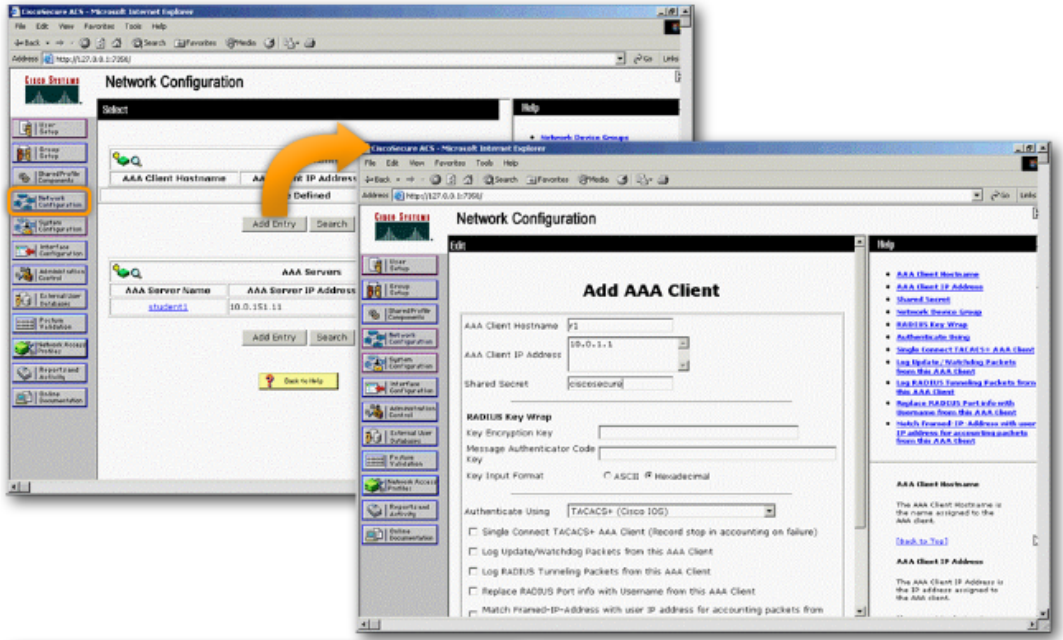
Paso 8. Haga clic en Submit and Apply.

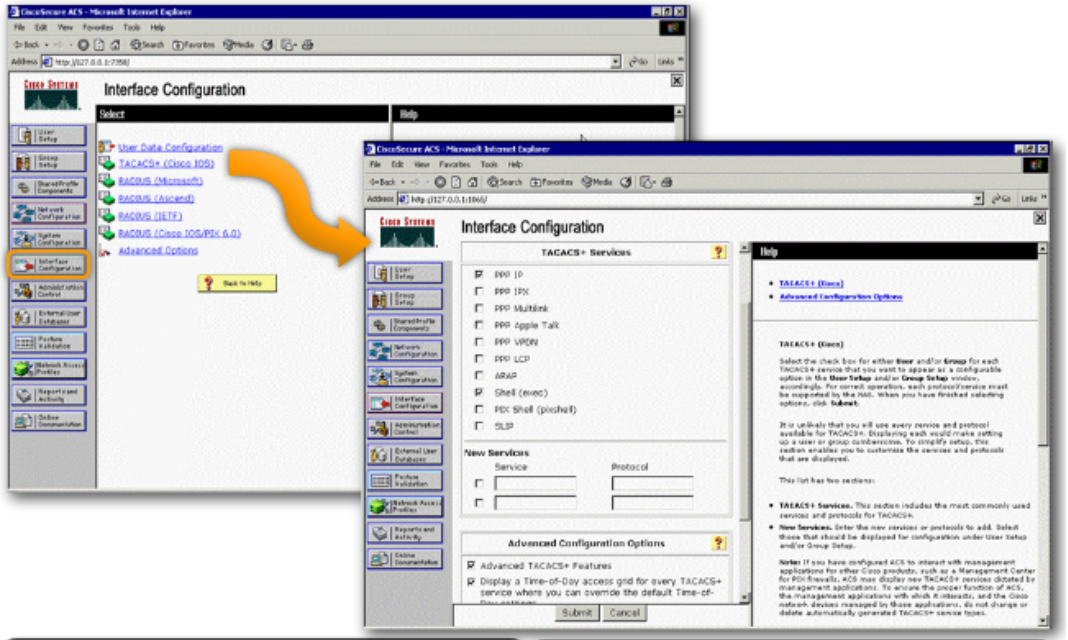
Las opciones disponibles en el botón de navegación de Configuración de Interfaz (Interface configuration) permiten al administrador controlar el despliegue de las opciones en la interfaz del usuario. Las opciones específicas desplegadas dependen de si se han agregado clientes TACACS+ o RADIUS al servidor:

Configuración de datos de usuario
TACACS+ (IOS de Cisco)
RADIUS (Microsoft)
RADIUS (Ascend)
RADIUS (IETF)
RADIUS (IOS/PIX)
Opciones avanzadas

El enlace User Data Configuration link permite a los administradores personalizar los campos que aparecen en las ventanas de configuración y setup del usuario. Los administradores pueden agregar campos como número de teléfono, lugar de trabajo, nombre del supervisor u otra información pertinente.

El enlace TACACS+ (IOS de Cisco) permite al administrador configurar los parámetros de TACACS+ y agregar nuevos servicios TACACS+. Los administradores también pueden configurar opciones avanzadas que afectan lo que se muestra en la interfaz de usuario.





Haga clic en cada botón para ver el contenido asociado.

El ACS Seguro de Cisco puede ser configurado para reenviar la autenticación de los usuarios a una o más bases de datos externas. El soporte para bases de datos de usuario externas significa que el ACS Seguro de Cisco no requiere una duplicación de las entradas para su creación en la base de datos de usuario. En las organizaciones en las que ya existe una base de datos de usuarios sustancial, como un ambiente Active Directory, el ACS Seguro de Cisco puede aprovechar el trabajo ya invertido construyendo la base de datos sin intervenciones adicionales.

En la mayoría de las configuraciones de bases de datos, salvo las bases de datos de Windows, el ACS Seguro de Cisco soporta solo una instancia de nombre de usuario y contraseña. Si se configura el ACS Seguro de Cisco para que use múltiples bases de datos de usuarios con nombres de usuario comunes almacenados en cada una, tenga cuidado con las configuraciones de las baes de datos. La primera base de datos que coincida con las credenciales de autenticación del usuario será la única que el ACS Seguro de Cisco usará para ese usuario. Por esta razón, es aconsejable que solo exista una instancia de un nombre de usuario en todas las bases de datos externas.

Use el botón External User Databases para configurar el ACS Seguro de Cisco para acceder a las bases de datos externas:

Paso 1. Haga clic en el botón External User Databases de la barra de navegación. Aparecerá la ventana External User Databases con los siguientes enlaces:

Unknown User Policy - (Política de usuario desconocida) Configura el procedimiento de autenticación para usuarios que no están en la base de datos del ACS Seguro de Cisco.
Database Group Mappings - (Mapeos de grupos en bases de datos) Configura qué privilegios de usuario heredan los usuarios de bases de datos externas cuando el ACS

Seguro de Cisco los autentica. En la mayoría de los casos, cuando un usuario es autenticado por medio de na base de datos de usuarios externa, los privilegios son extraídos del ACS Seguro de Cisco y no de la base de datos externa.

Database Configuration - (Configuración de bases de datos) Define los servidores externos con los que trabajará el ACS Seguro de Cisco.

Paso 2. Haga clic en Database Configuration. Aparecerá el panel External User Database Configuration, mostrando las siguientes opciones:

RSA SecurID Token Server
RADIUS Token Server
External ODBC Database
Windows Database
LEAP Proxy RADIUS Server
Generic LDAP

Paso 3. Para usar la base de datos de Windows como base de datos externa, haga clic en Windows Database. Aparecerá el panel Windows External User Database Configuration.

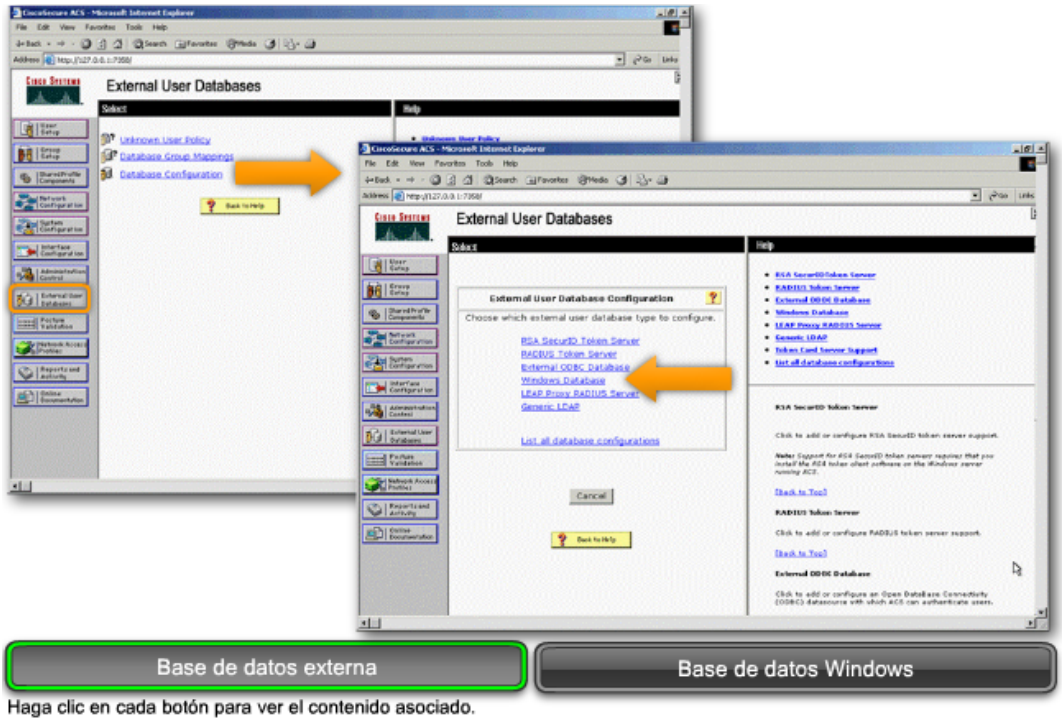
a configuración de base de datos externa de Windows tiene más opciones que otras configuraciones de bases de datos externas. Como el ACS Seguro de Cisco es nativo del sistema operativo Windows, los administradores pueden configurar funciones adicionales en el panel Windows External User Database Configuration.

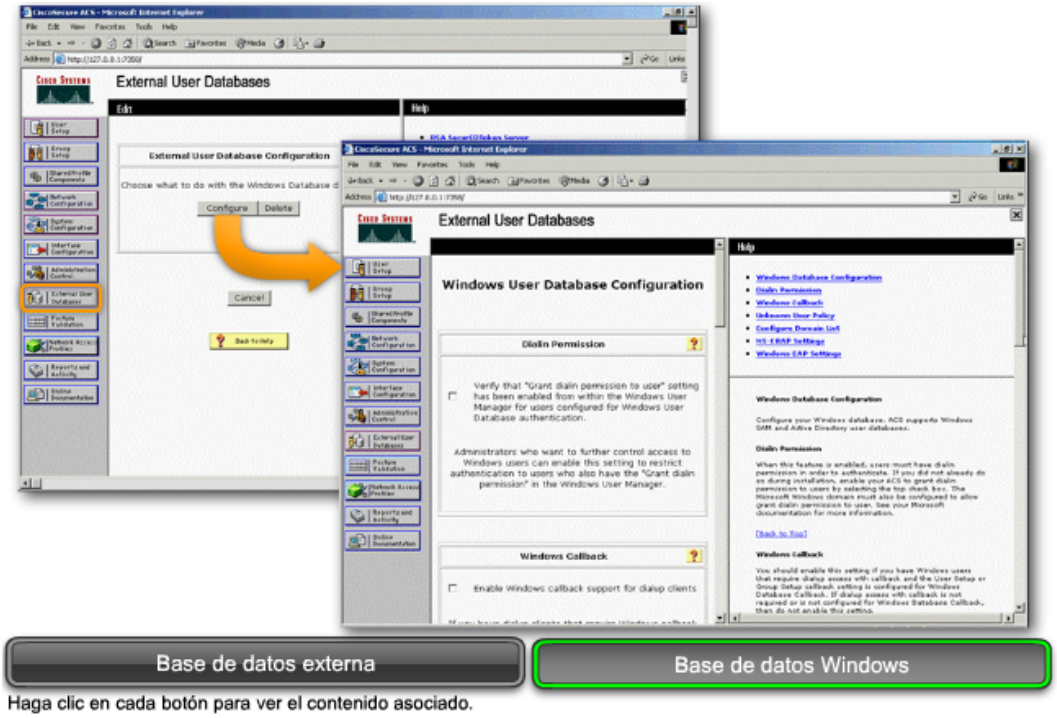
Paso 4. Para configurar las funciones adicionales de la base de datos de Windows, haga clic en Configure en el panel External User Database Configuration. Aparecerá la ventana Windows User Database Configuration.

Paso 5. Si se requiere mayor control sobre quién puede autenticarse a la red, se puede configurar la opción de permiso de Dialin. En la sección Dialin Permission, marque la casilla Verify that "Grant dialin permission to user" setting has been enabled from within the Windows User Manager for users configured for Windows User Database authentication. Además, asegúrese de que la casilla Grant dialin permission esté marcada en el perfil Windows dentro de Windows Users Manager.

La opción Dialin Permissions en el ACS Seguro de Cisco se aplica a más que solo las conexiones dialup. Si un usuario tiene esta opción marcada, se aplica a cualquier acceso que el usuario intente.

Otra opción que puede ser configurada usando la base de datos externa de Windows es el mapeo de bases de datos a dominios. El mapeo permite al administrador tener el mismo nombre de usuario en diferentes dominios, todos con diferentes contraseñas.





3.3.5 Configuracion de usuarios y grupos en el ACS seguro de Cisco

Luego de que se ha configurado el ACS Seguro de Cisco para comunicarse con una base de datos de usuarios externa, puede configurarse para autenticar usuarios con la base de datos de usuarios externa de alguna de estas dos maneras:

Por medio de la asignación específica de usuarios - Autentica a usuarios específicos con una base de datos externa.

Por medio de una política de usuarios desconocidos - Usa una base de datos externa para autenticar a los usuarios que no se hallan en la base de datos de usuario del ACS Seguro de Cisco. Este método no requiere que los administradores definan usuarios en la base de datos del ACS Seguro de Cisco.

Use el enlace External User Databases para configurar la política de usuarios desconocidos:

Paso 1. En la barra de navegación, haga clic en External User Databases.

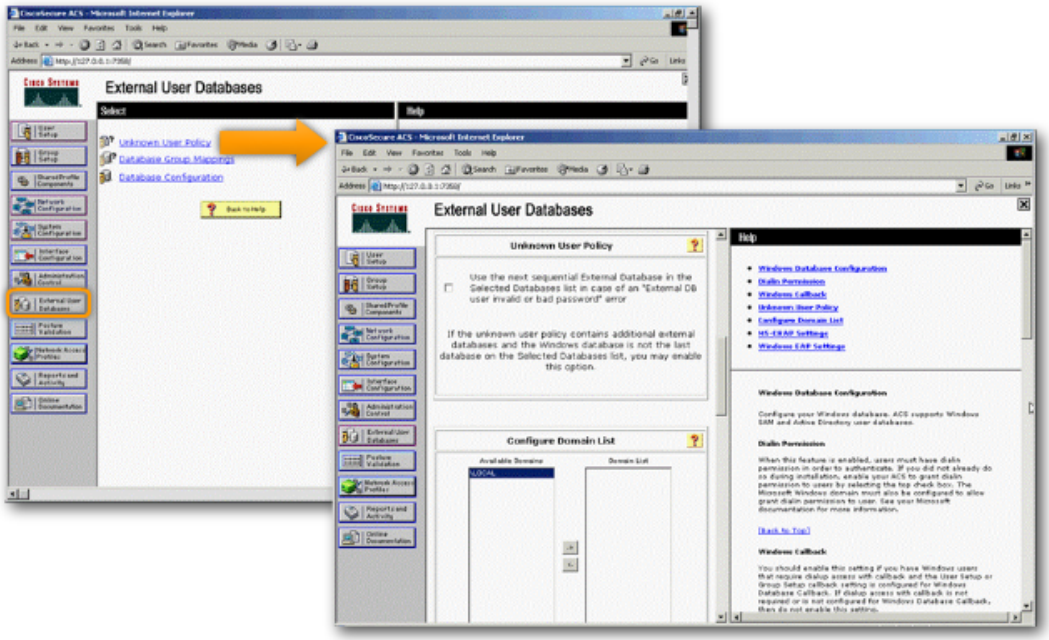
Paso 2. Haga clic en Unknown User Policy.

Paso 3. Habilite la política de usuarios desconocidos marcando la casilla en la sección Unknown User Policy.

Paso 4. Por cada base de datos a la que los administradores quieran que el ACS Seguro de Cisco tenga acceso para usarla al intentar autenticar usuarios desconocidos, vaya a la base de datos en la lista External Databases y haga clic en el botón de la flecha derecha para moverla a la lista Selected Databases. Para eliminar una base de datos de la lista Selected Databases, vaya a la base de datos y haga clic en el botón de la flecha izquierda para moverla de vuelta a la lista External Databases.

Paso 5. Para asignar el orden en el que el ACS Seguro de Cisco revisa las bases de datos externas al intentar autenticar a un usuario desconocido, haga clic en el nombre de una base de datos en la lista Selected Databases y haga clic en Up o Down para moverla a la posición deseada. Ubique las bases de datos que probablemente autenticarán usuarios desconocidos al principio de la lista.

Paso 6. Haga clic en Submit.



Cuando un usuario es autenticado por medio de una base de datos externa, la autorización que toma lugar es determinada por el ACS Seguro de Cisco. Esto puede complicar las cosas porque los usuarios que son autenticados por un servidor Windows pueden requerir una autorización diferente que los usuarios autenticados por un servidor LDAP.

A causa de esta necesidad potencial de autorizaciones diferentes, será necesario ubicar a los usuarios autenticados por el servidor Windows en un grupo y a los usuarios autenticados por el servidor LDAP en otro grupo. Para hacer esto, use mapeo de grupos de bases de datos.

Los mapeos de grupos de bases de datos permiten al administrador mapear un servidor de autenticación, como LDAP, Windows, ODBC y otros, a un grupo que ha sido configurado en el ACS Seguro de Cisco. En algunas bases de datos, el usuario solo puede pertenecer a un grupo. En otras, como LDAP y Windows, es posible el soporte de mapeo de grupos por miembros de grupos de bases de datos externas.

Una de las opciones que puede ser configurada en un grupo es la autorización de comandos por grupo, que usa el ACS Seguro de Cisco para autorizar qué comandos del router puede ejecutar un usuario que pertenece a un grupo. Por ejemplo, puede permitirse al grupo ejecutar cualquier comando de router salvo show running-config.

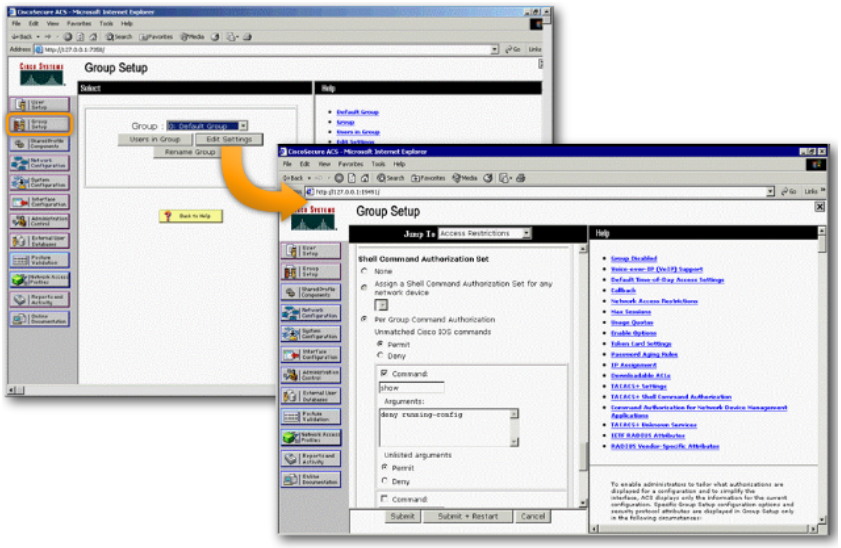
Paso 1. Haga clic en Group Setup en la barra de navegación.

Paso 2. Vaya al grupo a editar, por ejemplo, el grupo Default, y haga clic en Edit Settings.

Paso 3. Haga clic en Permit en la opción Unmatched Cisco IOS commands.

Paso 4. Marque la casilla Command e ingrese show en la casilla de texto. En la casilla de texto Arguments, ingrese deny running-config.

Paso 5. En la opción Unlisted Arguments, haga clic en Permit.



Agregar una cuenta de usuario y configurar el acceso del usuario son tareas críticas del ACS Seguro de Cisco:

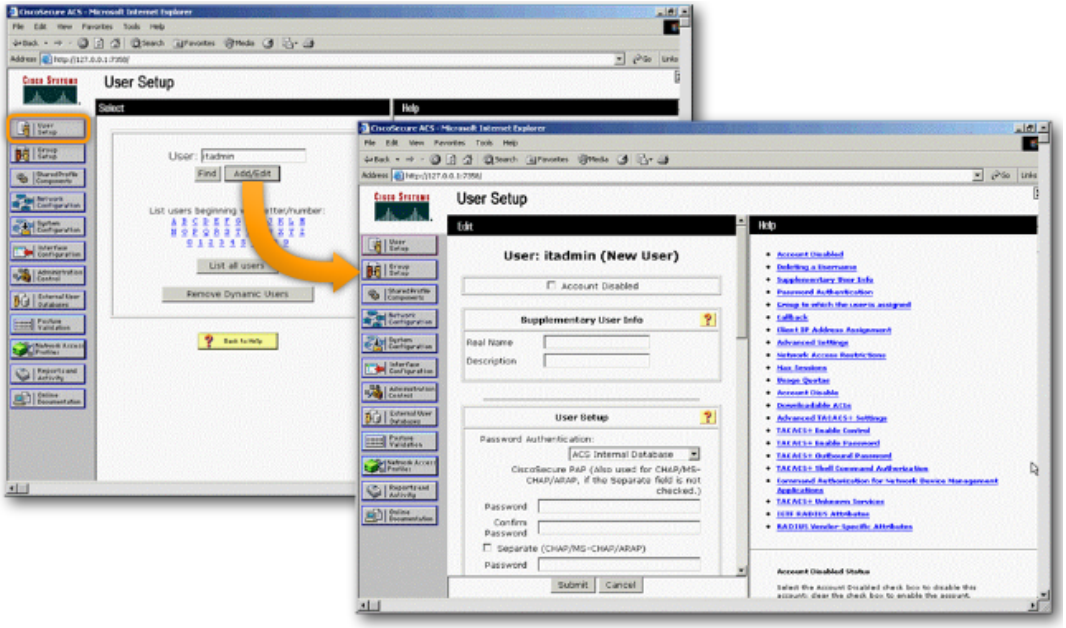
Paso 1. Haga clic en User Setup en la barra de navegación.

Paso 2. Ingrese un nombre de usuario en el campo User y haga clic en Add/Edit.

Paso 3. En el panel Edit, ingrese datos en los campos para definir la cuenta del usuario. Algunos de los campos generalmente necesarios son los campos de contraseña del usuario, TACACS+ enable control, TACACS+ enable password y comandos autorizados de shell de TACACS+.

Paso 4. Haga clic en Submit.

Si hay propiedades del usuario que son necesarias y no puede ver, verifique la configuración de interfaz. Para modificar la interfaz de usuario, vaya a Interface Configuration > User Data Configuration.



3.4.1 Configuracion de la autenticación de AAA basado en servidor con CLI

A diferencia de la autenticación AAA local, AAA basado en servidor debe identificar varios servidores TACACS+ y RADIUS que el servicio AAA debe consultar al autenticar y autorizar usuarios.

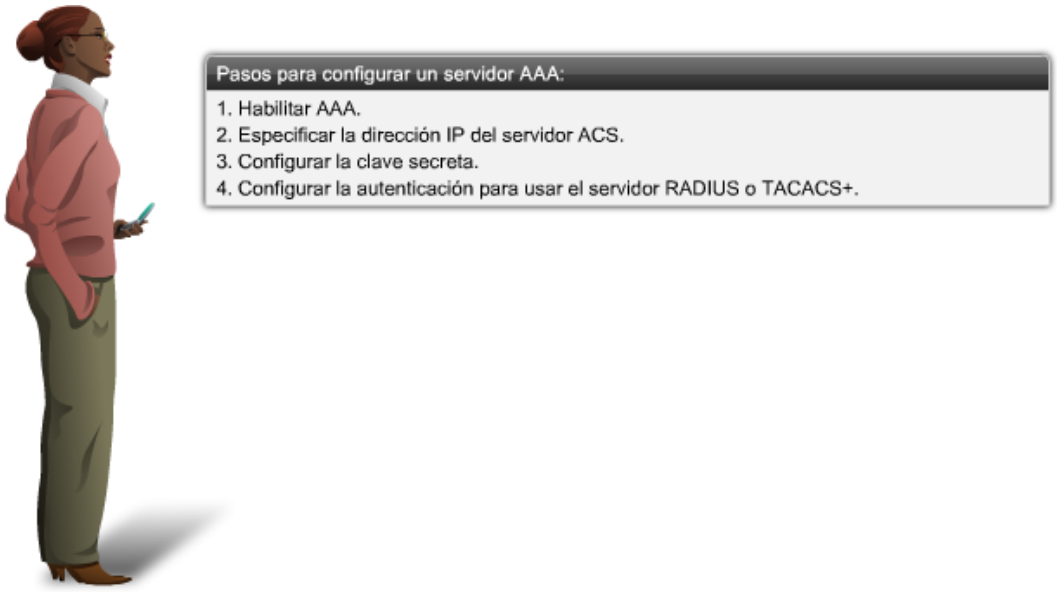
Hay algunos pasos básicos requeridos para configurgar la autenticación basada en servidor:

Paso 1. Habilite AAA globalmente para permitir el uso de todos los elementos AAA. Este paso es un prerequisito de todos los otros comandos AAA.

Paso 2. Especifique el ACS Seguro de Cisco que proporcionará servicios AAA al router. Este puede ser un servidor TACACS+ o RADIUS.

Paso 3. Configure la clave de cifrado necesaria para cifrar la transferencia de datos entre el servidor de acceso a la red y el ACS Seguro de Cisco.

Paso 4. Configure la lista de métodos de autenticación AAA para referirse al servidor TACACS+ o RADIUS. Para redundancia, es posible configurar más de un servidor.



Configuración de un servidor TACACS+ y clave de cifrado

Para configurar un servidor TACACS+, use el comando tacacs-server host dirección-ip single-connection.

La palabra clave single-connection mejora el rendimiento de TCP al mantener una sola conexión TCP durante el tiempo que dura la sesión. De otra manera, por defecto, se abre y cierra una conexión TCP por cada sesión. Si se solicita, se pueden identificar múltiples servidores TACACS+ por medio de sus respectivas direcciones IP usando el comando tacacs-server host.

A continuación, use el comando tacacs-server key clave para configurar la clave secreta compartida para cifrar la transferencia de datos entre el servidor TACACS+ y el router habilitado para AAA. Esta clave debe ser configurada exactamente igual en el router y el servidor TACACS+.

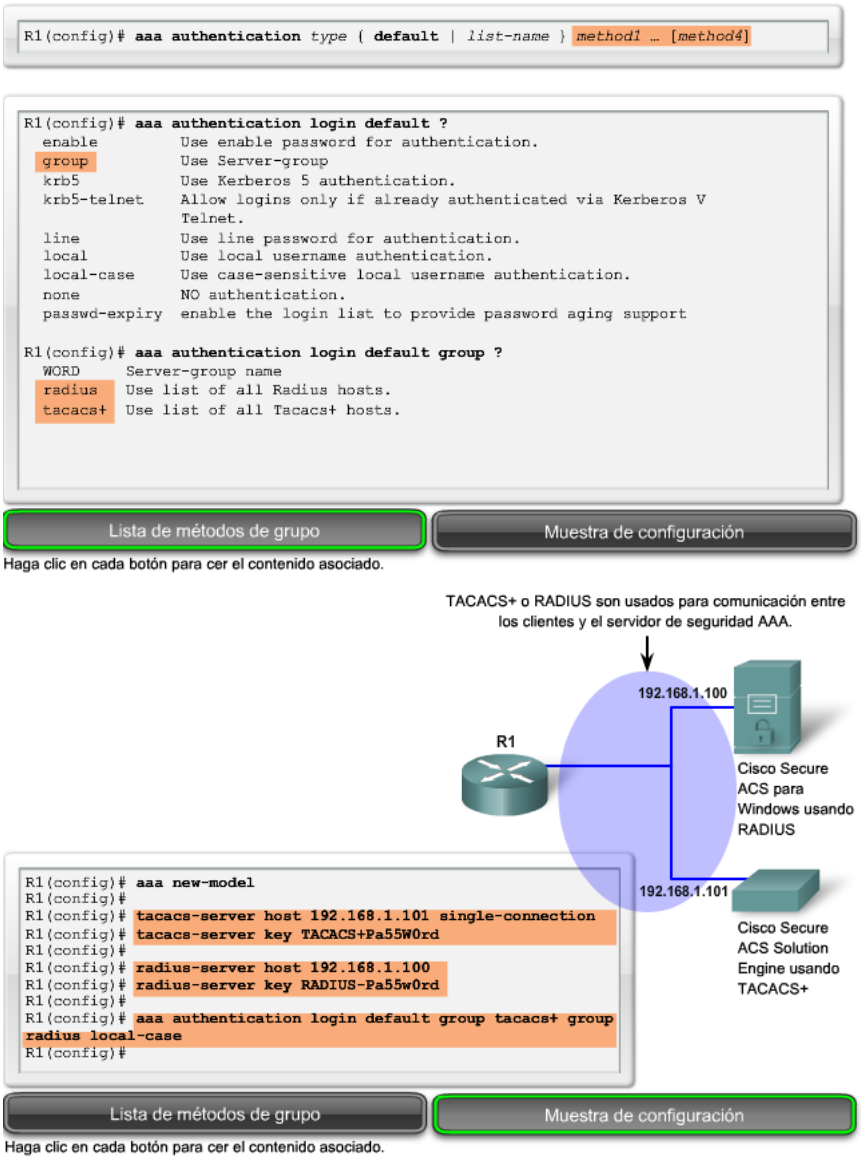
Configuración de un servidor RADIUS y clave de cifrado

Para configurar un servidor RADIUS, use el comando radius-server host dirección-ip. Como RADIUS usa UDP, no hay palabra clave equivalente a single-connection. Si se solicita, se pueden indentificar múltiples servidores RADIUS con el comando radius-server host para cada servidor.

Para configurar la clave secreta compartida para el cifrado de la contraseña, use el comando radius-server key clave. Esta clave debe ser configurada exactamente igual en el router y en el servidor RADIUS.

Configuración de autenticación para usar el servidor AAA

Una vez que se han identificado los servidores de seguridad AAA, los servidores deben ser incluidos en la lista de métodos del comando aaa authentication login. Los servidores AAA se identifican por medio de las palabras clave group tacacs+ o group radius. Por ejemplo, para configurar una lista de métodos para el ingreso por defecto para autenticar usando un servidor RADIUS, un servidor TACACS+o una base de datos de nombres de usuario local, use el comando aaa authentication login default group radius group tacacs+ local-case.



3.4.2 Configuracion de la autenticación AAA basada en servidor con SDM

Al usar SDM para soportar TACACS+, es necesario especificar una lista de servidores ACS Seguros de Cisco disponibles que proporcionen servicios TACACS+ al router:

Paso 1. Desde la página de inicio del SDM de Cisco, vaya a Configure > Additional Tasks > AAA > AAA Servers and Groups > AAA Servers.

Paso 2. Desde el panel AAA Servers, haga clic en Add. Aparecerá la ventana Add AAA Server. Vaya a TACACS+ en la lista Server Type.

Paso 3. Ingrese la dirección IP o nombre de host del servidor AAA en el campo Server IP or Host. Si el router no ha sido configurado para usar un servidor DNS, ingrese la dirección IP de un servidor DNS.

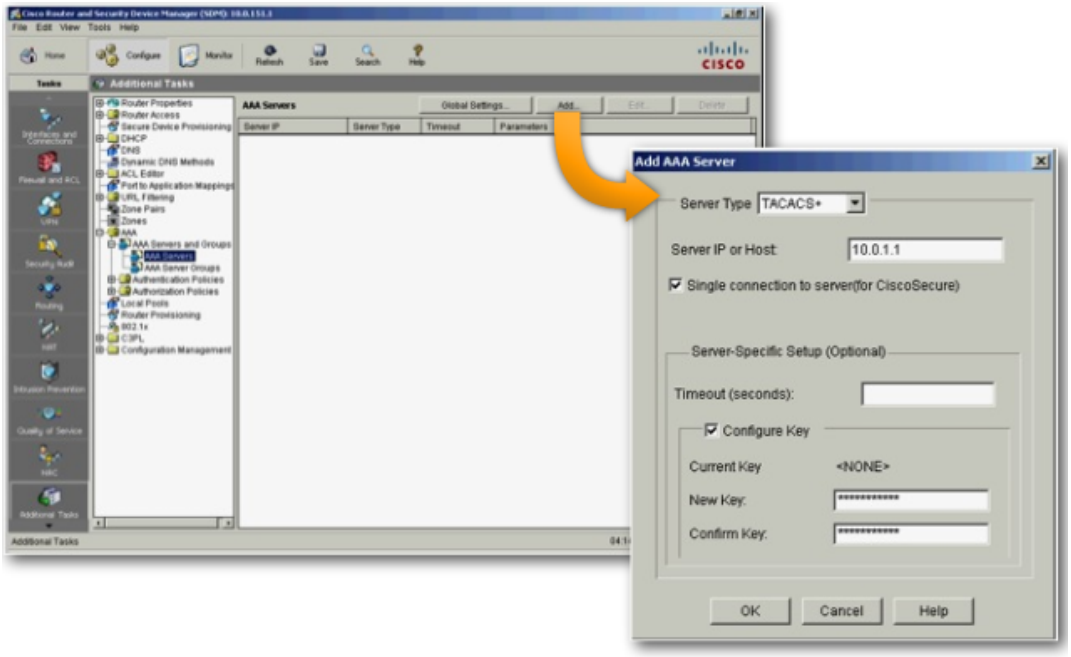
Paso 4. Puede configurarse el router para mantener una sola conexión abierta al servidor TACACS+ en lugar de abrir y cerrar conexiones TCP cada vez que se comunica con el servidor. Para hacer esto, marque la casilla Single Connection to Server.

Paso 5. Para invalidar los parámetros globales de servidores AAA y especificar un valor de vencimiento específico para el servidor, ingrese en la sección Server-Specific Setup un valor en el campo Timeout (seconds). Este campo determina el tiempo que el router esperará una respuesta del servidor antes de acudir al siguiente servidor en la lista de grupo. Si no se ingresa un valor, el router usará el valor configurado en la ventana AAA Servers Global Settings. El tiempo por defecto es de cinco segundos.

Paso 6. Para configurar una clave específica para el servidor, marque la casilla Configure Key e ingrese la clave que se usa para cifrar el tráfico entre el router y este servidor en el campo New Key. Reingrese la clave en el campo Confirm Key para confirmar. Si esta opción no se marca y no se ingresa un valor, el router usará el valor configurado en la ventana AAA Servers Global Settings.

Paso 7. Haga clic en OK.

El comando CLI ejemplo que el SDM de Cisco generaría basado en un servidor TACACS+ en la dirección IP 10.0.1.1 y con la clave TACACS+Pa55w0rd sería tacacs-server host 10.0.1.1 key TACACS+Pa55w0rd.



Luego de que se ha habilitado AAA y se han configurado los servidores TACACS+, el router puede ser configurado para usar el servidor ACS Seguro de Cisco para autenticar el acceso de los usuarios al router. Par configurar el router para que use el servidor ACS Seguro de Cisco para autenticación de inicio de sesión, debe crearse una lista de métodos de autenticación definida por el usuario. También puede editarse la lista de métodos por defecto. Tenga en consideración que la lista de métodos por defecto se aplica automáticamente a todas las interfaces y líneas, excepto aquéllas que tengan una lista de métodos definida por el usuario aplicada explícitamente.

El administrador puede usar el SDM de Cisco para configurar una lista de métodos de autenticación definida por el usuario:

Paso 1. En la página de inicio del SDM de Cisco, vaya a Configure > Additional Tasks > AAA > Authentication Policies > Login.

Paso 2. En el panel Authentication Login, haga clic en Add.

Paso 3. Para crear un nuevo método de autenticación, vaya a User Defined en la lista desplegable Name.

Paso 4. Ingrese el nombre de la lista de métodos de autenticación en el campo Specify, por ejemplo TACACS_SERVER.

Paso 5. Haga clic en Add para definir los métodos que usará esta política. Aparecerá la ventana Select Method List(s) for Authentication Login.

Paso 6. Vaya a group tacacs+ en la lista de métodos.

Paso 7. Haga clic en OK para agregar group tacacs+ a la lista de métodos y vuelva a la ventana Add a Method List for Authentication Login.

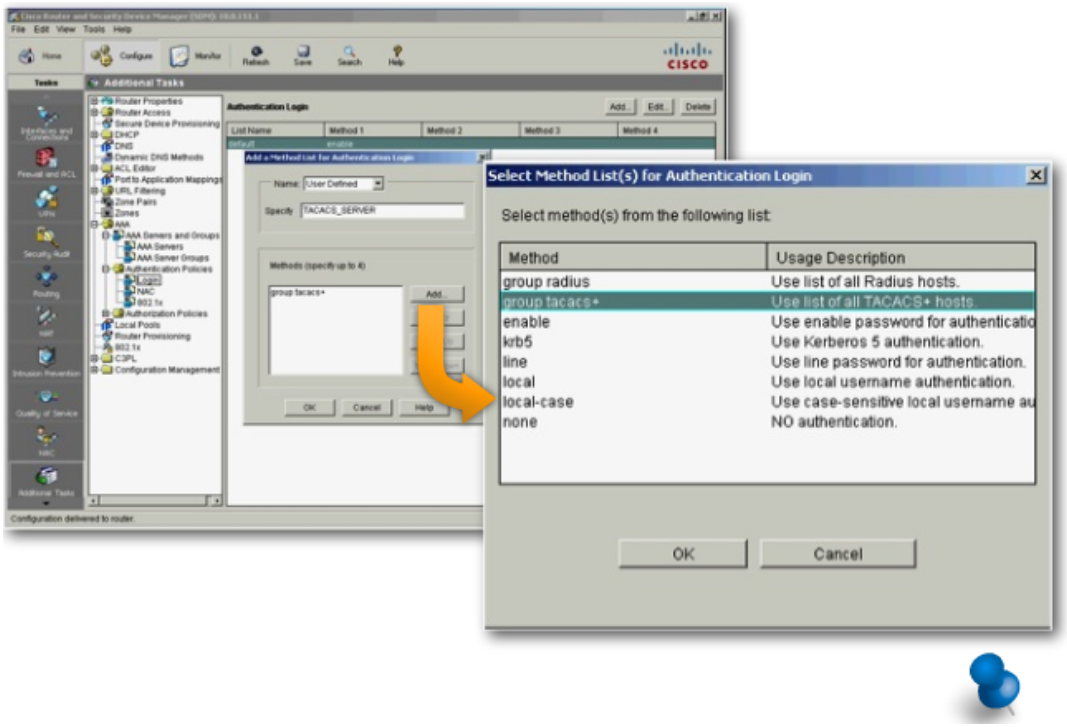
Paso 8. Haga clic en Add para agregar un método de resguardo a esta política. Aparecerá la ventana Select Method List(s) for Authentication Login.

Paso 9. Vaya a enable en la lista de métodos para usar la contraseña enable como método de autenticación de resguardo.

Paso 10. Haga clic en OK para agregar enable a la lista de métodos y vuelva a la ventana Add a Method List for Authentication Login.

Paso 11. Haga clic en OK para agregar la lista de métodos de autenticación y vuelva a la pantalla Authentication Login.

El comando CLI resultante que generará el SDM de Cisco será aaa authentication login TACACS_SERVER group tacacs+ enable.



Una vez que se han creado las listas de métodos de autenticación, aplique las listas a las líneas e interfaces del router.

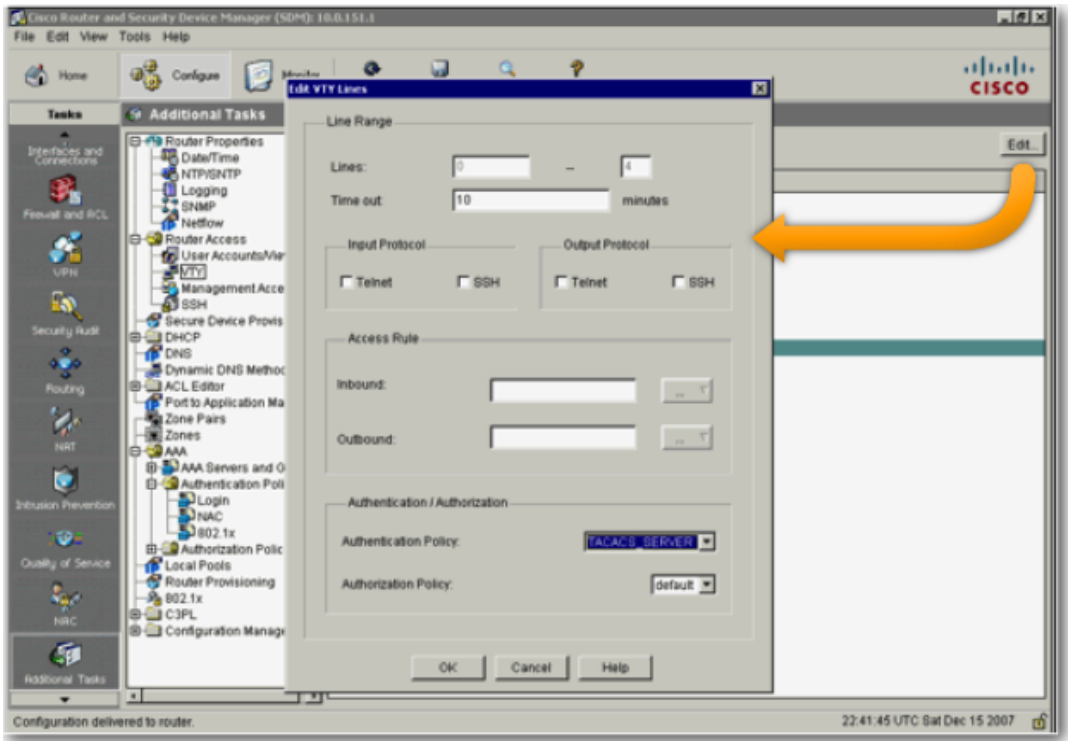
Puede usarse SDM para aplicar una política de autenticación a una línea del router:

Paso 1. Vaya a Configure > Additional Tasks > Router Access > VTY.

Paso 2. En la ventana VTY Lines window, haga clic en el botón Edit para efectuar cambios a las líneas vty. Aparecerá la ventana Edit VTY Lines.

Paso 3. En la casilla que contiene la lista Authentication Policy, elija la política de autenticación que aplicará a las líneas vty. Por ejemplo, la aplicación de la política de autenticación llamada TACACS_SERVER a las líneas vty 0 a 4 resulta en el comando CLI login authentication TACACS_SERVER.

También puede usarse CLI para aplicar una política de autenticación a las líneas o interfaces con el comando login authentication {default | nombre-lista} en el modo de configuración de línea o en el modo de configuración de interfaz.



3.4.3 Resolucion de problemas en la autenticación AAA basada en servidor

Cuando AAA está habilitado, generalmente es necesario monitorear el tráfico de autenticación y resolver problemas de configuración.

El comando debug aaa authentication es útil para la resolución de problemas porque proporciona una vista de alto nivel de la actividad de inicios de sesión.

El comando indica un mensaje de estado PASS cuando el intento de inicio de sesión TACACS+ es exitoso. Si el mensaje de estado que se muestra es FAIL, verifique la clave secreta.

```
R1# debug aaa authentication
AAA Authentication debugging is on
R1#
14:01:17: AAA/AUTHEN (567936829): Method=TACACS+
14:01:17: TAC+: send AUTHEN/CONT packet
14:01:17: TAC+ (567936829): received authen response status = PASS
14:01:17: AAA/AUTHEN (567936829): status = PASS
```

Otros dos comandos muy útiles al resolver problemas en AAA basado en servidor son el comando debug tacacs y el comando debug radius. Estos comandos pueden ser

usados para proporcionar información de debugging de AAA más detallada. Para deshabilitar la salida del debugging, use la forma no de estos comandos.

De forma similar al comando debug aaa authentication, el comando debug tacacs también indica mensajes de estado PASS o FAIL.

Para visualizar todos los mensajes TACACS+, use el comando debug tacacs. Para obtener resultados más precisos y visualizar información del proceso ayudante de TACACS+, use el comando debug tacacs events en modo EXEC privilegiado. El comando debug tacacs events muestra la apertura y cierre de una conexión TCP a un servidor TACACS+, los bytes leídos y escritos en la conexión y el estado TCP de la conexión. Use el comando debug tacacs events con precaución, ya que puede generar una cantidad sustanciosa de salida. Para deshabilitar la salida del debugging, use la forma no del comando.



```
R1# debug tacacs ?
  accounting      TACACS+ protocol accounting
  authentication  TACACS+ protocol authentication
  authorization   TACACS+ protocol authorization
  events          TACACS+ protocol events
  packet          TACACS+ packets
  <cr>
```

debug radius | debug tacacs | Status PASS | Status FAIL

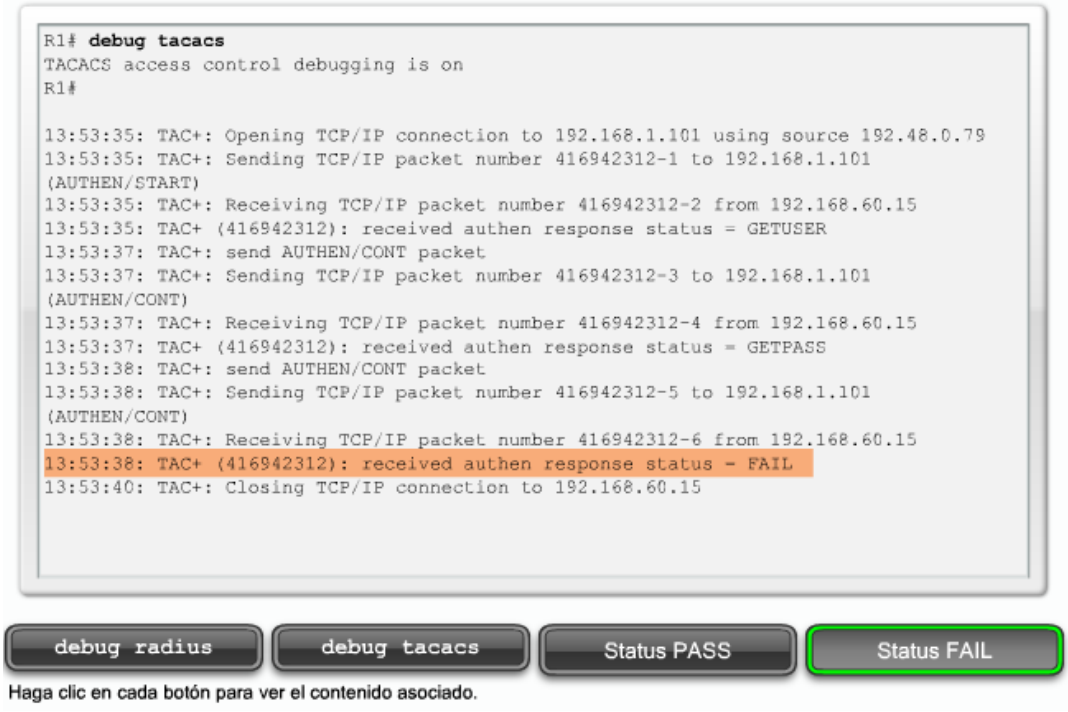
Haga clic en cada botón para ver el contenido asociado.

```
R1# debug tacacs
TACACS access control debugging is on
R1#

14:00:09: TAC+: Opening TCP/IP connection to 192.168.1.101 using source 10.116.0.79
14:00:09: TAC+: Sending TCP/IP packet number 383258052-1 to 192.168.1.101
(AUTHEN/START)
14:00:09: TAC+: Receiving TCP/IP packet number 383258052-2 from 192.168.60.15
14:00:09: TAC+ (383258052): received authen response status = GETUSER
14:00:10: TAC+: send AUTHEN/CONT packet
14:00:10: TAC+: Sending TCP/IP packet number 383258052-3 to 192.168.1.101
(AUTHEN/CONT)
14:00:10: TAC+: Receiving TCP/IP packet number 383258052-4 from 192.168.60.15
14:00:10: TAC+ (383258052): received authen response status = GETPASS
14:00:14: TAC+: send AUTHEN/CONT packet
14:00:14: TAC+: Sending TCP/IP packet number 383258052-5 to 192.168.1.101
(AUTHEN/CONT)
14:00:14: TAC+: Receiving TCP/IP packet number 383258052-6 from 192.168.60.15
14:00:14: TAC+ (383258052): received authen response status = PASS
14:00:14: TAC+: Closing TCP/IP connection to 192.168.60.15
```

debug radius | debug tacacs | Status PASS | Status FAIL

Haga clic en cada botón para ver el contenido asociado.



3.5.1 Configuracion de autorización de AAA basado en servidor

Mientras que la autenticación se ocupa de asegurarse de que el dispositivo o usuario final sea el que dice ser, la autorización se ocupa de permitir y prohibir acceso a ciertas áreas y programas de la red a los usuarios autenticados.

El protocolo TACACS+ permite la separación de la autenticación de la autorización. Puede configurarse el router para no permitir al usuario realizar ciertas funciones luego de una autenticación exitosa. La autorización puede configurarse tanto para el modo carácter (autorización exec) como para el modo paquete (autorización de red). Tenga en consideración que RADIUS no separa los procesos de autenticación y autorización.

Otro aspecto importante de la autorización es la habilidad de controlar el acceso de los usuarios a servicios específicos. El control del acceso a comandos de configuración simplifica enormemente la seguridad de la infraestructura en grandes redes empresariales. Los permisos por usuario en el ACS Seguro de Cisco simplifican la configuración de los dispositivos de red.

Por ejemplo, puede permitirse a un usuario autorizado acceder al comando show version pero no al comando configure terminal. El router pide permiso al ACS para ejecutar los comandos en nombre del usuario. Cuando el usuario emite el comando show version, el ACS envía una respuesta ACCEPT. Si el usuario emite el comando configure terminal, el ACS envía una respuesta REJECT.

Por defecto, TACACS+ establece una nueva sesión TCP por cada petición de autorización, lo que puede llevar a retrasos cuando los usuarios emiten comandos. El ACS Seguro de Cisco soporta sesiones TCP persistentes para mejorar el rendimiento.

Para configurar la autorización de los comandos, use el comando aaa authorization {network | exec | commands nivel} {default | nombre-lista} método1...[método4]. El tipo de servicio puede especificar los tipos de comandos o servicios:

commands nivel para comandos exec (shell)

exec para comenzar un exec (shell)

network para servicios de red (PPP, SLIP, ARAP)

Cuando la autorización AAA no está habilitada, se permite acceso sin restricciones a todos los usuarios. Luego de que inicia la autenticación, por defecto no se permite acceso a nadie. Esto significa que el administrador debe crear un usuario con derechos de acceso sin restricciones antes de que se habilite la autorización: no hacerlo deja al administrador sin forma de ingresar al sistema al momento en que ingresa el comando aaa authorization. La única manera de recuperarse de esto es reiniciar el router. Si es un router de producción, reiniciarlo puede no ser una opción. Asegúrese de que al menos un usuario tiene derechos de acceso sin restricciones.

```
R1(config)# aaa authorization {network | exec | commmands level}
{default | list-name} method1…[method4]
```

```
R1(config)# aaa authorization exec ?
  WORD     Named authorization list.
  default  The default authorization list.

R1(config)# aaa authorization exec default
```

Tipo de lista | Lista de método | Muestra de configuración

Haga clic en cada botón para ver el contenido asociado.

```
R1(config)# aaa authorization {network | exec | commmands level}
{default | list-name} method1…[method4]
```

```
R1(config)# aaa authorization exec default ?
  group             Use server-group.
  if-authenticated  Succeed if user has authenticated.
  krb5-instance     Use Kerberos instance privilege maps.
  local             Use local database.
  none              No authorization (always succeeds).

R1(config)# aaa authorization exec default group ?
  WORD      Server-group name
  radius    Use list of all Radius hosts.
  tacacs+   Use list of all Tacacs+ hosts.
```

Tipo de lista | Lista de método | Muestra de configuración

Haga clic en cada botón para ver el contenido asociado.




```
R1# conf t
R1(config)# username JR-ADMIN secret Str0ngPa55w0rd
R1(config)# username ADMIN secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authentication login default group tacacs+
R1(config)# aaa authorization exec default group tacacs+
R1(config)# aaa authorization network default group tacacs+
```

Tipo de lista | Lista de método | Muestra de configuración

Haga clic en cada botón para ver el contenido asociado.

Para configurar el router para que use el servidor ACS Seguro de Cisco para autorización, cree una lista de métodos de autorización definida por el usuario o edite la lista de métodos de autorización por defecto. La lista de métodos de autorización por defecto se aplica automáticamente a todas las interfaces excepto aquéllas que tengan una lista de métodos de autorización definida por el usuario explícitamente aplicada. La lista de métodos de autorización definida por el usuario invalida la lista de métodos de autorización por defecto.

El SDM de Cisco puede ser usado para configurar la lista de métodos de autorización por defecto para el acceso de modo carácter (exec):

Paso 1. Desde la página de inicio del SDM de Cisco, vaya a Configure > Additional Tasks > AAA > Authorization Policies > Exec.

Paso 2. En el panel Exec Authorization, haga clic en Add.

Paso 3. En la ventana Add a Method List for Exec Authorization, elija Default en la lista desplegable Name.

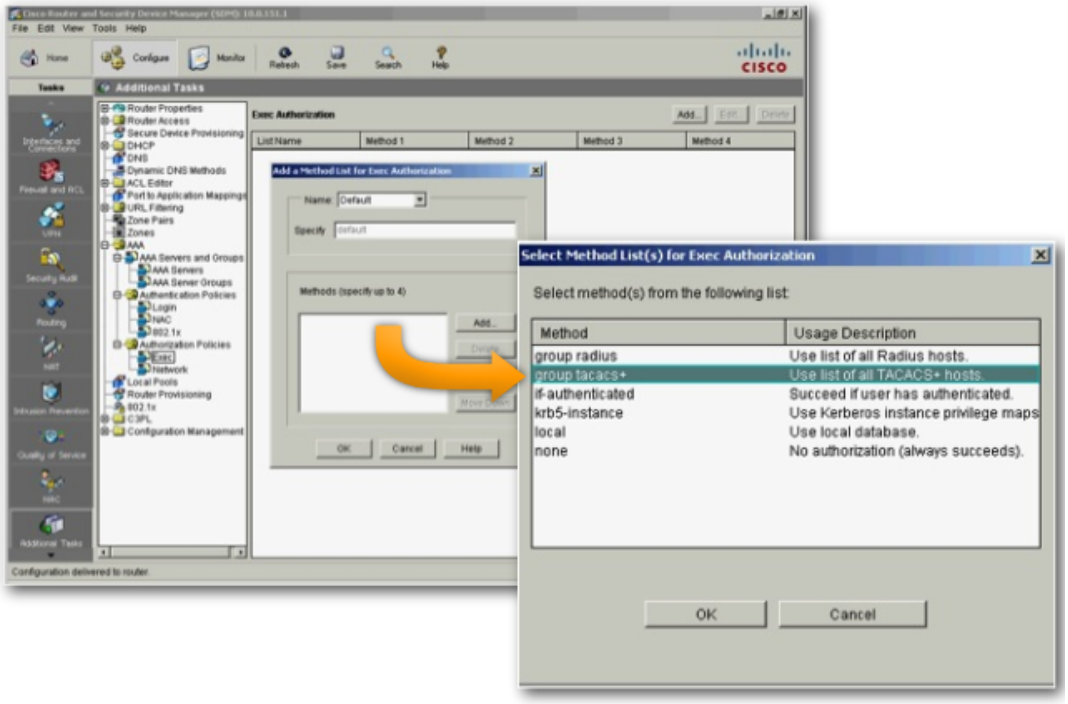
Paso 4. Haga clic en Add para definir los métodos que usará esta política.

Paso 5. En la ventana Select Method List(s) for Exec Authorization, elija group tacacs+ en la lista de métodos.

Paso 6. Haga clic en OK para volver a la ventana Add a Method List for Exec Authorization.

Paso 7. Haga clic en OK para volver al panel Exec Authorization.

El comando CLI resultante generado por el SDM de Cisco es aaa authorization exec default group tacacs+.



También puede usarse el SDM para configurar la lista de métodos de autorización por defecto para el modo paquete (red):

Paso 1. En la página de inicio del SDM de Cisco, vaya a Configure > Additional Tasks > AAA > Authorization Policies > Network.

Paso 2. En el panel Network Authorization, haga clic en Add.

Paso 3. En la ventana Add a Method List for Network Authorization, elija Default en la lista desplegable Name.

Paso 4. Haga clic en Add para definir los métodos que usará esta política.

Paso 5. En la ventana Select Method List(s) for Network Authorization, elija group tacacs+ en la lista de métodos.

Paso 6. Haga clic en OK para volver a la ventana Add a Method List for Network Authorization.

Paso 7. Haga clic en OK para volver al panel Network Authorization.

El comando CLI resultante generado por el SDM de Cisco es aaa authorization network default group tacacs+.

3.5.2 Configuracion del registro de auditoria de AAA basado en servidor

En ocasiones, algunas empresas desean mantener un registro de los recursos que los individuos o grupos utilizan. Ejemplos de esto incluyen una situación en la que un departamento cobra el acceso a otros departamentos o una empresa proporciona soporte interno a otra empresa. El registro de auditoría de AAA proporciona la habilidad de monitorear el uso, como el acceso dial-in, para registrar los datos obtenidos en una base de datos y producir reportes sobre los datos.

Aunque el registro de auditoría generalmente se considera un tema de administración de la red o administración financiera, se tratará brevemente en este capítulo por el vínculo estrecho que mantiene con la seguridad. Un problema de seguridad que solucionan los registros de auditoría es la creación de una lista de usuarios y la hora del día en la que se conectaron con el sistema. Si, por ejemplo, el administrador se entera de que un empleado se conecta con el sistema a la medianoche, esta información puede ser usada para investigar el propósito de la sesión.

Otra razón a favor de implementar registros de auditoría es la creación de una lista de los cambios que ocurren en la red, quién los realizó y la naturaleza exacta de los cambios. Conocer esta información ayuda a resolver problemas si los cambios causan resultados inesperados.

El ACS Seguro de Cisco sirve como repositorio central de la información de registros de auditoría, esencialmente monitoreando los eventos que toman lugar en la red. Cada sesión establecida a través del ACS Seguro de Cisco puede ser monitoreada y almacenada en el servidor. Esta información almacenada puede resultar de gran ayuda en la administración, las auditorías de seguridad, el planeamiento de la capacidad y el cobro de servicios por uso de la red.

De manera semejante a las listas de métodos de autenticación y autorización, las listas de métodos de registros de auditoría definen la manera en que se realizan los registros y

la secuencia que deben seguir los métodos que se usan. Una vez habilitados, la lista de métodos del registro de auditoría por defecto se aplica automáticamente a todas las interfaces, excepto aquéllas que tienen una lista nombrada de métodos de registro de auditoría explícitamente definida.



Para configurar el registro de auditoría de AAA, utilice el comando aaa accounting { network | exec | connection} {default | nombre-lista} {start-stop | stop-only | none} [broadcast] método1...[método4] en el modo de configuración global. Los parámetros network, exec y connection son palabras claves comúnmente utilizadas.

Como con la autenticación AAA, puede usarse la palabra clave default o un nombre-lista.

A continuación se configura el tipo de registro o disparador. El disparador especifica qué acciones causarán una actualización en los registros de auditoría. Los posibles disparadores son none, start-stop, stop-only.

Por ejemplo, para registrar el uso de sesiones EXEC y conexiones de red, use los comandos de configuración global.

R1(config)# aaa accounting exec default start-stop group tacacs+

R1(config)# aaa accounting network default start-stop group tacacs+

```
R1(config)# aaa accounting {network | exec | connection} { default |
list-name } {start-stop | stop-only | none} [broacast] method1…[method4]
```

```
R1(config)# aaa accounting exec ?
  WORD      Named Accounting list.
  default   The default accounting list.
```

Tipo de lista | Lista de métodos | Muestra de configuración

Haga clic en cada botón para ver el contenido asociado.


```
R1(config)# aaa accounting {network | exec | connection} { default |
list-name } {start-stop | stop-only | none} [broacast] method1…[method4]
```


```
R1(config)# aaa accounting exec default start-stop ?
  broadcast  Use Broadcast for Accounting
  group      Use Server-group

R1(config)# aaa accounting exec default start-stop group ?
  WORD     Server-group name
  radius   Use list of all Radius hosts.
  tacacs+  Use list of all Tacacs+ hosts.
```


Tipo de lista | Lista de métodos | Muestra de configuración

Haga clic en cada botón para ver el contenido asociado.

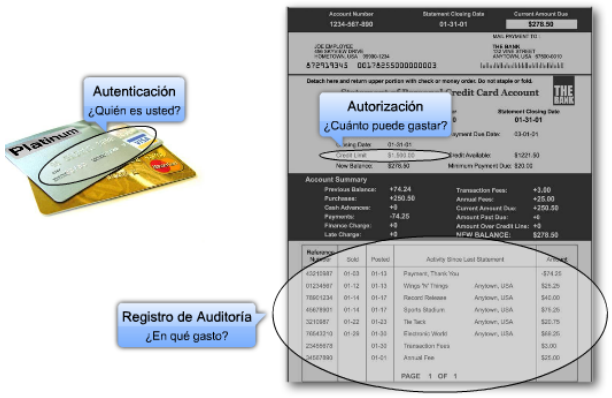



```
R1# conf t
R1(config)# username JR-ADMIN secret Str0ngPa55w0rd
R1(config)# username ADMIN secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authentication login default group tacacs+
R1(config)# aaa authorization exec default group tacacs+
R1(config)# aaa authorization network default group tacacs+
R1(config)# aaa accounting exec default start-stop group tacacs+
R1(config)# aaa accounting network default start-stop group tacacs+
```

Tipo de lista | Lista de métodos | Muestra de configuración

Haga clic en cada botón para ver el contenido asociado.

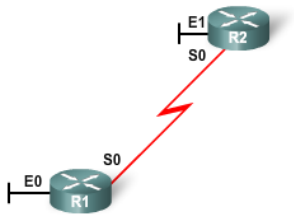
3.6.1 Resumen del capitulo



- El protocolo de autenticación, autorización y registro de auditoría de AAA provee un framework escalable para habilitar seguridad de acceso.
- AAA controla a quién se le permite conectarse a la red, que puede hacer y mantiene registro de lo que se ha hecho.

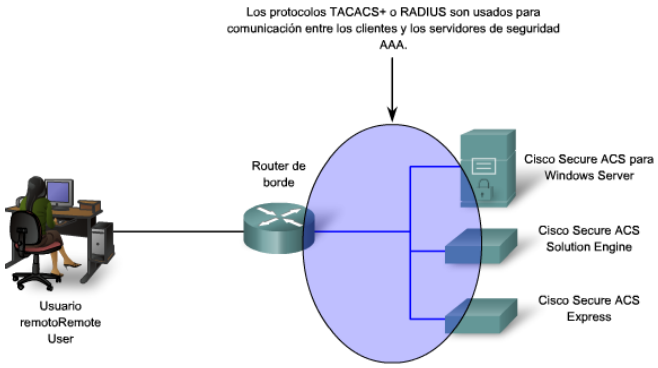
Haga clic en los botones para ver información resumida.

- En una red simple o pequeña, la autenticación AAA puede ser implementada usando una base de datos local.
- AAA Local puede ser configurado usando CLI y SDM.




```
R1# conf t
R1(config)# username JR-ADMIN secret Str0ngPa55w0rd
R1(config)# username ADMIN secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authentication login default local-case enable
R1(config)# aaa authentication login TELNET-LOGIN local-case
R1(config)# line vty 0 4
R1(config-line)# login authentication TELNET-LOGIN
```

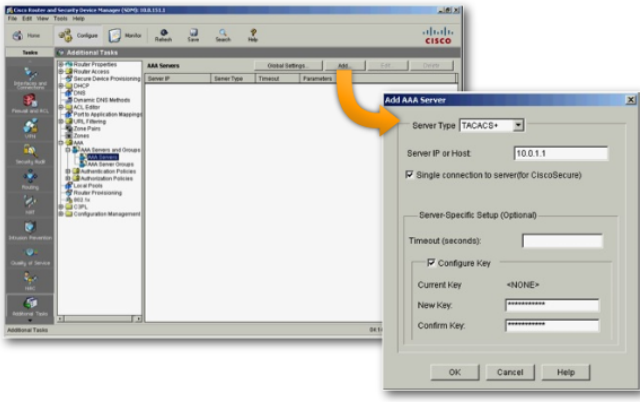
Haga clic en los botones para ver información resumida.



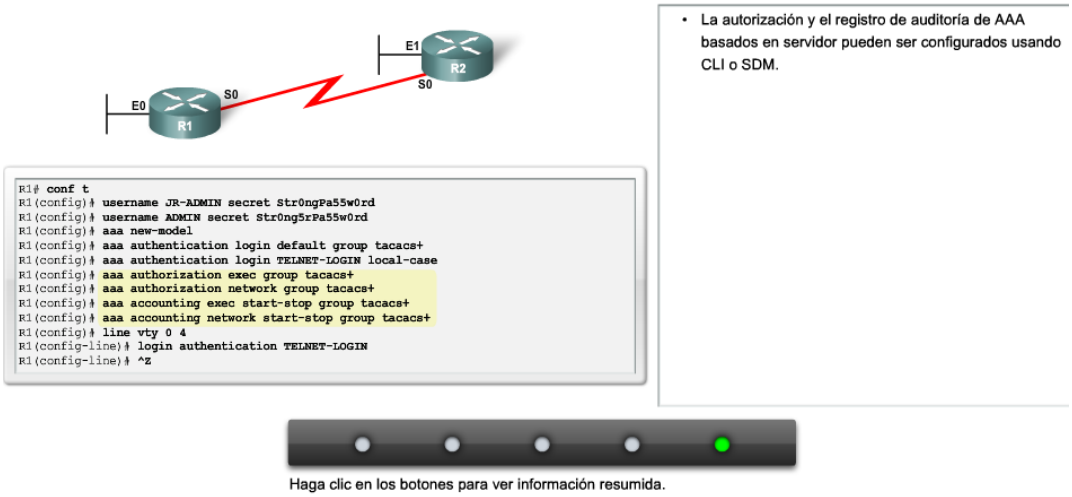
- En redes extensas o complejas, la autenticación AAA puede ser implementada usando AAA basada en servidor.
- Los servidores AAA pueden usar los protocolos RADIUS o TACACS+ para comunicarse con los routers clientes.
- El Servidor de Control de Acceso Cisco (ACS) puede ser usado para proveer servicios de servidor AAA.

Haga clic en los botones para ver información resumida.

- La autenticación AAA basada en servidor puede ser configurada usando CLI o SDM.



Haga clic en los botones para ver información resumida.



4 Implementacion de tecnologias de Firewall

4.0 Introduccion al Capitulo

4.0.1 Introduccion al Capitulo

A medida que las redes continuaron creciendo, se las comenzó a usar cada vez más para transferir y almacenar datos sensibles. Esto incrementó la necesidad de tecnologías de seguridad más fuertes, lo cual llevó a la invención del firewall. El término "firewall" originalmente se refería a una pared a prueba de fuego (fireproof wall), generalmente hecha de piedra o metal, que evitaba que se extendieran llamas de una estructura a otra que se conectaba con ella. Similarmente, en las redes, los firewalls separan las áreas protegidas de las no protegidas. Esto impide a los usuarios no autorizados acceder a recursos en redes protegidas.

Inicialmente, los únicos medios de proporcionar protección de firewall eran las listas de control de acceso (ACL), incluyendo estándar, extendidas, numeradas y nombradas. A fines de 1990, comenzaron a madurar otras tecnologías de firewall. Los firewalls de estados (stateful) usan tablas para seguir el estado en tiempo real de las sesiones end-to-end. Los firewalls de estado toman en consideración la naturaleza orientada a sesiones del tráfico de red. Los primeros firewalls de estados usaban la opción "TCP established" para las ACLs. Luego se usaron las ACLs reflexivas para reflejar dinámicamente cierto tipo de tráfico dirigido desde el interior de la red hacia el exterior de modo de poder permitir el retorno del mismo. Las ACLs dinámicas fueron desarrolladas para abrir un agujero en el firewall para tráfico aprobado por un período determinado de tiempo. Las ACLs basadas en tiempo fueron ideadas para aplicar ACLs durante ciertos momentos del día en días de la semana específicos. Con la proliferación de tipos de ACLs, empezó a volverse más y más importante poder verificar el comportamiento apropiado de estas ACLs con los comandos show y debug.

Hoy en días hay muchos tipos de firewalls disponibles, incluyendo los firewalls de filtrado de paquetes, de estados, de gateway de aplicación (proxy), de traducción de direcciones, basados en hosts, transparentes e híbridos. Los diseños de redes modernos deben incluir uno más firewalls cuidadosamente colocados de modo de proteger los

recursos que requieren protección, permitiendo el acceso en forma segura a los recursos que deben permanecer disponibles.

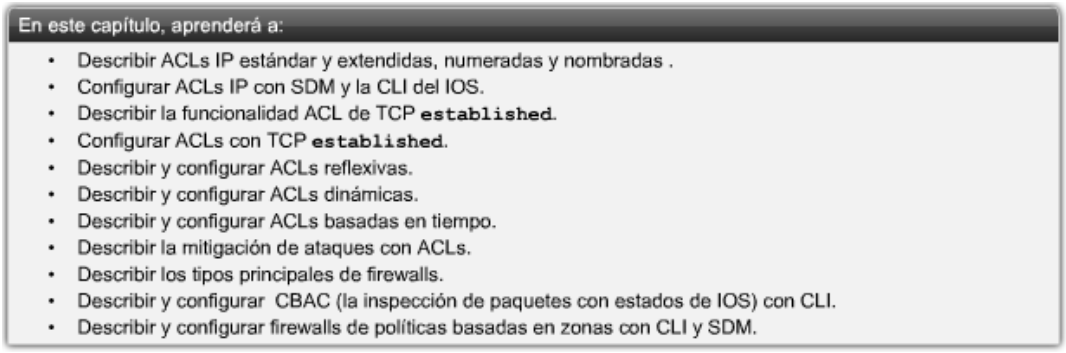
En la práctica de laboratorio del capítulo, Configuración de CBAC y Firewalls basados en zonas, los estudiantes usan CLI y SDM para configurar y probar un Firewall de Política Basada en Zonas y Control de Acceso Basado en el Contexto. La práctica está disponible en el manual de laboratorio en Academy Connection en cisco.netacad.net.

La primera actividad de Packet Tracer, Configuración de ACLs IP para mitigar ataques, proporciona a los alumnos práctica adicional en la implementación de las tecnologías presentadas en este capítulo. En particular, los alumnos aprenderán a configurar ACLs para asegurarse de que el acceso remoto a los routers esté disponible sólo desde las estaciones de administración. Los routers de borde se configuran con ACLs para mitigar ataques de red comunes y se examinan las ACLs para probar su efectiva operación.

La segunda actividad de Packet Tracer, Configuración del Control de Acceso Basado en el Contexto (Context-Based Access Control - CBAC), los estudiantes configuran un IOS firewall con CBAC en un router de perímetro. Se verifica la funcionalidad de CBAC con ping, Telnet y HTTP.

La última actividad de Packet Tracer del capítulo, Configuración de un Firewall de Política Basada en Zonas (Zone-Based Policy Firewall - ZPF), pide a los alumnos configurar una política ZPF en un router de perímetro. Se verifica la funcionalidad de ZPF con ping, Telnet y HTTP.

Las actividades de Packet Tracer para CCNA Security están disponibles en Academy Connection en cisco.netacad.net.



4.1.1 Configuracion ACLs IP estandar y extendidas con CLI

Las listas de control de acceso (access control lists - ACLs) se usan regularmente en las redes de computadoras y en la seguridad de las redes para mitigar ataques de red y controlar el tráfico de red. Los administradores usan las ACLs para definir y controlar las clases de tráfico en los dispositivos de networking tomando como base varios parámetros. Estos parámetros son específicos de las capas 2, 3, 4 y 7 del modelo OSI.

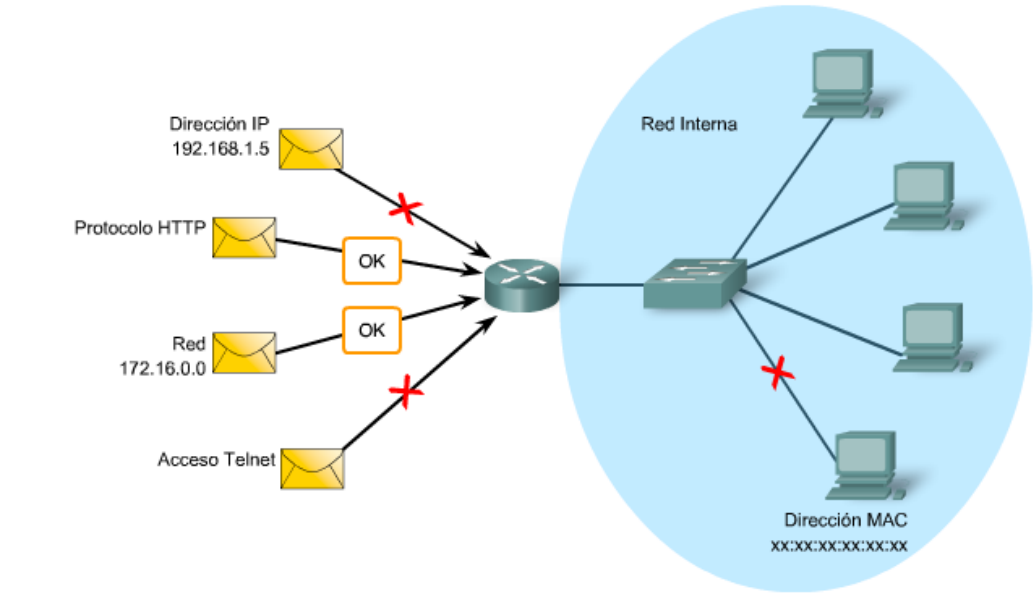
Prácticamente cualquier tipo de tráfico puede ser definido explícitamente usando apropiadamente una ACL numerada. Por ejemplo, antiguamente, el campo de tipo Ethernet en el encabezado de una trama Ethernet era usado para definir ciertos tipos de

tráfico. Un tipo Ethernet 0x8035 indicaba una trama de protocolo de resolución de direcciones inverso (Reverse Address Resolution Protocol - RARP). Las ACLs numeradas dentro del rango 200-299 eran usadas para controlar el tráfico de acuerdo con el tipo Ethernet.

También era común crear ACLs con la dirección MAC como base. Una ACL numerada dentro del rango 700-799 indica que el tráfico es clasificado y controlado con la dirección MAC como base.

Luego de que se especifica el tipo de clasificación, pueden establecerse los parámetros de control requeridos para esa ACL. Por ejemplo, una ACL numerada en el rango que va desde el 700 hasta el 799 puede ser usada para prohibir que un cliente con una dirección MAC específica se asocie con un punto de acceso predeterminado.

Hoy en día, para clasificar tráfico, los tipos de parámetros más comúnmente utilizados en las ACLs relacionadas con la seguridad tienen que ver con las direcciones IPv4 e IPv6 y con los números de puerto TCP y UDP. Por ejemplo, una ACL puede permitir a todos los usuarios con una dirección de red IP específica descargar archivos de Internet usando FTP seguro. Esa misma ACL puede ser usada para denegar a todas las direcciones IP el acceso al FTP tradicional.



Protocolo	Rango
IP	1-99, 1300-1999
IP extendida	100-199, 2000-2699
Código de tipo Ethernet	200-299
DECnet y DECnet extendido	300-399
XNS	400-499
XNS extendido	500-599
AppleTalk	600-699
Dirección Ethernet	700-799
IPX	800-899
IPX extendido	900-999
IPX SAP	1000-1099
Extended transparent bridging	1100-1199



ACLs estándar

Las ACLs numeradas entre 1-99 y 1300-1999 son ACLs IPv4 e IPv6 estándar. Las ACLs estándar filtran los paquetes examinando el campo de dirección IP de origen en el encabezado IP de ese paquete. Estas ACLs son usadas para filtrar paquetes basándose exclusivamente en la información de origen de capa 3.

Las ACLs estándar permiten o deniegan el tráfico basándose en la dirección de origen. Esta es la sintaxis del comando para configurar una ACL IP estándar numerada:

Router(config)# access-list {1-99} {permit | deny} dir-origen [wildcard-origen]

El primer valor especifica el número de la ACL. Para las ACLs estándar, el número deberá estar en el rango 1-99. El segundo valor especifica si lo que debe hacer es permitir o denegar el tráfico de la dirección IP origen configurada. El tercer valor es la dirección IP de origen que debe buscarse. El cuarto valor es la máscara wildcard que debe aplicarse a la dirección IP previamente configurada para indicar el rango.

ACLs extendidas

Las ACLs extendidas filtran los paquetes basándose en la información de origen y destino de las capas 3 y 4. La información de capa 4 puede incluir información de puertos TCP y UDP. Las ACLs extendidas otorgan mayor flexibilidad y control sobre el acceso a la red que las ACLs estándar. Esta es la sintaxis del comando para configurar una ACL IP extendida numerada:

Router(config)# access-list {100-199} {permit | deny} protocolo dir-origen [wildcard-origen] [operador operando] dir-destino [wildcard-destino] [operador operando] [established]

De manera similar a las ACLs estándar, el primer valor especifica el número de la ACL. Las ACLs numeradas entre 100-199 o 2000-2699 son ACLs extendidas. El siguiente valor especifica si lo que debe hacer es permitir o denegar de acuerdo al criterio que sigue. El tercer valor indica el tipo de protocolo. El administrador debe especificar IP, TCP, UDP u otros sub-protocolos de IP específicos. La dirección IP y la máscara wildcard de origen determinan dónde se origina el tráfico. La dirección IP y la máscara wildcard de destino son usadas para indicar el destino final del tráfico de red. Aunque el parámetro de puerto se define como opcional, cuando se configuran la dirección IP y máscara de destino, el administrador debe especificar el número de puerto que corresponda, ya sea por número o por nombre de puerto bien conocido. Si no es así, todo el tráfico con ese destino será descartado.

Todas las ACLs asumen un deny implícito, lo cual significa que si un paquete no coincide con ninguna de las condiciones especificadas en la ACL, el paquete será denegado. Una vez que la ACL ha sido creada, debe incluirse al menos una sentencia permit o todo el tráfico de la interfaz a la que se aplique será descartado.

Tanto las ACLs estándar como las extendidas pueden ser usadas para describir paquetes que entran o salen de una interfaz. La lista se recorre secuencialmente. La primera sentencia que coincida detiene la búsqueda en la lista y define la acción que se tomará.

Una vez que se ha creado la ACL IP numerada, sea estándar o extendida, el administrador debe aplicarla a la interfaz apropiada.

Este es el comando que se usa para aplicar la ACL a una interfaz:

Router(config-if)# ip access-group número-acl {in | out}

Este es el comando que se usa para aplicar la ACL a una línea vty:

Router(config-line)# access-class número-acl {in | out}

Las ACLs estándar filtran los paquetes IP basándose sólo en la dirección de origen.

```
access-list {1-99} {permit | deny} source-addr [source-wildcard]
```

ACL IP numerada estándar

ACL IP numerada extendida

Haga clic en los botones para ver las diferencias entre las ACLs IP numeradas estándar y extendidas.

Las ACLs estándar filtran los paquetes IP basándose sólo en la dirección de origen.

```
access-list {1-99} {permit | deny} source-addr [source-wildcard]
```

Las ACLs extendidas filtran los paquetes IP basándose en varios atributos que incluyen los siguientes:

- Direcciones IP de origen y destino
- Puertos TCP y UDP de origen y destino
- Tipo de protocolo (IP, ICMP, UDP, TCP o número de protocolo)

```
access-list {100-199} {permit | deny} protocol source-addr
[source-wildcard][operator operand] destination-addr [destination-
wildcard] [operator operand][established]
```



Haga clic en los botones para ver las diferencias entre las ACLs IP numeradas estándar y extendidas.

Es posible crear una ACL nombrada en lugar de una ACL numerada. Las ACLs nombradas deben especificarse como estándar o extendidas.

Router(config)# ip access-list [standard | extended] nombre_ACL

La ejecución de este comando ubica al usuario en el modo de subconfiguración en el que deberá ingresar los comandos permit y deny. Los comandos permit y deny tienen la misma sintaxis básica que los comandos de la ACL IP numerada.

Una ACL estándar nombrada puede usar sentencias deny y permit statements.

Router(config-std-nacl)# deny {origen [wildcard-origen] | any}

Router(config-std-nacl)# permit {origen [wildcard-origen] | any}

La ACL extendida nombrada ofrece parámetros adicionales.

Router(config-ext-nacl)# {permit | deny} protocolo dir-origen [wildcard-origen] [operador operando] dir-destino [wildcard-destino] [operador operando] [established]

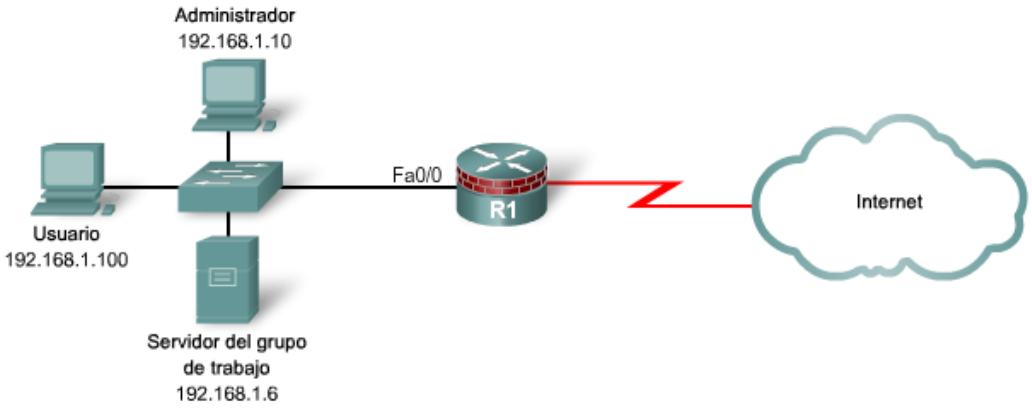
Las ventajas del uso de ACLs nombradas incluyen que el administrador puede borrar una entrada específica en una ACL nombrada yendo al modo de subconfiguración y prefijando el comando con el parámetro no. El uso del parámetro no en una entrada de una ACL numerada resultaría en la eliminación de toda la ACL. El administrador también puede agregar entradas en el medio de una ACL nombrada. Con una ACL numerada, los comandos sólo pueden agregarse al final de la ACL.

Una vez que las sentencias han sido generadas en la ACL, el administrador debe activar la ACL en una interfaz con el comando ip access-group, especificando el nombre de la ACL.

Router(config-if)# ip access-group nombre-ACL {in | out}

También puede usarse una ACL para permitir o denegar a direcciones IP específicas el acceso virtual. Las ACLs estándar permiten la aplicación de restricciones en la dirección IP o el rango IP de origen. Las ACLs extendidas también tienen esta función pero además aplican el protocolo de acceso, como el puerto 23 (Telnet) o el puerto 22 (SSH). La ACL extendida access-class sólo soporta la palabra clave any como destino. La lista de acceso debe ser aplicada en el puerto vty.

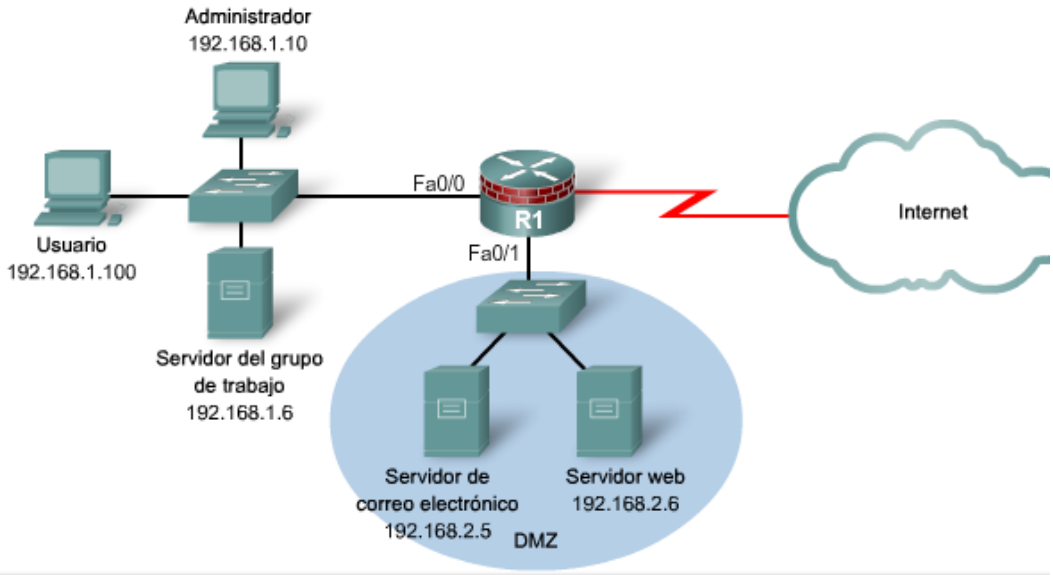
Router(config-line)# access-class nombre-ACL {in | out}




```
R1(config)# ip access-list standard RESTRICT_VTY
R1(config-std-nacl)# remark Permit only Admin host
R1(config-std-nacl)# permit host 192.168.1.10
R1(config-std-nacl)# exit
R1(config)# line vty 0 4
R1(config-line)# access-class RESTRICT_VTY in
```

ACL IP estándar nombrada | ACL IP extendida nombrada

Haga clic en cada botón para ver el contenido asociado.




```
R1(config)# ip access-list extended ACL-1
R1(config-ext-nacl)# remark LAN ACL
R1(config-ext-nacl)# deny ip host 192.168.1.6 any
```

```
R1(config-ext-nacl)# permit tcp 192.168.1.0 0.0.0.255 any established
R1(config-ext-nacl)# deny ip any any
R1(config-ext-nacl)# exit
```

```
R1(config)# interface Fa0/0
R1(config-if)# ip access-group ACL-1 in
R1(config-if)# exit
```

```
R1(config)# ip access-list extended ACL-2
R1(config-ext-nacl)# remark DMZ ACL
R1(config-ext-nacl)# permit tcp any host 192.168.2.5 eq 25
```

```
R1(config-ext-nacl)# permit tcp any host 192.168.2.6 eq 80
R1(config-ext-nacl)# deny ip any any
R1(config-ext-nacl)# exit
```

```
R1(config)# interface Fa0/1
R1(config-if)# ip access-group ACL-2 out
R1(config-if)# exit
```

ACL IP estándar nombrada | ACL IP extendida nombrada

Haga clic en cada botón para ver el contenido asociado.

Al final de una sentencia ACL, el administrador tiene la opción de configurar el parámetro log.

R1(config)# access-list 101 permit tcp 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255 eq 22 log

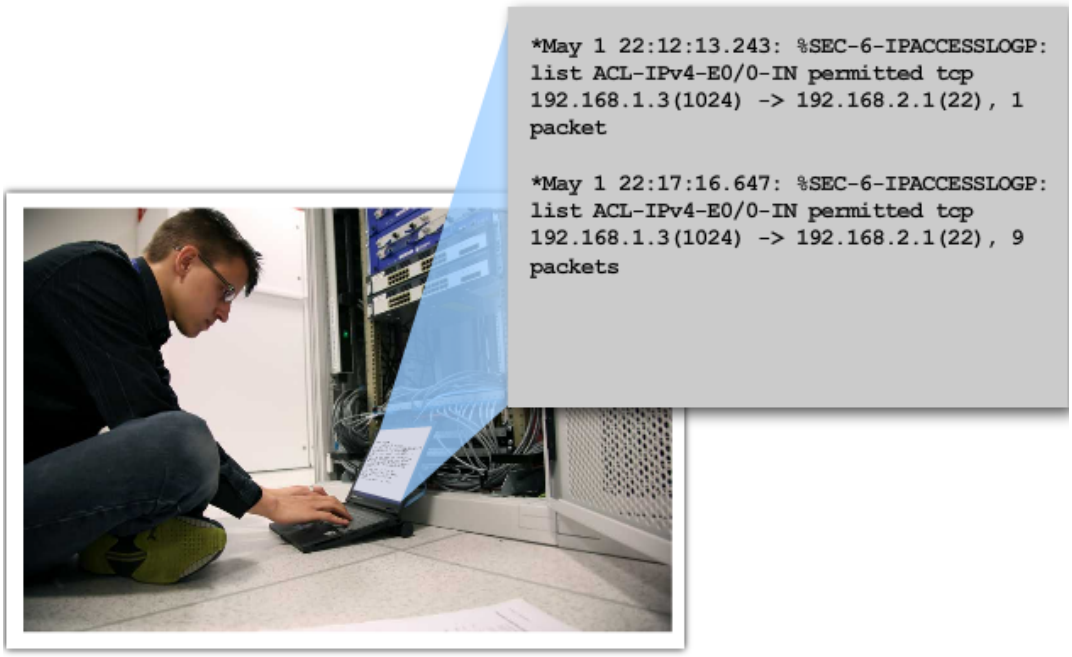
Si este parámetro se configura, el software IOS de Cisco compara los paquetes en búsqueda de una coincidencia con la sentencia. El router registra en una función de registro habilitada, como la consola, el buffer interno del router o un servidor syslog. Se registran muchos datos:

Acción - permit o deny

Protocolo - TCP, UDP o ICMP
Direcciones de origen y destino
Para TCP y UDP - números de puerto de origen y destino
Para ICMP - tipo de mensaje

Los mensajes de registro se generan en la primera coincidencia de paquete y luego en intervalos de cinco minutos.

La habilitación del parámetro log en un router Cisco afecta seriamente al rendimiento del dispositivo. Cuando se habilita el registro, los paquetes son transmitidos por conmutación de proceso o por conmutación rápida. El parámetro log debe ser usado solamente si la red está bajo ataque y el administrador está intentando determinar quién es el atacante. En este punto, el administrador debe habilitar el registro por el tiempo que sea necesario para reunir la información suficiente y luego dehabilitarlo.

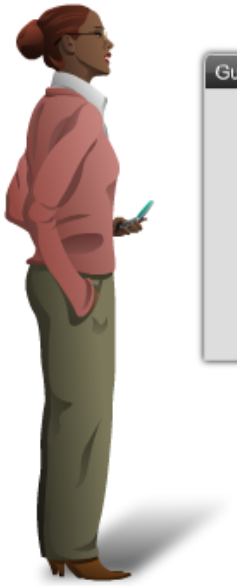


Deben considerarse varias advertencias al trabajar con ACLs:

deny all implícito - Todas las ACLs de Cisco terminan con una sentencia "deny all" implícita. Incluso si esta sentencia no está a la vista en la ACL, está allí.
Filtrado de paquetes de ACL estándar - Las ACLs estándar se limitan a filtrar los paquetes sólo por dirección de origen. Puede necesitar crear una ACL extendida para implementar su política de seguridad plenamente.
Orden de las sentencias - Las ACLs tienen una política de primera coincidencia. Cuando hay una coincidencia con una sentencia, el proceso de verificación de la lista se detiene. Ciertas sentencias ACLs son más específicas que otras y, por lo tanto, deben ocupar un lugar anterior en la ACL. Por ejemplo, el bloqueo de todo el tráfico UDP al principio de la lista niega la sentencia que permite los paquetes SNMP que usan UDP, que está más abajo en la lista. El administrador debe asegurarse de que las sentencias que están arriba en la ACL no nieguen sentencias posteriores.

Filtrado direccional - Las ACLs de Cisco tienen un filtro direccional que determina si los paquetes de entrada (hacia la interfaz) o los paquetes de salida (desde la interfaz) serán examinados. El administrador siempre debe revisar dos veces la dirección de los datos que la ACL filtra.
Modificación de ACLs - Cuando un router compara un paquete con una ACL, las entradas de la ACL son examinadas desde arriba hacia abajo. Cuando el router encuentra una sentencia que coincide, el procesamiento de la ACL se detiene y se permite o deniega el paquete según la entrada en la ACL. Cuando se agregan nuevas entradas a una ACL, siempre se agregan al final. Esto puede volverlas inútiles si una entrada anterior es menos específica. Por ejemplo, si una ACL tiene una entrada que deniega a la red 172.16.1.0/24 acceso a un servidor en una línea, pero en la siguiente línea se lo permite a un solo host de esa red, el host 172.16.1.5, el acceso le será denegado. Esto ocurre porque el router encuentra una coincidencia en los paquetes de 172.16.1.5 con la red 172.16.1.0/24 y deniega el tráfico sin leer la siguiente línea. Cuando una nueva sentencia vuelve inusable la ACL, debe crearse una nueva ACL con el orden de las sentencias correcto. La ACL vieja debe eliminarse, y la nueva ACL debe ser asignada a la interfaz del router correspondiente. Si se usa una versión 12.3 o posterior del IOS de Cisco, se pueden usar números de secuencia para garantizar que la nueva sentencia se agregue a la ACL en el orden correcto. La ACL se procesa de arriba hacia abajo basándose en los números de secuencia de las sentencias (del más bajo al más alto).
Paquetes especiales - Los paquetes generados por el router, como las actualizaciones de la tabla de enrutamiento, no están sujetos a las sentencias ACL de salida en el router de origen. Si la política de seguridad solicita un filtrado de este tipo de paquetes, deberá realizarlo una ACL de entrada en un router adyacente o un mecanismo diferente de filtrado en routers que usen ACLs.

Ahora que se han definido la sintaxis y las guías de creación de ACLs IP estándar y extendidas, veamos algunas situaciones específicas para las cuales las ACLs proporcionan una solución de seguridad



Guía de configuración de ACLs

- Las ACLs se crean globalmente y luego se aplican a las interfaces.
- La ACL puede filtrar el tráfico que pasa a través del router o el que va desde y hacia el router, dependiendo de cómo se aplique.
- Se permite solo una ACL por interfaz, por protocolo y por dirección.
- Estándar o extendida indica la información que se usa para filtrar los paquetes.
- Las ACLs se procesan de arriba hacia abajo. Una vez que el paquete coincide con una entrada de la ACL, se detiene el proceso y el paquete es permitido o denegado; por lo tanto, las sentencias más específicas deben ir antes en la lista.
- Todas las ACLs tienen una sentencia "deny all" al final, por lo que las listas deben tener por lo menos una sentencia permit para permitir que pase algún tipo de tráfico.

4.1.2 Uso de ACLs IP estandar y extendidas

Determinar si usar una ACL estándar o extendida depende del objeto general de toda la ACL. Por ejemplo, imagine una situación en la que debe denegarse acceso de todo el tráfico de una sola subred, 172.16.4.0, a otra subred, pero todo el tráfico restante debe permitirse.

En este caso, puede aplicarse una ACL estándar de salida en la interfaz Fa0/0:

R1(config)# access-list 1 deny 172.16.4.0 0.0.0.255

R1(config)# access-list 1 permit any

R1(config)# interface FastEthernet 0/0

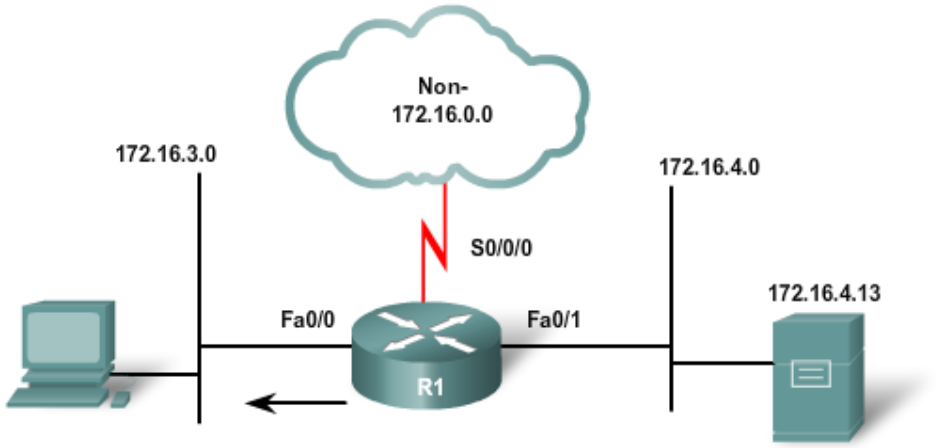
R1(config-if)# ip access-group 1 out

Se ha bloqueado a todos los hosts de la subred 172.16.4.0 la salida de la interfaz Fa0/0 hacia la subred 172.16.3.0.

Estos son los parámetros del comando access-list:

El parámetro 1 indica que esta ACL es una lista estándar.
El parámetro deny indica que el tráfico que coincida con los parámetros seleccionados no será reenviado.
El parámetro 172.16.4.0 es la dirección IP de la subred de origen.
El parámetro 0.0.0.255 es la máscara wildcard. Los ceros (0) indican posiciones que deben coincidir en el proceso; los unos (1) indican posiciones que serán ignoradas. La máscara con ceros (0) en los primeros tres octetos indica que esas posiciones deberán coincidir. El 255 indica que el último octeto será ignorado.
El parámetro permit indica que el tráfico que coincide con los parámetros seleccionados será reenviado.
El parámetro any es una abreviación de la dirección de IP del origen. Indica una dirección de origen 0.0.0.0 y una máscara wildcard 255.255.255.255; todas las direcciones de origen coincidirán.

A causa del deny implícito al final de todas las ACL, el comando access-list 1 permit any debe ser incluido para asegurar que sólo el tráfico de la subred 172.16.4.0 sea bloqueado y que todo el tráfico restante sea permitido.



Use una ACL estándar para bloquear todo el tráfico de la red 172.16.4.0/24 y permitir el resto del tráfico.

En comparación con las ACLs estándar, las ACLs extendidas permite que tipos específicos de tráfico sean denegados o permitidos. Imagine una situación en la que el tráfico FTP que proviene de una subred deba ser denegado sólo hacia otra subred. En este caso, se requiere una ACL extendida, ya que se filtra un tipo específico de tráfico.

R1(config)# access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 21

R1(config)# access-list 101 deny tcp 172.16.4.0 0.0.0.255 172.16.3.0 0.0.0.255 eq 20

R1(config)# access-list 101 permit ip any any

En esta ACL, se deniega el acceso FTP de la subred 172.16.4.0/24 a la subred 172.16.3.0/24. Todo el tráfico restante es permitido. Como se usa el puerto TCP 21 para los comandos del programa FTP y el puerto TCP 20 para la transferencia de datos FTP, ambos puertos son denegados.

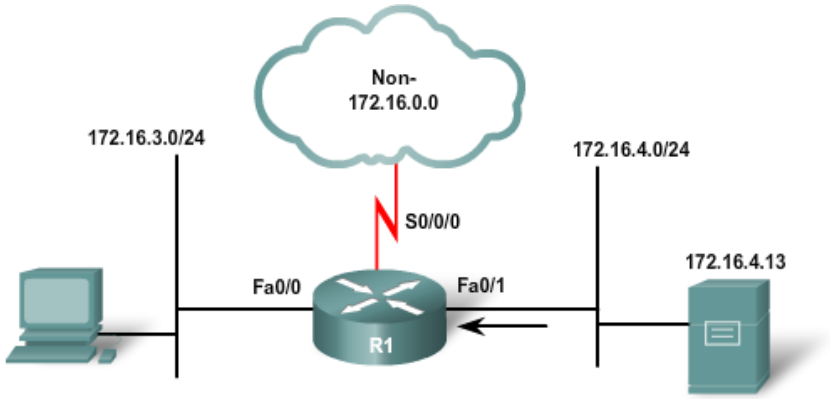
Se requiere una sentencia permit ip any any al final de la ACL: si no estuviera, se denegaría todo el tráfico por el deny implícito.

En este ejemplo, el mejor lugar para ubicar la ACL es de entrada en la interfaz Fa0/1. Esto asegura que el tráfico FTP no deseado sea descartado antes de malgastar los recursos de procesamiento del router.

Router(config)# interface fastethernet 0/1

Router(config-if)# ip access-group 101 in

Tenga en consideración que, en esta ACL, una sentencia permit any any invalida la sentencia implícita deny all al final de todas las ACL. Esto significa que todo el resto del tráfico, incluyendo el tráfico FTP que se origina en la red 172.16.4.0/24 y se dirige a cualquier red que no sea la 172.16.3.0/24, será permitido.

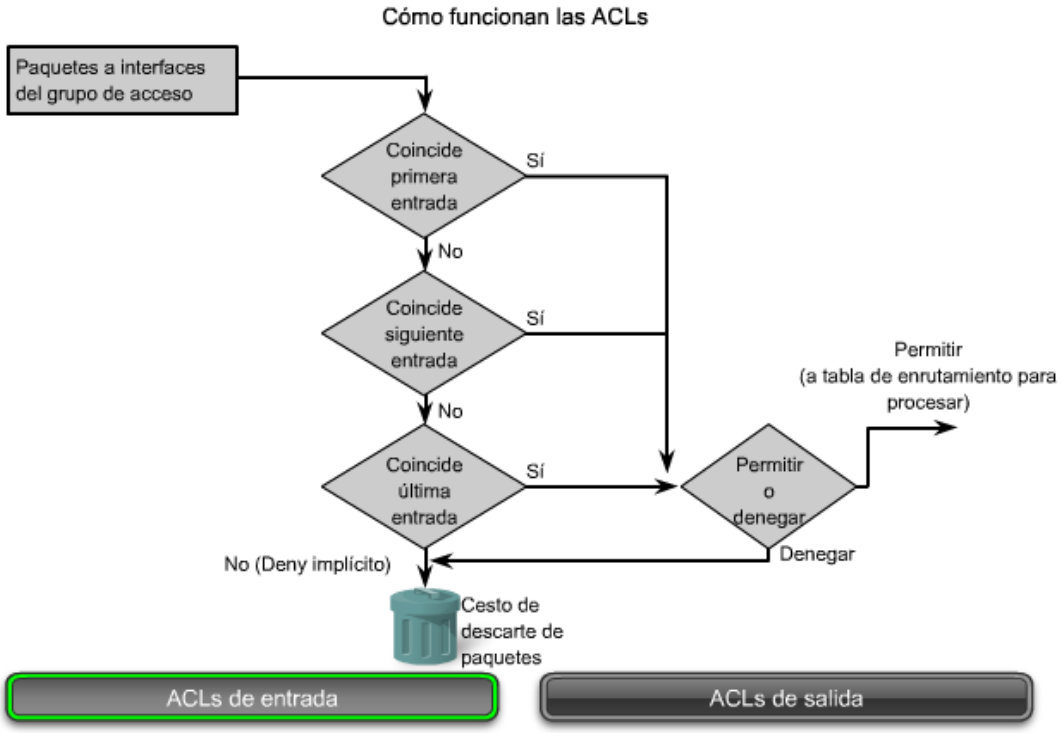


Use una ACL extendida para bloquear todo el tráfico FTP de la red 172.16.4.0/24 hacia la red 172.16.3.0/24 y permitir el resto del tráfico.

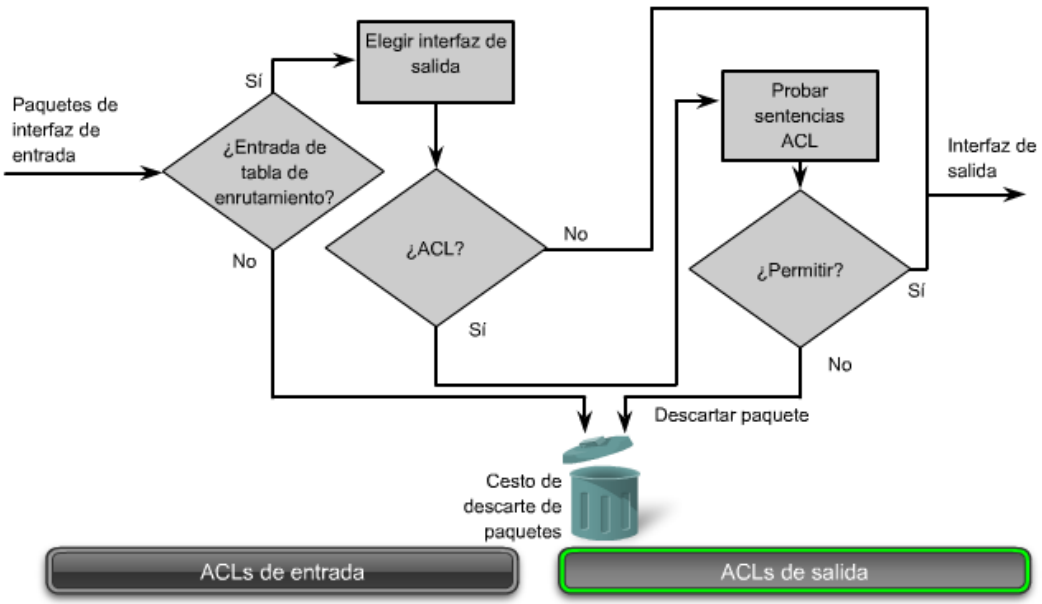
4.1.3 Topologia y flujo de las listas de control de acceso

La dirección del tráfico a través de un dispositivo de red es definida por las interfaces de entrada y salida del tráfico. El tráfico de entrada es aquél que ingresa al router, antes de acceder a la tabla de enrutamiento. El tráfico de salida es todo aquél que ingresó al router y fue procesado por él para determinar a dónde deberá reenviar los datos. Antes de que los datos sean reenviados fuera de esa interfaz, se examina la ACL de salida.

Dependiendo del tipo de dispositivo y el tipo de ACL configurada, el tráfico de retorno puede ser monitoreado dinámicamente.



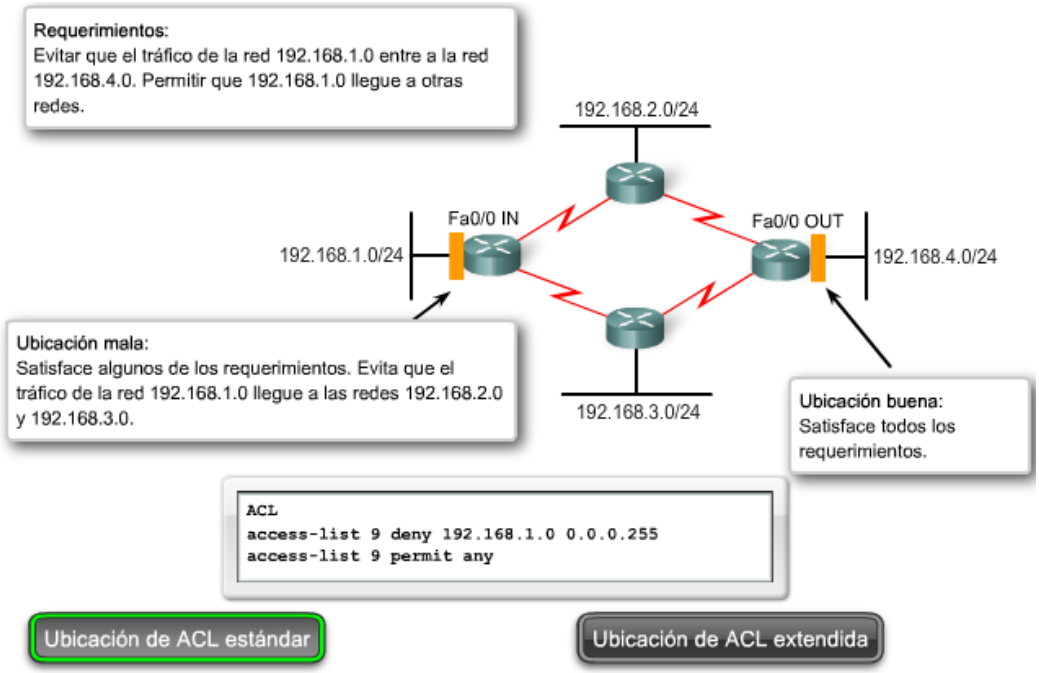
Ejemplo de ACL de salida

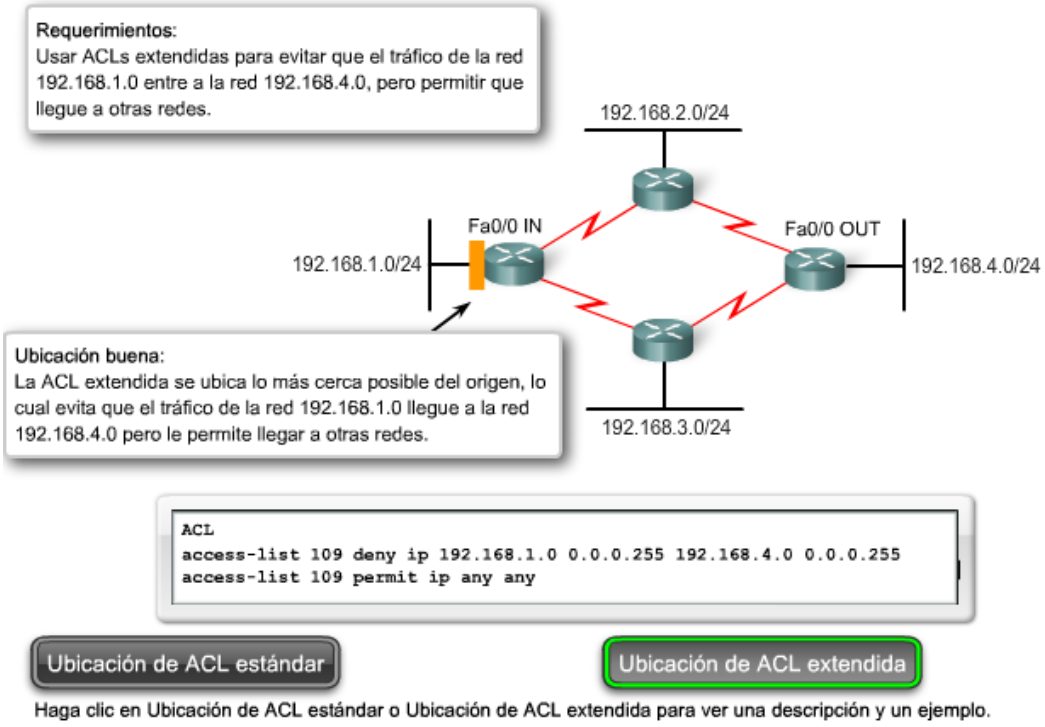


Además del flujo, es importante tener en consideración la ubicación de las ACLs. La ubicación depende del tipo de ACL que se use.

Ubicación de ACLs extendidas - Las ACLs extendidas se ubican en los routers lo más cerca del origen que se está filtrando como sea posible. Ubicar una ACL extendida demasiado lejos del origen resulta en un uso ineficiente de los recursos de red. Por ejemplo, los paquetes pueden ser enviados en una ruta larga sólo para ser descartados o denegados.

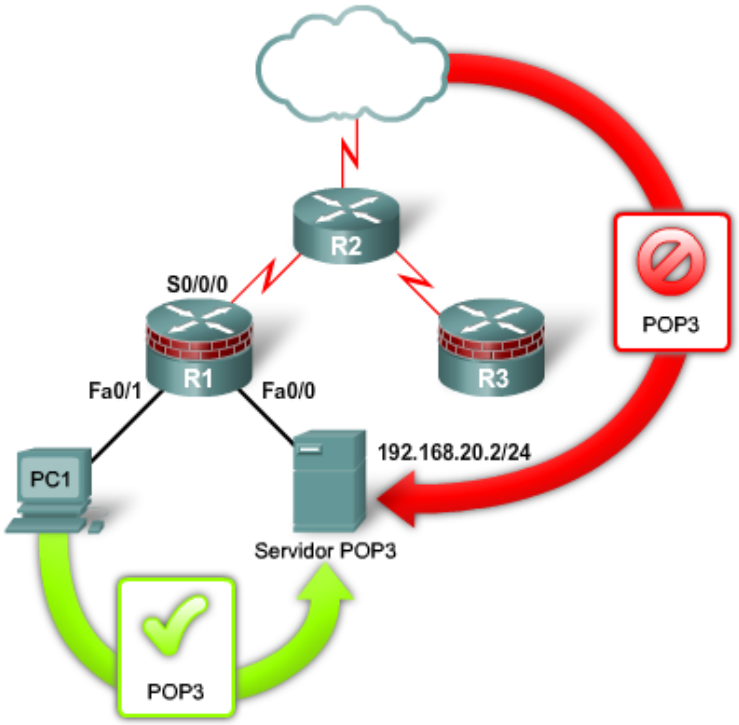
Ubicación de ACLs estándar - Las ACLs estándar se ubican lo más cerca del destino como sea posible. Las ACLs estándar filtran paquetes basándose sólo en la dirección de origen, por lo tanto, ubicarlas demasiado cerca del origen puede afectar adversamente a los paquetes al denegar todo el tráfico, incluyendo el válido.





Generalmente, las ACLs se usan para prevenir que la mayoría del tráfico ingrese a la red. Al mismo tiempo, permiten selectivamente algunos tipos de tráfico más seguros, como HTTPS (puerto TCP 443), para su uso en los negocios. Esto generalmente requiere el uso de ACLs extendidas y un conocimiento claro de los puertos que deben ser bloqueados y los que deben ser permitidos.

El programa Nmap puede ser usado para determinar qué puertos están abiertos en un dispositivo dado. Por ejemplo, una ACL no permite que el tráfico POP3 descargue correo electrónico a través de Internet de un servidor de correo en la red de la empresa, pero permite que el correo electrónico sea descargado desde una estación de trabajo dentro de la red de la empresa. La salida de un escaneo Nmap del servidor POP3 depende de dónde se origine el escaneo. Si el escaneo se realiza desde una PC dentro de la red, el puerto POP3 aparecerá abierto (puerto TCP 110).



Uso de ACL | Nmap

Haga clic en cada botón para ver el contenido asociado.

```
PC1$ nmap --system-dns 192.168.20.0/24
Interesting ports on webserver.branch1.com (192.168.20.2):
(The 1669 ports scanned but not shown below are in state: filtered)
PORT      STATE      SERVICE
110       open       pop3
```

Uso de ACL | Nmap

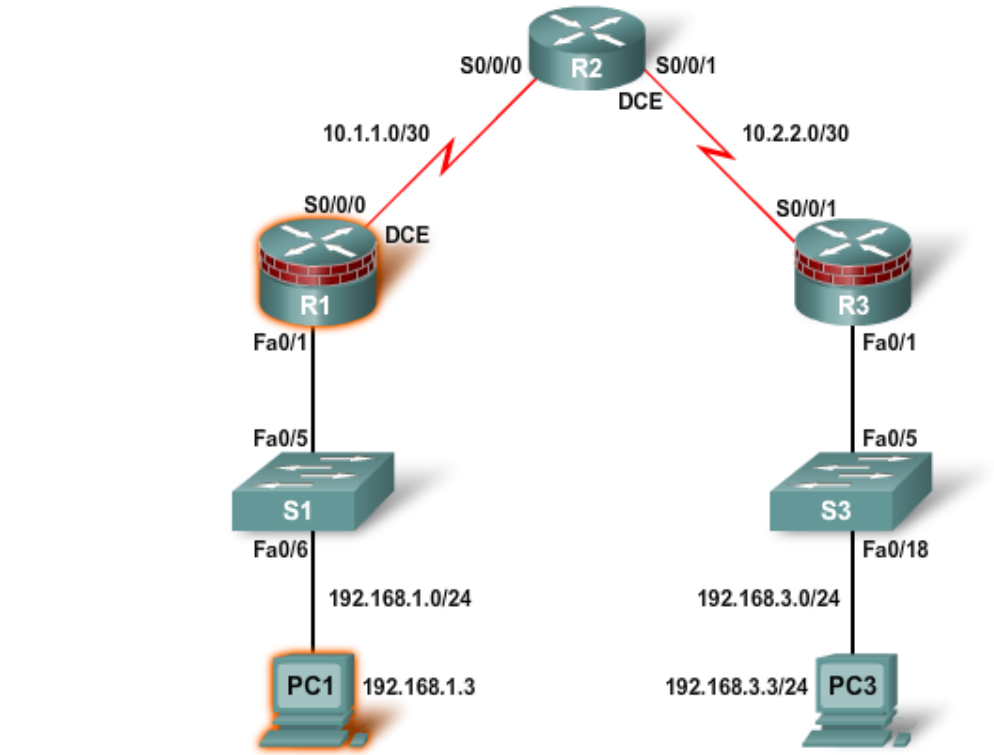
Haga clic en cada botón para ver el contenido asociado.

Luego de que se aplica una ACL a una interfaz, es importante verificar que esté funcionando como se desea, es decir, que el tráfico que debe ser denegado sea denegado y que el válido sea permitido.

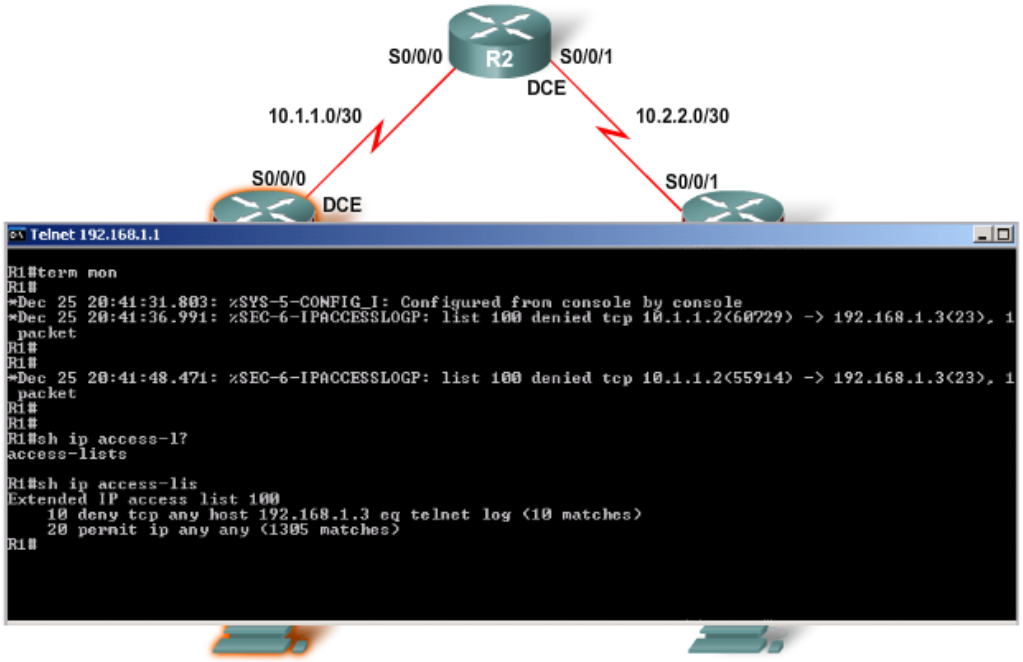
Aunque la opción log muestra coincidencias de paquetes registrados a medida que ocurren, puede ser una carga excesiva en los recursos del dispositivo de red. La opción log debe ser utilizada de manera provisoria para verificar y resolver problemas de configuración de una ACL.

El comando show ip access-list puede ser usado como medio básico para revisar el efecto de la ACL. Con este comando, sólo se registrará el número de paquetes que coincidan con una entrada de control de acceso (Access Control Entry - ACE) dada.

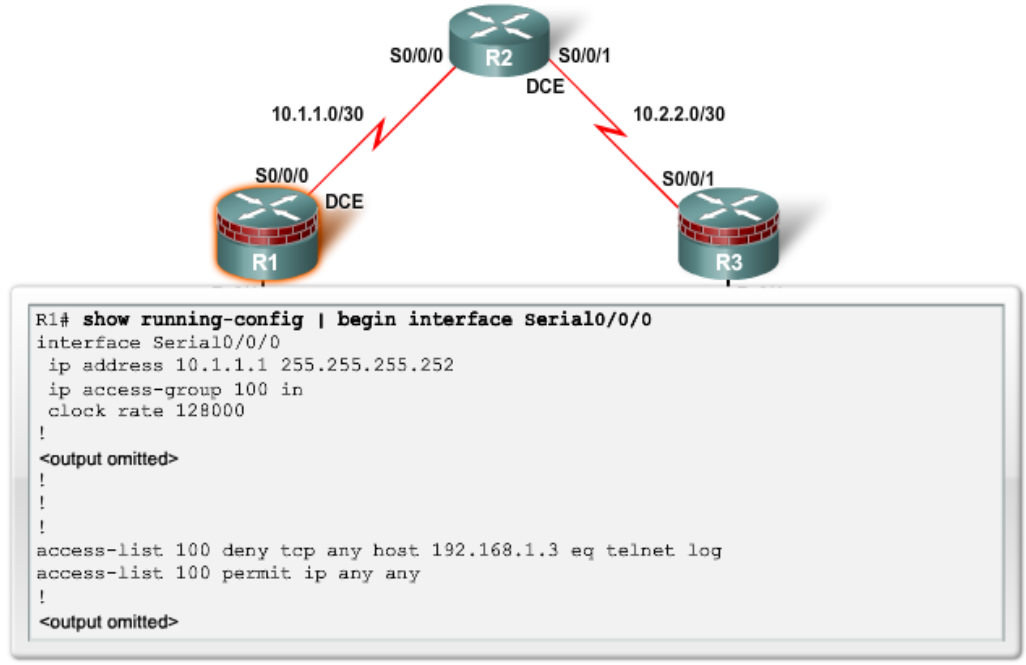
El show running-config puede ser utilizado para visualizar las interfaces que tienen ACLs aplicadas.



Pase por encima de R1 y PC1 para ver más información.



Pase por encima de R1 y PC1 para ver más información.



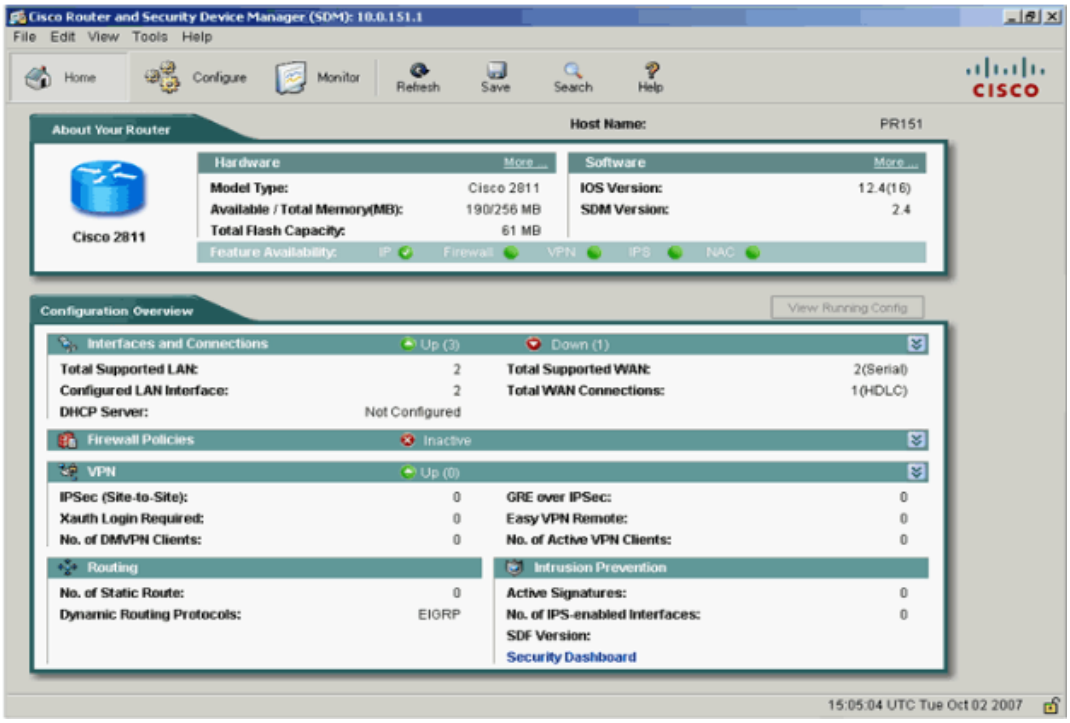
Pase por encima de R1 y PC1 para ver más información.

4.1.4 Configuracion de ACLs estandar y extendidas con SDM

Las ACLs se pueden configurar, ya sean estándar o extendidas, desde la CLI o usando el Administrador de Routers y Dispositivos de Seguridad de Cisco(SDM).

La ventana del SDM está dividida en dos marcos. El marco About Your Router contiene detalles de hardware y software. El marco Configuration Overview proporciona detalles de la configuración actual del router, incluyendo información de interfaz, firewall, VPN, enrutamiento e IPS.

El botón Configure arriba en la ventana de la aplicación SDM abre la lista de tareas (Tasks). Haga clic en el botón Additional Tasks para acceder a la página de configuración de ACLs.



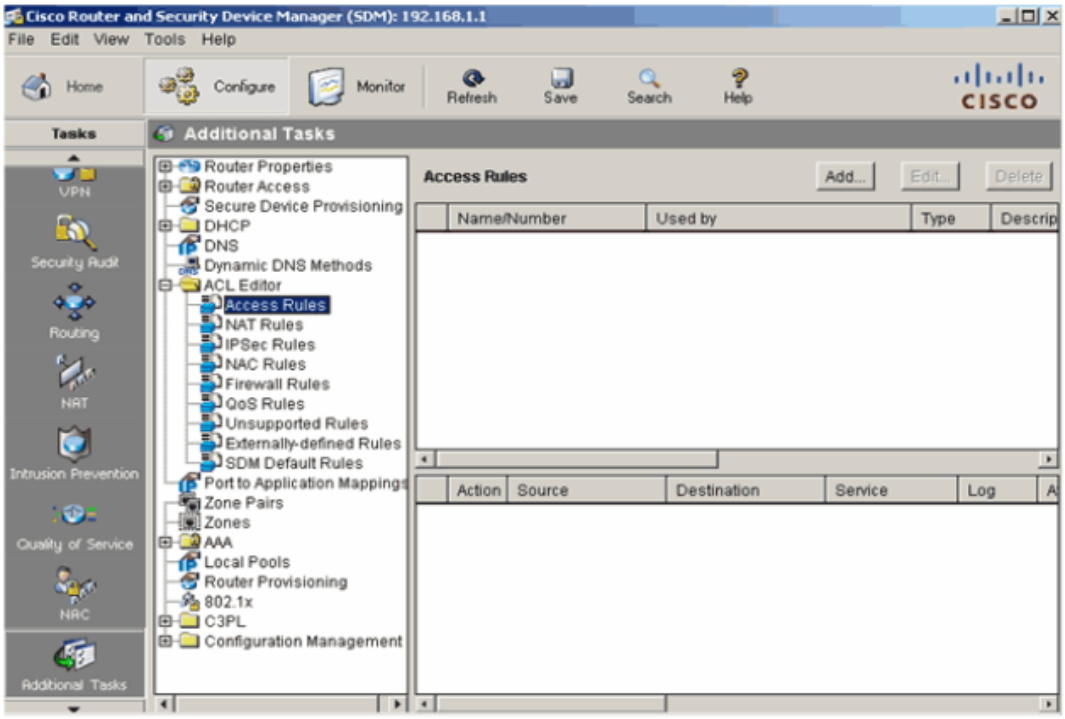
Las reglas definen cómo el router responde a un tipo particular de tráfico. A través del SDM de Cisco, el administrador puede crear reglas de acceso que causen que el router deniegue cierto tipo de tráfico pero permita algún otro. El SDM de Cisco proporciona reglas por defecto que el administrador puede utilizar al crear reglas de acceso.

El administrador también puede visualizar las reglas que no fueron creadas usando el SDM de Cisco, llamadas reglas externas, y las reglas cuya sintaxis el SDM de Cisco no soporta, llamadas reglas no soportadas.

La ventana SDM Rules (ACLs) Summary proporciona un resumen de las reglas en la configuración del router y acceso a otras ventanas para crear, editar y eliminar reglas. Para acceder a esta ventana, vaya a Configure > Additional Tasks > ACL Editor. Estos son los tipos de reglas que maneja el SDM de Cisco:

Reglas de acceso - Gobiernan el tráfico que ingresa y sale de la red. El administrador puede aplicar reglas de acceso a las interfaces y líneas vty del router.
Reglas NAT - Determinan qué direcciones IP privadas son traducidas a direcciones IP válidas de Internet.
Reglas IPsec - Determinan qué tráfico es cifrado en conexiones seguras.

Reglas NAC - Especifican qué direcciones IP son admitidas a la red o bloqueadas de ella.
Reglas de Firewall - Especifican las direcciones de origen y destino y si el tráfico será permitido o denegado.
Reglas QoS - Especifican el tráfico que pertenece a la clase de calidad de servicio (QoS) a la que la regla está asociada.
Reglas no soportadas - No fueron creadas usando el SDM de Cisco y no son soportadas por éste. Estas reglas sólo son leídas y no pueden ser modificadas usando el SDM de Cisco.
Reglas definidas externamente - No fueron creadas usando el SDM de Cisco pero son soportadas por éste. Estas reglas no pueden ser asociadas con ninguna interfaz.
Reglas SDM por defecto - Reglas predefinidas que utilizan los asistentes SDM de Cisco.



El SDM de Cisco se refiere a las ACLs como reglas de acceso. Al usar el SDM de Cisco, el administrador puede crear y aplicar reglas estándar (ACLs Estándar) y reglas extendidas (ACLs Extendidas). Estos son los pasos para configurar una regla estándar usando el SDM de Cisco:

Paso 1. Vaya a Configure > Additional Tasks > ACL Editor > Access Rules.

Paso 2. Haga clic en Add. Aparecerá la ventana Add a Rule. La lista desplegable contendrá sólo las interfaces cuyo estado sea up/up.

Paso 3. En la ventana Add a Rule, ingrese un nombre o número en el campo Name/Number.

Paso 4. En la lista desplegable Type, elija Standard Rule. También puede ingresar una descripción en el campo Description.

Paso 5. Haga clic en Add. Aparecerá la ventana Add a Standard Rule Entry.

Paso 6. En la lista desplegable "Select an action", elija Permit o Deny.

Paso 7. En la lista desplegable Type, elija un tipo de dirección:

A Network - (Red) Se aplica a todas las direcciones IP de una red o subred.
A Host Name or IP Address - (Dirección IP o nombre de host) Se aplica a una dirección IP o host específico.
Any IP address - (Cualquier dirección IP) Se aplica a cualquier dirección IP.

Paso 8. Dependiendo de lo que se haya seleccionado en la lista desplegable Type, deberán completarse estos campos adicionales:

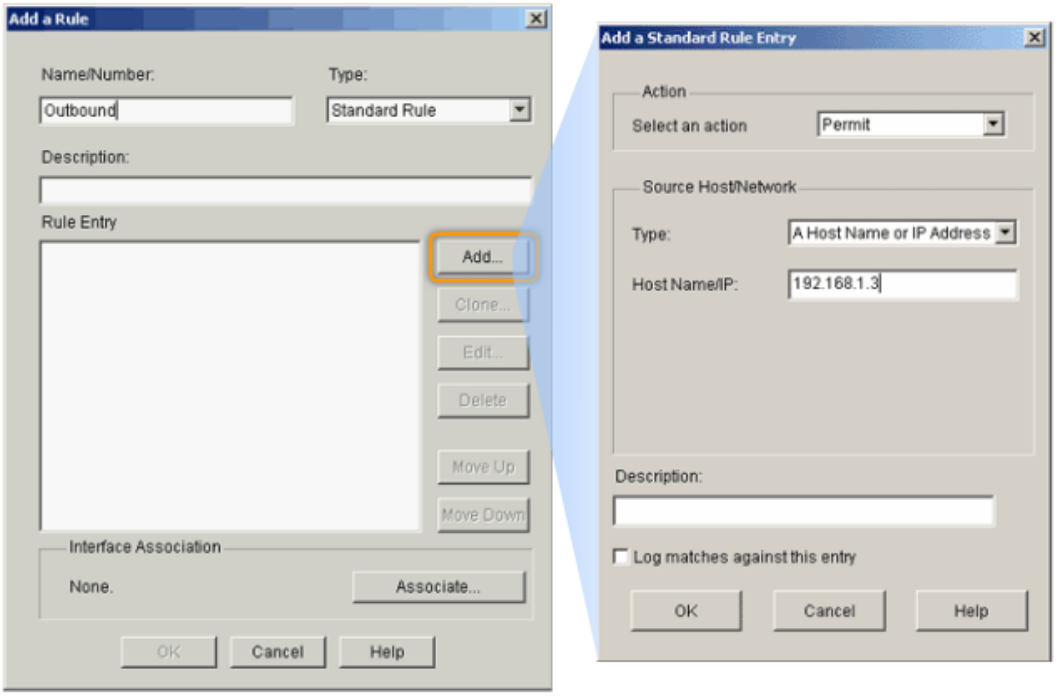
IP Address - (Dirección IP) Si seleccionó A Network, ingrese la dirección IP.
Wildcard Mask - (Máscara Wildcard) Si seleccionó A Network, especifique una máscara wildcar de la lista desplegable o ingrese una personalizada.
Hostname/IP - (Nombre de host/IP) Si seleccionó A Host Name or IP Address, ingrese el nombre o la dirección IP del host. Si ingresa un nombre de host, el router debe ser configurado para usar un servidor DNS.

Paso 9. (Opcional) Ingrese una descripción en el campo Description. La descripción debe tener menos de 100 caracteres.

Paso 10. (Opcional) Marque la casilla Log matches against this entry. Dependiendo de la configuración de syslog en el router, las coincidencias serán registradas en el buffer de registro local, enviadas a un servidor syslog o ambas.

Paso 11. Haga clic en OK.

Paso 12. Continúe agregando o editando entradas a la lista hasta que la ACL estándar esté completa. Si en algún momento desea cambiar el orden de las entradas en la lista Rule Entry, use los botones Move Up y Move Down.



Una vez completada la lista Rule Entry, el siguiente paso es aplicar la lista a una interfaz. Estos son los pasos necesarios para aplicar una regla a una interfaz:

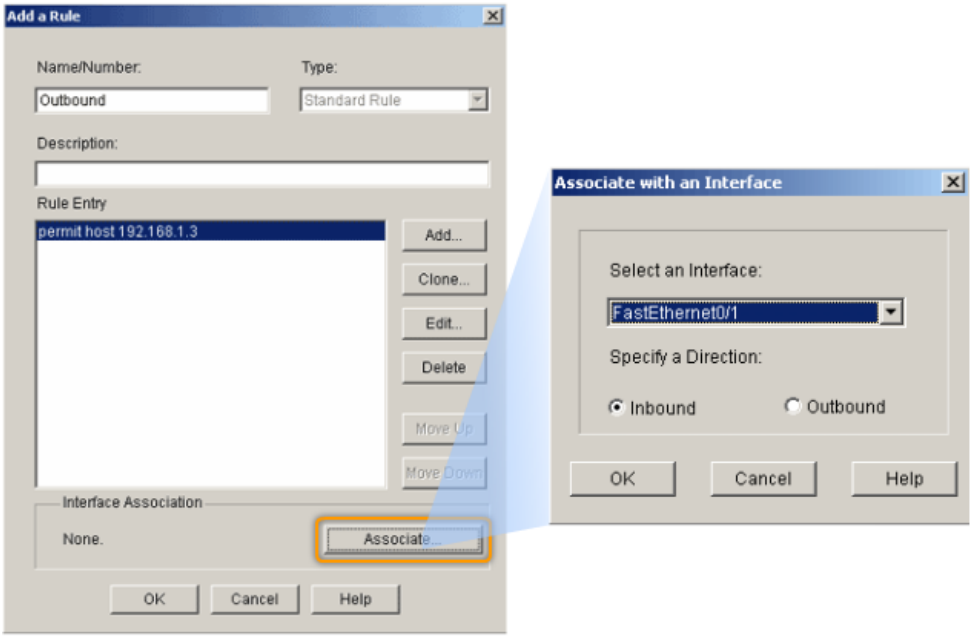
Paso 1. En la ventana Add a Rule, haga clic en Associate. Aparecerá la ventana "Associate with an Interface".

Paso 2. En la lista desplegable Select an Interface, elija la interfaz a la que se aplicará la regla. Sólo se mostrarán las interfaces cuyo estado sea up/up.

Paso 3. En la sección Specify a Direction, haga clic en Inbound o Outbound. Si el router debe revisar los paquetes que ingresan a la interfaz, haga clic en Inbound, en cambio, si el router debe reenviar el paquete a la interfaz de salida antes de compararlo con las entradas en la regla de acceso, haga clic en Outbound.

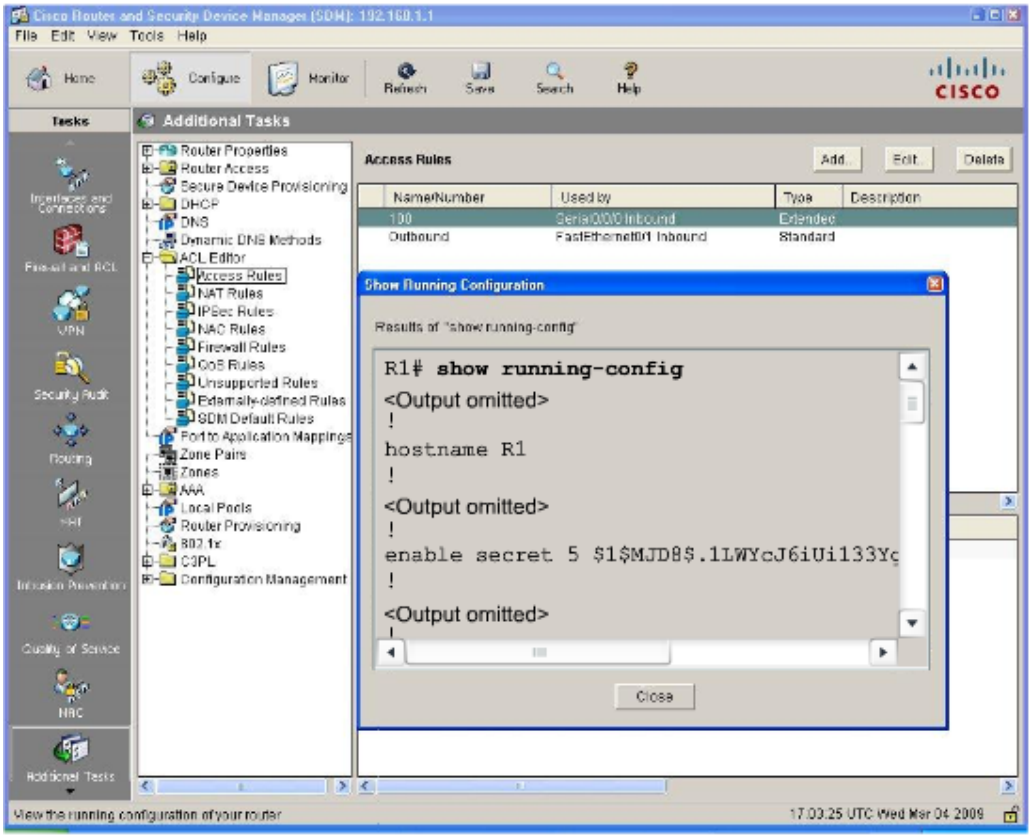
Paso 4. Si ya hay una regla asociada a la interfaz designada en la dirección deseada, aparecerá una ventana de información con las siguientes opciones:

Cancel the operation (Cancelar la operación).
Continue with the operation by appending the new rule entries to the access rule that is already applied to the interface (Continuar con la operación agregando las nuevas entradas a la regla de acceso ya aplicada a la interfaz).
Disassociate the existing rule from the interface and associate the new rule instead (Desasociar la regla existente de la interfaz y asociar la nueva regla en su lugar).



Para visualizar los comandos IOS generados por el SDM y enviados al router, vaya al archivo de configuración actual seleccionando View de la barra de menú seguido de Running Config.

Para configurar ACLs que manejen tráfico en ambos sentidos, como el de aplicaciones basadas en TCP, existen varias soluciones en los IOS.



4.1.5 Configuracion de TCP established y ACLs reflexivas

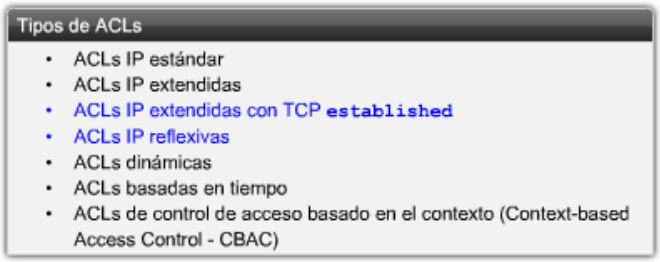
Con el tiempo, los ingenieros han creado filtros más sofisticados basándose en parámetros cada vez más precisos. Los ingenieros también han expandido el rango de plataformas y el rango de ACLs que pueden ser procesadas a la velocidad máxima del cable (wirespeed). Estas mejoras a las plataformas y las ACLs permiten a los profesionales de la seguridad en redes implementar soluciones de firewall de última generación sin sacrificar el rendimiento de la red.

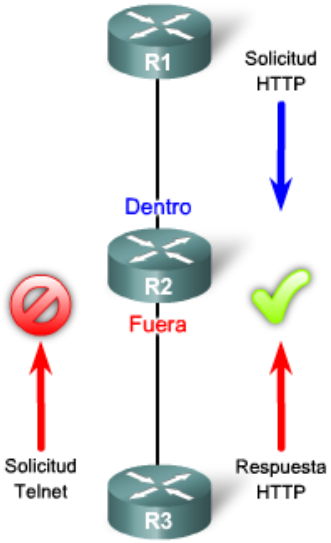
En una red moderna, el firewall de la red debe ubicarse entre el interior y el exterior de la red. La idea básica es que se bloquee el acceso al tráfico del exterior salvo que se lo permita explícitamente por medio de una ACL, o, si se trata de tráfico de retorno, que el mismo se corresponda con tráfico que se inició dentro de la red interna. Este es el rol fundamental de un firewall de red, ya sea un dispositivo de hardware dedicado o un router Cisco con un IOS firewall.

Muchas aplicaciones comunes usan TCP, ya que forma un circuito virtual entre dos extremos. La solución de filtrado de tráfico IOS de primera generación que soporta la naturaleza de dos vías de los circuitos virtuales TCP es la palabra clave TCP established de las ACLs IP extendidas. Presentada en 1995, la palabra clave established para las ACLs IP extendidas dió pie a la creación de un firewall de red primitivo en un router Cisco. Este bloqueaba todo el tráfico que provenía de Internet excepto el tráfico de respuesta de TCP asociado con el tráfico TCP establecido iniciado dentro de la red.

La solución de filtrado de sesiones de segunda generación fueron las ACLs reflexivas. Las ACLs reflexivas fueron introducidas al IOS en 1996. Estas ACLs filtran el tráfico basándose en las direcciones de origen y destino y los números de puerto, además de monitorear las sesiones. El filtrado de sesiones de las ACLs reflexivas usa filtros temporales que se eliminan una vez que la sesión finaliza.

La opción TCP established y las ACLs reflexivas son ejemplos de ACLs complejas.





Esta es la sintaxis de la opción TCP established en una ACL IP extendida numerada.

Router(config)# access-list {100-199} {permit | deny} protocolo dir-origen [wildcard-origen] [operador operando] dir-destino [wildcard-destino] [operador operando] [established]

La palabra clave established fuerza al router a revisar si los flags de control TCP ACK o RST están activados. Si el flag ACK está activado, se permite el tráfico TCP. Si no lo está, se asume que el tráfico está asociado con una nueva conexión iniciada fuera de la red.

El uso de la palabra clave established no implementa un firewall de estados en el router. No se mantiene información de estados para monitorear el tráfico iniciado dentro de la red. Todo lo que hace el parámetro established es permitir el paso de los segmentos TCP con el flag de control apropiado. El router no monitorea las conversaciones para determinar si el tráfico es de retorno, asociado con una conexión iniciada dentro de la red.

Por lo tanto, el uso de la palabra clave established para permitir el tráfico de retorno abre una brecha de seguridad en el router. Un hacker puede aprovecharse de esta brecha usando un generador de paquetes o escáner, como Nmap, para pasar paquetes TCP adentro de la red disfrazándolos como tráfico de retorno. Los hackers logran esto usando el generador de paquetes para que establezca el bit o los bits apropiados en el campo de control TCP.

La opción established no se aplica al tráfico UDP o ICMP, ya que el tráfico UDP e ICMP no utiliza flags de control como lo hace el tráfico TCP.

Segmento TCP

Posición de bits	Bits 0-3	4-7	8-15							16-31
0	Puerto origen									Puerto destino
32	Número de secuencia									
64	Número de confirmación									
96	Checksum	Reservado	CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Tamaño de ventana
128	Checksum		Puntero urgente							
160	Opciones (opcional)									
160/192+	Datos									

Paquete IP

+	0-3	4-7	8-15	16-18	19-31
0	Versión	Longitud del encabezado	Tipo de servicio (ahora DiffServ y ECN)	Longitud total	
32	Identificación			Flags	Posición del fragmento
64	Time to Live		Protocolo	Checksum del encabezado	
96	Dirección de origen				
128	Dirección de destino				
160	Opciones				
160 o 192+	Datos				

A pesar de la brecha de seguridad, el uso de la palabra clave established no proporciona una solución más segura ya que sólo hay coincidencia si el paquete TCP tiene los bits de control ACK o RST activados.

R1(config)# access-list 100 permit tcp any eq 443 192.168.1.0 0.0.0.255 established

R1(config)# access-list 100 permit tcp any 192.168.1.3 0.0.0.0 eq 22

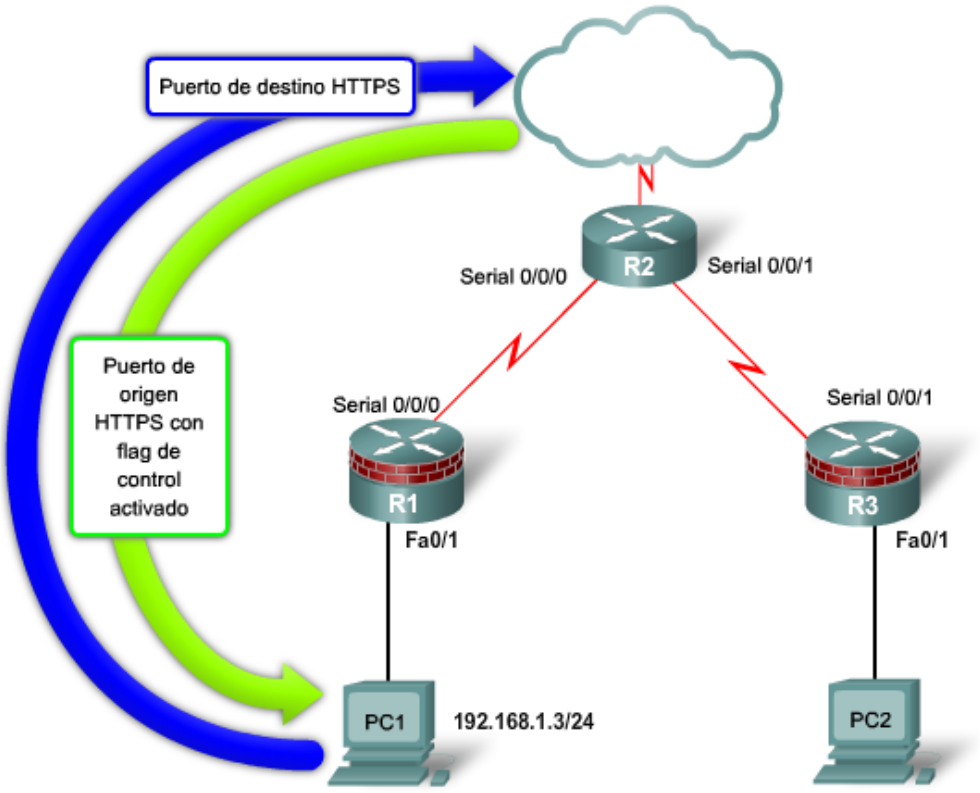
R1(config)# access-list 100 deny ip any any

R1(config)# interface s0/0/0

R1(config-if)# ip access-group 100 in

Si la palabra clave established se omitiera, todo el tráfico TCP que proviniera del puerto 443 se permitiría. Con la palabra clave, sólo el tráfico del puerto 443 que tenga el flag de control TCP ACK se permitirá.

Como es común en una configuración de firewall, todo el tráfico entrante se deniega salvo que se permita explícitamente (tráfico SSH, puerto 22) o salvo que esté asociado con tráfico que se genera dentro de la red (tráfico HTTPS en este caso). Se permite todo el tráfico que provenga del puerto 443 y de fuera de la red con el flag de control apropiado.



Las ACLs reflexivas fueron introducidas al IOS de Cisco en 1996, aproximadamente un año después de que se habilitó la opción established. Las ACLs reflexivas proporcionan una forma más real de filtrado de sesiones que el que ofrece la opción TCP established. Las ACLs reflexivas son mucho más difíciles de falsificar ya que deben coincidir muchos más criterios de filtrado antes de que se permita acceso a un paquete. Por ejemplo, se revisan las direcciones de origen y destino y los números de puerto, no sólo los bits ACK y RST. Además, el filtrado de sesiones usa filtros temporales que se eliminan una vez que la sesión finaliza. Esto agrega un límite de tiempo a la oportunidad de ataque del hacker.

La palabra clave established está disponible sólo para el protocolo TCP de capa superior. Los otros protocolos de capa superior, como UDP e ICMP, deben o permitir todo el tráfico ingresante o definir todos los pares de puertos y direcciones de origen y destino posibles, para cada protocolo.

La mayor limitación de las ACLs estándar y extendidas es que fueron diseñadas para filtrar conexiones unidireccionales en lugar de bidireccionales. Las ACLs estándar y extendidas no monitorean el estado de la conexión. Si alguien dentro de la red envía tráfico a Internet, es difícil permitir el ingreso a la red del tráfico de retorno de una manera segura sin abrir una gran brecha en el router de perímetro. Las ACLs reflexivas fueron desarrolladas para este propósito. Permiten al administrador realizar filtrado de sesiones para cualquier tipo de tráfico IP.

Las ACLs reflexivas trabajan utilizando entradas de control de acceso (ACEs) temporales insertadas en una ACL extendida, que se aplica en la interfaz externa del router de perímetro. Una vez que la sesión finaliza o la entrada temporal vence, es eliminada de la configuración de la ACL en la interfaz externa. Esto reduce la exposición de la red a ataques de DoS.

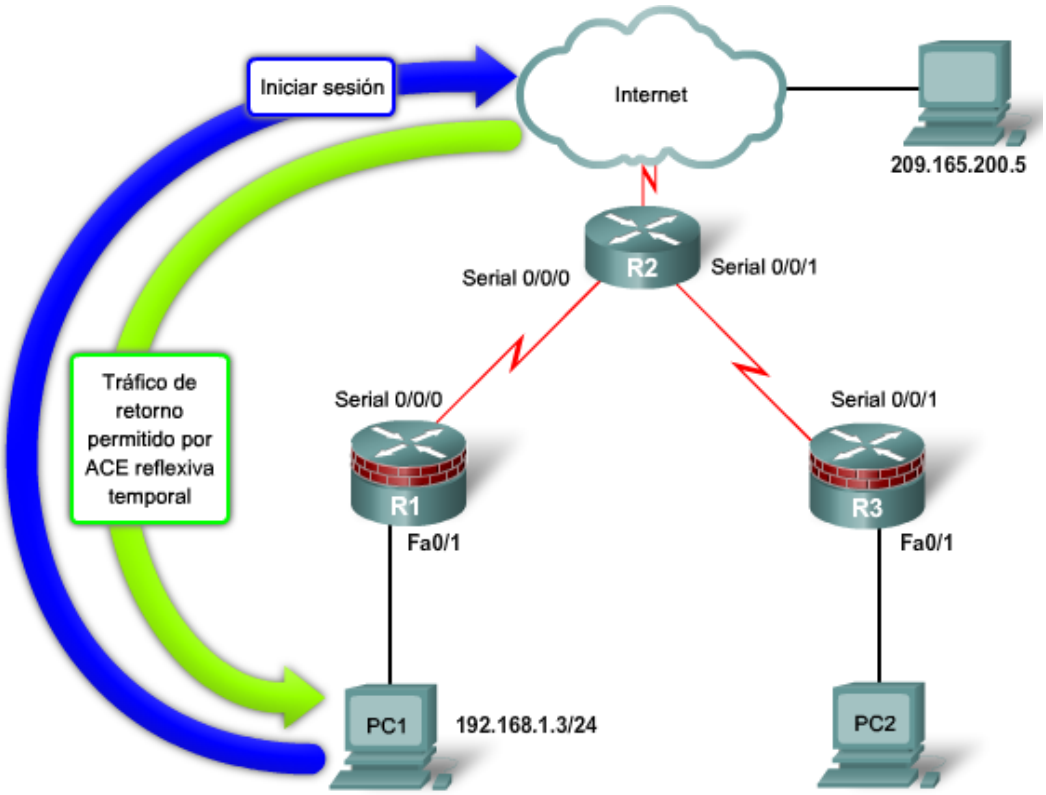
Para que esto funcione, una ACL extendida nombrada examina el tráfico a medida que éste sale de la red. La ACL puede ser aplicada como de entrada en una interfaz interna o de salida en una interfaz externa. Las ACEs examinan el tráfico asociado con nuevas sesiones usando el parámetro reflect. Las ACEs de conexión se crean dinámicamente basándose en estas sentencias (usando reflect) para permitir el tráfico de retorno. Sin las sentencias reflect, el tráfico de retorno se descarta por defecto. Por ejemplo, el administrador puede configurar las sentencias de la ACL para que examinen sólo las conexiones HTTP, permitiendo entonces la creación de ACEs reflexivas sólo temporales para el tráfico HTTP.

A medida que el tráfico deja la red, si coincide con una sentencia de permiso con un parámetro reflect, se agrega una entrada temporal a la ACL reflexiva. Por cada sentencia permit-reflect, el router crea una ACL reflexiva aparte.

La ACE reflexiva es una entrada invertida: la información de origen y destino se da vuelta. Por ejemplo, cuando un usuario en la estación de trabajo con la dirección IP 192.168.1.3 hace telnet 209.165.200.5, donde el número de puerto de origen es el 11000, se crea una ACE reflexiva como la siguiente:

```
R1(config-ext-nacl)# permit host 209.165.200.5 eq 23 host 192.168.1.3 eq 11000
```

Cualquier ACE reflexiva temporal que se cree contendrá la acción permit para permitir el ingreso a la sesión del tráfico de retorno.



La configuración de un router para que use ACLs reflexivas requiere sólo unos pocos pasos:

Paso 1. Cree una ACL interna que busque nuevas sesiones de salida y cree ACEs reflexivas temporales.

Paso 2. Cree una ACL externa que use las ACLs reflexivas para examinar el tráfico de retorno.

Paso 3. Active la ACL nombrada en las interfaces apropiadas.

Esta es la sintaxis de una ACL interna.

Router(config)# ip access-list extended nombre_ACL_interna

Router(config-ext-nacl)# permit protocolo dir-origen [máscara-origen] [operador operando] dir-destino [máscara-destino] [operador operando] [established] reflect nombre_ACL_reflexiva [timeout segundos]

Por ejemplo, estos son los comandos que se ajustan a una situación en que los usuarios internos navegan por Internet con un navegador web usando DNS.

R1(config)# ip access-list extended internal_ACL

R1(config-ext-nacl)# permit tcp any any eq 80 reflect web-only-reflexive-ACL

R1(config-ext-nacl)# permit udp any any eq 53 reflect dns-only-reflexive-ACL timeout 10

El IOS de Cisco crea dos ACEs reflexivas que mantienen información de sesión de conexiones web de salida (web-only-reflexive-ACL) y consultas DNS (dns-only-reflexive-ACL). Note que se ha configurado un tiempo de vencimiento de 10 segundos para las consultas DNS.

Luego de crear la ACL nombrada interna extendida, lo cual origina las ACEs reflexivas, debe hacerse referencia a las entradas temporales a medida que el tráfico fluye de vuelta a la red. Esto se logra creando una segunda ACL nombrada extendida. En esta ACL nombrada, se usa la sentencia evaluate para hacer referencia a las ACEs reflexivas que fueron creadas por la ACL interna.

Router(config)# ip access-list extended nombre_ACL_externa

Router(config-ext-nacl)# evaluate nombre_ACL_reflexiva

Continuando el ejemplo con tráfico HTTP y DNS, esta sintaxis crea una ACL externa que deniega todo el tráfico que se origina fuera de la red, pero permite el tráfico HTTP y DNS de retorno.

R1(config)# ip access-list extended external_ACL

R1(config-ext-nacl)# evaluate web-only-reflexive-ACL

R1(config-ext-nacl)# evaluate dns-only-reflexive-ACL

R1(config-ext-nacl)# deny ip any any

El último paso consiste en aplicar las ACLs.

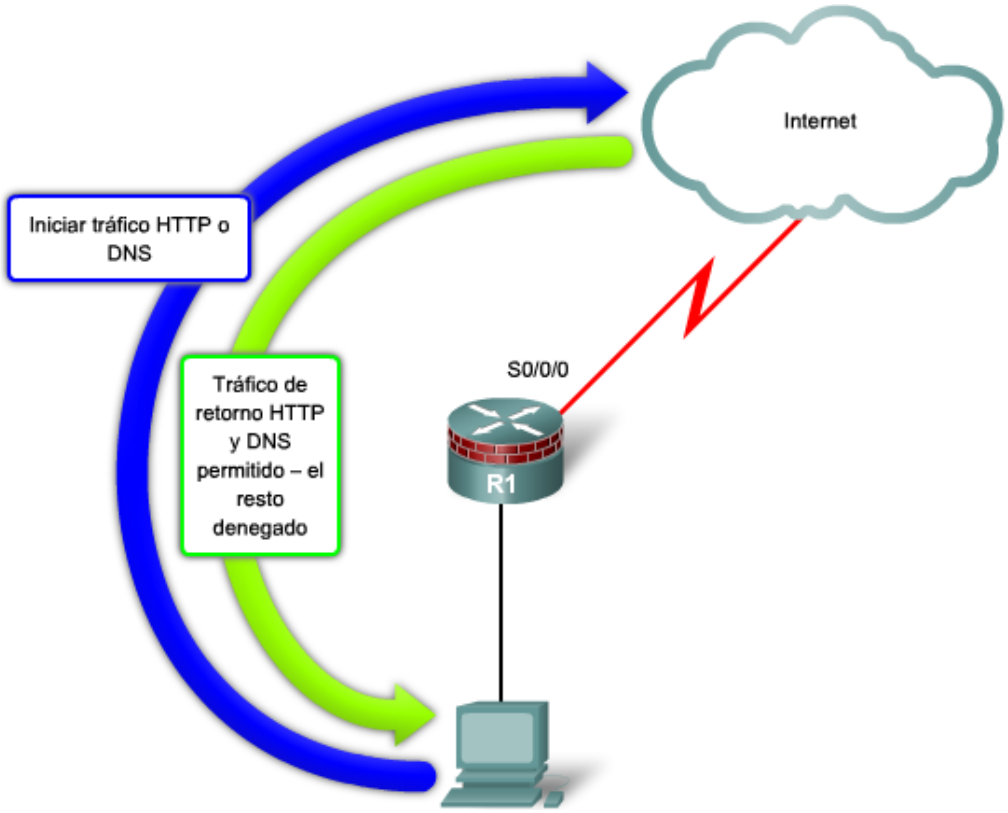
R1(config)# interface s0/0/0

R1(config-if)# description connection to the ISP.

R1(config-if)# ip access-group internal_ACL out

R1(config-if)# ip access-group external_ACL in

Las ACLs reflexivas proporcionaron la primera solución para el filtrado de sesiones en los routers Cisco. Las ACLs reflexivas son sólo uno de los diferentes tipos de ACLs complejas soportadas en los dispositivos de networking de Cisco. Algunas ACLs complejas son diseñadas para permitir conexiones dinámicas a través de routers construidas bajo demanda del usuario. Otras ACLs complejas se habilitan automáticamente en fechas u horas particulares.



4.1.6 Configuracion de ACLs dinamicas

Las ACLs dinámicas, también conocidas como "lock and key", fueron agregadas como una opción en los IOS de Cisco en 1996, antes que las ACLs reflexivas y el registro de ACLs estuviesen disponibles. Las ACLs dinámicas sólo pueden ser utilizadas para tráfico IP. Dependen de conectividad Telnet, autenticación (local o remota) y ACLs extendidas.

La configuración de una ACL dinámica comienza con la aplicación de una ACL extendida para bloquear el tráfico en el router. Los usuarios que quieran atravesar el router serán bloqueados hasta que utilicen Telnet para conectarse al router y logren autenticarse. La conexión Telnet es entonces descartada y se agrega una ACL dinámica de una sola entrada a la ACL extendida existente. Esto permite tráfico por un período de tiempo particular. El vencimiento puede ser tanto absoluto o por inactividad.

Una de las razones por las que pueden usarse ACLs dinámicas es para proporcionar a un usuario remoto específico o un grupo de usuarios remotos acceso a un host dentro de la red. Otra razón puede ser cuando un subgrupo de hosts de una red local necesita acceder a un host en una red remota que está protegido con un firewall.

Las ACLs dinámicas ofrecen estos beneficios de seguridad sobre las ACLs estándar y extendidas:

Mecanismo de desafío para autenticar usuarios individuales
Administración simplificada en grandes redes
Procesamiento reducido para ACLs

Menores oportunidades para los hackers de forzar una entrada a la red
Creación de acceso dinámico de usuarios a través de un firewall, sin comprometer otras restricciones de seguridad configuradas.

Tipos de ACLs

- ACLs IP estándar
- ACLs IP extendidas
- ACLs IP extendidas con TCP **`established`**
- ACLs IP reflexivas
- ACLs dinámicas
- ACLs basadas en tiempo
- ACLs de control de acceso basado en el contexto (Context-based Access Control - CBAC)

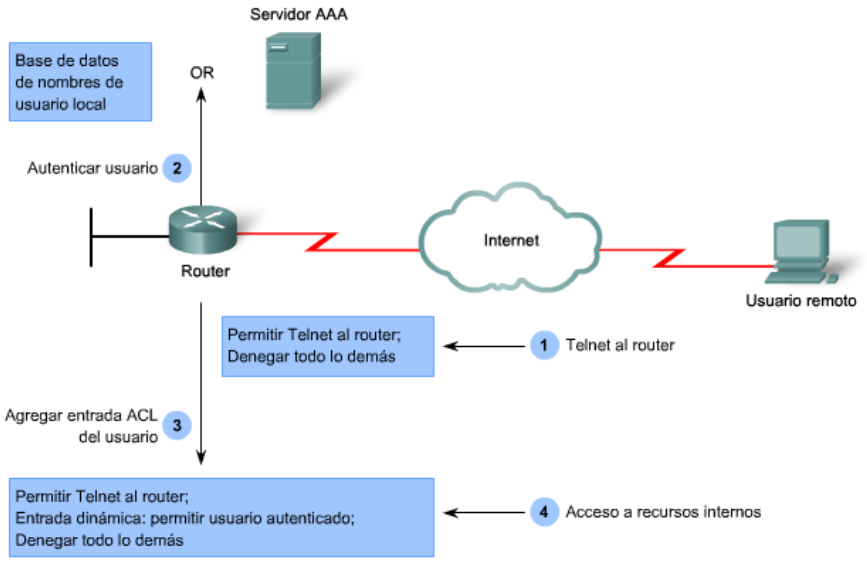
Una combinación de actividades solicitadas al usuario y automáticas ocurre en los dispositivos cuando se implementa e invoca una ACL dinámica.

Primero, el usuario remoto debe abrir una conexión Telnet o SSH al router, que la ACL externa del router debe permitir. Luego, el router pide al usuario su nombre de usuario y contraseña.

En el siguiente paso, el router autentica la conexión usando una base de datos de usuarios local definida con los comandos username, un servidor AAA que use los protocolos RADIUS o TACACS+ o el comando password en las líneas vty. Si la autenticación es exitosa, la conexión Telnet o SSH se cierra, ya que su función era exclusivamente de autenticación.

Una vez que el usuario ha sido autenticado exitosamente, el IOS de Cisco agrega una entrada a la ACL dinámica que ofrece acceso al usuario a los recursos internos configurados. No es posible establecer políticas de acceso por usuario. En su lugar, el administrador define una política para todos los usuarios de ACLs dinámicas y esta política se aplica a todos los usuarios autenticados.

Finalmente, el usuario puede acceder a los recursos internos, a los que, sin la entrada en la ACL dinámica no tendría acceso.



La configuración de una ACL dinámica toma unos pocos pasos básicos:

Paso 1. Cree una ACL extendida.

La ACL dinámica soporta ACLs extendidas tanto numeradas como nombradas. Una de las primeras entradas en la ACL permite acceso Telnet o SSH a una dirección IP en el router que los usuarios externos pueden utilizar. Además, como mínimo, se crea una entrada de reserva de lugar en la ACL, que, una vez que un usuario se autentica exitosamente, toma valores dinámicos concretos. La autenticación exitosa del usuario crea esta entrada dinámica.

Paso 2. Defina la autenticación.

Las ACLs dinámicas soportan los siguientes métodos de autenticación: local (base de datos de nombres de usuario), por servidor AAA externo y la contraseña de línea. Típicamente, la contraseña de línea no se utiliza porque con este método todos los usuarios deben emplear la misma contraseña.

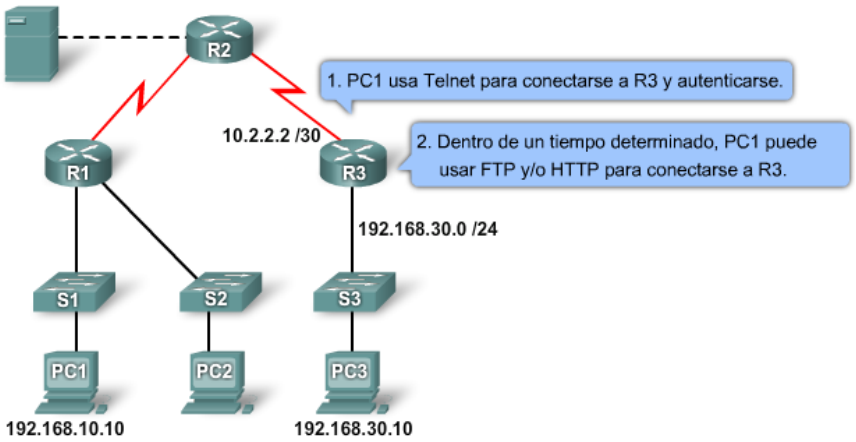
Paso 3. Habilite el método de autenticación dinámico.

Esto toma lugar en las líneas vty del router. Una vez que se habilita, el usuario puede crear entradas para la ACL dinámica en la ACL de la interfaz que hace referencia a la ACL dinámica.

Este es el comando usado para crear la entrada de ACL dinámica.

Router(config)# access-list {100-199} dynamic nombre_ACL_dinámica [timeout minutos] {permit | deny} protocolo dir-origen [wildcard-origen] [operador operando] dir-destino [wildcard-destino] [operador operando] [established]

La palabra clave dynamic permite al administrador especificar el nombre de la ACL dinámica que se usará. Este nombre debe ser único entre todas las ACLs nombradas en el router. El parámetro timeout es opcional. Especifica un vencimiento absoluto de la entrada dinámica que crea un usuario autenticado. El rango posible del vencimiento es de 1 a 9999 minutos.



Dos vencimientos están asociados con las entradas ACL: los absolutos y los que ocurren por inactividad. El vencimiento absoluto se especifica en la entrada de la ACL dinámica, mientras que el valor de vencimiento por inactividad se especifica por medio del comando autocommand, el cual habilita la autenticación lock and key en las líneas vty. Si no se especifican los tiempos de vencimiento, por defecto, la entrada nunca se vencerá. Por lo tanto, se recomienda configurar un tiempo de vencimiento, sea absoluto o por inactividad.

Luego del parámetro de vencimiento en la sentencia ACL, especifique qué tráfico de usuario deberá permitirse. Normalmente, se desconoce la dirección IP del usuario externo, por lo que deberá usar la palabra clave any.

Luego de crear la ACL extendida, para habilitar el permiso a Telnet y/o SSH y las entradas dinámicas, actívela en la interfaz del router con el comando ip access-group.

Habiendo configurado una base de datos de usuarios local, la última cosa que queda por hacer es habilitar la autenticación lock and key en las líneas vty.

Router(config)# line vty 0 4

Router(config-line)# autocommand access-enable host [timeout minutes]

El comando autocommand access-enable especifica la autenticación lock and key. Luego de que un usuario se autentica exitosamente, se inserta una entrada temporal en la ACL extendida. Esta entrada se ubica en el parámetro dynamic que reserva el lugar en la ACL extendida. La entrada temporal se agrega sólo en la interfaz a la que el usuario se conecta. Sin el comando autocommand access-enable, el router no creará las entradas ACL temporales.

El parámetro host es opcional. Cuando se especifica este parámetro, el IOS de Cisco reemplaza la palabra clave any de la ACL dinámica con la dirección IP del usuario. Si se aplica la ACL extendida como de entrada, la palabra clave any del origen se reemplaza con la dirección IP del usuario; si se aplica como de salida, la palabra clave que se reemplaza es la any de destino.

El parámetro de vencimiento opcional se usa para configurar el vencimiento por inactividad de la entrada temporal de la ACL del usuario.

Paso 1	`R3(config)# username Student password 0 cisco`
Paso 2	`R3(config)# access-list 101 permit tcp any host 10.2.2.2 eq telnet` `R3(config)# access-list 101 dynamic testlist timeout 15 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255`
Paso 3	`R3(config)# interface serial 0/0/1` `R3(config-if)# ip access-group 101 in`

Paso 4	`R3(config)# line vty 0 4`
	`R3(config-line)# login local`
	`R3(config-line)# autocommand access-enable host timeout 5`

Paso 1

Crea un nombre y una contraseña para autenticación.

Pase el puntero por encima de cada paso para más información.

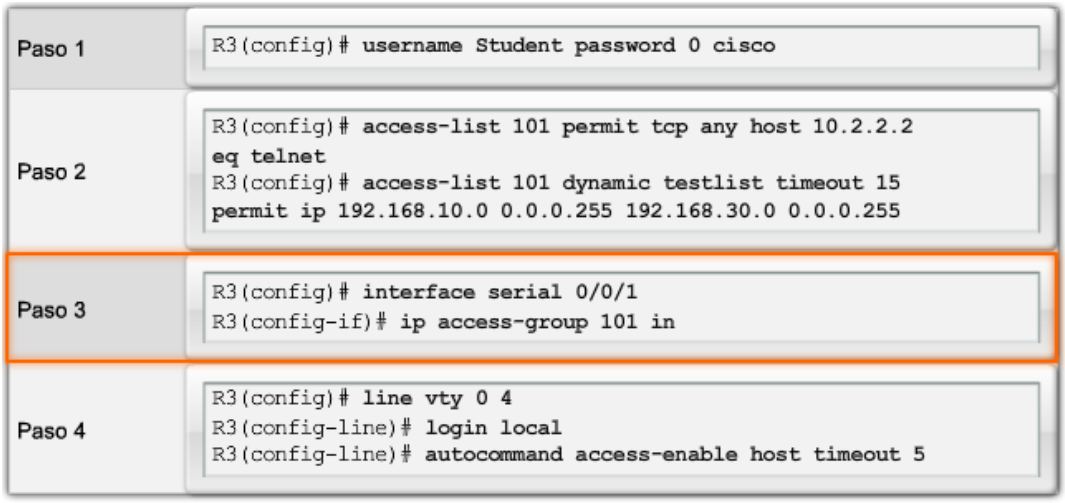
Paso 1	`R3(config)# username Student password 0 cisco`
Paso 2	`R3(config)# access-list 101 permit tcp any host 10.2.2.2 eq telnet` `R3(config)# access-list 101 dynamic testlist timeout 15 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255`
Paso 3	`R3(config)# interface serial 0/0/1` `R3(config-if)# ip access-group 101 in`

Paso 4	`R3(config)# line vty 0 4`
	`R3(config-line)# login local`
	`R3(config-line)# autocommand access-enable host timeout 5`

Paso 2

Permite al usuario abrir una conexión Telnet al router. La entrada ACL dinámica es ignorada hasta que se dispara el lock-and-key. La ventana se abrirá por 15 minutos y se cerrará automáticamente, esté siendo usada o no.

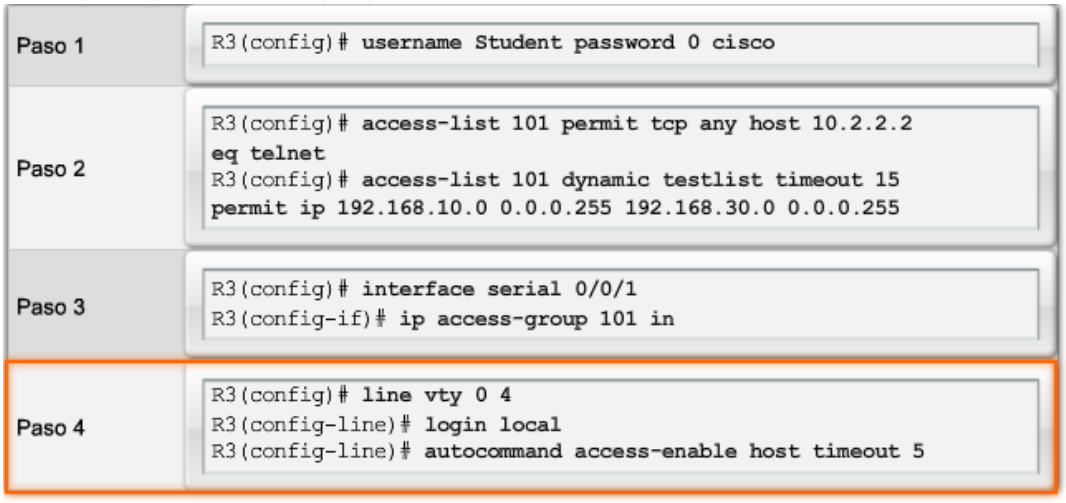
Pase el puntero por encima de cada paso para más información.



Paso 3

Aplica la ACL 101 a la interfaz S0/0/1.

Pase el puntero por encima de cada paso para más información.



Paso 4

Una vez que el usuario se autenticó por Telnet, se ejecuta el comando **autocommand** y la sesión Telnet termina. El usuario ahora puede acceder a la red 192.168.30.0. Si hay hasta 5 minutos de inactividad, la ventana se cierra.

Pase el puntero por encima de cada paso para más información.

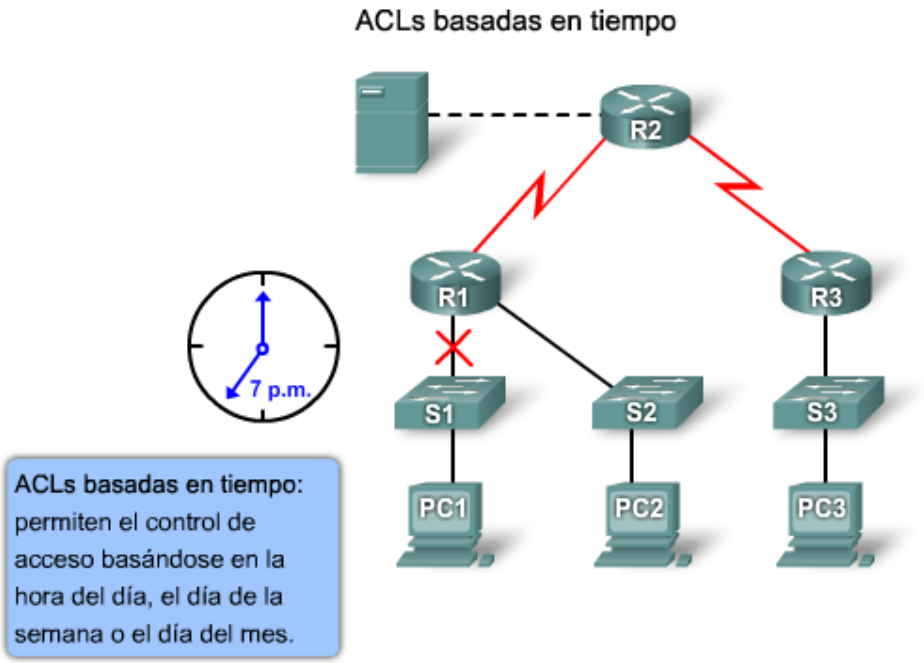
4.1.7 Configuracion de ACLs basadas en tiempo (Time-Based ACL)

Otra ACL compleja útil es la ACL basada en tiempo. Las ACLs basadas en tiempo, introducidas en el IOS de Cisco en 1998, son similares a las ACLs extendidas en función, salvo que además restringen el tráfico en base a la hora del día, el día de la semana o el día del mes.

Las ACLs basadas en tiempo ofrecen al profesional de la seguridad mayor control sobre los permisos de acceso a los recursos. En ocasiones, es necesario abrir una brecha de seguridad en el filtro de un router para permitir un tipo específico de tráfico. Este agujero no debe permanecer indefinidamente. Por ejemplo, puede permitirse a los usuarios acceder a Internet durante el almuerzo, pero no durante las horas de trabajo. Las ACLs basadas en tiempo permiten aplicar este tipo de política.

Las ACLs basadas en tiempo también permiten a los profesionales de la seguridad controlar los mensajes de registro. Las entradas ACL pueden registrar el tráfico en ciertos momentos del día, pero no constantemente. El administrador puede simplemente denegar el acceso sin analizar los varios registros generados durante las horas pico.

Las ACLs basadas en tiempo son una extensión de las ACLs extendidas numeradas y nombradas. El administrador crea entradas basadas en tiempo y usa el parámetro time-range para especificar el período de tiempo que la sentencia ACL será válida. El período de tiempo especificado puede ser recurrente o una instancia específica que ocurra una sola vez.



Al crear un rango de tiempo con el comando time-range, éste debe tener un nombre único. El nombre debe comenzar con una letra y no puede contener espacios. Utilice este nombre para asociar una sentencia ACL específica con este rango. La ejecución del comando time-range ubica al router en el modo de subconfiguración de ACL. En este modo, se pueden especificar dos tipos de rangos: de una sola vez (absoluto) y recurrente (periódico).

Estos son los comandos para la creación de un rango de tiempo.

Router(config)# time-range nombre_rango

Router(config-time-range)# absolute [hora_inicio fecha_inicio] [hora_fin fecha_fin]

Router(config-time-range)# periodic día_de_la_semana hh:mm to [día_de_la_semana] hh:mm

El comando absolute especifica un único período de tiempo para el cual el rango de tiempo es válido. Las sentencias ACL que hacen referencia a este rango de tiempo no son utilizadas luego de este período. El administrador puede especificar un tiempo de inicio, un tiempo de finalización o ambos. El tiempo especificado es de 24 horas: hh:mm, donde las horas pueden ir desde 0 hasta 23 y los minutos, desde 0 hasta 59. Por ejemplo, las 3 p.m. se representa como 15:00. La fecha se especifica como día mes año. El día se especifica como un número que puede ir de 1 a 31, el mes es el nombre del mes en inglés, como "May", y el año es un valor de cuatro dígitos, como 2003. Ejemplos de especificaciones de fechas son 19 November 2009 y 07 July 2010. Si se omite el tiempo de inicio, por defecto se usa la hora del router. Si se omite el tiempo de finalización, por defecto se usa 23:59 31 December 2035.

El comando periodic especifica un período de tiempo recurrente para el cual el rango de tiempo es válido. Se permiten múltiples comandos periodic dentro del mismo rango de tiempo. Especifique el tiempo de inicio y de finalización. El tiempo de finalización puede pertenecer a un día diferente. El primer parámetro especificado es el día de la semana (en inglés):

monday
tuesday
wednesday
thursday
friday
saturday
sunday
daily (todos los días)
weekdays (de lunes a viernes)
weekend (sábado y domingo)

El siguiente parámetro es el tiempo de inicio, especificado como hh:mm, seguido del parámetro to y el tiempo de finalización. Si se omite el parámetro del día de la semana, por defecto se usa el día de la semana configurado para el tiempo de inicio. Luego de esto va el tiempo de finalización, especificado como hh:mm. Es importante tomar en cuenta que el reloj del router debe estar configurado para que este comando opere como se requiere.

Luego de crear los rangos de tiempo, el administrador debe activarlos. Esto se logra agregando el parámetro time-range a la sentencia ACL. Las ACLs extendidas, tanto nombradas como numeradas, soportan esta función. Esta es la sintaxis de configuración de una ACL numerada.

Router(config)# access-list {100-199} {permit | deny} protocolo dir-origen [máscara-origen] [operador operando] dir-destino [máscara-destino] [operador operando] [established][log | log-input][established][time-range nombre_del_rango_de_tiempo]

Debe agregarse el rango de tiempo a la sentencia ACL. Una vez hecho esto, el IOS de Cisco procesa la sentencia ACL sólo cuando el tiempo del router cae dentro del período especificado por los comandos periodic o absolute definidos en la configuración time-range.

Paso 1	R1(config)# **time-range EVERYOTHERDAY** R1(config-time-range)# **periodic Monday Wednesday Friday 8:00 to 17:00**
Paso 2	R1(config)# **access-list 101 permit tcp 192.168.10.0 0.0.0.255 any eq telnet time-range EVERYOTHERDAY**
Paso 3	R1(config)# **interface s0/0/0** R1(config-if)# **ip access-group 101 out**

Paso 1

Primero, defina el rango de tiempo para implementar la ACL y otórguele un nombre; EVERYOTHERDAY en este caso.

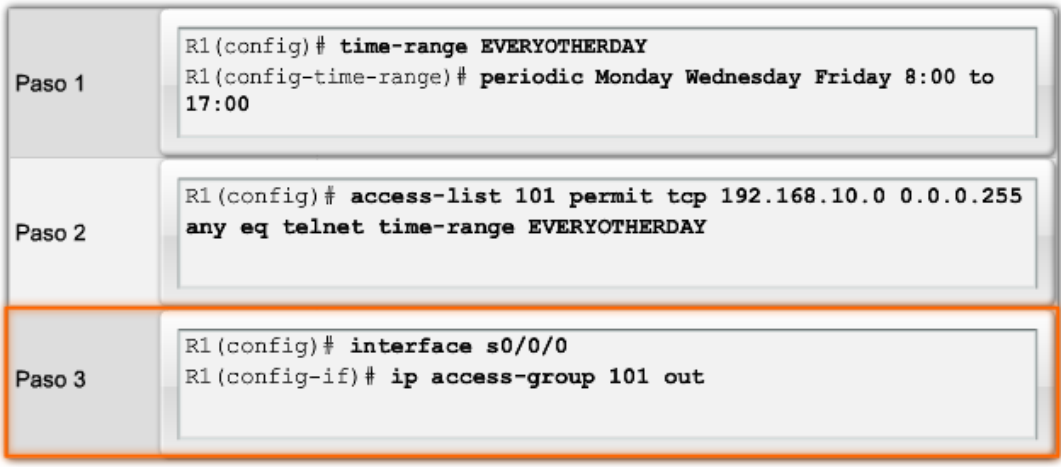
Pase el puntero por encima de cada paso para más información.

Paso 1	R1(config)# **time-range EVERYOTHERDAY** R1(config-time-range)# **periodic Monday Wednesday Friday 8:00 to 17:00**
Paso 2	R1(config)# **access-list 101 permit tcp 192.168.10.0 0.0.0.255 any eq telnet time-range EVERYOTHERDAY**
Paso 3	R1(config)# **interface s0/0/0** R1(config-if)# **ip access-group 101 out**

Paso 2

Aplique el rango de tiempo a la ACL.

Pase el puntero por encima de cada paso para más información.





Pase el puntero por encima de cada paso para más información.

Considere esta situación: un administrador de red requiere ACLs basadas en tiempo para aplicar una política mediante la cual no se permite a los usuarios acceder a Internet durante las horas laborables, excepto durante el almuerzo y las horas extra hasta las 7 p.m. cuando cierra la oficina. Esta es la ACL basada en tiempo que soporta el requerimiento:

R1(config)# time-range employee-time

R1(config-time-range)# periodic weekdays 12:00 to 13:00

R1(config-time-range)# periodic weekdays 17:00 to 19:00

R1(config-time-range)# exit

R1(config)# access-list 100 permit ip 192.168.1.0 0.0.0.255 any time-range employee-time

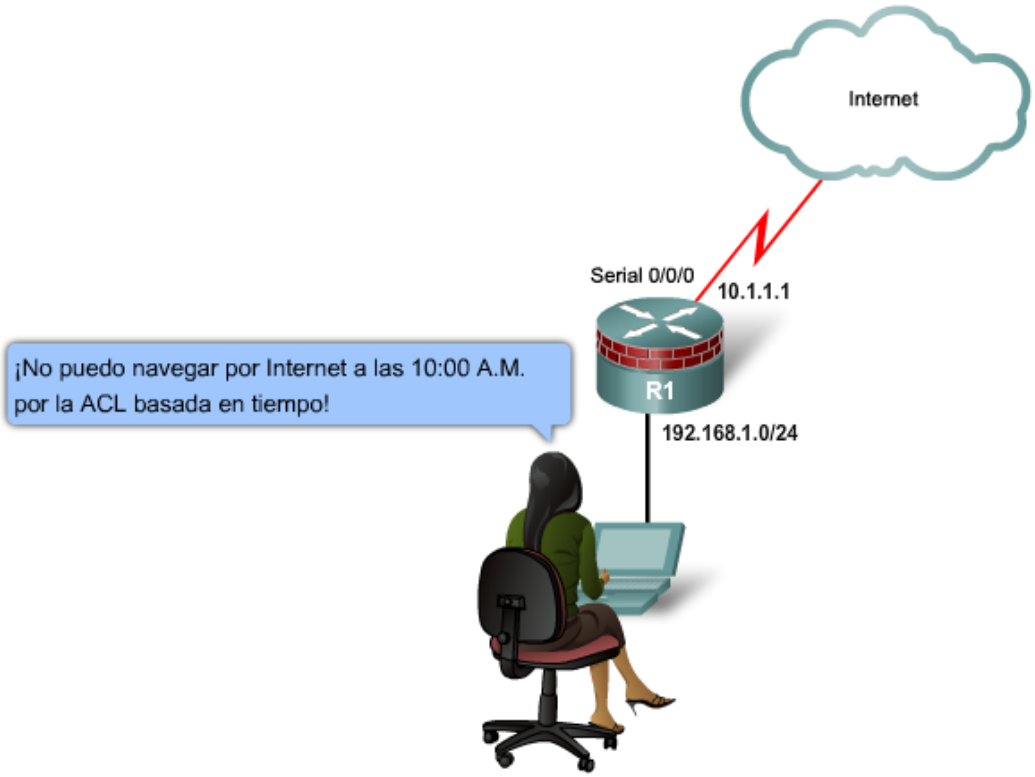
R1(config)# access-list 100 deny ip any any

R1(config)# interface FastEthernet 0/1

R1(config-if)# ip access-group 100 in

R1(config-if)# exit

En este ejemplo, los comandos permiten el acceso IP a Internet durante el almuerzo y las horas extra: la ACL 100 permite tráfico de los empleados a Internet durante el almuerzo y las horas de trabajo extra entre las 5 p.m. y las 7 p.m.



4.1.8 Resolucion de problemas en implementaciones de ACLs complejas

Para verificar la configuración ACL, use el comando show access-lists.

Router# show access-lists [número-ACL | nombre-ACL]

La salida del comando muestra cuántos paquetes coinciden con cada entrada de las ACLs, lo cual permite al usuario monitorear los paquetes específicos que han sido permitidos o denegados.

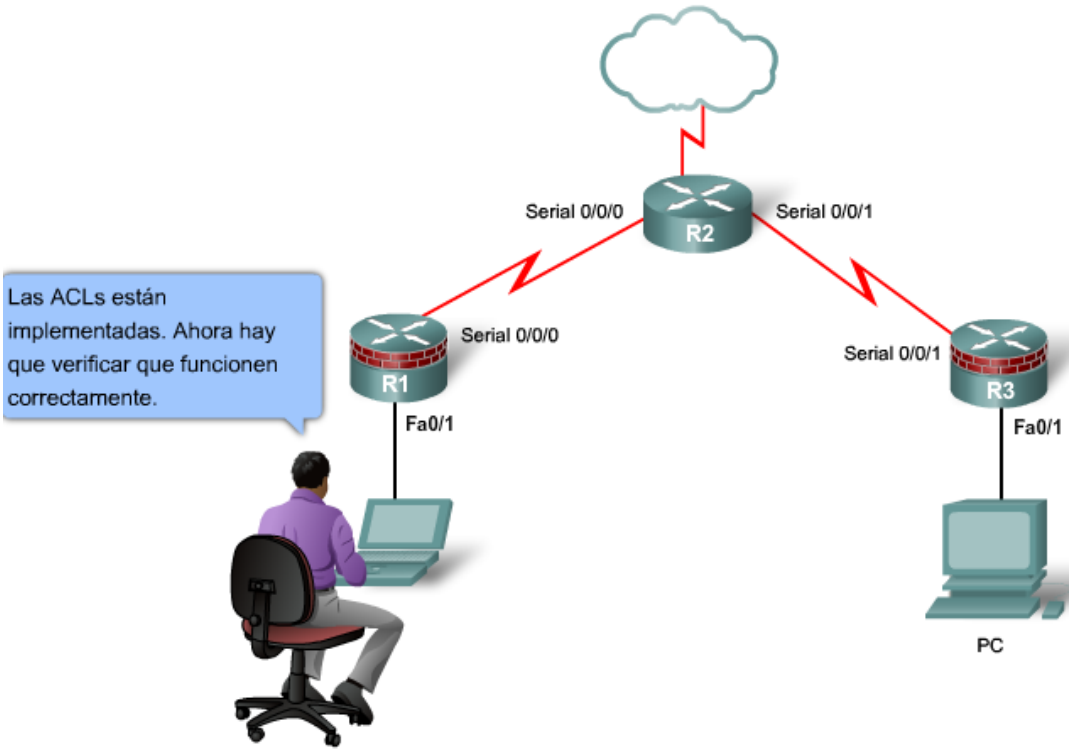
Para resolver problemas en una configuración ACL, use el comando debug ip packet.

Router# debug ip packet [número-ACL] [detail]

El comando debug ip packet es útil para analizar los mensajes que viajan entre los hosts locales y remotos. El debugging de paquetes IP captura los paquetes conmutados por procesos, incluyendo los paquetes recibidos, generados y reenviados.

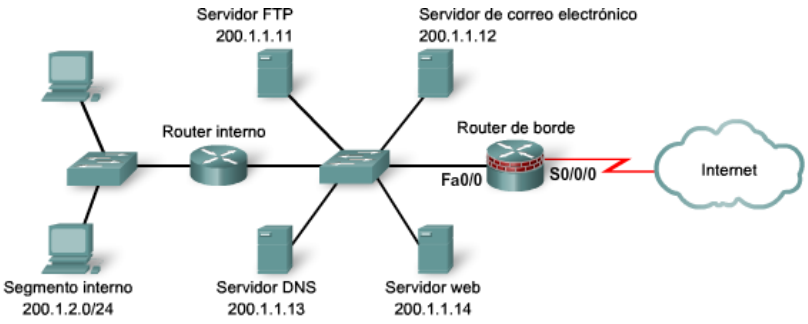
La opción detail muestra información de debugging de paquetes IP. Esta información incluye tanto los códigos y tipos de paquetes como los números de puerto de origen y destino.

Tenga en consideración un uso prudencial del comando debug ip packet en redes en producción, ya que su ejecución genera una cantidad importante de información y usa considerablemente los recursos del sistema.



Un contador ACL cuenta cuántos paquetes coinciden (sean permitidos o denegados) con cada línea de la ACL. Este número se muestra como número de coincidencias (number of matches).

Al verificar el número de coincidencias con el comando show access-lists, el administrador puede determinar si las ACLs IP estándar y extendidas configuradas están filtrando como se les pide. Por ejemplo, si una entrada tiene muchas más coincidencias que las esperadas, puede ser demasiado general. Esto puede indicar que la ACL no tiene el efecto buscado en el tráfico de la red.



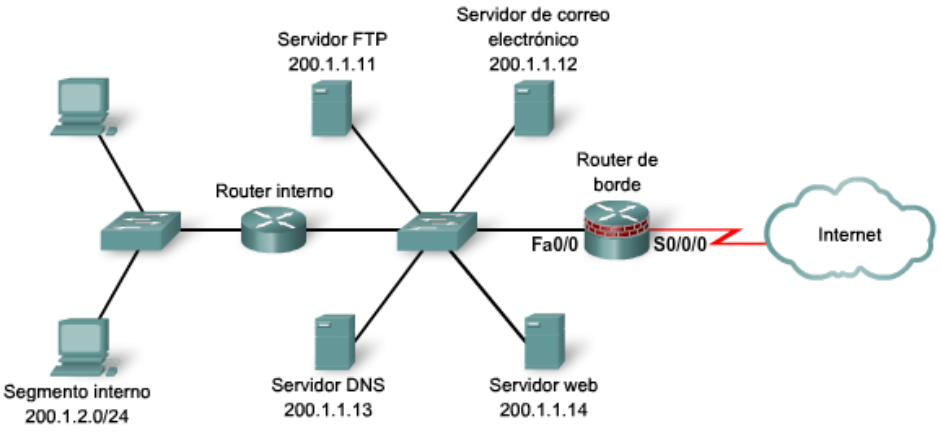

```
Perimeter# show access-list 100
Extended IP access list 100
    permit tcp any host 200.1.1.14 eq www  (189 matches)
    permit udp any host 200.1.1.13 eq domain (32 matches)
    permit tcp any host 200.1.1.12 eq smtp
    permit tcp any eq smtp host 200.1.1.12 established
    permit tcp any host 200.1.1.11 eq ftp
    permit tcp any host 200.1.1.11 eq ftp-data
    permit tcp any eq www 200.1.2.0 0.0.0.255 established
    permit udp any eq domain 200.1.2.0 0.0.0.255
    deny ip any any (1237 matches)
```

En la salida de debug ip packet, la denegación de un paquete se muestra explícitamente, lo cual permite una determinación granular y en tiempo real del éxito de la implementación ACL.

La "g" en la salida del comando debug ip packet indica el gateway del siguiente salto.

Se puede detener la salida del comando debug con el comando undebug all. A veces toma algunos minutos detenerla, dependiendo de qué comandos debug se han configurado y la cantidad de tráfico que pasa por el router.

Los comandos de verificación y resolución de problemas de las ACLs son relativamente fáciles de usar y no hay demasiados comandos para recordar. Es imperativo examinar las ACLs una vez implementadas para controlar su correcto funcionamiento.




```
Edge# debug ip packet
IP packet debugging is on

IP: s=200.0.2.2 (FastEthernet0/0), d=172.69.2.42 (Serial0/0/0), g=172.69.16.2, forward
IP: s=200.0.2.2 (FastEthernet0/0), d=172.16.2.42 (Serial0/0/0), g=172.69.16.2, forward
IP: s=200.0.2.2 (FastEthernet0/0), d=172.69.43.126 (Serial0/0/0), g=172.69.16.2, forward
IP: s=200.0.2.2 (FastEthernet0/0), d=172.16.2.42 (Serial0/0/0), g=172.69.16.2, access denied
```

4.1.9 Mitigacion de ataques con ACLs

Se puede usar ACLs para mitigar muchas amenazas de red:

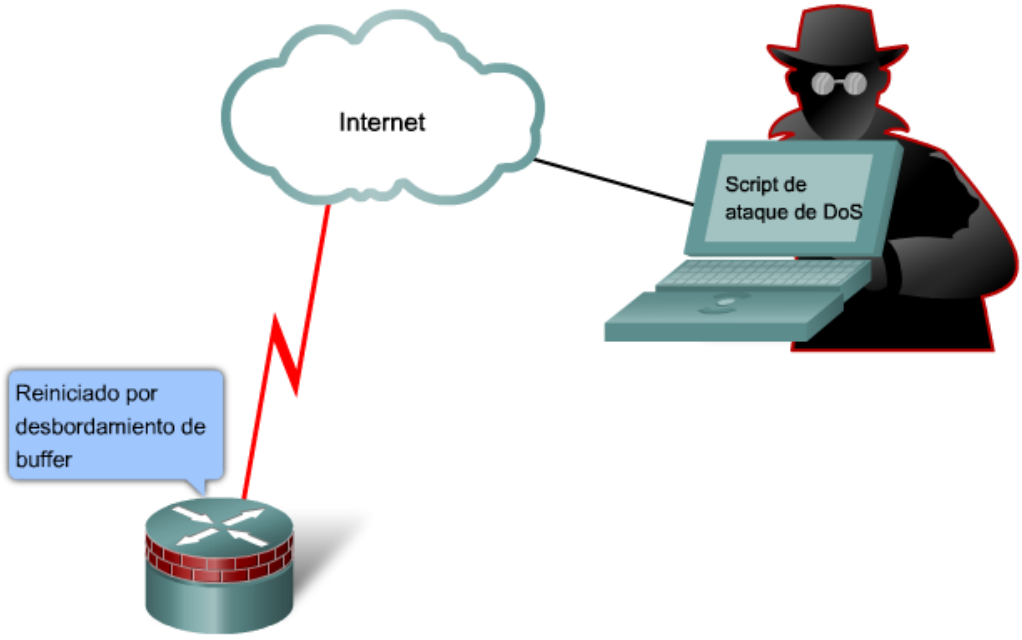
Falsificación de direcciones IP de entrada y de salida
Ataques de DoS SYN TCP
Ataques de DoS smurf

Adicionalmente, las ACLs filtran el siguiente tráfico:

Mensajes ICMP de entrada y de salida
traceroute

Los ataques de DoS tienden a ser los más devastadores en las redes. El IOS de Cisco soporta varias tecnologías diseñadas para minimizar el daño causado por los ataques de DoS. La mayoría de los ataque usa algún tipo de falsificación. Hay muchas clases de direcciones IP bien conocidas que nunca deben tomarse como direcciones IP de origen del tráfico que ingresa a la red de una organización. Hay ACLs específicas que son fáciles de implementar y previenen que los ataques se originen de estos tipos de direcciones.

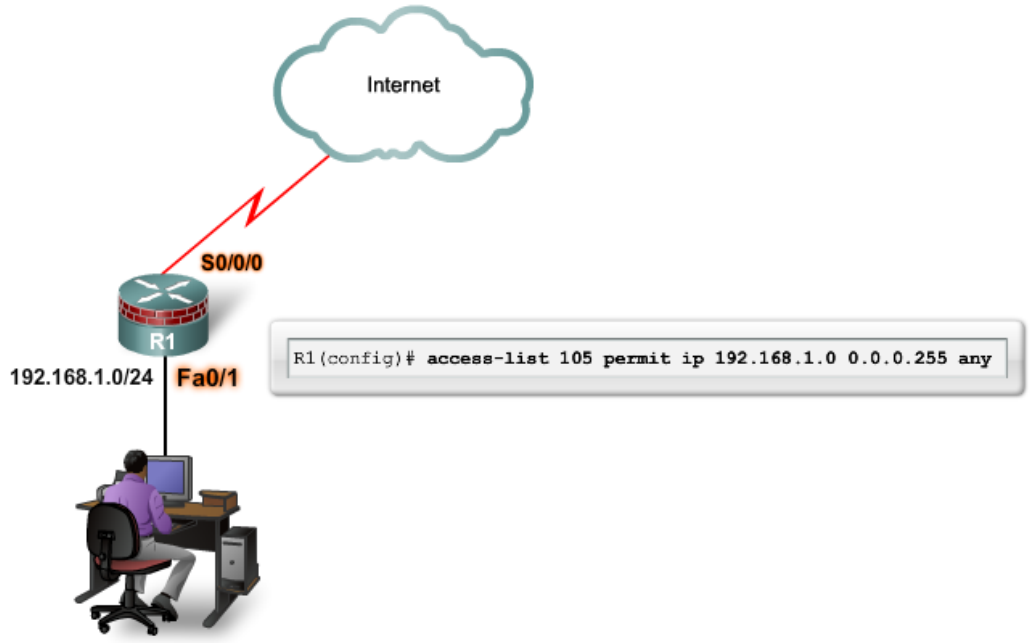
ICMP viene siendo muy utilizado en ataques de red desde hace varios años. El IOS de Cisco ahora soporta tecnologías específicas que evitan daños a la red que provengan de ataques basados en ICMP.



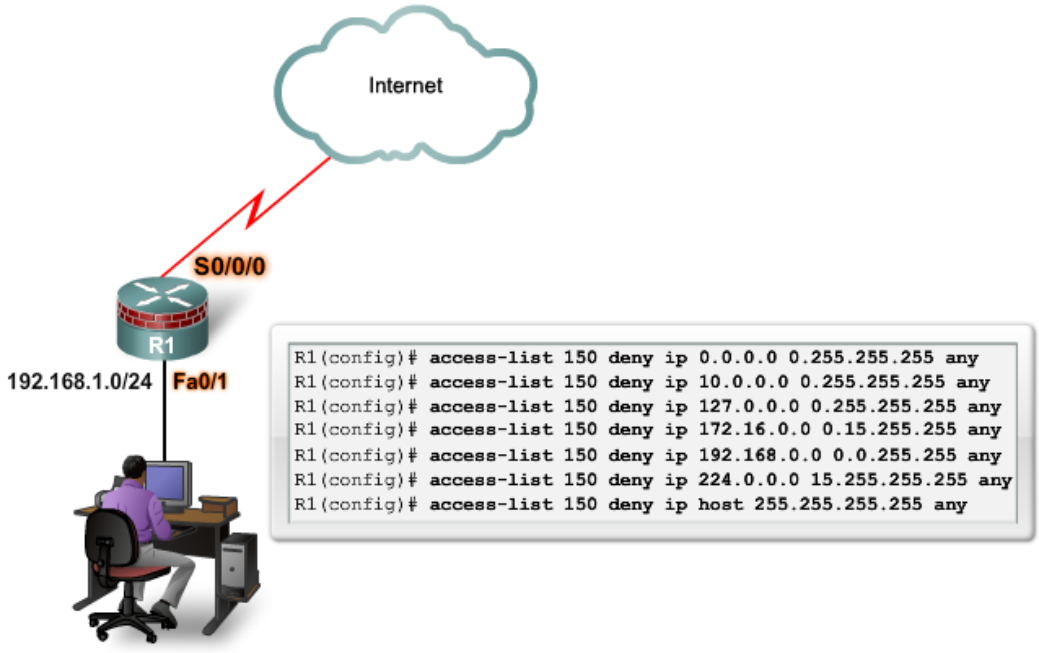
Ningún administrador debe permitir el ingreso a una red privada de paquetes IP cuya dirección de origen sea la de un host interno o una red interna. El administrador puede crear una ACL que deniegue todos los paquetes que contengan las siguientes direcciones IP en su campo de origen:

Cualquier dirección de host local (127.0.0.0/8)
Cualquier dirección privada reservada (RFC 1918, Address Allocation for Private Internets)
Cualquier dirección en el rango de direcciones IP multicast (224.0.0.0/4)

Los administradores no deben permitir la salida de paquetes IP con una dirección de origen que no sea una dirección IP válida para la red interna. Para este propósito, puede crearse una ACL que permita sólo aquellos paquetes que contengan direcciones de origen de la red interna y deniegue los restantes.



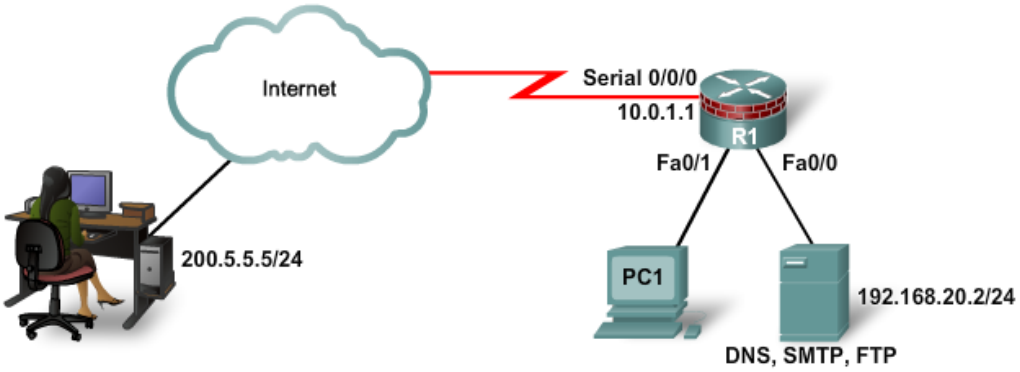
Pase el puntero por encima de cada interfaz para ver la ACL.



Pase el puntero por encima de cada interfaz para ver la ACL.

DNS, SMTP y FTP son servicios comunes a los que generalmente debe permitirse pasar por un firewall.

También es muy común que un firewall requiera una configuración para permitir protocolos necesarios para la administración del router. Por ejemplo, puede ser necesario permitir el paso de tráfico por un router interno para que el tráfico de mantenimiento de routers que proviene de un dispositivo externo pueda pasar. Telnet, SSH, syslog y SNMP son ejemplos de servicios que el router puede necesitar incluir. Siempre se prefiere SSH sobre Telnet.



De entrada en Serial 0/0/0

```
R1(config)# access-list 180 permit udp any host 192.168.20.2 eq domain
R1(config)# access-list 180 permit tcp any host 192.168.20.2 eq smtp
R1(config)# access-list 180 permit tcp any host 192.168.20.2 eq ftp
R1(config)# access-list 180 permit tcp host 200.5.5.5 host 10.0.1.1 eq telnet
R1(config)# access-list 180 permit tcp host 200.5.5.5 host 10.0.1.1 eq 22
R1(config)# access-list 180 permit udp host 200.5.5.5 host 10.0.1.1 eq syslog
R1(config)# access-list 180 permit udp host 200.5.5.5 host 10.0.1.1 eq snmptrap
```

Los hackers usan varios tipos de mensajes ICMP para atacar redes, sin embargo, varias aplicaciones usan mensajes ICMP para reunir información. La administración de redes usa mensajes ICMP generados automáticamente por el router.

Los hackers pueden usar paquetes eco ICMP para descubrir subredes y hosts de una red protegida y generar ataques de inundación DoS. Los hackers pueden usar mensajes de redirección ICMP para alterar las tablas de enrutamiento de los hosts. La entrada de mensajes eco y de redirección ICMP debe ser bloqueada por el router.

Se recomiendan varios mensajes ICMP para la correcta operación de la red y debe permitírseles la entrada:

Echo reply - (Respuesta de eco) Permite a los usuarios hacer ping a hosts externos.
Source quench - (Disminución del tráfico desde el origen) Solicita al remitente que disminuya la cantidad de tráfico de mensajes.
Unreachable - (Destino inalcanzable) Los mensajes unreachable se generan cuando un paquete es denegado administrativamente por una ACL.

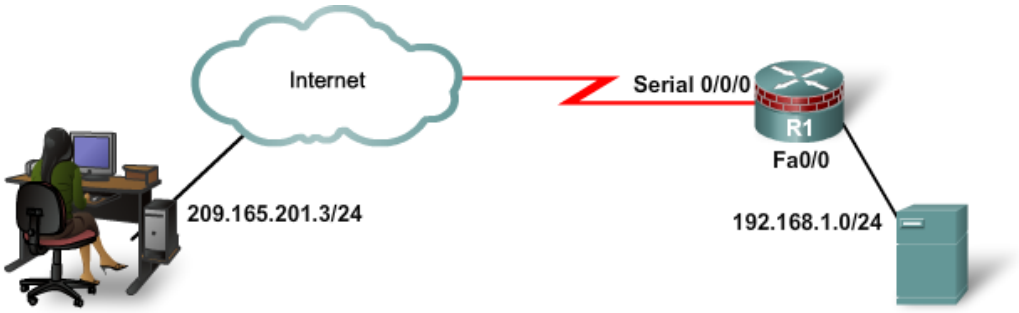
Se recomiendan varios mensajes ICMP para la correcta operación de la red y debe permitírseles la salida:

Echo - (Eco) Permite a los usuarios hacer ping a hosts externos.
Parameter problem - (Problema de parámetro) Informa al host sobre problemas en el encabezado del paquete.
Packet too big - (Paquete demasiado grande) Requerido para el descubrimiento de la unidad de transmisión máxima (MTU) de paquetes.
Source quench - (Disminución del tráfico desde el origen) Ahoga el flujo de tráfico si es necesario.

Todos los otros tipos de mensajes ICMP de salida deben ser bloqueados.

Las ACLs se usan para detener la falsificación de direcciones IP, permitir el paso por el firewall de servicios específicos y permitir sólo los mensajes ICMP requeridos.

Las ACLs son una herramienta dominante en la seguridad de las redes. Sin embargo, existen otras tecnologías que fueron desarrolladas para el IOS de Cisco para mejorar la funcionalidad del firewall. ¿Qué tecnologías superan a las ACLs tradicionales en la creación de un perímetro seguro para la red de una organización?



De entrada en S0/0/0

```
R1(config)# access-list 112 permit icmp any any echo-reply
R1(config)# access-list 112 permit icmp any any source-quench
R1(config)# access-list 112 permit icmp any any unreachable
R1(config)# access-list 112 deny icmp any any
R1(config)# access-list 112 permit ip any any
```

De entrada en Fa0/0

```
R1(config)# access-list 114 permit icmp 192.168.1.0 0.0.0.255 any echo
R1(config)# access-list 114 permit icmp 192.168.1.0 0.0.0.255 any parameter-problem
R1(config)# access-list 114 permit icmp 192.168.1.0 0.0.0.255 any packet-too-big
R1(config)# access-list 114 permit icmp 192.168.1.0 0.0.0.255 any source-quench
R1(config)# access-list 114 deny icmp any any
R1(config)# access-list 114 permit ip any any
```

4.2.1 Proteccion de redes con Firewalls

El término firewall se refería originalmente a una pared a prueba de fuego (generalmente hecha de piedra o metal), que evitaba que las llamas se extendieran entre las estructuras que conectaba. Luego, el término fue aplicado a la plancha de metal que separaba el compartimento del motor de un vehículo o aeronave del compartimento del pasajero. Eventualmente, el término se adaptó para su uso en las redes de computadoras: el firewall evita que tráfico indeseable ingrese a áreas restringidas de la red.

El firewall es un sistema o grupo de sistemas que aplica una política de control de acceso entre las redes. Puede incluir opciones como un router de filtrado de paquetes, un switch con dos VLANs y múltiples hosts con software de firewall.

Los firewalls son cosas diferentes para diferentes personas y organizaciones, pero todos comparten ciertas propiedades:

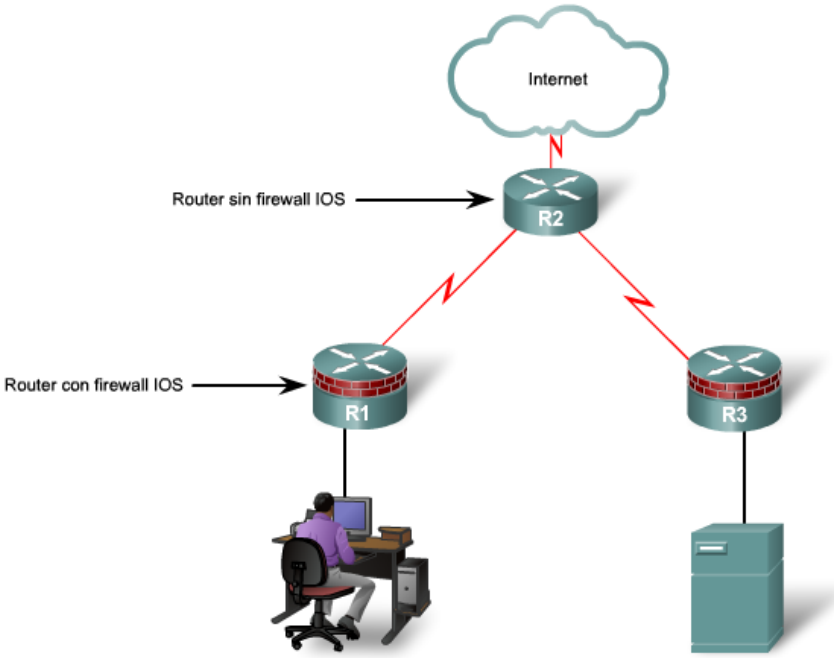
Resisten ataques

Son el único punto de tránsito entre las redes (todo el tráfico fluye a través del firewall)
Aplican la política de control de acceso

En 1988, DEC creó el primer firewall de red en la forma de un firewall de filtrado de paquetes. Estos firewalls primitivos inspeccionaban los paquetes para ver si coincidían con grupos de reglas establecidos, con la opción de reenviar o descartar los paquetes. Este tipo de filtrado de paquetes, conocido como filtrado sin estados (stateless), ocurre sin importar si el paquete es parte de un flujo de datos existente. Cada paquete es filtrado basándose exclusivamente en los valores de ciertos parámetros del encabezado del paquete, de manera similar al filtrado efectuado por las ACLs.

En 1989, AT&T Bell Laboratories desarrolló el primer firewall con estados (stateful). Los firewalls con estados filtran los paquetes basándose en la información extraída de los datos que fluyen a través del firewall y almacenada en él. Este tipo de firewall es capaz de determinar si un paquete pertenece a un flujo de datos existente. Las reglas estáticas, como las de los firewalls de filtrado de paquetes, son suplementadas por reglas dinámicas creadas en tiempo real para definir estos flujos activos. Los firewalls con estados ayudan a mitigar ataques de DoS que explotan conexiones activas a través de dispositivos de red.

Los firewalls no eran dispositivos autónomos, sino que los routers o servidores con funciones adicionales proporcionaban funcionalidad de firewall. Con el tiempo, muchas empresas desarrollaron firewalls autónomos. Los dispositivos de firewalls dedicados permitieron a los routers y switches librarse de la carga de memoria y procesamiento de efectuar el filtrado de paquetes. Los routers modernos, como los Routers de Servicios Integrados (Integrated Services Routers - ISRs) de Cisco, pueden ser usados como sofisticados firewalls con estados en las organizaciones que pueden no necesitar un firewall dedicado.



Algunos de los beneficios del uso de un firewall en una red:

Puede prevenir la exposición de hosts y aplicaciones sensibles a usuarios no confiables.
Puede sanitizar el flujo de protocolos, previniendo la explotación de fallas en los protocolos.
Puede bloquearse el acceso de datos maliciosos a servidores y clientes.
Puede hacer que la aplicación de la política de seguridad se torne simple, escalable y robusta.
Puede reducir la complejidad de la administración de la seguridad de la red al reducir la mayoría del control de acceso a la red a algunos puntos.

Los firewalls también tienen limitaciones:

Si está mal configurado, el firewall puede tener consecuencias serias (único punto de falla).
Muchas aplicaciones no pueden pasar a través del firewall en forma segura.
Los usuarios pueden intentar buscar maneras de sortear el firewall para recibir material bloqueado, exponiendo la red a potenciales ataques.
El rendimiento de la red puede disminuir.
Puede hacerse tunneling de tráfico no autorizado o puede disfrazárselo como tráfico legítimo.

Es importante entender los tipos diferentes de firewalls y sus capacidades específicas para poder usar el firewall adecuado para cada situación.

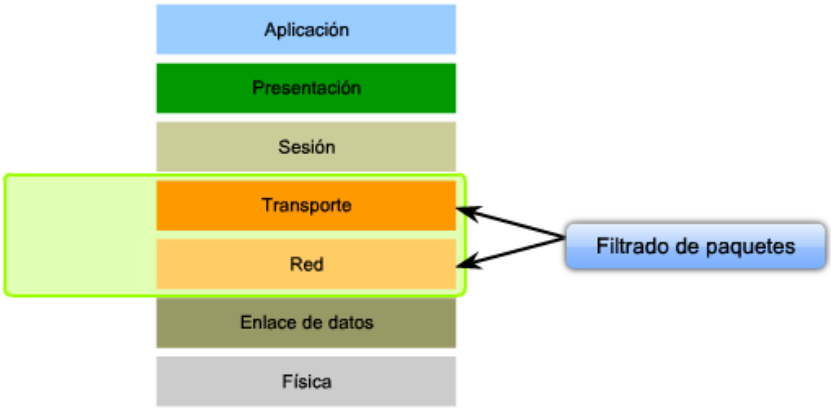


4.2.2 Tipos de firewall

Un sistema firewall puede estar compuesto por muchos dispositivos y componentes diferentes. Uno de los componentes es el filtrado de tráfico, que es lo que muchas

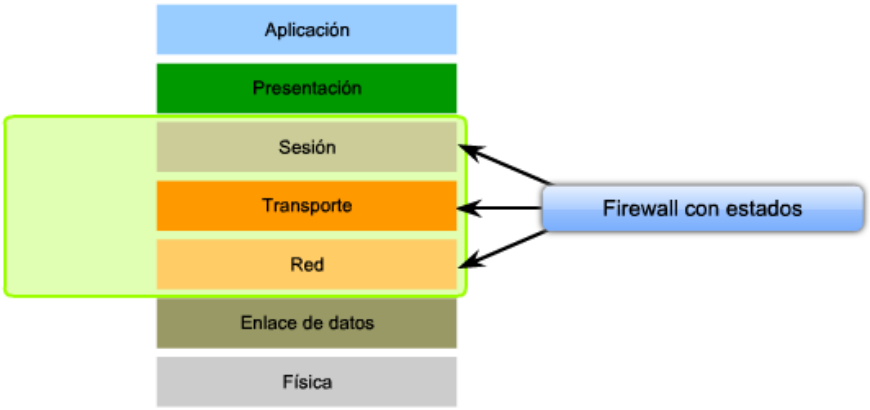
personas llaman firewall. Hay varios tipos de firewalls de filtrado, incluyendo los siguientes:

Firewall de filtrado de paquetes - (Packet-filtering firewall) Típicamente consiste en un router con la capacidad de filtrar paquetes con algún tipo de contenido, como información de capa 3 y, en ocasiones, de capa 4.
Firewall con estados - (Stateful firewall) Monitorea el estado de las conexiones, si están en estado de iniciación, transferencia de datos o terminación.
Firewall gateway de aplicación (proxy) - (Application gateway firewall) Filtra según información de las capas 3, 4, 5 y 7 del modelo de referencia OSI. La mayoría del control y filtrado del firewall se hace por software.
Firewall de traducción de direcciones - (Address translation firewall) Expande el número de direcciones IP disponibles y esconde el diseño del direccionamiento de la red.
Firewall basado en hosts (servidor y personal) - (Host-based firewall) Una PC o servidor que ejecuta software de firewall.
Firewall transparente - (Transparent firewall) Filtra tráfico IP entre un par de interfaces conmutadas.
Firewall híbrido - (Hybrid firewall) Es una combinación de varios tipos de firewalls diferentes. Por ejemplo, un firewall de inspección de aplicaciones combina un firewall con estados con un firewall de gateway de aplicación.



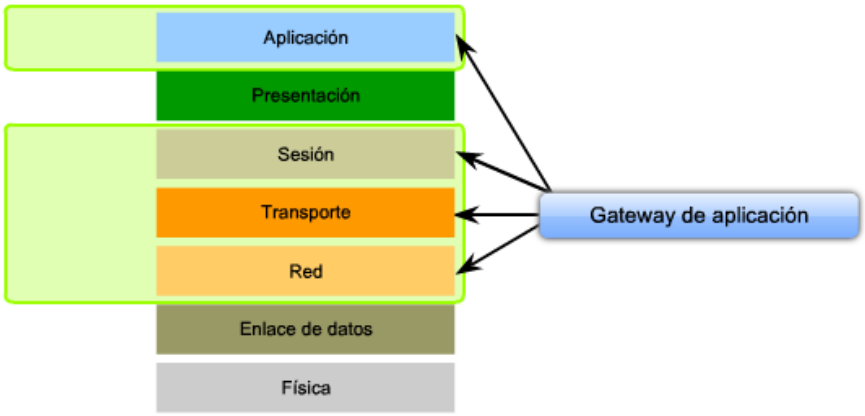
Firewall de filtrado de paquetes | Firewall con estados | Firewall proxy de aplicación | Firewall de traducción de direcciones

Haga clic en los botones para ver el contenido asociado.



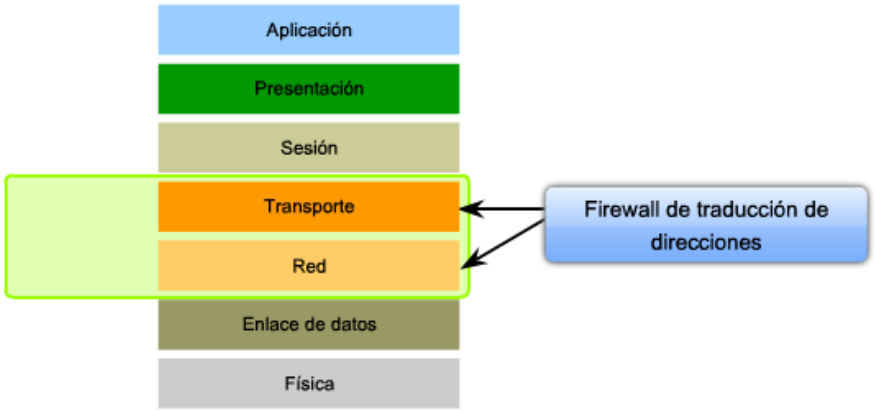
Firewall de filtrado de paquetes | **Firewall con estados** | Firewall proxy de aplicación | Firewall de traducción de direcciones

Haga clic en los botones para ver el contenido asociado.



Firewall de filtrado de paquetes | Firewall con estados | **Firewall proxy de aplicación** | Firewall de traducción de direcciones

Haga clic en los botones para ver el contenido asociado.



Firewall de filtrado de paquetes | Firewall con estados | Firewall proxy de aplicación | Firewall de traducción de direcciones

Haga clic en los botones para ver el contenido asociado.

Los firewalls de filtrado de paquetes trabajan principalmente en la capa de Red del modelo OSI y generalmente se los considera dispositivos de capa 3. Sin embargo, permiten y deniegan tráfico basándose en información de capa 4 como protocolo y números de puerto de origen y destino. El filtrado de paquetes usa ACLs para determinar si permite o deniega tráfico basándose en direcciones IP de origen y destino, protocolo, tipo de paquete y números de puerto origen y destino. Los firewalls de filtrado de paquetes generalmente son parte de un router firewall.

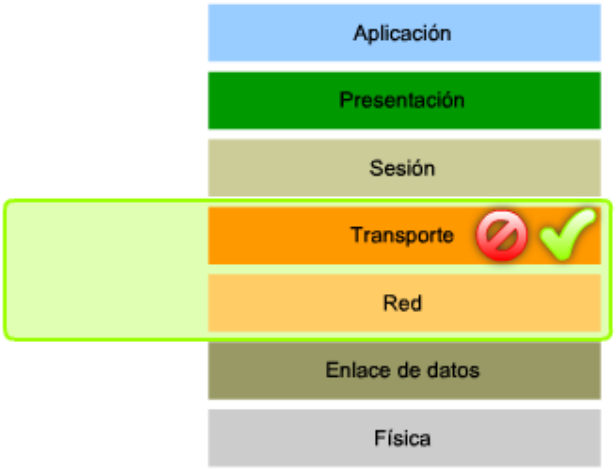
Los servicios usan puertos específicos. Por ejemplo, los servidores SMTP escuchan en el puerto 25 por defecto. Como los firewalls de filtrado de paquetes filtran el tráfico de acuerdo con información estática del encabezado del paquete, en ocasiones se los llama filtros estáticos. El administrador puede restringir ciertos puertos para restringir los servicios que los usan. Por ejemplo, el bloqueo del puerto 25 en una estación de trabajo específica puede prevenir que un virus se transmita a través de correo electrónico por Internet.

Los firewalls de filtrado de paquetes revisan una tabla simple para permitir o denegar el tráfico basándose en criterios específicos:

Dirección IP de origen
Dirección IP de destino
Protocolo
Número de puerto de origen
Número de puerto de destino
Recepción del paquete de sincronización e inicio de conexión (SYN)

Los filtros de paquetes no representan una solución de firewall completa, pero constituyen un elemento importante en ellas.

Firewall de filtrado de paquetes



Capas del modelo OSI Ventajas/Desventajas

Haga clic en los botones para ver el contenido asociado.

Firewall de filtrado de paquetes

Ventajas	• Pueden usarse grupos simples de reglas permit y deny para implementar un filtro de paquetes. • Los filtros de paquetes tienen un bajo impacto en el rendimiento de la red. • Los filtros de paquetes son de fácil implementación y la mayoría de los routers los soportan. • Los filtros de paquetes proporcionan un grado inicial de seguridad en una capa de red baja. • Los filtros de paquetes pueden realizar la mayoría de las tareas de un firewall de altas prestaciones a un precio mucho más bajo.
Desventajas	• El filtrado de paquetes es susceptible a la falsificación de direcciones IP. Los hackers envían paquetes arbitrarios que coinciden con los criterios de la ACL y pasan a través del filtro. • Los filtros de paquetes no filtran bien los paquetes fragmentados. Como los paquetes IP fragmentados llevan el encabezado TCP en el primer segmento y los filtros de paquetes filtran basándose en la información del encabezado IP, todos los fragmentos luego del primer segmento se pasan sin condiciones. Las decisiones de usar filtros de paquetes asumen que el filtro del primer fragmento aplica apropiadamente la política. • Las ACLs son difíciles de implementar y mantener correctamente. • Los filtros de paquetes no pueden filtrar ciertos servicios dinámicamente. Por ejemplo, las sesiones que usan negociaciones de puertos dinámicas son difíciles de filtrar sin abrir el acceso a un rango entero de puertos. • Los filtros de paquetes no usan estados. Examinan cada paquete individualmente y no se fijan en el contexto del estado de la conexión.

Capas del modelo OSI Ventajas/Desventajas

Haga clic en los botones para ver el contenido asociado.

Los firewalls con estados son la tecnología de firewall más versátil y común en uso actualmente. Proporcionan filtrado de paquetes con estados utilizando la información de conexiones mantenida en una tabla de estados. El filtrado con estados es una

arquitectura de firewall que se clasifica como de capa de Red, aunque, para algunas aplicaciones, también puede analizar tráfico de capas 4 y 5.

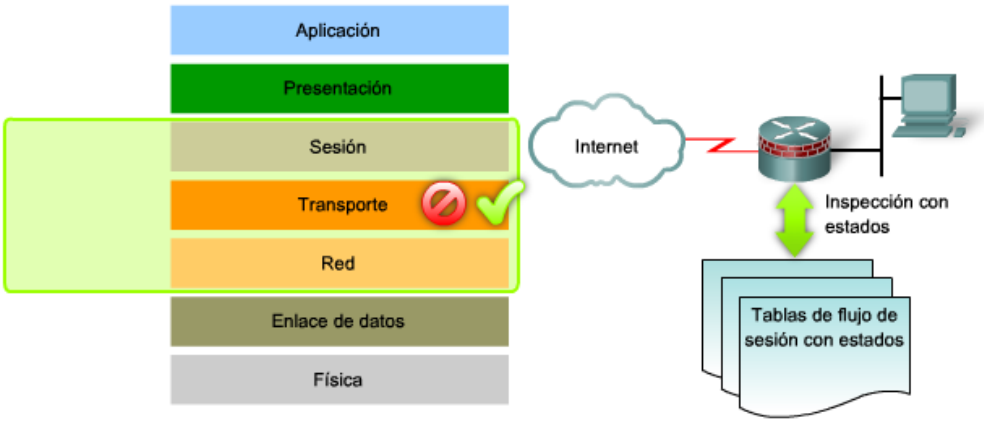
A diferencia del filtrado de paquetes estático, que examina paquetes en base a la información del encabezado del paquete, el filtrado con estados monitorea cada conexión que pasa por las interfaces del firewall y confirma su validez. Los firewalls con estados usan una tabla de estados para monitorear el proceso de la comunicación. El firewall examina la información en los encabezados de paquetes de capa 3 y segmentos de capa 4. Por ejemplo, el firewall busca en los encabezados TCP los bits de control synchronize (SYN), reset (RST), acknowledgment (ACK), finish (FIN) y otros para determinar el estado de la conexión.

Cada vez que se accede a un servicio externo, el firewall de filtrado de paquetes por estados retiene ciertos detalles de la solicitud y salva el estado de la solicitud en la tabla de estados. Cada vez que se establece una conexión TCP y UDP para conexiones de entrada o de salida, el firewall registra la información en una tabla de flujo de sesiones con estados. Cuando el sistema externo responde a una solicitud, el servidor firewall compara los paquetes recibidos con el estado salvado para permitir o denegar el acceso a la red.

La tabla de flujo de sesiones con estados contiene las direcciones de origen y destino, los números de puertos, información de secuencias TCP y flags adicionales por cada conexión TCP o UDP asociada con esa sesión particular. Esta información crea un objeto de conexión que el firewall usa para comparar los paquetes de entrada y salida con los flujos de sesiones en la tabla de flujo de sesiones con estados. El firewall permite los datos sólo si existe una conexión apropiada que justifique su paso.

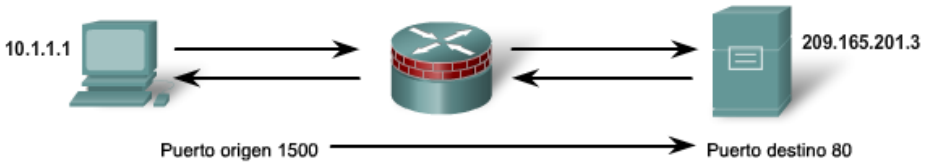
Los firewalls con estados más avanzados incluyen la capacidad de analizar comandos de puerto FTP y actualizar la tabla de estados para permitir que FTP trabaje transparentemente a través del firewall. Los firewalls con estados más avanzados también proporcionan interpretación de números de secuencia TCP y correlación de consultas y respuestas DNS para garantizar que el firewall permita que los paquetes vuelvan sólo en respuesta a solicitudes que se originan dentro de la red. Estas características reducen la amenaza de ataques de inundación RST TCP y envenenamiento de caché DNS.

Sin embargo, hay una desventaja potencial en el uso de filtrado con estados. Aunque la inspección con estados proporciona velocidad y transparencia, los paquetes dentro de la red deben poder salir de la red. Esto puede exponer las direcciones IP internas a potenciales atacantes. La mayoría de los firewalls tiene incorporados inspección por estados, traducción de direcciones de red (network address translation - NAT) y servidores proxy para mayor seguridad.



Capas del modelo OSI | Filtrado de paquetes con estados | Ventajas/Desventajas

Haga clic en los botones para ver el contenido asociado.



ACL interna (tráfico de salida)	ACL externa (tráfico de entrada)

`permit ip 10.0.0.0 0.0.0.255 any`	`Dynamic: permit tcp host 209.165.201.3 eq 80 host 10.1.1.1 eq 1500`
	`permit tcp any host 10.1.1.2 eq 25`
	`permit udp any host 10.1.1.2 eq 53`
	`deny ip any any`

Capas del modelo OSI | Filtrado de paquetes con estados | Ventajas/Desventajas

Haga clic en los botones para ver el contenido asociado.

Ventajas	• Los firewalls con estados se usan generalmente como medio principal de defensa ya que filtran el tráfico indeseable o innecesario. • Al proporcionar un control más estricto sobre la seguridad, los firewalls con estados fortifican el filtrado de paquetes. • Los firewalls con estados mejoran el rendimiento de los filtros de paquetes o los servidores proxy. • Los firewalls con estados defienden la red contra ataques de falsificación y DoS al determinar si los paquetes pertenecen a una conexión existente o provienen de una fuente no autorizada. • Los firewalls con estados proporcionan más información de registro que los firewalls de filtrado de paquetes.
Desventajas	• Los firewalls con estados no pueden evitar los ataques de capa de aplicación, ya que no examinan el contenido de la conexión HTTP. • No todos los protocolos funcionan con estados, como ocurre UDP e ICMP, lo cual hace que estos protocolos no tengan tanto soporte. • Algunas aplicaciones abren múltiples conexiones, lo cual requiere la apertura de un nuevo rango de puertos para permitir esta segunda conexión. • Los firewalls con estados no soportan autenticación de usuarios.

Capas del modelo OSI | Filtrado de paquetes con estados | Ventajas/Desventajas

Haga clic en los botones para ver el contenido asociado.

Cisco Systems proporciona varias opciones para que los profesionales de la seguridad en redes implementen soluciones de firewall. Estas incluyen el firewall IOS de Cisco, el PIX Security Appliances (este producto ya no está en circulación), y el Adaptive Security Appliances.

El firewall IOS de Cisco es una función especializada del IOS de Cisco que se ejecuta en los routers Cisco. Es un firewall de calidad profesional que soporta pequeñas y medianas empresas (PyMEs) y oficinas sucursales.

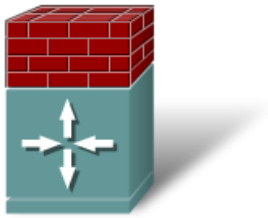
El Cisco PIX Security Appliance es un dispositivo autónomo que asegura una robusta ejecución de las políticas de usuario y aplicación, una protección multivector contra ataques y servicios de conectividad segura. El Cisco PIX Security Appliances puede acomodarse a una gama de requerimientos y tamaños de redes.

El Cisco ASA Adaptive Security Appliances es una solucion de fácil despliegue que integra capacidades de software, seguridad en comunicaciones unificadas Cisco (voz y video), capa de sockets seguros (SSL) y VPNs IPsec, IPS y servicios de seguridad de contenidos. Diseñado como un componente clave de las redes autodefensivas de Cisco, Cisco ASA proporciona servicios inteligentes de defensa de amenazas y comunicaciones seguras que detienen los ataques antes de que afecten la continuidad de los negocios. Los ASA fueron diseñados para proteger las redes de todos los tamaños y bajar los costos generales de despliegue y operación para la empresa al proporcionar una seguridad global multicapa.

Cuando se elige una de las varias opciones de solución de firewall, es importante llevar a cabo un análisis de costo versus riesgo. Cualquiera sea la decisión que se tome en la compra de una solución de firewall, es crítico contar con un diseño de red apropiado para el desarrollo exitoso del firewall.

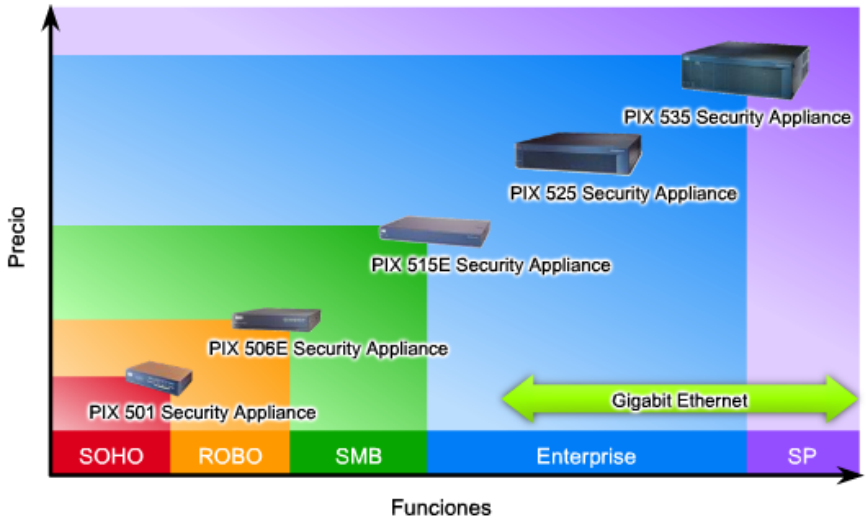
Funciones del firewall IOS de Cisco

- Framework de política basada en zonas para administración intuitiva
- Filtrado de aplicaciones peer-to-peer y de mensajería instantánea
- Firewalling de protocolo VoIP
- Firewalling de enrutamiento y forwarding virtual (Virtual routing and forwarding - VRF)
- Integración inalámbrica
- Failover con estados
- Soporte whitelist URL y blacklist URL
- Inspección de aplicaciones para tráfico web y de correo electrónico



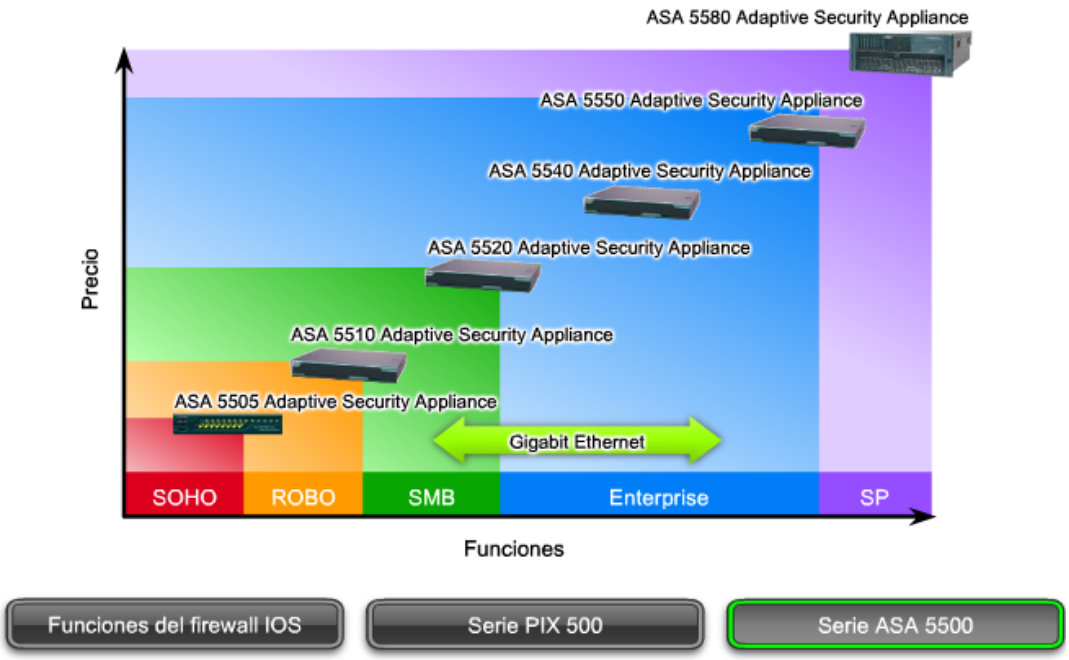
Funciones del firewall IOS | Serie PIX 500 | Serie ASA 5500

Haga clic en los botones para ver el contenido asociado.



Funciones del firewall IOS | Serie PIX 500 | Serie ASA 5500

Haga clic en los botones para ver el contenido asociado.



Haga clic en los botones para ver el contenido asociado.

4.2.3 Los Firewalls en el diseño de redes

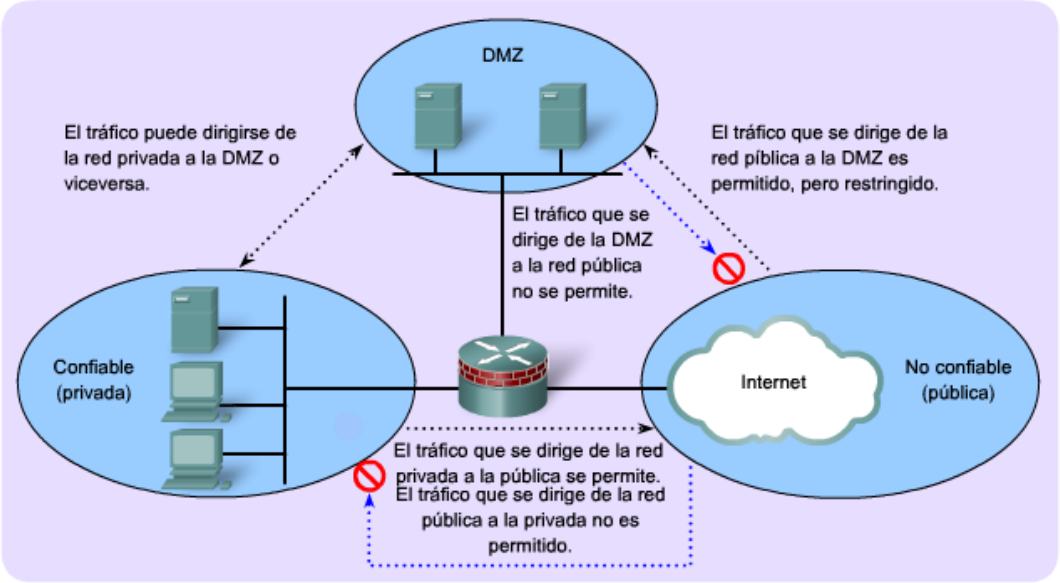
En la seguridad de las redes, a menudo se hace referencia a una zona desmilitarizada (demilitarized zone - DMZ). Una DMZ es una porción de red conectada con un firewall o grupo de firewalls. El término proviene de una descripción militar de un área ubicada entre zonas militares en la que no se permite conflicto.

Las DMZs definen las porciones de la red que son confiables y las que no lo son. El diseño de firewall principalmente se trata de interfaces de dispositivos que permiten o deniegan tráfico basándose en el origen, el destino y el tipo de tráfico.

Algunos diseños son tan simples como la designación de una red externa y una interna, determinadas por dos interfaces en un firewall. La red externa (o red pública) no es confiable, mientras que la interna (o red privada) sí lo es. En este caso, al tráfico proveniente de la red interna, se le permite pasar a través del firewall hacia afuera con pocas o ninguna restricción. El tráfico que se origina afuera generalmente es bloqueado o permitido muy selectivamente. El tráfico de retorno que proviene de la red externa, asociado con tráfico de origen interno, se le permite pasar de la interfaz no confiable a la confiable.

Un diseño más complicado puede involucrar tres o más interfaces en el firewall. En este caso, generalmente se trata de una interfaz externa, una interna y una DMZ. Se permite el tráfico libremente de la interfaz interna a la externa y la DMZ. Asimismo, se permite libremente el paso del tráfico que proviene de la DMZ por la interfaz externa. El tráfico de la interfaz externa, sin embargo, generalmente se bloquea salvo que esté asociado con tráfico de origen interno o de la DMZ. Con una DMZ, es común permitir tipos específicos de tráfico desde fuera, siempre que sea el tipo de tráfico correcto y que su

destino sea la DMZ. Este tipo de tráfico generalmente es correo electrónico, DNS, HTTP o HTTPS.



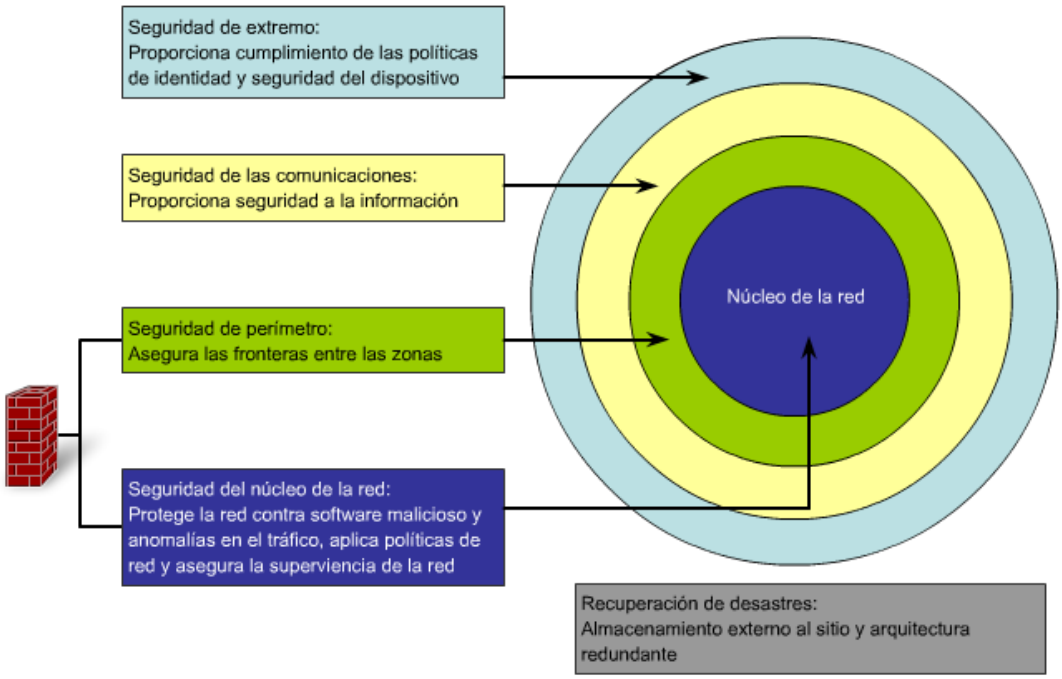
En un escenario de defensa por capas, los firewalls proporcionan seguridad perimetral de toda la red y de los segmentos de red internos en el núcleo. Por ejemplo, los profesionales de la seguridad en redes pueden usar un firewall para separar las redes de recursos humanos o de finanzas de una empresa de otras redes o segmentos de red dentro de la empresa.

La defensa por capas usa diferentes tipos de firewalls que se combinan en capas para agregar profundidad a la seguridad de la organización. Por ejemplo, el tráfico que ingresa de la red no confiable se topa con un filtro de paquetes en el router más externo. El tráfico se dirige al firewall "screened firewall" o "host bastión" que aplican más reglas al tráfico y descartan paquetes sospechosos. Un host bastión es una computadora reforzada que se ubica típicamente dentro de la DMZ. El tráfico va ahora a un screening router interior. El tráfico se moverá al host de destino interno sólo si pasa con éxito a través del filtrado entre el router externo y la red interna. Este tipo de configuración de DMZ se llama configuración screened subnet.

Un error común es considerar que sólo se necesita una topología de firewall en capas para asegurar una red interna. Este mito probablemente sea alimentado por el auge del negocio de los firewalls. El administrador de redes debe considerar muchos factores para construir una defensa completa y profunda:

Un número importante de las intrusiones proviene de hosts dentro de la red. Por ejemplo, los firewalls generalmente hacen muy poco para protegerse contra virus que se descargan a través del correo electrónico.
Los firewalls no ofrecen protección contra instalaciones de módems no autorizadas. Además, y más importantemente, el firewall no puede reemplazar a los administradores y usuarios informados.

Los firewalls no reemplazan mecanismos de resguardo y de recuperación de desastres que resulten de un ataque o falla en el hardware. Una defensa profunda debe incluir almacenamiento externo y una topología de hardware redundante.



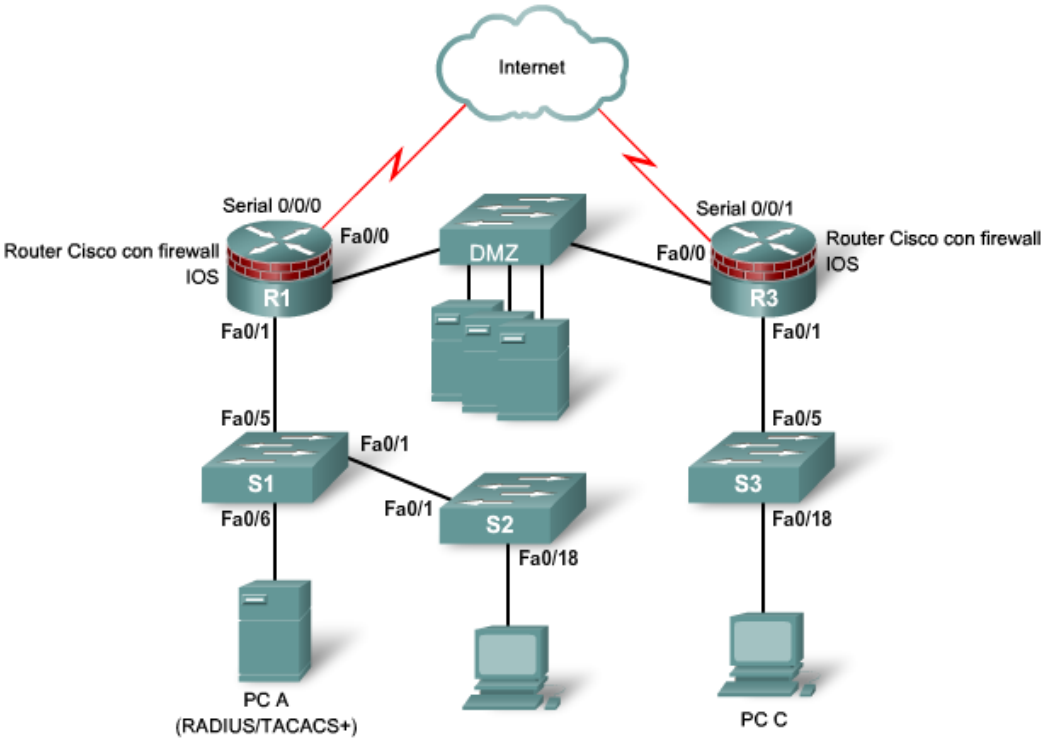
El profesional de la seguridad en redes es responsable de crear y mantener una política de seguridad, incluyendo una política de seguridad de firewall. Esta es una lista parcialmente genérica que sirve como punto de inicio para la política de seguridad de firewall:

Ubique los firewalls en las fronteras de seguridad claves.
Los firewalls son el principal dispositivo de seguridad pero no es aconsejable depender exclusivamente de un firewall para la seguridad de una red.
Deniegue todo el tráfico por defecto y permita sólo los servicios necesarios.
Asegúrese de que el acceso físico al firewall esté controlado.
Monitoree regularmente los registros del firewall. El Sistema de Respuesta, Análisis y Monitoreo de Seguridad de Cisco(MARS) es especialmente útil para este propósito.
Practique la administración de cambios para cambios de configuración en el firewall.
Los firewalls protegen principalmente contra ataques técnicos que se originan fuera de la red. Los ataques internos tienden a no ser de naturaleza técnica.

Buenas prácticas de firewalls

- Ubique los firewalls en las fronteras de seguridad.
- Los firewalls son los principales dispositivos de seguridad, sin embargo, no es buena idea depender exclusivamente de éstos.
- Deniegue todo el tráfico por defecto. Permita solo los servicios necesarios.
- Asegúrese de controlar el acceso físico al firewall.
- Monitoree regularmente los registros del firewall.
- Practique la administración de cambios para cambios de configuración en el firewall.
- Recuerde que los firewalls se concentran en proteger contra ataques técnicos originados fuera de la red.

Un router de Cisco que ejecuta el firewall IOS de Cisco es tanto un router como un firewall. Si hay dos firewalls, una opción de diseño viable es unirlos con una LAN que funcione como DMZ. Esta opción proporciona a los hosts en la red pública no confiable acceso redundante a los recursos de la DMZ.



4.3 Control de acceso basado en el contexto

4.3.1 Caracteristicas de CBAC

El control de acceso basado en el contexto (Context-Based Access Control - CBAC) es una solución disponible dentro del firewall IOS de Cisco. CBAC filtra inteligentemente los paquetes TCP y UDP en base a información de sesión de protocolo de capa de aplicación. Proporciona filtrado de capa de aplicación con estados, incluyendo protocolos que son específicos de aplicaciones únicas, así como protocolos y aplicaciones multimedia que requieren múltiples canales para la comunicación, como FTP y H.323.

CBAC también puede examinar las conexiones soportadas para ejecutar las traducciones de direcciones necesarias básandose en la información NAT y PAT contenida en el paquete. CBAC puede bloquear conexiones peer-to-peer (P2P), como las utilizadas por las aplicaciones Gnutella y KaZaA, así como el tráfico de mensajería instantánea como Yahoo!, AOL y MSN.

CBAC proporciona cuatro funciones principales: filtrado de tráfico, inspección de tráfico, detección de intrusos y generación de auditorías y alertas.

Filtrado de tráfico

CBAC puede ser configurado para permitir el paso de tráfico de retorno TCP y UDP específico a través del firewall cuando la conexión se inicia dentro de la red. Logra esto al crear entradas temporales en una ACL que de otra manera denegaría el tráfico. CBAC puede inspeccionar el tráfico para sesiones que se originan dentro o fuera de la red. También puede ser usado para los perímetros intranet, extranet e Internet de la red. CBAC examina no sólo la información de capas de red y de transporte, sino también la información de protocolo de capa de aplicación (como información de conexiones FTP) para conocer el estado de la sesión. Esto le permite soportar protocolos que involucran a múltiples canales creados como resultado de negociaciones en el canal de control. La mayoría de los protocolos multimedia y otros tantos protocolos (como FTP, RPC y SQL*Net) involucran a múltiples canales.

Inspección de tráfico

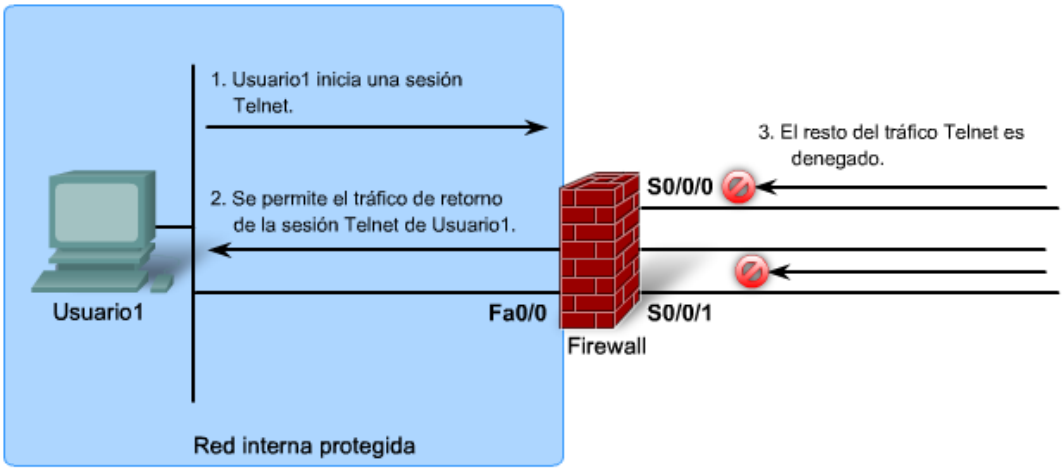
Como CBAC inspecciona paquetes de capa de aplicación y mantiene información de sesiones TCP y UDP, puede detectar y prevenir ciertos tipos de ataques de red como inundación SYN. Un ataque de inundación SYN ocurre cuando un atacante inunda a un servidor con un aluvión de solicitudes de conexión y no completa la conexión. El volumen resultante de conexiones "medio abiertas" abruma al servidor y causa que deniegue el servicio a solicitudes válidas. CBAC también contribuye a la protección contra ataques de DoS de otras maneras: inspecciona los números de secuencia de los paquetes de las conexiones TCP para ver si están dentro de los rangos experados y los descarta si le resultan sospechosos. CBAC también puede ser configurado para descartar conexiones medio abiertas, ya que éstas requieren procesamiento extra y recursos de memoria en el firewall.

Detección de intrusos

CBAC proporciona una cantidad limitada de detección de intrusos para la protección contra ataques SMTP específicos. Con la detección de intrusos, los mensajes syslog son revisados y monitoreados en búsqueda de firmas de ataques específicas. Ciertos tipos de ataques de red tienen características o firmas específicas. Cuando CBAC detecta un ataque basado en estas características específicas, reinicia las conexiones en cuestión y envía información al servidor syslog.

Generación de alertas y auditorías

CBAC también genera registros de auditorías y alertas en tiempo real. Las funciones de registros de auditoría mejoradas usan syslog para monitorear todas las transacciones de red y grabar las marcas de tiempo, hosts de origen y destino, puertos utilizados y el número total de bytes transmitidos en reportes avanzados basados en sesión. Las alertas en tiempo real envía mensajes syslog de error a las consolas de administración central cuando detectan actividad sospechosa.



Los primeros comandos CBAC fueron introducidos al software IOS de Cisco en 1997. CBAC es una mejora radical en comparación de las opciones de firewall TCP established y ACLs reflexivas en varios aspectos fundamentales:

Monitorea el establecimiento de conexiones TCP
Revisa los números de secuencia TCP
Inspecciona consultas y respuestas DNS
Inspecciona tipos de mensaje ICMP comunes
Soporta aplicaciones que se basan en conexiones múltiples
Inspecciona direcciones incrustadas
Inspecciona información de capa de aplicación

Es importante destacar que CBAC sólo ofrece filtrado para los protocolos especificados por el administrador, esto significa que, si el protocolo no es especificado, las ACLs existentes determinarán el filtrado del protocolo, ya que no se creará una entrada temporal. Adicionalmente, CBAC sólo ofrece detección y protección contra ataques que pasan a través del firewall. Típicamente, no ofrece protección contra ataques que se originan dentro de la red protegida excepto si el tráfico pasa a través de un router interno que tenga el firewall IOS de Cisco habilitado.

Aunque el concepto de una defensa perfecta no es alcanzable, CBAC detecta y previene contra la mayoría de los ataques populares de las redes. Sin embargo, no hay defensas impenetrables. Un atacante hábil y determinado puede aun encontrar maneras de lanzar un ataque efectivo.

Funciones CBAC

Monitorea el establecimiento de sesiones TCP
Examina los números de secuencia TCP

Inspecciona las consultas y respuestas DNS

Inspecciona tipos de mensajes ICMP comunes

Soporta aplicaciones con múltiples canales, como FTP y Multimedia

Inspecciona direcciones incrustadas

Inspecciona información de capa de aplicación

- Si una conexión TCP no se establece dentro de los 30 segundos luego de la recepción del primer segmento SYN, el IOS elimina la entrada de la tabla de estados y de la ACL.
- Una vez activado el flag FIN, que indica el fin de la conexión, el IOS elimina la entrada de la tabla de estados y de la ACL.
- Si no hay actividad en una sesión TCP por más de una hora, el IOS elimina la entrada.
- Si los números de secuencia no entran en el rango esperado, los paquetes se descartan.

Haga clic en las funciones CBAC para más información.

Funciones CBAC

Monitorea el establecimiento de sesiones TCP
Examina los números de secuencia TCP

Inspecciona las consultas y respuestas DNS

Inspecciona tipos de mensajes ICMP comunes

Soporta aplicaciones con múltiples canales, como FTP y Multimedia

Inspecciona direcciones incrustadas

Inspecciona información de capa de aplicación

- CBAC aproxima los tiempos de conexión UDP. SI no ve tráfico en una conexión UDP por más de 30 segundos, el IOS elimina la entrada de la tabla de estados y de la ACL.
- También se inspeccionan las consultas y respuestas DNS. Cuando un dispositivo interno genera una consulta DNS, CBAC espera que el servidor DNS remoto envíe una respuesta dentro de 5 segundos y si no lo hace la entrada ACL dinámica es eliminada para evitar un ataque de falsificación.

Haga clic en las funciones CBAC para más información.

Funciones CBAC

Monitorea el establecimiento de sesiones TCP
Examina los números de secuencia TCP

Inspecciona las consultas y respuestas DNS

Inspecciona tipos de mensajes ICMP comunes

Soporta aplicaciones con múltiples canales, como FTP y Multimedia

Inspecciona direcciones incrustadas

Inspecciona información de capa de aplicación

- La inspección del tráfico ICMP fue introducida en la Release 12.2(15)T del IOS de Cisco.
- Los tipos de mensajes ICMP inspeccionados incluyen: solicitud de eco, respuesta de eco, destino inalcanzable, tiempo excedido, solicitud de marca de tiempo y respuesta de marca de tiempo. Los otros tipos de mensajes ICMP no son inspeccionados.
- CBAC espera respuestas a los mensajes ICMP soportados por 10 segundos, si no se reciben, la conexión ICMP se elimina de la tabla de estados y la entrada ACL dinámica es eliminada.

Haga clic en las funciones CBAC para más información.

Funciones CBAC

Monitorea el establecimiento de sesiones TCP
Examina los números de secuencia TCP

Inspecciona las consultas y respuestas DNS

Inspecciona tipos de mensajes ICMP comunes

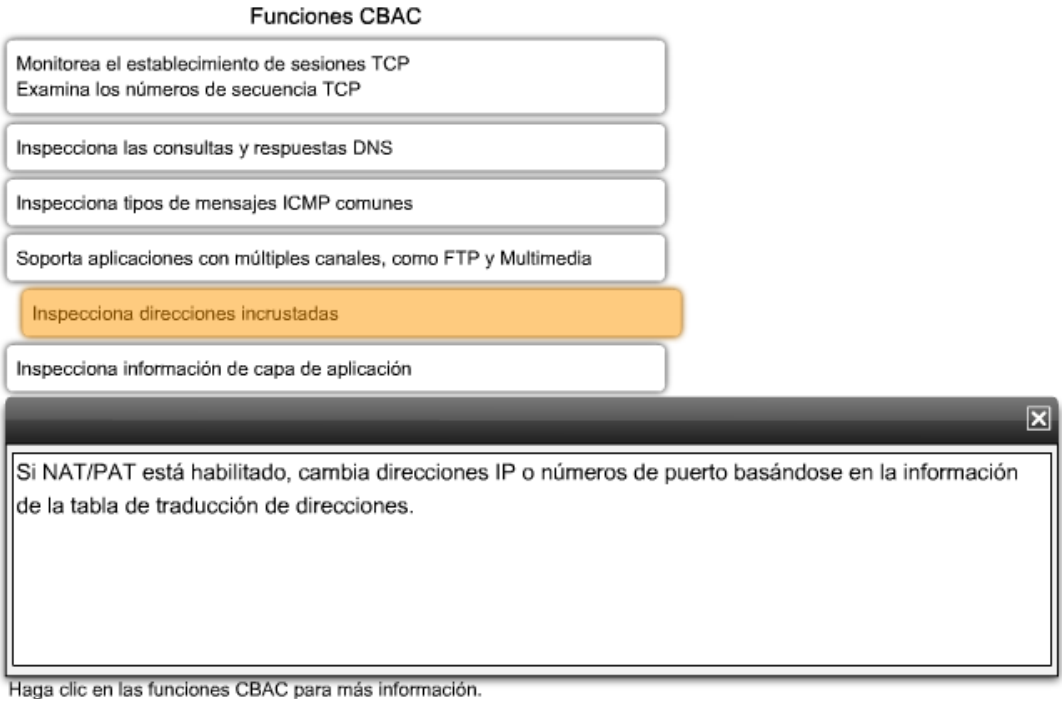
Soporta aplicaciones con múltiples canales, como FTP y Multimedia

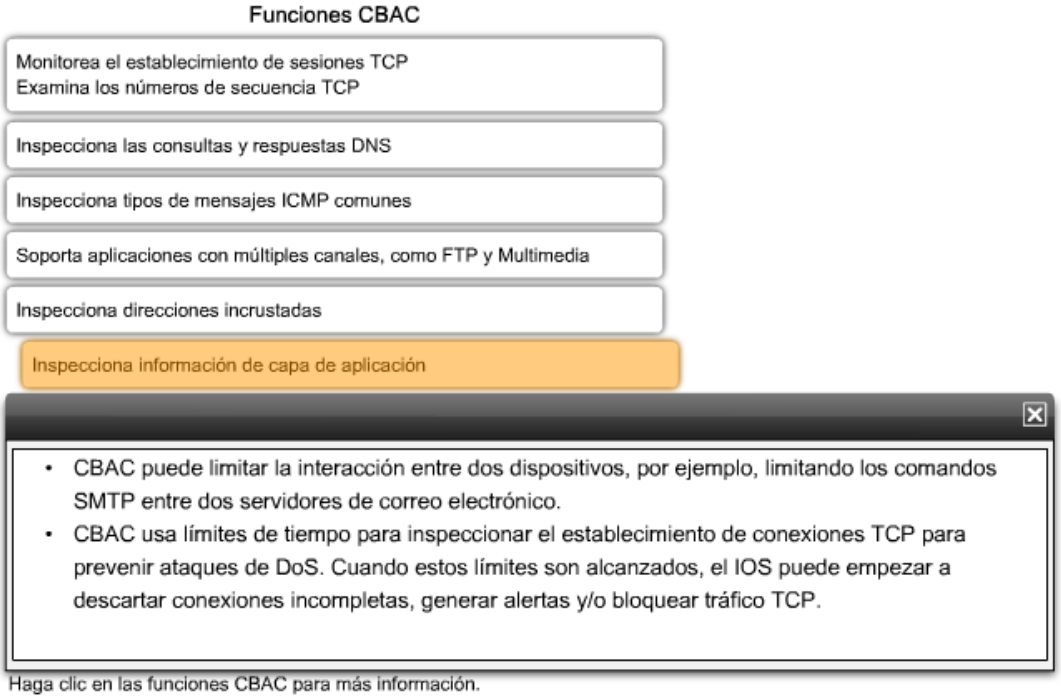
Inspecciona direcciones incrustadas

Inspecciona información de capa de aplicación

- CBAC inspecciona la conexión de control de estas aplicaciones para determinar si se está abriendo una conexión de datos u otra conexión.
- Si se están creando nuevas conexiones en conjunción con el canal de control, la información se agrega automáticamente a la ACL dinámica para permitir la conexión.

Haga clic en las funciones CBAC para más información.





4.3.2 Operación de CBAC

Sin CBAC, el filtrado de tráfico se limita a implementaciones ACL que examinan paquetes en la capa de red o, a lo sumo, la capa de transporte. CBAC usa un filtro de paquetes con estados que es sensible a las aplicaciones. Esto significa que el filtro es capaz de reconocer todas las sesiones de una aplicación dinámica. CBAC examina no sólo la información de capas de red y de transporte, sino también la información de protocolo de capa de aplicación (como información de conexiones FTP) para conocer el estado de la sesión. Esto le permite soportar protocolos que involucran a múltiples

canales creados como resultado de negociaciones en el canal de control. La mayoría de los protocolos multimedia y otros tantos protocolos (como FTP, RPC y SQL*Net) involucran a múltiples canales.

La tabla de estados monitorea las sesiones e inspecciona todos los paquetes que pasan a través del firewall de filtrado de paquetes con estados. CBAC luego usa la tabla de estados para configurar entradas de ACL dinámica que permitan el paso del tráfico de retorno a través del firewall o router de perímetro.

¿Cómo funciona CBAC? CBAC crea entradas en las ACLs de las interfaces del firewall agregando una entrada ACL temporal para una sesión específica. Estas entradas son creadas cuando tráfico específico sale de la red interna protegida a través del firewall. Las entradas temporales permiten el ingreso del tráfico de retorno que normalmente sería bloqueado y canales de datos adicionales a la red interna a través del firewall sólo si son parte de la misma sesión y tienen las mismas propiedades esperadas que el tráfico original que disparó al CBAC cuando salió por el firewall. Sin esta entrada temporal de ACL, este tráfico sería denegado por la ACL preexistente. La tabla de estados cambia dinámicamente y se adapta con el flujo de tráfico.



Asuma que un usuario inicia una conexión de salida, como Telnet, de una red protegida a una red externa, y se habilita CBAC para la inspección de tráfico Telnet. Asuma también que se aplica una ACL en la interfaz externa, previniendo la entrada de tráfico Telnet a la red protegida. Esta conexión atraviesa una operación de varios pasos:

1. Cuando el tráfico es generado y pasa por el router, si hay una ACL de entrada aplicada se la procesa primero. Si la ACL deniega este tipo de conexión de salida, el paquete se descarta. Si la ACL permite esta conexión entonces se examinan las reglas de inspección CBAC.

2. Basándose en las reglas de inspección de CBAC, el software IOS de Cisco puede inspeccionar la conexión. Si no se inspecciona el tráfico Telnet, se permite el paso al paquete y no se recolecta información. Si se lo inspecciona, la conexión pasa al siguiente paso.

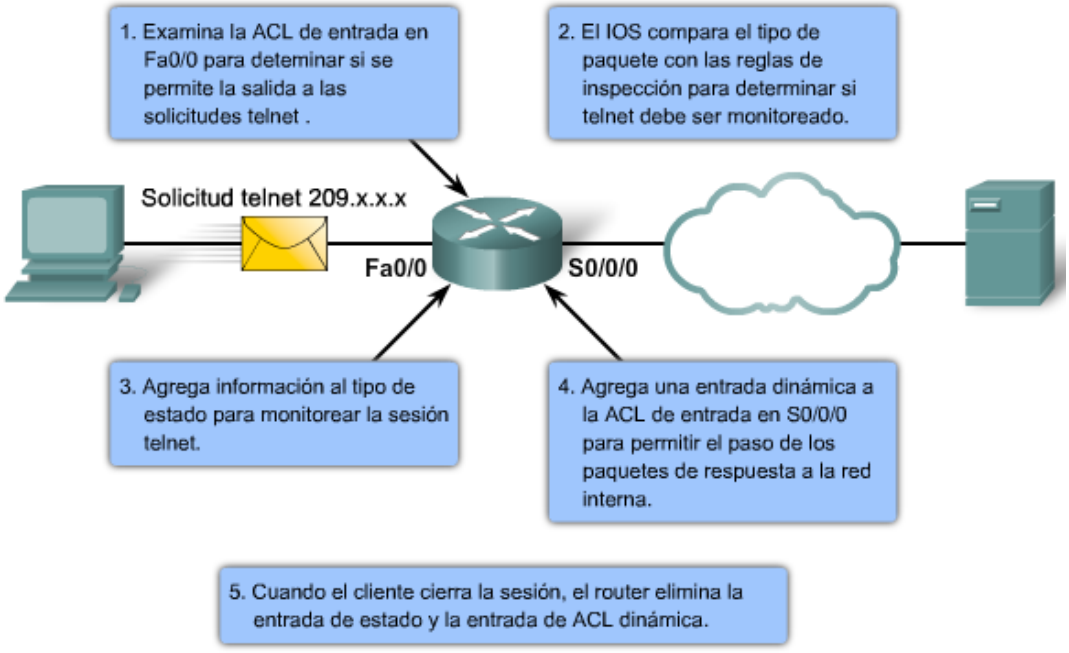
3. Se compara la información de conexión con las entradas en la tabla de estados. Si la conexión no existe actualmente, se agrega la entrada. Si existe, el temporizador de inactividad de la conexión se reinicia.

4. Si se agrega una nueva entrada, se agrega una ACL dinámica a la interfaz externa en la dirección de entrada (de la red externa a la red interna protegida). Esto permite que el tráfico de retorno de Telnet, es decir, los paquetes que son parte de la misma conexión Telnet previamente establecida con el paquete de salida, vuelvan a la red. Esta entrada temporal sólo está activa por el tiempo que la sesión permanezca abierta. Estas entradas ACL dinámicas no se guardan en la NVRAM.

5. Cuando la sesión termina, la información dinámica de la tabla de estados y las entradas de ACL dinámica son removidas.

Esto es muy similar a cómo se procesan las ACLs reflexivas. CBAC crea entradas temporales en las ACLs para permitir el tráfico de retorno. Estas entradas son creadas a medida que el tráfico inspeccionado deja la red y se eliminan cuando la conexión termina o se alcanza el tiempo de vencimiento de la conexión por inactividad. Además, como con las ACLs reflexivas, el administrador puede especificar qué protocolos inspeccionar, así como en qué interfaz y en qué dirección tomará lugar la inspección.

CBAC es flexible en su configuración, especialmente al elegir la dirección de la inspección del tráfico. En una configuración típica, CBAC se utiliza en el router o firewall de perímetro para permitir el acceso del tráfico de retorno a la red. CBAC también puede ser configurado para inspeccionar tráfico en dos direcciones: de entrada y de salida. Esto es útil al proteger dos partes de una red en la que dos lados inician ciertas conexiones y permiten que el tráfico de retorno llegue a su origen.



Tratamiento CBAC de TCP

Recuerde que TCP usa un saludo de tres vías. El primer paquete contiene una secuencia aleatoria de números y establece el flag SYN TCP. Cuando el router recibe el primer paquete de un flujo TCP con el flag SYN TCP, se examina la ACL de entrada ubicada en la interfaz de entrada asegurada. Si se permite el paquete, se crea una entrada de sesión dinámica. La sesión es despcrita por las direcciones de los extremos, números de puerto, números de secuencia y flags.

Todos los paquetes siguientes que pertenezcan a esta sesión se verifican con el estado actual y se descartan si resultan no ser válidos. ¿Cómo hace CBAC para determinar si un paquete es el subsiguiente dentro de una sesión ya establecida?

Cuando se transmite el paquete SYN TCP, el segundo paquete contiene una secuencia aleatoria de números que genera el host que responde, así como un número de secuencia de confirmación (el número de secuencia recibido se incrementa en uno), y se activan los flags SYN TCP y ACK. El tercer paquete confirma el paquete recibido e incrementa el número de secuencia del paquete en la secuencia de confirmación, sumando al número de secuencia el número apropiado de octetos transmitidos y activando el flag ACK.

Todos los segmentos subsiguientes incrementan sus números de secuencia en el número de octetos transmitidos y confirman el último segmento recibido con un incremento de uno, de acuerdo con la máquina de estado TCP. Luego del saludo de tres vías, todos los paquetes tienen el flag ACK activado hasta que la sesión termine. El router monitorea los números de secuencia y flags para determinar la sesión a la que los paquetes pertenecen.

Tratamiento CBAC de UDP

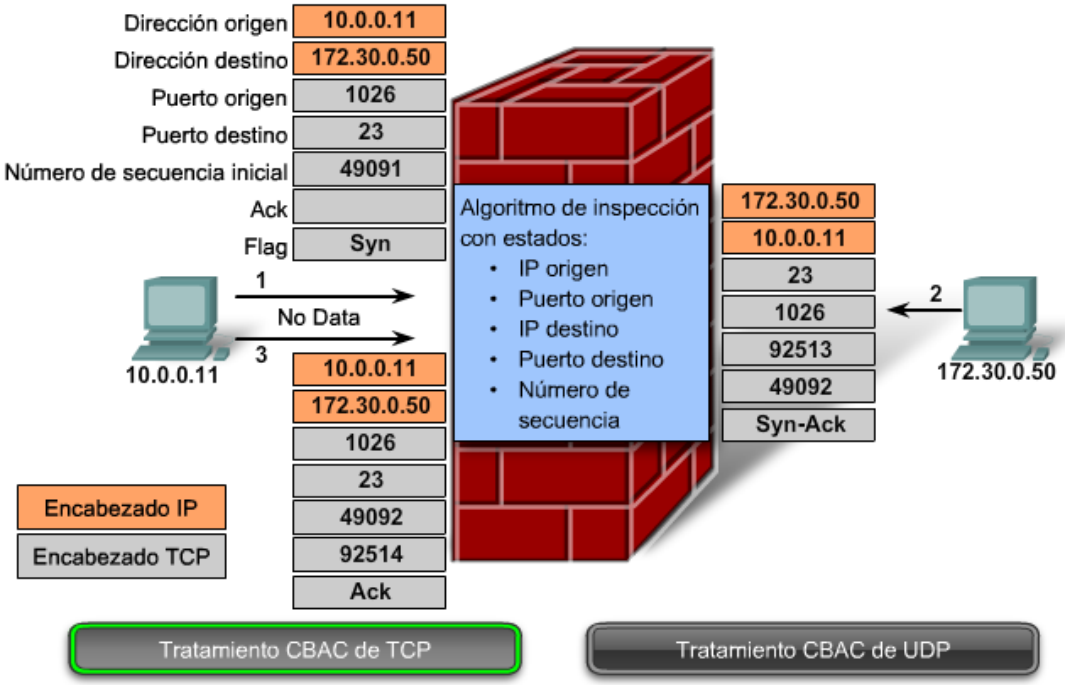
Con UDP, el router no puede monitorear números de secuencia o flags. No hay saludo de tres vías y no hay proceso de desconexión. Si se le permite el paso a través del router al primer paquete de un flujo UDP, se crea una entrada UDP en la tabla de conexiones. Las direcciones de los extremos y los números de puerto describen la entrada de conexión UDP. Cuando no se intercambian datos en la conexión por un tiempo configurable, tiempo de vencimiento UDP, la descripción de la conexión se elimina de la tabla de conexiones.

Tratamiento CBAC de otros protocolos IP

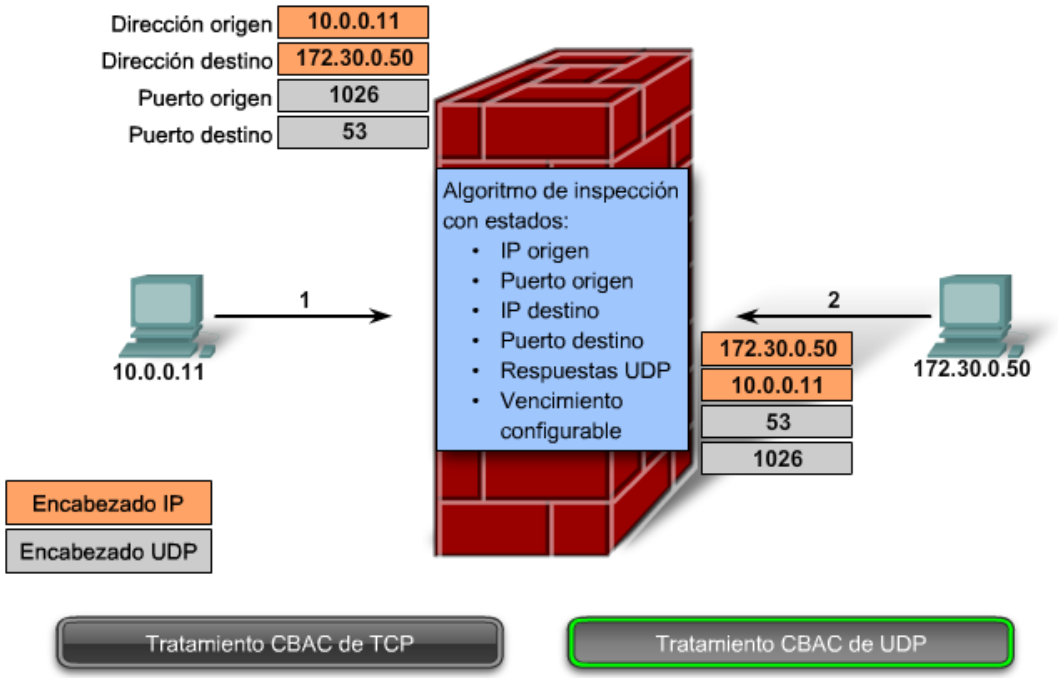
Generalmente, los firewalls con estados no monitorean otros protocolos, como GRE o IPSec, sino que manejan los protocolos sin estados, como lo haría un filtro de paquetes clásico. Si se proporciona soporte con estados a otros protocolos, el soporte es generalmente similar al soporte para UDP. Cuando se permite un flujo de protocolo, se permite el paso a todos los paquetes que coincidan con el flujo hasta que expire el temporizador de inactividad.

Las aplicaciones dinámicas, como FTP, SQLnet y muchos protocolos utilizados para señalización de voz, video y transferencia de medios, abren un canal en un puerto bien conocido y luego negocian canales adicionales a través de la sesión inicial. Los firewalls

con estados soportan estas aplicaciones dinámicas a través de funciones de inspección de aplicaciones. El filtro de paquetes con estados husmea la sesión inicial y analiza los datos de aplicación para conocer qué canales adicionales fueron negociados. Luego, el filtro de paquetes con estados aplica la política de que si se permite la sesión inicial, todos los canales adicionales de esa aplicación se permitirán también.



Haga clic en cada botón para ver el intercambio de paquetes para el tratamiento CBAC de TCP & UDP.



Haga clic en cada botón para ver el intercambio de paquetes para el tratamiento CBAC de TCP & UDP.

Con CBAC, los protocolos que serán inspeccionados se especifican en una regla de inspección. La regla de inspección se aplica a una interfaz en una dirección (de entrada o de salida) cuando se aplica la inspección. El motor del firewall inspecciona sólo los paquetes de los protocolos especificados si ya han pasado por la ACL de entrada que se aplica a la interfaz interna. Si la ACL deniega un paquete, el paquete se descarta y no es inspeccionado por el firewall.

Los paquetes que coinciden con la regla de inspección generan una entrada de ACL dinámica que permite el acceso del tráfico de retorno al firewall. El firewall crea y elimina ACLs a medida que las aplicaciones lo requieran. Cuando una aplicación se cierra, CBAC elimina todas las ACLs dinámicas de esa sesión.

El motor del firewall IOS de Cisco puede reconocer comandos específicos en las aplicaciones como comandos SMTP ilegales en el canal de control y detectar y prevenir ciertos ataques de capa de aplicación. Cuando se detecta un ataque, el firewall puede realizar varias acciones:

Generar mensajes de alerta
Proteger los recursos del sistema que puedan impedir el rendimiento del sistema
Bloquear los paquetes que provengan de atacantes sospechados

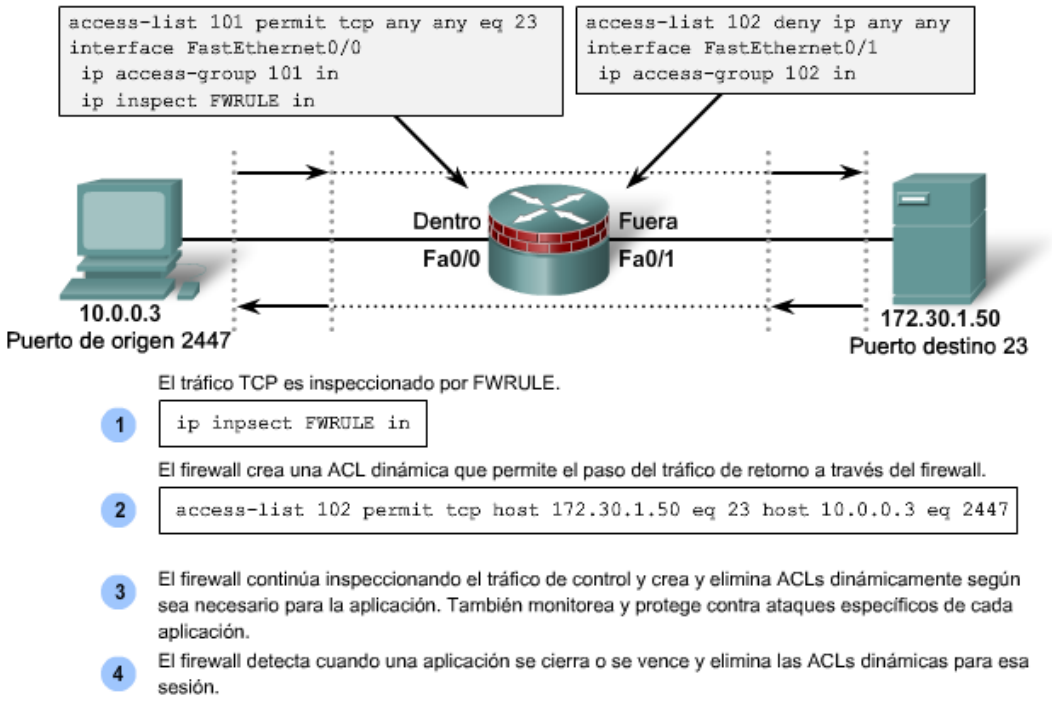
Pueden usarse los valores de vencimiento y umbral para manejar la información de estado de conexión. Estos valores ayudan a determinar cuándo descartar conexiones que no se han establecido enteramente o que vencen.

El firewall IOS de Cisco proporciona tres umbrales contra los ataques de DoS basados en TCP:

Número total de sesiones TCP medio abiertas
Número de sesiones medio abiertas en un intervalo de tiempo
Número de sesiones TCP medio abiertas por host

Si se supera un umbral establecido para las sesiones TCP medio abiertas, el firewall tiene dos opciones:

Envía un mensaje reset a los extremos de la sesión medio abierta más antigua, habilitando los recursos para servir a nuevos paquetes SYN.
Bloquea todos los paquetes SYN temporalmente durante un valor umbral configurable. Cuando el router bloquea un paquete SYN, el saludo de tres vías TCP nunca se inicia, lo cual evita que el router use recursos de procesamiento y memoria que las conexiones válidas pueden necesitar.



4.3.3 Configuracion de CBAC

La configuración de CBAC tiene cuatro pasos:

Paso 1. Elegir una interfaz - interna o externa.

Paso 2. Configurar ACLs IP en la interfaz.

Paso 3. Definir reglas de inspección.

Paso 4. Aplicar una regla de inspección a una interfaz.



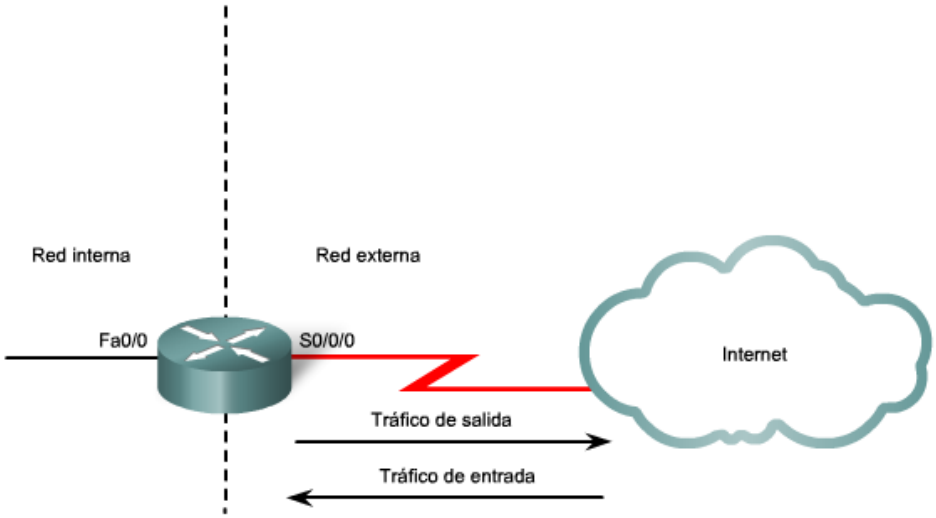
Elección de una interfaz

Primero determine las interfaces internas y externas para aplicar la inspección. Con CBAC, interno y externo se refiere a la dirección de la conversación. La interfaz en la que las sesiones pueden ser iniciadas debe seleccionarse como la interfaz interna. Las sesiones que tengan origen en la interfaz externa serán bloqueadas.

En una situación típica de dos interfaces en la que una se conecta con la red externa y la otra con la red protegida, CBAC evita que el tráfico de protocolos específicos ingrese al firewall y la red interna, salvo que sea parte de una sesión iniciada en la red interna.

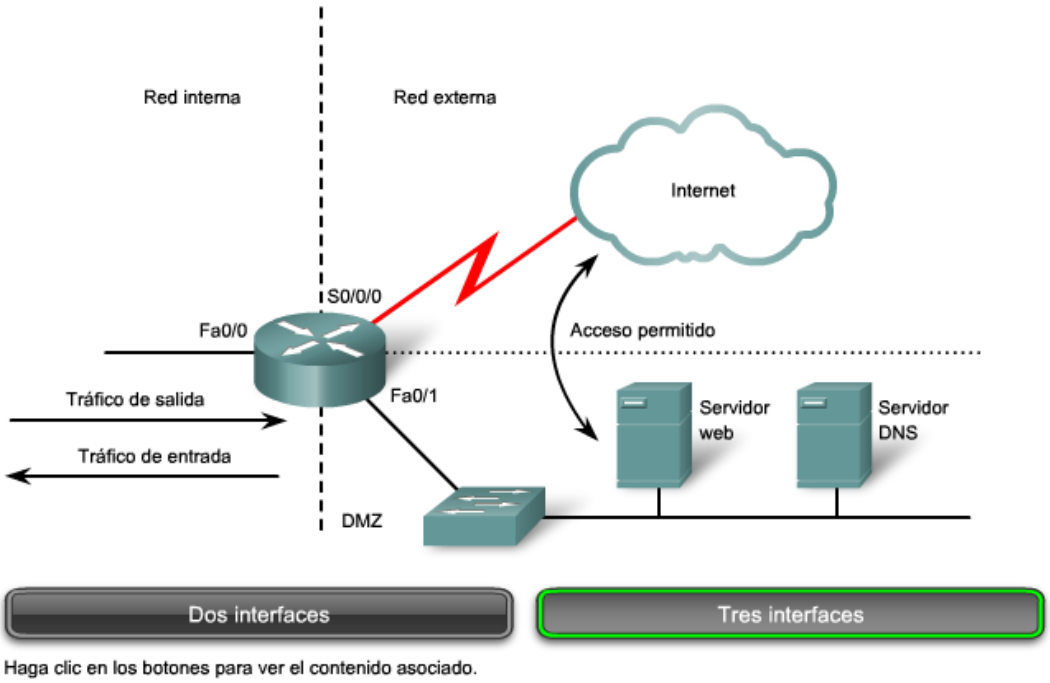
En un escenario de tres interfaces en el que la primera se conecta con la red externa, la segunda con una red en la DMZ y la tercera con la red protegida interna, el firewall puede permitir el paso de tráfico externo a recursos dentro de la DMZ, como DNS y servicios web. El mismo firewall puede luego evitar que el tráfico de protocolos específicos ingrese a la red interna, salvo que sea parte de una sesión iniciada en la red interna.

CBAC también puede ser configurado en dos direcciones en una o más interfaces. Configure el firewall en dos direcciones cuando las redes de ambos lados del firewall requieran protección, como en configuraciones extranet e intranet, y para la protección contra ataques de DoS. Si configura CBAC en dos direcciones, configure una dirección primero usando las designaciones de interfaz interna o externa. Cuando configure CBAC en la otra dirección, las designaciones de interfaz deben invertirse.



Dos interfaces | Tres interfaces

Haga clic en los botones para ver el contenido asociado.



Configuración de ACLs IP en la interfaz

Para que el firewall IOS de Cisco funcione correctamente, el administrador debe configurar ACLs IP en las interfaces interna, externa y DMZ.

Para proporcionar los beneficios de seguridad de las ACLs, el administrador debe configurar, como mínimo, ACLs en los routers de borde situados en el borde de la red entre las redes interna y externa. Esto proporciona un buffer básico desde la red externa o desde un área menos controlada de la red de una empresa a un área más sensible de la red.

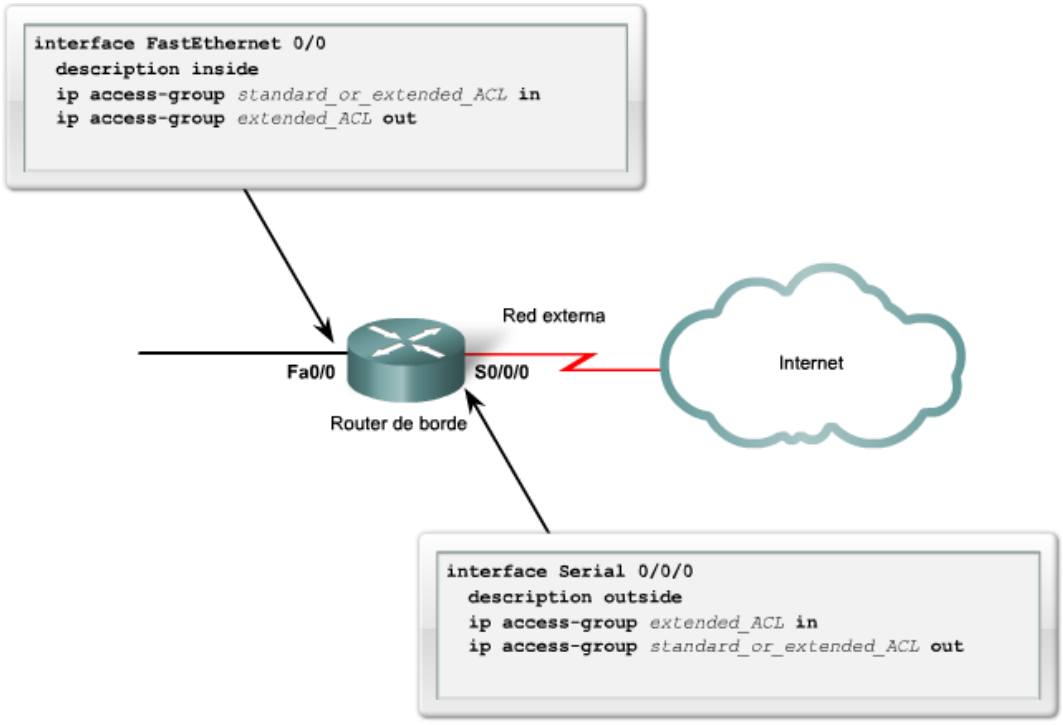
También se pueden posicionar las ACLs entre dos partes internas de una red para controlar el flujo de tráfico. Por ejemplo, si la red de investigación y desarrollo (I+D) de una empresa está separada de la red de recursos humanos por medio de un router, se puede implementar una ACL para evitar que los empleados de I+D tengan acceso a la red de recursos humanos.

Se pueden configurar ACLs en una interfaz para filtrar el tráfico de entrada, de salida o ambos. El administrador debe definir ACLs para cada protocolo habilitado en la interfaz para controlar el flujo de tráfico de ese protocolo. Use ACLs para determinar qué tipos de tráfico reenviar o bloquear en las interfaces del router. Por ejemplo, el administrador puede permitir el tráfico de correo electrónico pero bloquear el tráfico de Telnet.

Estos son algunos consejos para configurar ACLs IP en un firewall IOS de Cisco:

Comience con una configuración básica que permita todo el tráfico desde las redes protegidas a las redes no protegidas pero que bloquee el tráfico desde las redes no protegidas.

Permita el tráfico que deberá inspeccionar el firewall IOS de Cisco. Por ejemplo, si el firewall está configurado para inspeccionar Telnet, debe permitirse el tráfico Telnet en todas las ACLs que se apliquen al flujo inicial de Telnet.
Use ACLs extendidas para filtrar el tráfico que ingresa de las redes no protegidas. Para que el firewall IOS de Cisco cree entradas temporales dinámicamente, la ACL del tráfico de retorno debe ser extendida. Si el firewall sólo tiene dos conexiones, una a la red interna y otra a la red externa, la aplicación de ACLs de entrada en ambas interfaces funciona bien porque los paquetes son detenidos antes de tener oportunidad de afectar al router.
Configure protección antifalsificación al denegar todo el tráfico de entrada (de entrada en una interfaz externa) de una dirección de origen que coincida con una dirección de la red protegida. La protección antifalsificación evita que el tráfico de la red no protegida asuma la identidad de un dispositivo de la red protegida.
Deniegue los mensajes broadcast con la dirección de origen 255.255.255.255. Esta entrada ayuda a prevenir ataques de broadcast.
Por defecto, la última entrada en las ACLs es una denegación implícita de todo el tráfico IP que no está permitido específicamente en las otras entradas de la ACL.
Opcionalmente, el administrador puede agregar una entrada a la ACL que deniegue el tráfico IP con cualquier dirección de origen o destino, explicitando así la regla de denegación. Agregar esta entrada es útil si es necesario registrar la información de los paquetes denegados.



Definición de reglas de inspección

El administrador debe definir reglas de inspección para especificar qué protocolos de capa de aplicación inspeccionar en una interfaz. Normalmente, sólo es necesario definir una regla de inspección. La única excepción ocurre si es necesario habilitar el motor del

firewall en dos direcciones en una sola interfaz del firewall. En este caso, el administrador puede configurar dos reglas, una por cada dirección.

La regla de inspección debe especificar cada protocolo que se desea inspeccionar, así como UDP, ICMP o TCP genérico, si se desea. La inspección de TCP genérico y UDP permite dinámicamente el tráfico de retorno de las sesiones activas. La inspección de ICMP permite los paquetes de respuesta de eco se reenvíen como una respuesta a mensajes eco ICMP previamente enviados.

La regla de inspección consiste en una serie de sentencias, cada una especificando el protocolo y el mismo nombre de regla de inspección. Las reglas de inspección incluyen opciones para el control de mensajes de alerta y registro de auditoría.

Las reglas de inspección se configuran en el modo de configuración global.

Router(config)# ip inspect name nombre_inspección protocolo [alert {on | off}] [audit-trail {on | off}] [timeout segundos]

Ejemplo 1

En este ejemplo, la regla de inspección se llamará FWRULE. FWRULE inspecciona SMTP y FTP con alertas y registros de auditoría habilitados. FWRULE tiene un tiempo de vencimiento por inactividad de 300 segundos.

ip inspect name FWRULE smtp alert on audit-trail on timeout 300

ip inspect name FWRULE ftp alert on audit-trail on timeout 300

Ejemplo 2

En este ejemplo, la regla PERMIT_JAVA permite a todos los usuarios permitidos por la ACL estándar 10 descargar applets de Java.

ip inspect name PERMIT_JAVA http java-list 10

access-list 10 permit 10.224.10.0 0.0.0.255

Ejemplo 3

En este ejemplo, se define para su inspección por el firewall IOS de Cisco una lista de protocolos que incluye TCP genérico con un tiempo de vencimiento de 12 horas (normalmente 1 hora).

ip inspect name in2out rcmd

ip inspect name in2out ftp

ip inspect name in2out tftp

ip inspect name in2out tcp timeout 43200

ip inspect name in2out http

ip inspect name in2out udp

```
Router(config)#
ip inspect name inspection_name protocol [alert {on | off}] [audit-trail {on | off}]
[timeout seconds]
```

Parámetro	Descripción
inspection-name	Nombra el grupo de reglas de inspección. Si quiere agregar un protocolo a un grupo de reglas existente, use el mismo nombre de inspección para las reglas.
protocol	El protocolo a inspeccionar.
alert {on | off}	(Opcional) Para cada protocolo inspeccionado, puede encenderse o apagarse la generación de mensajes de alerta. Si no se selecciona una opción, se generan alertas basándose en la configuración del comando **ip inspect alert-off**.
audit-trail {on | off}	(Opcional) Para cada protocolo inspeccionado, puede encenderse o apagase la opción **audit-trail**. Si no se selecciona una opción, los mensajes **audit trail** se generan basándose en la configuración del comando **ip inspect audit-trail**.
timeout *seconds*	(Opcional) Especifique el número de segundos para establecer un vencimiento por inactividad que invalide los vencimientos por inactividad TCP o UDP globales para el protocolo especificado. Este vencimiento por inactividad invalida los vencimientos por inactividad TCP y UDP globales pero no invalida el vencimiento por inactividad DNS global.

Aplicación de una regla de inspección a una interfaz

El último paso para la configuración de CBAC es la aplicación de la regla de inspección a la interfaz.

Esta es la sintaxis del comando utilizado para activar una regla de inspección en una interfaz.

Router(config-if)# ip inspect nombre_inspección {in | out}

Para que el firewall IOS de Cisco sea efectivo, tanto las reglas de inspección como las ACLs deben ser aplicadas estratégicamente a todas las interfaces del router. Hay dos principios que guian la aplicación de reglas de inspección y ACLs en el router:

En la interfaz en la que se inicia el tráfico, aplique una ACL en la dirección de entrada para permitir sólo el tráfico solicitado y aplique la regla en la dirección de entrada para inspeccionar el tráfico solicitado.
En las otras interfaces, aplique una ACL en la dirección de entrada para denegar todo el tráfico, excepto el tráfico que no ha sido inspeccionado por el firewall, como GRE o ICMP que no está relacionado con mensajes de solicitud de eco y su respuesta.

Por ejemplo, un administrador necesita permitir a los usuarios internos iniciar tráfico TCP, UDP e ICMP con todas las fuentes externas. Se permite a los clientes externos comunicarse con el servidor SMTP server (209.165.201.1) y el servidor HTTP (209.165.201.2) que están localizados en la DMZ de la empresa. También es necesario permitir ciertos mensajes ICMP en todas las interfaces. Todo el resto del tráfico de la red externa es denegado.

Para este ejemplo, primero cree una ACL que permita las sesiones TCP, UDP e ICMP y deniegue todo el resto del tráfico.

R1(config)# access-list 101 permit tcp 10.10.10.0 0.0.0.255 any

R1(config)# access-list 101 permit udp 10.10.10.0 0.0.0.255 any

R1(config)# access-list 101 permit icmp 10.10.10.0 0.0.0.255 any

R1(config)# access-list 101 deny ip any any

Esta ACL será aplicada a la interfaz interna en dirección de entrada. La ACL procesa tráfico que se inicia en la red interna antes de dejar la red.

R1(config)# interface Fa0/0

R1(config-if)# ip access-group 101 in

Luego, cree una ACL extendida en la que el tráfico SMTP y HTTP sea permitido desde la red externa hacia la red DMZ solamente y deniegue todo el resto del tráfico.

R1(config)# access-list 102 permit tcp any 209.165.201.1 0.0.0.0 eq 80

R1(config)# access-list 102 permit tcp any 209.165.201.2 0.0.0.0 eq smtp

R1(config)# access-list 102 permit icmp any any echo-reply

R1(config)# access-list 102 permit icmp any any unreachable

R1(config)# access-list 102 permit icmp any any administratively-prohibited

R1(config)# access-list 102 permit icmp any any packet-too-big

R1(config)# access-list 102 permit icmp any any echo

R1(config)# access-list 102 permit icmp any any time-exceeded

R1(config)# access-list 102 deny ip any any

Esta ACL se aplica en la interfaz que conecta la red externa en la dirección de entrada.

R1(config)# interface S0/0/0

R1(config-if)# ip access-group 102 in

Si la configuración se detuviera allí, todo el tráfico de retorno, a excepción de los mensajes ICMP, sería denegado por causa de la ACL externa. A continuación, cree reglas de inspección para TCP y UDP.

R1(config)# ip inspect name MYSITE tcp

R1(config)# ip inspect name MYSITE udp

Estas reglas de inspección deberán aplicarse en la interfaz interna en dirección de entrada.

R1(config)# interface Fa0/0

R1(config-if)# ip inspect MYSITE in

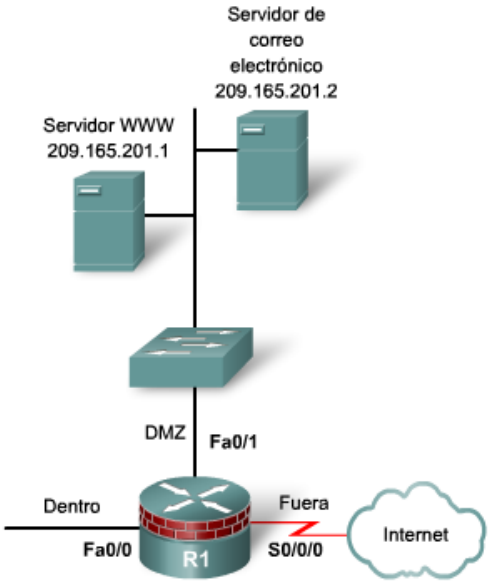
La lista de inspección crea automáticamente sentencias de ACL temporal en la ACL de entrada que se aplican a la interfaz externa para conexiones TCP y UDP. Esto permite el tráfico TCP y UDP que responde a solicitudes generadas en la red interna.

Para deshabilitar CBAC en el router, use el comando global no ip inspect.

Router(config)# no ip inspect

Este comando elimina todos los comandos CBAC, la tabla de estados y todas las entradas ACL temporales creadas por CBAC. También lleva todos los valores de vencimiento y umbral al valor por defecto. Luego de que se deshabilita CBAC, los procesos de inspección ya no están disponibles y el router utiliza sólo las implementaciones ACL actuales para filtrado.

```
ip inspect name MYSITE tcp
ip inspect name MYSITE udp
!
interface FastEthernet0/0
  ip address 10.10.10.254 255.255.255.0
  ip access-group 101 in
  ip inspect MYSITE in
!
interface FastEthernet0/1
  ip address 209.165.201.30 255.255.255.224
!
interface Serial0/0/0
  ip address 209.165.200.225 255.255.255.224
  ip access-group 102 in
!
access-list 101
  permit tcp 10.10.10.0 0.0.0.255 any
  permit udp 10.10.10.0 0.0.0.255 any
  permit icmp 10.10.10.0 0.0.0.255 any
  deny ip any any
access-list 102
  permit tcp any host 209.165.201.1 eq www
  permit tcp any host 209.165.201.2 eq smtp
  permit icmp any any echo-reply
  permit icmp any any unreachable
  permit icmp any any administratively-
    prohibited
  permit icmp any any packet-too-big
  permit icmp any any echo
  permit icmp any any time-exceeded
  deny ip any any
```



4.3.4 Resolucion de problemas de CBAC

La inspección CBAC soporta dos tipos de funciones de registro: alertas y auditorías.

Alertas

Las alertas muestran mensajes relacionados con la operación de CBAC, como recursos insuficientes del router, ataques de DoS y otras amenazas. Las alertas están habilitadas por defecto y se muestran automáticamente en la consola del router. El administrador puede deshabilitar las alertas globalmente, aunque es altamente recomendable que las alertas permanezcan habilitadas.

Router(config)# ip inspect alert-off

Además, el administrador puede deshabilitar y habilitar las alertas por regla de inspección; sin embargo, es altamente recomendable que las alertas permanezcan habilitadas.

Este es un ejemplo de una alerta que informa que alguien está intentando enviar un comando SMTP no aprobado a un servidor de correo electrónico:

%FW-4-SMTP_INVALID_COMMAND: Invalid SMTP command from initiator (209.165.201.5:49387)

CBAC puede detectar otros tipos de ataques SMTP:

Envío de un pipe (|) en los campos To o From de un mensaje de correo electrónico
Envío de :decode@ en el encabezado del mensaje de correo electrónico
Uso de los viejos comandos SMTP wiz y debug en el puerto SMTP
Ejecución de comandos arbitrarios para explotar una falla en el programa de correo electrónico Majordomo.

Este es un ejemplo de una alerta generada cuando un hacker trata de explotar la falla SMTP de Majordomo:

02:04:55: %FW-4-TCP_MAJORDOMO_EXEC_BUG: Sig:3107: Majordomo Execute Attack - from 209.165.201.5 to 192.168.1.1:

```
Router(config)#
no ip inspect alert-off
```

- Habilita alertas en tiempo real.

*Nota: Las alertas están habilitadas por defecto y se muestran automáticamente en la línea de consola del router. Si las alertas han sido deshabilitadas con el comando **ip inspect alert-off**, debe usarse la forma **no** de ese comando para volver a habilitarlas, como se ve arriba.

Auditorías

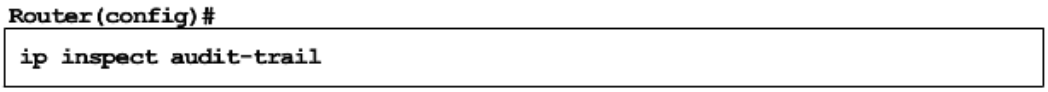
Las auditorías monitorean las conexiones que el CBAC inspecciona, incluyendo intentos de acceso válidos y no válidos. Por ejemplo, muestra cuando CBAC agrega o elimina una entrada de la tabla de estados. El registro de auditoría proporciona información estadística básica sobre la conexión. La auditoría está deshabilitada por defecto, pero puede ser habilitada con el siguiente comando:

Router(config)# ip inspect audit-trail

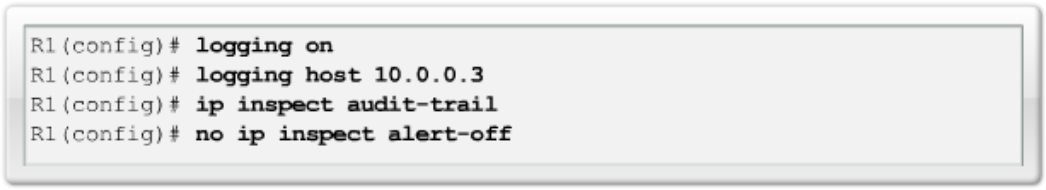
Por ejemplo, este mensaje de auditoría se crea para una conexión telnet iniciada por 192.1.1.2:

%FW-6-SESS_AUDIT_TRAIL: tcp session
initiator (192.168.1.2:32782) sent 22 bytes
responder (209.165.201.1:23) sent 200 bytes

Por defecto, las alertas y auditorías se muestran en la línea de consola. Esta información puede ser registrada en otros lugares, incluyendo el buffer interno del router o un servidor syslog externo.



- Habilita el envío de mensajes de registro de auditoría con syslog.



CBAC soporta muchos comandos show que pueden ser usados para ver las entradas temporales creadas en una ACL, la tabla de estados y la operación de CBAC. Para ver información sobre las inspecciones CBAC, use el comando show ip inspect.

Router# show ip inspect [parameter]

La siguiente salida del comando muestra las reglas de inspección configuradas para la regla de inspección inspect_outbound. Esta regla inspecciona tráfico TCP y UDP, ambos con sus tiempos de vencimiento por inactividad en los valores por defecto.

Router# show ip inspect name inspect_outbound

Inspection name inspect_outbound

cuseeme alert is on audit-trail is on timeout 3600

ftp alert is on audit-trail is on timeout 3600

http alert is on audit-trail is on timeout 3600

rcmd alert is on audit-trail is on timeout 3600

realaudio alert is on audit-trail is on timeout 3600

smtp max-data 20000000 alert is on audit-trail is on timeout 3600

tftp alert is on audit-trail is on timeout 30

udp alert is on audit-trail is on timeout 15

tcp alert is on audit-trail is on timeout 3600

En el siguiente ejemplo, la tabla de estados tiene dos entradas: 192.168.1.2 es dentro de la red y 209.165.201.1 es fuera de ella. La segunda entrada muestra al dispositivo interno abrir una conexión a un servidor FTP externo. La primera conexión muestra la conexión de datos que el servidor FTP abrió con el cliente interno. Así se muestra la creación dinámica de entradas ACL en la ACL extendida de entrada. El comando show ip access-list muestra las entradas ACL creadas dinámicamente por la ACL extendida de entrada.

Router# show ip inspect sessions
Established Sessions

Session 25A3378 (209.165.201.1:20)=>(192.168.1.2:32704) ftp-data SIS_OPEN

Session 25A5AC2 (192.168.1.2:32703)=>(209.165.201.1:21) ftp SIS_OPEN

Router# show ip access-list

Extended IP access list 100

permit tcp host 209.165.201.1 eq 21 host 192.168.1.2 eq 32703 (24 matches)

permit tcp host 209.165.201.1 eq 20 host 192.168.1.2 eq 32704 (88 matches)

<output omitted>

Hay dos entradas ACL dinámicas que permiten el tráfico de retorno del servidor FTP, 209.165.201.1, al cliente FTP, 192.168.1.1.

Parámetros **show ip inspect**

Parámetro	Explicación
name *inspection_name*	Limita lo que se muestra a las reglas de inspección especificadas.
config	Muestra toda la configuración de inspección CBAC del router.
interfaces	Muestra las reglas activadas en las interfaces de su router.
sessions	Muestra un resumen de las conexiones en la tabla de estados CBAC.
sessions [detail]	Muestra todos los detalles de las conexiones en la tabla de estados CBAC.
all	Muestra toda la información de las opciones de la lista de esa tabla.

Para una resolución de problemas de CBAC detallada, el administrador puede usar los comandos debug, que le permiten ver en tiempo real cómo opera CBAC en el router. El comando debug ip inspect puede inspeccionar varias aplicaciones y otros detalles de operación.

Router# debug ip inspect protocol parameter

Los nombres de aplicaciones que deben usarse para la inspección son cuseeme, dns, ftp-cmd, ftp-token, h323, http, netshow, rcmd, realaudio, rpc, rtsp, sip, skinny, smtp, sqlnet, streamworks, tftp y vdolive.

Esta salida del comando debug ip inspect timers permite al administrador determinar, entre otras cosas, cuándo se alcanzan los vencimientos por inactividad.

Router# debug ip inspect timers

Mar 2 01:20:43: CBAC sis 25A3604 pak 2541C58 TCP P ack 4223720032 seq 4200176225(22)

10.0.0.1:46409) => (10.1.0.1:21)

Mar 2 01:20:43: CBAC sis 25A3604 ftp L7 inspect result: PROCESS-SWITCH packet

*Mar 2 01:20:43: CBAC sis 25A3604 pak 2541C58 TCP P ack 4223720032 seq 4200176225(22)

(10.0.0.1:46409) => (10.1.0.1:21)

*Mar 2 01:20:43: CBAC sis 25A3604 ftp L7 inspect result: PASS packet

Mar 2 01:20:43: CBAC sis 25A3604 pak 2544374 TCP P ack 4200176247 seq 4223720032(30)

(10.0.0. 1:46409) <= (10.1.0.1:21)

Mar 2 01:20:43: CBAC sis 25A3604 ftp L7 inspect result: PASS packet

Mar 2 01:20:43: CBAC sis 25A3604 pak 25412F8 TCP P ack 4223720062 seq 4200176247(15)

(10.0.0. 1:46409) => (10.1.0.1:21)

Mar 2 01:20:43: CBAC sis 25A3604 ftp L7 inspect result: PASS packet

*Mar 2 01:20:43: CBAC sis 25C1CC4 pak 2544734 TCP S seq 4226992037(0) (10.1.0.1:20) =>

(10.0.0.1:46411)

Mar 2 01:20:43: CBAC sis 25C1CC4 pak 2541E38 TCP S ack 4226992038 seq 4203405054(0)

(10.1.0.1:20) <= (10.0.0.1:46411)

A partir de la versión 12.4(20)T del IOS de Cisco, el comando debug policy-firewall reemplaza al comando debug ip inspect.

CBAC ha producido un cambio dramático en la capacidad de los routers de Cisco de actuar como firewalls. CBAC tiene una versatilidad increíble, lo cual permite al router Cisco actuar como un verdadero firewall de estados. A pesar de la utilidad extrema de CBAC en la seguridad de las redes modernas, tiene sus desventajas. Nuevas tecnologías permiten una implementación más intuitiva y estructurada de los routers Cisco como firewalls IOS de Cisco y aportan a las funcionalidades de CBAC.

Parámetros **debug ip inspect**

Parámetro	Explicación
tcp	Muestra eventos de inspección TCP.
udp	Muestra eventos de inspección UDP.
icmp	Muestra eventos de inspección ICMP.
application_name	Muestra eventos de inspección de la aplicación especificada, como TFTP o SMTP.
events	Muestra eventos CBAC, incluyendo el procesamiento de paquetes.
object-creation	Muestra información sobre la adición de una entrada a la tabla de estados.
object-deletion	Muestra información sobre la eliminación de una entrada de la tabla de estados.
function-trace	Muestra información sobre las funciones de software que CBAC llama.
timers	Muestra información relacionada con los temporizadores CBAC, como que se han alcanzado los tiempos de vencimiento por inactividad de TCP o UDP.
detailed	Muestra información de los procesos CBAC en el router.

4.4 Firewall de politica basada en zonas

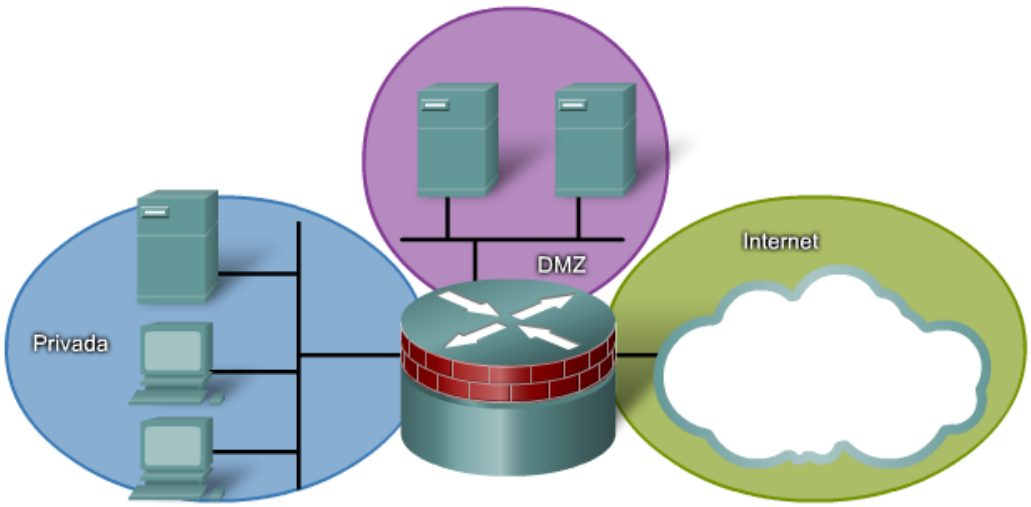
4.4.1 Caracteristicas del firewall de politica basada en zonas

En 2006, Cisco Systems introdujo el modelo de configuración del firewall de política basada en zonas con la versión 12.4(6)T del IOS de Cisco. Con este nuevo modelo, las interfaces son asignadas a zonas y luego se aplica una política de inspección al tráfico que se mueve entre las zonas. El firewall basado en zonas permite la aplicación de diferentes políticas de inspección a múltiples grupos de hosts conectados a la misma interfaz del router. Asimismo, tiene la habilidad de prohibir tráfico por medio de una política de deny-all por defecto entre las zonas del firewall.

El firewall de inspección de política basada en zonas (ZPF o ZBF o ZFW) soporta las funciones de firewalls anteriores, incluyendo inspección de paquetes con estados, inspección de aplicaciones, filtrado de URL y mitigación de ataques de DoS.

Las políticas de firewall se configuran usando el Cisco Common Classification Policy Language (C3PL), que utiliza una estructura jerárquica para definir la inspección del protocolo de red y permite a los hosts agruparse bajo una sola política de inspección.

Topología básica de seguridad por zonas



En este ejemplo, si se agrega una interfaz a la zona privada, los hosts conectados a la nueva interfaz en la zona privada pueden enviar tráfico a todos los hosts en la interfaz existente en la misma zona. Además, los hosts conectados a la nueva interfaz en la zona privada deben adherir a todas las políticas "privadas" existentes relacionadas con esa zona al enviar tráfico a otras zonas.

Las principales razones por las cuales los profesionales de seguridad en redes migran al modelo ZPF son la estructura y la facilidad de uso. El enfoque estructurado es útil para documentación y comunicación. La facilidad de uso hace que las implementaciones de seguridad en redes sean más accesibles a una comunidad más grande de profesionales de la seguridad.

Implementar CBAC es complejo y puede ser abrumador. A diferencia de ZPF, CBAC no utiliza ninguna estructura de datos jerárquica para modularizar la implementación. CBAC tiene las siguientes limitaciones:

Las múltiples políticas de inspección y ACLs en varias interfaces del router dificultan la correlación de las políticas del tráfico entre múltiples interfaces.
Las políticas no pueden asociarse a un grupo de hosts o subred con una ACL. Todo el tráfico que pasa por una interfaz dada está sujeto a la misma inspección.
El proceso depende demasiado de las ACLs.

Las zonas establecen las fronteras de seguridad en una red. La zona en sí define una frontera en la que el tráfico está sujeto a restricciones de políticas cuando cruza a otra región de la red. La política por defecto entre las zonas es de denegar todo. Si no se configura una política explícitamente, todo el tráfico que intente moverse entre las

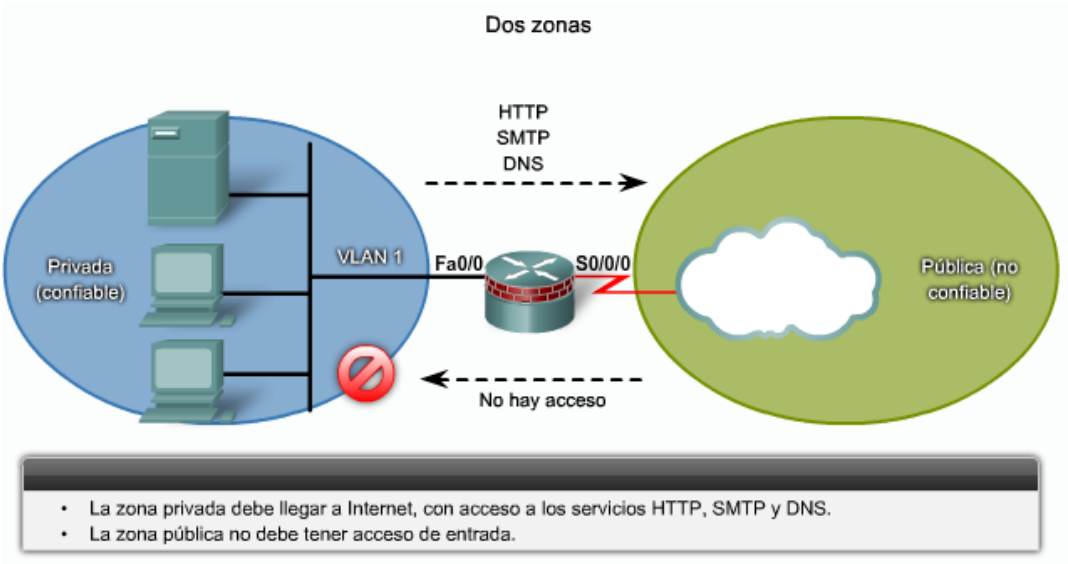
zonas será bloqueado. Esta es una desviación importante del modelo CBAC en el que el tráfico estaba permitido implícitamente hasta que fuera explícitamente bloqueado con una ACL.

Aunque muchos comandos ZPF aparentan ser similares a los comandos CBAC, no son iguales. Otro cambio significativo es la introducción del Cisco Common Classification Policy Language (C3PL). Este nuevo lenguaje de configuración de políticas facilita un enfoque modular sobre la implementación de firewalls.

Algunos de los beneficios de ZPF incluyen los siguientes:

No depende de ACLs.
La postura de seguridad del router es de bloquear salvo que sea explícitamente permitido.
Las políticas son de fácil lectura y resolución de problemas con C3PL.
Una política afecta cualquier tráfico dado, en lugar de necesitar múltiples ACLs y acciones de inspección.

Al decidir si implementar CBAC o zonas, debe tomarse en cuenta que ambos modelos de configuración pueden ser habilitados concurrentemente en el router. Sin embargo, los modelos no pueden ser combinados en la misma interfaz: una interfaz no puede ser configurada para inspección IP y como un miembro de una zona de seguridad al mismo tiempo.



El diseño de firewalls basados en zonas involucra algunos pasos:

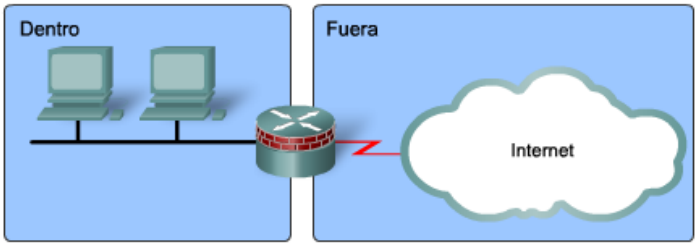
Paso 1. Determinar las zonas - La infraestructura de internetworking en cuestión debe ser dividida en zonas con diferentes niveles de seguridad. En este paso, el administrador no considera la implementación física del firewall (número de dispositivos, profundidad de la defensa, redundancia, etc), sino que se concentra en la separación de la infraestructura en zonas. Por ejemplo, la red pública a la que la red interna se conecta es una zona.

Paso 2. Establecimiento de políticas entre las zonas - Para cada par de zonas "origen-destino" (por ejemplo, desde la red interna hacia Internet), defina la sesión que los clientes en las zonas de origen pueden solicitar de los servidores en las zonas de destino. Estas sesiones son generalmente sesiones TCP y UDP, pero también pueden ser sesiones ICMP como un eco ICMP. Para el tráfico que no está basado en el concepto de sesiones, como IPsec Encapsulating Security Payload [ESP], el administrador debe definir flujos de tráfico unidireccionales del origen al destino y viceversa. Como en el paso 1, este paso se ocupa de los requerimientos de tráfico entre las zonas, no de la configuración física.

Paso 3. Diseño de la infraestructura física - Luego de identificar las zonas y documentar los requerimientos de tráfico, el administrador debe diseñar la infraestructura física tomando en cuenta los requerimientos de seguridad y disponibilidad. Esto incluye la estimación del número de dispositivos entre las zonas más seguras y las menos seguras y la determinación de dispositivos redundantes.

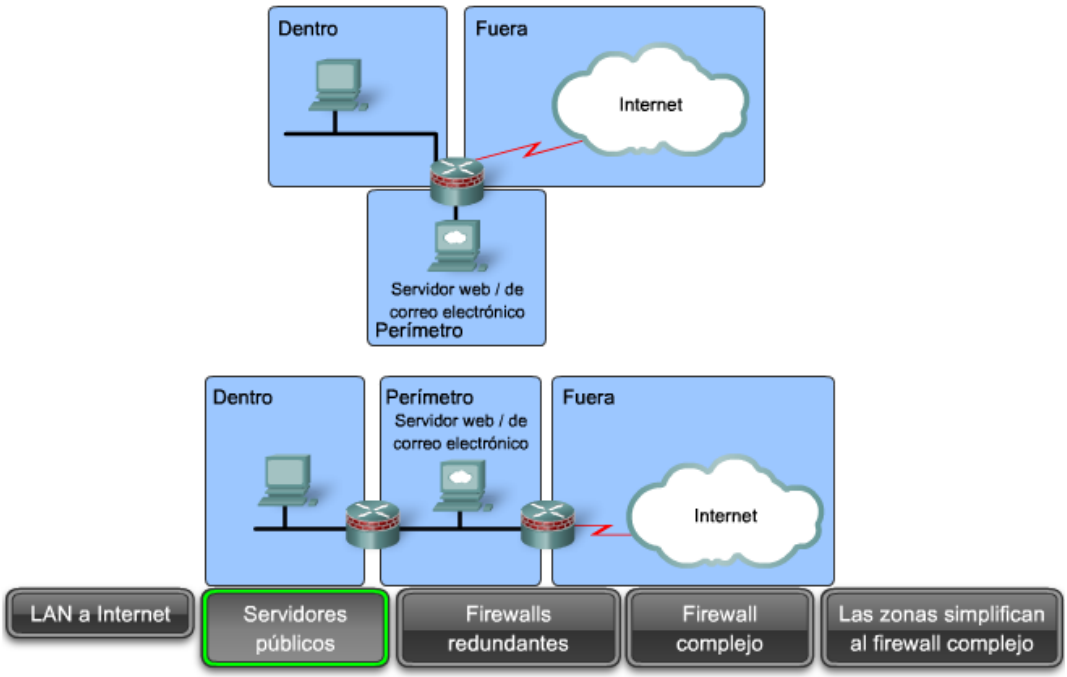
Paso 4. Identificación de subconjuntos en las zonas y fusión de requerimientos de tráfico - En cada dispositivo firewall del diseño, el administrador debe identificar subconjuntos en las zonas conectadas a sus interfaces y unir los requerimientos de tráfico en esas zonas. Por ejemplo, múltiples zonas pueden estar asociadas indirectamente con una sola interfaz en el router, resultando en una política interzona específica del dispositivo.

Algunos diseños ZPF comunes son un firewall LAN-a-Internet, un firewall con servidores públicos, firewalls redundantes y firewalls complejos.

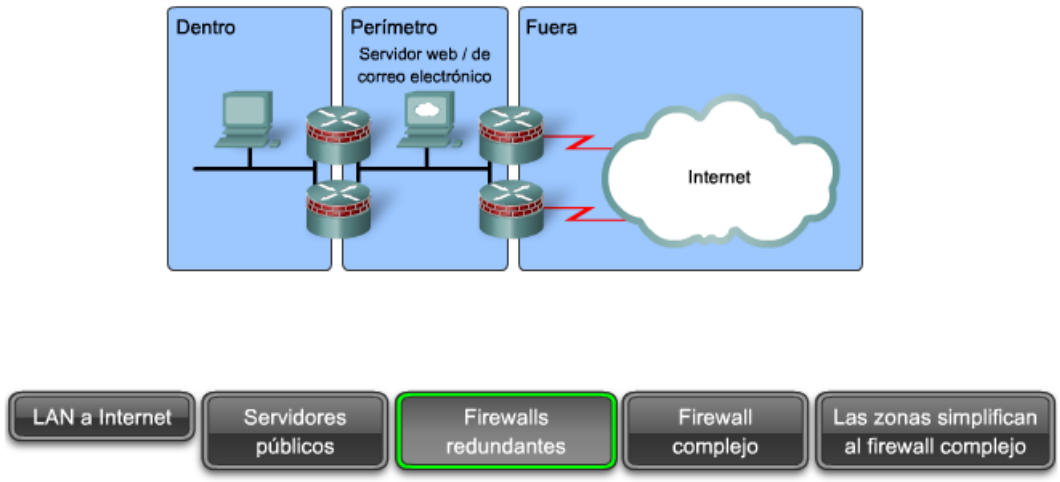


LAN a Internet | Servidores públicos | Firewalls redundantes | Firewall complejo | Las zonas simplifican al firewall complejo

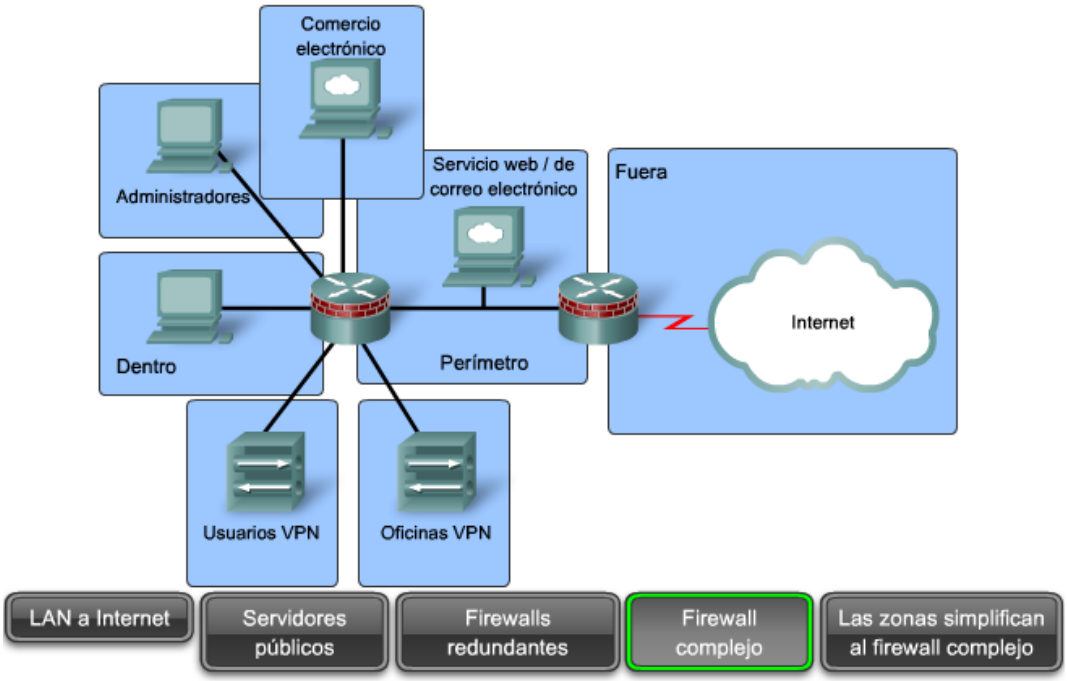
Haga clic en cada botón para ver el contenido asociado.



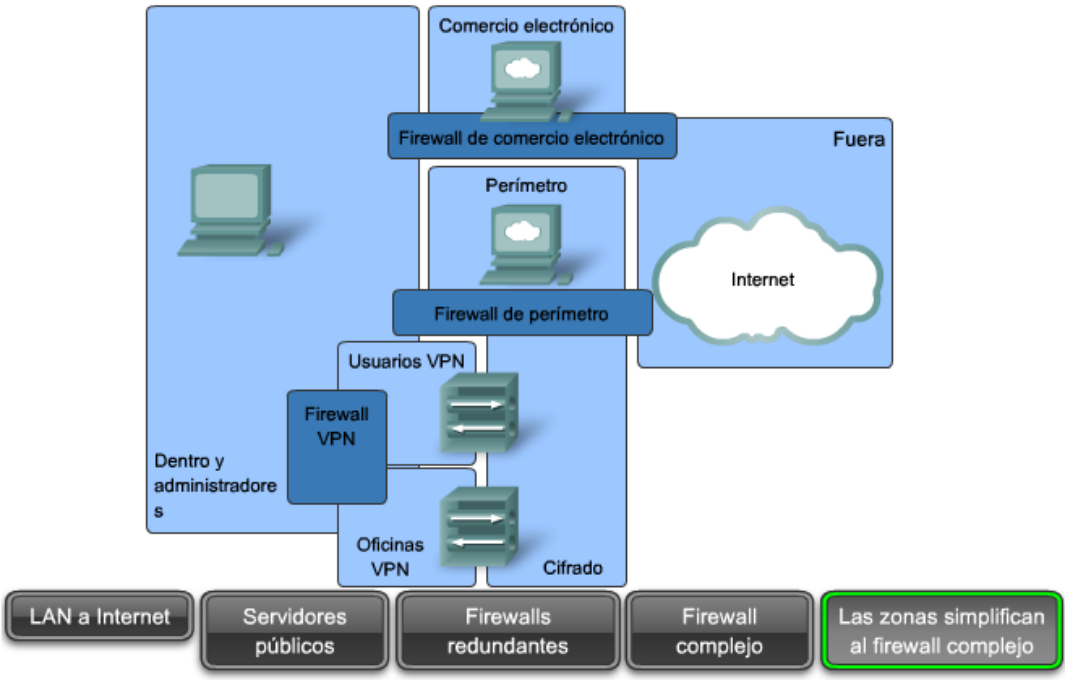
Haga clic en cada botón para ver el contenido asociado.



Haga clic en cada botón para ver el contenido asociado.



Haga clic en cada botón para ver el contenido asociado



Haga clic en cada botón para ver el contenido asociado.

4.4.2 Operación del firewall de politica basada en zonas

El firewall IOS de política basada en zonas puede llevar a cabo tres posibles acciones al ser configurado con el SDM de Cisco:

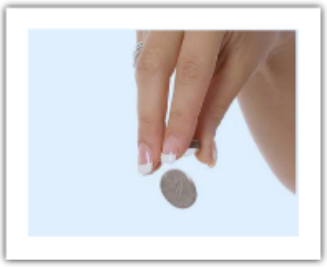
Inspect - (Inspeccionar) Configura la inspección de paquetes por estados del IOS de Cisco. Esta acción es equivalente a ingresar el comando CBAC ip inspect. Permite automáticamente el tráfico de retorno y potenciales mensajes ICMP. Para los protocolos que requieren múltiples sesiones paralelas de señalización y de datos (por ejemplo, FTP o H.323), la acción de inspección también maneja el correcto establecimiento de las sesiones de datos.
Drop - (Descartar) Análogo a una sentencia ACL deny. Hay una opción log disponible para registrar los paquetes rechazados.
Pass - (Pasar) Análogo a una sentencia ACL permit. La acción de paso no monitorea el estado de las conexiones o sesiones dentro del tráfico. El paso permite el tráfico en una sola dirección. Debe aplicarse una política correspondiente para permitir el paso del tráfico de retorno en la dirección opuesta.

Para aplicar límites de tasas al tráfico de una clase específica, use la opción police en conjunto con los comandos inspect o pass.

Acciones ZPF



Inspect (Inspeccionar)



Drop (Descartar)



Pass (Pasar)

La pertenencia de las interfaces del router a zonas está sujeta a varias reglas que gobiernan el comportamiento de las interfaces, como lo está el tráfico que se mueve entre interfaces que pertenecen a una zona:

Debe configurarse la zona antes de que el administrador pueda asignar interfaces a ella.
Si el tráfico debe fluir entre todas las interfaces de un router, cada interfaz debe ser miembro de una zona.
El administrador puede asignar una interfaz a sólo una zona de seguridad.
El flujo del tráfico se permite implícitamente entre las interfaces que pertenecen a la misma zona.
Para permitir el tráfico desde y hacia una interfaz que pertenece a una zona, debe configurarse una política que permita o inspeccione el tráfico entre esa zona y cualquier otra.
El tráfico no puede fluir entre una interfaz perteneciente a una zona y cualquier otra interfaz que no pertenezca a esa zona. El administrador puede aplicar acciones de paso, inspección y descarte sólo entre dos zonas.
Las interfaces que no han sido asignadas a una zona pueden usar la configuración CBAC de inspección de paquetes con estados.
Si un administrador no desea que una interfaz en el router sea parte de la política de firewall basado en zonas, puede ser necesario colocar esa interfaz en una zona y

configurar una política que deje pasar todo (también conocida como política falsa) entre esa zona y cualquier otra zona a la que se desee que fluya el tráfico.

Reglas del firewall de política basada en zonas para tráfico de aplicaciones

Se aplica la política por defecto para el tráfico y aplicación de política de origen de acuerdo con estas reglas:

¿Interfaz origen miembro de zona?	¿Interfaz destino miembro de zona?	¿Par de zonas existe?	¿Política existe?	RESULTADO
NO	NO	N/D	N/D	No hay impacto de zonas/política
SÍ (zona 1)	SÍ (zona 1)	N/D*	N/D	No se revisa la política (PASAR)
SÍ	NO	N/D	N/D	DESCARTAR
NO	SÍ	N/D	N/D	DESCARTAR
SÍ (zona 1)	SÍ (zona 2)	NO	N/D	DESCARTAR
SÍ (zona 1)	SÍ (zona 1)	SÍ	NO	DESCARTAR
SÍ (zona 1)	SÍ (zona 2)	SÍ	SÍ	acciones de la política

*El par de zonas debe tener zonas de origen y destino diferentes

Las reglas del firewall de política basada en zonas son diferentes cuando el router está involucrado en el flujo de tráfico y dependen de si el router es el origen o el destino del tráfico.

Cuando la interfaz está configurada para pertenecer a una zona, los hosts conectados a la interfaz están incluidos en la zona pero el tráfico que fluye desde y hacia las interfaces del router no es controlado por las políticas de la zona. En su lugar, todas las interfaces IP del router son automáticamente parte de la self zone. Para limitar el tráfico IP que se mueve hacia las direcciones IP del router desde las varias zonas del router, deben aplicarse las políticas. Pueden configurarse para bloquear, permitir o inspeccionar el tráfico entre la zona y la self zone del router y viceversa. Si no hay políticas entre una zona y la self zone, se permite el acceso de todo el tráfico a las interfaces del router sin pasar por inspección.

Se puede definir una política usando la self zone como la zona de origen o de destino. Esta es una zona definida por el sistema y no requiere que se configuren interfaces para pertenecer a ella. Un par de zonas que incluye a la self zone, junto con la política asociada a ésta, se aplica al tráfico que se dirige al router o que éste genera. No se aplica al tráfico que atraviesa el router.

Cuando el router está involucrado en el flujo de tráfico, reglas adicionales para firewalls de política basada en zonas gobiernan el comportamiento de la interfaz:

Todo el tráfico desde y hacia una interfaz dada es bloqueado implícitamente cuando se asigna la interfaz a una zona, excepto el tráfico desde o hacia otras interfaces en la misma zona y el tráfico hacia cualquier interfaz en el router.

Todas las interfaces IP del router son automáticamente parte de la self zone cuando se configura ZPF. La self zone es la única excepción a la política deny all por defecto. Todo el tráfico que se dirija a cualquier interfaz del router será permitido hasta que el tráfico sea explícitamente denegado.

La única excepción al enfoque deny all por defecto es el tráfico que fluye desde y hacia el router en sí. Este tráfico se permite por defecto: debe configurarse una política explícita para restringirlo.

Reglas del firewall de política basada en zonas para tráfico de router

¿Interfaz origen miembro de zona?	¿Interfaz destino miembro de zona?	¿Par de zonas existe?	¿Política existe?	RESULTADO
ROUTER	SÍ	NO	N/D	PASAR
ROUTER	SÍ	SÍ	NO	PASAR
ROUTER	SÍ	SÍ	SÍ	acciones de política
SÍ	ROUTER	NO	N/D	PASAR
SÍ	ROUTER	SÍ	NO	PASAR
SÍ	ROUTER	SÍ	SÍ	acciones de política

4.4.3 Configuracion del Firewall de politica basada en zonas con CLI

Hay varios pasos para configurar ZPF con la CLI:

Paso 1. Cree las zonas para el firewall con el comando zone security.

Paso 2. Defina clases de tráfico con el comando class-map type inspect.

Paso 3. Especifique políticas de firewall con el comando policy-map type inspect.

Paso 4. Aplique políticas de firewall a los pares de zonas de origen y destino usando el comando zone-pair security.

Paso 5. Asigne interfaces de router a las zonas usando el comando de interfaz zone-member security.

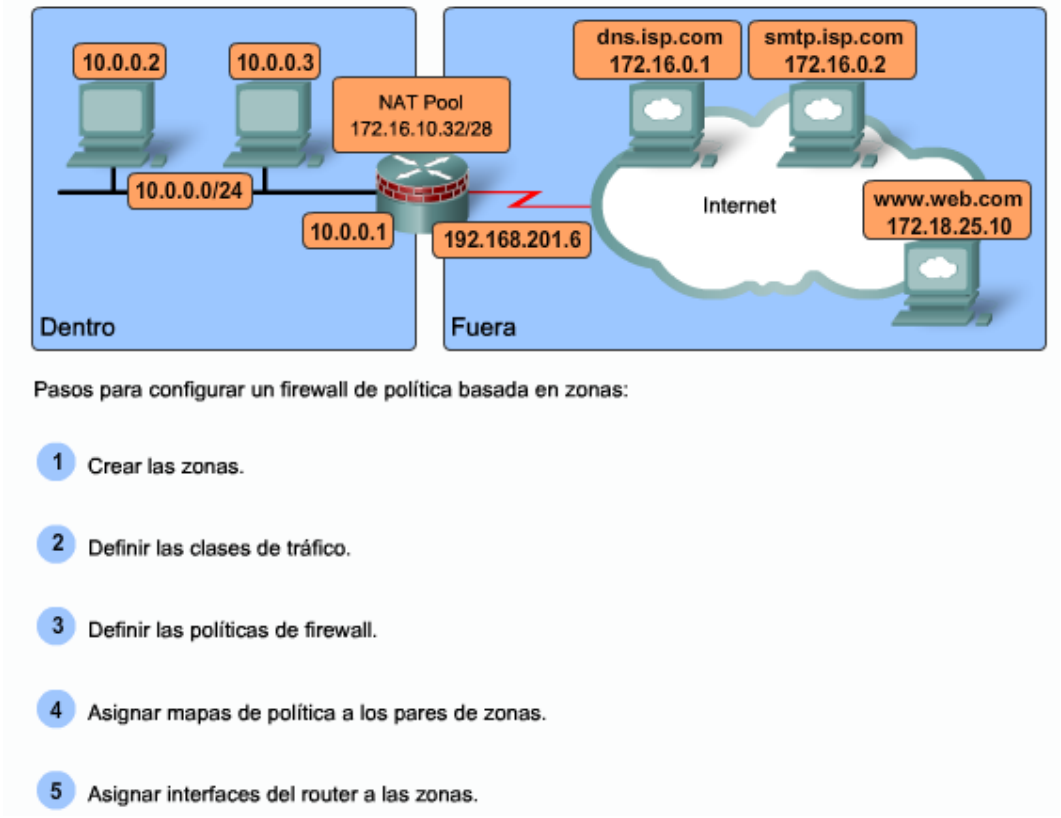
Al configurar ZPF con la CLI, deben considerarse varios factores:

Sólo pueden usarse los mapas de políticas definidos con type inspect con el comando zone-pair security.
Sólo pueden usarse los mapas de clases definidos con type inspect con type inspect.
Los nombres no pueden repetirse en los tipos de mapas de clases o de políticas. No puede haber un mapa de clases de calidad de servicio y un mapa de clases de inspección con el mismo nombre.
Debe configurarse una zona con el comando global zone security antes de que pueda ser usado en el comando de configuración de interfaz zone-member security.

Una interfaz no puede pertenecer a más de una zona. Para crear una unión de zonas de seguridad, especifique una nueva zona y mapa de políticas apropiado y pares de zonas. La función de firewall de política basada en zonas es un reemplazo de CBAC. Elimine el comando de configuración de interfaz ip inspect antes de aplicar el comando zone-member security.

El firewall de política basada en zonas puede coexistir con CBAC. El comando ip inspect puede ser usado en interfaces que no pertenecen a zonas de seguridad.
No puede haber flujo de tráfico entre una zona y una interfaz sin que se asigne una zona.
La aplicación del comando de configuración zone-member siempre resulta en una interrupción temporal del servicio.
La política interzona por defecto es de descartar todo el tráfico excepto si está especificado que no se lo haga en el comando de configuración zone-pair.
El router nunca filtra el tráfico entre interfaces en la misma zona.
El comando zone-member no protege el router en sí (el tráfico desde y hacia el router no es afectado) salvo que los pares de zonas sean configurados usando la self zone predefinida.

CBAC crea entradas dinámicamente en las ACLs asociadas con las interfaces en las que el comando ip inspect está configurado. ZPF no cambia las ACLs. Revise el uso de las ACLs antes de ingresar el comando zone-member.



Creación de las zonas

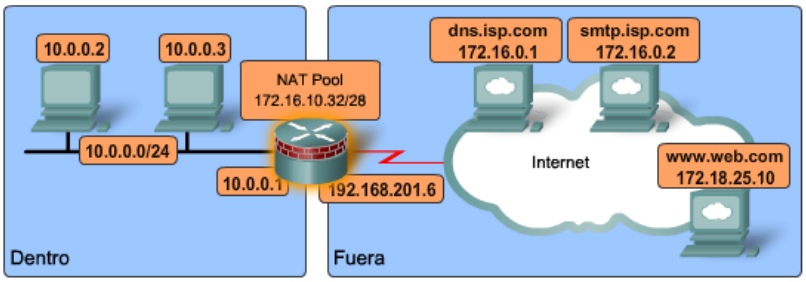
El administrador crea las zonas para el firewall con el comando zone security. Se recomienda hacer uso de la descripción opcional.

Router(config)# zone security nombre-zona

Router(config-sec-zone)# description línea-de-descripción

Piense en qué debe constituir las zonas. El consejo general es agrupar las interfaces que son similares desde una perspectiva de seguridad, en otras palabras, las interfaces que tienen necesidades de seguridad similares.

Paso 1: Crear zonas




```
FW(config)# zone security Inside
FW(config-sec-zone)# description Inside network
FW(config)# zone security Outside
FW(config-sec-zone)# description Outside network
```

Topología en zonas | Nmap pre-ZPF sin hosts activos | Nmap pre-ZPF con hosts activos

Haga clic en cada botón y los dispositivos resaltados para ver la configuración.

Escaneo de puerto externo sin hosts activos

```
External$ nmap --system-dns 172.16.10.32/28
(The 1671 ports scanned but not shown below are in state: closed)
PORT      STATE   SERVICE
23/tcp    open    telnet
79/tcp    open    finger
80/tcp    open    http

Nmap finished: 16 IP addresses (1 host up) scanned in 23.473 seconds
```

La configuración del firewall proporciona alguna seguridad porque NAT oculta los hosts internos de los potenciales intrusos. Un escaneo de puerto inicial desde fuera confirma esta suposición, ya que los intrusos potenciales solo pueden llegar a un host IP (el router mismo).

Topología en zonas | Nmap pre-ZPF sin hosts activos | Nmap pre-ZPF con hosts activos

Haga clic en cada botón y los dispositivos resaltados para ver la configuración.



Definición de clases de tráfico

Las clases de tráfico ZPF permiten al profesional de la seguridad en redes definir los flujos de tráfico de una manera tan granular como se desee.

Esta es la sintaxis para crear clases de tráfico ZPF.

Router(config)# class-map type inspect [match-any | match-all] nombre-mapa-clase

Para mapas de clases de nivel superior de capas 3 y 4, la opción match-any es el comportamiento por defecto.

Router(config)# class-map type inspect nombre-protocolo [match-any | match-all] nombre-mapa-clase

Para mapas de clase específicos de cada aplicación de capa 7, visite www.cisco.com para detalles de construcción.

La sintaxis para hacer referencia a listas de acceso dentro del mapa de clases es:

Router(config-cmap)# match access-group {grupo-acceso | name nombre-grupo-acceso}

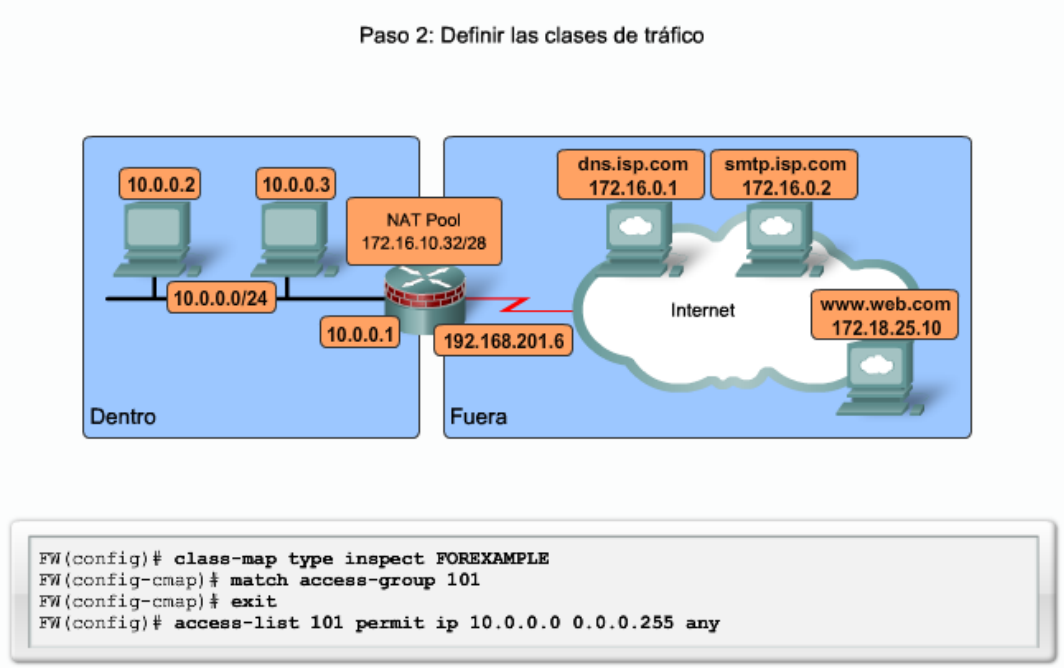
Los protocolos son comparados desde dentro del mapa de clases con la sintaxis:

Router(config-cmap)# match protocol nombre-protocolo

Se pueden configurar mapas de clases anidados usando la sintaxis:

Router(config-cmap)# match class-map nombre-mapa-clase

La habilidad de crear una jerarquía de clases y políticas anidando es una de las razones por las que ZPF constituye un enfoque tan potente para la creación de firewalls IOS de Cisco.




```
FW(config)# class-map type inspect FOREXAMPLE
FW(config-cmap)# match access-group 101
FW(config-cmap)# exit
FW(config)# access-list 101 permit ip 10.0.0.0 0.0.0.255 any
```

Especificación de políticas de firewall

De manera semejante a otros dispositivos modulares que usan la CLI para configurar el software IOS de Cisco, el administrador debe especificar qué hacer con el tráfico que coincide con la clase de tráfico deseada. Las opciones son pass (pasar), inspect (inspeccionar), drop (descartar) y police(aplicar una política).

Esta es la sintaxis para crear mapas de políticas ZPF.

Router(config)# policy-map type inspect nombre-mapa-política

Las clases de tráfico sobre las cuales debe realizarse una acción se especifican en el mapa de políticas.

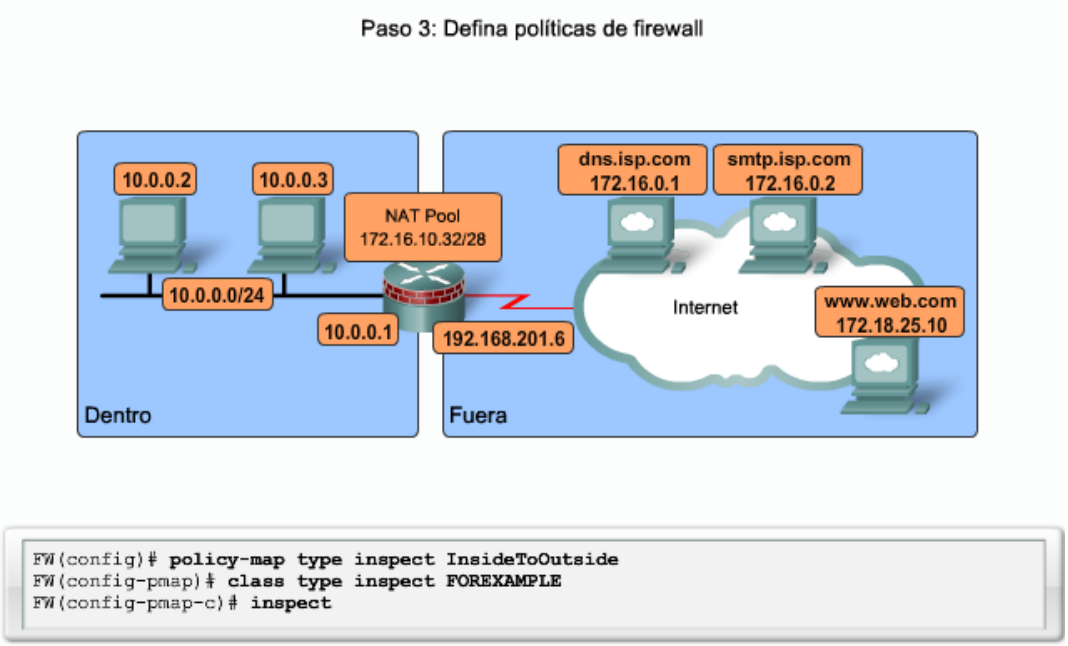
Router(config-pmap)# class type inspect nombre-clase

La clase por defecto (con la que coincide el resto del tráfico) se especifica por medio del siguiente comando:

Router(config-pmap)# class class-default

Por último, se especifica la acción que debe realizarse sobre el tráfico.

Router(config-pmap-c)# pass | inspect | drop [log] | police




```
FW(config)# policy-map type inspect InsideToOutside
FW(config-pmap)# class type inspect FOREXAMPLE
FW(config-pmap-c)# inspect
```

Aplicación de políticas de firewall

Luego de configurar la política de firewall, el administrador la aplica entre un par de zonas mediante el comando zone-pair security. Para aplicar una política, primero debe crearse un par de zonas. Especifique la zona de origen, la zona de destino y la política de manejo del tráfico que fluye entre ellas.

Router(config)# zone-pair security nombre-par-zonas [source nombre-zona-origen | self] destination [self | nombre-zona-destino]

Use el comando service-policy type inspect nombre-mapa-política para asociar un mapa de políticas y sus acciones asociadas a un par de zonas. Ingrese el comando luego del comando zone-pair security.

También puede configurarse la inspección profunda de paquetes (asociación de un mapa de políticas de capa 7 con un mapa de políticas de alto nivel). Esta es la sintaxis que se utiliza con la versión 12.4(20)T del IOS de Cisco.

Router(config-pmap-c)# service-policy {h323 | http | im | imap | p2p | pop3 | sip | smtp | sunrpc | urlfilter} mapa-política

El mapa de política es el nombre del mapa de políticas de capa 7 que se aplica al mapa de políticas de nivel superior de las capas 3 y 4.

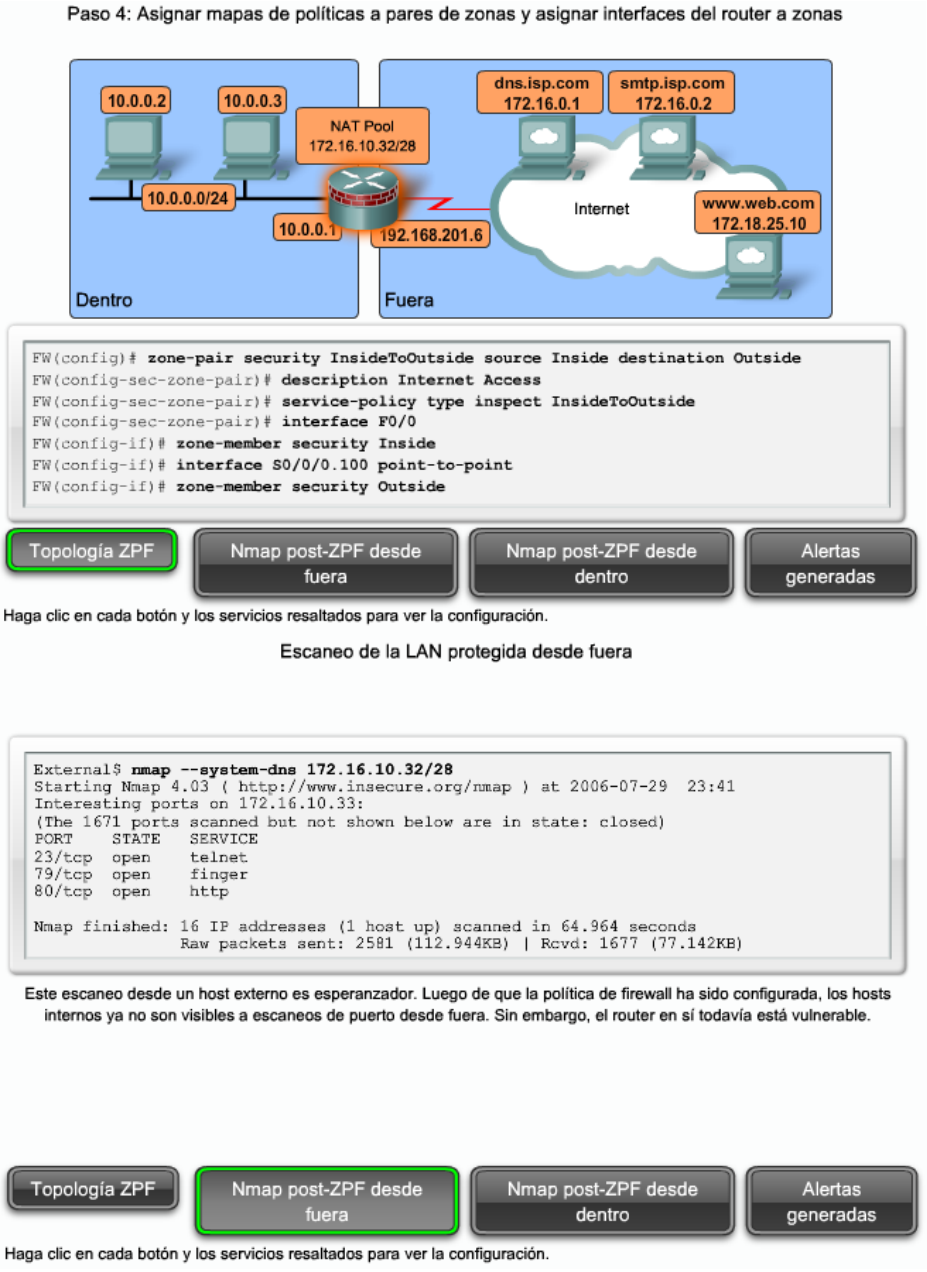
Asignación de interfaces

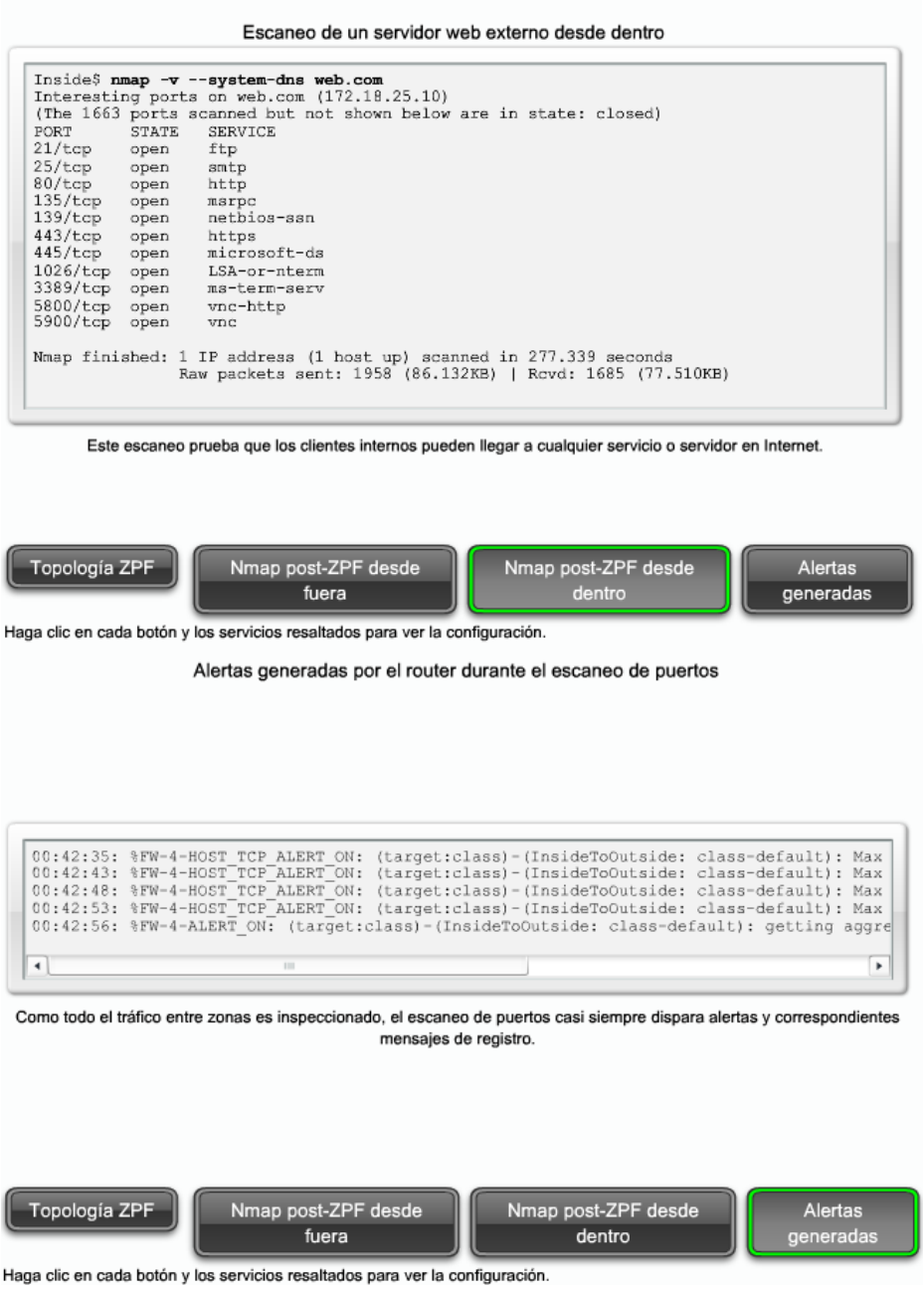
Por último, el administrador debe asignar interfaces a las zonas de seguridad apropiadas con el comando de interfaz zone-member.

Router(config-if)# zone-member security nombre-zona

El comando zone-member security coloca a la interfaz en una zona de seguridad, lo cual hace que todo el tráfico que se dirige desde y hacia la interfaz (excepto el tráfico que proviene del o se dirige al router) se descarte por defecto. Para permitir que el tráfico atraviese una interfaz que está en una zona de seguridad, la zona debe ser parte de un par de zonas que tenga una política aplicada. Si la política permite el tráfico (con las acciones de paso o inspección), éste podrá fluir a través de la interfaz.

La configuración de ZPF con la CLI puede parecer un poco intimidante al principio. La buena noticia es que hay dos maneras de configurar ZPF - con la CLI del IOS de Cisco o con el SDM de Cisco.





4.4.4 Configuracion del Firewall de politica basada en zonas con SDM

La configuración del firewall de política basada en zonas es mucho más fácil con el Administrador de Routers y Dispositivos de Seguridad de Cisco (SDM).

Hay cuatro pasos básicos para la configuración de ZPF con SDM:

Paso 1. Defina zonas.

Paso 2. Configure mapas de clases para describir el tráfico entre las zonas.

Paso 3. Cree mapas de políticas para aplicar acciones al tráfico de los mapas de clases.

Paso 4. Defina pares de zonas y asigne mapas de políticas a los pares de zonas.

A diferencia de la configuración CLI, con SDM, las interfaces están asociadas con las zonas en el paso 1.

Puede usarse una GUI nueva, similar a SDM, llamada Cisco Configuration Professional (CCP). Visite www.cisco.com/go/ciscocp para más detalles. CCP agrega la función de las comunidades (communities - grupos de dispositivos) para mejorar la administración de la red. Algunas tecnologías, como la inspección del protocolo SIP en la self zone, son soportadas por SDM pero no por CCP. Se requiere la versión 12.4(9)T del IOS de Cisco o posterior para ejecutar CCP. En el futuro, CCP reemplazará a SDM.



Definición de zonas

El primer paso al configurar el firewall de política basada en zonas IOS de Cisco con SDM es definir zonas. Una zona de seguridad es un grupo de interfaces en las cuales puede aplicarse una política de seguridad. Las interfaces en una zona comparten funciones o características comunes. Por ejemplo, el administrador puede ubicar dos interfaces que se conectan a la LAN local en una zona de seguridad y las interfaces que se conectan con Internet en otra zona de seguridad.

Para que el tráfico fluya entre todas las interfaces del router, todas las interfaces deben pertenecer a una zona de seguridad. Sin embargo, no es necesario que todas las interfaces del router pertenezcan a zonas de seguridad.

Estos son los pasos necesarios para crear una zona con SDM:

Paso 1. Vaya a Configure > Additional Tasks > Zones.

Paso 2. En el panel Zone haga clic en Add para crear una nueva zona.

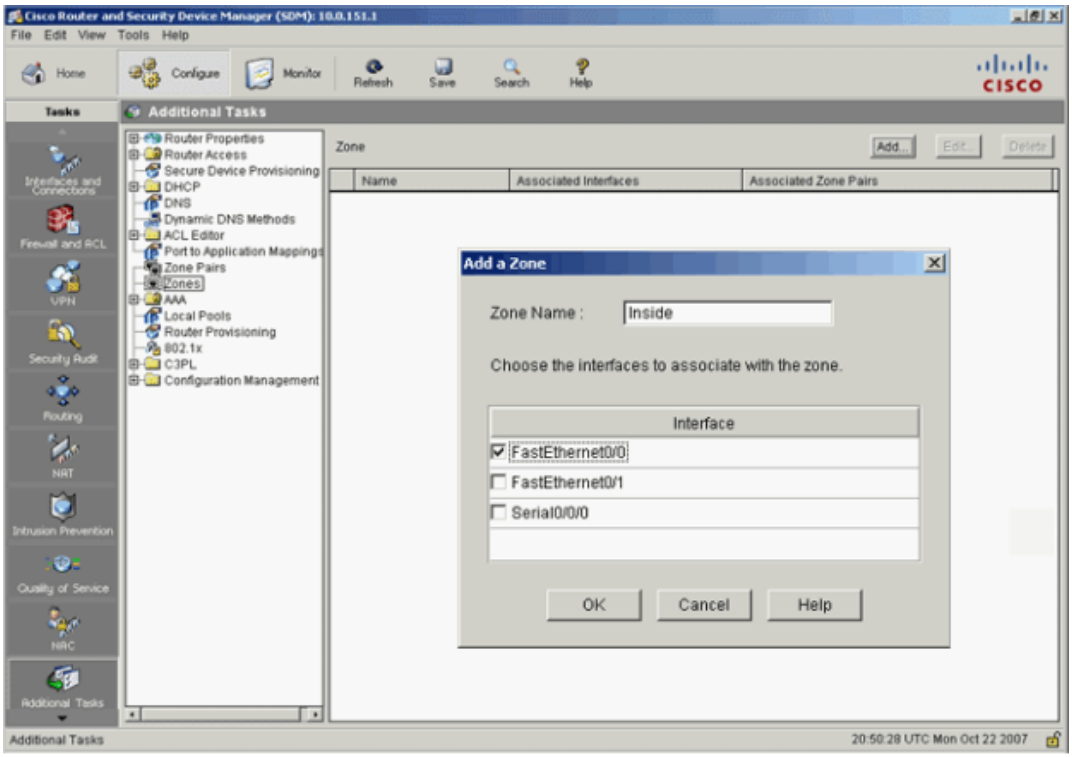
Paso 3. Aparecerá la ventana Add a Zone. Ingrese el nombre que desea darle a la zona en el campo Zone Name.

Paso 4. Elija las interfaces para esta zona marcando las casillas ubicadas junto al nombre de la interfaz. Como las interfaces físicas pueden ubicarse sólo en una zona, no aparecerán en la lista si ya han sido asignadas a una zona. Puede ubicar interfaces virtuales, como interfaces Dialer o Virtual Template, en varias zonas, por lo que estas interfaces siempre aparecerán en la lista.

Al asignar interfaces a las zonas, tenga en cuenta las reglas del firewall de política basada en zonas que gobiernan el comportamiento de las interfaces.

Paso 5. Haga clic en OK para crear la zona y a continuación haga clic en OK en la ventana Commands Delivery Status.

Luego de haber creado una zona, se pueden cambiar las interfaces asociadas a ella, pero no su nombre. Haga clic en Edit en el panel Zone para elegir diferentes interfaces para una zona existente. Haga clic en Delete en el panel Zone para eliminar una zona. Una zona perteneciente a una política sobre pares de zonas no puede ser eliminada.



Configuración de mapas de clases

El siguiente paso en la configuración de ZPF con SDM es la configuración de mapas de clases. Los mapas de clases identifican el tráfico y los parámetros de tráfico para la aplicación de la política.

Los mapas de clases de capas 3 y 4 filtran el tráfico basándose en criterios específicos:

Grupo de acceso - Una ACL estándar, extendida o nombrada puede filtrar el tráfico basándose en las direcciones y puertos de origen y destino.
Protocolo - El mapa de clases puede identificar protocolos de capa 4, como TCP, UDP e ICMP, así como servicios de aplicación como HTTP, SMTP y DNS. Cualquier servicio bien conocido o definido por el usuario que Port-to-Application Mapping (PAM) conozca puede ser especificado.
Mapa de clases - Puede anidarse un mapa de clases subordinado para proporcionar criterios de coincidencia adicionales.

Los mapas de clase pueden aplicar operadores match-any o match-all para determinar cómo aplicar el criterio de coincidencias. Si se especifica match-any, el tráfico debe coincidir con sólo uno de los criterios del mapa de clases. Si se especifica match-all, el tráfico debe coincidir con todos los criterios del mapa de clases que pertenezcan a esa clase particular.

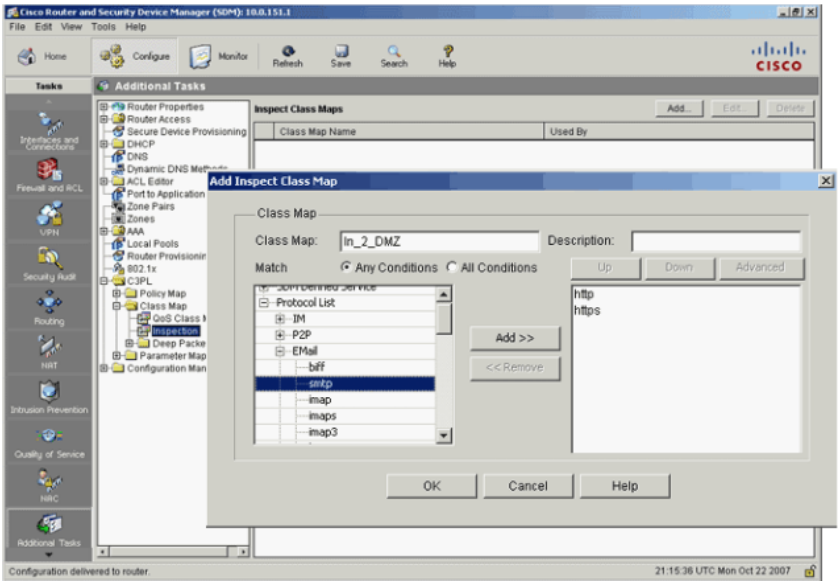
Estos son los pasos para crear un mapa de clases mediante SDM:

Paso 1. Vaya a Configure > Additional Tasks > C3PL > Class Map > Inspection.

Paso 2. En Inspection Class Maps, haga clic en Add.

Paso 3. Ingrese un nombre para el mapa de clases en el campo Class Map. Puede agregar una descripción en el campo Description. Seleccione los protocolos deseados de la lista y haga clic en Add>> para agregarlos a la lista de inspección de este mapa de clases.

Los mapas de clases pueden ser revisados, creados y editados en la ventana Inspect Class Map. El área Class Map Name de la ventana muestra una lista de los mapas de clases configurados; la porción inferior de la ventana muestra los detalles del mapa de clases seleccionado. Si fuera necesario editar un mapa de clases o ver más detalles, elija el mapa de clases de la lista y haga clic en Edit.



Creación de mapas de políticas

Una vez creados los mapas de clases, es tiempo de crear los mapas de políticas. Los mapas de clases se aplican dentro de los mapas de políticas. Los mapas de políticas especifican las acciones que deben realizarse cuando el tráfico coincide con un criterio, por lo que puede decirse que el mapa de política asocia clases de tráfico con acciones.

Los mapas de políticas de inspección especifican la acción que el router debe realizar sobre el tráfico que coincide con los criterios en los mapas de clases asociados. Estas son las acciones que soporta el mapa de políticas:

Pass - (Pasar) Se permite el paso del tráfico de una zona a la otra sólo en una dirección. El router no monitorea el estado de las conexiones o de la sesión.
Drop - (Descartar) El router descarta el tráfico no deseado y puede registrar el evento si se configura.
Inspect - (Inspeccionar) El router mantiene información de sesión y conexión basada en estados para permitir el tráfico de retorno desde una zona de destino a una zona de origen.

Estos son los pasos necesarios para la creación de un mapa de políticas con SDM:

Paso 1. Vaya a Configure > Additional Tasks > C3PL > Policy Map > Protocol Inspection.

Paso 2. En Protocol Inspection Policy Maps, haga clic en Add.

Paso 3. Ingrese un nombre para la política en el campo Policy Name y puede agregar una descripción en el campo Description. Podrá ver el nombre y la descripción que ingrese en la ventana Protocol Inspect Policy Maps.

Paso 4. Las columnas Class Map y Action muestran los mapas de clases asociados con este mapa de políticas, así como la acción que el router realiza con el tráfico descripto por el mapa de clases. Haga clic en Add para agregar un nuevo mapa de clases a la lista y configurar la acción.

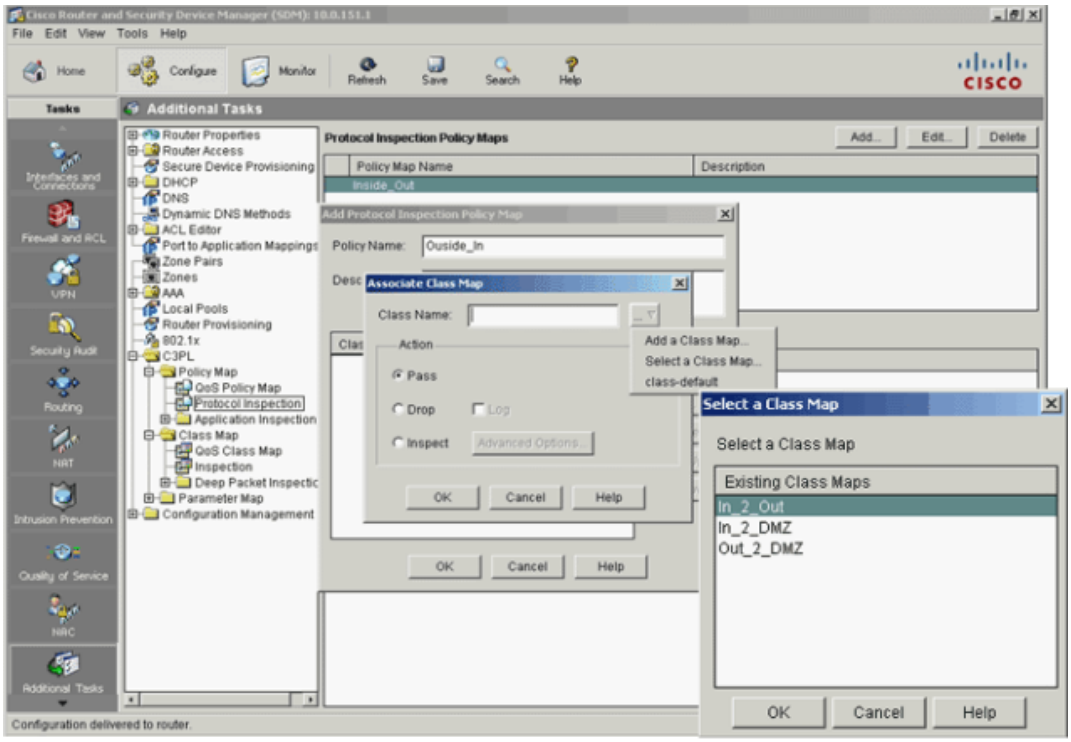
Paso 5. Aparecerá la ventana Associate Class Map. En el campo Class Name, ingrese el nombre del mapa de clases a aplicar. Si no conoce el nombre del mapa de clases o debe crearse uno nuevo, haga clic en la flecha inferior a la derecha del campo Class Name. Aparecerá un menú emergente para agregar un mapa de clases, elegir uno existente o elegir la clase por defecto.

Paso 6. Luego de seleccionar el mapa de clases, defina la acción que el mapa de políticas deberá realizar sobre el tráfico que coincida con el mapa de clases. En la sección Action, elija Pass, Drop, o Inspect según sean las necesidades particulares de este mapa de clases.

Paso 7. Haga clic en OK.

Paso 8. Para agregar otro mapa de clases a la política, haga clic en Add. Para modificar las acciones de un mapa de clases existente, vaya al mapa de clases en la lista Class Map y haga clic en Edit. Para eliminar un mapa de clases, vaya al mapa de clases en la lista Class Map y haga clic en Delete. Use los botones Move Up y Move Down para cambiar el orden en que se evalúan los mapas de clases.

Paso 9. Haga clic en OK. En la ventana Command Delivery Status, haga clic en OK.



Definición de pares de zonas

El par de zonas facilita la creación de una política de firewall unidireccional entre dos zonas de seguridad a especificarse. La dirección del tráfico se determina especificando zonas de seguridad de origen y destino. La misma zona no puede definirse como de origen y destino.

Si la intención es que el tráfico fluya en ambas direcciones entre dos zonas, debe crearse un par de zonas para cada dirección. Si la intención es que el tráfico fluya libremente entre todas las interfaces, cada interfaz debe configurarse en una zona.

Estos son los pasos necesarios para configurar un nuevo par de zonas con SDM:

Paso 1. Vaya a Configure > Additional Tasks > Zone Pairs.

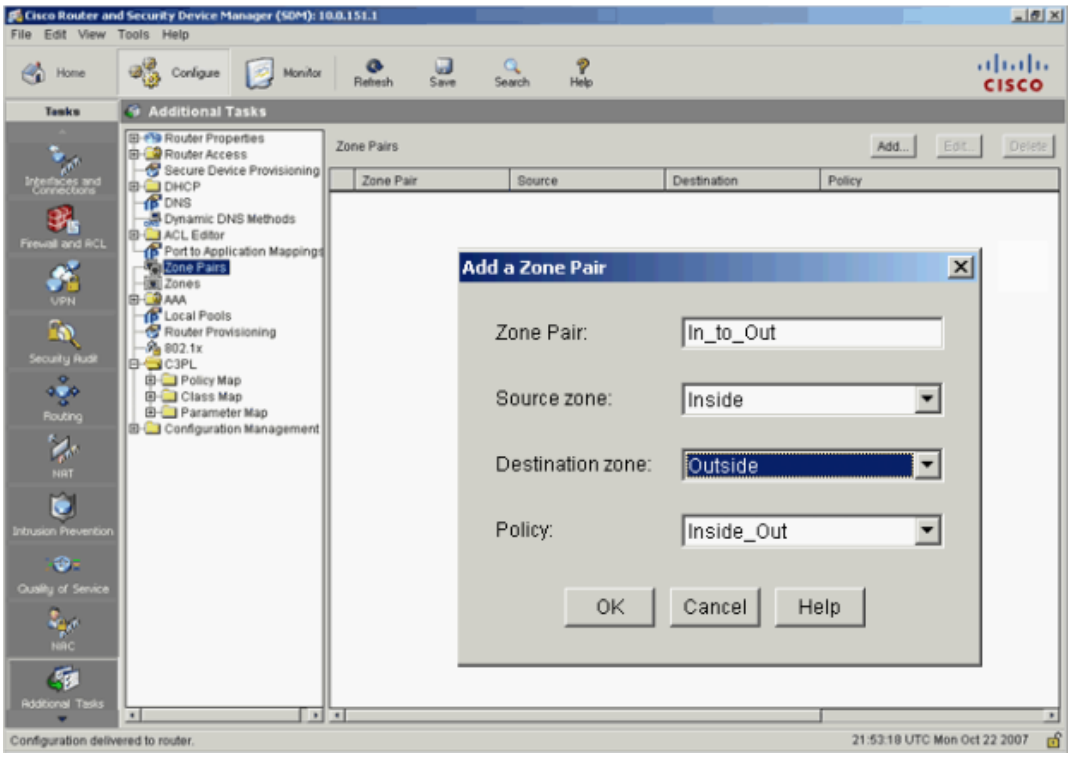
Paso 2. En el panel Zone Pairs, haga clic en Add. Aparecerá la ventana Add a Zone Pair.

Paso 3. En el campo Zone Pair, ingrese un nombre para el par de zonas. Elija una zona de origen de la que surgirá el tráfico y una zona de destino a la que éste se dirigirá, junto con la política que determinará qué tráfico puede atravesar las zonas.

Las listas de zona de origen y zona de destino contienen las zonas que están configuradas en el router y la self zone. La self zone puede ser usada en un par de zonas (como el par de zonas configurado para tráfico SNMP) para indicar el tráfico que se origina en el o se dirige al router en sí. La lista Policy contiene el nombre de cada mapa de políticas configurado en el router.

Paso 4. Haga clic en OK en la ventana Add a Zone Pair y haga clic en OK en la ventana Command Delivery Status.

Paso 5. Para editar un par de zonas, vaya al panel Zone Pairs, elija el par de zonas a editar y haga clic en Edit. Si edita un par de zonas, puede cambiar el mapa de políticas, pero no el nombre o las zonas de origen y destino.



4.4.5 Configuracion del Firewall de politica basada en zonas con el asistente SDM

El asistente de firewall básico del SDM de Cisco puede ayudarlo a implementar el firewall. El asistente lo guiará en la creación del firewall haciéndole preguntas sobre las interfaces del router, además de si la intención es configurar una red DMZ y qué reglas usar en el firewall.

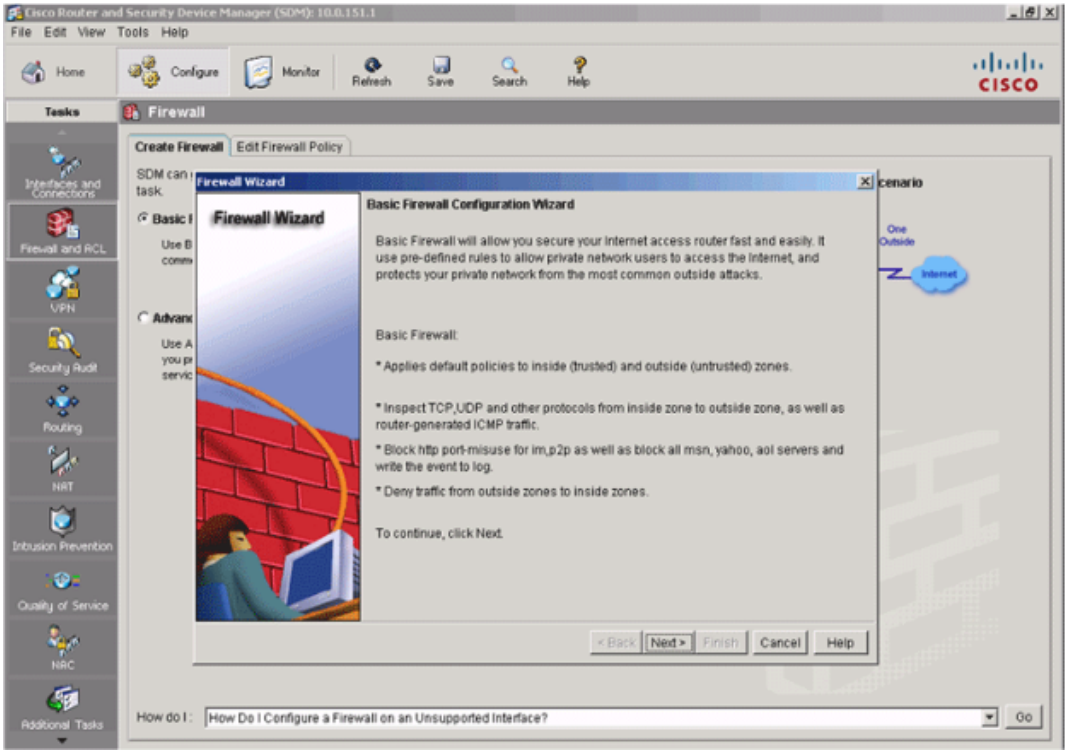
Estos son los pasos requeridos para acceder al asistente de configuración de firewall básico usando SDM:

Paso 1. En el SDM de Cisco, vaya a Configuration > Firewall and ACL.

Paso 2. En la pestaña Create Firewall, haga clic en la opción Basic Firewall y a continuación haga clic en el botón Launch the Selected Task.

Paso 3. Aparecerá la ventana Basic Firewall Configuration Wizard. Haga clic en Next para comenzar la configuración.

Si CBAC no está configurado en el router, los asistentes de firewall básico o avanzado crearán un firewall de política basada en zonas.



La primera tarea para configurar un firewall básico es definir las interfaces internas (confiables) y externas (no confiables). La interfaz externa (no confiable) generalmente es la interfaz del router que está conectada con Internet o con una WAN. La interfaz interna (confiable) generalmente es una interfaz física o lógica que se conecta con la LAN. Es posible seleccionar múltiples interfaces internas y externas.

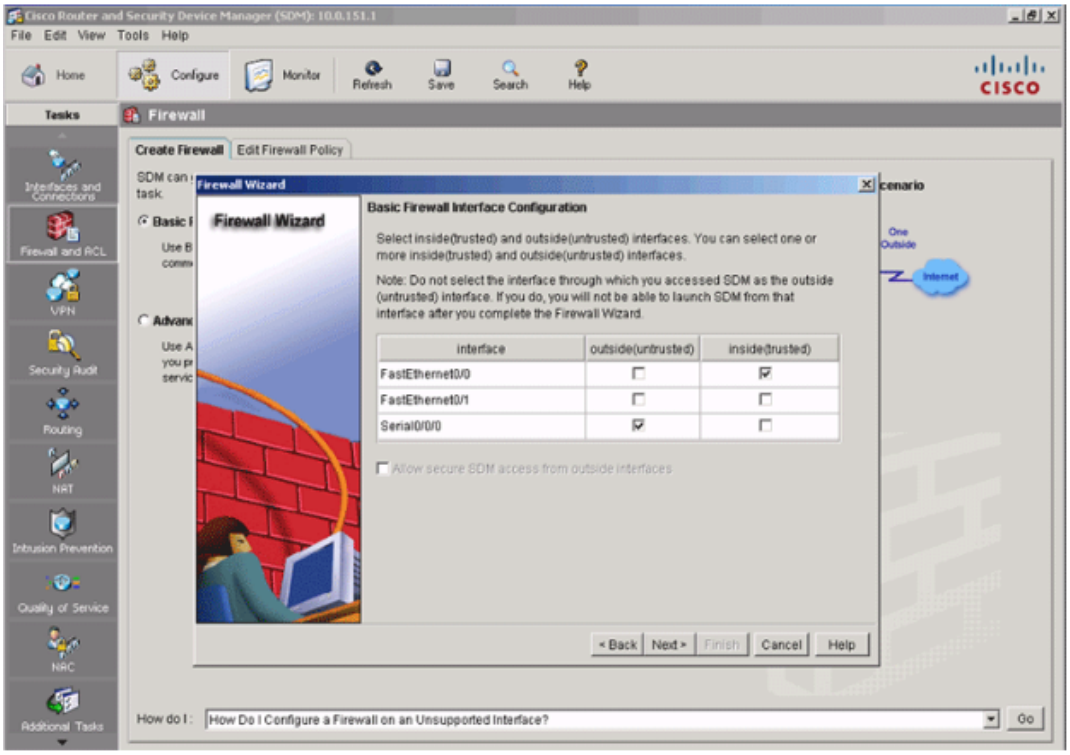
Estos son los pasos necesarios para configurar un firewall con el asistente de configuración básica del router:

Paso 1. En la ventana Basic Firewall Interface Configuration, marque las casillas outside (untrusted) e inside (trusted) para identificar cada interfaz como externa o interna respectivamente. Las interfaces externas se conectan con la WAN de la empresa o con Internet, mientras que las internas se conectan con la LAN. Puede elegirse más de una de cada una.

Paso 2. (Opcional) Marque la casilla Allow Secure Cisco SDM Access From Outside Interfaces si la intención es permitir a los usuarios fuera del firewall acceso al router mediante el SDM de Cisco. La elección de esta opción permite acceso HTTP seguro a la interfaz externa (no confiable). Como la conexión al firewall es de SDM seguro de Cisco, no es posible navegar la interfaz externa (no confiable) por medio de HTTP luego de que el asistente de firewall completa la configuración. Luego de hacer clic en Next, el asistente muestra una pantalla que permite al administrador especificar una dirección de red o dirección IP de host. El firewall se modifica para permitir acceso a la dirección especificada.

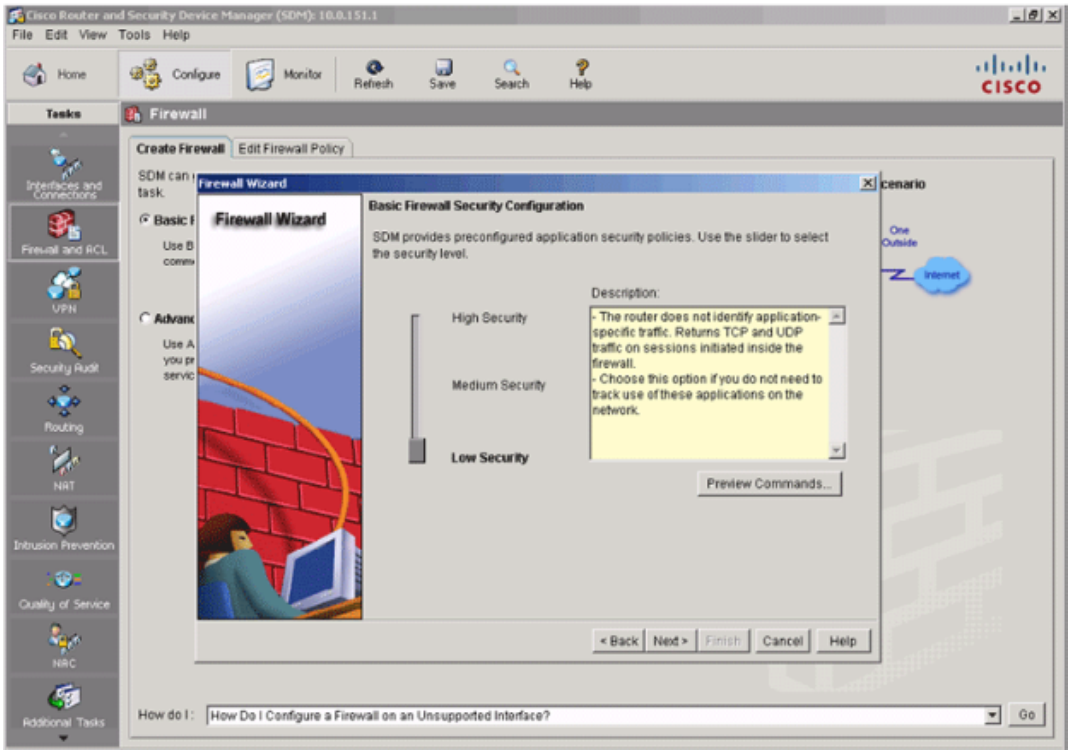
Paso 3. Haga clic en Next. Si la casilla Allow Secure SDM Access From the Outside Interfaces está marcada, aparecerá la ventana Configuring Firewall for Remote Access.

Paso 4. Especifique la red o el host de origen del que se permitirá el SDM de Cisco para administrar el router remotamente. Elija Network address, Host IP address o any de la lista desplegable Type y luego ingrese la dirección IP y máscara de subred.



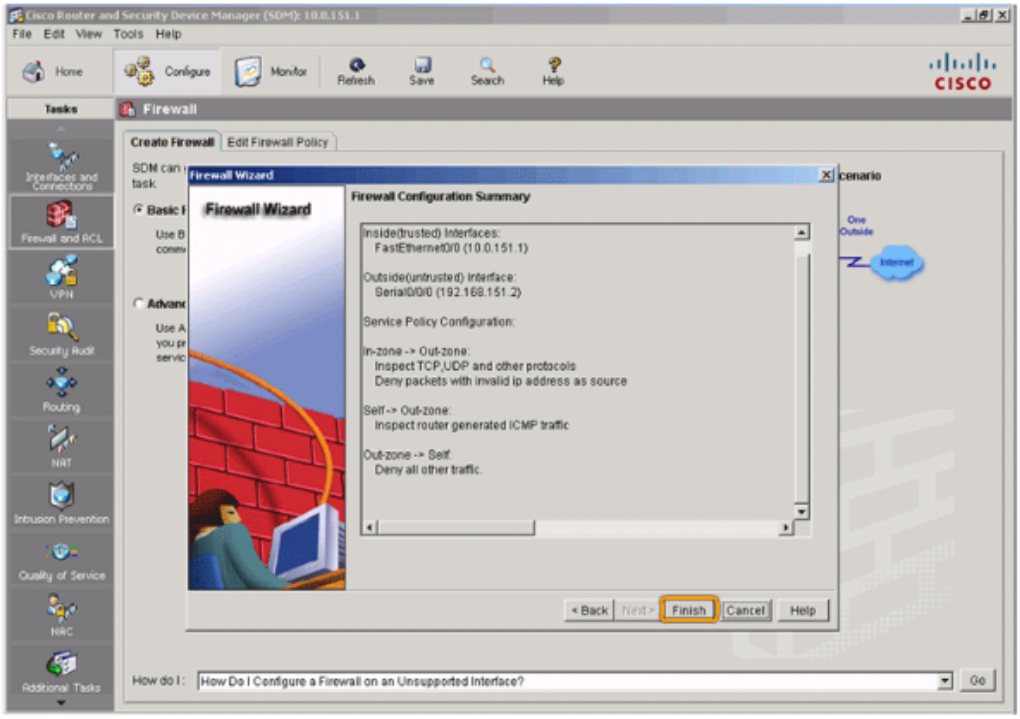
Una vez completada la configuración de interfaz, aparecerá la ventana Basic Firewall Security Configuration. El SDM de cisco proporciona políticas de seguridad preconfiguradas que pueden ser utilizadas para proteger la red. Use la barra de desplazamiento para seleccionar el nivel de seguridad deseado y para ver una descripción de la seguridad que proporciona.

En la ventana Basic Firewall Security Configuration, haga clic en el botón Preview Commands para visualizar los comandos IOS de Cisco que conforman la política seleccionada. El router debe estar configurado con la dirección IP de por lo menos un servidor DNS para que la seguridad de las aplicaciones funcione correctamente.



La ventana Firewall Configuration Summary muestra el nombre elegido para la política, SDM_HIGH, SDM_MEDIUM, o SDM_LOW y las sentencias de configuración que la componen.

Haga clic en Finish para completar la configuración. Los comandos ejecutados por el asistente de firewall básico son generalmente largos. Las configuraciones creadas por los asistentes tienden a ser bastante más exhaustivas que las creadas por una CLI o una configuración SDM manual.



Haga clic en el botón "Finish" resaltado para ver/ocultar la ventana

```
class-map type inspect match-any sdm-cls-insp-traffic
 match protocol cuseeme
 match protocol dns
 match protocol ftp
 match protocol h323
 match protocol https
 match protocol icmp
 match protocol imap
 match protocol pop3
 match protocol netshow
 match protocol shell
 match protocol realmedia
 match protocol rtsp
 match protocol smtp extended
 match protocol sql-net
 match protocol streamworks
 match protocol tftp
 match protocol vdolive
 match protocol tcp
```

Tráfico

```
 match protocol udp
class-map type inspect match-all sdm-insp-traffic
 match class-map sdm-cls-insp-traffic
class-map type inspect match-any SDM_EIGRP
 match access-group name SDM_EIGRP
class-map type inspect match-any SDM_EIGRP_TRAFFIC
 match class-map SDM_EIGRP
class-map type inspect match-all SDM_EIGRP_PT
 match class-map SDM_EIGRP_TRAFFIC
class-map type inspect match-any sdm-cls-icmp-access
 match protocol icmp
class-map type inspect match-all sdm-icmp-access
 match class-map sdm-cls-icmp-access
class-map type inspect match-all sdm-invalid-src
 match access-group 100
class-map type inspect match-all sdm-protocol-http
 match protocol http
!
policy-map type inspect sdm-permit-icmpreply
 class type inspect sdm-icmp-access
  inspect
 class class-default
  pass
policy-map type inspect sdm-inspect
 class type inspect sdm-invalid-src
  drop log
 class type inspect sdm-insp-traffic
  inspect
 class type inspect sdm-protocol-http
  inspect
 class class-default
policy-map type inspect sdm-permit
 class type inspect SDM_EIGRP_PT
  pass
 class class-default
```

Políticas

```
!
zone security out-zone
zone security in-zone
zone-pair security sdm-zp-self-out source self destination out-zone
 service-policy type inspect sdm-permit-icmpreply
zone-pair security sdm-zp-out-self source out-zone destination self
 service-policy type inspect sdm-permit
zone-pair security sdm-zp-in-out source in-zone destination out-zone
 service-policy type inspect sdm-inspect
!
interface FastEthernet0/0
 description $FW_INSIDE$
zone-member security in-zone
!
!
interface Serial0/0/0
 description $FW_OUTSIDE$
zone-member security out-zone
```

Zonas

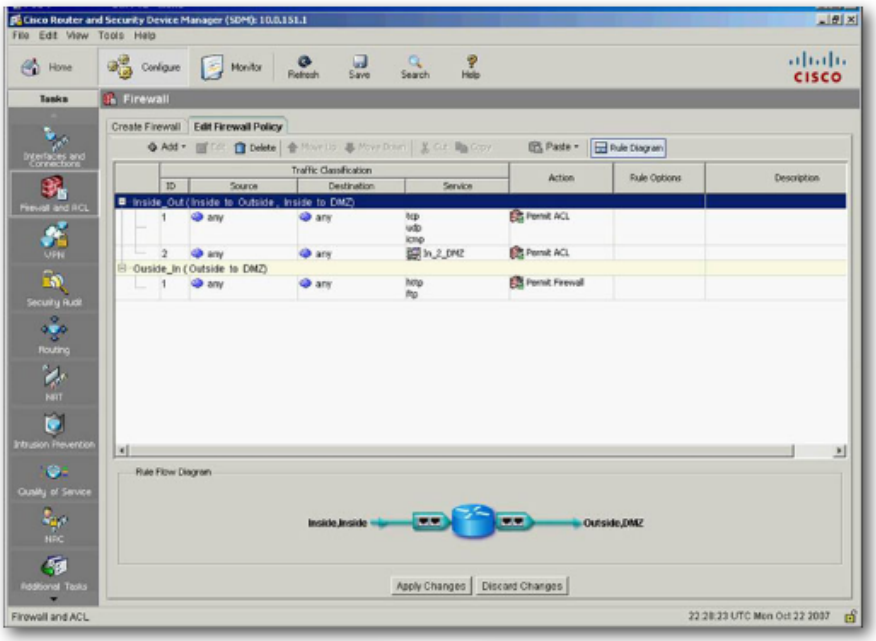
```
!
!
ip access-list extended SDM_EIGRP
 remark SDM_ACL Category=1
 permit eigrp any any
!
access-list 100 remark SDM_ACL Category=128
access-list 100 permit ip host 255.255.255.255 any
access-list 100 permit ip 127.0.0.0 0.255.255.255 any
access-list 100 permit ip 192.168.151.0 0.0.0.3 any
```

ACLs

4.4.6 Resolucion de problemas en el Firewall de politicas basada en zonas

Luego de crear el firewall de política basada en zonas, examínelo en el SDM yendo a Configure > Firewall and ACL y haciendo clic en la pestaña Edit Firewall Policy . Se mostrará una vista gráfica del firewall en el contexto de las interfaces del router. También es posible modificar el firewall en esta ventana.

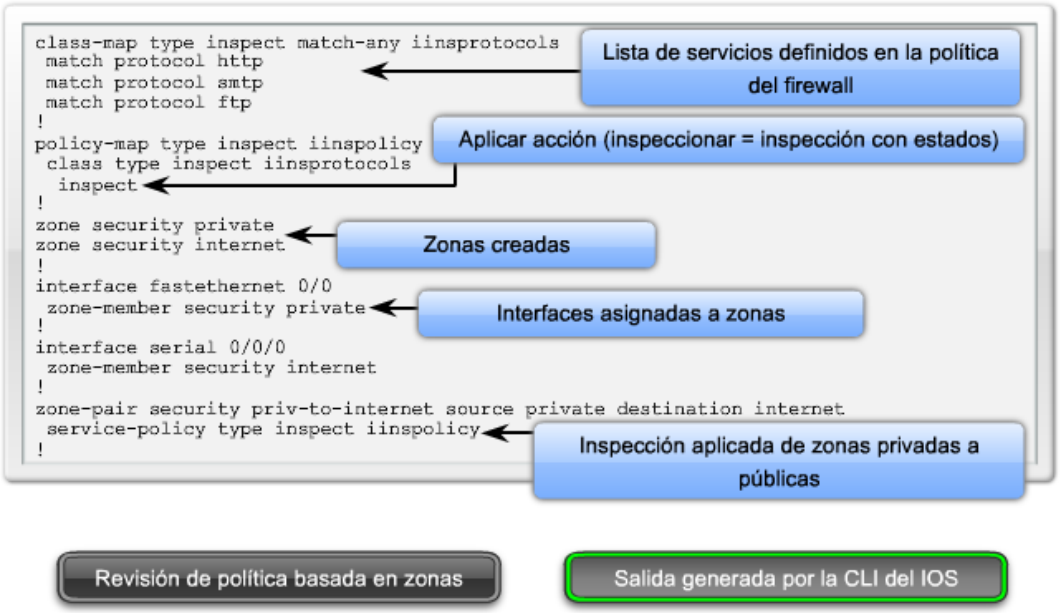
Los comandos ZPF en la CLI generados por un firewall de dos interfaces con parámetros de inspección por defecto no son tan extensos. Típicamente, los protocolos como HTTP, SMTP y FTP son inspeccionados en este tipo de situación. Un mapa de políticas aplica inspección con estados a los protocolos especificados en un mapa de clases. Se crean dos zonas, como privada e Internet, a la que se asocian la interfaz interna (zona privada) y la interfaz WAN (zona de Internet). Finalmente, se crea un par de zonas, que puede llamarse priv-to-internet, que tendrá a la zona privada como zona de origen y a la zona de Internet como zona destino y al cual se aplicará el mapa de políticas.



Revisión de política basada en zonas

Salida generada por la CLI del IOS

Haga clic en los botones para ver el contenido asociado.

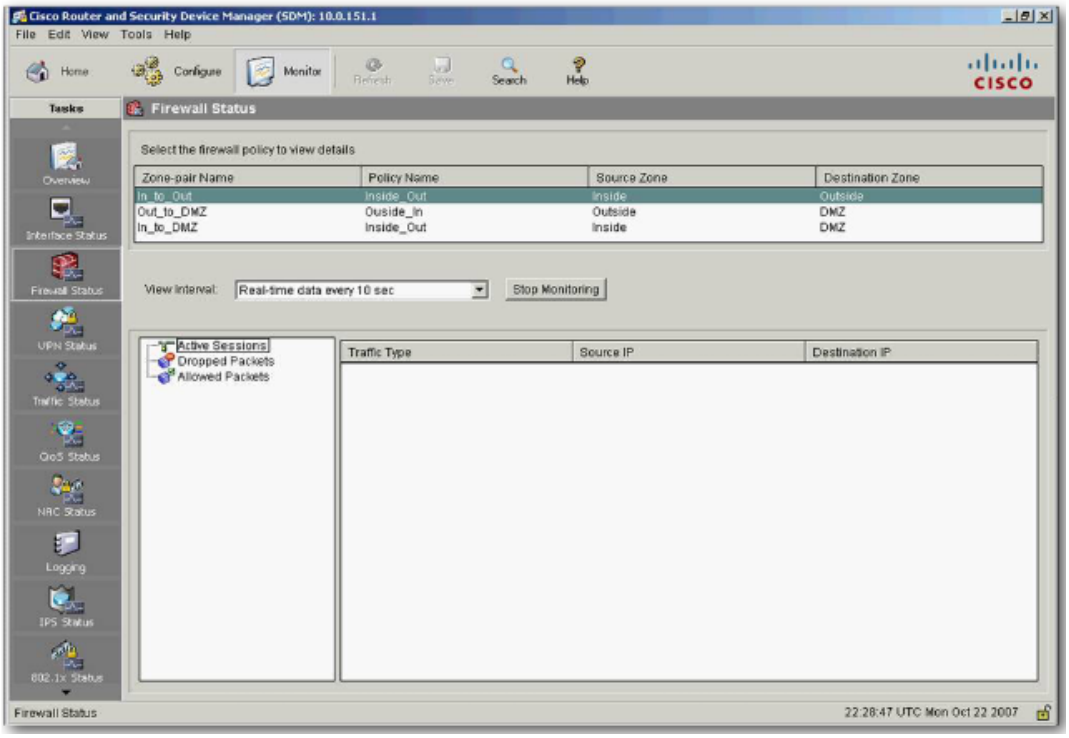


Haga clic en los botones para ver el contenido asociado.

Si el router ejecuta una imagen IOS de Cisco que soporta ZPF, puede usarse el SDM para mostrar el estado de la actividad del firewall para cada par de zonas configurado en el router. Para mostrar la información de estado del firewall, vaya a Monitor > Firewall Status.

El área de lista de políticas del firewall muestra el nombre de la política, la zona de origen y la zona de destino de cada par de zonas. Elija una de las siguientes opciones para especificar cómo deben recolectarse los datos:

Real-time data every 10 sec - Los datos se reportan cada 10 segundos. Cada marca en el eje horizontal del gráfico Dropped Packets and Allowed Packets representa 10 segundos.
60 minutes of data polled every 1 minute - Los datos se reportan cada 1 minuto. Cada marca en el eje horizontal del gráfico Dropped Packets and Allowed Packets representa 1 minuto.
12 hours of data polled every 12 minutes - Los datos se reportan cada 12 minutos. Cada marca en el eje horizontal del gráfico Dropped Packets and Allowed Packets representa 12 minutos.



Use el comando show policy-map type inspect zone-pair session para examinar las conexiones activas en la tabla de estados ZPF. La salida del siguiente comando muestra conexiones activas de 10.0.2.12 al puerto 80 de 172.26.26.51.

Router# show policy-map type inspect zone-pair session

Zone-pair: CNS-PAIR

Service-policy inspect : HTTP-Policy

Class-map: HTTP-Class (match-all)

Match: access-group 110

Match: protocol http

Inspect

Established Sessions

Session 643BCF88 (10.0.2.12:3364)=>(172.26.26.51:80) http SIS_OPEN

Created 00:00:10, Last heard 00:00:00

Bytes sent (initiator:responder) [1268:64324]

Session 643BB9C8 (10.0.2.12:3361)=>(172.26.26.51:80) http SIS_OPEN

Created 00:00:16, Last heard 00:00:06

Bytes sent (initiator:responder) [2734:38447]

Session 643BD240 (10.0.2.12:3362)=>(172.26.26.51:80) http SIS_OPEN

Created 00:00:14, Last heard 00:00:07

Bytes sent (initiator:responder) [2219:39813]

Session 643BBF38 (10.0.2.12:3363)=>(172.26.26.51:80) http SIS_OPEN

Created 00:00:14, Last heard 00:00:06

Bytes sent (initiator:responder) [2106:19895]

Class-map: class-default (match-any)

Match: any

Drop (default action)

58 packets, 2104 bytes

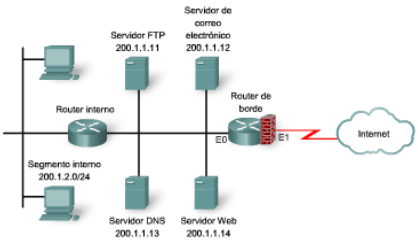
El firewall IOS de política basada en zonas de Cisco proporciona diseño y configuración de firewall de última generación. Lo que empezó con TCP established en 1995 ha evolucionado para convertirse en una rica gama de tecnologías para asegurar las redes.

Pero los firewalls solos no pueden proporcionar una solución de seguridad completa. Se requieren otras tecnologías para construir una infraestructura segura. La prevención de intrusiones en las redes es otra tecnología de seguridad que se necesita para soportar el firewall de la red. La prevención de intrusiones ayuda enormemente a cerrar brechas de seguridad en las redes modernas.

```
Router# show policy-map type inspect zone-pair session
```

- Muestra estadísticas de sesión del firewall de política basada en zonas

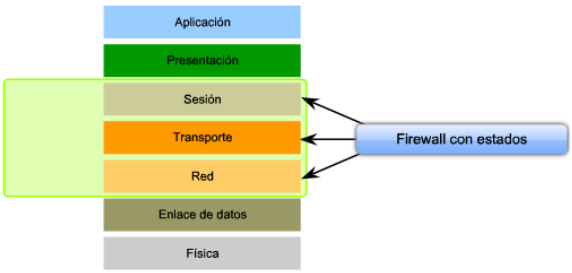
4.5.1 Resumen del capitulo




```
Perimeter# show access-list 100
Extended IP access list 100
    permit tcp any host 200.1.1.14 eq www  (189 matches)
    permit udp any host 200.1.1.13 eq domain (32 matches)
    permit tcp any host 200.1.1.12 eq smtp
    permit tcp any eq smtp host 200.1.1.12 established
    permit tcp any host 200.1.1.11 eq ftp
    permit tcp any host 200.1.1.11 eq ftp-data
    permit tcp any eq www 200.1.2.0 0.0.0.255 established
    permit udp any eq domain 200.1.2.0 0.0.0.255
    deny ip any any (1237 matches)
```

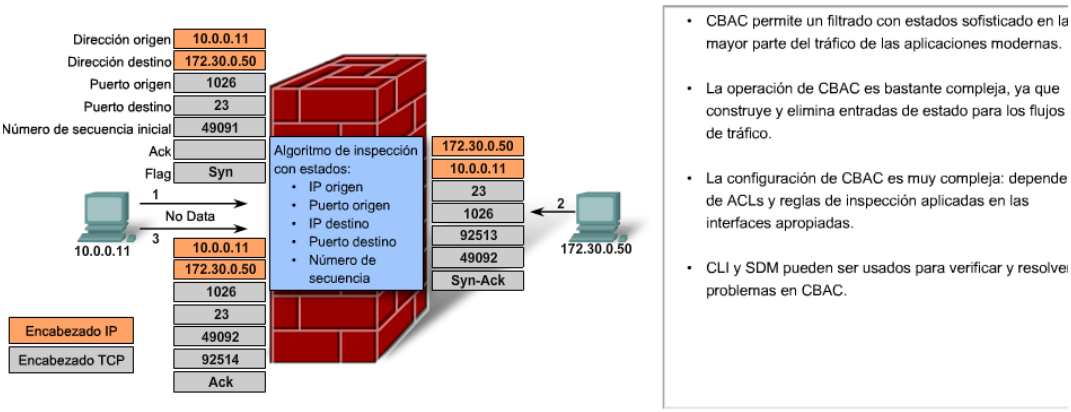
- Las ACLs IP estándar y extendidas son la herramienta fundamental para un filtrado básico de tráfico de red.
- Cómo se crean y se aplican las ACLs IP estándar y extendidas depende del tipo de tráfico y dónde están el origen y el destino del tráfico.
- Las ACLs están asociadas con el flujo de tráfico en la red. La topología de la red determina cómo se crean y se aplican las ACLs.
- Las ACLs pueden ser creadas y aplicadas con SDM.
- La opción TCP established y las ACLs reflexivas extienden la función de las ACLs para tomar en cuenta la naturaleza de doble sentido del tráfico de red.
- Las ACLs dinámicas proporcionan una solución especializada, abriendo agujeros temporales en el firewall.
- Las ACLs basadas en tiempo permiten a los administradores seleccionar la hora del día y el día de la semana para aplicar la ACL.
- Tanto CLI como SDM proporcionan la capacidad de validar la correcta implementación de ACLs.
- Si son creadas y aplicadas apropiadamente, las ACLs mitigan un amplio rango de ataques de red.

- Ls firewalls proporcionan seguridad de perímetro, ya que definen las partes interna y externa de la red.
- Existen muchos tipos diferentes de firewalls, aunque los firewalls con estados proporcionan la mayor seguridad.
- Hoy en día, el diseño de las redes debe tomar en consideración la selección del tipo de firewall y su correcta ubicación.





Haga clic en los botones para información resumida.



5 Implementacion de prevencion de intrusiones

5.0 Introducion al capitulo

5.0.1 Introducion al capitulo

Los desafíos de seguridad que los administradores de red de hoy en día enfrentan no pueden ser administrados exitosamente por una sola aplicación de cualquier tipo. Aunque la implementación de las funciones de hardening (fortificación) de dispositivos, control de acceso AAA y firewall son parte de una red segura, por sí solas no pueden defender a la red contra los rápidos virus y gusanos de Internet. La red debe ser capaz de reconocer y mitigar instantáneamente las amenazas de virus y gusanos.

Tampoco es posible contener a los intrusos en algunos puntos de la red. Se requiere prevención de intrusiones en toda la red para detectar y detener ataques en cada punto de entrada o salida.

Se requiere también un cambio de paradigma de arquitectura de red para defenderse contra los ataques de rápido movimiento y evolución. Esto debe incluir sistemas de detección y prevención eficientes en cuanto a su costo, como sistemas de detección de

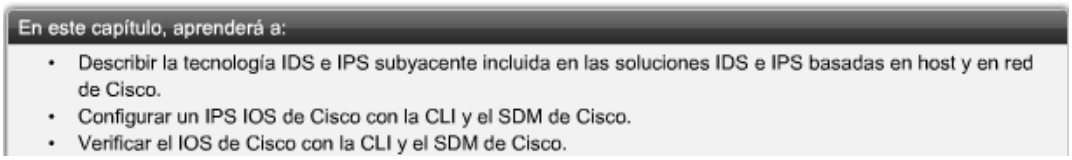
intrusiones (IDS) o el más escalable sistema de prevención de intrusiones (IPS). La arquitectura de red integra estas soluciones en los puntos de entrada y salida de la red.

Al implementar IDS y/o IPS, es importante familiarizarse con los tipos de sistemas disponibles, enfoques basados en host y basados en red, la ubicación de estos sistemas, el rol de las categorías de firmas y las posibles acciones que puede efectuar el IOS del router Cisco cuando detecta un ataque.

En una práctica de laboratorio exhaustiva, Configuración de un sistema de prevención de intrusiones (IPS) con la CLI y el SDM, los alumnos aprenderán a configurar IPS utilizando la CLI, modificar las firmas IPS, verificar la funcionalidad de IPS y registrar los mensajes IPS en un servidor syslog. Luego, los estudiantes configurarán IPS usando SDM, modificarán firmas, usarán una herramienta de escaneo para simular un ataque y usarán SDM Monitor para verificar la funcionalidad de IPS. El laboratorio está disponible en el manual de laboratorio en Academy Connection en cisco.netacad.net.

La actividad de Packet Tracer, Configuración de sistemas de prevención de intrusiones (IPS) IOS con CLI, proporciona a los alumnos práctica adicional en la implementación de las tecnologías presentadas en este capítulo. Luego, los alumnos configurarán IPS usando CLI, modificarán las firmas de IPS y verificarán su funcionalidad.

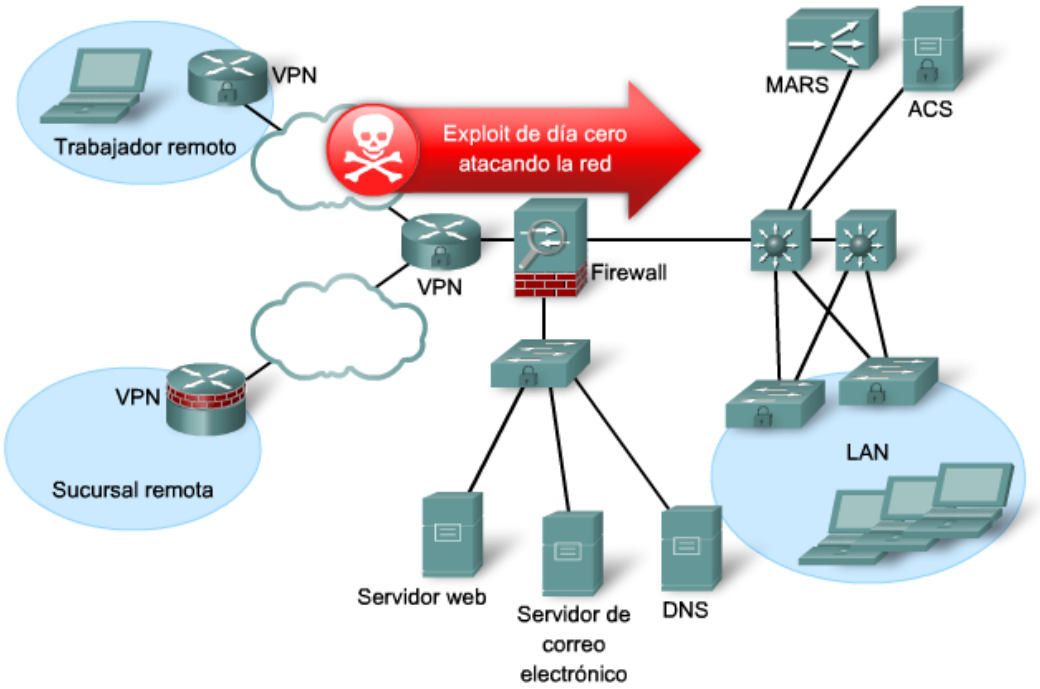
Las actividades de Packet Tracer para CCNA Security están disponibles en Academy Connection en cisco.netacad.net.



5.1.1 Caracteristicas de IDS e IPS

Los gusanos y virus de Internet pueden diseminarse por el mundo en cuestión de minutos. La red debe reconocer y mitigar instantáneamente amenazas de gusanos o virus. Los firewalls no pueden hacerlo todo y no protegen a la red contra malware y ataques de día cero.

El ataque de día cero, también conocido como amenaza de día cero, es un ataque de computadoras que intenta explotar las vulnerabilidades del software que son desconocidas o no han sido publicadas por el proveedor de software. El término hora cero describe el momento en que el exploit es descubierto. Durante el tiempo que le tome al proveedor desarrollar y disponibilizar un parche, la red será vulnerable a estos exploits. Para defenderse contra ataques de rápido movimiento, es necesario que los profesionales de la seguridad en redes expandan su enfoque sobre la arquitectura de las redes. Ya no es posible contener el ingreso de intrusos colocando seguridad en algunos pocos puntos de la red.



Un enfoque sobre la prevención del ingreso de gusanos y virus a la red es que el administrador monitoree continuamente la red y analice los archivos del registro generados por los dispositivos de red. Esta solución no es muy escalable, ya que analizar manualmente los archivos del registro es una tarea que toma mucho tiempo y constituye una perspectiva limitada de los ataques que se lanzan contra la red. Para cuando se analizan los registros, el ataque ya empezó.

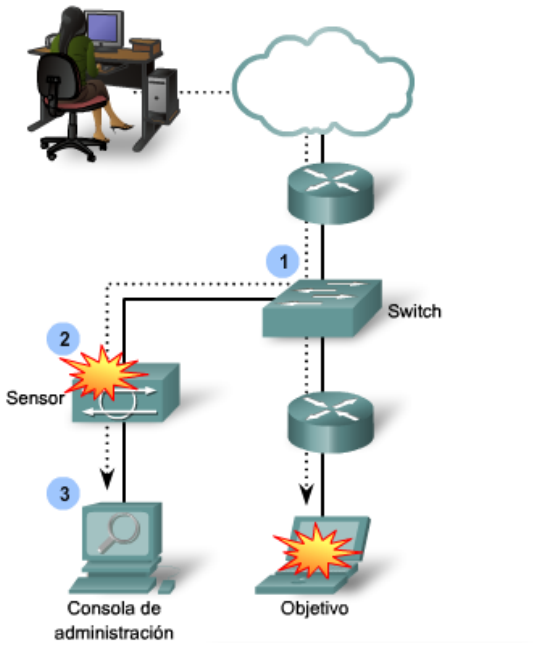
Los sistemas de detección de intrusiones (Intrusion Detection Systems) o IDSs fueron implementados para monitorear de manera pasiva el tráfico de la red. Un IDS copia el tráfico de red y lo analiza en lugar de reenviar los paquetes reales. Compara el tráfico capturado con firmas maliciosas conocidas de manera offline del mismo modo que el software que busca virus. Esta implementación offline de IDS se conoce como modo promiscuo.

La ventaja de operar con una copia del tráfico es que el IDS no tiene efectos negativos sobre el flujo real de paquetes del tráfico reenviado. La desventaja de operar con una copia del tráfico es que el IDS no puede evitar que el tráfico malicioso de ataques de un solo paquete alcance el sistema objetivo antes de aplicar una respuesta para detener el ataque. El IDS generalmente requiere asistencia de otros dispositivos de red, como routers y firewalls, para responder a un ataque.

Es mejor implementar una solución que detecte e inmediatamente trate el problema en la red según corresponda.

Sistemas de detección de intrusos

1. Se lanza un ataque en una red que tiene un sensor en modo IDS promiscuo; por lo tanto, se envían copias de todos los paquetes al sensor IDS para análisis. Sin embargo, la máquina a la que el ataque está dirigido experimentará el ataque malicioso.
2. El sensor IDS busca coincidencias entre el tráfico malicioso y las firmas y envía al switch un comando para denegarle el acceso.
3. El IDS envía una alarma a una consola de administración con el propósito de registrar el incidente y otros.



El sistema de prevención de intrusiones (Intrusion Prevention System) o IPS se apoya en la ya existente tecnología IDS. A diferencia del IDS, un dispositivo IPS se implementa en modo en línea. Esto significa que todo el tráfico de entrada y de salida debe fluir a través de él para ser procesado. El IPS no permite que los paquetes ingresen al lado confiable de la red sin ser analizados primero. Puede detectar y tratar inmediatamente un problema según corresponda.

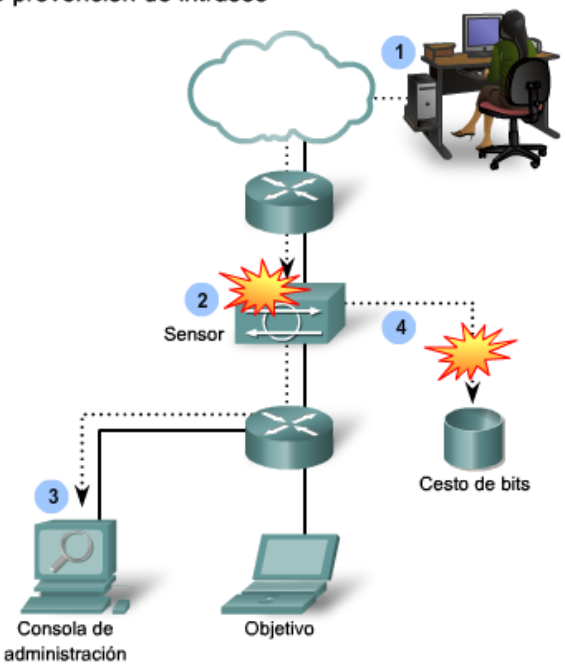
El IPS monitorea el tráfico de capas 3 y 4 y analiza los contenidos y la carga de los paquetes en búsqueda de ataque sofisticados insertos en ellos, que pueden incluir datos maliciosos pertenecientes a las capas 2 a 7. Las plataformas IPS de Cisco usan una mezcla de tecnologías de detección, incluyendo detecciones de intrusiones basadas en firma, basadas en perfil y de análisis de protocolo. Este análisis, más profundo, permite al IPS identificar, detener y bloquear ataques que pasarían a través de un dispositivo firewall tradicional. Cuando un paquete pasa a través de una interfaz en un IPS, no es enviado a la interfaz de salida o confiable hasta haber sido analizado.

La ventaja de operar en modo en línea es que el IPS puede evitar que los ataques de un solo paquete alcancen el sistema objetivo. La desventaja es que un IPS mal configurado o una solución IPS inapropiada pueden tener efectos negativos en el flujo de paquetes del tráfico reenviado.

La mayor diferencia entre IDS e IPS es que un IPS responde inmediatamente y no permite el paso de tráfico malicioso, mientras que el IDS puede permitir que el tráfico malicioso pase antes de responder.

Sistema de prevención de intrusos

1. Se lanza un ataque en una red que tiene un sensor en modo IPS (modo en línea).
2. El sensor IPS analiza los paquetes a mendida que entran a la interfaz del sensor IPS. El sensor IPS busca coincidencias entre el tráfico malicioso y las firmas y el ataque se detiene inmediatamente.
3. El sensor IPS puede enviar una alarma a la consola de administración con el propósito de registrar el incidente u otros.
4. El tráfico que viola una política puede ser descartado por el sensor IPS.



Las tecnologías IDS e IPS comparten en efecto varias características: ambas se despliegan como sensores. Un sensor IDS o IPS puede ser cualquiera de los siguientes dispositivos:

Un router configurado con software IPS IOS de Cisco
Un dispositivo diseñado específicamente para proporcionar servicios IDS o IPS dedicados
Un módulo de red instalado en un dispositivo de seguridad adaptable, switch o router

Las tecnologías IDS e IPS usan firmas para detectar patrones de mal uso en el tráfico de la red. La firma es un grupo de reglas que usa el IDS o IPS para detectar actividad típica de intrusiones. Las firmas pueden ser usadas para detectar brechas de seguridad severas, ataques de red comunes y recolección de información. Las tecnologías IDS e IPS pueden detectar tanto patrones de firma atómicos (de un solo paquete) como compuestos (multipaquete).

¿Puede un sensor IPS reemplazar completamente a un sensor IDS?



Características comunes de IDS e IPS:

1. Ambas tecnologías se despliegan como sensores.
2. Ambas tecnologías usan firmas para detectar patrones de mal uso en el tráfico de la red.
3. Ambas pueden detectar patrones atómicos (de un solo paquete) o patrones compuestos (multipaquete).

Ventajas y desventajas de IDS

Una ventaja principal de una plataforma IDS es que se despliega en modo promiscuo. Como el sensor IDS no está en línea, no tiene impacto en el desempeño de la red. No introduce latencia, jitter u otros problemas de flujo de tráfico. Además, si un sensor falla, no afecta el desempeño de la red: solo afecta la capacidad del IDS de analizar los datos.

Pero existen muchas desventajas de desplegar una plataforma IDS en modo promiscuo. Las acciones de respuesta del sensor IDS no pueden detener el paquete disparador y no garantizan la detención de una conexión. También son menos útiles en la detención de virus de correo electrónico y ataques automatizados como gusanos.

Los usuarios que despliegan acciones de respuesta del sensor IDS deben tener una política de seguridad bien definida, combinada con un buen entendimiento operativo de sus despliegues IDS. Los usuarios deben dedicar tiempo al ajuste de los sensores IDS para lograr los niveles esperados de detección de intrusiones.

Finalmente, como los sensores IDS no operan en línea, la implementación IDS es más vulnerable a las técnicas de evasión usadas por varias amenazas.

Ventajas y desventajas de IPS

El despliegue de una plataforma IPS en modo en línea también tiene ventajas y desventajas.

Una ventaja sobre IDS es que puede configurarse un sensor IPS para realizar un descarte de paquetes que puede detener el paquete disparador, los paquetes de una conexión o los paquetes originados en una dirección IP determinada. Además, al estar en línea, el sensor IPS puede usar técnicas de normalización del flujo para reducir o eliminar muchas de las capacidades de evasión existentes.

Una desventaja del IPS es que los errores, la falla y la sobrecarga del IPS con demasiado tráfico pueden tener efectos negativos en el desempeño de la red. Esto ocurre porque el IPS debe ser desplegado en línea y el tráfico debe poder pasar a través de él. Un sensor IPS puede afectar el rendimiento de la red introduciendo latencia y jitter. Por lo tanto, el sensor IPS debe ser de tamaño e implementación apropiados para que las aplicaciones sensibles al tiempo, como VoIP, no sufran efectos negativos.

Consideraciones del despliegue

El uso de una de estas tecnologías no significa que el administrador no pueda usar la otra. De hecho, las tecnologías IDS e IPS pueden complementarse entre sí. Por ejemplo, un IDS puede ser implementado para validar la operación de IPS, ya que el IDS puede ser configurado para realizar una inspección de paquetes más profunda en forma offline. Esto permite al IPS concentrarse en menos patrones de tráfico, pero más críticos, en línea.

Decidir cuál implementación usar está basado en los objetivos de seguridad de la organización establecidos en la política de seguridad de la red.

Comparación de soluciones IDS e IPS

	Ventajas	Desventajas
IDS (Modo promiscuo)	• No tiene impacto sobre la red (latencia, jitter) • No tiene impacto sobre la red si el sensor falla • No tiene impacto sobre la red si el sensor se sobrecarga	• La acción de respuestas no puede detener los paquetes disparadores • Se requieren ajustes correctos para las acciones de respuesta • Se debe tener una política de seguridad bien definida • Más vulnerable a técnicas de evasión
IPS (Modo en línea)	• Detiene paquetes disparadores • Puede usar técnicas de normalización de flujo	• Los problemas de los sensores pueden afectar el tráfico de la red • La sobrecarga del sensor tiene impacto sobre la red • Se debe tener una política de seguridad bien definida • Algún impacto en la red (latencia, jitter)

5.1.2 Implementaciones de IPS basadas en HOST

La protección contra virus y amenazas requiere una solución de extremo a extremo. Por esta razón, las tecnologías IDS e IPS son típicamente desplegadas con dos implementaciones: las basadas en red y las basadas en host.

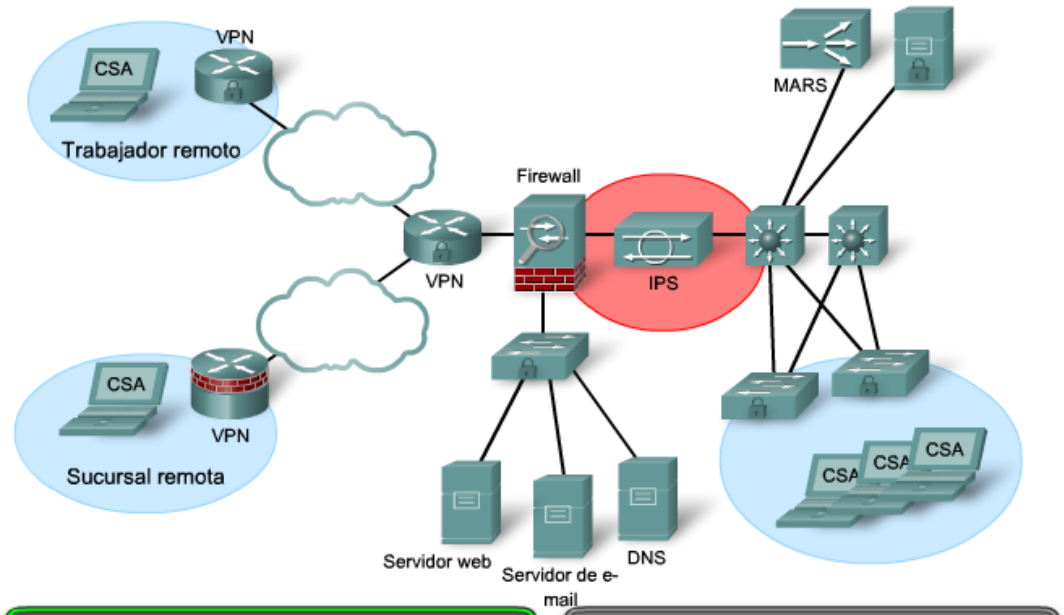
Implemetanciones IPS basadas en red

Las implementaciones IPS basadas en red analizan la actividad de toda la red en búsqueda de actividad maliciosa. Los dispositivos de red, como los routers ISR, los dispositivos firewall ASA, los módulos de red Catalyst 6500 o los dispositivos IPS

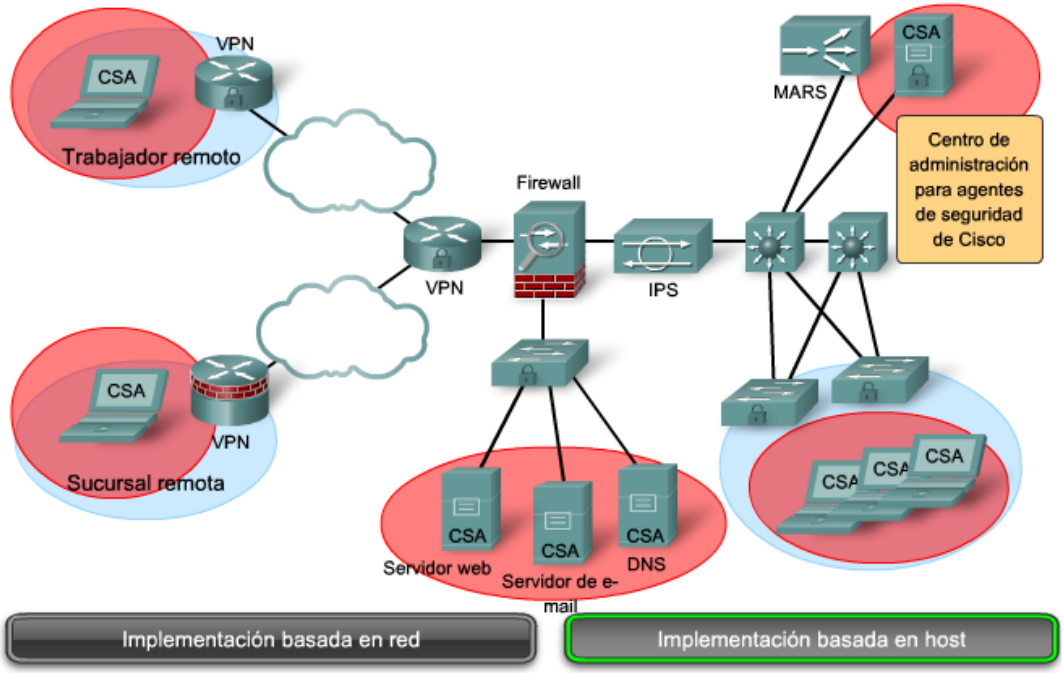
dedicados son configurados para monitorear firmas conocidas. También pueden detectar patrones de tráfico anormal.

Implementaciones IPS basadas en host

Las implementaciones basadas en hosts son instaladas en computadoras individuales usando software de sistemas de prevención de intrusiones de host (host intrusion prevention system - HIPS) como el Agente de Seguridad de Cisco (CSA). Los HIPS auditan los archivos de registro del host, los sistemas de archivos del host y los recursos. Una forma simple de HIPS habilita los registros del sistema y el análisis del registro en el host, lo cual constituye un enfoque extremadamente laborioso. El software CSA ayuda a administrar HIPS y asegura los hosts proactivamente. Una ventaja significativa del HIPS es que puede monitorear los procesos del sistema operativo y proteger los recursos críticos del sistema, incluyendo los archivos que pueden existir solo en ese host específico. Combina el análisis de comportamiento y filtros de firma con las mejores características de software antivirus, firewalls de red y firewalls de aplicación en un solo paquete.



Haga clic en los botones para ver el contenido asociado.



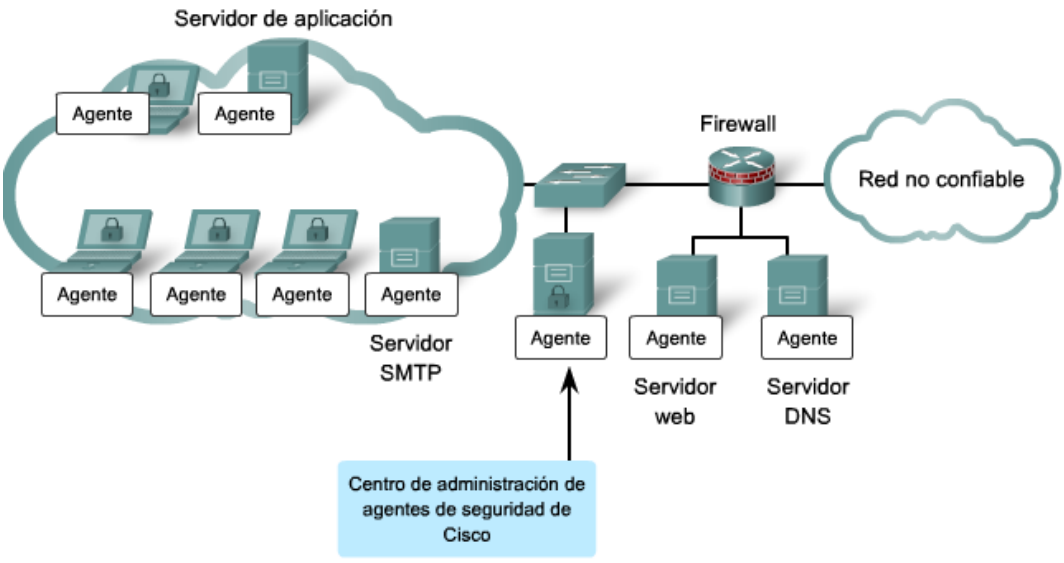
El CSA proporciona seguridad de host a las empresas ya que despliega agentes que las defienden contra los ataques que proliferan a través de las redes. Estos agentes operan usando un grupo de políticas que son asignadas selectivamente a cada nodo del sistema de la red por el administrador.

El CSA contiene dos componentes:

Centro de administración - Instalado en un servidor central y administrado por un administrador de red.
Agente de seguridad - Instalado y ejecutado en un sistema host. Muestra el ícono de bandera de agente (la pequeña banderita roja) en la bandeja del sistema.

El CSA examina continuamente procesos, registros de eventos de seguridad, archivos del sistema críticos y registros del sistema en búsqueda de entradas maliciosas. Puede ser instalado en servidores de acceso público, servidores de correo electrónico de la empresa, servidores de aplicación y escritorios de usuario. Notifica los eventos a un servidor de consola de administración central ubicado dentro del firewall de la empresa.

Cuando se instala en un host, el CSA controla la operación del sistema, protegiendo a los sistemas con políticas configuradas y desplegadas por los administradores de red a los agentes. Estas políticas permiten o deniegan acciones específicas del sistema. Los agentes deben revisar si la acción se permite o deniega antes de acceder y actuar sobre cualquier recurso de la red. Este proceso ocurre transparentemente y no afecta el rendimiento general del sistema. Salvo que ocurra una operación errante o inesperada en el sistema, el agente no interfiere con las operaciones diarias.



El CSA proporciona seguridad proactiva, ya que controla el acceso a los recursos del sistema. El CSA puede detener ataques, sin actualizaciones, por medio de una identificación del comportamiento malicioso y su respuesta en tiempo real. Este enfoque evita la carrera para actualizar las defensas para seguir el paso a los últimos exploits para proteger los hosts, incluso en el día cero, de los nuevos ataques. Por ejemplo, los gusanos Nimda y SQL Slammer provocaron millones de dólares de daños a las empresas en el primer día de su aparición antes de que aparecieran las actualizaciones. Las redes protegidas con CSA, sin embargo, detuvieron estos ataques identificando su comportamiento como malicioso.

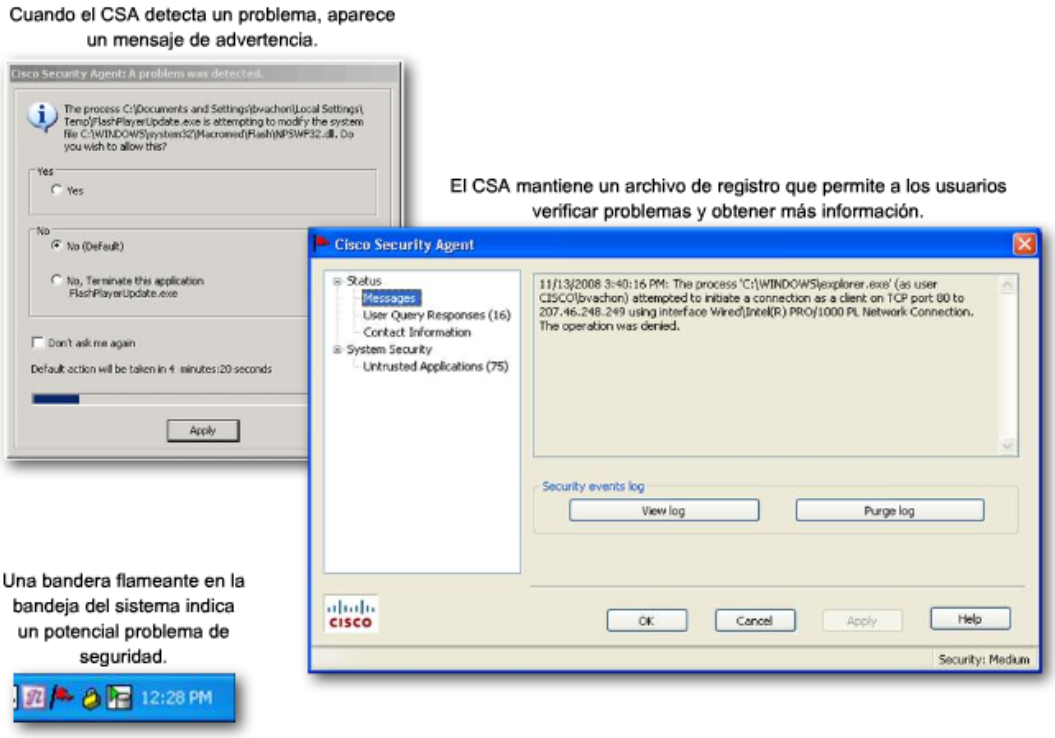
El CSA muestra al usuario una acción cuando se detecta un problema. El usuario debe permitir o denegar la acción, o terminar el proceso cuando intente acceder a los recursos del sistema del usuario. Típicamente, aparecerá una ventana emergente que pide al usuario seleccionar uno de los tres botones de opción excluyente (radio buttons) cuando se dispara una regla en cuestión:

Yes - Permite a la aplicación acceso a los recursos en cuestión.
No - Deniega a la aplicación acceso a los recursos en cuestión.
No, terminar esta aplicación - Deniega a la aplicación acceso a los recursos en cuestión e intenta terminar el proceso de la aplicación. El nombre de la aplicación en cuestión será desplegado con la opción de terminar.

Por ejemplo, si el CSA reconoce que una actualización de software está siendo instalada, solicita una acción. Si el usuario está instalando una actualización de software legítima, debe permitir que la operación continúe. Sin embargo, si el usuario no conoce la existencia de la instalación y la solicitud aparece sin razón válida alguna, probablemente deba denegar la acción.

Dependiendo de la versión del CSA de Cisco instalado, aparecerá el ícono de una pequeña bandera naranja o roja en la bandeja del sistema Windows. Cuando CSA deniega una acción del sistema, se incluye un mensaje que informa al usuario sobre este

evento en el registro. Para llamar la atención del usuario, la bandera naranja aparece y desaparece y la roja flamea. El usuario también puede ver el archivo de registro del CSA que contiene todos los eventos de seguridad que han tomado lugar en el sistema.



Usar un HIPS presenta muchas ventajas. Con el HIPS, puede determinarse fácilmente el éxito o fracaso de un ataque. El IPS de red envía una alarma disparada por la presencia de actividad intrusiva pero no siempre puede establecer el éxito o fracaso de un ataque. El HIPS tampoco tiene que preocuparse por los ataques de fragmentación o de Time to Live (TTL) variable, ya que la pila del host se ocupa de estos problemas. El HIPS tiene acceso al tráfico luego de que ha sido descifrado.

El HIPS tiene, sin embargo, dos desventajas mayores. No proporciona un panorama completo de la red. Como el HIPS examina sólo la información a nivel de host local, éste tiene dificultades en construir un panorama preciso de la red o coordinar los eventos que toman lugar en toda la red. Adicionalmente, el HIPS debe correr en todos los sistemas de la red. Esto requiere verificar que todos los sistemas operativos en uso en toda la red lo soporten.

Las implementaciones IPS basadas en host y basadas en red se complementan entre sí al asegurar los múltiples puntos de entrada y salida de la red.

Ventajas y desventajas de los HIPS

Ventajas	Desventajas
• Puede determinarse fácilmente el éxito o fracaso de un ataque. • Los HIPS no tienen que preocuparse por ataques de fragmentación o Time to Live (TTL) variable. • Los HIPS tienen acceso al tráfico de forma no cifrada.	• Los HIPS no proporcionan una visualización completa de la red. • Los HIPS deben ser soportados en múltiples sistemas operativos.

5.1.3 Implementaciones IPS basadas en red

Un IPS de red puede ser implementado usando un dispositivo IPS dedicado, como el IPS 4200 series o puede ser agregado a un router ISR, un dispositivo firewall ASA o un switch Catalyst 6500.

Los sensores detectan actividad maliciosa y no autorizada en tiempo real y pueden realizar acciones cuando sea necesario. Los sensores se despliegan en puntos designados de la red que permiten a los administradores de seguridad monitorear la actividad de la red a medida que toma lugar, sin importar la ubicación del blanco del ataque.

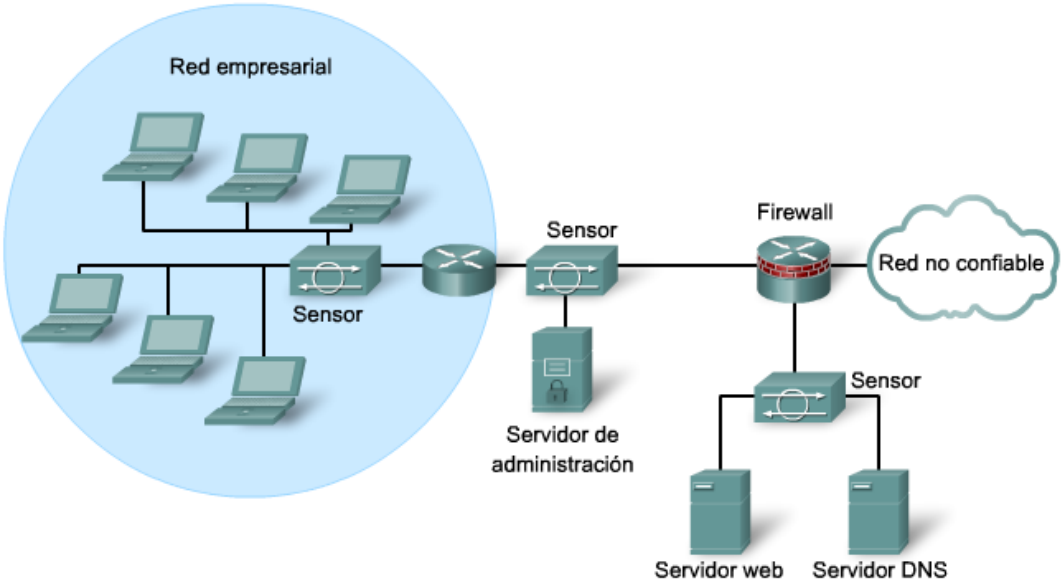
Los sensores pueden ser implementados de muchas maneras. Pueden ser agregados a un router ISR con un IPS Advanced Integration Module (AIM) o un Network Module Enhanced (IPS NME), o agregados a un dispositivo de firewall ASA con un Inspection and Prevention Security Services Module (ASA AIP-SSM). También pueden ser agregados a un switch Catalyst 6500 por medio de un Intrusion Detection System Services Module (IDSM-2).

Los sensores IPS de red generalmente se ajustan para el análisis de prevención de intrusiones. En el sistema operativo subyacente de la plataforma sobre la que se monta el IPS se quitan los servicios de red innecesarios y se aseguran los servicios esenciales. Esto se conoce como fortificación (hardening). El hardware incluye tres componentes.

Placa de red (Network interface card) o NIC - El IPS de red debe poder conectarse a cualquier red (Ethernet, Fast Ethernet, Gigabit Ethernet).
Procesador - La prevención de intrusiones requiere ciclos de CPU para realizar análisis de detección de intrusiones y búsqueda de coincidencias en los patrones.
Memoria - El análisis de detección de intrusiones hace un uso intensivo de la memoria, que afecta directamente la habilidad de un IPS de red de detectar un ataque eficientemente y de manera precisa.

Los IPS de red otorgan a los administradores de seguridad una perspectiva de seguridad de tiempo real sobre sus redes sin importar el crecimiento. Pueden agregarse hosts adicionales a las redes protegidas sin requerir más sensores. Solo se requerirán sensores adicionales cuando su tasa de capacidad de tráfico se exceda, cuando su rendimiento no satisfaga las necesidades actuales o cuando una revisión en la política de seguridad o diseño de la red solicite sensores adicionales para ayudar a aplicar fronteras de

seguridad. Cuando se agregan nuevas redes, los sensores adicionales son fáciles de desplegar.



Los ISRs 1841, 2800 y 3800 de Cisco pueden ser configurados (por medio de la CLI o del SDM) para soportar funciones IPS usando IPS IOS de Cisco, lo cual es parte del grupo de funciones del firewall IOS de Cisco. Esto no requiere la instalación de un módulo IPS pero sí requiere la descarga de archivos de firmas y una memoria adecuada para cargarlas. Sin embargo, este despliegue debe ser limitado a una pequeña organización con patrones de tráfico limitados.

Para volúmenes de tráfico mayores, los sensores IPS de Cisco pueden ser implementados en dispositivos autónomos o como módulos agregados a los dispositivos de red.

Además de los IPS IOS de Cisco, Cisco ofrece una variedad de soluciones de IPS basadas en dispositivos y módulos:

El Advanced Integration Module (AIM) IPS de Cisco y Network Module Enhanced (IPS NME) - Integra el IPS en un ISR de Cisco para pequeñas y medianas empresas (PyMEs) y ambientes de oficinas sucursales. Proporciona funciones IPS avanzadas y de nivel de empresa y satiface las necesidades de seguridad de las sucursales, que están en constante crecimiento. También puede escalar en rendimiento para satisfacer los requisitos de ancho de banda WAN de las oficinas sucursales mientras se mantiene el bajo costo de la solución para empresas de todos los tamaños. Los administradores deben revisar el software y hardware del IOS de Cisco para asegurar la compatibilidad. El IPS IOS de Cisco y el AIM IPS / NME IPS no pueden ser usados en conjunto: el IPS IOS de Cisco debe estar deshabilitado cuando se instala el IPS AIM de Cisco.

Cisco Adaptive Security Appliance Advanced Inspection and Prevention Security Services Module (ASA AIP-SSM) - Utiliza tecnología de inspección y prevención avanzada para proporcionar servicios de seguridad de alto rendimiento como servicios de prevención de intrusiones y anti-X avanzados. Los productos ASA AIP-SSM de

Cisco incluyen un módulo ASA AIP-SSM-10 con 1 GB de memoria, un módulo ASA AIP-SSM-20 con 2 GB de memoria y un módulo ASA AIP-SSM-40 con 4 GB de memoria.
Sensores IPS 4200 Series de Cisco - Combinan servicios de prevención de intrusiones en línea con tecnologías innovadoras que mejoran la exactitud en la detección, clasificación y detención de amenazas, incluyendo gusanos, spyware, adware y virus de red. Como resultado, pueden detenerse más amenazas sin el riesgo de descartar tráfico de red legítimo. El software de sensor IPS de Cisco versión 5.1 incluye habilidades de detección aumentadas y funciones de escalabilidad, adaptabilidad y rendimiento mejoradas.

Cisco Catalyst 6500 Series Intrusion Detection System Services Module (IDSM-2) - Como parte de la solución IPS de Cisco, trabaja en conjunto con otros componentes para proteger eficientemente la estructura de datos.

Con el incremento en la complejidad de las amenazas de seguridad, lograr soluciones de seguridad de red eficientes es crítico para mantener un alto nivel de protección. La protección vigilante asegura la continuidad de los negocios y minimiza los efectos de intrusiones costosas.



Cisco IPS AIM and Network Module Enhanced (IPS NME)

- Integra IPS a los routers ISR Cisco 1841 (solo IPS AIM), 2800 y 3800
- IPS AIM ocupa una ranura AIM interna en el router y tiene sus propias CPU y DRAM
- Monitorea hasta 45 Mb/s de tráfico
- Proporciona protección de intrusiones con todas las funciones
- Es capaz de monitorear el tráfico de todas las interfaces del router
- Puede inspeccionar tráfico GRE e IPsec que ha sido descifrado en el router
- Entrega una exhaustiva protección de intrusiones en las oficinas sucursales, aislando las amenazas de la red de la empresa
- Ejecuta la misma imagen de software que Cisco IPS Sensor Appliances



Cisco ASA AIP-SSM

- Módulo de alto rendimiento diseñado para proporcionar servicios de seguridad adicionales al Cisco ASA 5500 Series Adaptive Security Appliance
- Diseño sin disco para mejorar la confiabilidad
- Interfaz Ethernet 10/100/1000 externa para administración y descargas de software
- Capacidad de prevención de intrusiones
- Ejecuta la misma imagen de software que Cisco IPS Sensor appliances



Cisco IPS 4200 Series Sensors

- Dispositivo concentrado en la protección de los dispositivos, servicios y aplicaciones de la red
- Proporciona una detección de ataques sofisticada



Cisco Catalyst 6500 Series IDSM-2

- Módulo de protección contra intrusiones integrado al switch que proporciona un servicio de seguridad de gran valor en el dispositivo del núcleo de la red
- Soporta un número ilimitado de VLANs
- Capacidad de prevención de intrusiones
- Ejecuta la misma imagen de software que Cisco IPS Sensor Appliances

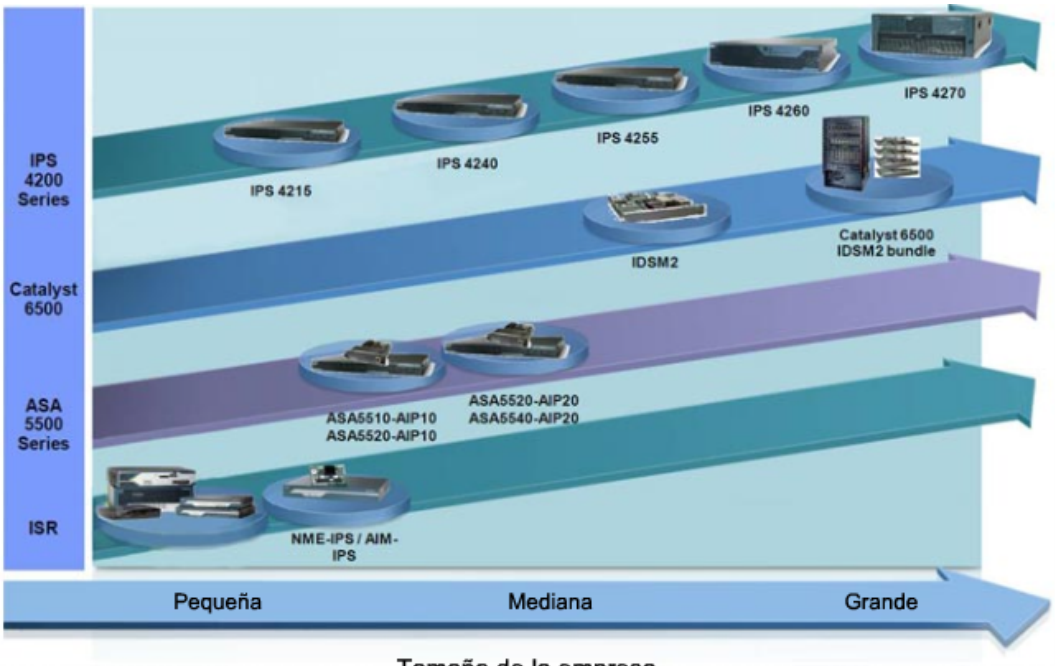
La elección de un sensor varía dependiendo de los requisitos de la organización. Varios factores tienen impacto sobre la elección de sensores IPS y su despliegue.

Cantidad de tráfico en la red
Topología de la red
Presupuesto de seguridad
Personal de seguridad disponible para el manejo del IPS

Las pequeñas implementaciones como oficinas sucursales pueden requerir solo un router ISR habilitado para IPS IOS de Cisco. A medida que los patrones de tráfico aumentan, el ISR puede ser configurado para manejar las funciones IPS fuera de la carga usando un IPS NME o AIM.

Instalaciones mayores pueden ser desplegadas usando su dispositivo ASA 5500 existente con un ASA AIP.

Las empresas y los proveedores de servicios pueden requerir dispositivos IPS dedicados o un Catalyst 6500 con un módulo IDSM-2 de red.



Los IPS de red tienen varias ventajas y desventajas. Una ventaja es que el sistema de monitoreo basado en red puede ver fácilmente los ataques que están tomando lugar en toda la red. Esto proporciona un indicador claro de la cantidad de ataques que la red está recibiendo. Además, como el sistema de monitoreo solo examina tráfico de la red, no tiene necesidad de soportar todos los sistemas operativos utilizados en la red.

También hay desventajas en el uso de IPS de red. Cifrar los datos de la red puede cegar al IPS de red, impidiendo la detección de los ataques. Otro problema es que el IPS tiene problemas para reconstruir tráfico fragmentado para fines de monitoreo. Finalmente, a medida que las redes se agrandan en cuanto al ancho de banda, se vuelve más difícil ubicar los IPS de red en un solo punto y capturar todo el tráfico exitosamente. La eliminación de este problema requiere el uso de más sensores en toda la red, lo cual incrementa los costos.

Recuerde que un HIPS examina información a nivel de host local o sistema operativo, mientras que el IPS de red examina los paquetes que viajan a través de la red en búsqueda de signos de actividad intrusiva. No son tecnologías que compitan entre sí,

sino que se complementan. Ambas deben ser desplegadas para garantizar una red segura de extremo a extremo.

Comparación de HIPS e IPS de red

	Ventajas	Desventajas
HIPS	• Específico de cada host • Protege a los hosts luego del descifrado • Proporciona protección de cifrado de nivel de aplicación	• Depende del sistema operativo • No son vistos eventos de red de nivel menor • El host es visible para los atacantes
IPS de red	• Eficiente en el costo • No es visible en la red • Independiente del sistema operativo • Son vistos eventos de red de menor nivel	• No puede examinar tráfico cifrado • No sabe si un ataque fue exitoso

5.2.1 Caracteristicas de las firmas IPS

Para detener el tráfico malicioso, la red debe ser capaz de identificarlo primero. Afortunadamente, el tráfico malicioso tiene características, o "firmas", distintivas. Una firma es un grupo de reglas que los IDS e IPS usan para detectar actividad intrusiva típica, como ataques de DoS. Estas firmas identifican puntualmente gusanos, virus, anomalías en los protocolos o tráfico malicioso específico. Las firmas IPS son conceptualmente similares al archivo virus.dat usado por escáners de virus.

Cuando los sensores escanean los paquetes de la red, usan las firmas para detectar ataques conocidos y responder con acciones predefinidas. Un paquete malicioso tiene un tipo de actividad y una firma específicas. Un sensor IDS o IPS examina el flujo de datos usando varias firmas diferentes. Cuando un sensor encuentra una coincidencia entre una firma y un flujo de datos, realiza una acción, como asentar el evento en el registro o enviar una alarma al software de administración del IDS o IPS.

Las firmas tienen tres atributos distintivos:

Tipo
Disparador (alarma)
Acción



Tipos de firma

Los tipos de firma generalmente se categorizan como atómicos o compuestos.

Atómicos

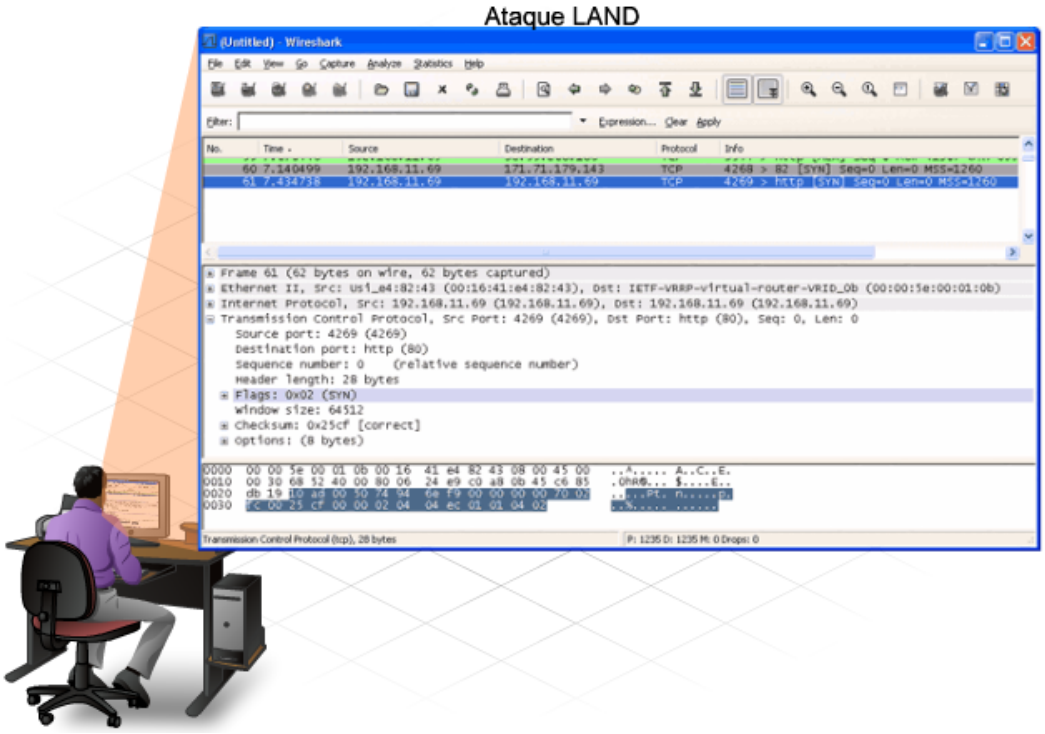
La firma atómica es la forma más simple. Consiste en un solo paquete, actividad o evento examinado para determinar si coincide con una forma configurada. Si lo hace, se dispara una alarma y se realiza una acción de firma. Como estas firmas están asociadas a un solo evento, no requieren que un sistema de intrusiones mantenga información de estado. El estado se refiere a las situaciones en las que se requieren múltiples paquetes de información que no se reciben necesariamente al mismo tiempo. Por ejemplo, si se necesita mantener información de estado, será necesario que el IDS o IPS monitoree el saludo de tres vías de las conexiones TCP establecidas. Con las firmas atómicas, toda la inspección puede ser lograda en una operación atómica que no requiere conocimiento de las actividades pasadas o futuras.

La detección de firmas atómicas consume un mínimo de recursos (como la memoria) en el dispositivo IPS o IDS. Estas firmas son fáciles de identificar y entender gracias a que se las compara con un evento o paquete específico. El análisis de tráfico de estas firmas atómicas generalmente puede ser llevado a cabo muy rápida y eficientemente. Por ejemplo, un ataque LAND es una firma atómica, ya que envía un paquete SYN TCP (de inicio de conexión) falso con la dirección IP del host víctima y un puerto abierto como origen y destino. La razón por la que el ataque LAND funciona es porque hace que la máquina se responda a sí misma permanentemente. Se requiere un paquete para identificar este tipo de ataque. Los IDS son particularmente vulnerables a los ataques atómicos, porque hasta que encuentran el ataque, los paquetes únicos maliciosos se permiten dentro de la red. Los IPS, sin embargo, evitan la entrada de estos paquetes a la red.

Compuestos

Las firmas compuestas también se conocen como firmas con estados (stateful signatures). Este tipo de firma identifica una secuencia de operaciones distribuidas en múltiples hosts durante un período de tiempo arbitrario. A diferencia de las firmas atómicas, las firmas compuestas, al ser firmas con estados, generalmente requieren varios datos para asociar una firma de ataque, por lo que el dispositivo IPS debe mantener información de estados. La cantidad de tiempo que las firmas deben mantener la información de estados se conoce como horizonte de eventos.

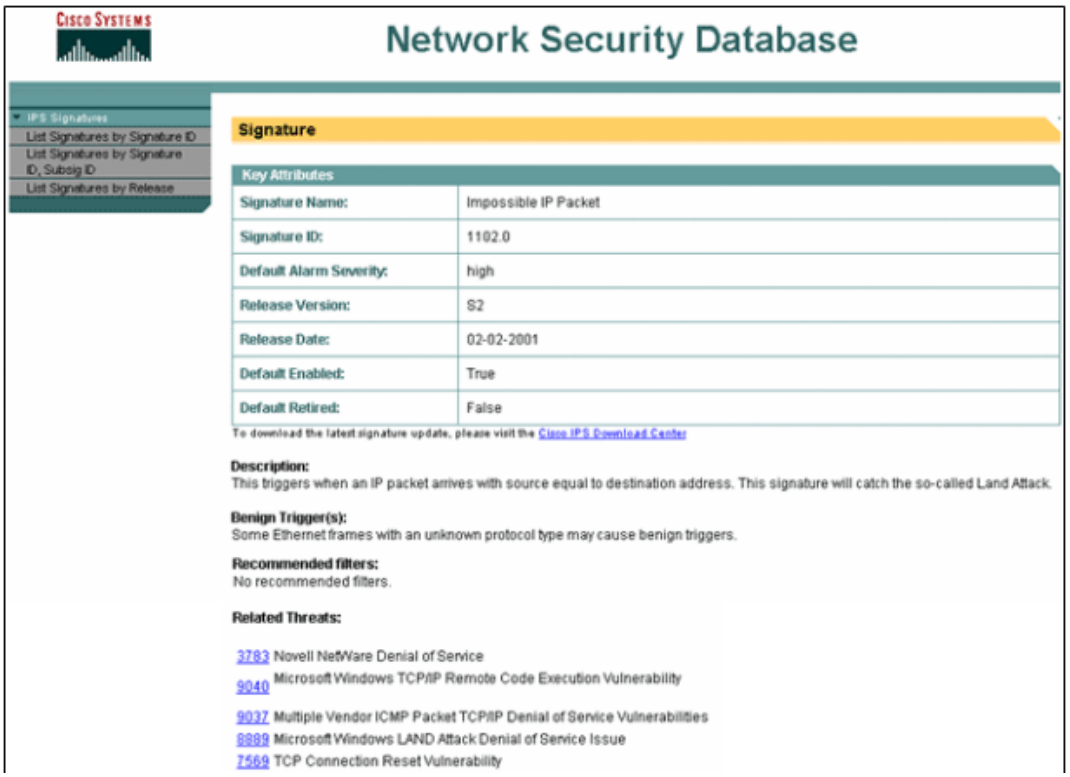
La longitud de un horizonte de eventos varía de una firma a la otra. El IPS no puede mantener la información de estados por un período indeterminado sin eventualmente quedarse sin recursos. Por lo tanto, un IPS usa un horizonte de eventos configurado para determinar cuánto tiempo debe buscar una firma de ataque específica cuando se detecta un componente inicial de firma. Configurar la longitud del horizonte de eventos es un balance entre el consumo de los recursos del sistema y la capacidad de detectar un ataque que toma lugar durante un período extenso de tiempo.



Las amenazas de seguridad en la red ocurren cada vez más seguido y se diseminan más rápido. A medida que se identifican nuevas amenazas, deben crearse nuevas firmas y subirlas a un IPS. Para facilitar este proceso, todas las firmas están contenidas dentro de un archivo de firmas y se suben al IPS regularmente.

El archivo de firma contiene un paquete de firmas de red que actúan como actualización a la base de datos de firmas residente en el producto Cisco con funciones IPS o IDS. Esta base de datos de firmas es usada por la solución IPS o IDS para comparar el tráfico de red y los patrones de datos dentro de la biblioteca del archivo de firmas. El IPS o IDS usa esta comparación para detectar tráfico de red con comportamiento sospechoso.

Por ejemplo, el ataque LAND es identificado en la firma Impossible IP Packet (firma 1102.0). Un archivo de firma contiene esa firma y muchas más. Las redes que despliegan los archivos de firmas más recientes están mejor protegidas contra los intrusos de red.



Para hacer el escaneo de firmas más eficiente, el software IOS de Cisco se apoya en los micro-motores de firmas (signature micro-engines - SME), que categorizan las firmas comunes en grupos. El software IOS de Cisco puede entonces escanear en búsqueda de múltiples firmas basándose en las características del grupo, en lugar de una por vez.

Cuando el IDS o IPS se habilita, se carga o construye un SME en el router. Cuando se construye un SME, el router puede necesitar compilar la expresión regular de la firma. Una expresión regular es una forma sistemática de especificar una búsqueda de un patrón en una serie de bytes.

El SME luego busca actividad maliciosa en un protocolo específico. Cada motor define un grupo de parámetros legales con rangos o grupos de valores permitidos para los protocolos y los campos examinados por el motor. Los paquetes atómicos y compuestos son escaneados por los micro-motores que reconocen los protocolos contenidos dentro de los paquetes. Las firmas pueden ser definidas usando los parámetros ofrecidos por el SME.

Cada SME extrae valores del paquete y pasa porciones de éste al motor de expresión regular. Este, a su vez, puede buscar múltiples patrones al mismo tiempo.

Los SMEs disponibles varían según la plataforma, la versión del IOS de Cisco y la versión del archivo de firma. El IOS de Cisco versión 12.4(6)T define cinco micro-motores:

Atomic - (Atómico) Consta de firmas que examinan paquetes simples, como ICMP y UDP.
Service - (Servicio) Consta de firmas que examinan los servicios que son atacados.

String - (Cadena de texto) Consta de firmas que usan patrones basados en expresiones regulares para detectar intrusos.
Multi-string - (Multi-cadena) Soporta búsquedas flexibles de coincidencias en patrones y firmas Trend Labs.
Other - (Otros) Motor interno que trata firmas misceláneas.

Los SMEs son actualizados constantemente. Por ejemplo, antes del versión 12.4(11)T, el formato de firma del IPS de Cisco usaba la versión 4.x. A partir del IOS 12.4(11)T, Cisco ha introducido la versión 5.x, un formato de firma IPS mejorado. La nueva versión soporta parámetros de firma cifrados y otras funciones como clasificación de riesgo de la firma, que clasifica la firma en términos de riesgo de seguridad.

Existen varios factores para considerar al determinar los requisitos del router para mantener las firmas. Primero, compilar una expresión regular requiere más memoria que el almacenamiento final de la expresión regular. Determine los requisitos de memoria final de la firma terminada antes de cargar y unir las firmas. Estime cuántas firmas pueden soportar las plataformas de router. El número de firmas y motores que pueden ser adecuadamente soportadas depende exclusivamente de la memoria disponible. Por esta razón, configure los routers habilitados con IPS IOS de Cisco con el máximo de memoria posible.

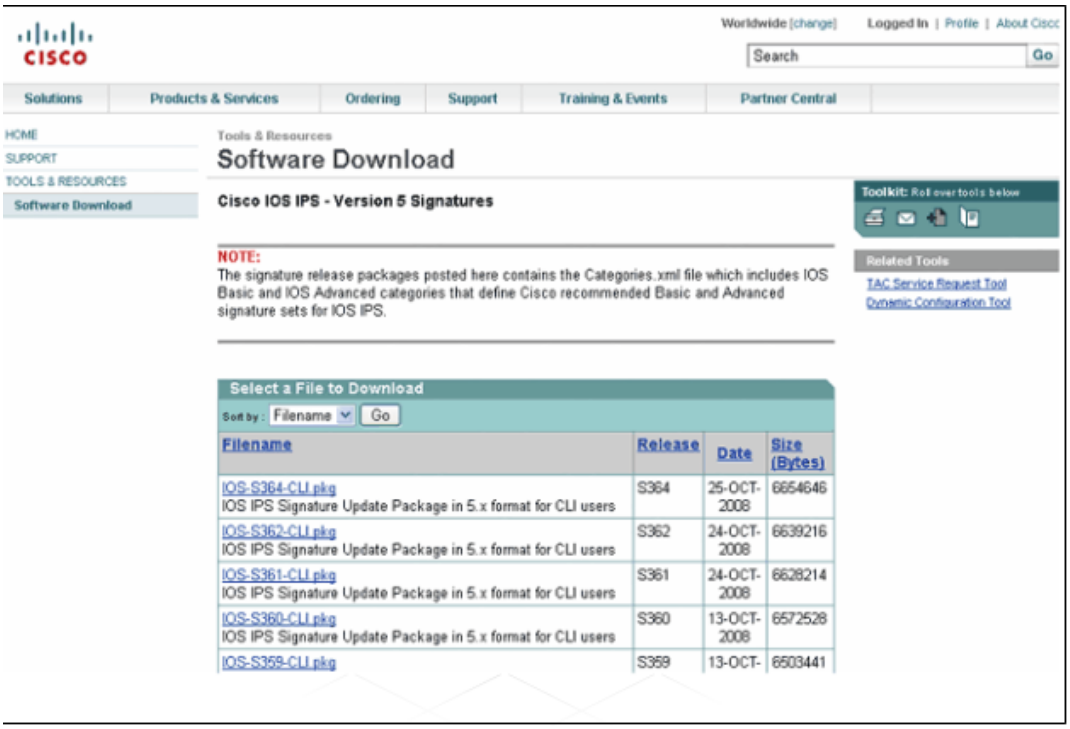
Versión 4.x SME anterior al 12.4(11)T	Versión 5.x SME 12.4(11)T y posterior	Descripción
ATOMIC.IP	ATOMIC.IP	Provee alarmas IP simples de capa 3
ATOMIC.ICMP	ATOMIC.IP	Provee alarmas Internet Control Message Protocol (ICMP) simples basadas en: tipo, código, secuencia e ID
ATOMIC.IPOPTIONS	ATOMIC.IP	Provee alarmas simples basadas en el descifrado de opciones de capa 3
ATOMIC.UDP	ATOMIC.IP	Provee alarmas de paquetes User Datagram Protocol (UDP) simples basadas en: puerto, sentido y longitud de los datos
ATOMIC.TCP	ATOMIC.IP	Provee alarmas de paquetes TCP simples basadas en: puerto, destino y flags
SERVICE.DNS	SERVICE.DNS	Analiza el servicio Domain Name System (DNS)
SERVICE.RPC	SERVICE.RPC	Analiza el servicio remote-procedure call (RPC)
SERVICE.SMTP	STATE	Inspecciona Simple Mail Transfer Protocol (SMTP)
SERVICE.HTTP	SERVICE.HTTP	Provee un motor de cadenas de texto basado en la decodificación del protocolo HTTP que incluye desofuscación de URL antievasiva
SERVICE.FTP	SERVICE.FTP	Provee alarmas especiales de decodificación de servicio FTP
STRING.TCP	STRING.TCP	Ofrece servicios de motor de inspección de patrones TCP basados en expresiones regulares
STRING.UDP	STRING.UDP	Como STRING.TCP, pero basado en UDP
STRING.ICMP	STRING.ICMP	Como STRING.TCP, pero basado en ICMP
MULTI-STRING	MULTI-STRING	Soporta búsquedas flexibles de coincidencias en patrones y firmas Trend Labs
OTHER	NORMALIZER	Provee motor interno para tratar firmas misceláneas

Cisco investiga y crea firmas para nuevas amenazas y comportamiento malicioso a medida que son descubiertos y los publica regularmente. Generalmente, los archivos de firmas IPS de menor prioridad se publican cada dos semanas. Si la amenazas es severa, Cisco publica archivos de firmas unas horas después de la identificación.

Para proteger la red, el archivo de firma debe ser actualizado regularmente. Cada actualización incluye nuevas firmas y todas las firmas de la versión anterior. Por

ejemplo, el archivo de firma IOS-S361-CLI.pkg incluye todas las firmas del archivo IOS-S360-CLI.pkg además de las nuevas firmas creadas para las amenazas descubiertas luego de su publicación.

Así como los antivirus deben actualizar constantemente sus bases de datos de virus, los administradores de red deben vigilar y descargar las actualizaciones al archivo de firmas IPS. Las nuevas firmas están disponibles en Cisco.com. Es necesario iniciar una sesión CCO para obtenerlas.



5.2 Firmas IPS

5.2.3 Alarmas de firma IPS

Alarma de firma

El corazón de toda firma IPS es la alarma de firma, también conocida como disparador de firma. Considere un sistema de seguridad hogareño. El mecanismo disparador para una alarma contra robos podría ser un detector de movimientos que detecte el movimiento de un individuo cuando ingresa a un cuarto protegido con una alarma.

El disparador de la firma de un sensor IPS puede ser cualquier cosa que pueda señalar a un intruso o una violación a las políticas de seguridad. Un IPS de red puede disparar una acción de firma si detecta un paquete cuya carga contiene una cadena específica que se dirige a un puerto específico. Un IPS basado en host puede disparar una acción de firma cuando se invoca una llamada a una función específica. Cualquier cosa que pueda señalizar una intrusión o violación a las políticas de seguridad puede ser utilizada como mecanismo disparador.

Los sensores IDS e IPS de Cisco (Sensores IPS 4200 Series de Cisco y Catalyst 6500 - IDSM) pueden usar cuatro tipos de disparadores de firma:

Detección basada en patrones
Detección basada en anomalías
Detección basada en políticas
Detección basada en honeypots

Estos mecanismos disparadores pueden ser aplicados tanto a firmas atómicas como compuestas. Los mecanismos disparadores pueden ser simples o complejos. Cada IPS incorpora firmas que usan uno o más de estos mecanismos disparadores básicos para disparar acciones de firmas.

Otro mecanismo disparador común es la llamada decodificación de protocolos. En lugar de solo buscar un protocolo en cualquier parte del paquete, las decodificaciones de protocolos fragmentan el paquete según los campos del protocolo y luego buscan patrones específicos u otros aspectos malformados en los campos específicos del protocolo. La ventaja de la decodificación de protocolos es que permite una inspección más granular del tráfico y reduce el número de falsos positivos (tráfico que genera una alerta pero en realidad no constituye una amenaza para la red).

	Ventajas	Desventajas
Detección basada en patrones	• Configuración fácil • Menos falsos positivos • Buen diseño de firma	• No hay detección de firmas desconocidas • Inicialmente devuelve muchos falsos positivos • Deben crearse, actualizarse y ajustarse las firmas
Detección basada en anomalías	• Simple y confiable • Políticas personalizadas • Puede detectar ataques desconocidos	• Salida genérica • Debe crearse la política
Detección basada en políticas	• Configuración fácil • Puede detectar ataques desconocidos	• Dificultad para perfilar la actividad típica en grandes redes • El perfil del tráfico debe ser constante
Detección basada en honeypots	• Ventana para ver los ataques • Distrae y confunde a los atacantes • Disminuye la velocidad y evita los ataques • Recolecta información sobre el ataque	• Servidor honeypot dedicado • El servidor honeypot no puede ser confiable

Detección basada en patrones

La detección basada en patrones, también conocida como detección basada en firmas, es el mecanismo disparador más simple, ya que busca un patrón predefinido específico. Un sensor IDS o IPS basado en firmas compara el tráfico de la red con una base de datos de ataques conocidos y dispara una alarma o detiene las comunicaciones si se encuentra una coincidencia.

El disparador de firmas puede ser textual, binario o incluso una serie de llamadas a función. Puede ser detectado en un solo paquete (atómico) o en una secuencia de paquetes (compuesto). En la mayoría de los casos, el patrón se asocia con la firma solo si el paquete sospechoso se asocia con un servicio particular o que viaja desde o hacia

un puerto en particular. Esta técnica de búsqueda de coincidencias ayuda a reducir la cantidad de inspección que se realiza en cada paquete. Sin embargo, dificulta a los sistemas la tarea de tratar protocolos y ataques que no utilizan puertos bien definidos, como los troyanos y su tráfico asociado, que pueden moverse a voluntad.

En la etapa inicial de la incorporación de un IDS o IPS basados en patrones, antes de ajustar las firmas, puede haber muchos falsos positivos. Luego de que el sistema haya sido ajustado a los parámetros específicos de la red, habrá menos falsos positivos que con un enfoque basado en políticas.

Disparador de firma	Tipo de firma	
	Firma atómica	Firma compuesta
Detección basada en patrones	No se requieren estados para examinar los patrones para determinar si debe aplicarse la acción de la firma	Debe mantener estados o examinar múltiples ítems para determinar si debe aplicarse la acción de la firma
Ejemplo	Detección de una solicitud ARP (Address Resolution Protocol) con una dirección Ethernet de origen FF:FF:FF:FF:FF:FF	Búsqueda de la cadena de texto "confidential" en múltiples paquetes de una sesión TCP

Detección basada en anomalías

La detección basada en anomalías, también conocida como detección basada en perfiles, involucra primero la definición de un perfil de lo que se considera normal para la red o el host. Este perfil normal puede ser determinado monitoreando la actividad de la red o aplicaciones específicas en el host durante un período de tiempo. También puede basarse en una especificación definida, como una RFC. Luego de definir la actividad normal, la firma dispara una acción si ocurre actividad que excede un umbral específico que no está incluido en el perfil normal.

La ventaja de la detección basada en anomalías es que pueden detectarse ataques nuevos y previamente no publicados. En lugar de tener que definir un gran número de firmas para varias situaciones de ataque, el administrador simplemente define un perfil para actividad normal. Cualquier actividad que se desvía de este perfil es considerada anormal y dispara una acción de firma.

A pesar de esta ventaja obvia, muchas desventajas pueden dificultar el uso de las firmas basadas en anomalías. Por ejemplo, una alerta proveniente de una firma de anomalías no necesariamente indica un ataque: solo indica una desviación de la actividad normal definida, que, en ocasiones, puede ocurrir a causa de tráfico válido. A medida que la red evoluciona, la actividad normal generalmente cambia, por lo que la definición debe ser redefinida.

Otra cuestión a considerar es que el administrador debe garantizar que la red está libre de ataques durante la etapa de aprendizaje. De lo contrario, la actividad de ataque será considerada tráfico normal. Deben tomarse precauciones para asegurar que la red esté libre de ataques mientras se establece la actividad normal. Sin embargo, puede ser dificultoso definir el tráfico normal porque la mayoría de las redes consiste en una mezcla heterogénea de sistemas, dispositivos y aplicaciones que están en constante cambio.

Cuando una firma genera una alerta, puede ser difícil asociar la alerta con un ataque específico, ya que la alerta indica solo que se ha detectado tráfico anormal. Se requiere un análisis más profundo para determinar si el tráfico realmente representa un ataque y qué ha logrado. Adicionalmente, si el tráfico de ataque resulta ser parecido al tráfico normal, el ataque puede pasar enteramente desapercibido.

Disparador de firma	Tipo de firma	
	Firma atómica	Firma compuesta
Detección basada en anomalías	No se requieren estados para identificar actividad desviada del perfil normal.	Se requieren estados para identificar actividad desviada del perfil normal.
Ejemplo	Detección de tráfico que se dirige a un puerto destino que no está en el perfil normal	Verificación de conformidad de protocolos para tráfico HTTP

Detección basada en políticas

La detección basada en políticas, también conocida como detección basada en comportamiento, es similar a la detección basada en patrones, pero en lugar de tratar de definir patrones específicos, el administrador define comportamientos sospechosos basándose en un análisis histórico.

El uso de comportamientos permite que una sola firma cubra toda una clase de actividades sin necesidad de especificar cada situación individual. Por ejemplo, tener una firma que dispara una acción cuando un cliente de correo electrónico invoca cmd.exe permite al administrador aplicar la firma a cualquier aplicación cuyo comportamiento imite las características básicas de un cliente de correo electrónico sin tener que aplicar la firma individualmente a cada aplicación de cliente de correo electrónico individualmente. Por lo tanto, si un cliente instala una nueva aplicación de correo electrónico, la firma permanecerá vigente.

Detección basada en honeypots

La detección basada en honeypots usa un servidor ficticio para atraer a los atacantes. El propósito del enfoque de honeypots es distraer a los atacantes de los dispositivos de red reales. Al montar diferentes tipos de vulnerabilidades en el servidor honeypot, los administradores pueden analizar los tipos de ataques y patrones de tráfico malicioso entrantes. Los sistemas honeypot raramente se usan en ambientes de producción. Los antivirus y otros proveedores tienden a usarlos para investigación.

Disparador de firma	Tipo de firma	
	Firma atómica	Firma compuesta
Detección basada en políticas	No se requiere estado para identificar comportamiento no deseado.	Se requiere actividad previa (estado) para identificar comportamiento no deseado.
Ejemplo	Detección de paquetes fragmentados anormalmente grandes examinando solo el último fragmento.	Un host SUN Unix envía solicitudes RPC a hosts remotos sin consultar inicialmente al programa PortMapper de SUN.

Cisco ha implementado funciones IPS en su software IOS. Los IPS IOS de Cisco usan tecnología de las líneas de productos de sensores IDS e IPS de Cisco, incluyendo los sensores IPS 4200 Series y el Catalyst 6500 Series Intrusion Detection System Services Module (IDSM).

Existen muchos beneficios en el uso de la solución IPS IOS de Cisco:

Utiliza la infraestructura de enrutamiento subyacente para proporcionar una capa adicional de seguridad.
Como el IPS IOS de Cisco está en línea y es soportado en un amplio rango de plataformas de enrutamiento, los ataques pueden ser mitigados efectivamente para denegar tráfico malicioso proveniente tanto desde fuera como desde dentro de la red.
Cuando se usa el IPS IOS de Cisco en conjunto con las soluciones de IDS de Cisco, firewall IOS de Cisco, red privada virtual (VPN) y Control de Admisión a la Red (NAC), proporciona protección contra amenazas en todos los puntos de entrada de la red.
Es soportado por herramientas de administración fáciles de usar y efectivas, como el SDM de Cisco, el Sistema de Respuesta, Análisis y Monitoreo de Seguridad de Cisco(MARS) y el Administrador de Seguridad de Cisco.
Soporta aproximadamente 2,000 firmas de ataque de la misma base de datos de firmas disponible en los dispositivos IPS de Cisco. La cantidad varía dependiendo de la cantidad de memoria disponible en el router.

Sensor Cisco IPS 4200 Series



5.2.3 Ajuste de alarmas de firma IPS

Falsas alarmas

Los mecanismos disparadores pueden generar alarmas que son falsos positivos o falsos negativos. Estas alarmas deben ser tratadas en la implementación de un sensor IPS.

Una alarma de falso positivo es un resultado esperado pero no deseable. Ocurre cuando el sistema de intrusos genera una alarma luego de procesar tráfico normal que no debería disparar una alarma. El análisis de falsos positivos limita el tiempo del que dispone el analista de seguridad para examinar actividad de intrusos real en la red. Si esto ocurre, el administrador debe asegurarse de ajustar el IPS para cambiar estos tipos de alarma a negativos reales. Un negativo real describe una situación en la que el tráfico de red normal no genera una alarma.

Un falso negativo ocurre cuando el sistema de intrusos falla en la generación de una alarma luego de procesar tráfico de un tipo de ataque que está configurado para detectar.

Es imperativo que el sistema de intrusos no genere falsos negativos, porque esto significa que los ataques conocidos no están siendo detectados. El objetivo es que estas alarmas sean mostradas como positivos reales. Un positivo real describe una situación en la cual el sistema de intrusos genera una alarma en respuesta al tráfico de ataque conocido.

Tipo de alarma	Actividad de la red	Actividad IPS	Resultado
Falso positivo	Tráfico de usuario normal	Alarma generada	Ajustar alarma
Falso negativo	Tráfico de ataque	Alarma no generada	Ajustar alarma
Positivo real	Tráfico de ataque	Alarma generada	Situación ideal
Negativo real	Tráfico de usuario normal	Alarma no generada	Situación ideal

Las alarmas se disparan cuando se cumplen parámetros específicos. El administrador debe equilibrar el número de alarmas incorrectas que pueden ser toleradas y la habilidad de la firma de detectar intrusos reales. Si hay pocas alarmas, puede ser que se esté permitiendo la entrada a la red de paquetes sospechosos, pero el tráfico de red fluirá más rápidamente. Sin embargo, si los sistemas IPS usan firmas sin ajustar, producirán muchas alarmas de falso positivo.

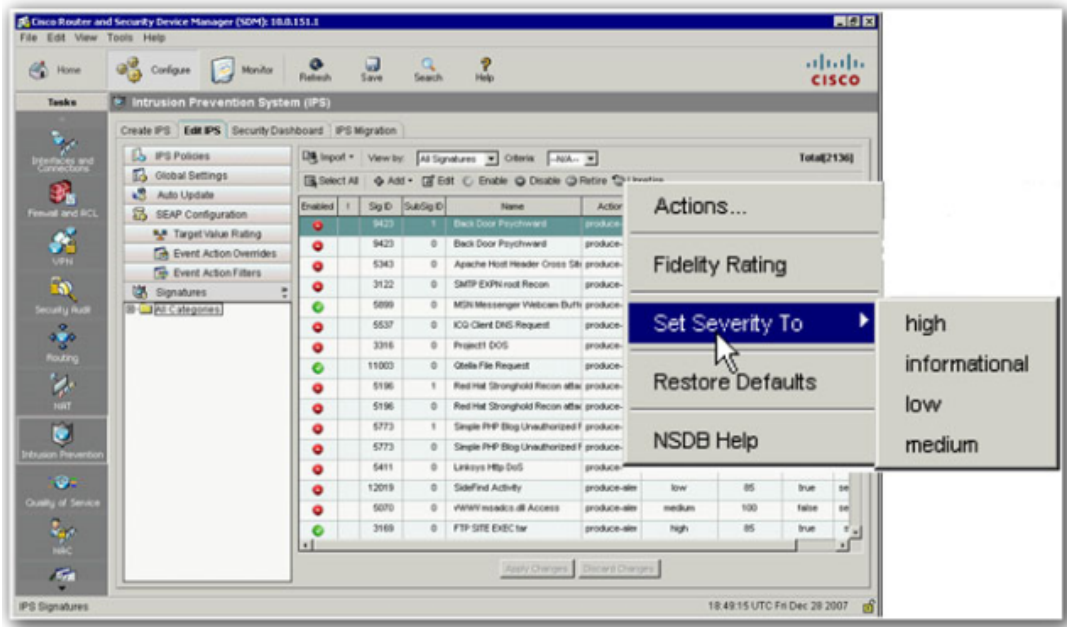
Una firma se ajusta en uno de cuatro niveles (listados alfabéticamente), basándose en la severidad percibida de la firma:

Alto - Se detectan los ataques usados para ganar acceso o causar un ataque de DoS y una amenaza inmediata es extremadamente probable.
Bajo - La actividad de red anormal que puede ser considerada maliciosa es detectada, pero una amenaza inmediata es poco probable.
Informativo - La actividad que dispara la firma no es considerada una amenaza inmediata, pero la información provista es útil.
Medio - Se detecta la actividad de red anormal que puede ser considerada maliciosa y una amenaza inmediata es probable.

Deben considerarse varios factores en la implementación de las alarmas usadas por la firma:

El nivel asignado a la firma determina el nivel de severidad de la alarma.
Al ajustar una alarma de firma, el nivel de severidad de la firma debe ser el mismo que el de la alarma.
Para minimizar la cantidad de falsos positivos, el administrador debe estudiar los patrones de tráfico existentes y luego ajustar las firmas para reconocer patrones de intrusos atípicos (fuera de la caracterización).

El ajuste de las firmas debe basarse en los patrones de tráfico reales de la red.



5.2.4 Acciones de firma IPS

Cada vez que una firma detecta actividad para la cual está configurada, dispara una o más acciones. Las acciones que pueden llevarse a cabo son:

Generar una alerta.
Ingresar la actividad en el registro.
Descartar o detener la actividad.
Reiniciar una conexión TCP.
Bloquear actividad futura.
Permitir la actividad.

Las acciones disponibles dependen del tipo de firma y la plataforma.

Categoría	Alerta específica	Descripción
Generación de una alerta	Producir alerta	• Esta acción ingresa el evento al Event Store como una alerta.
	Producir alerta detallada (verbose)	• Esta acción incluye una transcripción del paquete ofensivo codificada en la alerta. ***
Registro de la actividad	Registrar paquetes atacantes	• Esta acción inicia el registro IP de los paquetes que contienen la dirección del atacante y envía una alerta. ***
	Registrar paquetes pares	• Esta acción inicia el registro IP de los paquetes que contienen el par de direcciones del atacante y la víctima. ***
	Registrar paquetes de la víctima	• Esta acción inicia el registro IP de los paquetes que contienen la dirección de la víctima y envía una alerta. ***
Descartar o prevenir la actividad	Denegar atacante en línea	• Esta acción termina el paquete actual y los futuros provenientes de la dirección del atacante por un tiempo específico de tiempo. • El sensor mantiene una lista de los atacantes denegados actualmente por el sistema. • Las entradas pueden ser removidas de la lista manualmente o se puede esperar que el temporizador expire. • El temporizador se desliza en cada entrada. Por lo tanto, si el atacante A está actualmente denegado pero inicia un nuevo ataque, el temporizador para el atacante A se reinicia y este permanece en la lista de atacantes denegados hasta que el nuevo temporizador expire.
		• El temporizador se desliza en cada entrada. Por lo tanto, si el atacante A está actualmente denegado pero inicia un nuevo ataque, el temporizador para el atacante A se reinicia y este permanece en la lista de atacantes denegados hasta que el nuevo temporizador expire. • Si la lista de atacantes denegados está llena y no puede añadirse una nueva entrada, el paquete será denegado de cualquier forma.
	Denegar conexión en línea	• Esta acción termina el paquete actual y los futuros en este flujo TCP.
	Denegar paquete en línea	• Esta acción termina el paquete.
Reinicio de una conexión TCP	Reiniciar conexión TCP	• Esta acción envía TCP resets para tomar control del flujo TCP y terminarlo.
Bloqueo de actividad futura	Solicitar bloqueo de conexión	• Esta acción envía una solicitud a un dispositivo de bloqueo para bloquear esta conexión.
	Solicitar bloqueo de host	• Esta acción envía una solicitud a un dispositivo de bloqueo para bloquear el host del atacante.
	Solicitar SNMP trap	• Esta acción envía una solicitud al componente de notificaciones del sensor para llevar a cabo una notificación SNMP (Simple Network Management Protocol). ***

*** Se ingresará una alerta en el Event Store, incluso si la acción Produce Alert no está seleccionada.

generación de una alarma

El monitoreo de las alertas generadas por los sistemas IPS basados en host y en red es vital para entender los ataques lanzados contra la red. Si un atacante causa una inundación de alertas falsas, la inspección de estas alertas puede abrumar al analista de seguridad. Tanto los IPS basados en host como los basados en red incorporan dos tipos de alertas para permitir al administrador monitorear eficientemente la operación de la red: las alertas atómicas y la alertas resumidas. Entender estos tipos de alertas es crítico para proporcionar la protección más efectiva a la red.

Alertas atómicas

Las alertas atómicas se generan cada vez que una firma se dispara. En algunas situaciones, este comportamiento es útil e indica todas las ocurrencias de un ataque específico. Sin embargo, un atacante puede lograr inundar la consola de monitor con miles de alertas falsas dirigidas hacia el dispositivo o aplicacion IPS.

Alertas resumidas

En lugar de generar alertas en cada instancia de una firma, algunas soluciones IPS permiten al administrador generar alertas resumidas. Una alerta resumida consta de una sola alerta que indica múltiples ocurrencias de la misma firma para la misma dirección o puerto de origen. Las alarmas resumidas limitan el número de alertas generadas y dificultan al atacante consumir los recursos del sensor.

Con los modos resumidos, el administrador también recibe información relacionada con la cantidad de veces que la actividad que coincide con las características de la firma ha sido observada durante un período determinado de tiempo. Cuando se usa el resumen de alarmas, la primera instancia de actividad intrusiva generalmente dispara una alerta normal. Luego, otras instancias de la misma actividad (alarmas duplicadas) se cuentan hasta el final del intervalo de resumen de la firma. Cuando el tiempo especificado por el intervalo de resumen ha pasado, se envía una alarma resumida que indica el número de alarmas ocurridas durante el intervalo de tiempo.

Algunas soluciones IPS también habilitan el resumen automático aunque el comportamiento por defecto es generar alertas atómicas. En esta situación, si el número de alertas atómicas excede un umbral configurado en un período de tiempo específico, la firma cambia automáticamente a la generación de alertas resumidas en lugar de alertas atómicas. Luego de un período configurado de tiempo, la firma vuelve a su configuración original. El resumen automático permite al administrador regular automáticamente el número de alertas generadas.

Como híbrido entre las alertas atómicas y las resumidas, algunas soluciones IPS también permiten la generación de una sola alerta atómica y luego deshabilitan las alertas de esa firma y dirección de origen por un período de tiempo específico. Esto evita que el administrador sea abrumado con alertas pero indica efectivamente que un sistema específico muestra un comportamiento sospechoso.

Categoría	Alerta específica	Descripción
Generación de una alerta	Producir alerta	• Esta acción ingresa el evento al Event Store como una alerta.
	Producir alerta detallada (verbose)	• Esta acción incluye una transcripción del paquete ofensivo codificada en la alerta. ***
Registro de la actividad	Registrar paquetes atacantes	• Esta acción inicia el registro IP de los paquetes que contienen la dirección del atacante y envía una alerta. ***
	Registrar paquetes pares	• Esta acción inicia el registro IP de los paquetes que contienen el par de direcciones del atacante y la víctima. ***
	Registrar paquetes de la víctima	• Esta acción inicia el registro IP de los paquetes que contienen la dirección de la víctima y envía una alerta. ***
Descartar o prevenir la actividad	Denegar atacante en línea	• Esta acción termina el paquete actual y los futuros provenientes de la dirección del atacante por un tiempo específico de tiempo. • El sensor mantiene una lista de los atacantes denegados actualmente por el sistema. • Las entradas pueden ser removidas de la lista manualmente o se puede esperar que el temporizador expire. • El temporizador se desliza en cada entrada. Por lo tanto, si el atacante A está actualmente denegado pero inicia un nuevo ataque, el temporizador para el atacante A se reinicia y este permanece en la lista de atacantes denegados hasta que el nuevo temporizador expire. • Si la lista de atacantes denegados está llena y no puede añadirse una nueva entrada, el paquete será denegado de cualquier forma.
	Denegar conexión en línea	• Esta acción termina el paquete actual y los futuros en este flujo TCP.
	Denegar paquete en línea	• Esta acción termina el paquete.
Reinicio de una conexión TCP	Reiniciar conexión TCP	• Esta acción envía TCP resets para tomar control del flujo TCP y terminarlo.
Bloqueo de actividad futura	Solicitar bloqueo de conexión	• Esta acción envía una solicitud a un dispositivo de bloqueo para bloquear esta conexión.
	Solicitar bloqueo de host	• Esta acción envía una solicitud a un dispositivo de bloqueo para bloquear el host del atacante.
	Solicitar SNMP trap	• Esta acción envía una solicitud al componente de notificaciones del sensor para llevar a cabo una notificación SNMP (Simple Network Management Protocol. ***

*** Se ingresará una alerta en el Event Store, incluso si la acción Produce Alert no está seleccionada.

Registro de la actividad

En algunas situaciones, el administrador no dispone necesariamente de suficiente información para detener una actividad. Por lo tanto, registrar las acciones o paquetes revisados para que luego puedan ser analizados más profundamente es muy importante. Al llevar a cabo un análisis detallado, el administrador puede identificar exactamente lo que está ocurriendo y tomar una decisión sobre si debe permitirse o denegarse en el futuro.

Por ejemplo, si un administrador configura una firma para buscar la cadena de texto /etc/password y registrar la acción con la dirección IP del atacante cada vez que la firma se dispara, el dispositivo IPS registrará el tráfico de la dirección IP del atacante durante un período de tiempo determinado o un número de bytes específico. Esta información de registro generalmente es almacenada en el dispositivo IPS en un archivo específico. Como la firma también genera una alerta, el administrador puede observar la alerta en la

consola de administración. Luego, los datos de registro pueden ser recolectados del dispositivo IPS y puede analizarse la actividad del atacante en la red luego de que se disparó la alarma inicial.

Categoría	Alerta específica	Descripción
Generación de una alerta	Producir alerta	• Esta acción ingresa el evento al Event Store como una alerta.
	Producir alerta detallada (verbose)	• Esta acción incluye una transcripción del paquete ofensivo codificada en la alerta. ***
Registro de la actividad	Registrar paquetes atacantes	• Esta acción inicia el registro IP de los paquetes que contienen la dirección del atacante y envía una alerta. ***
	Registrar paquetes pares	• Esta acción inicia el registro IP de los paquetes que contienen el par de direcciones del atacante y la víctima. ***
	Registrar paquetes de la víctima	• Esta acción inicia el registro IP de los paquetes que contienen la dirección de la víctima y envía una alerta. ***
Descartar o prevenir la actividad	Denegar atacante en línea	• Esta acción termina el paquete actual y los futuros provenientes de la dirección del atacante por un tiempo específico de tiempo. • El sensor mantiene una lista de los atacantes denegados actualmente por el sistema. • Las entradas pueden ser removidas de la lista manualmente o se puede esperar que el temporizador expire. • El temporizador se desliza en cada entrada. Por lo tanto, si el atacante A está actualmente denegado pero inicia un nuevo ataque, el temporizador para el atacante A se reinicia y este permanece en la lista de atacantes denegados hasta que el nuevo temporizador expire.
		• Si la lista de atacantes denegados está llena y no puede añadirse una nueva entrada, el paquete será denegado de cualquier forma.
	Denegar conexión en línea	• Esta acción termina el paquete actual y los futuros en este flujo TCP.
	Denegar paquete en línea	• Esta acción termina el paquete.
Reinicio de una conexión TCP	Reiniciar conexión TCP	• Esta acción envía TCP resets para tomar control del flujo TCP y terminarlo.
Bloqueo de actividad futura	Solicitar bloqueo de conexión	• Esta acción envía una solicitud a un dispositivo de bloqueo para bloquear esta conexión.
	Solicitar bloqueo de host	• Esta acción envía una solicitud a un dispositivo de bloqueo para bloquear el host del atacante.
	Solicitar SNMP trap	• Esta acción envía una solicitud al componente de notificaciones del sensor para llevar a cabo una notificación SNMP (Simple Network Management Protocol). ***

*** Se ingresará una alerta en el Event Store, incluso si la acción Produce Alert no está seleccionada.

Descarte o prevención de la actividad

Una de las acciones más poderosas de parte de un dispositivo IPS es el descarte o prevención de una actividad. Esta acción permite al dispositivo detener un ataque antes de que pueda llevar a cabo actividad maliciosa. A diferencia de un dispositivo IDS tradicional, el dispositivo IPS reenvía paquetes activamente a través de dos de sus interfaces. El motor de análisis determina cuáles paquetes deberán ser reenviados y cuáles descartados.

Además de descartar paquetes individuales, la acción de descarte puede ser expandida para descartar todos los paquetes de una sesión específica o incluso todos los paquetes

de un host específico por un período de tiempo determinado. El descarte del tráfico de una conexión o host permite al IPS conservar los recursos sin tener que analizar cada paquete por separado.

Categoría	Alerta específica	Descripción
Generación de una alerta	Producir alerta	• Esta acción ingresa el evento al Event Store como una alerta.
	Producir alerta detallada (verbose)	• Esta acción incluye una transcripción del paquete ofensivo codificada en la alerta. ***
Registro de la actividad	Registrar paquetes atacantes	• Esta acción inicia el registro IP de los paquetes que contienen la dirección del atacante y envía una alerta. ***
	Registrar paquetes pares	• Esta acción inicia el registro IP de los paquetes que contienen el par de direcciones del atacante y la víctima. ***
	Registrar paquetes de la víctima	• Esta acción inicia el registro IP de los paquetes que contienen la dirección de la víctima y envía una alerta. ***
Descartar o prevenir la actividad	Denegar atacante en línea	• Esta acción termina el paquete actual y los futuros provenientes de la dirección del atacante por un tiempo específico de tiempo. • El sensor mantiene una lista de los atacantes denegados actualmente por el sistema. • Las entradas pueden ser removidas de la lista manualmente o se puede esperar que el temporizador expire. • El temporizador se desliza en cada entrada. Por lo tanto, si el atacante A está actualmente denegado pero inicia un nuevo ataque, el temporizador para el atacante A se reinicia y este permanece en la lista de atacantes denegados hasta que el nuevo temporizador expire.
		• Si la lista de atacantes denegados está llena y no puede añadirse una nueva entrada, el paquete será denegado de cualquier forma.
	Denegar conexión en línea	• Esta acción termina el paquete actual y los futuros en este flujo TCP.
	Denegar paquete en línea	• Esta acción termina el paquete.
Reinicio de una conexión TCP	Reiniciar conexión TCP	• Esta acción envía TCP resets para tomar control del flujo TCP y terminarlo.
Bloqueo de actividad futura	Solicitar bloqueo de conexión	• Esta acción envía una solicitud a un dispositivo de bloqueo para bloquear esta conexión.
	Solicitar bloqueo de host	• Esta acción envía una solicitud a un dispositivo de bloqueo para bloquear el host del atacante.
	Solicitar SNMP trap	• Esta acción envía una solicitud al componente de notificaciones del sensor para llevar a cabo una notificación SNMP (Simple Network Management Protocol). ***

*** Se ingresará una alerta en el Event Store, incluso si la acción Produce Alert no está seleccionada.

Reinicio de una conexión TCP

La acción TCP Reset Signature es una acción básica que puede ser utilizada para terminar conexiones TCP generando un paquete para la conexión con el flag TCP RST activado. Muchos dispositivos IPS usan la acción de reinicio de TCP para terminar una conexión TCP abruptamente si está llevando a cabo operaciones no deseables. La acción de reinicio de conexiones TCP puede ser usada en conjunto con la denegación de paquetes y la denegación de acciones de conexión. Las acciones de denegación de paquetes y de flujo no causan automáticamente la acción de reinicio TCP.

Bloqueo de actividad futura

La mayoría de los dispositivos IPS tiene la capacidad de bloquear tráfico futuro haciendo que el dispositivo IPS actualice las listas de control de acceso (ACLs) en uno de los dispositivos de la infraestructura. La ACL detiene el tráfico de un sistema atacante sin solicitar el consumo de los recursos del IPS mediante el análisis del tráfico. Luego de un período de tiempo configurado, el dispositivo IPS elimina la ACL. Los dispositivos IPS de red generalmente proporcionan esta función de bloqueo con otras acciones como el descarte de paquetes no deseables. Una ventaja de la acción de bloqueo es que un solo dispositivo IPS puede detener el tráfico de varias ubicaciones en toda la red, sin importar su propia ubicación. Por ejemplo, un dispositivo IPS ubicado bien dentro de la red puede aplicar ACLs en el router o firewall de perímetro.

Permitir la actividad

La acción final es Allow Signature. Puede parecer un poco confuso, ya que la mayoría de los dispositivos IPS está diseñada para detener o prevenir el tráfico no deseable de una red. La acción de permiso es necesaria para que el administrador pueda definir las excepciones de las firmas configuradas. Al descartar el tráfico de una conexión o host, el IPS conserva los recursos sin tener que analizar cada paquete por separado. Configurar excepciones permite a los administradores aplicar un enfoque más restrictivo sobre la seguridad, ya que pueden primero denegar todo y luego permitir solo la actividad necesaria.

Por ejemplo, suponga que el departamento de informática escanea regularmente su red con un escáner de vulnerabilidades común. Este escaneo hará que el IPS dispare varias alertas. Estas serán las mismas alertas que el IPS generará cuando un atacante escanee la red. Al permitir las alertas del host de escaneo del departamento de informática, el administrador puede proteger la red de escaneos intrusivos, al tiempo que elimina los falsos positivos generados por el escaneo de rutina realizado por el departamento.

Algunos dispositivos IPS ofrecen la acción de permiso indirectamente a través de otros mecanismos, como filtros de firmas. Si un IPS no proporciona la acción de permiso directamente a través de una acción como permitir ('permit' o 'allow'), el administrador deberá buscar en la documentación del producto el mecanismo utilizado para permitir excepciones a las firmas.

Categoría	Alerta específica	Descripción
Generación de una alerta	Producir alerta	• Esta acción ingresa el evento al Event Store como una alerta.
	Producir alerta detallada (verbose)	• Esta acción incluye una transcripción del paquete ofensivo codificada en la alerta. ***
Registro de la actividad	Registrar paquetes atacantes	• Esta acción inicia el registro IP de los paquetes que contienen la dirección del atacante y envía una alerta. ***
	Registrar paquetes pares	• Esta acción inicia el registro IP de los paquetes que contienen el par de direcciones del atacante y la víctima. ***
	Registrar paquetes de la víctima	• Esta acción inicia el registro IP de los paquetes que contienen la dirección de la víctima y envía una alerta. ***
Descartar o prevenir la actividad	Denegar atacante en línea	• Esta acción termina el paquete actual y los futuros provenientes de la dirección del atacante por un tiempo específico de tiempo. • El sensor mantiene una lista de los atacantes denegados actualmente por el sistema. • Las entradas pueden ser removidas de la lista manualmente o se puede esperar que el temporizador expire. • El temporizador se desliza en cada entrada. Por lo tanto, si el atacante A está actualmente denegado pero inicia un nuevo ataque, el temporizador para el atacante A se reinicia y este permanece en la lista de atacantes denegados hasta que el nuevo temporizador expire.
		• Si la lista de atacantes denegados está llena y no puede añadirse una nueva entrada, el paquete será denegado de cualquier forma.
	Denegar conexión en línea	• Esta acción termina el paquete actual y los futuros en este flujo TCP.
	Denegar paquete en línea	• Esta acción termina el paquete.
Reinicio de una conexión TCP	Reiniciar conexión TCP	• Esta acción envía TCP resets para tomar control del flujo TCP y terminarlo.
Bloqueo de actividad futura	Solicitar bloqueo de conexión	• Esta acción envía una solicitud a un dispositivo de bloqueo para bloquear esta conexión.
	Solicitar bloqueo de host	• Esta acción envía una solicitud a un dispositivo de bloqueo para bloquear el host del atacante.
	Solicitar SNMP trap	• Esta acción envía una solicitud al componente de notificaciones del sensor para llevar a cabo una notificación SNMP (Simple Network Management Protocol). ***

*** Se ingresará una alerta en el Event Store, incluso si la acción Produce Alert no está seleccionada.

5.2.5 Administracion y monitoreo IPS

El monitoreo de los eventos relacionados con la seguridad de una red también es un aspecto crucial de la protección de una red contra ataques. Aunque un IPS puede prevenir varios ataques, entender los que están siendo lanzados contra la red permite al administrador evaluar cuán fuertes son las protecciones actuales y qué mejoras pueden ser necesarias a medida que la red crece. Sólo monitoreando los eventos de seguridad de la red el administrador podrá identificar con precisión los ataques y las violaciones a la política de seguridad que toman lugar en la red.



Método de administración

Los sensores IPS pueden ser administrados individual o centralmente. La configuración individual de cada dispositivo IPS es el proceso más sencillo si solo hay un par de sensores. Por ejemplo, una red que tiene el IPS IOS de Cisco en algunos pocos routers puede ser administrada con el SDM. La administración individual de varios routers y sensores IPS se vuelve difícil y toma mucho tiempo.

En una red grande, un sistema de administración centralizada que permite al administrador configurar y administrar todos los dispositivos IPS desde un único sistema central debe ser implementado. El uso del enfoque de administración centralizada para grandes despliegues de sensores reduce los requisitos de tiempo, personal y permite una mayor visibilidad en todos los eventos que toman lugar en una red.

Correlación de eventos

La correlación de eventos se refiere al proceso por el cual se correlacionan ataques y otros eventos que toman lugar simultáneamente en diferentes puntos de una red. El uso de Network Time Protocol (NTP) para hacer que los dispositivos deriven su fecha y hora del servidor NTP permite una mayor precisión en las marcas de tiempo de todas las alertas generadas por los IPS. Una herramienta de correlación podrá luego ordenar las alertas basándose en las marcas de tiempo. El administrador debe permitir NTP en todos los dispositivos de red para otorgar marcas de tiempo a los eventos con un sistema de tiempo común. Estas marcas de tiempo podrán ser usadas luego para evaluar con precisión cúando tomó lugar un evento específico en relación con otros eventos, sin importar cuál dispositivo detectó el evento.

Otro factor que facilita la correlación de eventos es el despliegue de una función de monitoreo centralizado en la red. Al monitorear todos los eventos IPS en una sola ubicación, el administrador mejora importantemente la precisión de la correlación de los eventos.

También se recomienda el despliegue de un producto que permita al administrador correlacionar no solo los eventos IPS sino otros eventos de la red, como mensajes syslog y entradas NetFlow. El producto Cisco Security Monitoring, Analysis and Response System (Cisco Security MARS) puede proporcionar este nivel de correlación.

Personal de seguridad

Los dispositivos IPS tienden a generar varias alertas y otros eventos durante el procesamiento de tráfico de la red. Las grandes empresas requieren el personal de seguridad apropiado para analizar esta actividad y determinar qué tan bien el IPS está protegiendo la red. Examinar estas alertas también permite a los operadores de la red ajustar y optimizar la operación del IPS en relación con los requisitos únicos de la red.

Plan de respuesta a incidentes

Si un sistema de la red se halla comprometido, debe implementarse un plan de respuesta. El sistema comprometido debe ser devuelto al estado en que estaba antes del ataque. Debe determinarse si el sistema comprometido llevó a pérdida de propiedad intelectual o al compromiso de otros sistemas en la red.

Características de MARS

- MARS se usa para administrar de manera centralizada todos los sensores IPS.
- MARS se usa para correlacionar todos los eventos IPS y Syslog en una ubicación central.
- La funcionalidad MARS debe estar integrada en el plan de respuesta a incidentes identificada en la política de seguridad de la red.



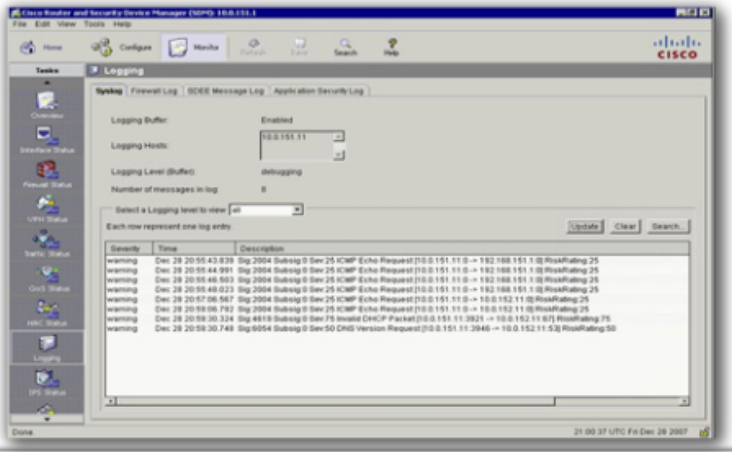
Aunque la CLI puede ser utilizada para configurar un despliegue de IPS, es más simple utilizar un administrador de dispositivos basado en GUI. Existen muchas soluciones de software de administración de Cisco, diseñadas para ayudar a los administradores a gestionar su solución IPS. Algunas proporcionan soluciones IPS administradas localmente, mientras que otras proporcionan soluciones de administración más centralizada.

Existen dos soluciones de administración local de IPS:

Administrador de Routers y Dispositivos de Seguridad de Cisco (SDM)
Administrador de Dispositivos IPS de Cisco IPS (IDM)

Existen tres soluciones de administración centralizada de IPS:

Visor de Eventos IDS de Cisco (IEV)
Administrador de Seguridad de Cisco (CSM)
Sistema de Respuesta, Análisis y Monitoreo de Seguridad de Cisco (MARS)

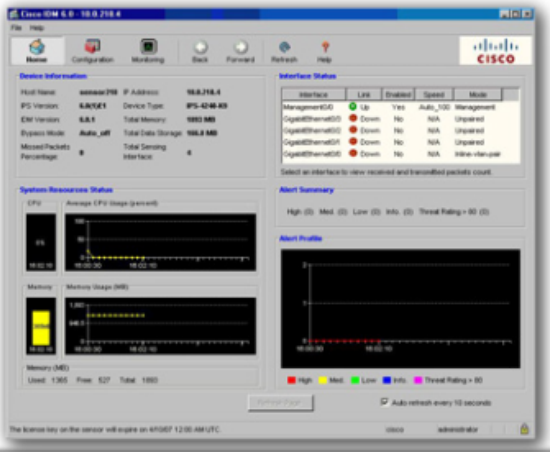


Administrador de Routers y Dispositivos de Seguridad de Cisco (SDM)

- El IPS IOS de Cisco monitorea y evita intrusiones al comparar el tráfico con las firmas de amenazas conocidas y bloquear el tráfico cuando detecta una amenaza.
- El SDM de Cisco permite a los administradores controlar la aplicación del IPS IOS de Cisco a las interfaces, importar y editar archivos de definición de firmas (SDF) de Cisco.com y configurar la acción que el IPS IOS de Cisco debe realizar si detecta una amenaza.

SDM | IDM | IEV | CSM | MARS

Haga clic en los botones para ver el contenido asociado.

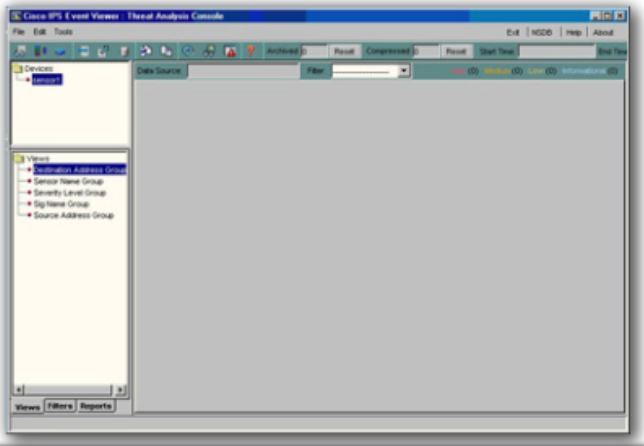


Cisco IPS Device Manager (IDM)

- El IDM de Cisco es una herramienta de configuración basada en web para los dispositivos IPS de red.
- Se entrega sin costo adicional con el software de Sensor IPS de Cisco.
- IDM es una aplicación Java basada en web que permite al administrador configurar y administrar el sensor.
- El servidor web de IDM reside en el sensor y puede accederse a él a través de un navegador web.

SDM | IDM | IEV | CSM | MARS

Haga clic en los botones para ver el contenido asociado.

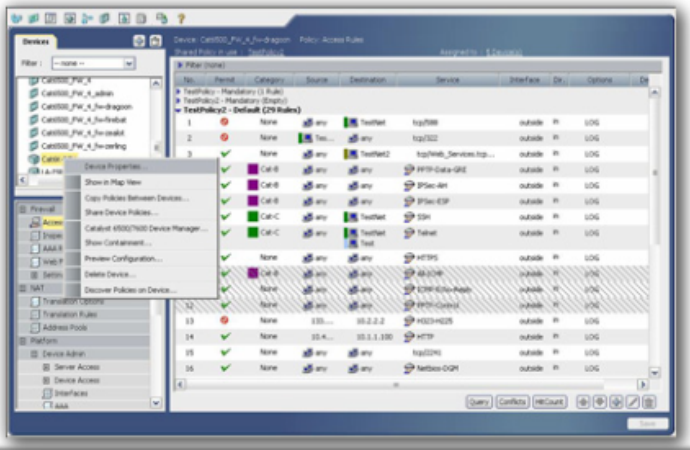


Cisco IPS Event Viewer (IEV)

- El IEV de Cisco es una aplicación basada en Java que permite a los administradores visualizar y administrar las alarmas de hasta cinco sensores.
- Con el IEV de Cisco, los administradores pueden conectarse a y visualizar alarmas en tiempo real o en archivos de registro importados.
- Los administradores pueden configurar filtros y vistas para administrar las alarmas.
- Los administradores también pueden importar y exportar datos de los eventos para un análisis más profundo.

SDM | IDM | **IEV** | CSM | MARS

Haga clic en los botones para ver el contenido asociado.



Administrador de Seguridad de Cisco (CSM)

- El Administrador de Seguridad de Cisco es una solución potente pero muy fácil de usar que administra centralmente todos los aspectos de la configuración de los dispositivos y las políticas de seguridad de los firewalls, VPNs e IPS Cisco.
- Proporciona soporte a sensores IPS e IPS IOS de Cisco.
- Soporta actualizaciones automáticas de firmas y software de sensor IPS basadas en políticas.
- Incluye un asistente de actualizaciones de firmas que permite revisión y edición fáciles antes del despliegue.

SDM | IDM | IEV | **CSM** | MARS

Haga clic en los botones para ver el contenido asociado.



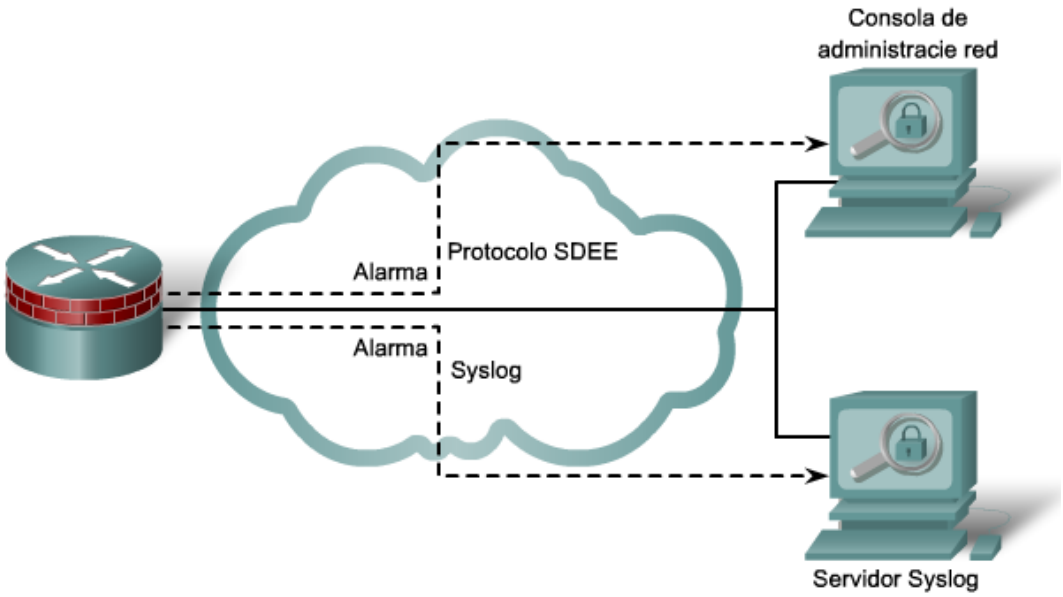
Los sensores IPS y el IPS IOS de Cisco generan alarmas cuando una firma habilitada se dispara. Estas alarmas se almacenan en el sensor y pueden ser visualizadas localmente o una aplicación de administración central como MARS puede sacar las alarmas de los sensores.

Cuando se detecta una firma de ataque, la función IPS del IOS de Cisco puede enviar un mensaje syslog o una alarma en formato Secure Device Event Exchange (SDEE). Este formato fue desarrollado para mejorar la comunicación de eventos generados por dispositivos de seguridad. Principalmente comunica eventos IDS, pero está diseñado para ser extensible y permite la inclusión de tipos de eventos adicionales a medida que se definen.

El SDM de Cisco puede monitorear los eventos syslog y los generados por SDEE y las alarmas comunes en los mensajes del sistema SDEE, incluyendo las alarmas de firmas IPS.

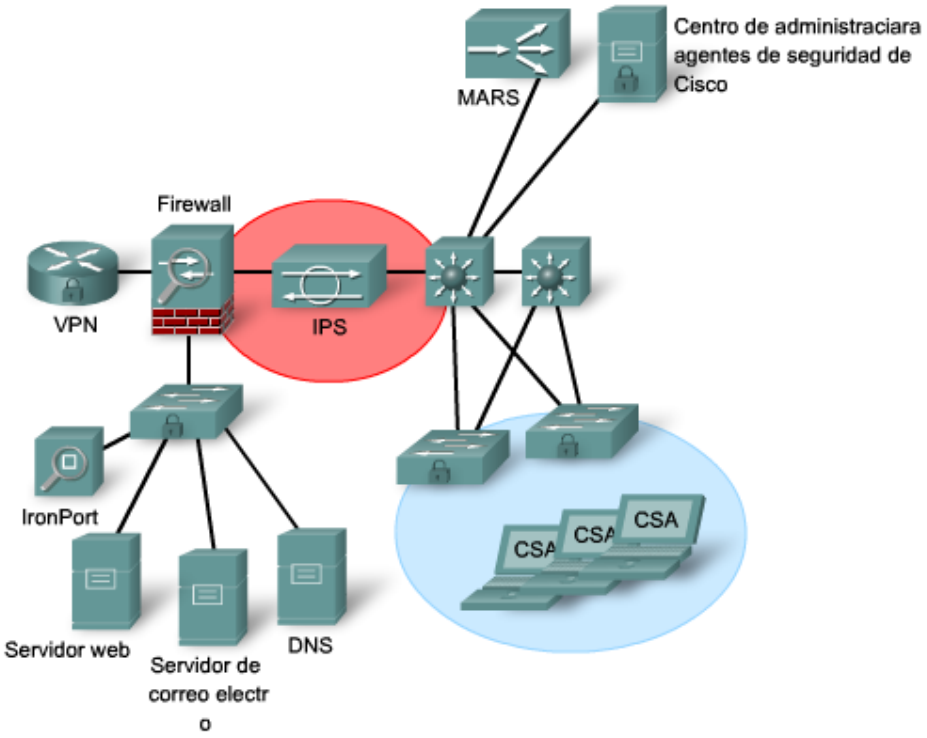
Un mensaje de alarma de sistema SDEE tiene este tipo de formato:

%IPS-4-SIGNATURE:Sig:1107 Subsig:0 Sev:2 RFC1918 address [192.168.121.1:137 ->192.168.121.255:137]



La administración de firmas en varios dispositivos IPS puede ser dificultosa. Para mejorar la eficiencia de los IPS en una red, considere usar estas buenas prácticas de configuración recomendadas.

La necesidad de actualizar los sensores con los últimos paquetes de firmas debe equilibrarse con el tiempo de inactividad momentáneo durante el cual la red será vulnerable a ataques.
Al desplegar una gran implementación de sensores, actualice los paquetes de firmas automáticamente en lugar de hacerlo manualmente en cada sensor. Esto otorga al personal de operaciones de seguridad más tiempo para analizar los eventos.
Cuando se encuentran disponibles nuevos paquetes de firmas, descárguelos a un servidor seguro dentro de la red de administración. Use otro IPS para proteger este servidor de ataques externos.
Ubique los paquetes de firmas en un servidor FTP dedicado dentro de la red de administración. Si no se encuentra disponible una actualización de firmas, puede crearse una firma personalizada para detectar y mitigar un ataque específico.
Configure el servidor FTP para permitir acceso de solo lectura a los archivos dentro del directorio en el que se encuentran los paquetes de firmas.
Configure los sensores para buscar nuevos paquetes de firmas en el servidor FTP periódicamente, como una vez por semana o en un cierto día. Escalone el momento del día en que cada sensor busca nuevos paquetes de firmas en el servidor FTP, quizás con una ventana de cambio predeterminada. Esto evita que múltiples sensores abrumen el servidor FTP pidiendo el mismo archivo al mismo tiempo.
Mantenga sincronizados los niveles de firma soportados en la consola de administración con los paquetes de firmas de los sensores.



5.3.1 Configuracion del IPS IOS Cisco con la CLI

El IPS IOS de Cisco permite a los administradores gestionar la prevención de intrusos en los routers que usan el IOS de Cisco versión 12.3(8)T4 o posterior. El IPS IOS de Cisco monitorea y previene intrusos comparando el tráfico con firmas de amenazas conocidas y bloqueando el tráfico cuando se detecta una amenaza.

Usar la CLI del IOS de Cisco con las firmas de formato IPS IOS 5.x toma varios pasos. El IOS de Cisco versión 12.4(10) y los anteriores usaban firmas de formato IPS 4.x y algunos comandos IPS han cambiado.

Para implementar el IPS IOS:

Paso 1. Descargar los archivos IPS IOS.

Paso 2. Crear un directorio de configuración IPS IOS en la flash.

Paso 3. Configurar una clave criptográfica IPS IOS.

Paso 4. Habilitar el IPS IOS.

Paso 5. Cargar el paquete de firmas del IPS IOS en el router.



Antes de la versión 12.4(11)T del IOS de Cisco, el IPS IOS de Cisco proporcionaba firmas integradas en la imagen del software IOS de Cisco y soporte a las firmas importadas. En las versiones T-Train del IOS de Cisco anteriores a la 12.4(11)T, y en todas las versiones 12.4 Mainline del software IOS de Cisco, la selección de firmas IPS involucra la carga de un archivo XML en el router. Este archivo, llamado archivo de definición de firmas (signature definition file - SDF), contiene una descripción detallada de cada firma seleccionada en el formato de firma 4.x del software de Sensor IPS de Cisco.

A partir de la versión 12.4(11)T del IOS de Cisco, no hay firmas integradas (hard-coded) en el software IOS de Cisco. En su lugar, todas las firmas se almacenan en un archivo de firma separado y debe ser importado. Las versiones 12.4(11)T y posteriores del IOS usan los archivos de firma de formato 5.x, que pueden ser descargados de Cisco.com (requiere un inicio de sesión).

Paso 1. Descarga del archivo IPS IOS.

Antes de configurar IPS, es necesario descargar los archivos del paquete de firmas del IPS IOS y la clave criptográfica pública de Cisco.com. Los archivos IPS específicos que se descargarán varían en relación con la versión en uso. Solo los clientes registrados pueden descargar los archivos de paquete y clave.

IOS-Sxxx-CLI.pkg - Este es el paquete de firmas más reciente.
realm-cisco.pub.key.txt - Esta es la clave criptográfica pública utilizada por el IPS IOS.

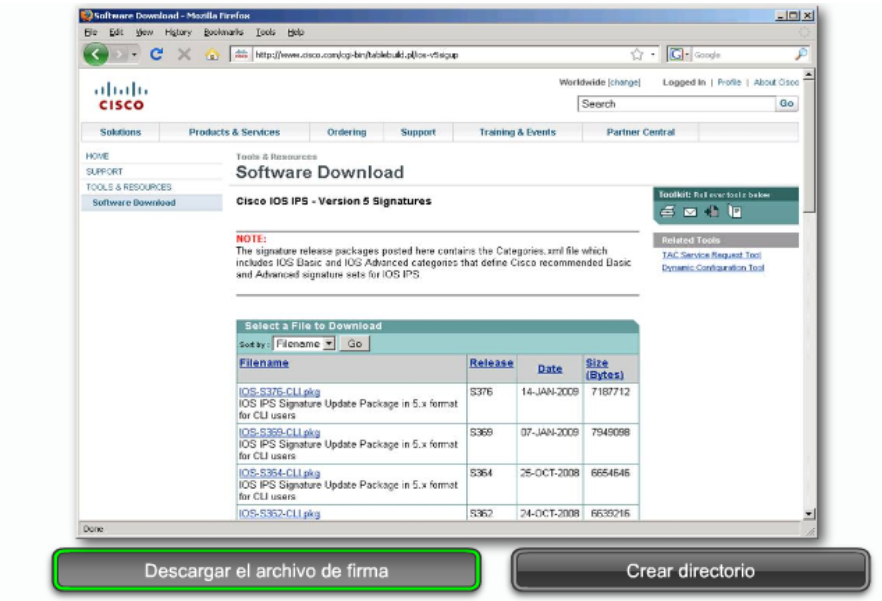
Paso 2. Creación de un directorio de configuración IPS IOS en la flash.

El segundo paso es crear un directorio en la flash para almacenar los archivos de firmas y configuraciones. Use el comando EXEC privilegiado mkdir nombre-directorio para crear el directorio.

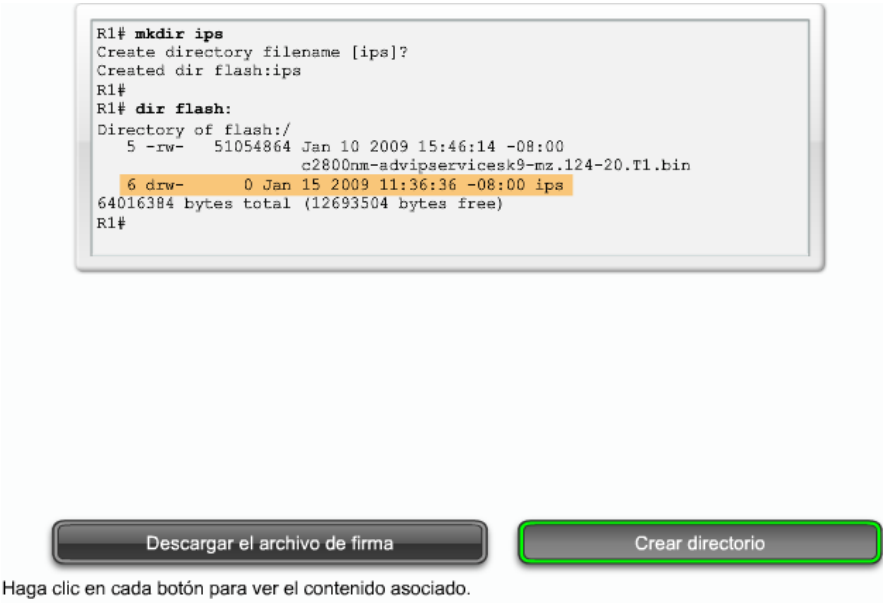
El IPS IOS soporta cualquier sistema de archivos del IOS de Cisco como ubicación de configuración con los accesos de escritura apropiados. Puede usarse un dispositivo USB conectado al puerto USB del router como ubicación alternativa para almacenar los archivos de firmas y configuraciones. El dispositivo USB debe permanecer conectado al puerto USB del router si se lo utiliza como ubicación del directorio de configuración del IPS IOS.

Otros comandos que resultan útiles incluyen rename nombre-actual nuevo-nombre. Esto permite al administrador cambiar el nombre del directorio.

Para verificar los contenidos de la flash, ingese el comando EXEC privilegiado dir flash:.



Haga clic en cada botón para ver el contenido asociado.



Haga clic en cada botón para ver el contenido asociado.

Paso 3. Configuración de una clave criptográfica IPS IOS.

A continuación, configure la clave criptográfica utilizada por el IPS IOS. Esta clave está ubicada en el archivo realm-cisco.pub.key.txt descargado en el Paso 1.

La clave criptográfica verifica la firma digital del archivo de configuración principal (sigdef-default.xml). El contenido del archivo está firmado con una clave privada de Cisco para garantizar su autenticidad e integridad.

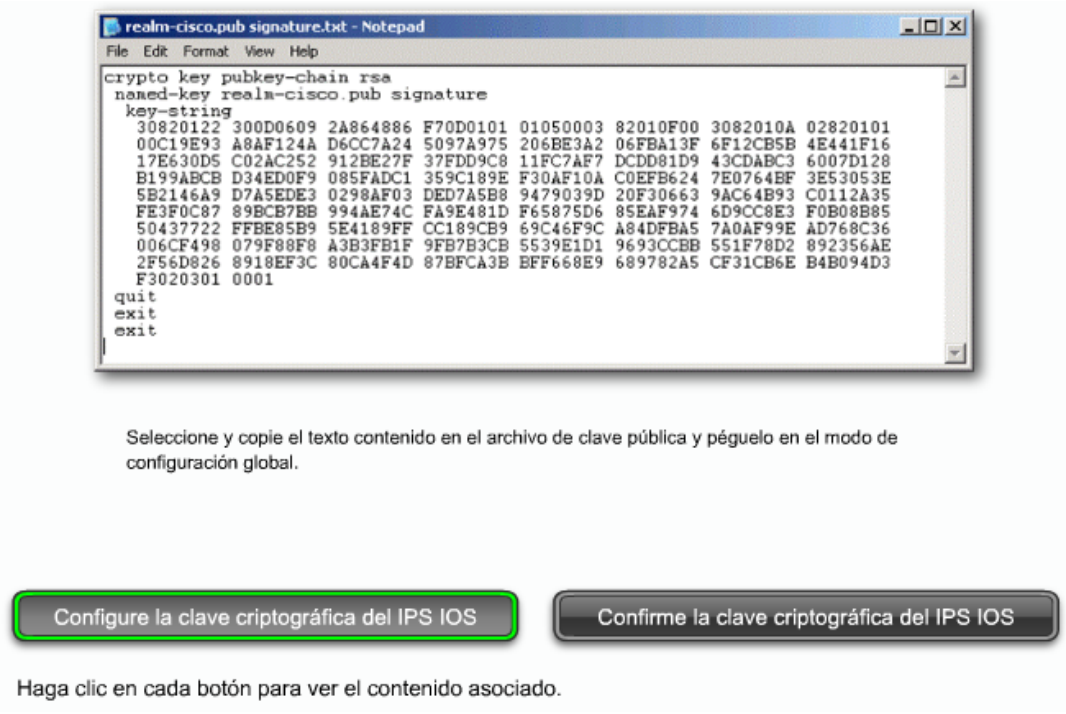
Para configurar la clave criptográfica del IPS IOS, abra el archivo de texto, copie sus contenidos y péguelos en el modo de configuración global. El archivo de texto emite los comandos para generar la clave RSA.

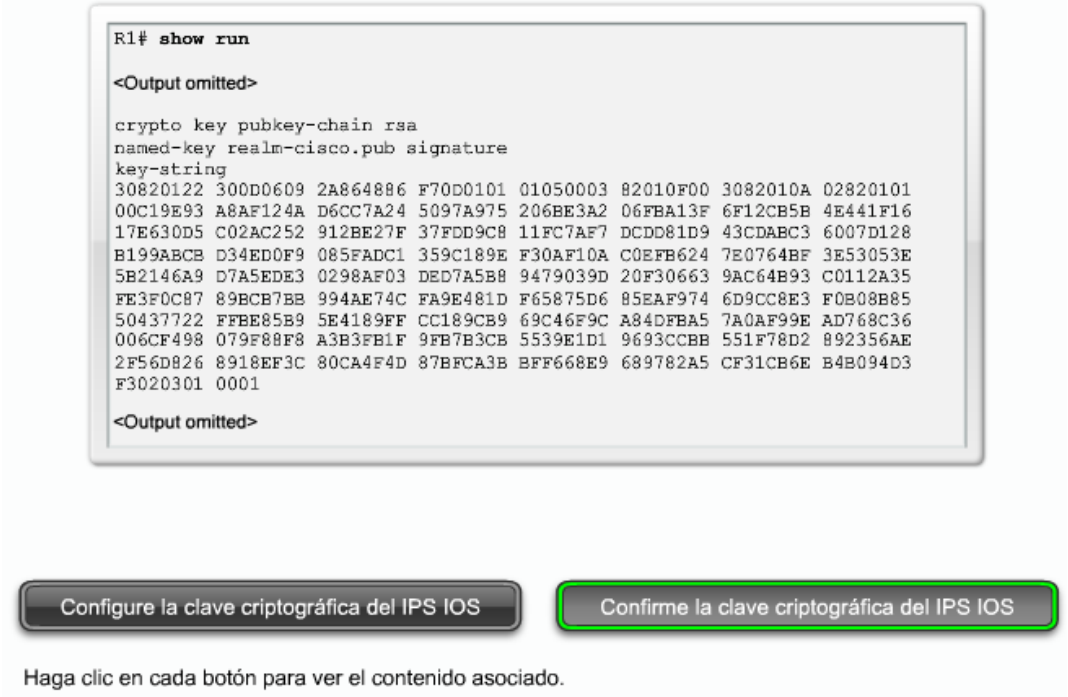
Cuando se compila la firma, se genera un mensaje de error si la clave criptográfica no es válida. Este es un ejemplo de un mensaje de error:

%IPS-3-INVALID_DIGITAL_SIGNATURE: Invalid Digital Signature found (key not found)

Si la clave está configurada incorrectamente, debe ser eliminada y reconfigurada. Use los comandos no crypto key pubkey-chain rsa y no named-key realm-cisco.pub signature para reconfigurar la clave.

Ingrese el comando show run en el prompt del router para confirmar que la clave criptográfica esté configurada.





Paso 4. Habilitar el IPS IOS.

El cuarto paso consiste en la configuración del IPS IOS, lo cual es un proceso que consta de varios pasos.

1) Identifique el nombre de la regla IPS y especifique la ubicación.

Use el comando ip ips name [nombre-regla] [ACL opcional] para crear un nombre para la regla. Opcionalmente, puede configurarse una lista de control de acceso (ACL) para filtrar el tráfico escaneado. Todo el tráfico que la ACL permite está sujeto a inspección por el IPS. El tráfico denegado por la ACL no es inspeccionado por el IPS.

Use el comando ip ips config location flash:nombre-directorio para configurar la ubicación del almacenamiento de la firma IPS. Antes del IOS 12.4(11)T, se usaba el comando ip ips sdf location.

2) Habilite la notificación de eventos de registro y SDEE.

Para usar SDEE, primero debe habilitarse el servidor HTTP con el comando ip http server. Si el servidor HTTP no está habilitado, el router no podrá responder a los clientes SDEE porque no podrá ver las solicitudes. Las notificaciones SDEE están deshabilitadas por defecto y deben ser habilitadas explícitamente. Use el comando ip ips notify sdee para habilitar la notificación de eventos SDEE IPS. El IPS IOS también soporta registros para enviar notificaciones de eventos. SDEE y la función de registro pueden ser usados independientemente o habilitados simultáneamente. El registro de notificaciones está habilitado por defecto. Si la consola de registro está habilitada, los mensajes de registro IPS serán mostrados en la consola. Use el comando ip ips notify log para habilitar el registro de notificaciones.

3) Configure la categoría de la firma.

Todas las firmas se agrupan en categorías jerárquicas, lo que ayuda a clasificarlas para agruparlas y ajustarlas más fácilmente. Las tres categorías más comunes son all, basic y advanced.

Las firmas utilizadas por el IPS IOS para escanear el tráfico pueden ser dadas de baja (retired) o reincorporadas (unretired). Dar de baja una firma significa que el IPS IOS no la compilará en la memoria para escanear. Reincorporarla implica instruir al IPS IOS para compilar la firma en la memoria y usarla para escanear el tráfico. Cuando se configura por primera vez el IPS IOS, todas las firmas de la categoría all deben ser dadas de baja y luego algunas selectas deben ser reincorporadas a una categoría que haga menos uso de la memoria. Para dar de baja y reincorporar las firmas, primero ingrese al modo de categoría de IPS con el comando ip ips signature-category. Luego, use el comando category nombre-categoría para cambiar la categoría. Por ejemplo, use el comando category all para ingresar el modo de acción de categoría all. Para dar de baja una categoría, use el comando retired true. Para reincorporar una categoría, use el comando retired false.

Advertencia: No reincorpore la categoría all. Esta categoría de firma contiene todas las firmas de la versión de firmas. El IPS IOS no puede compilar y usar todas las firmas de una vez, porque esto agotaría su memoria.

El orden en el cual las categorías de firmas se configuran en el router también es importante. El IPS IOS procesa los comandos de categoría en el orden listado en la configuración. Algunas firmas pertenecen a múltiples categorías. Si se configuran varias categorias y una firma pertenece a más de una de ellas, el IPS IOS usa las propiedades de la firma en la categoría que se configuró por último, por ejemplo, dada de baja, reincorporada o acciones.

4) Aplique la regla IPS a una interfaz deseada y especifique la dirección.

Use el comando de configuración de interfaz ip ips nombre-regla [in | out] para aplicar la regla IPS. El argumento in significa que solo el tráfico que ingresa a la interfaz será inspeccionado por el IPS. El argumento out especifica que solo el tráfico que sale de la interfaz será inspeccionado por el IPS.

```
R1(config)# ip ips name iosips
R1(config)# ip ips name ips list ?
<1-199> Numbered access list
WORD Named access list
R1(config)#
R1(config)# ip ips config location flash:ips
R1(config)#
```

- Se crea la regla `iosips`.
- Se identifica la ubicación del IPS en flash como `flash:ips`.

Crear la regla IPS y la ubicación del archivo IPS | Habilitar notificaciones de eventos de registro y SDEE | Configurar las categorías de firmas | Asignar la regla IPS a una interfaz

Haga clic en cada botón para ver el contenido asociado.

```
R1(config)# ip http server
R1(config)# ip ips notify sdee
R1(config)# ip ips notify log
R1(config)#
```

Las notificaciones de eventos de registro y SDEE están habilitados.

Crear la regla IPS y la ubicación del archivo IPS | Habilitar notificaciones de eventos de registro y SDEE | Configurar las categorías de firmas | Asignar la regla IPS a una interfaz

Haga clic en cada botón para ver el contenido asociado.

```
R1(config)# ip ips signature-category
R1(config-ips-category)# category all
R1(config-ips-category-action)# retired true
R1(config-ips-category-action)# exit
R1(config-ips-category)#
R1(config-ips-category)# category ios_ips basic
R1(config-ips-category-action)# retired false
R1(config-ips-category-action)# exit
R1(config-ips-category)# exit
Do you want to accept these changes? [confirm] y
R1(config)#
```

- La categoría IPS **all** ha sido dada de baja.
- La categoría IPS **basic** ha sido reincorporada.



Haga clic en cada botón para ver el contenido asociado.

```
R1(config)# interface GigabitEthernet 0/0
R1(config-if)# ip ips iosips in
R1(config-if)# exit
R1(config)# exit
```

- Se aplica la regla IPS en dirección de entrada.

```
R1(config)# interface GigabitEthernet 0/1
R1(config-if)# ip ips iosips in
R1(config-if)# ip ips iosips out
R1(config-if)# exit
R1(config)# exit
```

- Se aplica la regla IPS en las direcciones de entrada y salida.



Haga clic en cada botón para ver el contenido asociado.

Paso 5. Cargar el paquete de firmas IPS IOS en el router.

El último paso consiste en que el administrador suba el paquete de firmas al router. El método más común utilizado es FTP o TFTP. Para copiar el paquete de firmas descargado desde el servidor FTP hacia el router, asegúrese de usar el parámetro idconf al final del comando.

copy ftp://ftp_user:contraseña@dirección_IP_servidor/paquete_firmas idconf

Para verificar que el paquete de firmas esté compilado apropiadamente, el administrador utiliza el comando show ip ips signature count.

```
R1# copy ftp://cisco:cisco@10.1.1.1/IOS-S376-CLI.pkg idconf
Loading IOS-S310-CLI.pkg !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 7608873/4096 bytes]
*Jan 15 16:44:47 PST: %IPS-6-ENGINE_BUILDS_STARTED: 16:44:47 PST Jan 15 2008
*Jan 15 16:44:47 PST: %IPS-6-ENGINE_BUILDING: multi-string - 8 signatures - 1 of
                      13 engines
*Jan 15 16:44:47 PST: %IPS-6-ENGINE_READY: multi-string - build time 4 ms -
                      packets for this engine will be scanned
*Jan 15 16:44:47 PST: %IPS-6-ENGINE_BUILDING: service-http - 622 signatures - 2
                      of 13 engines
*Jan 15 16:44:53 PST: %IPS-6-ENGINE_READY: service-http - build time 6024 ms -
                      packets for this engine will be scanned


*Jan 15 16:45:18 PST: %IPS-6-ENGINE_BUILDING: service-smb-advanced - 35
                      signatures - 12 of 13 engines
*Jan 15 16:45:18 PST: %IPS-6-ENGINE_READY: service-smb-advanced - build time 16
                      ms - packets for this engine will be scanned
*Jan 15 16:45:18 PST: %IPS-6-ENGINE_BUILDING: service-msrpc - 25 signatures - 13
                      of 13 engines
*Jan 15 16:45:18 PST: %IPS-6-ENGINE_READY: service-msrpc - build time 32 ms -
                      packets for this engine will be scanned
*Jan 15 16:45:18 PST: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 31628 ms
```

Copiar las firmas del servidor FTP.

Copiar la firma | Verificar la firma

Haga clic en cada botón para ver el contenido asociado.

```
R1# show ip ips signature count
Cisco SDF release version S310.0 ← signature package release version
Trend SDF release version V0.0
Signature Micro-Engine: multi-string: Total Signatures 8
multi-string enabled signatures: 8
multi-string retired signatures: 8



Signature Micro-Engine: service-msrpc: Total Signatures 25
service-msrpc enabled signatures: 25
service-msrpc retired signatures: 18
service-msrpc compiled signatures: 1
service-msrpc inactive signatures - invalid params: 6
Total Signatures: 2136
Total Enabled Signatures: 807
Total Retired Signatures: 1779
Total Compiled Signatures:
      351 ← total compiled signatures for the IOS IPS Basic category
Total Signatures with invalid parameters: 6
Total Obsoleted Signatures: 11
R1#
```

Copiar la firma | Verificar la firma

Haga clic en cada botón para ver el contenido asociado.

5.3.2 Configuracion del IPS IOS Cisco con el SDM

El SDM de Cisco proporciona controles para la aplicación del IPS IOS de Cisco en las interfaces, la importación y edición de archivos de firmas de Cisco.com y la configuración de la acción que el IPS IOS de CIsco tomará si la amenaza es detectada. Las tareas de administración de los routers y dispositivos de seguridad están

desplegadas en un panel de tareas en el lado izquierdo de la página de inicio del SDM de Cisco. Vaya a Configure > Intrusion Prevention para visualizar las opciones de prevención de intrusos en el SDM de Cisco.

Java requiere un mínimo de memoria heap de 256 MB en la computadora host del SDM para configurar el IPS IOS con el SDM. Si se genera un error cuando se selecciona el botón Launch IPS Rule Wizard, debe cambiarse el tamaño de memoria heap para Java en la computadora host. Para esto, salga del SDM de Cisco y abra el panel de control de Windows. Haga clic en la opción Java, que abrirá el panel de control de Java. Seleccione la pestaña Java y haga clic en el botón View bajo las Java Applet Runtime Settings. En el campo Java Runtime Parameter ingrese -Xmx256m exactamente y haga clic en OK.

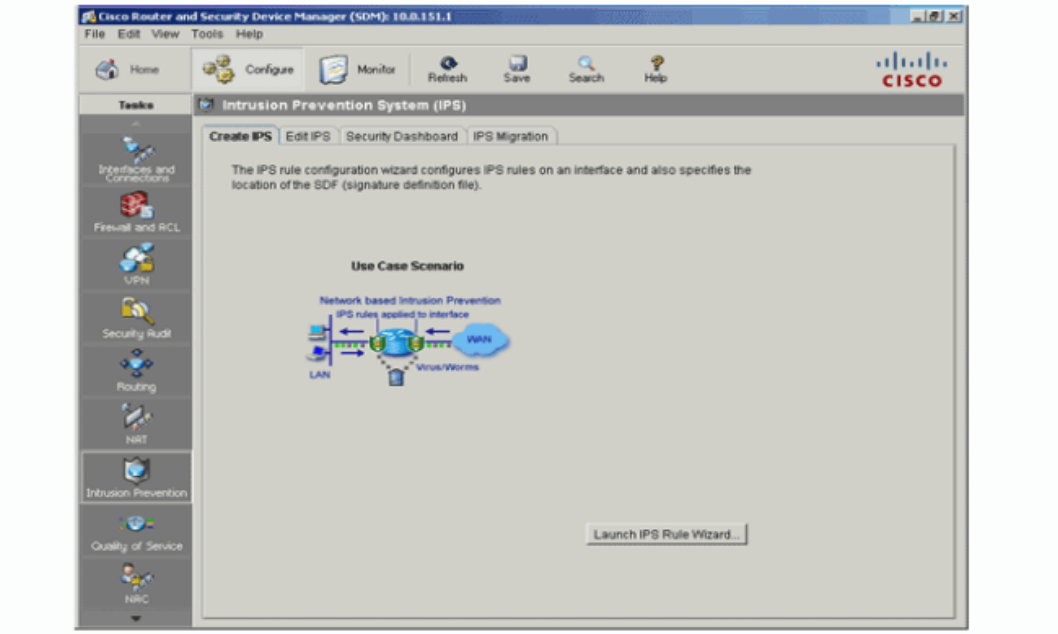
Con el tamaño de memoria heap de Java correctamente configurado, el SDM muestra cuatro pestañas en la ventana del Intrusion Prevention Systems (IPS). Use las pestañas en la parte superior de la ventana IPS para configurar o monitorear el IPS.

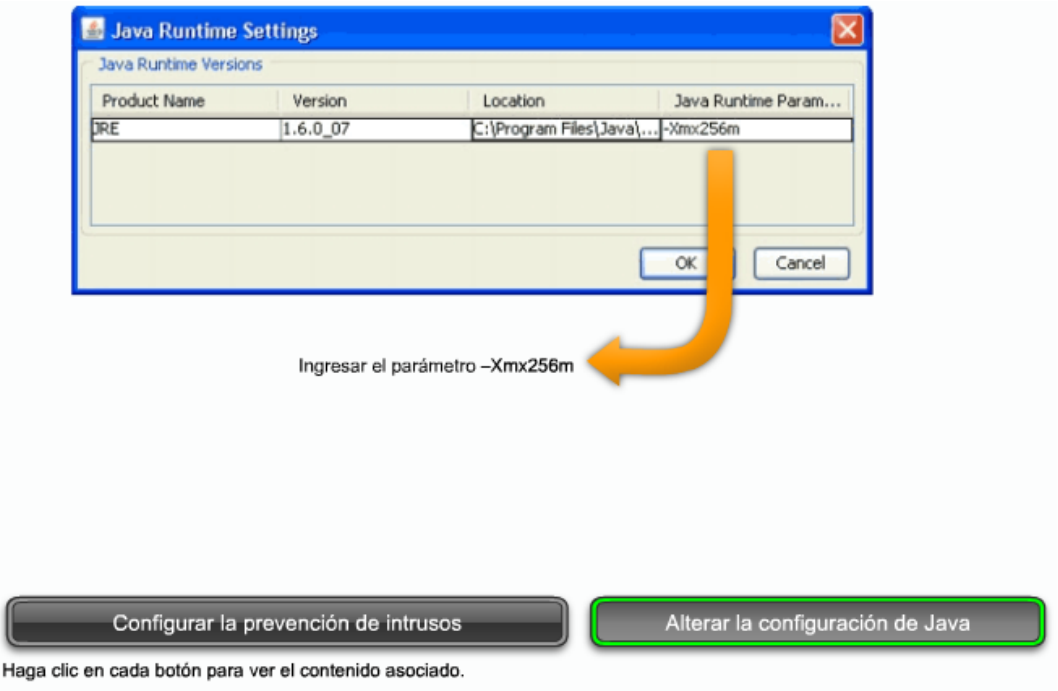
Create IPS - Contiene el asistente de IPS Rule que puede ser utilizado para crear una nueva regla de IPS IOS de Cisco.
Edit IPS - Edita las reglas IPS IOS de Cisco y las aplica o elimina de las interfaces.
Security Dashboard - Para ver la tabla de Top Threats y desplegar firmas asociadas con ellas.
IPS Migration - Para migrar las configuraciones IPS IOS de Cisco que fueron creadas con versiones anteriores del software IOS de Cisco. La migración IPS no está disponible en versiones anteriores a la versión 12.4(11)T.

Las primeras tres pestañas son útiles en la creación y los ajustes de los IPS. La pestaña referida a la migración de IPS está disponible cuando el router ejecuta un IOS de Cisco versión 12.4(11)T o posterior. Debe ser utilizada para convertir archivos de firma personalizados o modificados de la versión 4.x a la versión 5.x antes de implementar el IPS.

El administrador puede usar SDM para crear una nueva regla en un router Cisco tanto manualmente usando la pestaña Edit IPS o automáticamente usando el asistente IPS Rule.

La guía de despliegue del IPS IOS de Cisco recomienda usar el asistente IPS Rule. El asistente no solo configura la regla, sino que también lleva a cabo todos los pasos de la configuración del IPS IOS de Cisco.





La configuración del IPS IOS de Cisco en un router o dispositivo de seguridad con el SDM de Cisco involucra varios pasos.

Paso 1. Vaya a Configure > Intrusion Prevention > Create IPS.

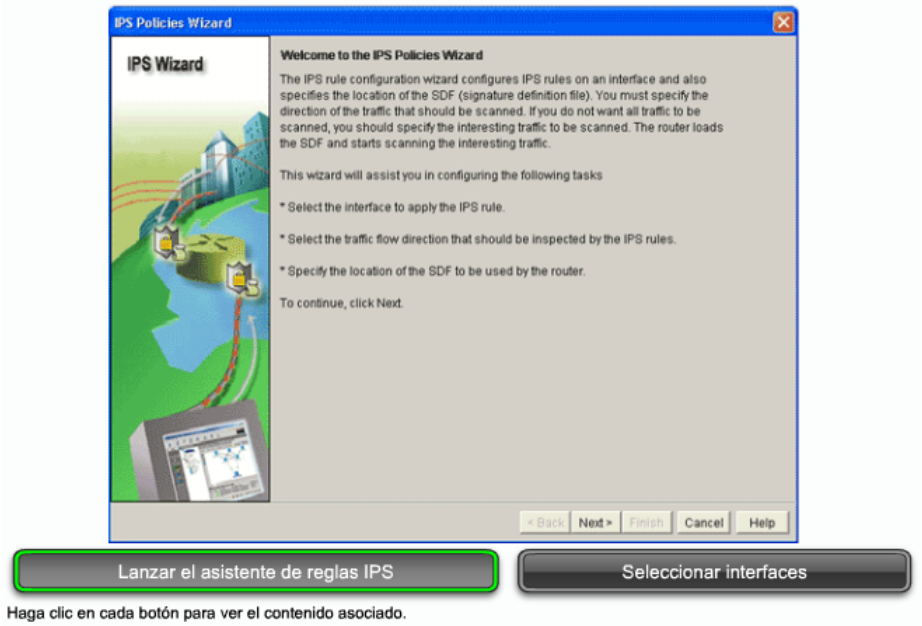
Paso 2. Haga clic en el botón Launch IPS Rule Wizard.

Paso 3. Lea la pantalla Welcome to the IPS Policies Wizard y haga clic en Next.

Identifique las interfaces a las que se aplicará el IPS IOS de Cisco. Decida si se deberá aplicar la regla al tráfico de entrada o al de salida. Si se marcan ambas casillas (la de entrada y la de salida), se aplicará la regla al tráfico que fluya en cualquiera de las dos direcciones.

Paso 4. En la ventana Select Interfaces, elija las interfaces en las que se aplicará la regla IPS y la dirección del tráfico marcando una o ambas casillas.

Paso 5. Haga clic en Next.



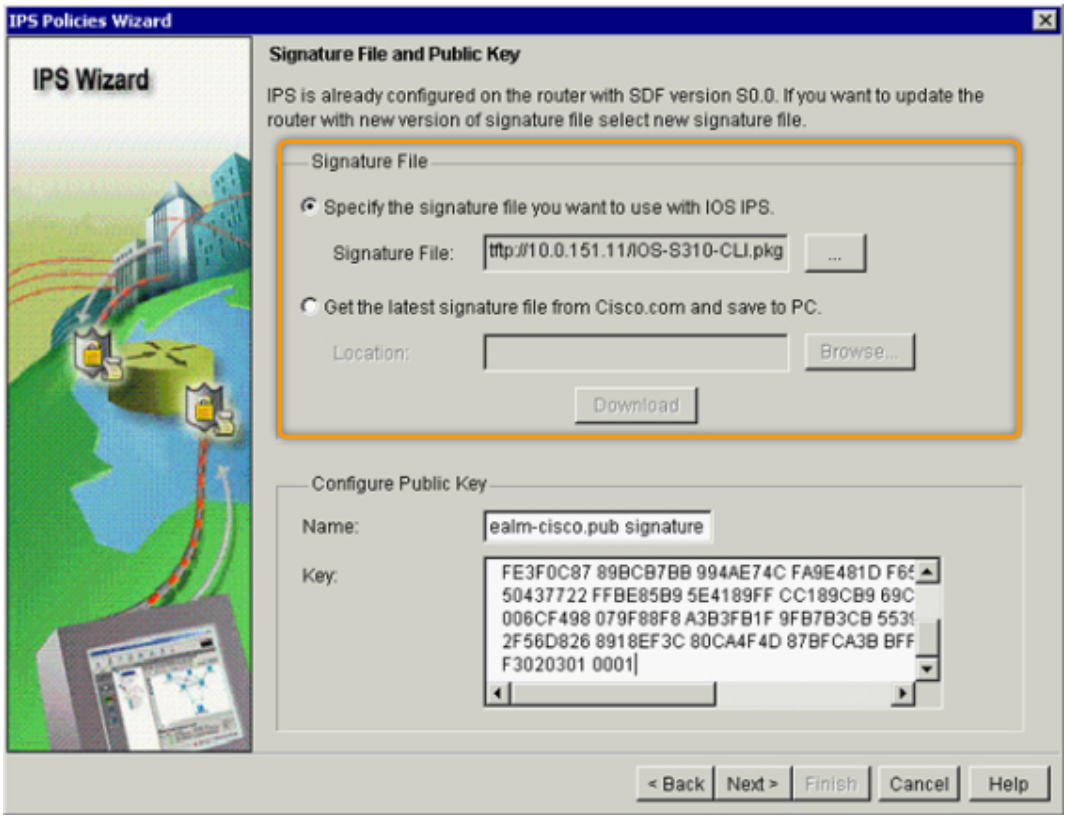


El IPS IOS de Cisco compara el tráfico con las firmas contenidas en el archivo de firmas, que puede estar ubicado en la memoria flash del router o en un sistema remoto que el router puede alcanzar. Pueden especificarse múltiples ubicaciones de archivos de firmas para que, si el router no puede entrar en contacto con la primera ubicación, pueda intentar entrar en contacto con otras ubicaciones hasta obtener un archivo de firmas.

Paso 6. En el panel Signature File en la ventana Signature File and Public Key, seleccione una de las dos opciones: Specify the signature file you want to use with the IOS IPS (especificar el archivo de firmas que quiere usar con el IPS IOS) o Get the latest signature file from Cisco.com and save to PC (obtener el archivo de firmas más reciente de Cisco.com y guardarlo en la PC) y llene la casilla de texto apropiada. El archivo de firmas es un paquete de actualización del IPS IOS cuyo nombre sigue la convención IOS-Snnn-CLI.pkg, en la que nnn es el número del grupo de firmas.

Paso 7. Para descargar el archivo de firmas más reciente de Cisco.com, haga clic en Download.

El archivo de firmas del IPS IOS de Cisco contiene información de firmas por defecto. Cualquier cambio efectuado a esta configuración no será guardado en el archivo de firmas sino en un archivo especial llamado archivo delta. El archivo delta se guarda en la memoria flash del router. Para mayor seguridad, el archivo delta debe estar firmado digitalmente con una clave que también se obtiene de Cisco.com.



Ubique la información de la clave pública en los campos Name y Key.

Paso 8. Obtenga su clave pública en http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup.

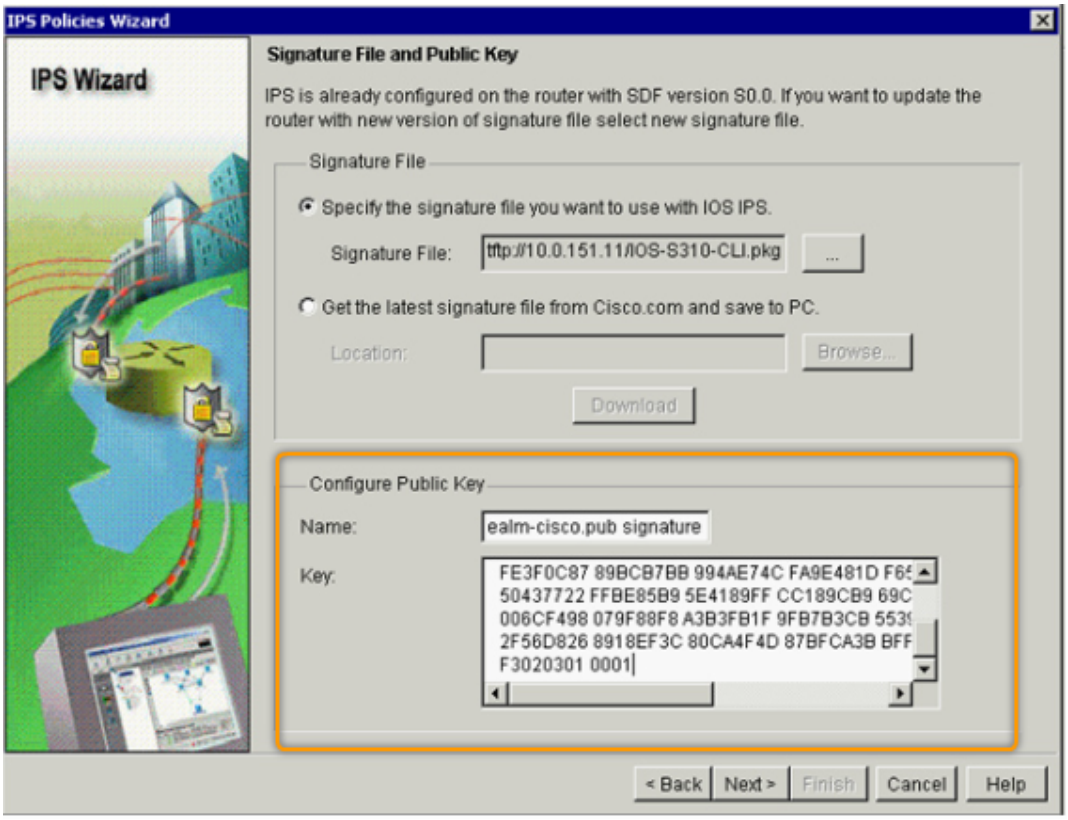
Paso 9. Descargue la clave en una PC.

Paso 10. Abra el archivo de la clave en un editor de texto y copie el texto luego de la frase "named-key" en el campo Name. Por ejemplo, si la línea de texto es "named-key realm-cisco.pub signature", copie "realm-cisco.pub signature" en el campo Name.

Paso 11. Copie el texto entre la frase "key-string" y la palabra "quit" en el campo Key. El texto puede tener el siguiente aspecto:

30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101 00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16 17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128 B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E 5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35 FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85 50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36 006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE 2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3 F3020301 0001

Paso 12. Haga clic en Next.



A partir de la versión 12.4(11) del IOS de Cisco, pueden especificarse la ubicación de almacenamiento de la información de firma y la categoría de tipo de firma.

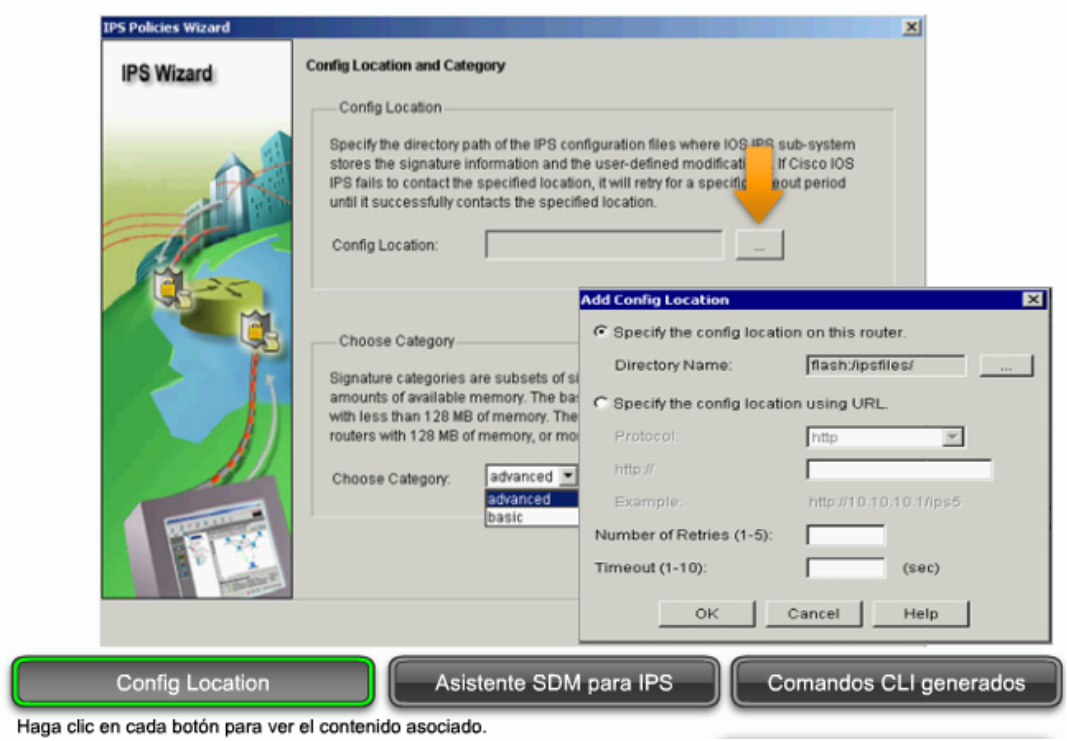
Paso 13. En la ventana Config Location and Category, en la sección Config Location, haga clic en el botón de elipsis (...) al lado del campo Config Location para especificar dónde deben almacenarse los archivos de firmas XML, incluyendo el archivo delta que se crea cuando se efectúan cambios en el archivo de firmas.

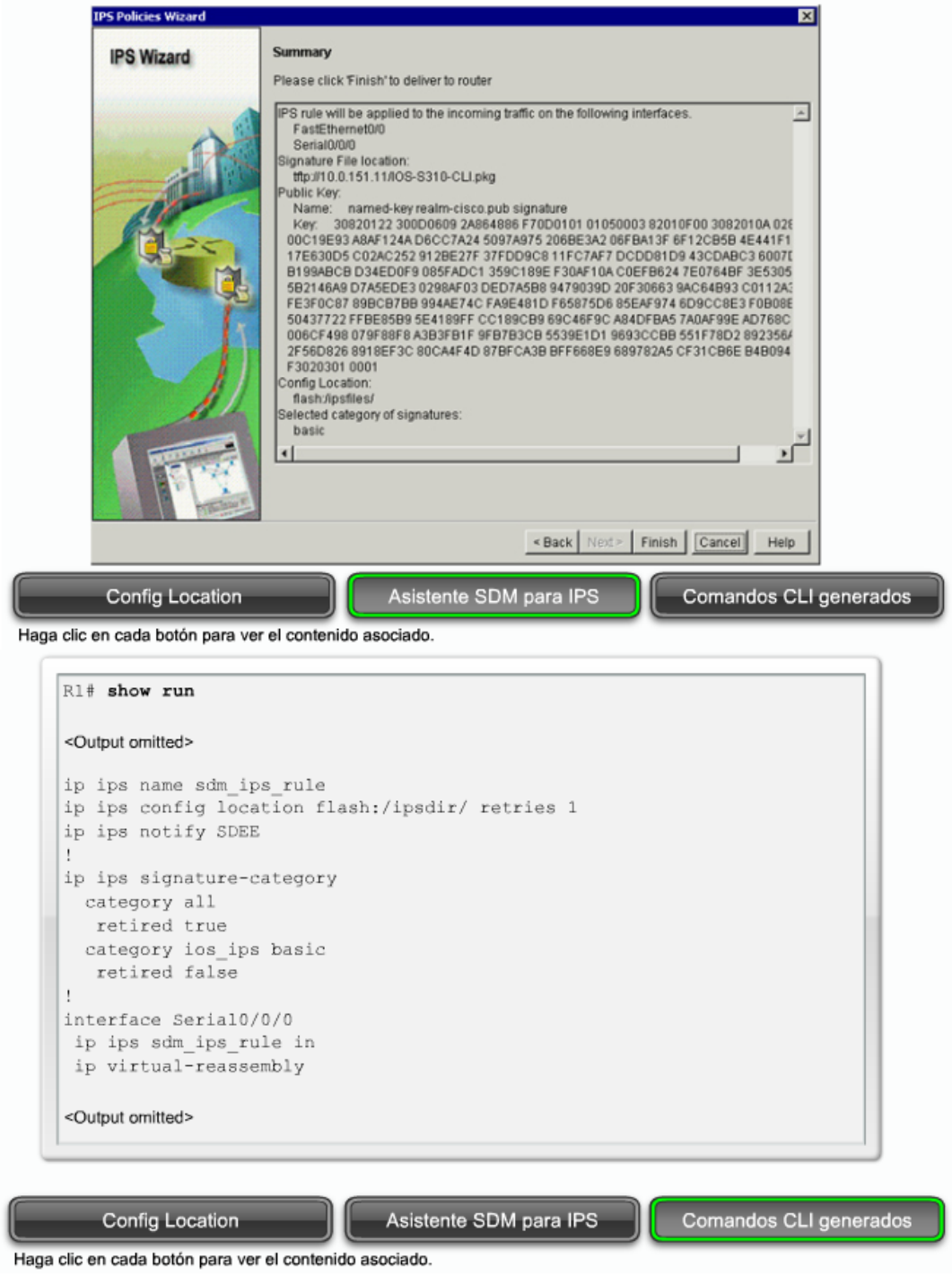
Paso 14. Como la memoria del router y las restricciones de recursos pueden limitar el uso de todas las firmas disponibles, elija una categoría en el campo Choose Category que permita al IPS IOS de Cisco funcionar con eficiencia en el router. La categoría de firmas basic es apropiada para los routers que constan de menos de 128 MB de memoria flash, mientras que la categoría de firma advanced es apropiada para los routers de más de 128 MB de memoria flash.

Paso 15. Haga clic en Finish. El IPS Policies Wizard confirma la información configurada en una pantalla de resumen.

Use el comando show running-config para verificar la configuración IPS generada por el SDM IPS Wizard.

Virtual Fragment Reassembly (VFR) permite al firewall IOS de Cisco crear las ACLs dinámicas apropiadas, protegiendo a la red contra varios ataques de fragmentación. Para habilitar VFR en una interfaz, use el comando ip virtual-reassembly en el modo de configuración de interfaz.





5.3.3 Modificacion de las firmas IPS IOS de Cisco

La CLI del IOS de Cisco puede ser usada para dar de baja o reincorporar firmas individuales o un grupo de firmas que pertenezca a la misma categoría de firmas. Cuando un grupo de firmas se da de baja o reincorpora, todas las firmas en esa categoría son dadas de baja o reincorporadas.

Algunas firmas reincorporadas (tanto reincorporadas individualmente como dentro de una categoría) pueden no compilar por memoria insuficiente, parámetros no válidos o si la firma está obsoleta.

```
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# ip ips signature-definition
R1(config-sigdef)# signature 6130 10
R1(config-sigdef-sig)# status
R1(config-sigdef-sig-status)# retired true
R1(config-sigdef-sig-status)# exit
R1(config-sigdef-sig)# exit
R1(config-sigdef)# exit
Do you want to accept these changes? [confirm] y
R1(config)#
```

Este ejemplo muestra cómo retirar firmas individuales, en este caso, la firma 6130 con el ID subsig 10.

Dando de baja una firma en forma individual | Reincorporando una categoría de firmas

Haga clic en cada botón para ver el contenido asociado.

```
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# ip ips signature-category
R1(config-ips-category)# category ios_ips basic
R1(config-ips-category-action)# retired false
R1(config-ips-category-action)# exit
R1(config-ips-category)# exit
Do you want to accept these changes? [confirm] y
R1(config)#
```

Este ejemplo muestra cómo reincorporar todas las firmas que pertenecen a la categoría Basic del IOS IPS.

Dando de baja una firma en forma individual | Reincorporando una categoría de firmas

Haga clic en cada botón para ver el contenido asociado.

La CLI del IOS de Cisco también puede usarse para cambiar las acciones de firma de una firma o un grupo de ellas basándose en las categorías. Para cambiar una acción, debe usar el comando event-action en el modo IPS Category Action mode o el Signature Definition Engine.

El comando event-action tiene varios parámetros, incluyendo produce-alert, deny-packet-inline y reset-tcp-connection.

```
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# ip ips signature-definition
R1(config-sigdef)# signature 6130 10
R1(config-sigdef-sig)# engine
R1(config-sigdef-sig-engine)# event-action produce-alert
R1(config-sigdef-sig-engine)# event-action deny-packet-inline
R1(config-sigdef-sig-engine)# event-action reset-tcp-connection
R1(config-sigdef-sig-engine)# exit
R1(config-sigdef-sig)# exit
R1(config-sigdef)# exit
Do you want to accept these changes? [confirm] y
R1(config)#
```

Este ejemplo muestra cómo cambiar las acciones de firma a alertar, descartar y reiniciar en la firma 6130 con un ID subsig 10.

Cambiar acciones de la firma | Cambiar acciones de la categoría

Haga clic sobre cada botón para ver el contenido asociado.

```
R1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)# ip ips signature-definition
R1(config-ips-category)# category ios_ips basic
R1(config-ips-category-action)# event-action produce-alert
R1(config-ips-category-action)# event-action deny-packet-inline
R1(config-ips-category-action)# event-action reset-tcp-connection
R1(config-ips-category-action)# exit
R1(config-ips-category)# exit

Do you want to accept these changes? [confirm] y
R1(config)#
```

Este ejemplo muestra cómo cambiar las acciones de todas las firmas que pertenecen a la categoría Basic del IPS IOS.

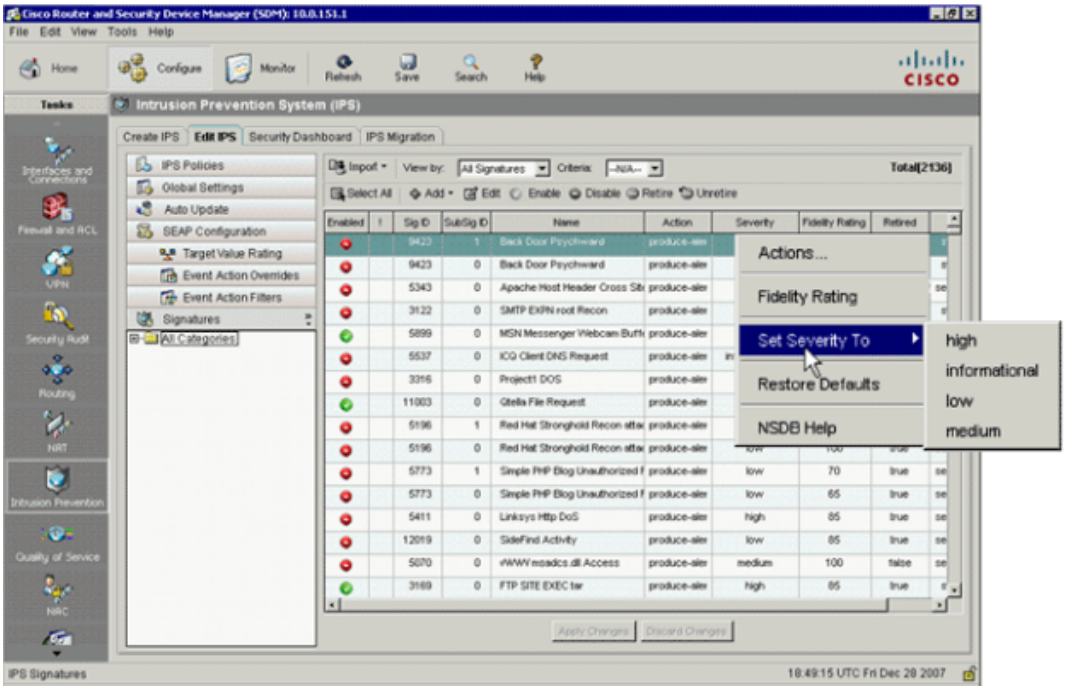
Cambiar acciones de la firma | Cambiar acciones de la categoría

Haga clic sobre cada botón para ver el contenido asociado.

Las firmas IPS se cargan como parte del procedimiento para crear una regla IPS IOS de Cisco usando el asistente IPS Rule. Para ver las firmas configuradas en el router, vaya a Configure > Intrusion Prevention > Edit IPS > Signatures > All Categories. Como las firmas optimizan la configuración, confirme que todas las firmas correctas están cargadas en el router o dispositivo de seguridad. Desde esta ventana, los

administradores pueden agregar firmas personailzadas o importar firmas descargadas desde Cisco.com. También pueden editar, eliminar, habilitar y deshabilitar firmas.

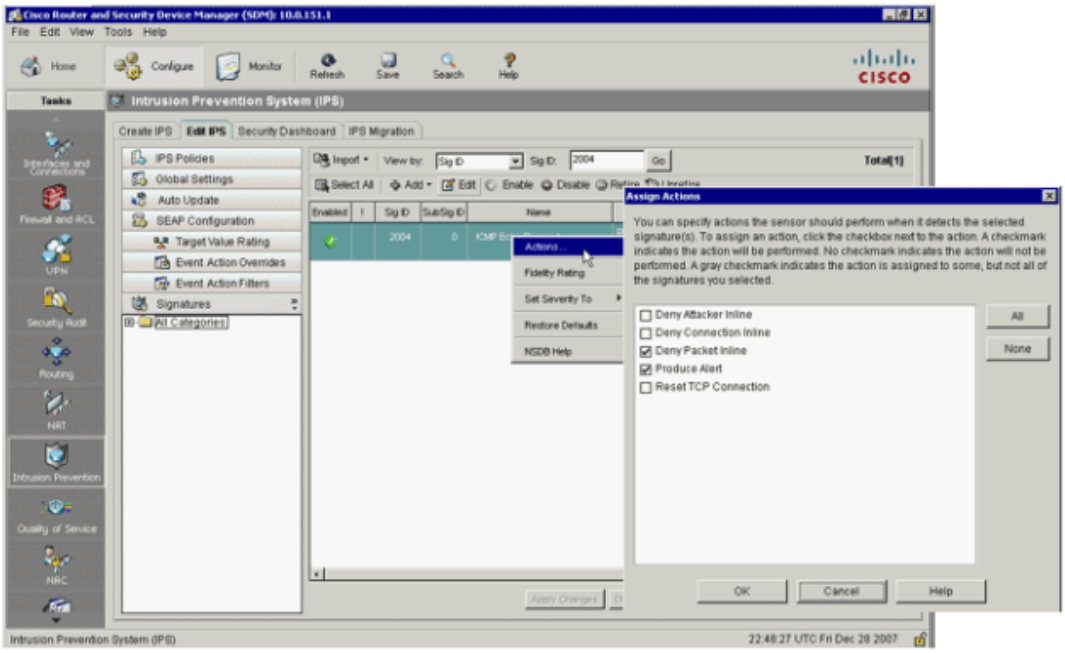
El árbol de firmas permite al administrador filtrar la lista de firmas de acuerdo con el tipo que quiere visualizar. Para modificar una firma, haga clic derecho sobre ella y elija una opción del menú contextual. Para cambiar la severidad de la firma, vaya a Set Severity To.



El SDM de Cisco puede ser usado para ajustar una configuración de firma. Para ajustar una firma, vaya a Configure > Intrusion Prevention > Edit IPS > Signatures > All Categories. Aparecerá una lista de las firmas disponibles.

Para modificar una acción de firma, haga clic derecho sobre ella y elija Actions en el menú contextual. Aparecerá la ventana Assign Actions. Las acciones disponibles dependen de la firma, pero las siguientes son las más comunes:

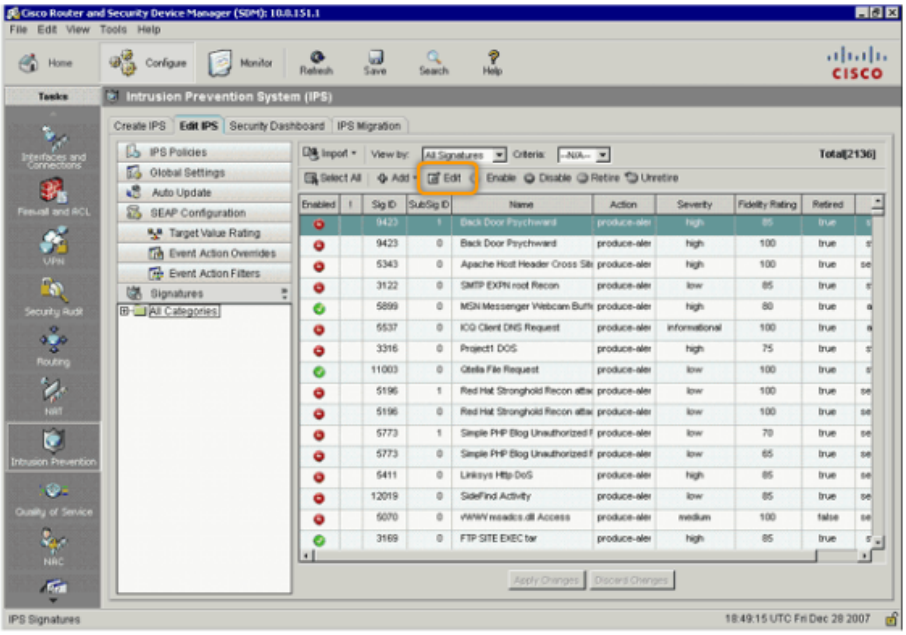
Deny Attacker Inline - Crear una ACL que deniega todo el tráfico proveniente de la dirección IP considerada origen del ataque por el sistema IPS IOS de Cisco.
Deny Connection Inline - Descartar el paquete y todos los paquetes futuros de este flujo TCP.
Deny Packet Inline - No transmitir este paquete (solo en línea).
Produce Alert - Generar un mensaje de alarma.
Reset TCP Connection - Envía TCP resets para terminar el flujo TCP.



Para acceder a y configurar parámetros de firma, seleccione la firma y luego haga clic en el botón Edit en la ventana Intrusion Prevention System (IPS).

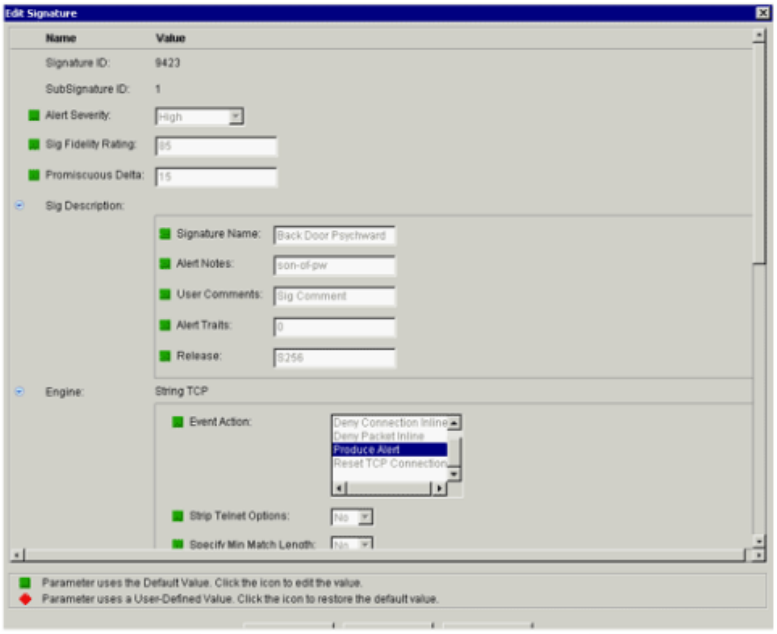
Las firmas tienen diferentes parámetros:

Signature ID - Muestra el valor numérico único asignado a esta firma. Este valor permite al IPS IOS de Cisco identificar una firma en particular.
SubSignature ID - Muestra el valor numérico único asignado a esta subfirma. El ID de subfirma identifica una versión más granular de una firma general.
Alert Severity - Muestra la severidad de la alerta de esta firma.
Sig Fidelity Rating - Muestra el nivel de confianza en la detección de un positivo real.
Promiscuous Delta - Muestra el valor usado para determinar la seriedad de la alerta. No se recomienda cambiar la configuración de delta promiscuo.
Sig Description - Incluye el nombre de la firma, las notas de la alerta, los comentarios de los usuarios, los rasgos de la alerta y el número de versión.
Engine - Contiene información sobre el motor que la firma usa y sus características operativas.
Event Counter - Muestra el contador de eventos, la clave del contador de eventos y si debe especificarse un intervalo de alerta. El intervalo de alerta permite al administrador definir un tratamiento especial para los eventos cronometrados.
Alert Frequency - Configuración que define la frecuencia de la alerta.
Status - Muestra si la firma está habilitada o dada de baja.



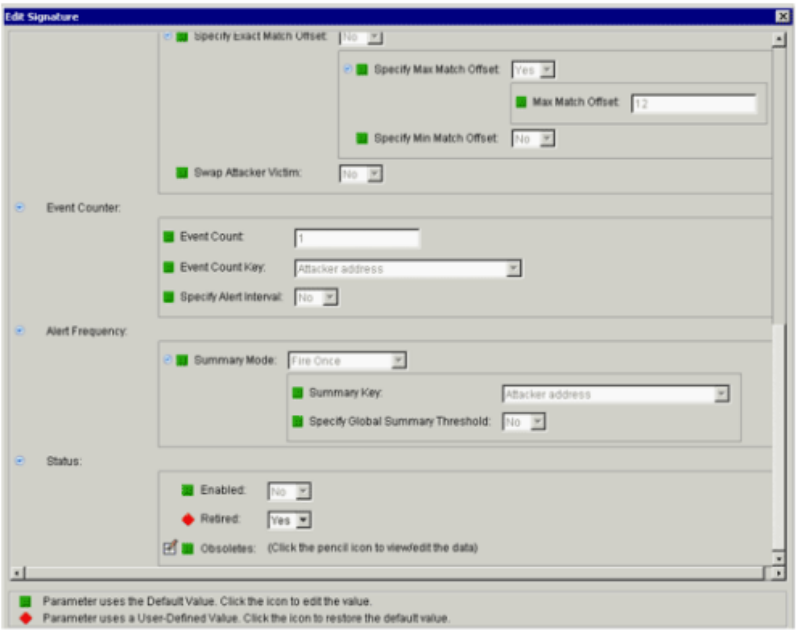
Editar la firma | Parámetros de firma - 1 | Parámetros de firma - 2

Haga clic en cada botón para ver el contenido asociado.



Editar la firma | Parámetros de firma - 1 | Parámetros de firma - 2

Haga clic en cada botón para ver el contenido asociado.



5.4.1 Verificacion del IPS IOS de Cisco

Luego de implementar el IPS, es necesario verificar la configuración para garantizar una correcta operación. Pueden usarse diversos comandos show para verificar la configuración del IPS IOS.

El comando de modo EXEC privilegiado show ip ips puede ser usado con otros parámetros para proporcionar información IPS específica.

El comando show ip ips all muestra todos los datos de configuración IPS. La salida de este comando puede ser extensa, dependiendo de la configuración del IPS.
El comando show ip ips configuration muestra datos de configuración adicionales que no se muestran en la salida del comando show running-config.
El comando show ip ips interfaces muestra datos de la configuración de interfaces. La salida de este comando muestra reglas de entrada y salida aplicadas a interfaces específicas.

El comando show ip ips signatures verifica la configuración de firmas. Este comando también puede ser utilizado con la palabra clave detail para obtener una salida más específica.
El comando show ip ips statistics muestra el número de paquetes auditados y el número de alarmas enviadas. La palabra clave opcional reset reinicia la salida para reflejar las estadísticas más recientes.

Use el comando clear ip ips configuration para deshabilitar IPS, eliminar todas las entradas de configuración IPS y liberar los recursos dinámicamente. El comando clear ip ips statistics reinicia las estadísticas sobre los paquetes analizados y las alarmas enviadas.

```
R1# show ip ips all
IPS Signature File Configuration Status
    Configured Config Locations: flash:/ipsdir/
    Last signature default load time: 04:39:33 UTC Jan 15 2009
    Last signature delta load time: -none-
    Last event action (SEAP) load time: -none-

    General SEAP Config:
    Global Deny Timeout: 3600 seconds
    Global Overrides Status: Enabled
    Global Filters Status: Enabled

IPS Auto Update is not currently configured

IPS Syslog and SDEE Notification Status
    Event notification through syslog is enabled
    Event notification through SDEE is enabled

IPS Signature Status
    Total Active Signatures: 693
    Total Inactive Signatures: 1443

IPS Packet Scanning and Interface Status
    IPS Rule Configuration
      IPS name myips
    IPS fail closed is disabled
    IPS deny-action ips-interface is false
    Fastpath ips is enabled
    Quick run mode is enabled
    Interface Configuration
      Interface FastEthernet0/1
        Inbound IPS rule is not set
        Outgoing IPS rule is myips

IPS Category CLI is not configured
```

show ip ips all | show ip ips configuration | show ip ips interfaces | show ip ips signatures | show ip ips statistics

Haga clic en cada botón para ver el contenido asociado.

```
R1# show ip ips configuration
Event notification through syslog is enabled
Event notification through Net Director is enabled
Default action(s) for info signatures is alarm
Default action(s) for attack signatures is alarm
Default threshold of recipients for spam signature is 25
PostOffice:HostID:5 OrgID:100 Addr:10.2.7.3 Msg dropped:0
HID:1000 OID:100 S:218 A:3 H:14092 HA:7118 DA:0 R:0
    CID:1 IP:172.21.160.20 P:45000 S:ESTAB (Curr Conn)
Audit Rule Configuration
 Audit name AUDIT.1
    info actions alarm

<Output omitted>
```

show ip ips all | show ip ips configuration | show ip ips interfaces | show ip ips signatures | show ip ips statistics

Haga clic en cada botón para ver el contenido asociado.

```
R1# show ip ips interfaces
Interface Configuration
      Interface FastEthernet0/0
        Inbound IPS rule is sdm_ips_rule
        Outgoing IPS rule is not set
      Interface FastEthernet0/1
        Inbound IPS rule is sdm_ips_rule
        Outgoing IPS rule is not set
R1#
```

show ip ips all | show ip ips configuration | show ip ips interfaces | show ip ips signatures | show ip ips statistics

Haga clic en cada botón para ver el contenido asociado.

```
R1# show ip ips signature | include 5000
SigID:SubID   On   Action   Sev   Trait   MH   AI   CT   TI   AT FA  WF Version
-----------   --   ------   ---   -----   --   --   --   --   -----  ----------

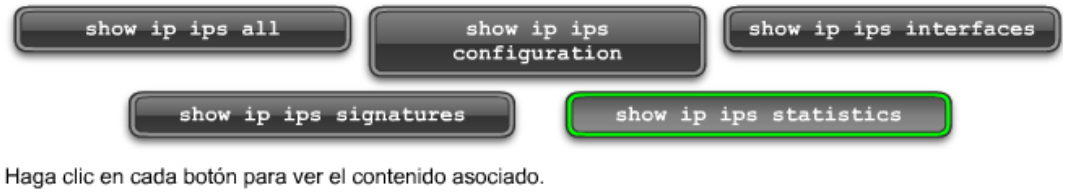
50000:0       N    A        HIGH  0       0    0    0    0    FA  N   OPACL
50000:1       N    A        HIGH  0       0    0    0    0    FA  N   OPACL
50000:2       N    A        HIGH  0       0    0    0    0    FA  N   OPACL

R1#
```



Haga clic en cada botón para ver el contenido asociado.

```
R1# show ip ips statistics
Signature audit statistics [process switch:fast switch]
  signature 2000 packets audited: [0:2]
  signature 2001 packets audited: [9:9]
  signature 2004 packets audited: [0:2]
  signature 3151 packets audited: [0:12]
Interfaces configured for audit 2
Session creations since subsystem startup or last reset 11
Current session counts (estab/half-open/terminating) [0:0:0]
Maxever session counts (estab/half-open/terminating) [2:1:0]
Last session created 19:18:27
Last statistic reset never
HID:1000 OID:100 S:218 A:3 H:14085 HA:7114 DA:0 R:0
R1#
```

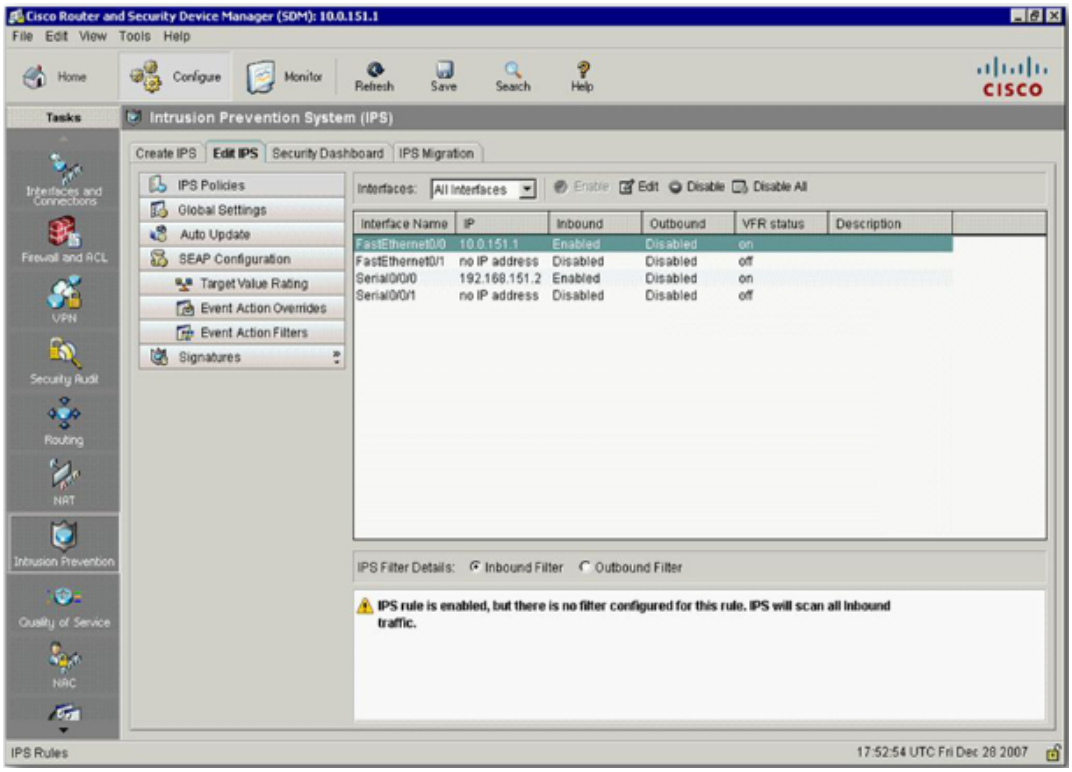


Haga clic en cada botón para ver el contenido asociado.

Para verificar la configuración de IPS en el router usando SDM, vaya a Configure > Intrusion Prevention > Edit IPS. La pestaña Edit IPS muestra todas las interfaces del router y si están configuradas para el IPS IOS de Cisco. Si aparece "Enabled" en la columna "Inbound" (de entrada) o "Outbound" (de salida), el IPS IOS de Cisco está habilitado para el tráfico que fluye en esa dirección en esa interfaz. Si aparece "Disabled" en alguna de las dos columnas, el IPS IOS de Cisco está deshabilitado para el tráfico que fluye en esa dirección en esa interfaz.

El campo Virtual Fragment Reassembly (VFR) Status muestra el estado de VFR en la interfaz. Si VFR está habilitado en esa interfaz, la columna muestra la palabra "On". Si VFR estña deshabilitado, la columna muestra la palabra "Off".

La pestaña Edit IPS también contiene botones que permiten al adminsitrador configurar y administrar las políticas, mensajes de seguridad y firmas del IPS IOS de Cisco.



5.4 Verificacion y monitoreo de IPS
5.4.2 Monitoreo del IPS IOS de Cisco

A partir de la versión 12.3(11)T del IOS de Cisco, el IPS IOS de Cisco proporciona dos métodos para reportar las alertas de intrusiones IPS:

SDM Security Device Event Exchange (SDEE)
Registro del IOS de Cisco mediante syslog

Para especificar el método de notificación de eventos, use el comando de configuración global ip ips notify [log | sdee].

La palabra clave log envía mensajes en formato syslog.
La palabra clave sdee envía mensajes en formato SDEE.

```
R1# config t
R1(config)# logging 192.168.10.100
R1(config)# ip ips notify log
R1(config)# logging on
R1(config)#
```

SDEE es el método preferido para reportar la actividad IPS. SDEE usa HTTP y XML para proporcionar una interfaz estandarizada. Puede ser habilitado en un router IPS IOS con el comando ip ips notify sdee. El router IPS IOS de Cisco conservará su capacidad de enviar alertas IPS por medio de syslog.

Los administradores deben también habilitar HTTP o HTTPS en el router cuando habilitan SDEE. El uso de HTTPS garantiza la seguridad de los datos en su camino a través de la red.

Cuando las notificaciones del SDEE de Cisco están deshabilitadas, todos los eventos almacenados se pierden. Se aloca un nuevo buffer cuando las notificaciones se rehabilitan. SDEE usa un mecanismo pull, lo cual significa que las solicitudes provienen de la aplicación de administración de la red y el router IDS o IPS responde. SDEE se vuelve entonces el formato estándar en todos los proveedores para comunicar eventos en una aplicación de administración de red.

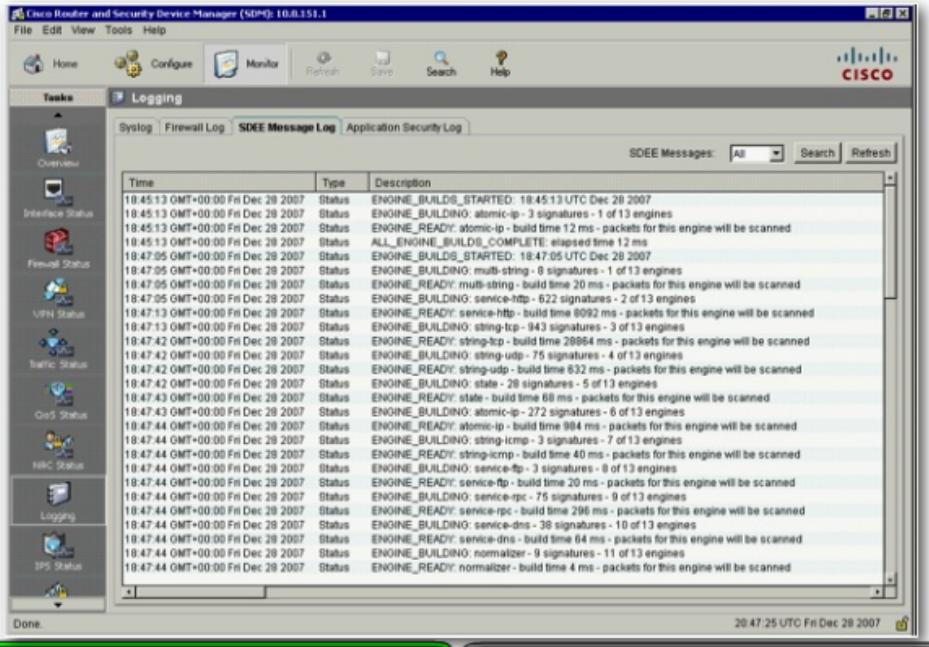
Por defecto, el buffer almacena hasta 200 eventos. Si se solicita un buffer más pequeño, todos los eventos almacenados se pierden. Si se solicita un buffer más grande, los eventos se guardan. El tamaño por defecto del buffer puede ser alterado con el comando ip sdee events eventos. El número máximo de eventos es 1000. El comando clear ip ips sdee {events | subscription} limpia los eventos o suscripciones SDEE.

El comando ip ips notify reemplaza al comando ip audit notify obsoleto. Si el comando ip audit notify es parte de una configuración existente, el IPS lo interpreta como el comando ip ips notify.

```
R1# config t
R1(config)# ip http server
R1(config)# ip http secure-server
R1(config)# ip ips notify sdee
R1(config)# ip sdee events 500
R1(config)#
```

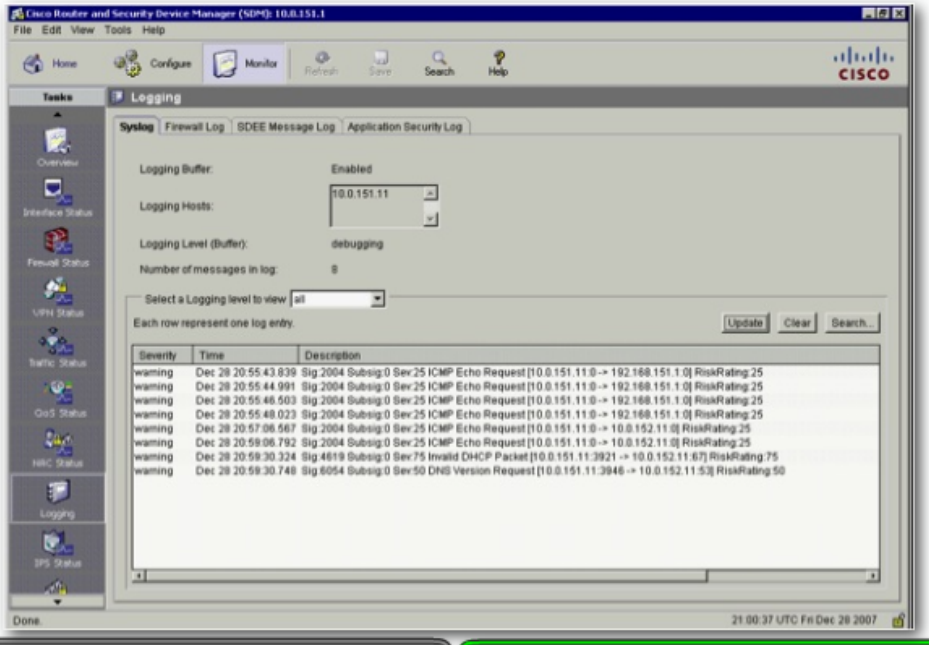
Para ver los mensajes SDEE, debe usarse un dispositivo de administración como MARS o software de administración como IEV, CSM o SDM. Por ejemplo, para ver los mensajes de alarma SDEE en el SDM de Cisco, vaya a Monitor > Logging > SDEE Message Log.

Los mensajes syslog también pueden ser visualizados en SDM yendo a Monitor > Logging > Syslog.



SDEE | Syslog

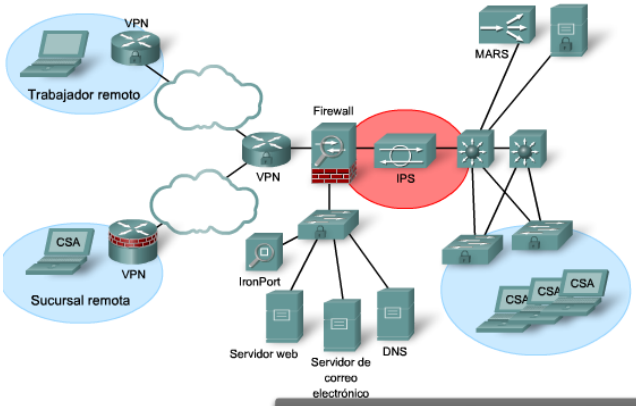
Haga clic en cada botón para ver el contenido asociado.



SDEE | Syslog

Haga clic en cada botón para ver el contenido asociado.

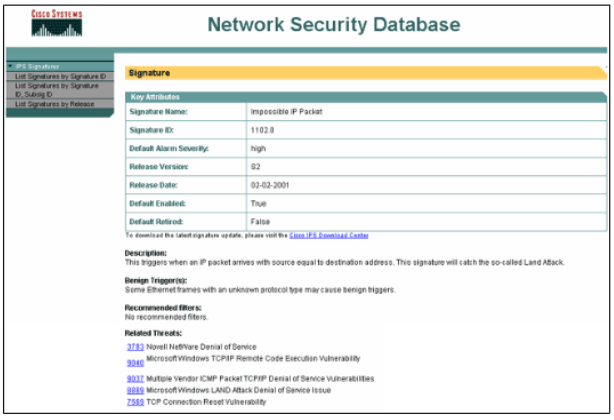
5.5.1 Resumen del capitulo



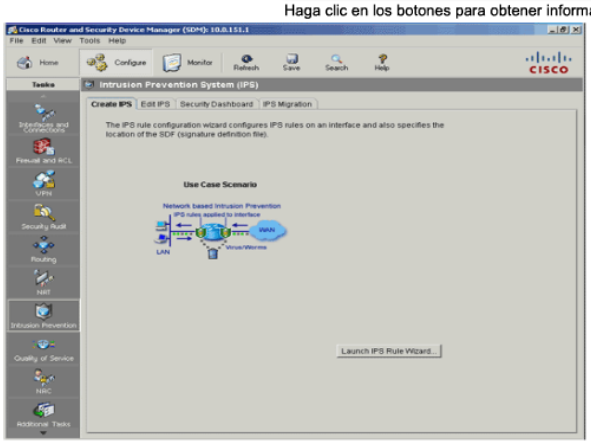
- El IPS basado en red se implementa en línea mientras que el IDS se implementa fuera de línea.
- Implemente IPSs basados en red y basados en host para asegurar la red contra rápidos gusanos y virus de Internet.

Haga clic en los botones para obtener información resumida.

- Las firmas son parecidas a los archivos .dat del antivirus, ya que proporcionan al IPS una lista de problemas identificados.
- Las firmas IPS se configuran para usar varios disparadores y acciones.
- Las firmas pueden necesitar una personalización para la red específica.
- Monitoree continuamente la solución IPS para asegurarse de que proporcione un nivel adecuado de protección.

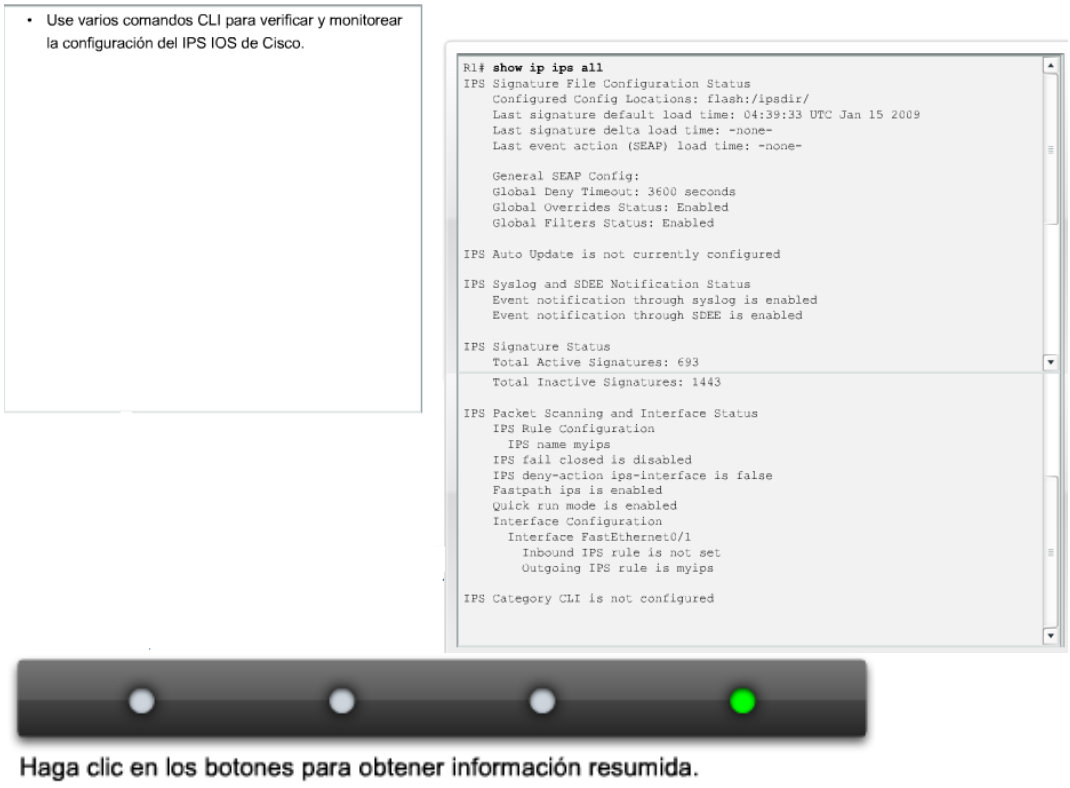


Haga clic en los botones para obtener información resumida.



- Implemente IPS IOS de Cisco con CLI o SDM.
- Modifique las firmas IPS con CLI o SDM.

Haga clic en los botones para obtener información resumida.



6 Seguridad de la red de area local

6.0 Introduccion al capitulo

6.0.1 Introduccion al capitulo

Una red segura es sólo tan fuerte como su eslabón más débil. Por este motivo, además de asegurar el perímetro de la red, es también importante asegurar los dispositivos finales que residen dentro de la red. La seguridad de terminales incluye asegurar tanto los dispositivos de infraestructura de red de la LAN como los dispositivos finales, como las estaciones de trabajo, servidores, teléfonos IP, puntos de acceso, y dispositivos de la red de área de almacenamiento (SAN - Storage Area Network). Existen diferentes aplicaciones y dispositivos de seguridad de terminales para lograr este objetivo, incluyendo dispositivos de seguridad Cisco IronPort, NAC (Network Admission Control), y CSA (Agente de Seguridad de Cisco).

La seguridad de terminales también incluye asegurar la capa 2 de la infraestructura de red para prevenir ataques de capa 2 tales como la falsificación de direcciones MAC (spoofing) y ataques de manipulación de STP. Las configuraciones de seguridad de capa 2 incluyen habilitar la seguridad de puertos, BPDU Guard, Root Guard, control de tormentas, Cisco switched port analyzer (SPAN), y SPAN remoto (RSPAN).

Finalmente, el tipo de soluciones de seguridad implementadas dependen del tipo de tecnologías LAN utilizadas. Por ejemplo, las redes que implementan tecnologías inalámbricas, VoIP, y SANs, contienen consideraciones y soluciones adicionales de seguridad.

En una práctica de laboratorio extensiva del capítulo, Seguridad de switches de capa 2, los alumnos realizarán la siguiente configuración en un switch de capa 2: acceso SSH, control de tormentas de broadcast, PortFast, BPDU Guard, Root Guard, seguridad de puertos, y Switched Port Analyzer. Los alumnos también verificarán diferentes configuraciones, controlarán la actividad de puertos utilizando Wireshark, y analizarán el origen de un ataque. El laboratorio se encuentra en el manual de laboratorios de Academy Connection en cisco.netacad.net.

Una actividad de Packet Tracer, Seguridad de capa 2, provee a los alumnos práctica adicional implementando las tecnologías presentadas en este capítulo. Los alumnos utilizarán parámetros de seguridad STP para mitigar ataques STP, habilitarán el control de tormentas para prevenir tormentas de broadcast, y configurarán seguridad de puertos para prevenir ataques de desborde de la tabla de direcciones MAC.

En una segunda actividad de Packet Tracer, Seguridad VLAN de capa 2, los alumnos crearán una VLAN administrativa, incorporando una PC de administración, e implementando una ACL para prevenir el acceso de usuarios externos a la VLAN administrativa.

Las actividades de Packet Tracer para CCNA Security se encuentran en Academy Connection en cisco.netacad.net.

En este capítulo usted aprenderá a:

- Describir la seguridad de terminales con IronPort.
- Describir la seguridad de terminales con Network Admission Control.
- Describir la seguridad de terminales con el Agente de Seguridad de Cisco.
- Describir los ataques de falsificación de direcciones MAC, ataques de manipulación de STP, ataques de desbordamiento de direcciones MAC, ataques de tormentas de LAN, y ataques de VLAN.
- Describir técnicas específicas de mitigación para ataques de Capa 2.
- Configurar seguridad de puertos, BPDU Guard, Root Guard, control de tormentas, SPAN y RSPAN.
- Describir consideraciones de seguridad para wireless, VoIP y SAN.
- Describir soluciones de seguridad para wireless, VoIP y SAN.

6.1 Seguridad de terminales

6.1.1 Introduccion a la seguridad de terminales

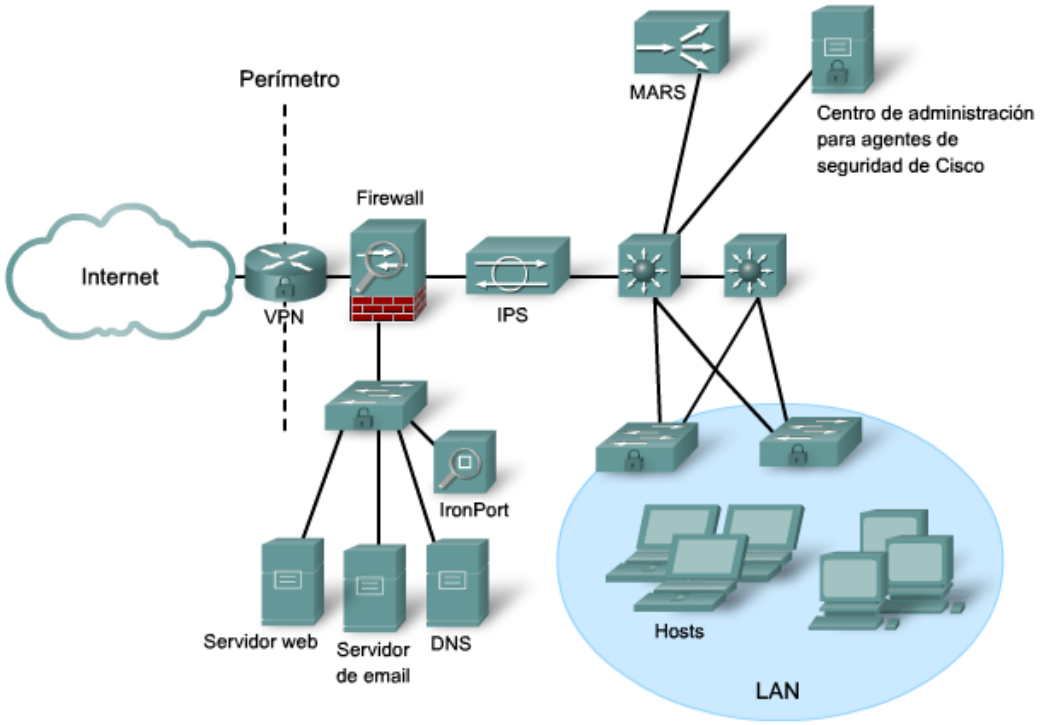
Las amenazas de alto perfil discutidas con más frecuencia en los medios son las amenazas externas, tales como gusanos de Internet o ataques DoS. Pero asegurar internamente una red de área local (LAN) es tan importante como asegurar el perímetro de la red. Sin una LAN segura, los usuarios de la organización pueden ser incapaces de obtener acceso a la red, lo que puede reducir significativamente su productividad.

Muchos administradores de red desarrollan sus propias estrategias de seguridad partiendo desde el perímetro de la red, y trabajando hacia adentro de la LAN. Otros administradores desarrollan sus estrategias de seguridad de la red dentro de la LAN y trabajan hacia el perímetro. Sin importar el enfoque utilizado, es vital asegurar dos áreas específicas: las terminales y la infraestructura de la red.

La LAN está compuesta por terminales de red. Una terminal, o host, es un sistema o dispositivo individual que actúa como cliente de red. Las terminales comunes son laptops, desktops, teléfonos IP, y asistentes digitales personales (PDAs). Los servidores también pueden ser considerados terminales. La estrategia de seguridad desde adentro

hacia afuera (LAN-to-perimeter) se basa en la idea de que si los usuarios no practican la seguridad desde sus estaciones de trabajo, ninguna cantidad de medidas de seguridad podrá garantizar la seguridad de la red.

La infraestructura de red es otra área para enfocar la seguridad de la LAN. La mitigación de ataques es parte de asegurar una LAN. Estos ataques incluyen la falsificación de direcciones MAC (spoofing), manipulación de STP, desbordamiento de la tabla de direcciones MAC, tormentas de LAN, y ataques de VLAN. Otro elemento a asegurar en la infraestructura de red son los dispositivos no terminales de la LAN. Éstos incluyen switches, dispositivos inalámbricos, dispositivos de telefonía IP, y dispositivos de almacenamiento.



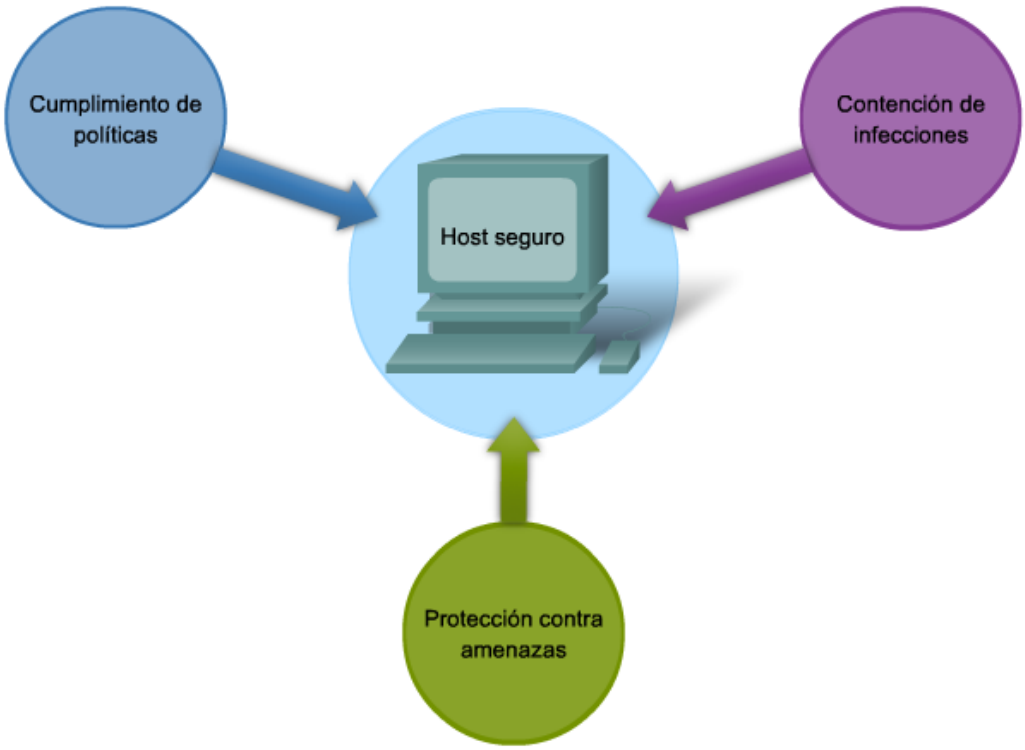
Antes de asegurar la infraestructura de la red, el foco inicial debe ser la seguridad de las terminales. Los hosts deben estar protegidos contra virus, troyanos, gusanos y otras amenazas de seguridad. La estrategia de Cisco para tratar la seguridad de las terminales se basa en tres elementos:

Control de Admisión a la Red de Cisco (NAC) - La solución NAC asegura que cada terminal cumpla con las políticas de seguridad de la red antes de otorgarle el acceso a la misma. NAC provee acceso a dichos dispositivos y asegura que los dispositivos que no cumplen con las políticas tengan el acceso denegado, sean puestos en cuarentena u obtengan un acceso restringido a los recursos.
Protección de terminales - La tecnología basada en comportamiento está disponible con el Agente de Seguridad de Cisco (CSA), el cual protege a las terminales contra amenazas generadas por virus, troyanos y gusanos. Los dispositivos de seguridad de perímetro IronPort complementan a CAS enfocándose en la seguridad del correo electrónico y los sitios web.

Contención de infecciones de red - Dirigida a los métodos de ataque más nuevos, los cuales pueden comprometer a la red, la contención se enfoca en automatizar elementos claves del proceso de respuesta a infecciones. Los elementos NAC, CAS e IPS de la Red Autodefensiva de Cisco (SDN) proveen este servicio.

Es necesaria una estrategia de seguridad de terminales debido a que el software suele tener puntos débiles. El software seguro (confiable) está diseñado para proteger a los datos y soportar intentos de ataques. Históricamente, el software seguro fue utilizado sólo dentro de sistemas militares y sistemas comerciales críticos. En general, este tipo de software es realizado a medida.

El software no seguro puede hacerse más confiable reforzándolo o bloqueando sus vulnerabilidades. Para reforzar un programa, es necesario conocer la documentación de sus componentes de software internos, la cual no suele ser provista por sus desarrolladores. Además, para asegurar el software es necesario asegurar los sistemas operativos y cualquier otra aplicación que se ejecute dentro del sistema operativo.



Los sistemas operativos proporcionan servicios básicos de seguridad a las aplicaciones:

Código confiable y ruta confiable - Aseguran que la integridad del sistema operativo no ha sido violentada. El código confiable asegura que el código del sistema operativo no ha sido comprometido. Un sistema operativo puede demostrar integridad verificando todo el código ejecutado mediante códigos de autenticación de mensajes (HMACs) o firmas digitales. La verificación de integridad del software incorporado puede ser necesaria durante su instalación. También pueden utilizarse firmas digitales. Las rutas confiables se refieren a la función que permite asegurar que el usuario está utilizando un

sistema genuino y no un troyano. Un ejemplo de una ruta confiable es la secuencia de teclas Ctrl-Alt-Delete necesaria para ingresar al sistema en Windows Server y Windows XP.
Contexto de ejecución privilegiado - Provee autenticación de identidad y ciertos privilegios basados en dicha identidad.
Protección y aislamiento de la memoria de los procesos - Proporciona una separación de los otros usuarios y sus datos.
Control de acceso a los recursos - Asegura la confidencialidad e integridad de los datos.

Un atacante puede socavar todos estos servicios. Si tanto el código confiable o las rutas confiables no están disponibles o se ven comprometidos, el sistema operativo y todas sus aplicaciones pueden ser fácilmente reemplazados por código hostil. Un sistema operativo puede hacerse más vulnerable si existe la necesidad de dar soporte a protocolos antiguos, heredados.



Los sistemas operativos modernos proveen a cada proceso con una identidad y privilegios. Es posible modificar los privilegios durante la operación de un programa o durante una misma sesión de usuario. Por ejemplo, UNIX posee la función suid (set user ID) y Windows dispone de la función runas.

Estas son algunas técnicas que ayudan a proteger a las terminales de las vulnerabilidades del sistema operativo:

Concepto del menor privilegio - Para proteger mejor a las terminales, nunca debe asignarse a un proceso un nivel mayor de privilegios que los necesarios para realizar su tarea.

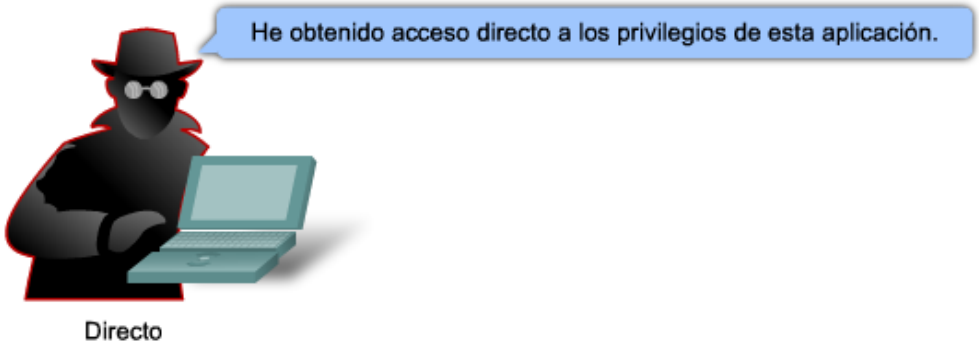
Aislamiento entre procesos - El aislamiento entre procesos puede ser virtual o físico. Por ejemplo, la protección de memoria puede realizarse por hardware. Algunos sistemas operativos confiables proveen aislamiento utilizando compartimientos de ejecución lógicos.

Monitor de referencias - Un monitor de referencias es un concepto de control de acceso referido a un mecanismo o proceso que funciona como intermedio para todos los accesos a objetos. Provee un punto central para todas las decisiones de políticas, implementando funciones de auditoría para realizar un seguimiento de los accesos. Además del monitor de referencias que existe por lo general en un sistema operativo, CSA funciona también como un monitor de referencias.
Porciones de código pequeñas y verificables - Para todas las funciones de seguridad, la idea es tener porciones de código pequeñas y fáciles de verificar, administradas y monitoreadas por un monitor de referencias.

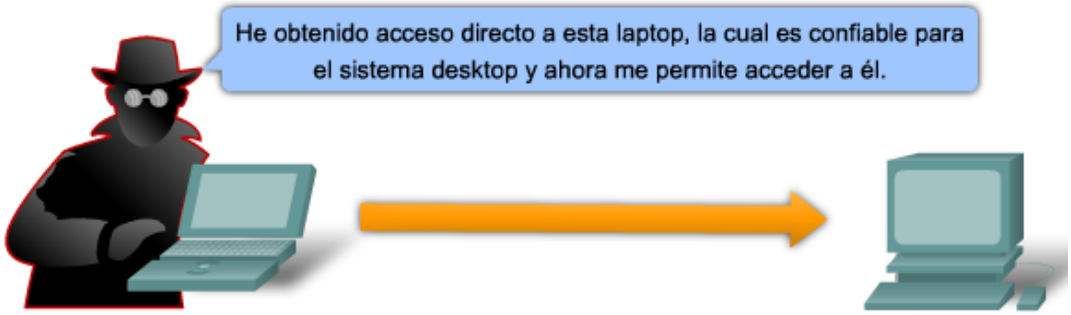
En general, el objetivo final de un atacante es una aplicación que se ejecute en el host, la cual procese datos sensibles a los cuales el atacante desea tener acceso. Los ataques a las aplicaciones pueden ser directos o indirectos. En un ataque directo, el atacante engaña a la aplicación para que realice una tarea con sus propios privilegios. En un ataque indirecto, el atacante primero compromete otro subsistema para luego atacar a la aplicación mediante dicho subsistema (escalada de privilegios).

Cuando un atacante tiene la opción de comunicarse directamente con la aplicación objetivo, dicha aplicación debe estar protegida en forma adecuada. Por ejemplo, un atacante podría intentar un ataque DoS a una aplicación específica. Otro ejemplo de un ataque directo a una aplicación objetivo es si el atacante utiliza fallas de dicha aplicación para pasar por alto sus controles de acceso con el fin de obtener acceso de lectura o escritura a sus datos sensibles.

En otro escenario, un atacante gana acceso en forma indirecta a los datos sensibles mediante una cadena de cesiones de los componentes de otros sistemas. Por ejemplo, un atacante obtiene primero un acceso de usuario de nivel básico al sistema en el que residen los datos sensibles. Luego, explotando una falla en cualquier aplicación local, el atacante obtiene privilegios de administración del sistema (escalada de privilegios). Utilizando estos privilegios, el atacante puede leer o escribir sobre la mayoría de los objetos del sistema, incluyendo los datos sensibles de la aplicación objetivo.



Directo



Indirecto

Cisco Systems provee diferentes componentes para asegurar una solución de seguridad de terminales robusta. Los componentes primarios de esta solución son:

IronPort
Cisco NAC
CSA

Los dispositivos de seguridad de perímetro Cisco IronPort dan protección a las empresas contra amenazas de Internet, enfocada en la seguridad de correo electrónico y sitios web, dos de las principales consideraciones de seguridad en las terminales. En este caso, las terminales son aseguradas por dispositivos que funcionan en el perímetro de la red.

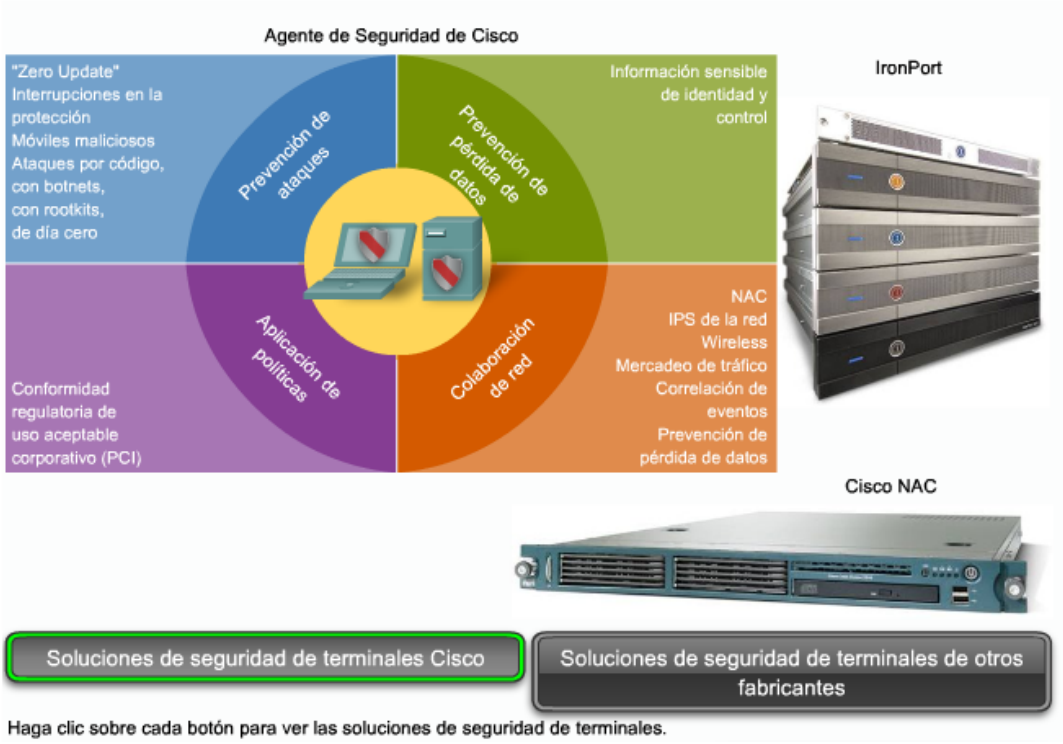
NAC utiliza la infraestructura de la red para implementar la política de seguridad en todos los dispositivos que requieran acceso a recursos de red. Con NAC, los profesionales de seguridad de red pueden autenticar, autorizar, evaluar y remediar a usuarios y máquinas cableados, inalámbricos y remotos, previo a su acceso a la red. NAC identifica si los dispositivos de red cumplen o no con las políticas de seguridad, y repara cualquier vulnerabilidad antes de permitir su acceso a la red.

CSA provee una solución de seguridad de terminales completamente integrada, la cual combina prevención de pérdida de datos definida por políticas con prevención de ataques de "día cero" (zero-update attack) y detección de antivirus, en una misma consola de administración. CSA defiende a las terminales contra la pérdida de datos

causada tanto por malware como por acciones de los usuarios y ejecuta políticas de seguridad y uso aceptable dentro de una infraestructura de administración simple.

IronPort, NAC y CSA tienen cierto solapamiento en su soporte funcional de seguridad de terminales. Estas tecnologías, cuando son utilizadas en paralelo, agregan capas de protección y operan entre sí. Se combinan para proveer protección de las vulnerabilidades del sistema operativo contra ataques directos e indirectos.

Aunque existen un número de alternativas a las soluciones de seguridad de terminales provista por Cisco Systems, la limitación de estos otros sistemas es que no proveen una solución de extremo a extremo para asegurar la red. Algunos de los mayores proveedores de soluciones de seguridad de terminales son McAfee, Symantec, Juniper, SonicWALL y Fortinet.





6.1.2 Seguridad de terminales con IronPort

Cisco Systems adquirió IronPort Systems en 2007. IronPort es un proveedor líder de dispositivos anti-spam, anti-virus y anti-spyware. IronPort utiliza SenderBase, la base de datos de detección de amenazas más grande del mundo, para proveer medidas de seguridad preventivas y reactivas.

IronPort ofrece diferentes dispositivos de seguridad:

C-Series - Dispositivo de seguridad de correo electrónico para el control de virus y spam.
S-Series - Dispositivo de seguridad web para el filtrado de spyware, filtrado de URLs y anti-malware.
M-Series - Dispositivo de administración de seguridad, complementa los dispositivos de seguridad de correo electrónico y servidores web mediante la administración y monitoreo de las políticas de la organización, configurando y auditando información.

Los dispositivos M-Series son herramientas de administración flexibles, para la centralización y consolidación de políticas y datos de ejecución. Proporcionan a los profesionales de seguridad una única interfaz para administrar todos los sistemas de seguridad de la capa de aplicación.

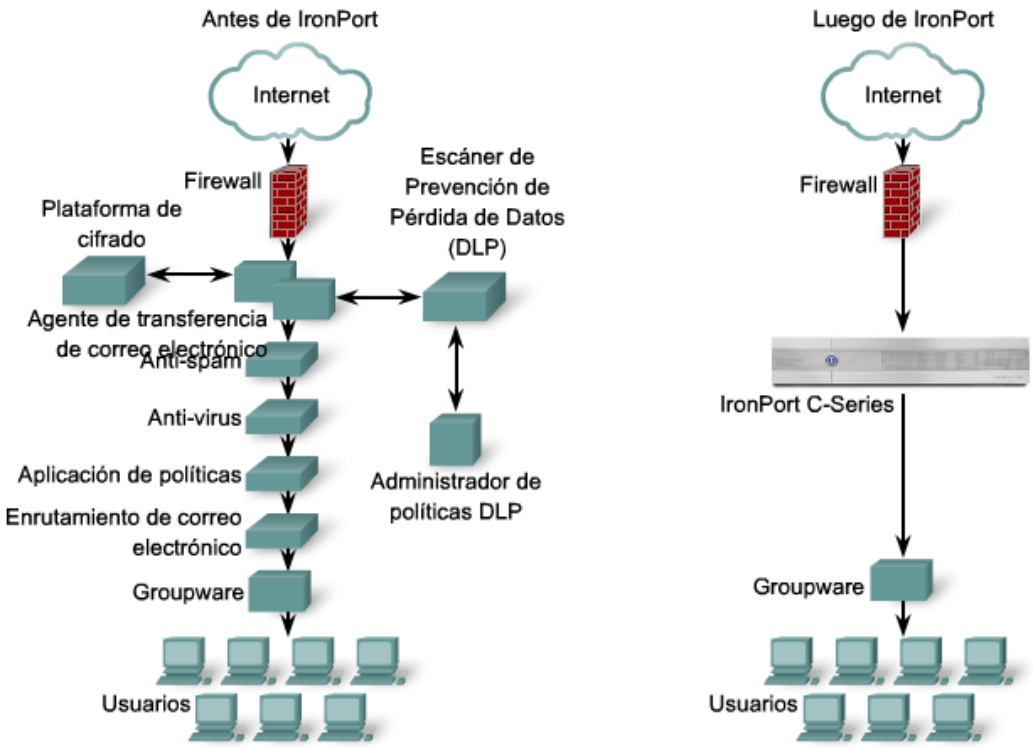
Al proveer soluciones de seguridad instalados en el gateway de la red, IronPort habilita una defensa perimetral que ayuda a prevenir amenazas de Internet de todo tipo, antes de que alcancen las estaciones de trabajo de los empleados.

Productos Cisco IronPort



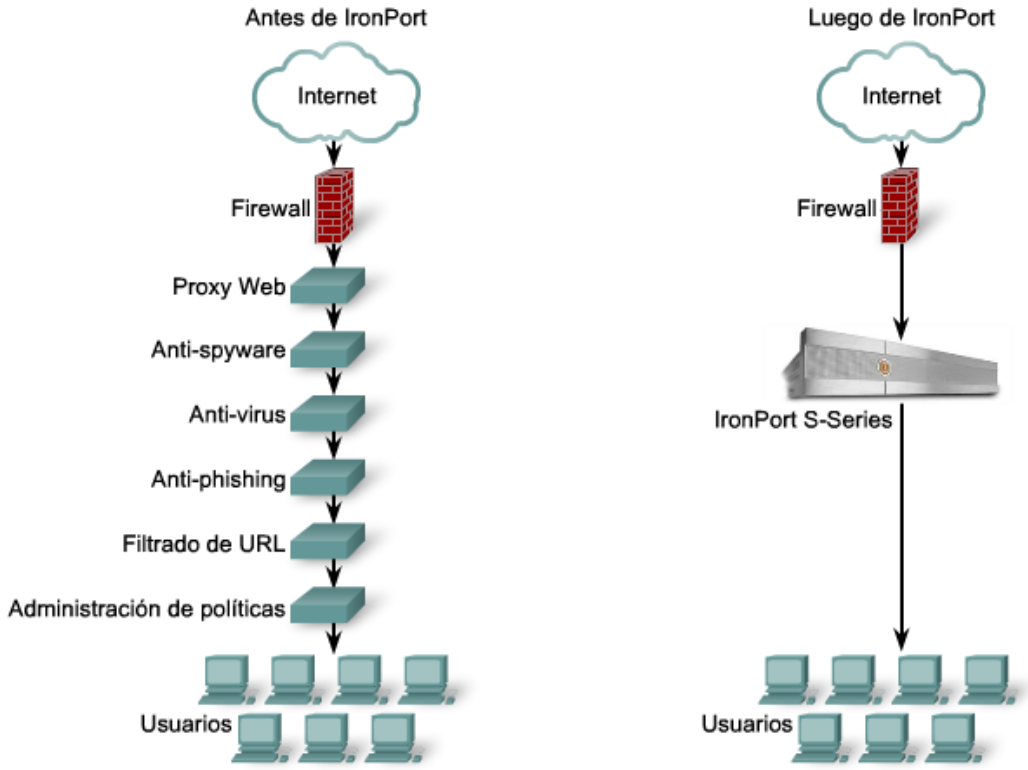
IronPort SenderBase es el servicio de monitoreo de tráfico de correo electrónico más grande del mundo. SenderBase recolecta datos de más de 100.000 ISPs, universidades y corporaciones. Mide más de 120 parámetros diferentes para cualquier servidor de correo electrónico en Internet. Esta base de datos masiva recibe más de cinco mil millones de consultas por día, con un streaming de datos en tiempo real proveniente de todos los continentes, tanto de pequeños como de grandes proveedores de red. SenderBase posee la vista más ajustada de los patrones de envío de cualquier remitente de correo electrónico debido al tamaño de la base de datos. Se ha mantenido como la base de datos más grande del mundo debido a la precisión de sus datos. IronPort licencia datos de SenderBase a la comunidad Open Source y a otras instituciones que participan en la lucha contra el spam.

Los ocho ISPs más grandes y más del 20 por ciento de las mayores compañías del mundo utilizan los dispositivos de seguridad de correo electrónico IronPort C-Series. Al proteger los sistemas de correo electrónico de las empresas de todos los tamaños, los períodos de inactividad asociados al spam, a los virus y a una amplia variedad de otras amenazas han sido reducidos. El sistema también reduce la carga de trabajo del personal técnico.



El spyware se ha convertido en uno de los problemas de seguridad más significativos de las corporaciones. Más del 80 por ciento de las PCs corporativas están infectadas con spyware, pero menos del 10 por ciento de las corporaciones han desarrollado defensas de spyware perimetrales. La velocidad, variedad y malicia de los ataques de spyware y malware basado en web han resaltado la importancia de una plataforma segura y robusta para proteger al perímetro de la red empresarial de dichas amenazas. IronPort S-Series es un rápido dispositivo de seguridad web, el cual ofrece múltiples motores de barrido anti-malware en un único dispositivo integrado. S-Series incluye la tecnología Web Reputation y el motor Dynamic Vectoring and Stream (DVS) exclusivos de IronPort, una nueva tecnología que permite el filtrado de spyware basado en firmas.

El profesional de seguridad puede ejecutar motores de barrido de forma simultánea para ofrecer mayor protección contra amenazas de malware, con un mínimo impacto en el desempeño. Esto provee protección contra una amplia variedad de amenazas basadas en la web, desde ataques de adware, phishing y pharming, hasta amenazas más dañinas como troyanos, gusanos y otros ataques de monitoreo de sistemas.



6.1.3 Seguridad de terminales con control de adminision de red

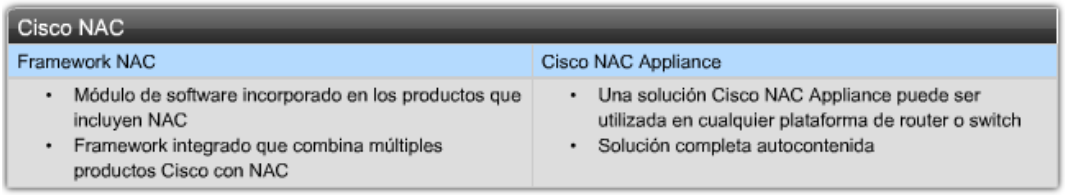
El propósito de NAC se divide en dos partes: permitir el acceso a la red únicamente a usuarios y sistemas autorizados (administrados o no administrados) y asegurar el cumplimiento de las políticas de seguridad de la red.

NAC ayuda a mantener la estabilidad de la red al proveer cuatro características importantes: autenticación y autorización, evaluación de posturas (evaluación del cumplimiento de las políticas de la red en los dispositivos entrantes), cuarentena de sistemas que no cumplan con las políticas y resolución de los problemas en los sistemas que no cumplan con las políticas de la red.

Los productos Cisco NAC se dividen en dos categorías:

Framework NAC - El framework NAC utiliza la infraestructura de red Cisco existente y software de terceros para implementar el cumplimiento de la política de seguridad en todas las terminales. El framework NAC es apropiado para todos los ambientes de red de alta performance con diferentes terminales. Estos ambientes requieren una solución consistente de LAN, WAN, wireless, extranet y acceso remoto, que se integre en la seguridad existente y repare software, herramientas y procesos. Las cuatro funciones de NAC pueden ser provistas por diferentes dispositivos o por uno solo.
Cisco NAC Appliance - La solución Cisco NAC Appliance concentra las cuatro funciones NAC en un mismo dispositivo y provee una solución completa para el control del acceso a la red. Esta solución resulta apropiada para redes de mediana escala que requieran una solución completa e independiente. Cisco NAC Appliance es ideal para las organizaciones que necesiten un rastreo simple e integrado de las actualizaciones del

sistema operativo, del antivirus y de las vulnerabilidades. No requiere una red Cisco para su funcionamiento.

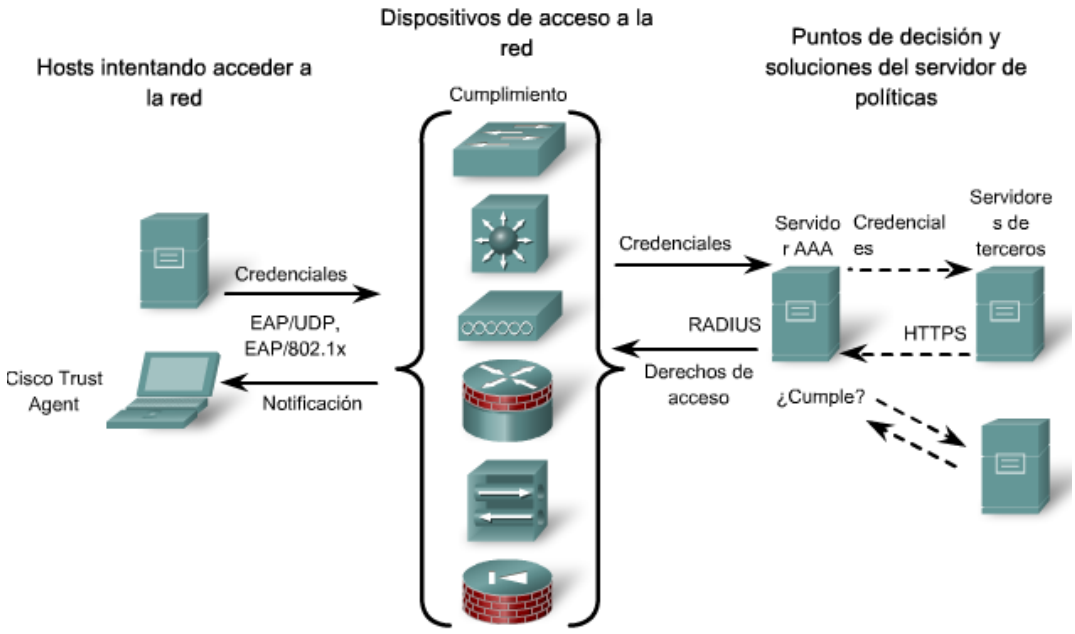


- Ofrece a los clientes una opción en el tiempo de implementación
- Se adapta a los requisitos de protección de la inversión de los usuarios

Los componentes de un framework NAC proveen control de acceso basado en la conformidad con las políticas. Las funciones de NAC, incluyendo autenticación, autorización, y registro de auditoría (AAA - Authentication, Authorization, Accounting), barrido y remedio son realizadas por otros productos Cisco, tales como el Servidor de Control de Acceso Seguro de Cisco (ACS), o productos asociados como TrendMicro.

El objetivo tanto del framework NAC como de Cisco NAC Appliance es asegurar que sólo se permita el acceso a la red a aquellos hosts que sean autenticados y a los cuales se haya examinado y aprobado su situación de seguridad. Por ejemplo, las laptops de la compañía que han sido utilizadas fuera de la empresa por un período de tiempo y pueden no haber recibido las últimas actualizaciones de seguridad, o pueden haber sido infectadas en otros sistemas no deben conectarse a la red hasta haber sido examinadas y aprobadas.

Los dispositivos de acceso a la red funcionan como la capa de aplicación de políticas. Fuerzan a los clientes a realizar una solicitud al servidor RADIUS para su autenticación y autorización. El servidor RADIUS puede consultar a otros dispositivos, como el servidor anti-virus TrendMicro, y responder a los dispositivos de la red encargados de controlar la utilización de las políticas de acceso. Sólo cuando se ha verificado que se cumplen estos requisitos, el host puede ser identificado y admitido en la red.



El dispositivo Cisco NAC Appliance consolida todas las funciones del framework NAC en un mismo dispositivo de red, cumpliendo con todos los mismos roles. Los siguientes componentes principales ejecutan estas tareas:

Cisco NAC Appliance Server (NAS) - Dispositivo utilizado para realizar el control de acceso a la red. Este dispositivo de seguridad se implementa al nivel de la red. Puede ser implementado en banda o fuera de banda en la capa 2 o 3, como un gateway virtual o como un gateway IP real, y puede ser instalado en forma central o distribuida. Cisco NAS realiza verificaciones de conformidad de los dispositivos a medida que los usuarios intentan acceder a la red.
Cisco NAC Appliance Manager (NAM) - Interfaz centralizada de administración, utilizada por el personal de soporte técnico. Cisco NAM provee una interfaz basada en web para la creación de políticas de seguridad y administración de usuarios online. También puede actuar como un proxy de autenticación para autenticar servidores internos. Los administradores pueden utilizarlo para establecer roles de usuarios, verificaciones de conformidad, y requisitos de solución de problemas. Cisco NAM interactúa con Cisco NAS, que es el componente de cumplimiento de políticas del dispositivo Cisco NAC Appliance.

Cisco NAC Appliance Agent (NAA) - Software cliente que facilita la administración de la red. Este agente liviano de sólo lectura se ejecuta en una terminal. Realiza una inspección profunda del perfil de seguridad de la máquina local, analizando sus configuraciones de registro, servicios y archivos. Mediante esta inspección, NAA puede determinar si un dispositivo cuenta con una base de anti-virus actualizada, actualizaciones de seguridad, o los últimos hotfix de Windows. Un hotfix es una actualización crítica que puede instalarse mientras se ejecuta la aplicación, para resolver sus vulnerabilidades. Permite corregir el problema forzando la actualización de seguridad en el host. En los activos no administrados, Cisco NAA puede ser descargado bajo demanda.

Actualizaciones del conjunto de reglas - Las actualizaciones automáticas son utilizadas para mantener un nivel de seguridad alto, proveyendo siempre las últimas actualizaciones de virus y parches de software para los hosts en cuarentena.

Cisco NAS
- Funciona como un dispositivo en banda o fuera de banda para el control de acceso a la red

Cisco NAM
- Centraliza la administración para administradores, personal de soporte y operadores

Cisco NAA
- Cliente liviano opcional para barridos de registros basados en dispositivos en ambientes no administrados

Actualizaciones del conjunto de reglas
- Actualizaciones automáticas planificadas para anti-virus, actualizaciones críticas, y otras aplicaciones







Cisco NAC Appliance extiende NAC a todos los métodos de acceso a la red, incluyendo el acceso mediante LANs, gateways de acceso remoto y puntos de acceso inalámbricos. Cisco NAC Appliance también realiza revisiones de estado a los usuarios invitados.

Una vez implementado, Cisco NAC Appliance provee varios beneficios:

Reconoce usuarios, sus dispositivos y sus roles en la red. Este primer paso ocurre en el punto de autenticación, antes de que el código malicioso pueda causar cualquier daño.
Evalúa si las máquinas cumplen o no las políticas de seguridad. Las políticas de seguridad pueden incluir software anti-virus o anti-spyware específico, actualizaciones del sistema operativo o parches. Cisco NAC Appliance soporta políticas que varían de acuerdo al tipo de usuario, tipo de dispositivo o sistema operativo.
Asegura el cumplimiento de las políticas de seguridad bloqueando, aislando y reparando las máquinas que presenten no conformidades.

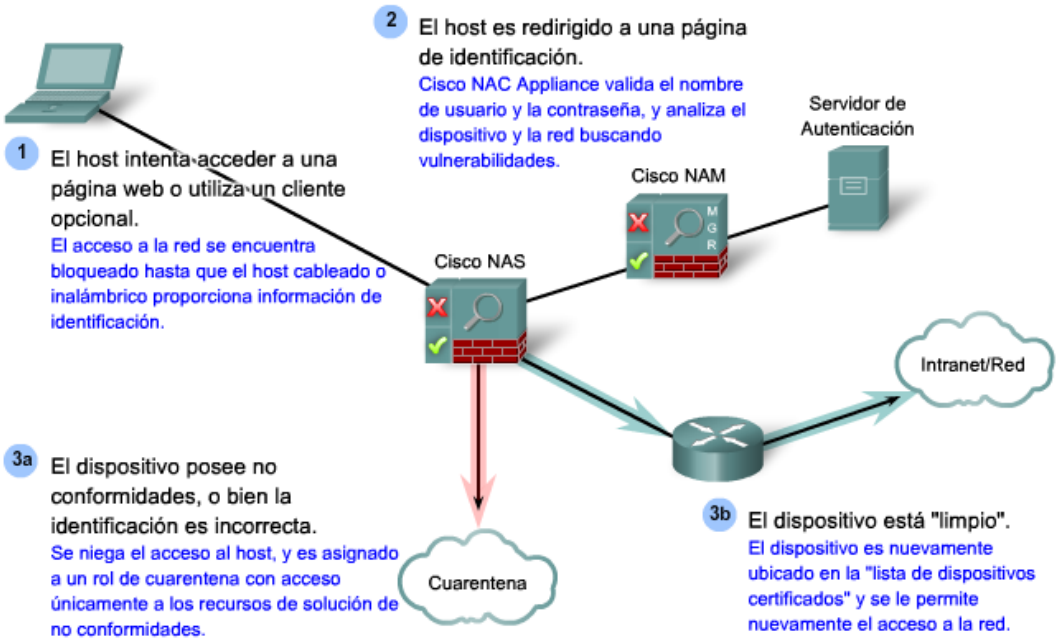
Las máquinas que presenten no conformidades son redirigidas a un área de cuarentena, donde se realiza la reparación a discreción de un profesional de seguridad.

El proceso de Cisco NAC Appliance involucra diferentes pasos:

Paso 1. El usuario intenta acceder a un recurso de la red.

Paso 2. El usuario es redirigido a una página de identificación.

Paso 3. El host es autenticado y opcionalmente se analiza su conformidad con las políticas. Si las cumple, se permite el acceso del host a la red. Si se encuentran incumplimientos, el host es puesto en cuarentena en una VLAN, donde puede ser actualizado para resolver las no conformidades.



Cisco NAA es la interfaz de software que ven los usuarios al interactuar con Cisco NAC Appliance. Existen tres ventanas de acceso:

1. La primera ventana es la ventana de identificación inicial, donde el usuario ingresa su nombre de usuario y su contraseña, y se verifica la conformidad del sistema.

2. Si la verificación falla, se otorga al usuario un acceso temporal y se le presenta la ventana "You Have Temporary Access".

3. Si existe una solución disponible, la ventana "Please Download and Install the Required Software" invita al usuario a instalar el software necesario para eliminar las no conformidades.



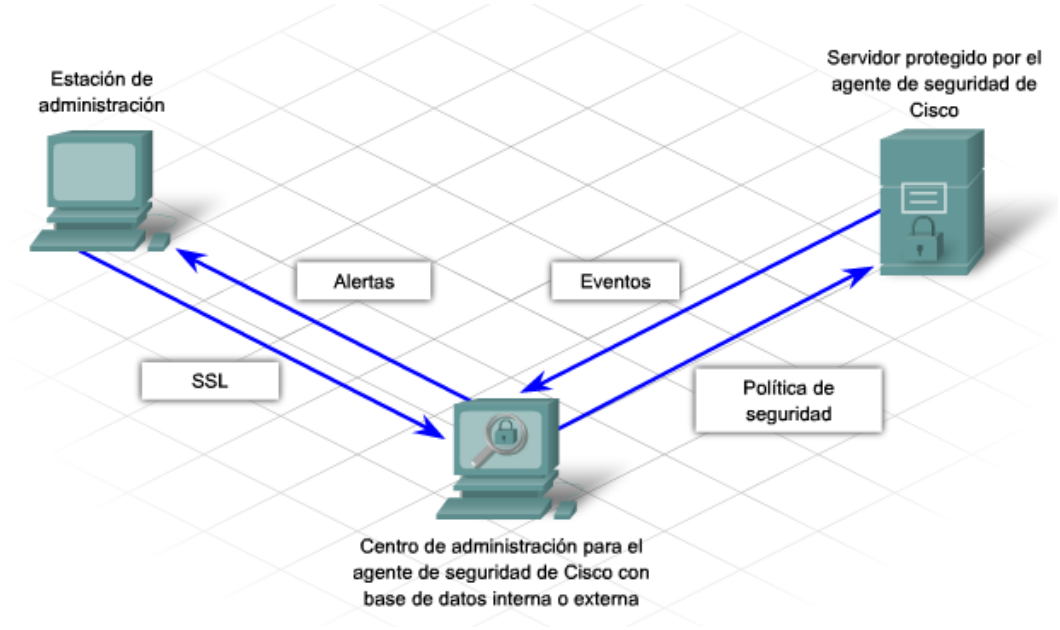
6.1.4 Seguridad de terminales con el agente de seguridad de Cisco

El Agente de Seguridad de Cisco (CSA), un sistema de prevención de intrusión basado en host (HIPS - Host-based Intrusion Prevention System), es un producto que provee seguridad de terminales mediante la protección contra amenazas para sistemas de servidores y desktop. Debido a que una única consola de administración puede soportar hasta 100.000 agentes, es una solución muy escalable.

El modelo de arquitectura CSA consiste en dos componentes:

Centro de Administración para CSA - Permite al administrador dividir a los host de la red en grupos de acuerdo a sus funciones y requisitos de seguridad y luego configurar las políticas de seguridad para dichos grupos. Puede mantener un registro de violaciones de seguridad y enviar alertas por correo electrónico o pager.
Cisco Security Agent - El componente CSA se instala en el sistema host, controla en forma permanente la actividad del sistema local y analiza sus operaciones. CSA ejecuta acciones proactivas para bloquear los intentos de actividad maliciosa y solicita actualizaciones de las políticas al Centro de Administración a intervalos configurables.

Puede utilizarse una interfaz web con SSL para conectarse en forma segura desde una estación de trabajo de administración al Centro de Administración de CSA.



Cuando una aplicación necesita acceso a recursos del sistema, realiza una llamada del sistema operativo al kernel. CSA intercepta estas llamadas, y las compara con la política de seguridad almacenada en cache. Si la solicitud no viola esta política, es enviada al kernel para su ejecución.

Si la llamada viola la política de seguridad, CSA bloquea esta petición y realiza dos acciones:

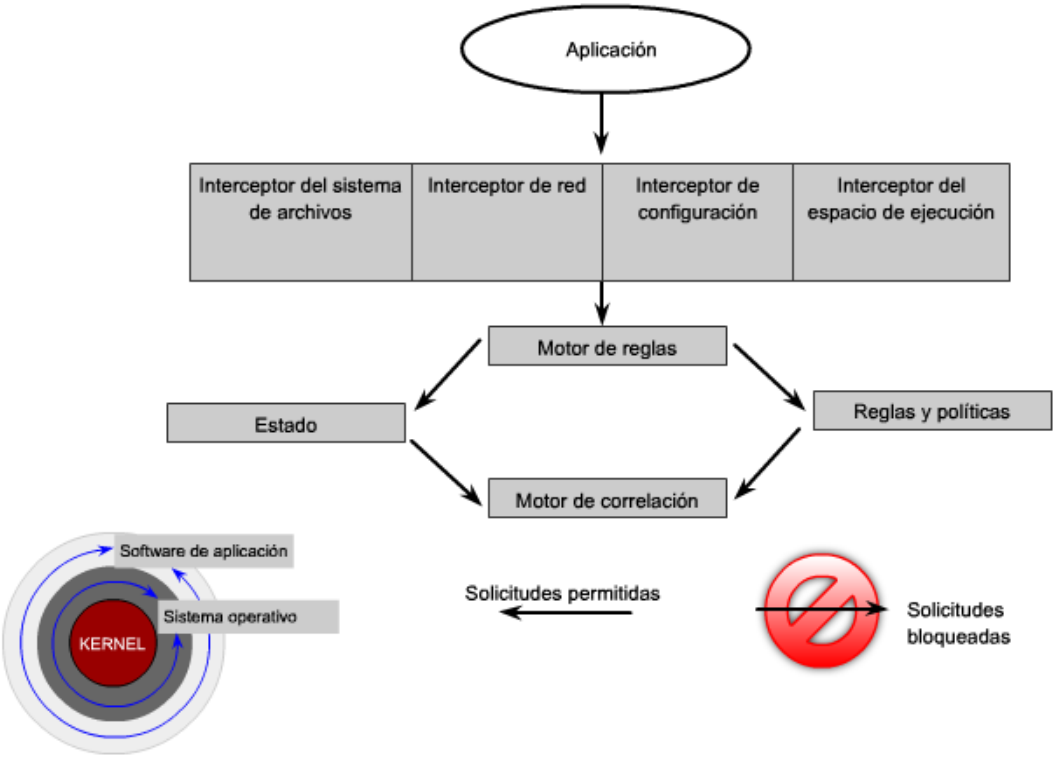
Envía el mensaje de error apropiado a la aplicación.
Se genera una alerta y se la envía al Centro de Administración para CSA.

CSA correlaciona esta llamada al sistema en particular con otras llamadas realizadas por otras aplicaciones o procesos, y realiza un seguimiento de estos eventos para detectar actividad maliciosa.

CSA proporciona protección a través de la implementación de cuatro interceptores:

Interceptor del sistema de archivos - Todas las solicitudes de lectura o escritura de archivos son interceptadas y luego permitidas o denegadas de acuerdo a la política de seguridad.
Interceptor de red - Se controlan los cambios de la especificación de interfaz del controlador de red (NDIS - Network Driver Interface Specification) y se verifican las conexiones de red, de acuerdo a la política de seguridad. El número de conexiones de red permitidas en un momento determinado también puede limitarse para prevenir ataques DoS.
Interceptor de configuración - Las solicitudes de lectura y escritura sobre el registro de Windows o la ejecución de archivos de control (rc) en UNIX, son interceptadas. Esto ocurre debido a que las modificaciones de configuración del sistema operativo pueden tener serias consecuencias. Por lo tanto, CSA controla en forma estricta las solicitudes de lectura y escritura sobre el registro.

Interceptor del espacio de ejecución - Este interceptor se ocupa del mantenimiento de la integridad del ambiente de ejecución dinámica de cada aplicación, detectando y bloqueando solicitudes para escribir en posiciones de memoria que no le pertenecen a la aplicación que realiza la solicitud. Los intentos de inyectar código, como pueden ser librerías compartidas o librerías de enlace dinámico (DLL), también son detectados y bloqueados. El interceptor también detecta ataques de desbordamiento de buffer, preservando así la integridad de los recursos dinámicos como el sistema de archivos, la configuración de servicios web, la memoria, y la entrada y salida de red.



Interceptando la comunicación entre las aplicaciones y el sistema subyacente, CSA combina la funcionalidad de diferentes propuestas tradicionales de seguridad:

Firewall distribuido - El interceptor de red realiza las funciones de un firewall de host.
HIPS - El interceptor de red colabora con el interceptor de espacio de ejecución, para proveer la capacidad de alertas de un HIPS con la aplicación proactiva de una política de seguridad.
Aislamiento de aplicaciones - El aislamiento de aplicaciones (application sandbox) es un espacio de ejecución donde es posible ejecutar los programas sospechosos con un menor acceso a los recursos del sistema. Este servicio de seguridad es provisto por una combinación entre el sistema de archivos, la configuración y los interceptores de espacio de ejecución.
Prevención de gusanos de red - Los interceptores de red y de espacio de ejecución proveen prevención de gusanos sin la necesidad de actualizaciones.

Monitor de integridad de archivos - Los interceptores del sistema de archivos y de configuración funcionan como un monitor de integridad de archivos.

Las políticas por defecto que se encuentran previamente configuradas en CSA implementan todas estas características de seguridad. Si fuera necesario, los usuarios pueden crear o modificar las políticas.

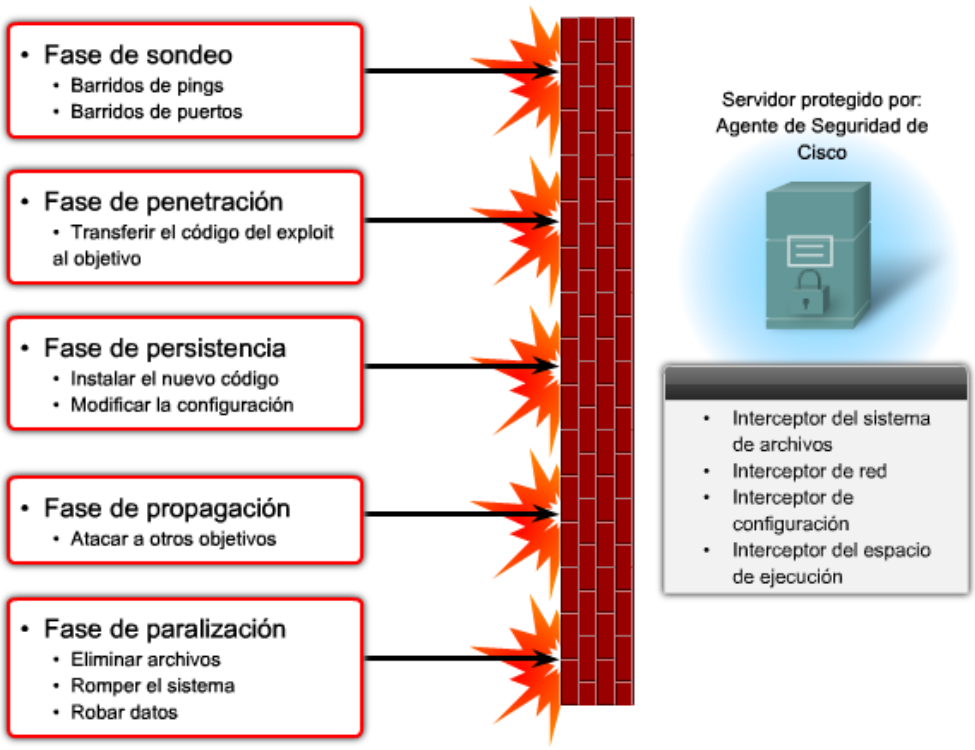
Aplicación de seguridad	Interceptor de red	Interceptor de sistema de archivos	Interceptor de configuración	Interceptor de espacio de ejecución
Firewall distribuido	X	N/A	N/A	N/A
Prevención de intrusión de host	X	N/A	N/A	X
Aislamiento de aplicaciones	N/A	X	X	X
Prevención de gusanos de red	X	N/A	N/A	X
Monitor de integridad de archivos	N/A	X	X	N/A

Existen miles de variantes de ataques maliciosos y constantemente surgen nuevos ataques con el fin de aprovechar las vulnerabilidades descubiertas. Un análisis de la progresión lógica de un ataque ayuda a ilustrar como casi cualquier ataque intenta obtener el control de mecanismos centrales del sistema objetivo. Existen diferencias significativas entre los mecanismos de ataque utilizados en las fases de sondeo y de penetración en comparación con los mecanismos de ataque en la fase de persistencia.

Las primeras dos etapas cambian en forma continua, a medida que se descubren nuevas vulnerabilidades y nuevos exploits son creados casi a diario. Combatir ataques en las fases de sondeo y de penetración requiere una constante actualización de firmas de IPS maliciosos y defensas de firewall, a medida que estos ataques evolucionan. En estas etapas tempranas, los ataques también se prestan a técnicas de evasión, tales como la codificación Unicode de cadenas web o el solapamiento de fragmentos de paquetes. Ataques que se alteren en la etapa de penetración requieren una cantidad significativa de investigación ya que pueden generar falsas alarmas, las cuales requieren una extensa revisión de un administrador de seguridad.

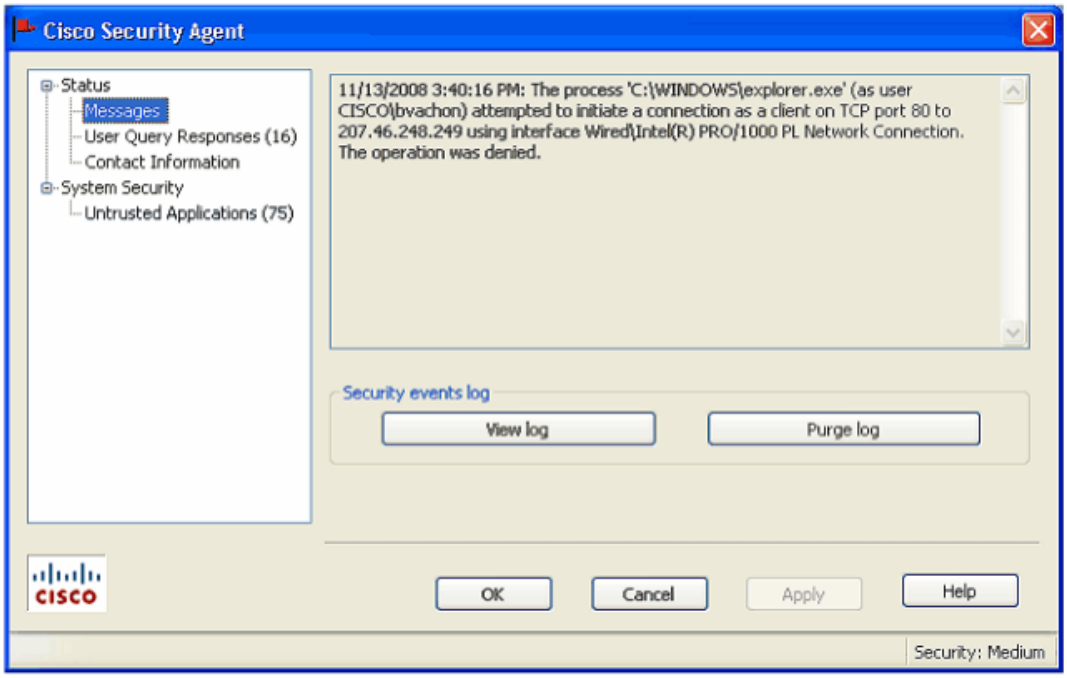
En contraste con esto, los mecanismos de ataque en la fase de persistencia y las fases siguientes son comparativamente estables. Las actividades maliciosas de un atacante se ven limitadas y un ataque requiere realizar llamadas del sistema al kernel con el fin de acceder a los recursos del sistema. El código malicioso puede intentar modificar el sistema operativo, modificar archivos, crear o alterar conexiones de red, o violar el espacio de memoria del proceso activo.

Debido a que la identificación consistente en ataques en sus fases tempranas es casi imposible, CSA se enfoca en proveer una seguridad proactiva controlando el acceso a los recursos del sistema. Este enfoque evita la necesidad de actualizar las defensas para mantenerse al día con los ataques más recientes y proteger al host de nuevos ataques. Por ejemplo, los gusanos Nimda y Slammer costaron millones de dólares en daños a empresas durante su primer día de aparición, antes de que hubiera actualizaciones disponibles, pero CSA evitó estos ataques identificando su comportamiento malicioso sin la necesidad de actualizaciones.



CSA genera mensajes en las máquinas cliente, los cuales son registrados y están visibles en la consola CSA. Un usuario o administrador puede revisar estos mensajes registrados. Estos mensajes incluyen fecha y hora, severidad, texto descriptivo, código de evento, nombre del archivo, nombre del proceso, IP origen y destino, ID de regla, código de botón, puertos origen y destino, usuario, paquete de red y evento en crudo.

IronPort, NAC y CSA trabajan en conjunto para proveer una solución completa, exhaustiva y transparente para la seguridad de terminales de una LAN. Sin embargo, una LAN puede ser vulnerable a un gran número de ataques de capa 2 y ataques de VLAN. Más allá de la seguridad de terminales, la mitigación de ataque en la LAN es una prioridad.



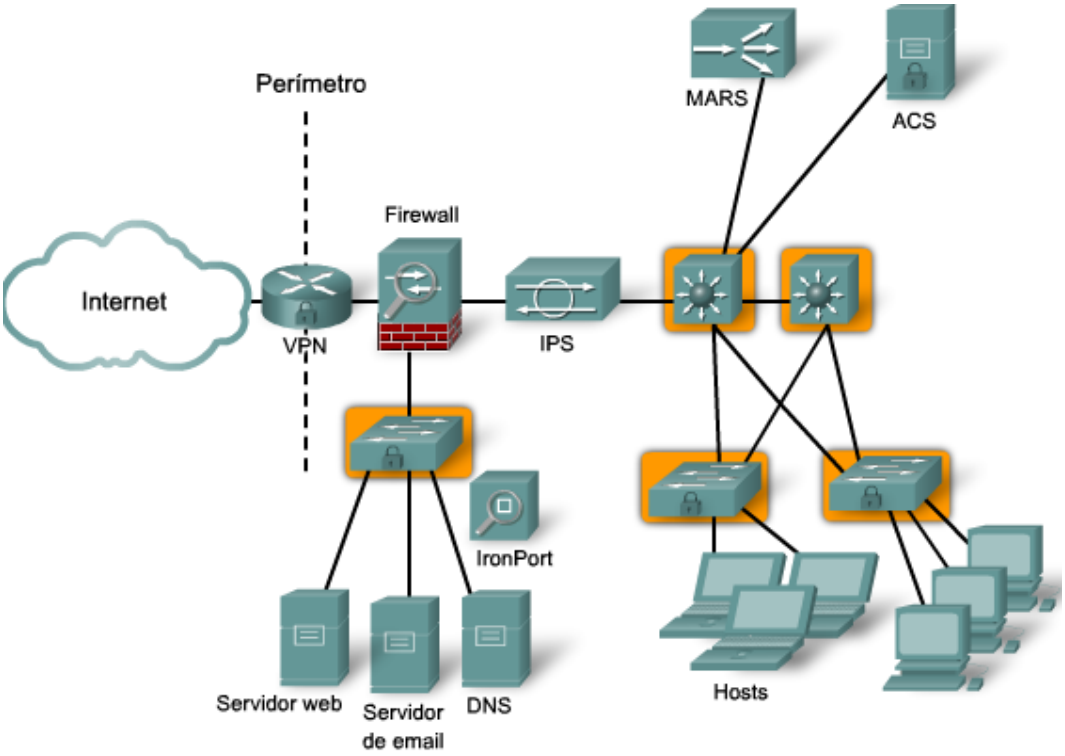
6.2 Consideraciones de seguridad de capa 2

6.2.1 Introduccion a la seguridad de capa 2

Los profesionales de seguridad de redes deben mitigar ataques dentro de la infraestructura de capa 2. Estos ataques incluyen la falsificación de direcciones MAC (spoofing), manipulación de STP, desbordamiento de la tabla de direcciones MAC, tormentas de LAN y ataques de VLAN.

El primer paso en la mitigación de ataques como estos es comprender las amenazas subyacentes impuestas por la infraestructura de capa 2. La capa 2 puede ser un eslabón muy débil para las capas OSI superiores, ya que si la capa 2 se ve comprometida, los hackers pueden trabajar luego hacia arriba. Es importante para el profesional de seguridad de redes recordar que los ataques de capa 2 suelen requerir acceso desde el interior, ya sea un empleado o un visitante.

Otra consideración fundamental es el desbordamiento del buffer. Los desbordamientos de buffer son a menudo la fuente de los ataques DoS. Los desbordamientos de buffer pueden ser utilizados para permitir la ejecución de código arbitrario dentro de un programa, y obtener privilegios no autorizados.

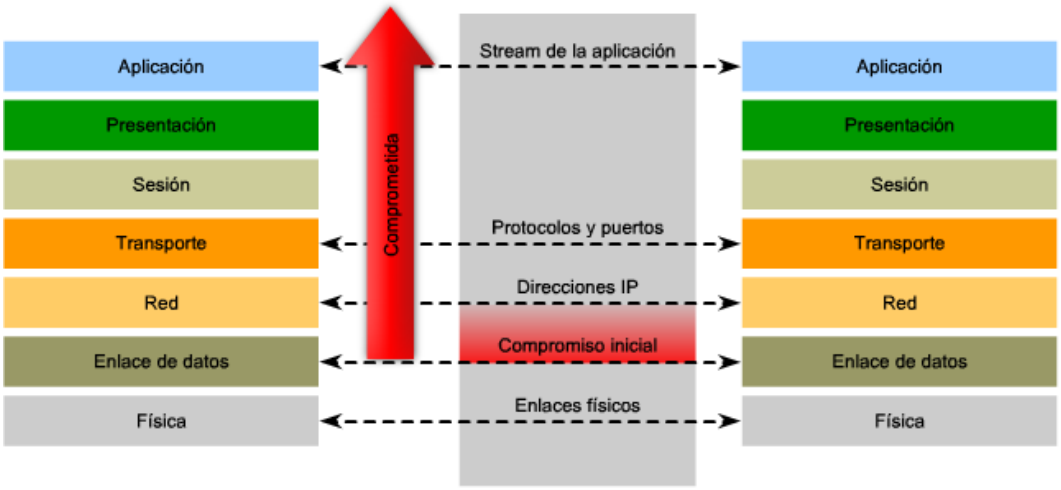


La capa 2 es la capa de enlace de datos en el modelo OSI. Es una de las siete capas diseñadas para trabajar en conjunto, pero con autonomía. La capa 2 opera por encima de la capa física y debajo de las capa de red y transporte. La independencia de la capa 2 permite la interoperabilidad y la interconectividad. Desde la perspectiva de la seguridad, la independencia de la capa 2 crea un desafío ya que si la capa se ve comprometida, las otras capas no se enteran de este hecho, por lo que también quedan expuestas. La seguridad de la red es tan segura como su eslabón más débil, y ese eslabón es por lo general la capa de enlace de datos.

Para ayudar a prevenir la explotación de la capa 2, una aplicación debe validar de forma cuidadosa los datos ingresados por el usuario. Estos datos pueden contener datos con formatos incorrectos, secuencias de control o demasiados datos, como es el caso del desbordamiento del buffer. Debe recordarse que los exploits de desbordamiento de buffer intentan sobrescribir la memoria de una aplicación.

Los desbordamientos de buffer son tal vez el método más común de ataque a aplicaciones actualmente en Internet. Son los más utilizados para obtener acceso a los privilegios de root o para causar ataques DoS.

Las herramientas como el Agente de Seguridad de Cisco pueden ser utilizadas para prevenir desbordamientos de buffer.



- Si la capa de enlace de datos es hackeada, las comunicaciones se ven comprometidas sin que las otras capas sean conscientes de este problema.
- La seguridad es sólo tan fuerte como el eslabón nás débil.
- Al hablar de seguridad de una red, la Capa de Enlace de Datos es en general el eslabón más débil.

6.2.2 Ataques de falsificación de direcciones MAC

A diferencia de los hubs, los switches regulan el flujo de datos entre sus puertos, creando redes instantáneas que contiene sólo los dos dispositivos que se comunican entre sí en un momento determinado. Los switches logran esto reenviando los datos por puertos específicos en base a las direcciones MAC. Los switches mantienen tablas de direcciones MAC, también conocidas como tablas de memoria de contenido direccionable (CAM - Content-Addressable Memory), para hacer un seguimiento de las direcciones MAC origen asociadas con cada puerto de conmutación. Estas tablas son completadas mediante un proceso de aprendizaje de direcciones del switch.

Es importante notar que las tramas de datos son enviadas por sistemas y dispositivos finales, y sus direcciones de origen y destino no son modificadas en todo el dominio de conmutación. Si un switch recibe una trama de datos y su dirección MAC de destino no está en la tabla, el switch reenvía la trama a través de todos sus puertos, excepto el puerto por el que fue recibida la trama. Cuando el nodo destino responde, el switch registra la dirección MAC de dicho nodo en la tabla de direcciones a partir del campo de dirección de origen de la trama. El switch completa la tabla de direcciones MAC registrando la dirección MAC de origen de una trama, y asociando dicha dirección con el puerto por el que la trama fue recibida.

En redes con múltiples switches conectados entre sí, las tablas de direcciones MAC registran múltiples direcciones para los puertos de interconexión de los switches. Estas direcciones MAC reflejan nodos remotos o nodos que se encuentran conectados a otro switch dentro del dominio de conmutación.

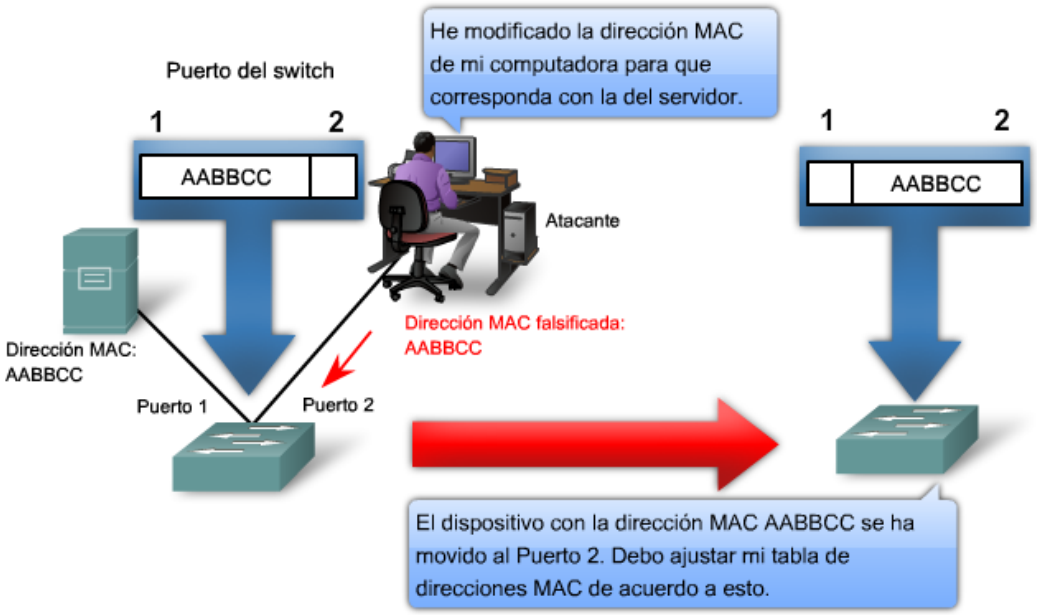
El método utilizado por los switches para completar la tabla de direcciones MAC conlleva a la vulnerabilidad conocida como falsificación de MAC. Los ataques de

falsificación ocurren cuando un host se hace pasar por otro para recibir datos que le serían inaccesibles de otra forma o para sortear configuraciones de seguridad.



Lo ataques de falsificación de MAC ocurren cuando un atacante altera la dirección MAC de su host de forma tal que coincida con la dirección MAC de otro host conocido. El host atacante envía entonces una trama a través de la red con la nueva dirección MAC configurada. Cuando el switch recibe la trama, examina su dirección MAC origen. El switch sobrescribe la entrada correspondiente a dicha dirección MAC, asignándole un nuevo puerto. A partir de ese momento, las tramas destinadas al host original son redirigidas inadvertidamente al host atacante.

Cuando el switch modifica la tabla de direcciones MAC, el host original no recibe más tráfico hasta que él mismo envía tráfico. Cuando el host original envía tráfico, el switch recibe y examina la trama, resultando en una nueva modificación de la tabla de direcciones MAC, volviendo a asociar la dirección MAC al puerto original.

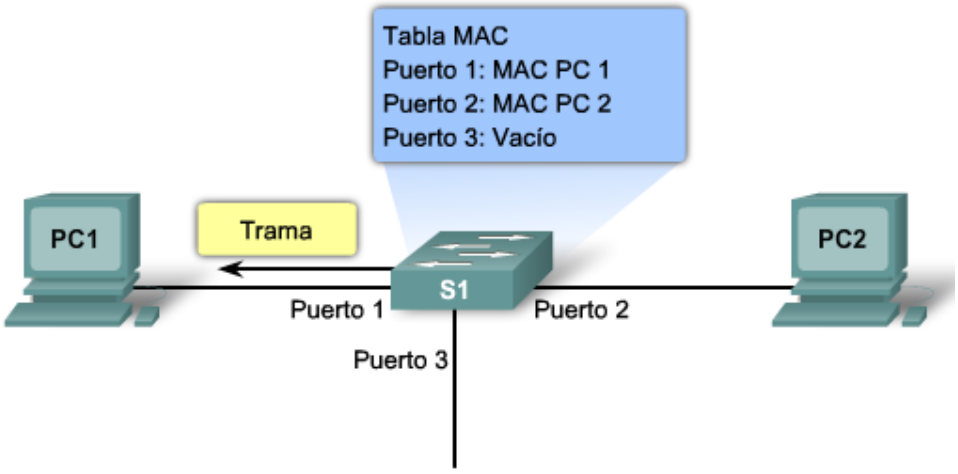


6.2.3 Ataques por desbordamiento de la tabla de direcciones MAC

Además de los ataques de falsificación de MAC, los ataques por desbordamiento de la tabla de direcciones MAC también son posibles en los dispositivos de capa 2. Recuerde que los switches utilizan direcciones MAC para dirigir las comunicaciones de la red a través de la trama de conmutación (switch fabric) hasta el puerto apropiado, hacia el nodo destino. El término trama (fabric) se refiere a los circuitos integrados y la programación del dispositivo que permiten la operación del equipo. Por ejemplo, la trama de conmutación es la responsable de controlar los caminos que atraviesan los datos en el switch. La tabla de direcciones MAC del switch contiene las direcciones MAC que se encuentran accesibles a través de un puerto físico determinado y los parámetros de VLAN asociados a cada uno. Cuando un switch de capa 2 recibe una trama, busca la dirección MAC destino en la tabla de direcciones MAC y reenvía la trama según corresponda.

La clave para comprender cómo funcionan los ataques por desbordamiento de direcciones MAC es saber que las tablas de direcciones MAC tienen un tamaño limitado. La inundación MAC se aprovecha de esta limitación bombardeando al switch con direcciones MAC falsas, hasta llenar por completo la tabla de direcciones MAC. Si se ingresan las suficientes entradas en dicha tabla antes de que expiren las más antiguas, la tabla se llena al punto en que no pueden aceptarse nuevas direcciones MAC. Cuando esto ocurre, el switch comienza a inundar todos sus puertos con todo el tráfico entrante, ya que no puede aprender más direcciones MAC legítimas. El switch, en esencia, funciona como un hub. Como resultado, el atacante puede ver todas las tramas enviadas entre otros dos hosts. El tráfico es reenviado sólo dentro de la misma VLAN, por lo que el intruso sólo puede ver el tráfico de la VLAN en la que se encuentre conectado.

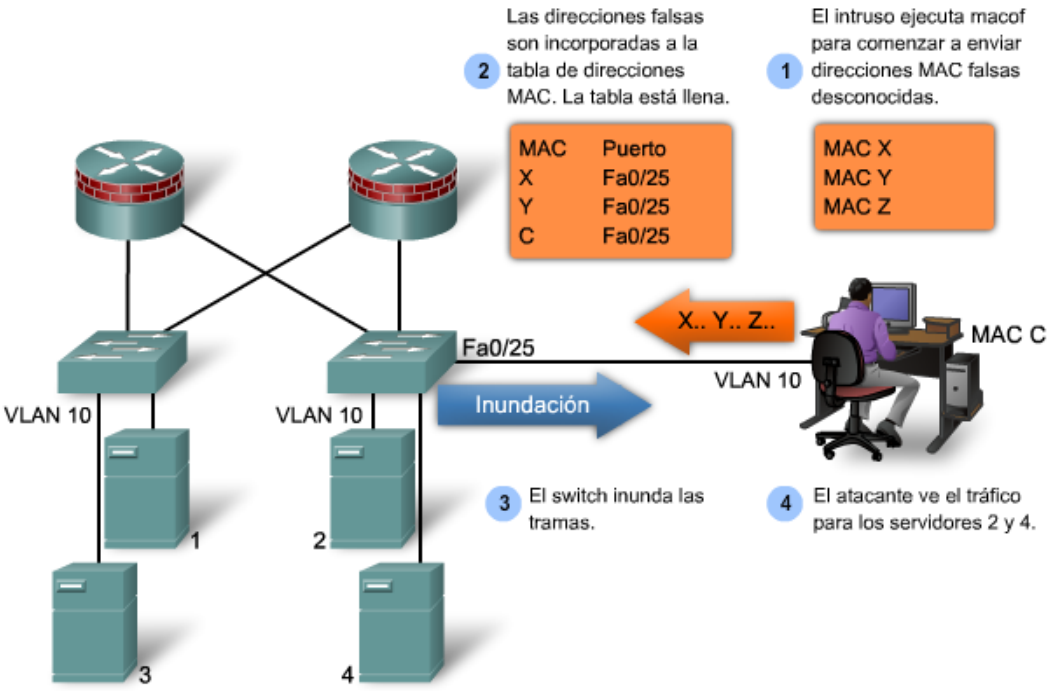
Si el intruso no mantiene la inundación de direcciones MAC inválidas, eventualmente el switch hará envejecer las entradas más antiguas de la tabla de direcciones MAC y volverá a actuar nuevamente como un switch.



El switch puede reenviar tramas entre PC1 y PC2 sin causar inundaciones debido a que la tabla de direcciones MAC contiene mapeos entre puertos y direcciones MAC oara estas PCs.

La forma más común para implementar un ataque por desbordamiento de la tabla de direcciones MAC es utilizando la herramienta macof . Esta herramienta inunda el switch con tramas que con tienen direcciones MAC e IP de origen y destino generadas en forma aleatoria. Durante un corto período de tiempo, la tabla de direcciones MAC se llena. Cuando la tabla se encuentra completa con direcciones MAC inválidas, el switch comienza a reenviar todas las tramas que recibe, a través de todos sus puertos. Mientras macof se esté ejecutando, la tabla del switch permanece llena y el switch continúa comportándose de esta forma.

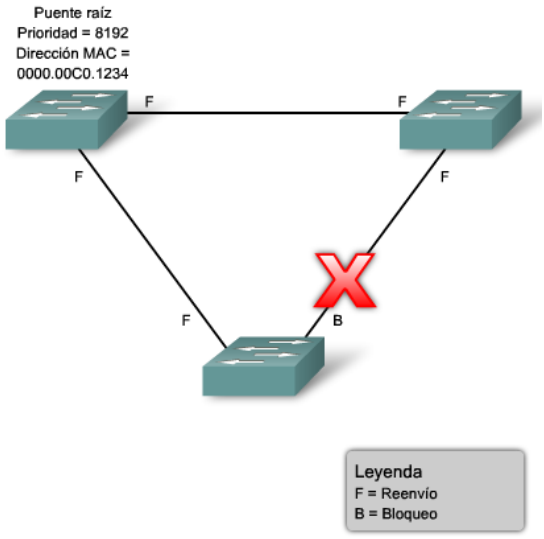
Tanto los ataques de falsificación de MAC como los ataques por desborde de la tabla de direcciones MAC pueden ser mitigados configurando seguridad de puertos en el switch. Con la seguridad de puertos, el administrador puede especificar en forma estática las direcciones MAC en un puerto particular del switch o bien puede permitir que el switch aprenda en forma dinámica un número determinado de direcciones MAC por cada puerto. En general, especificar en forma estática las direcciones MAC no es una solución administrable en un ambiente de producción. Permitir que el switch aprenda en forma dinámica un número fijo de direcciones MAC es una solución administrativamente escalable.



6.2.4 Ataques de manipulación STP

Otra vulnerabilidad en los dispositivos de capa 2 es el Protocolo de Spanning Tree (STP). STP es un protocolo de capa 2 que asegura una topología libre de bucles. STP opera seleccionando un puente raíz y construyendo una topología de árbol a partir de dicha raíz. STP admite redundancia, pero al mismo tiempo asegura que sólo un enlace se encuentra operacional en un momento dado y no existen bucles.

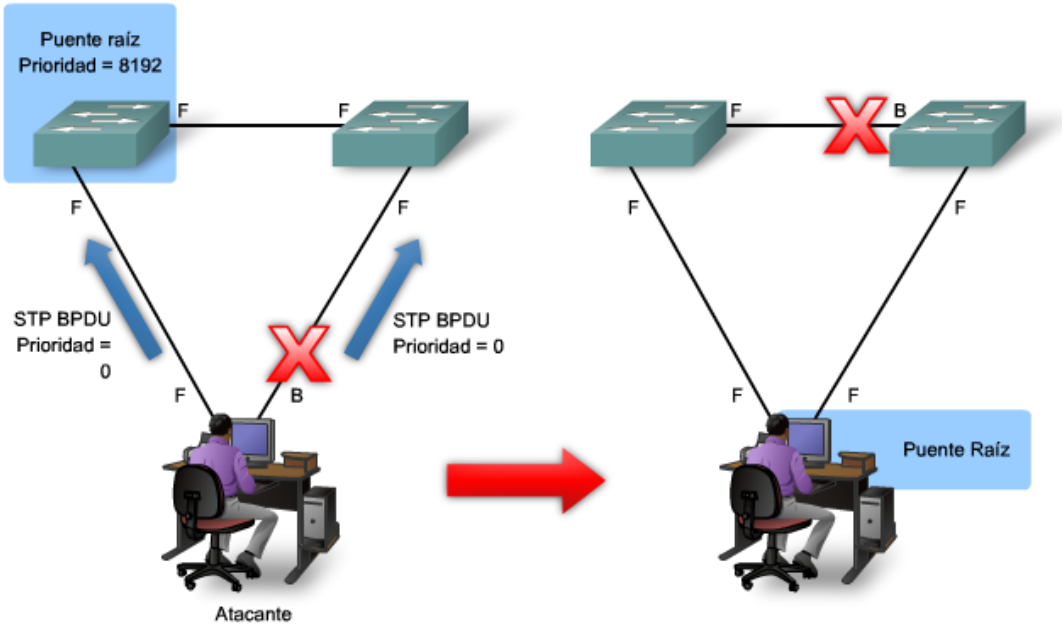
Los atacantes de la red pueden manipular a STP para llevar adelante su ataque, modificando la topología de la red. Un atacante puede lograr que su host sea visto como el puente raíz, falsificando así al puente raíz real. Todo el tráfico del dominio conmutado inmediato atraviesa entonces el puente raíz falso (el sistema atacante).



Para llevar adelante un ataque de manipulación de STP, el host atacante realiza un broadcast de BPDUs con cambios en la topología y configuración del STP, forzando la re-calculación del spanning-tree. Los BPDUs enviados por el host atacante anuncian la presencia de un puente con menor prioridad, en un intento de ser seleccionado como el puente raíz. Si tiene éxito, el host atacante se convierte en el puente raíz y puede observar una variedad de tramas que le resultarían inaccesibles de otra forma.

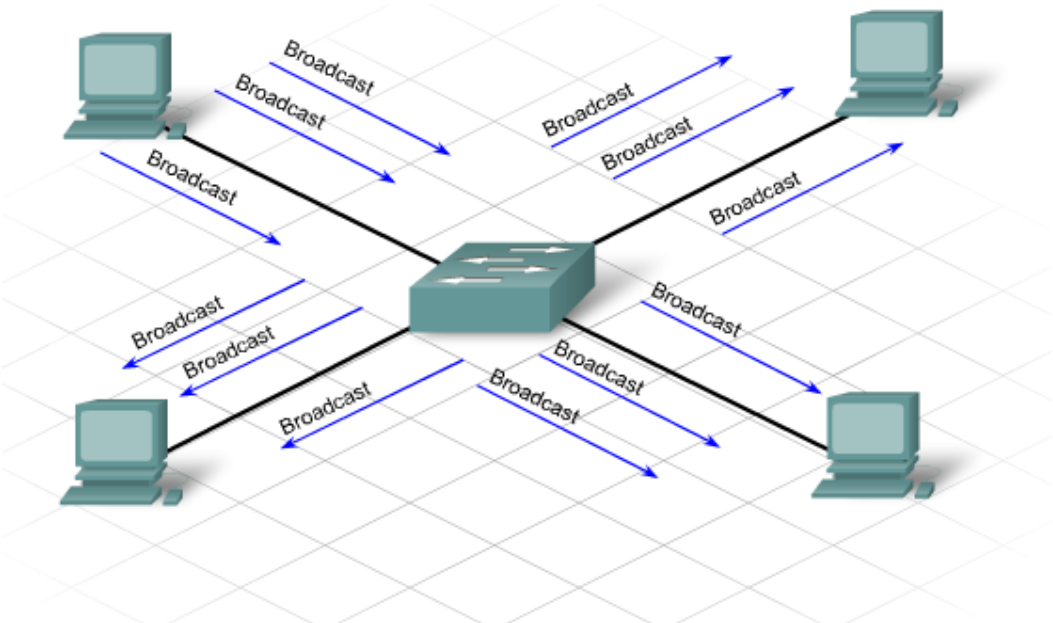
Este ataque puede ser utilizado para usurpar los tres objetivos de la seguridad: confidencialidad, integridad y disponibilidad.

Las técnicas de mitigación para la manipulación de STP incluyen la habilitación de PortFast y la utilización de root guard y BPDU guard.



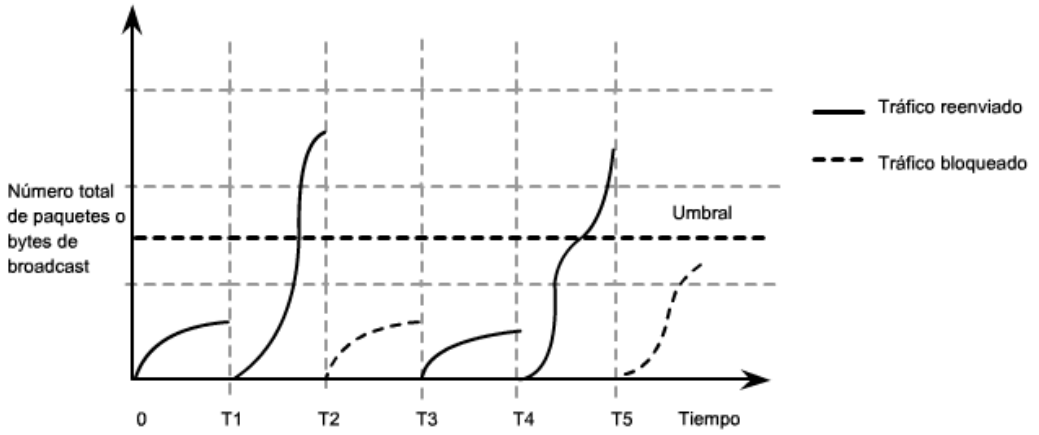
6.2.5 Ataques de tormenta de LAN

Los dispositivos de capa 2 son también vulnerables a los ataques de tormenta de LAN. Una tormenta de LAN ocurre cuando los paquetes inundan la LAN, creando un exceso de tráfico y degradando el desempeño de la red. Estas tormentas pueden ser causadas por errores en la implementación de la pila de protocolos, errores en la configuración de la red, o por usuarios realizando ataques DoS. También pueden ocurrir tormentas de broadcast. Debe recordar que los switches siempre reenvían las tramas de broadcast a través de todos sus puertos. Algunos protocolos necesarios, tales como el Protocolo de Resolución de Direcciones (ARP) y el Protocolo de Configuración Dinámica de Hosts (DHCP), utilizan broadcast. Por lo tanto, los switches deben ser capaces de reenviar el tráfico de broadcast.



Todos los puertos de la misma VLAN son inundados con paquetes broadcast, multicast, o unicast. Estas tormentas pueden incrementar la utilización del CPU en un switch hasta un 100%, reduciendo el desempeño de la red.

Si bien no es posible prevenir todos los tipos de tormentas de paquetes y broadcast excesivos, sí es posible suprimirlos implementando un control de tormentas. El control de tormentas previene las alteraciones en el tráfico de una LAN causadas por tormentas de broadcast, multicast o unicast provenientes de una interfaz física. El control de tormentas (o supresión de tráfico) monitorea los paquetes que pasan desde una interfaz hacia el bus de conmutación y determina si el paquete es unicast, multicast o broadcast. El switch cuenta el número de paquetes de cada tipo específico recibidos en un cierto período de tiempo y compara estas medidas con un umbral de supresión predefinido. El control de tormentas bloquea el tráfico cuando el límite definido es alcanzado.



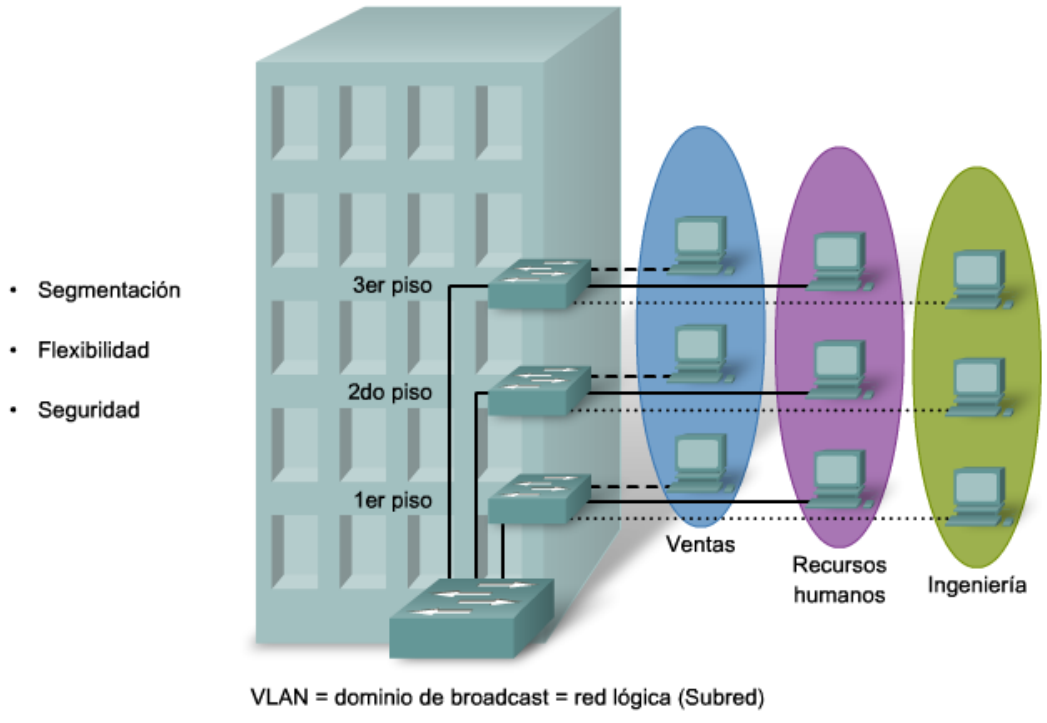
Si el control de tormentas se encuentra habilitado, cuando la cantidad de tráfico especificado excede el umbral dentro de un lapso de tiempo especificado, todo el tráfico del mismo tipo es descartado durante el próximo lapso de tiempo. En este ejemplo, el tráfico de broadcast reenviado excedió el umbral configurado entre los intervalos de tiempo T1 y T2, y entre T4 y T5. Por lo tanto, el tráfico de broadcast es bloqueado durante los intervalos que siguen a T2 y T5. En el próximo intervalo de tiempo (por ejemplo, T3), si el tráfico de broadcast no excede el umbral, entonces es nuevamente reenviado.

6.2.6 Ataques de VLAN

Una VLAN es un dominio de broadcast lógico que se extiende a través de múltiples segmentos LAN. Dentro de la red conmutada, las VLANs proveen segmentación y flexibilidad en la organización. Una estructura de VLAN puede ser diseñada para permitir la agrupación de estaciones en forma lógica de acuerdo a su función, grupo de trabajo o aplicación, sin importar la ubicación física de los usuarios. Cada puerto del switch puede ser asignado sólo a una VLAN, agregando así una capa de seguridad. Los puertos de una VLAN comparten el broadcast, mientras que los puertos en diferentes VLAN no comparten broadcasts. Contener los broadcasts dentro de una VLAN mejora el desempeño general de la red.

Utilizando tecnología VLAN, es posible agrupar a los puertos del switch y sus usuarios conectados en comunidades definidas lógicamente, tales como trabajadores del mismo departamento, grupos de producción multifuncionales o diversos grupos que compartan la misma aplicación de red. Una VLAN puede existir en un único switch o extenderse a través de múltiples switches. Las VLANs pueden incluir hosts de un mismo edificio o ser infraestructuras de múltiples edificios. Las VLANs también pueden conectarse a través de redes de área metropolitana (MANs).

Existe varios tipos diferentes de ataques de VLAN que prevalecen en las redes conmutadas modernas. En lugar de listar todos los tipos de ataques, es importante comprender la metodología general detrás de estos ataques y los principales enfoques para mitigarlos.



La arquitectura de VLAN simplifica el mantenimiento de la red y mejora la performance, pero también abre la puerta a los abusos. El salto de VLAN (VLAN hopping) permite que el tráfico de una VLAN sea visto desde otra VLAN, con ayuda

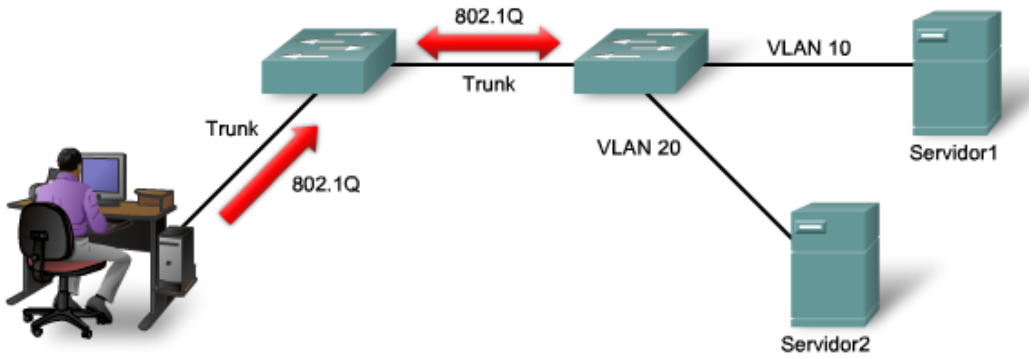
del router. Bajo determinadas circunstancias, los atacantes pueden capturar datos y extraer contraseñas y otra información sensible. El ataque funciona aprovechando un puerto troncal configurado incorrectamente. Por defecto, los puertos troncales tienen acceso a todas las VLANs y transmiten el tráfico de múltiples VLANs a través del mismo enlace físico, normalmente entre switches. Los datos que atraviesan estos enlaces pueden estar encapsulados con IEEE 802.1Q o ISL (Inter-Link Switch).

En un ataque básico de salto de VLAN, el atacante aprovecha la configuración automática por defecto de los enlaces troncales de la mayor parte de los switches. El atacante configura un sistema para que simule ser un switch. Esta falsificación requiere que el host atacante pueda emular las señales de ISL o 802.1Q junto con las señales del protocolo DTP (Dynamic Trunking Protocol) propietario de Cisco. Engañando al switch para que asuma que se trata de otro switch con un enlace troncal, el atacante puede obtener acceso a todas las VLANs permitidas en dicho enlace. Para tener éxito, este ataque requiere que el puerto se encuentre configurado con trunking automático o dinámico. Como resultado, el atacante es miembro de todas las VLANs admitidas en el enlace troncal y por lo tanto puede enviar y recibir tráfico a todas las VLANs.

Un ataque de salto de VLAN puede ser disparado de dos formas:

Mediante la falsificación de mensajes DTP del host atacante, generando que el switch ingrese en modo de trunking. A partir de aquí, el atacante puede enviar tráfico etiquetado con la VLAN deseada y el switch luego envía los paquetes al destino. Incorporando un switch ilegal y habilitando el trunking. El atacante tiene así acceso a las VLANs del switch atacado a partir del switch ilegal.

La mejor forma de prevenir los ataques básicos de salto de VLAN consiste en deshabilitar el trunking en todos los puertos, a excepción de aquellos que lo requieran. En los puertos donde el trunking deba estar disponible, se deben deshabilitar las negociaciones DTP y habilitar el trunking en forma manual.



El atacante ve el tráfico destinado a los servidores.

Otro tipo de ataque de VLAN es el ataque de salto de VLAN con doble etiquetado (o doble encapsulación). Este tipo de ataque toma ventaja de la forma en la que opera el hardware de la mayoría de los switches. En general los switches realizan sólo un nivel de des-encapsulación 802.1Q. Esto permite al atacante, en determinadas situaciones, pueda insertar una etiqueta 802.1Q oculta dentro de la trama. Esta etiqueta permite que

la trama sea dirigida a una VLAN diferente a la especificada en la etiqueta 802.1Q original. Una característica importante de los ataques de salto de VLAN con doble encapsulación es que funciona incluso si los enlaces troncales se encuentran deshabilitados.

Un ataque de salto de VLAN con doble encapsulación consiste de cuatro pasos:

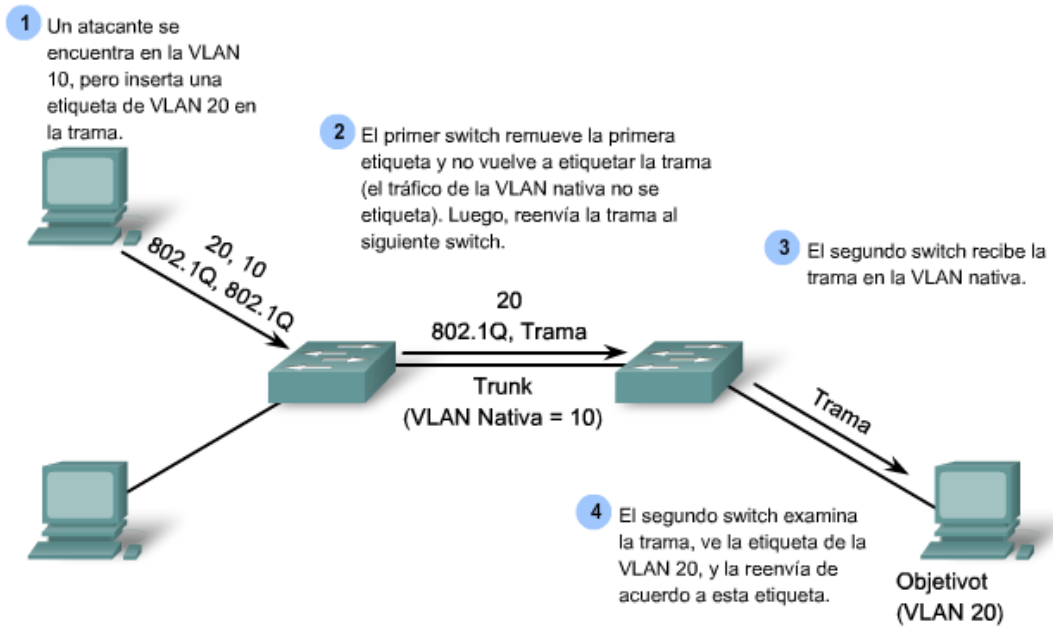
1. El atacante envía una trama con una doble etiqueta 802.1Q al switch. El encabezado externo tiene la etiqueta de VLAN del atacante, que es igual a la VLAN nativa del puerto troncal. A los fines de este ejemplo, asuma que es la VLAN 10. La etiqueta interna es la VLAN víctima, en este ejemplo, la VLAN 20.

2. La trama llega al switch, el cual toma la primera etiqueta 802.1Q de 4 bytes. El switch observa que la trama está destinada a la VLAN 10, que es la VLAN nativa. El switch entonces reenvía el paquete a través de los puertos de la VLAN 10 luego de remover la etiqueta de la VLAN 10. En el puerto troncal, una vez removida la etiqueta de la VLAN 10, el paquete no es vuelto a etiquetar ya que es parte de la VLAN nativa. En este punto, la etiqueta de la VLAN 20 se encuentra intacta y no ha sido inspeccionada por el primer switch.

3. La trama llega al segundo switch, quien desconoce que originalmente correspondía a la VLAN 10. El tráfico de la VLAN nativa no es etiquetado por el switch que lo envía, de acuerdo a la especificación de 802.1Q.

4. El segundo switch sólo ve la etiqueta 802.1Q interna enviada por el atacante y asume que la trama está destinada a la VLAN 20. El segundo switch envía la trama al puerto de la víctima o lo distribuye por todos sus puertos, dependiendo de si existe una entrada en la tabla de direcciones MAC para el host destino.

Este tipo de ataque es unidireccional y funciona sólo cuando el atacante y el puerto troncal se encuentran en la misma VLAN nativa. No es tan sencillo frustrar este tipo de ataques como lo es en el caso de los ataques de salto de VLAN básicos. La mejor solución consiste en asegurar que la VLAN nativa del puerto troncal es diferente a la VLAN nativa de los puertos de usuario. De hecho, se considera una buena práctica de seguridad el utilizar como señuelo una VLAN que no se encuentre en uso en una LAN conmutada para que funcione como VLAN nativa para todos los enlaces troncales 802.1Q en la red.



Nota: este ataque funciona sólo si el enlace troncal usa la misma VLAN nativa que el atacante.

6.3 Configuracion de la seguridad de capa 2

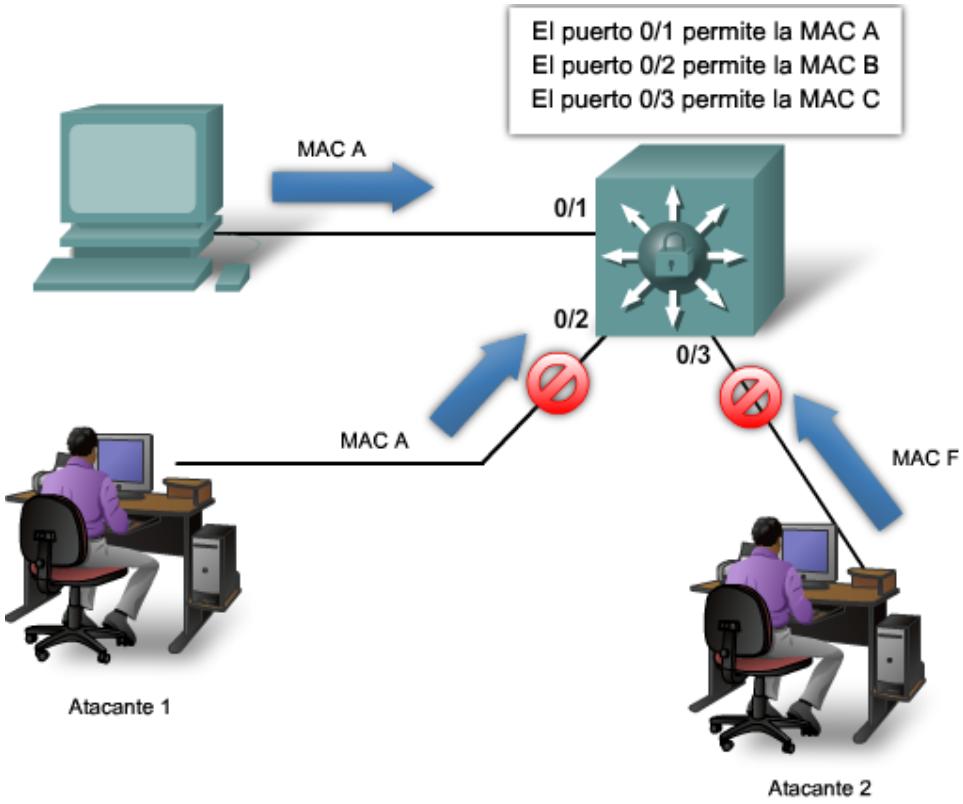
6.3.1 Configuracion de la seguridad de puertos

Una vez comprendidas las vulnerabilidades de los dispositivos de capa 2, el próximo paso consiste en implementar técnicas de mitigación para prevenir los ataques que se aprovechan de dichas vulnerabilidades. Por ejemplo, para prevenir la falsificación de MAC y el desbordamiento de la tabla de direcciones MAC, debe habilitarse seguridad de puertos (port security).

La seguridad de puertos permite a los administradores especificar en forma estática las direcciones MAC permitidas en un puerto determinado, o permitir al switch aprender en forma dinámica un número limitado de direcciones MAC. Limitando a uno el número de direcciones MAC permitidas en un puerto, la seguridad de puerto puede ser utilizada para controlar la expansión no autorizada de la red.

Una vez que las direcciones MAC son asignadas a un puerto seguro, dicho puerto no reenvía tramas cuyas direcciones MAC de origen no se encuentren en el grupo de direcciones definidas. Cuando un puerto configurado con seguridad recibe una trama, se compara la dirección MAC de origen de la trama contra la lista de direcciones de origen seguras que fueron configuradas en forma manual o automática (aprendidas) en el puerto. Si la dirección MAC de un dispositivo conectado al puerto no se encuentra en la lista de direcciones seguras, el puerto puede apagarse hasta ser habilitado nuevamente por un administrador (modo por defecto) o bien puede descartar las tramas provenientes de hosts no seguros (modo "restrict"). El comportamiento del puerto depende en cómo se encuentra configurado para responder a una violación de seguridad.

Se recomienda que el administrador configure la seguridad de puertos para que los mismos se apaguen en lugar de descartar tramas ante una violación de seguridad. La opción "restrict" puede fallar ante la carga de un ataque intensivo.



Los siguientes son los pasos necesarios para configurar seguridad de puertos en un puerto de acceso:

Paso 1. Configure una interfaz como interfaz de acceso.

Switch(config-if)# switchport mode access

Si la interfaz se encuentra en el modo por defecto (dynamic auto), la misma no puede ser configurada como un puerto seguro.

Paso 2. Habilitar la seguridad de puerto en la interfaz utilizando el comando switchport port-security.

La sintaxis completa incluye un conjunto de parámetros opcionales.

Switch(config-if)# switchport port-security [mac-address dirección-mac [vlan {id-vlan | {access | voice}}]] | [mac-address sticky [dirección mac| vlan {id-vlan | {access | voice}}]] [maximum valor [vlan {vlan-list | {access | voice}}]]

Paso 3. Configurar el número máximo de direcciones MAC seguras para la interfaz. (Opcional)

Switch(config-if)# switchport port-security maximum valor

El rango es entre 1 y 132. El valor por defecto es 1.



Haga clic sobre cada botón para ver el contenido asociado.

Parámetro	Descripción
mac-address *mac-address*	(Opcional) Especifica una dirección MAC segura para el puerto, ingresando la dirección MAC de 48 bits. Es posible agregar direcciones MAC adicionales hasta la cantidad máxima configurada.
vlan *vlan-id*	(Opcional) Sólo para los puertos troncales, especificar la ID de VLAN y la dirección MAC. Si no se especifica una ID de VLAN, se utiliza la VLAN nativa.
vlan access	(Opcional) Sólo para los puertos de acceso, especificar la VLAN como una VLAN de acceso.
vlan voice	(Opcional) Sólo para puertos de acceso, especificar la VLAN como una VLAN de Voz. Nota: La palabra clave **voice** se encuentra disponible sólo si se ha configurado una VLAN de voz en el puerto, y si dicho puerto no se encuentra en una VLAN de acceso.
mac-address sticky [*mac-address*]	(Opcional) Habilita la interfaz para el aprendizaje de modo sticky, ingresando sólo las palabras clave **mac-address sticky**. Cuando el aprendizaje sticky se encuentra habilitado, la interfaz incorpora todas las direcciones MAC seguras que aprende en forma dinámica, guardándolas en la configuración de ejecución, y convirtiendo dichas direcciones en direcciones MAC seguras sticky. Nota: Es posible especificar una dirección MAC segura sticky ingresando las palabras clave **mac-address sticky** *mac-address*. Sin embargo, para ingresar direcciones MAC seguras estáticas, se recomienda utilizar el comando de configuración de interfaz **mac-address** *mac-address*.
maximum *value*	(Opcional) Configura el número máximo de direcciones MAC seguras permitidas para la interfaz. El número máximo de direcciones que puede ser configurado en un switch está dado por el número máximo de direcciones MAC permitidas en un sistema. El SDM determina este número, el cual representa el total de direcciones MAC disponibles, incluyendo aquellas utilizadas por otras funciones de capa 2, y cualquier dirección MAC de origen configurada en las interfaces. Por defecto, la configuración es 1.
vlan [*vlan-list*]	(Opcional) Para los enlaces troncales, es posible configurar un número máximo de direcciones MAC seguras permitidas en una VLAN. Si la palabra clave **vlan** no es ingresada, se utiliza el valor por defecto. **vlan**: configura un valor máximo por VLAN. **vlan** *vlan-list*: configura un valor máximo por VLAN en un rango de VLANs separado por un guión, o en una serie de VLANs separadas por comas. Para las VLANs no especificadas, se utiliza el valor máximo por defecto.



Haga clic sobre cada botón para ver el contenido asociado.

Una vez habilitada la seguridad del puerto, es necesario establecer las reglas de violación del puerto de acceso. Las reglas de violación se refieren a las acciones que debe realizar el switch en el caso de que ocurra una violación de seguridad.

Estos son los pasos para configurar la violación de seguridad del puerto en un puerto de acceso:

Paso 1. Configure el modo de violación. Esta es la acción que el switch realiza cuando se detecta una violación de seguridad. Si no se especifica un modo de violación, el modo por defecto apaga administrativamente el puerto.

Switch(config-if)# switchport port-security violation {protect | restrict | shutdown | shutdown vlan}

Cuando un puerto seguro se encuentra en el estado "error-disable" (deshabilitado por error), significa que ha ocurrido una violación y el puerto se encuentra deshabilitado.

Para recuperar el funcionamiento del puerto, debe utilizarse el comando de configuración global errdisable recovery cause psecure-violation, o bien puede habilitarse en forma manual ingresando los comandos de configuración de interfaz shutdown y no shutdown.

Paso 2. Ingrese una dirección MAC segura estática para la interfaz.

Switch(config-if)# switchport port-security mac-address dirección-mac

Repita este comando cuantas veces sea necesario para cada dirección MAC segura que deba incorporarse.

Paso 3. Habilite el modo de aprendizaje "sticky" (adhesivo) en la interfaz.

Switch(config-if)# switchport port-security mac-address sticky

Cuando se encuentra habilitado el modo de aprendizaje "sticky", la interfaz agregará todas las direcciones MAC seguras que aprenda en forma dinámica hasta el máximo permitido configurado. Estas direcciones MAC se almacenan en la configuración de ejecución (running configuration).

Utilice el comando de configuración de interfaz no switchport port-security para devolver a la interfaz a su estado por defecto de puerto no seguro. Las direcciones seguras aprendidas como "sticky" permanecen como parte de la configuración de ejecución.

Utilice el comando de configuración de interfaz no switchport port-security maximum valor para devolver a la interfaz al número por defecto de direcciones MAC seguras.

Utilice el comando de configuración de interfaz no switchport port-security violation {protect | restrict} para devolver al modo de violación a su condición por defecto (modo shutdown).

```
Switch(config-if)#
switchport port-security violation {protect | restrict | shutdown |
shutdown vlan}
```

- Configura el modo de violación (opcional)

```
Switch(config-if)#
switchport port-security mac-address mac-address
```

- Ingresa una dirección MAC segura y estática para la interfaz (opcional)

```
Switch(config-if)#
switchport port-security mac-address sticky
```

- Habilita el aprendizaje sticky en la interfaz (opcional)

Configuración de violaciones de seguridad de Port Security | Parámetros de `switchport port-security violation`

Haga clic sobre cada botón para ver el contenido asociado.

Parámetro	Descripción
protect	(Opcional) Configura el modo de protección (protect) ante violaciones de seguridad. Cuando el número de direcciones MAC seguras alcanza el límite permitido para el puerto, los paquetes con direcciones de origen desconocidas son descartados hasta que se eliminan suficientes direcciones MAC seguras, o bien se incrementa el número máximo de direcciones permitidas. No se envían notificaciones cuando ocurre una violación de seguridad.
restrict	(Opcional) Configura el modo de restricción (restrict) ante violaciones de seguridad. Cuando el número de direcciones MAC seguras alcanza el límite permitido para el puerto, los paquetes con direcciones de origen desconocidas son descartados hasta que se eliminan suficientes direcciones MAC seguras, o bien se incrementa el número máximo de direcciones permitidas. Además, se envía una notificación SNMP, se registra un mensaje de syslog, y se incrementa el contador de violaciones.
shutdown	(Opcional) Configura el modo de desactivación (shutdown) ante violaciones de seguridad. En este modo, una violación de seguridad en un puerto causa que la interfaz sea inmediatamente deshabilitada por estado de error y se apague el LED frontal del puerto. Además, se envía una notificación SNMP, se registra un mensaje de syslog, y se incrementa el contador de violaciones. Cuando un puerto seguro se encuentra deshabilitado por estado de error, es posible reactivarlo ingresando el comando de configuración global **errdisable recovery cause psecure-violation**, o bien puede volver a habilitarse ingresando los comandos de configuración de interfaz **shutdown** y **no shutdown**.
shutdown vlan	Configura el modo de desactivación por VLAN ante violaciones de seguridad. En este modo, sólo la VLAN en la que ocurrió la violación queda deshabilitada por estado de error.

Configuración de violaciones de seguridad de Port Security | Parámetros de `switchport port-security violation`

Haga clic sobre cada botón para ver el contenido asociado.

El envejecimiento de la seguridad de puertos (Port Security Aging) puede ser utilizado para configurar los temporizadores de las direcciones seguras estáticas y dinámicas de un puerto. Es posible configurar dos tipos de envejecimiento por puerto:

Absoluto - Las direcciones seguras del puerto son eliminadas una vez concluido el tiempo de envejecimiento.
Inactividad - Las direcciones seguras del puerto son eliminadas sólo si se encuentran inactivas por el tiempo de envejecimiento especificado.

El envejecimiento permite remover direcciones MAC seguras de un puerto seguro si la necesidad de remover las direcciones MAC existentes en forma manual. Los temporizadores de envejecimiento pueden ser incrementados para asegurar que las direcciones MAC seguras más antiguas permanezcan incluso cuando se incluyan nuevas direcciones MAC. Debe considerarse que la cantidad máxima de direcciones seguras por puerto también puede ser configurada. El envejecimiento de las direcciones seguras configuradas en forma manual puede ser habilitado o deshabilitado por puerto.

Utilice el comando switchport port-security aging {static | time tiempo | type {absolute | inactivity}} para habilitar o deshabilitar el envejecimiento estático para un puerto seguro o para configurar el tipo y tiempo de envejecimiento.

```
Switch(config-if)#
switchport port-security aging {static | time time | type {absolute |
inactivity}}
```

- Habilita o deshabilita el envejecimiento estático de los puertos seguros, o configura el tiempo o tipo de envejecimiento.

Confguración de envejecimiento de Port Security

Parámetros de envejecimiento de Port Security

Haga clic sobre cada botón para ver el contenido asociado.

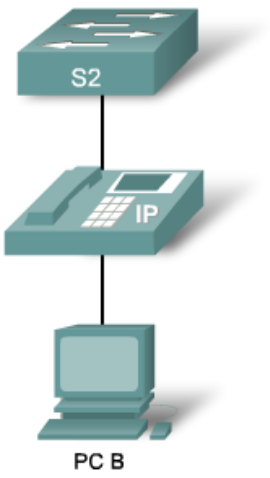
Parámetro	Descripción
static	Habilita el envejecimiento para direcciones seguras configuradas estáticamente en este puerto.
time *time*	Especifica el tiempo de envejecimiento de este puerto. El rango se encuentra entre 0 y 1440 minutos. Si el tiempo es 0, el envejecimiento queda deshabilitado en este puerto.
type absolute	Configura el tipo de envejecimiento absoluto. Todas las direcciones seguras de este puerto expiran exactamente luego del tiempo especificado (en minutos) y son removidas de la lista de direcciones seguras.
type inactivity	Configura el tipo de envejecimiento por inactividad. Las direcciones seguras en este puerto expiran cuando no se recibe tráfico proveniente de dicha dirección durante el período de tiempo especificado.

Confguración de envejecimiento de Port Security

Parámetros de envejecimiento de Port Security

Haga clic sobre cada botón para ver el contenido asociado.

Una configuración típica de seguridad para un puerto de voz requiere dos direcciones MAC seguras. Las direcciones en general son aprendidas en forma dinámica. Una dirección MAC corresponde al teléfono IP, y la otra dirección corresponde a la PC conectada al teléfono IP. Las violaciones a esta política suelen resultar en la deshabilitación del puerto. El temporizador de envejecimiento para las direcciones MAC aprendidas se configura en dos horas.




```
Switch(config-if)#
switchport mode access
switchport port-security
switchport port-security maximum 2
switchport port-security violation shutdown
switchport port-security mac-address sticky
switchport port-security aging time 120
```

6.3.2 Verificacion de la seguridad de puertos

Cuando la seguridad de puertos se encuentra habilitada, el administrador debe utilizar los comandos show para verificar si el puerto ha aprendido la dirección MAC. Además, los comandos show resultan de utilidad para monitorear y resolver problemas de las configuraciones de port-security. Pueden ser utilizados para ver información tal como el número máximo de direcciones MAC que pueden asociarse a un puerto, el contador de violaciones, o el modo actual de violación.

Utilice el comando show port-security para ver la configuración de seguridad de los puertos, incluyendo el contador de violaciones, las interfaces configuradas y las acciones de seguridad ante violaciones.

Utilice el comando show port-security [interface id-interfaz] para ver la configuración de seguridad de puerto para una interfaz específica, incluyendo el número máximo de direcciones MAC seguras permitidas para dicha interfaz, el número de direcciones MAC seguras conocidas por la interfaz, el número de violaciones de seguridad que han ocurrido y el modo de violación.

```
sw-class# show port-security
Secure Port  MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                 (Count)       (Count)          (Count)
-----------------------------------------------------------------------------
     Fa0/12              2            0                  0         Shutdown
-----------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

```
sw-class# show port-security interface f0/12
Port Security              : Enabled
Port status                : Secure-down
Violation mode             : Shutdown
Maximum MAC Addresses      : 2
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Aging time                 : 120 mins
Aging type                 : Absolute
SecureStatic address aging : Disabled
Security Violation Count   : 0
```

Utilice el comando show port-security [interface id-interfaz] address para ver todas las direcciones MAC seguras configuradas en todas las interfaces del switch o en una interfaz específica, junto con la información de envejecimiento correspondiente a cada dirección.

```
sw-class# show port-security address

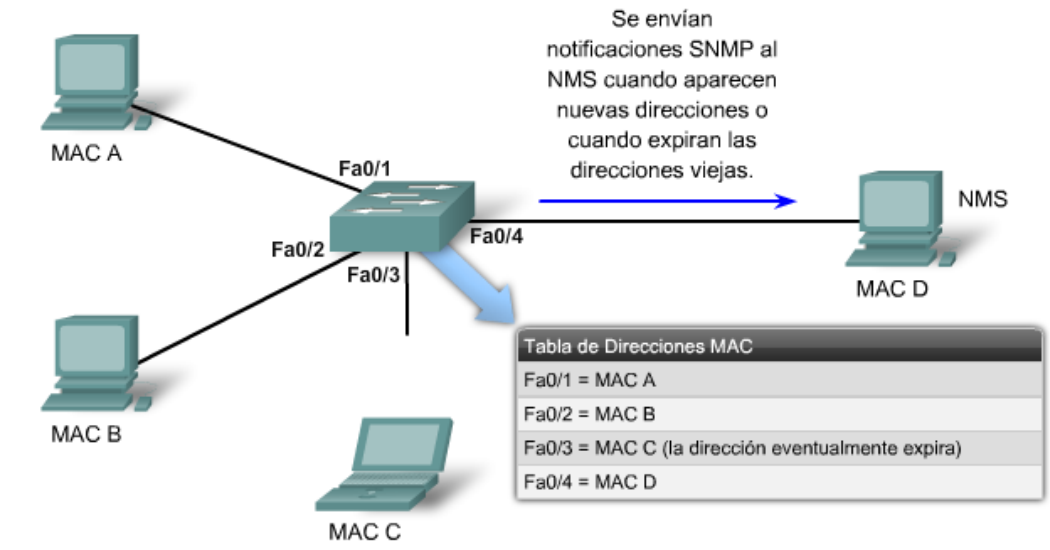
Secure Mac Address Table
------------------------------------------------------------------
Vlan    Mac Address       Type                Ports    Remaining Age
                                                          (mins)
----    -----------       ----                -----    -------------
   1    0000.ffff.aaaa    SecureConfigured    Fa0/12       -
------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 0
Max Addresses limit in System (excluding one mac per port) : 1024
```

Los administradores de red necesitan un método para monitorear quiénes están utilizando la red y dónde se encuentran. Por ejemplo, si el puerto F2/1 del switch es seguro, se genera un trap (notificación) SNMP cuando una entrada desaparece de la tabla de direcciones MAC de dicho puerto.

La funcionalidad de notificaciones de direcciones MAC envía traps SNMP a la estación de administración de la red (NMS - Network Management Station) cada vez que una dirección MAC se incorpora o se elimina de las tablas de reenvío. Las notificaciones de direcciones MAC son generadas sólo para las direcciones MAC dinámicas y seguras.

Las notificaciones de direcciones MAC permiten al administrador de la red monitorear las direcciones MAC aprendidas, así como también las direcciones MAC que son removidas al expirar su temporizador de envejecimiento.

Utilice el comando de configuración global mac address-table notification para habilitar las notificaciones de direcciones MAC en el switch.



En el ejemplo, la laptop con la MAC C se ha desconectado de la red. El temporizador del puerto Fa0/3 en el switch eventualmente expirará, y se enviará una notificación SNMP al servidor NMS.

6.3.3 Configuracion de BPDU Guard y Root Guard

Para mitigar la manipulación de STP, es necesario habilitar PortFast, root guard y BPDU guard, los comandos de mejora de STP. Estas funciones aseguran la selección de un puente raíz y hacen valer los límites del dominio STP.

PortFast

La función de spanning-tree PortFast causa que una interfaz configurada como un puerto de acceso de capa 2 realice la transición del estado bloqueado (blocking) al estado de reenvío (forwarding) en forma inmediata, pasando por alto los estados de escucha (listening) y aprendizaje (learning). PortFast puede ser utilizado en puertos de acceso de capa 2 para conectar una única estación de trabajo o servidor, para permitir a dichos dispositivos conectarse a la red en forma inmediata, en lugar de esperar a que finalice la convergencia de STP.

Debido a que el propósito de PortFast es minimizar el tiempo que los puertos de acceso deben esperar hasta que la convergencia de STP, este modo sólo debe ser utilizado en los puertos de acceso. Si se habilita PortFast en un puerto que se conecte con otro switch, existe el riesgo de crear un bucle de spanning-tree.

Este comando configura PortFast al mismo tiempo para todos los puertos no troncales.

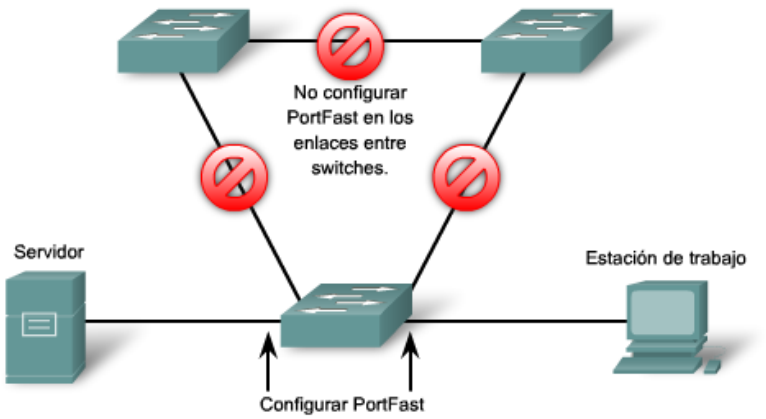
Switch(config)# spanning-tree portfast default

Este comando configura PortFast en una interfaz.

Switch(config-if)# spanning-tree portfast

Este comando verifica que PortFast ha sido configurado en una interfaz.

Switch# show running-config interface FastEthernet 0/8



Comando	Parámetro
`Switch(config-if)# spanning-tree portfast`	Habilita PortFast en un puerto de acceso de capa 2 y lo fuerza a pasar al estado de reenvío en forma inmediata.
`Switch(config-if)# no spanning-tree portfast`	Deshabilita PortFast en un puerto de acceso de capa 2. PortFast se encuentra deshabilitado por defecto.
`Switch(config)# spanning-tree portfast default`	Habilita globalmente la función de PortFast en todos los puertos que no sean de trunking.
`Switch# show running-config interface` *type slot/port*	Indica si PortFast ha sido configurado en un puerto.

BPDU Guard

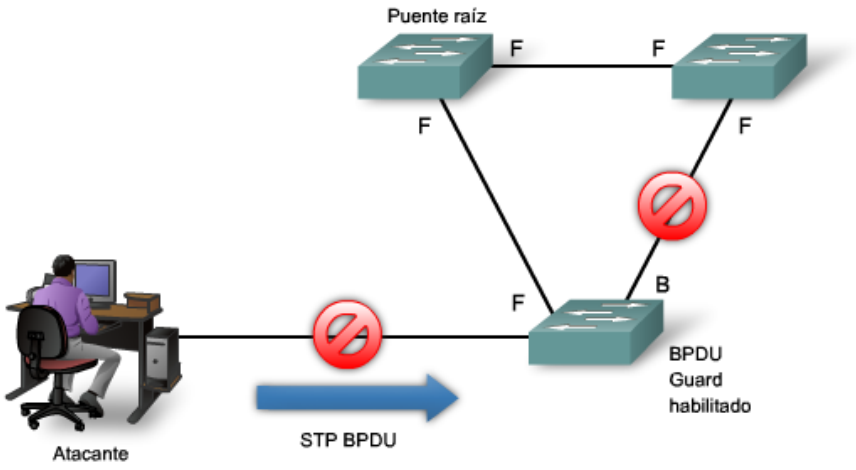
La función de STP BPDU Guard permite a los diseñadores de la red mantener predecible a la topología de red activa. BPDU Guard es utilizada para proteger a la red conmutada de posibles problemas causados por recibid BPDUs en puertos que no deberían recibirlos. La recepción de BPDUs podría ser accidental o parte de un intento no autorizado de agregar un switch a la red.

Si un puerto configurado con PortFast recibe un BPDU, STP puede colocar dicho puerto en modo deshabilitado, utilizando BPDU Guard.

BPDU Guard se implementa mejor sobre puertos de usuario, para prevenir las extensiones de red clandestinas de un host atacante.

Utilice este comando para habilitar BPDU Guard en todos los puertos que tengan habilitado PortFast.

Switch(config)# spanning-tree portfast bpduguard default




```
Switch(config)#
spanning-tree portfast bpduguard default
```

- Habilita BPDU Guard en forma global para todos los puertos con PortFast habilitado

Para ver información sobre el estado de spanning tree, utilice el comando show spanning-tree summary. En este ejemplo, BDPU Guard está habilitado.

Switch# show spanning-tree summary

Root bridge for: VLAN0001, VLAN0004-VLAN1005
VLAN1013-VLAN1499, VLAN2001-VLAN4094

EtherChannel misconfiguration guard is enabled

Extended system ID is enabled

Portfast is enabled by default

PortFast BPDU Guard is enabled

Portfast BPDU Filter is disabled by default

Loopguard is disabled by default

UplinkFast is disabled

BackboneFast is disabled

Pathcost method used is long

<output omitted>

Otro comando útil para verificar la configuración de BPDU Guard es show spanning-tree summary totals.

```
Switch# show spanning-tree summary totals
Root bridge for: none.
PortFast BPDU Guard is enabled
UplinkFast is disabled
BackboneFast is disabled
Spanning tree default pathcost method used is short
Name                 Blocking Listening Learning Forwarding STP Active
-------------------- -------- --------- -------- ---------- ----------
  1 VLAN                  0        0         0        1          1

<output omitted>
```

Root Guard

La función Root Guard de los switches Cisco provee un método para asegurar la selección de puentes raíz en la red. Root Guard limita los puertos del switch a través de los cuales puede negociarse el puente raíz. Si un puerto habilitado con Root Guard recibe BPDUs superiores a aquellos que envía el puente raíz actual, dicho puerto pasa a un estado "root-inconsistent", efectivamente similar al estado de escucha (listening) de STP, y no se reenvían más datos a través del mismo.

Debido a que un administrador puede configurar la prioridad del puente a cero en forma manual, Root Guard puede parecer innecesario. Configurar la prioridad de un switch a cero no garantiza que el mismo será seleccionado como puente raíz, debido a que puede existir otro switch con prioridad cero y una dirección MAC menor, y por lo tanto será seleccionado como puente raíz.

Root Guard se implementa mejor en puertos conectados a switches que no deberían ser el puente raíz.

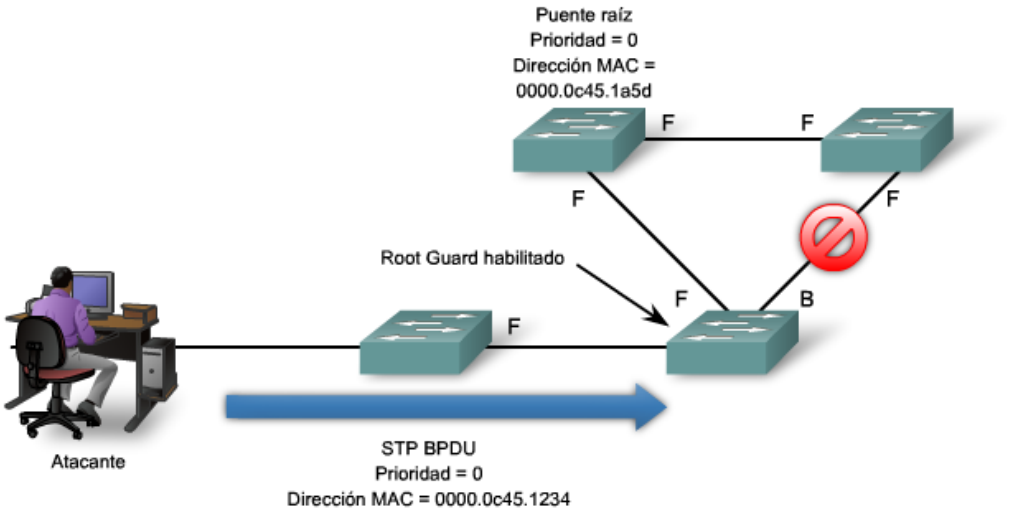
Con Root Guard, si un host atacante envía BPDUs falsificadas en un intento de convertirse en el puente raíz, una vez recibido el BPDU, el mismo es ignorado y el puerto pasa al estado "root-inconsistent". El puerto se recupera tan pronto como dejan de recibirse los BPDUs ofensivos.

BPDU Guard y Root Guard son similares, pero tienen diferentes impactos. BPDU Guard deshabilita el puerto al recibir un BPDU, si dicho puerto tiene PortFast habilitado. Esta deshabilitación niega a estos puertos en forma efectiva la participación en el proceso STP. El administrador debe volver a habilitarlos en forma manual, o configurar un temporizador automático.

Root Guard permite que el dispositivo participe del proceso STP siempre y cuando no intente convertirse en raíz. Si Root Guard bloquea el puerto, la recuperación subsecuente es automática. La recuperación ocurre tan pronto como el dispositivo culpable deja de enviar BPDUs superiores.

Este es el comando para configurar Root Guard en una interfaz.

Switch(config-if)# spanning-tree guard root




```
Switch(config-if)#
spanning-tree guard root
```

- Habilita Root Guard por cada interfaz

Para verificar el funcionamiento de Root Guard, utilice el comando show spanning-tree inconsistentports. Debe considerarse que el switch pone al puerto en el estado "root-inconsistent" si éste recibe BPDUs que no debería recibir. El puerto se recupera en el momento en que deja de recibir dichos BPDUs.

```
Switch# show spanning-tree inconsistentports
Name                 Interface              Inconsistency
-------------------- ---------------------- ------------------
VLAN0001             FastEthernet3/1        Port Type Inconsistent
VLAN0001             FastEthernet3/2        Port Type Inconsistent
VLAN1002             FastEthernet3/1        Port Type Inconsistent
VLAN1002             FastEthernet3/2        Port Type Inconsistent
VLAN1003             FastEthernet3/1        Port Type Inconsistent
VLAN1003             FastEthernet3/2        Port Type Inconsistent
VLAN1004             FastEthernet3/1        Port Type Inconsistent
VLAN1004             FastEthernet3/2        Port Type Inconsistent
VLAN1005             FastEthernet3/1        Port Type Inconsistent
VLAN1005             FastEthernet3/2        Port Type Inconsistent

Number of inconsistent ports (segments) in the system :10
```

6.3.4 Configuracion de control de tormentas

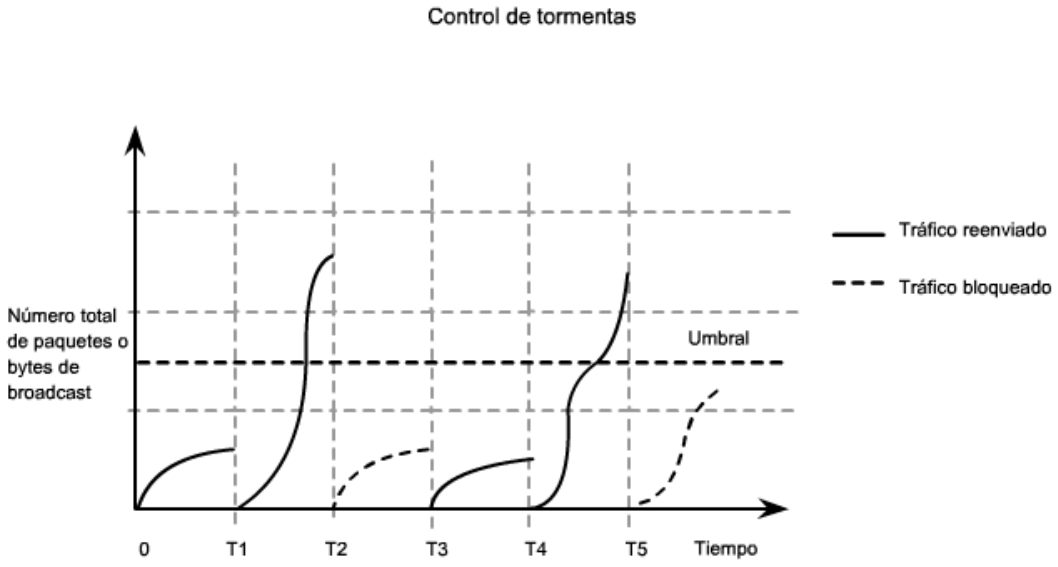
Los ataques de tormenta de LAN puede ser mitigados utilizando el control de tormentas para monitorear umbrales de supresión predefinidos. Al habilitar el control de tormentas, es posible configurar un umbral superior y un umbral inferior.

El control de tormentas utiliza uno de los siguientes métodos para medir la actividad del tráfico:

Ancho de banda como un porcentaje del total de ancho de banda disponible en el puerto, y que puede utilizarse para tráfico de broadcast, multicast o unicast.
Tasa de tráfico en paquetes por segundo recibidos como broadcast, multicast o unicast.
Tasa de tráfico en bits por segundo recibidos como broadcast, multicast o unicast.
Tasa de tráfico en paquetes por segundo y por pequeñas tramas. Esta funcionalidad se habilita en forma global. El umbral para pequeñas tramas debe configurarse para cada interfaz.

Con cada método, el puerto bloquea el tráfico una vez alcanzado el umbral superior. El puerto permanece bloqueado hasta que la tasa de tráfico cae por debajo del umbral inferior, si fue especificado, y luego reanuda el reenvío normal. Si el umbral inferior no ha sido especificado, el switch bloquea todo el tráfico hasta que el mismo cae por debajo del umbral superior. El umbral, o nivel de supresión, se refiere al número de paquetes permitidos antes de tomar una acción. En general, mientras más alto sea el nivel de supresión, menos efectiva será la protección contra las tormentas de broadcast.

Utilice el comando de configuración de interfaz storm-control para habilitar el control de tormentas en una interfaz y para configurar el valor del umbral para cada tipo de tráfico. El nivel de supresión del control de tormentas debe ser configurado como un porcentaje de ancho de banda total del puerto, como la tasa de recepción de tráfico en paquetes por segundo, o la tasa de recepción de tráfico en bits por segundo.



Cuando el nivel de supresión del tráfico se especifica como un porcentaje (hasta con dos decimales) del total de ancho de banda, el nivel puede estar entre 0.00 y 100.00. Un umbral de 100 por ciento indica que no se ha seleccionado un límite para el tipo de tráfico especificado (broadcast, multicast o unicast). Un valor de 0.00 representa que todo el tráfico del tipo especificado será bloqueado.

Los porcentajes de los umbrales son aproximados, debido a las limitaciones del hardware y la forma en la que los paquetes de diferentes tamaño son contabilizados. Dependiendo de los tamaños de los paquetes que conforman el tráfico entrante, los

umbrales reales utilizados pueden diferir de los configurados por varios puntos porcentuales.

El control de tormentas es soportado por interfaces físicas. A partir de la versión del IOS Cisco 12.2(25), el control de tormentas también puede ser configurado sobre EtherChannels. Al habilitar el control de tormentas sobre un EtherChannel, su configuración se propaga a las interfaces físicas de dicho EtherChannel.

Esta es la sintaxis completa del comando storm-control.

storm-control {{broadcast | multicast | unicast} level {nivel [level-low] | bps bps [bps-low] | pps pps [pps-low]}} | {action {shutdown | trap}}

Las opciones trap y shutdown son independientes entre sí.

Si se configura la acción trap, el switch enviará mensajes de registro SNMP cuando ocurra una tormenta.

Si se configura la acción shutdown el puerto es deshabilitado durante la tormenta, y debe utilizarse el comando de configuración de interfaz no shutdown para volver a habilitarlo.

Cuando ocurre una tormenta y la acción es filtrar el tráfico, si el nivel de supresión inferior no fue especificado, el switch bloquea todo el tráfico hasta que la tasa cae por debajo del nivel de supresión superior. En cambio, si el nivel de supresión inferior fue especificado, el switch bloquea todo el tráfico hasta que la tasa cae por debajo de este nivel.

```
Switch(config-if)# storm-control broadcast level 75.5
Switch(config-if)# storm-control multicast level pps 2k 1k
Switch(config-if)# storm-control action shutdown
```

- Habilita la protección contra tormentas de broadcast.
- Habilita la protección contra tormentas de multicast.
- Especifica la acción que debe realizarse cuando se alcanza el umbral.

Configuración de control de tormentas | Parámetros de `storm-control`

Haga clic sobre cada botón para ver el contenido asociado.

Parámetro	Descripción
broadcast	Este parámetro habilita el control de tormentas de broadcast en la interfaz.
multicast	Este parámetro habilita el control de tormentas de multicast en la interfaz.
unicast	Este parámetro habilita el control de tormentas de unicast en la interfaz.
level *level* [*level-low*]	Especifica los niveles de supresión superior e inferior como un porcentaje del total de ancho de banda del puerto. *level*: Nivel de supresión superior, con hasta dos posiciones decimales. El rango es entre 0.00 y 100.00. Bloquea los paquetes excedentes de la tormenta cuando se alcanza el nivel especificado. *level-low*: (Opcional) Nivel de supresión inferior, con hasta dos posiciones decimales. El rango es entre 0.00 y 100.00. Este valor debe ser menor o igual que el valor de supresión superior. Si el nivel de supresión inferior no se encuentra configurado, se utiliza el nivel de supresión superior como límite.
level bps *bps* [*bps-low*]	Especifica los niveles de supresión superior e inferior como la tasa de bits por segundo a la que es recibido el tráfico en el puerto. *bps*: Nivel de supresión superior, con hasta una posición decimal. El rango es entre 0.0 y 10000000000.0. Bloquea los paquetes excedentes de la tormenta cuando se alcanza el nivel especificado en bps. *bps-low*: (Opcional) Nivel de supresión inferior, con hasta una posición decimal. El rango es entre 0.0 y 10000000000.0. Este valor debe ser menor o igual que el valor de supresión superior. Utilizar sufijos de métricas tales como k, m y g para umbrales con números grandes.
level pps *pps* [*pps-low*]	Especifica los niveles de supresión superior e inferior como la tasa de paquetes por segundo a la que es recibido el tráfico en el puerto. *pps*: Nivel de supresión superior, con hasta una posición decimal. El rango es entre 0.0 y 10000000000.0. Bloquea los paquetes excedentes de la tormenta cuando se alcanza el nivel especificado en pps. *pps-low*: (Opcional) Nivel de supresión inferior, con hasta una posición decimal. El rango es entre 0.0 y 10000000000.0. Este valor debe ser menor o igual que el valor de supresión superior. Utilizar sufijos de métricas tales como k, m y g para umbrales con números grandes.
action { **shutdown** | **trap**}	Define la acción a realizar cuando ocurre una tormenta en un puerto. La acción por defecto es filtrar el tráfico y no enviar una notificación SNMP. Las palabras clave tienen los siguientes significados: **shutdown**: Deshabilita el puerto durante una tormenta **trap**: Envía una notificación SNMP cuando ocurre una tormenta

Configuración de control de tormentas | Parámetros de `storm-control`

Haga clic sobre cada botón para ver el contenido asociado.

Utilice el comando show storm-control [interface] [{broadcast | multicast | unicast | history}] para verificar la configuración del control de tormentas. Este comando muestra los niveles de supresión del control de tormentas en todas las interfaces, o bien para la interfaz especificada, para el tipo de tráfico indicado. Si no se especifica ningún tipo de tráfico, por defecto se asume el tráfico de broadcast.

```
Switch# show storm-control
Interface    Filter State   Upper       Lower      Current
---------    -------------  ----------  ---------  ---------
Gi0/1        Forwarding     20 pps      10 pps     5 pps
Gi0/2        Forwarding     50.00%      40.00%     0.00%

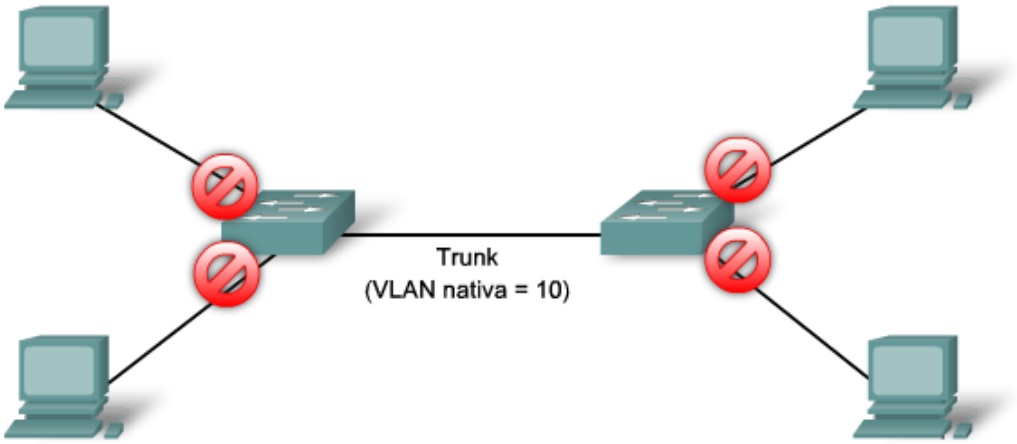
<output omitted>
```

6.3.5 Configuracion de la seguridad del enlace troncal de VLAN

La mejor forma de mitigar un ataque de salto de VLAN es asegurando que el trunking sólo se encuentra habilitado en los enlaces que lo requieran. Además, las negociaciones DTP (auto trunking) deben estar deshabilitadas y el trunking debe configurarse manualmente.

Para prevenir los ataques de salto de VLAN con doble encapsulación 802.1Q, el switch debe ver más allá dentro de la trama para determinar si contiene más de una etiqueta de VLAN. Desafortunadamente, el hardware de la mayoría de los switches está optimizado para buscar sólo una etiqueta y luego conmutar la trama. El problema del desempeño versus la seguridad requiere que los administradores logren un cuidadoso balance entre sus requisitos.

La mitigación de los ataques de salto de VLAN con doble encapsulación 802.1Q requiere varias modificaciones en la configuración de VLAN. Uno de los elementos más importantes es utilizar una VLAN nativa dedicada en todos los enlaces troncales. Este ataque puede evitarse fácilmente siguiendo la práctica recomendada de no utilizar VLANs nativas para enlaces troncales en ningún otro puerto del switch. Además, deben deshabilitarse todos los puertos no utilizados del switch, y colocarlos en una VLAN sin uso.



- Deshabilitar el trunking en todos los puertos de acceso.
- Deshabilitar el auto trunking y habilitar el trunking en forma manual.
- Asegurarse de que la VLAN nativa es utilizada sólo en las líneas de trunk.

Para controlar el trunking de los puertos, existen diferentes opciones.

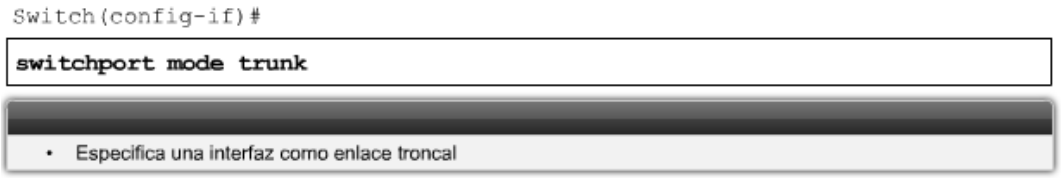
Para los enlaces que no deban ser troncales, utilice el comando de configuración de interfaz switchport mode access para deshabilitar el trunking.

Se necesitan tres pasos para crear un enlace troncal:

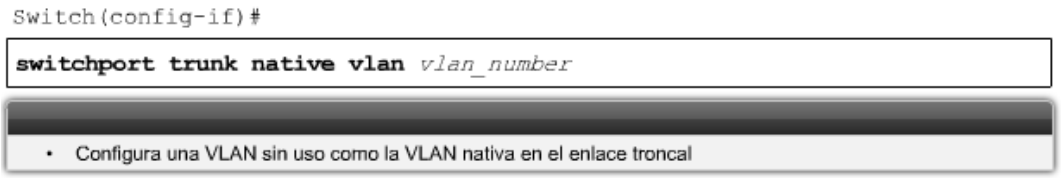
Paso 1. Utilice el comando de configuración de interfaz switchport mode trunk para convertir a la interfaz en un enlace troncal.

Paso 2. Utilice el comando de configuración de interfaz switchport nonegotiate para prevenir la generación de tramas DTP.

Paso 3. Utilice el comando switchport trunk native vlan número_vlan para asignar una VLAN sin uso como la VLAN nativa del trunk. La VLAN nativa por defecto es la VLAN 1.





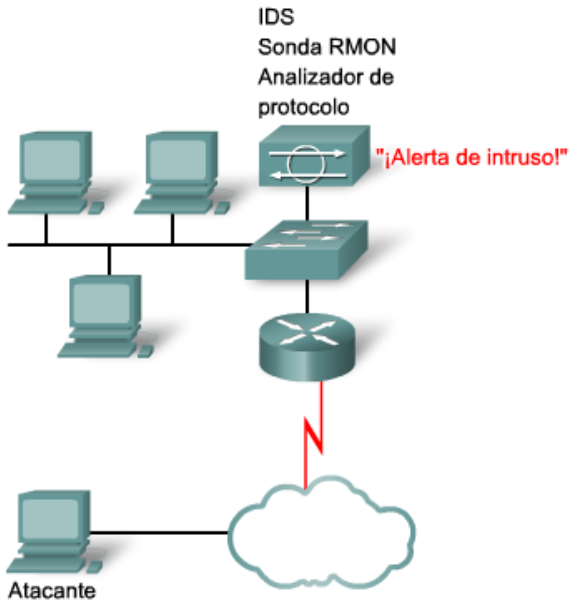


6.3.6 Configuracion del analizador de puertos conmutados Cisco

Además de las técnicas de mitigación, es también posible configurar un dispositivo de capa 2 de forma tal que soporte el análisis de tráfico. El tráfico de red que atraviesa los puertos o VLANs puede ser analizado utilizando un Analizador de Puertos Conmutados (SPAN - Switched Port Analyzer), o un SPAN remoto (RSPAN). SPAN puede enviar una copia del tráfico desde un puerto a otro del mismo switch, donde se encuentra conectado un analizador de red o dispositivo de monitoreo. RSPAN puede enviar una copia de todo el tráfico a un puerto de un switch diferente. SPAN copia el tráfico recibido, enviado, o ambos, en puertos o VLANs origen hacia un puerto destino para su análisis. SPAN no afecta la conmutación del tráfico de la red en los puertos o VLANs origen . El puerto destino está dedicado para el uso de SPAN. A excepción del tráfico requerido por las sesiones de SPAN o RSPAN, los puertos destino no reciben o reenvían tráfico. Las interfaces deben ser monitoreadas en ambas direcciones, mientras que las VLANs deben ser monitoreadas sólo en una dirección.

SPAN no es requerido para syslog o SNMP. SPAN es utilizado para replicar el tráfico, mientras que syslog y SNMP se configuran para enviar datos en forma directa al servidor apropiado. SPAN no mitiga ataques, pero habilita el monitoreo de la actividad maliciosa.

- Un puerto de SPAN replica el tráfico hacia otro puerto donde se conecta un dispositivo de monitoreo.
- Sin esto, puede ser difícil rastrear a los hackers una vez que se encuentran dentro de la red.



Una sesión SPAN puede ser configurada para monitorear el tráfico del puerto origen hacia un puerto destino. En este ejemplo, la configuración existente de SPAN para la sesión 1 es eliminada, y luego el tráfico bidireccional es replicado desde el puerto origen Gigabit Ethernet 0/1 al puerto destino Gigabit Ethernet 0/2, reteniendo el método de encapsulación.

Switch(config)# no monitor session 1

Switch(config)# monitor session 1 source interface gigabitethernet0/1

Switch(config)# monitor session 1 destination interface gigabitethernet0/2 encapsulation replicate

Switch(config)# end

Otro ejemplo ilustra la captura del tráfico recibido y retransmitido de las VLANs 10 y 20, respectivamente.

Switch(config)# monitor session 1 source vlan 10 rx

Switch(config)# monitor session 1 source vlan 20 tx

Switch(config)# monitor session 1 destination interface FastEthernet 3/4

Para verificar la configuración de SPAN, utilice el comando show monitor session número-sesión.

```
Switch(config)#
monitor session session_number source {interface interface-id [, | -] [both
| rx | tx]} | {vlan vlan-id [, | -] [both | rx | tx]}| {remote vlan vlan-id}
```

```
Switch(config)#
monitor session session_number destination {interface interface-id [, | -]
[encapsulation {dot1q | replicate}] [ingress {dot1q vlan vlan-id | untagged
vlan vlan-id | vlan vlan-id}]} | {remote vlan vlan-id}
```

Configurando SPAN | Verificando SPAN

Haga clic sobre cada botón para ver el contenido asociado.

```
Switch# show monitor session 1
Session 1
---------
Type                          : Local Session
Source VLANs                  :
    RX Only                   : 10
    TX Only                   : 20
Destination Ports             : Fa3/4
    Encapsulation             : Native
          Ingress             : Disabled
```

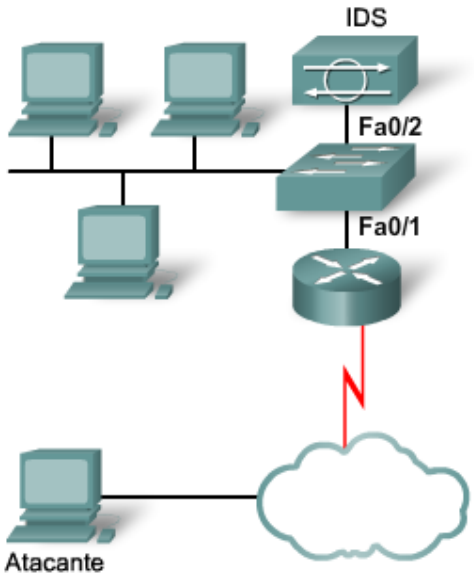
Configurando SPAN | Verificando SPAN

Haga clic sobre cada botón para ver el contenido asociado.

Un sistema de detección de instrusiones (IDS - Intrusion Detection System) tiene la habilidad de detectar el mal uso, abuso y acceso no autorizado a los recursos de la red. SPAN puede ser utilizado para replicar el tráfico hacia otro puerto donde se encuentre conectada una sonda o un sensor del IDS: Cuando el sensor del IDS detecta un intruso, el sensor envía una señal TCP Reset, la cual interrumpe la conexión del intruso dentro de la red, removiéndolo en forma inmediata.

SPAN es en general implementado cuando se incorpora un IDS a la red. Los dispositivos IDS necesitan leer todos los paquetes de una o más VLANs y SPAN puede ser utilizado para hacer llegar dichos paquetes al dispositivo IDS.

Utilizar SPAN para replicar el tráfico de entrada y de salida desde el puerto Fa0/1 hacia el puerto Fa0/2.

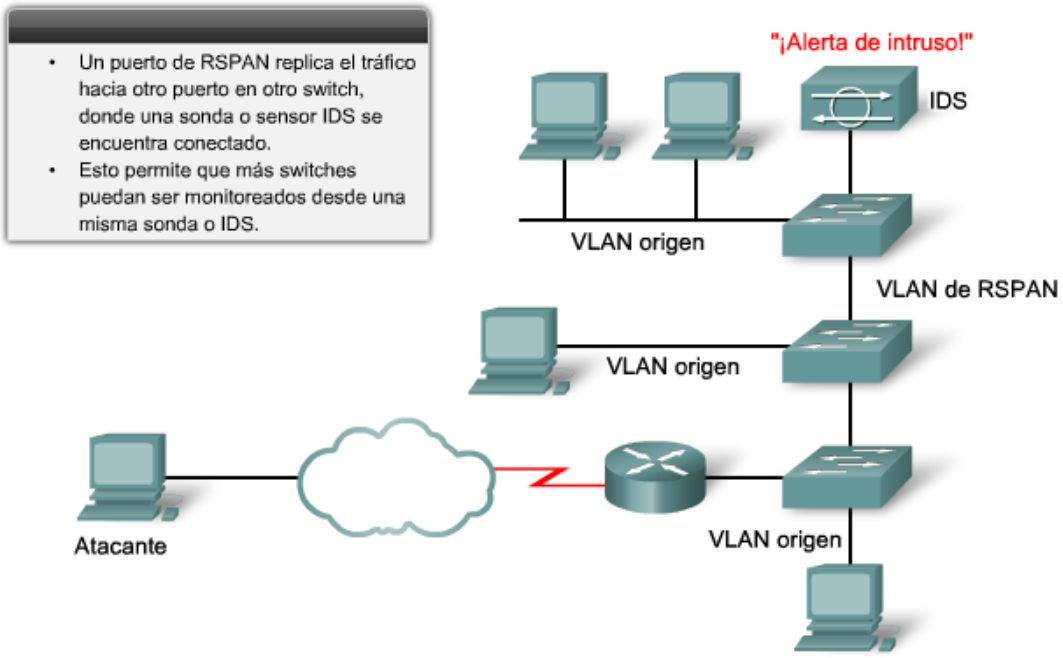


6.3.7 Configuracion de un analizador remoto de puertos conmutados Cisco

RSPAN posee todas las características de SPAN, y además incluye soporte para puertos origen y puertos destino que se encuentren distribuidos a través de múltiples switches, permitiendo el monitoreo de cualquier puerto destino ubicado dentro de la VLAN de RSPAN. Esto permite al administrador monitorear el tráfico de un switch utilizando un dispositivo conectado a otro switch.

RSPAN puede ser utilizado para reenviar el tráfico hacia el IDS, quien lo analiza en busca de comportamientos maliciosos. Los puertos origen del tráfico replicado pueden encontrarse en múltiples switches. Si el propósito es la detección de intrusiones, el IDS examina el tráfico reenviado por todos los dispositivos de origen. Si un atacante compromete a la red interna a través de un router perimetral, se reenvía una copia del tráfico del intruso hacia el IDS para su análisis.

Al igual que con SPAN, RSPAN no es requerido para syslog o SNMP y es sólo utilizado para replicar el tráfico, no para enviar datos en forma directa a un servidor definido. RSPAN no mitiga ataques, pero permite el monitoreo de actividad maliciosa.



Para configurar RSPAN, comience configurando la VLAN de RSPAN. En este ejemplo, se crea la VLAN 100 y se la configura como VLAN de RSPAN.

2960-1(config)# vlan 100

2960-1(config-vlan)# remote-span

2960-1(config-vlan)# exit

Luego, es necesario configurar los puertos y VLANs de origen para RSPAN. El tráfico capturado desde el puerto de origen es replicado hacia un puerto reflector dedicado, el cual funciona simplemente como una interfaz de loopback, la cual refleja el tráfico capturado hacia la VLAN de RSPAN. El tráfico no es enviado a través del puerto, simplemente provee un mecanismo de loopback interno para las sesiones de origen de RSPAN. Un puerto reflector existe sólo para una sesión de origen de RSPAN. En este ejemplo, existe sólo un puerto origen.

2960-1(config)# monitor session 1 source interface FastEthernet 0/1

2960-1(config)# monitor session 1 destination remote vlan 100 reflector-port FastEthernet 0/24

2960-1(config)# interface FastEthernet 0/2

2960-1(config-if)# switchport mode trunk

Finalmente, configure el reenvío del tráfico de RSPAN a través de una interfaz hacia el IDS. En este ejemplo, el tráfico destinado a la VLAN 100 es reenviado a través de la interfaz Fast Ethernet 0/2.

2960-2(config)# monitor session 2 source remote vlan 100

2960-2(config)# monitor session 2 destination interface FastEthernet 0/3

2960-2(config)# interface FastEthernet 0/2

2960-2(config-if)# switchport mode trunk



Utilice los comandos show monitor y show interfaces trunk para verificar la configuración de RSPAN.

SPAN y RSPAN son utilizados con el propósito de analizar protocolos y detectar y prevenir intrusiones. Se han explorado una variedad de herramientas y tecnologías para asegurar la infraestructura de la red. IronPort, NAC y CSA aseguran a las terminales contra diferentes amenazas, incluyendo desbordamientos de buffer, virus, troyanos y gusanos. Las tecnologías tales como BPDU Guard y Root Guard trabajan para prevenir los ataques de manipulación de STP. El control de tormentas ayuda a prevenir las tormentas de LAN. La seguridad de puertos asegura que sólo los hosts apropiados se conectan a los puertos del switch. Las buenas prácticas de conmutación de capa 2 previenen los ataques de VLAN. Pero las LANs modernas también incluyen dispositivos inalámbricos, dispositivos de telefonía IP, y dispositivos de almacenamiento de red. Estos dispositivos y el tráfico asociado a ellos también necesitan ser asegurados.



Verificar RSPAN:

```
show monitor [session {session_number | all | local | range list |
remote} [detail]]
```

Verificar RSPAN | Ejemplos de verificación

Haga clic sobre cada botón para ver el comando de verificación y la salida asociada.

```
2960-1# show monitor
Session 1
---------
Type               : Remote Source Session
Source Ports       :
    Both           : Fa0/1
Reflector Port     : fa0/24
Dest RSPAN VLAN    : 100
2960-1# show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/2       on           802.1q         trunking      1
Port      Vlans allowed on trunk
Fa0/2       1-4094
Port        Vlans allowed and active in management domain
Fa0/2       1-30,100
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/2       1-30,100
```

```
2960-2# show interfaces trunk
Port        Mode         Encapsulation  Status        Native vlan
Fa0/2       on           802.1q         trunking      1
Port      Vlans allowed on trunk
Fa0/2       1-4094
Port        Vlans allowed and active in management domain
Fa0/2       1-30,100
Port        Vlans in spanning tree forwarding state and not pruned
Fa0/2       1-30,100
2960-2# show monitor session 2
Session 2
---------
Type               : Remote Destination Session
Source RSPAN VLAN  : 100
Destination Ports  : Fa0/3
    Encapsulation  : Native
          Ingress  : Disabled
```

Verificar RSPAN | Ejemplos de verificación

6.3.8 Practicas recomendadas para la capa 2

Los lineamientos de la capa 2 dependen de la política de seguridad propia de una organización.

Es importante administrar a los switches de manera similar a los routers, utilizando protocolos seguros o métodos fuera de banda, si la política lo permite. Apagar los dispositivos que no sean necesarios y los puertos que no se utilicen. Implementar varios servicios de seguridad, tales como seguridad de puertos y mejoras del STP, según como sea necesario y como sea soportado por el hardware. Deshabilitar CDP (Cisco Discovery Protocol) en los puertos donde no se conecten dispositivos de red, con la excepción de aquellos puertos conectados a teléfonos IP de Cisco.

- Administrar los switches de forma segura (SSH, administración fuera de banda, ACLs, etc.).
- Configurar todos los puertos no troncales como puertos de usuario (a menos que se utilice Cisco VoIP).
- Utilizar seguridad de puertos, cuando sea posible, para los puertos de acceso.
- Habilitar la mitigación de ataques de STP (BPDU Guard, Root Guard).
- Utilizar Cisco Discovery Protocol sólo donde sea necesario – es útil con los teléfonos.
- Configurar PortFast en todos los puertos no troncales.
- Configurar Root Guard y puertos raíz para STP.
- Configurar BPDU Guard en todos los puertos no troncales.



Por defecto, la VLAN 1 es la VLAN administrativa. Además, por defecto, todos los puertos son miembros de la VLAN 1 (VLAN1 es la VLAN de usuarios por defecto). También, VLAN1 es la VLAN nativa por defecto para todos los puertos troncales. Por este motivo, es muy recomendado que la VLAN 1 no sea utilizada con ningún fin. Todos los puertos no utilizados deben ser asignados a una VLAN sin uso. Todos los puertos troncales deben ser asignados a una VLAN vacía y sin uso. La VLAN administrativa debe ser asignada a una VLAN sin uso, la cual no coincida con ninguna VLAN de usuario, ni la VLAN administrativa, ni la VLAN nativa.

- Siempre utilizar una ID de VLAN dedicada y sin utilizar como VLAN nativa en los puertos de enlaces troncales.
- No utilizar la VLAN 1 para nada.
- Deshabilitar todos los puertos no utilizados y asignarlos a una VLAN sin utilizar.
- Configurar manualmente todos los enlaces troncales y deshabilitar DTP en los puertos de trunk.
- Configurar todos los puertos que no sean de trunk con el comando **`switchport mode access`**.



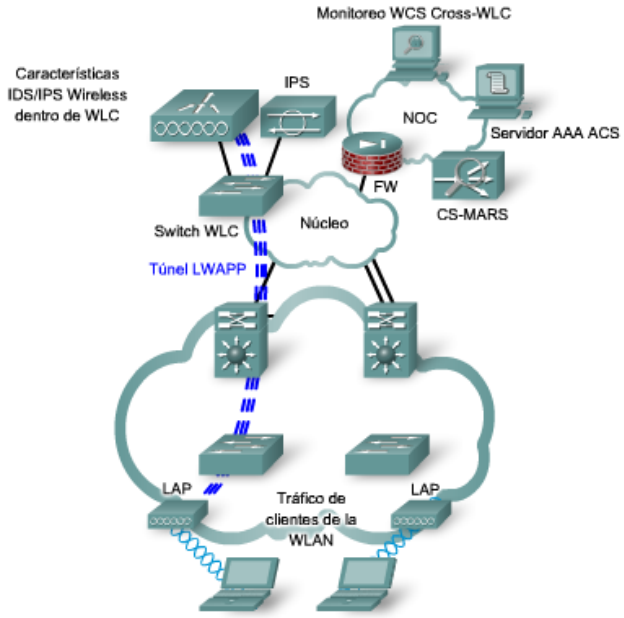
6.4 Seguridad de Wirelees, VOIP, SAN

6.4.1 Consideraciones de seguridad de tecnologias avanzadas empresariales

La tecnología de LAN inalámbrica ha sido una poderosa fuente de impulso para los avances en la seguridad de la red. Un acceso más fácil a la red a través de dispositivos inalámbricos conlleva una mayor necesidad de soluciones de seguridad inalámbrica más abarcativas.

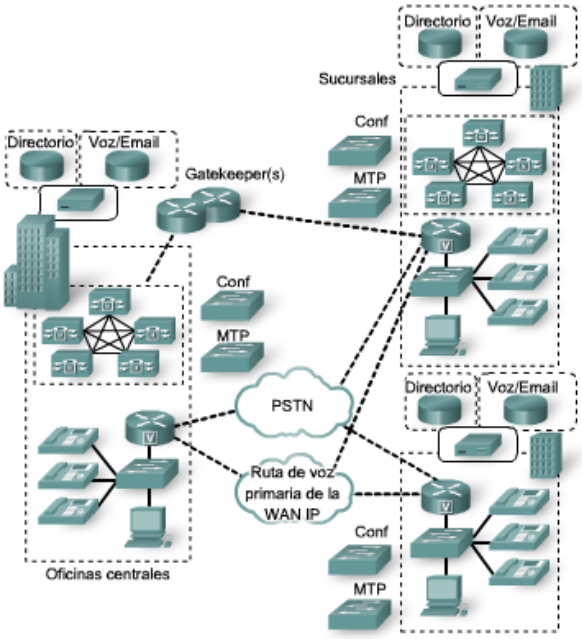
De forma similar, el advenimiento de la Voz sobre IP (VoIP) y todos los dispositivos y tecnologías asociados (telefonía IP), ha motivado diversos avances en la seguridad. ¿Quién desearía que su llamada telefónica sea interceptada por un hacker? Resulta valioso describir los motivos de las implementaciones VoIP, los componentes requeridos en las redes VoIP, y los problemas relacionados al servicio de VoIP. El desarrollo natural indica explorar las implicaciones de implementar medidas de seguridad en redes IP que transportan voz.

Las Redes de Área de Almacenamiento (SANs - Storage Area Networks) ofrecen una solución al creciente costo del tiempo de inactividad de las redes y servidores. Debido a que el propósito de la seguridad de una red es asegurar los datos (incluyendo voz y video) y el hecho de que actualmente los datos en general residen en una SAN, es esencial que dicha SAN también sea segura.



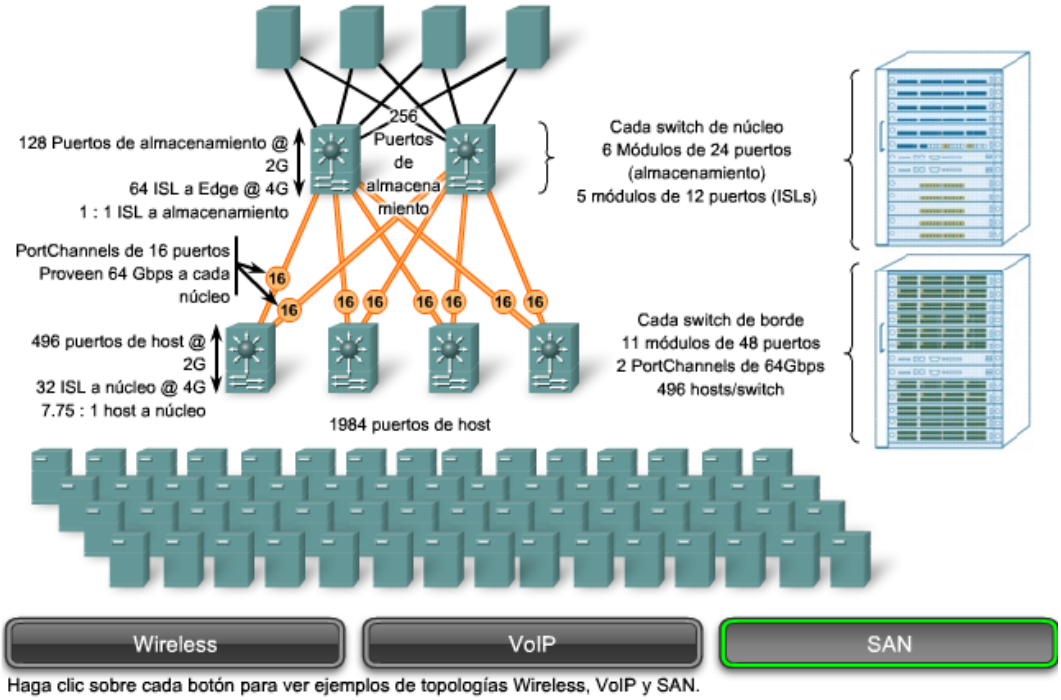
Wireless | VoIP | SAN

Haga clic sobre cada botón para ver ejemplos de topologías Wireless, VoIP y SAN.



Wireless | VoIP | SAN

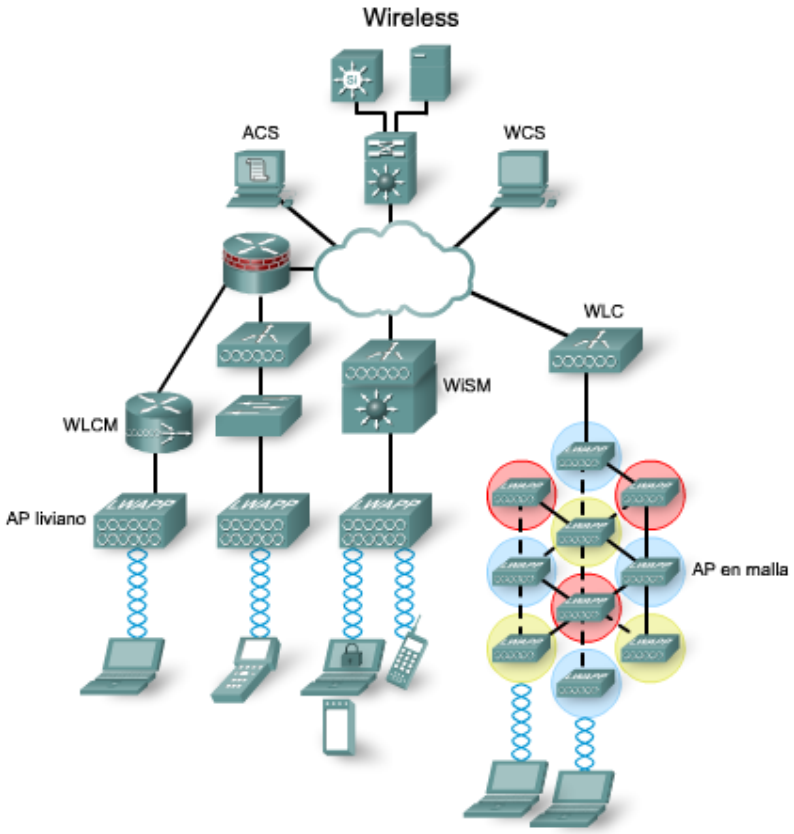
Haga clic sobre cada botón para ver ejemplos de topologías Wireless, VoIP y SAN.



Las redes empresariales modernas en general emplean controladores inalámbricos, puntos de acceso, y sistemas de administración inalámbricos para proveer una protección global contra ataques inalámbricos. El ambiente inalámbrico se asegura mediante una protección contra amenazas integrada en la infraestructura , visibilidad avanzada en el ambiente RF, y la colaboración de seguridad de la red cableada.

Una solución integrada a la infraestructura para la seguridad global inalámbrica reduce los costos a la vez que simplifica las operaciones de seguridad. Esta solución presenta una variedad de beneficios:

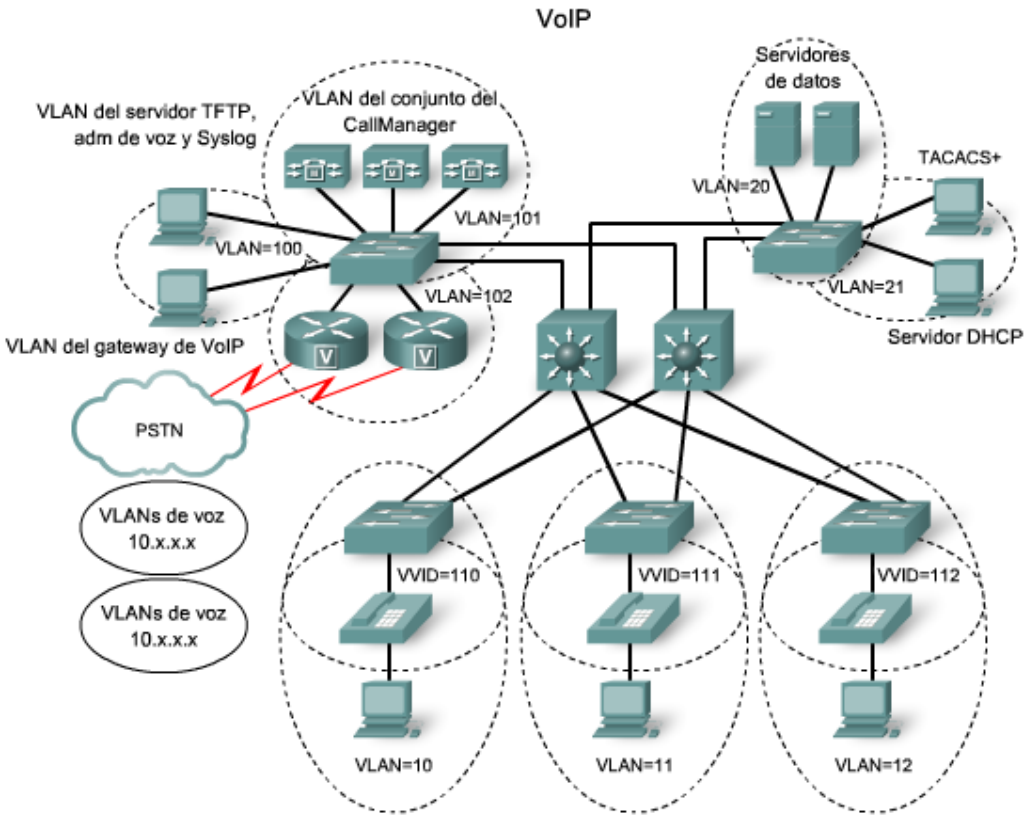
La capacidad proactiva de detección de intrusos y amenazas detecta los ataques inalámbricos y los previene.
La protección global y extendida resguarda los datos y comunicaciones confidenciales.
Una única identidad y política de usuario simplifica la administración de usuarios y da protección contra accesos no autorizados.
La colaboración con los sistemas de seguridad de la red cableada genera un conjunto superior de funcionalidades y protección de seguridad inalámbrica.



Los teléfonos IP, las PBXs IP (Private Branch Exchanges), los gateways de voz, los sistemas de correo de voz, y los protocolos requeridos, son también comunes en una red empresarial. Estas tecnologías y protocolos aumentan la productividad y finalmente ahorran costos de telefonía a la organización. Utilizando una PBX IP, las organizaciones pueden eliminar las PBXs de legado y disfrutar de los beneficios de la telefonía IP sobre una red convergente. Una PBX IP provee funciones de control de llamadas y, cuando es utilizada en conjunto con teléfonos IP o aplicaciones de telefonía, puede proveer funciones de PBX en forma distribuida y escalable. Los modelos de implementación para soluciones de telefonía IP de Cisco caen dentro de una de estas tres categorías:

Implementación de un único sitio
Procesamiento centralizado de llamadas con sucursales remotas
Procesamiento distribuido de llamadas
Agrupación a través de una WAN IP

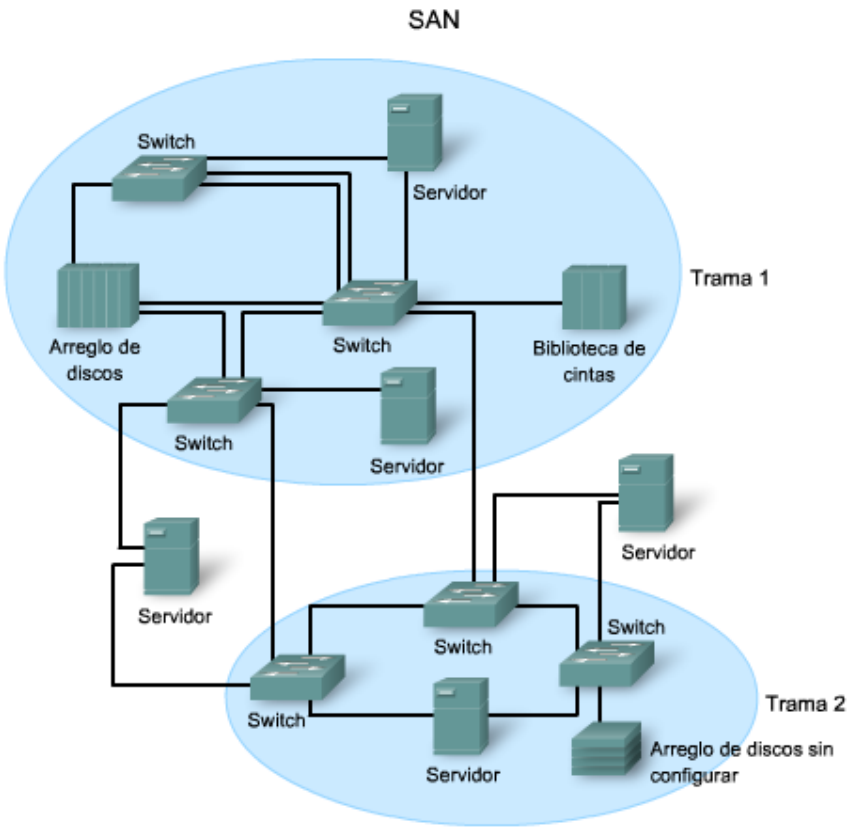
La selección del modelo de implementación depende de los requisitos de la organización, tales como el tamaño de la red, funciones y disponibilidad del ancho de banda de la WAN.



Las redes empresariales también utilizan redes de área de almacenamiento. El almacenamiento de red es un tema central en las arquitecturas de los centros de datos actuales, los cuales proveen una plataforma de red que permite a los departamentos de IT obtener menores costos de propiedad, una mejor resiliencia (capacidad de recuperarse ante una falla), y una mayor agilidad. Las soluciones de almacenamiento de red proveen:

Protección de la inversión - En un mismo chasis y con la misma configuración del switch, pueden convivir tecnologías de primera, segunda y tercera generación.
Virtualización - Los administradores de IT pueden disponer de su estructura de almacenamiento.
Seguridad - Los datos se encuentran protegidos durante su almacenamiento y al ser transportados y replicados.
Consolidación - Los profesionales de almacenamiento pueden consolidar los recursos aprovechando las plataformas SAN altamente escalables e inteligentes.
Disponibilidad - El acceso instantáneo a los datos está disponible desde múltiples capas de recuperación ante desastres.

Las LANs inalámbricas utilizan tecnología de radiofrecuencia (RF). La tecnología RF ha existido desde fines del siglo XIX. La tecnología VoIP se volvió disponible comercialmente en los años '90. La tecnología SAN no ingresó formalmente en el mercado hasta inicios del 2000. Este enfoque sigue el orden histórico.



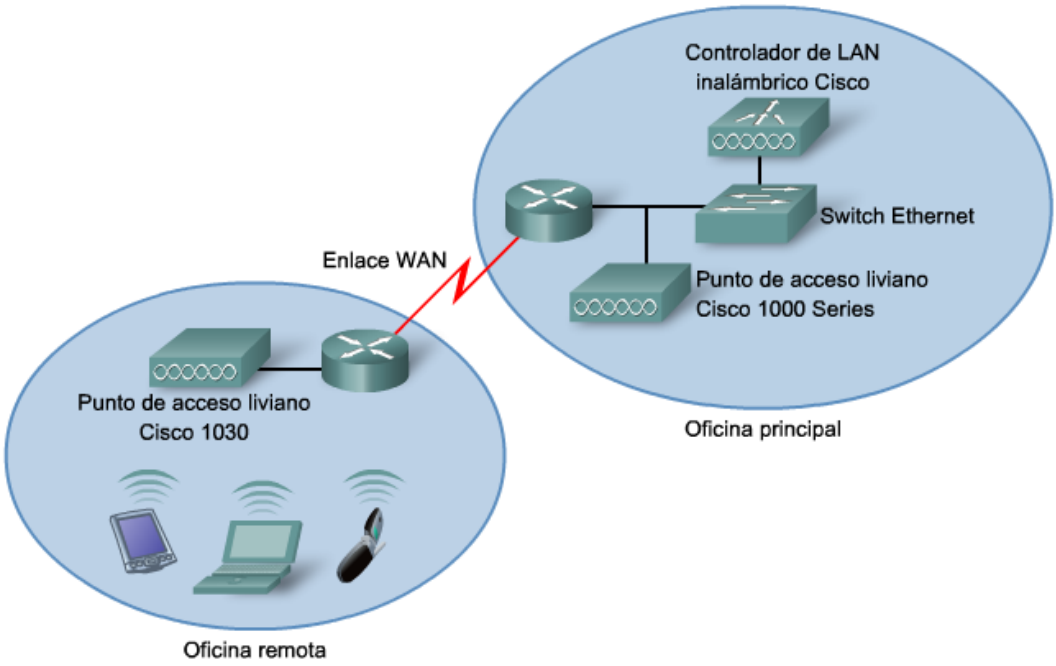
6.4.2 Consideraciones de seguridad inalambrica

A comienzos del 2000, el modelo de implementación de los puntos de acceso (AP) autónomos fue reemplazado en forma rápida por el modelo de implementación de puntos de acceso livianos. Los APs livianos dependen de los controladores LAN inalámbricos (WLCs - Wireless LAN Controllers) para su configuración. Esto difiere de los APs autónomos, los que requieren la configuración individual de cada dispositivo. La solución de AP liviano más controlador inalámbrico posee ciertos beneficios que antes no se encontraban disponibles, tales como la detección y ubicación de APs ilegales.

Los WLCs de Cisco son responsables por las funciones de LAN inalámbrica disponibles en todo el sistema, tales como las políticas de seguridad, prevención de intrusiones, administración de RF, QoS, y la movilidad. Estas funciones trabajan en conjunto con los APs y el WCS (Wireless Control System) de Cisco para soportar aplicaciones inalámbricas. Desde servicios de voz y datos hasta el seguimiento de posiciones, los WLCs de Cisco proveen el control, la escalabilidad, la seguridad y la confiabilidad para construir redes inalámbricas seguras y de escala empresarial, ubicadas desde pequeñas oficinas regionales hasta grandes campus.

Los WLCs de Cisco se integran en forma fluida en las redes empresariales existentes. Se comunican con los APs livianos sobre cualquier infraestructura de capa 2 o de capa 3, utilizando LWAPP (LightWeight Access Point Protocol). Estos dispositivos soportan la automatización de numerosas funciones de configuración y administración de WLAN, a través de todas las ubicaciones de la empresa.

Debido a que los WLCs de Cisco soportan los estándares IEEE 802.11a/b/g y 802.11n, las organizaciones pueden implementar la solución que mejor se adapte a sus requisitos individuales. Las organizaciones puede ofrecer una cobertura robusta con 802.11a/b/g o proveer un mejor desempeño con el rendimiento cinco veces mayor y la mayor confiabilidad de 802.11n.

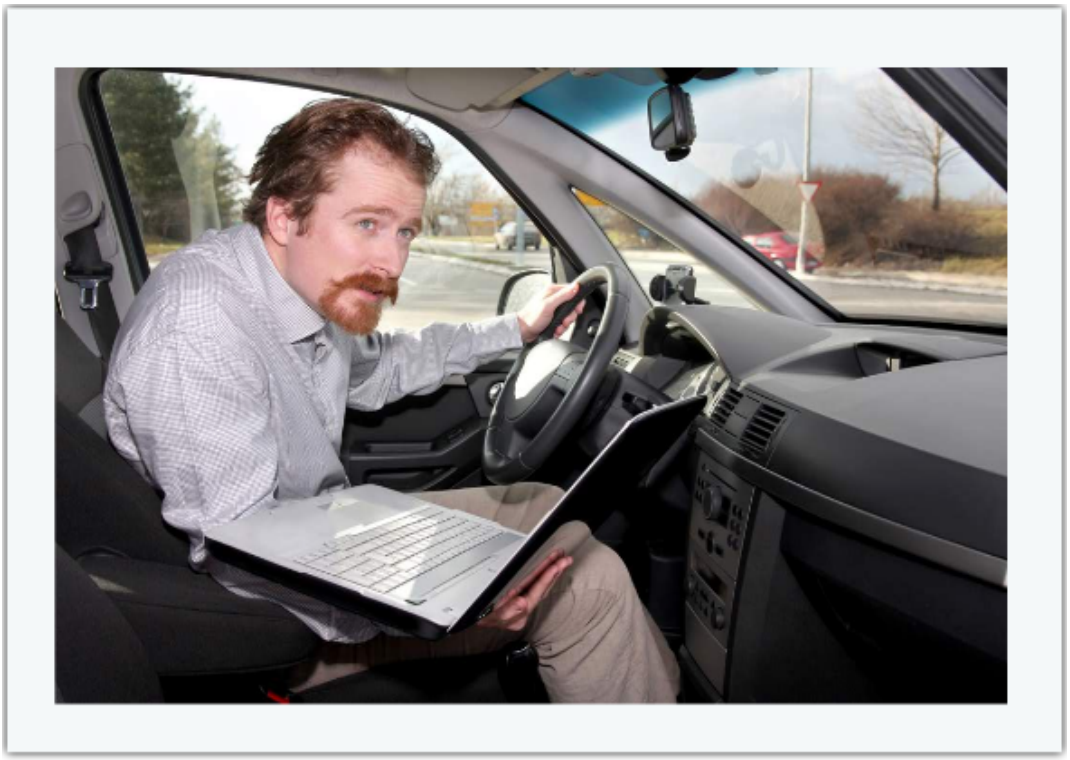


Con el acceso inalámbrico omnipresente a Internet, los hackers han expandido sus oportunidades para conectarse en forma encubierta a las redes. Ya sea un hacker experimentado o un novato en tecnologías inalámbricas, abundan las oportunidades para explotar vulnerabilidades en las redes inalámbricas.

La forma más popular de hacking inalámbrico es el llamado "war driving", donde los hackers intentan obtener acceso a las redes inalámbricas desde sus laptops mientras conducen sus automóviles a través de áreas metropolitanas o suburbanas. Un vecino puede ingresar en forma no autorizada a la red inalámbrica de su vecino con el fin de obtener acceso gratuito a Internet, o bien para acceder a información confidencial. Los aeropuertos, locales de comidas rápidas y cafés suelen ofrecer acceso a Internet a sus clientes, lo que da a los hackers la oportunidad de aprovechar los datos de otros usuarios. Un hacker puede incluso intentar conectarse a otra computadora utilizando el modo ad-hoc en un área pública.

Nunca es seguro conectarse a una red inalámbrica abierta, especialmente en un área pública, a menos que la conexión sea seguida por una conexión VPN cifrada hacia otra red. Con respecto a las redes empresariales, debe recordar que la mayor parte de los ataques de seguridad provienen desde el interior. Estos ataques pueden ser generados en forma intencional por un empleado descontento, o bien pueden ser activados en forma no intencional por una computadora infectada por un virus. Muchas organizaciones,

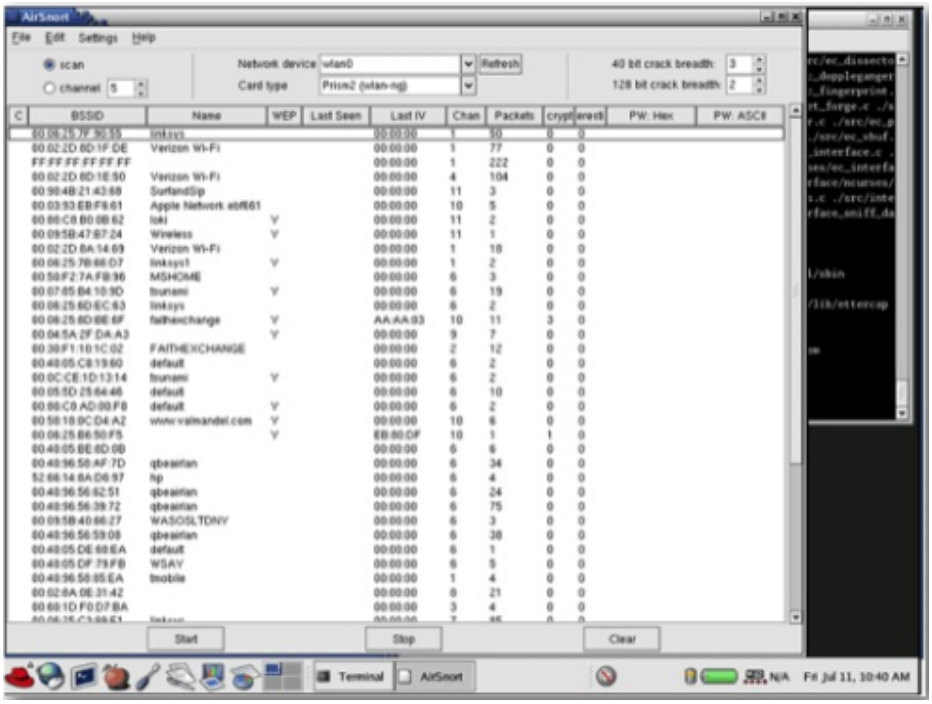
como parte de sus políticas de seguridad, no permiten a sus empleados instalar sus propios APs en el lugar de trabajo.



Los hackers de redes inalámbricas cuentan con una variedad de herramientas a su disposición, dependiendo de su nivel de sofisticación y determinación:

Network Stumbler encuentra redes inalámbricas.
Kismet muestra las redes inalámbricas que no publican sus SSIDs.
AirSnort captura y quiebra claves WEP.
CoWPAtty quiebra claves WPA-PSK (WPA1).
ASLEAP recolecta datos de autenticación.
Wireshark puede explorar datos de una red Ethernet inalámbrica y SSIDs 802.11.

Para el hacker más determinado, los analizadores de espectro pueden ser utilizados para identificar, clasificar y encontrar el origen de señales Wi-Fi RF. Los analizadores de espectro modernos pueden identificar tipos específicos de dispositivos que causan interferencias RF y rastrearlos a sus ubicaciones físicas.



6.4.3 Soluciones de seguridad de redes inalambricas

Las primeras LANs inalámbricas (WLANs) emergieron en 1990. Estas WLANs eran totalmente abiertas, sin requisitos de autenticación o cifrado. La primera opción de seguridad para las WLANs fue el Service Set IDentifier (SSID). Implementaciones posteriores habilitaron la utilización de SSIDs sin que fuera necesario que los APs los publiquen.

El estándar IEEE 802.11b definió el protocolo de seguridad Wired Equivalent Privacy (WEP) para el cifrado de los datos entre los terminales de radio. Durante varios años, las implementaciones WEP fueron el único medio para asegurar las WLANs. Las debilidades de WEP llegaron al desarrollo de tecnologías más nuevas, basadas en protocolos como Temporal Key Integrity Protocol (TKIP) y cifrados tales como Advanced Encryption Standard (AES). WPA (Wi-Fi Protected Access) implementa TKIP y es más seguro que WEP. WPA2 implementa AES y es más seguro que WPA. WPA2, una implementación de interoperabilidad para 802.11i, es actualmente lo más nuevo en seguridad de redes inalámbricas.

A lo largo del tiempo, se incorporó autenticación como una opción para asegurar a las WLANs, y es ahora un componente fundamental en las políticas de redes inalámbricas empresariales. La arquitectura 802.11i especifica a 802.11X para autenticación, resultando en la utilización de EAP y un servidor de autenticación.

Al diseñar y utilizar redes inalámbricas, es bueno que el profesional de seguridad de la red mantenga un nivel apropiado de paranoia. Las redes inalámbricas son extremadamente atractivas para los hackers.

Afortunadamente, si se toman determinadas precauciones, los administradores de red pueden disminuir el riesgo para los usuarios de la red inalámbrica. El administrador de la red debe tener en cuenta varias consideraciones de seguridad:

Las redes wireless que utilizan WEP o WPA/TKIP no son muy seguras y son vulnerables a ataques de hacking.
Las redes inalámbricas que utilizan WPA2/AES deben tener una frase clave (pass phrase) de al menos 21 caracteres.
Si existe una VPN IPsec disponible, procurar utilizarla al conectarse a cualquier LAN inalámbrica pública.
Si no es necesario el acceso inalámbrico, deshabilitar la radio o NIC inalámbrica.

Como profesional de seguridad de la red, el implementar una solución inalámbrica debe requerir absolutamente WPA2/AES junto con autenticación. La autenticación debe ser administrada mediante un servidor de autenticación centralizado.

6.4.4 Consideraciones de seguridad VOIP

VoIP es la transmisión de tráfico de voz sobre redes basadas en IP. IP fue diseñado originalmente para redes de datos, pero su éxito lo ha llevado a ser adaptado para el tráfico de voz.

VoIP se ha vuelto popular en mayor parte debido a las reducciones de costos que permite por sobre las redes de telefonía tradicionales. En las redes telefónicas tradicionales, la mayor parte de la gente paga un cargo mensual fijo por llamadas locales, y un cargo por minuto para las llamadas de larga distancia. Las llamadas de VoIP son realizadas utilizando Internet, siendo que la mayor parte de las conexiones a Internet tienen un cargo mensual fijo. Utilizando las conexiones de Internet tanto para el tráfico de datos como el de voz, los consumidores reducen su cargo telefónico mensual. Para las llamadas internacionales, el ahorro monetario puede resultar enorme.

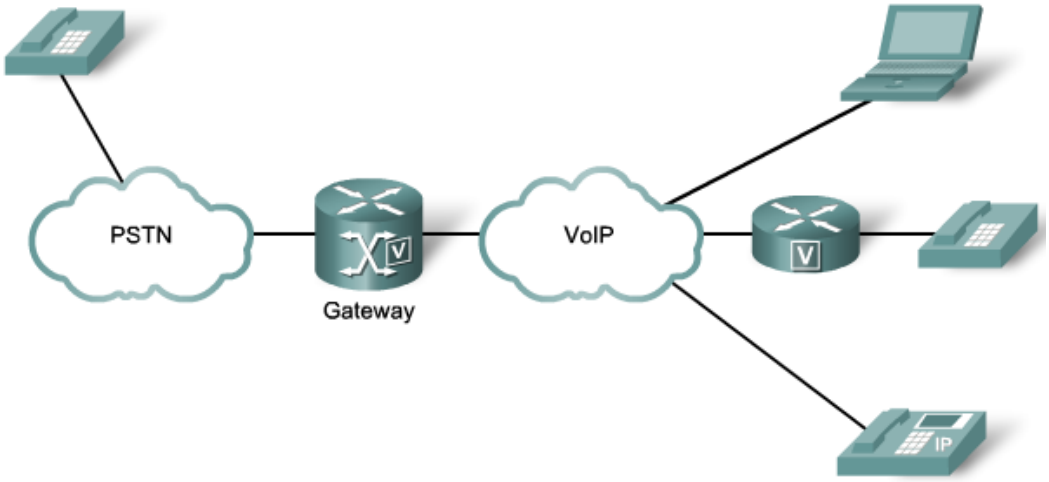
Las ventajas comerciales que llevan a la implementación de las redes VoIP han cambiado con el tiempo. Comenzando por una simple convergencia de los medios, estas ventajas evolucionaron para incluir la convergencia de la inteligencia de conmutación de llamadas y la experiencia de usuario completa. Originalmente, los cálculos de retorno de la inversión se centraban en ahorros de desvío de tráfico y convergencia de redes. Aunque estos ahorros son todavía relevantes, los avances en las tecnologías de voz permiten a las organizaciones y proveedores de servicios diferenciar sus productos ofreciendo funcionalidades avanzadas.

VoIP posee un número de ventajas comerciales:

Los menores costos telefónicos son significativos. Los proveedores de servicios de VoIP cobran hasta un 50 por ciento menos por el servicio de conectividad telefónica. Los aumentos en la productividad debido al servicio de telefonía VoIP pueden ser substanciales. Algunas empresas han reportado incrementos en su productividad de hasta tres horas por semana, por empleado. Funciones tales como encuéntrame/sígueme, oficina remota, clic-para-llamar, integración con Outlook, correo de voz unificado, teleconferencias y herramientas colaborativas permiten incrementos en la productividad.

Los costos de mudanzas, incorporaciones y cambios también son menores. La flexibilidad de VoIP permite mover un teléfono fácilmente entre estaciones de trabajo.
Los costos de servicio y mantenimiento pueden ser menores.
Muchos sistemas VoIP requieren poco o ningún entrenamiento de los usuarios.

Los costos de telefonía móvil disminuyen ya que los empleados realizan las llamadas desde sus laptops, en lugar de utilizar teléfonos celulares. Estas llamadas son parte de los costos de la red y cuestan sólo el monto de la conexión a Internet.
Los costos de telefonía de trabajadores remotos disminuyen y desaparecen los costos de instalación. La comunicación de voz tiene lugar sobre una conexión de banda ancha.
VoIP permite la mensajería unificada. Los sistemas de información están integrados.
El sistema soporta el cifrado de las llamadas de voz.
Es necesario menos personal administrativo para contestar llamadas.



Una red que soporte tráfico de voz tiene un número de componentes:

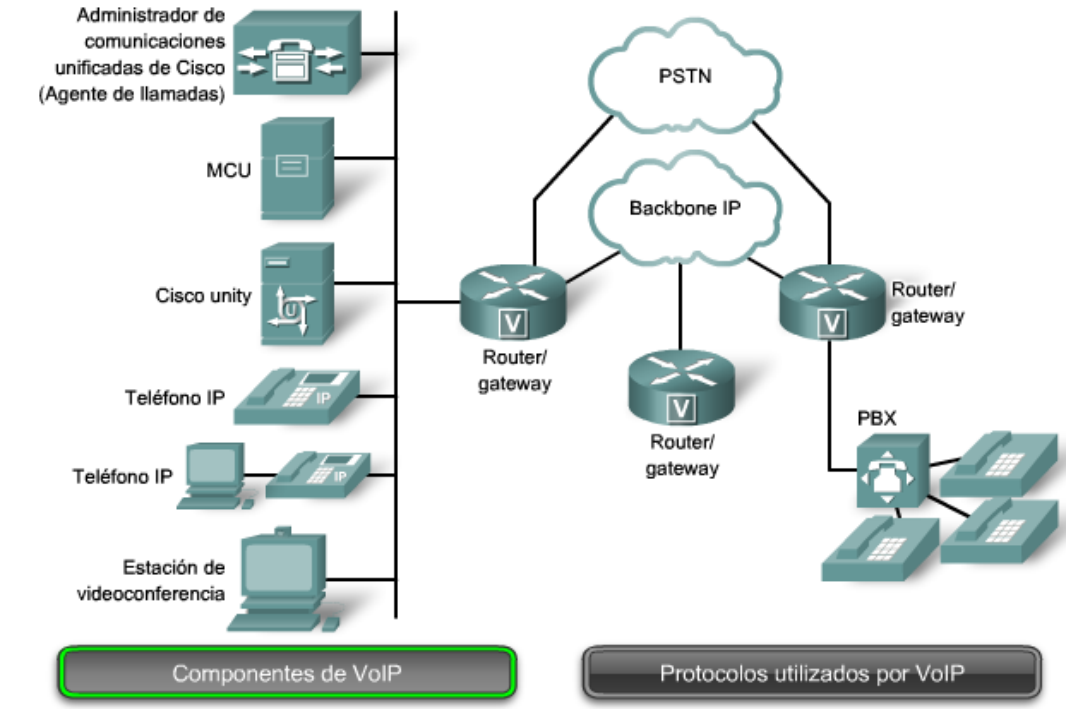
Teléfonos IP - Proveen voz IP en el escritorio.
Gatekeeper - Provee Control de Admisión de Llamadas (CAC - Call Admission Control), control y administración del ancho de banda, y traducción de direcciones.
Gateway - Realiza la traducción entre redes VoIP y no VoIP, tales como PSTN. Los gateways también proporcionan acceso físico a dispositivos de voz analógicos y digitales locales, como teléfonos, máquinas de fax, y PBXs.
Unidad de Control Multipunto (MCU - Multipoint Control Unit) - Provee conectividad en tiempo real para que participantes en múltiples ubicaciones puedan asistir a una misma videoconferencia.

Agente de llamadas (Call agent) - Provee el control de llamadas para teléfonos IP, CAC, administración y control de ancho de banda, y traducción de direcciones. Los productos Administrador de Comunicaciones Unificadas de Cisco y la Edición Empresarial del Administrador de Comunicaciones Unificadas de Cisco funcionan como agentes de llamadas.
Servidores de Aplicaciones - Proveen servicios tales como correo de voz y mensajería unificada, en productos como Cisco Unity.

Estación de Videoconferencia - Provee a los usuarios finales de acceso a videoconferencias. La estación de videoconferencia contiene un dispositivo de captura de video y un micrófono. El usuario puede recibir el audio y video originado en la estación del usuario remoto.

Otros componentes, tales como aplicaciones de voz, sistemas de Respuesta de Voz Interactiva (IVR - Interactive Voice Response), y teléfonos por software, proveen servicios adicionales que apuntan a las necesidades de los sitios empresariales.

VoIP depende de un número de protocolos especializados, incluyendo H.323, Media Gateway Control protocol (MGCP), Session Initiation Protocol (SIP), Skinny Call Control Protocol (SCCP), y Real-Time Protocol (RTP).



Haga clic sobre cada botón para ver los componentes y protocolos de VoIP.

Protocolo VoIP	Descripción
H.323	Protocolo estándar de ITU para conferencias interactivas; evolucionó a partir del estándar de ISDN H.320; flexible, complejo
MGCP	Estándar emergente de IETF para el control del gateway PSNT; control de dispositivo liviano
Megaco/H.248	Estándar conjunto de IETF e ITU para el control del gateway con soporte para múltiples tipos de gateway; evolucionó a partir del estándar MGCP
SIP	Protocolo de IETF para conferencias interactivas y no interactivas; más simple pero menos maduro que H.323
RTP	Protocolo estándar de IETF para streaming de medios
RTCP	Protocolo de IETF que provee control de información fuera de banda para un flujo de RTP
SRTP	Protocolo de IETF que cifra el tráfico de RTP cuando abandona el dispositivo de voz
SCCP	Protocolo propietario de Cisco utilizado entre el Administrador de Comunicaciones Unificadas de Cisco y los teléfonos IP de Cisco



Haga clic sobre cada botón para ver los componentes y protocolos de VoIP.

Las comunicaciones VoIP ocurren sobre la red de datos tradicional. Por este motivo, el asegurar las comunicaciones de voz se relaciona directamente con asegurar la red de datos. Existen diversas amenazas específicas de las redes VoIP.

Acceso no autorizado a los recursos de voz

Los hackers pueden manipular los sistemas de voz, las identidades de usuarios, y configuraciones de teléfonos, e interceptar mensajes de correo de voz. Si los hackers obtienen acceso al sistema de correo de voz, pueden modificar el mensaje de saludo, el cual puede tener un impacto negativo en la imagen y reputación de la compañía. Un hacker que obtiene acceso a la PBX o al gateway de voz puede desactivar puertos de voz o modificar parámetros del enrutamiento de voz, afectando el acceso al servicio dentro y a través de la red.

Comprometer los recursos de la red

El objetivo de una red segura es asegurar que las aplicaciones, procesos y usuarios pueden operar en forma confiable y segura, utilizando los recursos compartidos de la red. Debido a que la infraestructura compartida de la red transporta voz y datos, la seguridad y el acceso a la infraestructura de la red son críticos al asegurar las funciones de voz. Al estar instalados sobre una red de datos, los sistemas de voz IP son objetivos potenciales para hackers quienes antes sólo se enfocaban en PCs, servidores y aplicaciones de datos. Los hackers tienen ayuda en su búsqueda de vulnerabilidades en los sistemas de voz IP gracias a los protocolos y estándares abiertos bien conocidos que son utilizados en las redes IP.

Espionaje

El espionaje (Eavesdropping) involucra la intercepción no autorizada de paquetes de voz o RTP. El espionaje deja expuesta información confidencial o propietaria, obtenida interceptando y reensamblando paquetes en un stream de voz. Los hackers utilizan una variedad de herramientas para llevarlo adelante.

Ataques DoS

Los ataques DoS se definen como ataques de sobrecarga del equipamiento de procesamiento de llamadas, con el fin de denegar el acceso de los usuarios legítimos a los servicios. La mayoría de los ataques DoS coinciden con una de las siguientes tres categorías:

La sobrecarga de recursos de la red involucra la sobrecarga de los recursos requeridos para el funcionamiento apropiado de un servicio. El recurso de red es en general el ancho de banda. El ataque DoS utiliza todo el ancho de banda disponible, provocando que los usuarios autorizados no puedan acceder a los servicios requeridos.
La inanición de recursos del host involucra la utilización de todos los recursos críticos del host. Cuando el uso de estos recursos es llevado al máximo por el ataque DoS, el servidor ya no puede responder a las solicitudes legítimas de servicio.

Un ataque fuera de los límites involucra la utilización de estructuras ilegales de paquetes y datos inesperados, los cuales pueden causar fallas en el sistema operativo del dispositivo remoto. Un ejemplo de este tipo de ataques es la utilización de combinaciones ilegales de flags TCP. La mayoría de las pilas TCP/IP se desarrollan para responder a un uso apropiado, no están desarrolladas para enfrentar anomalías. Cuando la pila recibe datos ilegales, puede no ser capaz de procesar el paquete, causando la falla del sistema.



- Reconocimiento
- Ataques directos como spam sobre telefonía IP (SPIT) y falsificación (spoofing)
- Ataques de espionaje y man-in-the-middle
- Ataques DoS como inanición de DHCP, inundaciones, y fuzzing

El spam de VoIP, o SPIT (Spam Over Internet Telephony), son lotes de mensajes no solicitados enviados mediante VoIP a todos los usuarios finales de una red empresarial. Además de causar molestias, los grandes volúmenes de llamadas pueden afectar significativamente la disponibilidad y productividad de las terminales. Debido a que las

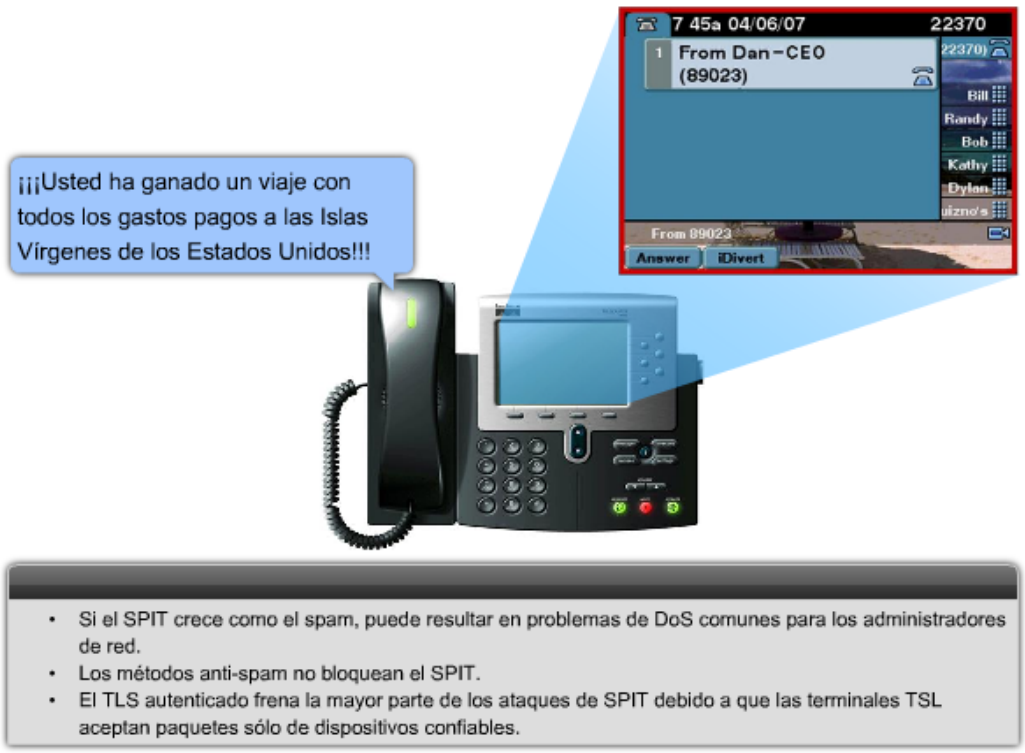
llamadas masivas son además difíciles de rastrear, puede ser utilizadas para fraudes, uso no autorizado, y violaciones a la privacidad.

Hasta el momento, el spam de VoIP es poco frecuente, pero tiene el potencial para convertirse en un problema mayor. SPIT puede ser generado de forma similar al spam de correo electrónico, con botnets apuntando a millones de usuarios de VoIP desde las máquinas comprometidas.

El spam ha sido un problema por años. El correo electrónico comercial no solicitado y malicioso es actualmente la mayor parte del correo electrónico del mundo. Por ejemplo, en Europa, de acuerdo al analista Radicati, se enviaron unos 16 mil millones de mensajes de spam por día en 2006, representando el 62 por ciento de todos los mensajes de correo electrónico de Europa. Se espera que este número se incremente a 37 mil millones de mensajes de spam diarios para 2010. Existe la preocupación de que VoIP sufrirá el mismo destino que el correo electrónico.

Otra preocupación sobre SPIT es que los métodos de prevención de spam no funcionarán. La naturaleza de tiempo real de las llamadas de voz hace que lidiar con SPIT sea un desafío aun mayor que tratar el spam de correo electrónico. Deben inventarse nuevos métodos para resolver los problemas de SPIT.

Authenticated Transport Layer Security (TLS) puede evitar la mayor parte de los ataques de SPIT, debido a que las terminales sólo aceptan paquetes de dispositivos confiables.



- Si el SPIT crece como el spam, puede resultar en problemas de DoS comunes para los administradores de red.
- Los métodos anti-spam no bloquean el SPIT.
- El TLS autenticado frena la mayor parte de los ataques de SPIT debido a que las terminales TSL aceptan paquetes sólo de dispositivos confiables.

Dos tipos comunes de fraude en las redes de VoIP son el "vishing" y el fraude de tarifas.

El vishing (combinación de los términos "voice" y "phishing") utiliza la telefonía para recolectar información, como detalles de cuentas, directamente de los usuarios. Uno de los primeros casos reportados de vishing afectó a PayPal. Las víctimas recibieron primero un correo electrónico que pretendía provenir de PayPal, pidiendo la confirmación de los datos de sus tarjetas de crédito a través del teléfono. A aquellos que llamaron al número indicado en el mensaje se les solicitó ingresar su número de tarjeta de crédito con el teclado del teléfono. Una vez ingresado el número, los perpetradores de este fraude fueron capaces de robar dinero de las cuentas de sus víctimas.

Debido al bajo costo de realizar llamadas por VoIP, en comparación con el sistema telefónico estándar, los atacantes pueden realizar miles de llamadas a gente por muy bajo costo. Los usuarios aún pueden confiar en el teléfono más que en la web, pero estas técnicas de spam pueden socavar su confianza en VoIP.

El fraude de tarifas es el robo del servicio de telefonía de larga distancia mediante el acceso no autorizado a un troncal PSTN (una línea externa) o a un sistema de correo de voz o PBX. El fraude de tarifas es una industria ilegal multimillonaria, y todas las organizaciones son vulnerables. El robo puede también ser definido como el uso del sistema de telefonía tanto por usuarios autorizados como no autorizados, para acceder a números no autorizados, tales como cuentas de tarifas reducidas.

Este fraude no es nuevo, y las PBXs siempre han sido vulnerables. La diferencia es que muy poca gente puede hackear una PBX, en comparación al número de personas irrumpiendo activamente en los sistemas IP. Para protegerse de tales fraudes, los administradores de red utilizan funciones que existen en el sistema Administrador de Comunicaciones Unificadas de Cisco para controlar las llamadas telefónicas, tales como filtros de llamadas, particiones, o Códigos de Autorización Forzada (FACs - Forced Authorization Codes).

Otro problema de seguridad de VoIP que se incrementa se relaciona con SIP (Session Initiation Protocol). Se espera que la utilización creciente de SIP para VoIP abra un nuevo frente en la guerra de la seguridad. SIP es un protocolo relativamente nuevo, el cual ofrece poca seguridad inherente. Algunas de sus características también lo hacen vulnerable a hackers, como utilizar extensiones SIP que puedan crear agujeros de seguridad.

Ejemplos de hacks para SIP incluyen el secuestro de registraciones, los cuales permiten al hacker interceptar llamadas entrantes y redirigirlas, la manipulación de mensajes, que permite al hacker modificar los paquetes de datos transmitidos entre direcciones SIP, y el derrumbamiento de sesiones, lo que permite al hacker finalizar llamadas o realizar ataques DoS apuntados a VoIP inundando el sistema con solicitudes de finalización.



Un fraude toma diferentes formas:

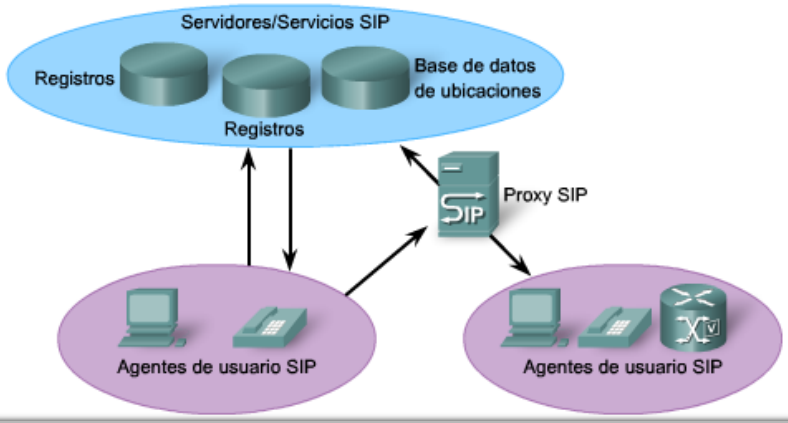
- Vishing - Una versión de voz del phishing utilizada para comprometer la confidencialidad.
- Robo y fraude de tarifas - Es el robo de servicios telefónicos.

Utilice funciones del Administrador de Comunicaciones Unificadas de Cisco para protegerse contra fraudes.

- Las particiones limitan qué partes del plan de llamadas pueden acceder determinados teléfonos.
- Los planes de llamadas filtran el control de acceso a números telefónicos abusivos.
- Los FACs previenen las llamadas no autorizadas y proveen mecanismos de rastreo.

Fraude | Vulnerabilidades SIP

Haga clic sobre cada botón para obtener más información sobre los tipos de fraude y vulnerabilidades SIP.



- Secuestro de inscripciones – Permite a un hacker interceptar llamadas entrantes y volver a enrutarlas.
- Manipulación de mensajes – Permite a un hacker modificar los paquetes de datos que viajan entre dos direcciones SIP.
- Interrupción de la sesión – Permite al hacker terminar llamadas o llevar adelante ataques DoS apuntados a VoIP.

Fraude | Vulnerabilidades SIP

Haga clic sobre cada botón para obtener más información sobre los tipos de fraude y vulnerabilidades SIP.

6.4.5 Soluciones de seguridad VOIP

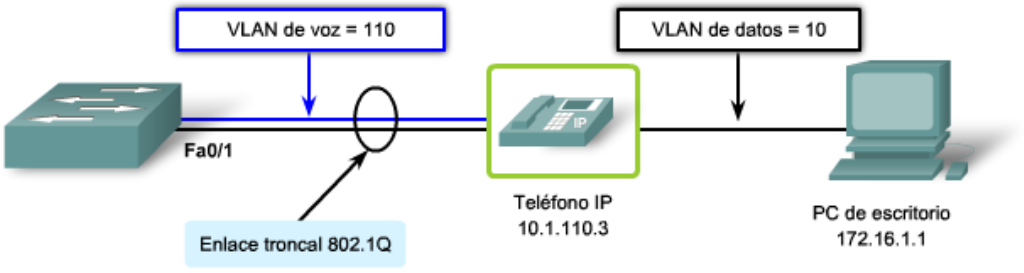
Muchas soluciones de seguridad IP pueden ser implementadas sólo en dispositivos de capa 3. Debido a la arquitectura del protocolo, la capa 2 ofrece muy poca o ninguna seguridad inherente. Comprender y establecer dominios de broadcast es uno de los conceptos fundamentales en el diseño de las redes IP seguras. Muchos ataques simples

pero peligrosos pueden ser disparados si el dispositivo atacante reside dentro del mismo dominio de broadcast que el sistema objetivo. Por este motivo, los teléfonos IP, gateways IP, y estaciones de administración de la red deben ubicarse siempre en su propia subred, en forma separada del resto de las redes de datos, y entre sí.

Para asegurar la privacidad e integridad de las comunicaciones, las transmisiones de voz deben protegerse contra el espionaje y la manipulación. Las tecnologías de redes de datos tales como VLANs permiten segmentar el tráfico de voz del tráfico de datos, previniendo el acceso a la VLAN de voz desde la VLAN de datos. La utilización de VLANs separadas para voz y datos previene a los atacantes o sus aplicaciones de observar o capturar el tráfico de otras VLANs a medida que atraviesa el cable físico. Al asegurarse de que cada dispositivo se conecta a la red utilizando una infraestructura conmutada, las herramientas de captura de tráfico también pueden volverse menos efectivas.

Asignar el tráfico de voz a VLANs específicas para segmentar en forma lógica el tráfico de datos y voz es una práctica recomendada por toda la industria. Tanto como sea posible, los dispositivos identificados como dispositivos de voz deben ser restringidos a las VLANs de voz dedicadas. Esta solución asegura que sólo puedan comunicarse con otros recursos de voz. Más importante aún, el tráfico de voz se mantiene separado de la red de datos general, donde podría ser fácilmente interceptado o manipulado. Disponer de una VLAN específica para voz facilita la aplicación de listas de control de acceso de VLANs (VACLs) para proteger el tráfico de voz.

Al comprender los protocolos utilizados entre dispositivos en la red VoIP, es posible implementar ACLs efectivas en las VLANs de voz. Los teléfonos IP envían sólo tráfico RTP entre sí y nunca existe motivo alguno para que envíen tráfico TCP o ICMP a otro teléfono IP. Los teléfonos IP envían unos pocos protocolos TCP y UDP para comunicarse con sus servidores. Muchos de los ataques a teléfonos IP pueden ser evitados utilizando ACLs en las VLANs de voz para prevenir desviaciones de estos principios.



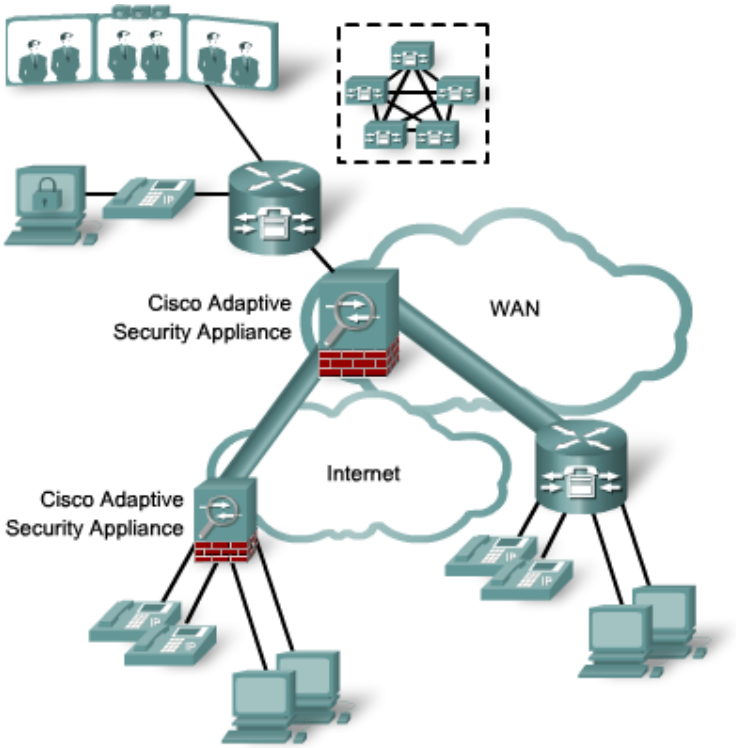
- Crea un dominio de broadcast separado para el tráfico de voz.
- Protege contra la manipulación y el espionaje.
- Vuelve poco efectivas a las herramientas de captura de paquetes.
- Facilita la implementación de VACLs específicas para el tráfico de voz.

Los firewalls pueden inspeccionar paquetes y compararlos con las reglas configuradas en base a los puertos especificados. Resulta difícil especificar de antemano qué puertos serán utilizados en una llamada de voz, debido a que los puertos son negociados dinámicamente durante el establecimiento de la llamada.

Cisco ASA Adaptive Security Appliances inspecciona los protocolos de voz para asegurar que las solicitudes SIP, SCCP, H.323 y MGCP conforman los estándares de voz. Cisco ASA Adaptive Security Appliances también puede proveer estas funcionalidades para ayudar en la protección del tráfico de voz:

Asegurar que las solicitudes SIP, SCCP, H.323, y MGCP corresponden con los estándares.
Prevenir el envío de métodos SIP inapropiados al Administrador de Comunicaciones Unificadas de Cisco.
Límite de solicitudes SIP.
Aplicar la política de llamadas (whitelist, blacklist, caller/called party, SIP Uniform Resource Identifier).
Abrir puertos en forma dinámica para aplicaciones Cisco.
Habilitar llamadas sólo para los "teléfonos registrados".
Habilitar la inspección de llamadas telefónicas cifradas.

Los firewalls Cisco IOS también proveen muchas de estas características de seguridad.



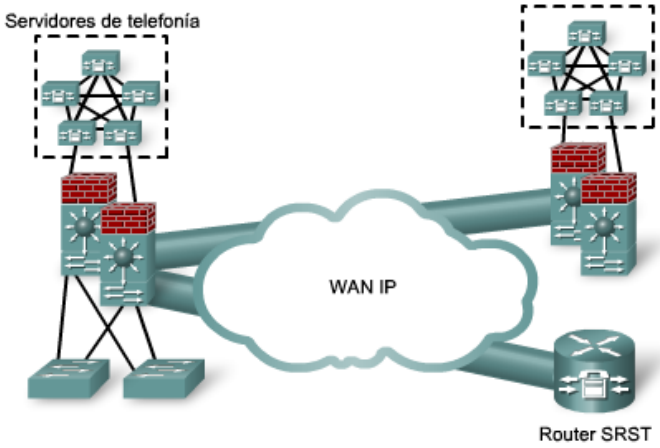
Las VPNs son ampliamente utilizadas para proveer conexiones seguras a las redes corporativas. Las conexiones pueden originarse desde una sucursal comercial, una oficina hogareña (SOHO), un trabajador a distancia, o un usuario móvil. IPsec puede ser utilizado para los servicios de autenticación y confidencialidad. Para facilitar el

desempeño, se recomienda que los túneles VPN terminen dentro de un firewall. El firewall es utilizado para inspeccionar y proteger los protocolos de texto plano.

Al implementar VPNs a través de Internet o una red pública, es importante considerar la ausencia de QoS. Cuando sea posible, QoS debe ser acordado con el proveedor mediante un acuerdo de nivel de servicio (SLA - Service Level Agreement). Un SLA es un documento que detalla los parámetros esperados de QoS para los paquetes que atraviesan la red del proveedor.

Las comunicaciones de voz no funcionan bien (o incluso no funcionan) si hay latencia. Debido a que las VPNs seguras cifran los datos, pueden crear un cuello de botella al procesar los paquetes con su algoritmo de cifrado. El problema suele volverse peor a medida que se incrementa la seguridad.

VoIP es totalmente compatible con DES o 3DES siempre y cuando la VPN entregue la velocidad de transmisión necesaria. Internacionalmente, las corporaciones pueden encontrarse con otros problemas que afecten las comunicaciones de voz. El Departamento de Comercio de los Estados Unidos impone restricciones en la exportación de ciertas tecnologías de cifrado. Usualmente, DES es exportable, mientras que 3DES no lo es. Sin embargo, las regulaciones toman numerosas formas, desde exclusiones completas de exportación aplicadas en ciertos países, hasta permitir la exportación de 3DES a industrias y usuarios específicos. La mayoría de las corporaciones con VPNs extendidas por fuera de los Estados Unidos deben consultar si su proveedor de VPN posee productos exportables, y cómo se ven afectadas por las regulaciones de exportación las redes que los utilizan.



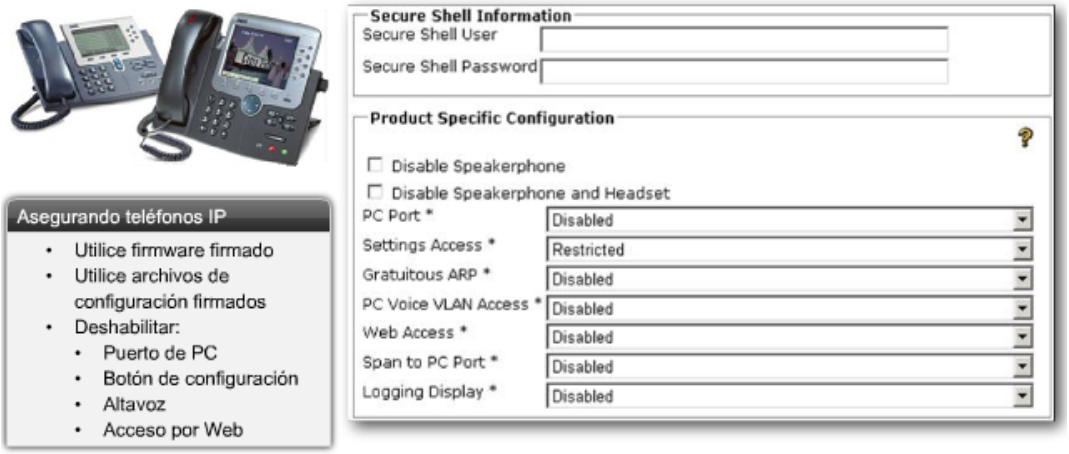
Prácticas de seguridad recomendadas para VoIP

- Utilizar IPsec para la autenticación
- Utilizar IPsec para proteger todo el tráfico, no sólo el de voz
- Considerar un SLA con el proveedor del servicio
- Terminar en un concentrador VPN o un router grande dentro de un firewall, para obtener estos beneficios:
  - Desempeño
  - Complejidad de configuración reducida
  - Límites organizacionales administrados

Al asegurar el tráfico de voz, no debe olvidarse asegurar también a los servidores de aplicaciones de voz. Las versiones más nuevas del Administrador de Comunicaciones Unificadas de Cisco deshabilitan los servicios innecesarios y los nombres de usuario por

defecto, permiten sólo la instalación de imágenes firmadas, poseen CSA instalado, y soportan protocolos de administración seguros.

Combinando la seguridad de transporte, provista por LANs seguras, firewalls y VPNs, con las características de seguridad de las aplicaciones y hosts disponibles con el Administrador de Comunicaciones Unificadas de Cisco y los teléfonos Cisco, es posible lograr un ambiente de telefonía IP con un alto nivel de seguridad.



6.4.6 Consideraciones de seguridad SAN

Una SAN es una red especializada que permite un acceso seguro y confiable entre servidores y recursos de almacenamiento externos. En una SAN, el dispositivo de almacenamiento no es propiedad exclusiva de un servidor en particular. En su lugar, los dispositivos de almacenamiento son compartidos entre todos los servidores de la red como recursos pares. De la misma forma que una LAN puede ser utilizada para conectar clientes y servidores, una SAN puede ser utilizada para conectar servidores con almacenamiento, servidores entre sí, y dispositivos de almacenamiento entre sí.

Una SAN no necesita encontrarse en una red separada físicamente. Puede ser una subred dedicada que transporta sólo tráfico comercial crítico de entrada/salida entre los servidores y los dispositivos de almacenamiento. Una SAN, por ejemplo, no debería transportar tráfico de propósito general como correo electrónico y otras aplicaciones de usuario final. Debe limitarse a tráfico de entrada/salida, como la lectura de un archivo desde un disco, o escribir en un archivo en un disco. Esta solución de red permite evitar riesgos y reducciones de desempeño inaceptables, que son inherentes cuando una sola red es utilizada para todas las aplicaciones.

Las salidas de servicio de la red y los servidores cuestan a las compañías grandes sumas de dinero en pérdidas de negocios y productividad. Al mismo tiempo, la cantidad de información que debe ser administrada y almacenada se incrementa dramáticamente cada año.

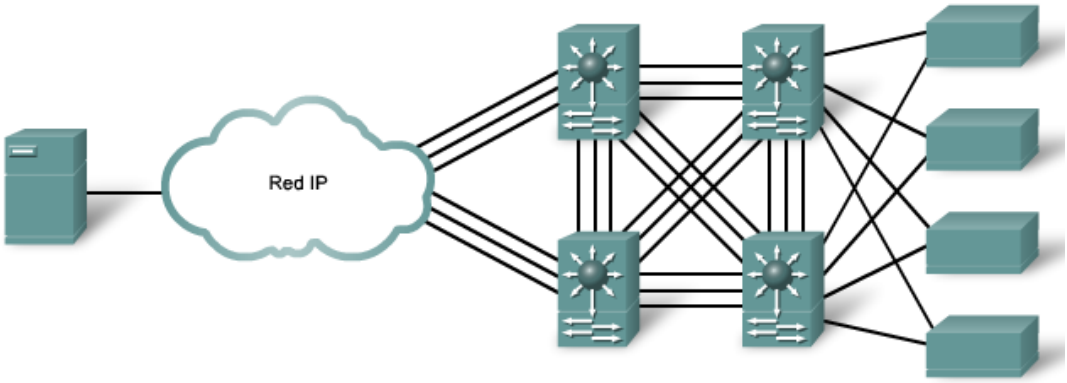
Las SANs ofrecen una respuesta al creciente volumen de datos que deben ser almacenados en una red comercial. Implementando SAN, los usuarios pueden quitar la

carga del tráfico de almacenamiento de entre las operaciones diarias de la red, y establecer una conexión directa entre los medios de almacenamiento y los servidores.

Las SANs están evolucionando rápidamente en las infraestructuras empresariales para cumplir con los tres requisitos primarios de negocios:

Reducir los gastos operativos.
Incrementar la agilidad para soportar cambios en las prioridades comerciales, requisitos de aplicaciones, y crecimiento de las ganancias.
Mejorar la replicación, copias de respaldo, y recuperación de larga distancia, para cumplir con los requisitos regulatorios y mejores prácticas de la industria.

Cisco provee un enfoque empresarial para la implementación de SANs escalables, con alta disponibilidad y de fácil administración. Las soluciones Cisco para SANs inteligentes son una parte integral de la arquitectura del centro de datos de una empresa. Las soluciones SAN de Cisco proveen un medio preferible para acceder, administrar y proteger los recursos de información a través de una variedad de tecnologías de transporte de SAN. Éstas incluyen canal de fibra (Fibre Channel), canal de fibra sobre IP (FCIP - Fibre Channel over IP), Internet Small Computer Systems Interface (iSCSI), Gigabit Ethernet, o redes ópticas.



Red especializada que permite un acceso rápido y confiable entre servidores y recursos de almacenamiento externos.

Todas las grandes tecnologías de transporte SAN se basan en el modelo de comunicaciones SCSI. De muchas formas, una SAN puede ser descripta como la fusión entre SCSI y las redes. El protocolo de comandos SCSI es el estándar por defecto que se utiliza en forma extensiva en aplicaciones de almacenamiento de alto desempeño. El comando SCSI puede ser transportado a través de un canal de fibra SAN o encapsulado en IP, y llevado a través de redes IP.

Existen tres grandes tecnologías de transporte SAN:

Canal de fibra - Esta tecnología es el transporte primario de SAN para la conectividad de host a SAN. Tradicionalmente, las SANs han requerido una infraestructura dedicada separada para interconectar a los hosts con los sistemas de almacenamiento. El

protocolo primario de transporte para esta interconexión han sido los Canales de Fibra. Las redes de Canales de Fibra proveen un transporte serial para el protocolo SCSI.

iSCSI - Mapea SCSI sobre TCP/IP. Es otro modelo de conectividad de host a SAN, utilizado típicamente en la LAN. iSCSI aprovecha la inversión en redes IP existentes para construir y extender las SANs. Esto se logra utilizando TCP/IP para transportar los comandos SCSI, datos y el estado entre los hosts, o iniciadores, y los dispositivos de almacenamiento, u objetivos, tales como subsistemas de almacenamiento y dispositivos de cinta.
FCIP - El popular modelo SAN a SAN es utilizado con frecuencia sobre una WAN o una MAN. Los diseñadores de SAN pueden utilizar el protocolo de estándar abierto FCIP para romper la barrera de distancia entre las soluciones actuales de canal de fibra y habilitar la interconexión de SANs aisladas a través de distancias extendidas.

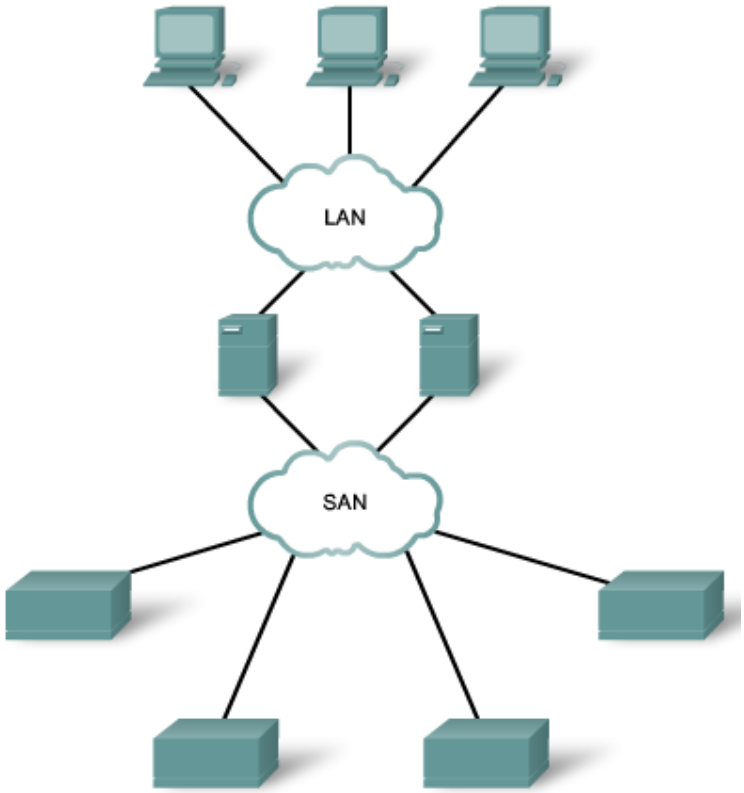
En el almacenamiento de las computadoras, un número de unidad lógica (LUN - Logical Unit Number) es una dirección de 64 bits para una unidad de disco individual y, por extensión, el dispositivo de disco mismo. El término es utilizado en el protocolo SCSI como una forma de diferenciar unidades de disco individuales dentro de un mismo dispositivo SCSI, como puede ser un arreglo de discos.

El enmascaramiento de LUN es un proceso de autorización que hace al LUN disponible para algunos hosts y no disponible para otros. El enmascaramiento de LUN se implementa en forma primaria a nivel del adaptador de bus del host (HBA - Host Bus Adapter). El enmascaramiento de LUN que se implementa a este nivel es vulnerable a cualquier ataque que comprometa al HBA.

Los beneficios de seguridad del enmascaramiento de LUN son limitados porque, con muchos HBAs, es posible falsificar la dirección de origen. El enmascaramiento de LUN es principalmente una forma de protegerse contra los servidores que intenten corromper discos pertenecientes a otros servidores.

Por ejemplo, los servidores Windows incorporados a una SAN pueden corromper volúmenes que no pertenezcan a Windows, intentando escribir etiquetas de volumen de Windows sobre ellos. Enmascarando los LUNs de los volúmenes no pertenecientes a Windows desde el servidor Windows, esto puede prevenirse ya que de esta forma el servidor Windows no tiene conocimiento de los volúmenes que no le pertenecen.

Hoy en día, los LUNs en general no son unidades de disco individuales, sino particiones virtuales (o volúmenes) de un conjunto RAID (Redundant Array of Independent Disks).



Un WWN (World Wide Name) es una dirección de 64 bits utilizada por las redes de canal de fibra para identificar en forma unívoca a cada elemento de la red.

La zonificación puede utilizar WWNs para asignar permisos de seguridad. La zonificación puede también utilizar servidores de nombres en los switches para permitir o denegar el acceso a WWNs específicos en la trama del switch.

La utilización de WWNs con fines de seguridad es inherentemente inseguro, debido a que el WWN de un dispositivo es un parámetro configurable por el usuario. La zonificación utilizada por los WWNs es susceptible al acceso no autorizado, ya que las zonas pueden ser pasadas por alto si un atacante es capaz de falsificar el WWN de un HDA autorizado. Un HBA es un adaptador de entrada/salida que se ubica entre el bus del host y el bucle del canal de fibra, y administra la información entre ambos canales.



Cisco MDS 9124 Fibre Channel Fabric Switch

En las redes de almacenamiento, la zonificación de un canal de fibra consiste en la partición de la trama del canal de fibra en conjuntos más pequeños. Si una SAN

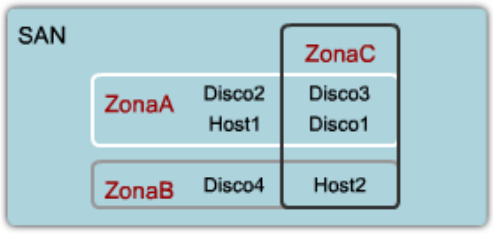
contiene varios dispositivos de almacenamiento, alguno de ellos no necesariamente debe poder interactuar con los demás dispositivos en la SAN.

La zonificación puede a veces ser confundida con el enmascaramiento de LUN, debido a que ambos procesos tienen el mismo objetivo. La diferencia es que la zonificación se implementa sobre la trama del switch, mientras que el enmascaramiento de LUN se realiza sobre los dispositivos terminales. La zonificación es también potencialmente más segura. Los miembros de una zona sólo ven a otros miembros de la misma zona. Los dispositivos pueden ser miembros de más de una zona.

Existen algunas reglas simples que deben tenerse en cuenta sobre el funcionamiento de la zonificación:

Los miembros de una zona sólo pueden ver a otros miembros de la misma zona.
Las zonas pueden ser configuradas en forma dinámica, en base a los WWNs.
Los dispositivos pueden ser miembros de más de una zona.
La zonificación de la trama de conmutación puede realizarse en el puerto o en el dispositivo, en base al puerto físico del switch, el WWN del dispositivo, o el ID del LUN.

La zonificación de la trama del canal de fibra tiene el beneficio de asegurar el acceso a los dispositivos y permitir la coexistencia de los sistemas operativos. La zonificación se aplica sólo a la topología de trama de conmutación, no existe en las topologías de canal de fibra más simples.

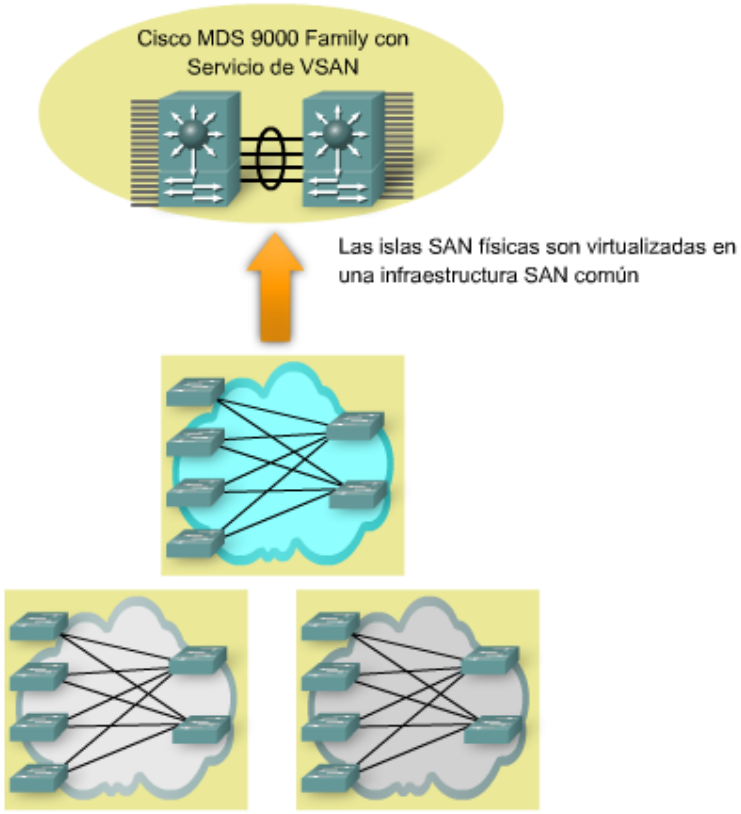


Ejemplo de zonificación. Observe que los dispositivos pueden ser miembros de más de una zona.

Una red virtual de área de almacenamiento (VSAN) es una colección de puertos de un conjunto de switches conectados mediante un canal de fibra, formando una trama virtual. Los puertos pueden ser particionados dentro de un mismo switch, creando múltiples VSANs. Adicionalmente, múltiples switches pueden unir cualquier número de puertos para formar una misma VSAN. De esta forma, las VSANs se parecen mucho a las VLANs. Al igual que las VLANs, el tráfico es etiquetado a medida que atraviesa los enlaces entre switches con un ID de VSAN.

Los eventos de la trama son aislados por VSAN. Las VSANs utilizan un aislamiento basado en hardware, por lo que el tráfico se etiqueta en forma explícita con información de la VSAN a través de los enlaces entre switches. También es posible recolectar estadísticas por cada VSAN.

Las VSANs fueron inventadas originalmente por Cisco, pero actualmente han sido adoptadas como un estándar ANSI.

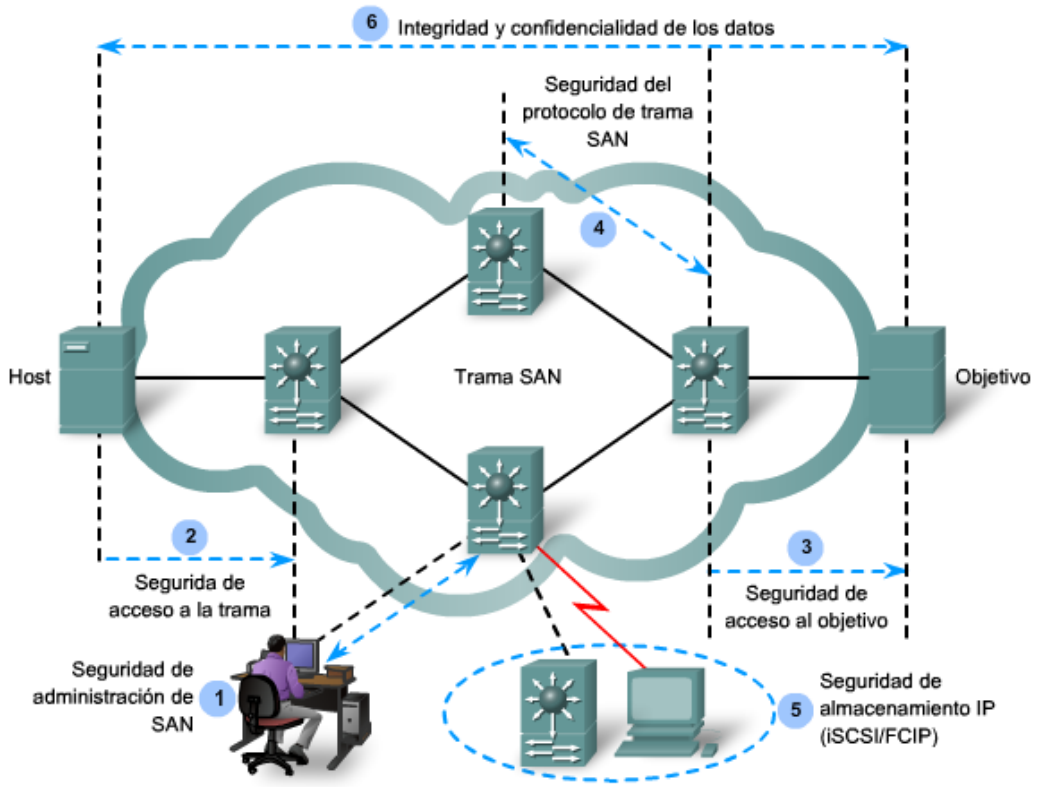


6.4.7 Soluciones de seguridad SAN

Con el fin de asegurar las SANs, es necesario asegurar la trama de las SANs, todos los hosts asociados, y los discos en sí.

Existen seis áreas críticas a considerar cuando se asegura una SAN:

Administración de la SAN - Asegurar los servicios de administración utilizados para administrar la SAN.
Acceso a la trama - Acceso seguro a la trama. La trama de la SAN se refiere al hardware que conecta los servidores a los dispositivos de almacenamiento.
Acceso a los objetivos - Asegurar el acceso a los dispositivos de almacenamiento (objetivos) y a los LUNs.
Protocolos SAN - Asegurar los protocolos utilizados en la comunicación de switch a switch.
Acceso al almacenamiento IP - FCIP y iSCSI seguros.
Integridad y secreto de los datos - Cifrado de los datos a medida que atraviesa las redes, y al ser almacenado en los discos.



Existen diferentes tipos de herramientas disponibles para la administración de SANs, las cuales pueden administrar el desempeño a nivel de dispositivos y a nivel de aplicaciones, además de ofrecer servicios de reportes y monitoreo. Cualquiera sea la herramienta de administración utilizada, debe asegurarse que el acceso a la misma sea seguro. Al administrar una SAN, existen otros aspectos de seguridad a tener en cuenta:

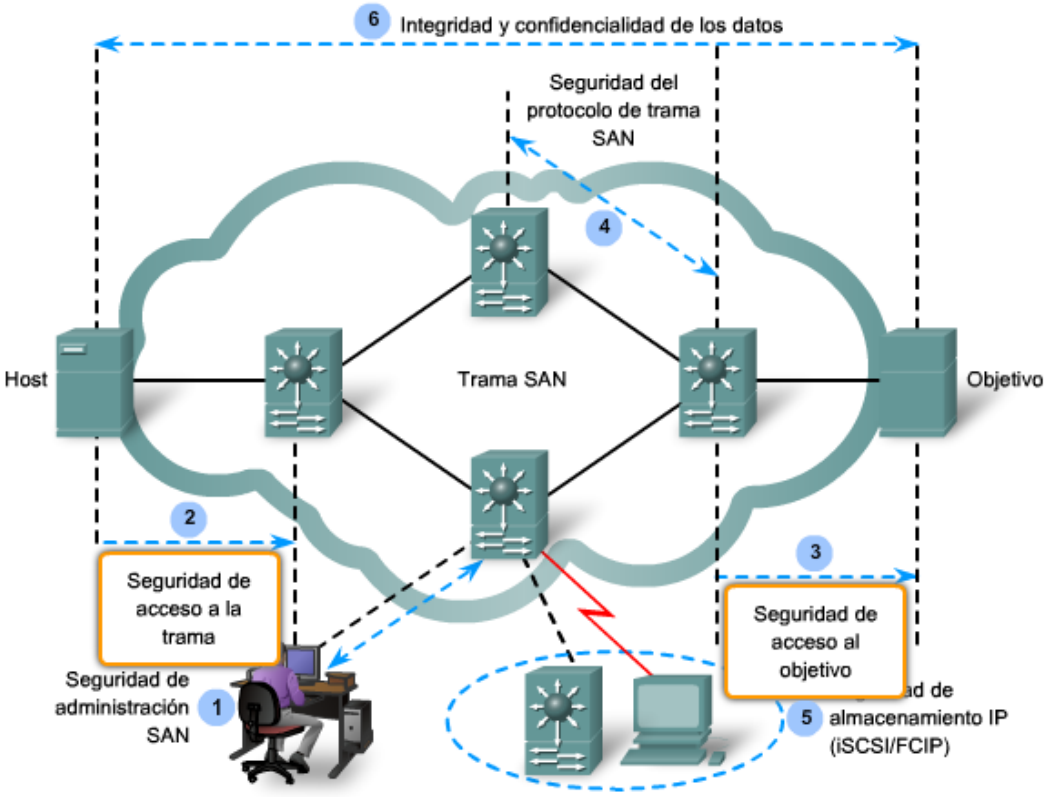
Interrupción de proceso de conmutación - Un ataque DoS puede causar una carga excesiva del CPU, impidiendo su reacción a eventos de la trama.
Arriesgar la trama - Las configuraciones modificadas o perdidas pueden resultar en cambios a los servicios o puertos configurados.
Arriesgar la integridad y confidencialidad de los datos - Poner en peligro los datos compromete la integridad y confidencialidad de la información almacenada.



Para asegurar la integridad de los datos de las aplicaciones, la integridad de LUN, y el desempeño de las aplicaciones, es necesario asegurar tanto la trama como el acceso a los objetivos.

Si la trama y el acceso a los objetivos no son seguros, esto puede resultar en el acceso no autorizado a los datos. El acceso no autorizado significa que la integridad y confidencialidad de los datos han sido comprometidas. Los datos también pueden haber sido corrompidos o eliminados. Si el LUN se ve comprometido en forma accidental o intencional, los datos pueden perderse y la disponibilidad puede verse amenazada. Finalmente, el desempeño y disponibilidad de las aplicaciones pueden verse afectados por eventos de trama o de entrada/salida innecesarios, debido a que el procesador se mantiene más ocupado que lo requerido.

Para prevenir este tipo de problemas, deben utilizarse las VSANs y la zonificación.



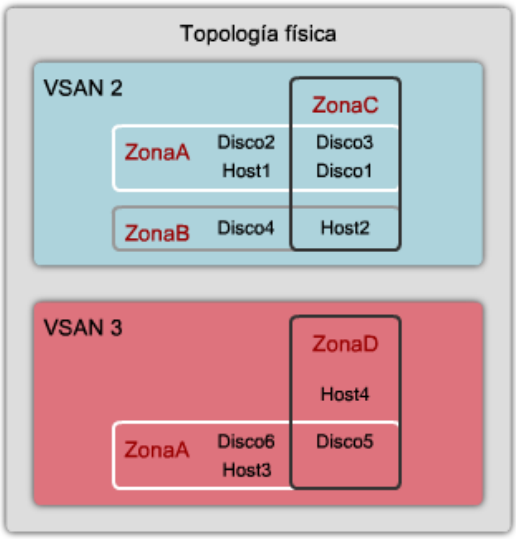
Las VSANs y las zonas son tecnologías complementarias que funcionan bien juntas como control de seguridad en una SAN. El primer paso al configurar estos protocolos complementarios es asociar los puertos físicos con una VSAN, de forma similar a asociar puertos del switch a una VLAN, y luego dividir dichas VSANs en zonas.

La zonificación es el mecanismo primario para asegurar el acceso a objetivos de la SAN (discos y cintas). Existen dos métodos principales de zonificación, uno fuerte y otro débil. La zonificación débil restringe los servicios de nombres de la trama, mostrando a un dispositivo sólo un subconjunto de dispositivos permitidos. Cuando un servidor busca en el contenido de la trama, sólo puede ver a los dispositivos que tiene permitido

ver. Sin embargo, cualquier servidor puede intentar contactar otros dispositivos de la red en base a sus direcciones.

En contraste, la zonificación fuerte restringe las comunicaciones a través de la trama. Esta zonificación es la más utilizada, debido a que es la más segura.

Relación entre las VSANs y las zonas



Dos VSANs con múltiples zonas en cada una. Los discos y los hosts están dedicados a las VSANs aunque tanto hosts como discos pueden pertenecer a múltiples zonas dentro de una misma VSAN. Sin embargo, no pueden pertenecer a más de una VSAN.

Para asegurar los datos durante su transmisión, se emplean diferentes técnicas. iSCSI implementa varias estrategias comunes a las redes IP. Por ejemplo, las ACLs IP son análogas a las zonas de canal de fibra, las VLANs son similares a las VSANs, y la seguridad de puertos IEEE 802.1X se asemeja a la seguridad de puertos de los Canales de Fibra.

Para la seguridad en la transmisión de datos, se utilizan diferentes protocolos de cifrado y autenticación:

Diffie-Hellman Challenge Handshake Authentication Protocol (DH-CHAP)
Fibre Channel Authentication Protocol (FCAP)
Fibre Channel Password Authentication Protocol (FCPAP)
Encapsulating Security Payload (ESP)
Fibre Channel Security Protocol (FC-SP)

La seguridad FCIP combina varias características de la seguridad IP en los routers basados en el Cisco IOS:

IPsec para la seguridad sobre redes públicas
Servicios de cifrado de alta velocidad sobre hardware especializado
Filtrado por firewall

Asegurar las SANs completa el proceso de asegurar la LAN: asegurar las terminales, los switches, el ambiente wireless, la infraestructura VoIP, y las SANs.

Al referirse a asegurar la LAN, se han realizado muchas referencias a IPsec. IPsec es un medio de cifrado de datos entre terminales, como es el caso de un túnel VPN. Para comprender el funcionamiento de IPsec, es necesario poseer un conocimiento básico sobre criptografía.

iSCSI combina muchas de las características de seguridad inherentes a Ethernet e IP:

- Las ACLs son como las zonas de Fibre Channel
- Las VLANs son como las VSANs de Fibre Channel
- La seguridad de puertos de 802.1X es como la seguridad de puertos de Fibre Channel

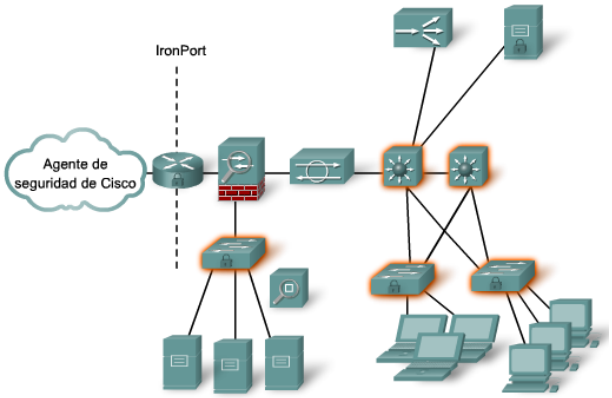
La seguridad FCIP combina muchas características de seguridad IP en los routers basados en Cisco IOS:

- Conexiones VPN IPsec a través de redes públicas
- Servicios de cifrado de alta velocidad en hardware especializado
- Puede ser ejecutado a través de un firewall

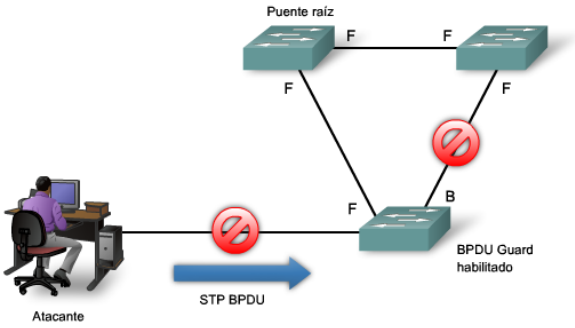
6.5.1 Resumen del capitulo



- Al nivel de la Capa 2, existe un número de vulnerabilidades que requieren técnicas de mitigación especializadas.
- Los ataques de falsificación de direcciones MAC se ven minimizados con la utilización de seguridad de puertos.
- Los ataques por manipulación de STP son manejados por BPDU Guard y Root Guard.
- Los ataques por desbordamiento de la tabla de direcciones MAC son resueltos con seguridad de puertos, BPDU Guard y Root Guard.
- El control de tormentas es utilizado para mitigar los ataques de tormentas de LAN.



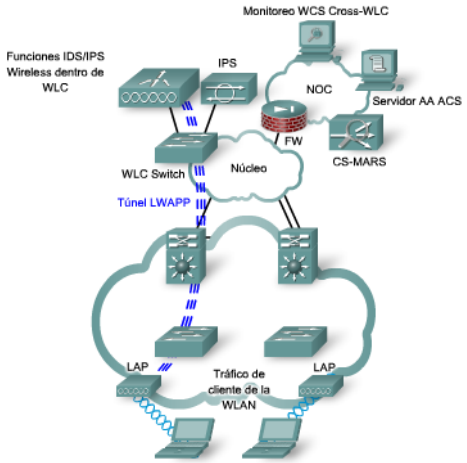
Haga clic sobre cada botón para ver la información asociada.



- La seguridad de puertos provee una solución de seguridad básica en la Capa de Acceso.
- La seguridad de puertos se verifica utilizando los comandos show de CLI y el comando de notificaciones `mac address-table`.
- BPDU Guard y Root Guard están diseñados para mitigar ataques de STP.
- SPAN habilita la replicación de puertos, lo que permite monitorear el tráfico a través del switch.
- RSPAN extiende la fncionalidad de SPAN a múltiples switches y a los enlaces troncales entre ellos.

Haga clic sobre cada botón para ver la información asociada.

- Las redes empresariales modernas implementan dispositivos wireless, VoIP y SAN, que requieren soluciones de seguridad especializadas.
- Las tecnologías wireless son las más proclives a los ataques de red. Un número de tecnologías ha evolucionado para mitigar estos ataques.
- Con la creciente adopción de VoIP, han surgido varias consideraciones de seguridad específicas de la tecnología VoIP. Avances recientes en la seguridad de VoIP se refieren a estas preocupaciones.
- La tecnología SAN permite un acceso a los datos más rápido, simple y confiable. Asegurar los datos es el objetivo principal, por lo que se han desarrollado tecnologías específicas para protejer a



Haga clic sobre cada botón para ver la información asociada.

7- Sistemas Criptográficos
7.0 Introducción al capitulo
7.0.1 Introducción al capitulo

Una red puede ser asegurada mediante la fortificación de los dispositivos (device hardening), control de acceso AAA, funciones de firewall, e implementaciones IPS. Estas funciones combinadas protegen al mismo tiempo a los dispositivos de infraestructura y a los dispositivos finales de la red local. Pero, ¿cómo se protege el tráfico de red al atravesar la Internet pública? La respuesta es mediante métodos criptográficos.

La criptología es la ciencia que crea y rompe códigos secretos. El desarrollo y utilización de estos códigos es llamado criptografía y el romper códigos es llamado criptoanálisis. La criptografía ha sido utilizada por siglos para proteger documentos secretos. Por ejemplo, Julio César utilizó un cifrado alfabético simple para cifrar mensajes enviados a sus generales en el campo de batalla. Sus generales conocían la clave requerida para descifrar los mensajes. En la actualidad, se utilizan métodos criptográficos modernos de muchas formas para asegurar las comunicaciones.

Las comunicaciones seguras requieren una garantía de que el mensaje no ha sido falseado y que realmente proviene de quien indica el remitente (autenticación). Además, debe garantizar que nadie interceptó ni alteró el mensaje (integridad). Finalmente, las comunicaciones seguras garantizan que, si el mensaje es capturado, no podrá ser descifrado (confidencialidad).

Los principios de la criptología pueden ser utilizados para explicar cómo se utilizan los protocolos y algoritmos modernos para asegurar las comunicaciones. Muchas redes actuales aseguran la autenticación mediante protocolos tales como HMAC. La integridad se logra implementando MD5 o SHA-1. La confidencialidad de los datos se asegura mediante algoritmos de cifrado simétrico, incluyendo DES, 3DES y AES o algoritmos asimétricos, incluyendo RSA y la infraestructura de clave pública (PKI). Los algoritmos de cifrado simétrico se basan en la premisa de que cada participante de la comunicación conoce una clave pre-compartida. Los algoritmos de cifrado asimétrico se basan en la presunción de que los participantes de la comunicación no poseen una clave compartida previamente y deben establecer un método seguro para hacerlo.

En la práctica de laboratorio del capítulo, Exploración de métodos de cifrado, los estudiantes descifrarán un mensaje previamente cifrado utilizando el cifrador Vigenere, crearán un mensaje cifrado con Vigenere y utilizarán esteganografía para insertar un mensaje secreto en un gráfico. La práctica de laboratorio se encuentra en el manual de laboratorio en Academy Connection, en cisco.netacad.net.

En este capítulo aprenderá a:

- Explicar que la criptología consiste en la criptografía (codificar mensajes) y el criptoanálisis (decodificar mensajes) y cómo estos conceptos se aplican a la criptografía moderna.
- Explicar cómo el asegurar las comunicaciones mediante diferentes medios criptográficos, incluyendo el cifrado, el hashing y las firmas digitales aseguran la confidencialidad, la integridad, la autenticación y el no repudio.
- Describir el uso y el propósito de los hashes y las firmas digitales, proporcionando autenticación e integridad.
- Explicar cómo se asegura la autenticación.
- Explicar cómo se asegura la integridad.
- Explicar cómo se asegura la confidencialidad de los datos utilizando algoritmos de cifrado y claves pre-compartidas.
- Explicar cómo se asegura la confidencialidad de los datos utilizando algoritmos asimétricos con una infraestructura de clave pública para proveer y garantizar los certificados digitales.

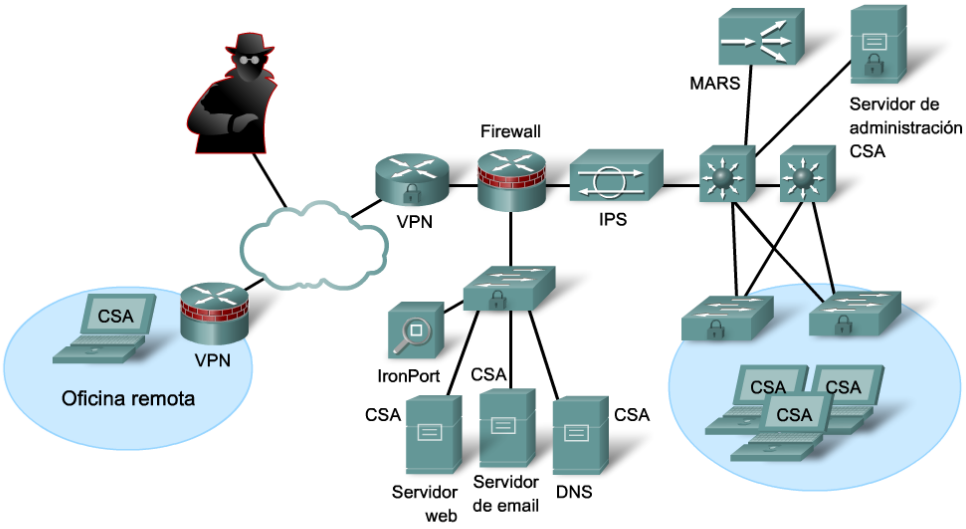
El primer objetivo de los administradores de red es asegurar la infraestructura de la red, incluyendo routers, switches, servidores y hosts. Esto se logra utilizando técnicas de fortificación (hardening), control de acceso AAA, ACLs y firewalls y monitoreando amenazas utilizando IPS.

7.1.1 Seguridad de las comunicaciones

El siguiente objetivo es asegurar los datos a medida que viajan a través de diferentes enlaces. Esto puede incluir el tráfico interno, pero la mayor preocupación es proteger los datos que viajan por fuera de la organización hacia sucursales, trabajadores remotos y socios de negocios.

Asegurar las comunicaciones involucra algunas tareas principales:

Autenticación - Garantiza que los mensajes no son falsos y realmente provienen del remitente indicado.
Integridad - Similar a la función de checksum, garantiza que nadie ha interceptado y alterado el mensaje.
Confidencialidad - Garantiza que, si el mensaje es capturado, no podrá ser descifrado.



- El tráfico entre los sitios debe ser seguro.
- Deben tomarse medidas para asegurar que el tráfico no pueda ser alterado, fraguado o descifrado, si fuera interceptado.

Autenticación

La autenticación garantiza que el mensaje proviene del origen del que dice provenir. La autenticación es similar a ingresar un número de información personal (PIN) seguro para realizar operaciones en un cajero automático. El PIN sólo debe ser conocido por el usuario y la institución financiera. El PIN es un secreto compartido que ayuda a prevenir fraudes.

La autenticación puede lograrse a través de métodos criptográficos. Esto es especialmente importante para aplicaciones y protocolos tales como IP o el correo electrónico, los cuales no poseen mecanismos incorporados para prevenir el fraude del remitente.

El no repudio de datos (Data Nonrepudiation) es un servicio similar, que permite al autor de un mensaje ser identificado de forma unívoca. Al utilizar servicios de no repudio, el autor no puede negar ser el origen del mensaje. Puede parecer que los servicios de autenticación y de no repudio cumplen la misma función. Sin embargo, aunque ambos se refieren a la cuestión de probar la identidad del remitente, existe una diferencia entre los dos.

La parte más importante del no repudio es que el dispositivo no puede repudiar o refutar la validez del mensaje enviado. El no repudio se basa en el hecho de que sólo el remitente posee las características o firma únicas contenidas en el mensaje. El dispositivo receptor del mensaje no puede saber cómo se insertaron estas características en el mensaje para probar su autenticidad, ya que si lo supiera, podría hacerse pasar por el origen.

Por otro lado, si la preocupación principal es que el dispositivo receptor pueda validar el origen y no existe riesgo de que el dispositivo receptor imite al origen, entonces no es importante si tanto el origen como el destino saben cómo tratar el mensaje para probar la autenticidad. Un ejemplo de autenticidad versus no repudio es el intercambio de datos entre dos computadoras de la misma compañía versus el intercambio de datos entre un cliente y un sitio web de comercio electrónico. Las dos computadoras dentro de la misma organización pueden intercambiar datos sin la necesidad de probar cuál de ellas envió el mensaje. Lo único que debe probarse es que lo que una reciba haya sido enviado por la otra. En este caso, las dos computadoras pueden compartir el mismo modo de transformar sus mensajes.

Esta práctica no es aceptable en las aplicaciones de negocios, tales como los comercios virtuales donde pueden comprarse productos online. Si el comercio virtual supiera cómo sus clientes transforman sus mensajes para probar su autenticidad, podría fácilmente crear órdenes de compra "falsas". En este escenario, el remitente debe ser el único que conoce cómo transformar sus mensajes. Así, el comercio online puede probar ante otros que la orden de compra fue realmente enviada por un cliente y el cliente no puede argumentar que la orden no es válida.



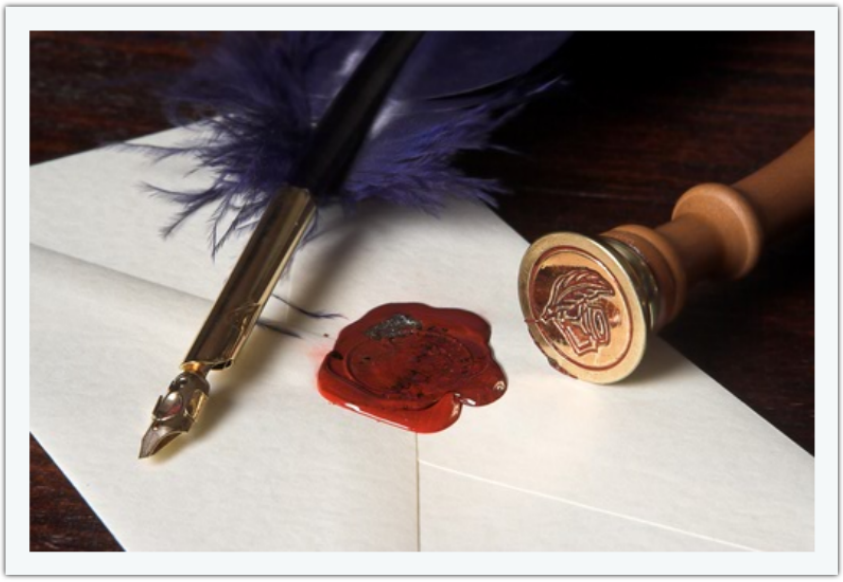
- Se requiere el Número de Identificación Personal (PIN) de un cajero automático para la autenticación.
- El PIN es un secreto compartido entre el titular de la cuenta bancaria y la institución financiera.

Integridad

La integridad de los datos asegura que los mensajes no son alterados durante su transmisión. Gracias a la integridad de los datos, el receptor puede verificar que el mensaje recibido es idéntico al mensaje enviado y que no hubo ninguna manipulación intermedia.

Los nobles europeos aseguraban la integridad de datos de sus documentos lacrando los sobres. En general, el sello era creado sobre un anillo y solían incluir el escudo familiar, iniciales, un retrato o un símbolo o lema personal del propietario del anillo. Un sello intacto en un sobre garantizaba la integridad de su contenido. Además, garantizaba la

autenticidad basándose en la impresión única del ello.



- Un sello de cera intacto en el sobre asegura su integridad.
- El sello único e intacto asegura que nadie ha leído su contenido.

Confidencialidad

La confidencialidad de los datos asegura la privacidad, de forma tal que sólo el destinatario pueda leer el mensaje. El cifrado es el proceso de codificar los datos para que no puedan ser leídos por partes no autorizadas.

Cuando hablamos de cifrado, los datos legibles son denominados texto plano o texto claro, mientras que la versión cifrada se denomina criptograma (en inglés, ciphertext). El mensaje legible en texto plano es convertido en un criptograma, el cual es ilegible. El descifrado revierte el proceso. Se requiere una clave para cifrar y descifrar un mensaje. La clave es el enlace entre el texto plano y el criptograma.

Históricamente, se han utilizado diferentes métodos y algoritmos de cifrado. Se dice que Julio César aseguraba sus mensajes tomando dos alfabetos, uno al lado del otro y luego desplazando uno de ellos un número específico de lugares. El número de lugares desplazados era la clave. Él convirtió texto plano en criptogramas utilizando esta clave y sólo sus generales, quienes también tenían la clave, sabían cómo descifrar los mensajes. Este método es conocido como Cifrado César.

Utilizar una función de hash es otra forma de asegurar la confidencialidad de los datos. Una función de hash transforma un conjunto de caracteres en una representación de la misma que suele ser más corta y de longitud fija. La diferencia entre el cifrado y el hashing es cómo se almacenan los datos. Con el texto cifrado, los datos pueden ser descifrados utilizando una clave. Con la función de hash, una vez que los datos son ingresados y convertidos utilizando dicha función, el texto plano se pierde. Los datos de hash sólo resultan útiles en comparaciones. Por ejemplo, cuando un usuario ingresa una contraseña, dicha contraseña es convertida en un hash y luego comparada con el valor de hash almacenado. Si el usuario olvida su contraseña, es imposible descifrar el valor almacenado y la contraseña debe restablecerse.

El propósito del cifrado y el hashing es garantizar la confidencialidad, de forma tal que sólo las entidades autorizadas puedan leer el mensaje.



- Julio César enviaba mensajes cifrados a sus generales en el campo de batalla.
- Incluso si los mensajes eran interceptados, sus enemigos no podían leerlos y, menos aún, descifrarlos.

7.1.2 Criptografía

Autenticación, integridad y confidencialidad son componentes de la criptografía. La criptografía es tanto la práctica como el estudio del ocultamiento de la información.

Los servicios criptográficos son la base de muchas implementaciones de seguridad y son utilizados para asegurar la protección de los datos cuando los mismos pueden quedar expuestos a partes no confiables. Comprender las funciones básicas de la criptografía y cómo el cifrado proporciona confidencialidad e integridad son partes importantes de la creación de una política de seguridad exitosa. También es importante comprender los problemas involucrados con la administración de la clave de cifrado.

La historia de la criptografía comienza en círculos diplomáticos hace miles de años. Los mensajeros de las cortes reales llevaban los mensajes cifrados a otras cortes. Ocasionalmente, otras cortes no involucradas en la comunicación intentaban robar los mensajes destinados a aquellos reinos que consideraban adversarios. Poco tiempo después, los comandantes militares comenzaron a utilizar el cifrado para asegurar sus mensajes.

Se han utilizado varios métodos, dispositivos físicos y mecanismos de cifrado con el fin de cifrar y descifrar textos:

Uno de los métodos más antiguos puede haber sido la Escítala de la Antigua Grecia, una barra aparentemente utilizada por los espartanos como mecanismo para el cifrado por

transposición. El destinatario recibía una barra (escítala) idéntica sobre la que se enrollaba el mensaje transpuesto.
El Cifrado César es un cifrado simple por sustitución, utilizado por Julio César en el campo de batalla para cifrar un mensaje de forma rápida y que este pueda ser descifrado por sus comandantes. El método de cifrado puede comparar dos manuscritos con texto, desplazando uno de los manuscritos un número clave determinado de lugares o moviendo en dial interno de una rueda de cifrado un número clave de espacios.
El Cifrado Vigenere fue inventado por el francés Blaise de Vigenere en el siglo XVI, utilizando un sistema polialfabético de cifrado. Basado en el Cifrado César, permite cifrar texto plano utilizando una clave de múltiples letras.
Thomas Jefferson, el tercer presidente de los Estados Unidos, inventó un sistema de cifrado que se cree que utilizó cuando fue secretario de estado, entre 1790 y 1793.
Arthur Scherbius inventó en 1918 un dispositivo de codificación electromecánico llamado Enigma que vendió a Alemania. Este dispositivo sirvió como modelo para las máquinas que utilizaron todos los grandes participantes de la Segunda Guerra Mundial. Se estima que si 1000 criptoanalistas probaran cuatro claves por minuto, todo el día todos los días, tomaría 1.800.000.000 años probarlas a todas. Alemania sabía que sus mensajes cifrados podían ser interceptados por los aliados, pero nunca pensó que podrían descifrarlos.
También durante la Segunda Guerra Mundial, Japón descifró todos los códigos que inventaron los americanos. Era necesario un sistema de codificación más elaborado y la respuesta surgió en la forma de traductores de código navajo. No sólo no existían palabras en el idioma navajo para los términos militares, sino que el lenguaje no posee escritura. Además, menos de 30 personas fuera de las reservas navajo podían hablarlo y ninguno de ellos era japonés. Hacia el final de la guerra, más de 400 indios navajo trabajaban como traductores de código.

Cada uno de estos métodos de cifrado utiliza un algoritmo específico, llamado cifrador, para cifrar y descifrar mensajes. Un cifrador consiste en una serie de pasos bien definidos, los cuales pueden ejecutarse como un procedimiento para cifrar y descifrar mensajes.

Existen diferentes métodos para crear texto cifrado:

Transposición
Substitución
Vernam



Escítala - (700 A.C.)

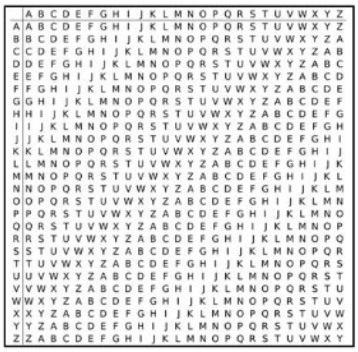


Tabla Vigenere



Dispositivo de cifrado Jefferson



Máquina alemana Enigma

En los cifrados por transposición, las letras no se reemplazan, sino que son reordenadas. Un ejemplo de este tipo de cifrado es tomar el mensaje FLANK EAST ATTACK AT DAWN y luego transponerlo como NWAD TAKCATTA TSAE KNALF. En este ejemplo, la clave es revertir las letras.

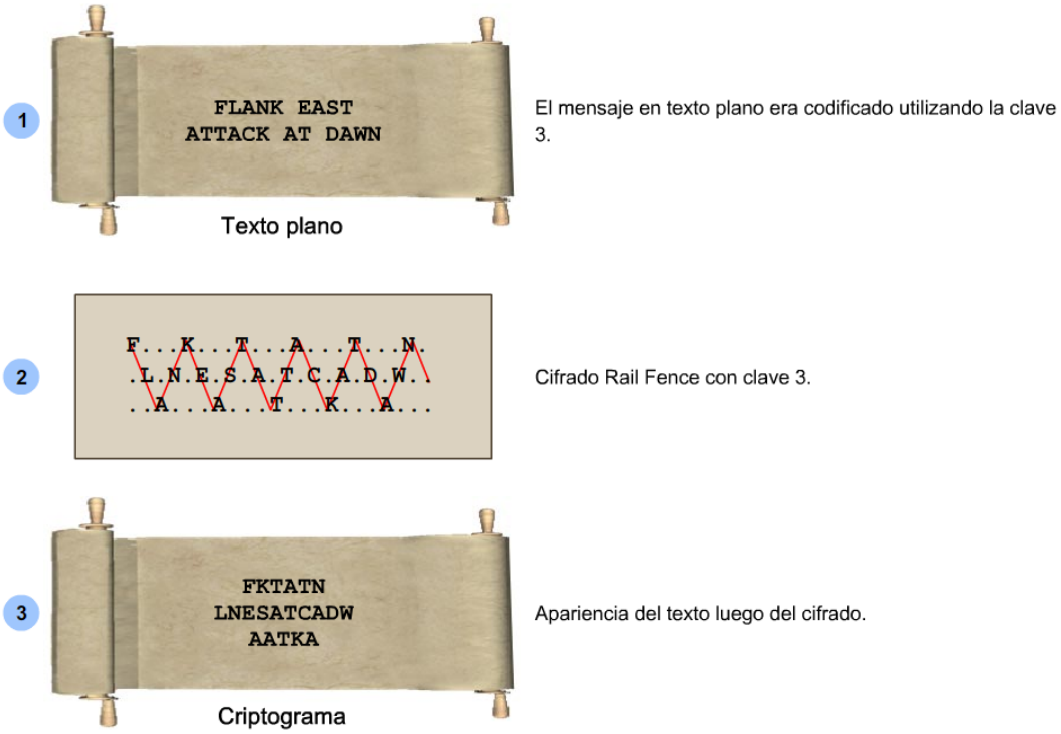
Otro ejemplo de un cifrado por transposición es conocido como Cifrado Rail Fence. En esta transposición, las palabras son deletreadas como si se tratara de los rieles de una valla, es decir, algunos por delante y otros por detrás de varias líneas paralelas. Por ejemplo, un cifrado Rail Fence que utiliza "tres" como clave, especifica que se requieren tres líneas para crear el código cifrado. Para leer el mensaje, debe hacerse en forma diagonal, de arriba abajo, siguiendo las líneas de la valla.

F...K...T...A...T...N.

.L.N.E.S.A.T.C.A.D.W..

..A...A...T...K...A...

Los algoritmos de cifrado modernos, tales como DES (Data Encryption Standard) y 3DES (Triple Data Encryption Standard) todavía utilizan transposición como parte del algoritmo.



Los cifradores por sustitución reemplazan una letra por otra. En su forma más simple, los cifrados por sustitución retienen la frecuencia de letras del mensaje original.

El Cifrado César era un cifrado por sustitución simple. Cada día se utilizaba una clave diferente para ajustar el alfabeto. Por ejemplo, si la clave del día era 3, la letra A era desplazada tres espacios a la derecha, resultando en un mensaje codificado que utilizaba la letra D en lugar de la letra A. La letra E sería el reemplazo de la letra B y así sucesivamente. Si la clave del día era 8, la A se convierte en I, la B se convierte en J y así sucesivamente.

Como el mensaje completo se basaba en el mismo desplazamiento clave, el Cifrado César es conocido como un cifrado de sustitución monoalfabético. Es también relativamente fácil de romper. Por este motivo, se inventaron los cifrados polialfabéticos, tales como el Cifrado Vigenere. El método fue descripto originalmente por Giovan Battista Bellaso en 1553, pero el esquema fue atribuido mas tarde en forma errónea al diplomático y criptógrafo francés Blaise de Vigenere.

El Cifrado Vigenere se basa en el Cifrado César, excepto en que cifra el texto utilizando diferentes desplazamientos polialfabéticos de clave para cada letra del texto plano. Los diferentes desplazamientos son identificados utilizando una clave compartida entre el autor y el receptor. El mensaje en texto plano puede ser cifrado y descifrado utilizando la Tabla de Cifrado Vigenere.

Para ilustrar cómo funciona la Tabla de Cifrado Vigenere, suponga que el autor y el receptor poseen una clave secreta compartida, compuesta por estas letras: SECRETKEY. El autor utiliza esta clave secreta para codificar el texto plano FLANK EAST ATTACK AT DAWN:

La F (FLANK) es codificada mirando la intersección entre la columna F y la fila que comienza con S (SECRETKEY), lo cual resulta en la letra cifrada X.
La L (FLANK) es codificada mirando la intersección entre la columna L y la fila que comienza con E (SECRETKEY), lo cual resulta en la letra cifrada P.
La A (FLANK) es codificada mirando la intersección entre la columna A y la fila que comienza con C (SECRETKEY), lo cual resulta en la letra cifrada C.
La N (FLANK) es codificada mirando la intersección entre la columna N y la fila que comienza con R (SECRETKEY), lo cual resulta en la letra cifrada E.
La K (FLANK) es codificada mirando la intersección entre la columna K y la fila que comienza con E (SECRETKEY), lo cual resulta en la letra cifrada O.

El proceso continúa hasta que el texto completo del mensaje FLANK EAST ATTACK AT DAWN se encuentra cifrado. El proceso también puede revertirse. Por ejemplo, la letra F es la letra cifrada X si fue codificada mirando la intersección de la fila F (FLANK) y la columna que comienza con S (SECRETKEY).

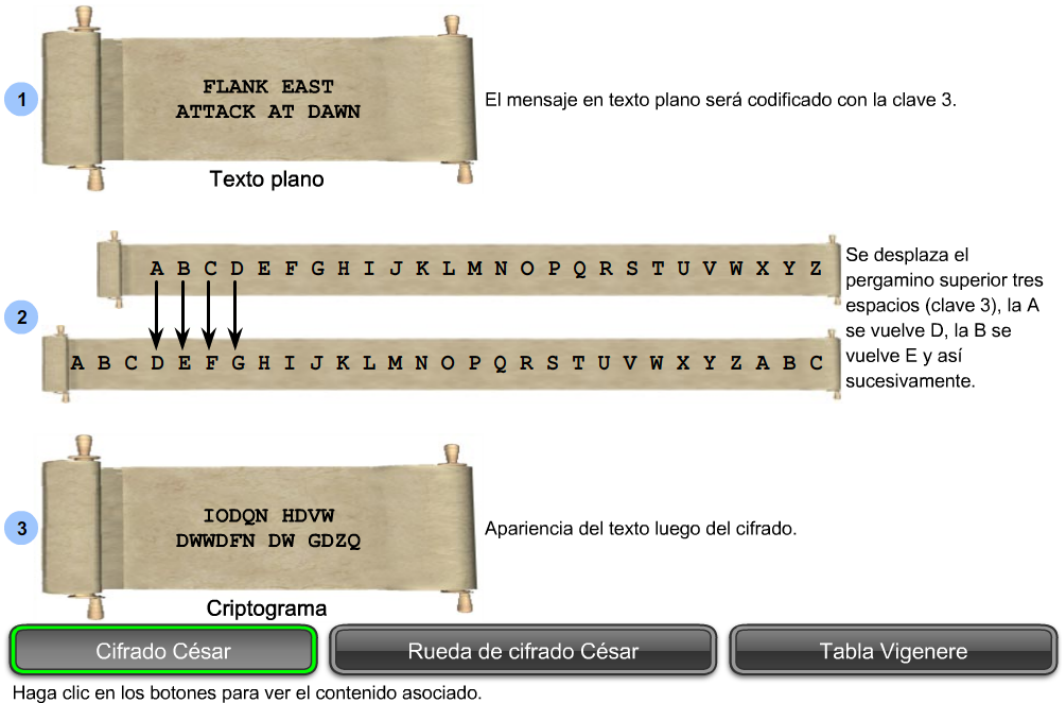
Cuando se utiliza el Cifrado Vigenere y el mensaje es más largo que la clave, entonces se repite la clave. Por ejemplo, para codificar FLANK EAST ATTACK AT DAWN es necesario utilizar la clave SECRETKEYSECRETKEYSEC:

Clave secreta: SECRE TKEY SECRET KE YSEC

Texto plano: FLANK EAST ATTACK AT DAWN

Texto cifrado: XPCEO XKUR SXVRGD KX BSAP

Aunque el Cifrado Vigenere utiliza una clave más larga, aún puede ser descubierto. Por este motivo, fue necesario desarrollar un mejor método de cifrado.



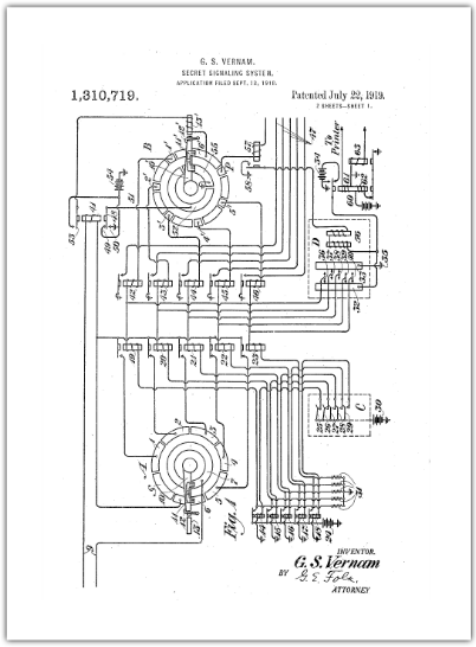


	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
B	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a
C	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b
D	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c
E	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d
F	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e
G	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f
H	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g
I	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h
J	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i
K	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j
L	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k
M	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l
N	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m
O	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n
O	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
Q	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p
R	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q
S	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r
T	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s
U	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t

Gilbert Vernam fue un ingeniero de AT&T Bell Labs que, en 1971, inventó y patentó el cifrador de flujo y luego co-inventó la "libreta de un solo uso". Vernam propuso un cifrador de teletipo, el cual registraba en una cinta de papel una clave preparada que consistía en una secuencia de números no repetidos y de longitud arbitraria. Esta clave era luego combinada carácter por carácter con el mensaje en texto plano para producir el criptograma. Para descifrar el criptograma, se combinaba carácter por carácter la misma cinta de papel, produciendo el texto plano original. Cada cinta se utilizaba una sola vez, de allí el término "libreta de un solo uso". Mientras la cinta clave no se repitiera ni fuera

reutilizada, este tipo de cifrado era inmune a los ataques de criptoanálisis, ya que los criptogramas disponibles no revelan el patrón de la clave.

La utilización de libretas de un solo uso en el mundo real presenta algunas dificultades inherentes. Una de ellas es el desafío de crear datos aleatorios. Debido a que poseen una base matemática, las computadoras son incapaces de crear datos realmente aleatorios. Además, si la clave es utilizada más de una vez, se vuelve fácil de descubrir. RC4 es un ejemplo de este tipo de cifrado ampliamente utilizado en Internet. De nuevo, debido a que las claves son generadas por una computadora, no son verdaderamente aleatorias. Además de estos problemas, la distribución de la clave también es un desafío para este tipo de cifrado.



Cifrado de teletipo

- Inventado por el Cuerpo de Señales de la Armada Noruega en 1950, la máquina ETCRRM utiliza el método de cifrado de flujo Vernam.
- Fue utilizado por los Estados Unidos y el gobierno de Rusia para intercambiar información.
- El mensaje en texto plano se procesa con la operación lógica XOR junto con una cinta clave, la cual contiene una cadena aleatoria de datos con la misma longitud que el texto cifrado.
- Una vez cifrado el mensaje, se destruye la clave.
- El extremo receptor procesa los datos a la inversa, utilizando una cinta clave idéntica para procesar el mensaje.

7.1.3 Criptoanálisis

Desde que existe la criptografía, existe también el criptoanálisis. El criptoanálisis es la práctica y el estudio para determinar el significado de la información cifrada (romper el código) sin tener acceso a la clave secreta compartida.

A través de la historia, han existido muchas instancias de criptoanálisis:

- El cifrado Vigenere fue absolutamente seguro hasta que fue quebrado a mediados del siglo XIX por el criptógrafo inglés Charles Babbage.
- María Estuardo participó de un complot para destronar a la Reina Isabel I, enviando mensajes cifrados a sus co-conspiradores. Al quebrarse el código utilizado en este complot, María fue decapitada en 1587.
- Las comunicaciones cifradas con Enigma fueron utilizadas por los alemanes para navegar y dirigir sus submarinos a través del Atlántico. Los criptoanalistas británicos y polacos quebraron el código alemán Enigma. Winston Churchill consideró éste un punto de quiebre en la Segunda Guerra Mundial.

En el criptoanálisis se utilizan diversos métodos.

Ataque por fuerza bruta

En un ataque por fuerza bruta, el atacante prueba todas las claves posibles con el algoritmo de descifrado, sabiendo que eventualmente una de ellas funcionará. Todos los algoritmos de cifrado son vulnerables a este ataque. En promedio, un ataque por fuerza bruta tiene éxito al recorrer un 50 por ciento de las combinaciones posibles. El objetivo de los criptógrafos modernos es tener un número de combinaciones lo suficientemente grande como para que un ataque por fuerza bruta resulte demasiado costoso y tome demasiado tiempo.

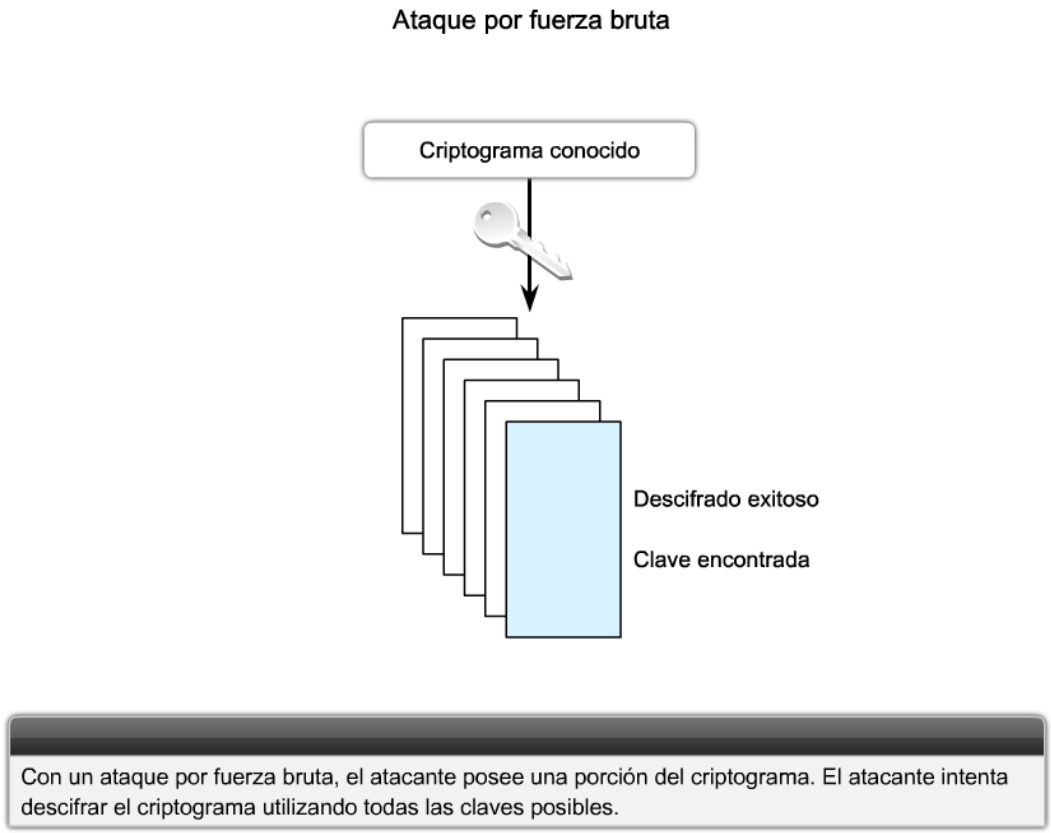
Recientemente, se ha utilizado una máquina de descifrado DES (DES cracking machine) para recuperar una clave DES de 56 bits en 22 horas utilizando fuerza bruta. Se estima que, con el mismo equipamiento, llevaría unos 149 billones de años romper una clave AES, utilizando el mismo método.

Ataque de criptograma

En un ataque de criptograma, el atacante conoce los criptogramas de varios mensajes, todos los cuales han sido cifrados utilizando el mismo algoritmo, pero no conoce el texto plano original. El trabajo del atacante consiste en recuperar tantos criptogramas como sea posible. Es incluso mejor para el atacante deducir la clave o las claves utilizadas para cifrar el mensaje, con el fin de descifrar otros mensajes cifrados con las mismas claves. El atacante puede realizar un análisis estadístico para deducir la clave. Este tipo de ataques ya no son prácticos, porque los algoritmos modernos generan salidas pseudoaleatorias resistentes a los análisis estadísticos.

Ataque con texto plano conocido

En un ataque con texto plano conocido, el atacante tiene acceso al criptograma de varios mensajes, pero también tiene cierto conocimiento sobre el texto plano contenido en dichos criptogramas. Conociendo el protocolo subyacente, el tipo de archivo o alguna cadena de caracteres característica, que aparecen en el texto plano, el atacante utiliza un ataque por fuerza bruta para probar diferentes claves hasta que el descifrado con la clave correcta genera un resultado que aparenta tener sentido. Este ataque puede ser el más práctico, ya que los atacantes generalmente pueden asumir algunas partes del texto plano subyacente si pueden capturar el criptograma. Los algoritmos modernos hacen improbable el éxito de este ataque, ya que, en promedio, los atacantes deben buscar en aproximadamente la mitad de las posibilidades para lograr su objetivo.



Con un ataque por fuerza bruta, el atacante posee una porción del criptograma. El atacante intenta descifrar el criptograma utilizando todas las claves posibles.

Ataque con texto plano seleccionado

En un ataque con texto plano seleccionado, el atacante elige qué datos cifrar con el dispositivo de cifrado y observa el criptograma resultante. Un ataque con texto plano seleccionado es más potente que un ataque con texto plano conocido porque el texto plano seleccionado puede proporcionar más información sobre la clave. Este ataque no es muy práctico porque, a menos que la red de confianza haya sido infiltrada y el atacante tenga acceso a información confidencial, en general resulta difícil o incluso imposible capturar tanto el criptograma como el texto plano a la vez.

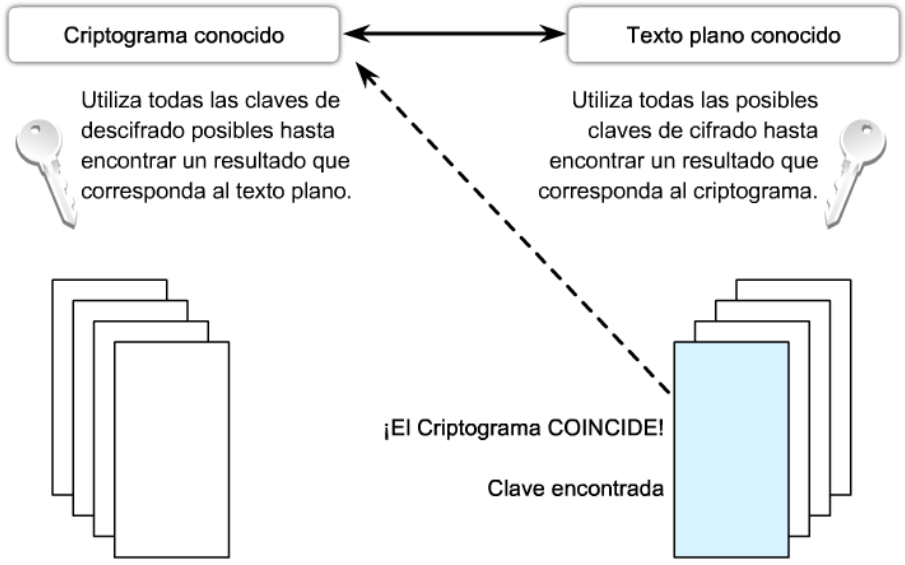
Ataque con criptograma seleccionado

En un ataque con criptograma seleccionado, el atacante puede seleccionar diferentes criptogramas para descifrar y tiene acceso al texto plano descifrado. Con estos dos componentes, el atacante puede buscar entre las combinaciones de claves posibles y determinar cuál de ellas descifra el criptograma seleccionado para convertirlo en el texto plano capturado. Por ejemplo, el atacante tiene acceso a un dispositivo de cifrado a prueba de manipulaciones (tamperproof) con una clave integrada. El atacante debe deducir la clave integrada procesando datos a través del dispositivo. Este ataque es análogo al ataque con texto plano seleccionado y, al igual que este, resulta poco práctico. A menos que la red de confianza haya sido infiltrada y el atacante ya posea acceso a la información confidencial, resulta difícil o incluso imposible para el atacante capturar al mismo tiempo el criptograma y el texto plano correspondiente.

Ataque por encuentro a medio camino (Meet-in-the-Middle)

El ataque por encuentro a medio camino es un conocido ataque de texto plano. El atacante conoce una porción del texto plano y su correspondiente criptograma. El texto plano es cifrado con todas las claves posibles y se almacenan los resultados. El criptograma es luego descifrado utilizando todas las claves posibles, hasta que uno de los resultados coincide con uno de los valores almacenados.

Ataque Meet-in-the-Middle

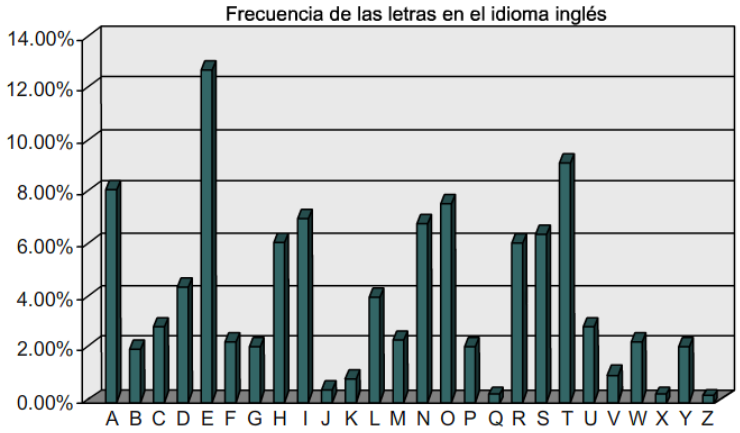


Con el ataque Meet-in-the-Middle, el atacante posee una misma porción de texto tanto en texto plano como en criptograma. El atacante intenta descifrar el criptograma con todas las claves posibles, a la vez que intenta cifrar el texto plano con otro conjunto de claves posibles, hasta encontrar una coincidencia.

Como un ejemplo sobre cómo seleccionar el método de criptoanálisis, considere el caso de un código cifrado mediante el Cifrado César. La mejor forma de romper el código es utilizando fuerza bruta. Debido a que existen sólo 25 rotaciones posibles, probar todas las posibilidades y observar cuál de ellas devuelve un resultado con sentido no conlleva un esfuerzo muy grande.

Un acercamiento más científico consiste en utilizar el hecho que algunos caracteres del alfabeto son utilizados con más frecuencia que otros. Este método es llamado "análisis de frecuencia". Por ejemplo, en el idioma inglés, las letras E, T y A son las más utilizadas, mientras que las letras J, Q, X y Z son las menos utilizadas. Comprender este patrón puede ayudar a descubrir qué letras están probablemente incluidas en el mensaje cifrado.

Por ejemplo, en el mensaje con Cifrado César IODQN HDVW DWWDFN DW GDZQ, la letra cifrada D aparece seis veces, mientras que la letra cifrada W aparece cuatro veces. Existe una gran posibilidad de que las letras cifradas D y W representen las letras en texto plano E, T o A. En este caso, la letra D representa la letra A y la letra W representa la letra T.



El gráfico muestra la frecuencia de las letras en el idioma inglés.

Por ejemplo, las letras E, T y A son las más utilizadas.



Texto Cifrado

En este mensaje cifrado, existen 6 ocurrencias de las letras cifradas D y 4 ocurrencias de la letra cifrada W.

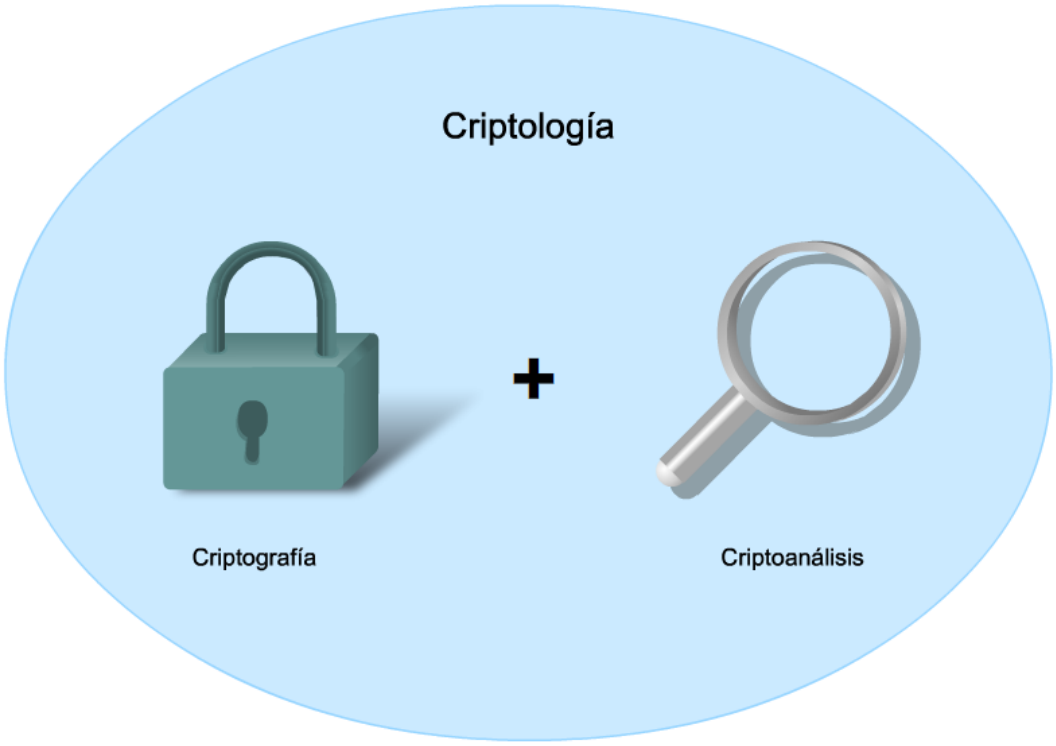
Un atacante sólo debería reemplazar la letra cifrada D con la letra en texto plano más popular, incluyendo E, T y finalmente A.

Al probar la letra A se revela un patrón de desplazamiento de 3 y el atacante podrá descifrar el mensaje entero.

La criptología es la ciencia de crear y romper códigos secretos. Combina dos disciplinas separadas: la criptografía, que es el desarrollo y utilización de códigos y el criptoanálisis, que es la ruptura de dichos códigos. Existe una relación simbiótica entre ambas disciplinas, porque cada una hace mejor a la otra. Las organizaciones de seguridad emplean miembros de ambas disciplinas y los ponen a trabajar unos contra otros.

En algunos momentos de la historia, una de las disciplinas ha estado más avanzada que la otra. Por ejemplo, durante la Guerra de los Cien Años entre Francia e Inglaterra, los criptoanalistas se encontraban más adelantados que los criptógrafos. Francia creía que el cifrado Vigenere era irrompible. Sin embargo, los británicos fueron capaces de romperlo. Algunos historiadores creen que el resultado de la Segunda Guerra Mundial dependió mucho de que el bando ganador fue mucho más exitoso en romper los códigos de su adversario que el bando perdedor. En la actualidad, se cree que los criptógrafos llevan la delantera.

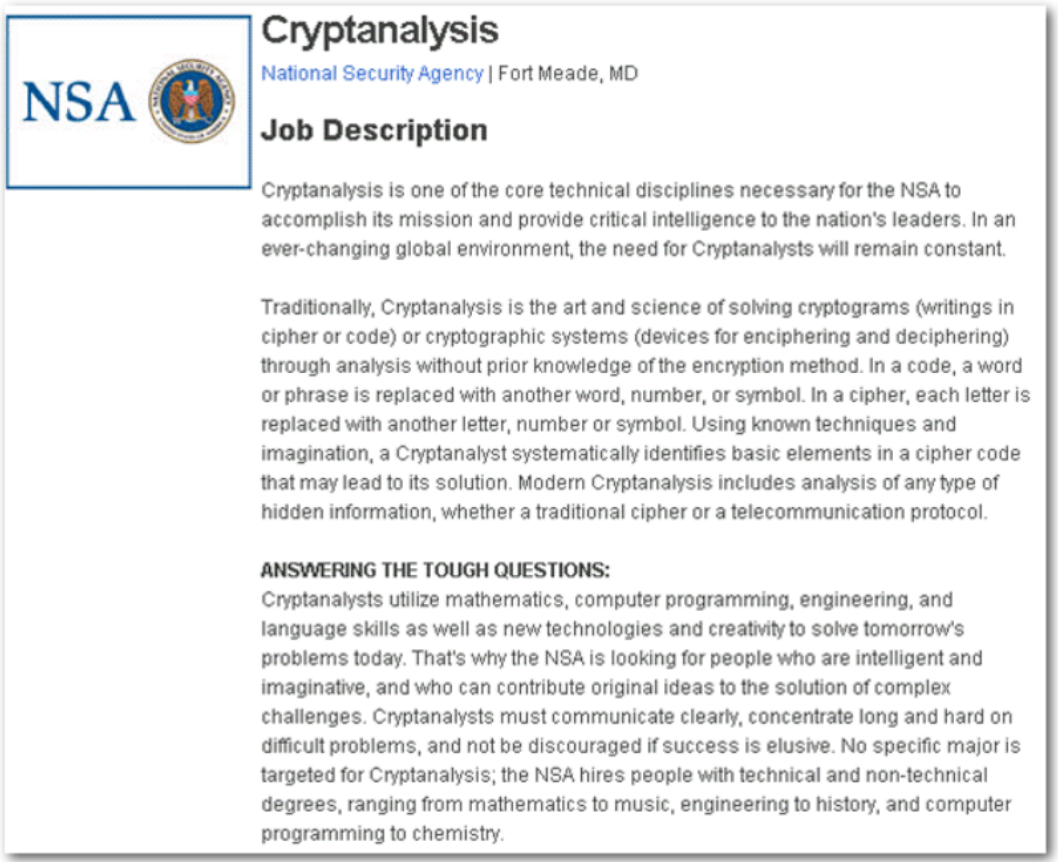
7.1.4 Cristología



El criptoanálisis es muy utilizado por los gobiernos en la vigilancia militar y diplomática, por empresas al probar la fortaleza de sus procedimientos de seguridad y por hackers maliciosos para explotar vulnerabilidades de sitios web.

Aunque el criptoanálisis suele ser relacionado con fines maliciosos, en realidad es una necesidad. Es un hecho irónico de la criptografía que resulte imposible probar que un algoritmo sea seguro. Sólo puede probarse que no es vulnerable a ataques criptoanalíticos conocidos. Por lo tanto, es necesario que matemáticos, eruditos y expertos en seguridad forense sigan intentando romper los métodos de cifrado.

Ejemplo de descripción laboral de criptoanálisis



Cryptanalysis

National Security Agency | Fort Meade, MD

Job Description

Cryptanalysis is one of the core technical disciplines necessary for the NSA to accomplish its mission and provide critical intelligence to the nation's leaders. In an ever-changing global environment, the need for Cryptanalysts will remain constant.

Traditionally, Cryptanalysis is the art and science of solving cryptograms (writings in cipher or code) or cryptographic systems (devices for enciphering and deciphering) through analysis without prior knowledge of the encryption method. In a code, a word or phrase is replaced with another word, number, or symbol. In a cipher, each letter is replaced with another letter, number or symbol. Using known techniques and imagination, a Cryptanalyst systematically identifies basic elements in a cipher code that may lead to its solution. Modern Cryptanalysis includes analysis of any type of hidden information, whether a traditional cipher or a telecommunication protocol.

ANSWERING THE TOUGH QUESTIONS:

Cryptanalysts utilize mathematics, computer programming, engineering, and language skills as well as new technologies and creativity to solve tomorrow's problems today. That's why the NSA is looking for people who are intelligent and imaginative, and who can contribute original ideas to the solution of complex challenges. Cryptanalysts must communicate clearly, concentrate long and hard on difficult problems, and not be discouraged if success is elusive. No specific major is targeted for Cryptanalysis; the NSA hires people with technical and non-technical degrees, ranging from mathematics to music, engineering to history, and computer programming to chemistry.

En el mundo de las redes y las comunicaciones, la autenticación, la integridad y la confidencialidad de los datos se implementan de diversas formas, utilizando diferentes protocolos y algoritmos. La selección del protocolo y algoritmo varía de acuerdo al nivel de seguridad requerido para alcanzar las metas establecidas en la política de seguridad de la red.

Por ejemplo, para la integridad de los mensajes, MD5 (Message-Digest 5) es más rápido pero menos seguro que SHA2. La confidencialidad puede ser implementada utilizando DES, 3DES o el muy seguro AES. Nuevamente, la selección depende de los requisitos de seguridad especificados en el documento de la política de seguridad de la red.

Los algoritmos de cifrado antiguos, como el Cifrado César o la máquina Enigma, se basaban en el secreto de los algoritmos para obtener confidencialidad. Con la tecnología moderna, donde la ingeniería inversa suele ser simple, en general se utilizan algoritmos de dominio público. Con la mayoría de los algoritmos modernos, un descifrado exitoso requiere el conocimiento de las claves criptográficas apropiadas. Esto quiere decir que la seguridad del cifrado reside en la discreción de las claves y no del algoritmo. ¿Cómo pueden mantenerse secretas las claves?

	Integridad	Autenticación	Confidencialidad
Valores de hash, protocolos y algoritmos criptográficos	MD5 SHA	HMAC-MD5 HMAC-SHA-1 RSA y DSA	DES 3DES AES

7.2.1 Hash Criptográficos

Una función de hash toma datos binarios, llamados mensaje y produce una representación abreviada del mismo, llamada digesto de mensaje. El hashing se basa en una función matemática de un solo sentido relativamente fácil de computar, pero significativamente más difícil de invertir. Moler café es un buen ejemplo de una función de un solo sentido. Es fácil moler granos de café, pero es casi imposible volver a juntar las pequeñas partículas para reconstruir los granos originales.

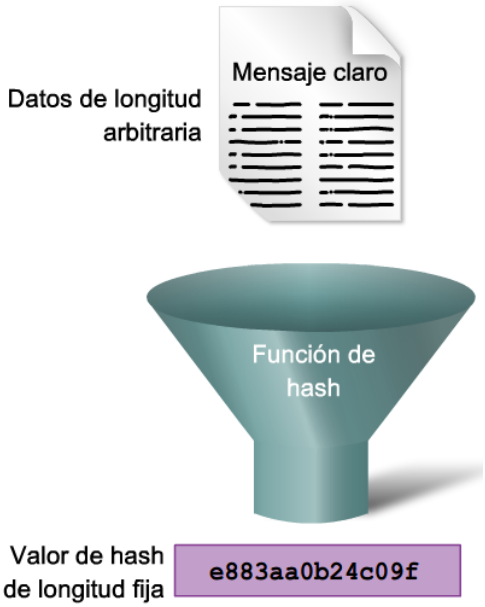
La función de hashing criptográfico está diseñada para verificar y asegurar la integridad de los datos. Puede ser también utilizada para verificar la autenticación. El procedimiento toma un bloque variable de datos y devuelve una cadena de longitud fija, llamada valor de hash o digesto del mensaje.

El proceso de hashing es similar a la suma de verificación (checksum) de la comprobación de redundancia cíclica (CRC). Por ejemplo, dado un valor de CRC, resulta sencillo generar datos con el mismo CRC. Con las funciones de hash, no es viable computacionalmente que a partir de dos conjuntos de datos diferentes se obtenga el mismo resultado de hash. Cada vez que se modifican los datos, el valor de hash también cambia. Debido a esto, los valores de hash criptográficos son también conocidos como huellas digitales. Pueden ser utilizados para detectar la duplicación de archivos de datos y cambios de versión y otros usos similares. Estos valores son utilizados para proteger los datos contra cambios accidentales o intencionales o su corrupción intencional.

La función de hash criptográfico se aplica en muchas situaciones diferentes:

Para proporcionar una prueba de autenticidad, cuando es utilizada con una clave secreta de autenticación simétrica, como IPsec o autenticación de protocolos de enrutamiento.
Para proporcionar autenticación generando respuestas de único uso de una vía a los desafíos de protocolos de autenticación como CHAP (PPP Challenge Authentication Protocol).
Para proporcionar pruebas de verificación de la integridad del mensaje, como en los contratos firmados digitalmente y certificados de infraestructura de clave pública (PKI), como los que deben aceptarse al acceder a un sitio seguro utilizando un navegador web.

- Se utilizan hashes para asegurar la integridad.
- Los hashes se basan en funciones de una vía.
- La función de hash convierte datos arbitrarios en un digesto de longitud fija, conocido como valor de hash, digesto del mensaje, digesto o huella digital.

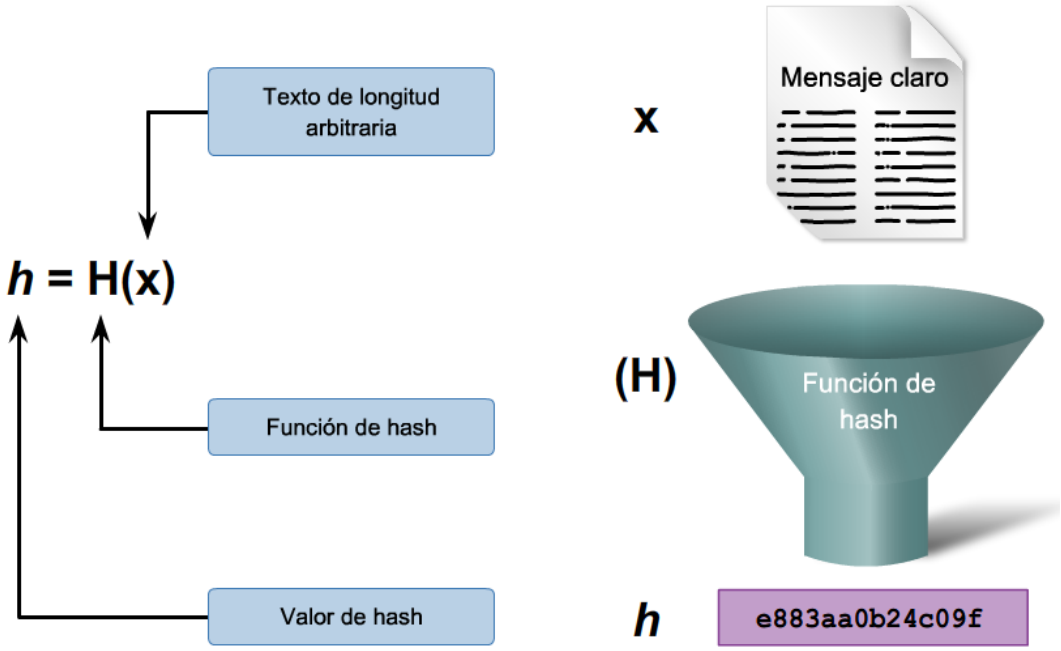


Matemáticamente, una función de hash (H) es un proceso que toma una entrada (x) y devuelve una cadena de longitud fija, llamada valor de hash (h). La fórmula para el cálculo es h = H(x).

Una función de hash criptográfico debe tener las siguientes propiedades:

La entrada puede tener cualquier longitud.
La salida debe ser de longitud fija.
H(x) es relativamente fácil de calcular, cualquiera sea el valor de x.
H(x) es una función de un solo sentido y no es invertible.
H(x) es una función libre de colisiones, por lo que dos valores diferentes de entrada resultarán siempre en dos valores de hash diferentes.

Si una función de hash es difícil de invertir, entonces se la considera una función de un solo sentido. Para que sea difícil de invertir, dado un valor cualquiera de h, debe ser computacionalmente inviable encontrar una entrada (x) tal que H(x) = h.

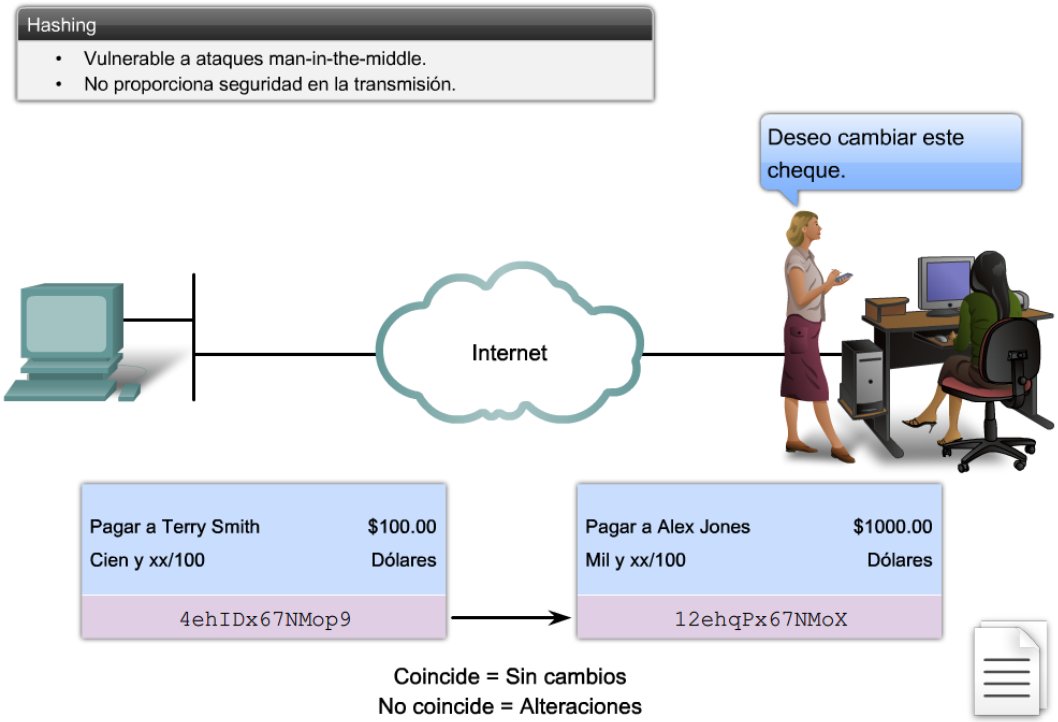


Las funciones de hash resultan útiles al momento de asegurar que los datos no han sido cambiados de forma accidental, pero no permite asegurar que no han sido cambiados deliberadamente. Por ejemplo, el remitente quiere asegurar que el mensaje no sea alterado en el camino al receptor. El dispositivo origen procesa el mensaje con un algoritmo de hash y calcula su huella digital de longitud fija. Esta huella digital se agrega luego al mensaje y se envía todo el conjunto al receptor. El dispositivo destino elimina la huella digital del mensaje y lo procesa con el mismo algoritmo de hashing. Si el hash calculado por el destinatario es igual al recibido junto con el mensaje, entonces el mensaje no ha sufrido alteraciones durante su transmisión.

Cuando el mensaje atraviesa una red, un atacante potencial puede interceptarlo, modificarlo, recalcular el hash y agregarlo en el mensaje modificado. El proceso de hashing evita sólo las modificaciones accidentales del mensaje, como puede ser un error en la comunicación. No hay ninguna característica que sea única del remitente en el proceso de hashing, por lo que cualquiera puede calcular el hash de cualquier dato, siempre y cuando cuente con la función de hash correcta.

Existen dos funciones de hash bien conocidas:

Message Digest 5 (MD5) con digestos de 128 bits
Secure Hash Algorithm 1 (SHA-1) con digestos de 160 bits



7.2.2 Integridad con MD5 y SHA-1

El algoritmo MD5 es un algoritmo de hashing desarrollado por Ron Rivest y utilizado actualmente por una amplia variedad de aplicaciones en Internet.

MD5 es una función de un solo sentido que facilita el cálculo de hash para los datos ingresados, pero vuelve inviable el cálculo de los datos originales dado un único valor de hash. MD5 es también libre de colisiones: es poco probable obtener el mismo valor de hash a partir de dos conjuntos diferentes de datos. MD5 es esencialmente una secuencia compleja de operaciones binarias simples, tales como OR Exclusivo (XOR) y rotaciones, que se ejecutan sobre los datos y producen un digesto del mensaje de 128 bits.

El algoritmo principal se basa en una función de compresión, la cual opera sobre bloques. La entrada es un bloque de datos más un resultado de bloques previos. Los bloques de 512 bits se dividen en 16 sub-bloques de 32 bits. Estos bloques son luego reordenados con operaciones simples en un bucle principal, el cual consiste en cuatro iteraciones. La salida del algoritmo es un conjunto de cuatro bloques de 32 bits que se concatenan para formar un único valor de hash de 128 bits. La longitud del mensaje se codifica así en un digesto.

MD5 se basa en MD4, un algoritmo anterior. MD4 ha sido decodificado y MD5 es ahora considerado menos seguro que SHA-1, según muchas autoridades de la criptografía.

Algoritmo MD5

- Es utilizado en una variedad de aplicaciones en Internet.
- Utiliza una función de hash de una vía - fácil de computar y es imposible calcular los datos a partir del hash.
- Produce un hash de 128 bits a partir de una secuencia compleja de operaciones binarias simples.



El Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos desarrolló SHA (Secure Hash Algorithm), el algoritmo especificado en SHS (Secure Hash Standard). SHA-1, publicado en 1994, corrige una falla no publicada de SHA. Su diseño es muy similar al de las funciones de hash MD4 y MD5 desarrolladas por Ron Rivest.

El algoritmo SHA-1 toma un mensaje con menos de 2^64 bits de longitud y produce un digesto de 160 bits. El algoritmo es apenas más lento que MD5, pero al generar un digesto más largo, es más seguro contra ataques de colisión por fuerza bruta y ataques de inversión.

El NIST publicó cuatro funciones de hash adicionales para la familia SHA, cada uno con digestos más largos:

SHA-224 (224 bits)
SHA-256 (256 bits)
SHA-384 (384 bits)
SHA-512 (512 bits)

Estas cuatro versiones son conocidas en forma conjunta como SHA-2, aunque el término SHA-2 no ha sido estandarizado. SHA-1, SHA-224, SHA-256, SHA-384 y SHA-512 son los algoritmos seguros de hash requeridos por ley para su utilización en ciertas aplicaciones del gobierno de los Estados Unidos, incluyendo su uso dentro de otros algoritmos y protocolos criptográficos, para la protección de información sensible no clasificada.

Características de SHA

- Toma un mensaje de entrada con una longitud menor a 2^64 bits y produce un digesto del mensaje de 160 bits.
- El algoritmo es levemente más lento que MD5.
- SHA-1 es una revisión que corrige una falla no publicada en el SHA original.
- SHA-224, SHA-256, SHA-384, y SHA-512 son versiones más nuevas y seguras de SHA, conocidas en forma colectiva como SHA-2.

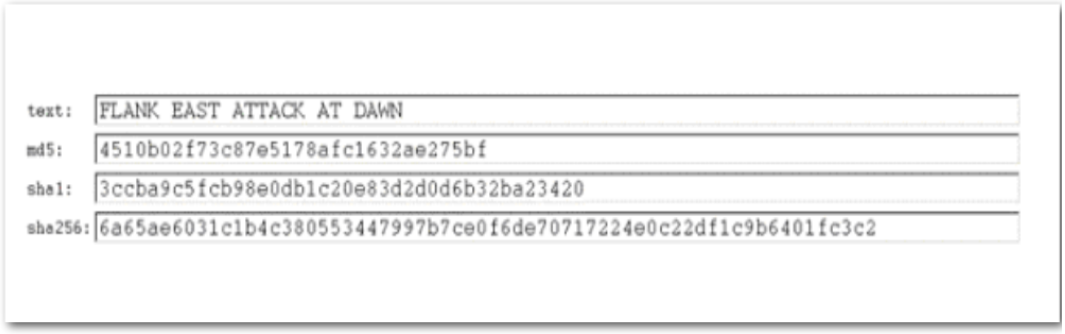


Tanto MD5 como SHA-1 se basan en MD4. Esto hace que MD5 y SHA-1 sean similares en muchos aspectos. SHA-1 y SHA-2 son más resistentes a los ataques por fuerza bruta, ya que sus digestos son al menos 32 bits más extensos que los digestos de MD5.

SHA-1 involucra 80 pasos, mientras que MD5 involucra sólo 64 pasos. El algoritmo SHA-1 además debe procesar un búfer de 160 bits, en lugar de los 128 bits de búfer de MD5. Debido a su menor cantidad de pasos, en general, MD5 se ejecuta con más rapidez, dado el mismo dispositivo.

Al seleccionar un algoritmo de hashing, es preferible usar SHA-1 o SHA-2 ante MD5. No ha sido probado que MD5 contenga fallas críticas, pero su seguridad es cuestionable en la actualidad. Si el desempeño es un problema, el algoritmo MD5 es levemente más rápido que el algoritmo para SHA-1. Debe considerarse que MD5 puede probarse como menos seguro que SHA-1.

¿Se utiliza hashing sólo para probar la integridad de los datos?



En este ejemplo, se muestran los hashes resultantes a partir del texto plano utilizando MD5, SHA-1 y SHA256. Note la diferencia en la longitud de las claves entre los diferentes algoritmos. Cuánto más larga sea la clave, más segura será la función de hash.

7.2.3 Autenticidad con HMAC

En la criptografía, un código de autenticación de hash con clave (HMAC o KHMAC - Keyed-Hash Authentication Code) es un tipo de código de autenticación de mensajes (MAC). Un HMAC se calcula utilizando un algoritmo específico, el cual combina una función de hash criptográfico con una clave secreta. Las funciones de hash son la base de mecanismo de protección de HMAC.

Sólo el remitente y el destinatario del mensaje conocen la clave secreta y la salida de la función de hash depende ahora de los datos de entrada y de la clave secreta. Sólo los participantes que tienen acceso a la clave secreta pueden calcular el digesto de una función HMAC. Esta característica evita los ataques de tipo man-in-the-middle y proporciona autenticación del origen de los datos.

Si ambos participantes comparten una clave secreta y utilizan funciones HMAC para la autenticación, si un participante recibe un digesto HMAC del mensaje construido en forma apropiada, esto indica que el otro participante fue quien originó el mensaje, porque es la única otra entidad que conoce la clave secreta.

La fuerza criptográfica de HMAC depende de la fuerza criptográfica de la función de hash subyacente, el tamaño y la calidad de la clave y la longitud en bits del resultado de la función de hash.

Las tecnologías de Cisco utilizan dos funciones HMAC bien conocidas:

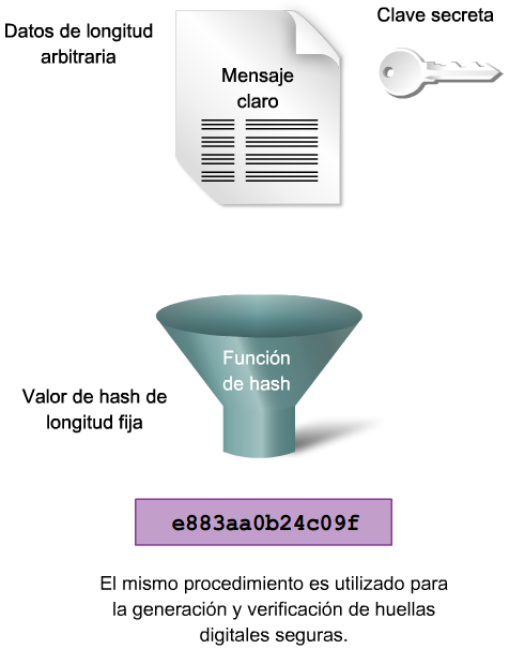
MD5 con clave (HMAC-MD5), basado en el algoritmo de hashing MD5
SHA-1 con clave (HMAC-SHA-1), basado en el algoritmo de hashing SHA-1

Cuando se genera un digesto HMAC, se ingresan datos con una longitud arbitraria en la función de hash, junto con la clave secreta. El resultado es un hash de longitud fija que depende tanto de los datos como de la clave secreta.

La distribución de las claves secretas debe realizarse con extremo cuidado y sólo a las partes involucradas porque, si la clave se ve comprometida, otro participante puede falsear y modificar los paquetes, violando la integridad de los datos.

Características de HMAC

- HMACs utilizan una clave secreta adicional como entrada para la función de hash, sumando autenticación además de integridad.
- La clave secreta es conocida por el remitente y el destinatario y combate los ataques de tipo man-in-the-middle.
- HMAC se basa en funciones de hash existentes, tales como MD5 y SHA-1.

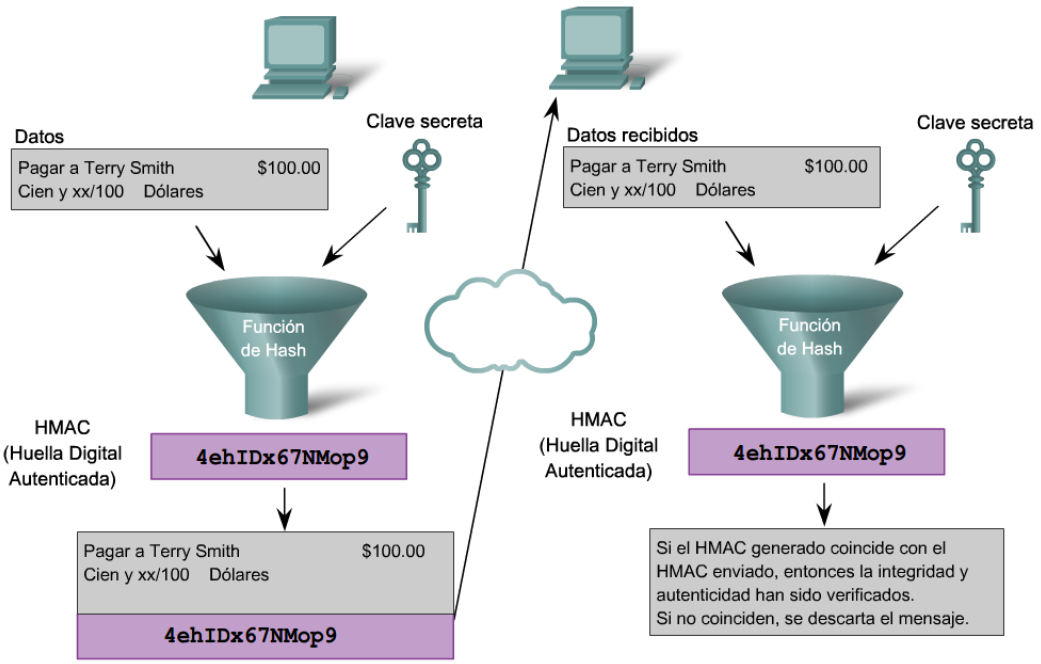


Considere un ejemplo donde un remitente desea asegurarse de que el mensaje no sea alterado durante su transmisión y quiere proporcionar un método para que el receptor pueda autenticar el origen del mensaje.

El dispositivo origen ingresa los datos y la clave secreta en el algoritmo de hashing y calcula una huella digital HMAC de longitud fija. Esta huella digital autenticada es luego agregada al mensaje y se envía el conjunto al destinatario.

El dispositivo receptor remueve la huella digital del mensaje y utiliza el mensaje en texto plano junto con su clave secreta como entrada para la misma función de hashing. Si la huella digital calculada por el destinatario es igual a la huella digital enviada junto con el mensaje, el contenido del mensaje no ha sido alterado. Además, el origen del mensaje ha sido autenticado, ya que sólo el remitente posee una copia de la clave secreta. La función HMAC ha asegurado la autenticidad del mensaje.

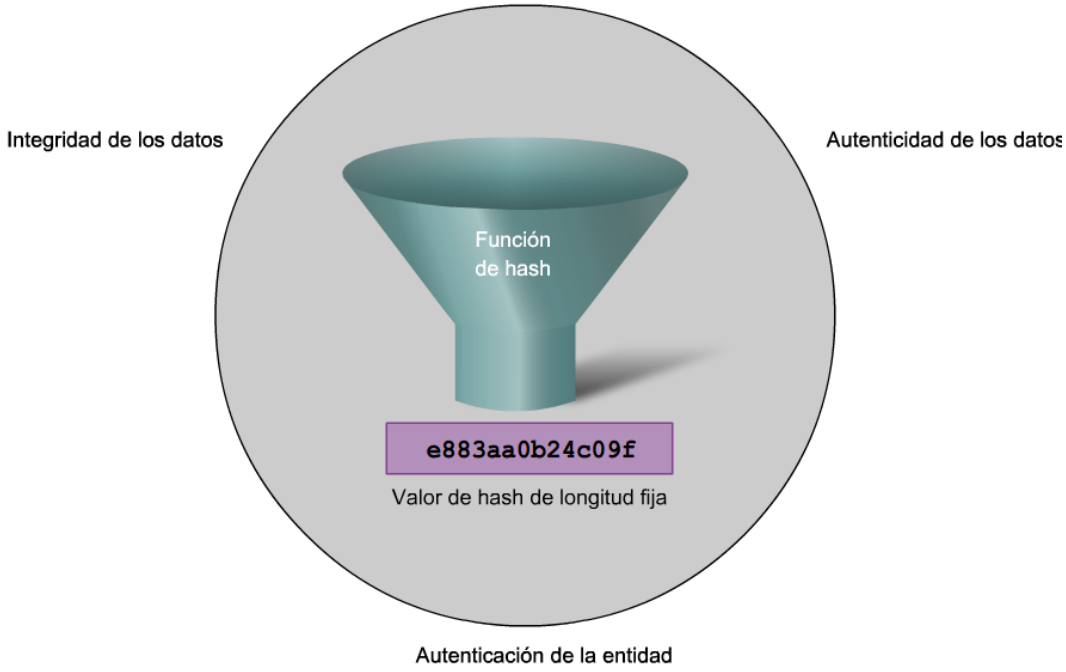
Las VPNs IPsec se basan en funciones HMAC para autenticar el origen de cada paquete y proporcionar una verificación de integridad de los datos.



Los productos Cisco utilizan hashing con fines de autenticación de entidades, integridad de datos y autenticación de datos:

Los routers Cisco IOS utilizan hashing con claves secretas de forma similar a HMAC para incorporar autenticación de información a las actualizaciones de los protocolos de enrutamiento.
Los gateways y clientes IPsec utilizan algoritmos de hashing, tales como MD5 y SHA-1 en modo HMAC, para proveer integridad y autenticidad de paquetes.
Las imágenes de software de Cisco, que se descargan desde Cisco.com, disponen de un checksum MD5 con el que los clientes pueden verificar la integridad de las imágenes descargadas.
El hashing también puede utilizarse como una forma de proporcionar claves secretas para cifrar datos. Por ejemplo, TACACS+ utiliza un hash MD5 como clave para cifrar la sesión.

Las firmas digitales son una alternativa a HMAC.



7.2.4 Administración de claves.

La administración de claves suele considerarse la parte más difícil en el diseño de un criptosistema. Muchos criptosistemas han fallado debido a errores en su administración de claves y todos los algoritmos criptográficos modernos requieren procedimientos de administración del claves. En la práctica, la mayor parte de los ataques a los sistemas criptográficos están dirigidos al nivel de la administración de claves, en lugar del algoritmo criptográfico en sí. Existen algunas características esenciales a considerar sobre la administración de claves:

Generación - Era tarea de César seleccionar la clave de su cifrado. La clave del cifrador Vigenere también es seleccionada por el remitente y el destinatario. En los sistemas criptográficos modernos, la generación de claves es en general un proceso automatizado y no llevado a cabo por el usuario final. Es necesaria la utilización de buenos generadores de números aleatorios para asegurar que todas las claves puedan ser igualmente generadas; así, los atacantes no pueden predecir qué claves tienen más posibilidades de ser utilizadas.
Verificación - Algunas claves son mejores que otras. Casi todos los algoritmos criptográficos tienen algunas claves débiles que no deberían ser utilizadas. Con la ayuda de procedimientos de verificación de claves, es posible regenerarlas si llegaran a aparecer. Con el Cifrado César, utilizar una clave de 0 o 26 no cifra el mensaje y, por lo tanto, no deberían ser utilizadas.
Almacenamiento - En un sistema operativo multi-usuario moderno que utiliza criptografía, una clave puede ser almacenada en la memoria. Esto presenta un posible problema cuando la memoria es llevada al disco, ya que un troyano instalado en la PC puede tener acceso a las claves privadas de dicho usuario.
Intercambio - Los procesos de administración de claves deben proveer un mecanismo de intercambio de claves que permita resolver un acuerdo seguro sobre el material de generación de claves con el otro participante, probablemente sobre un medio no confiable.

Revocación y destrucción - La revocación notifica a todas las partes interesadas que una clave determinada ha sido comprometida y no debe seguir siendo utilizada. La destrucción elimina las claves viejas, evitando que los atacantes maliciosos puedan recuperarlas.

Se utilizan dos términos para describir a las claves: longitud de clave (key length) y espacio de claves (keyspace). La longitud de la clave es la cantidad de bits que la conforman, mientras que el espacio de claves es la cantidad de posibilidades que pueden generarse con una cantidad específica de bits. A medida que aumenta la longitud de la clave, el espacio de claves se incrementa en forma exponencial:

Una longitud de 2 bits (2^2) = espacio de claves de 4, porque existen cuatro claves posibles (00, 01, 10 y 11).
Una longitud de 3 bits (2^3) = espacio de claves de 8, porque existen ocho claves posibles (000, 001, 010, 011, 100, 101, 110 y 111).
Una longitud de 4 bits (2^4) = espacio de 16 claves posibles.
Una longitud de 40 bits (2^40) = espacio de 1.099.511.627.776 claves posibles.



El espacio de claves de un algoritmo es el conjunto de todas las claves posibles. Una clave con una longitud de n bits produce un espacio de claves de 2^n posibles valores. Agregando un bit a la clave, se duplica el tamaño del espacio de claves. Por ejemplo, DES con sus claves de 56 bits tiene un espacio de claves mayor a 72.000.000.000.000.000 (2^56) combinaciones posibles. Agregando un bit a la longitud de la clave, el espacio de claves se duplica y un atacante necesita el doble de tiempo para buscar entre todas las posibilidades.

Casi cualquier algoritmo posee claves débiles en su espacio de claves, el cual permite que un atacante quiebre el cifrado de forma rápida. Las claves débiles muestran regularidades en el cifrado o producen un cifrado pobre. Por ejemplo, DES posee cuatro claves para las cuales el cifrado es igual al descifrado. Esto quiere decir que si una de estas claves débiles es utilizada para cifrar un texto plano, el atacante puede utilizar la clave débil para cifrar el criptograma y revelar el texto plano.

Las claves débiles DES son aquellas que producen 16 subclaves idénticas. Esto ocurre cuando los bits de la clave son:

Unos y ceros alternados (0101010101010101)
Letras F y E alternadas (FEFEFEFEFEFEFEFE)
E0E0E0E0F1F1F1F1
1F1F1F1F0E0E0E0E

Es muy poco probable que dichas claves sean seleccionadas, pero aún así las implementaciones deben verificar todas las claves y prevenir el uso de claves débiles. Con la generación manual de claves, debe tenerse especial cuidado para evitar definir claves débiles.



- Por cada bit incorporado a la clave DES, el atacante requerirá el doble de tiempo para buscar en el espacio de claves.
- Mientras más largas son las claves, más seguras se vuelven, pero también requieren más recursos y pueden afectar el desempeño.

Es posible crear diferentes tipos de claves criptográficas:

Claves simétricas, que pueden ser intercambiadas entre dos routers que soporten una VNP
Claves asimétricas, utilizadas para asegurar aplicaciones HTTPS
Firmas digitales, utilizadas para conectarse a un sitio web seguro
Claves hash, utilizadas en la generación de claves simétricas y asimétricas, firmas digitales y otros tipos de aplicaciones

Sin importar el tipo de clave del que se trate, todas comparten problemas similares. Seleccionar una longitud de clave adecuada es un problema. Si el sistema criptográfico es confiable, la única forma de quebrarlo es mediante un ataque por fuerza bruta. El ataque por fuerza bruta consiste en una búsqueda a través de todo el espacio de claves probando todas las claves posibles hasta encontrar una capaz de descifrar los datos. Si el espacio de claves es lo suficientemente grande, la búsqueda requiere una enorme cantidad de tiempo, volviendo impracticable el esfuerzo.

En promedio, un atacante debe buscar a través de la mitad de todo el espacio de claves antes de encontrar la clave correcta. El tiempo requerido para lograr esta búsqueda

depende del poder de cómputo del que dispone el atacante. Las longitudes de clave actuales vuelven el intento insignificante, porque tomaría millones o billones de años completar la búsqueda, cuando se utiliza una clave lo suficientemente larga. Con los algoritmos modernos confiables, la fortaleza de la protección depende únicamente de la longitud de la clave. Debe seleccionarse una longitud de clave que proteja la confidencialidad o integridad de los datos por un período adecuado de tiempo. Los datos que son más sensibles deben mantenerse en secreto por un tiempo más extenso y deben utilizar claves más largas.

	Clave simétrica	Clave asimétrica	Firma digital	Hash
Protección de hasta 3 años	80	1248	160	160
Protección de hasta 10 años	96	1776	192	192
Protección de hasta 20 años	112	2432	224	224
Protección de hasta 30 años	128	3248	256	256
Protección contra computadoras cuánticas	256	15424	512	512

- La figura ilustra las expectativas actuales para longitudes de clave válidas.
- Los cálculos se basan en el hecho de que el poder computacional seguirá creciendo al ritmo actual y su habilidad para realizar ataques por fuerza bruta crecerá al mismo ritmo. Si se descubre un método alternativo a la fuerza bruta contra un algoritmo en particular, las longitudes de clave de la imagen se volverán obsoletas.
- Notar la corta longitud de las claves simétricas, ilustrando que los algoritmos simétricos son el tipo de algoritmo más fuerte.

El desempeño es otro problema que puede influenciar la selección de una longitud de clave determinada. El administrador debe encontrar un buen balance entre la velocidad y la fortaleza de un algoritmo, porque algunos algoritmos, tales como RSA (Rivest, Shamir and Adelman) se ejecutan en forma lenta debido a la gran longitud de sus claves. Debe encontrarse una protección adecuada, a la vez que deben mantenerse fluidas las comunicaciones a través de redes no confiables.

La posible inversión realizada por el atacante también debe afectar la selección de longitud de la clave. Al evaluar el riesgo de intrusión para un algoritmo de cifrado, deben estimarse los recursos del atacante y por cuánto tiempo deben protegerse los datos. Por ejemplo, el DES clásico puede quebrarse en un par de minutos, con una máquina de 1 millón de dólares. Si el valor de los datos protegidos es significativamente mayor el millón de dólares necesario para conseguir la máquina que los descifre, entonces el DES clásico es una mala elección. El atacante necesitaría un millón de años o más, para romper una protección con 3DES de 168 bits o RC4 de 128 bits, lo cual hace que cualquiera estos dos algoritmos sea una opción más adecuada en este caso.

Debido al rápido avance en la tecnología y en los métodos de criptoanálisis, la longitud de clave necesaria para una aplicación en particular se incrementa en forma constante. Por ejemplo, parte de la fortaleza del algoritmo RSA es la dificultad para factorizar números grandes. Si un número de 1024 bits es difícil de factorizar, entonces un número de 2048 bits será aún más difícil. Incluso con las computadoras más rápidas existentes hoy en día, tomaría varias vidas completas factorizar un número de 1024 bits que sea factor de dos números primos de 512 bits. Por supuesto, esta ventaja se perdería si se descubre una forma fácil de factorizar números grandes, pero los criptógrafos consideran muy poco probable dicha posibilidad. La regla "mientras más larga la clave, mejor" es válida, excepto por posibles razones de rendimiento.



Claves más cortas = procesamiento más rápido, pero menos seguro



Claves más largas = procesamiento más lento, pero más seguro

7.3.1 Cifrado

El cifrado criptográfico puede proporcionar confidencialidad en diferentes capas del modelo OSI, incorporando varias herramientas y protocolos:

Los dispositivos de cifrado de enlace propietarios proveen confidencialidad a nivel de la capa de enlace de datos.
Los protocolos de capa de red, tales como la suite de protocolos IPsec, proveen confidencialidad a nivel de la capa de red.
Los protocolos tales como Secure Sockets Layer (SSL) o Transport Layer Security (TSL) proporcionan confidencialidad a nivel de la capa de sesión.
El correo electrónico seguro, las sesiones seguras de base de datos (Oracle SQL*net) y la mensajería segura (sesiones de Lotus Notes) proveen confidencialidad a nivel de la capa de aplicación.

Existen dos enfoques para asegurar la seguridad de los datos cuando se utilizan varios métodos de cifrado. El primero consiste en proteger los algoritmos. Si la seguridad de un sistema de cifrado se basa en mantener en secreto a los algoritmos en sí, debe custodiarse en extremo el código del algoritmo. Si se revela el algoritmo, cada una de las partes involucradas debe cambiar de algoritmo. El segundo enfoque indica proteger las claves. Con la criptografía moderna, todos los algoritmos son públicos: las claves criptográficas son las que aseguran el secreto de los datos. Estas son secuencias de bits, las cuales se ingresan en el algoritmo de cifrado junto con los datos a cifrar.

Dos clases básicas de algoritmos de cifrado protegen las claves: simétrico y asimétrico. Ambos difieren en el uso que hacen de las claves. Los algoritmos de cifrado simétricos utilizan la misma clave, también llamada clave secreta, para cifrar y descifrar los datos. La clave debe ser pre-compartida. Una clave pre-compartida es bien conocida por ambos participantes antes de comenzar la comunicación cifrada. Dado que ambas partes deben custodiar la clave secreta, los algoritmos de cifrado aplicados pueden utilizar claves de menor longitud. Las claves más cortas dan como resultado tiempos de ejecución más rápidos. Los algoritmos simétricos son generalmente menos intensivos computacionalmente que los algoritmos asimétricos.

Los algoritmos de cifrado asimétricos utilizan diferentes claves para cifrar y descifrar los datos. Los mensajes seguros pueden ser intercambiados sin la necesidad de una clave pre-compartida. Debido a que ambas partes no poseen una clave pre-compartida, deben utilizarse claves muy largas para frustrar a los atacantes. Estos algoritmos utilizan muchos recursos y tienen una ejecución más lenta. En la práctica, los algoritmos asimétricos son cientos y hasta miles de veces más lentos que los algoritmos simétricos.



Para comprender mejor las diferencias entre ambos tipos de algoritmos, considere un ejemplo donde Alice y Bob viven en diferentes localidades y desean intercambiar mensajes secretos entre sí a través del sistema de correo. En este ejemplo, Alice desea enviar un mensaje secreto a Bob.

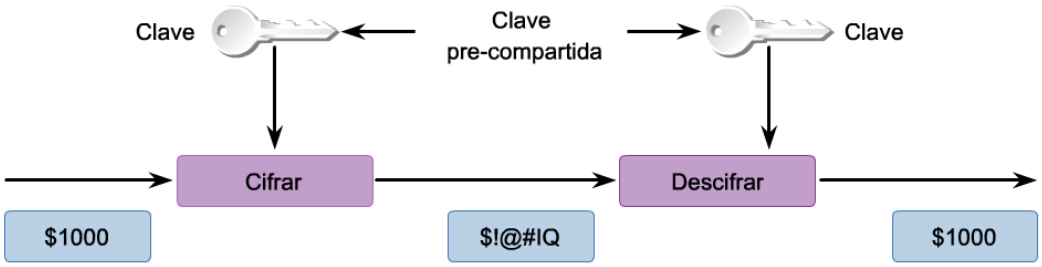
Algoritmo simétrico

En el ejemplo del algoritmo simétrico, Alice y Bob poseen llaves idénticas para un mismo candado. Estas llaves fueron intercambiadas antes de enviar cualquier mensaje secreto. Alice escribe un mensaje secreto y lo guarda en una pequeña caja, la cual cierra utilizando el candado con su llave. Luego, envía la caja a Bob. El mensaje se encuentra seguro dentro de la caja a medida que ésta viaja a través del sistema de correo postal. Cuando Bob recibe la caja, utiliza su llave para abrir el candado y recuperar el mensaje. Bob puede utilizar la misma caja y candado para enviar un mensaje secreto a Alice.

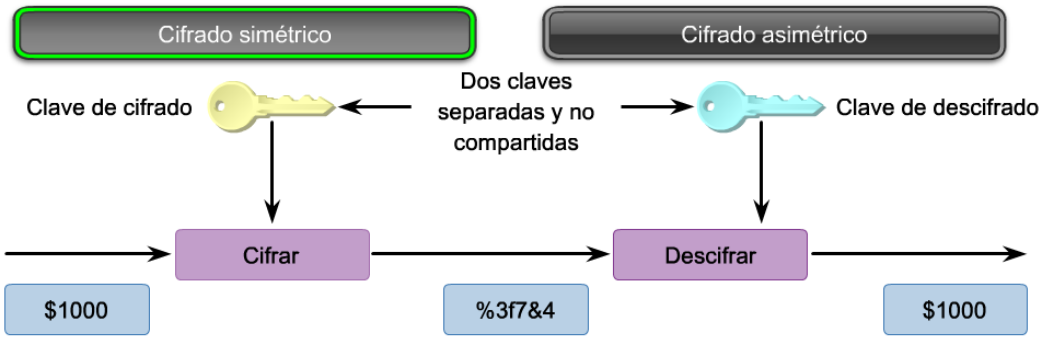
Algoritmo asimétrico

En el ejemplo del algoritmo asimétrico, Bob y Alice no intercambiaron llaves antes de enviar sus mensajes secretos. En su lugar, Bob y Alice poseen candados diferentes con sus llaves diferentes correspondientes. Cuando Alice decide enviar un mensaje secreto a Bob, primero debe contactarlo y pedirle que le envíe su candado abierto en la caja. Bob

envía el candado, pero retiene su llave. Cuando Alice recibe el candado, escribe el mensaje secreto y lo guarda en la caja. También pone su candado abierto dentro de la caja, pero retiene su llave. Luego, cierra la caja con el candado de Bob. Una vez que Alice cierra la caja, ya no es capaz de acceder a su contenido porque no posee la llave para ese candado. Entonces, envía la caja a Bob. A medida que la caja recorre el sistema de correo, nadie puede abrirla. Cuando Bob recibe la caja, puede utilizar su llave para abrir el candado y recuperar el mensaje de Alice. Para enviar una respuesta segura, Bob guarda su mensaje secreto en la caja junto con su candado abierto y cierra la caja con el candado de Alice. Luego, Bob envía la caja nuevamente a Alice.



- Los algoritmos de cifrado simétrico son mejor conocidos como algoritmos de clave secreta compartida.
- La longitud de clave usual es de 80 - 256 bits.
- El remitente y el destinatario deben compartir una clave secreta.
- Son por lo general muy rápidos (velocidad de transmisión) debido a que estos tres algoritmos se basan en operaciones matemáticas simples.
- Algunos ejemplos de algoritmos de cifrado simétrico son DES, 3DES, AES, IDEA, RC2/4/5/6 y Blowfish.



- Los algoritmos de cifrado asimétrico son mejor conocidos como algoritmos de clave pública.
- La longitud de clave usual es de 512 - 4096 bits.
- El remitente y el destino no comparten una clave secreta.
- Estos algoritmos son relativamente lentos debido a que se basan en algoritmos computacionales complejos.
- Algunos ejemplos de algoritmos de cifrado asimétrico son RSA, ElGamal, curvas elípticas y DH.



El cifrado simétrico es la forma más utilizada de criptografía, debido a que una menor longitud de clave aumenta la velocidad de ejecución. Además, los algoritmos de clave

simétrica se basan en operaciones matemáticas simples, que pueden ser fácilmente aceleradas por hardware. El cifrado simétrico es utilizado con frecuencia para cifrar datos a la velocidad de transmisión en las redes de datos y para proporcionar cifrado en bloques cuando se requiere privacidad de los datos, como por ejemplo en una VPN.

Con el cifrado simétrico, la administración de claves puede ser un desafío. Las claves de cifrado y descifrado son las mismas. El origen y el destinatario del mensaje deben intercambiar la clave secreta simétrica (utilizando un canal seguro) antes de comenzar el cifrado. La seguridad de un algoritmo simétrico se basa en mantener en secreto de la clave simétrica. Obteniendo la clave, cualquiera puede cifrar y descifrar los mensajes.

DES, 3DES, AES, SEAL y las series RC (Rivest Ciphers), incluyendo RC2, RC4, RC5 y RC6, son algoritmos bien conocidos de cifrado con clave simétrica. Existen muchos otros algoritmos de cifrado, tales como Blowfish, Twofish, Threefish y Serpent. Sin embargo, estos protocolos no son soportados por plataformas Cisco o bien aún no han ganado una aceptación masiva.

Algoritmo de cifrado simétrico	Longitud de la clave (en bits)	Descripción
DES	56	Diseñado por IBM durante la década del '70 y adoptado como estándar del NIST hasta 1997. Aunque ha sido considerado anticuado, DES sigue siendo muy utilizado. DES fue diseñado para ser implementado sólo por hardware y por lo tanto es extremadamente lento por software.
3DES	112 y 168	Basado en la utilización de DES tres veces consecutivas: los datos son cifrados tres veces. Por lo tanto, es considerado mucho más fuerte que DES. Sin embargo, es lento al compararlo con algunos nuevos cifrados por bloques, como AES.
AES	128, 192, y 256	AES es veloz tanto por software como por hardware, es relativamente fácil de implementar y requiere muy poca memoria. Como nuevo estándar de cifrado, está siendo implementado actualmente en gran escala.
Software Encryption Algorithm (SEAL)	160	SEAL es un algoritmo alternativo a DES, 3DES y AES. Utiliza una clave de cifrado de 160 bits y tiene un menor impacto sobre la CPU al compararlo con otros algoritmos basados en software.
Las series RC	RC2 (40 y 64) RC4 (1 a 256) RC5 (0 a 2040) RC6 (128, 192, y 256)	Los algoritmos RC son un conjunto de algoritmos de cifrado de clave simétrica inventado por Ron Rivest. RC1 nunca fue publicado y RC3 fue quebrado antes de poder ser utilizado. RC4 es el cifrado de flujo más utilizado a nivel mundial. RC6, un cifrado por bloques de 128 bits, está basado en gran parte en RC5 y fue un finalista de AES desarrollado en 1997.

Las técnicas más utilizadas de criptografía de cifrado simétrico son los cifrados de bloque y los cifrados de cadena.

Cifrado por bloques

El cifrado por bloques (block cipher) transforma un bloque de texto plano de longitud fija en un bloque criptográfico común de 64 o 128 bits. El tamaño del bloque define qué cantidad de datos puede cifrarse por vez. Actualmente, el tamaño del bloque, también conocido como longitud fija, es en general de 64 o 128 bits. La longitud de la clave se refiere a la clave de cifrado utilizada. Este criptograma es descifrado aplicando la transformación inversa del bloque criptográfico, utilizando la misma clave secreta.

El cifrado por bloques en general resulta en una salida de datos más larga que los datos de entrada, debido a que el criptograma debe ser un múltiplo del tamaño de los bloques. Por ejemplo, DES cifra bloques en porciones de 64 bits, utilizando una clave de 56 bits. Para lograr esto, el algoritmo de bloques toma una porción de datos por vez, por ejemplo porciones de 8 bytes, hasta que se rellena el bloque completo. Si hay menos datos que los necesarios para completar un bloque, el algoritmo agrega datos artificiales (blancos) hasta que los 64 bits son utilizados.

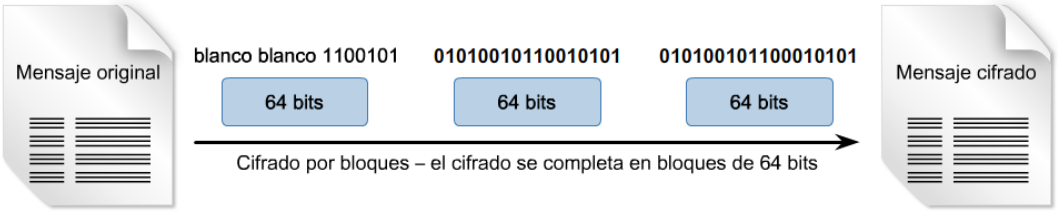
El cifrado por bloques incluye DES con bloques de 64 bits, AES con bloques de 128 bits y RSA con bloques de tamaño variable.

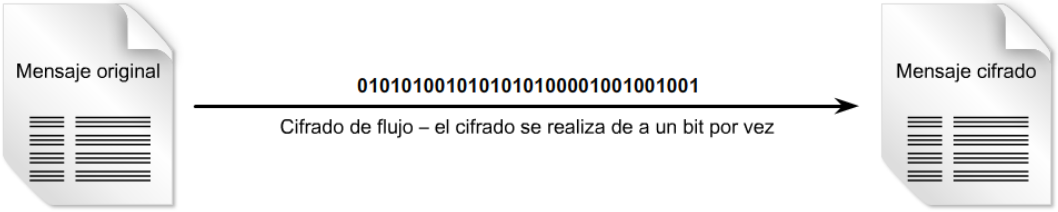
Cifrado de flujo

A diferencia del cifrado por bloques, el cifrado de flujo (stream cipher) codifica el texto plano de a un byte o un bit por vez. Los cifrados de flujo pueden verse como un cifrado de bloque con un tamaño de bloque de un bit. Con el cifrado de flujo, la transformación de estas unidades más pequeñas de texto plano es variable, dependiendo de dónde se encuentren durante el proceso de cifrado. El cifrado de flujo puede ser mucho más rápido que el cifrado por bloques y en general no incrementa el tamaño de los mensajes, ya que pueden cifrar un número arbitrario de bits.

El cifrado Vigenere es un ejemplo del cifrado de flujo. Este cifrado es periódico, debido a que su clave es de longitud infinita y la misma se repite si es más corta que el mensaje.

El cifrado de flujo incluye A5, el cual es utilizado para cifrar las comunicaciones de teléfonos celulares GSM y el cifrado RC4. DES también puede ser utilizado en modo de cifrado de flujo.





Seleccionar un algoritmo de cifrado es una de las decisiones más importantes que debe tomar un profesional de seguridad al construir un sistema criptográfico. Deben considerarse dos aspectos importantes al seleccionar un algoritmo de cifrado para una organización:

Que el algoritmo sea confiable para la comunidad criptográfica. Muchos algoritmos nuevos pueden romperse con rapidez, por lo que resultan preferibles aquellos algoritmos que han resistido ataques por varios años. Los inventores y vendedores suelen promover en exceso los beneficios de los nuevos algoritmos.
Que el algoritmo proteja de forma adecuada contra los ataques por fuerza bruta. Un buen algoritmo criptográfico está diseñado de forma tal que resista los ataques criptográficos comunes. La mejor forma de acceder a los datos protegidos por el algoritmo es intentar descifrarlos utilizando todas las claves posibles. La cantidad de tiempo necesario para este tipo de ataque depende de la cantidad de claves posibles, pero en general es muy extenso. Con claves de longitud apropiada, estos ataques son considerados impracticables. Si el algoritmo es considerado confiable, no existen atajos para quebrarlo y el atacante debe recorrer todo el espacio de claves para adivinar la clave correcta. El algoritmo debe permitir longitudes de clave que satisfagan los requisitos de confidencialidad de la organización. Por ejemplo, DES no provee una protección suficiente para los requisitos modernos, debido a sus claves cortas.

Otros criterios a considerar:

Que el algoritmo soporte claves extensas de longitud variable y escalabilidad. La longitud variable de claves y la escalabilidad son también dos atributos deseables de un buen algoritmo de cifrado. Mientras más larga sea la clave de cifrado, más tiempo debe dedicar un atacante para quebrarla. Por ejemplo, una clave de 16 bits tiene 65.536 combinaciones posibles, mientras que una clave de 56 bits tiene 7,2 x 10^16 combinaciones posibles. La escalabilidad provee una longitud de clave flexible y permite al administrador seleccionar la fortaleza y velocidad del cifrado requerido.
Que el algoritmo no tenga restricciones de exportación e importación. Deben considerarse con cuidado las restricciones de importación y exportación al utilizar el cifrado internacionalmente. Algunos países no permiten la exportación de algoritmos de cifrado o sólo la permiten si se utilizan claves más cortas. Asimismo, algunos países imponen restricciones de importación sobre los algoritmos criptográficos.

	DES	3DES	AES
El algoritmo es confiable para la comunidad criptográfica.	Reemplazado por 3DES	Sí	Evaluación en curso
El algoritmo da una protección adecuada contra ataques por fuerza bruta.	No	Sí	Sí

7.3.2 Data Encryptation Estándard (DES)

El Data Encryption Standard (DES) es un algoritmo de cifrado simétrico, utilizado normalmente en modo de cifrado por bloques. El algoritmo DES es en esencia una secuencia de permutaciones y sustituciones de bits de datos, combinadas con una clave de cifrado. Se utiliza el mismo algoritmo y la misma clave tanto para el cifrado como el descifrado.

DES tiene una longitud de clave fija. La clave tiene una longitud de 64 bits, pero sólo se utilizan 56 bits para el cifrado. Los 8 bits restantes son utilizados para la paridad. El bit menos significativo de cada byte de la clave es utilizado para indicar la paridad impar.

Una clave DES siempre tiene una longitud de 56 bits. Cuando se utiliza DES con una clave débil de 40 bits, la clave de cifrado contiene 40 bits secretos y 16 bits conocidos, lo cual conforma una clave de 56 bits. En este caso, la fortaleza de la clave DES es de 40 bits.

Características de DES	
Descripción	Estándar de cifrado de datos
Línea de tiempo	Estandarizado en 1976
Tipo de algoritmo	Simétrico
Tamaño de clave (en bits)	56 bits
Velocidad	Media
Tiempo para romperlo (Asumiendo una computadora que pueda probar 255 claves por segundo)	Días (6.4 días con la máquina COPACABANA, un dispositivo especializado en cracking)
Recursos consumidos	Medio

Aunque DES utiliza en general el método de cifrado por bloques, también puede utilizar el método de cifrado de flujo. Para cifrar o descifrar más de 64 bits de datos, DES utiliza dos métodos de cifrado por bloque estandarizados, Electronic Code Book (ECB) o Cipher Block Chaining (CBC).

Ambos métodos de cifrado utilizan la operación lógica XOR con la siguiente definición:

1 XOR 1 = 0

1 XOR 0 = 1

0 XOR 1 = 1

0 XOR 0 = 0

Método de cifrado por bloques

El método ECB cifra en forma serial cada bloque de 64 bits de texto plano utilizando la misma clave de 56 bits. Si dos bloques de texto plano idénticos son cifrados utilizando la misma clave, sus criptogramas correspondientes son iguales. Por lo tanto, un atacante podría identificar tráfico similar o idéntico que fluya a través de un canal de comunicación. El atacante podría entonces, incluso sin conocer el significado del tráfico, construir un catálogo de mensajes y utilizarlos luego como una posibilidad para obtener un acceso no autorizado. Por ejemplo, un atacante podría capturar, sin saberlo, la secuencia de identificación de un usuario con privilegios de administrador cuyo tráfico se encuentre protegido con DES-ECB y luego reenviarlo. Este riesgo es indeseable y por esto fue creado el modo CBC, para mitigar este riesgo.

En el método CBC, cada bloque de texto plano de 64 bits es procesado mediante la operación lógica XOR en conjunto con el bloque cifrado anterior y luego cifrado utilizado la clave DES. Así, el cifrado de cada bloque depende del bloque anterior. Luego, el cifrado de dos bloques de texto plano iguales puede resultar en diferentes bloques cifrados.

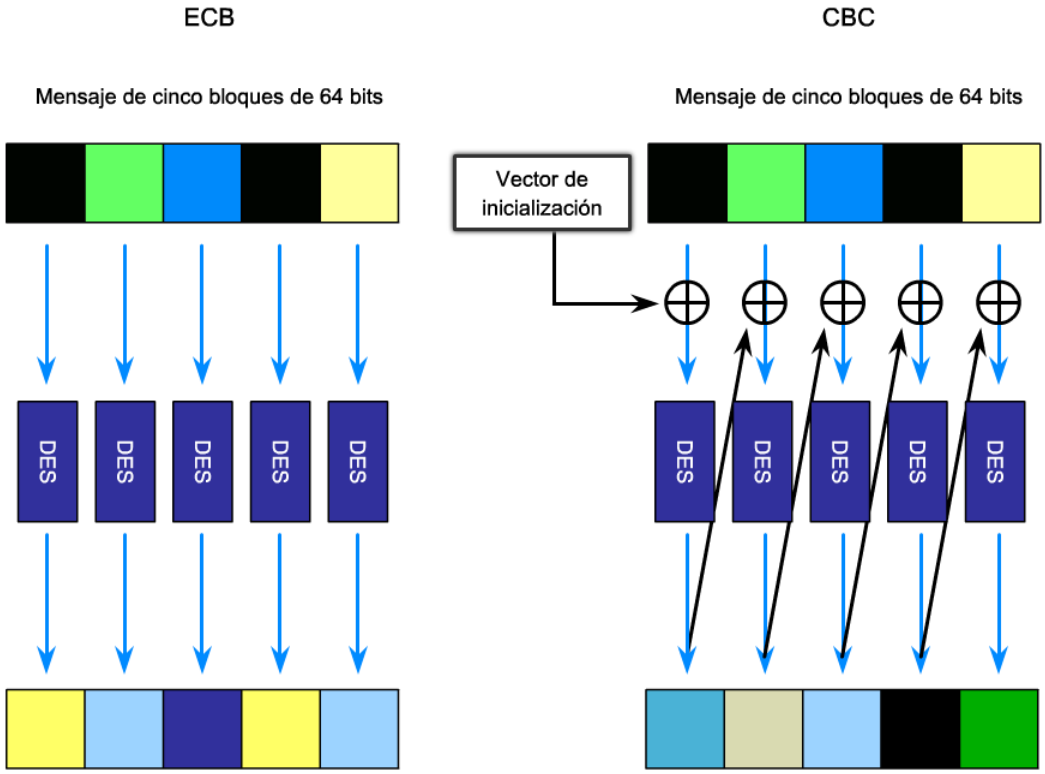
El modo CBC puede colaborar con la protección contra ciertos ataques, pero no resulta útil contra ataques sofisticados de criptoanálisis o un ataque extendido por fuerza bruta.

Método de cifrado de flujo

Para cifrar o descifrar más de 64 bits de datos, DES utiliza dos métodos comunes de cifrado de flujo:

Cipher feedback (CFB), el cual es similar al método CBC y puede cifrar cualquier cantidad de bits, incluyendo bits o caracteres aislados.
Output feedback (OFB) genera bloques de caracteres aleatorios, los cuales luego son procesados con la función lógica XOR en conjunto con los bloques de texto plano, para obtener el criptograma.

Con el método de cifrado de flujo, se utilizan criptogramas previos y la clave secreta para generar una cadena de bits pseudo-aleatoria, la cual sólo puede generarse con la clave secreta. Para cifrar los datos, los mismos deben procesarse bit por bit o incluso byte por byte, utilizando la operación lógica XOR en conjunto con la cadena pseudo-aleatoria de bits, para obtener el criptograma. El proceso de descifrado es similar. El receptor genera la misma secuencia pseudo-aleatoria utilizando la clave secreta y obtiene el texto plano al procesar dicha secuencia junto con el criptograma, utilizando la operación lógica XOR.



Deben considerarse varios aspectos al utilizar datos cifrados con DES:

Cambiar las claves con frecuencia, para prevenir ataques por fuerza bruta.

Utilizar un canal seguro para comunicar las claves DES entre los participantes de la comunicación.
Considerar la utilización de DES en el modo CBC. Con CBC, el cifrado de cada bloque de 64 bits depende del bloque anterior. CBC es el modo más utilizado de DES.
Probar la fortaleza de una clave antes de utilizarla. DES posee 4 claves débiles y 12 claves semi-débiles. Debido a que existen 2^56 posibles claves DES, la probabilidad de seleccionar una de estas claves es muy pequeña. Sin embargo, debido a que la prueba de las claves no tiene un impacto significativo en el tiempo de cifrado, se recomienda su ejecución.

Debido a la poca longitud de sus claves, DES es considerado un buen protocolo para proteger datos por un período corto de tiempo. 3DES es una mejor opción para proteger datos. Posee un algoritmo muy confiable y que posee una mayor fortaleza de seguridad.



7.3.3 DES

Con los avances en el poder de procesamiento de las computadoras, las claves DES originales de 56 bits se volvieron demasiado cortas para soportar ataques realizados con tecnología de mediano presupuesto. Una forma de aumentar la longitud efectiva de la

clave DES, sin modificar el algoritmo bien analizado, consiste en utilizar repetidas veces el mismo algoritmo con diferentes claves.

La técnica de aplicar DES tres veces seguidas a un mismo bloque de texto plano es conocida como 3DES. En la actualidad, los ataques por fuerza bruta sobre 3DES son considerados impracticables debido a que los algoritmos básicos han sido bien analizados durante sus más de 35 años de utilización. Por lo tanto, es considerado muy confiable.

La implementación IPsec de Cisco utiliza DES y 3DES en el modo CBC.

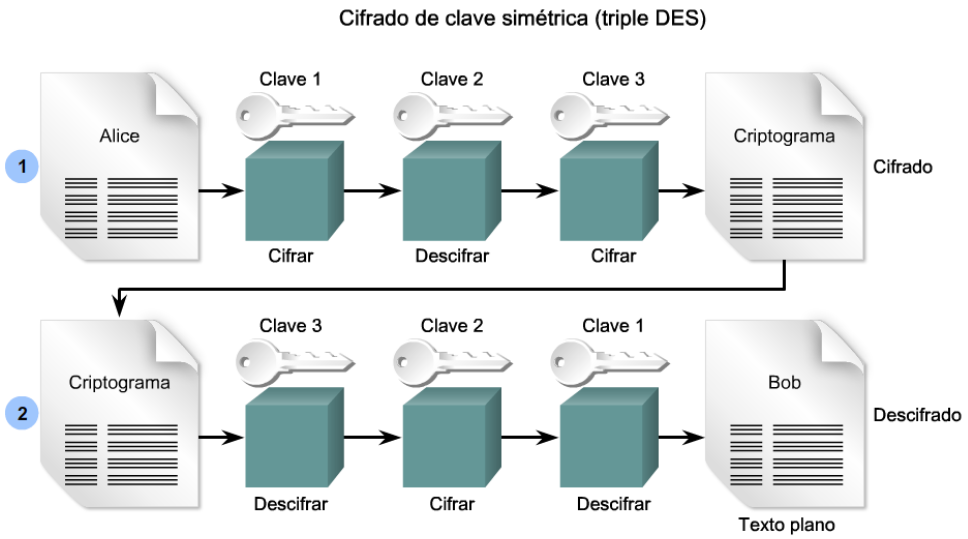
Características de 3DES	
Descripción	Estándar de cifrado de datos triple
Línea de tiempo	Estandarizado en 1977
Tipo de algoritmo	Simétrico
Tamaño de clave (en bits)	112 y 168 bits
Velocidad	Lenta
Tiempo para romperlo (Asumiendo una computadora que pueda probar 255 claves por segundo)	4.6 miles de millones de años, con tecnología actual
Recursos consumidos	Medio

3DES utiliza un método llamado 3DES-Encrypt-Decrypt-Encrypt (3DES-EDE) para cifrar texto plano. Primero, el mensaje es cifrado utilizando la primera clave de 56 bits, llamada K1. Luego, los datos se descifran utilizando la segunda clave de 56 bits, llamada K2. Finalmente, los datos son nuevamente cifrados con la tercera clave de 56 bits, llamada K3.

El procedimiento 3DES-EDE es mucho más efectivo en el aumento de la seguridad que el simple cifrado de los datos tres veces con tres claves diferentes. Cifrando datos tres veces consecutivas utilizando claves diferentes de 56 bits equivale a una fortaleza de clave de 58 bits. El procedimiento 3DES-EDE, por otro lado, provee un cifrado con una longitud efectiva de clave de 168 bits. Si las claves K1 y K3 son iguales, como sucede en algunas implementaciones, se obtiene un cifrado menos seguro de 112 bits.

Para descifrar el mensaje, debe utilizarse el proceso inverso a 3DES-EDE. Primero, el criptograma se descifra utilizando la clave K3. Luego, los datos son cifrados utilizando la clave K2. Finalmente, los datos vuelven a descifrarse utilizando la clave K1.

Aunque 3DES es muy seguro, también consume recursos en forma intensiva. Por este motivo, se desarrolló el algoritmo de cifrado AES, el cual ha sido probado tan seguro como 3DES, pero con resultados mucho más veloces.



1. El texto claro de Alice debe ser cifrado utilizando la clave 1. El criptograma es descifrado utilizando una clave diferente, la clave 2. Finalmente el resultado es cifrado utilizando otra clave, la clave 3.

2. Cuando el texto cifrado con 3DES es recibido, el proceso se revierte. El criptograma debe ser primero descifrado utilizando la clave 3, cifrado con la clave 2 y finalmente descifrado utilizando la clave 1.

7.3.4 Advanced Encryption Standard (AES)

Durante algunos años, se había pensado que DES llegaría eventualmente al final de su utilidad. En 1997 fue anunciada la iniciativa AES y se invitó al público a proponer esquemas de cifrado para reemplazar a DES. Luego de un proceso de estandarización de 5 años, durante los cuales se presentaron y evaluaron 15 diseños diferentes, el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST) seleccionó el cifrado por bloques de Rijndael para el algoritmo AES.

El cifrado Rijndael, desarrollado por Joan Daemen y Vincent Rijmen, posee una longitud de bloque y longitud de clave variables. Rijndael es un cifrado por bloques iterativo, lo que significa que el bloque de entrada inicial y la clave de cifrado atraviesan múltiples ciclos de transformación antes de generar los datos de salida. El algoritmo puede operar sobre bloques de tamaños variables, utilizando claves de diferente longitud. Pueden utilizarse claves de 128 bits, 192 bits o 256 bits, para cifrar bloques de datos de 128, 192 o 256 bits de longitud y es posible utilizar cualquiera de las nueve combinaciones de bloques y claves.

La implementación Rijndael aceptada para AES contiene sólo algunas capacidades del algoritmo Rijndael. El algoritmo fue escrito de forma tal que la longitud de los bloques o de la clave puedan ser fácilmente extendidos en múltiplos de 32 bits y el sistema está diseñado específicamente para su implementación por hardware o por software en un amplio rango de procesadores.

El algoritmo AES ha sido analizado extensivamente y ahora es utilizado en todo el mundo. Aunque no ha sido probado con el uso cotidiano en igual grado que 3DES, AES con cifrado Rijndael es el algoritmo más eficiente. Puede ser utilizado en ambientes de baja latencia y gran volumen de transferencia, especialmente cuando 3DES no puede procesar los requisitos de latencia o transferencia. Se espera que aumente la confianza

en AES con el transcurso del tiempo, a medida que se intenten más ataques en su contra.

Características de AES	
Descripción	Estándar de cifrado avanzado
Línea de tiempo	Estándar oficial desde 2001
Tipo de algoritmo	Simétrico
Tamaño de clave (en bits)	128, 192, y 256
Velocidad	Alta
Tiempo para romperlo (Asumiendo una computadora que pueda probar 255 claves por segundo)	149 trillones de años
Recursos consumidos	Bajos

Más información

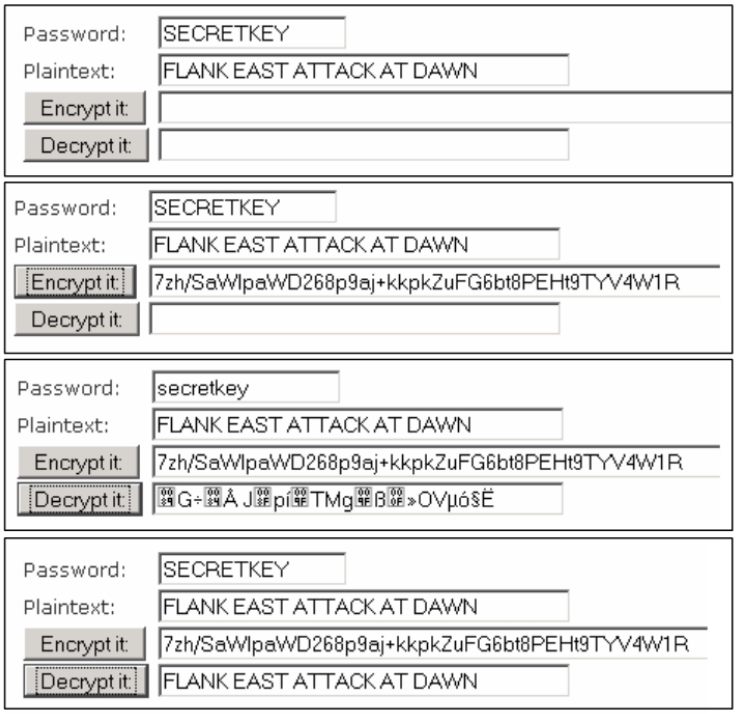
Para obtener más información sobre AES, visite http://www.nist.gov/aes. En 2008, el NIST llevó adelante una competencia, similar a la de la iniciativa AES, para desarrollar una nueva versión de SHA. Para obtener más información, visite http://csrc.nist.gov/groups/ST/hash/sha-3/index.html

AES fue seleccionado para reemplazar a DES por diferentes razones. La longitud de clave de AES la vuelve mucho más segura que DES. AES se ejecuta con mayor velocidad que 3DES sobre hardware de similares características. AES es más eficiente que DES y 3DES, usualmente por un factor de cinco cuando es comparado con DES. AES es más adecuado en ambientes de baja latencia y alta transferencia, especialmente si se utiliza sólo cifrado por software.

A pesar de estas ventajas, AES es un algoritmo relativamente joven. La regla de oro de la criptografía establece que un algoritmo maduro es siempre más confiable. Por lo tanto, 3DES es la opción más confiable en términos de fortaleza, porque ha sido probado y analizado por 35 años.

AES se encuentra disponible como transformación de cifrado en los siguientes dispositivos VPN de Cisco:

Tráfico protegido por IPsec utilizando la versión del IOS Cisco 12.2(13)T o posterior
Software Cisco PIX Firewall versión 6.3 o posterior
Software Cisco ASA versión 7.0 o posterior
Software Cisco VPN 3000 versión 3.6 o posterior



En este ejemplo, se ingresan la clave SECRETKEY y el texto plano.

Ahora están cifrados utilizando AES 128.

Un intento de descifrar el texto utilizando la clave incorrecta, en minúsculas.

Un segundo intento de descifrar el texto, utilizando la clave correcta, muestra el texto plano original.

7.3.5 Algoritmos de Cifrado Alternativos

SEAL (Software-optimized Encryption Algorithm) es un algoritmo alternativo a los algoritmos DES, 3DES y AES, basados en software. Phillip Rogaway y Don Coppersmith diseñaron SEAL en 1993. Es un cifrado de flujo que utiliza una clave de cifrado de 160 bits. Al ser un cifrado de flujo, los datos deben ser cifrados de forma continua, por lo que es más veloz que el cifrado por bloques. Sin embargo, posee una fase de inicialización más extensa, durante la cual se crea un conjunto grande de tablas utilizando SHA.

SEAL tiene un menor impacto sobre el CPU, comparado con otros algoritmos basados en software. A partir de la versión del IOS Cisco 12.3(7)T se incorporó soporte para SEAL.

SEAL tiene varias restricciones:

El router Cisco y el otro extremo deben soportar IPsec.
El router Cisco y el otro extremo deben ejecutar una imagen de IOS con claves de longitud k9 (subsistema k9).
El router y el otro extremo no deben incluir cifrado IPsec por hardware.

Características de SEAL	
Descripción	Algoritmo de cifrado optimizado por software
Línea de tiempo	Publicado por primera vez en 1994. La versión actual es la 3.0 (1997)
Tipo de algoritmo	Simétrico
Tamaño de clave (en bits)	160
Velocidad	Alta
Tiempo para romperlo (Asumiendo una computadora que pueda probar 255 claves por segundo)	Desconocido, pero considerado muy seguro
Recursos consumidos	Bajos

Los algoritmos RC fueron diseñados en parte o completamente por Ronald Rivest, quien también inventó MD5. Los algoritmos RC están ampliamente distribuidos en muchas aplicaciones de red debido a su velocidad favorable y su capacidad de utilizar claves de longitud variable.

Existe una cantidad de algoritmos RC ampliamente utilizados:

RC2 - Cifrado por bloques con clave de longitud variable, diseñado como un reemplazo para DES.
RC4 - Cifrado de flujo más utilizado a nivel mundial. Este algoritmo consiste en un cifrado de flujo Vernam con clave de longitud variable, utilizado con frecuencia en productos de cifrado de archivos y para comunicaciones seguras, tales como dentro de SSL. El cifrado por software se ejecuta rápidamente y es considerado seguro, aunque puede implementarse en forma insegura, como en el caso de WEP (Wired Equivalent Privacy).
RC5 - Cifrado por bloques rápido, con longitudes variables de bloque y de clave. RC5 puede ser utilizado como reemplazo para DES, si el tamaño de los bloques se configura en 64 bits.
RC6 - Desarrollado en 1997, RC6 fue un finalista de AES (Rijndael ganó). Rivest, Sidney y Yin diseñaron un cifrado por bloques de 128 a 256 bits basado en RC5. Su objetivo principal de diseño era cumplir con los requisitos de AES.

Código de Ron o códigos Rivest				
Descripción	RC2	RC4	RC5	RC6
Línea de tiempo	1987	1987	1994	1998
Tipo de algoritmo	Cifrado por bloques	Cifrado de flujo	Cifrado por bloques	Cifrado por bloques
Tamaño de clave (en bits)	40 y 64	1 - 256	0 a 2040 bits (se sugiere 128)	128, 192, o 256

7.3.6 Intercambio de claves Diffie-Hellman

Whitfield Diffie y Martin Hellman inventaron el algoritmo Diffie-Hellman (DH) en 1976. El algoritmo DH es la base de la mayoría de los métodos automáticos de intercambio de claves actuales y es uno de los protocolos de red más comunes hoy día. Diffie-Hellman no es un mecanismo de cifrado y no es utilizado para cifrar datos sino que es un método para intercambiar de forma segura las claves para cifrar datos.

En un sistema de claves simétricas, ambos extremos de la comunicación deben tener claves idénticas. El intercambio seguro de dichas claves siempre se ha presentado como un desafío. Los sistemas de claves asimétricas resuelven este desafío porque utilizan dos claves. Una clave es llamada clave privada, mientras que la otra se llama clave pública. La clave privada es secreta y sólo conocida por el usuario. La clave pública se comparte en forma abierta y se distribuye con facilidad.

DH es un algoritmo matemático que permite a dos computadoras generar una clave secreta idéntica en ambos sistemas, sin haberse comunicado con anterioridad. La nueva clave compartida nunca es realmente intercambiada entre los participantes. Pero debido a que ambas partes la conocen, puede ser utilizada para cifrar el tráfico entre los dos sistemas. Su seguridad se basa en la dificultad de calcular los logaritmos discretos de números muy grandes.

DH es usado en general para el intercambio de datos utilizando una VPN IPsec, datos cifrados en Internet utilizando SSL o TSL o cuando se intercambian datos con SSH.

Desafortunadamente, los sistemas de clave asimétrica son extremadamente lentos para cualquier tipo de cifrado masivo. Por este motivo, es común cifrar el grueso del tráfico utilizando un algoritmo simétrico como DES, 3DES o AES y utilizar un algoritmo DH para crear las claves utilizadas por el algoritmo de cifrado.

Características de DH	
Descripción	Algoritmo Diffie-Hellman
Línea de tiempo	1976
Tipo de algoritmo	Asimétrico
Tamaño de la clave (en bits)	512, 1024, 2048
Velocidad	Lento
Tiempo para romperlo (Asumiendo una computadora que pueda probar 255 claves por segundo)	Desconocido, pero considerado muy seguro
Recursos consumidos	Medio

Para comprender mejor cómo se utiliza DH, considere este ejemplo de comunicación entre Alice y Bob.

1. Para iniciar el intercambio DH, Alice y Bob deben acordar dos números no secretos. El primer número, g, es un número base (también conocido como generador). El segundo número, p, es un número primo utilizado como módulo. Estos números en general son públicos y son seleccionados a partir de una tabla de valores conocidos. En general, g es un número muy pequeño, tal como 2, 3, 4 o 5 y p es un número primo mayor.

2. Luego, Alice genera su número secreto Xa y Bob genera su número secreto Xb.

3. En base a g, p y su número secreto X, Alice calcula un valor público (Ya) utilizando el algoritmo DH. Luego envía su valor público (Ya) a Bob.

4. Bob también calcula un valor público (Yb) utilizando g, p y su número secreto. Bob envía su número público (Yb) a Alice. Estos valores no son iguales.

5. Ahora Alice ejecuta un segundo algoritmo DH utilizando el valor público de Bob (Yb) como número base.

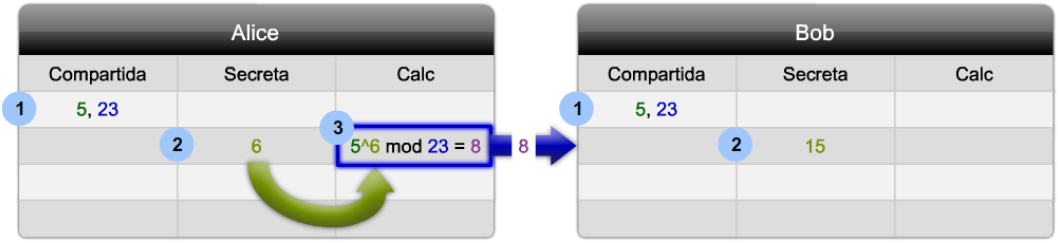
6. Bob también ejecuta un segundo algoritmo DH utilizando el valor público de Alice (Ya) como número base.

Como resultado, Alice y Bob obtuvieron el mismo valor (Z). Este nuevo valor es ahora la clave secreta compartida entre Alice y Bob y puede ser utilizada por el algoritmo de cifrado como la clave compartida entre Alice y Bob.

Cualquiera que se encuentre escuchando el canal de comunicación es incapaz de calcular el valor secreto, porque sólo g, p, Ya, y Yb son conocidos y al menos un valor secreto es necesario para calcular el secreto compartido. A menos que los atacantes puedan calcular el algoritmo discreto de la ecuación anterior para recuperar Xa o Xb, no podrán obtener el secreto compartido.

Aunque DH es utilizado con algoritmos simétricos para crear claves compartidas, es importante recordar que en realidad se trata de un algoritmo asimétrico.

¿Qué otros algoritmos asimétricos existen y para qué son utilizados?

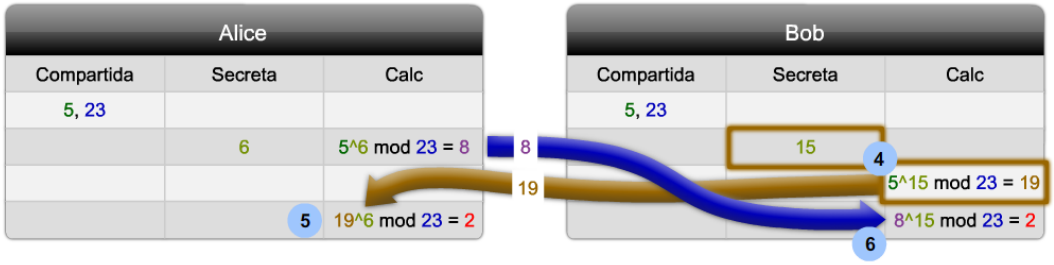


1. Alice y Bob acuerdan utilizar los mismos dos números. Por ejemplo, el número base g = 5 y el número primo p = 23

2. Alice genera un número secreto Xa = 6. Bob genera un número secreto Xb = 15

3. Alice ejecuta el algoritmo DH: g^Xa módulo p = Ya;
g^Xa módulo p = (5^6 módulo 23) = 8 = Ya. Este valor es enviado a Bob.

DH Pasos 1-3 | DH Pasos 4-6



4. Bob ejecuta el algoritmo DH:
   g^x módulo p = (5^15 módulo 23) = 19 (Yb). Este nuevo número es enviado a Alice.

5. Alice ejecuta un nuevo algoritmo DH: **Yb^Xa módulo p = Z;**
   Y^x módulo p = (19^6 módulo 23) = 2.

6. Bob ejecuta un nuevo algoritmo DH: **Ya^Xb módulo p = Z;**
   Y^x módulo p = (8^15 módulo 23) = 2.

DH Pasos 1-3 | DH Pasos 4-6

7.4.1 Cifrado simétrico versus asimétrico

Los algoritmos asimétricos, también conocidos como algoritmos de clave pública, están diseñados de forma tal que la clave utilizada para cifrar los datos sea diferente a la utilizada para descifrarlos. La clave de descifrado no puede ser calculada en un tiempo razonable a partir de la clave de cifrado y viceversa.

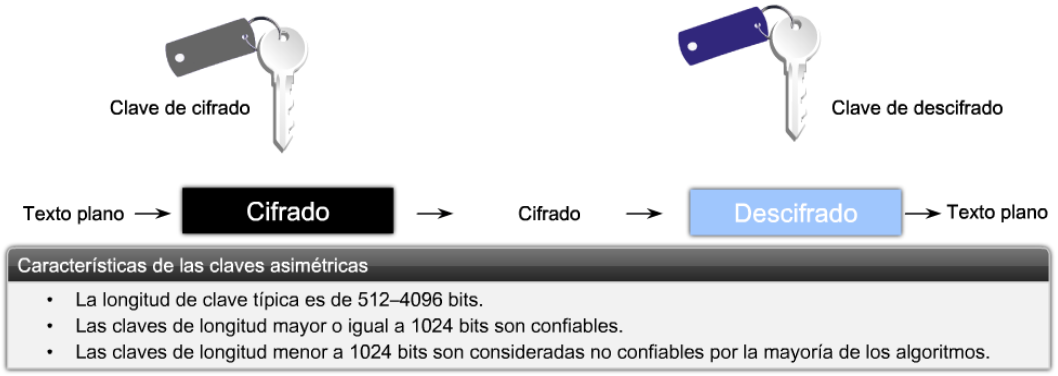
En el ejemplo, Alice y Bob no intercambiaron las claves pre-compartidas antes de comenzar la comunicación. En su lugar, cada uno disponía de candados separados y sus correspondientes llaves. De este mismo modo, los algoritmos simétricos son utilizados para intercambiar mensajes sin haber tenido nunca un secreto compartido antes del intercambio.

Existen cuatro protocolos que utilizan algoritmos de clave asimétrica:

Internet Key Exchange (IKE), un componente fundamental de las VPNs IPsec
Secure Socket Layer (SSL), ahora implementado como el estándar IETF TLS
SSH
Pretty Good Privacy (PGP), un programa de computadora que provee privacidad y autenticación criptográficas y se utiliza con frecuencia para incrementar la seguridad de las comunicaciones de correo electrónico

Los algoritmos asimétricos utilizan dos claves: una clave pública y una clave privada. Ambas pueden utilizarse en el proceso de cifrado, pero se requiere la clave complementaria correspondiente para su descifrado. Por ejemplo, si se utiliza una clave pública para cifrar los datos, la clave privada correspondiente los descifra. La operación inversa también es válida: si se cifran los datos con la clave privada, debe utilizarse la clave pública correspondiente para descifrarlos.

Este proceso permite que los algoritmos asimétricos proporcionen autenticación, integridad y confidencialidad.

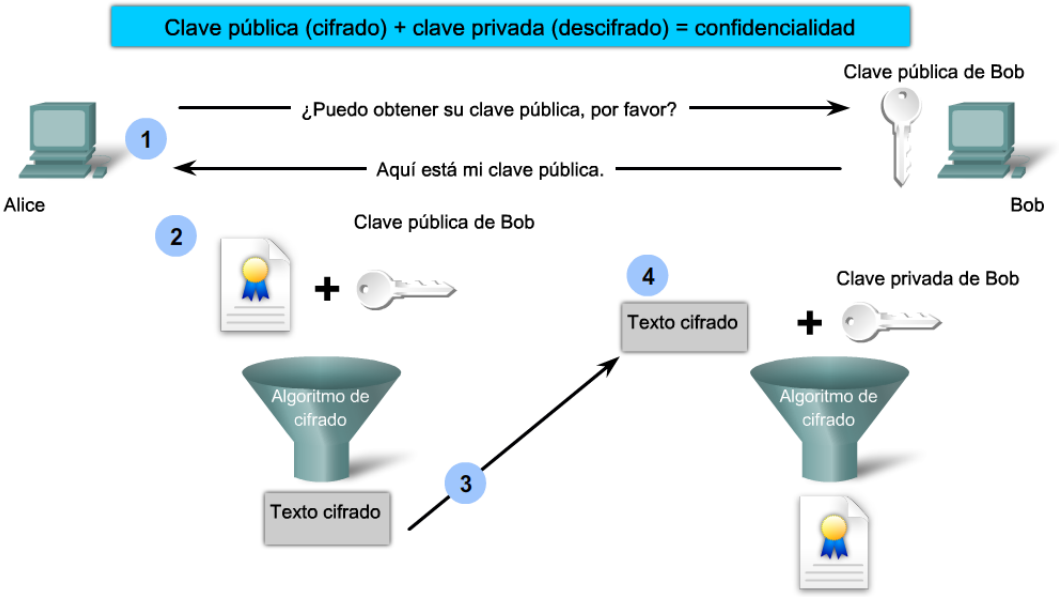


El objetivo de confidencialidad de los algoritmos asimétricos se logra cuando el proceso de cifrado comienza con la clave pública. El proceso puede resumirse utilizando la siguiente fórmula:

clave pública (cifrado) + clave privada (descifrado) = confidencialidad

Cuando la clave pública es utilizada para cifrar los datos, la clave privada debe ser utilizada para descifrar los datos. Sólo uno de los hosts posee la clave privada, por lo tanto, se logra la confidencialidad.

Si la clave privada se ve comprometida, debe generarse otro par de claves para reemplazar a la clave comprometida.

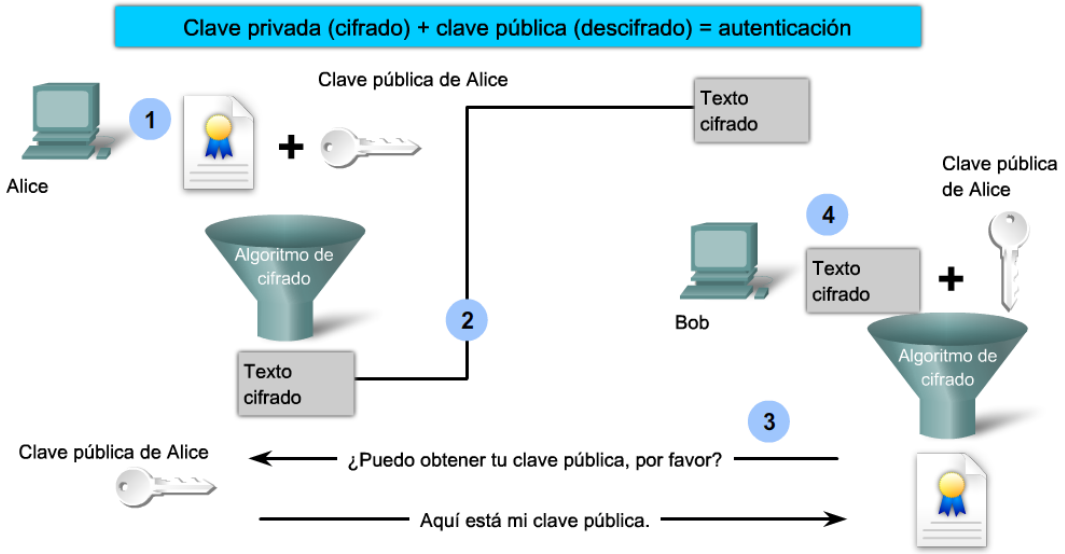


1. Alice obtiene la clave pública de Bob.
2. Alice utiliza la clave pública de Bob para cifrar un mensaje utilizando un algoritmo acordado previamente.
3. Alice transmite el mensaje cifrado a Bob.
4. Bob utiliza su clave privada para descifrar y revelar le mensaje.

El objetivo de autenticación de los algoritmos asimétricos se logra cuando el proceso de cifrado comienza con la clave privada. El proceso puede resumirse utilizando la siguiente fórmula:

clave privada (cifrado) + clave pública (descifrado) = autenticación

Cuando la clave privada es utilizada para cifrar los datos, la clave pública correspondiente debe ser utilizada para descifrar los datos. Debido a que sólo un host posee la clave privada, sólo dicho host puede haber cifrado el mensaje, probando así la autenticidad del remitente. En general, no se intenta preservar el secreto de la clave pública, por lo que cualquier número de hosts puede descifrar el mensaje. Cuando un host descifra exitosamente un mensaje utilizando una clave pública, confía en que la clave privada cifró el mensaje, lo cual verifica la identidad del remitente. Esta es una forma de autenticación.



1. Alice cifra el mensaje con su clave privada.
2. Alice transmite el mensaje cifrado a Bob.
3. Bob necesita verificar que el mensaje realmente proviene de Alice. Solicita y obtiene la clave pública de Alice.
4. Bob utiliza la clave pública para descifrar exitosamente el mensaje y autenticar que el mensaje realmente proviene de Alice.

Para enviar un mensaje que asegure su confidencialidad, autenticación e integridad, es necesaria la combinación de dos fases de cifrado.

Fase 1 - Confidencialidad

Alice desea enviar un mensaje a Bob, asegurando la confidencialidad del mensaje (sólo Bob puede leer el documento en texto plano). Alice utiliza la clave pública de Bob para cifrar el mensaje. Sólo Bob puede descifrarlo, utilizando su clave privada.

Fase 2 - Autenticación e Integridad

Además, Alice desea asegurar la autenticación e integridad del mensaje (Bob está seguro de que el documento no ha sido modificado y que fue enviado por Alice). Alice utiliza su clave privada para cifrar un hash del mensaje. De esta forma, Bob puede utilizar la clave pública de Alice para verificar que el mensaje no ha sido modificado (el hash recibido es igual al calculado localmente, en base a la clave pública de Alice). Además, esto verifica que Alice es realmente quien envió el mensaje, porque nadie más posee su clave privada.

Al enviar un mensaje cifrado con la clave pública de Bob y un hash cifrado con la clave privada de Alice, se aseguran la confidencialidad, la autenticidad y la integridad.

Existe una variedad de algoritmos de clave asimétrica bien conocidos:

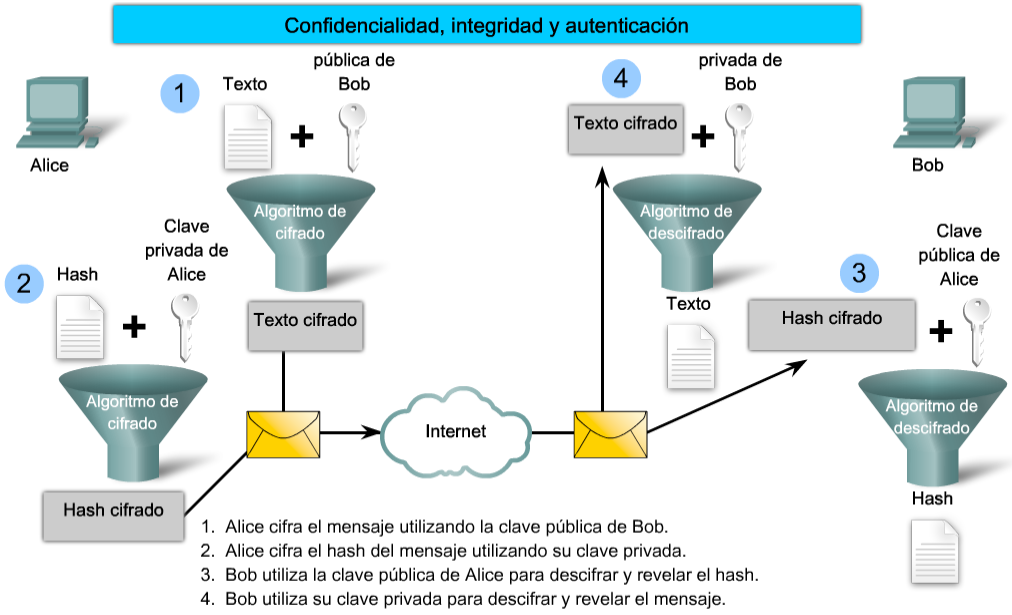
Diffie-Hellman
Digital Signature Standard (DSS), el cual incorpora el Algoritmo de Firma Digital (DSA - Digital Signature Algorithm)
Algoritmos de cifrado RSA
ElGamal
Técnicas de curva elíptica

Aunque las matemáticas difieren con cada algoritmo, todos comparten un rasgo: todos los cálculos requeridos son complicados. Sus diseños se basan en problemas computacionales, tales como la factorización o el cómputo de logaritmos discretos de números extremadamente grandes. Como resultado, el tiempo de ejecución de los algoritmos asimétricos es más extenso. De hecho, los algoritmos asimétricos pueden ser hasta 1.000 veces más lentos que los algoritmos simétricos. Debido a la falta de velocidad, los algoritmos simétricos son utilizados en general en mecanismos criptográficos de bajo volumen, tales como intercambio de claves cuando no existen mecanismos inherentes de intercambio y firmas digitales.

La administración de claves de los algoritmos asimétricos tiende a ser más simple que la de los algoritmos simétricos, debido a que usualmente una de las claves de cifrado y descifrado puede hacerse pública.

Las longitudes de clave típicas para los algoritmos simétricos son entre 512 y 4096 bits. Las claves con longitudes iguales o mayores a 1024 bits son considerada confiables, mientras que las claves de longitud menor a 1024 bits son consideradas poco fiables para la mayoría de los algoritmos.

No resulta relevante comparar la longitud de clave entre los algoritmos simétricos y asimétricos, debido a que el diseño subyacente de las dos familias de algoritmos difiere en gran medida. Para ilustrar este punto, en general se considera que una clave de cifrado RSA de 2048 bits es equivalente a una clave RC4 de 128 bits, en términos de resistencia contra ataques por fuerza bruta.



Dos fases de cifrado | Algoritmos de clave asimétrica

Algoritmo de cifrado asimétrico	Longitud de clave (en bits)	Descripción
DH	512, 1024, 2048	El algoritmo Diffie-Hellman es un algoritmo de clave pública inventado en 1976 por Whitfield Diffie y Martin Hellman. Permite que dos participantes lleguen a un acuerdo sobre una clave que puede utilizarse para cifrar mensajes que deseen enviarse entre sí. La seguridad de este algoritmo depende de la premisa de que resulta fácil elevar números a una cierta potencia, pero es difícil computar qué potencia fue utilizada dado un número y el resultado.
Digital Signature Standard (DSS) y Digital Signature Algorithm (DSA)	512 - 1024	DSS fue creado por el NIST y especifica a DSA como su algoritmo para firmas digitales. DSA es un algoritmo de clave pública basado en el esquema de firmas ElGamal. La velocidad de creación de firmas es similar a RSA, pero es entre 10 y 40 veces más lento para la verificación.
Algoritmos de cifrado RSA	512 a 2048	Desarrollado por Ron Rivest, Adi Shamir, y Leonard Adleman en el MIT en 1977. Es un algoritmo para criptografía de clave pública basado en la dificultad para factorizar números muy grandes. Es el primer algoritmo conocido como apropiado para firmas y cifrado a la vez y uno de los primeros grandes avances en la criptografía de clave pública. Es ampliamente utilizado en los protocolos de comercio electrónico, y se lo considera seguro debido a la utilización de claves suficientemente largas e implementaciones actualizadas.
ElGamal	512 - 1024	Algoritmo de cifrado de claves asimétricas para la criptografía de clave pública, el cual se basa en el acuerdo de claves Diffie-Hellman. Fue descripto por Taher ElGamal en 1984 y es utilizado en el software GNU Privacy Guard, PGP, y otros criptosistemas. Una desventaja del sistema ElGamal es que el mensaje cifrado se vuelve muy grande, unas dos veces el tamaño del mensaje original y por este motivo sólo es utilizado para mensajes pequeños, tales como las claves secretas.
Técnicas de curva elíptica	160	La criptografía de curva elíptica fue inventada por Neil Koblitz y Victor Miller a mediados de los '80. Puede ser utilizado para adaptar muchos algoritmos criptográficos, tales como Diffie-Hellman o ElGamal. La principal ventaja de la criptografía de curva elíptica es que la claves pueden ser mucho mas pequeñas.

Dos fases de cifrado | Algoritmos de clave asimétrica

7.4.2 Firmas digitales

Las firmas manuscritas han sido utilizadas por mucho tiempo como prueba de autoría de los contenidos de un documento. Las firmas digitales pueden proporcionar las mismas funciones que las firmas manuscritas y mucho más. Por ejemplo, asuma que un cliente envía instrucciones de una transacción mediante un correo electrónico a su agente de bolsa y la transacción resulta mala para el cliente. Es concebible que el cliente pueda alegar no haber enviado nunca la orden de la transacción o que alguien fraguó su correo electrónico.

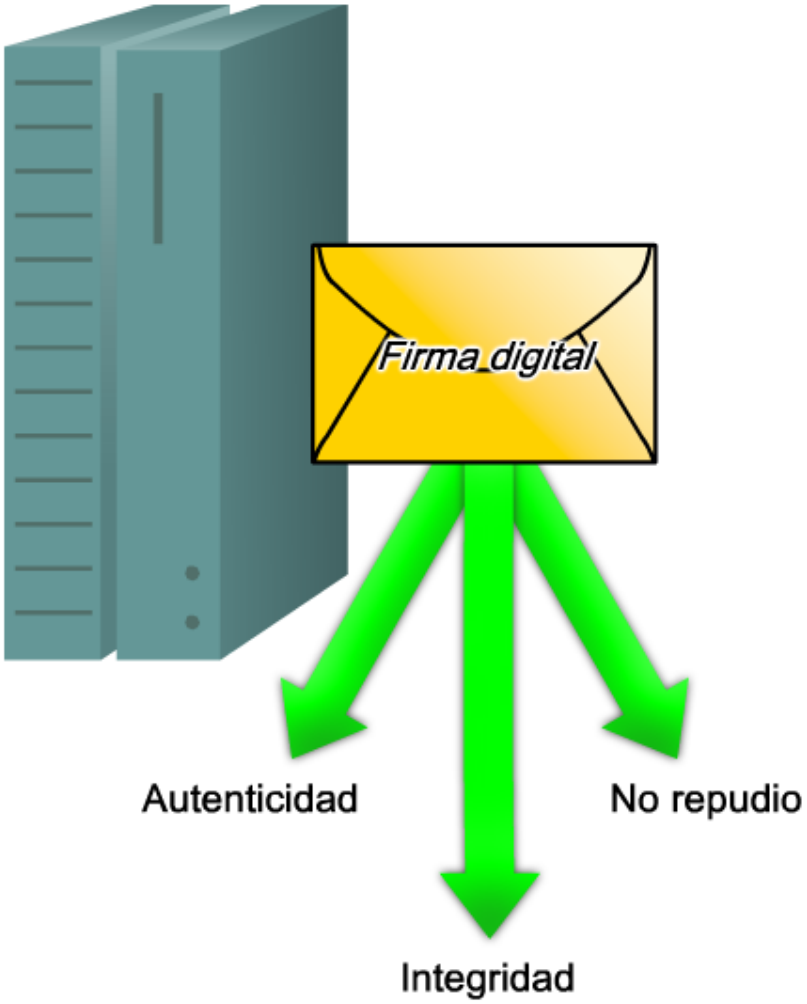
El corredor de bolsa podría protegerse exigiendo la utilización de firmas digitales antes de aceptar instrucciones por correo electrónico. De hecho, las firmas digitales son utilizadas en las siguientes situaciones:

Para proveer una prueba única del origen de los datos, los cuales sólo pueden ser generados por un único participante, tales como firmas de contratos en ambientes de comercio electrónico.
Para autenticar a un usuario, utilizando la clave privada de dicho usuario y la firma que genera.
Para probar la autenticidad e integridad de certificados PKI.
Para proveer una marca de tiempo segura utilizando una fuente de tiempo confiable.

Específicamente, las firmas digitales proveen tres servicios básicos de seguridad:

Autenticidad de los datos firmados digitalmente - Las firmas digitales autentican un origen, probando que un cierto participante ha visto y firmado los datos en cuestión.
Integridad de los datos firmados digitalmente - Las firmas digitales garantizan que los datos no han sido modificados desde el momento en que fueron firmados.
No repudio de la transacción - El destinatario puede enviar los datos de un tercero, quien acepta la firma digital como prueba de que este intercambio de datos tuvo lugar. Quien firma los datos no puede repudiar haber firmado los datos.

Para comprender mejor el no repudio, considere la utilización de funciones HMAC, las cuales además proveen garantías de autenticidad e integridad. Con las funciones HMAC, dos o más participantes comparten la misma clave de autenticación y pueden calcular la huella digital HMAC. Por lo tanto, presentar los datos recibidos junto con su huella digital HMAC ante un tercero no sirve como prueba de que el otro participante envió estos datos. Otro usuario pudo haber generado los datos con la misma huella digital HMAC, porque todos tienen una copia de la clave de autenticación HMAC. Con las firmas digitales, cada participante posee una clave de firma única y secreta, la cual no es compartida con ningún otro participante. De esta forma se vuelve posible el no repudio.



Las firmas digitales poseen propiedades específicas que permiten probar la autenticación de entidades y la integridad de los datos:

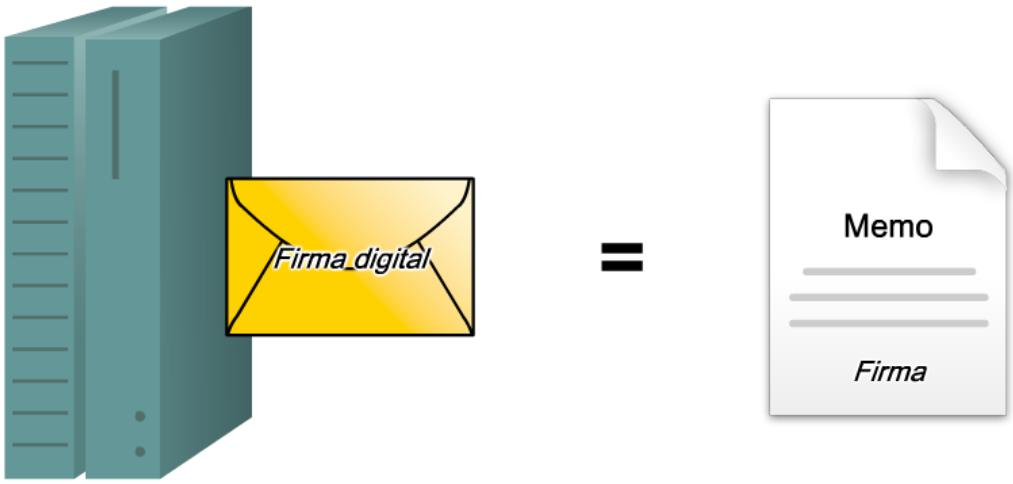
La firma es auténtica y no puede ser falseada. Es una prueba de que el firmante, nadie más, ha firmado el documento.
La firma no es reutilizable. La firma es parte del documento y no puede ser movida a un documento diferente.
La firma es inalterable. Una vez firmado un documento, éste no puede ser alterado.
La firma no puede ser repudiada. Por motivos legales, la firma y el documento son considerados objetos físicos. Los firmantes no pueden alegar luego que no fueron ellos quienes realizaron la firma.

En algunos países, incluyendo los Estados Unidos, las firmas digitales son consideradas equivalente a las firmas manuscritas, siempre y cuando cumplan con determinadas características. Algunas de estas características incluyen la protección adecuada de la autoridad de certificación, la firma confiable de todas las demás claves públicas y la protección adecuada de las claves privadas de los usuarios. Con este escenario, los

usuarios son responsables de mantener privadas sus claves privadas, porque una clave privada robada puede ser utilizada para robar su identidad.

Muchos productos Cisco utilizan firmas digitales:

Los gateways y clientes IPsec utilizan firmas digitales para autenticar sus sesiones IKE (Internet Key Exchange) si el administrador selecciona certificados digitales y el método de autenticación RSA IKE.
Los terminales SSL de Cisco, tales como los servidores Cisco IOS HTTP y el Administrador de Dispositivos de Seguridad Adaptativo de Cisco (ASDM), utilizan firmas digitales para probar la identidad del servidor SSL.
Algunos protocolos de administración de servicios orientados a voz, utilizados para su instalación y facturación, usan firmas digitales para autenticar a las partes involucradas.



Los procedimientos actuales de firma digital no son simplemente implementados durante operaciones públicas. De hecho, una firma digital moderna se basa en una función de hash y un algoritmo de clave pública.

El proceso de firma digital consta de seis pasos:

1. El dispositivo de origen (firmador) calcula un hash a partir del documento.

2. El dispositivo de origen cifra el hash con la clave privada del firmador.

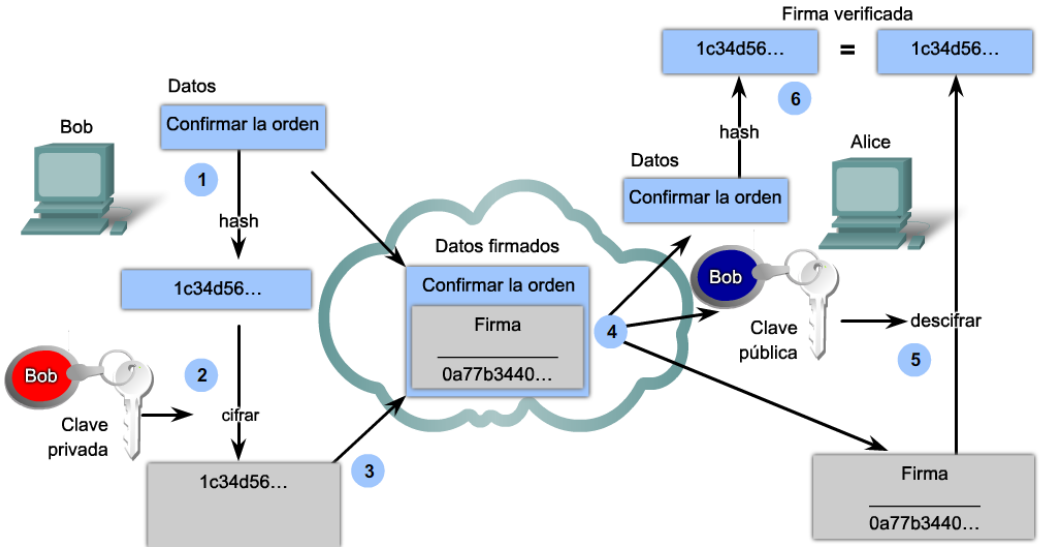
3. El hash cifrado, conocido como firma, es incorporado al documento.

4. El dispositivo de destino (verificador) acepta el documento con la firma digital y obtiene la clave pública del dispositivo de origen.

5. El dispositivo de destino descifra la firma utilizando la clave pública del dispositivo de origen. Este paso revela el valor de hash calculado por el dispositivo de origen.

6. El dispositivo de destino calcula un hash a partir del documento, sin incluir su firma y compara este hash con el hash descifrado a partir de la firma. Si ambos valores de hash coinciden, el documento es auténtico. Fue firmado por quien se supone como firmador y no ha sido modificado desde que se generó la firma.

Se requieren tanto el cifrado como las firmas digitales para asegurar que el mensaje es privado y no ha sido modificado.



Existen seis pasos en el proceso de firma digital:
1. El dispositivo de origen (firmante) crea un hash del documento.
2. El dispositivo de origen cifra el hash con su clave privada.
3. El hash cifrado, conocido como firma, se agrega al documento.
4. El dispositivo de destino (verificador) acepta el documento con la firma digital, y obtiene la clave pública del dispositivo de origen.
5. El dispositivo de destino descifra la firma utilizando la clave pública del dispositivo de origen. Este paso revela el valor de hash que se asume generado por el dispositivo origen.
6. El dispositivo de destino calcula un hash del documento recibido, sin su firma, y lo compara con el hash descifrado a partir de la firma. Si ambos coinciden, entonces el documento es auténtico, fue firmado por el origen, y no ha sido modificado desde que fue firmado.

Además de asegurar la autenticidad e integridad de los mensajes, las firmas digitales son muy utilizadas para asegurar la autenticidad e integridad del código de programas clásicos y móviles. Los archivos ejecutables o posiblemente el paquete de instalación completo de un programa, son envueltos con una firma digital, la cual permite al usuario final verificar dicha firma antes de instalar el programa.

La firma digital de código provee ciertas seguridades sobre el mismo:

El código no ha sido modificado desde que fue publicado.
El código es auténtico y fue realmente originado por quien lo publica.
Quien publica el código no puede negar esta acción. Esto provee no repudio sobre el acto de publicación.

La firma digital puede ser falseada sólo por alguien que obtenga la clave privada de quien publica el código. El nivel de seguridad de las firmas digitales es extremadamente alto si la clave privada se encuentra adecuadamente protegida.

El usuario del programa también debe obtener la clave pública, la cual es utilizada para verificar la firma. El usuario sólo puede obtener la clave de forma segura. Por ejemplo, la clave podría estar incluida con la instalación del sistema operativo o ser transferida en forma segura a través de la red.

Proteger la clave privada es uno de los elementos más importantes al utilizar firmas digitales. Si la clave de la firma de una entidad se ve comprometida, el atacante puede firmar datos en el nombre de dicha entidad y no es posible su repudio. Para intercambiar claves de verificación de forma escalable, debe utilizarse un método seguro pero accesible.



Las firmas digitales son muy utilizadas para firmar código:

- Quien publica el software agrega una firma digital al ejecutable, firmado con su propia clave de firma.
- El usuario del software necesita obtener la clave pública de su editor, o el certificado de CA del editor si se utiliza PKI.

Los algoritmos asimétricos bien conocidos, tales como RSA o DSA (Digital Signature Algorithm), son utilizados en general para realizar las firmas digitales.

DSA

En 1994, el instituto NIST de los Estados Unidos seleccionó a DSA como el Estándar de Firma Digital (DSS - Digital Signature Standard). DSA está basado en el problema del logaritmo discreto y sólo puede proveer firmas digitales.

Sin embargo, DSA ha recibido algunas críticas. Quienes lo critican aducen que DSA no posee la flexibilidad de RSA. La verificación de firmas es demasiado lenta y el proceso mediante el cual el NIST seleccionó a DSA fue demasiado secreto y arbitrario. En respuesta a estas críticas, DSS ahora incorpora dos posibles algoritmos adicionales: Criptografía de Clave Pública Reversible Utilizando Firma Digital (la cual utiliza RSA) y el Algoritmo de Firma Digital de Curva Elíptica (ECDSA - Elliptic Curve Digital Signature Algorithm).

El administrador de red debe decidir si RSA o DSA resulta más adecuado para una situación determinada. La generación de firmas DSA es más veloz que la verificación de firmas DSA. Por otro lado, la verificación de firmas en RSA es más veloz que la generación de firmas.

Características de DSA	
Descripción	Digital Signature Algorithm (DSA)
Línea de tiempo	1994
Tipo de algoritmo	Provee firmas digitales
Ventajas	La generación de firmas es rápida
Desventajas	La verificación de firmas es lenta

7.4.3 Rivest, Shamir y Alderman

RSA es uno de los algoritmos asimétricos más comunes. Ron Rivest, Adi Shamir y Len Adleman inventaron el algoritmo RSA en 1977. Se trata de un algoritmo patentado de clave pública. Su patente expiró en septiembre del año 2000 y el algoritmo es ahora del dominio público. De todos los algoritmos de clave pública que fueron propuestos a través de los años, RSA es por mucho el más sencillo de comprender e implementar.

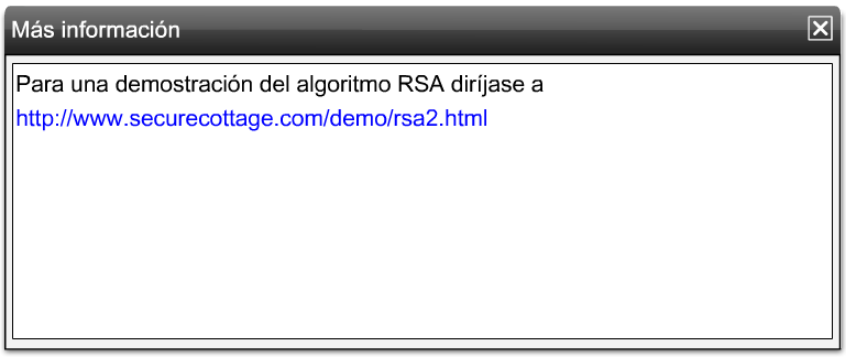
El algoritmo RSA es muy flexible porque posee una clave de longitud variable, por lo que la clave puede ser acortada para acelerar el procesamiento. A cambio, mientras más corta es la clave, menos seguro es el algoritmo.

Las claves RSA tienen por lo general entre 512 y 2048 bits de longitud. RSA ha soportado años de criptoanálisis intensivo. Aunque la seguridad de RSA nunca ha sido probada o refutada, esto sugiere cierto nivel de confianza en el algoritmo. La seguridad de RSA se basa en la dificultad de factorizar números muy grandes. En caso de descubrirse un método sencillo para factorizar estos números grandes, la efectividad de RSA se vería destruida.

El algoritmo RSA se basa en una clave pública y en una clave privada. La clave pública puede ser distribuida, pero la clave privada debe ser mantenida en secreto. No es posible determinar la clave privada a partir de la clave pública, utilizando ningún algoritmo computable y viceversa.

Las claves RSA son de largo plazo y en general son cambiadas o renovadas luego de algunos meses o incluso años. Actualmente es el método más común de generación de firmas y es ampliamente utilizado en los sistemas de comercio electrónico y protocolos de Internet.

Características de RSA	
Descripción	Ron Rivest, Adi Shamir, y Len Adleman
Línea de tiempo	1977
Tipo de algoritmo	Algoritmo asimétrico
Tamaño de la clave (en bits)	512 - 2048
Ventajas	La verificación de firmas es rápida
Desventajas	La generación de firmas es lenta



RSA implementado por hardware es unas cien veces más lento que DES, e implementado por software es unas mil veces más lento que DES. Este problema de rendimiento es la razón principal por la que RSA sólo es utilizada en general para proteger pequeñas cantidades de datos.

RSA es utilizado principalmente para asegurar la confidencialidad de los datos mediante el cifrado y para la autenticación o no repudio de los datos, o ambos, mediante la generación de firmas digitales.

7.4.4 Infraestructura de clave publica

En grandes organizaciones, no resulta práctico que todas las partes intercambien documentos de identificación continuamente. Con protocolos confiables de terceros, todos los individuos acuerdan aceptar la decisión de un tercero neutral. Se presume que dicha tercera parte realiza una investigación en profundidad previa a la emisión de las credenciales. Luego de esta investigación profunda, la tercera parte emite credenciales difíciles de falsificar. A partir de ese punto, todos los individuos que confían en esta tercera parte simplemente aceptan las credenciales que emita. Los servidores de certificados son un ejemplo de una tercera parte confiable.

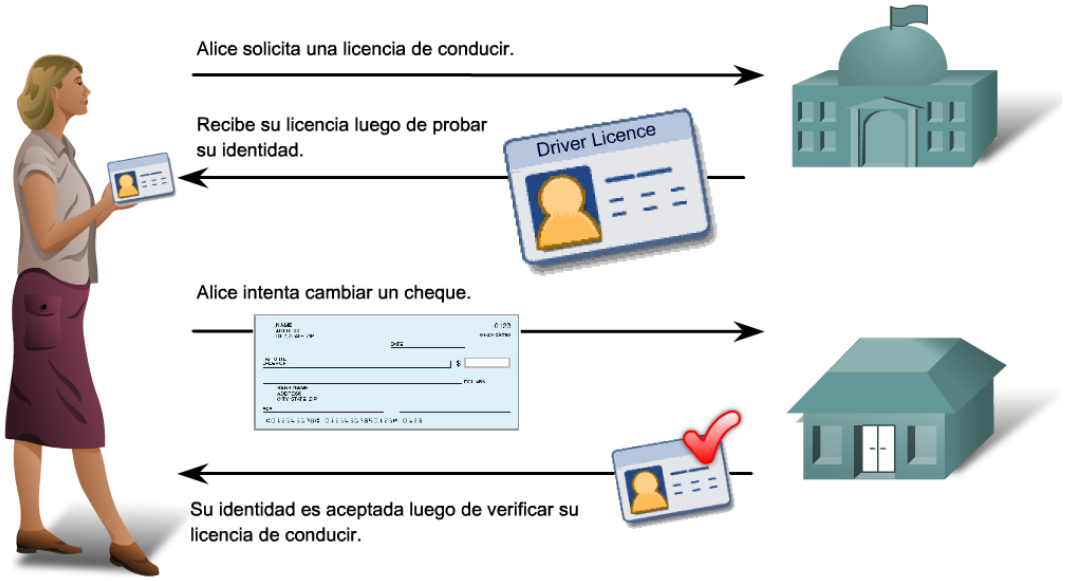
Como ejemplo, una organización grande como Cisco dedica mucho trabajo para identificar a sus empleados y contratistas y luego emite una credencial de identificación. Esta credencial es relativamente difícil de falsificar. Se toman medidas para proteger la integridad de la credencial y su emisión. Debido a estas medidas, todo el personal de Cisco acepta esta credencial como fidedigna de la identidad de cualquier individuo.

Si este método no existiera y 10 individuos necesitaran validarse entre sí, serían necesarias 90 validaciones para que todos se encuentren validados entre sí. Agregar a un único individuo al grupo requeriría unas 20 validaciones adicionales, ya que cada uno de los 10 individuos originales debe autenticar al nuevo integrante, quien a su vez debe autenticar a los 10 integrantes originales. Este método no resulta escalable.

En este otro ejemplo, asuma que Alice solicita una nueva licencia de conducir. Durante este proceso, envía evidencia de su identidad y sus calificaciones para conducir. Su solicitud es aprobada y se emite la nueva licencia. Más tarde, Alice necesita cambiar un cheque en el banco. Al presentar el cheque al cajero, éste le solicita una identificación. El banco, debido a que confía en la agencia gubernamental que emitió la licencia de conducir, verifica su identidad y le paga el cheque.

Los servidores de certificados funcionan como la oficina de licencias de conducir. La licencia es una analogía del certificado en una Infraestructura de Clave Pública (PKI - Public Key Infrastructure) u otra tecnología que soporte certificados.

¿Cómo funciona realmente PKI?



PKI es el framework de servicios necesario para soportar tecnologías basadas en clave pública de gran escala. PKI soporta soluciones muy escalables y se está volviendo una solución de autenticación muy importante para las VPNs.

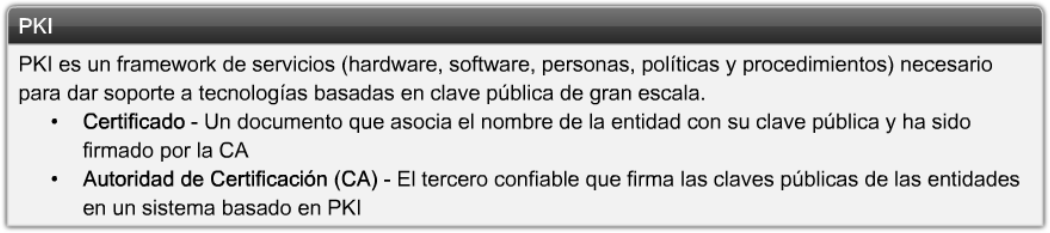
PKI consiste en un conjunto de componentes técnicos, organizativos y legales, necesarios para establecer un sistema que permita la utilización a gran escala de criptografía de clave pública, con el fin de proveer servicios de autenticación, confidencialidad, integridad y no repudio. El framework PKI está conformado por el hardware, el software, las personas, las políticas y los procedimientos necesarios para crear, administrar, almacenar, distribuir y revocar los certificados digitales.

Deben definirse dos términos muy importantes al referirse a PKI: certificados y Autoridad de Certificación (CA - Certificate Authority).

Los certificados son utilizados con diferentes fines en una red. Los certificados son información pública. Contienen el enlace entre los nombres y las claves públicas de las entidades y usualmente son publicados en un directorio centralizado para que otros usuarios de la PKI tengan acceso a ellos.

La CA es una entidad confiable que emite los certificados. El certificado de un usuario siempre está firmado por una CA. Cada CA además posee un certificado que contiene su clave pública, firmado por sí mismo y denominado Certificado de CA o, más adecuadamente, Certificado auto-firmado de CA.

Un solo servidor de CA puede dar servicios a muchas aplicaciones que requieran certificados digitales con fines de autenticación. Utilizar servidores de CA es una solución que simplifica la administración de la autenticación y además provee una seguridad fuerte debido a la fortaleza de los mecanismos criptográficos utilizados en combinación con los certificados digitales.



PKI es más que sólo un CA y sus usuarios. Además de implementar esta tecnología, construir una PKI grande involucra mucho trabajo organizativo y legal. Existen cinco componentes principales de una PKI:

Usuarios de la PKI, los cuales pueden ser personas, dispositivos y servidores
CAs para la administración de claves
Almacenamiento y protocolos
Un marco de trabajo organizativo de soporte, conocido como autenticación de prácticas y usuarios utilizando LRAs (Local Registration Authorities)
Marco legal de soporte

Muchos vendedores ofrecen servidores CA como un servicio administrado o como un producto de usuario final, incluyendo VeriSign, Entrust Technologies, RSA, CyberTrust, Microsoft y Novell. Las CAs, especialmente aquellas subcontratadas, pueden emitir certificados de diversas clases, lo que determina qué tan confiable es un certificado. Un único vendedor del servicio, como puede ser VeriSign, puede utilizar una única CA, emitiendo certificados de diferentes clases y sus clientes utilizan la CA de acuerdo al nivel de confianza deseado o requerido.

Una clase de certificado suele identificarse con un número. Mientras mayor sea el número, más confiable resulta el certificado. La confianza en un certificado suele estar determinada por lo riguroso del procedimiento utilizado para verificar la identidad del titular al momento de su emisión:

La Clase 0 tiene fines de pruebas solamente, por lo que no se han realizado verificaciones.
La Clase 1 es para individuos que se enfocan en la verificación del correo electrónico.
La Clase 2 es para organizaciones que requieran una prueba de identidad.
La Clase 3 es para la firma de servidores y programas, para los cuales la CA que emite el certificado realiza verificaciones y pruebas de identidad y autoridad independientes.
La Clase 4 es para transacciones de comercio electrónico entre empresas.
La Clase 5 es para organizaciones privadas o seguridad gubernamental.

Por ejemplo, un certificado de clase 1 puede requerir una respuesta por correo electrónico de su titular para confirmar la acción de enrolarse. Este tipo de confirmación es una autenticación débil del titular. Para un certificado de clase 3 o 4, el futuro titular debe probar su identidad y autenticar la clave pública presentándose en persona con al menos dos documentos de identificación oficiales.

VeriSign

http://www.verisign.com

Entrust
Securing Digital Identities & Information

http://www.entrust.com

cybertrust
certified perimeter

http://www.verizonbusiness.com/

Novell

http://www.novell.com

RSA
The Security Division of EMC

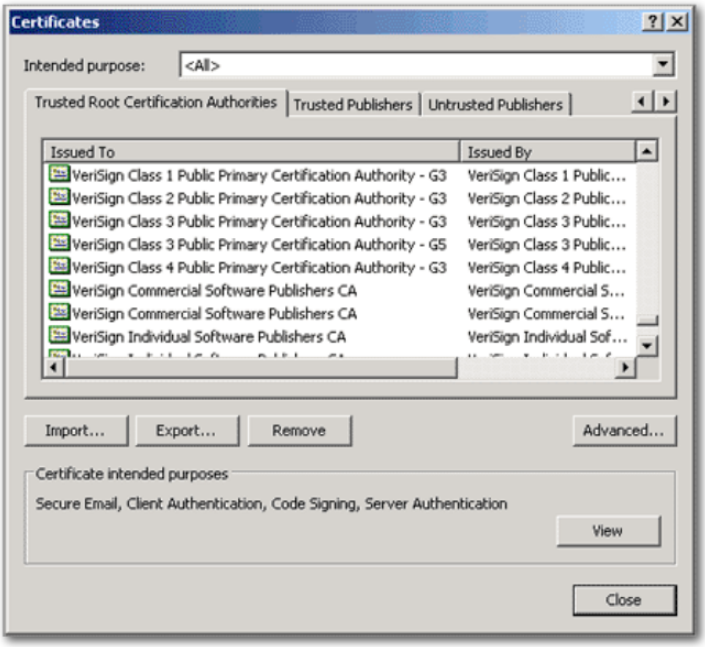
http://www.rsa.com/

Microsoft

http://www.microsoft.com

Proveedores de CA

Ejemplo de certificados Verisign



Proveedores de CA

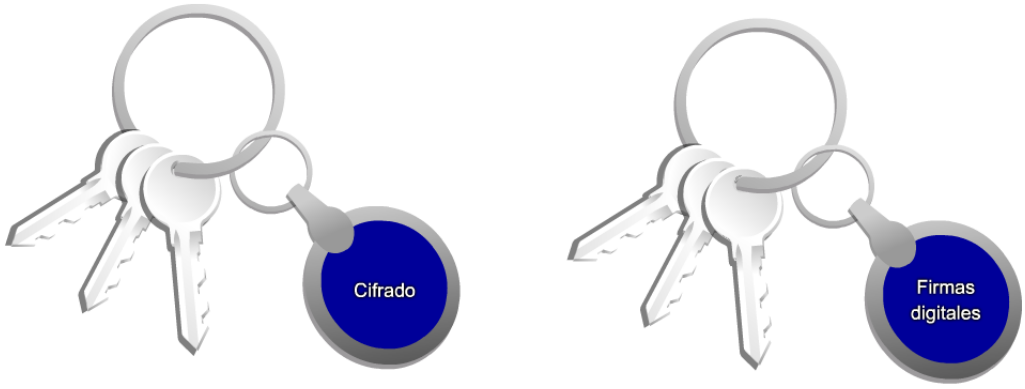
Ejemplo de certificados Verisign

Algunas PKIs ofrecen la posibilidad, o incluso requieren el uso, de dos pares de claves por entidad. El primer par de claves pública y privada se utilizan sólo para operaciones de cifrado. La clave pública cifra los datos y la clave privada los descifra. El segundo par de claves pública y privada se utilizan en operaciones de firma digital. La clave privada genera la firma y la clave pública la verifica.

Estas claves también son llamadas claves de uso o claves especiales. Pueden diferir en su longitud o incluso en la selección del algoritmo de clave pública. Si la PKI requiere dos pares de claves por entidad, el usuario entonces posee dos certificados: un certificado de cifrado con la clave pública del usuario, que se utiliza para cifrar datos, y un certificado de firma con la clave pública del usuario, que se utiliza para verificar la firma digital del usuario.

Los siguientes son escenarios típicos que emplean claves de uso:

Cuando se utiliza un certificado de cifrado con más frecuencia que un certificado de firma, el par de claves pública y privada está más expuesto debido a su uso frecuente. En este caso, puede resultar una buena idea acortar el tiempo de vida del par de claves y modificarlo con más frecuencia, mientras el par de claves privada y pública utilizado para la firma digital se mantiene por un tiempo mayor.
Cuando se requieren diferentes niveles de cifrado y firma digital debido a requisitos legales, de exportación o de desempeño, las claves de uso permiten al administrador asignar diferentes longitudes a cada uno de los dos pares.
Cuando se desea recuperar claves, como en el caso de que la clave privada del usuario sea almacenada en un repositorio central por motivos de respaldo. Las claves de uso permiten al usuario respaldar sólo la clave privada del par de cifrado. La clave privada de firma permanece siempre con el usuario, permitiendo un verdadero no repudio.



7.4.5 Estándares PKI





El borrador e información adicional sobre PKI se encuentran disponibles en http://www.ietf.org.

La estandarización e interoperabilidad de diferentes proveedores de PKI es todavía un problema al interconectar diferentes PKIs. La interoperabilidad entre una PKI y sus servicios de soporte, tales como LDAP (Lightweighted Directory Access Protocol) y directorios X.500, es una preocupación, debido a que muchos proveedores han propuesto e implementado soluciones propietarias en lugar de esperar al desarrollo de estándares. El estado de la interoperabilidad es muy básico, incluso luego de 10 años de desarrollo de programas para PKI.

Para tratar este problema de interoperabilidad, la IETF formó un grupo de trabajo denominado PKIX (Public-Key Infrastructure X.500), dedicado a promocionar y estandarizar PKI en Internet. Este grupo de trabajo ha publicado el borrador de un conjunto de estándares, X.509, detallando formatos comunes de datos y protocolos relacionados a PKI en una red.

X.509 es un estándar bien conocido que define los formatos básicos de PKI, tales como el formato de certificado y el formato de la lista de revocación de certificados (CRL - Certificate Revocation List), con el fin de permitir una interoperabilidad básica. El estándar ha sido ampliamente utilizado durante años en muchas aplicaciones de Internet, tales como SSL e IPsec.

El estándar X.509 versión 3 (X.509v3) define el formato de un certificado digital. Los certificados eran utilizados tradicionalmente al nivel de capa de aplicación para ofrecer una autenticación fuerte a las aplicaciones. Cada aplicación puede tener una implementación diferente del proceso de autenticación, pero todas utilizan un tipo de certificado similar, con el formato X.509.

Este formato ya es utilizado de forma extensiva en la infraestructura de Internet:

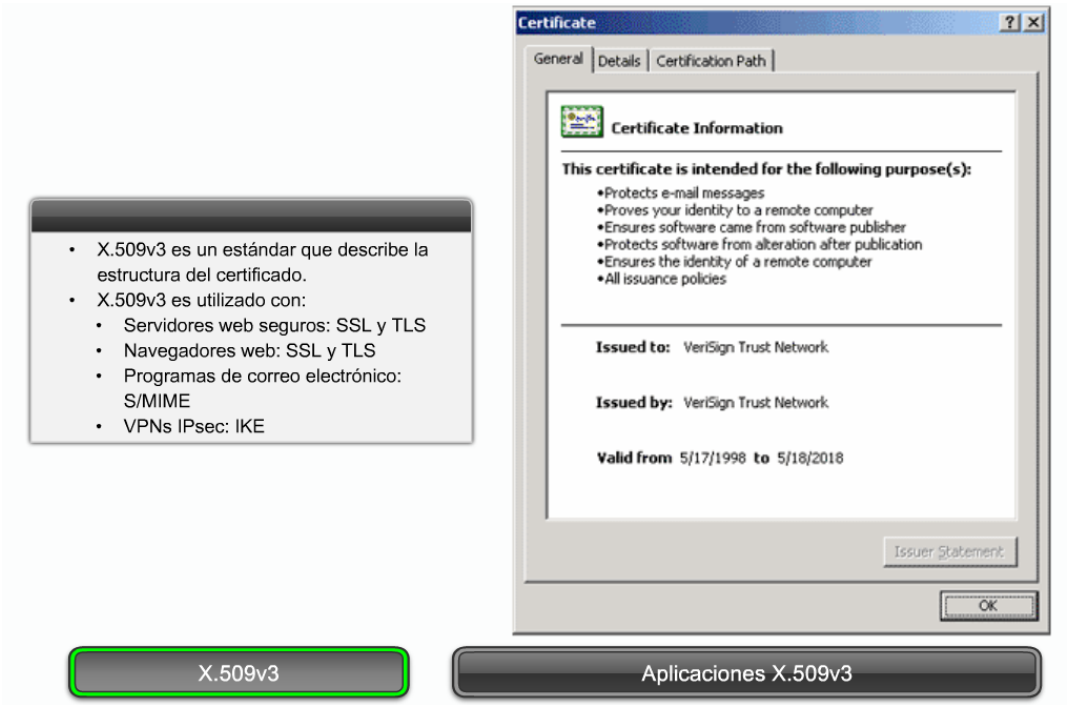
Los servidores web seguros utilizan X.509v3 para la autenticación de sitios web con los protocolos SSL y TSL.
Los navegadores web utilizan X.509v3 para implementar los certificados de cliente HTTPS con el protocolo SSL. SSL es la autenticación basada en certificados más utilizada a nivel mundial. Otras aplicaciones bien conocidas, tales como SMTP (Simple

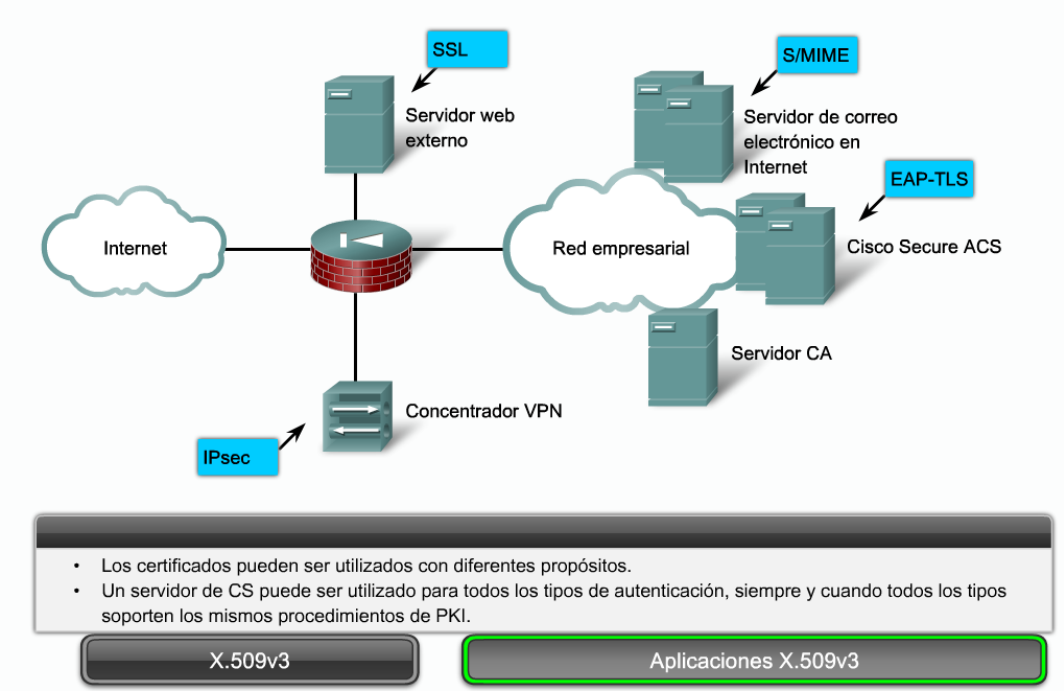
Mail Transfer Protocol), LDAP y POP3 (Post Office Protocol versión 3), que utilizaban autenticaciones débiles y no cifraban los datos, fueron modificadas para utilizar SSL.
Los clientes de correo electrónico de los usuarios, que soportan protección de los correos electrónicos mediante el protocolo S/MIME (Secure/Multipurpose Internet Mail Extensions), utilizan X.509.
Las VPNs IPsec, en las que los certificados pueden ser utilizados como un mecanismo de distribución de claves públicas para la autenticación basada en RSA IKE, utilizan X.509.
PGP (Pretty Good Privacy) es una aplicación desarrollada originalmente por Phil Zimmerman, un defensor de la privacidad, para que los usuarios finales pudieran entablar comunicaciones confidenciales utilizando el cifrado. El uso más frecuente de PGP es asegurar el correo electrónico. PGP también reconoce el certificado X.509.

Los certificados son también utilizados por los dispositivos de red en las capas de red o aplicación. Los routers Cisco, concentradores Cisco VPN y firewalls Cisco PIX pueden utilizar certificados para autenticar los pares IPsec.

Los switches Cisco pueden utilizar certificados para autenticar dispositivos finales conectados a los puertos LAN. La autenticación utiliza 802.1X entre los dispositivos adyacentes y puede ser derivada a un ACS central mediante EAP-TLS (Extensible Authentication Protocol con TLS).

Los routers Cisco también pueden proporcionar soporte TN3270, el cual no incluye cifrado o autenticación fuerte. Los routers Cisco pueden ahora utilizar SSL para establecer sesiones TN3270 seguras.





Otro estándar PKI importante es PKCS (Public-Key Cryptography Standards). PKCS se refiere a un grupo de estándares criptográficos de clave pública diseñados y publicados por RSA Laboratories. PKCS provee interoperabilidad básica a aplicaciones que utilizan criptografía de clave pública. PKCS define los formatos de bajo nivel para el intercambio seguro de datos arbitrarios, tales como datos cifrados o firmados.

Como lo indica el sitio web de RSA Laboratories, "Los estándares de criptografía de clave pública sin especificaciones producidas por RSA Laboratories en cooperación con desarrolladores de sistemas seguros de todo el mundo, con el propósito de acelerar la implementación de la criptografía de clave pública".

Estándares PKCA RSA:

- **PKCS #1:** Estándar de Criptografía RSA
- **PKCS #3:** Estándar de Acuerdo de Llaves DH
- **PKCS #5:** Estándar de Criptografía Basada en Contraseña
- **PKCS #6:** Estándar de Sintaxis de Certificado Extendido
- **PKCS #7:** Estándar de Sintaxis de Mensaje Criptográfico
- **PKCS #8:** Estándar de Sintaxis de Clave Privada
- **PKCS #10:** Estándar de Sintaxis de Solicitud de Certificado
- **PKCS #12:** Estándar de Sintaxis de Intercambio de Información Personal
- **PKCS #13:** Estándar de Criptografía de Curva Elíptica
- **PKCS #15:** Estándar de Formato de Información del Token Criptográfico

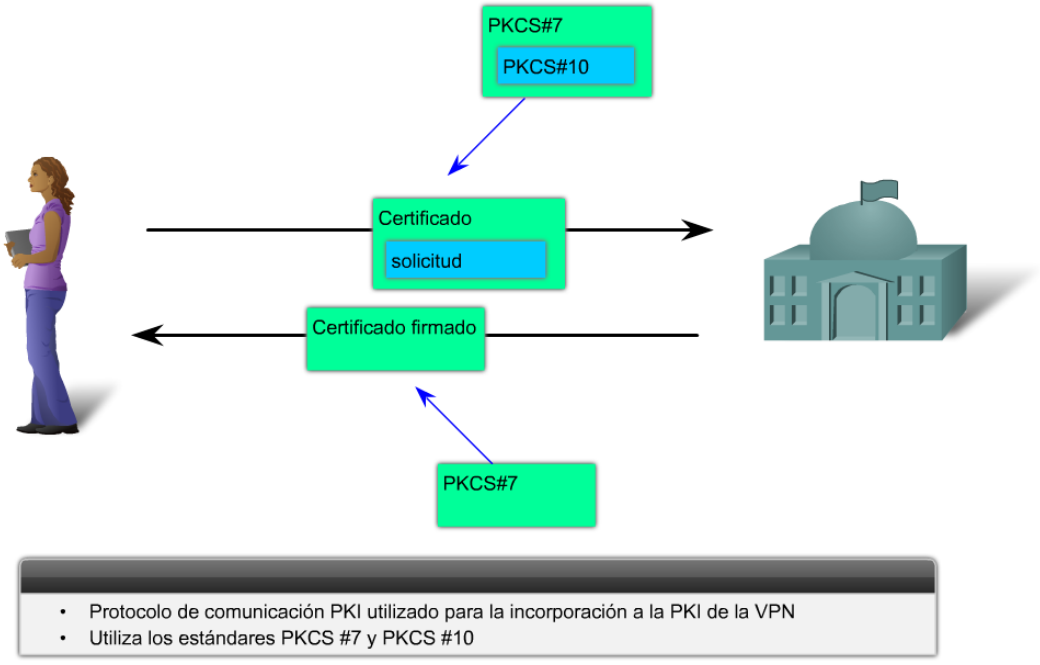
El uso de la tecnología de clave pública ha crecido en forma incremental y se ha vuelto la base de la seguridad basada en estándares, como en el caso de los protocolo IKE e IPsec. Con el uso de los certificados de clave pública en los protocolos de seguridad de red, llega la necesidad de un protocolo de administración de certificados para los clientes PKI y los servidores CA. Estos clientes y servidores pueden soportar operaciones de ciclo de vida de los certificados, tales como incorporación y revocación de certificados y acceso a certificados y a la CRL.

Por ejemplo, una entidad comienza una transacción de incorporación creando una solicitud de certificado utilizando PKCS #10 (estándar de sintaxis de solicitud de certificado) y la envía a la CA, la cual está implementada utilizando PKCS #7 (estándar de sintaxis de mensaje cifrado). Una vez que la CA recibe la solicitud, puede realizar una de estas tres funciones:

Aprobar automáticamente la solicitud.
Enviar el certificado de vuelta.
Forzar a la entidad a esperar hasta que el operador pueda autenticar de forma manual la identidad de quien realizó la solicitud.

El objetivo final es que cualquier usuario de la red sea capaz de solicitar un certificado digital de forma fácil y electrónica. Previamente, estos procesos requerían un ingreso intensivo de datos por parte de los administradores de la red y no resultaban apropiados para implementaciones en gran escala. La IETF diseñó SCEP (Simple Certificate Enrollment Protocol) para hacer que la emisión y revocación de certificados digitales sea lo más escalable posible. El objetivo de SCEP es soportar la emisión segura de certificados a dispositivos de red en forma escalable, utilizando la tecnología existente en la medida de lo posible.

SCEP es ahora utilizado por fabricantes de equipamiento de red y compañías de software, quienes desarrollan métodos simplificados de administración de certificados en implementaciones a gran escala para usuarios finales.



7.4.6 Autoridades de Certificación

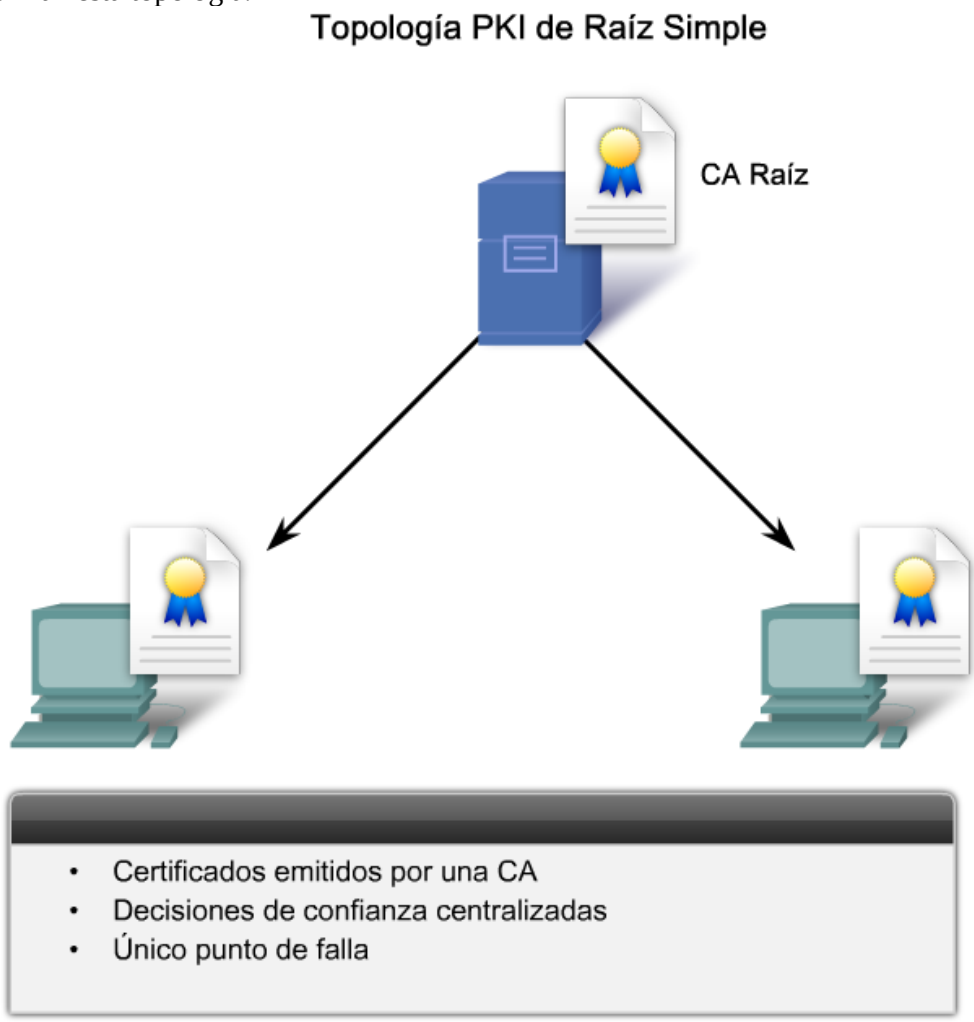
Las PKIs pueden formar diferentes topologías de confianza, incluyendo incluyendo topologías PKI de raíz simple (single-root), topologías CA jerárquicas y topologías CA de certificación cruzada (cross-certified).

Topología PKI de raíz simple

En el modelo PKI de raíz simple, una única CA, también conocida como CA raíz, emite todos los certificados a los usuarios finales. El beneficio es la simplicidad. Sin embargo, existen las siguientes desventajas:

Resulta difícil de escalar a un ambiente grande.
Requiere una administración estrictamente centralizada.
Utilizar una única clave de firma privada conlleva una vulnerabilidad crítica. Si la clave es robada, toda la PKI se desmoronará, ya que no es posible seguir confiando en la CA como único firmador.

Debido a su simplicidad, las VPNs administradas por una sola organización a menudo utilizan esta topología.



Topología CA jerárquica

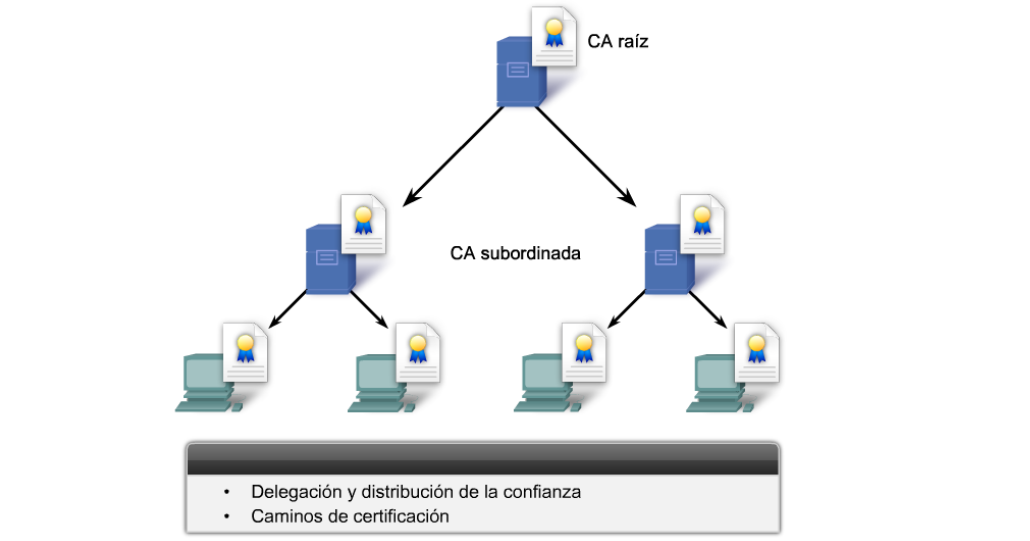
Dejando de lado las CA de raíz simple, las topologías más complejas involucran múltiples CAs dentro de la misma organización. En las topologías jerárquicas, las CAs pueden emitir certificados a usuarios finales y a CAs subordinadas, las cuales a su vez emiten certificados a usuarios finales, otras CAs o ambos. De esta forma, el árbol de CAs y usuarios finales se construye de forma tal que cada CA puede emitir certificados a CAs de niveles inferiores y usuarios finales.

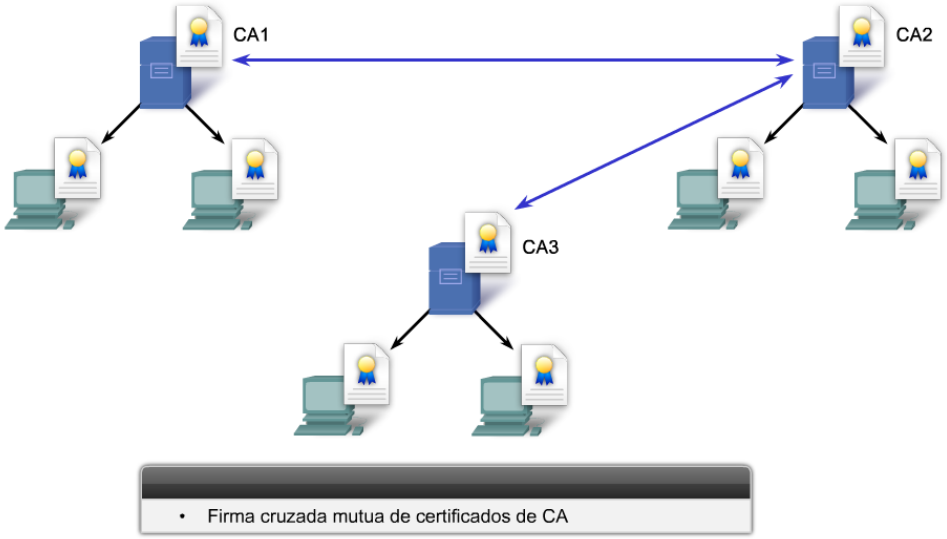
Los beneficios principales de una topología PKI jerárquica son las mejoras en la escalabilidad y la administración. Las decisiones de confianza pueden ser ahora distribuidas de forma jerárquica a ramas más pequeñas. La distribución funciona bien en la mayoría de las organizaciones grandes. Por ejemplo, una gran compañía puede tener una CA raíz, la cual emite los certificados a las CAs de nivel 2. Estas CAs de nivel 2 emiten a su vez los certificados a los usuarios finales. Debido a que la clave de firma raíz es poco utilizada una vez que se emitieron los certificados a las CAs subordinadas, dicha clave está menos expuesta y por lo tanto es más confiable. Además, si la clave de una CA subordinada es robada, sólo una rama de la PKI se vuelve no confiable.

Un problema de las topologías PKI jerárquicas es encontrar el camino de certificación para un certificado determinado. Puede resultar difícil determinar la cadena en el proceso de firmas. Esta tarea aumenta en dificultad a medida que más CAs se agregan entre la CA raíz y el usuario final.

Topología CA de certificación cruzada

Otro enfoque de las PKIs jerárquicas son las denominadas CA de certificación cruzada. En esta implementación, un conjunto de CAs de raíz simple establece relaciones horizontales de confianza mediante la intercambiando en forma cruzada sus certificados de CA propios.





CA jerárquica | CA de certificación cruzada

Haga clic sobre cada botón para ver el contenido asociado.

Dado que las PKIs son jerárquicas por naturaleza, la autoridad de certificación que emite un certificado puede ser una CA raíz (la CA de nivel superior en la jerarquía) o bien una CA subordinada. La PKI puede utilizar hosts adicionales, llamados autoridades de registro (RAs) para aceptar pedidos de inscripción en la PKI. Las RAs son empleadas para recudir la carga de trabajo de las CAs en un ambiente que soporta un gran número de transacciones de certificación o cuando la CA se encuentra fuera de línea.

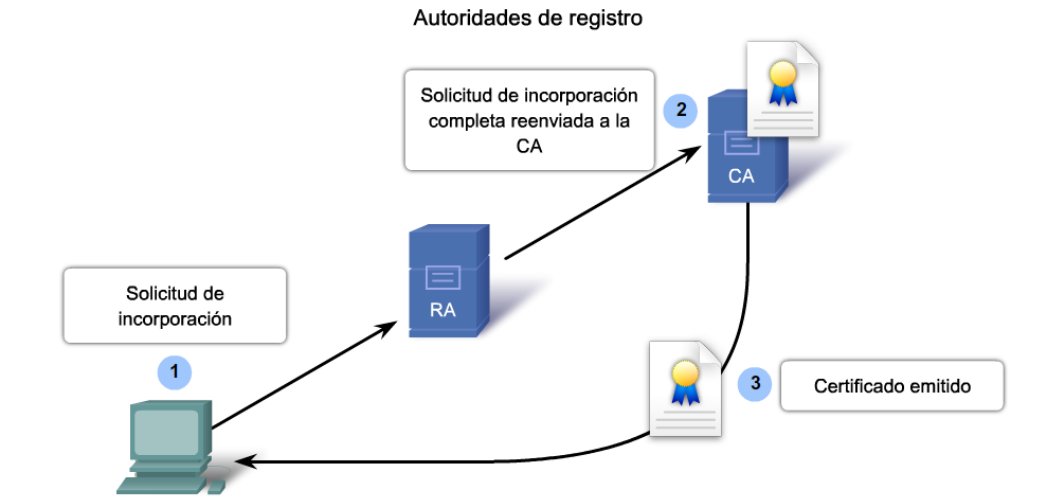
En un ambiente más complejo, puede asignarse a la RA las tareas de verificar la identidad del usuario, establecer contraseñas para las transacciones de administración de certificados, enviar solicitudes de inscripción junto con los atributos organizacionales apropiados u otra información de la CA y resolver otras tareas tales como la revocación de certificados y la re-inscripción.

Por lo general, las siguientes tareas son derivadas a la RA:

Autenticación de usuarios al momento de registrarse en la PKI
Generación de claves para usuarios que no pueden generar sus propias claves
Distribución de certificados luego de la registración

Es importante notar que la RA sólo tiene el poder de aceptar solicitudes de registración y enviarlas a la CA. No tiene permitida la emisión de certificados o la publicación de CRLs. La CA es responsable de estas funciones.

¿Cómo se recuperan, registran y utilizan los certificados?



1. Los hosts envían las solicitudes de certificados a la RA.
2. Una vez que la Autoridad de Registro incorpora información específica a la solicitud de certificado, y la misma es aprobada de acuerdo a la política de la organización, la solicitud es reenviada al a Autoridad de Certificación.
3. La CA firma la solicitud del certificado y la envía de vuelta al host.

En el procedimiento de autenticación de CA, el primero paso del usuario al contactar la PKI es obtener en forma segura una copia de la clave pública de la CA. Dicha clave pública verifica todos los certificados emitidos por la CA y resulta vital para la operación apropiada de la PKI.

La clave pública, llamada certificado auto-firmado, también es distribuida en la forma de un certificado emitido por la CA misma. Sólo la CA raíz emite un certificado auto-firmado.

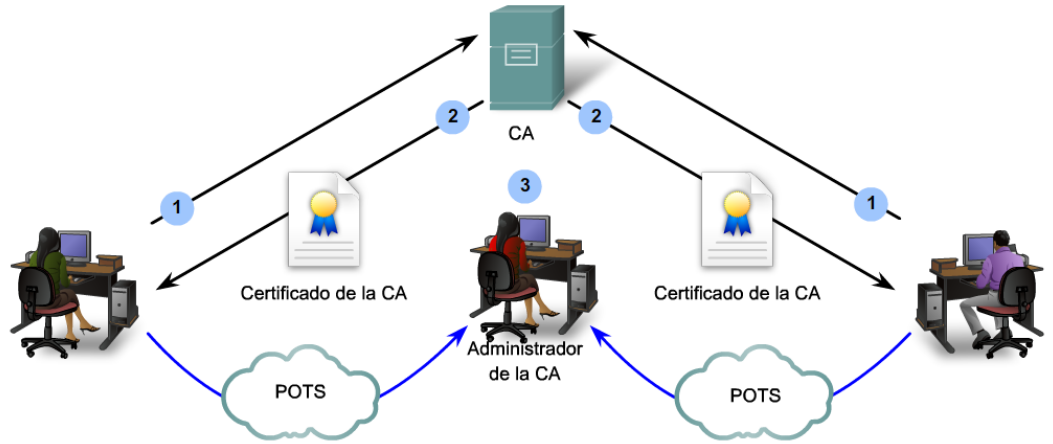
Para comprender mejor cómo son recuperados los certificados de la CA, considere este ejemplo:

1. Alice y Bob solicitan un certificado a la CA, el cual contiene la clave pública de la CA.

2. Al recibir el certificado de la CA, cada uno de los sistemas que lo solicitaron verifican la validez del certificado utilizando criptografía de clave pública.

3. Alice y Bob finalizan la verificación realizada por sus sistemas, telefoneando al administrador de la CA y verificando la clave pública y número de serie del certificado.

Los certificados de la CA son recuperados a través de la red y la autenticación se realiza por fuera de la red, utilizando el teléfono.



1. Alice y Bob solicitan el certificado de la CA que contiene la clave pública de la CA.
2. Una vez recibido el certificado de la CA, cada sistema (de Alice y Bob) verifica la validez del certificado utilizando criptografía de clave pública.
3. Alice y Bob continúan con la verificación técnica realizada por sus sistemas, telefoneando al administrador de la CA y verificando la clave pública y el número de serie del certificado.

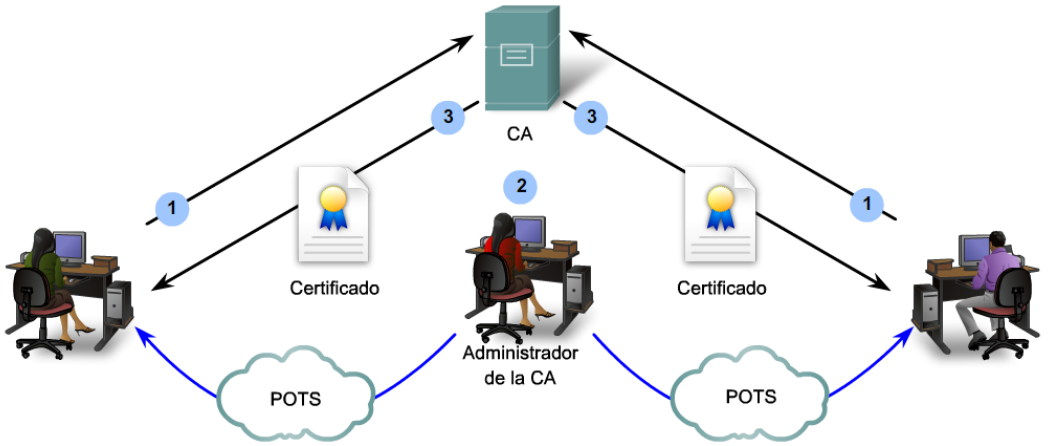
7.4.7 Certificados Digitales y CAs

Una vez obtenido el certificado de la CA, Alice y Bob envían solicitudes de certificados a la CA:

1. Ambos sistemas envían una solicitud de certificado cada uno, incluyendo su clave pública junto con cierta información de identificación. Toda la información es cifrada utilizando la clave pública de la CA.

2. Al recibir las solicitudes de certificados en el servidor de la CA, el administrador de la CA realiza un llamado telefónico a Alice y a Bob para confirmar sus solicitudes y las claves públicas. El administrador de la CA emite los certificados agregando cierta información adicional a las solicitudes recibidas y firmando todo el conjunto.

3. Luego, cada usuario final obtiene en forma manual su certificado o bien SCEP lo obtiene en forma automática. Finalmente, el certificado es instalado en el sistema.



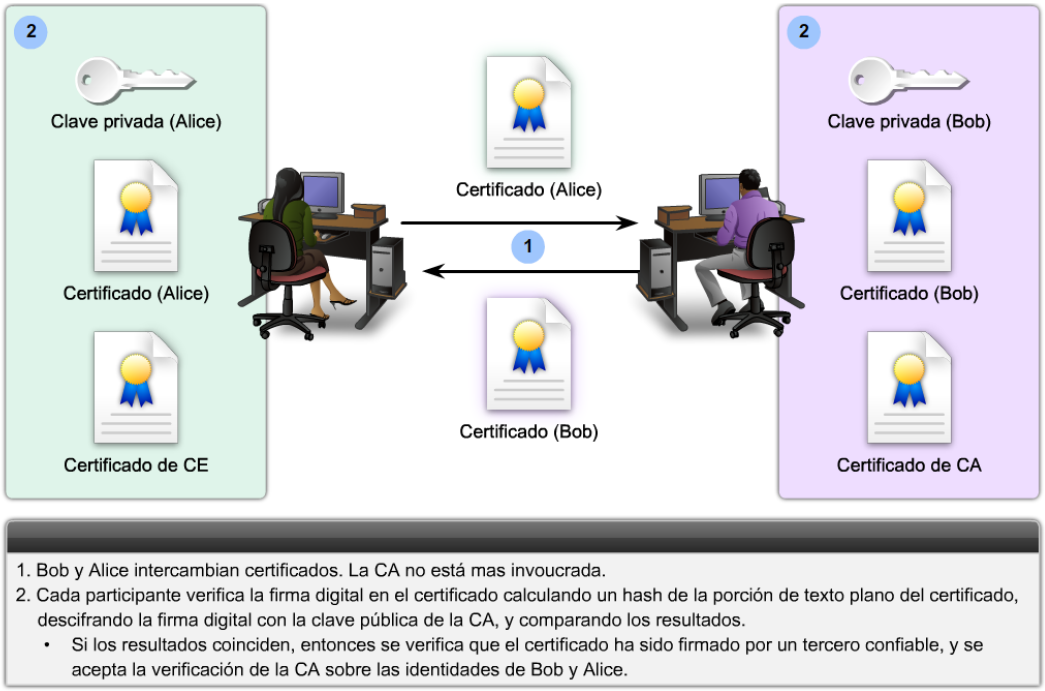
1. Ambos sistemas envían una solicitud de certificado, la cual incluye sus claves públicas junto con cierta información de identificación. Toda esta información es cifrada utilizando la clave pública de la CA.
2. Una vez recibida la solicitud, el administrador de la CA telefonea a Alice y Bob para confirmar el envío y la clave pública, y emite el certificado agregando datos adicionales a la solicitud, y firmando todo el conjunto.
3. Finalmente, cada usuario final puede rescargar el certificado en forma manual, o el SCEP lo hace en forma automática. Luego, el certificado se instala en el sistema.

Habiendo instalado certificados firmados por la misma CA, Bob y Alice están ahora listos para autenticarse entre sí:

1. Bob y Alice intercambian certificados. La CA ya no está involucrada.

2. Cada participante verifica la firma digital del certificado calculando un hash sobre la porción de texto plano del mismo, descifrando la firma digital utilizando la clave pública de la CA y comparando los resultados. Si coinciden, se verifica que el certificado haya sido firmado por un tercero confiable y se obtiene la confirmación de la CA sobre la identidad de Bob y Alice.

La autenticación ya no requiere la presencia del servidor de la CA y los usuarios intercambian sus certificados con las claves públicas.



PKI como mecanismo de autenticación posee diferentes características:

Para autenticarse entre sí, los usuarios deben obtener el certificado de la CA y sus propios certificados. Estos pasos requieren una autenticación por fuera de la red. Una vez realizada esta verificación, la presencia de la CA no es necesaria nuevamente hasta que alguno de los certificados involucrados expire.
Los sistemas de clave pública utilizan claves asimétricas en las que una clave es pública y la otra es privada. Una de las características de estos algoritmos consiste en que los datos cifrados con una clave sólo pueden ser descifrados con la otra. Esto provee el no repudio.
La administración de claves se ve simplificada, ya que los usuarios pueden intercambiar sus certificados con libertad. La validez de los certificados recibidos se verifica utilizando la clave pública de la CA, la cual debe ser conocida por los usuarios.
Debido a la fortaleza de los algoritmos involucrados, los administradores pueden configurar un tiempo de vida extenso para los certificados, el cual suele medirse en años.

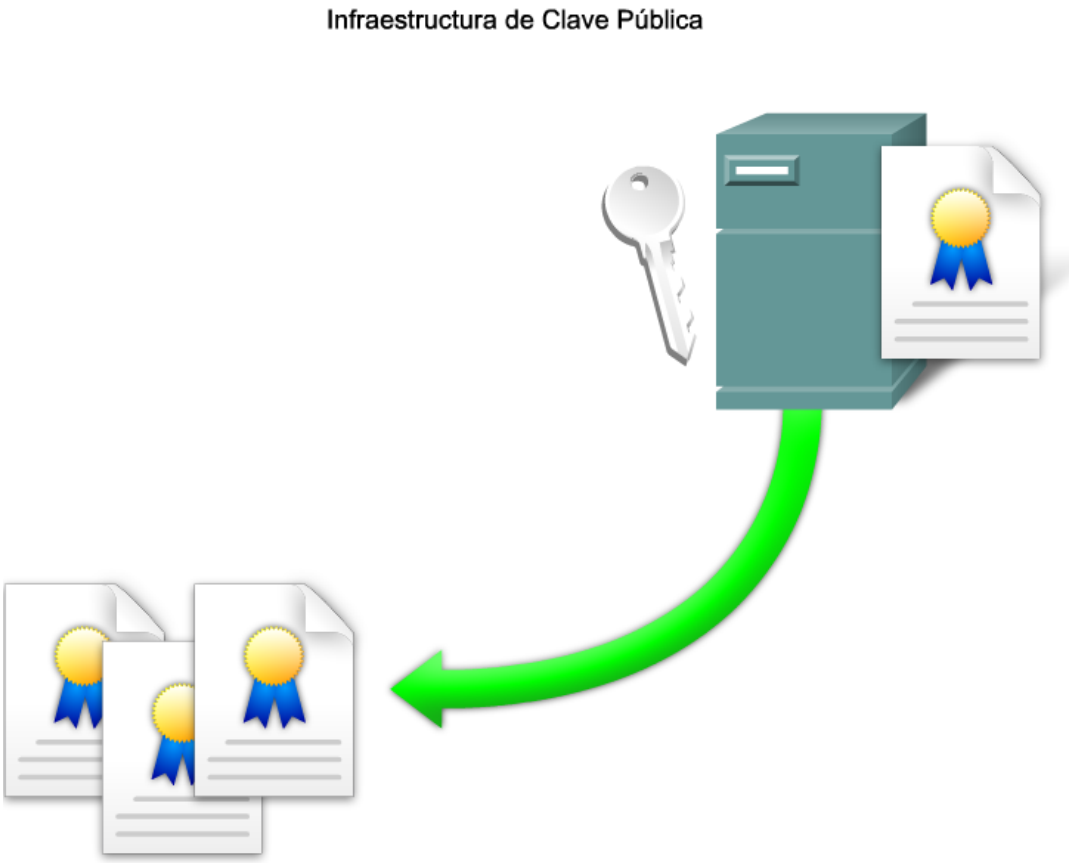
Las siguientes son desventajas de utilizar terceros confiables relacionadas con la administración de las claves:

El certificado de un usuario se ve comprometido (la clave privada ha sido robada).
El certificado de la CA ha sido comprometido (la clave privada ha sido robada).
El administrador de la CA cometió un error (factor humano).

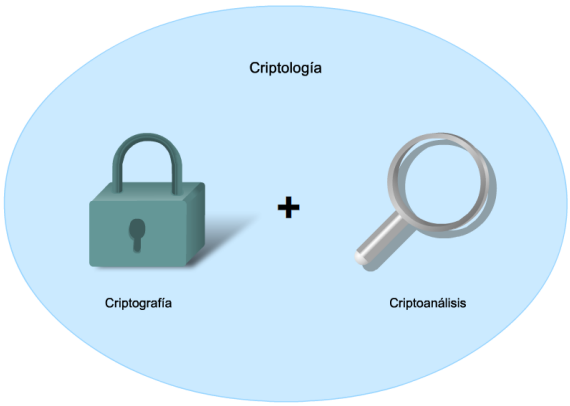
El tipo de PKI a implementar varía dependiendo de las necesidades de la organización. Puede ser necesario que los administradores combinen la autenticación de clave pública con otro mecanismo de autenticación para incrementar el nivel de seguridad y así proveer más opciones de autorización. Por ejemplo, implementar IPsec utilizando

certificados para la autenticación y XAUTH (Extended Authentication) con contraseñas de único uso creadas con tokens de hardware conforma un esquema de autenticación superior si se lo compara con el solo uso de certificados.

Cualquiera sea la elección del administrador, la implementación PKI debe basarse en los requisitos especificados en la política de seguridad de la red.



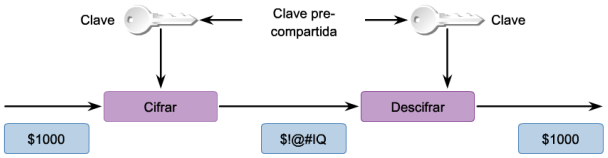
7.5.1 Resumen del Capitulo



- Las comunicaciones seguras requieren integridad, autenticación, y confidencialidad.
- La Criptografía se relaciona con el desarrollo y la utilización de métodos de cifrado.
- El Criptoanálisis se relaciona con la solución o la ruptura de un método de cifrado criptográfico.
- La Criptología es la combinación de la Criptografía y el Criptoanálisis.

- Los hashes criptográficos juegan un rol importante al asegurar el tráfico de una red.
- La integridad es proporcionada utilizando el algoritmo MD5 o el algoritmo SHA-1.
- La autenticidad es provista utilizando HMAC.
- La confidencialidad se logra utilizando varios algoritmos de cifrado.

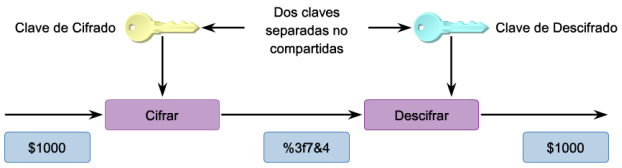
	Integridad	Autenticación	Confidencialidad
Hashes, protocolos y algoritmos criptográficos	MD5 SHA	HMAC-MD5 HMAC-SHA-1 RSA y DSA	DES 3DES AES



- Los algoritmos de cifrado simétrico son mejor conocidos como algoritmos de clave secreta compartida.
- La longitud de clave usual tiene entre 80 y 256 bits.
- El remitente y el destinatario deben compartir una clave secreta.
- Son en general miu rápidos (velocidad de transmisión) debido a que estos algoritmos se basan en operaciones matemáticas simples.
- Ejemplos de algoritmos de cifrado simétrico son DES, 3DES, AES, IDEA, RC2/4/5/6, y Blowfish.

Cifrado Simétrico | Cifrado Asimétrico

- El cifrado puede implementarse utilizando un algoritmo simétrico o asimétrico.
- Pueden utilizarse varios algoritmos de cifrado simétrico. Cada opción varía de acuerdo al grado de protección y su facilidad de implementación.
- Diffie-Hellman es un algoritmo de hashing utilizado para soportar DES, 3DES, y AES.

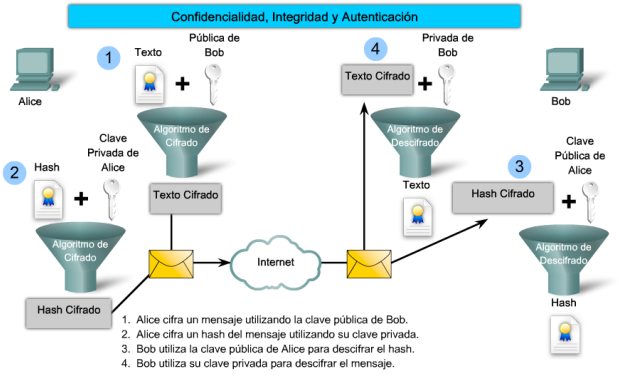


- Los algoritmos de cifrado asimétricos son mejor conocidos como algoritmos de clave pública.
- a longitud de clave usual tiene entre 512 y 4096 bits.
- El remitente y el destinatario no comparten una clave secreta.
- Estos algoritmos son relativamente lentos debido a que se basan en algoritmos computacionales complejos.
- Ejemplos de algoritmos de cifrado asimétrico son RSA, ElGamal, curvas elípticas, y DH.

Cifrado Simétrico | **Cifrado Asimétrico**

- El cifrado puede implementarse utilizando un algoritmo simétrico o asimétrico.
- Pueden utilizarse varios algoritmos de cifrado simétrico. Cada opción varía de acuerdo al grado de protección y su facilidad de implementación.
- Diffie-Hellman es un algoritmo de hashing utilizado para soportar DES, 3DES, y AES.

- El cifrado asimétrico puede utilizar firmas digitales, como en el caso del algoritmo RSA, para proveer autenticación y confidencialidad.
- El cifrado asimétrico es usualmente implementado utilizando una infraestructura de clave pública (PKI).



8 Implementacion de redes privadas Virtuales
8.0 Introduccion al capitulo
8.0.1 Introduccion al capitulo

as organizaciones utilizan redes privadas virtuales (VPNs) para crear una conexión de red privada de extremo a extremo (túnel) sobre redes de terceros, tales como Internet o extranets. El túnel elimina la barrera de la distancia y permite que los usuarios remotos tengan acceso a recursos de la red central. Sin embargo, las VPNs no garantizan que la información se mantenga segura mientras atraviesa el túnel. Por este motivo, se aplican métodos criptográficos modernos a las VPNs, con el fin de establecer conexiones seguras de redes privadas de extremo a extremo.

El protocolo IP Security (IPsec) proporciona el framework para configurar VPNs seguras y es utilizado con frecuencia a través de Internet para conectar sucursales de oficinas, empleados remotos y socios comerciales. Es una forma confiable de mantener la privacidad de las comunicaciones a la vez que se optimizan las operaciones, se reducen costos y se permite una administración flexible de la red.

Es posible implementar VPNs de sitio a sitio seguras, entre un sitio central y uno remoto, utilizando el protocolo IPsec. IPsec puede también ser utilizado en túneles de acceso remoto, para el acceso de trabajadores a distancia. La aplicación Cisco VPN Client es un método para establecer una VPN de acceso remoto con IPsec. Además de IPsec, puede utilizarse el protocolo Secure Sockets Layer (SSL) para establecer conexiones de acceso remoto VPN.

En la primera práctica de laboratorio del capítulo, Configuración de una VPN de sitio a sitio utilizando el IOS de Cisco y SDM, los estudiantes realizarán la configuración de una VPN IPsec utilizando el CLI de routers perimetrales, para luego verificar la operación de una VPN IPsec. Otra VPN de sitio a sitio con IPsec será configurada y verificada utilizando SDM.

En la segunda práctica de laboratorio, Configuración de un cliente y un servidor para una VPN de acceso remoto, los alumnos realizarán la configuración de una ZPF con SDM en un router perimetral, seguido por un servidor Cisco Easy VPN Server. Luego, se ejecutará la instalación y configuración de un cliente Cisco VPN Client en una PC. Se deberá probar la conexión VPN de acceso remoto.

Los laboratorios se encuentran en el manual de laboratorios de Academy Connection, en cisco.netacad.net.

Una actividad del Packet Tracer, Configure y verifique una VPN de sitio a sitio con IPsec utilizando la CLI, proporciona a los alumnos de práctica adicional en la implementación de las tecnologías presentadas en este capítulo. Los estudiantes aseguran y prueban una conexión WAN entre dos redes remotas utilizando una VPN de sitio a sitio con IPsec. Las actividades de Packet Tracer para CCNA Security se encuentran en Academy Connection en cisco.netacad.net.

En este capítulo, aprenderá a:

- Describir el propósito y tipos de VPNs y definir dónde utilizar VPNs en una red.
- Describir cómo configurar un túnel GRE VPN.
- Describir los conceptos y tecnologías fudamentales de las VPNs y términos utilizados por IPsec VPNs.
- Describir cómo configurar una IPsec VPN de sitio a sitio.
- Configurar una IPsec VPN de sitio a sitio con autenticación PSK utilizando CLI y Cisco SDM.
- Describir los dos métodos comunes de acceso remoto utilizado en redes empresariales.
- Describir cómo se utiliza el Cisco VPN Client en una IPsec VPN de acceso remoto.
- Describir cómo se utiliza Secure Socket Layer (SSL) en una VPN de acceso remoto.
- Configurar una IPsec VPN de acceso remoto utilizando CLI y Cisco SDM.

8.1 VPNS

8.1.1 Repaso de VPN

Soluciones tales como los diferentes métodos de cifrado y PKI permiten a las empresas extender sus redes en forma segura a través de Internet. Una forma en que las empresas logran esta expansión es mediante redes privadas virtuales (VPNs).

Una VPN es una red privada que se crea mediante el uso de túneles sobre una red pública, usualmente Internet. En lugar de utilizar conexiones físicas dedicadas, una VPN utiliza conexiones virtuales enrutadas a través de Internet, desde la organización hasta el sitio remoto. Las primeras VPNs eran estrictamente túneles IP, los cuales no incluían autenticación o cifrado de los datos. Por ejemplo, Generic Routing Encapsulation (GRE) es un protocolo de tunneling desarrollado por Cisco que puede encapsular una amplia variedad de protocolos de capa de red dentro de túneles IP. Esto crea un enlace virtual punto a punto entre routers Cisco en puntos remotos sobre una red IP. Otros ejemplos de VPNs que no incluyen en forma automática medidas de seguridad son las redes Frame Relay, ATM PVCs, Conmutación Multi-Protocolo con Etiquetas (Multiprotocol Label Switching - MPLS).

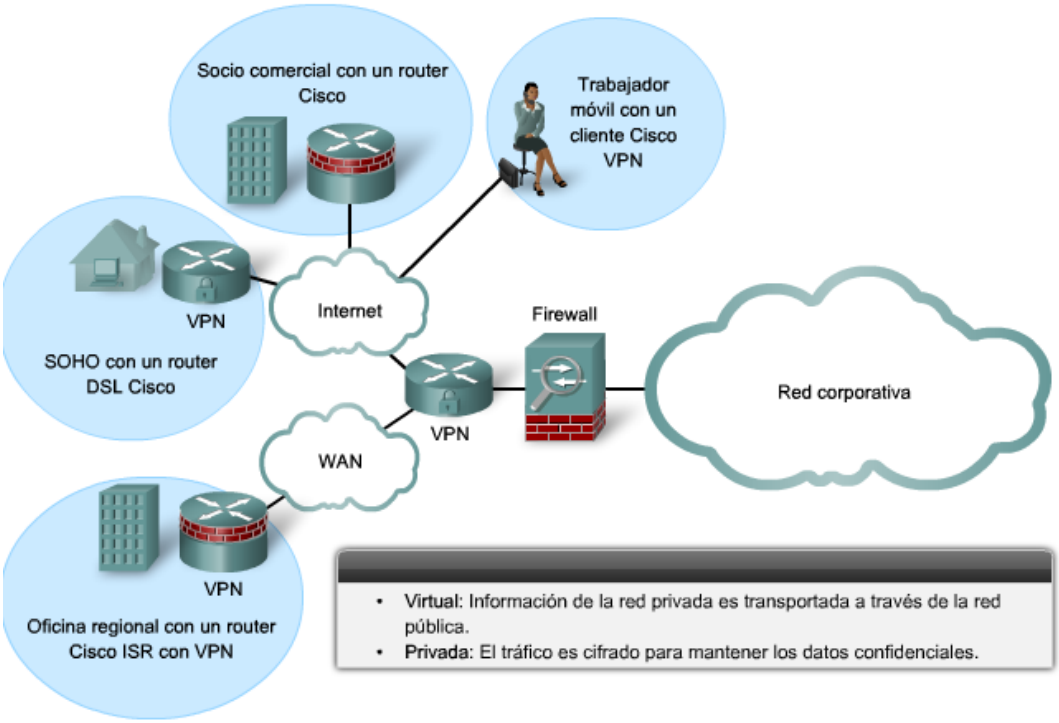
Una VPN es un entorno de comunicaciones en el que el acceso está estrictamente controlado para permitir conexiones entre pares dentro de una comunidad de interés definida. La confidencialidad se logra mediante el cifrado del tráfico dentro de la VPN. En la actualidad, una implementación segura de VPN con cifrado es lo que generalmente se equipara con el concepto de una red privada virtual.

Las VPNs tienen muchos beneficios:

Costos menores - Las VPNs permiten a las organizaciones utilizar Internet, un medio de transporte rentable provisto por terceros, para conectar oficinas y usuarios remotos al sitio principal de la corporación. Las VPNs eliminan los costosos enlaces WAN dedicados y los bancos de módems. Además, con el advenimiento de las tecnologías de banda ancha más económicas, tales como DSL, las organizaciones pueden utilizar VPNs para reducir sus costos de conectividad, a la vez que incrementan el ancho de banda para las conexiones remotas.

Seguridad - Las VPNs proveen el más alto nivel de seguridad utilizando protocolos avanzados de cifrado y autenticación, los cuales protegen los datos del acceso no autorizado.
Escalabilidad - Las VPNs permiten que las corporaciones utilicen la infraestructura de Internet disponible en los dispositivos y proveedores de servicio de Internet (Internet

Service Providers - ISPs). Esto facilita la incorporación de nuevos usuarios, por lo que la corporación puede incrementar su capacidad en forma importante sin incorporar infraestructura significativa.
Compatibilidad con tecnología de banda ancha - Las VPNs permiten que los trabajadores móviles, los trabajadores remotos y aquellas personas que quieran extender su jornada laboral aprovechando la ventaja de la conectividad de banda ancha de alta velocidad, obtengan acceso a sus redes corporativas, proveyendo a los trabajadores de una mejor flexibilidad y eficiencia. La conexiones de banda anda de alta velocidad proveen una solución rentable a la conexión de oficinas remotas.



En el sentido más simple, una VPN conecta dos extremos sobre una red pública para formar una conexión lógica. Las conexiones lógicas pueden realizarse tanto en la capa 2 como en la capa 3 del modelo OSI. Las tecnologías VPN pueden clasificarse en líneas generales, de acuerdo a estos modelos de conexión lógica, como VPNs de capa 2 o VPNs de capa 3. Establecer la conectividad entre sitios con una VPN de capa 2 o de capa 3 es lo mismo. Se agrega un encabezado de entrega al inicio de los datos, para que alcance el sitio de destino. Este capítulo se enfoca en la tecnología VPN de capa 3.

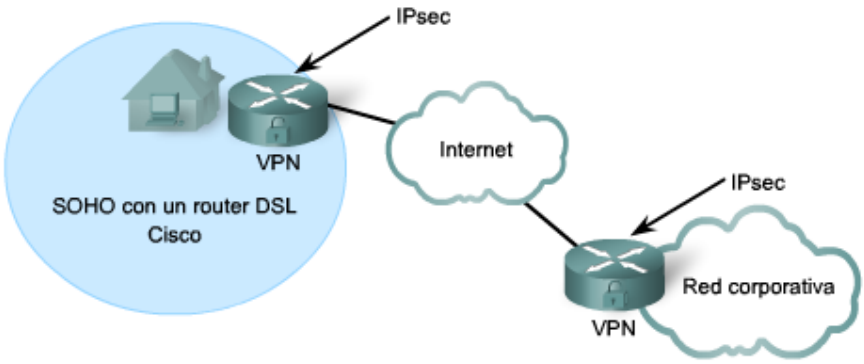
Ejemplos comunes de VPNs de capa 3 son GRE, MPLS e IPsec. Las VPNs de capa 3 pueden ser conexiones de sitios punto a punto, como GRE e IPsec o pueden establecer conectividad "any-to-any" entre varios sitios utilizando MPLS.

El protocolo GRE (Generic Routing Encapsulation) fue desarrollado originalmente por Cisco y luego estandarizado como el RFC 1701. RFC 1702 define el encabezado de entrega IP para GRE. Un túnel GRE entre dos sitios con accesibilidad IP pueden ser considerados una VPN, dado que los datos privados entre los sitios están encapsulados en un encabezado de entrega.

Utilizado en sus comienzos por Cisco, MPLS fue primero conocido como conmutación de etiquetas y luego estandarizado por el IETF como MPLS. Cada vez más, los proveedores de servicios despliegan MPLS para ofrecer servicios de VPN MPLS a sus clientes. Las VPNs MPLS utilizan etiquetas para encapsular los datos originales o "carga útil", para formar una VPN.

¿Cómo logra el administrador de la red prevenir las capturas ilegales de los datos en una VPN? Cifrar los datos es una forma de protegerlos. El cifrado de datos se logra desplegando dispositivos de cifrado en cada extremo. IPsec es un conjunto de protocolos desarrollado con el respaldo de IETF para obtener servicios seguros sobre redes IP de conmutación de paquetes. Internet es la red de conmutación de paquetes más omnipresente. Por lo tanto, una VPN IPsec implementada sobre la Internet pública puede proveer importantes reducciones de costos a una corporación, en comparación con una VPN de línea arrendada.

Los servicios IPsec proporcionan autenticación, integridad, control de acceso y confidencialidad. Con IPsec, la información intercambiada entre los sitios remotos puede ser cifrada y verificada. Tanto las VPNs de acceso remoto como las de sitio a sitio pueden implementarse utilizando IPsec.



8.1.2 Topologias VPN

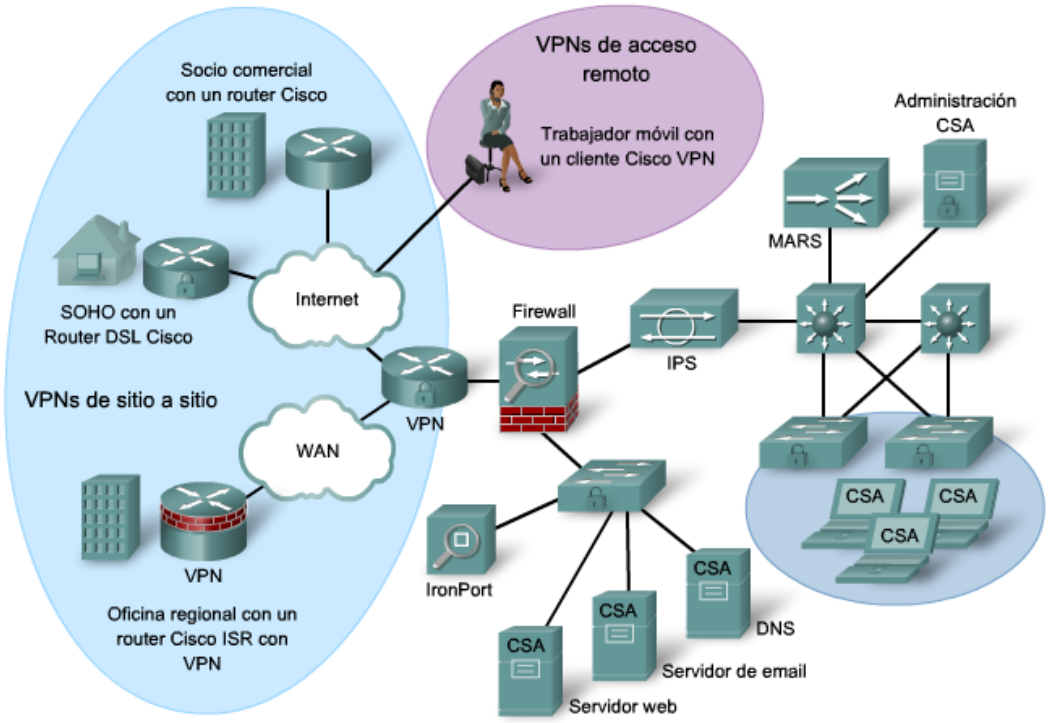
Existen dos tipos básicos de redes VPN:

Sitio a sitio
Acceso remoto

Una VPN de sitio a sitio se crea cuando los dispositivos de conexión en ambos extremos de la conexión VPN conocen la configuración VPN de antemano. La VPN permanece estática y los hosts internos no tienen conocimiento de la existencia de la VPN. Las redes Frame Relay, ATM, GRE y MPLS son ejemplos de VPNs de sitio a sitio.

Una VPN de acceso remoto se crea cuando la información de la VPN no se configura en forma estática, sino que se permite que la información cambie en forma dinámica y puede ser habilitada o deshabilitada. Considere un trabajador a distancia que necesita acceder a datos corporativos a través de Internet. Su conexión VPN puede no estar

activa en todo momento. La PC del trabajador es responsable de establecer la VPN. La información requerida para establecer la conexión VPN, como puede ser la dirección IP del trabajador a distancia, cambia dinámicamente de acuerdo a la ubicación del mismo.



VPN de sitio a sitio

Una VPN de sitio a sitio es una extensión de una red WAN clásica. Las VPNs de sitio a sitio conectan redes completas entre sí. Por ejemplo, pueden conectar redes de sucursales a la red de la oficina central de la compañía. En el pasado, era necesaria una línea arrendada o una conexión Frame Relay para comunicar estos sitios, pero debido a que la mayoría de las corporaciones ahora disponen de acceso a internet, estas conexiones pueden reemplazarse con VPNs de sitio a sitio.

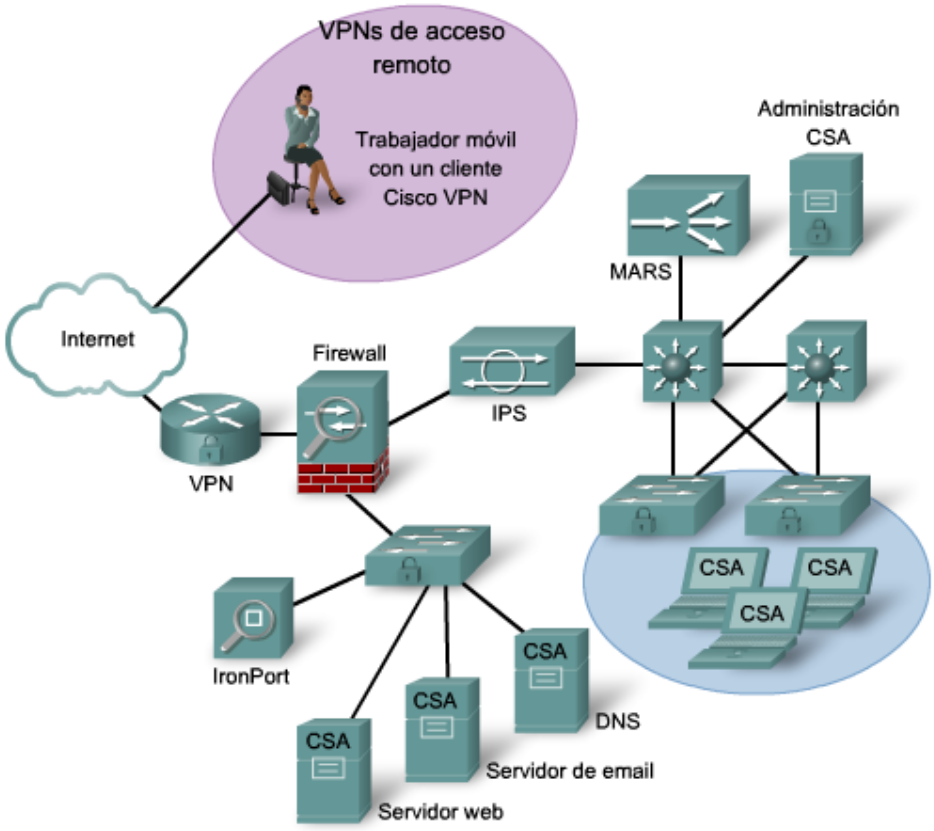
En una VPN de sitio a sitio, los hosts envían y reciben tráfico TCP/IP normal a través del gateway VPN, el cual puede ser un router, un firewall, un concentrador Cisco VPN Concentrator o un dispositivo Cisco ASA 5500 Series Adaptive Security Appliance. El gateway de la VPN es responsable de encapsular y cifrar el tráfico saliente de un sitio en particular y enviarlo a través del túnel VPN sobre Internet hacia otro gateway de VPN en el sitio de destino. Cuando el paquete es recibido en el otro extremo, el gateway de VPN que lo recibe le quita los encabezados, descifra el contenido y direcciona el paquete hacia el host destino dentro de su red privada.

VPN de acceso remoto

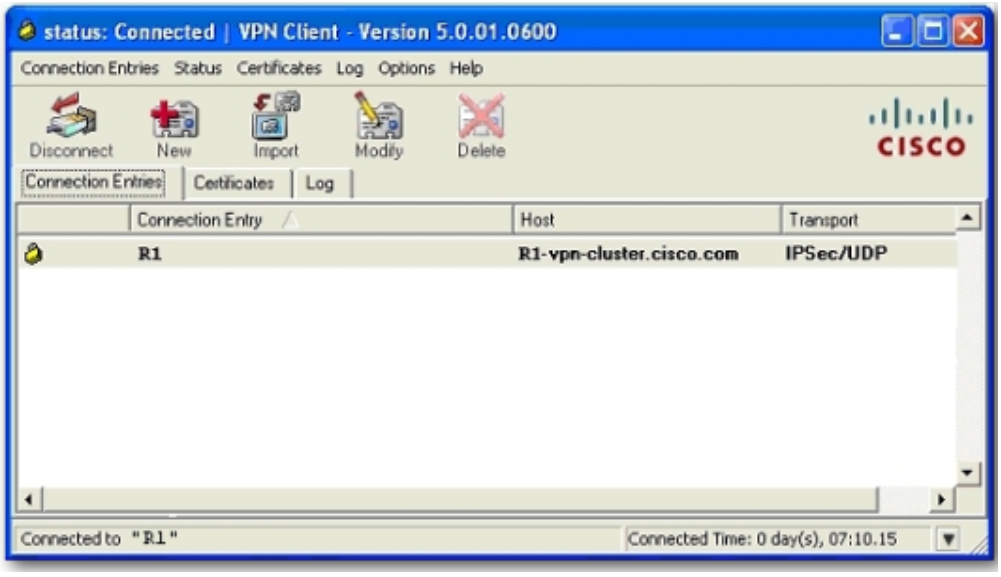
Las VPNs de acceso remoto son una evolución de las redes de conmutación de circuitos, tales como el servicio de telefonía básica (POTS) o ISDN. Las VPNs de acceso remoto pueden cubrir las necesidades de tráfico de los trabajadores a distancia, los usuarios móviles y los clientes de la empresa. Las VPNs de acceso remoto soportan

una arquitectura cliente-servidor, donde un cliente VPN (el host remoto) requiere un acceso seguro a la red de la empresa mediante un servidor VPN instalado en el límite de la red.

En el pasado, las corporaciones daban soporte a los usuarios remotos utilizando redes de acceso telefónico e ISDN. Con el advenimiento de las VPNs, un usuario móvil requiere simplemente de acceso a Internet para comunicarse con la oficina central. En el caso de los trabajadores a distancia, su conectividad a Internet es en general una conexión de banda ancha.



En una VPN de acceso remoto, cada host tiene una aplicación Cisco VPN Client. Cuando el host intenta enviar tráfico destinado a la VPN, la aplicación Cisco VPN Client encapsula y cifra dicho tráfico antes de enviarlo a través de Internet hacia el gateway VPN en el borde de la red destino. Una vez recibido el tráfico, el gateway VPN se comporta como en una VPN de sitio a sitio.



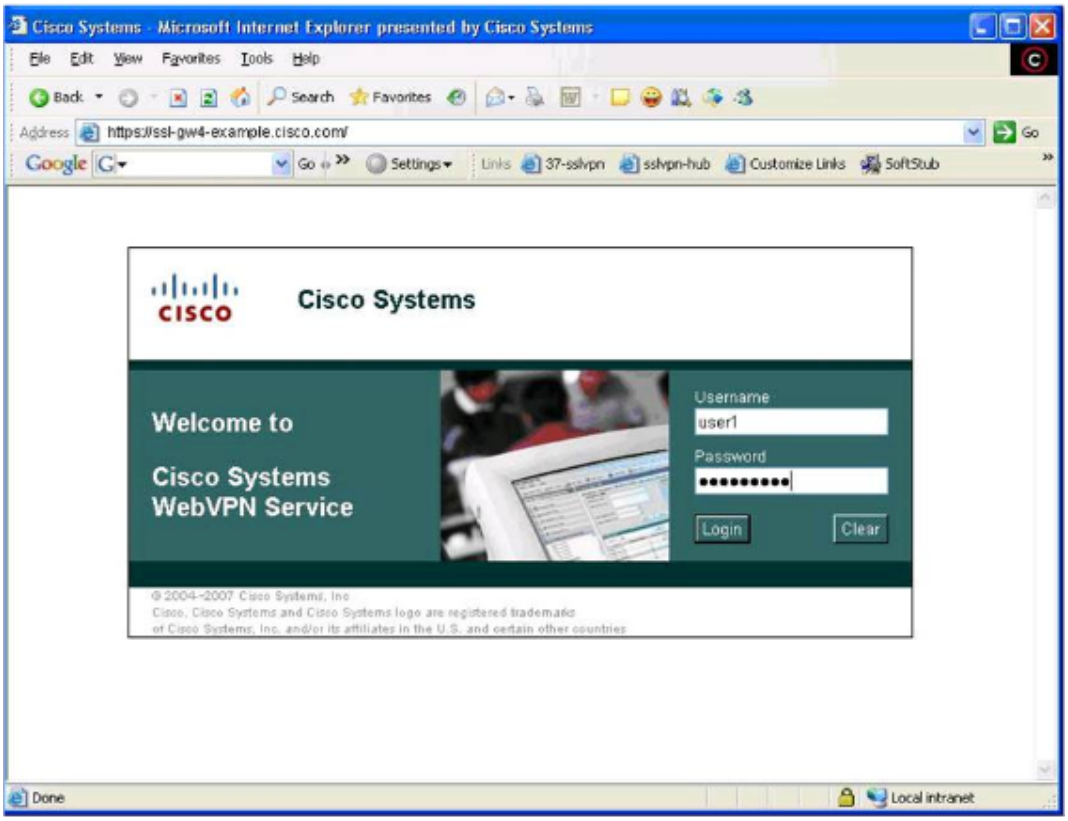
Una tecnología de acceso remoto emergente es el IOS Cisco VPN SSL. Esta tecnología provee conectividad de acceso remoto desde casi cualquier host con acceso a Internet utilizando un navegador web y cifrado nativo SSL (Secure Sockets Layer). Las VPNs con SSL permiten a los usuarios acceder a sitios y servicios web, incluyendo la habilidad de acceder a archivos, enviar y recibir correo electrónico y ejecutar aplicaciones basadas en TCP sin utilizar VPN IPsec Client. Proveen la flexibilidad para soportar el acceso seguro de todos los usuarios, sin importar desde qué host intenten establecer la conexión. Esta flexibilidad permite que las compañías extiendan sus redes empresariales seguras para cualquier usuario autorizado, proveyendo así conectividad de acceso remoto a recursos corporativos desde cualquier host conectado a Internet.

Una VPN SSL dispone actualmente de dos modos de acceso: sin cliente y con cliente liviano. En una VPN SSL sin cliente, el cliente remoto sólo necesita un navegador web con SSL para acceder a servidores web HTTP o HTTPS de la LAN corporativa. En un ambiente VPN SSL con cliente liviano, el cliente remoto debe descargar un pequeño applet basado en Java para obtener un acceso seguro a las aplicaciones TCP que utilizan números de puerto estáticos. UDP no es soportado en ambientes de clientes livianos.

Las VPNs con SSL son apropiadas para poblaciones de usuarios que requieren control de acceso por aplicación o por servidor, o acceso desde estaciones de trabajo no provistas por la empresa. Las VPNs con SSL no son un reemplazo completo de las VPNs con IPsec. Las VPNs con IPsec permiten un acceso seguro a todas las aplicaciones cliente-servidor de la organización. Además, las VPNs con SSL no soportan el mismo nivel de seguridad criptográfica soportado por las VPNs con IPsec. Mientras que las VPNs con SSL no pueden reemplazar a las VPNs con IPsec, en muchos casos son complementarias, ya que resuelven diferentes problemas. Este enfoque complementario permite que un solo dispositivo resuelva todos los requisitos de los usuarios de acceso remoto.

El beneficio primario de las VPNs con SSL es que son compatibles con DMVPNs (Dynamic Multipoint VPNs), Cisco IOS Firewalls, IPsec, sistemas de prevención de intrusos (IPSs), Cisco Easy VPN y NAT (Network Address Translation).

La restricción primaria de las VPNs con SSL es que actualmente sólo disponen de soporte de software. La CPU del router procesa las conexiones de la VPN SSL. La aceleración VPN integrada que se encuentra disponible en routers de servicios integrados solo acelera conexiones IPsec.



8.1.3 Soluciones VPN

La línea de productos VPN de Cisco incluye diversos dispositivos para soportar una VPN remota o sitio a sitio:

Routers y switches Cisco con capacidad VPN - Una buena opción para clientes de todos los tamaños que buscan tomar ventaja de su infraestructura de red existente para implementar VPNs y seguridad, integrando al mismo tiempo todos los servicios en un único dispositivo con la más amplia selección de interfaces WAN y LAN.

Dispositivos Cisco PIX 500 Series Security Appliances - Proveen servicios de seguridad de red integrados, robustos y de clase empresarial, incluyendo un firewall de estados (stateful inspection firewall), inspección profunda de protocolos y aplicaciones y VPN IPsec. Los dispositivos PIX 500 Series Security Appliances son una excelente opción para organizaciones cuyas políticas de seguridad recomiendan separar la administración de la infraestructura de seguridad para establecer una demarcación clara entre la operación de red y la seguridad. El producto Cisco PIX 500 Series ya no se encuentra a la venta. Sin embargo, existe una gran cantidad de equipos instalados.

Dispositivos Cisco ASA 5500 Series Adaptive Security Appliances - Dispositivos de seguridad "todo en uno" que proveen seguridad de clase empresarial y VPN IPsec a pequeños y medianos negocios y a grandes redes empresariales en una aplicación construida en forma modular. Los dispositivos incorporan un amplio rango de servicios integrados de seguridad, incluyendo firewall, ISP y VPN. Los equipos Cisco ASA 5500 Series Appliances son ideales para clientes que buscan un firewall robusto combinado con un soporte global de VPN.
Concentradores Cisco VPN 3000 Series - Ofrecen tanto conectividad VPN SSL como VPN IPsec en una única plataforma, sin el costo del licenciamiento de características individuales. Los concentradores Cisco VPN 3000 Series ya no se encuentran a la venta.
Routers SOHO - Muchos routers hogareños de banda ancha, como los Linksys, también soportan VPNs.

En la mayoría de las redes, los dispositivos ya se encuentran instalados. Si este es el caso, es necesario verificar si la interoperabilidad entre los diferentes dispositivos es posible. Por ejemplo, la red de un cliente tiene un dispositivo Cisco ASA 5500 Series Adaptive Security Appliance en un extremo y un router Cisco en el otro. La interoperabilidad VPN de sitio a sitio es posible seleccionando, como mínimo, las siguientes versiones de software: Cisco IOS Release 12.2(8)T y Cisco ASA 5500 Series Adaptive Security Appliance versión 8.0.

Con routers Cisco ejecutando software Cisco IOS, las organizaciones pueden implementar y escalar VPNs de sitio a sitio en cualquier topología, desde una topología hub-and-spoke, hasta topologías más complejas como VPNs de malla completa. Además, las características de seguridad del Cisco IOS combinan la capacidad de VPN con firewall, prevención de intrusiones y capacidades extensivas del Cisco IOS, incluyendo calidad de servicio (QoS) y soporte de enrutamiento avanzado, multiprotocolo y multicast.

Producto	VPN de acceso remoto	VPN de sitio a sitio
Router Cisco con VPN	Rol secundario	Rol primario
Dispositivos Cisco PIX 500 Series Security	Rol secundario	Rol primario
Dispositivos Cisco ASA 5500 Series Adaptive Security	Rol primario	Rol secundario
Concentradores Cisco VPN 3000 Series	Rol primario	Rol secundario
Routers SOHO	Rol primario	Rol secundario

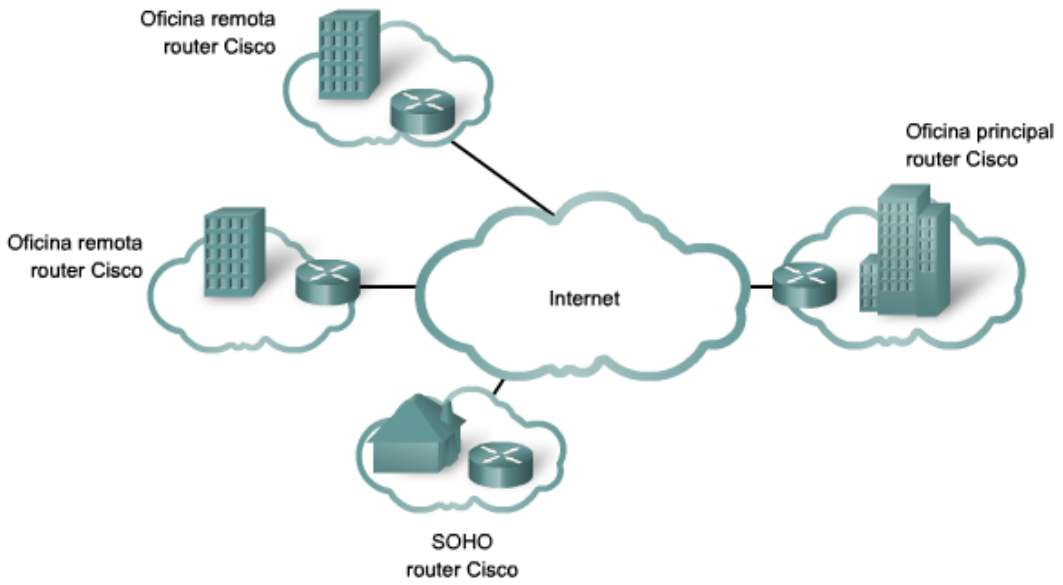
Cisco ofrece un conjunto de routers optimizados para VPN. El software Cisco IOS para routers combina servicios de VPN con servicios de enrutamiento. El software Cisco VPN incorpora seguridad fuerte utilizando cifrado y seguridad. Estos routers optimizados para VPN proveen una alta performance para soluciones VPN de sitio a sitio, de intranet y de extranet.

Los conjuntos de características del Cisco IOS incorporan varias funcionalidades VPN:

VPN con capacidad de voz y video(Voice and Video VPN - V3PN) - Integra telefonía IP, QoS e IPsec, proveyendo un servicio VPN de extremo a extremo que ayuda a asegurar la entrega a tiempo de aplicaciones sensibles a la latencia, tales como voz y video.

Tolerancia a fallas con estados de IPsec (IPsec stateful failover) - Provee una capacidad rápida y escalable para mantener un buen servicio ante fallas de la red durante las sesiones VPN entre los sitios remoto y central. Con la disponibilidad de soluciones de tolerancia a fallas con estados y sin estados, tales como Hot Standby Router Protocol (HSRP), la tolerancia a fallas con estados de IPsec asegura un máximo tiempo de operación de las aplicaciones críticas.
Dynamic Multipoint Virtual Private Network (DMVPN) - Permite el auto-abastecimiento de VPNs de sitio a sitio con IPsec, combinando tres características del IOS de Cisco: el protocolo de resolución de próximo salto (Next Hop Resolution Protocol - NHRP), GRE multipunto y VPN IPsec. Esta combinación facilita la provisión de desafíos a los clientes y provee una conectividad segura entre todos los extremos.

Integración entre IPsec y MPLS - Permite a los ISPs mapear sesiones IPsec en forma directa en una MPLS VPN. Esta solución puede ser implementada en routers de borde ubicados en el mismo lugar, que se encuentren conectados al router de borde de la red MPLS del proveedor que usa software IOS de Cisco. Esta solución permite al ISP extender su servicio de VPN en forma segura más allá de los límites de la red MPLS, utilizando la infraestructura pública IP que conecta en forma segura las oficinas empresariales de usuarios remotos, trabajadores a distancia y usuarios móviles, desde cualquier lugar de la red corporativa.
Cisco Easy VPN - Simplifica la implementación de VPN para oficinas remotas y trabajadores a distancia. La solución Cisco Easy VPN centraliza la administración de la VPN a través de todos los dispositivos VPN de Cisco, reduciendo así la complejidad de administración de las implementaciones VPN.



Para los servicios VPN, los dispositivos Cisco ASA 5500 Series Adaptative Appliances ofrecen tecnologías flexibles que entregan soluciones que se adaptan a los requisitos de conectividad sitio a sitio y de acceso remoto. Estos dispositivos proveen conectividad de acceso remoto y sitio a sitio, basado en VPN IPsec y VPN SSL, de fácil administración. Las empresas pueden crear conexiones seguras a través de las redes públicas, para el acceso de usuarios móviles, sitios remotos y socios comerciales.

Como componente importante de la Red Auto-Defensiva de Cisco (Cisco Self-Defending Network), los dispositivos Cisco ASA 5500 Series Adaptive Security Appliances proveen una contención proactiva de amenazas, controlan la actividad de la red y de las aplicaciones y proveen conectividad VPN flexible, a la vez que se mantienen rentables.

Los dispositivos Cisco ASA 5500 Series Adaptive Security Appliances ofrecen otros servicios, tales como prevención de intrusiones, Cisco VPN SSL, e integración avanzada de módulos (advanced integration module - AIM) para mejorar las capacidades de procesamiento de los dispositivos. Estas son algunas de las características que proveen los dispositivos Cisco ASA 5500 Series Adaptive Security Appliances:

Plataforma flexible - Ofrece VPN tanto con IPsec como SSL en una misma plataforma, eliminando la necesidad de proveer soluciones paralelas. Además de los servicios VPN, los dispositivos Cisco ASA 5500 Series Adaptive Security Appliances ofrecen servicios de firewall de inspección de aplicaciones y prevención de intrusiones.
Clusters flexibles - Permite implementaciones de acceso remoto que pueden escalarse en forma rentable distribuyendo en forma equitativa las sesiones VPN entre todos los dispositivos Cisco ASA 5500 Series Adaptive Security Appliances y Cisco VPN 3000 Series Concentrators sin requerir intervención del usuario.

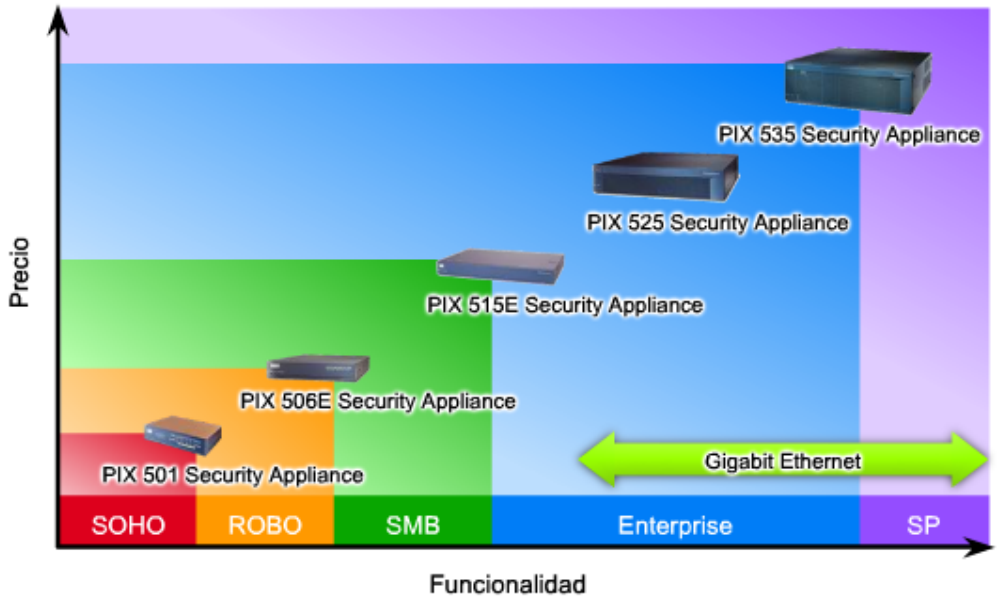
Cisco Easy VPN - Provee una arquitectura VPN de acceso remoto escalable, rentable y fácil de administrar. Los dispositivos Cisco ASA 5500 Series Adaptive Security Appliances envían las más recientes políticas de seguridad VPN hacia los dispositivos y clientes VPN remotos, asegurándose que las políticas en los extremos remotos se encuentran actualizadas antes de establecer la conexión.
Actualizaciones automáticas Cisco VPN Client - Permite que el software Cisco VPN Client, operando en estaciones de trabajo remotas, se actualicen en forma automática.
Cisco IOS VPN SSL - Ofrece una VPN SSL de Cisco con capacidades de VPN SSL sin cliente y de cliente liviano.
Infraestructura VPN para aplicaciones contemporáneas - Permite la convergencia de voz, video y datos a través de una red asegurada con IPsec, combinando un soporte VPN de sitio a sitio robusto con funciones de inspección detallada, QoS, enrutamiento y tolerancia a fallas con estados

Administración Web integrada - Permite la administración de los dispositivos Cisco ASA 5500 Series Adaptive Security Appliances utilizando la interfaz web integrada Cisco Adaptive Security Device Manager (ASDM). La interfaz Cisco ASDM administra todas las funciones de seguridad y VPN de los dispositivos.

Cada dispositivo Cisco ASA 5500 Series Adaptive Security Appliance soporta un número de pares VPN:

Cisco ASA 5505 - 10 pares VPN IPsec y 25 pares VPN SSL, con una licencia Base y 25 pares VPN (IPsec o SSL) con una licencia Security Plus
Cisco ASA 5510 - 250 pares VPN
Cisco ASA 5520 - 750 pares VPN

Cisco ASA 5540 - 5000 pares VPN IPsec y 2500 pares VPN SSL
Cisco ASA 5550 - 5000 pares VPN

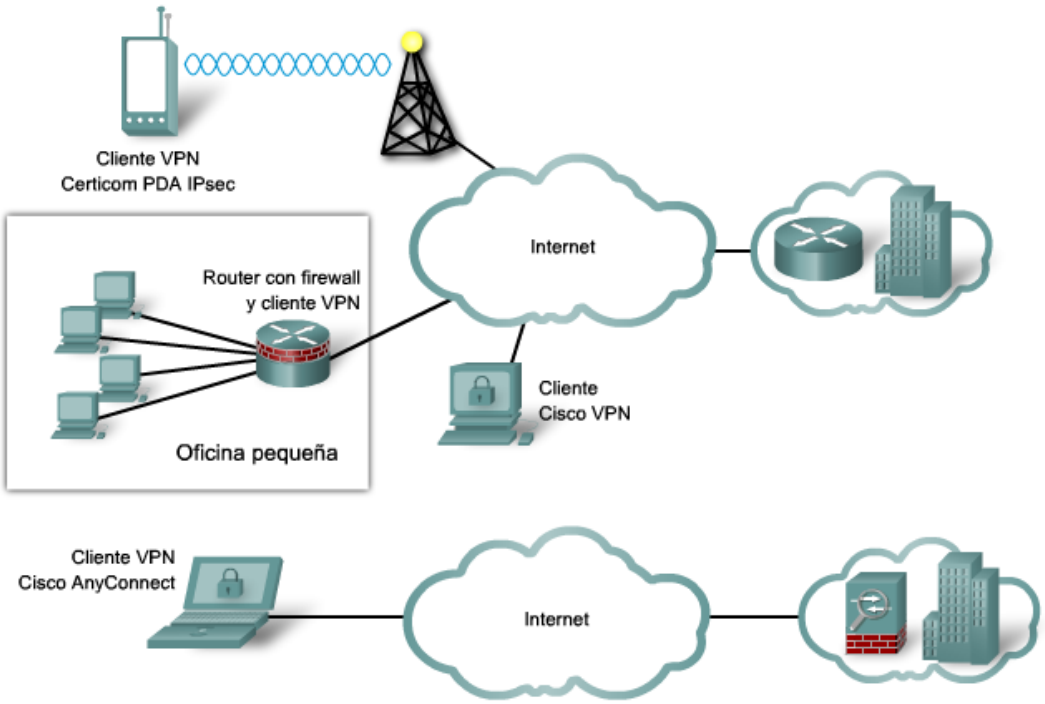


Las VPNs de acceso remoto de Cisco pueden utilizar cuatro clientes IPsec:

Cliente Certicom - Un cliente inalámbrico, el cual se ejecuta en un asistente personal inalámbrico (PDA) que utiliza los sistemas operativos Palm o Microsoft Windows Mobile. El software de cliente inalámbrico Certicom permite a las compañías extender aplicaciones empresariales críticas, tales como su correo electrónico y herramientas de administración de relación con los clientes (Customer Relatioship Manager - CRM), de forma tal que los profesionales móviles habiliten sus dispositivos portátiles para conectarse a los gateways VPN corporativos para obtener un acceso inalámbrico seguro.

Cisco VPN Client - Instalado en la PC o laptop de un individuo, el programa Cisco VPN Client permite a las organizaciones establecer túneles VPN punto a punto cifrados, para lograr una conectividad segura de los empleados móviles o trabajadores a distancia. El función Cisco Easy VPN permite al Cisco VPN Client recibir las políticas de seguridad del dispositivo VPN del sitio central, el Cisco Easy VPN Server, cuando se realiza una conexión a un túnel VPN, minimizando los requisitos de configuración en el sitio remoto.
Cisco Remote Router VPN Client - Se trata de un router remoto Cisco, configurado como cliente VPN, el cual conecta una LAN de una oficina pequeña u hogareña (SOHO) a la VPN

Cisco AnyConnect VPN Client - Cliente VPN de última generación que provee a los usuarios remotos de conexiones VPN seguras a los dispositivos Cisco ASA 5500 Series Adaptive Security Appliance que ejecuten Cisco ASA 5500 Series Software Versión 8.0 o superior o Cisco ASDM Versión 6.0 o superior. No puede conectarse con dispositivos Cisco PIX o Cisco VPN 3000 Series Concentrator. El programa Cisco AnyConnect VPN Client soporta Windows Vista, Windows XP, Windows 2000, Mac OS X (Versión 10.4 o superior) sobre Intel o PowerPC y Red Hat Linux (Versión 9 o superior).



Para mejorar el rendimiento y delegar la tarea de cifrado a hardware especializado, la familia de dispositivos Cisco VPN ofrece módulos de hardware de aceleración:

AIM - Un amplio rango de routers Cisco pueden ser equipados con AIM. Los módulos de integración avanzada se instalan dentro del chasis del router y liberan al CPU del router de las tareas de cifrado.
Cisco VPN IPsec Shared Port Adapter (SPA) - Proporciona funciones VPN escalables y rentables para switches Cisco Catalyst 6500 Series y routers Cisco 7600 Series. Utilizando el módulo Cisco 7600 Series/Catalyst 6500 Series Services SPA Carrier-400, cada slot del switch Cisco Catalyst 6500 Series o del router Cisco 7600 Series puede soportar hasta dos Cisco VPN IPsec SPAs.
Cisco PIX VPN Accelerator Card+ (VAC+) - El módulo de firewall PIX VAC+ proporciona aceleración por hardware hasta una tasa de transferencia máxima de 425 Mb/s de cifrado IPsec DES, 3DES o AES.



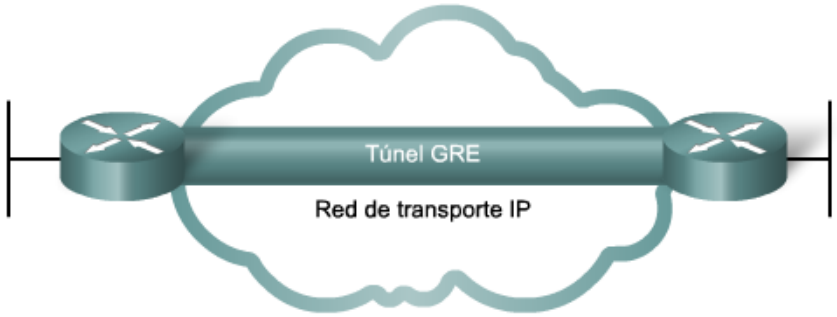
Cisco IPsec VPN SPA

8.2.1 Configuracion de un tunel GRE sitio a sitio

GRE (Generic Routing Encapsulation) es un protocolo de tunneling definido en las RFC 1702 y 2784. Fue desarrollado originalmente por Cisco Systems para la creación de enlaces punto a punto entre routers Cisco en puntos remotos sobre una red IP.

GRE soporta tunneling multiprotocolo. Puede encapsular paquetes de múltiples protocolos dentro de un túnel IP. Esta función se realiza agregando un encabezado GRE adicional entre el paquete de datos y el encabezado de túnel IP. El tunneling IP con GRE permite la expansión de la red conectando subredes multiprotocolo a través de un ambiente troncal con un único protocolo. GRE también soporta tunneling IP multicast. Los protocolos de enrutamiento utilizados a través del túnel permiten el intercambio dinámico de información de enrutamiento en la red virtual.

Los túneles GRE son sin estados. Cada extremo del túnel no mantiene información sobre el estado o disponibilidad del otro extremo del túnel. Esta característica permite a los proveedores de servicio (SPs) proveer túneles IP a clientes que no requieren conocer la arquitectura interna del túnel en el extremo del SP. Los clientes tienen entonces la flexibilidad de configurar o reconfigurar su arquitectura IP manteniendo la conectividad. Esto crea un enlace punto a punto virtual entre routers en puntos remotos de la red IP. GRE no incluye ningún mecanismo de seguridad fuerte para proteger los datos transmitidos.



Protocolo de tunneling GRE

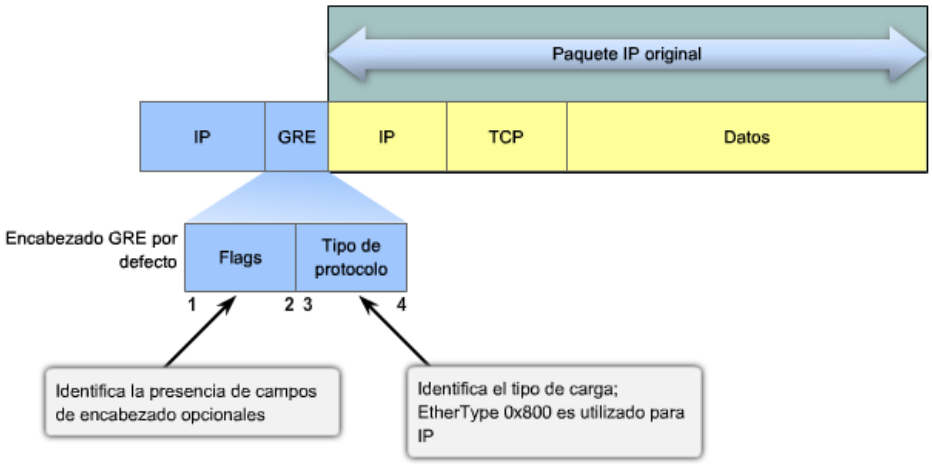
- Encapsula una amplia variedad de tipos de paquetes de protocolos dentro de los túneles IP.
- Crea un enlace virtual punto a punto entre routers Cisco en puntos remotos, a través de una red IP.
- Utiliza IP como transporte.
- Utiliza un encabezado adicional para soportar multicasting IP y cualquier otro protocolo de capa 3 del modelo OSI.

GRE encapsula el paquete IP original completo, con un encabezado IP estándar y un encabezado GRE. Un encabezado de túnel GRE contiene al menos 2 campos obligatorios de 2 bytes:

Flag GRE
Tipo de protocolo

GRE utiliza un campo de tipo de protocolo en el encabezado GRE para soportar la encapsulación de cualquier protocolo de capa 3 del modelo OSI. El encabezado GRE, junto con el encabezado de tunneling IP, agrega al menos 24 bytes de sobrecarga adicional a los paquetes enviados a través del túnel.

Encapsulación con GRE



La configuración de un túnel GRE consta de cinco pasos:

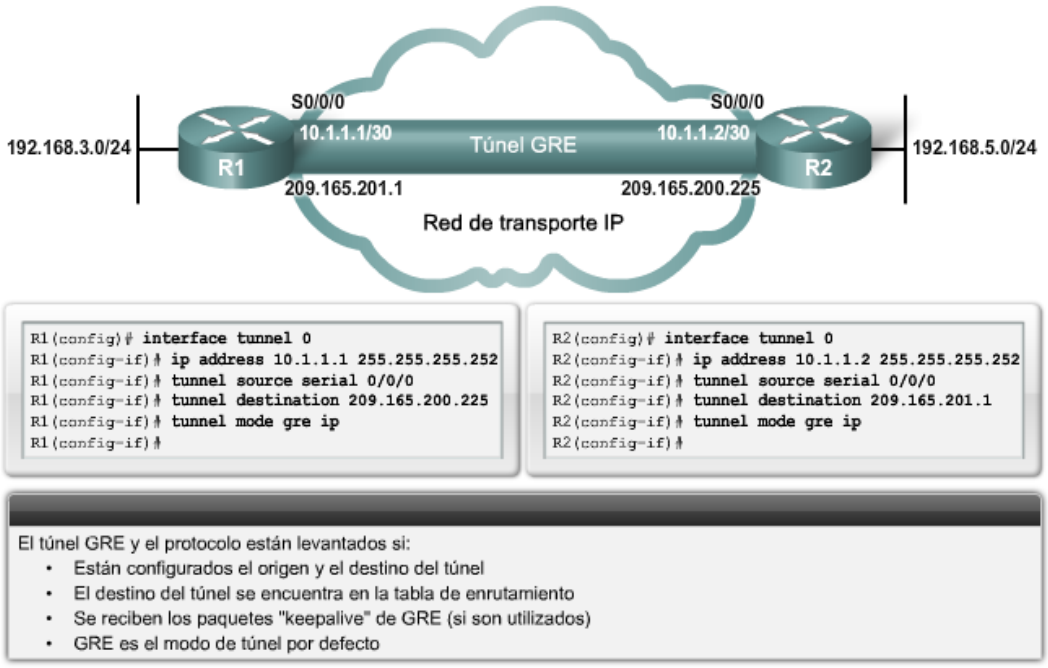
Paso 1. Crear la interfaz del túnel utilizando el comando interface tunnel 0.

Paso 2. Asignar una dirección IP al túnel.

Paso 3. Identificar la interfaz del túnel origen utilizando el comando tunnel source.

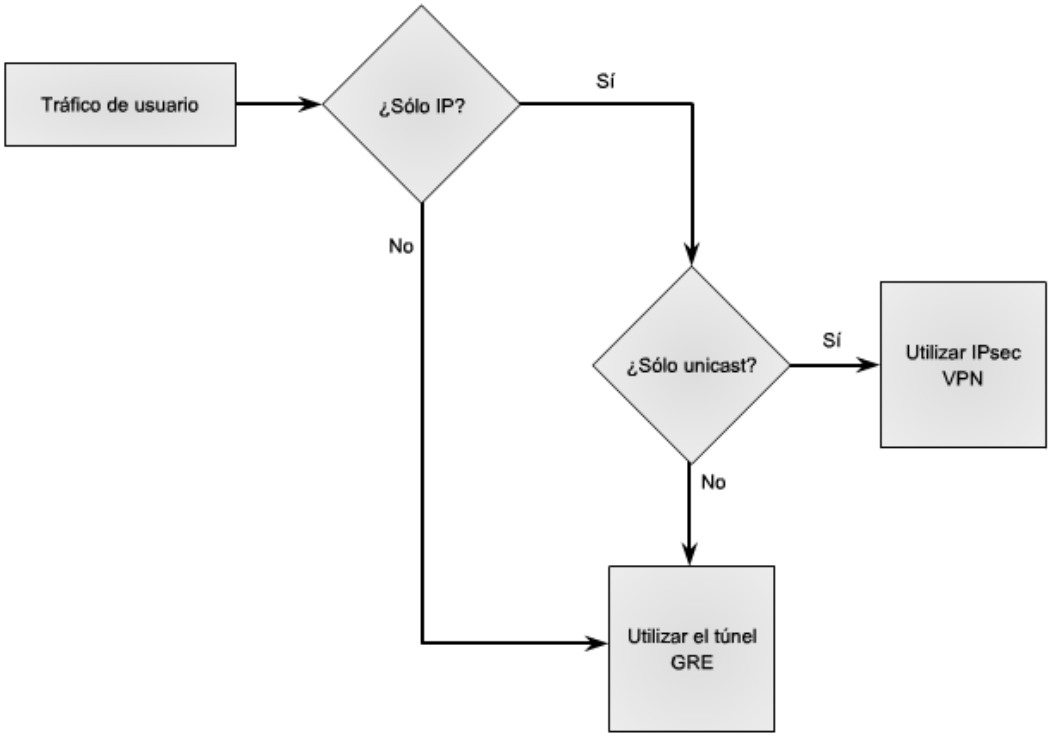
Paso 4. Identificar el destino del túnel utilizando el comando tunnel destination.

Paso 5. Configurar qué protocolo será encapsulado por GRE utilizando el comando tunnel mode gre.



Las ventajas de GRE consisten en que puede ser utilizado para tunelizar tráfico no IP sobre una red IP. Además y a diferencia de IPsec, que sólo soporta tráfico unicast, GRE soporta tráfico multicast y broadcast a través del enlace de túnel. Por lo tanto, los protocolos de enrutamiento son soportados por GRE.

GRE no provee cifrado. Si fuera necesario, debe configurarse IPsec.



8.3.1 Introduccion a IPSEC

IPsec es un estándar IETF (RFC 2401-2412) que define cómo debe configurarse una VPN utilizando el protocolo de direccionamiento IP. IPsec no está asociado a ningún tipo de cifrado, autenticación, algoritmos de seguridad o tecnología de claves específicos. IPsec es un framework de estándares abiertos que define las reglas para comunicaciones seguras. IPsec se basa en algoritmos existentes para implementar el cifrado, la autenticación y el intercambio de claves.

IPsec funciona en la capa de red, protegiendo y autenticando los paquetes IP entre los dispositivos IPsec participantes (pares). Como resultado, IPsec puede proteger virtualmente todo el tráfico de aplicaciones, ya que la protección puede ser implementada desde la capa 4 hasta la capa 7. Todas las implementaciones de IPsec tienen un encabezado de capa 3 en texto plano, para evitar problemas en el enrutamiento. IPsec funciona sobre todos los protocolos de capa 2, tales como Ethernet, ATM, Frame Relay, SDLC (Synchronous Data Link Control) y HDLC (High-Level Data Link Control).

El framework IPsec está formado por cinco bloques:

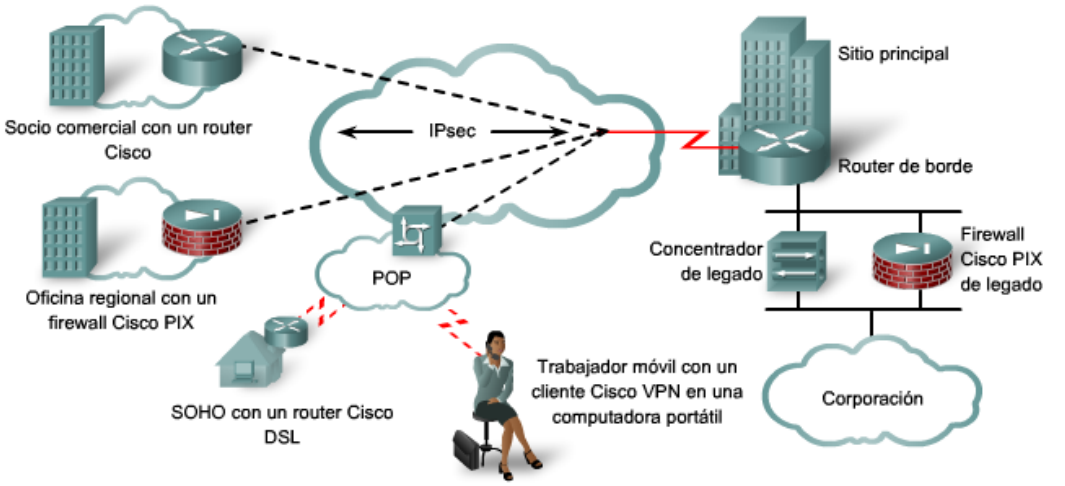
El primero representa el protocolo IPsec. Las opciones incluyen ESP o AH.
El segundo representa el tipo de confidencialidad implementada utilizando un algoritmo de cifrado como DES, 3DES, AES o SEAL. La opción depende del nivel de seguridad requerido.
El tercero representa la integridad, que puede implementarse utilizando MD5 o SHA.
El cuarto representa cómo se establece la clave secreta compartida. Los dos métodos posibles son pre-compartida y firma digital utilizando RSA.

El último representa el grupo de algoritmos DH. Existen cuatro algoritmos de intercambio de clave DH diferentes de los cuales es posible elegir: DH Group 1 (DH1), DH Group 2 (DH2), DH Group 5 (DH5) y DH Group 7 (DH7). El tipo de grupo seleccionado depende de las necesidades específicas.

IPsec provee el framework y el administrador selecciona los algoritmos que serán utilizados para implementar los servicios de seguridad dentro de dicho framework. Al no asociar IPsec a algoritmos específicos, permite la implementación de nuevos y mejores algoritmos sin modificar los estándares IPsec.

IPsec puede asegurar un camino entre un par de gateways, un par de hosts o un gateway y un host. Utilizando el framework, IPsec provee las siguientes funciones esenciales de seguridad:

Confidencialidad - IPsec asegura la confidencialidad mediante el uso de cifrado.
Integridad - IPsec asegura que los datos llegan a destino sin modificaciones, utilizando algoritmos de hash como MD5 y SHA.
Autenticación - IPsec utiliza IKE (Internet Key Exchange) para autenticar a los usuarios y dispositivos que puedan llevar a cabo comunicaciones en forma independiente. IKE utiliza varios tipos de autenticación, incluyendo nombre de usuario y contraseña, contraseña de un único uso, biométrica, claves pre-compartidas (PSKs) y certificados digitales.
Intercambio seguro de claves - IPsec utiliza el algoritmo DH para proveer un método de intercambio de claves públicas entre los pares, para establecer una clave compartida secreta.

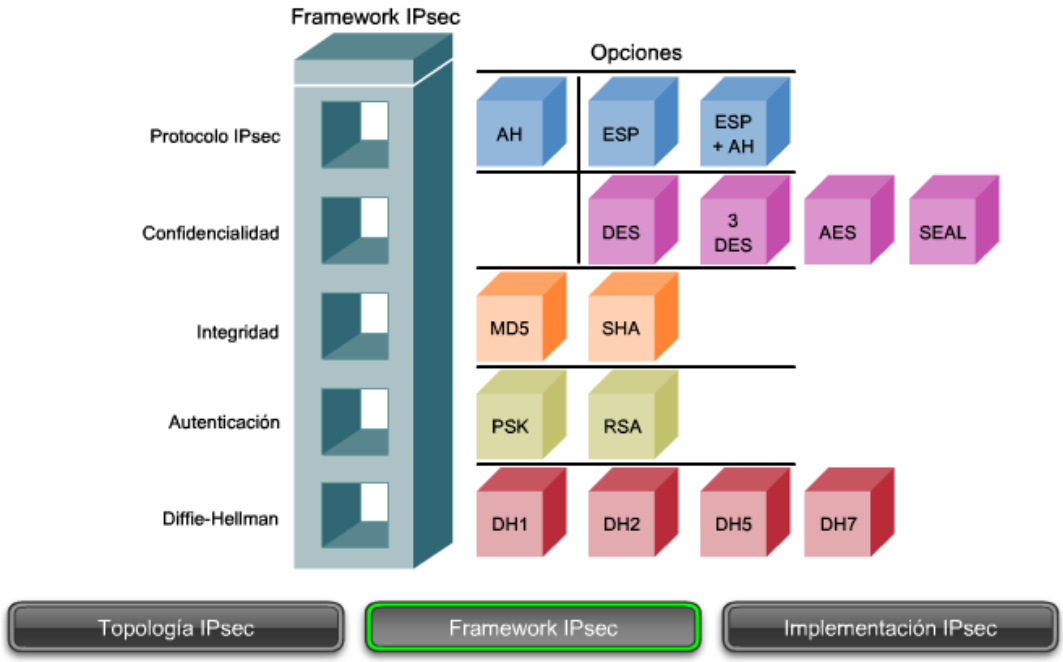


IPsec trabaja en la capa de red, protegiendo y autenticando los paquetes IP.

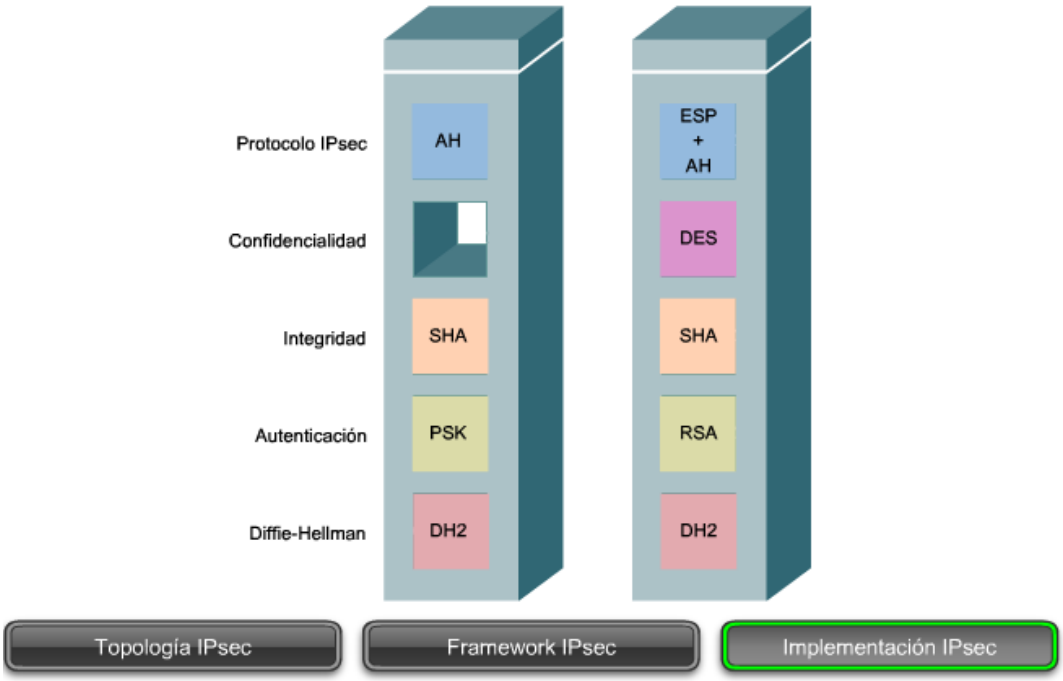
- Es un framework de estándares abiertos, independiente de los algoritmos.
- Provee confidencialidad de datos, integridad de datos y autenticación de origen.

Topología IPsec | Framework IPsec | Implementación IPsec

Haga clic en los botones para ver el contenido asociado.



Haga clic en los botones para ver el contenido asociado.



Haga clic en los botones para ver el contenido asociado.

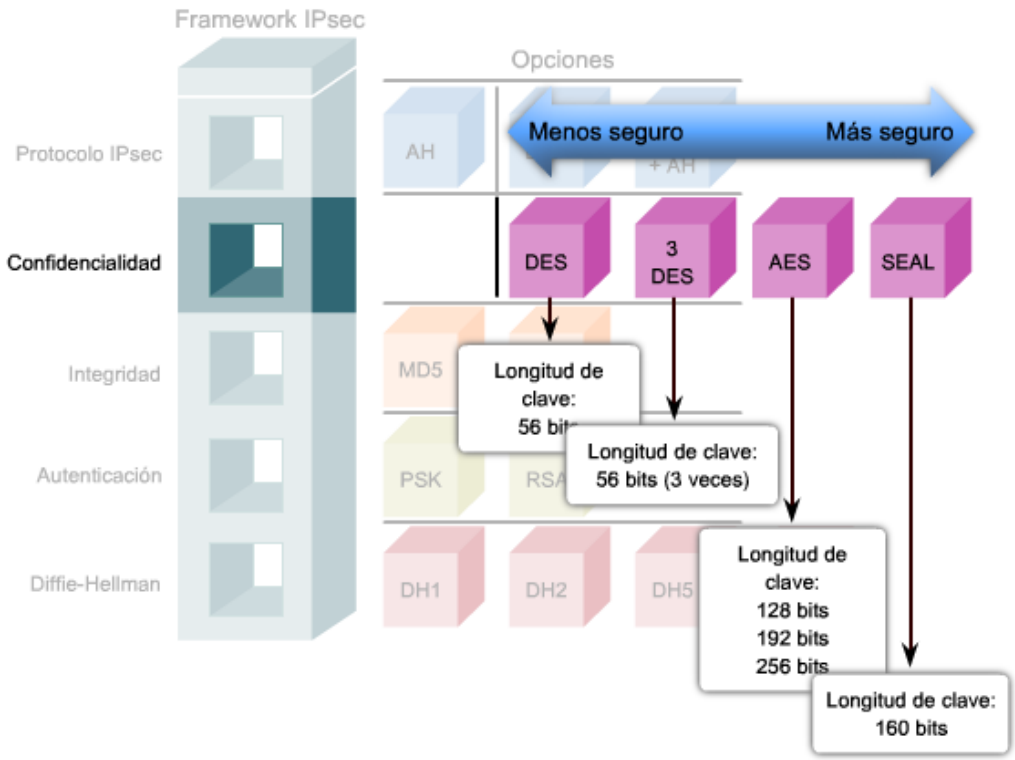
Confidencialidad

La confidencialidad se logra mediante el cifrado del tráfico que transita la VPN. El grado de seguridad depende de la longitud de la clave utilizada por el algoritmo de cifrado. Si alguien intenta romper la clave mediante un ataque de fuerza bruta, el número de posibilidades a probar está en función de la longitud de la clave. El tiempo

de procesamiento de todas las posibilidades depende del poder de cómputo del dispositivo atacante. Mientras más corta sea la clave del algoritmo de cifrado, más fácil es romperla. Una clave de 64 bits puede llevar aproximadamente un año para romperla con una computadora relativamente sofisticada. Romper una clave de 128 bits, con la misma computadora, puede llevar unos 10^19 años.

Los siguientes son algunos algoritmos de cifrado y longitudes de clave que utilizan las VPNs:

DES - Utiliza una clave de 56 bits, asegurando un cifrado de alta performance. DES es un sistema de cifrado de clave simétrica.
3DES - Una variante de DES de 56 bits. 3DES utiliza tres claves independientes de cifrado de 56 bits por cada bloque de 64 bits, proveyendo así un cifrado significativamente más fuerte que DES. 3DES es un sistema de cifrado de clave simétrica.
AES - Provee una seguridad más fuerte que DES y es computacionalmente más eficiente que 3DES. AES ofrece tres longitudes de clave diferentes: 128 bits, 192 bits y 256 bits. AES es un sistema de cifrado de clave simétrica.
Software-Optimized Encryption Algorithm (SEAL)-Es un cifrador de flujo desarrollado en 1993 por Phillip Rogaway y Don Coppersmith, el cual utiliza una clave de 160 bits. SEAL es un sistema de cifrado de clave simétrica.



Integridad

La próxima función crítica de una VPN es la integridad de los datos. Asuma que Jeremy escribe un cheque por $100 a Sonya. El cheque es luego enviado por correo a Sonya, pero es interceptado por un atacante. El atacante cambia el nombre y el monto del

cheque e intenta cobrarlo. Dependiendo de la calidad de la falsificación en el cheque alterado, el atacante puede tener éxito.

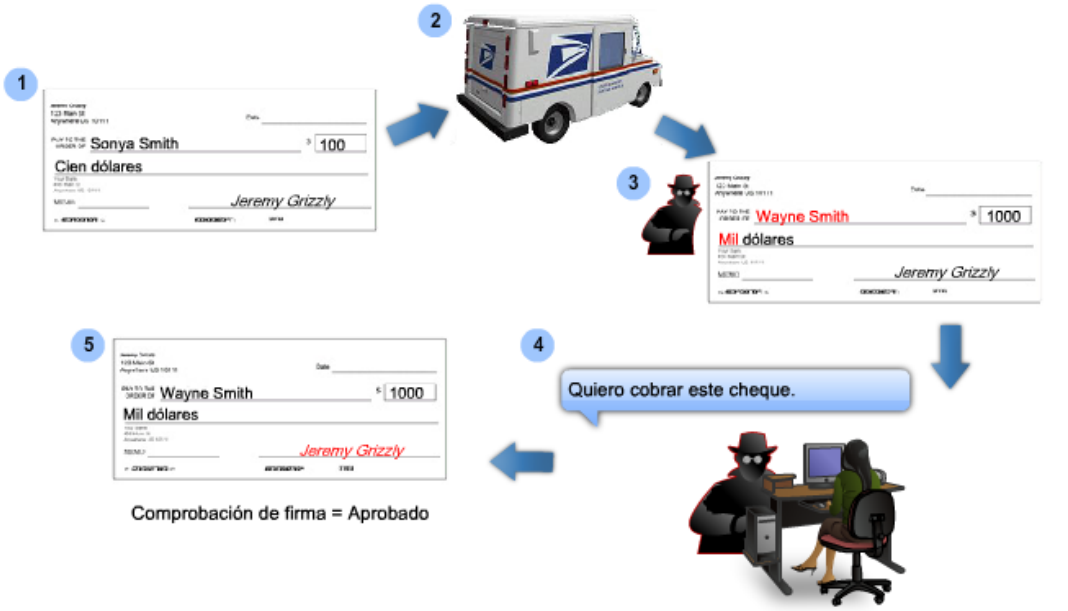
Este escenario se aplica a las VPNs porque los datos son transportados sobre la Internet pública. Potencialmente, estos datos pueden ser interceptados y modificados. Se requiere un método para probar la integridad de los datos y así garantizar que el contenido no ha sido alterado. Un algoritmo de integridad de datos puede proporcionar esta garantía.

Hashed Message Authentication Codes (HMAC) es un algoritmo de integridad de datos que garantiza la integridad del mensaje utilizando un valor de hash. En el dispositivo local, se procesa el mensaje y una clave secreta compartida utilizando un algoritmo de hash, el cual produce un valor de hash. Este valor se agregado al mensaje, el cual es luego enviado a través de la red. En el dispositivo remoto, se recalcula el valor de hash y se compara con el valor de hash recibido. Si el hash transmitido es idéntico al hash calculado, se verifica la integridad del mensaje. Sin embargo, si no coinciden, el mensaje fue alterado y es invalidado.

Existen dos algoritmos HMAC comunes:

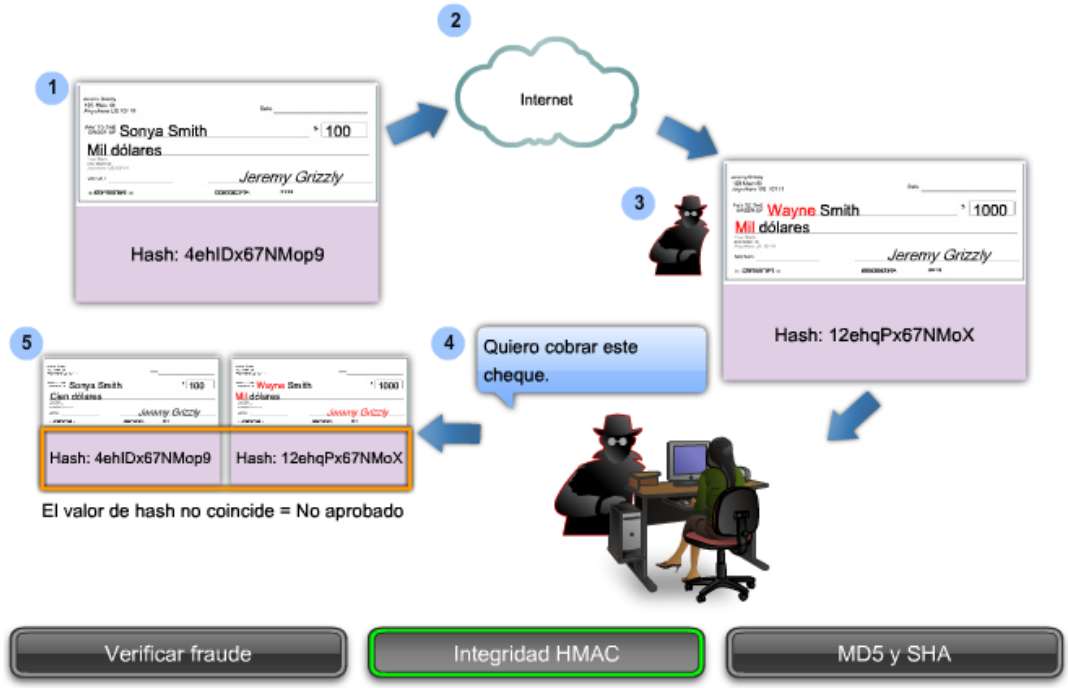
HMAC-Message Digest 5 (HMAC-MD5) - Utiliza una clave secreta compartida de 128 bits. Se combina el mensaje de longitud variable con la clave secreta compartida de 128 bits y se ejecuta el algoritmo de hash HMAC-MD5. La salida es un hash de 128 bits.
HMAC-Secure Hash Algorithm 1 (HMAC-SHA-1) - Utiliza una clave secreta de 160 bits. Se combina el mensaje de longitud variable con la clave secreta compartida de 160 bits y se ejecuta el algoritmo de hash HMAC-SHA-1. La salida es un hash de 160 bits.

HMAC-SHA-1 es considerado más criptográficamente fuerte que HMAC-MD5. Es recomendado cuando es importante obtener una seguridad levemente superior.



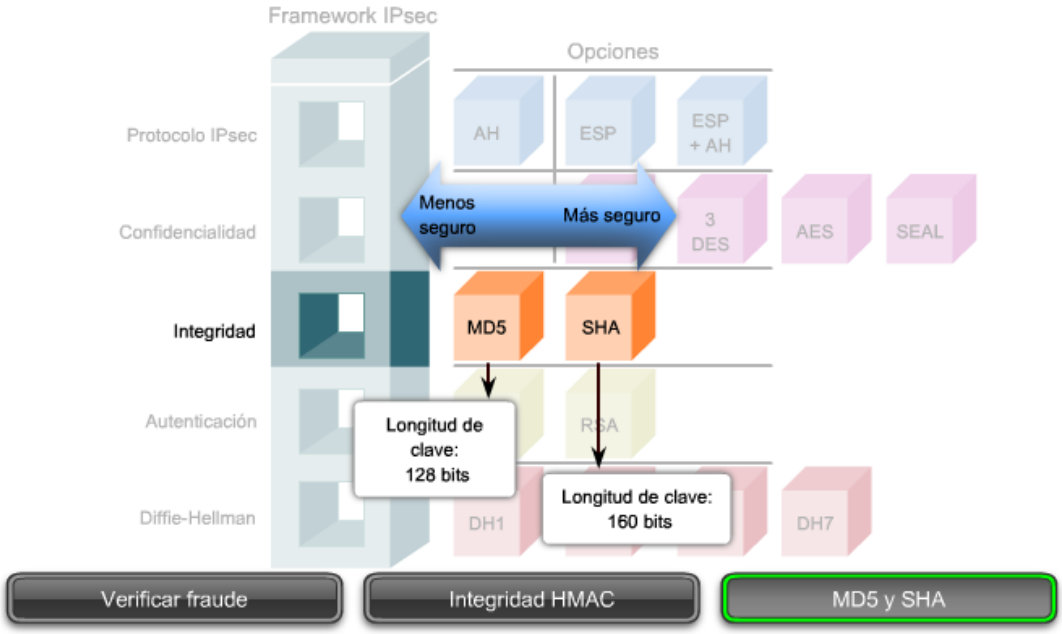
Verificar fraude | Integridad HMAC | MD5 y SHA

Haga clic en los botones para ver el contenido asociado.



Verificar fraude | Integridad HMAC | MD5 y SHA

Haga clic en los botones para ver el contenido asociado.



Haga clic en los botones para ver el contenido asociado.

Autenticación

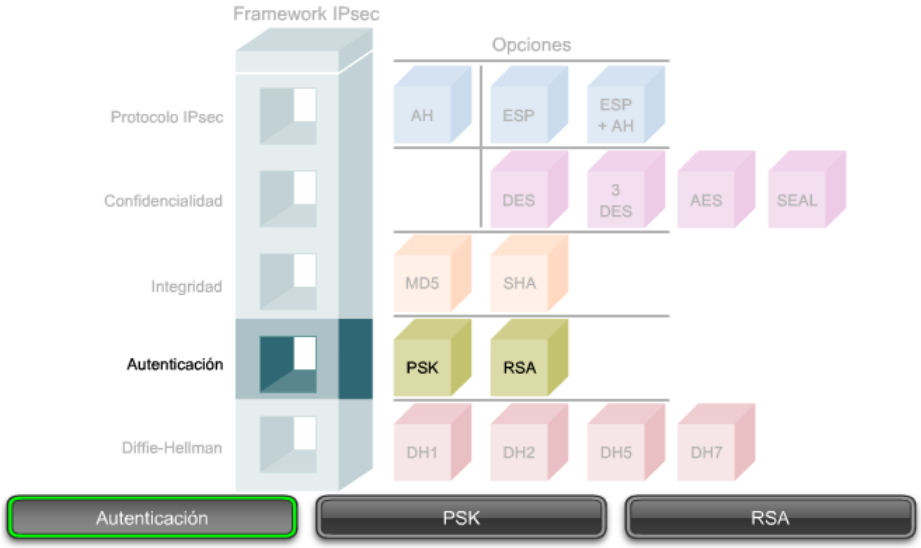
Cuando se realizan negocios a través de grandes distancias, es necesario conocer (autenticar) al individuo en el otro extremo del teléfono, correo electrónico o fax. Lo mismo sucede con las redes VPN. El dispositivo en el otro extremo del túnel VPN debe ser autenticado antes de considerar seguro al camino de la comunicación.

En la Edad Media, un sello garantizaba la autenticidad de un documento. En los tiempos modernos, un documento firmado se legaliza con un sello y una forma. En la era electrónica, un documento se firma utilizando la clave de cifrado privada del remitente, llamada firma digital. Una firma se autentica descifrando la misma con la clave pública del remitente.

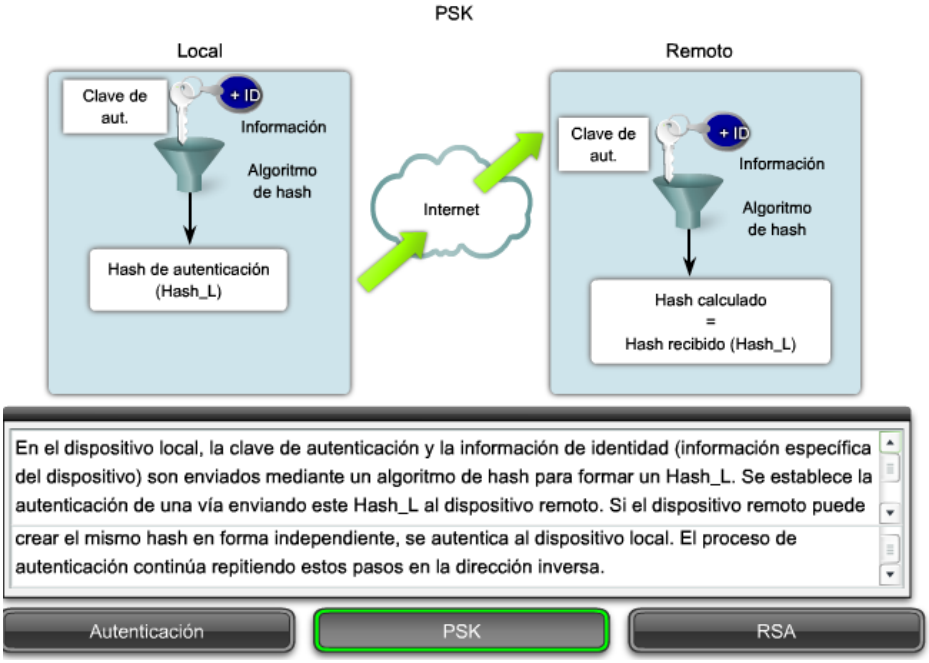
Existen dos métodos principales para configurar la autenticación de pares.

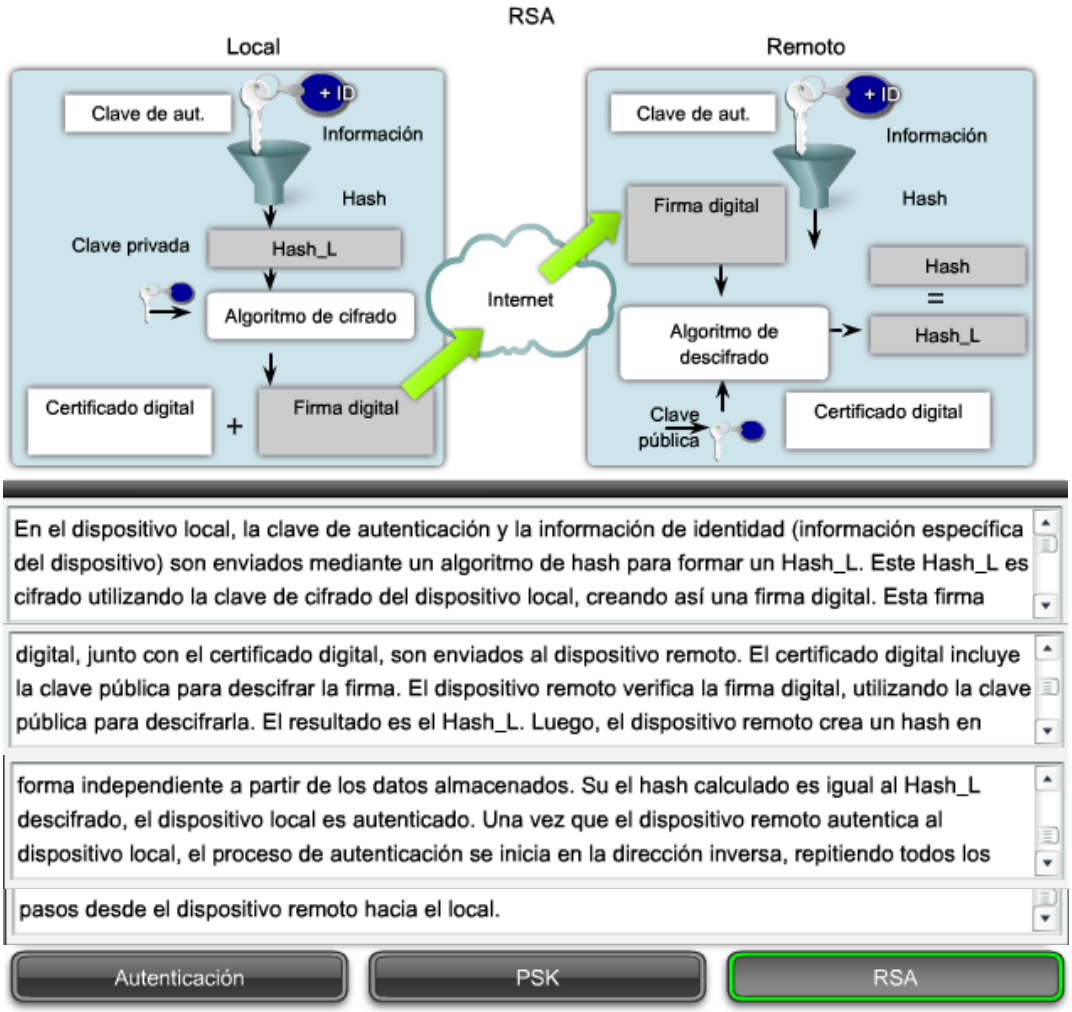
Claves pre-compartidas (Pre-shared Keys - PSKs) - Se ingresa una clave pre-compartida en cada uno de los pares en forma manual y es utilizada para autenticar a cada par. En cada extremo, la PSK se combina con otra información para formar la clave de autenticación. Cada par debe autenticar al par opuesto para que el túnel pueda considerarse seguro. Las claves pre-compartidas son fáciles de configurar en forma manual, pero no son muy escalables, ya que cada par IPsec debe estar configurado con la clave pre-compartida de cada uno de los demás pares con los cuales se comunica. Firmas RSA - El intercambio de certificados digitales autentica a los pares. El dispositivo local calcula un hash y lo cifra con su clave privada. El hash cifrado se agrega al mensaje, el cual es enviado al extremo remoto y funciona como una firma. En el extremo remoto, el hash cifrado es descifrado utilizando la clave pública del extremo local. Si el hash descifrado coincide con el hash recalculado, la firma es genuina. Cada par debe autenticar a su par opuesto para que el túnel pueda considerarse seguro.

Un tercer método de obtener la autenticación es mediante números de único uso (nonces - numbers used once) cifrados con RSA. Estos números son generados en forma aleatoria por cada par. Este método requiere que la clave pública de uno de los dos pares sea conocida por el otro par antes de que el envío del tercer y cuarto mensaje del intercambio IKE se lleven a cabo. Por este motivo, las claves públicas deben copiarse en forma manual en cada par, como parte del proceso de configuración. Este método de autenticación es el menos utilizado.



Haga clic en los botones para ver el contenido asociado.





Intercambio seguro de claves

Los algoritmos de cifrado como DES, 3DES y AES, además de los algoritmos de hashing MD5 y SHA-1, requieren una clave secreta simétrica compartida para ejecutar las funciones de cifrado y descifrado. ¿Cómo obtienen los dispositivos la clave secreta compartida?

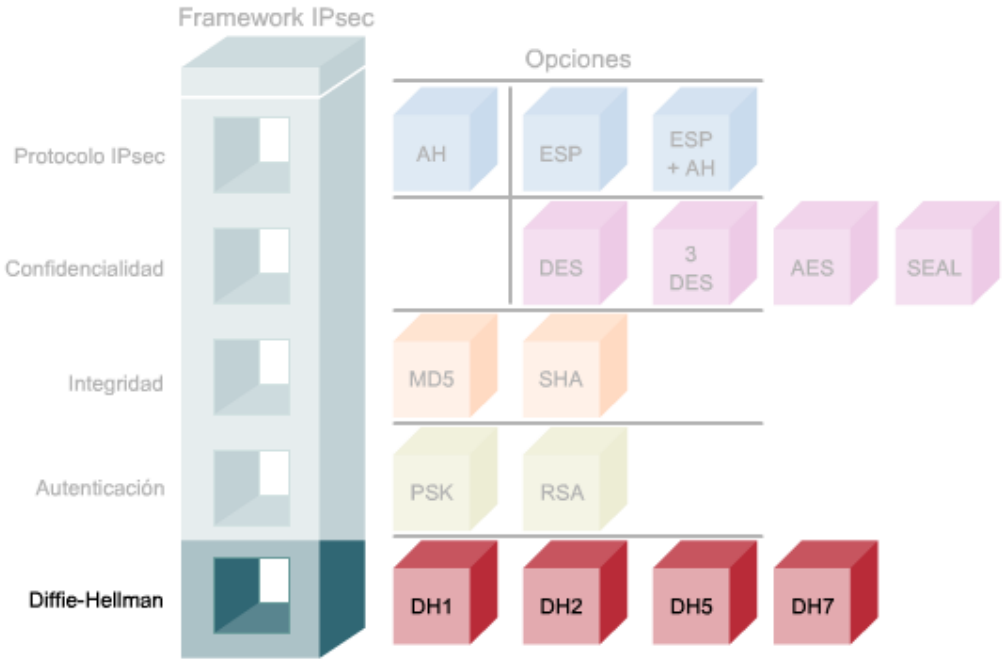
Es posible utilizar el correo electrónico, un mensajero o el correo postal nocturno, para enviar las claves secretas compartidas a los administradores de los dispositivos. Pero el método más fácil de intercambio de claves es el método de intercambio de claves públicas entre los dispositivos de cifrado y descifrado.

El Intercambio de claves Diffie-Hellman (DH) es un método de intercambio de claves públicas que proporciona un método para establecer una clave pública secreta entre dos pares que sólo ellos conocen, incluso cuando se comuniquen a través de un canal no seguro.

Las variaciones del algoritmo de intercambio de claves DH son conocidas como grupos DH. Existen cuatro grupos DH: 1, 2, 5 y 7.

Los grupos DH 1, 2 y 5 soportan exponenciación sobre un módulo primo con un tamaño de clave de 768 bits, 1024 bits y 1536 bits, respectivamente.
Los clientes Cisco 3000 soportan los grupos DH 1, 2 y 5. El cifrado DES y 3DES soportan los grupos DH 1 y 2.
El cifrado AES soporta los grupos DH 2 y 5.
El cliente Certicom movianVPN soporta el grupo 7.
El grupo 7 soporta criptografía de curva elíptica (Elliptical Curve Cryptography - ECC), la cual reduce el tiempo necesario para generar las claves.

Durante la configuración del túnel, los pares VPN negocian qué grupo DH utilizarán

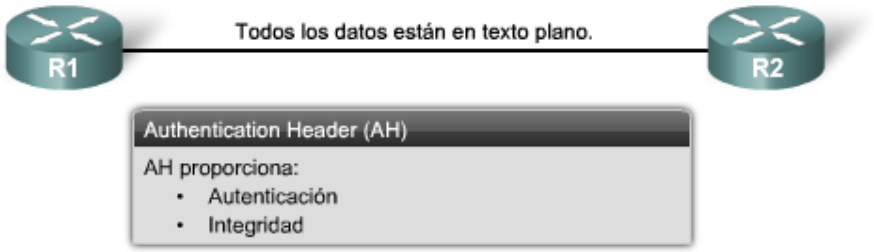


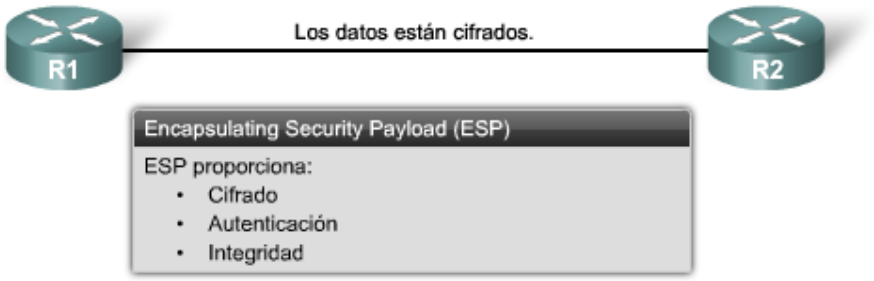
8.3.2 Protocolos de seguridad IPSEC

Psec es un framework de estándares abiertos. IPsec detalla los mensajes para asegurar las comunicaciones, pero se basa en algoritmos existentes. Los dos protocolos principales del framework IPsec son AH y ESP. El protocolo IPsec es el primer bloque de construcción del framework. La selección de AH o ESP establece qué otros bloques estarán disponibles:

Authentication Header (AH) - AH, que es el protocolo IP 51, es el protocolo apropiado para utilizar cuando no se requiere o no se permite la confidencialidad. Asegura que el origen de los datos es R1 o R2 y verifica que los datos no han sido modificados durante la transmisión. AH no provee confidencialidad de datos (cifrado) de los paquetes. Todo el texto se transporta sin cifrar. Si se utiliza únicamente el protocolo AH, se provee una protección débil.

Encapsulating Security Payload (ESP) - ESP, que es el protocolo IP 50, puede proveer confidencialidad y autenticación. Proporciona confidencialidad ejecutando el cifrado de los paquetes IP. El cifrado de estos paquetes resguarda los datos y la identidad tanto del origen como del destino. ESP provee autenticación para el paquete IP interno y el encabezado ESP. La autenticación proporciona la autenticidad del origen de los datos y la integridad de los mismos. Aunque tanto el cifrado como la autenticación son opcionales en ESP, debe seleccionarse uno como mínimo.





Encabezado de autenticación

AH logra la autenticación aplicando funciones hash de una vía con clave al paquete, para crear el hash correspondiente. Este hash se combina con el texto y se transmite. El receptor detecta si hubo cambios en cualquier parte del paquete durante su transmisión, ejecutando la misma función hash de una vía sobre el paquete recibido, comparando luego el resultado con el valor del hash recibido. El hecho de que el hash de una vía involucre una clave secreta compartida por ambos sistemas asegura además la autenticidad.

La función AH se aplica al paquete completo, excepto por aquellos campos del encabezado IP que se modifican durante la transmisión. Por ejemplo, los campos TTL (Time To Live) que son modificados por los routers durante la transmisión de los datos son campos mutables.

El proceso AH ocurre en el siguiente orden:

1. Se calcula el hash sobre el encabezado IP y los datos del paquete, utilizando la clave secreta compartida.

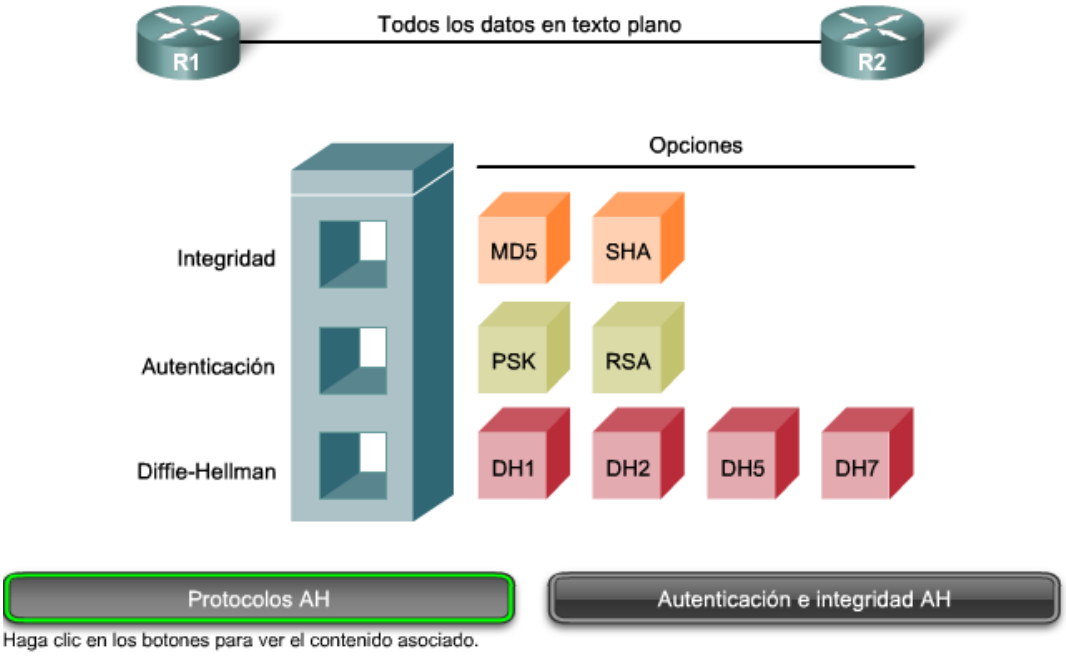
2. El hash construye un nuevo encabezado AH, el cual es insertado en el paquete original.

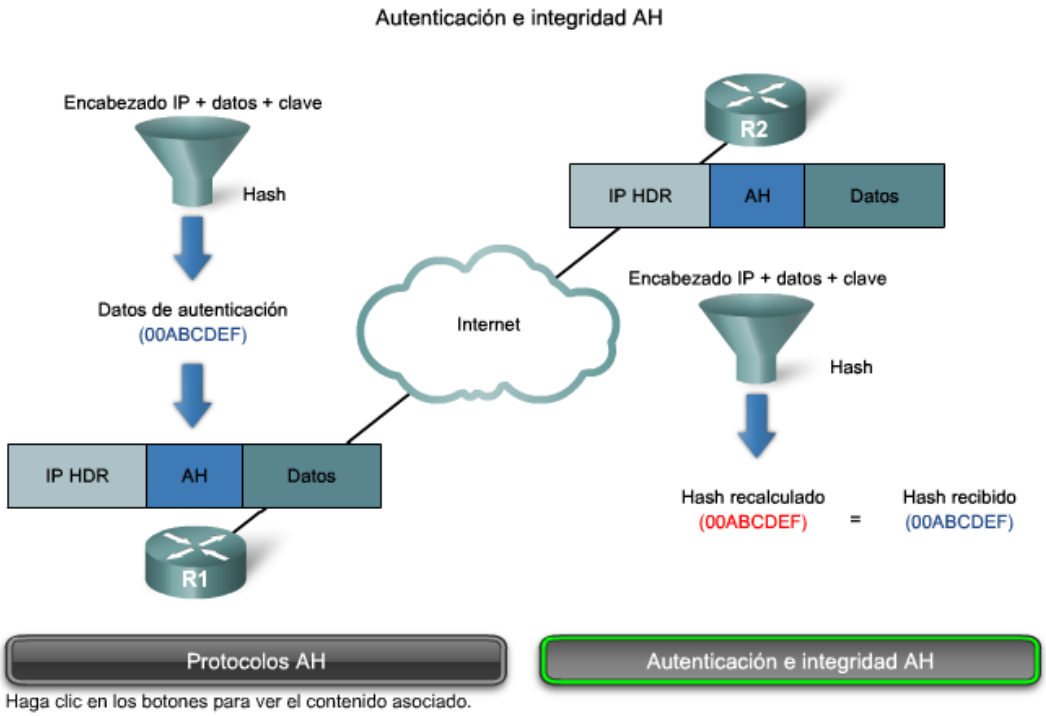
3. Se transmite el nuevo paquete al router IPsec correspondiente.

4. El router destinatario calcula el hash del encabezado y los datos del paquete, utilizando la clave secreta compartida, extrae el hash transmitido en el encabezado AH y compara ambos hashes.

Los hashes deben coincidir perfectamente. Si se modificó al menos un bit en el paquete transmitido, el hash calculado sobre el paquete transmitido es diferente y no será igual al transmitido en el encabezado AH.

AH soporta los algoritmos HMAC-MD5 y HMAC-SHA-1. AH puede presentar problemas si el entorno utiliza NAT.





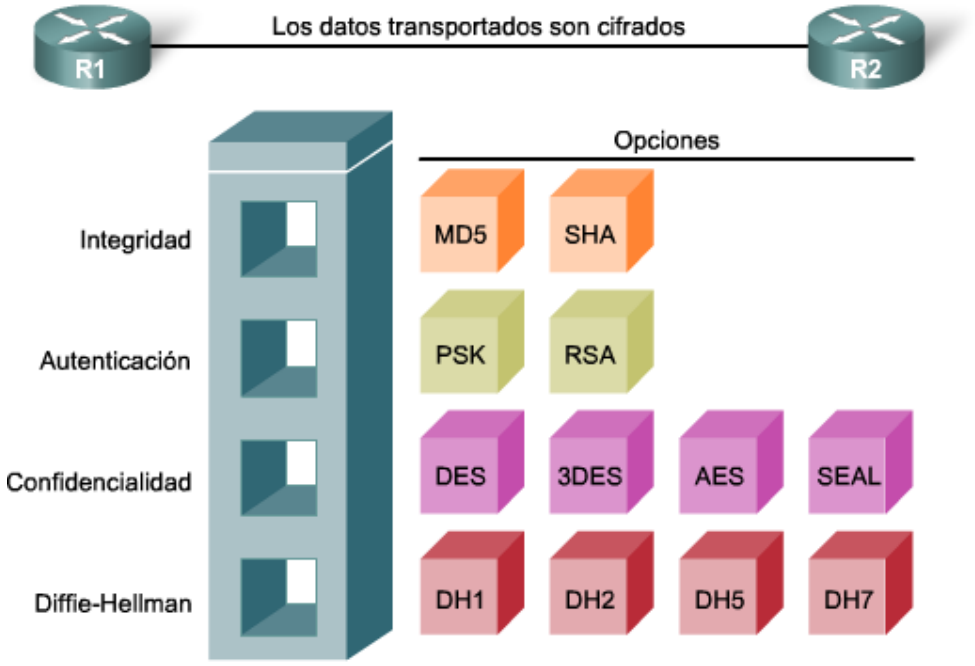
ESP

ESP provee confidencialidad cifrando los datos. Soporta una variedad de algoritmos de cifrado simétricos. Si se selecciona ESP como protocolo IPsec, debe también seleccionarse un algoritmo de cifrado. El algoritmo por defecto para IPsec es DES de 56 bits. Los productos Cisco también soportan el uso de 3DES, AES y SEAL, para un cifrado más fuerte.

ESP puede proveer integridad y autenticación. Primero, se cifran los datos. Luego, los datos cifrados se procesan con un algoritmo de hash, HMAC-MD5 o HMAC-SHA-1. El hash provee autenticación e integridad de datos del paquete.

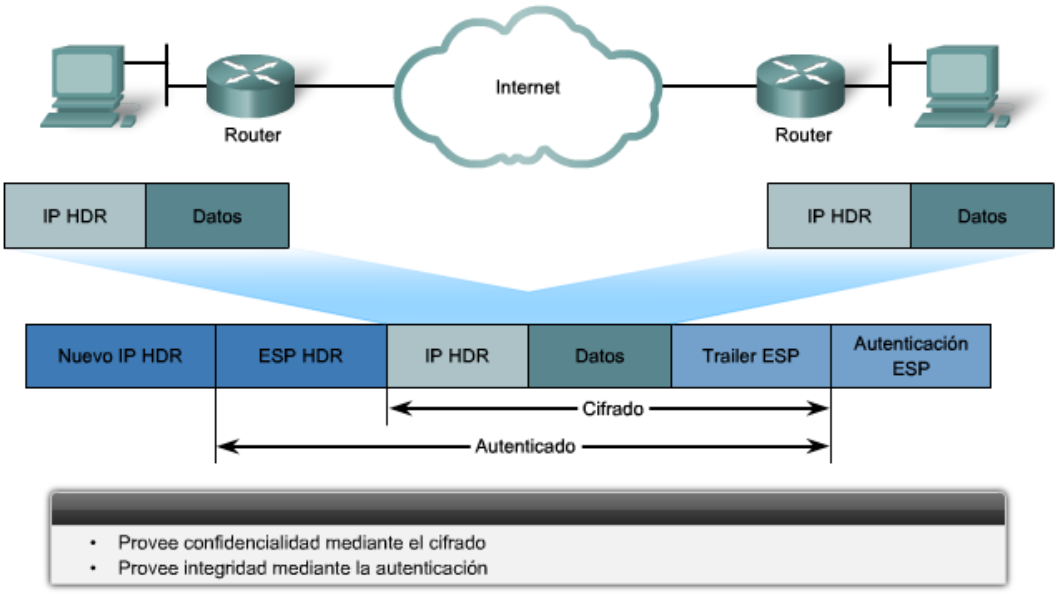
Opcionalmente, ESP puede imponer protección contra ataques de repetición. La protección contra ataques de repetición verifica que cada paquete sea único y no pueda ser duplicado. Esta protección asegura que un hacker no pueda interceptar paquetes e insertar paquetes modificados en el flujo de datos. La protección contra ataques de repetición funciona haciendo un seguimiento de los números de secuencia de los paquetes y utilizando una ventana deslizante en el extremo destino. Cuando se establece una conexión entre el origen y el destino, se inicializan sus contadores en cero. Cada vez que se envía un paquete, se agrega un número de secuencia en el origen del paquete. El destino utiliza la ventana deslizante para determinar qué número de secuencia se espera. El destino verifica que el número de secuencia del paquete no esté duplicado y es recibido en el orden correcto. Por ejemplo, si la ventana deslizante del destino está configurada en 1, el destino espera recibir el paquete con el número de secuencia 1. Luego de recibirlo, la ventana deslizante se mueve al 2. Cuando ocurre la detección de un paquete duplicado, como por ejemplo si el destino recibe un segundo paquete con el número de secuencia 1, se envía un mensaje de error, el paquete duplicado se descarta y se registra el evento.

La protección anti-replay es generalmente utilizada con ESP, pero también es soportada por AH.



Los datos originales están bien protegidos por ESP porque se cifra el paquete IP original y la cola (trailer) ESP. Con la autenticación ESP, se incluyen en el proceso de hashing el paquete IP y la cola cifrados y el encabezado ESP. Finalmente, se agrega un nuevo encabezado IP al paquete autenticado. Se utiliza la nueva dirección IP para enrutar el paquete a través de Internet.

Cuando se seleccionan tanto autenticación como cifrado, primero se realiza el cifrado. Una razón para aplicar este orden de procesamiento es que facilita la rápida detección y descarte de paquetes duplicados o defectuosos en el dispositivo destino. Previo al descifrado del paquete, el receptor puede autenticar el contenido. Haciendo esto, se pueden detectar problemas con rapidez y reducir potencialmente el impacto de los ataques DoS.



ESP y AH pueden aplicarse a los paquetes IP de dos formas diferentes, en modo transporte y en modo túnel.

Modo transporte

En el modo transporte, la seguridad es provista sólo a partir de la capa de transporte del modelo OSI y las capas superiores. El modo transporte protege los datos del paquete pero mantiene la dirección IP original en texto plano. La dirección IP original puede utilizarse para enrutar el paquete a través de Internet.

El modo de transporte ESP es utilizado entre hosts. El modo de transporte funciona bien con GRE, porque GRE esconde las direcciones de los dispositivos finales agregando su propia IP.

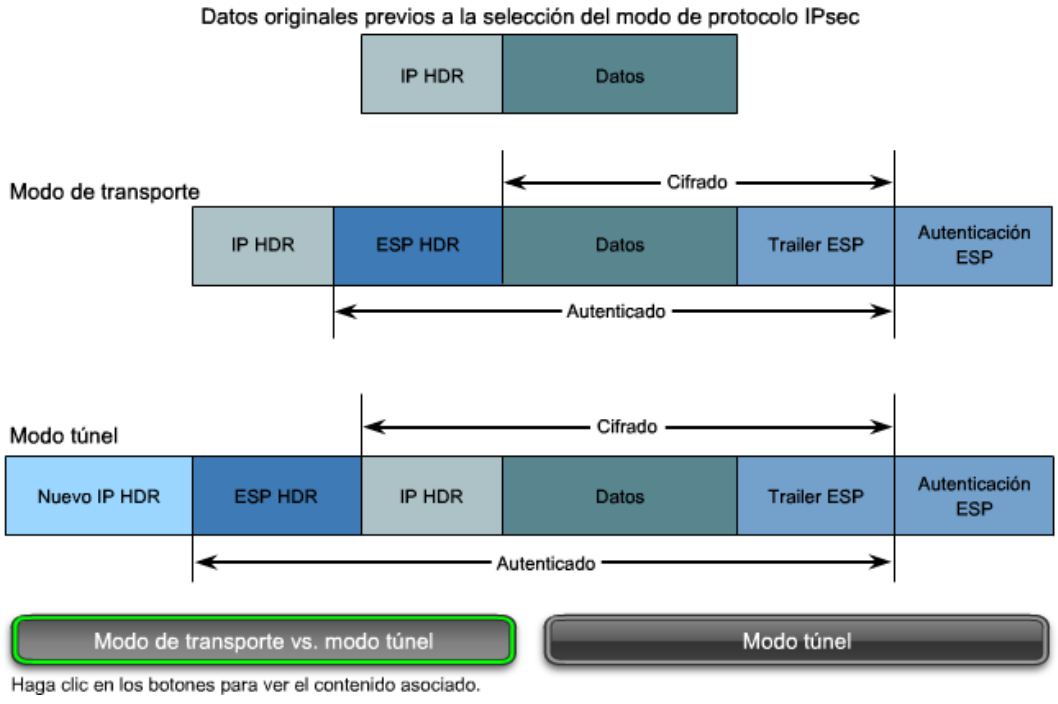
Modo túnel

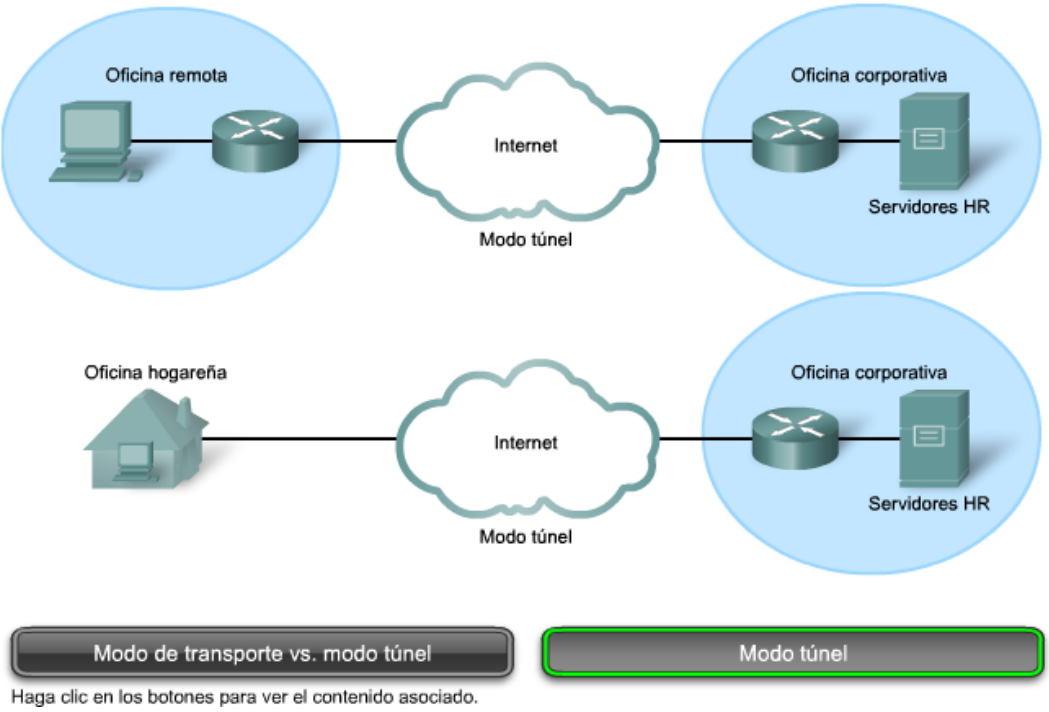
El modo túnel provee seguridad para el paquete IP original completo. El paquete IP original se cifra y luego es encapsulado en otro paquete IP. Esto es conocido como "Cifrado IP en IP". La dirección IP del paquete IP externo es utilizada para enrutar el paquete a través de Internet.

El modo túnel ESP es utilizado entre el host y un gateway de seguridad o entre dos gateways de seguridad. Para las aplicaciones "gateway a gateway", en lugar de cargar IPsec en todas las computadoras de las oficinas remotas y centrales, es más sencillo ejecutar el cifrado IP en IP y la encapsulación en los gateways de seguridad.

El modo túnel ESP es utilizado en la aplicación IPsec de acceso remoto. Una oficina hogareña puede no disponer de un router para realizar el cifrado y encapsulación IPsec. En este caso, se ejecuta un cliente IPsec en la PC, el cual realiza la encapsulación y cifrado IPsec. Luego, en la oficina corporativa, el router es quien desencapsula y descifra el paquete.

El proceso VPN involucra la selección y aplicación de muchos parámetros. ¿Cómo negocia IPsec estos parámetros de seguridad?





8.3.3 Intercambios de claves en Internet

La solución VPN IPsec negocia los parámetros de intercambio de claves, establece una clave compartida, autentica al otro extremo y negocia los parámetros de cifrado. Los

parámetros negociados entre los dispositivos se conocen como asociación de seguridad (Security Association - SA).

Asociaciones de seguridad

Un SA es un bloque de construcción básico de IPsec. Las asociaciones de seguridad son mantenidas dentro de una base de datos de SA (SADB), la cual se establece en cada dispositivo. Una VPN tiene registros SA que definen los parámetros de cifrado IPsec y registros SA que definen los parámetros de intercambio de claves.

Todos los sistemas criptográficos, incluyendo el cifrado César, el cifrado Vigenere, la máquina Enigma y hasta los algoritmos de cifrado modernos, deben lidiar con problemas de administración de claves. Diffie-Hellman (DH) es utilizado para crear una clave secreta compartida. Sin embargo, IPsec utiliza el protocolo Internet Key Exchange (IKE) para establecer el proceso de intercambio de claves.

En lugar de transmitir las claves en forma directa a través de la red, IKE calcula las claves compartidas en base al intercambio de una serie de paquetes de datos. Esto evita que un tercero pueda descifrar las claves, incluso si logra capturar todos los datos intercambiados utilizados para calcularlas.

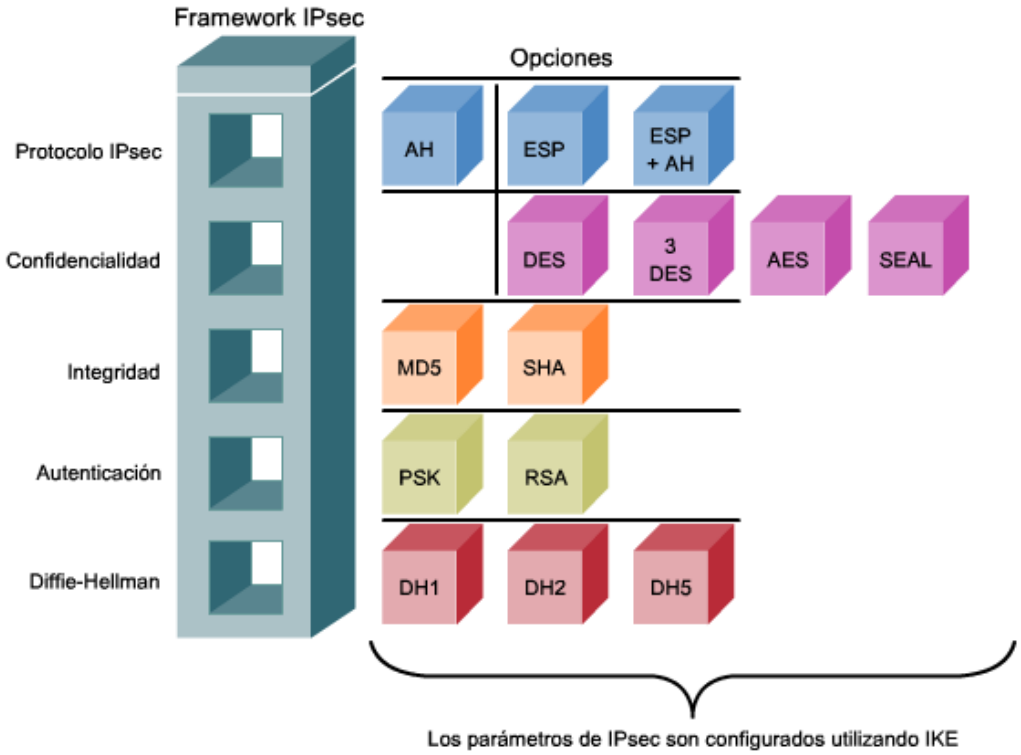
IKE utiliza el puerto UDP 500 para intercambiar la información IKE entre los gateways de seguridad. Los paquetes del puerto UDP 500 deben estar permitidos en todas las interfaces IP involucradas en la conexión de ambos extremos.

IKE está definido en la RFC2409. Se trata de un protocolo híbrido, que combina el protocolo ISAKMP (Internet Security Association and Key Management Protocol) y los métodos de intercambio de claves Oakley y Skeme. ISAKMP define el formato del mensaje, la mecánica del protocolo de intercambio de claves y el proceso de negociación para construir un SA para IPsec. ISAKMP no define cómo se administran o comparten las claves entre los pares IPsec. Oakley y Skeme tienen cinco grupos de claves definidos. De estos grupos, los routers Cisco soportan el Grupo 1 (claves de 768 bits), Grupo 2 (claves de 1024 bits) y Grupo 5 (claves de 1536 bits).

IKE combina estos protocolos para establecer conexiones IPsec seguras entre los dispositivos. Establece las SAs acordadas entre los pares. Cada par debe tener idénticos ISAKMP y parámetros IPsec, para establecer una VPN operacional y segura. Notar que los términos ISAKMP y IKE con comúnmente utilizados en la industria para referirse a IKE.

Una alternativa a la utilización de IKE es configurar en forma manual todos los parámetros requeridos para establecer una conexión segura IPsec. Este proceso es poco práctico, ya que no es escalable.

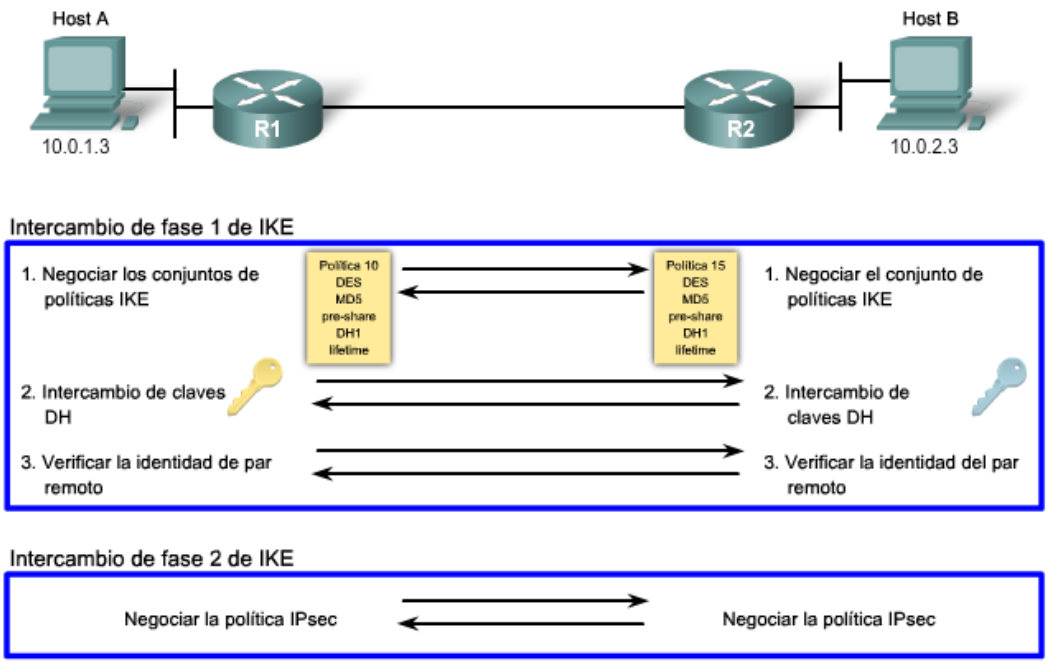
¿Cómo funciona IKE?



Para establecer un canal de comunicación segura entre dos pares, el protocolo IKE ejecuta dos fases:

Fase 1 - Dos pares IPsec realizan la negociación inicial de SAs. El propósito básico de la fase 1 es negociar los conjuntos de políticas IKE, autenticar a los pares y establecer un canal seguro entre ellos. Puede implementarse de un modo principal (contacto inicial, más largo) o de un modo agresivo (luego del contacto inicial).
Fase 2 - EL proceso IKE ISAKMP negocia los SAs en nombre de IPsec. Puede ser negociado en un modo rápido.

En la fase 1 se determinan los conjuntos de transformación, los métodos de hash y otros parámetros. Una sesión IKE comienza con un router (el iniciador) que envía una propuesta al otro router (el receptor). La propuesta enviada por el iniciador define qué protocolos de cifrado y autenticación son aceptables, por cuánto tiempo deben permanecer activas las claves y si debe aplicarse PFS (Perfect Forward Secrecy). PFS es una propiedad que asegura que las claves utilizadas para proteger los datos no sean utilizadas para derivar ninguna otra clave. PFS asegura que si una clave se ve comprometida, las claves anterior y posterior permanecen seguras.



Ocurren tres intercambios durante la fase 1 de IKE. Son conocidos como primer, segundo y tercer intercambio.

Primer intercambio

El primer intercambio entre el iniciador y el receptor establece la política básica de seguridad. Los pares negocian y se ponen de acuerdo sobre los algoritmos y hashes que se utilizarán para asegurar las comunicaciones IKE. En lugar de negociar cada protocolo en forma individual, los protocolos se agrupan en conjuntos, llamados conjuntos de políticas IKE. Primero se intercambian los conjuntos de políticas IKE.

El iniciador transmite primero las propuestas para los esquemas de cifrado y autenticación a utilizar. El receptor busca una política ISAKMP adecuada. El receptor selecciona la propuesta que mejor se adapte a su situación de seguridad y envía luego otra propuesta al iniciador. Si se encuentra una política que coincida entre los pares, continúa la fase 1 de IKE. Si no se encuentran coincidencias, se da de baja el túnel.

Los números de los conjuntos de políticas son sólo significativos para el dispositivo VPN y no se corresponden entre dos pares VPN. En una aplicación punto a punto, cada extremo puede requerir sólo una única política IKE definida. En un ambiente hub-and-spoke, el sitio central puede requerir múltiples políticas IKE para satisfacer a todos los pares remotos.

Segundo intercambio

El segundo intercambio crea e intercambia las claves públicas DH entre los dos extremos. DH permite a dos participantes, que no tenían conocimiento previo entre ellos, establecer una clave secreta compartida sobre un canal de comunicación no seguro.

Los dos pares ejecutan el protocolo de intercambio de claves DH para adquirir el material necesario por los diferentes algoritmos de cifrado y hashing sobre los que IKE e IPsec deben ponerse de acuerdo.

Existen diferentes niveles de intercambios de claves DH disponibles en el software Cisco IOS:

DH Grupo 1 - Resulta en 768 bits de datos para generar claves. Este grupo es la opción usual cuando el algoritmo de cifrado es DES.
DH Grupo 2 - Resulta en 1024 bits de datos para generar claves. Este grupo es la opción usual cuando el algoritmo de cifrado es 3DES.
DH Grupo 5 - Resulta en 1536 bits de datos para generar claves. DH 5 debe ser utilizado con AES.
DH Grupo 7 (criptografía de curva elíptica [ECC]) - Genera claves IPsec cuando el campo de curva elíptica es de 163 bits. Este grupo fue diseñado para ser utilizado con hosts de poca potencia, como las PDAs.

Es importante contar con suficientes datos para generar claves, para el algoritmo seleccionado. Utilizando el algoritmo DH, cada par genera una clave secreta compartida sin efectuar realmente un intercambio. Todas las negociaciones posteriores estarán cifradas utilizando la clave secreta generada por DH.

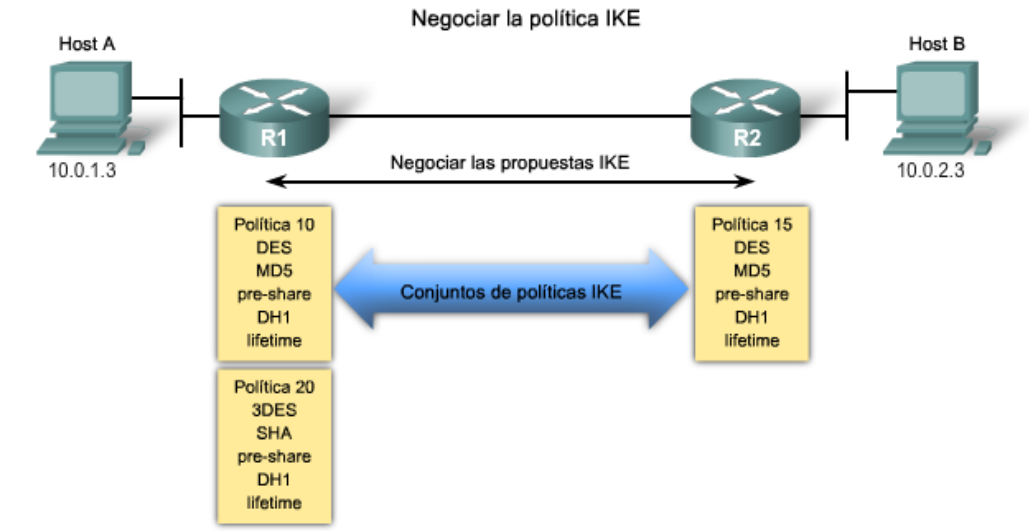
Tercer intercambio

Cada dispositivo final debe autenticar al otro extremo antes de considerar seguro el camino de la comunicación. El último intercambio de la fase 1 de IKE autentica al par remoto.

El iniciador y el receptor se autentican mutuamente utilizando uno de los tres métodos de autenticación de datos origen:

PSK
Firma RSA
Número cifrado de un solo uso RSA

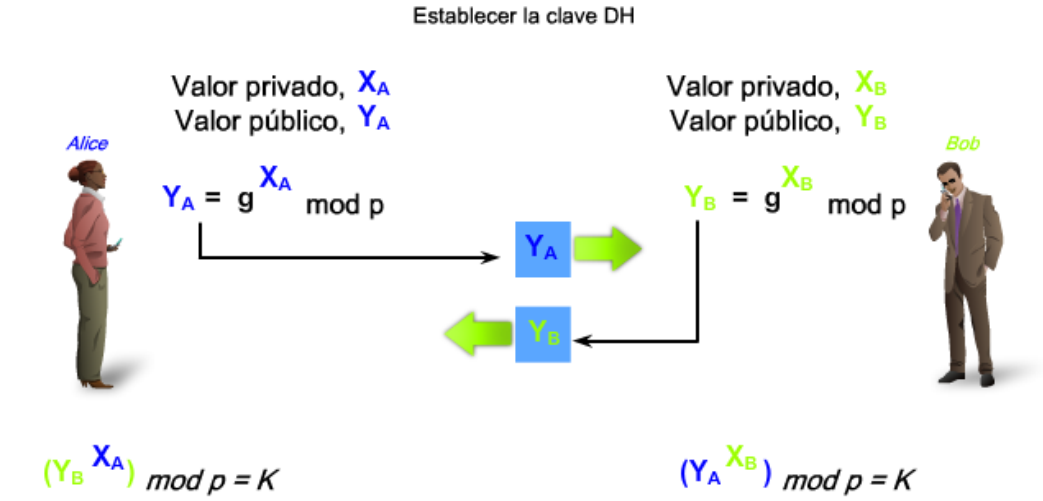
Las negociaciones SA de la fase 1 son bidireccionales, es decir, los datos pueden ser enviados y recibidos utilizando la misma clave de cifrado. Incluso si el flujo de datos de la negociación SA entre dos pares IPsec se ve comprometida, existen muy pocas posibilidades de que las claves de cifrado puedan ser descifradas.



Negocia políticas IKE compatibles para proteger el intercambio IKE

Primer intercambio | Segundo intercambio | Tercer intercambio

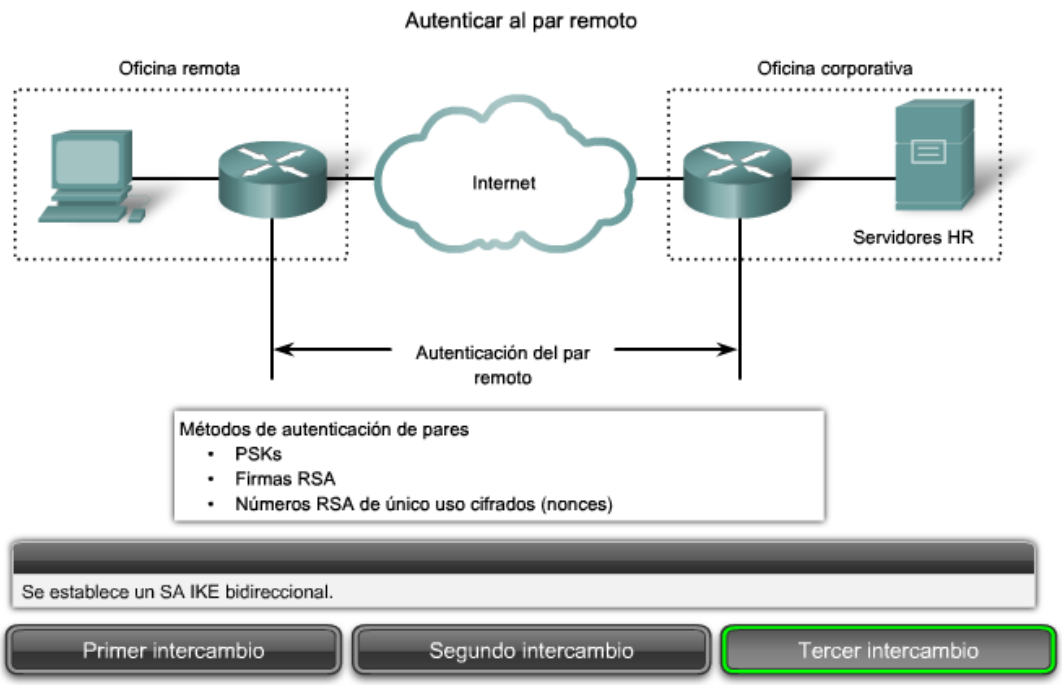
Hacer click sobre los botones para ver el contenido asociado.



Se realiza un intercambio DH para establecer el material generador de claves.

Primer intercambio | Segundo intercambio | Tercer intercambio

Hacer click sobre los botones para ver el contenido asociado.



Los tres intercambios de la fase 1 de IKE ocurren en lo que se denomina modo principal. El resultado del modo principal es un camino de comunicación seguro para los intercambios siguientes entre los pares.

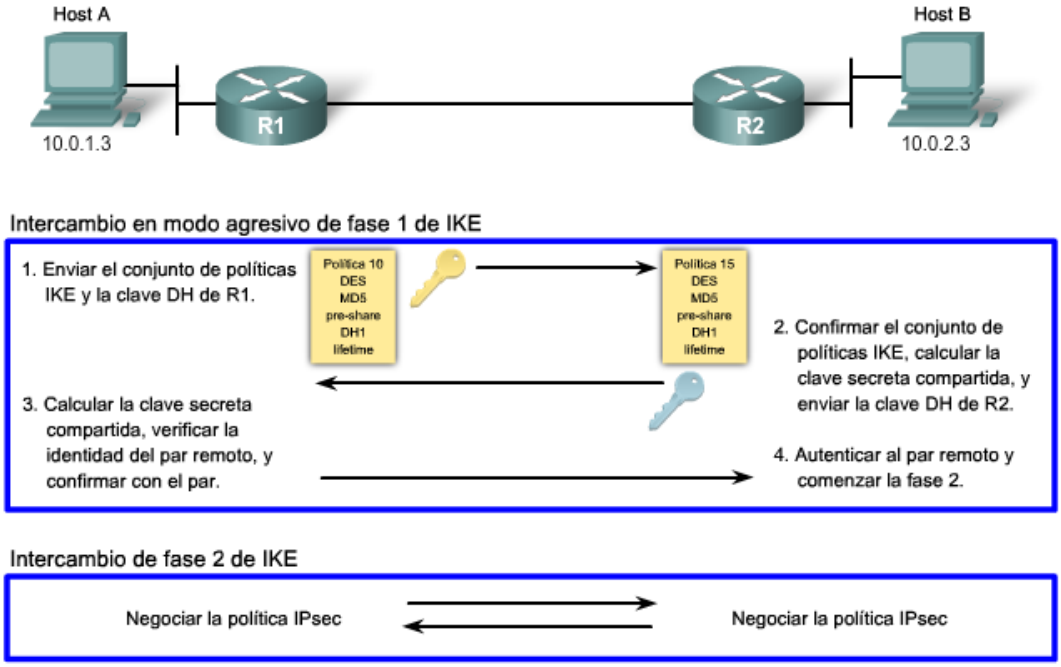
La fase 1 de IKE puede desarrollarse también en modo agresivo. Este modo es más rápido que el modo principal porque hay menos intercambios. El modo agresivo comprime las fases de negociación SA de IKE en un solo intercambio con tres paquetes. El modo principal requiere tres intercambios con seis paquetes.

Los paquetes del modo agresivo incluyen:

Primer paquete - El iniciador empaqueta todo lo necesario para la negociación SA en el primer mensaje, incluyendo la clave pública DH.
Segundo paquete - El receptor responde con los parámetros aceptables, información de autenticación y su clave pública DH.
Tercer paquete - El iniciador luego envía una confirmación de recepción de la información.

La negociación del modo agresivo es más rápida y las ID del iniciador y del receptor se trasmiten en texto plano.

Una vez establecida la SA de IKE, comienza la negociación de la fase 2.

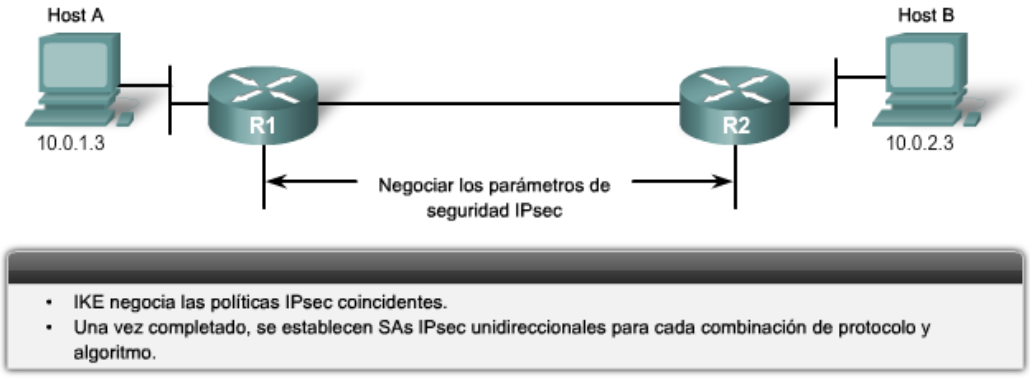


El objetivo de la fase 2 de IKE es negociar los parámetros de seguridad IPsec que serán utilizados para asegurar el túnel IPsec. La fase 2 es llamada modo rápido y sólo puede ocurrir una vez que IKE ha establecido el túnel seguro en la fase 1. El proceso IKE ISAKMP negocia las SAs en nombre de IPsec, que necesita las claves de cifrado para operar. El modo rápido negocia las SAs de la fase 2. En esta fase, las SAs utilizadas por IPsec son unidireccionales. Por lo tanto, se requiere un intercambio de claves separado por cada flujo de datos.

La fase 2 de IKE ejecuta las siguientes funciones:

Negocia los parámetros de seguridad IPsec, conocidos como conjuntos de transformación IPsec
Establece las SAs IPsec
Renegocia las SAs IPsec en forma periódica, para asegurar la seguridad
Opcionalmente, realiza un intercambio DH adicional

El modo rápido también renegocia una nueva SA IPsec cuando expira el tiempo de vida de una SA. Básicamente, el modo rápido refresca los datos de generación de claves que crea la clave secreta compartida, basada en los datos de generación de claves derivados del intercambio DH en la fase 1.



8.4 Implementacion de VPNs IPsec sitio a sitio con CLI

8.4.1 Configuracion de una VPN IPsec de sitio a sitio

Una VPN es un canal de comunicación utilizado para formar una conexión lógica entre dos extremos sobre una red pública. Las VPNs no necesariamente incluyen cifrado y autenticación. Las VPNs IPsec utilizan el protocolo IKE para establecer comunicaciones seguras.

La negociación de una VPN IPsec involucra diferentes pasos, los cuales incluyen las fases 1 y 2 de la negociación IKE.

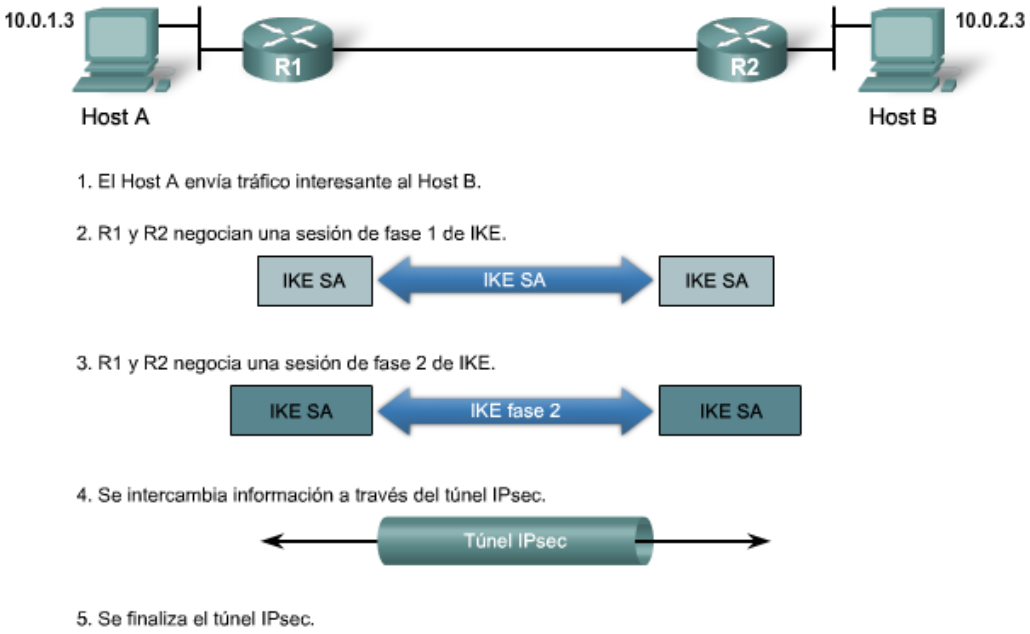
1. Un túnel IPsec se inicia cuando un host A envía tráfico "interesante" al host B. El tráfico es considerado interesante cuando viaja entre los pares IPsec y cumple con los criterios definidos en una crypto ACL.

2. Comienza la fase 1 de IKE. Los pares IPsec negocian la política de asociación de seguridad (SA) IKE. Cuando los pares son autenticados, se crea un túnel seguro utilizando ISAKMP.

3. Comienza la fase 2 de IKE. Los pares IPsec utilizan el túnel seguro autenticado para negociar las transformaciones SA IPsec. La negociación de la política compartida determina cómo se establecerá el túnel IPsec.

4. Se crea el túnel IPsec y se transfieren los datos entre los pares IPsec de acuerdo a los parámetros configurados en los conjuntos de transformación IPsec.

5. El túnel IPsec termina cuando se eliminan las SAs IPsec o cuando expira su tiempo de vida.



Deben completarse algunas tareas básicas para configurar una VPN IPsec de sitio a sitio.

Tarea 1. Asegurar que las ACLs configuradas en la Interfaz son compatibles con la configuración IPsec. Usualmente existen restricciones en las interfaces utilizadas por el tráfico VPN. Por ejemplo, bloquear todo el tráfico que no sea IPsec o IKE.

Tarea 2. Crear una política ISAKMP para determinar los parámetros ISAKMP que serán utilizados para establecer el túnel.

Tarea 3. Definir el conjunto de transformación IPsec. La definición de los conjuntos de transformación define los parámetros que utiliza el túnel IPsec. Este conjunto puede incluir los algoritmos de cifrado e integridad.

Tarea 4. Crear una crypto ACL. La crypto ACL define qué tráfico es enviado a través del túnel IPsec y protege el proceso IPsec.

Tarea 5. Crear y aplicar un crypto-map. El crypto-map agrupa los parámetros configurados previamente y define los dispositivos IPsec. Este se aplica a la interfaz de salida del dispositivo VPN.



Tareas para configurar IPsec:

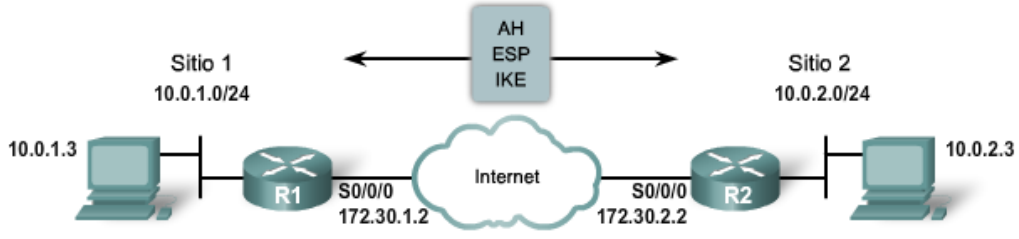
Tarea 1:Asegurar que las ACLs son compatibles con IPsec.
Tarea 2:Crear una política ISAKMP (IKE).
Tarea 3:Configurar el conjunto de transformación IPsec.
Tarea 4:Crear una crypto ACL.
Tarea 5:Crear y aplicar el crypto-map.

8.4.2 Tarea 1 – Configurar ACLS compatibles

El primer paso para configurar el Cisco IOS ISAKMP es asegurar que las ACLs existentes en los routers perimetrales, firewalls u otros routers no bloquean el tráfico IPsec. Los routers perimetrales en general implementan políticas de seguridad restrictivas con ACLs, donde sólo se permite tráfico específico y se deniega todo el otro tráfico. Dichas políticas restrictivas bloquean el tráfico IPsec. Por lo tanto, deben agregarse sentencias específicas de permiso en las ACLs.

Asegurarse de que las ACLs estén configuradas de forma tal que el tráfico ISAKMP, ESP (Encapsulating Security Payload) y AH (Authentication Header) no se encuentre bloqueado en las interfaces utilizadas por IPsec.

ESP tiene asignado el número de protocolo IP 50.
AH tiene asignado el número de protocolo 51.
ISAKMP utiliza el puerto UDP 500.

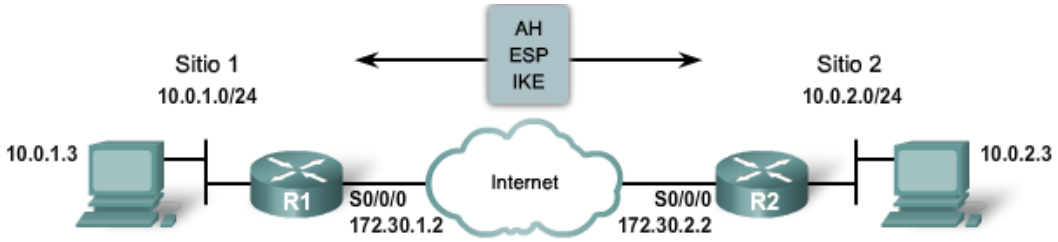


Asegurar que el tráfico de los protocolos 50 (ESP), 51 (AH) y el puerto UDP 500 (ISAKMP) no está bloqueado por ACLs de entrada en las interfaces utilizadas por IPsec.

Para permitir AH, ESP e ISAKMP en una interfaz IPsec y a la vez denegar todo el tráfico innecesario, debe editarse la ACL existente o bien crearse una nueva ACL.

Para permitir el tráfico AH, utilizar el comando access-list acl permit ahp wildcard origen wildcard destino.
Para permitir el tráfico ESP, utilizar el comando access-list acl permit esp wildcard origen wildcard destino.
Para permitir el tráfico ISAKMP, utilizar el comando access-list acl permit udp wildcard origen wildcard destino eq isakmp.

Utilizar el comando show access-list para verificar las sentencias.



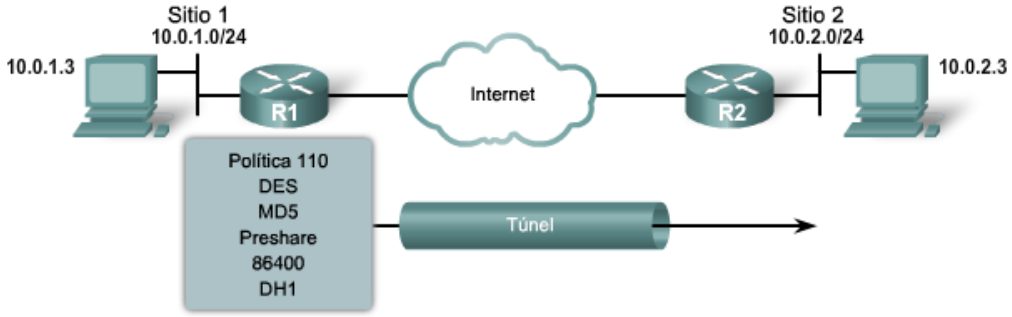

```
R1(config)# access-list 102 permit ahp host 172.30.2.2 host 172.30.1.2
R1(config)# access-list 102 permit esp host 172.30.2.2 host 172.30.1.2
R1(config)# access-list 102 permit udp host 172.30.2.2 host 172.30.1.2 eq isakmp
R1(config)# interface Serial0/0/0
R1(config-if)# ip address 172.30.1.2 255.255.255.0
R1(config-if)# no shutdown
R1(config-if)# ip access-group 102 in
R1(config-if)# exit
R1(config)# exit
R1#
R1# show access-lists
    access-list 102 permit ahp host 172.30.2.2 host 172.30.1.2
    access-list 102 permit esp host 172.30.2.2 host 172.30.1.2
    access-list 102 permit udp host 172.30.2.2 host 172.30.1.2 eq isakmp
```

8.4.3 Tarea 2 – Configurar IKE

La segunda tarea importante en la configuración del soporte Cisco IOS ISAKMP es definir los parámetros dentro de la política IKE. IKE utiliza estos parámetros durante la negociación para establecer la conexión entre los extremos IPsec.

Es posible configurar múltiples políticas IPsec en cada extremo participante. Cuando se configuran las políticas, debe asignarse un número único de prioridad a cada una. Utilice el comando crypto isakmp policy prioridad, donde la prioridad es un número que identifica unívocamente a la política IKE y le asigna una prioridad. Utilice un número entero entre 1 y 10.000, siendo 1 la más alta prioridad y 10.000 la más baja. Debe asignarse el número disponible más bajo a la política más segura.

El comando crypto isakmp policy invoca al modo de configuración de la política ISAKMP. Configurar los parámetros ISAKMP en este modo. Si los comandos no son configurados en forma explícita, se utilizan valores por defecto. Por ejemplo, si el comando hash no se configura explícitamente, IKE utiliza el valor SHA por defecto.




```
router(config)#
crypto isakmp policy priority
```

Define los parámetros contenidos en la política IKE

```
R1(config)# crypto isakmp policy 110
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# encryption des
R1(config-isakmp)# group 1
R1(config-isakmp)# hash md5
R1(config-isakmp)# lifetime 86400
```

Comando `crypto isakmp policy` | Parámetros ISAKMP

Haga clic en los botones para ver el contenido asociado.

Parámetros ISAKMP

Parámetro	Palabra clave	Valores aceptados	Valor por defecto	Descripción
encryption	des 3des aes aes 192 aes 256	Data Encryption Standard (DES) de 56 bits Triple DES AES de 128 bits AES de 192 bits AES de 256 bits	des	Algoritmo de cifrado del mensaje
hash	sha md5	SHA-1 (variante de HMAC) MD5 (variante de HMAC)	sha	Algoritmo de integridad del mensaje (hash)
authentication	pre-share rsa-encr rsa-sig	Claves precompartidas Nonces RSA cifrados Firmas RSA	rsa-sig	Método de autenticación de pares
group	1 2 5	Diffie-Hellman (DH) de 768 bits DH de 1024 bits DH de 1536 bits	1	Parámetros de intercambio de claves (identificador de grupo DH)
lifetime	*seconds*	Puede especificarse cualquier cantidad de segundos	86,400 segs (un día)	Tiempo de vida de SA establecidos por ISAKMP

Nota: Los parámetros reales pueden variar según la imagen del IOS utilizada.

Comando `crypto isakmp policy` | Parámetros ISAKMP

Haga clic en los botones para ver el contenido asociado.

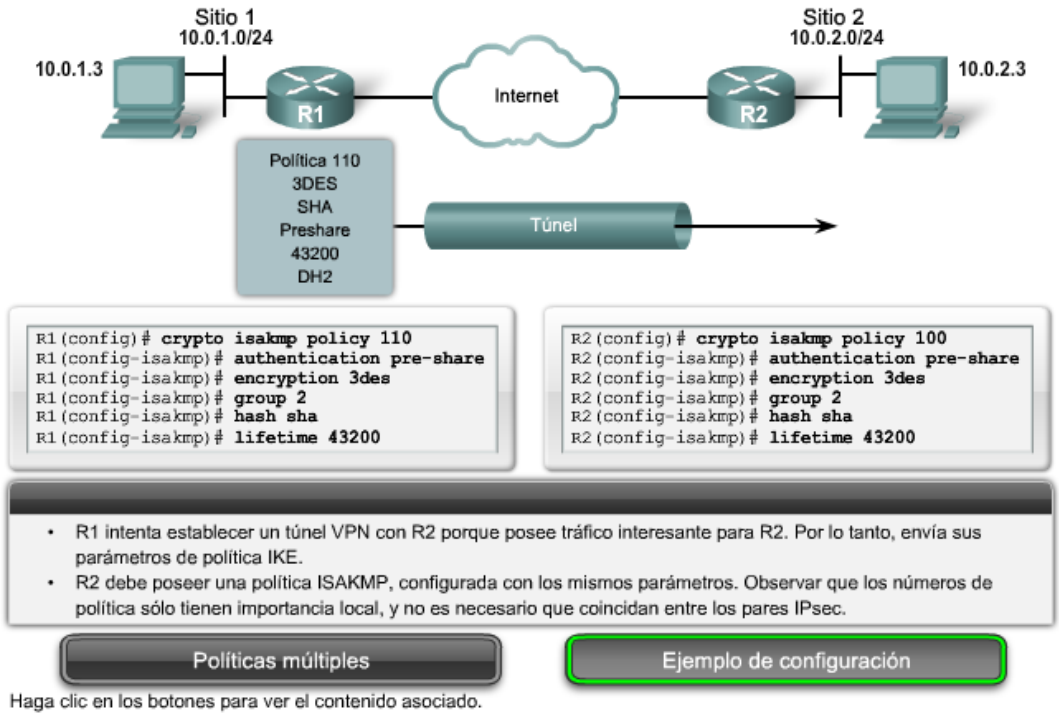
Ambos extremos deben negociar las políticas ISAKMP antes de acordar la SA a utilizar para IPsec.

Cuando comienza la negociación ISAKMP en el modo principal de la fase 1 IKE, el par que inicia la negociación envía todas sus políticas al par remoto, el cual busca una que coincida con sus propias políticas. El extremo remoto busca una coincidencia siguiendo

el orden de prioridad, comenzando por comparar su política de prioridad más alta, hasta encontrar una que coincida con las políticas recibidas por el otro extremo.

Se encuentra una coincidencia cuando las políticas de ambos extremos contienen el mismo cifrado y autenticación, el mismo hash, iguales parámetros DH y cuando la política del extremo remoto especifica un tiempo de vida menor o igual al tiempo de vida de la política con la cual se está comparando. Si el tiempo de vida no es igual, se utiliza el tiempo de vida más corto. Debe asignarse el menor número de prioridad disponible a la política más segura, para que la misma sea analizada y genere una coincidencia antes que cualquier otra política menos segura.

Si no se encuentra una coincidencia aceptable, ISAKMP rechaza la negociación y no se establece IPsec. Si se encuentra una coincidencia, ISAKMP completa la negociación del modo principal y se crean las SAs IPsec durante el modo rápido de la fase 2 IKE.



Para el cifrado se requieren PSKs. Dado un extremo cualquiera, puede configurarse la misma clave para ser compartida entre múltiples pares remotos. Una solución más segura consiste en especificar diferentes claves para compartir entre diferentes pares de extremos.

Configurar una PSK con el comando de configuración global crypto isakmp key. Esta clave debe estar configurada si el comando authentication pre-share fue configurado en la política ISAKMP.

crypto isakmp key clave address peer-address

crypto isakmp key clave hostname nombre de host

Por defecto, la identidad ISAKMP utiliza la dirección IP. Para utilizar el parámetro nombre de host la identidad ISAKMP debe ser configurada con el nombre del host, utilizando el comando de configuración global crypto isakmp identity hostname. Además, debe existir un DNS accesible para resolver el nombre del host.

```
router(config)#
crypto isakmp key keystring address peer-address
```

```
router(config)#
crypto isakmp key keystring hostname hostname
```

Parámetro	Descripción
keystring	Este parámetro especifica el PSK. Utilizar cualquier combinación de caracteres alfanuméricos de hasta 128 bytes.. Este PSK debe ser idéntico en ambos pares.
peer-address	Este parámetro especifica la dirección IP del par remoto.
hostname	Este parámetro especifica el nombre de host del par remoto. Es el nombre del host concatenado con su nombre de dominio (por ejemplo, myhost.domain.com).

- Los parámetros *peer-address* o *hostname* pueden ser utilizados, pero deben ser consistentes entre los pares.
- Si se utiliza *hostname* entonces debe configurarse además el comando **crypto isakmp identity hostname**.

crypto isakmp key | Ejemplo de configuración

Hacer click sobre los botones para ver el contenido asociado.




```
R1(config)# crypto isakmp policy 110
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# encryption 3des
R1(config-isakmp)# group 2
R1(config-isakmp)# hash sha
R1(config-isakmp)# lifetime 43200
R1(config-isakmp)# exit
R1(config)# crypto isakmp key cisco123 address 172.30.2.2
R1(config)#
```

Nota:

- La cadena de caracteres cisco123 coincide.
- Se especificó un método de identidad de dirección.
- Las políticas ISAKMP son compatibles.
- Los valores por defecto no deben estar configurados.

```
R2(config)# crypto isakmp policy 110
R2(config-isakmp)# authentication pre-share
R2(config-isakmp)# encryption 3des
R2(config-isakmp)# group 2
R2(config-isakmp)# hash sha
R2(config-isakmp)# lifetime 43200
R2(config-isakmp)# exit
R2(config)# crypto isakmp key cisco123 address 172.30.1.2
R2(config)#
```

crypto isakmp key | Ejemplo de configuración

Hacer click sobre los botones para ver el contenido asociado.

8.4.4 Tarea 3 – Configurar el conjunto de transformacion

Un conjunto de transformación es una combinación de transformaciones IPsec individuales, las cuales son designadas para representar una política de seguridad de tráfico específica. Durante la negociación ISAKMP de SA para IPsec, la cual ocurre durante el modo rápido de la fase 2 IKE, los pares acuerdan utilizar un conjunto de transformación específico para proteger un flujo particular de datos.

Los conjuntos de transformación consisten en una combinación de transformaciones AH, una transformación ESP y el modo IPsec (ya sea modo túnel o de transporte). Los conjuntos de transformación se limitan a una transformación AH y una o dos transformaciones ESP. Es posible configurar múltiples conjuntos de transformación. Luego, pueden especificarse uno o más de estos conjuntos a una entrada del crypto-map. La negociación SA de IPsec utiliza el conjunto de transformación definido en la entrada del crypto-map para proteger el flujo de datos especificado por la ACL de dicha entrada.

Para definir un conjunto de transformación, especificar entre una y cuatro transformaciones utilizando el comando de configuración global crypto ipsec transform-set. Este comando invoca al modo de configuración de transformaciones criptográficas

crypto ipsec transform-set nombre-conjunto-transformación transform1 [transform2] [transform3] [transform4]

Cada transformación representa un protocolo de seguridad IPsec (AH o ESP) además del algoritmo asociado. Estos protocolos y algoritmos son especificados dentro del modo de configuración de transformaciones criptográficas. En un conjunto de transformaciones, especificar el protocolo AH, el protocolo ESP o ambos. Si se selecciona un protocolo ESP, debe especificarse también un conjunto de transformación de cifrado ESP o bien un conjunto de transformación de cifrado ESP y un conjunto de transformación de autenticación ESP.

Durante la negociación, los pares buscan un conjunto de transformación que contenga el mismo criterio en ambos extremos (combinación de protocolos, algoritmos y otras configuraciones). Cuando se encuentra un conjunto que cumpla con esta condición, el mismo es seleccionado y aplicado al tráfico protegido como parte de las SAs IPsec en ambos extremos.

Cuando no se utiliza ISAKMP para establecer las SAs, debe utilizarse un único conjunto de transformación. En esta instancia, el conjunto de transformación no se negocia.

```
router(config)#
crypto ipsec transform-set transform-set-name transform1 [transform2]
[transform3][transform4]
```

Parámetros de crypto ipsec transform-set

Comando	Descripción
transform-set-name	Este parámetro especifica el nombre del conjunto de transformación creado (o modificado).
transform1, transform2, transform3, transform4	Tipo del conjunto de transformación. Especificar hasta cuatro "transformaciones": un Authentication Header (AH), un cifrado ESP (Encapsulating Security Payload), una autenticación ESP. Estas transformaciones definen los protocolos y algoritmos de seguridad IPsec (IP Security).

- Un conjunto de transformación es una combinación de transformaciones Ipsec que conforman una política de seguridad para el tráfico.
- Un conjunto de transformación puede tener una transformación AH y hasta dos transformaciones ESP.

Comando transform set | Combinaciones de transformaciones

Haga clic en los botones para ver el contenido asociado.

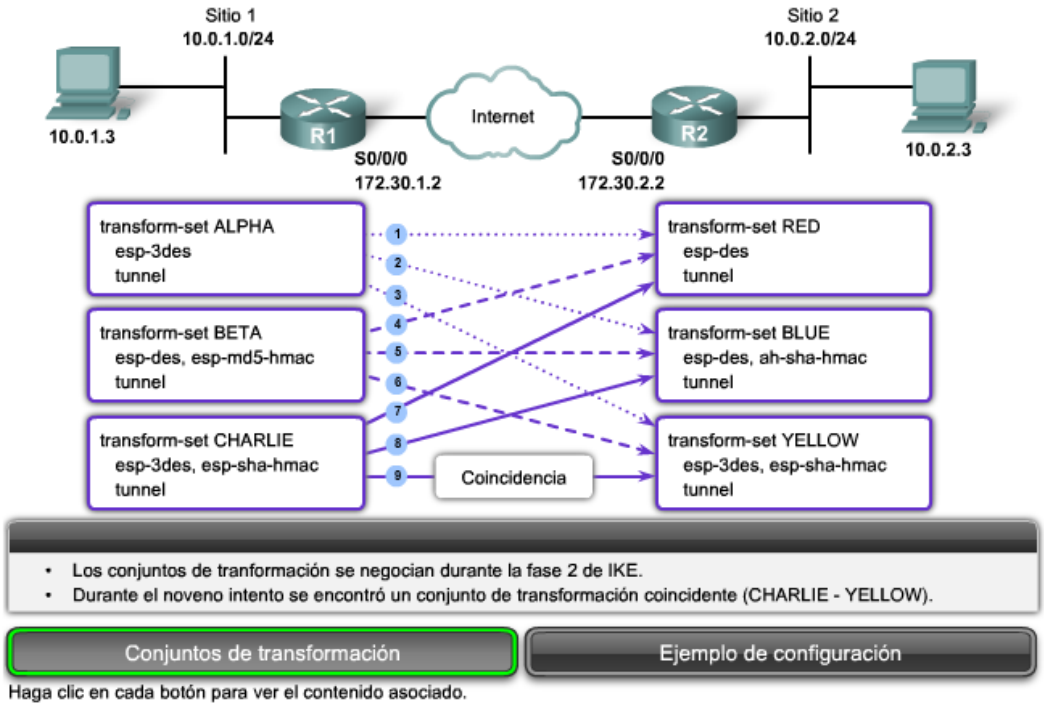
Tipo de transformación	Transformación	Descripción
Transformación AH *(Seleccionar sólo una)*	ah-md5-hmac	• AH con algoritmo de autenticación MD5 (Message Digest 5) (una variante de HMAC [Hash-based Message Authentication Code])
	ah-sha-hmac	• AH con algoritmo de autenticación SHA (Secure Hash Algorithm) (una variante de HMAC)
Transformación de cifrado ESP *(Seleccionar sólo una)*	esp-aes	• ESP con cifrado Advanced Encryption Standard (AES) de 128 bits
	esp-aes 192	• ESP con cifrado AES de 192 bits
	esp-aes 256	• ESP con cifrado AES de 256 bits
	esp-des	• ESP con cifrado Data Encryption Standard (DES) de 56 bits
	esp-3des	• ESP con cifrado DES (3DES or Triple DES) de 168 bits
	esp-null	• Sin algoritmo de cifrado
	esp-seal	• ESP con cifrado SEAL de 160 bits
Transformación de autenticación ESP *(Seleccionar sólo una)*	esp-md5-hmac	• ESP con autenticación MD5 (variante de HMAC)
	esp-sha-hmac	• ESP con autenticación SHA (variante de HMAC)
Transformación de compresión IP	comp-lzs	• Compresión IP con algoritmo Lempel-Ziv-Stac (LZS)

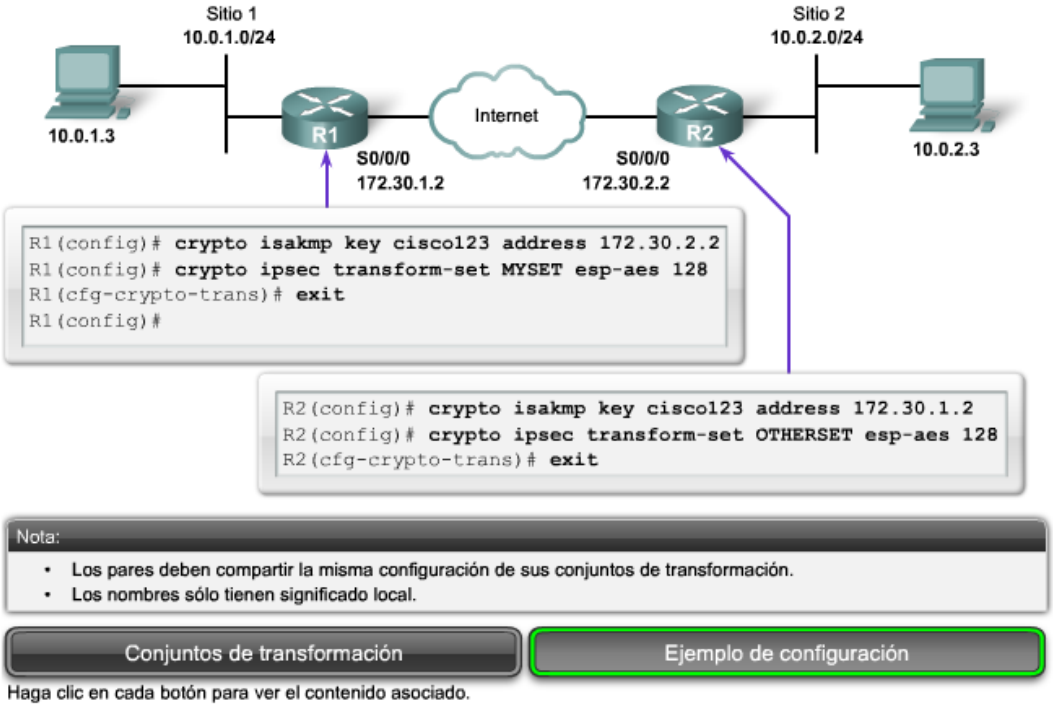
Comando transform set | Combinaciones de transformaciones

Haga clic en los botones para ver el contenido asociado.

Los conjuntos de transformación se negocian durante el modo rápido de la fase 2 IKE. Cuando se configuran múltiples conjuntos de transformación, esta operación debe realizarse desde el más seguro hasta el menos seguro, de acuerdo con la política de seguridad de la red.

Los pares IPsec buscan un conjunto de transformación que coincida en ambos extremos y concuerden en una propuesta de transformación unidireccional por cada SA. Por ejemplo, asuma que R1 y R2 están negociando un conjunto de transformación. R1 tiene configurados los conjuntos ALPHA, BETA y CHARLIE, mientras que R2 tiene configurados los conjuntos RED, BLUE y YELLOW. Cada conjunto de trasformación de R1 se compara con los conjuntos de R2. Los conjuntos ALPHA, BETA y CHARLIE son comparados con el conjunto RED. No se encuentra coincidencia. Luego, todos los conjuntos de R1 se comparan con el conjunto de R2 BLUE. Finalmente, los conjuntos de R1 se comparan con el conjunto YELLOW en R2. Se encuentra una coincidencia entre YELLOW y CHARLIE. Por lo tanto, son seleccionados y aplicados al tráfico protegido como parte de las SAs IPsec en ambos extremos.

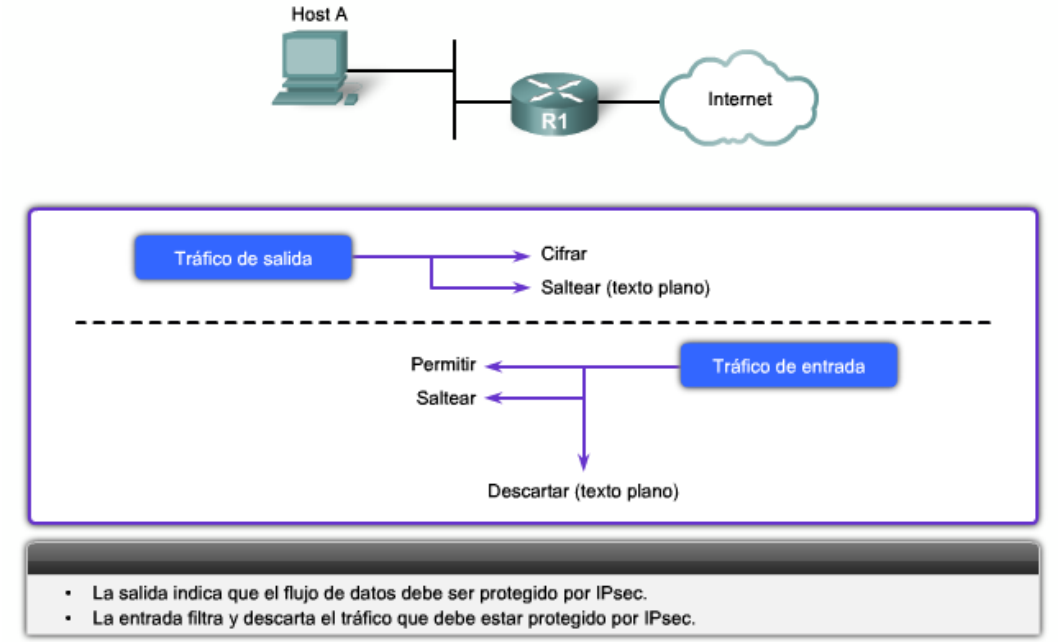




8.4.5 Tarea 4 – Configurar las Crypto ACLs

Las crypto ACLs identifican los flujos de tráfico a proteger. Las crypto ACLs de salida seleccionan el tráfico saliente que IPsec debe proteger. El tráfico no seleccionado se envía como texto plano. De ser necesario, es posible crear ACLs de entrada para filtrar y descartar el tráfico que debería haber sido protegido por IPsec.

Las ACLs IP extendidas seleccionan el tráfico IP a ser cifrado, basándose en el protocolo, dirección IP, red, subred y puerto. Aunque la sintaxis de la ACL es la misma que en las ACLs IP extendidas, los significados son levemente diferentes en las crypto ACLs. Por ejemplo, la sentencia permit especifica que aquellos paquetes que coincidan con ellas deben ser cifrados y la sentencia deny indica que los paquetes no serán cifrados. El tráfico no es necesariamente descartado a partir de una sentencia deny. Las crypto ACLs se procesan de manera similar a una ACL IP extendida aplicada al tráfico de salida de una interfaz.



La sintaxis de comandos básicos para una ACL IP extendida es:

access-list número-lista-acceso {permit | deny} protocolo origen wildcard-origen destino wildcard-destino

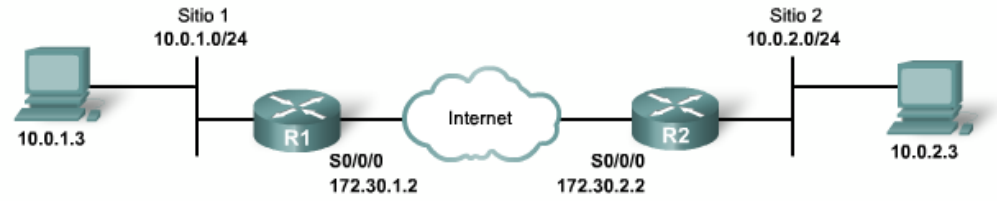
Las crypto ACLs de salida definen el tráfico interesante que debe cifrarse. Todo el tráfico restante se transmite como texto plano.

Las crypto ACLs de entrada informan al router qué tráfico debe recibirse como tráfico cifrado. Cuando el tráfico coincide con una sentencia permit, el router espera que el mismo se encuentre cifrado. Si se recibe tráfico entrante en texto plano y éste coincide con una sentencia permit de la crypto ACL de entrada, dicho tráfico es descartado. Este descarte ocurre porque se esperaba que el tráfico recibido en texto plano se encontrara protegido por IPsec y cifrado, pero no lo estaba.

El administrador puede desear que cierto tráfico reciba una combinación de protección IPsec (sólo autenticación) y otro tráfico reciba una combinación diferente (autenticación y cifrado). Para lograr esto, debe crear dos crypto ACLs diferentes, para definir los dos tipos de tráfico. Entonces, diferentes entradas del crypto-map utilizan estas ACLs para especificar las diferentes políticas IPsec.

El administrador debe ser lo más restrictivo posible al momento de definir qué paquetes proteger con una crypto ACL. No se recomienda el uso de la palabra clave any. Se desaconseja fuertemente el uso de la sentencia permit any any, ya que ocasiona que todo el tráfico de salida sea protegido. Entonces, todo el tráfico entrante que no cuente con protección IPsec es descartado en forma silenciosa, incluyendo paquetes de protocolos de enrutamiento, NTP, echo, respuestas de echo y otros. Si resulta necesario utilizar la palabra clave any en una sentencia permit, incorporar antes una serie de sentencias deny para filtrar el tráfico que no deba estar protegido.

La crypto ACL se asocia con un crypto-map, el cual a su vez se asigna a una interfaz específica.




```
router(config)#
access-list access-list-number {deny | permit} protocol source source-
wildcard destination destination-wildcard
```

Comando	Descripción
permit	Todo el tráfico que coincida con las condiciones especificadas por esta opción será protegido utilizando criptografía, de acuerdo a la política descripta por la entrada correspondiente del crypto-map.
deny	Esta opción indica al router que debe mantener el tráfico en texto plano.
protocol	Esta opción indica el tráfico que debe protegerse utilizando criptografía en base a su protocolo, como puede ser TCP, UDP o ICMP. Si el protocolo indicado es IP, entonces todo el tráfico IP que coincida con la sentencia permit será cifrado.
source and *destination*	Si la sentencia de la ACL es de tipo permit, estas son las redes, subredes o hosts entre los cuales debe protegerse el tráfico. Si se trata de una sentencia deny, entonces el tráfico entre el origen y destino especificados se envía en texto plano.

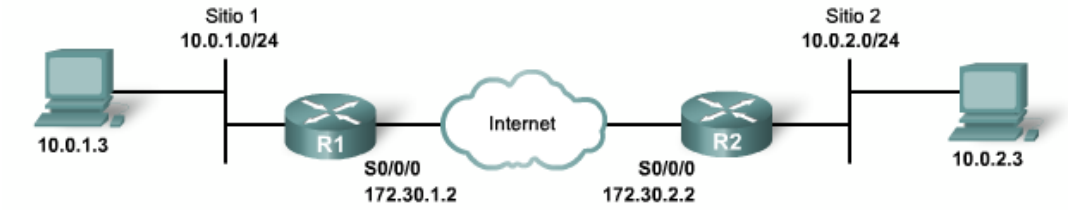
Para IPsec, deben configurarse crypto ACLs simétricas. Cuando un router recibe paquetes cifrados desde un par IPsec, utiliza la misma ACL para determinar qué paquetes entrantes debe descifrar, analizando las direcciones de origen y destino en la ACL en orden inverso. El criterio de la ACL se aplica hacia adelante sobre el tráfico que sale del router y hacia atrás sobre el tráfico que entra al router. Por lo tanto, la dirección origen de la ACL de salida se vuelve la dirección destino en la ACL de entrada.

Por ejemplo, asuma que para el Sitio 1, se aplica protección IPsec al tráfico entre los hosts de la red 10.0.1.0/24 cuando los datos salen de la interfaz S0/0/0 en R1, con dirección a los hosts de la red 10.0.2.0/24 del Sitio 2. Para el tráfico originado en hosts de la red 10.0.1.0/24 en el Sitio 1, con destino a hosts de la red 10.0.2.0/24 en el Sitio 2, la entrada de la ACL en R1 se evalúan de la siguiente forma:

Origen = hosts en la red 10.0.1.0/24
Destino = hosts en la red 10.0.2.0/24

Para el tráfico entrante, con origen en los hosts de la red 10.0.2.0/24 en el Sitio 2, destinado a hosts de la red 10.0.1.0/24 en el Sitio 1, se evalúa la misma entrada en la ACL de R1, de la siguiente forma:

Origen = hosts de la red 10.0.2.0/24
Destino = hosts de la red 10.0.1.0/24



Aplicado al tráfico de salida de S0/0/0 en R1:

```
R1(config)# access-list 110 permit tcp 10.0.1.0 0.0.0.255 10.0.2.0 0.0.0.255
```

Aplicado al tráfico de salida de S0/0/0 en R2:

```
R2(config)# access-list 101 permit tcp 10.0.2.0 0.0.0.255 10.0.1.0 0.0.0.255
```

8.4.6 Tarea 5 – Aplicar el Cryto-Map

Las entradas del crypto-map creadas para IPsec combinan los parámetros de configuración necesarios para las SAs IPsec, incluyendo los siguientes:

Qué tráfico proteger, utilizando una crypto ACL
Granularidad del flujo a proteger mediante un conjunto de SAs
Quién es el par remoto IPsec, lo cual determina hacia dónde debe enviarse el tráfico protegido por IPsec
Dirección local del tráfico IPsec (opcional)
Qué tipo de seguridad IPsec debe aplicarse a este tráfico, seleccionado a partir de una lista de uno o más conjuntos de transformación

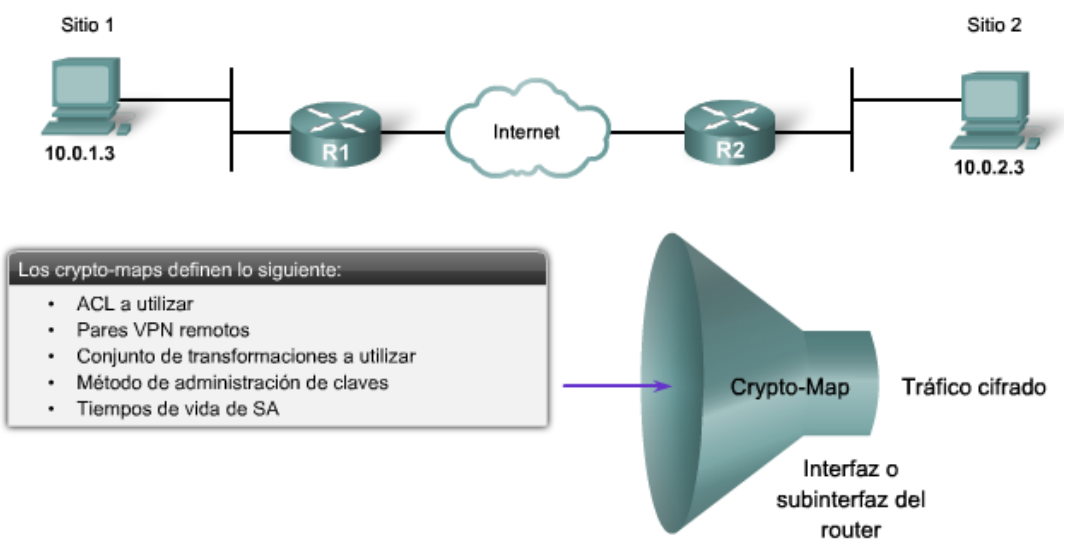
Las entradas del crypto-map con el mismo nombre pero diferente número de secuencia se agrupan en un conjunto de crypto-maps.

Sólo puede asignarse un único crypto-map a una misma interfaz. El crypto-map puede incluir una combinación de CET (Cisco Encryption Technology) e IPsec utilizando IKE. Múltiples interfaces pueden compartir el mismo crypto-map, si se aplica la misma política a múltiples interfaces. Si se crea más de una entrada de crypto-map para una interfaz dada, debe utilizarse el número de secuencia (núm-sec) de cada entrada para darles una prioridad. A menor número de secuencia, mayor es la prioridad. Cuando el tráfico alcanza la interfaz a la que se asignó el crypto-map, el mismo es evaluado contra las entradas del mapa comenzando por la de mayor prioridad.

Deben crearse múltiples entradas en el crypto-map para una interfaz determinada, si se cumple cualquiera de las siguientes condiciones:

Distintos pares IPsec manejan diferentes flujos de datos.
Debe aplicarse diferente seguridad IPsec a distintos tipos de tráfico (en el mismo o en diferentes pares IPsec). Por ejemplo, si el tráfico entre un conjunto de subredes requiere autenticación y el tráfico entre otro conjunto de subredes requiere cifrado y

autenticación. En este caso, deben definirse los diferentes tipos de tráfico en dos ACLs separadas y crear una entrada separada en el crypto-map para cada crypto ACL.
IKE no es utilizado para establecer un conjunto particular de SAs y deben especificarse múltiples entradas de ACL, crear ACLs separadas (una por cada sentencia permit) y especificar una entrada de crypto-map separada por cada ACL.



Utilizar el comando de configuración global crypto map para crear o modificar una entrada de crypto-map e ingresar al modo de configuración de crypto-map. Configurar las entradas de crypto-map que referencian mapas dinámicos con la menor prioridad en un conjunto de crypto-maps (deben tener el número de secuencia más alto). La sintaxis y parámetros del comando son los siguientes:

crypto map nombre-mapa núm-sec cisco

crypto map nombre-mapa núm-sec ipsec-manual

crypto map nombre-mapa núm-sec ipsec-isakmp [dynamic nombre-mapa-dinámico]

no crypto map nombre-mapa [núm-sec]

Utilizando el comando de configuración global crypto map se ingresa al modo de configuración de crypto-map. Desde aquí, se configuran distintos componentes IPsec, incluyendo qué crypto ACL, dirección remota y conjunto de transformación deben utilizarse.

Las ACLs para las entradas de crypto-map etiquetadas como IPsec-manual están restringidas a una única sentencia permit y se ignoran las sentencias siguientes. Las SAs establecidas por una entrada particular de crypto-map corresponden a un único flujo de datos. Para soportar múltiples SAs establecidas en forma manual para diferentes tipos de tráfico, deben definirse múltiples crypto ACLs para luego aplicar cada una a una entrada IPsec-manual separada. Cada ACL incluye una sentencia permit que define el tráfico que debe protegerse.

Es posible especificar dos pares en un crypto-map para redundancia. Si el primer par no puede ser contactado, se utiliza el segundo par. No existe límite en el número de pares redundantes que pueden ser configurados.

```
router(config)#
crypto map map-name seq-num ipsec-manual
crypto map map-name seq-num ipsec-isakmp [dynamic dynamic-map-name]
```

Parámetros de `crypto map`

Parámetros del comando	Descripción
map-name	Define el nombre asignado al crypto-map generado o indica el nombre del crypto-map a editar.
seq-num	El número asignado a la entrada del crypto-map.
ipsec-manual	Indica que ISAKMP no será utilizado para establecer las SAs IPsec.
ipsec-isakmp	Indica que ISAKMP será utilizado para establecer las SAs IPsec.
cisco	(Valor por defecto) Indica que CET será utilizado en lugar de IPsec para proteger el tráfico.
dynamic	(Opcional) Especifica que esta entrada del crypto-map referencia a un crypto-map estático preexistente. Si esta palabra clave es utilizada, ninguno de los comandos de configuración de crypto-map están disponibles.
dynamic-map-name	(Opcional) Especifica el nombre del crypto-map dinámico que debe ser utilizado como template de la política.

Comando `crypto map` | Comandos de configuración de un Crypto-Map | Ejemplo de configuración

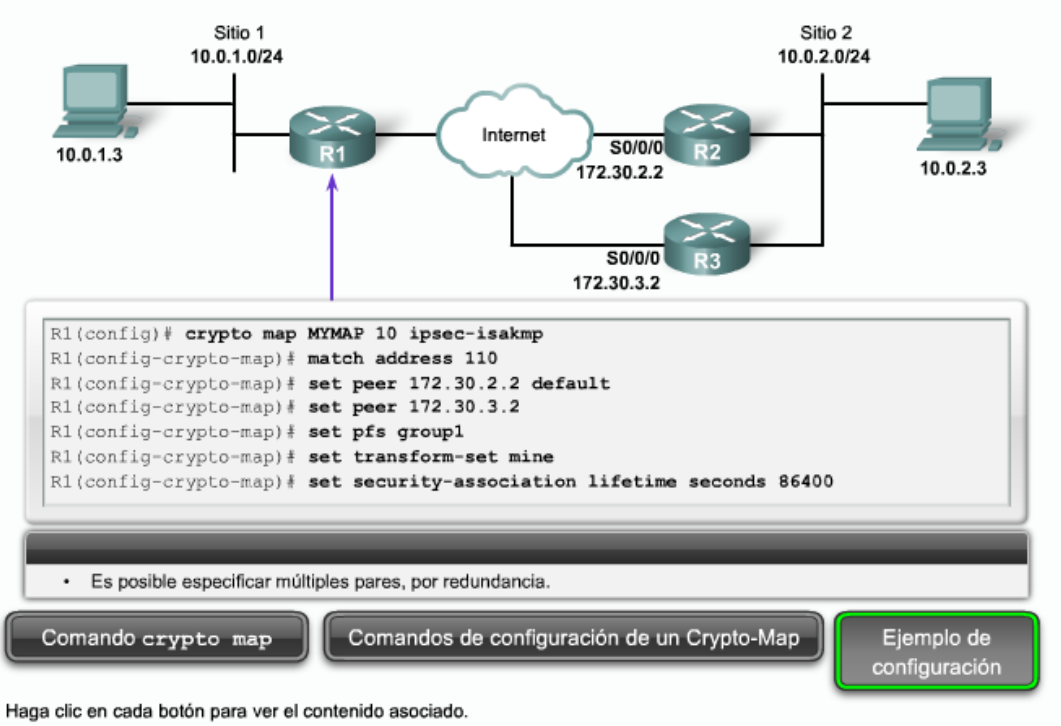
Haga clic en cada botón para ver el contenido asociado.

Comandos de configuración del modo `crypto map`

Comando	Descripción
set	Utilizado con los comandos **peer**, **pfs**, **transform-set**, y **security-association**.
peer [*hostname* | *ip-address*]	Especifica los pares IPsec permitidos por dirección IP o nombre de host.
pfs [**group1** | **group2**]	Especifica el Grupo 1 o Grupo 2 DH.
transform-set [*set_name(s)*]	Especifica la lista de conjuntos de transformación en orden de prioridad. Cuando se utiliza el parámetro **ipsec-manual** con el comando **crypto map**, sólo puede definirse un único conjunto de transformación. Cuando se utilizan los parámetros **ipsec-isakmp** o **dynamic** con el comando **crypto map**, pueden especificarse hasta seis conjuntos de transformación.
security-association lifetime	Configura los parámetros de tiempo de vida de SA en segundos o kilobytes.
match address [*access-list-id* | *name*]	Identifica una ACL extendida por su nombre o número. El valor debe coincidir con los argumentos access-list-number o name de una ACL IP extendida previamente definida.
no	Utilizado para eliminar los comandos ingresados con el comando **set**.
exit	Sale del modo de configuración de crypto-map.

Comando `crypto map` | Comandos de configuración de un Crypto-Map | Ejemplo de configuración

Haga clic en cada botón para ver el contenido asociado.



Una vez configurados los parámetros del crypto-map, debe asignarse el mismo a las interfaces, utilizando el comando de configuración de interfaz crypto map.

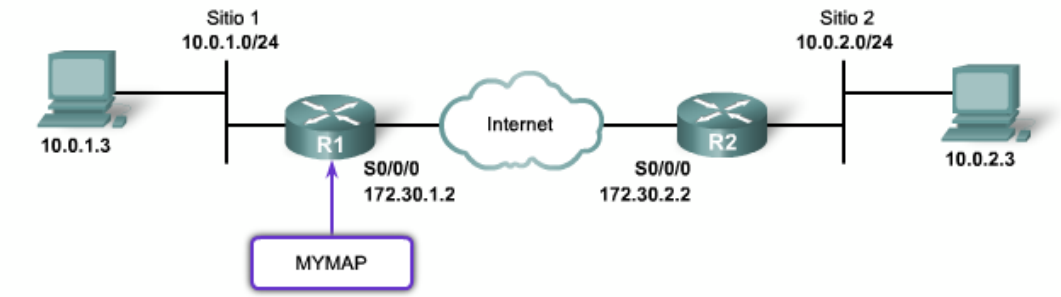
El crypto-map es aplicado a la interfaz de salida del túnel VPN utilizando el comando de configuración de interfaz crypto map.

crypto map nombre-mapa

nombre-mapa es el nombre del crypto-map aplicado a la interfaz.

Debe asegurarse de configurar además la información de enrutamiento necesaria para enviar paquetes a través del túnel.

Todo el tráfico IPsec que atraviesa la interfaz donde se aplicó el crypto-map es evaluado contra el conjunto de crypto-maps configurado. Si la entrada de crypto-map ve tráfico saliente que debe estar protegido y el crypto-map especifica la utilización de IKE, se negocia una SA con el par remoto, acordando los parámetros incluidos en la entrada del crypto-map.




```
router(config-if)#
crypto map map-name
```

```
R1(config)# interface serial0/0/0
R1(config-if)# crypto map MYMAP
```

- Aplica el crypto-map a la interfaz de salida
- Activa la política IPsec

8.4.7 Verificar y resolver problemas de la configuración IPsec

Las VPNs pueden ser complejas y a veces no operan como es esperado. Por este motivo, existe una variedad de comandos útiles para verificar su operación y resolver problemas cuando sea necesario.

El mejor momento para familiarizarse con estos comandos y la información obtenida es cuando la red opera en forma correcta. De esta forma, las anomalías pueden detectarse al utilizarlos para resolver problemas.

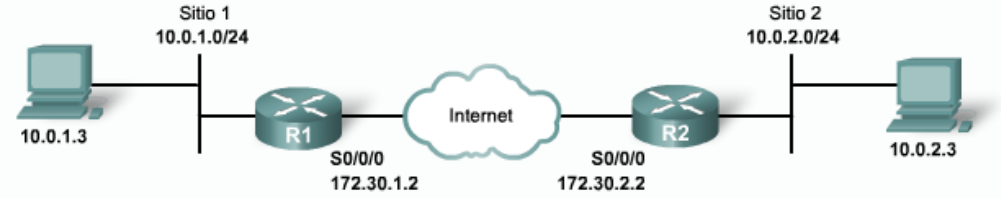
Comando show	Descripción
`show crypto map`	Muestra los crypto-maps configurados
`show crypto isakmp policy`	Muestra las políticas IKE configuradas
`show crypto ipsec sa`	Muestra los túneles IPsec establecidos
`show crypto ipsec transform-set`	Muestra los conjuntos de transformación IPsec configurados
`debug crypto isakmp`	Depura los eventos IKE
`debug crypto ipsec`	Depura los eventos IPsec

Para ver todos los crypto-maps configurados, utilizar el comando show crypto map. Este comando verifica las configuraciones y muestra el tiempo de vida de las SAs. El comando show running-config también revela muchos de estos datos.

Utilizar el comando show crypto isakmp policy para mostrar las políticas IKE configuradas y las políticas IKE por defecto. Este comando resulta útil porque revela toda la información de configuración ISAKMP (IKE).

Utilizar el comando show crypto ipsec transform-set para mostrar todos los conjuntos de transformación configurados. Dado que los conjuntos de transformación determinan

el nivel de protección con el que los datos son transmitidos a través del túnel, es importante verificar la fortaleza de la política de protección IPsec.



router#

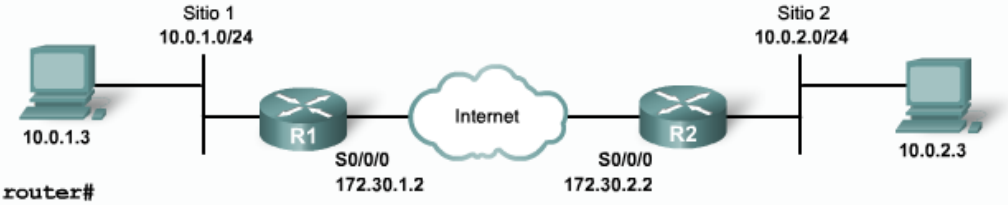
show crypto map

- Muestra los crypto-maps configurados actualmente.

```
R1# show crypto map
Crypto Map "MYMAP" 10 ipsec-isakmp
        Peer = 172.30.2.2
        Extended IP access list 110
            access-list 110 permit ip host 10.0.1.3 host 10.0.2.3
        Current peer: 172.30.2.2
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={ MYSET, }
```

show crypto map | show crypto isakmp policy | show crypto ipsec transform-set

Haga clic en los botones para ver el contenido asociado.



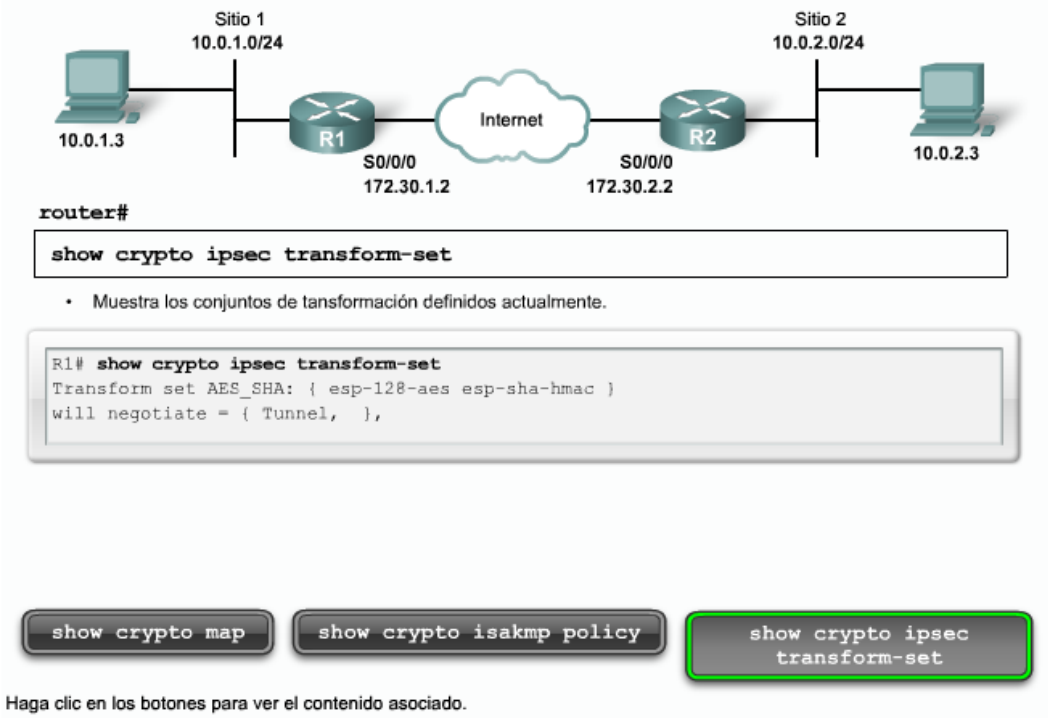
router#

show crypto isakmp policy

```
R1# show crypto isakmp policy
Protection suite of priority 110
      encryption algorithm:   3DES - Data Encryption Standard (168 bit keys).
      hash algorithm:         Secure Hash Standard
      authentication method:  preshared
      Diffie-Hellman group:   #2 (1024 bit)
      lifetime:               86400 seconds, no volume limit
Default protection suite
      encryption algorithm:   DES - Data Encryption Standard (56 bit keys).
      hash algorithm:         Secure Hash Standard
      authentication method:  Rivest-Shamir-Adleman Signature
      Diffie-Hellman group:   #1 (768 bit)
      lifetime:               86400 seconds, no volume limit
```

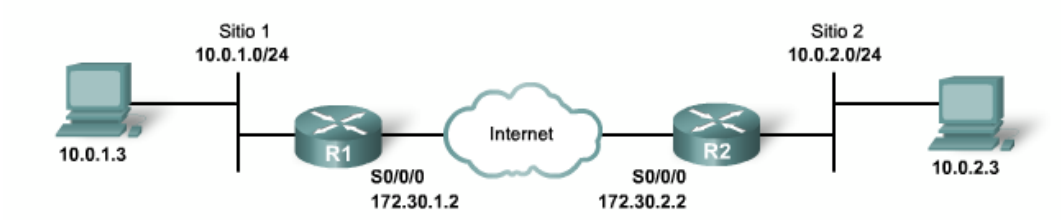
show crypto map | show crypto isakmp policy | show crypto ipsec transform-set

Haga clic en los botones para ver el contenido asociado.



Uno de los comandos más útiles es show crypto ipsec sa. Si la salida indica que existe una SA establecida, se asume que el resto de la configuración está funcionando. Entre los datos presentados, los valores pkts encrypt y pkts decrypt indican que el tráfico está siendo transmitido a través del túnel.

Un comando igualmente útil es show crypto isakmp sa. Este comando muestra todas las SAs IKE actuales. El estado QM_IDLE indica que existe una SA IKE activa.




```
R1# show crypto ipsec sa
Interface: Serial0/0/0
         Crypto map tag: MYMAP, local addr. 172.30.1.2
         local ident (addr/mask/prot/port): (172.30.1.2/255.255.255.255/0/0)
       remote ident (addr/mask/prot/port): (172.30.2.2/255.255.255.255/0/0)
       current_peer: 172.30.2.2
    PERMIT, flacs={origin_is_acl,}
       #pkts encaps: 21, #pkts encrypt: 21, #pkts digest 0
       #pkts decaps: 21, #pkts decrypt: 21, #pkts verify 0
       #send errors 0, #recv errors 0
local crypto endpt.: 172.30.1.2, remote crypto endpt.: 172.30.2.2
path mtu 1500, media mtu 1500
current outbound spi: 8AE1C9C
```

Para utilizar comandos de depuración para resolver problemas de conectividad en la VPN, conéctese al router Cisco mediante una terminal.

El comando debug crypto isakmp muestra información detallada sobre los procesos de negociación IKE de fase 1 y fase 2. El comando debug crypto ipsec muestra información detallada sobre los eventos IPsec.

Al igual que con otros comandos de depuración, utilice el comando debug crypto isakmp con precaución, ya que el proceso de depuración puede causar problemas de rendimiento en el equipo. Utilice el comando undebug all para desactivar la depuración tan pronto como sea posible.

```
router#
debug crypto isakmp
```

```
1d00h: ISAKMP (0:1): atts are not acceptable. Next payload is 0 1d00h: ISAKMP
(0:1); no offers accepted!
1d00h: ISAKMP (0:1): SA not acceptable!
1d00h: %CRYPTO-6-IKMP_MODE_FAILURE: Processing of Main Mode failed with peer
at 172.30.2.2
```

- Este es un ejemplo del mensaje de error del modo principal.
- La falla del modo principal sugiere que la política de fase 1 no coincide en ambos extremos.
- Verificar que la política de la fase 1 se encuentra en ambos extremos, y que todos sus atributos coinciden.

8.5 Implementacion de VPNs IPsec de sitio a sitio con SDM

8.5.1 Configuracion de IPsec con SDM

Además de configurar VPNs IPsec a través de CLI, es posible configurarlas utilizando un asistente SDM.

Para seleccionar e iniciar un asistente VPN, siga los siguientes pasos:

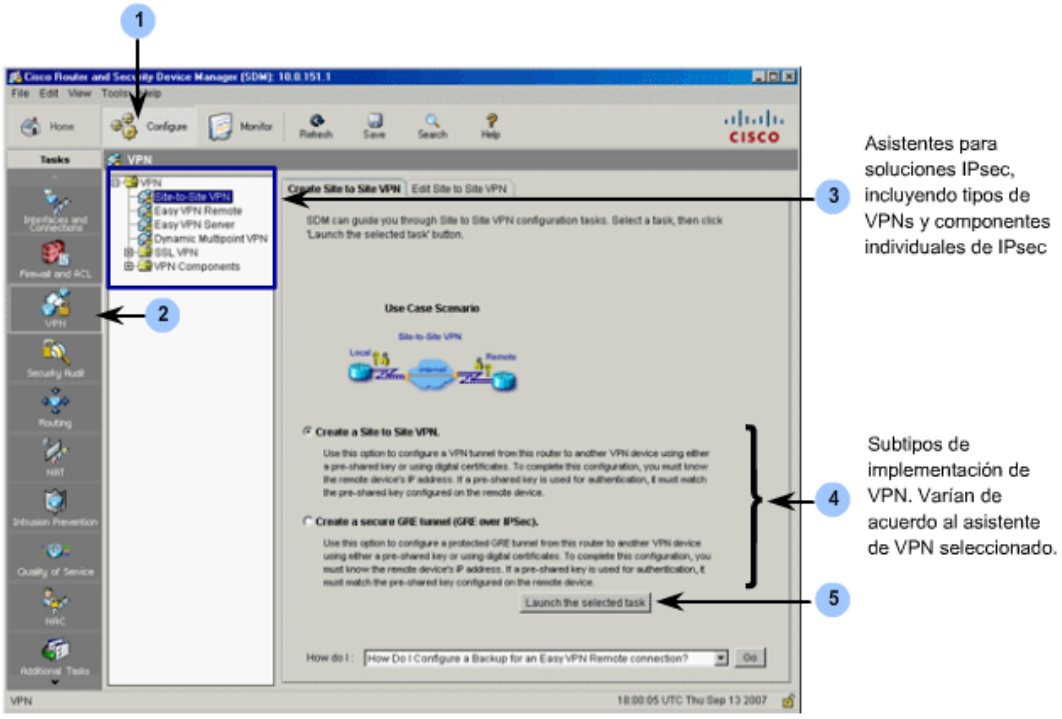
Paso 1. Haga clic sobre Configure en la barra de herramientas principal.

Paso 2. Haga clic sobre el botón VPN a la izquierda para abrir la página de VPN.

Paso 3. Seleccione un asistente en la ventana de VPN.

Paso 4. Haga clic sobre el subtipo de implementación de VPN.

Paso 5. Haga clic sobre el botón Launch the selected task para iniciar el asistente.



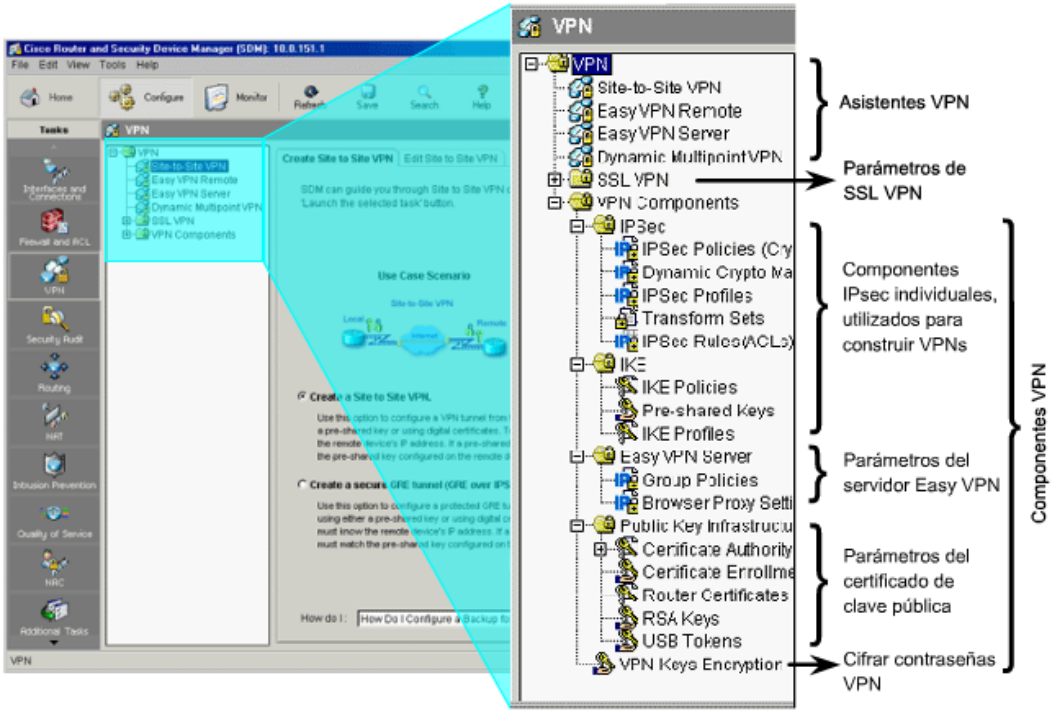
Los asistentes Cisco SDM para VPN utilizan dos fuentes para crear una conexión VPN: los datos ingresados por el usuario durante el proceso paso a paso del asistente y componentes VPN configurados previamente.

Cisco SDM proporciona algunos componentes por defecto: dos políticas IKE y un conjunto de transformación IPsec para el asistente de configuración rápida.

Los asistentes VPN crean otros componentes durante el proceso de configuración paso a paso. Algunos componentes deben estar configurados antes de que los asistentes puedan utilizarse. Por ejemplo, los componentes PKI deben estar configurados antes de utilizar el asistente de PKI.

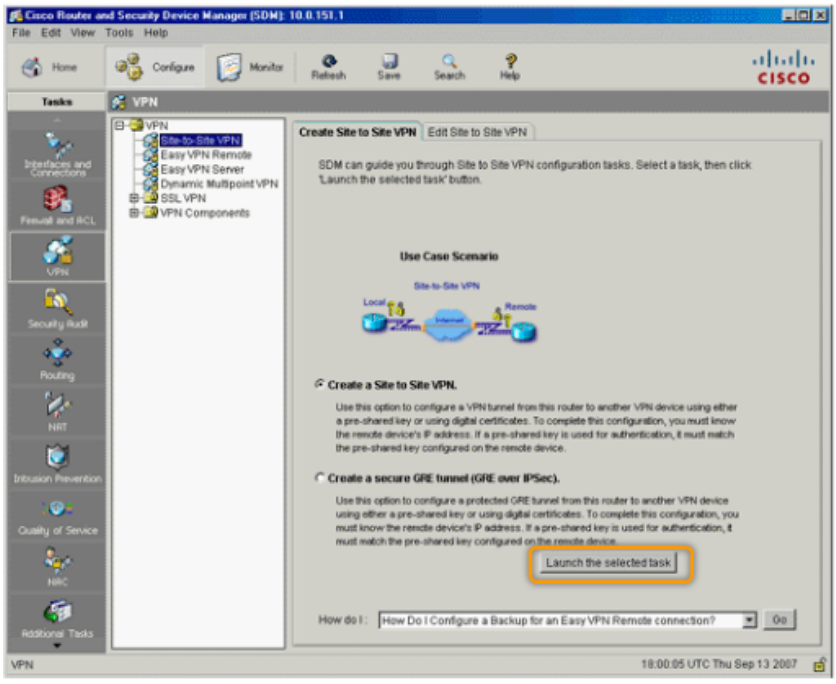
La barra de navegación de VPN contiene tres secciones principales:

La pestaña VPN - Contiene los asistentes para crear VPN de sitio a sitio, Easy VPN Remote, Easy VPN Server y VPN multipunto dinámica. Los asistentes VPN simplifican la configuración de los componentes individuales de una VPN. La sección de componentes IPsec puede ser entonces utilizada para modificar parámetros que pueden haber sido mal configurados durante el proceso paso a paso del asistente VPN.
La pestaña VPN SSL - Utilizada para configurar los parámetros de VPNs SSL.
Componentes VPN - Utilizada para configurar componentes VPN tales como IPsec, IKE, políticas de grupo y configuración de proxy para Easy VPN Server, infraestructura de clave pública (para autenticación IKE utilizando certificados digitales) y claves de Cifrado VPN. Utilice esta ventana para especificar una clave maestra cuando se cifren claves VPN, tales como PSKs, claves Cisco Easy VPN y claves de autenticación extendida (XAUTH). Cuando las claves se encuentran cifradas, se vuelven ilegibles para quien lea el archivo de configuración del router.



Utilice un navegador web para iniciar el Cisco SDM en un router. Seleccione el asistente de VPN en Configure > VPN > Site-to-Site VPN.

Para crear y configurar una clásica VPN de sitio a sitio, haga clic en la opción Create a Site-to-Site VPN de la pestaña Create Site-to-Site VPN. Luego, haga clic en el botón Launch the selected task.

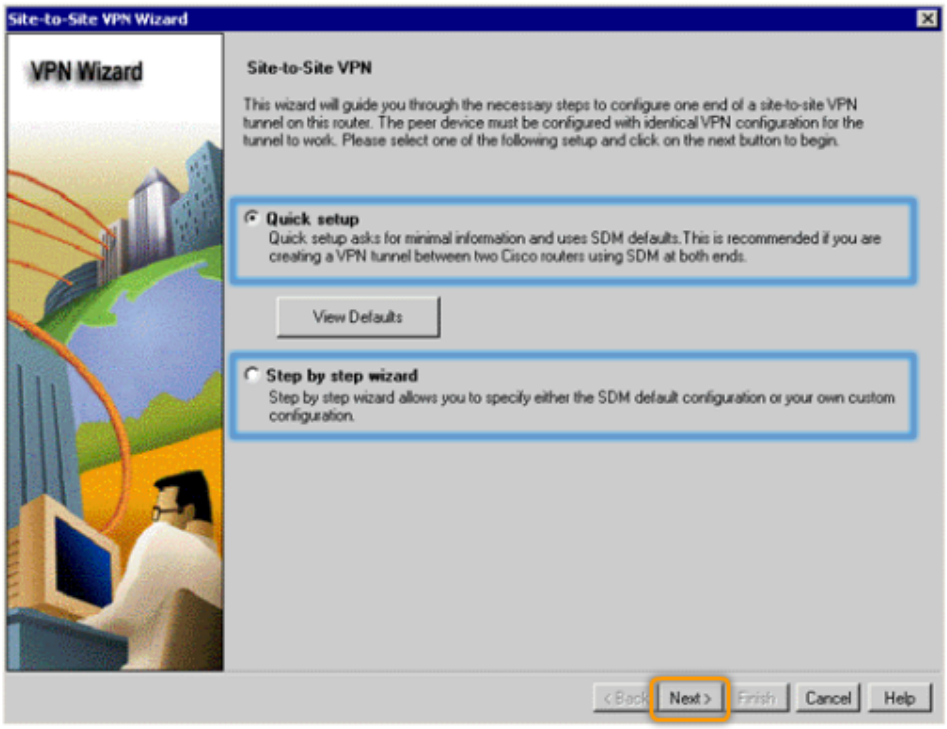


En esta instancia, una ventana muestra las opciones Quick setup y Step by step wizard.

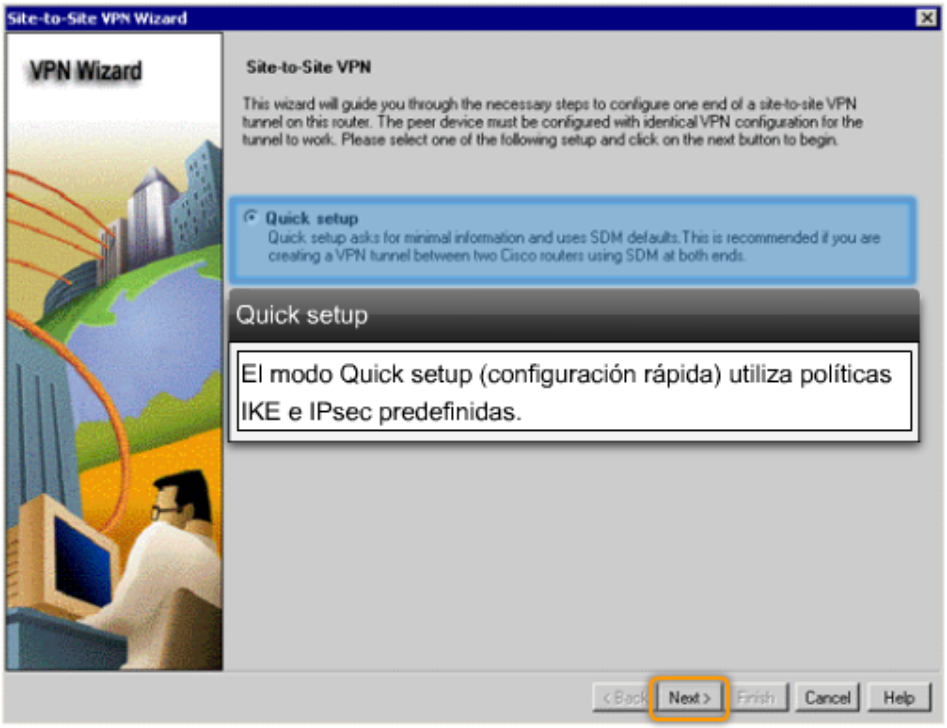
La opción Quick setup utiliza las políticas IKE y conjuntos de transformación IPsec por defecto del Cisco SDM. Permite a un administrador junior configurar en forma rápida una VPN IPsec utilizando los mejores parámetros de seguridad.

El asistente Step by step wizard permite al administrador especificar todos los detalles finos de una VPN IPsec.

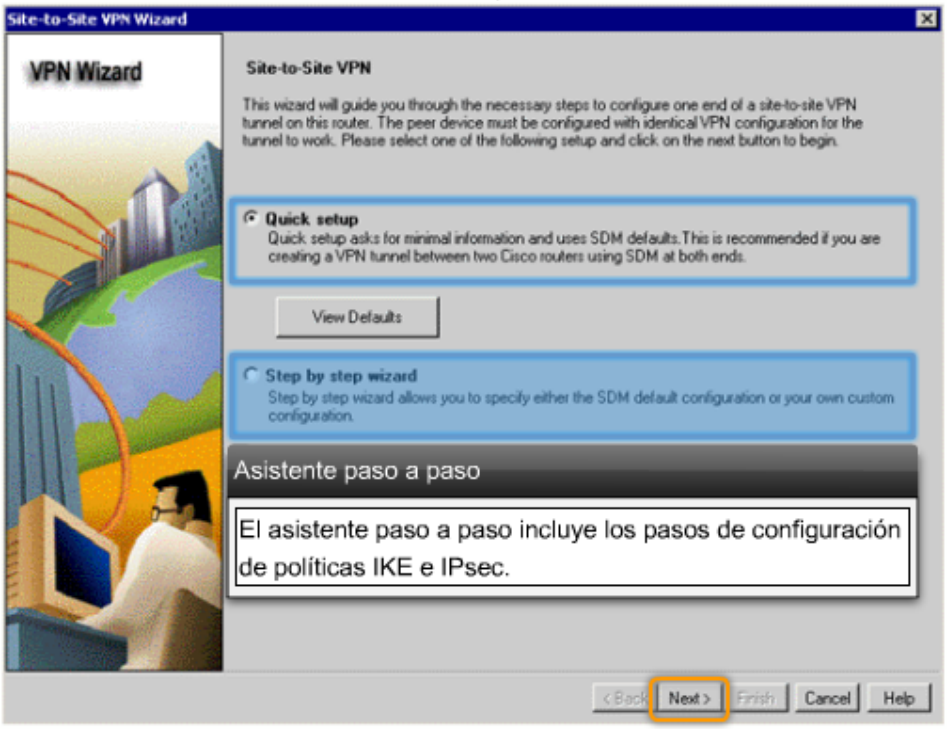
Haga clic en el botón Next para configurar los parámetros de la conexión VPN.



Pase el cursor sobre las áreas resaltadas con azul para ver más información sobre el modo del asistente.



Pase el cursor sobre las áreas resaltadas con azul para ver más información sobre el modo del asistente.



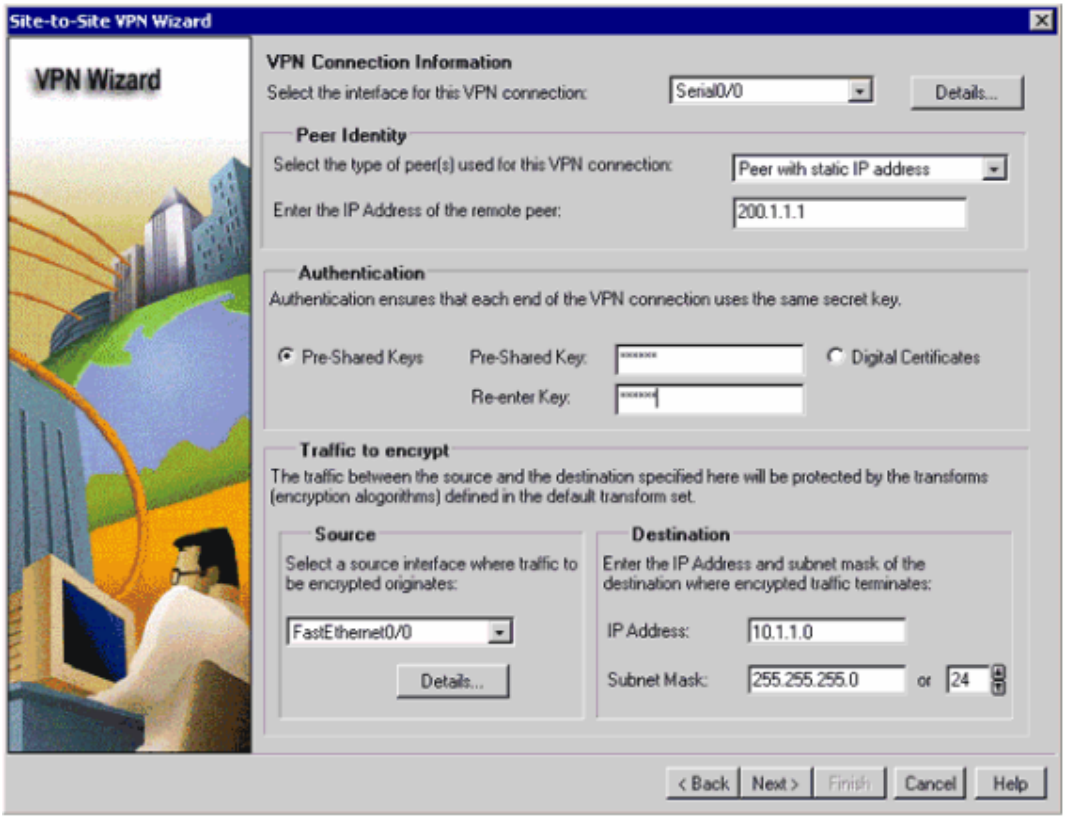
Pase el cursor sobre las áreas resaltadas con azul para ver más información sobre el modo del asistente.

8.5.2 Asistente VPN – Configuracion Rapida

La opción de configuración rápida utiliza una sola ventana para configurar la conexión VPN e incluye los siguientes parámetros:

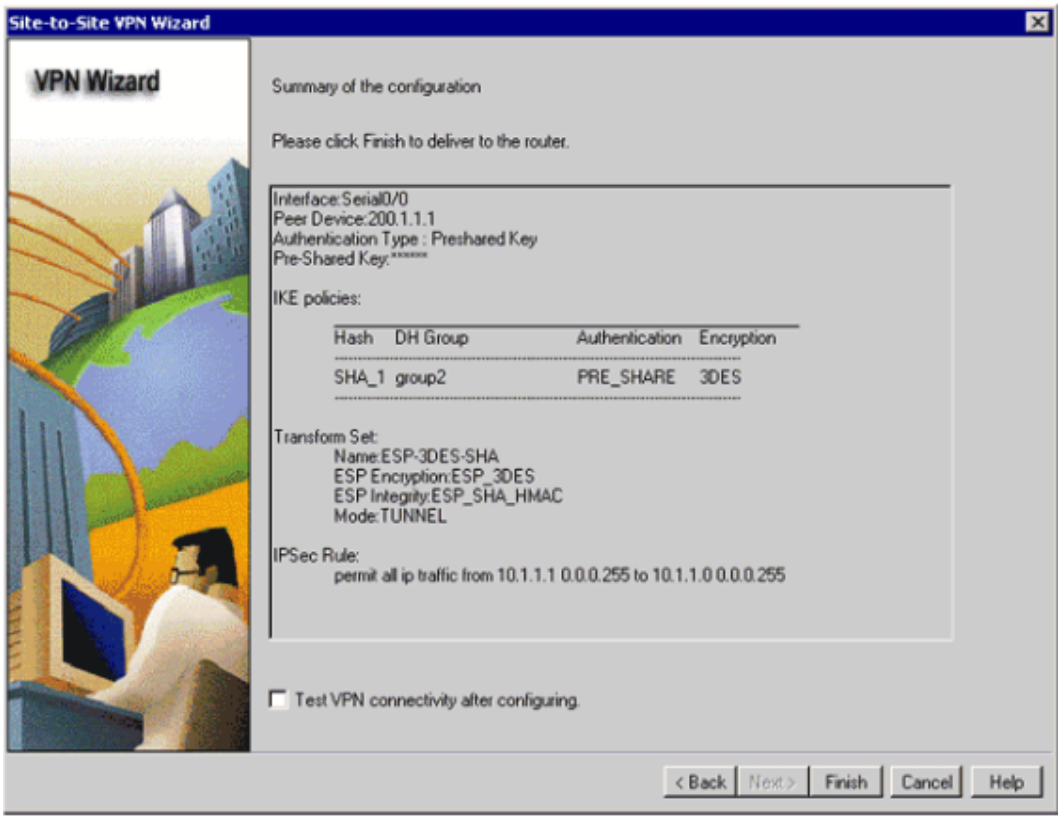
Interfaz a utilizar por la conexión VPN (usualmente la interfaz externa)
Información de identidad del par, la cual incluye el tipo de par y su dirección IP
Método de autenticación, ya sea PSKs (especificar el secreto) o certificados digitales (seleccionar un certificado creado de antemano)
Tráfico a cifrar, identificando la interfaz origen y la subred IP destino

Cisco SDM proporciona una política IKE por defecto para determinar la autenticación, un conjunto de transformación por defecto para controlar el cifrado de datos y una regla IPsec por defecto que cifra todo el tráfico entre el router y el dispositivo remoto.



Cuando todos los parámetros están configurados, verifique la configuración en la página de resumen antes de hacer clic en Finish.

La configuración rápida es mejor aplicada cuando tanto el router local como el sistema remoto son routers Cisco con Cisco SDM. La configuración rápida configura cifrado 3DES si la misma es soportada por la imagen del Cisco IOS. En caso contrario, configura cifrado DES. Si se requiere cifrado AES o SEAL, debe utilizarse el asistente paso a paso (Step-by-Step).



8.5.3 Asistente VPN – Configuracion paso a paso (Step-by-Step)

El asistente paso a paso requiere múltiples pasos para configurar una conexión VPN e incluye los siguientes parámetros:

Configuración de conexión, incluyendo la interfaz externa, identidad del par y credenciales de autenticación.
Propuestas IKE, tales como prioridad, cifrado, el algoritmo HMAC (Hashed Message Authentication Code), el método de autenticación IKE, el grupo DH (Diffie-Hellman) y el tiempo de vida IKE.
Información del conjunto de transformación IPsec, incluyendo nombre, algoritmo de integridad, algoritmo de cifrado, modo de operación (túnel o transporte) y compresión
Tráfico a proteger, identificando las subredes únicas de origen y destino o definiendo una ACL para su uso en VPNs más complejas.

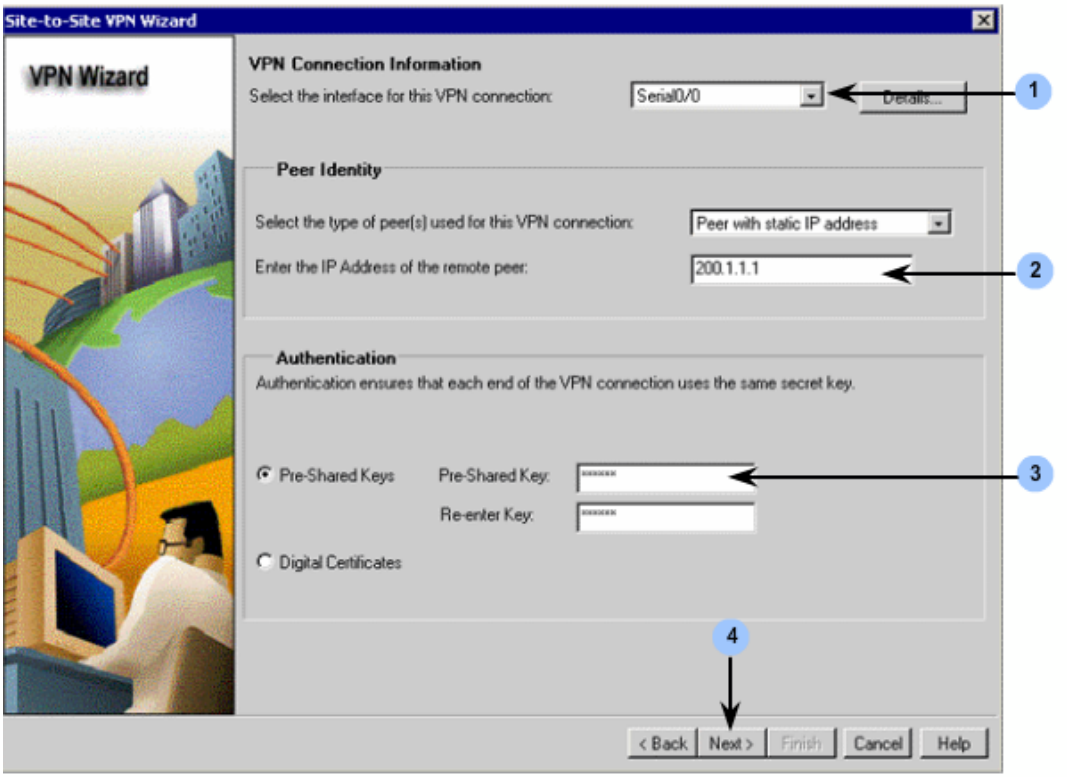
La primer tarea en el asistente paso a paso es configurar las opciones de conexión.

Paso 1. Seleccione la interfaz externa que se conectará al par IPsec a través de la red no confiable.

Paso 2. Especifique la dirección IP del par.

Paso 3. Seleccione el método de autenticación y especificar las credenciales. Utilice PSKs largas y aleatorias para prevenir ataques de diccionario y de fuerza bruta contra el IKE.

Paso 4. Haga clic sobre Next para ir a la siguiente tarea.



La segunda tarea del asistente paso a paso es configurar las propuestas IKE. Es posible crear una propuesta IKE personalizada o utilizar la propuesta IKE por defecto.

Propuesta IKE personalizada

Para crear una propuesta IKE personalizada, debe agregar un nuevo IKE.

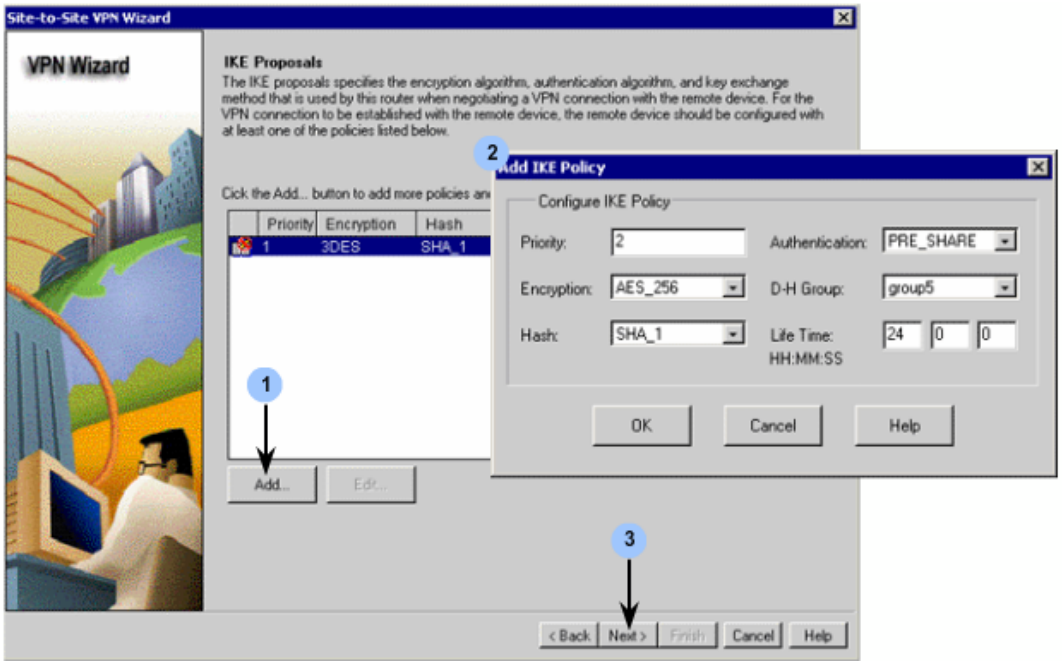
Paso 1. Haga clic en el botón Add para definir una propuesta y especificar su prioridad, algoritmo de cifrado, algoritmo de hashing, método de autenticación IKE, grupo DH y tiempo de vida IKE.

Paso 2. Haga clic sobre OK cuando la propuesta IKE esté completa.

Paso 3. Una vez agregadas las políticas IKE, seleccione la propuesta a utilizar. Haga clic sobre Next para seguir con la siguiente tarea

Propuesta IKE predefinida

Para utilizar la propuesta IKE predefinida, seleccione Next en la página IKE Proposal. De esta forma, selecciona la propuesta IKE predefinida por defecto



La tercera tarea del asistente paso a paso consiste en configurar el conjunto de transformación. Es posible crear un conjunto de transformación IPsec personalizado o utilizar un conjunto predefinido.

Conjunto de transformación IPsec personalizado

Para crear un conjunto de transformación IPsec personalizado, es necesario agregar un nuevo conjunto.

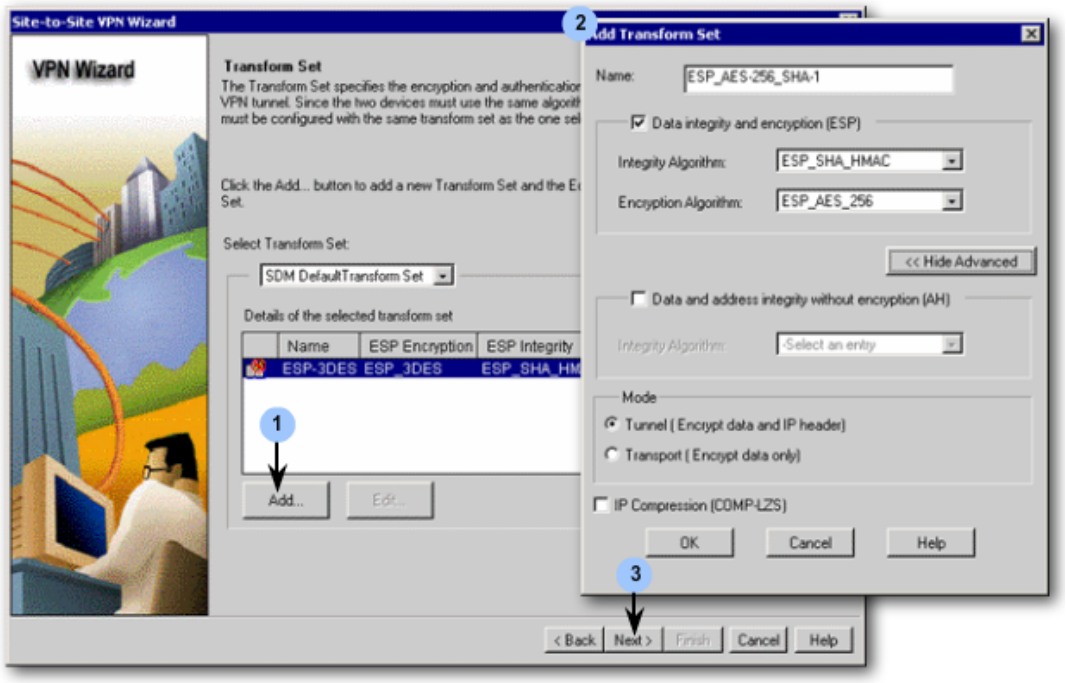
Paso 1. Haga clic sobre el botón Add para definir el conjunto de transformación y especificar su nombre, algoritmo de integridad, algoritmo de cifrado, modo de operación y compresión opcional.

Paso 2. Haga clic sobre OK cuando el conjunto de transformación esté completo.

Paso 3. Una vez agregados los nuevos conjuntos de transformación, seleccione cuál de ellos será utilizado y haga clic en Next para proceder a la siguiente tarea.

Conjunto de transformación IPsec predefinido

Para utilizar el conjunto de transformación IPsec, haga clic sobre Next en la página Transform Set. El conjunto de transformación predefinido será seleccionado por defecto.



La cuarta tarea del asistente paso a paso consiste en configurar qué tráfico requiere protección.

Para proteger todo el tráfico entre una subred IP y otra:

Paso 1. En la ventana Traffic to Protect, haga clic sobre la opción Protect all traffic between the following subnets.

Paso 2. Defina la dirección IP y máscara de subred de la red local donde se origina el tráfico IPsec.

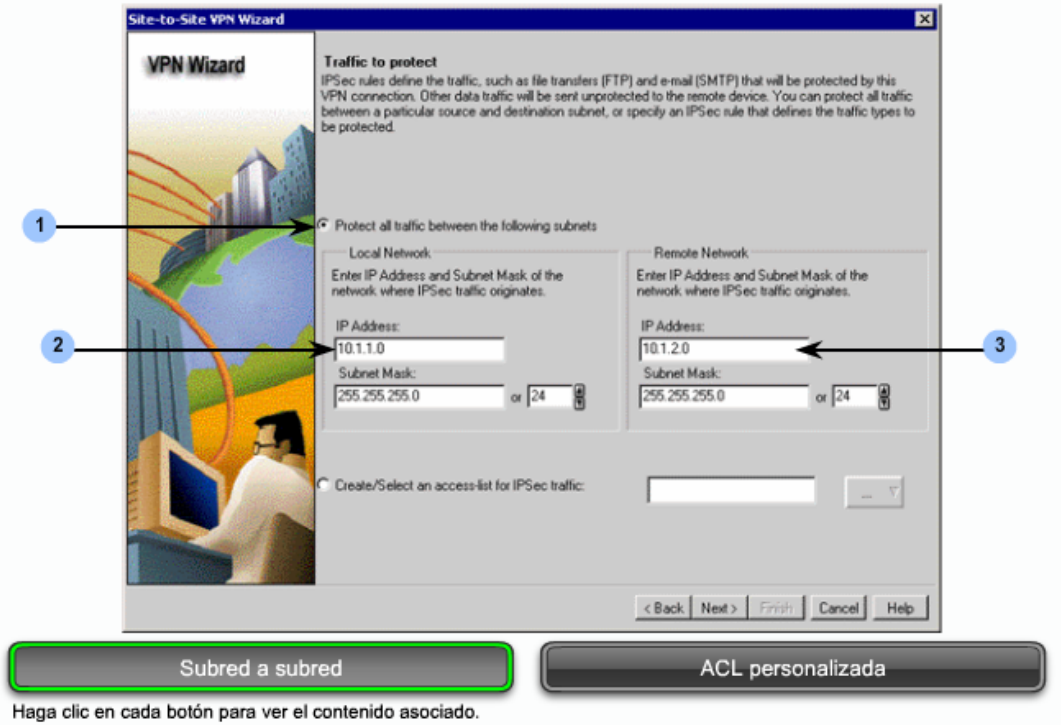
Paso 3. Defina la dirección IP y máscara de subred de la red remota hacia donde se envía el tráfico IPsec.

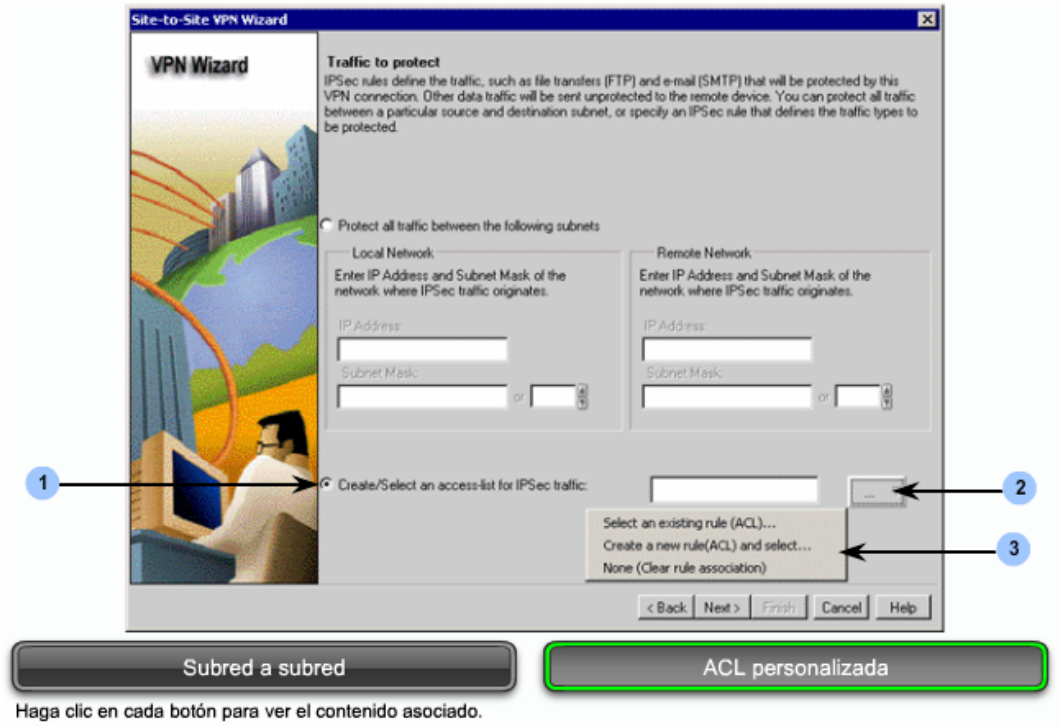
Para especificar una ACL Personalizada (regla IPsec) que defina el tipo de tráfico a proteger:

Paso 1. En la ventana Traffic to Protect, haga clic sobre la opción Create/Select an access-list for IPSec traffic.

Paso 2. Haga clic sobre el botón de puntos suspensivos (...) para seleccionar una ACL existente o para crear una nueva.

Paso 3. Para utilizar una ACL existente, seleccione la opción Select an existing rule (ACL). Para crear una nueva ACL, seleccione la opción Create a new rule (ACL) and select.





Al crear una nueva ACL para definir el tráfico que requiere protección, se presenta una ventana que lista la lista de reglas de acceso creadas:

Paso 1. Asigne un nombre y una descripción a la regla de acceso.

Paso 2. Haga clic sobre el botón Add para comenzar a agregar las entradas de la regla.

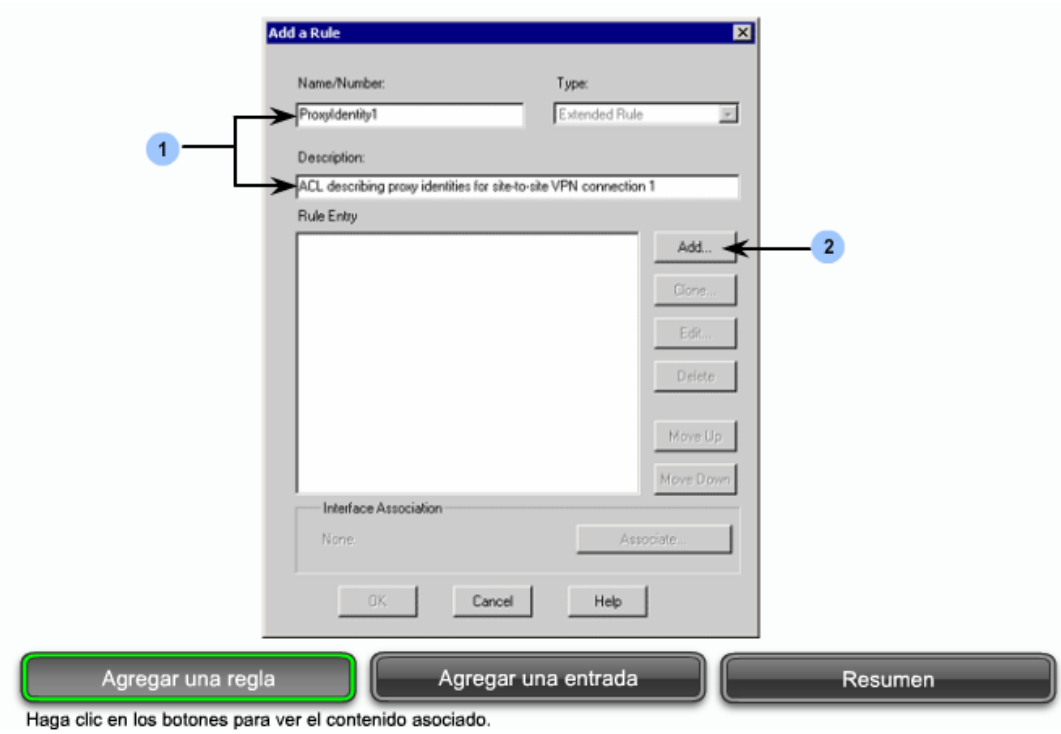
Luego de crear una nueva ACL, debe especificar las entradas dentro de dicha ACL.

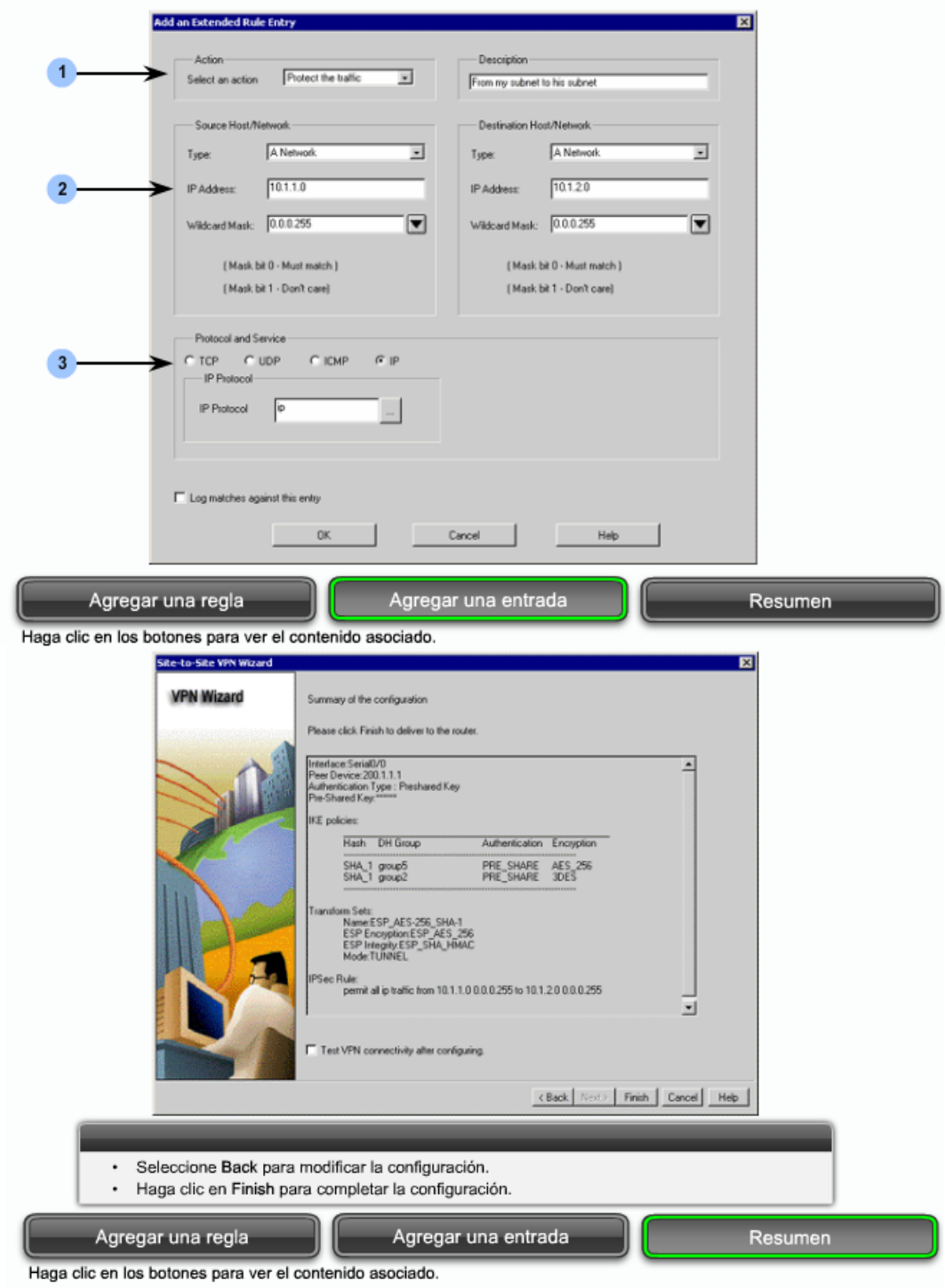
Paso 1. Seleccione una acción de la lista Select an Action e ingrese una descripción para la entrada en el recuadro Description.

Paso 2. Defina los hosts o redes de origen en el panel Source Host/Network y los hosts o redes de destino en el panel Destination Host/Network. Cada entrada define un par de direcciones o redes origen y destino. Asegúrese de utilizar wildcards y no la máscara de subred en el campo Wildcard Mask.

Paso 3. (Opcional) Para proporcionar protección adicional para un protocolo específico, seleccione el protocolo entre las opciones TCP, UDP o ICMP y los números de puerto. Si selecciona IP como protocolo, la regla se aplica a todo el tráfico IP.

Al finalizar la configuración, el asistente presenta un resumen con los parámetros seleccionados. Para modificar esta configuración, haga clic en el botón Back. Para completar la configuración, haga clic en el botón Finish.



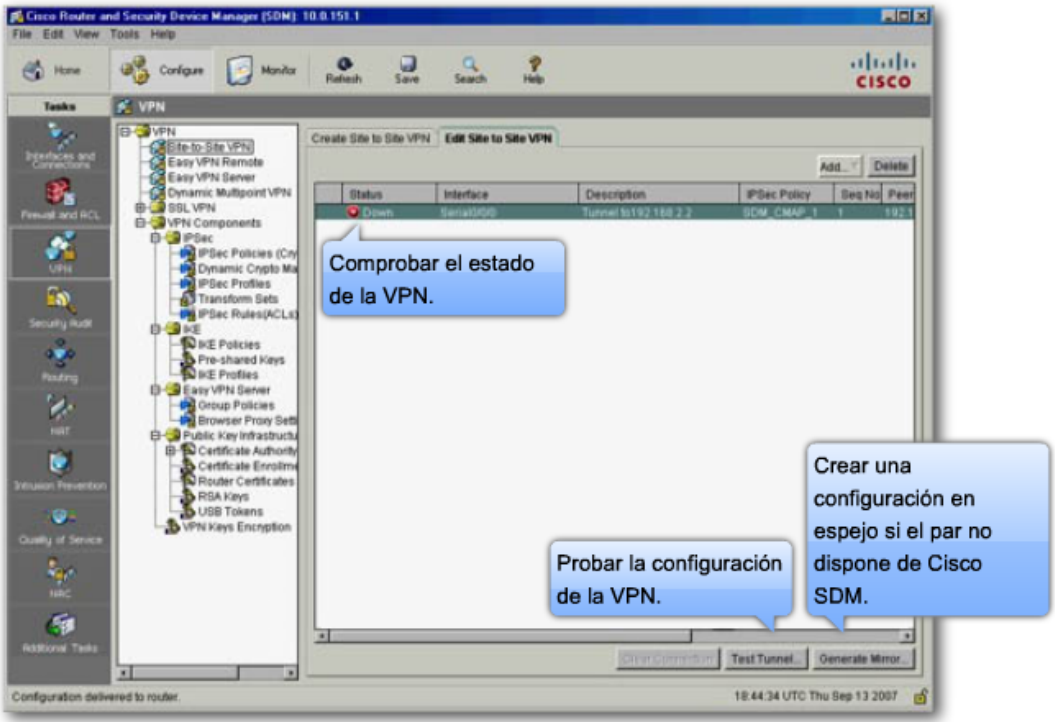


8.5.4 Verificacion, monitoreo y resolucion de problemas de VPNs

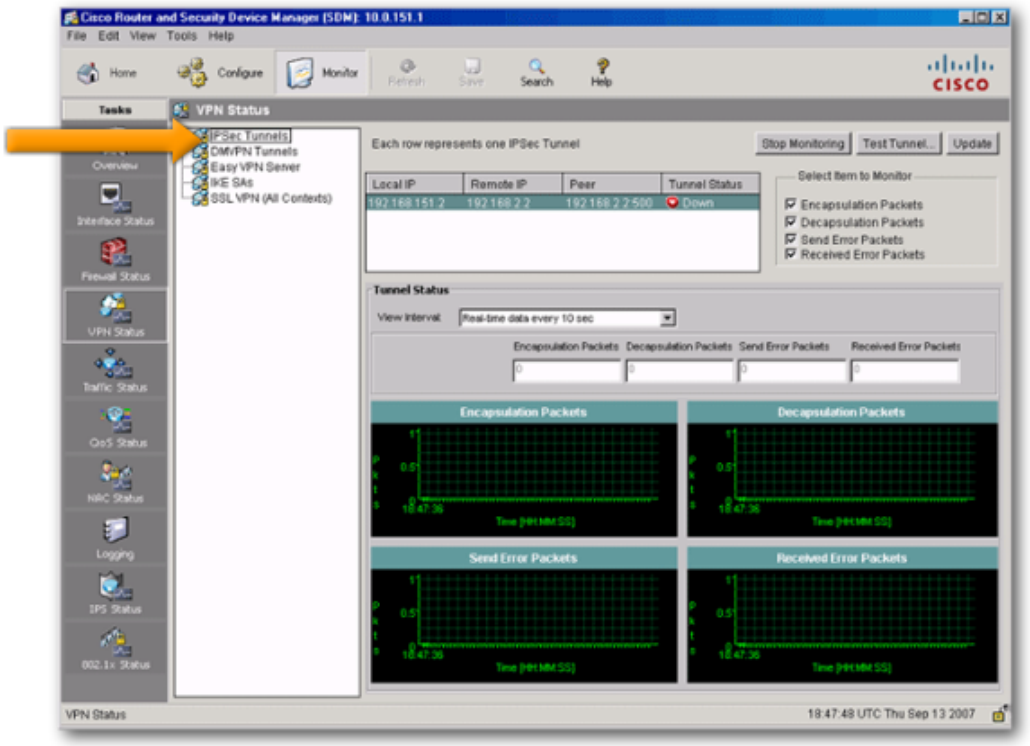
Una vez configurada una VPN IPsec, es necesario probarla para verificar su operación.

Para probar la configuración de un túnel VPN, ingrese en Configure > VPN > Site-to-Site VPN > Edit Site-to-Site VPN y seleccione el botón Test Tunnel.

También puede utilizar el botón Generate Mirror para generar una configuración en espejo, la cual es requerida en el otro extremo del túnel. Esto resulta útil si el otro router no tiene un Cisco SDM y sólo puede utilizarse la interfaz de línea de comandos (CLI) para configurar el túnel.



Para ver todos los túneles IPsec, sus parámetros y su estado, seleccione Monitor > VPN Status > IPsecTunnels.



Lista todos los túneles IPsec, sus parámetros y su estado.

8.6 Implementacion de VPNs de acceso remoto

8.6.1 El escenario corporativo cambiante

¿Cuántas horas dedican los empleados a viajar hacia y desde su trabajo todos los días? ¿Qué sucede si hay embotellamientos de tránsito? ¿Cómo pueden resultar productivas estas horas? La respuesta es el teletrabajo.

El teletrabajo también es conocido como trabajo a distancia. Los empleados teletrabajadores disponen de flexibilidad de su ubicación y horarios. Los empleadores ofrecen la opción de teletrabajo porque les permite ahorrar en alquileres, servicios y otros costos adicionales. Las organizaciones que tienen los mejores logros con un programa de trabajo a distancia aseguran que esta forma de trabajo es voluntaria, sujeta a decisión gerencial, operacionalmente posible y no genera costos adicionales.

Las organizaciones de trabajo a distancia aprovechan al máximo las nuevas tecnologías y las nuevas formas de trabajo. Con el trabajo a distancia, el foco se encuentra sobre el trabajo realizado y no sobre el lugar donde se realiza. Este aspecto del teletrabajo nos acerca a una sociedad global, permitiendo que individuos de todo el mundo trabajen en conjunto. Como uno de los transformadores clave del espacio laboral de la próxima década, no existen dudas de que reformará en forma dramática e inevitable la forma en que el trabajo se lleva a cabo.







El teletrabajo ofrece beneficios organizacionales, sociales y ambientales. Hay estudios que han demostrado que el teletrabajo mejora la calidad de vida, disminuyendo el estrés relacionado con el trabajo. También permite acomodarse a aquellos empleados con problemas de salud o discapacidades. El trabajo a distancia reduce el consumo de energía, disminuyendo la polución generada por el transporte. Además, aumenta las ganancias de la organización, mejora la contratación y la retención y puede ofrecer posibilidades de un mayor alcance global. Disponer de trabajadores a distancia en diferentes zonas horarias permite asegurar que la compañía se encuentra virtualmente abierta las 24 horas.

Aunque el teletrabajo presenta muchos beneficios, existen también algunas desventajas. Por ejemplo, aquellos empleados que trabajan desde sus hogares pueden experimentar distracciones que no se presentarían en la oficina. Además, las compañías que ofrecen programas de trabajo a distancia deben considerar riesgos mayores, ya que los datos viajan a través de redes públicas y las organizaciones deben confiar en que sus empleados mantengan sus sistemas seguros.

Beneficios del trabajo a distancia:

Beneficios organizacionales:

- Continuidad de las operaciones
- Aumento en la capacidad de respuesta
- Acceso a la información seguro, confiable y manejable
- Integración rentable de datos, voz, video y aplicaciones
- Aumento en la productividad, satisfacción y retención de los empleados

Beneficios sociales:

- Mayores oportunidades de empleo para grupos marginados
- Menos estrés relacionado al tiempo de viaje

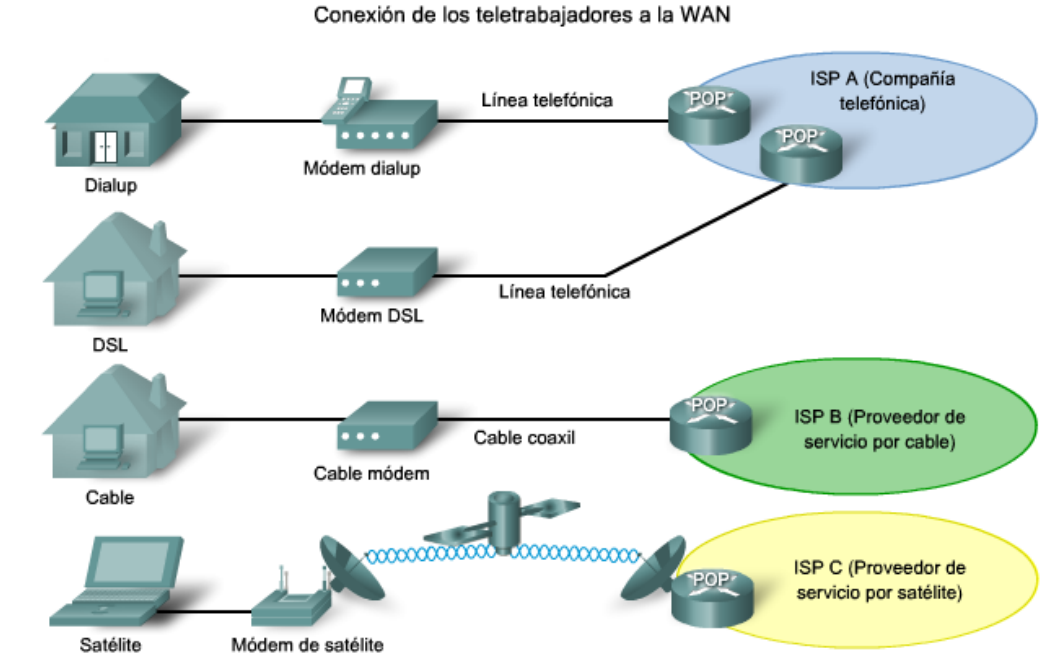
Beneficios ambientales:

- Reducción en la huella de carbono, tanto para los trabajadores individuales como para las organizaciones

Los trabajadores a distancia en general requieren acceso a Internet de alta velocidad. Este acceso puede ser provisto utilizando conexiones a Internet de banda ancha, tales como DSL, Cable o Satélite. Aunque es posible utilizar conexiones de acceso telefónico, la velocidad disponible es demasiado lenta y no es considerada adecuada para el trabajo a distancia.

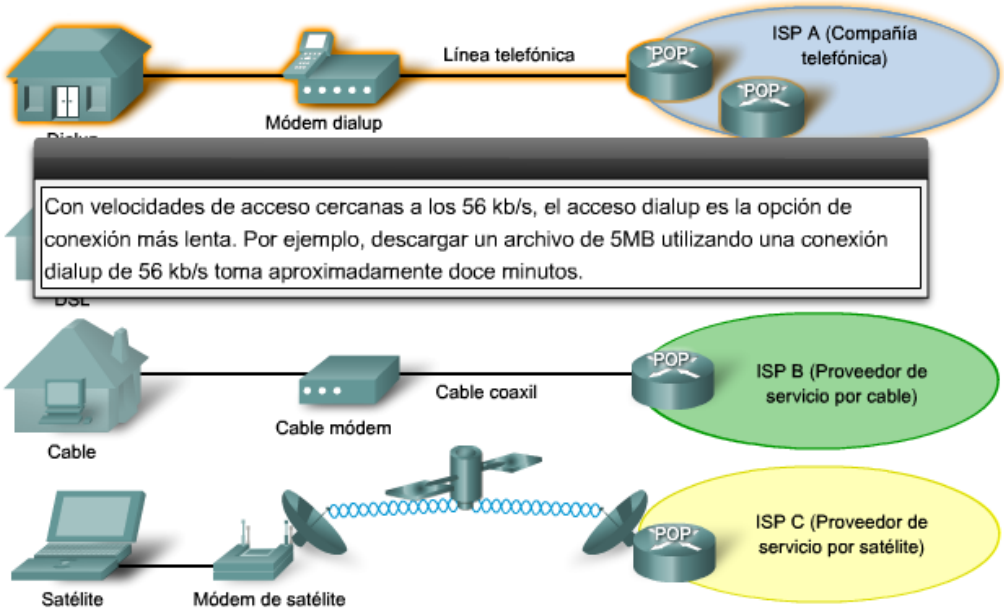
También son necesarias computadoras laptop o desktop y muchas implementaciones también requieren telefonía VoIP para obtener servicios telefónicos transparentes.

La seguridad es una preocupación importante para las compañías. El acceso remoto a las ubicaciones corporativas se realiza utilizando un acceso remoto por VPN.



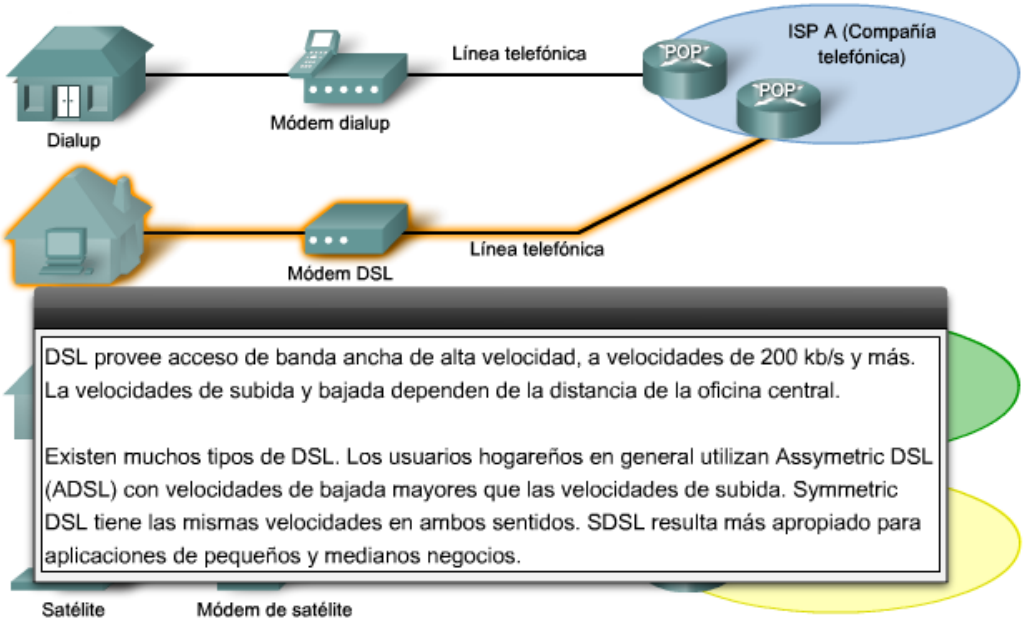
Pase el cursor sobre cada tipo de conexión para más información.

Conexión de los teletrabajadores a la WAN

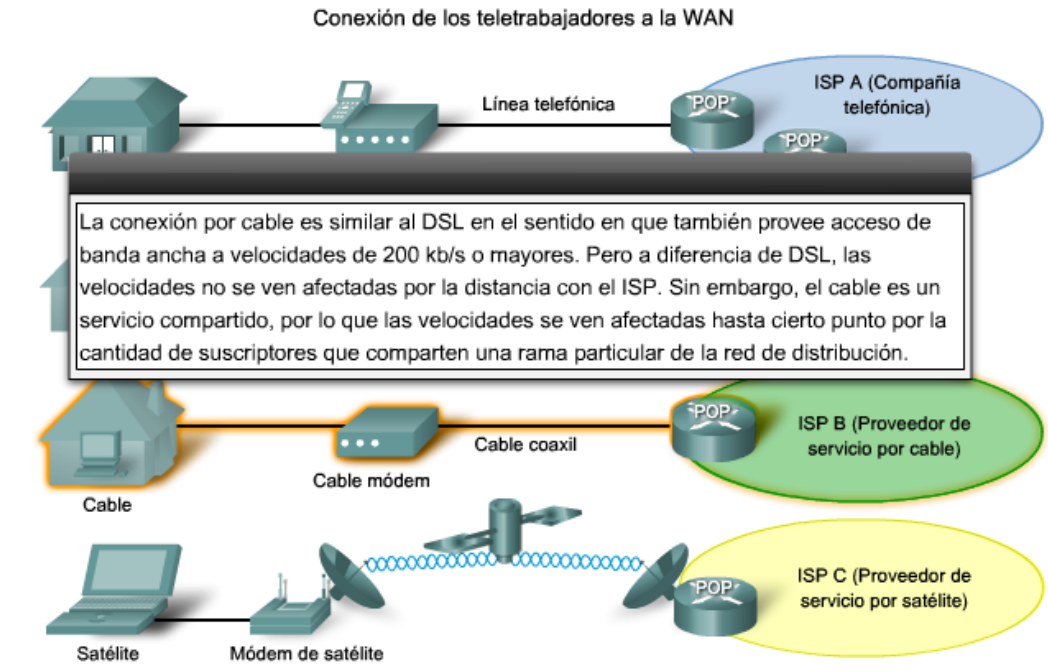


Pase el cursor sobre cada tipo de conexión para más información.

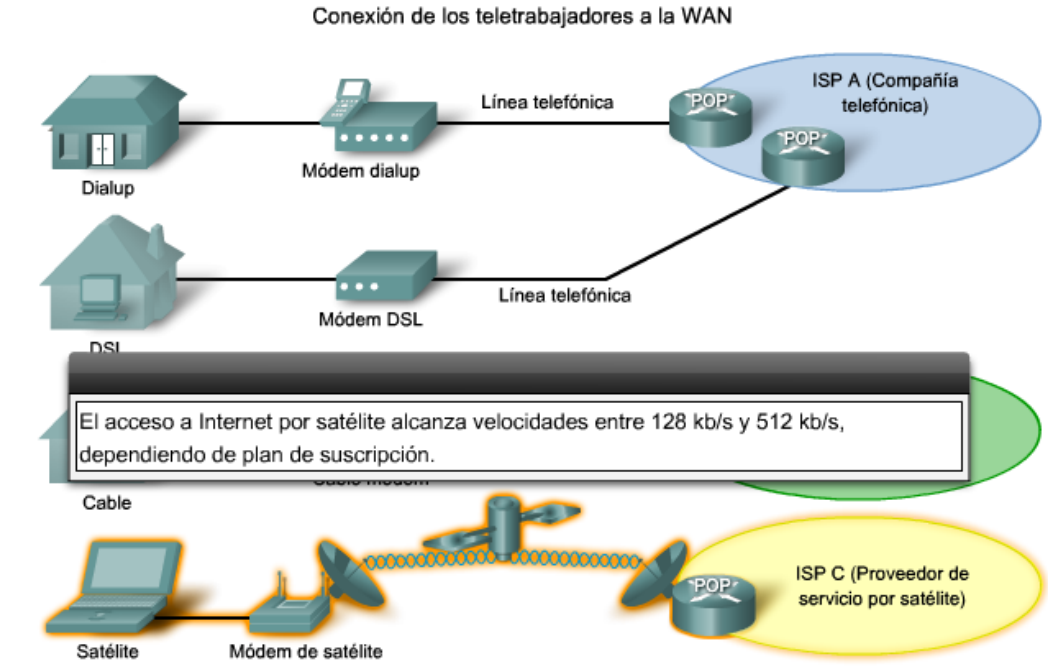
Conexión de los teletrabajadores a la WAN



Pase el cursor sobre cada tipo de conexión para más información.



Pase el cursor sobre cada tipo de conexión para más información.



Pase el cursor sobre cada tipo de conexión para más información.

8.6.2 Introduccion a las VPNs de acceso remoto

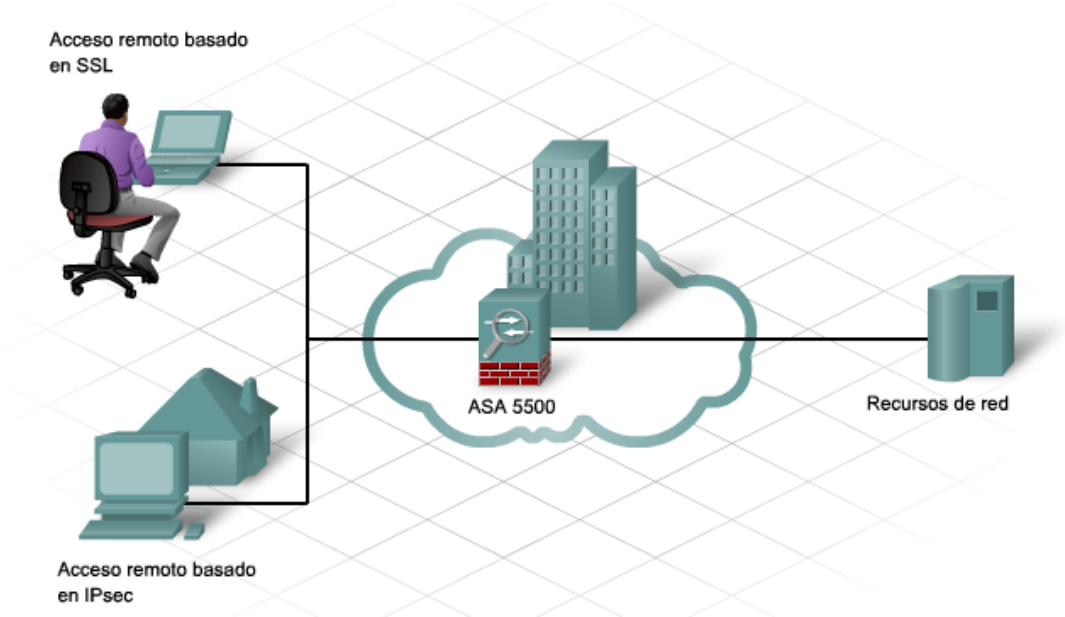
La omnipresencia de Internet, combinada con las tecnologías VPN actuales, permite a las organizaciones extender el alcance de sus redes en forma segura y rentable, para alcanzar a cualquier persona, en cualquier lugar y en cualquier momento.

Las VPNs se han vuelto la solución lógica para la conectividad de acceso remoto por muchas razones. Las VPNs proveen comunicaciones seguras con permisos de acceso ajustados a usuarios individuales, tales como empleados, contratistas y socios. También mejoran la productividad, extendiendo la red y aplicaciones corporativas en forma segura, al mismo tiempo que se reducen los costos y se aumenta la flexibilidad.

Utilizando tecnología VPN, los empleados pueden esencialmente llevar consigo su oficina, influyendo el acceso al correo electrónico y sus aplicaciones de red. Las VPNs pueden también permitir que los contratistas y socios tengan un acceso limitado a servidores, sitios web o archivos específicos requeridos. Este acceso a la red les permite contribuir a la productividad del negocio sin comprometer la seguridad de la red.

Existen dos métodos principales para implementar VPNs de acceso remoto:

Secure Sockets Layer (SSL)
IP Security (IPsec)



El método de VPN implementado se basa en los requisitos de acceso de los usuarios y de los procesos de IT de la organización.

Tanto la tecnología IPsec como VPN SSL ofrecen acceso a virtualmente cualquier aplicación o recurso de la red. Las VPNs SSL ofrecen características como conectividad simple desde máquinas de escritorio no controladas por la compañía, poco o nulo mantenimiento del software en ellas y portales web personalizados para el usuario luego de identificarse.

IPsec excede SSL de muchas formas significativas:

Número de aplicaciones soportadas
Fortaleza de su cifrado
Fortaleza de su autenticación

Seguridad general

Cuando la seguridad es un problema, IPsec es la elección superior. Si el soporte y la facilidad de instalación son el punto principal, debe considerarse SSL.

VPN IPsec y VPN SSL son complementarias, ya que resuelven diferentes problemas. Dependiendo de sus necesidades, una organización puede implementar una o ambas. Este enfoque complementario permite que un solo dispositivo, tal como un router ISR o un firewall ASA, pueda resolver todos los requisitos de los usuarios de acceso remoto. Mientras que muchas soluciones ofrecen IPsec o SSL, las soluciones de acceso remoto VPN de Cisco ofrecen ambas tecnologías en una misma plataforma con administración unificada. Ofrecer tanto IPsec como SSL permite a las organizaciones personalizar sus VPNs de acceso remoto sin ningún tipo de hardware adicional o complejidad administrativa.

	SSL	IPsec
Aplicaciones	Aplicaciones web, archivos compartidos, correo electrónico	Todas las aplicaciones basadas en IP
Cifrado	Moderada Longitudes de clave desde 40 bits hasta 128 bits	Más fuerte Longitudes de clave desde 56 bits hasta 256 bits
Autenticación	Moderada Autenticación de una vía o de dos vías	Más fuerte Autenticación de dos vías utilizando secretos compartidos o certificados digitales
Facilidad de uso	Muy fácil	Moderada Puede resultar dificultosa para usuarios no técnicos
Opciones de conexión	Cualquier dispositivo puede conectarse	Sólo pueden conectarse dispositivos específicos con configuraciones específicas

8.6.3 VPNs SSL

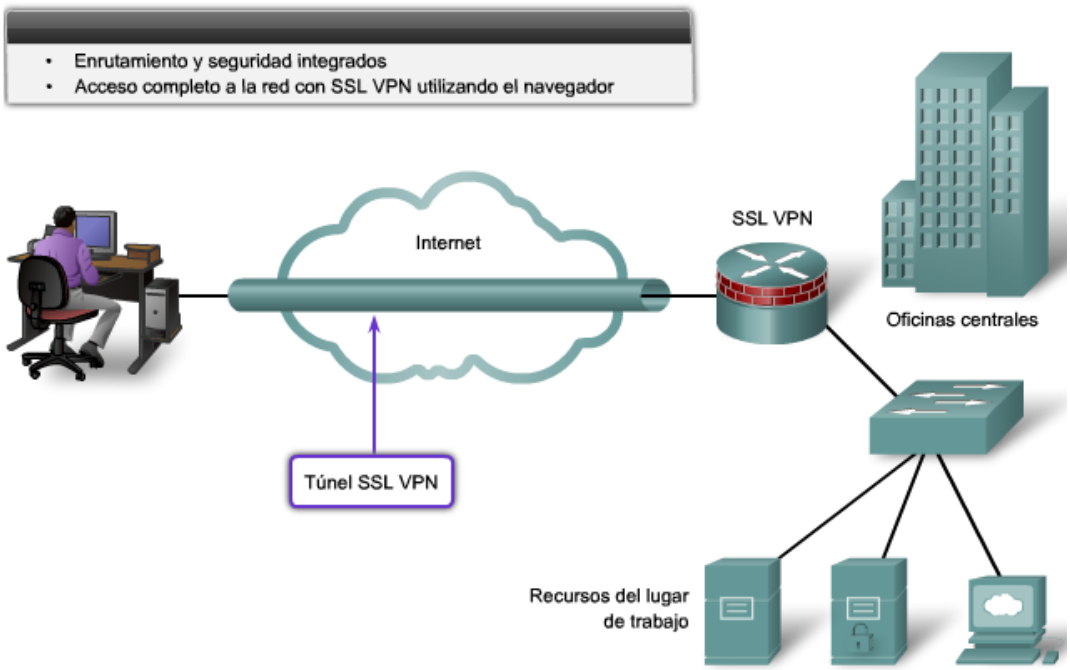
Cisco IOS VPN SSL es una tecnología emergente que proporciona conectividad de acceso remoto a casi cualquier ubicación conectada a Internet, utilizando un navegador web y cifrado SSL nativo. Desarrollado originalmente por Netscape, SSL ha sido aceptado en la Web de forma universal.

Una VPN SSL no requiere un cliente de software instalado previamente en el host remoto. Proporciona conectividad de acceso remoto a los recursos corporativos a cualquier usuario autorizado, desde cualquier ubicación en Internet.

El protocolo SSL soporta una variedad de diferentes algoritmos criptográficos para operaciones tales como autenticar al servidor y al cliente entre sí, transmitir certificados y establecer claves de sesión. Las soluciones Cisco VPN SSL pueden ser personalizadas para empresas de cualquier tamaño. Estas soluciones proveen muchas funcionalidades y beneficios de la conectividad de acceso remoto:

Acceso basado en Web sin clientes y acceso completo a la red, sin software instalado previamente en el equipo. Esto facilita el acceso remoto personalizado basado en el

usuario y los requisitos de seguridad y minimiza el costo de soporte de los equipos desktop.
Protección contra virus, gusanos, spyware y hackers, integrando seguridad en la red y en la plataforma Cisco VPN SSL. Esto reduce los costos y la complejidad de la administración, eliminando la necesidad de equipos e infraestructura adicionales de seguridad.
Licenciamiento simple, flexible y rentable. SSL utiliza una única licencia. No existen licencias por funcionalidad. Los aumentos en la cantidad de usuarios son flexibles y rentables. Una implementación puede comenzar con unos 10 usuarios y luego escalar a medida que sea necesario.
Un mismo dispositivo tanto para VPN SSL y VPN IPsec. Esto reduce los costos y la complejidad de administración, permitiendo servicios robustos de VPN de acceso remoto y sitio a sitio desde una misma plataforma, unificando su administración.



Las VPNs SSL proveen diferentes tipos de acceso:

Sin cliente
Cliente liviano
Cliente pesado

VPN SSL provee tres modos de acceso remoto en los routers con Cisco IOS: sin cliente (clientless), cliente liviano (thin client) y cliente pesado (full client). Los dispositivos ASA tienen dos modos: sin cliente (el cual incluye el reenvío de puertos sin cliente y de cliente liviano) y el cliente AnyConnect (que reemplaza al túnel completo)

Modo de acceso sin cliente

En el modo sin cliente, el usuario remoto accede a la red interna o corporativa utilizando un navegador web en la máquina cliente. El acceso sin cliente no requiere de un software VPN especializado instalado en el equipo desktop. Todo el tráfico VPN es transmitido y entregado a través de un navegador web estándar. No se requiere otro tipo de software, eliminando así muchos problemas de soporte. Utilizando una conexión sin cliente, es posible acceder a todas las aplicaciones web y algunas aplicaciones cliente/servidor, tales como intranets, aplicaciones con interfaz web, correo electrónico, calendarios y servidores de archivos.

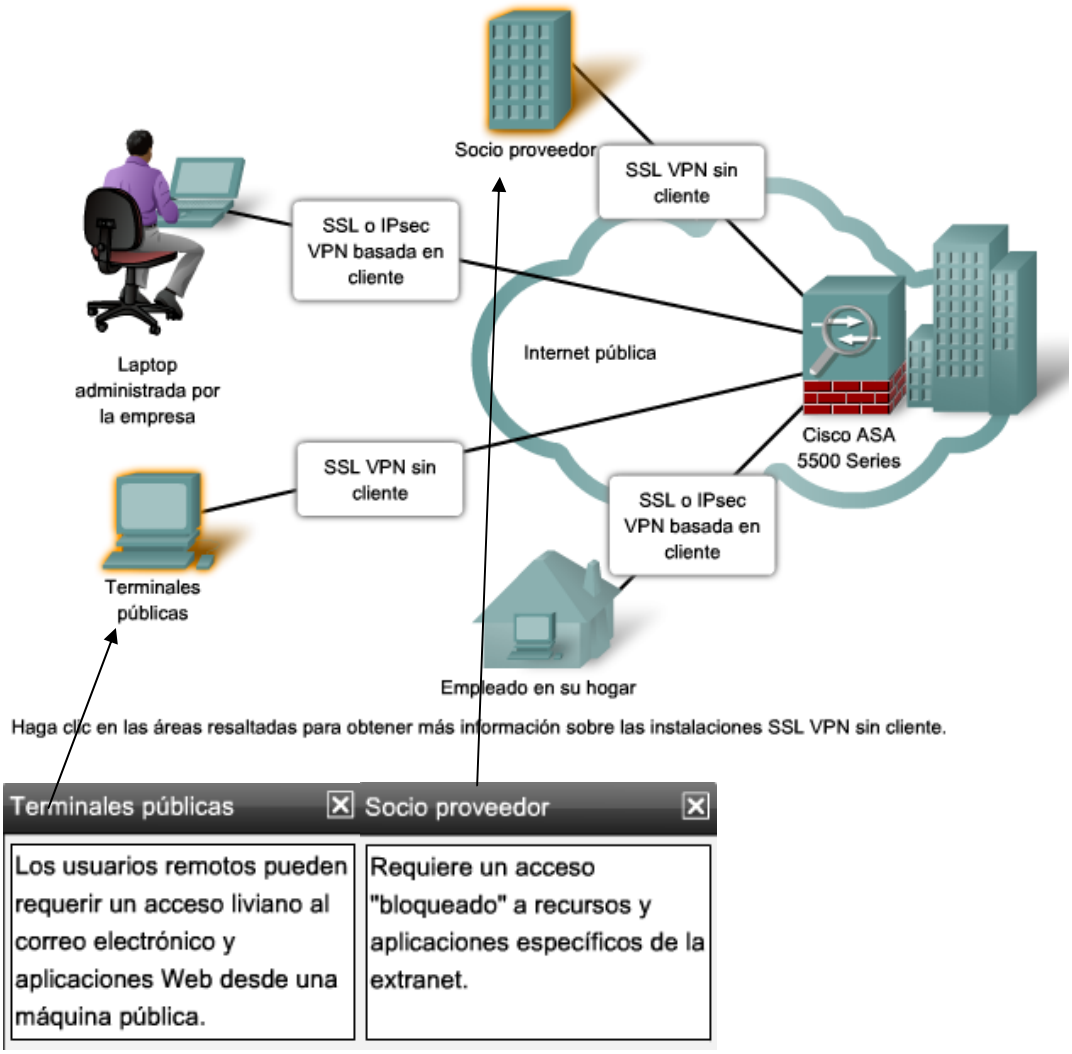
No todas las aplicaciones cliente/servidor son accesibles mediante clientes SSL. Sin embargo, este acceso limitado es muchas veces una solución perfecta para socios comerciales o contratistas, quienes deben acceder sólo a un conjunto limitado de recursos en la red de la organización. No funciona para empleados que requieren acceso completo a la red.

Modo de cliente liviano

El modo de cliente liviano, llamado a veces reenvío de puertos TCP, asume que la aplicación cliente utiliza TCP para conectarse a un puerto de un servidor bien conocido. En este modo, el usuario remoto descarga un applet Java utilizando un enlace provisto en la página del portal. El applet Java actúa como un proxy TCP en la máquina cliente para los servicios configurados en el gateway de la VPN SSL. El applet Java inicia una nueva conexión SSL para cada conexión del cliente.

El applet Java inicia una petición HTTP desde el cliente del usuario remoto hacia el gateway de la VPN SSL. El nombre y número de puerto del servidor interno de correo electrónico está incluido en la petición. El gateway VPN crea una conexión TCP para dicho servidor y puerto de correo electrónico interno.

El modo de cliente liviano es también conocido como un tipo de modo sin cliente y puede ser utilizado en cualquier equipo que soporte VPNs sin cliente. Extiende la capacidad de las funciones criptográficas del navegador web para permitir el acceso remoto a aplicaciones basadas en TCP, tales como POP3, SMTP, IMAP, Telnet y SSH.

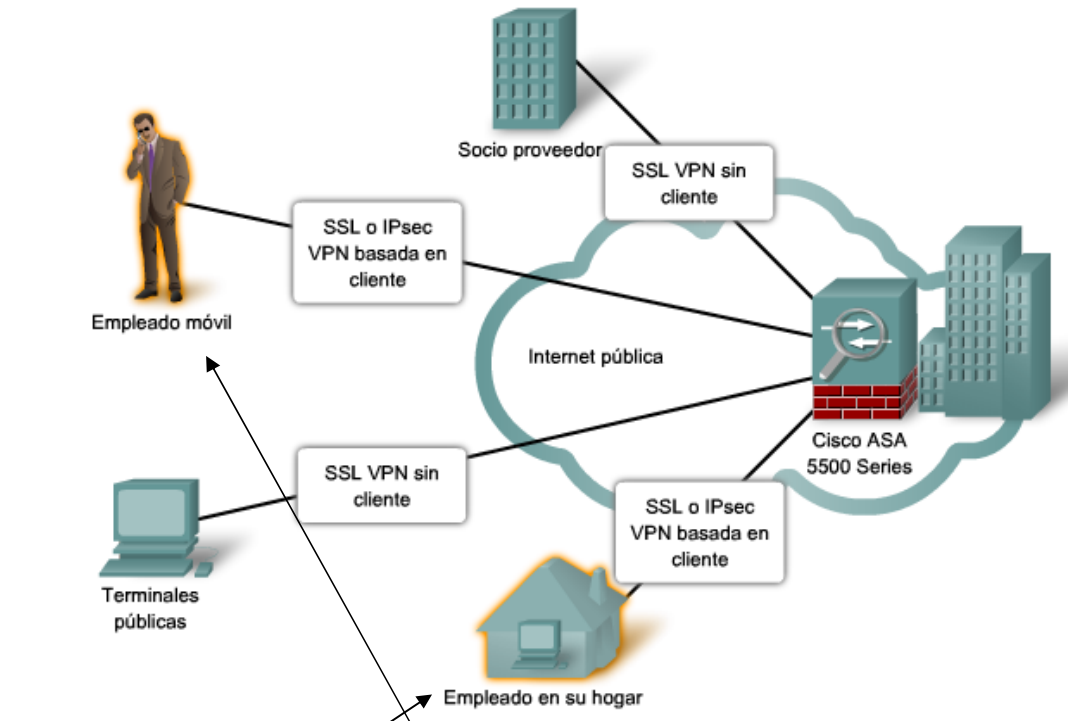


Modo de acceso de túnel completo

El modo de túnel completo (Full Tunnel) permite el acceso completo a la red corporativa utilizando un túnel VPN SSL, el cual es utilizado para transportar datos al nivel de capa de red (IP). Este modo soporta la mayor parte de las aplicaciones basadas en IP, tales como Microsoft Outlook, Microsoft Exchange, Lotus Notes Email y Telnet. El ser parte de la VPN SSL es transparente para las aplicaciones que se ejecutan en el cliente. Se descarga un applet Java para manipular el túnel entre el host cliente y el gateway de la VPN SSL. El usuario puede utilizar cualquier aplicación como si el host cliente se encontrara dentro de la red interna.

Este cliente VPN, debido a que es descargado en forma dinámica y actualizado sin ninguna distribución manual de software o interacción con el usuario final, requiere poco o nulo soporte por parte de las organizaciones de IT, minimizando así los costos de implementación y operación. Al igual que con el acceso sin cliente, el modo de acceso completo ofrece un acceso total y personalizado en base a los privilegios de acceso del usuario final. El modo de acceso completo es una opción natural para los empleados que necesitan acceso remoto a las mismas aplicaciones y recursos de red que

utiliza dentro de la oficina o para cualquier aplicación cliente/servidor que no puede ser transportada a través de conexiones sin cliente basadas en web.



Haga clic en las áreas resaltadas para obtener más información sobre las instalaciones SSL VPN basadas en cliente.

Empleado en su hogar

Los teletrabajadores requieren acceso completo y consistente a los recursos y aplicaciones de la red corporativa.

Empleado móvil

Los usuarios de acceso remoto requieren un acceso simple y transparente a los recursos de la red corporativa.

Establecer una sesión SSL involucra los siguientes pasos:

Paso 1. El usuario ejecuta una conexión saliente con el puerto TCP 443.

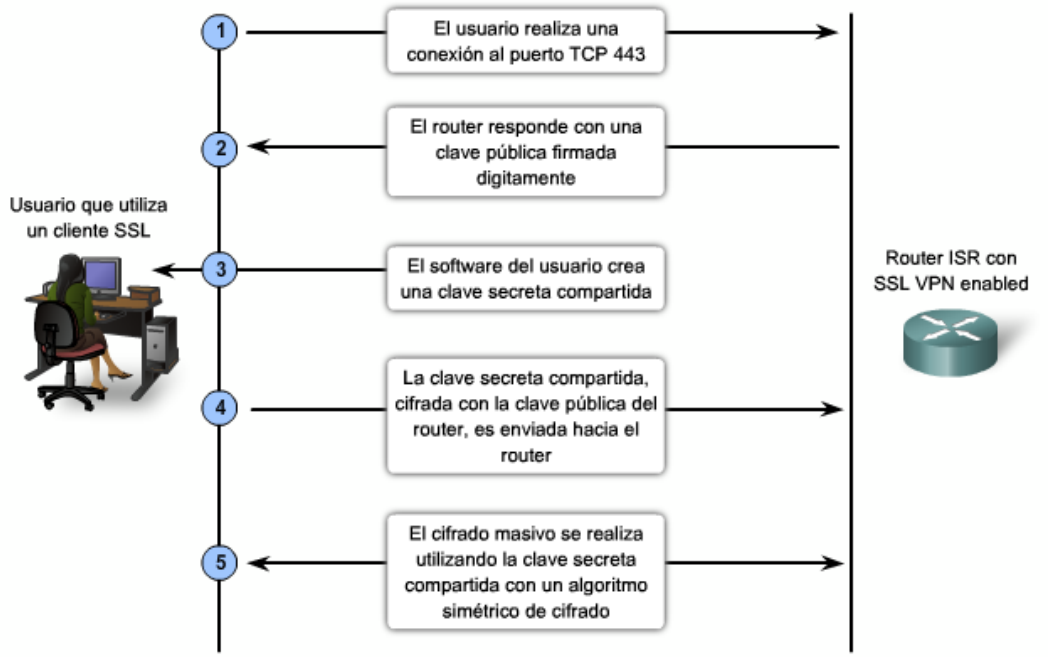
Paso 2. El router responde con un certificado digital que contiene una clave pública firmada digitalmente por una CA (Certificate Authority) confiable.

Paso 3. La computadora del usuario genera una clave secreta compartida que usan ambos participantes.

Paso 4. La clave compartida es cifrada con la clave pública del router y es transmitida hacia el router. El software del router es capaz de descifrar el paquete utilizando su clave privada. Ahora ambos participantes de la sesión conocen la clave secreta compartida.

Paso 5. La clave es utilizada para cifrar la sesión SSL.

SSL utiliza algoritmos de cifrado con claves de longitud entre 40 y 128 bits.



Antes de la implementación de los servicios de VPN SSL en routers con Cisco IOS, debe analizarse el ambiente actual para determinar qué características y modos pueden resultar útiles en la implementación.

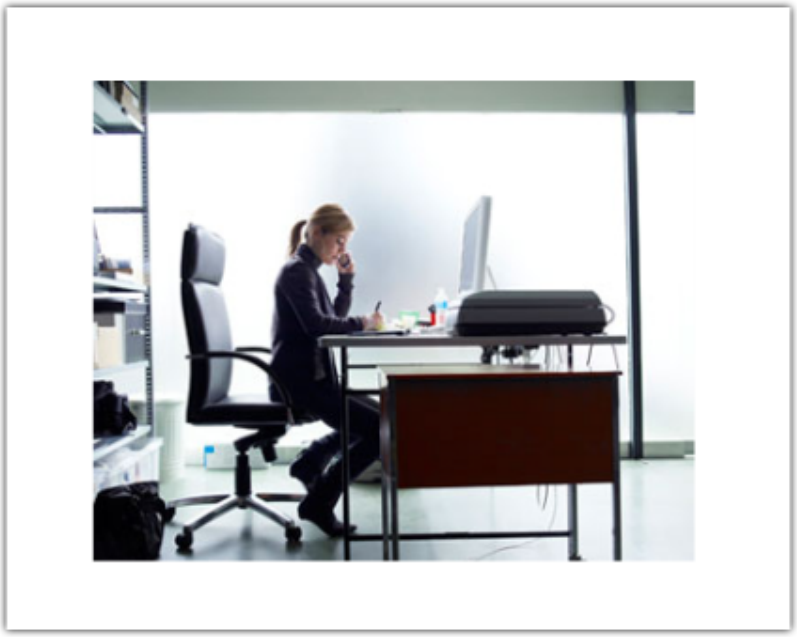
Existen varias consideraciones de diseño para una VPN SSL:

Conectividad de los usuarios - Determinar si los usuarios se conectan a la red corporativa desde computadores compartidas, tales como las de una biblioteca o local de Internet. En este caso, utilizar el modo de VPN SSL sin cliente.
Características del router - Un router con Cisco IOS puede ejecutar diferentes características, tales como túneles VPN IPsec, motores de enrutamiento y procesos de firewall. Habilitar la funcionalidad de VPN SSL puede agregar una carga de procesamiento importante si el router ya se encuentra ejecutando varias de estas otras funciones.

Hardware del router - El proceso VPN SSL consume recursos de CPU y memoria en forma intensiva. Antes de implementar una VPN SSL en un router con Cisco IOS, debe asegurarse de balancear los motores VPN SSL acelerados por hardware, tales como AIM-VPN/SSL-1, AIM-VPN/SSL-2 y AIM-VPN/SSL-3. Ingrese a www.cisco.com para más información sobre los módulos de hardware para VPN SSL.
Planificación de la infraestructura - Es importante considerar la ubicación de los dispositivos terminales de la VPN. Antes de implementar una VPN SSL en un Cisco IOS, hágase preguntas como: ¿Debe ubicarse la VPN SSL detrás del firewall? Si así fuera, ¿qué puertos deben estar abiertos? ¿Es necesario que el tráfico cifrado atraviese otro conjunto de firewalls? Si así fuera, ¿qué puertos deben abrirse?

Alcance de la implementación - Los administradores de seguridad de la red necesitan determinar el tamaño de la implementación de la VPN SSL, especialmente la cantidad de usuarios que podrán conectarse en simultáneo para obtener acceso a la red. Si un router Cisco no fuera suficiente para soportar los requisitos de los usuarios, deben considerarse balanceadores de carga o esquemas de clústeres de servidores, para acomodar a todos los usuarios remotos potenciales.

Las VPNs SSL son opciones viables para muchas organizaciones. Sin embargo, la configuración de las VPNs SSL se encuentra fuera del alcance de este curso. Visite www.cisco.com para conocer más sobre los comandos de configuración necesarios para implementar VPNs SSL y descargar las guías de referencia.



8.6.4 Cisco Easy VPN

Mientras que las VPNs SSL resultan útiles en muchos casos, muchas aplicaciones requieren la seguridad de una conexión VPN IPsec para su autenticación y para cifrar datos. Establecer una conexión entre dos sitios puede ser complicado y en general requiere coordinación entre los administradores de red en cada extremo para configurar los parámetros de la VPN. Cuando se despliegan VPNs para teletrabajadores y pequeñas sucursales, la facilidad de implementación es crítica si los recursos técnicos no se encuentran disponibles para configurar la VPN en el extremo remoto.

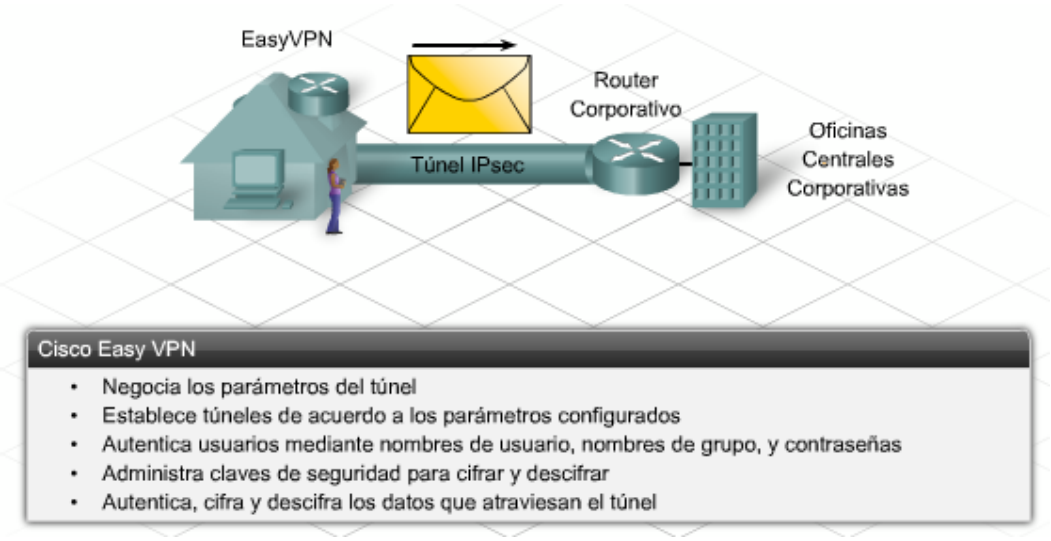
La solución Cisco Easy VPN ofrece flexibilidad, escalabilidad y facilidad de uso para VPNs de sitio a sitio y de acceso remoto. Consiste de tres componentes:

Cisco Easy VPN Server - Un router Cisco IOS o un equipo Cisco PIX / ASA Firewall, funcionando como el dispositivo cabecera de la VPN de acceso remoto o sitio a sitio.
Cisco Easy VPN Remote - Un router Cisco IOS o un equipo Cisco PIX / ASA Firewall, funcionando como cliente VPN remoto.

Cisco Easy VPN Client - Una aplicación soportada por una PC, utilizada para acceder al servidor Cisco VPN.

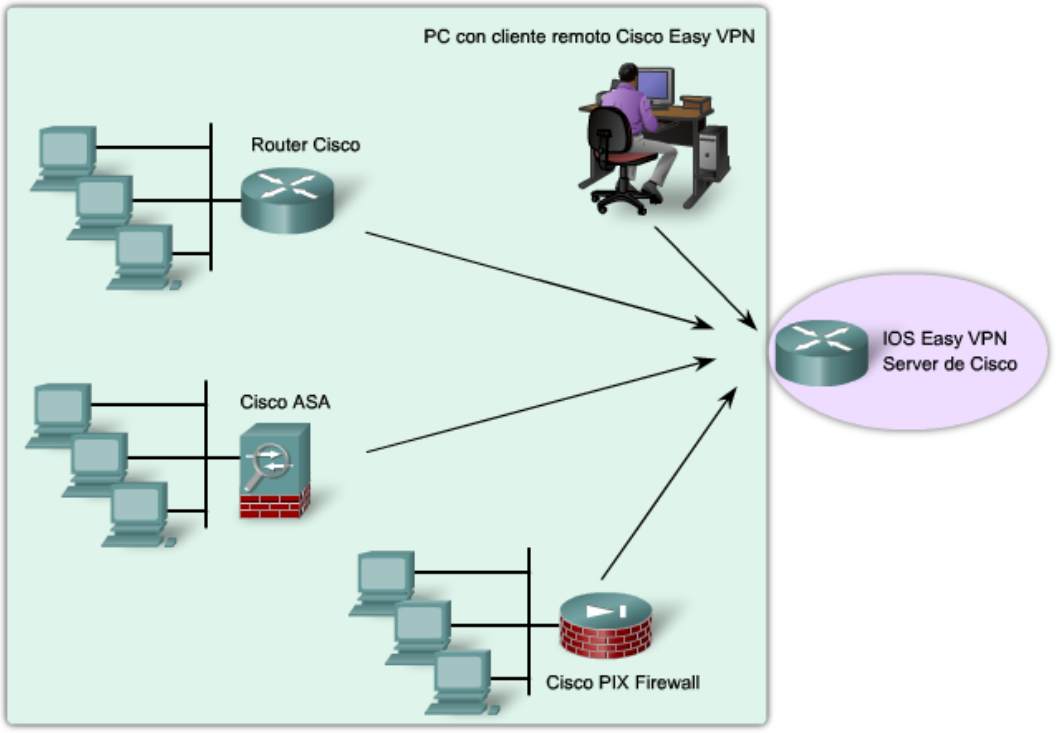
La mayor parte de los parámetros de la VPN se definen en el Cisco IOS Easy VPN Server para simplificar la implementación. Cuando un cliente remoto inicia una conexión de túnel VPN, el Cisco Easy VPN Server envía las políticas IPsec al cliente y crea la conexión de túnel VPN IPsec correspondiente.

Los dispositivos remotos pueden ser trabajadores móviles ejecutando el cliente Cisco Easy VPN en PCs para establecer fácilmente conexiones VPN con el dispositivo Cisco Easy VPN Server a través de Internet. También puede ser un dispositivo Cisco ejecutando la funcionalidad Cisco Easy VPN Remote, la cual le permite ser un cliente del Easy VPN Server. Esto quiere decir que los individuos en pequeñas sucursales no necesitan ejecutar el software cliente de la VPN en sus PCs.



El Cisco Easy VPN Server hace posible que los trabajadores remotos que utilizan clientes VPN en sus PCs puedan crear túneles IPsec seguros para acceder a la intranet de sus oficinas centrales, donde se almacenan datos y aplicaciones críticas. Permite a los routers Cisco IOS y firewalls Cisco PIX y ASA funcionar como cabeceras VPN en VPNs de acceso remoto y de sitio a sitio. Los dispositivos de las oficinas remotas utilizan la funcionalidad Cisco Easy VPN Remote o la aplicación Cisco VPN Client para conectarse al servidor, el cual luego envía las políticas de seguridad definidas hacia los dispositivos VPN remotos. Esto asegura que dichas conexiones utilicen políticas actualizadas desde el momento en que se establecen las conexiones.

Cisco Easy VPN Remote permite que los routers Cisco IOS, firewalls Cisco PIX, clientes Cisco VPN 3002 o clientes de software, actúen como clientes remotos VPN. Estos dispositivos pueden recibir políticas de seguridad desde un Cisco Easy VPN Server, minimizando los requisitos de configuración en los dispositivos remotos. Esta solución de bajo costo es ideal para oficinas remotas con poco soporte IT o para grandes instalaciones con equipamiento local de clientes, donde no resulta práctico configurar los dispositivos remotos en forma individual.



Cuando un cliente se conecta a un servidor, toma lugar la negociación para asegurar la VPN:

1. El cliente VPN inicia el proceso de fase 1 IKE. Si se utiliza una clave pre-compartida para la autenticación, el cliente VPN inicia el modo agresivo. Si se utilizan certificados digitales para la autenticación, el cliente VPN inicia el modo principal.

2. El cliente VPN establece una SA ISAKMP. Para reducir la configuración manual en el cliente VPN, las propuestas ISAKMP de Easy VPN incluyen todas las combinaciones de algoritmos de cifrado y hash, métodos de autenticación y tamaños de grupos DH.

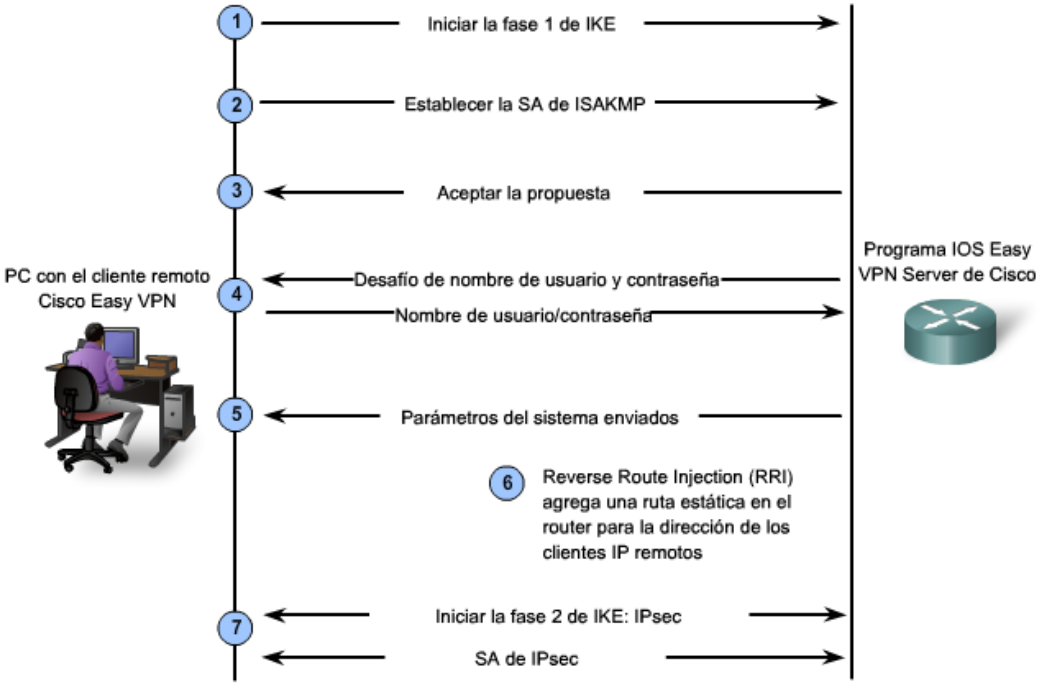
3. Easy VPN Server acepta la propuesta de SA. La política ISAKMP puede consistir de diferentes propuestas, pero el Easy VPN Server utiliza la primera coincidencia, por lo tanto siempre deben configurarse primero las políticas más seguras. En este punto, finaliza la autenticación de los dispositivos y comienza la autenticación del usuario.

4. Easy VPN Server inicia el desafío de nombre de usuario y contraseña. La información ingresada se verifica contra las entidades de autenticación utilizando protocolos AAA (Autenticación, autorización y registro de auditoría - Authentication, Authorization and Accounting) tales como RADIUS y TACACS+. También pueden utilizarse tokens a través del proxy AAA. Los dispositivos VPN configurados para controlar a los clientes VPN remotos siempre deben asegurar la autenticación de los usuarios.

5. Se inicia el proceso de configuración de modo. Los restantes parámetros del sistema (dirección IP, DNS, atributos de división de túnel y demás) son enviados al cliente VPN en este punto.

6. Se inicia el proceso Reverse Route Injection (RRI). RRI asegura la creación de una ruta estática en el Cisco Easy VPN Server para el direccionamiento IP interno de cada cliente VPN.

7. El modo rápido IPsec completa la conexión. La conexión se completa una vez que se crearon las SAs IPsec.



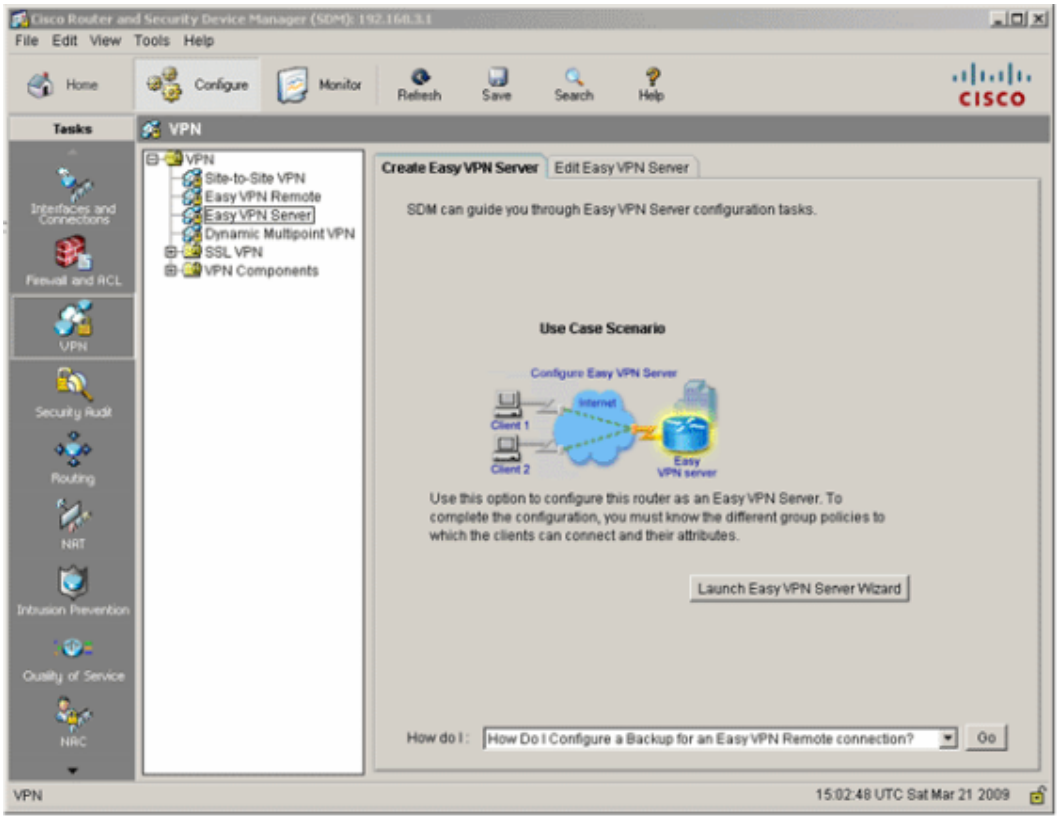
8.6.5 Configuracion de un servidor VPN con SDM

Configurar la funcionalidad Cisco Easy VPN Server utilizando SDM consiste en dos tareas principales:

Tarea 1. Configurar los prerrequisitos, tales como AAA, privilegios de usuario y la contraseña secreta de modo enable, en base al diseño de VPN elegido.

Tarea 2. Configurar el Cisco Easy VPN Server.

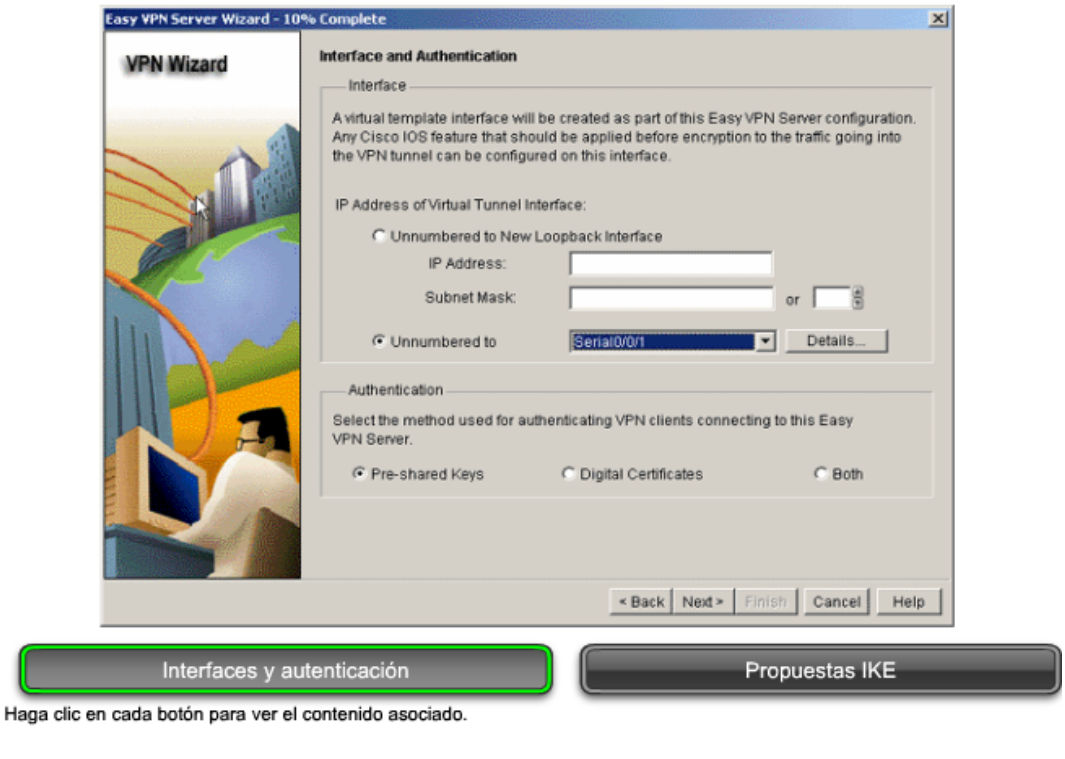
Desde la página principal del SDM, seleccione el botón Configure, luego haga clic sobre el botón VPN Task y seleccione la opción Easy VPN Server. Si no se ha configurado previamente AAA, el asistente solicitará configurarlo. Si AAA se encuentra deshabilitado en el router, configure AAA antes de iniciar la configuración de Easy VPN Server y cree al menos un usuario administrador.



Luego de lanzar el asistente del Easy VPN Server, se muestra la ventana Interface and Authentication. Especifique la interfaz del router donde terminará la conexión VPN (por ejemplo, Serial 0/0/1) y el método de autenticación (por ejemplo, claves pre-compartidas o certificados digitales).

Haga clic sobre Next para mostrar la ventana Ike Proposals. Al configurar las propuestas IKE, utilizar la política por defecto definida por el SDM o agregar una política IKE personalizada, especificando estos parámetros requeridos:

Prioridad de la política IKE
Autenticación (PRE-SHARE or RSA-SIG)
Grupo D-H (1, 2 o 5)
Algoritmo de cifrado (DES, 3DES o AES)
Hash (SHA-1 o MD5)
Tiempo de vida IKE

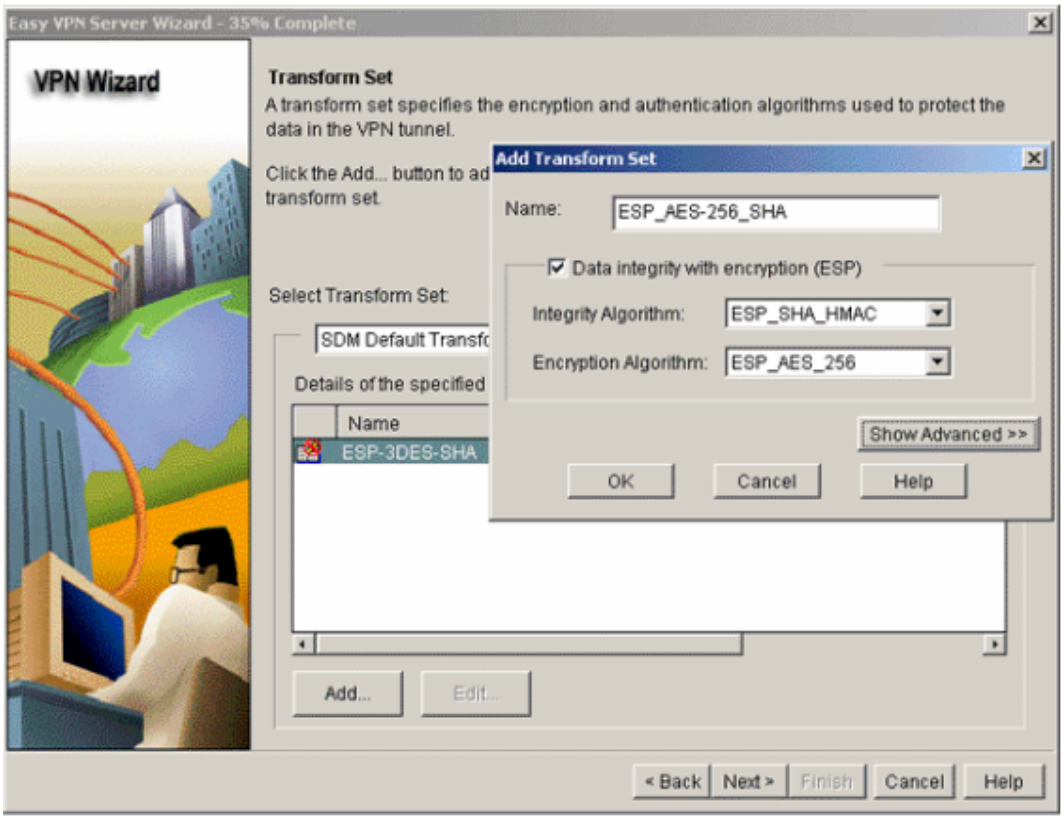




Cisco SDM proporciona un conjunto de transformación por defecto. Utilice este conjunto por defecto o cree un nuevo conjunto de transformación IPsec utilizando estos parámetros:

Nombre del conjunto de transformación
Algoritmo de cifrado (DES, 3DES, AES o SEAL)
HMAC (SHA-1 o MD5)

Compresión opcional
Modo de operación (túnel o transporte)



La ventana de Group Authorization and Group Policy Lookup se presenta a continuación. Existen tres opciones donde almacenar las políticas de grupo VPN:

Local - Todos los grupos se encuentran en la configuración del router, en su NVRAM.
RADIUS - El router utiliza el servidor RADIUS para autorización de grupos.
RADIUS y Local - El router puede examinar las políticas almacenadas en la base de datos del servidor AAA, el cual puede alcanzarse mediante RADIUS.

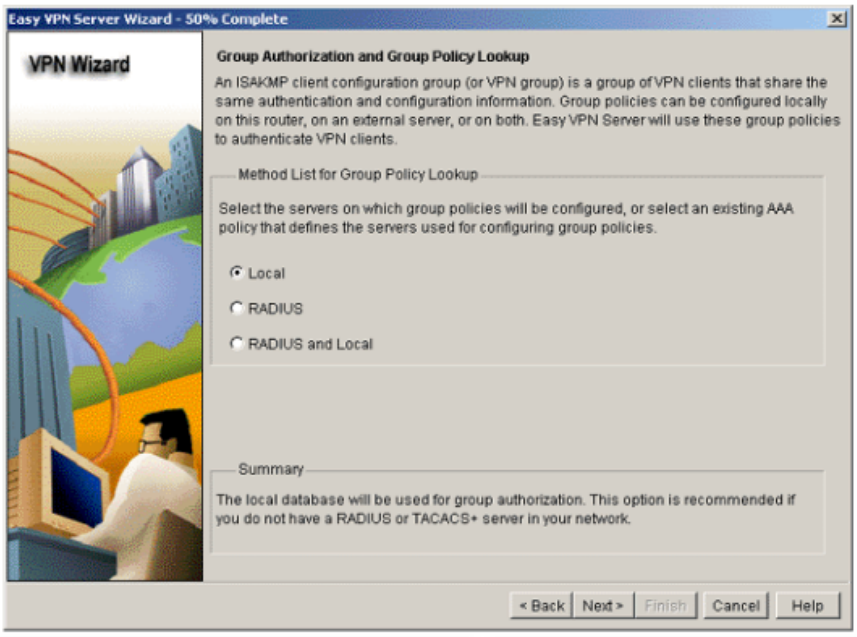
Haga clic sobre Next para configurar los parámetros del grupo de autorización. Seleccione el botón Add para agregar una nueva política de grupo. La pestaña General permite la configuración de los siguientes parámetros:

Nombre del grupo
Claves pre-compartidas
Información del pool de direcciones IP
Número máximo de conexiones permitidas

Otras pestañas se refieren a las siguientes opciones:

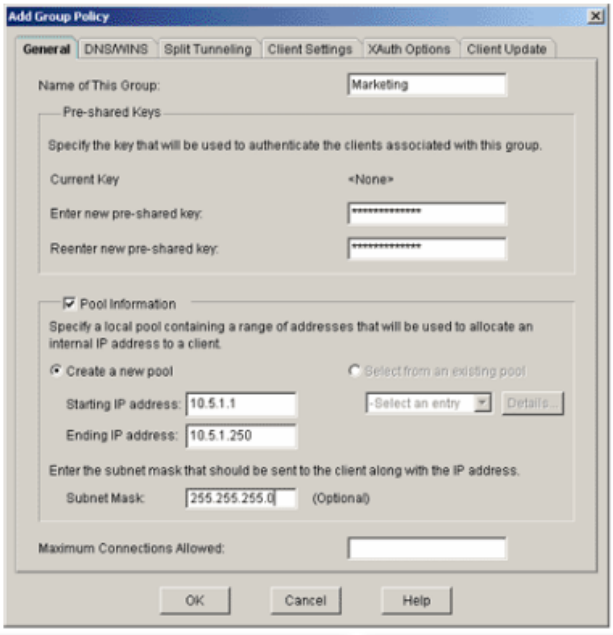
DNS/WINS
Split Tunneling
Client Settings

XAuth Options
Client Update



Búsqueda de autorización de grupo | Agregar política de grupo

Haga clic en cada botón para ver el contenido asociado.

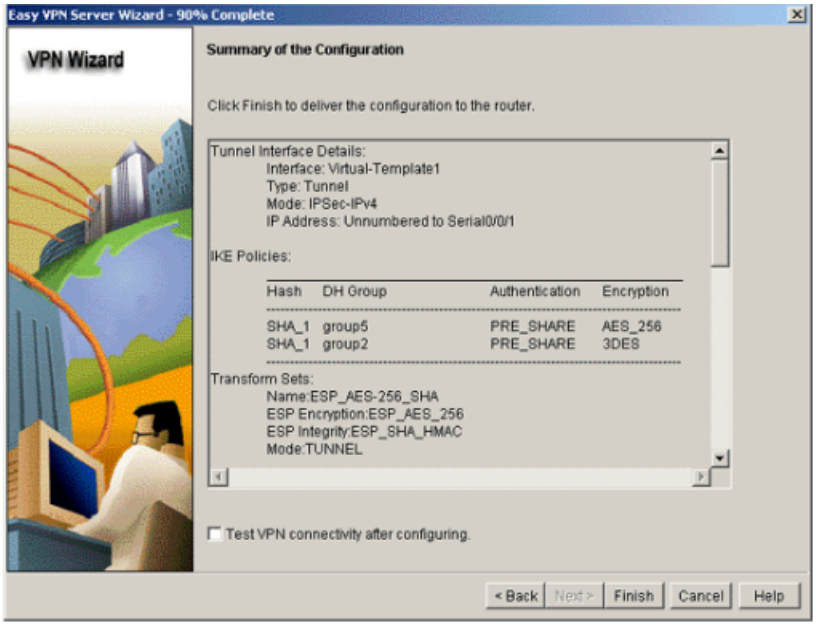


Búsqueda de autorización de grupo | Agregar política de grupo

Haga clic en cada botón para ver el contenido asociado.

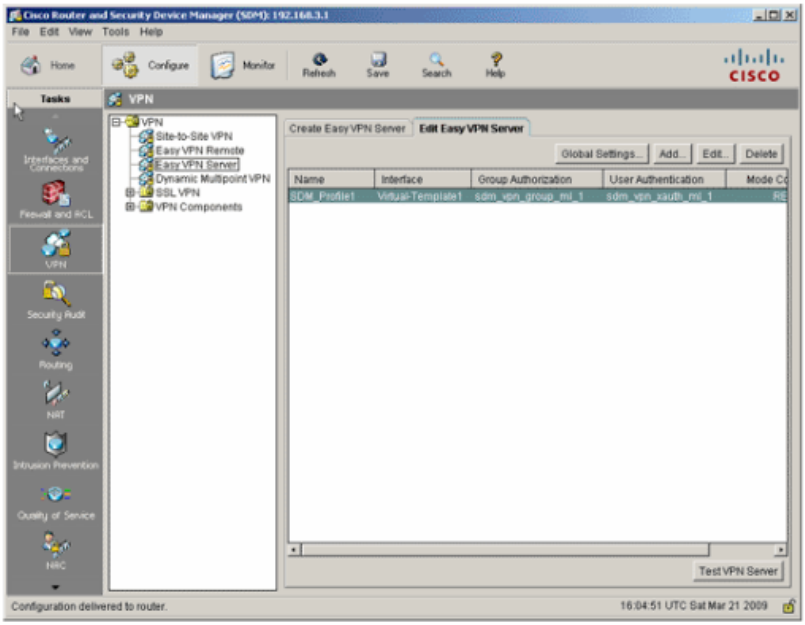
Una vez completados todos los pasos, el asistente de Easy VPN Server presenta un resumen con los parámetros configurados. Haga clic sobre Back para corregir cualquier error en la configuración. En caso contrario, seleccione Finish para aplicar la configuración al router.

La configuración de Easy VPN Server puede luego ser verificada. Ejecute una prueba para confirmar la configuración correcta del túnel, seleccionando el botón Test VPN Server al final de la página Edit Easy VPN Server. De esta forma se accede a la ventana de resolución de problemas de VPN, la cual muestra los resultados de validación de la VPN.



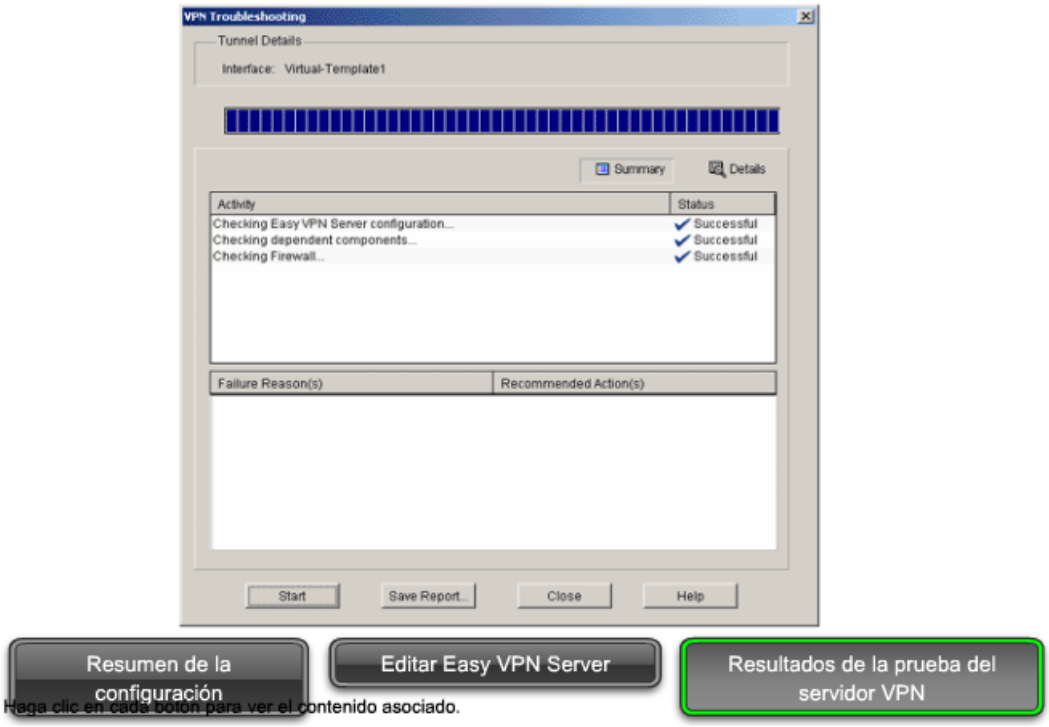
Resumen de la configuración | Editar Easy VPN Server | Resultados de la prueba del servidor VPN

Haga clic en cada botón para ver el contenido asociado.



Resumen de la configuración | Editar Easy VPN Server | Resultados de la prueba del servidor VPN

Haga clic en cada botón para ver el contenido asociado.

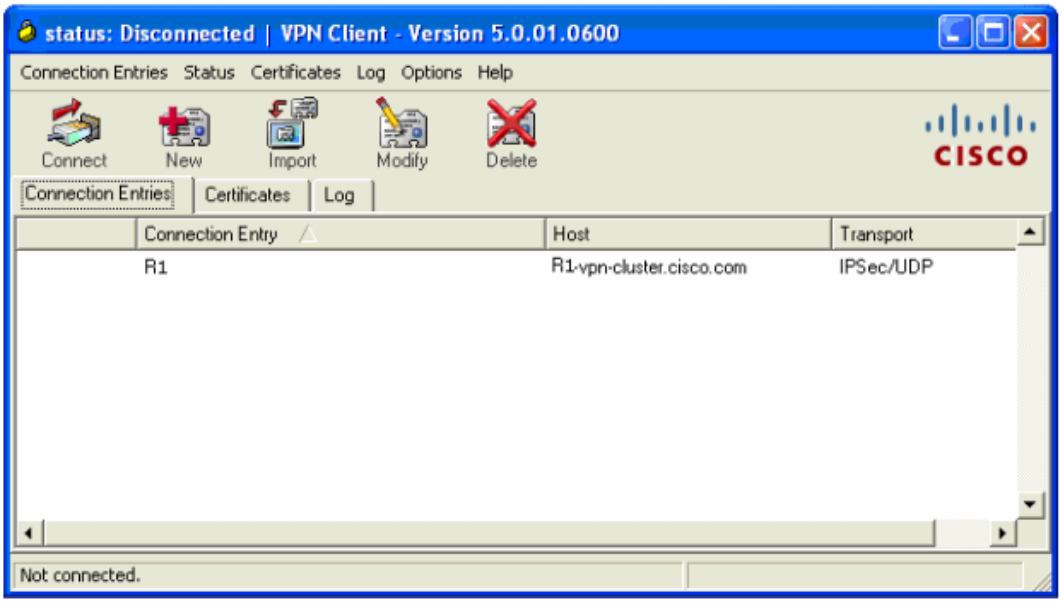


8.6.6 Conectarse con un cliente VPN

Cisco VPN Client es de simple instalación y operación. Permite a las organizaciones establecer túneles cifrados de extremo a extremo, para una conectividad segura con empleados móviles o trabajadores a distancia. Esta implementación liviana de IPsec es compatible con todos los productos Cisco VPN.

Cuando se lo configura para una implementación masiva, la identificación inicial requiere la intervención del usuario. Cisco VPN Client soporta las novedosas capacidades de Cisco Easy VPN, entregando una arquitectura VPN de acceso remoto escalable, rentable y fácil de administrar, la cual elimina los costos operativos asociados al mantenimiento de políticas consistentes y métodos de administración de claves.

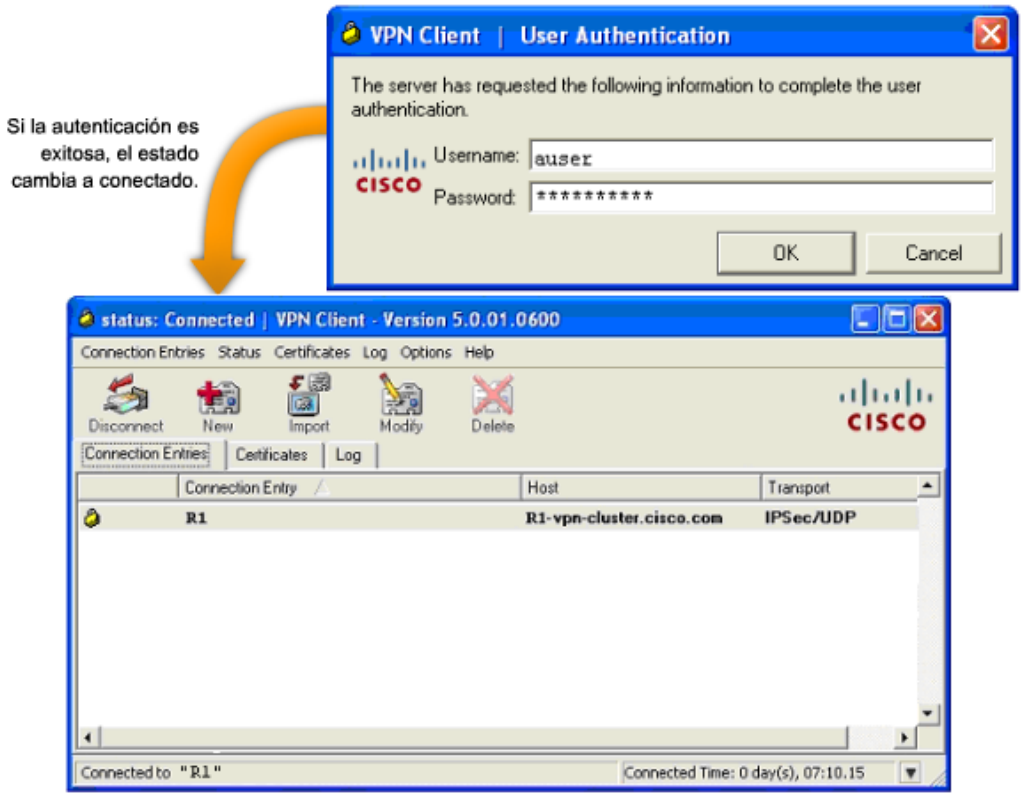
Cisco Easy VPN permite que Cisco VPN Client reciba políticas de seguridad para una conexión de túnel VPN directamente desde el dispositivo VPN central (Cisco Easy VPN Server), minimizando los requisitos de configuración en el extremo remoto. Esta solución simple y escalable resulta ideal para implementaciones grandes de acceso remoto, donde no resulta práctico configurar políticas individuales para múltiples PCs remotas.



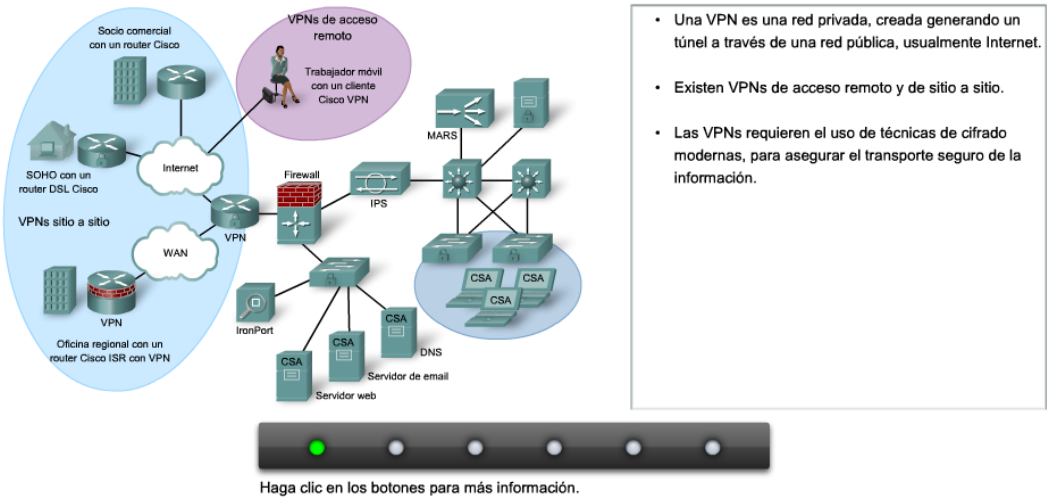
Al instalar Cisco Easy VPN, abra la ventana del cliente Cisco Easy VPN para iniciar la conexión VPN IPsec en una PC.

La aplicación lista los sitios pre-configurados disponibles. Haga doble clic sobre un sitio. En el cuadro de diálogo de autenticación del usuario, ingrese los datos para la autenticación con el sitio. Una vez autenticado, el cliente Cisco Easy VPN Client muestra el estado conectado.

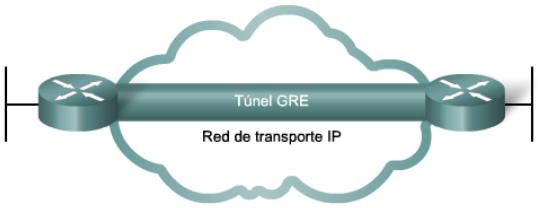
La configuración del cliente Easy VPN sobrepasa el alcance de este curso. Ingrese a www.cisco.com para más información.



8.7.1 Resumen del capitulo



- Generic Routing Encapsulation (GRE) es un protocolo de tunneling utilizado para crear enlaces punto a punto entre routers Cisco.
- GRE soporta tunneling multiprotocolo, incluyendo IP.
- GRE puede ser utilizado en combinación con IPsec.

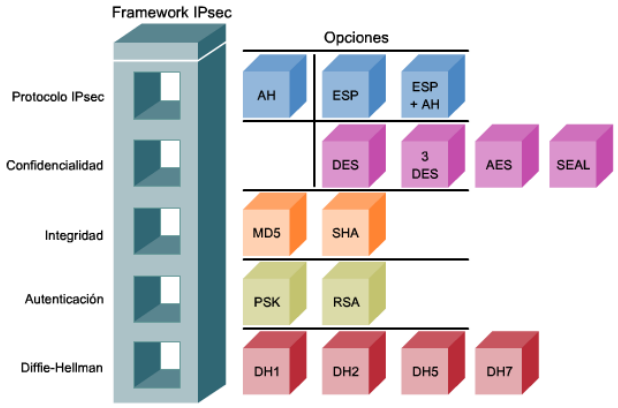


Protocolo de túnel GRE

- Encapsula una amplia variedad de protocolos dentro de túneles IP.
- Crea un enlace virtual punto apunto entre routers Cisco ubicados en puntos remotos de una red IP.
- Utiliza IP para el transporte.
- Utiliza un encabezado adicional para soportar multicasting IP y cualquier otro protocolo de Capa 3 del modelo OSI.



Haga clic en los botones para más información.



- IPsec es un framework de estándares abiertos que establece las reglas para las comunicaciones seguras.
- IPsec se apoya en algoritmos existentes para obtener cifrado, autenticación, e intercambio de claves.
- IPsec puede encapsular un paquete utilizando Authentication Header (AH) o Encapsulation Security Protocol (ESP), el cual es más seguro.
- IPsec utiliza el protocolo Internet Key Exchange (IKE) para establecer el proceso de intercambio de claves.



Haga clic en los botones para más información.

- La primera tarea en la creación de una VPN de sitio a sitio es asegurar que las ACLs en los routers perimetrales, firewalls u otros routers, no bloqueen el tráfico IPsec.
- La segunda tarea es definir los parámetros de la política IKE, la cual es utilizada durante la negociación para establecer los pares ISAKMP.
- La tercera tarea es definir un conjunto de transformación IPsec, el cual consiste en una combinación de una transformación AH, una transformación ESP y el modo IPsec.
- La cuarta tarea consiste en configurar la crypto ACL para definir qué tráfico es protegido a través del túnel IPsec.



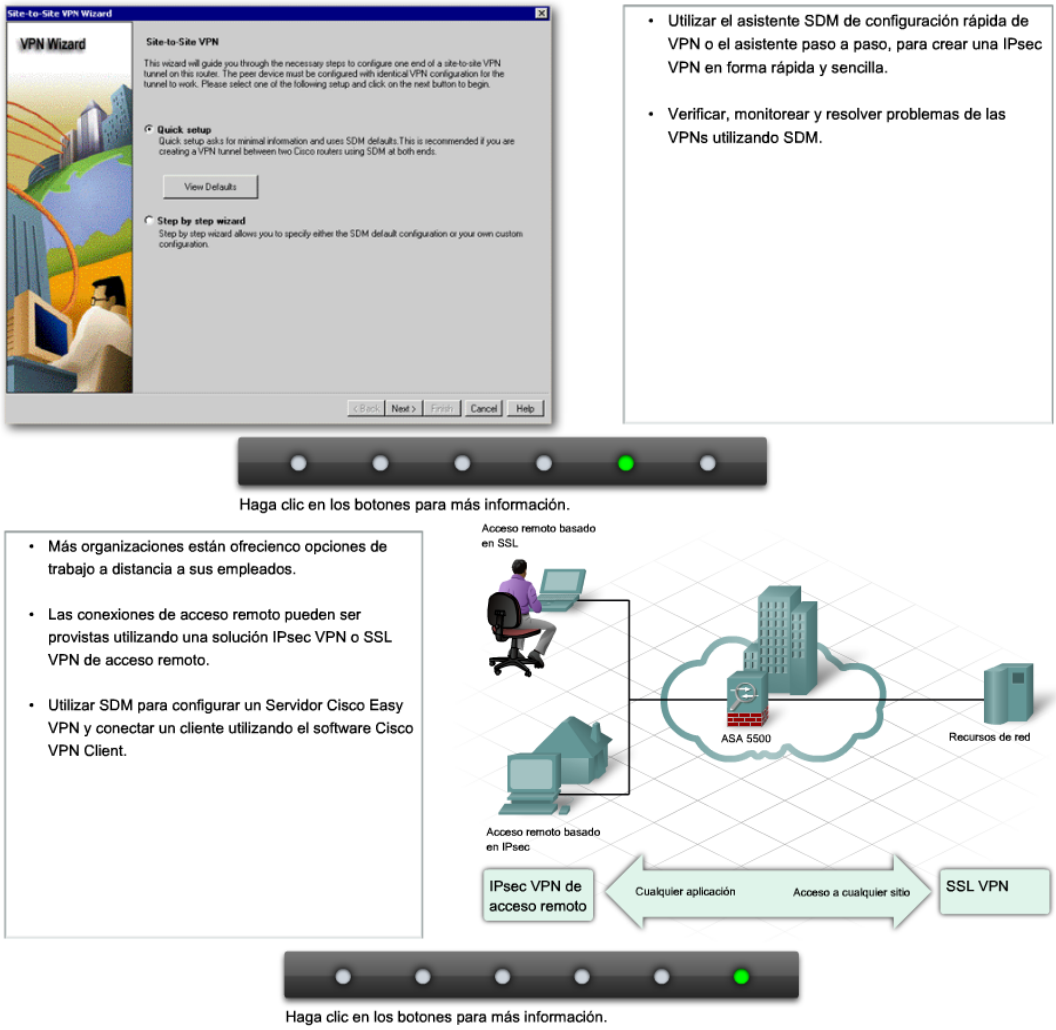
Los crypto-maps definen lo siguiente:

- ACL a utilizar
- Pares VPN remotos
- Conjunto de transformación a utilizar
- Método de administración de claves
- Tiempos de vida de SA





Haga clic en los botones para más información.



9 Administración de una red segura

9.0 Introducción al capitulo

9.0.1 Introducción al capitulo

La mitigación de ataques de red requiere un enfoque englobador de extremo a extremo, que incluya la creación y el mantenimiento de políticas de seguridad basadas en las necesidades de seguridad de la organización. El primer paso al establecer las necesidades de seguridad de una empresa es identificar amenazas probables y realizar un análisis de riesgo, cuyos resultados se usan para establecer las implementaciones de seguridad de hardware y software, las políticas de mitigación y el diseño de la red.

Para ayudar a simplificar el diseño de la red, se recomienda que todos los mecanismos de seguridad provengan del mismo proveedor. La Red Autodefensiva de Cisco (Cisco Self-Defending Network - SDN) es una solución de seguridad en redes englobadora y de extremo a extremo. El Administrador de Seguridad de Cisco y el MARS de Cisco proporcionan opciones de administración de red para soluciones SDN de Cisco.

Una vez diseñada la red, la seguridad de las operaciones implica las prácticas diarias necesarias para desplegar y mantener el sistema de seguridad. Parte de mantener un

sistema de seguridad es probarlo. El equipo de operaciones lleva a cabo las pruebas de seguridad para asegurar que las implementaciones de seguridad estén operando correctamente. Las pruebas también se utilizan para profundizar en el planeamiento de la continuidad de los negocios, que trata la continuidad de las operaciones de la empresa si ocurre un desastre o una interrupción prolongada en el servicio.

Luego de que se implementa una red segura y se establecen los planes de continuidad, deben actualizarse continuamente esos planes y documentos basándose en las cambiantes necesidades de la empresa. Por esta razón, es necesario comprender el ciclo de vida de desarrollo del sistema (system development life cycle - SDLC) para evaluar los cambios en el sistema y ajustar las implementaciones de seguridad. El SDLC comprende cinco fases: iniciación, adquisición y desarrollo, implementación, operaciones y mantenimiento y descarte. Es importante incluir las consideraciones de seguridad en todas las fases del SDLC.

Un sistema de seguridad en la red no puede prevenir completamente que los activos sean vulnerables a amenazas. Constantemente se desarrollan nuevos ataques y se identifican vulnerabilidades que pueden ser usadas para sortear las soluciones de seguridad. Además, los sistemas de seguridad técnicos, administrativos y físicos pueden ser vencidos si la comunidad de usuarios finales no se atiene a las prácticas y procedimientos de seguridad. Debe mantenerse una política de seguridad englobadora que identifique los activos de la empresa, especifique los requisitos de hardware y software para la protección de esos activos, clarifique los roles y responsabilidades del personal y estableza el procedimiento protocolar apropiado para responder a brechas de seguridad. Al establecer y seguir políticas de seguridad, las empresas pueden minimizar las pérdidas y daños que resultan de ataques a su red.

En una englobadora práctica de laboratorio , Desarrollo e implementación de políticas de seguridad, los alumnos crean una política de seguridad básica, refuerzan los routers de la red y configuran las opciones de acceso y autenticación remotos, NTP y registros, un firewall CBAC, un firewall ZPF, IPS usando la CLI y SDM, además de hacer copias de resguardo de las imágenes del router y los archivos de configuración, reforzar los switches de la red, configurar las opciones de acceso y autenticación remotos, mitigar ataques STP y configurar y probar VPNs IPsec de acceso remoto. La práctica está disponible en el manual de laboratorio en Academy connection en cisco.netacad.net.

La actividad de Packet Tracer, Configuración de una red para su operación segura, proporciona a los alumnos práctica adicional en la implementación de las tecnologías presentadas en este último capítulo. Los alumnos aseguran el router con contraseñas fuertes y cifrado de contraseñas, aseguran la consola y las líneas VTY, configuran banners de inicio de sesión, autenticación AAA local, SSH, syslog y NTP y refuerzan los routers de la red, además de configurar CBAC y ZPF y asegurar los switches de red. Las actividades de Packet Tracer para CCNA Security están disponibles en Academy Connection en cisco.netacad.net.

En este capítulo, aprenderá a:

- Describir los principios de un diseño de red seguro.
- Describir la identificación de amenazas y el análisis de riesgos.
- Describir la gestión y la evasión de riesgos.
- Describir las Redes Autodefensivas de Cisco.
- Describir la Suite de Manejo de Seguridad de Cisco y el Portfolio de Seguridad Integrado de Cisco.
- Describir la seguridad de las operaciones.
- Describir las herramientas y técnicas de pruebas de seguridad en la red.
- Describir la continuidad de los negocios y recuperación de desastres.
- Describir el concepto de ciclo de vida de desarrollo del sistema y su aplicación a un ciclo de vida de red segura.
- Describir el propósito y el funcionamiento de una política de seguridad en red.

9.1 Principios de un diseño de red seguro

9.1.1 Asegurarse de que la red sea segura

La mitigación de ataques de red requiere un enfoque englobador y de extremo a extremo:

Asegure los dispositivos con AAA, SSH, CLI basada en roles, syslog, SNMP y NTP.
Asegure los servicios con AutoSecure y one-step lockdown.
Proteja los extremos de la red, como estaciones de trabajo y servidores, contra virus, troyanos y gusanos con Cisco NAC, Cisco IronPort y Agente de Seguridad de Cisco.
Use el firewall IOS de Cisco y ACLs para asegurar los recursos internamente y protegerlos de ataques externos.
Agregue al firewall IOS de Cisco la tecnología IPS de Cisco para evaluar el tráfico con una base de datos de firmas de ataques.
Proteja la LAN siguiendo las prácticas recomendadas de capa 2 y VLAN y usando una variedad de tecnologías que incluye BPDU guard, root guard, PortFast y SPAN.

A pesar de estas técnicas de seguridad, los hackers están siempre desarrollando nuevas formas de atacar a las redes. Una parte importante de la implementación de una red segura es la creación y el mantenimiento de políticas de seguridad para mitigar tipos de ataques existentes y nuevos. Estas políticas aplican un enfoque estructurado, informado y consistente para la seguridad de las redes. Al desarrollar políticas de seguridad, deben contestarse varias preguntas:

Necesidades de negocios - ¿Qué espera hacer la empresa con la red? ¿Cuáles son las necesidades de la empresa? Sin importar las implicancias de seguridad, las necesidades de los negocios deben ser lo primero.
Identificación de amenazas - ¿Qué tipos de amenazas son más probables dado el propósito de la empresa? Por ejemplo, una institución financiera tendrá amenazas diferentes que una universidad.
Análisis de riesgos - ¿Cuál es el análisis de costo contra beneficio de la implementación de las tecnologías de seguridad? ¿Cómo afectan las últimas técnicas de seguridad al entorno de la red y cuál es el riesgo de no implementarlas?
Necesidades de seguridad - ¿Cuáles son las políticas, los estándares y las recomendaciones necesarias para satisfacer las necesidades y contrarrestar los riesgos de la empresa?
Prácticas recomendadas por la industria - ¿Cuáles son las prácticas de seguridad confiables, bien entendidas y recomendadas que emplean empresas similares?

Operaciones de seguridad - ¿Cuáles son los procedimientos actuales para respuesta a incidentes, monitoreo, mantenimiento y auditoría del sistema implementados para cumplir con las normas?



Cuando se diseña e implementa una red segura, se asumen muchas cuestiones de seguridad. Desafortunadamente, asumir sin fundamentos cómo y dónde se usará el sistema puede llevar a mecanismos de seguridad rotos, mal configurados o violados. Una suposición mal hecha puede ser que más usuarios necesitan usar un protocolo, como FTP, que los que realmente lo usan.

Una suposición equivocada tiene ramificaciones negativas en todo el trabajo de diseño. Puede influenciar una decisión de diseño y luego propagarse a otras decisiones que dependen de ella. Las decisiones equivocadas son especialmente peligrosas en etapas tempranas del diseño de un sistema seguro cuando se modelan las amenazas y se estiman los riesgos. Generalmente es fácil corregir o mejorar un solo aspecto de la implementación de un sistema, como una configuración de firewall. Sin embargo, los errores de diseño, como la ubicación del firewall, son extremadamente difíciles o imposibles de corregir sin invertir importantes cantidades de tiempo y tecnología.

Hay algunos consejos que pueden ayudarlo a evitar realizar suposiciones erróneas:

Tenga en consideración que cualquier aspecto del sistema de seguridad puede fallar. Cuando diseña un sistema, analice, para cada elemento, qué pasaría si fallara, estime la probabilidad de que falle y analice todas las posibles consecuencias, tomando en cuenta los fallos en cascada de otros elementos.
Identifique los elementos que hagan fail-open. El fail-open ocurre cuando una falla inhabilita la función de seguridad. Idealmente, los elementos de seguridad deberían ser a prueba de fallas, es decir que, si el elemento falla, debería volver por defecto a un estado seguro, como el bloqueo de todo el tráfico.

Intente identificar todas las posibilidades de ataque. Una manera de lograr esto es con un análisis de arriba abajo de los posibles fallos del sistema, lo cual involucra una evaluación de la simplicidad y probabilidad de cada ataque al sistema. Este tipo de análisis se denomina comúnmente análisis de árbol de ataques.
Evalúe la posibilidad de explotación. Concéntrese en los recursos necesarios para crear un ataque, no en la obscuridad de una vulnerabilidad particular. Asegúrese de tomar en cuenta avances tecnológicos.
Asuma que la gente se equivoca. Por ejemplo, los usuarios pueden usar el sistema de manera inapropiada, lo cual puede comprometer su seguridad involuntariamente.
Los atacantes pueden no usar técnicas comunes y bien establecidas para comprometer el sistema. En cambio, pueden estresar el sistema con ataques aparentemente aleatorios en búsqueda de información sobre cómo se comporta el sistema en condiciones inesperadas.
Controle todas sus suposiciones con otras personas, ya que pueden ofrecer una perspectiva diferente sobre las amenazas potenciales y su probabilidad. Cuanta más gente cuestione las suposiciones, es más probable que se logre identificar aquellas erróneas.

MAS INFORMACION
El cifrado de películas DVD, que utiliza un algoritmo débil llamado Content Scrambling System (CSS), es un ejemplo de suposiciones mal hechas sobre el alcance de uso del sistema. La suposición original era que los discos DVD serían usados solo en reproductores de hardware, donde las claves de deschifrado podían ser almacenadas en un chip resistente a manipulaciones dentro del reproductor, lo cual haría difícil comprometer los DVD hasta para los atacantes más habilidosos. Sin embargo, cuando aparecieron los reproductores DVD de sofware, rápidamente se aplicó ingeniería inversa en los discos DVD, ya que hacer que el software sea resistente a manipulaciones es casi imposible frente a un atacante determinado. Las claves fueron recuperadas de uno de los reproductores populares y se publicó un algoritmo en Internet junto con las claves.

La respuesta estratégica de la industria del DVD fue intentar censurar la publicación del algoritmo CSS y las claves, pero la decisión de la corte de que el código fuente del algoritmo CSS era esencialmente libertad de expresión detuvo muchos de sus esfuerzos.

Otro ejemplo de una suposición errónea o mal hecha fue la falta de cifrado del tráfico de celulares de Estados Unidos de América. Cuando los teléfonos celulares fueron presentador, la suposición fue que los escáners, que podían interceptar el tráfico de celulares, eran muy caros para montar cualquier ataque a gran escala contra la confidencialidad de las llamadas en las redes celulares. En un par de años, el precio de estos escáners se redujo al punto de que estaban disponibles para casi cualquiera. Por lo tanto, las suposiciones erróneas comprometieron la política de protección de la red celular.

El servicio de celular de siguiente generación usa transmisión digital, pero se realizó la misma suposición de que los escáneres digitales usados para interceptar tráfico eran demasiado caros. A medida que la tecnología avanza, la historia se ha repetido en las transmisiones digitales.

9.1.2 Identificación de amenazas y análisis de riesgos

Uno de los primeros pasos para establecer las necesidades de seguridad de una empresa es la identificación de amenazas posibles. La identificación de amenazas proporciona a la empresa una lista de amenazas a las que el sistema puede estar sujeto en un ambiente particular. Para identificar las amenazas, es importante hacerse preguntas:

¿Cuáles son las posibles vulnerabilidades del sistema?
¿Cuáles pueden ser las consecuencias si se explotan las vulnerabilidades del sistema?

Por ejemplo, la identificación de amenazas en la conexión de un sistema de e-banking podría incluir:

Compromiso interno del sistema - El atacante usa los servidores de e-banking expuestos para ingresar a un sistema interno del banco.
Robo de datos de los clientes - El atacante roba los datos personales y financieros de los clientes del banco de la base de datos de clientes.
Transacciones falsas de un servidor externo - El atacante altera el código de la aplicación de e-banking y ejecuta transacciones arbitrarias haciéndose pasar por un usuario legítimo.
Transacciones falsas con el PIN o la tarjeta inteligente de un cliente asaltado - El atacante roba la identidad del cliente y ejecuta transacciones maliciosas desde la cuenta comprometida.
Ataque interno al sistema - Un empleado del banco encuentra una falla en el sistema y monta un ataque.
Errores de ingreso de datos - El usuario ingresa datos incorrectos o efectúa solicitudes de transacción incorrectas.
Destrucción del centro de datos - Un evento cataclísmico daña importantemente o destruye el centro de datos.

La identificación de vulnerabilidades en una red implica entender las aplicaciones importantes utilizadas y las diferentes vulnerabilidades que tengan las aplicaciones y el hardware. Puede requerir un tiempo significativo de investigación por parte del administrador de la red

Amenazas identificadas



El análisis de riesgos es el estudio sistemático de las incertidumbres y los riesgos. Estima la probabilidad y severidad de las amenazas a un sistema y proporciona a la organización una lista de prioridades. Los analistas de riesgos identifican el riesgo, determinan cómo y cuándo puede aparecer y estiman el impacto (financiero u otros) de un resultado adverso.

El primer paso al desarrollar un análisis de riesgos es la evaluación de cada amenaza para determinar su severidad y probabilidad:

Compromiso interno del sistema - Extremadamente severo y probable si se usa software no confiable para pasar datos a la red interna.
Datos del cliente robados - Severo y probable si el servidor externo es vulnerable a intrusos, lo que puede comprometer el sistema operativo o aplicación.
Transacciones falsas si se irrumpe en el servidor externo - Severo y probable si el servidor externo es vulnerable a intrusos, lo que puede comprometer el sistema operativo o aplicación.
Transacciones falsas si se roba el PIN o la tarjeta inteligente del cliente - Severidad limitada porque compromete cuentas individuales. Probable solo si las credenciales robadas no son detectadas rápidamente.
Ataque interno al sistema - Extremadamente severo y probable si ya ha habido ataques internos contra los datos de la empresa.
Errores de ingreso de datos - Severidad moderada y probable por error humano.
Destrucción del centro de datos - Extremadamente severo pero poco probable ya que requiere un evento de proporciones épicas, como un desastre natural.

Luego de la evaluación de la severidad y la probabilidad de las amenazas, la información se utiliza en el análisis de riesgos. Hay dos tipos de análisis de riesgos en la seguridad de la información: cuantitativo y cualitativo.

Análisis de riesgos cuantitativo

El análisis de riesgos cuantitativo usa un modelo matemático para asignar una representación monetaria al valor de los activos, el costo de las amenazas realizadas y el costo de las implementaciones de seguridad. Las representaciones monetarias generalmente se basan en costo anual.

Análisis de riesgo cualitativo

Hay muchas maneras de llevar a cabo un análisis de riesgo cualitativo. Un método utiliza un modelo basado en la situación. Este enfoque es conveniente para grandes ciudades, estados o provincias y países ya que en estos casos no es práctico hacer listas de los activos, lo cual constituye el primer paso en cualquier análisis de riesgo cuantitativo. Si un gobierno nacional decidiera confeccionar una lista de todos sus activos, estos habría cambiado cientos o miles de veces mientras la lista se llenaba y nunca llegaría a ser correcta.

Con un análisis de riesgo cualitativo, la investigación es exploratoria y no siempre se puede graficar o probar matemáticamente. Se concentra mayormente en entender por qué hay riesgos y cómo se pueden resolver de diferentes maneras. El análisis de riesgos cuantitativo es más preciso matemáticamente y es utilizado por las empresas como justificación de los costos de las contramedidas. Por esta razón, el siguiente tema es una profundización en la construcción del análisis de riesgo cuantitativo.



Análisis de riesgo cuantitativo

El análisis de riesgo cuantitativo usa fórmulas específicas para determinar el valor de las variables de decisión de riesgos. Éstas incluyen fórmulas que calculan el asset value (valor de activos - AV), el exposure factor (factor de exposición - EF), la single loss expectancy (expectativa de una sola pérdida - SLE), la annualized rate of occurrence (tasa anual de ocurrencias - ARO) y la annualized loss expectancy (expectativas de pérdidas anuales - ALE).

Valor de activos

El valor de activos incluye el precio de compra y los costos de desarrollo y mantenimiento. En el caso de una base de datos o un servidor web, el AV también incluye el costo de desarrollo. El AV es un número difícil de calcular.

Factor de exposición

El factor de exposición es una estimación del grado de destrucción que puede llegar a tomar lugar. Por ejemplo, considere la posibilidad de que una inundación afecte el centro de datos de e-banking. ¿Cuál es la probabilidad de que lo destruya? ¿Sería del 60 por ciento, 80 por ciento o 100 por ciento? El equipo de evaluación de riesgos debe evaluar todas las posibilidades y luego tomar una determinación. Si existe una copia de resguardo de todos los medios y datos en otro lugar físico, las únicas pérdidas serían de hardware y productividad. Por lo tanto, una inundación tendría un factor de destrucción del 60 por ciento.

Como un ejemplo adicional, considere los errores de ingreso de datos, que son mucho menos dañinos que una inundación. Un solo error de ingreso de datos probablemente constituirá menos que una fracción del porcentaje de exposición, o .001 por ciento.

Expectativa de una sola pérdida - SLE

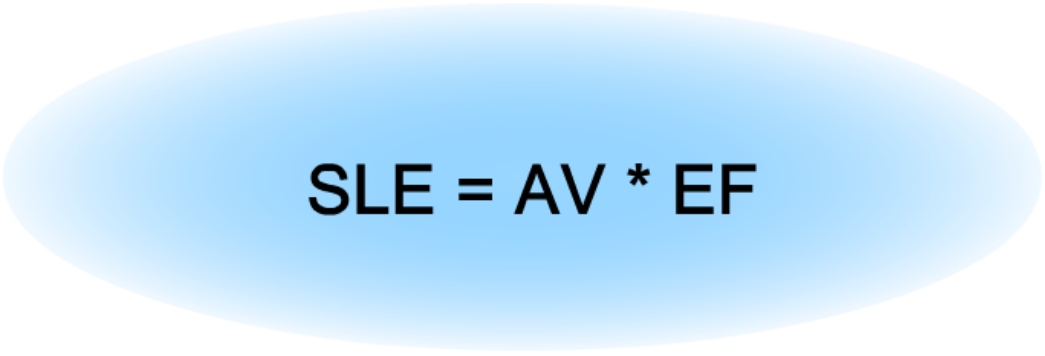
El cálculo de la expectativa de una sola pérdida representa la pérdida esperada resultante de una sola ocurrencia de la amenaza. La SLE se define como AV multiplicado por EF. Usando los ejemplos anteriores, los cálculos de SLE resultarían en lo siguiente:

Amenaza de inundación

El EF es de 60 por ciento
El AV de la empresa es de US$10,000,000
La SLE es US$10,000,000 * .60 = US$6,000,000

Error de ingreso de datos

El EF es de .001 por ciento
El AV de los datos y bases de datos es de US$1,000,000
La SLE es US$1,000,000 * 0.00001 = US$10



Fórmula del análisis de riesgos cuantitativo

- El AV es el costo de un activo individual.
- El EF es la pérdida, representada por un porcentaje, que puede representar una amenaza sobre los activos.
- La SLE es el resultado de AV * EF o el costo de una sola ocurrencia de la amenaza.

Tasa anual de ocurrencias - ARO

La tasa de ocurrencias anual estima la frecuencia de un evento y se usa para calcular la ALE.

Usando los ejemplos anteriores, el tipo de inundación que afecte al centro de datos sería la peor inundación del siglo, por lo que tendría una oportunidad de 1/100 de ocurrir este año, lo cual significaría una ARO de 1/100 para la inundación.

En cuanto a los errores de ingreso de datos, estime unos 500 por día. Como la empresa permanece abierta 250 días al año, el ARO de los errores de ingreso de datos será 500 * 250 o 125,000 ocurrencias totales.

Expectativas de pérdidas anuales - ALE

Los analistas de riesgos calcula la ALE en términos anuales para estimar el costo a la empresa si no toma medidas para contrarrestar las amenazas existentes. La ALE deriva de la multiplicación de la SLE por la ARO. Los cálculos ALE para los ejemplos son sorprendentes.

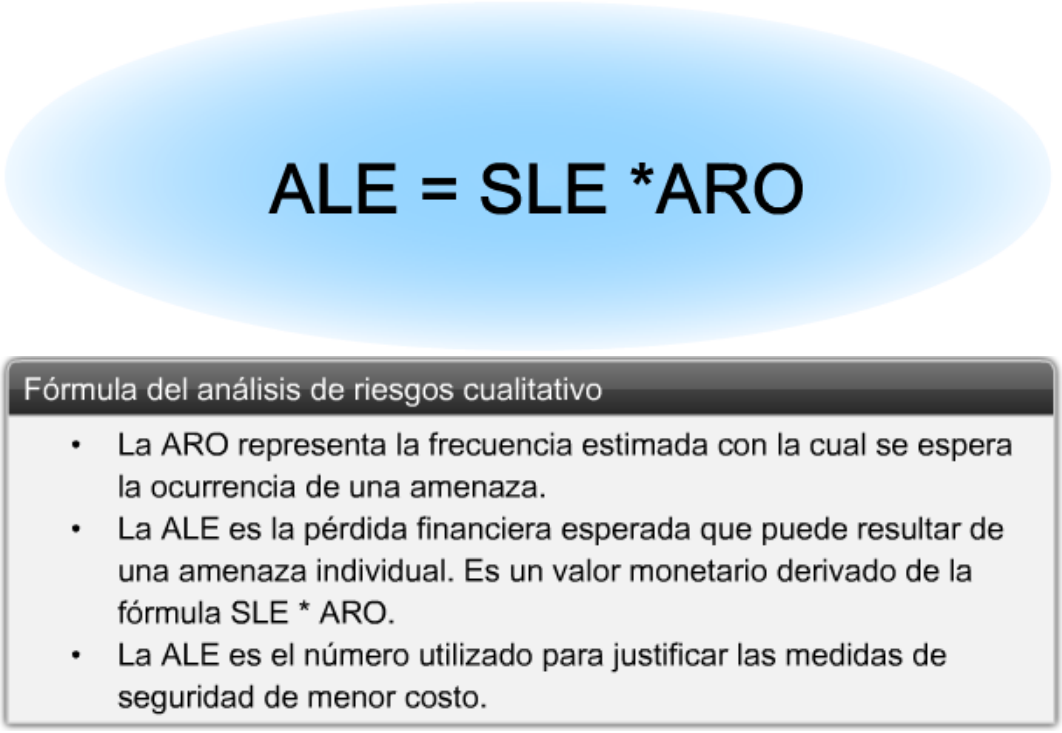
Amenaza de inundación

La SLE es de US$6,000,000
La ARO es de .01
La ALE es de US$6,000,000 * .01 = US$60,000

Errores de ingreso de datos

La SLE es de US$10
La ARO es de 125,000
La ALE es de US$10 * 125,000 = US$1,250,000

Gastar US$50,000 para mejorar la seguridad de las aplicaciones de bases de datos para reducir los errores de ingreso de datos se ha vuelto ahora una decisión fácil. Igualmente fácil es rechazar una propuesta para mejorar las defensas contra inundación que costarán US$3,000,000.



Es necesario realizar un análisis de riesgos cuantitativo para todas las amenazas identificadas durante el proceso de identificación de riesgos.

Deben indicarse en una lista todas las amenazas identificadas, el costo relativo de cada una y el costo total si ocurrieran todas las amenazas esperadas. Esta lista debe luego ordenarse según criterios de severidad y costo relativo de las amenazas.

Si la organización tiene una lista de 10 amenazas esperadas, puede priorizar las amenazas y tratar las más serias primero. Esta organización por prioridades permite al administrador concentrar los recursos donde pueden hacer más falta. A modo de ejemplo, suponga que una organización compiló esta lista de amenazas y costos:

Abuso interno de la red - US$1,000,000 en pérdidas de productividad
Error de ingreso de datos - US$500,000
Gusanos - US$100,000
Virus - US$10,000
Robo de laptop - US$10,000

Asuma que actualmente existe una solución antivirus y que debe decidirse si actualizarla. En base al análisis cuantitativo, puede determinarse que los recursos serán mejor utilizados tratando el abuso interno de la red que actualizando la solución antivirus.

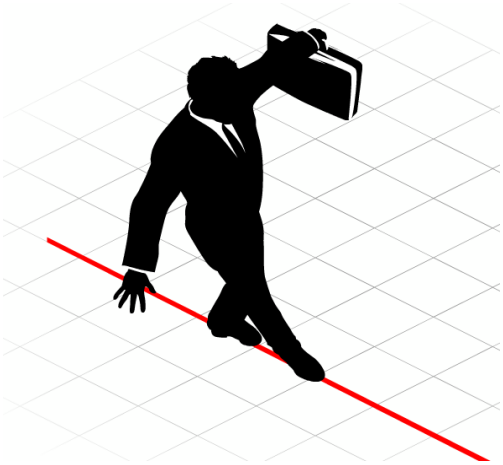
En los incidentes que constituyen materia de seguridad nacional, no es aconsejable basar las decisiones en el costo.

9.1.3 Gestión y mitigación de riesgos

Una vez que las amenazas han sido identificadas y los riesgos estimados, debe desplegarse una estrategia de protección contra los riesgos. Existen dos maneras muy diferentes de tratar los riesgos:

Gestión de riesgos - Este método despliega mecanismos de protección para reducir los riesgos a un nivel aceptable. La gestión de riesgos es el aspecto más básico y difícil de la construcción de sistemas seguros, ya que requiere un vasto conocimiento de los riesgos, ambientes de riesgo y métodos de mitigación.

Mitigación de riesgos - Este método elimina el riesgo evitando las amenazas enteramente, lo cual generalmente no es una opción en el mundo comercial, donde los riesgos controlados o gestionados permiten mayores ganancias.



Considere el banco que quiere proporcionar servicios de e-banking. La gestión de riesgos puede ser ilustrada por decisiones estratégicas de alto nivel que describen cómo mitigar cada riesgo. Tenga en consideración que no todas las técnicas de mitigación son implementadas basándose en la fórmula de riesgo versus costo en el análisis de riesgo cuantitativo:

Compromiso interno del sistema - Proporcione los mínimos privilegios necesarios a los usuarios internos para realizar tareas específicas y use aplicaciones seguras que minimicen el acceso interno.
Datos de usuario robados - Mantenga los datos de los usuarios en los servidores internos y solo transfiera datos al exterior bajo demanda.
Transacciones falsas si se irrumpe en el servidor externo - Permita solo ataques man in the middle en el servidor externo y diseñe la aplicación del servidor externo para que no permita transacciones arbitrarias para las cuentas de cliente.
Transaccionse falsas si el PIN o la tarjeta inteligente del cliente son robados - Use una actualización frecuente de las listas de revocación y tenga un contrato con el usuario que lo obligue a asumir responsabilidad sobre las tarjetas token robadas.
Ataque interno al sistema - Limite estrictamente el acceso a la aplicación y proporcione auditorías estrictas a todos los accesos desde dentro.
Error de ingreso de datos - Mejore la seguridad de las aplicaciones de base de datos y proporcione un sistema de verificación redundante para reducir los errores de ingreso de datos.

Destrucción del centro de datos - Asegúrese de que las copias de resguardo se conserven fuera del sitio y de que haya equipamiento de repuesto a mano. Mejore las defensas contra inundaciones levantando los equipos del suelo, entre otras precauciones.



Con un enfoque de mitigación de riesgos, la empresa puede decidir no ofrecer los servicios de e-banking por los riesgos que puede llegar a ocasionar. Una actitud como esa puede ser válida en algunas organizaciones militares, pero generalmente no es una opción en el mundo de los negocios. Las organizaciones que pueden gerenciar los riesgos generalmente son las que tienen más ganancias.

Una vez que se han identificado las amenazas, la organización realiza el análisis apropiado. Si deciden gerenciar los riesgos, el siguiente paso es crear una solución de seguridad.



9.2.1 Introducción a la Red Autodefensiva de Cisco

En años anteriores, las amenazas de origen interno y externo se movían con lentitud, lo cual facilitaba la defensa contra ellas. Ahora, los gusanos de Internet se diseminan por el mundo en cuestión de minutos. Los sistemas de seguridad y la red en sí deben reaccionar instantáneamente. A medida que evoluciona la naturaleza de las amenazas, la postura defensiva asumida por los administradores y los profesionales de la seguridad en redes debe también evolucionar. Sin embargo, es importante que la evolución de las soluciones de seguridad en redes no introduzca complejidad.

La complejidad es uno de los mayores enemigos de la seguridad. La complejidad dificulta al administrador o diseñador predecir cómo interactuarán las partes del sistema, haciendo que éste se torne difícil o incluso imposible de analizar desde una perspectiva de seguridad. La simplicidad en el diseño e implementación debe, entonces, ser uno de los objetivos principales del diseñador. Para satisfacer necesidades de seguridad complejas, considere usar múltiples mecanismos simples y fáciles de verificar.

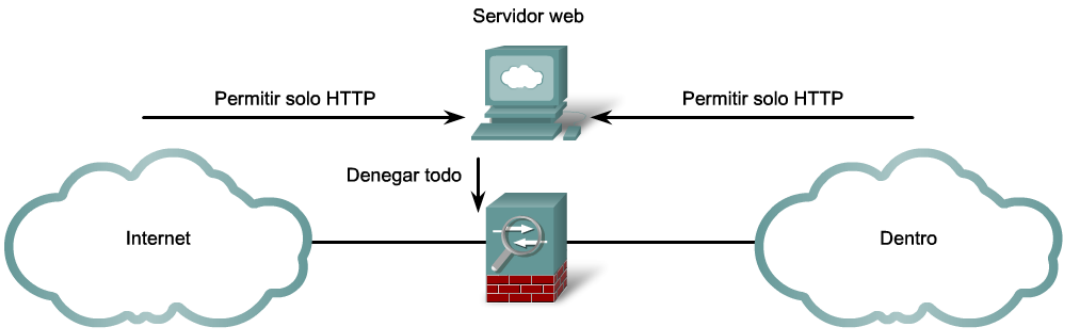
La simplicidad es un beneficio para los usuarios finales del sistema. Si el usuario final no comprende el sistema adecuadamente, éste puede ser comprometido a causa de un mal uso no intencional. Una manera de introducir simplicidad es deshabilitar los servicios innecesarios que el sistema ofrezca, lo cual elimina muchas posibilidades de ataques potenciales. En un dispositivo de usuario final, esta práctica se conoce como la aplicación del privilegio mínimo (least privilege).

El concepto del privilegio mínimo especifica que cada sujeto, usuario, programa o host debe tener solo los privilegios mínimos necesarios para llevar a cabo sus tareas. Tener demasiados privilegios les permite a los usuarios finales hacer más daño, sea intencional o no, que no tenerlos. Los privilegios mínimos también simplifican el análisis del sistema en búsqueda de posibles fallas.

Además de deshabilitar los servicios innecesarios en los dispositivos host, la simplicidad también implica deshabilitar los servicios y funciones innecesarios en los dispositivos de red. Esto se conoce como hardening (fortificación).

Otra manera de simplificar la seguridad es ayudar las funciones del usuario final. Por ejemplo, si el correo electrónico debe ser cifrado para enviarse a socios externos, la solución más simple es usar tecnología, como un gateway de correo electrónico, para automatizar el cifrado del correo electrónico.

Por último, la simplicidad debe estar incluida en el diseño de seguridad. Existen muchos proveedores de soluciones de seguridad. Para ayudar a simplificar el diseño, se recomienda que todos los mecanismos de seguridad provengan del mismo proveedor. La Red Autodefensiva de Cisco (SDN) es una solución englobadora y de extremo a extremo para la seguridad de las redes.



Concepto del privilegio mínimo

- Los usuarios internos y externos solo necesitan acceso al programa del servidor web en el host expuesta.
- El servidor web no necesita abrir conexiones desde dentro hacia fuera.
- El firewall aplica estos permisos mínimos.

La Red Autodefensiva de Cisco usa la red para identificar, prevenir y adaptarse a las amenazas. A diferencia de las estrategias de solución puntual (point solutions), en las que los productos se compran individualmente sin considerar cuáles productos funcionan mejor juntos, el enfoque basado en red es estratégico y está a la altura de los desafíos actuales, facilitando la evolución de la capacidad de tratar nuevas amenazas de seguridad.

Para permitir esta estrategia, la Red Autodefensiva de Cisco tiene tres principios fundamentales:

Integración - La seguridad debe ser incorporada a la infraestructura existente. La seguridad está integrada, no agregada.
Colaboración - Los servicios de seguridad deben trabajar en conjunto con los servicios de red existentes para resaltar las fortalezas de cada área.
Adaptación - La red debe tener la habilidad de evolucionar y ajustarse inteligentemente basándose en las necesidades cambiantes y amenazas emergentes.

Principios de la Red Autodefensiva de Cisco

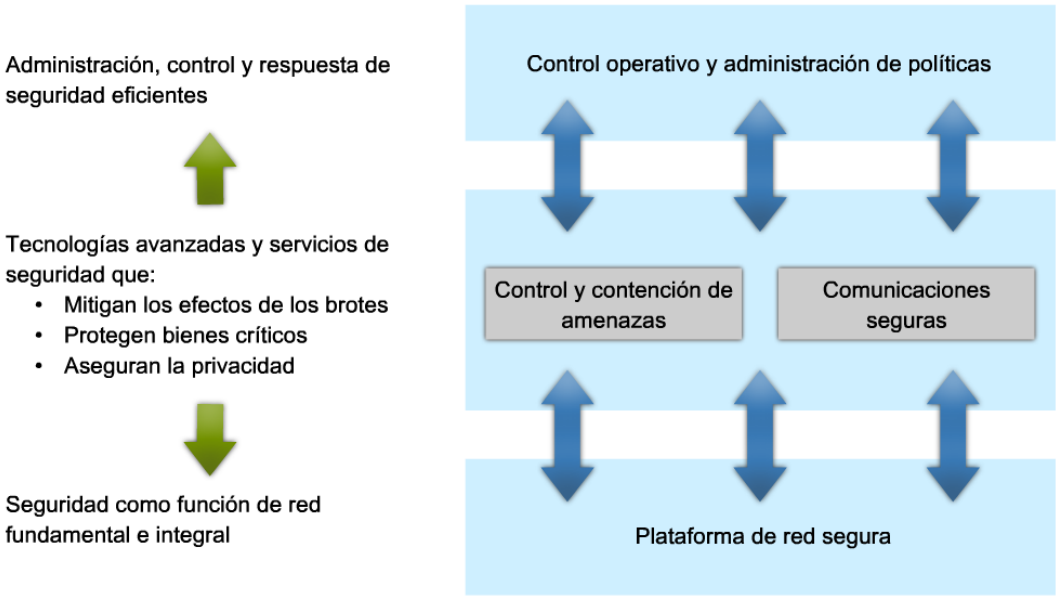


La estrategia de la Red Autodefensiva de Cisco comienza con una plataforma de red fuerte, segura y flexible, sobre la cual se ubicarán los servicios de seguridad según se necesite. Hay varios servicios de seguridad disponibles a través de la Red Autodefensiva de Cisco:

Control y contención de amenazas - Incluye dispositivos y servicios que limitan la exposición a amenazas y la extensión del daño a la red si las amenazas se realizan.
Comunicaciones seguras - Incluye dispositivos y servicios que aseguran la confidencialidad y privacidad de las comunicaciones sensibles, sea comunicación de datos o de voz o comunicación inalámbrica.
Control operativo y administración de políticas - Incluye una suite de herramientas que componen un framework para una administración y aplicación de las políticas escalable que extienda la seguridad de extremo a extremo.

El uso de soluciones puntuales de varios proveedores distintos incrementa los costos en el transcurso del tiempo, ya que da pie a ajustes, inconsistencias y complejidades agregadas al diseño de la red que no estaban contemplados en el diseño original. Con el tiempo, la Red Autodefensiva de Cisco incrementa el valor de la inversión, ya que usa una infraestructura común. La administración se realiza más eficientemente cuando es simplificada, permitiendo la identificación y resolución de brechas antes de que se tornen vulnerabilidades serias en el diseño de la red.

Definición de Red Autodefensiva de Cisco



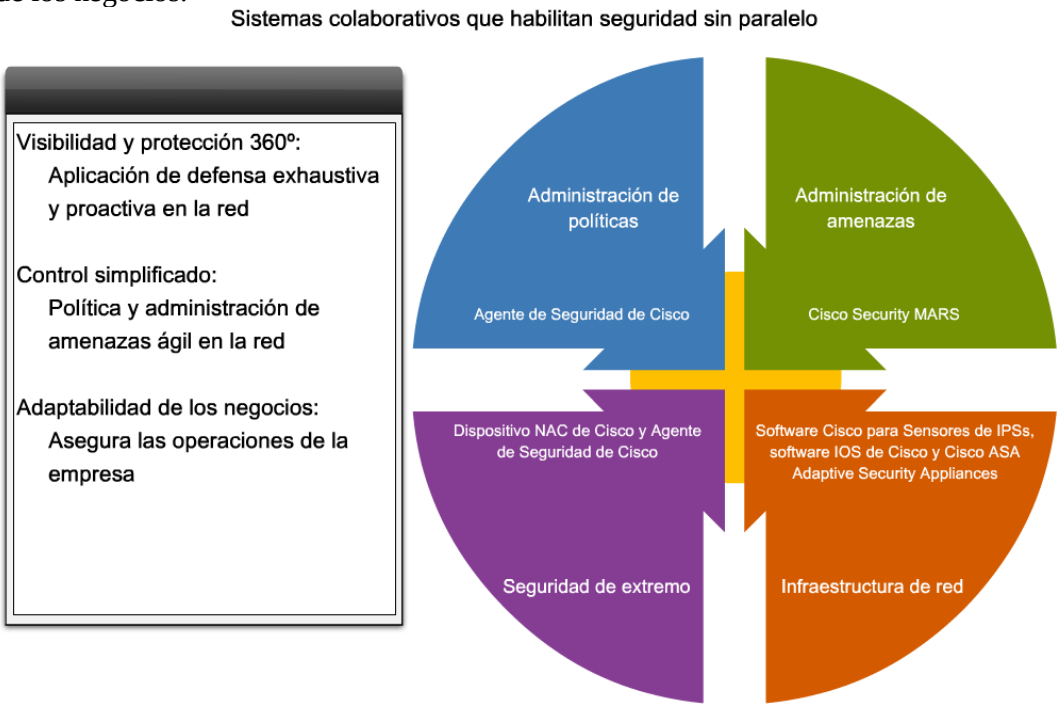
El enfoque de la Red Autodefensiva de Cisco es englobador e incluye las siguientes herramientas para proporcionar servicios de seguridad:

El Administrador de Seguridad de Cisco proporciona gestión de políticas.
El Sistema de Respuesta, Análisis y Monitoreo de Seguridad de Cisco (MARS) proporciona gestión de amenazas.
El software IOS de Cisco, las Cisco Adaptive Security Appliances y el Software Cisco para Sensores de Sistemas de Prevención de Intrusiones proporcionan seguridad a las redes.
Los dispositivos NAC de Cisco y el Agente de Seguridad de Cisco proporcionan seguridad de punto final.

Existen varios beneficios adicionales que resultan de este enfoque englobador y exhaustivo:

Visibilidad y protección de 360 grados - Resulta en una defensa comprensiva y proactiva de la red. Los datos de amenazas de toda la infraestructura se transmiten eficientemente en una amplia variedad de sistemas y dispositivos. La identificación de amenazas multivector captura violaciones a las políticas, explotaciones de vulnerabilidades y comportamientos extraños.
Control simplificado - Agiliza la gestión de políticas en toda la red y la implementación de las políticas en toda la infraestructura en una amplia variedad de sistemas y dispositivos.
Resistencia de los negocios - Asegura las operaciones de la empresa. La colaboración y correlación en varios sistemas, estaciones de trabajo y administración permite respuestas adaptadas a las amenazas en tiempo real. Éste es un elemento vital de la estrategia de la Red Autodefensiva de Cisco.

Este grupo de soluciones mejoradas de control y contención proporcionan una protección de amenazas exhaustiva en toda la infraestructura, asegurando la continuidad de los negocios.



9.2.2 Soluciones para la SDN de Cisco

Control y contención de amenazas

La solución de Control y contención de amenazas de Cisco protege la red, los servidores, las estaciones de trabajo y la información, ya que proporciona protección de estación de trabajo basada en el comportamiento, mitigación DDoS, prevención de intrusos, antivirus de red, aplicación de la política y respuesta proactiva. Regula el acceso a la red, aisla los sistemas infectados, evita el ingreso de intrusos y protege los activos críticos de los negocios. La solución de Control y contención de amenazas contrarresta el tráfico malicioso como gusanos, virus y malware antes de que afecten a los negocios a través del uso de una política, una configuración y una gestión de eventos amenazantes centralizadas.

La solución de Control y contención de amenazas contiene tres elementos:

Control de amenazas para estaciones de trabajo - Este elemento defiende a la red de las amenazas comúnmente introducidas a través del uso de Internet, como virus, spyware y otro contenido malicioso. Los productos Cisco que proporcionan control de amenazas para estaciones de trabajo incluyen el Agente de Seguridad Cisco para Desktops, los Cisco ASA de la Serie 5500 Adaptive Security Appliances (Content Security Edition), Router de Servicios Integrados Cisco, el IPS de Cisco y el dispositivo NAC de Cisco.
Control de amenazas para infraestructura - Este elemento protege al servidor y la infraestructura de aplicaciones contra ataques e intrusos. También los defiende contra

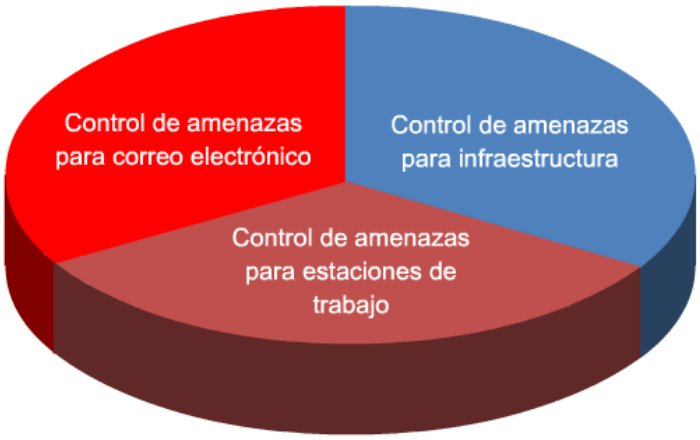
intentos internos y externos de penetrar o atacar servidores y recursos de información a través de vulnerabilidades en las aplicaciones o el sistema operativo. Los productos que proporcionan control de amenazas en la infraestructura incluyen el Agente de Seguridad de Cisco para Servidores, el Cisco IPS, las soluciones de firewall de Cisco incluyendo los ASA de la serie 5500 y Módulo de Servicios de Firewall de la serie Catalyst 6500 de Cisco, el Módulo Motor de Control de Aplicación de Cisco, el Cisco Application Velocity System (AVS), seguridad XML, el Cisco Security MARS y el Administrador de Seguridad de Cisco.

Control de amenazas para correo electrónico - Este elemento protege la productividad de los negocios, la disponibilidad de los recursos y la confidencialidad de la información al detener las amenazas que se originan en el correo electrónico.

La solución de Control y contención de amenazas de Cisco tiene varios beneficios:

* Protege proactivamente contra amenazas
* Aplica el cumplimiento de la política en la estación de trabajo para parches y actualizaciones manejables
* Contiene infecciones y brotes proactivamente con mitigación distribuida

Control de amenazas y contención de Cisco



La solución de control de amenazas para correo electrónico ofrece las siguientes capacidades:

- Filtrado de repudio, autenticación de correo electrónico y control de flujo
- Escaneo de contenido, anti-spam avanzado y aplicación de la política
- Cifrado de información confidencial
- Filtrado innovador de brotes de virus

La solución de control de amenazas para estaciones de trabajo ofrece las siguientes capacidades:

- Evaluación de la integridad del punto final, incluyendo descargas de los últimos service packs de seguridad o definiciones y cuarentenas de antivirus de sistemas no compatibles

- Detección y prevención de ataques a nivel de red para proteger a los sistemas víctimas de hackers
- Monitoreo de comportamiento en cada sistema para construir defensas de "día cero"
- Contención de amenazas en los sistemas infectados y prevención del contagio de infecciones a otros dispositivos

La solución de control de amenazas para infraestructura ofrece las siguientes capacidades:

- Monitoreo de patrones de conducta y correlación de estos con otra información de seguridad de redes para proporcionar una imagen clara de los eventos en toda la infraestructura IT
- Habilitación de la implementación de políticas de seguridad para mitigar amenazas en tiempo real
- Prioridad de los recursos para concentrarse en las amenazas y ataques más importantes
- Detección de amenazas desde ambos extremos y la infraestructura de la red
- Correlación de amenazas en una ubicación central

Comunicaciones seguras

Muchas organizaciones usan la flexibilidad y eficiencia de costo de Internet para extender sus redes a oficinas sucursales, teleconmutadores, clientes y socios. Cuando una organización extiende su red de esta manera, asegurar la privacidad e integridad de toda la información enviada a través de Internet es vital. Esto requiere una infraestructura de comunicaciones manejable y de costo eficiente que permita comunicaciones seguras, algo que puede lograrse mediante el uso de IPsec y VPNs SSL.

Implementar una infraestructura de comunicaciones segura tiene varios beneficios:

- Mejora la productividad y eficiencia de los negocios
- Permite nuevas aplicaciones de negocios
- Ayuda a cumplir con las regulaciones relativas a la privacidad de la información

La solución Cisco Secure Communications es un grupo de servicios de seguridad esenciales en la Red Autodefensiva de Cisco. La solución de comunicaciones seguras comprende dos grandes elementos. Ambos usan criptografía para fines de confidencialidad:

- Comunicaciones seguras para acceso remoto - Proporciona un acceso altamente seguro y personalizable a las redes y aplicaciones empresariales estableciendo un túnel cifrado a través de Internet.

- Comunicaciones seguras para conexiones de sitio a sitio - Proporciona una infraestructura WAN basada en Internet para conectar sucursales, oficinas privadas o socios a todas las partes de la red.



Control operativo y administración de políticas

El control operativo y la administración de políticas ayudan a automatizar, simplificar e integrar la red para reducir los costos operativos y mejorar la productividad. La Suite de Manejo de Seguridad de Cisco es un framework de productos y tecnologías diseñados para la administración y aplicación de políticas escalables en la Red Autodefensiva de Cisco.

Hay dos componentes en la Suite de Manejo de Seguridad de Cisco: Administrador de Seguridad de Cisco y Sistema de Respuesta, Análisis y Monitoreo de Seguridad de Cisco. Estos componentes trabajan juntos para manejar de manera centralizada la red y para cumplir funciones críticas como disponibilidad, capacidad de respuesta, resistencia y seguridad consistentes. El Administrador de Seguridad de Cisco y el Sistema de

Respuesta, Análisis y Monitoreo de Seguridad de Cisco fueron diseñados para complementar a los productos CiscoWorks. Esta solución integrada simplifica y automatiza las tareas asociadas con las operaciones de administración de seguridad, incluyendo configuración, monitoreo, análisis y respuesta.

La Suite de Manejo de Seguridad de Cisco proporciona beneficios como:

- Mayor velocidad y precisión en el despliegue de las políticas
- Mejor visibilidad para monitorear la seguridad de extremo a extremo
- Respuesta más rápida a las amenazas
- Aplicación del cumplimiento de las políticas empresariales
- Perfeccionamiento de la administración del flujo de trabajo adecuado



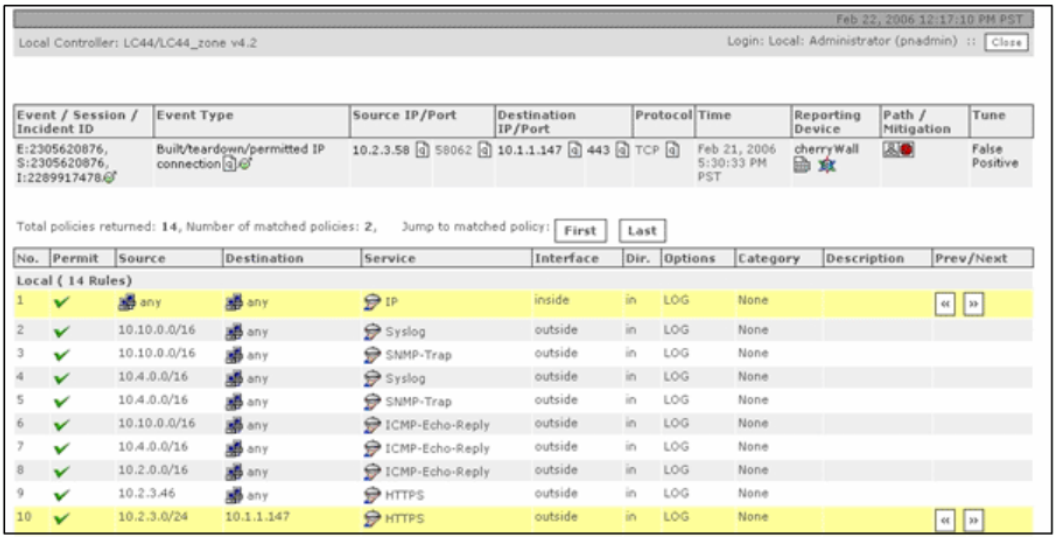
El Administrador de Seguridad de Cisco es una solución potente y fácil de usar que ayuda a aprovisionar a todos los aspectos de las configuraciones de los dispositivos y las políticas de seguridad de la familia de productos de seguridad Cisco de manera centralizada. La solución es efectiva incluso en la administración de redes pequeñas de menos de 10 dispositivos, pero es suficientemente escalable como para administrar eficientemente grandes redes de miles de dispositivos. La escalabilidad se logra a través de técnicas de administración inteligentes basadas en políticas que pueden simplificar la administración. El Administrador de Seguridad de Cisco incluye las siguientes características:

- Soporta aprovisionamiento de las plataformas de router Cisco que ejecutan imágenes de software de seguridad del IOS de Cisco, incluyendo las ASA 5500 Series Adaptive Security Appliances, las Cisco PIX de la serie 500 Security

Appliances, los Cisco IPS 4200 Series Sensors y el Cisco Catalyst 6500 Series Advanced Inspection and Prevention Security Services Module (AIP-SSM).

- Responde más rápidamente a las amenazas al permitir al administrador definir y asignar nuevas políticas de seguridad a miles de dispositivos en solo unos pasos.
- Tiene una rica interfaz gráfica de usuario (GUI) que proporciona facilidad en el uso.
- Múltiples vistas proporcionan métodos flexibles para administrar dispositivos y políticas, incluyendo la habilidad de administrar la red de seguridad visualmente en un mapa de topología.
- Contiene una extensiva ayuda animada diseñada para el nuevo usuario, lo cual reduce el tiempo de aprendizaje.
- Permite al administrador especificar, centralmente, qué políticas son compartidas y heredadas automáticamente por los nuevos dispositivos.
- Se integra con el Servidor de Control de Acceso Seguro de Cisco (ACS) para dar como resultado funciones granulares de administración y control de acceso basado en roles.
- Se integra con Cisco Security MARS para correlacionar eventos con las reglas de firewall asociadas y tomar decisiones más rápidamente, incrementando el tiempo de funcionamiento de la red.
- Cuenta con la habilidad de asignar tareas específicas a cada administrador durante el despliegue de una política, con control de cambios y monitoreo formal, lo cual resulta en una mejor coordinación de grupo.

Administrador de Seguridad de Cisco

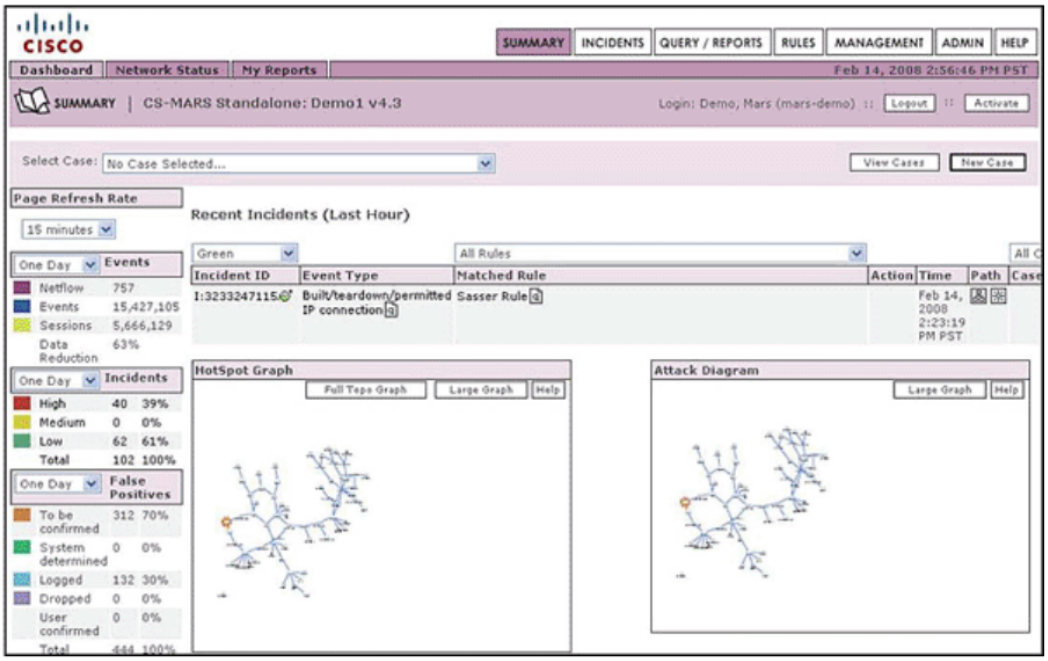


El Cisco Security MARS proporciona monitoreos de seguridad para aplicaciones de host y dispositivos de seguridad de la red hechos por Cisco y otros proveedores. El Cisco Security MARS ofrece los siguientes beneficios:

Reduce significativamente los falsos positivos al proveer una vista de extremo a extremo de la red.
Define las respuestas de mitigación más efectivas al monitorear la configuración y topología del ambiente.

Promueve la detección de anomalías en el ambiente mediante la provisión de NetFlow para análisis de comportamiento en la redNetFlow.
Porporciona un acceso rápido y fácil a los informes de cumplimiento de auditorías con más de 150 informes personalizables listos para ser usados.
Efectúa recomendaciones precisas para la remoción de las amenazas, incluyendo la habilidad de visualizar la trayectoria del ataque e identificar la fuente de la amenaza con gráficos topológicos detallados que simplifican la respuesta de seguridad a nivel de capa 2 y superiores.

Cisco Security MARS



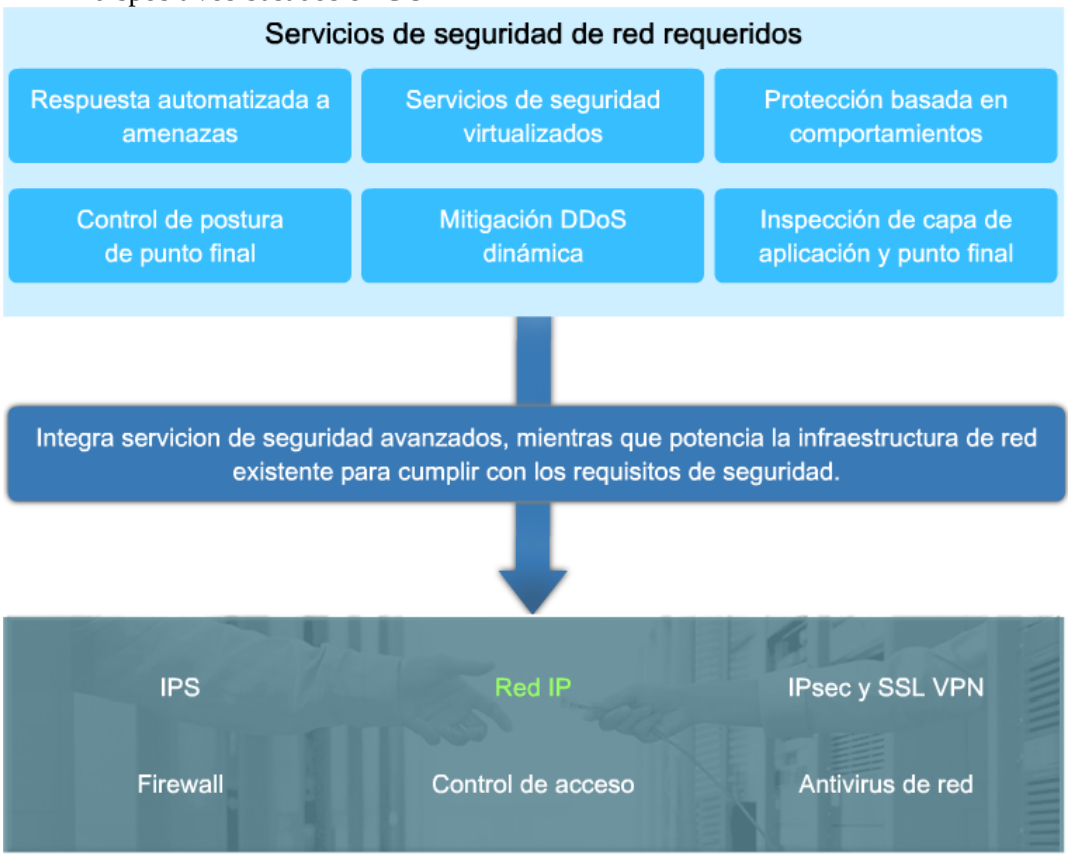
9.2.3 Portfolio de Seguridad Integrado de Cisco

Una red verdaderamente segura requiere varios productos y tecnologías que colaboren sin problemas en todas las plataformas y se integren perfectamente a la infraestructura de la red. No existe un solo producto o tecnología que sea capaz de asegurar una red por sí solo.

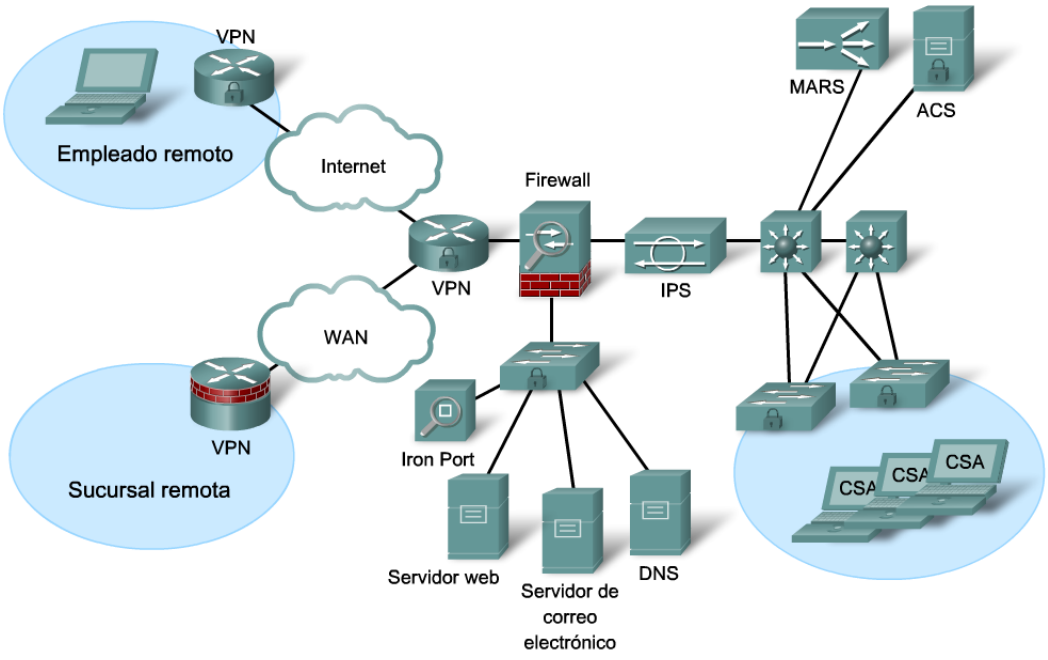
Cisco ofrece la gama de productos de seguridad integrados más amplia de la industria. Este grupo está diseñado para satisfacer las necesidades y los diversos modelos de despliegue de cualquier red y ambiente. Estos productos de seguridad integrados proporcionan una solución exhaustiva:

- Las plataformas IOS de Cisco con IPS, VPN y firewall con estados integrados para soportar conectividad IP segura
- Las Cisco Adaptive Security Appliances con VPN integrada para garantizar seguridad de perímetro, control de acceso e IPS
- Las Cisco PIX Security Appliances con VPN integrada para garantizar seguridad de perímetro y control de acceso

- IDS e IPS de red basados en dispositivos e IDS e IPS de red integrados para routers IOS de Cisco, Cisco PIX Security Appliances y Cisco ASA
- Software de protección de extremos Agente de Seguridad de Cisco para proteger servidores y estaciones de trabajo de los efectos dañinos de las amenazas
- Cisco Secure ACS para garantizar que los usuarios tengan la autoridad apropiada para acceder a los recursos de la empresa
- Módulos de seguridad para switches y routers Cisco que proporcionan seguridad en todo el centro de datos
- Productos de administración de seguridad, incluyendo el Administrador de Seguridad de Cisco, el Cisco Security MARS, el Administrador de Routers y Dispositivos de Seguridad de Cisco (SDM) y otros administradores de dispositivos basados en GUI



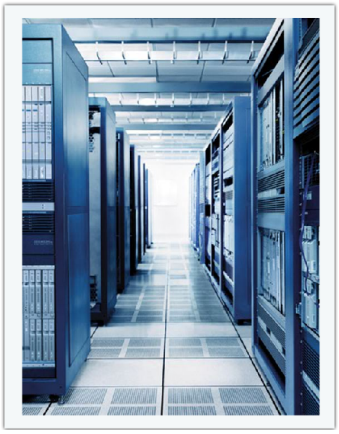
La mayoría de las empresas no adoptan todos los componentes de la Red Autodefensiva de Cisco de una vez. Esto ocurre porque puede volverse difícil monitorear todos los subsistemas requeridos a la vez sin desestabilizar la integridad de los servicios IT. Adicionalmente, algunas empresas dudan si confiar los controles de seguridad a un sistema automatizado hasta estar seguros de que el sistema opera de manera confiable. El diseño de Red Autodefensiva de Cisco satisface estas preocupaciones al proveer productos que se pueden desplegar independientemente unos de los otros. Más adelante, podrán agregarse otros productos a medida que la confianza crezca en el diseño de seguridad en general.



9.3.1 Introduccion a la seguridad de las operaciones

Aunque la Red Autodefensiva de Cisco aumenta el nivel de seguridad, no puede garantizar una red completamente invulnerable. Los nuevos tipos de ataques y avances en las tecnologías de hacking todavía constituyen amenazas incluso para los sistemas más seguros. Además, todas las redes son vulnerables a ataques si la planificación, implementación, operaciones y mantenimiento de la red no adhieren a las prácticas diarias necesarias para desplegar y mantener un sistema seguro.

La seguridad de las operaciones inicia con el proceso de planificación e implementación de la red. Durante estas fases, el equipo de operaciones analiza el diseño, identifica los riesgos y vulnerabilidades y realiza las adaptaciones necesarias proactivamente. Luego de que la red está implementada, comienzan las verdaderas tareas operativas, incluyendo el mantenimiento diario del ambiente. Estas actividades son rutinarias y permiten que el ambiente, los sistemas y las aplicaciones funcionen de manera correcta y segura.



Las responsabilidades del equipo de operaciones están relacionadas con todo lo necesario para mantener a la red, los sistemas de computadoras, las aplicaciones y el ambiente corriendo de manera segura y protegida. Estos individuos se ocupan de los controles o soluciones de seguridad que se usan para proteger el hardware, el software y los medios cada día. Esto incluye la protección de amenazas en el ambiente de las operaciones, intrusos internos y externos y operaciones que acceden a los recursos de manera inapropiada.

El equipo de operaciones generalmente tiene el objetivo de evitar problemas recurrentes, reducir las fallas de hardware a un nivel aceptable y reducir el impacto de las fallas o rupturas del hardware. Deben investigar eventos inusuales o inexplicables, cargas iniciales de programas no programadas, desviaciones del estándar y otras condiciones anormales que puedan tomar lugar en la red. Aunque las personas a cargo de las operaciones son responsables de asegurar que los sistemas estén protegidos y continúen ejecutándose de manera predecible, es importante aclarar que la administración es responsable del comportamiento y la corrección del personal. Por esta razón, es necesario que la administración trabaje cerca del equipo de operaciones para asegurar la continuidad de la seguridad de la red.

Para asegurar un ambiente de trabajo seguro en el departamento de operaciones, deben integrarse ciertos principios fundamentales a las actividades diarias:

- Separación de tareas - Control de dos personas y doble operador
- Rotación de tareas
- Recuperación confiable - Preparación de fallas y recuperación del sistema
- Controles de cambios y configuración



9.3.2 Principios de la seguridad de las operaciones

Separación de las tareas

La separación (o división) de las tareas (SoD) es uno de los principios fundamentales del control interno y es uno de los más difíciles y a menudo más costosos de lograr. La SoD establece que ningún individuo debe tener control sobre dos o más fases de una transacción u operación. En cambio, las responsabilidades son asignadas de tal manera que incorporen cheques y balances. Esto hace que un fraude intencional se vuelva más difícil de perpetrar, ya que requiere que dos o más individuos o partes conspiren.

El término SoD ya es popular en los sistemas financieros. Estas empresas no combinan roles como la recepción de cheques, la aprobación de descuentos, el depósito de dinero y la conciliación del estado de cuentas. Esto contribuye a reducir el daño potencial de las acciones de una persona. Similarmente, los departamentos de IT deben organizarse para lograr una adecuada separación en las tareas. Existen dos métodos.

El primer método es conocido como el principio de control de dos personas (two-person control principle). Establece que la tarea deberá ser realizada por dos individuos, y cada uno es responsable de evaluar y aprobar el trabajo del otro. Además de proporcionar un registro de auditoría y reducir las oportunidades de fraude, este principio tiene el beneficio agregado de reducir los errores de configuración. Por los costos indirectos involucrados, esta práctica generalmente se limita a responsabilidades consideradas riesgos potenciales de seguridad.

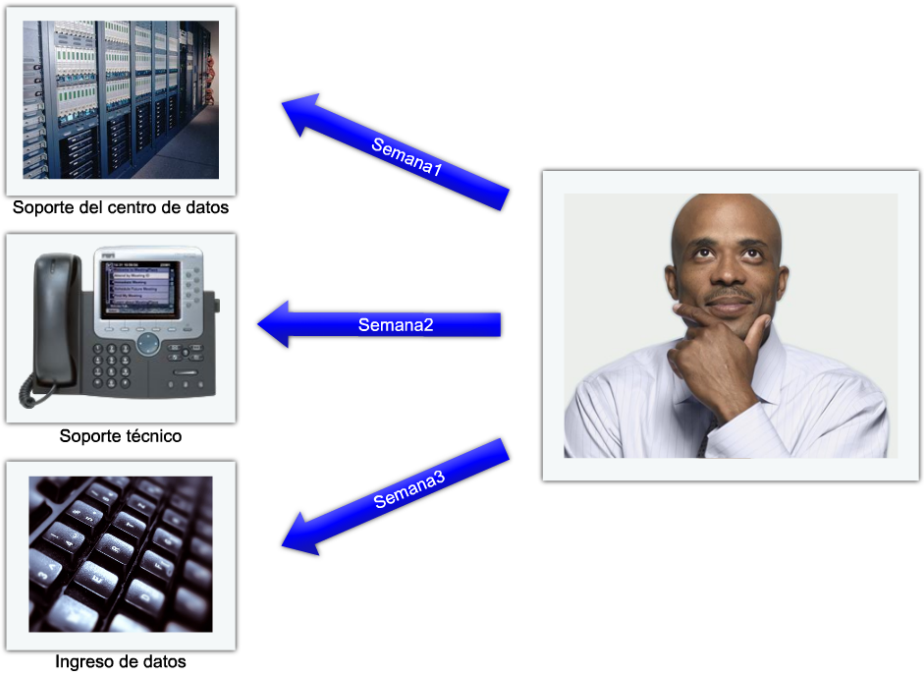
Otro método para implementar SoD es el principio de doble operador, en el que una tarea se divide y cada parte es asignada a un individuo. La tarea no puede completarse hasta que ambos completen su parte. Un ejemplo del principio de doble operador es un cheque que requiere dos firmas para que el banco lo acepte.

Rotación de tareas

La rotación de las tareas, o rotación de trabajo, es una medida de seguridad en la que se asigna a los individuos tareas específicas por un tiempo determinado antes de moverlos a otra tarea. Para implementar este principio exitosamente, es importante que los individuos estén suficientemente capacitados para completar más de un trabajo.

La revisión por pares es parte de la rotación de tareas. Por ejemplo, suponga que un esquema de rotación de tareas consta de cinco personas rotando en cinco roles diferentes durante la semana. La revisión por pares en el trabajo ocurre aún sin que haya intención de llevarla a cabo. Cuando cinco personas realizan una misma tarea en el transcurso de la semana, cada una de las personas indefectiblemente debe revisar el trabajo de los demás.

Además de proporcionar seguridad, la rotación de tareas también previene el aburrimiento y le da al personal una mayor amplitud de exposición a la operación en toda la red. Esto crea un departamento de operaciones fuerte y flexible, ya que cada miembro es capaz de llevar a cabo diferentes tareas.



Recuperación confiable

Una de las maneras más fáciles de comprometer un sistema es hacer que se reinicie y tomar control de él antes de que sus defensas se carguen. Por esta razón, la recuperación confiable es un principio importante de la seguridad de las operaciones. Este principio establece que los sistemas fallan en algún punto, por lo cual debe establecerse un proceso de recuperación. La manera más común en que puede prepararse el sistema para la recuperación frente a fallas es la creación de copias de resguardo regulares.

La creación de copias de resguardo de los datos es una práctica estándar en la mayoría de los departamentos de informática. Tenga en consideración que muchos programas de software de creación de copias de resguardo usan una cuenta que pasa por alto la seguridad de los archivos. Por lo tanto, los individuos que tienen derechos suficientes para crear copias de reguardo de los datos tienen acceso a archivos a los que normalmente no tendrían acceso. Lo mismo ocurre con los individuos que tienen derechos suficientes para restaurar los datos.

Los profesionales de la seguridad proponen que se cumplan las siguientes prácticas en relación con los programas de creación de copias de resguardo:

- Un empleado subalterno debe ser el responsable de cargar los medios vacíos.
- El software de creación de copias de resguardo debe usar una cuenta desconocida por los empleados para pasar por alto la seguridad de los archivos.
- Otro empleado debe retirar los medios de almacenamiento de las copias de resguardo y almacenarlas de manera segura en el sitio físico mientras es asistido por otro empleado.
- Otra copia de resguardo debe ser almacenada en otro sitio físico por un tercer empleado, acompañado por otro empleado.

Una de las maneras más sencillas para el atacante de obtener un archivo de contraseña (o cualquier otro dato) es obtener acceso a la cinta en la que se almacena la copia de resguardo, ya que ésta no siempre se maneja o almacena de manera segura.

Prepararse para la falla del sistema es también una parte importante de la seguridad de las operaciones:

- Cree copias de resguardo de los datos críticos regularmente
- Evalúe quién tendrá acceso a los archivos para hacer copias de resguardo y qué tipos de acceso tendrá
- Asegure los medios de almacenamiento de las copias de resguardo

La recuperación del sistema sigue a la falla del sistema. Hay muchos ejemplos de programas y aplicaciones que tienen funciones de recuperación del sistema incorporadas:

- Sistemas operativos y aplicaciones que tienen modo monousuario (single-user) o a prueba de fallos (safe).
- La capacidad de recuperar archivos que fueron abiertos cuando ocurrió el problema. El proceso de guardado automático incluido en muchas aplicaciones de escritorio es un ejemplo de esta capacidad. Los volcados de memoria (memory dumps) que realizan muchos sistemas operativos cuando el sistema falla son otro ejemplo de esta capacidad.
- La capacidad de retener las configuraciones de seguridad en un archivo luego de la caída del sistema es crítica para que la seguridad no sea pasada por alto al hacer que el sistema se caiga intencionalmente.

- La capacidad de recuperar y retener configuraciones de seguridad para archivos críticos del sistema como el registro, los archivos de configuración y los archivos de contraseñas.



Un servidor con un array de discos montado en un rack puede ser usado para realizar copias de seguridad.

Control de cambios y configuración

El control de cambios y configuración es un procseo que debe ser implementado para garantizar que se usen métodos y procedimientos estandarizados para manejar los cambios eficientemente. Se define cambio como un evento que tiene como resultado un cambio de estado en uno o más ítems de configuración. El cambio debe ser aprobado por la administración, ser eficiente en cuanto al costo y constituir una mejoría a los procesos de negocios con un riesgo mínimo a la infraestructura informática y la seguridad.

Los controles de cambios y configuración deben tratar tres componentes principales: los procesos que tienen como objetivo minimizar la interrupción del sistema y la red, las copias de resguardo y los cambios deshechos que salen mal y orientación sobre la utilización económica del tiempo y los recursos.

Estas son algunas sugerencias para lograr cambios efectivos y seguros a la configuración:

- Asegúrese de que el cambio es implementado de manera ordenada y con pruebas formales
- Asegúrese de que los usuarios finales sean notificados con anticipación del cambio cuando sea necesario
- Analice los efectos del cambio luego de implementarlo

Aunque el proceso de control de cambios difiere de empresa a empresa, ciertos patrones saltan a la vista en la gestión de cambios. Hay cinco pasos en un proceso de control de cambios modelo:

Paso 1. Solicitar la introducción del cambio.

Paso 2. Catalogar el cambio propuesto.

Paso 3. Programar el cambio.

Paso 4. Implementar el cambio.

Paso 5. Reportar el cambio a las partes relevantes.

La seguridad de las operaciones minimiza el daño a la red al proporcionar procesos organizados para el personal de seguridad. Afortunadamente, la efectividad de la solución de seguridad de las operaciones puede ser probada sin necesidad de esperar una amenaza real, gracias a las pruebas de seguridad de red.



9.4.1 Introducción a las pruebas de seguridad de red

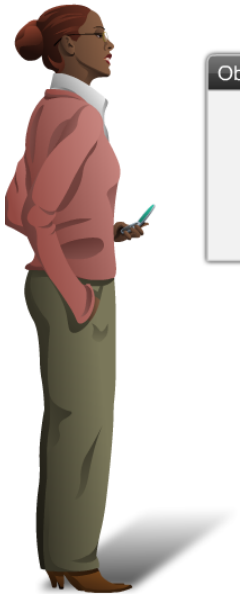
Las pruebas de seguridad de red se realizan para asegurar que todas las implementaciones de seguridad de cierta red estén operando correctamente. Típicamente, las pruebas de seguridad de red son realizadas durante las etapas de implementación y operación, luego de que el sistema ha sido desarrollado, instalado e integrado.

Las pruebas de seguridad ofrecen una profundización en las tareas administrativas como el análisis de riesgos y planes de contingencia. Es importante documentar los resultados de las pruebas de seguridad y que los mismos estén disponibles para el personal en otras áreas de IT.

Durante la etapa de implementación, las pruebas de seguridad se llevan a cabo en partes específicas del sistema de seguridad.

Luego de que la red está enteramente integrada y operativa, se realiza una Prueba y Evaluación de Seguridad (Security Test and Evaluation - ST&E). La ST&E es una prueba o análisis de las medidas de protección que se ubican en la red operativa.

Los exámenes deben repetirse periódicamente cada vez que un cambio es realizado en el sistema. En los sistemas de seguridad que protegen información crítica o hosts expuestos a constantes amenazas, las pruebas de seguridad deben tomar lugar más seguido.



Objetivos de ST&E:

- Descubrir fallas de diseño, implementación y operación que puedan llevar a la violación de la política de seguridad.
- Determinar la adecuación de los mecanismos de seguridad, garantías y propiedades de dispositivos para aplicar la política de seguridad.
- Evaluar el grado de consistencia entre la documentación del sistema y su implementación.

Luego de que una red está operativa, es importante determinar su estado de seguridad. Pueden llevarse a cabo muchas pruebas para evaluar el estado operativo del sistema:

- Escaneo de la red
- Escaneo de vulnerabilidades
- Cracking de contraseñas
- Revisión del registro
- Controladores de integridad
- Detección de virus
- War dialing
- War driving (pruebas de LANs inalámbricas u 802.11)
- Pruebas de penetración

Algunas técnicas de pruebas son predominantemente manuales, mientras que otras están altamente automatizadas. Sin importar el tipo de prueba, el personal que establece y lleva a cabo las pruebas debe tener conocimientos suficientes en las áreas de seguridad y redes, lo que incluye una vasta experiencia en las siguientes áreas: seguridad en redes, firewalls, sistemas de prevención de intrusos (IPSs), sistemas operativos, programación y protocolos de red, como TCP/IP.

Button

Escaneo de vulnerabilidades

Cracking de contrase/b>

Revisiel registro

Controladores de integridad

Deteccie virus

War dialing

War driving (pruebas de LANs inalricas u 802.11)

Pruebas de penetracib>



Escaneo de red

Ejecucie un programa que puede hacer ping a las computadoras, escanearlas en bda de puertos TCP listening y mostra los tipos de recursos disponibles en la red. Algunos programas de escaneo pueden encontrar y reportar nombres de usuario, grupos y recursos compartidos. Los administradores de red pueden usar esta informaciara fortificar sus redes.

Escaneo de vulnerabilidades

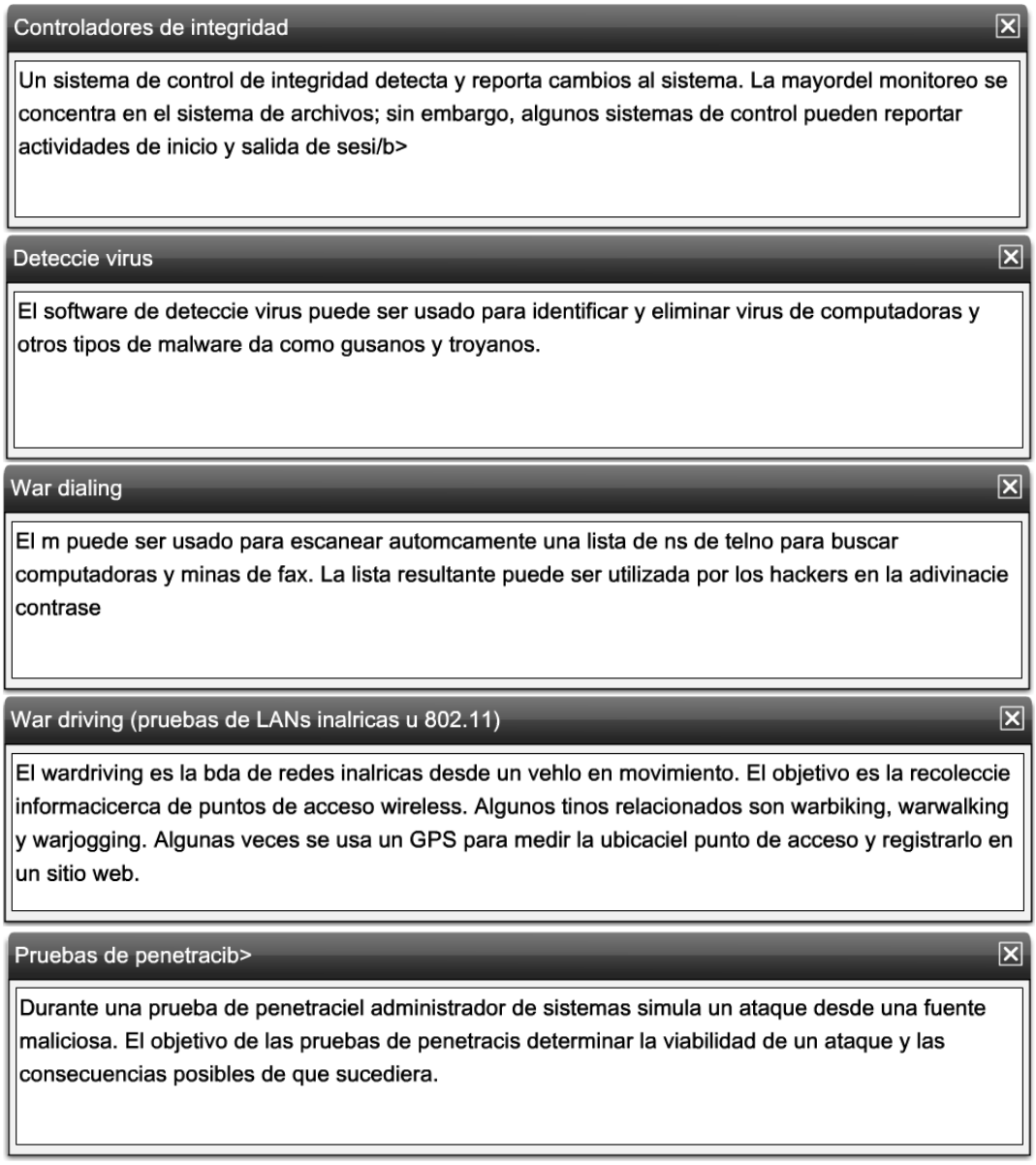
Software de escaneo de vulnerabilidades que puede detectar potenciales debilidades en sistemas probados. Estas debilidades pueden incluir una mala configuracicontraseen blanco o por defecto u objetivos potenciales de ataques DoS. Algunos paquetes de software permiten al administrador intentar colapsar el sistema a travde la vulnerabilidad identificada.

Cracking de contrase/b>

El administrador de sistemas puede usar una herramienta de cracking de contrasepara buscar contraseflmente adivinables. Estas contraseno son seguras y deben ser cambiadas. Las polcas de contrasedeben incluir gu para prevenir el uso de contrasedles.

Revisiel registro

El administrador de sistemas puede revisar los registros de seguridad para identificar potenciales amenazas de seguridad. La actividad de red anormal debe ser investigada. Existen paquetes de software que ayudan en la organizaci evaluacie archivos de registro largos.



Las pruebas de seguridad de red pueden usarse de varias maneras:

- Como punto de referencia para acciones correctivas
- Para definir las actividades de mitigación para tratar vulnerabilidades identificadas
- Como punto de referencia para monitorear el progreso de la empresa en el cumplimiento de los requisitos de seguridad
- Para evaluar el estado de la implementación de los requisitos de seguridad del sistema
- Para llevar a cabo un análisis de costo versus beneficio para mejorías en la seguridad del sistema
- Para mejorar otras actividades como evaluación de riesgos, Certificación y Autorización (Certification and Authorization - C&A) y esfuerzos de mejoras de rendimiento.

9.4.2 Herramientas de pruebas de seguridad de red

Existen muchas herramientas diseñadas para probar la seguridad de los sistemas y redes. Algunas de estas herramientas son de código abierto, mientras que otras son herramientas comerciales que requieren la adquisición de una licencia.

Dos de las herramientas de prueba de seguridad más comúnmente usadas son Nmap y SuperScan.

Nmap
GFI LANguard
Tripwire
Nessus
L0phtcrack
Metasploit
SuperScan



Nmap

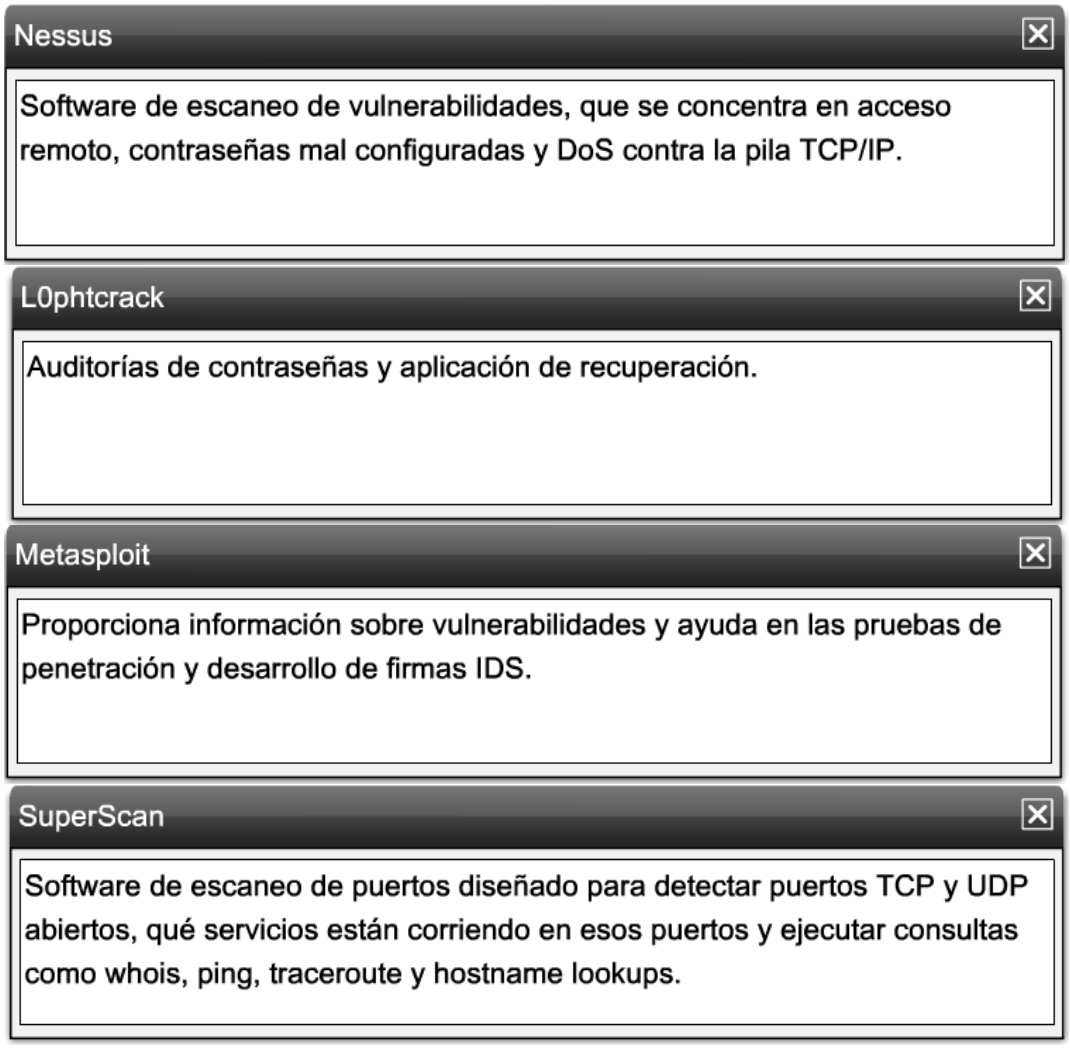
Descubre computadoras y servicios, creando un map de la red.

GFI LANguard

Escáner de red y seguridad que detecta vulerabilidades.

Tripwire

Evalúa y valida configuraciones informáticas contra políticas internas, estándares y buenas prácticas de seguridad.



Nmap

Nmap es el escáner más popular de bajo nivel disponible al público. Es fácil de usar e incluye un rango de funciones excelentes que pueden ser usadas para el mapeo y el reconocimiento de la red. La función básica de Nmap permite a los usuarios completar varias tareas:

- Escaneo clásico de puertos TCP y UDP - búsqueda de diferentes servicios en un solo host.
- Barrido clásico de puertos TCP y UDP - búsqueda del mismo servicio en múltiples hosts.
- Escaneos y barridos sigilosos de puertos TCP y UDP (Stealth scans and sweeps) - similar a los escaneos y barridos clásicos, pero más difíciles de detectar por el host o IPS objetivo.
- Identificación remota del sistema operativo, conocida comúnmente como OS fingerprinting.

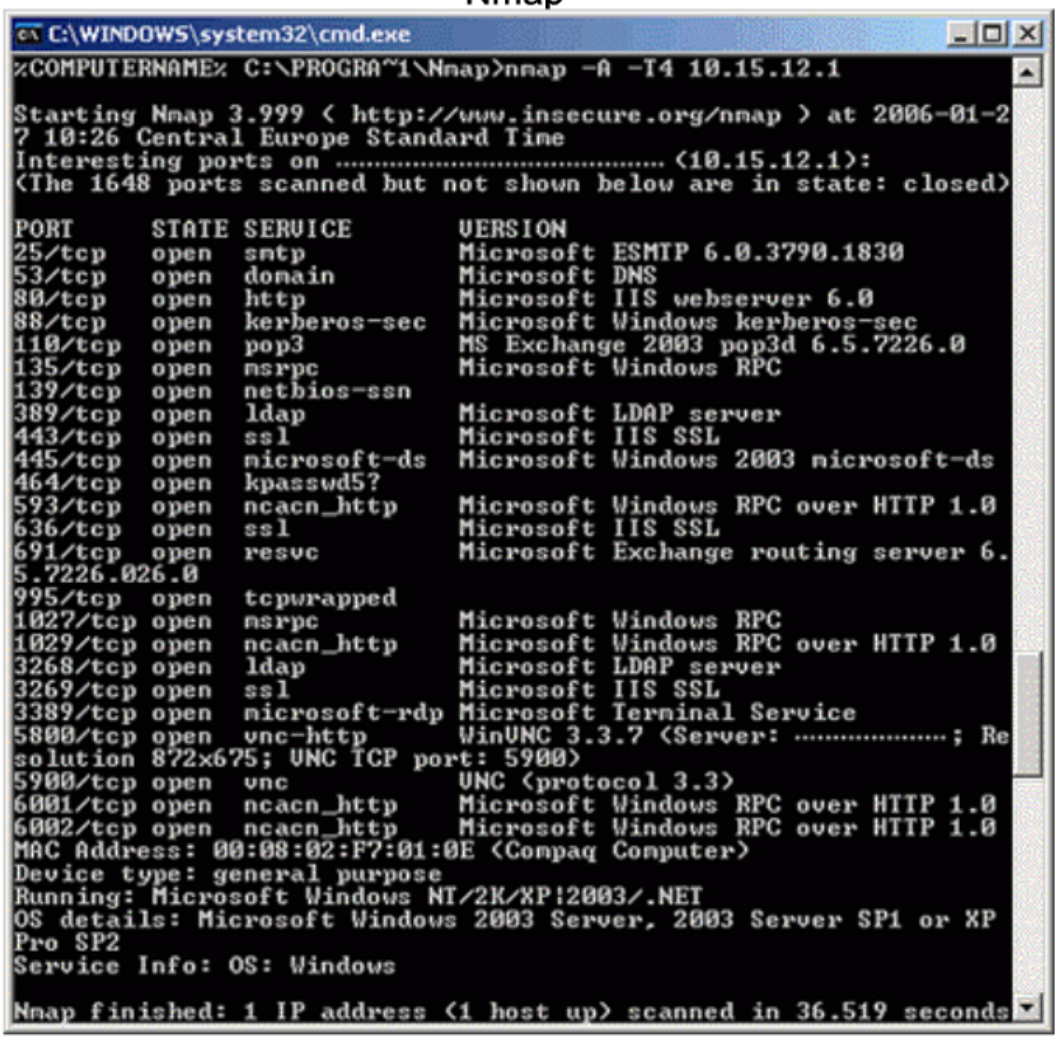
Las funciones avanzadas de Nmap incluyen el escaneo de protocolos, conocido como escaneo de puertos de capa 3. Esta función identifica el soporte de protocolos de capa 3 en el host. Ejemplos de protocolos que pueden ser identificados incluyen GRE y OSPF.

Aunque Nmap puede ser usado para pruebas de seguridad, también puede ser utilizado con fines maliciosos. Nmap tiene una función adicional que le permite usar hosts anzuelo en la misma LAN que el host objetivo para enmascarar el origen del escaneo.

Nmap no tiene funciones de capa de aplicación y puede ejecutarse en UNIX, Linux, Windows y OS X.

Existen tanto una versión de consola como una gráfica; el programa Nmap y la GUI Zenmap pueden ser descargados de Internet.

Nmap



SuperScan

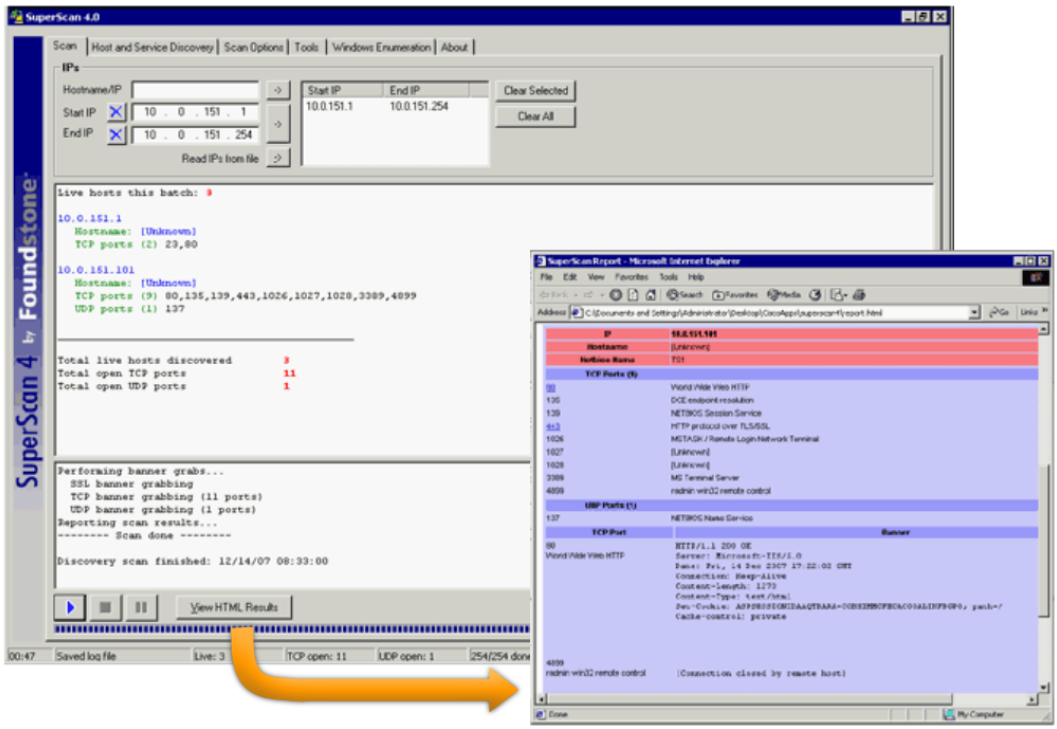
SuperScan es una herramienta de escaneo de Microsoft Windows. Corre en la mayoría de las versiones de Windows y requiere privilegios de administrador. Windows XP SP2 ya no soporta raw sockets, que limitan la habilidad de SuperScan y otras herramientas de escaneo.

Un raw socket es un socket que permite al usuario acceder directamente al encabezado de un paquete de datos y manipularlo.

Aunque SP2 ha mejorado el aspecto de seguridad de esta herramienta, pueden restaurarse algunas funciones con el comando **net stop SharedAccess** ingresado en la línea de comandos de Windows.

SuperScan versión 4 tiene varias funciones muy útiles:

- Velocidad de escaneo ajustable
- Soporte para rangos IP ilimitados
- Detección de hosts mejorada con múltiples métodos ICMP
- Escaneo SYN TCP
- Escaneo UDP (dos métodos)
- Generación simple de reportes de HTML
- Escaneo de puerto de origen
- Resolución rápida de nombre de host
- Banner grabbing exhaustivo
- Extensa base de datos de descripciones de lista de puertos incluida
- Orden aleatorio en los escaneos IP y de puertos
- Varias herramientas útiles (ping, traceroute y whois)
- Gran capacidad de enumeración de hosts Windows



Las herramientas **como Nmap y SuperScan** pueden llevar a cabo pruebas de penetración efectivas en una red y determinar sus vulnerabilidades, mientras ayudan a anticipar posibles mecanismos de ataque. Sin embargo, las pruebas de red no pueden preparar al administrador de red para resolver cada problema de seguridad.

La buena noticia es que las redes se pueden recuperar de la mayoría de los problemas adaptando la solución de seguridad. La mala noticia es que antes de adaptar la solución de seguridad es posible que un ataque cause interrupciones o incluso un daño catastrófico. El daño catastrófico es una interrupción seria de los servicios de red o una destrucción completa de los datos o sistemas de red. El daño catastrófico también puede ser causado por un evento cataclísmico. La empresa debe tener un plan de recuperación y continuar ofreciendo sus servicios si ocurre una interrupción o destrucción de la red.



9.5.1 Planeamiento de Continuidad

El planeamiento de la continuidad de los negocios trata las operaciones continuadas de la organización en caso de un desastre o interrupción prolongada del servicio que afecte a la misión de la organización. Estos planes tratan una fase de respuesta de emergencias, una fase de recuperación y la fase de retorno a las operaciones normales. Estas fases deben incluir un framework de corto a medio plazo para continuar las operaciones de la organización. Cada fase también identifica las responsabilidades del personal y los recursos disponibles durante un incidente.

Los planes de contingencia y recuperación de desastres no tratan cada suposición o escenario posible, sino que se concentran en los eventos más probables e identifican un método aceptable de recuperación. Los planes y procedimientos deben ser ensayados periódicamente para asegurarse de que sean efectivos y bien entendidos.

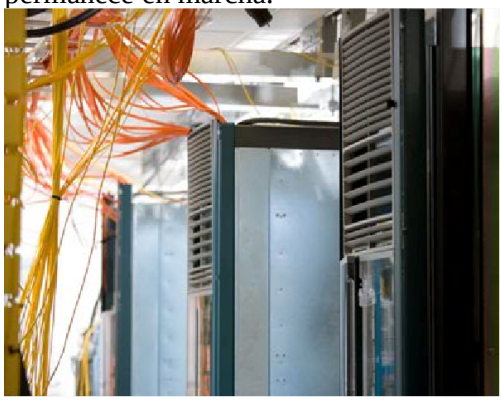
Por ejemplo, el planeamiento de la continuidad de los negocios puede incluir los siguientes:

- Mover o reubicar los componentes y personas críticos al negocio a una ubicación remota mientras la ubicación original se encuentra bajo refacciones
- Usar diferentes canales de comunicación para clientes, socios y accionistas hasta que las operaciones vuelvan a la normalidad



La recuperación de desastres es el proceso por el cual se vuelve a obtener acceso a los datos, el hardware y el software necesario para continuar con las operaciones críticas de negocios luego de un desastre natural o de origen humano. También incluye planes para enfrentarse a la pérdida de empleados clave. El plan de recuperación de desastres es parte del planeamiento de la continuidad de los negocios.

Luego de los eventos del 11 de septiembre de 2001, cuando muchas compañías perdieron datos irremplazables, el esfuerzo que solía ponerse a la protección de los datos cambió. Se estima que algunas empresas gastan hasta un 25 por ciento de su presupuesto de IT en planeamiento de recuperación de desastres para evitar mayores pérdidas. Algunas investigaciones indican que de las compañías que han tenido una pérdida mayor de registros computarizados, 43 por ciento nunca vuelve a abrir, 51 por ciento cierra luego de dos años y sólo 6 por ciento permanece en marcha.



9.5.2 Interrupciones y copias de resguardo

Al planear la recuperación de desastres y la continuidad de los negocios, el primer paso es la identificación de los tipos posibles de desastres e interrupciones. No todas las interrupciones de las operaciones de negocios son

iguales. Un buen plan de recuperación de desastres toma en cuenta la magnitud de la interrupción, reconociendo que existen diferencias entre catástrofes, desastres e incidentes menores.
La única manera de evitar la destrucción es la redundancia. Cuando un componente es destruido, debe ser reemplazado por un componente redundante. Este componente puede ser de emergencia, adquirido por la organización para fines de recuperación de desastres, o un nuevo dispositivo provisto por el proveedor de servicio contratado por la organización. Si el proveedor de servicios es responsable de proporcionar componentes redundantes, esta información debe estar contenida en el acuerdo de nivel de servicios (service level agreement - SLA). El SLA también debe cubrir la redundancia o proporcionar algún tipo de compensación cuando el servicio es interrumpido.

En una escala mucho más grande, la organización puede requerir instalaciones redundantes si un evento catastrófico resulta en la destrucción de las instalaciones originales. Las instalaciones redundantes se conocen como sitios calientes, tibios y fríos.

Cada uno de estos tipos está disponible a precios diferentes con diferentes tiempos de inactividad resultantes. Con los sitios calientes, se requieren instalaciones completamente redundantes con equipamiento casi idéntico. El copiado de los datos a estas instalaciones redundantes es parte de las operaciones normales, por lo que, en caso de una catástrofe, sólo deben aplicarse los cambios de datos más recientes para reiniciar las operaciones enteramente. Las empresas que necesitan responder en segundos generalmente emplean un balanceo de carga global (global load balancing - GLB) y SANs distribuidas para responder rápidamente. Con este tipo de redundancia, la empresa puede recuperarse rápidamente de una interrupción o de una destrucción completa.

Los sitios tibios son instalaciones físicamente redundantes, pero el software y los datos no son almacenados y actualizados en los equipos. Se requiere la asistencia de un equipo de recuperación de desastres para acudir físicamente a las instalaciones redundantes y ponerlas en marcha. Dependiendo de cuánto software y datos esté en juego, puede tomar días antes de volver a las operaciones normales.

El sitio frío generalmente es un centro de datos vació con racks, electricidad, enlaces WAN y calefacción, ventilación y aire acondicionado, pero sin equipamiento. En esta instancia, la organización debe adquirir los routers, switches, firewalls y otro equipamiento para lograr reconstruir todo. Las operaciones podrán restaurarse sólo después de que las copias de resguardo hayan sido subidas al nuevo equipamiento. Esta opción es la menos costosa en términos de dinero anual, pero generalmente toma semanas volver a las operaciones normales.

El tipo de redundancia, sea por equipamiento de emergencia, acuerdos de redundancia SLA o requisitos de redundancia de instalaciones, depende del tipo de desastre que la organización juzgue posible y la sensibilidad al tiempo de los datos críticos. Cuantas más opciones de redundancia ubique la organización, más alto el costo. Sin embargo, no tener planes de resguardo y opciones de

recuperación puede resultar en la pérdida de tanto ingresos como confianza de los clientes.

Es importante considerar que la recuperación de desastres y la continuidad de los negocios no sólo incluyen las opciones de redundancia sino también todos los pasos y personal requeridos pra implementar el plan de resguardo.

9.6.1 Introducción al SDLC

Los planes de continuidad de los negocios y recuperación de desastres son documentos en constante cambio. Deben ser ajustados a cambios en el ambiente, equipamiento y necesidades de los negocios. Estos cambios no solo afectan los planes de continuidad sino todos los aspectos de las operaciones de la red. La documentación debe ser mantenida y actualizada regularmente y las necesidades de seguridad deben ser evaluadas constantemente.

La evaluación de cambios en el sistema y el ajuste de los planes son parte del ciclo de vida del sistema. Tenga en consideración que el término "sistema" puede referirse a un solo dispositivo o a un grupo de dispositivos que operan juntos dentro de la red.



Un ciclo de vida de desarrollo del sistema general (system development life cycle - SDLC) incluye cinco fases:

1. Inicio

2. Adquisición y desarrollo

3. Implementación

4. Operación y mantenimiento

5. Descarte

Al usar el SDLC para diseñar una red, cada fase debe incluir un mínimo de requisitos de seguridad, lo cual resulta en una seguridad menos costosa y más efectiva en comparación con la adición de seguridad a un sistema operativo

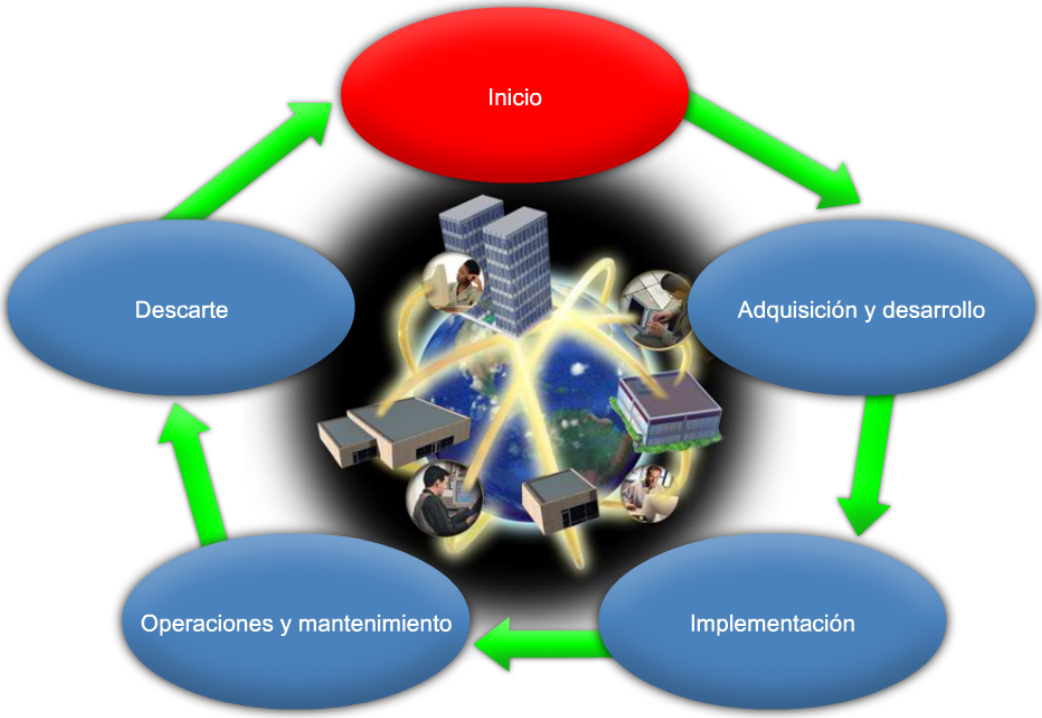
luego del hecho. Esta inclusión intencional de la seguridad en cada fase del ciclo de vida es parte del proceso de administración del ciclo de vida de la red segura.



9.6.2 Fases del SDLC

Estas son las tareas de seguridad relacionadas con la fase de inicio del SDLC:

- **Categorización de seguridad** - Definir tres niveles de impacto potencial a las organizaciones o individuos si hay una brecha de seguridad: bajo, moderado y alto. Los estándares de categorización de seguridad ayudan a las organizacioes a efectuar la elección de controles de seguridad apropiada para sus sistemas de información.
- **Estimación preliminar de riesgos** - Describir inicialmente las necesidades de seguridad básicas del sistema que define el ambiente de amenazas en el que éste opera.



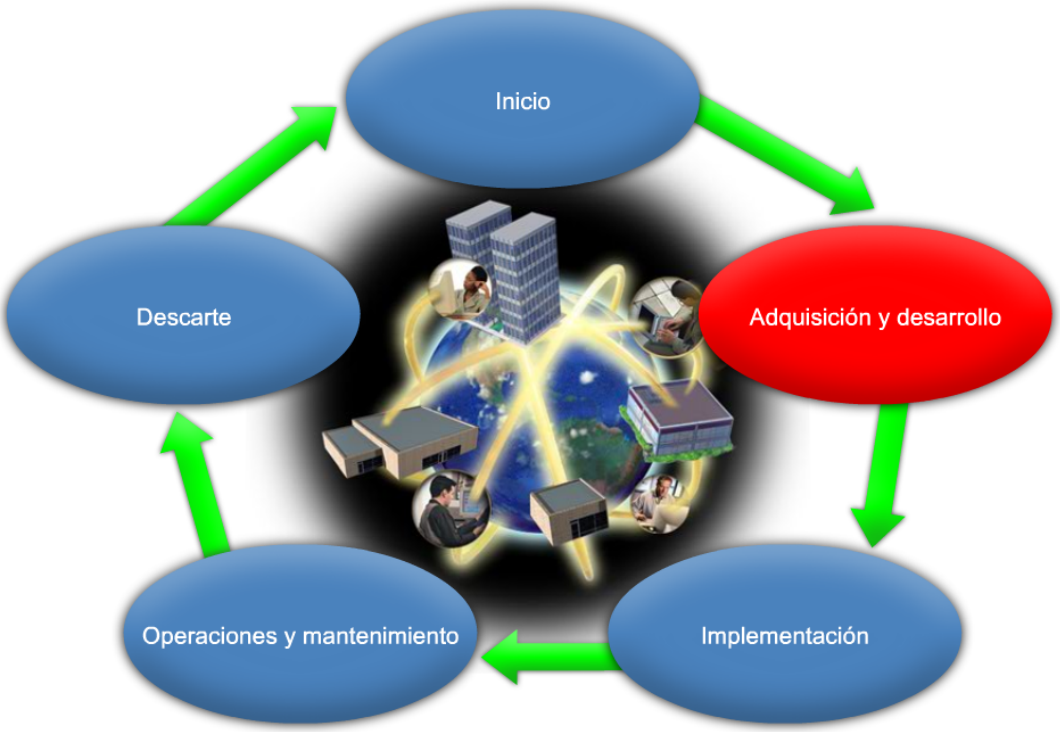
Adquisición y desarrollo

Estas son las tareas de seguridad relacionadas con la fase de adquisición y desarrollo del SDLC:

- Evaluación de riesgos - Identificar los requisitos de protección del sistema a través de un proceso formal de evaluación de riesgos. Este análisis se construye sobre la evaluación de riesgos llevada a cabo en la fase de inicio, pero es más profundo y específico.
- requisitos funcionales de seguridad - Analizar las necesidades operativas al tratar el ambiente de seguridad del sistema, la política de seguridad de la información de la empresa y la arquitectura de seguridad de la empresa.
- requisitos de garantía de seguridad - Tratar las actividades de desarrollo requeridas y la evidencia de garantía necesaria para producir el nivel deseado de confianza en que la seguridad de la información está funcionando correcta y efectivamente. El análisis, basado en requisitos de seguridad legales y funcionales, sirve como base para determinar cuánta y qué tipos de garantías se necesitan.
- Consideración y reporte de costos de seguridad - Determinar qué porción del costo de desarrollo debe destinarse a la seguridad de la información en el ciclo de vida del sistema. Estos costos incluyen hardware, software, personal y capacitación.
- Planeamiento de seguridad - Documento completo de los controles de seguridad acordados. El plan de seguridad también describe con detalle los sistemas de información e incluye adjuntos o referencias a documentos claves que soportan el programa de seguridad de la información de la organización. Ejemplos de documentos que soportan el programa de seguridad de la información incluyen un plan de

administración de configuración, plan de contingencias, plan de respuesta a incidentes, plan de capacitación en seguridad, reglas de comportamiento, evaluación de riesgos, pruebas de seguridad y resultados de evaluaciones, acuerdos de interconexión de sistemas, autorizaciones y acreditaciones de seguridad y un plan de acción e hitos.

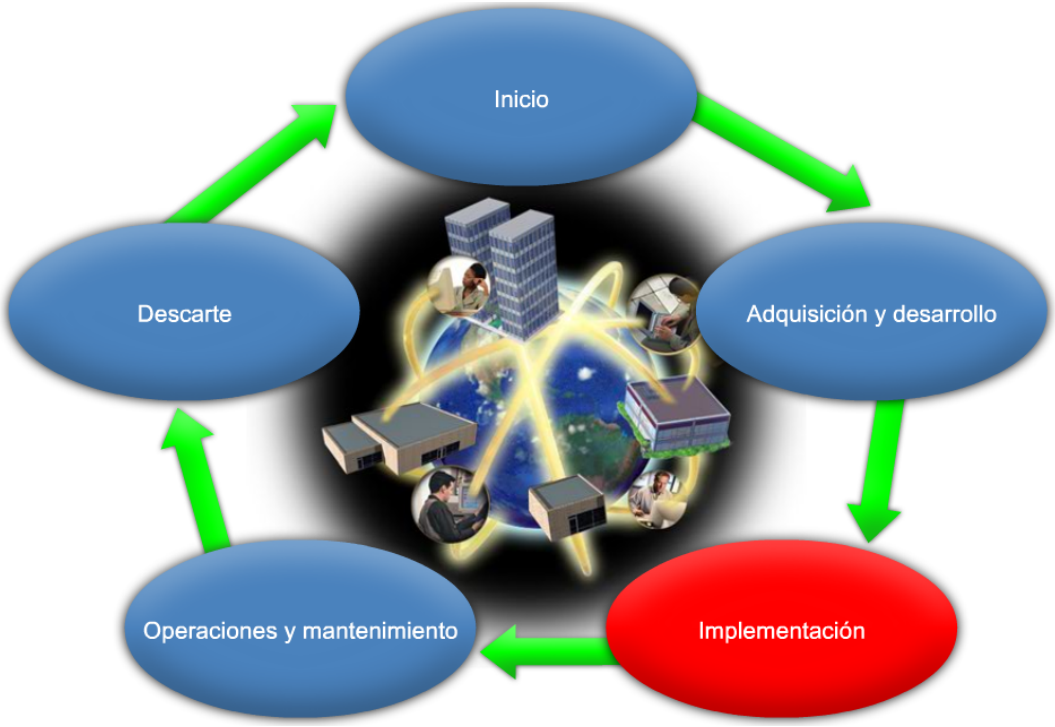
- Desarrollo de un control de seguridad - Asegurarse de que los controles de seguridad descriptos en los planes de seguridad sean diseñados, desarrollados e implementados. Los planes de seguridad de los sistemas de información actualmente operativos pueden necesitar el desarrollo de controles de seguridad adicionales para suplementar los controles ya existentes o la modificación de los controles seleccionados considerados menos efectivos.
- Prueba y evaluación de seguridad del desarrollo - Asegurarse de que los controles de seguridad desarrollados para un nuevo sistema de información estén trabajando correcta y efectivamente. Algunos tipos de controles de seguridad, principalmente aquellos de naturaleza no-técnica, no pueden ser probados y evaluados hasta que el sistema de información esté despleagado. Estos controles son generalmente controles de administración y operaciones.
- Otros componentes de planeamiento - Considerar todos los componentes necesarios para el proceso de desarrollo al incorporar seguridad al ciclo de vida de la red. Estos componentes incluyen el contrato apropiado, la participación de todos los grupos funcionales necesrios dentro de una organización, la participación del certificador y el acreditador y el desarrollo y la ejecución de los planes y procesos de contrato.



Implementación

Estas son las tareas de seguridad relacionadas con la fase de implementación del SDLC:

- Inspección y aceptación - Validar y verificar que la funcionalidad descripta por la especificación esté incluida en las prestaciones.
- Integración del sistema - Asegurarse de que el sistema esté integrado en el sitio operativo donde se despliega el sistema de información. Las configuraciones y switches del control de seguridad deben estar habilitados de acuerdo con las instrucciones del proveedor y las guías de implementación de seguridad disponibles.
- Certificación de seguridad - Usar técnicas y procedimientos de verificación establecidos. Este paso otorga confianza a los empleados de la organización de que se están tomando las precauciones y contramedidas apropiadas. La certificación de seguridad también descubre y describe las vulnerabilidades conocidas del sistema de información.
- Acreditación de seguridad - Proporcionar la autorización de seguridad necesaria para procesar, almacenar y transmitir la información requerida. Esta autorización es otorgada por un empleado superior de la organización y está basada en la efectividad verificada de los controles de seguridad a un nivel acordado de garantía y un riesgo residual identificado dirigido a los bienes u operaciones de la organización.



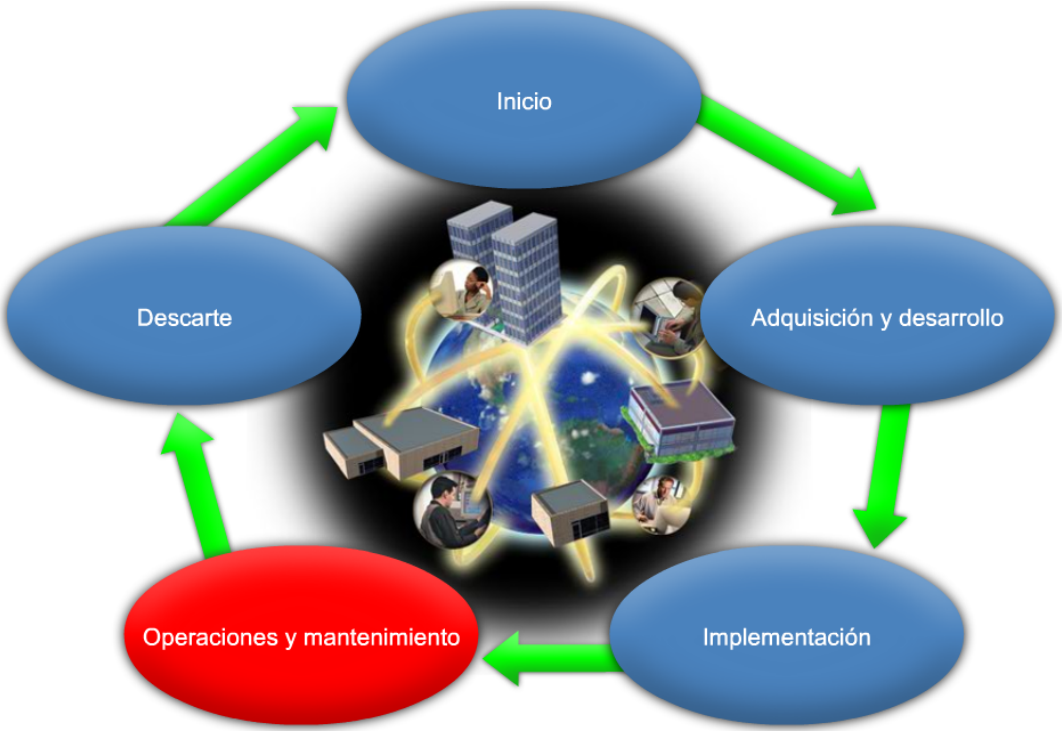
Operaciones y mantenimiento

Estas son las tareas de seguridad relacionadas con la fase de operaciones y mantenimiento del SDLC:

- Administración y control de la configuración - Considerar los potenciales impactos de seguridad que pueden ser causados por cambios específicos a un

sistema de información o su ambiente. Los procedimientos de administración y control de la configuración son críticos para establecer un punto de partida de componentes de hardware, software y firmware y luego controlar y mantener un inventario preciso de los cambios al sistema.

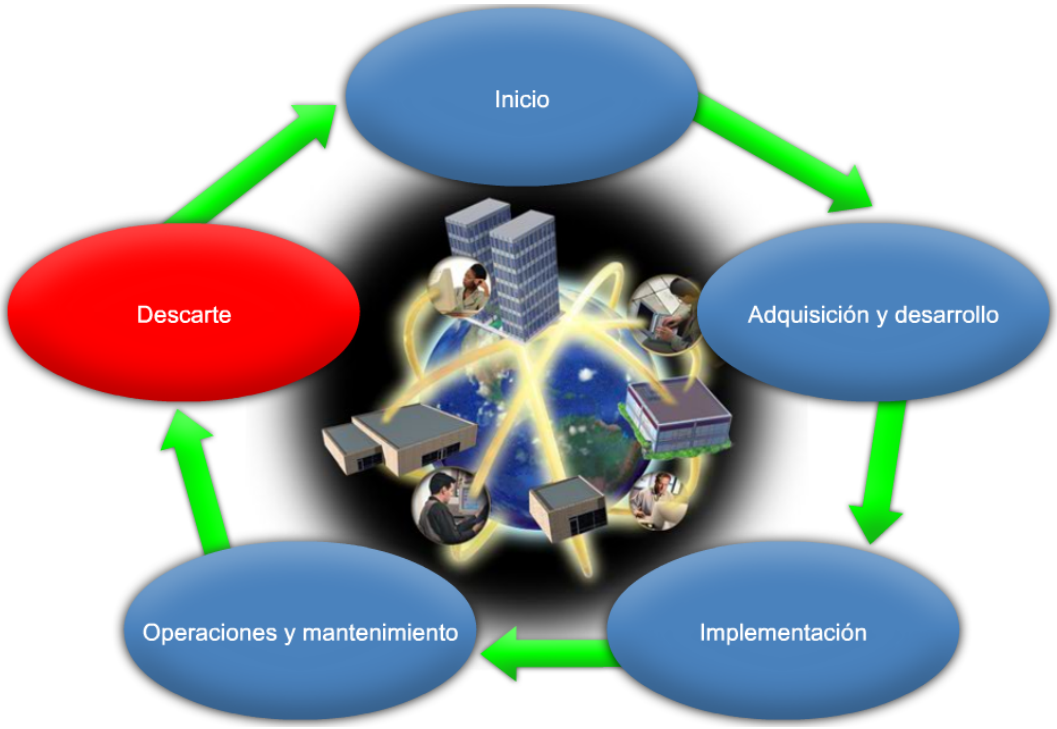
- Monitoreo continuo - Asegurarse de que los controles continúen siendo efectivos por medio pruebas y evaluaciones periódicas. Reportar el estado de seguridad del sistema de información a los empleados apropiados es una actividad esencial en un programa de seguridad de la información exhaustivo.



Descarte

Estas son las tareas de seguridad relacionadas con la fase de descarte del SDLC:

- **Preservación de la información** - Retener información según sea necesario para cumplir con los requisitos legales y hacer lugar a futuros cambios tecnológicos que pueden volver obsoleto al método de recuperación.
- **Saneamiento de los medios** - Asegurarse de que los datos sean eliminados, borrados y sobreescritos según sea necesario.
- **Descarte de hardware y software** - Descartar el hardware y el software según las órdenes del empleado de seguridad del sistema de información.



9.7.1 Generalidades de las políticas de seguridad

El ciclo de vida de red segura es un proceso de revisión y reevaluación de las necesidades de seguridad y de equipamiento a medida que la red cambia. Uno de los aspectos importantes de esta evaluación constante es entender cuáles activos de la organización deben ser protegidos, incluso mientras que los activos cambian.

Determine cuáles son los activos de la organización haciéndose estas preguntas:

- ¿Qué tiene la organización que otros quieren?
- ¿Qué procesos, datos o sistemas de información son críticos para la organización?
- ¿Qué detendría a la organización de seguir con los negocios o cumplir su misión?

Las respuestas pueden identificar activos como bases de datos críticas, aplicaciones vitales, información importante de clientes y empleados, información comercial clasificada, discos compartidos, servidores de correo electrónico y servidores web.

Los sistemas de seguridad en red protegen estos activos, pero un sistema de seguridad por sí solo no puede prevenir que los activos sean vulnerables a amenazas. Todos los sistemas de seguridad técnica, administrativa y física pueden ser vulnerados si la comunidad de usuarios finales no adhiere a las políticas y procedimientos de seguridad.



Las políticas de seguridad están diseñadas para proteger los activos.

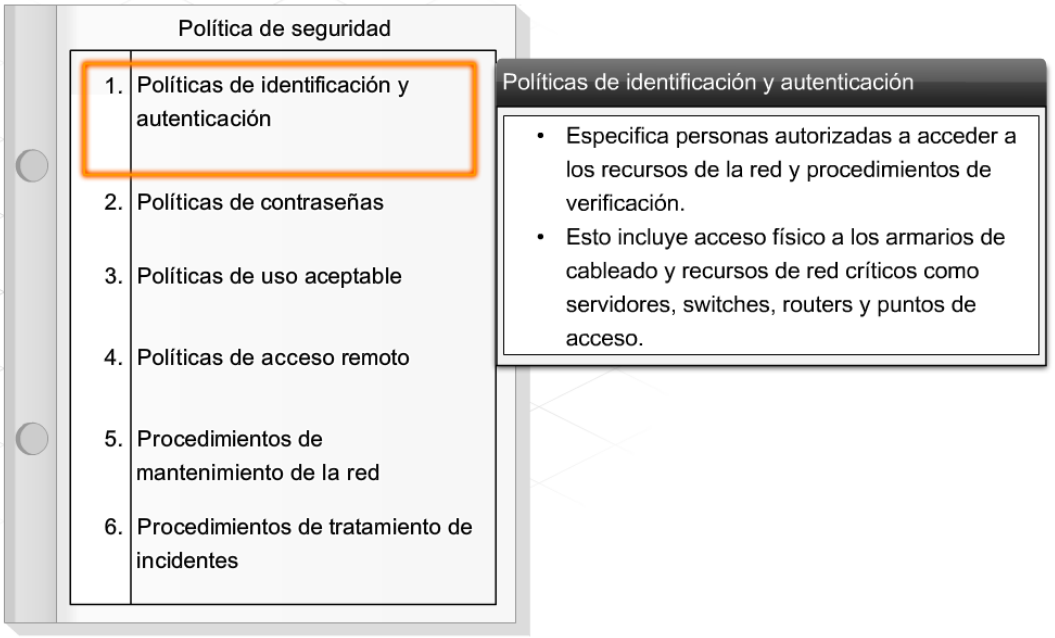
La política de seguridad es un grupo de objetivos de seguridad para una empresa, reglas de comportamiento para los usuarios y administradores y requisitos del sistema. Estos objetivos, reglas y requisitos garantizan colectivamente la seguridad de la red y los sistemas de computación de la empresa. De manera similar a un plan de continuidad, la política de seguridad es un documento en constante evolución basado en los cambios de los requisitos de tecnología, negocios y empleados.

Una política de seguridad exhaustiva tiene varios de beneficios:

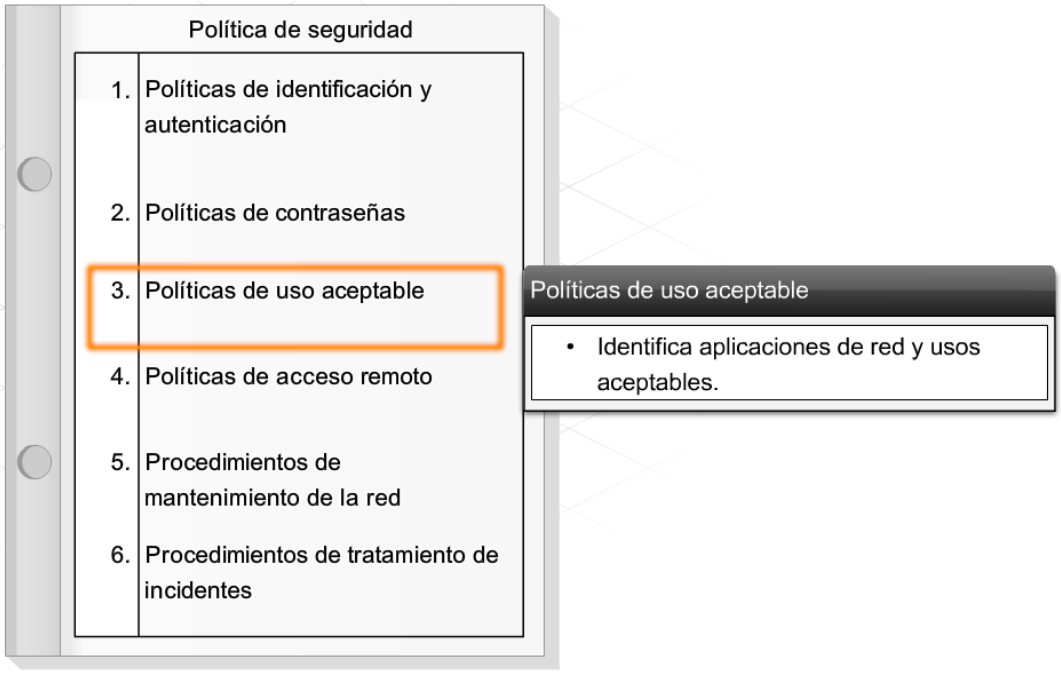
- Demuestra el compromiso de la organización por la seguridad.
- Establece las reglas de comportamiento esperado.
- Garantiza consistencia en las operaciones del sistema, la adquisición y el uso de hardware y software y el mantenimiento.
- Define las consecuencias legales de los actos maliciosos.
- Otorga al personal de seguridad el respaldo de la administración.

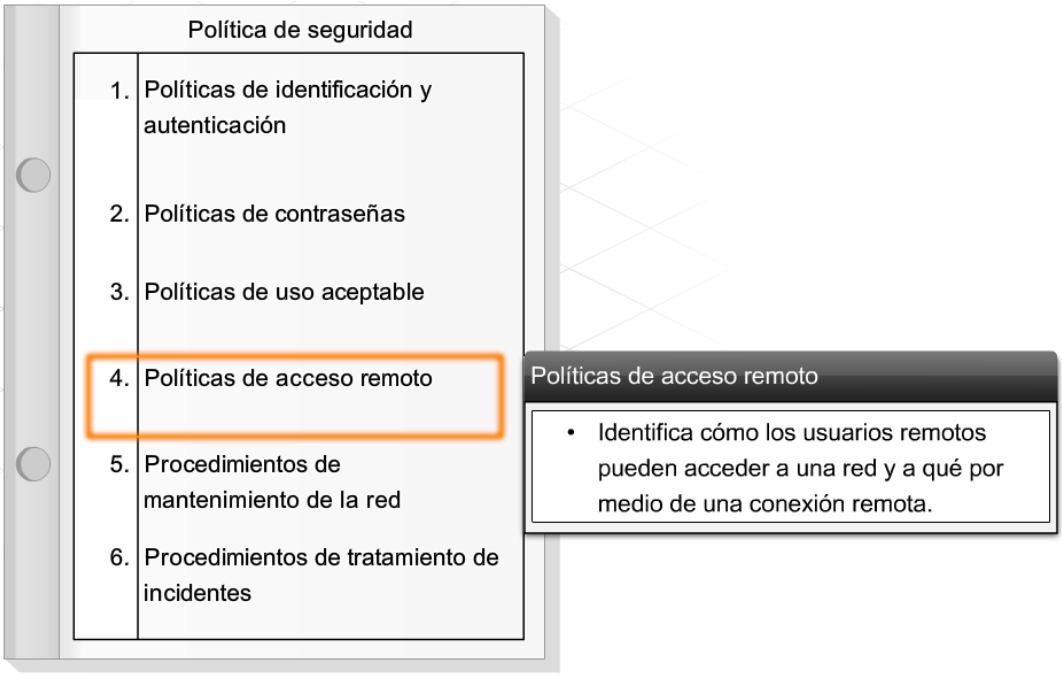
Las políticas de seguridad se usan para informar a los usuarios, al personal y a los administradores de los requisitos de la organización en relación con la protección de la tecnología y los activos de información. La política de seguridad también especifica los mecanismos necesarios para cumplir los requisitos de seguridad y proporciona una base para la adquisición, configuración y auditoría de sistemas de computadoras y redes para revisar su conformidad con la política.

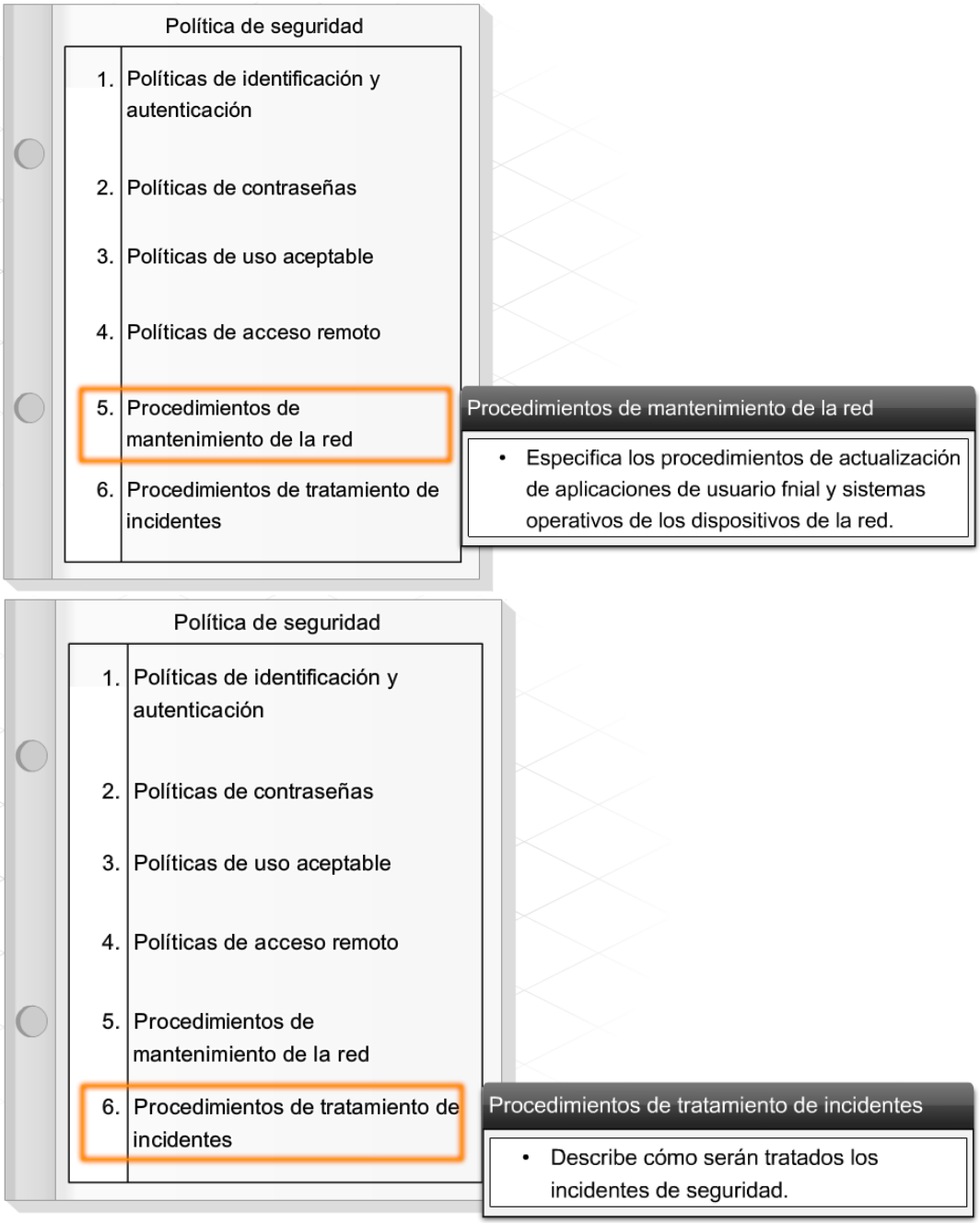
Uno de los componentes de política de seguridad más comunes es una política de uso aceptable o apropiada (AUP). Este componente define lo que se permite hacer a los usuarios en los diferentes componentes del sistema. Esto incluye el tipo de tráfico permitido en la red. La AUP debe ser lo más explícita posible para evitar malentendidos. Por ejemplo, una AUP puede listar sitios web específicos, grupos de noticias o aplicaciones que hacen un uso intensivo del ancho de banda cuya visita está prohibida en las computadoras o la red de la empresa.


Política de seguridad
1. Políticas de identificación y autenticación
2. Políticas de contraseñas
3. Políticas de uso aceptable
4. Políticas de acceso remoto
5. Procedimientos de mantenimiento de la red
6. Procedimientos de tratamiento de incidentes
Políticas de identificación y autenticación
• Especifica personas autorizadas a acceder a los recursos de la red y procedimientos de verificación.
• Esto incluye acceso físico a los armarios de cableado y recursos de red críticos como servidores, switches, routers y puntos de acceso.


Política de seguridad
1. Políticas de identificación y autenticación
2. Políticas de contraseñas
3. Políticas de uso aceptable
4. Políticas de acceso remoto
5. Procedimientos de mantenimiento de la red
6. Procedimientos de tratamiento de incidentes
Políticas de contraseñas
• Asegura que las contraseñas cumplan requisitos mínimos y sean cambiadas regularmente.


Política de seguridad
1. Políticas de identificación y autenticación
2. Políticas de contraseñas
3. Políticas de uso aceptable
4. Políticas de acceso remoto
5. Procedimientos de mantenimiento de la red
6. Procedimientos de tratamiento de incidentes
Políticas de uso aceptable
• Identifica aplicaciones de red y usos aceptables.


Política de seguridad
1. Políticas de identificación y autenticación
2. Políticas de contraseñas
3. Políticas de uso aceptable
4. Políticas de acceso remoto
5. Procedimientos de mantenimiento de la red
6. Procedimientos de tratamiento de incidentes
Políticas de acceso remoto
• Identifica cómo los usuarios remotos pueden acceder a una red y a qué por medio de una conexión remota.



El público objetivo de la política de seguridad es cualquier persona que tenga acceso a la red. El público interno incluye el personal como administradores y ejecutivos, departamentos y unidades de negocios, personal técnico y empleados. El público externo también consta de un grupo variado que incluye socios, clientes, proveedores, consultores y contratistas. Es probable que un documento no pueda satisfacer las necesidades de todo el público de una organización grande. La meta es asegurarse de que los documentos de política de seguridad sean consistentes con las necesidades del público objetivo.

El público detemina el contenido de la política. Por ejemplo, probablemente sea innecesario incluir una descripción de por qué algo es necesario en una política dirigida al personal técnico, ya que puede asumirse que ya conocen por qué se

incluye ese requisito particular. Los administradores probablemente no estarán muy interesados en los aspectos técnicos de la necesidad de un requisito particular. En cambio, querrán un resumen de alto nivel de los principios sobre los que se basa el requisito. Los empleados generalmente requieren más información sobre la necesidad de reglas de seguridad particulares. Si entienden las razones por las cuales se establecen las reglas, será más probable que las cumplan.



Administración



Usuario final

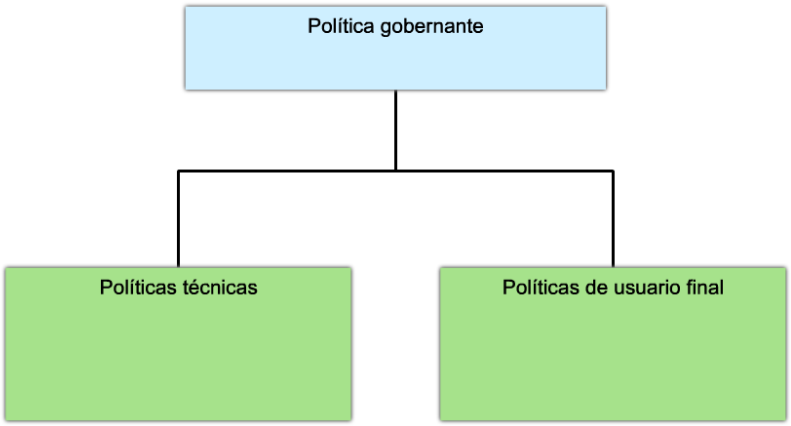


Ingeniero

9.7.2 Estructura de la política de seguridad

La mayoría de las empresas usa un conjunto de políticas para satisfacer la variedad de necesidades. Estos documentos generalmente tienen una estructura jerárquica:

- **Política gobernante** - El tratamiento de alto nivel de las guías de seguridad que son importantes para toda la compañía. Los administradores y el personal técnico son el público objetivo. La política gobernante controla todas las interacciones relacionadas con la seguridad entre las unidades de negocios y departamentos de la compañía.
- **Política técnica** - Usada por el personal de seguridad para llevar a cabo responsabilidades de seguridad del sistema. Este tipo de política es más detallada que la política gobernante y es más específica en relación con el sistema o el problema que trata. Por ejemplo, puede describir cuestiones de control de acceso y seguridad física.
- **Política de usuario final** - Cubre todas las cuestiones de seguridad que son importantes para los usuarios finales. Estos pueden ser empleados, clientes y cualquier otro usuario individual de la red.



Política gobernante

La política gobernante describe los objetivos generales de seguridad de la empresa a los administradores y el personal técnico. Cubre todas las interacciones relacionadas con la seguridad entre las unidades de negocios y departamentos de la compañía.

La política gobernante se alinea con las políticas existentes de la compañía y tiene la misma importancia que estas otras políticas (políticas de recursos humanos y otras que mencionen cuestiones de seguridad, como correo electrónico, uso de computadoras u otros temas relacionados con la informática).

Las políticas gobernantes incluyen varios componentes:

- Declaración del tema que la política trata
- Cómo se aplica la política al ambiente
- Roles y responsabilidades de los afectados por la política
- Acciones, actividades y procesos permitidos y prohibidos
- Consecuencias del incumplimiento

Política técnica

Las políticas técnicas son documentos detallados utilizados por el personal técnico para cumplir con sus responsabilidades de seguridad diarias. Estas políticas son específicas de cada sistema y cuestión a tratar, como la seguridad del router y la seguridad física. En esencia, son manuales de seguridad que describen lo que el personal técnico debe hacer, pero no cómo los individuos realizan sus funciones.

Las políticas técnicas se subdividen en áreas técnicas específicas que incluyen:

- General
- Correo electrónico
- Acceso remoto
- Telefonía
- Uso de aplicaciones
- Uso de la red
- Comunicaciones inalámbricas



Políticas Generales

- AUP: Define el uso aceptable de los servicios de computación y equipamiento, como correo electrónico, y las medidas apropiadas de seguridad que los empleados deben tomar para proteger los recursos de la empresa y la información propietaria.
- Política de solicitud de acceso y cuentas: Formaliza el proceso de solicitud de acceso y cuentas dentro de la organización. Los usuarios y administradores de sistema que ignoren los procesos estándar de solicitudes de cuenta y acceso pueden causar acciones legales contra la empresa.
- Política de evaluación de adquisiciones: Define las responsabilidades relacionadas con las adquisiciones de la empresa y los requisitos mínimos que deben ser cumplidos por el grupo de seguridad de la información para una evaluación de adquisición.
- Política de auditorías: Lleva a cabo auditorías y evaluaciones de riesgos para asegurar la integridad de la información y los recursos, investiga incidentes, garantiza la conformidad con políticas de seguridad y monitorea la actividad de los usuarios y el sistema cuando sea apropiado.
- Política de sensibilidad de la información: Define los requisitos de clasificación y aseguración de información de manera apropiada para su nivel de sensibilidad.
- Política de contraseña: Define los estándares de creación, protección y renovación de contraseñas fuertes.
- Política de evaluación de riesgos: Define los requisitos y proporciona la autoridad al equipo de seguridad de la información para identificar, evaluar y mitigar riesgos a la infraestructura de información asociada con los negocios en marcha.
- Política de servidor web global: Define los estándares requeridos por todos los hosts web.

Políticas de acceso remoto

- Política de acceso dial-in: Define el eacceso dial-in apropiado y su uso por personal autorizado.
- Política de acceso remoto: Define los estándares para conectarse a la red de la organización desde cualquier host o red externos a la organización.
- Política de seguridad de red privada virtual (VPN): Define los requisitos para IP Security (IPSec) de acceso remoto u otras conexiones VPN a la red de la organización.

Políticas de aplicación

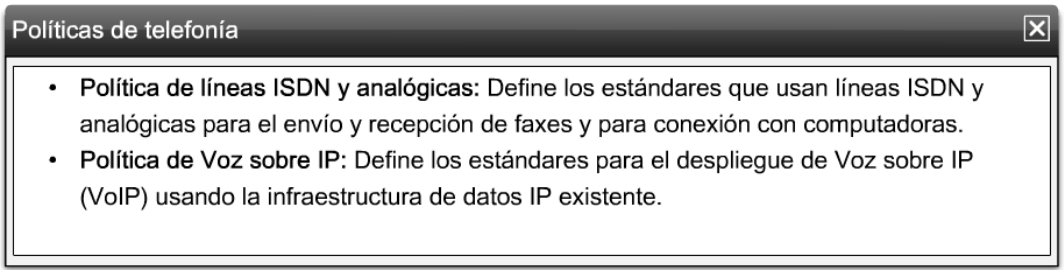
- Política de cifrado aceptable: Define los requisitos para los algoritmos de cifrado de la organización.
- Política de proveedor de servicio de aplicación (ASP): Define los criterios mínimos de seguridad que el ASP debe ejecutar antes de que la organización lo utilice en un proyecto.
- Política de codificación de credenciales de base de datos: Define los requisitos para almacenar y recuperar con seguridad los nombres de usuario y contraseñas de las bases de datos.
- Políticas de comunicaciones interproceso: Define los requisitos de seguridad que dos o más procesos deben cumplir para comunicarse entre sí usando un socket de red o de sistema operativo. Por ejemplo, solicitar el uso de HTTPS.
- Política de seguridad de proyectos: Define los requisitos de los administradores de proyectos para revisar todos los proyectos en búsqueda de posibles requisitos de seguridad.
- Política de protección del código fuente: Establece requisitos mínimos de seguridad de la información para administrar el código fuente de un producto.

Políticas de comunicación inalámbrica

- Política de uso: Define los estándares para sistemas inalámbricos usados para conectarse a la red.

Política de correo electrónico

- Política de correo electrónico reenviado automáticamente: Define las reglas para habilitar el reenvío automático de correo electrónico a otra cuenta. Generalmente, esta política restringe el reenvío automático de correo electrónico a un destino externo sin aprobación previa del administrador o director apropiado.
- Política de correo eletrónico: Define los estándares de uso del correo electrónico. La creación, distribución y recepción de SPAM puede ser cubierta aquí como en el AUP.



Política de Red

- Política de extranet: Define los requisitos de una organización de un tercero cuando ese tercero debe acceder a la red. Esto generalmente incluye firmar un acuerdo de conexión con el tercero.
- Requisitos mínimos para la política de acceso a la red: Define los estándares y requisitos para cualquier dispositivo que requiera conectividad a la red interna.

- Estándares de acceso a la red: Definen los estándares para la seguridad del acceso físico a los puertos en todos los puertos de datos de una red cableada o inalámbrica.
- Política de seguridad de routers y switches: Define los estándares mínimos de configuración de seguridad para routers y switches dentro de la red o ubicados en un ambiente de producción.
- Política de seguridad de servidores: Define los estándares mínimos de configuración de seguridad para servidores dentro de la red o ubicados en un ambiente de producción.

Política de usuario final

Las políticas de usuario final cubren todas las reglas relacionadas con la seguridad de la información que los usuarios finales deben conocer y seguir. Las políticas de usuario final pueden superponerse con las políticas técnicas. Estas políticas generalmente se agrupan en un solo documento para facilitar su uso.

Muchos grupos destino diferentes requieren políticas de usuario final, y cada grupo puede tener que aceptar una política de usuario diferente. Por ejemplo, la política de usuario final de los empleados puede ser diferente de la de los clientes.



Cliente



Empleado



Socio

9.7.3 Estándares, guías y procedimientos

Las políticas de seguridad son documentos de resumen de alto nivel. El personal de seguridad utiliza documentos detallados para implementar las políticas de seguridad. Estos incluyen los estándares, guías y procedimientos.

Los estándares, guías y procedimientos son los que contienen los detalles de lo definido en las políticas. Cada documento sirve a una función diferente, cubre especificaciones diferentes y apunta a un público diferente. Separar estos documentos facilita su actualización y mantenimiento.



Documentos estándar

Los estándares ayudan al personal informático a mantener consistencia en las operaciones de la red. Los estándares incluyen las tecnologías necesarias para usos específicos, los requisitos de versión de hardware y software, requisitos de programas y cualquier otro criterio que debe seguirse en la organización. Esto ayuda al personal informático a mejorar la eficiencia y la simplicidad en el diseño, el mantenimiento y la resolución de problemas.

Uno de los principios de seguridad más importantes es la consistencia. Por esta razón, es necesario que las organizaciones establezcan estándares. Cada organización desarrolla estándares para soporar su ambiente operativo único. Por ejemplo, si una organización soporta 100 routers, es importante que los 100 routers estén configurados bajo los estándares establecidos. Los estándares de configuración de dispositivos están definidos en la sección técnica de la política de seguridad de la organización.

Documentos guía

Las guías proporcionan listas de sugerencias sobre cómo mejorar las cosas. Son parecidas a los estándares pero más flexibles y no tan obligatorias. Las guías pueden ser usadas para definir cómo se desarrollan los estándares y para garantizar adherencia a las políticas de seguridad en general.

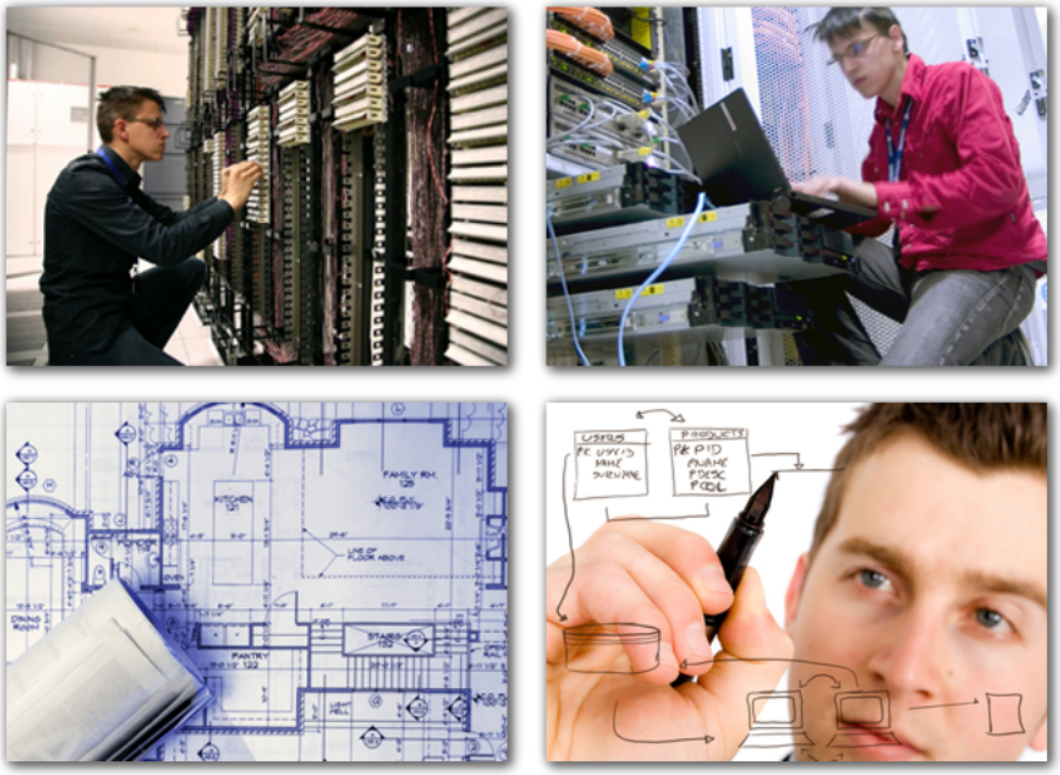
Algunas de las guías más útiles, que pueden ser halladas en los repositorios de las organizaciones, son denominadas buenas prácticas. Además de las buenas prácticas definidas por la organización, hay varias guías disponibles:

- El Computer Security Resource Center del National Institute of Standards and Technology (NIST)
- Las guías de configuración de seguridad de la National Security Agency (NSA)
- El estándar Common Criteria



Documentos de procedimientos

Los documentos de procedimientos son más largos y detallados que los estándares y las guías. Los documentos de procedimients incluyen detalles de implementación, generalmente instrucciones y gráficos paso a paso. Los documentos de procedimientos son extremadamente importantes en organizaciones grandes para proporcionar la consistencia de despliegue necesaria en un ambiente seguro.



9.7.4 Roles y responsabilidades

Todas las personas que forman parte de una organización, desde el CEO (chief executive officer) hasta los empleados más recientes, son consideradas usuarios finales de la red y deben adherir a la política de seguridad de la organización. El

desarrollo y mantenimiento de la política de seguridad se delega a roles específicos dentro del departamento de IT.

Siempre debe consultarse a los administradores de nivel ejecutivo durante la creación de la política de seguridad para asegurar que ésta sea exhaustiva, cohesiva y legalmente vinculante. Las organizaciones más pequeñas pueden tener solo un puesto ejecutivo que supervise todos los aspectos de las operaciones, incluyendo las operaciones de la red. La estructura de negocios y reportes de la organización depende del tamaño e industria de la organización.

Algunos de los títulos ejecutivos más comunes incluyen:

- Chief Executive Officer (CEO) - Es directamente responsable del éxito de la organización. Todos los empleados executivos dependen del CEO.
- Chief Technology Officer (CTO) - Identifica y evalúa nuevas tecnologías y maneja su desarrollo para alcanzar las metas de la organización. Mantiene y mejora los sistemas actuales de la empresa, mientras que dirige todas las cuestiones relacionadas con la tecnología en soporte de las operaciones.
- Chief Information Officer (CIO) - Responsable de los sistemas informáticos y computacionales que soportan las metas de la empresa, incluyendo un despliegue exitoso de nuevas tecnologías y procesos de trabajo. Las organizaciones medianas y pequeñas típicamente combinan las responsabilidades del CTO y el CIP en una sola persona que puede usar cualquiera de los dos títulos. Si la organización tiene tanto un CIO como un CTO, el CIO generalmente es el responsable de los procesos y las prácticas que soportan el flujo de la información, mientras que el CTO es el responsable de la infraestructura tecnológica.
- Chief Security Officer (CSO) - Desarrolla, implementa y administra la estrategia, los programas y los procedimientos de seguridad de la organización asociados con todos los aspectos de la operación de los negocios, incluyendo la propiedad intelectal. Una tarea crítica realizada por la persona que tenga este título es limitar la exposición a la responsabilidad en áreas de riesgo financiero, físico y personal.
- Chief Information Security Officer (CISO) - Parecido al CSO, excepto que este título se concentra específicamente en la seguridad informática. Una de las responsabilidades más críticas del CISO es el desarrollo y la implementación de la política de seguridad. El CISO puede elegir ser el autor principal de la política de seguridad o delegar a alguien la autoría. De cualquier manera, el CISO será responsable del contenido de la política de seguridad.

9.7.5 Concientización y capacitación en seguridad

La seguridad técnica, administrativa y física puede ser fácilmente pasada por alto si la comunidad de usuarios finales no se acata a las políticas de seguridad. Para ayudar a asegurar el cumplimiento de la política de seguridad, debe llevarse a cabo un programa de concientización en seguridad. Los líderes deben desarrollar un programa que mantenga a todos concientes de las cuestiones de seguridad y capacite al personal en relación a cómo trabajar juntos para mantener la seguridad de sus datos.

El programa de concientización en seguridad refleja las necesidades de negocios de la organización atenuadas por riesgos conocidos. Informa a los usuarios sobre sus responsabilidades en la seguridad informática y explica las reglas de comportamiento requeridas para el uso de los datos y sistemas informáticos dentro de la empresa. Este programa debe explicar todas las políticas y procedimientos informáticos. El programa de concientización en seguridad es crucial para el éxito financiero de cualquier organización. Disemina la información que todos los usuarios finales necesitan para conducir los negocios con eficacia al tiempo que protegen a la organización de pérdidas de capital intelectual, datos críticos e incluso equipamiento físico. El programa de concientización en seguridad también detalla las sanciones que la organización impondrá al incumplimiento. Esta porción del programa debe ser parte de las capacitaciones ofrecidas a los nuevos empleados.

Los programas de concientización en seguridad generalmente tienen dos componentes principales:

- Campañas de concientización
- Capacitación y educación

Campañas de concientización

Las campañas de concientización generalmente están dirigidas a todos los niveles de la organización, incluyendo los puestos ejecutivos.

Los esfuerzos de concientización en seguridad están diseñados para cambiar el comportamiento o reforzar las buenas prácticas de seguridad. La concientización está definida en la NIST Special Publication 800-16 de la siguiente manera: "La concientización no es una capacitación. El propósito de las presentaciones de concientización es simplemente el de concentrar la atención en la seguridad. La concientización pretende permitir a los individuos reconocer los problemas de seguridad informática y responder de acuerdo con la situación dada. Durante las actividades de concientización, el alumno recibe información... La concientización trata de llegar a públicos numerosos usando técnicas de presentación atractivas."

Un ejemplo de un tema que puede tratarse durante una sesión de concientización (o material de concientización que puede distribuirse) es la protección contra virus. El tema puede ser tratado brevemente mediante la descripción de un virus, qué debe hacer el usuario para proteger el sistema y cómo actuar si descubre un virus.

Hay muchos métodos que permiten mejorar la conciencia en seguridad:

- Charlas, videos
- Carteles, artículos y boletines informativos
- Premios otorgados por buenas prácticas de seguridad
- Recordatorios, como banners al inicio de la sesión, mouse pads, tazas de café y anotadores



Capacitación y educación

La capacitación busca impartir las habilidades de seguridad necesarias a los usuarios finales que pueden ser o no miembros del personal informático. La diferencia más significativa entre la concientización y la capacitación es que ésta última enseña habilidades que permite a la persona realizar una tarea específica, mientras que la concientización sólo se concentra en los problemas de seguridad. Las habilidades que adquieren los usuarios durante la capacitación se construyen sobre la base de la información adquirida en las campañas de concientización en seguridad. Continuar la campaña de concientización en seguridad con una capacitación dirigida a públicos específicos ayuda a consolidar la información presentada y las habilidades impartidas. El contenido de la capacitación no debe necesariamente llevar a un título formal de una institución de altos estudios, pero puede contener muchos de los temas tratados en materias de algunas carreras terciarias o universitarias.

Un ejemplo de un curso de capacitación para personal no-informático es uno que trate prácticas de seguridad apropiadas específicas de las aplicaciones que el usuario final debe usar, como bases de datos. Un ejemplo de capacitación de personal informático es un curso de seguridad que trata en detalle los controles de administración, operativos y técnicos que deben ser implementados.

Un curso de capacitación en seguridad efectivo requiere planeamiento, implementación, mantenimiento y evaluación periódica apropiados. El ciclo de vida de un curso de capacitación en seguridad consta de varios tipos:

Paso 1. Identifique el alcance, las metas y los objetivos del curso. El alcance del curso proporciona capacitación a todas las personas que interectúan con los sistemas informáticos. Como los usuarios necesitan una capacitación que se relacione directamente con su uso de un sistema en particular, es necesario suplementar el programa que abarca toda la organización con cursos más específicos de cada sistema.

Paso 2. Identifique y eduque al personal de capacitación. Es importante que los que capaciten tengan conocimientos suficientes de problemas, principios y técnicas relativos a la seguridad de las computadoras. También es imperativo que sepan cómo comunicar información e ideas efectivamente.

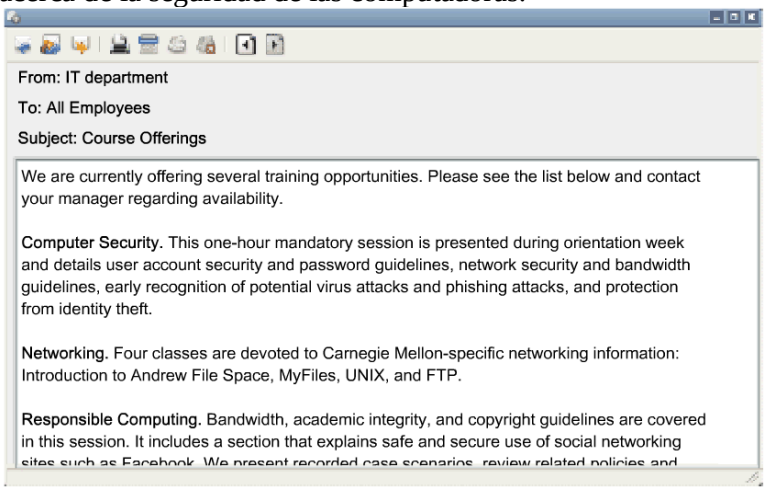
Paso 3. Identifique su público destino. No todos necesitan el mismo grado o tipo de información de seguridad de computadoras para realizar una tarea asignada. Los cursos de capacitación en seguridad que presentan sólo la información necesaria por un público en particular y omiten información irrelevante obtienen los mejores resultados.

Paso 4. Motive a la administración y los empleados. Considere usar técnicas de motivación para demostrar a la administración y los empleados que su participación en un curso de capacitación beneficia a la organización.

Paso 5. Administre los cursos. Algunas consideraciones importantes para administrar el curso incluyen la selección de métodos, temas, materiales y técnicas de presentación de capacitación apropiados.

Paso 6. Mantenga los cursos. Manténgase informado en relación con cambios en los requisitos de seguridad y tecnología de computadoras. Los cursos de capacitación que hoy satisfacen las necesidades de la organización pueden volverse obsoletos cuando la organización empiece a usar una nueva aplicación o cambie su ambiente, mediante, por ejemplo, el despliegue de VoIP.

Paso 7. Evalúe los cursos. Las evaluaciones buscan establecer cuánta información es retenida, si se están siguiendo los procedimientos de seguridad y la actitud general acerca de la seguridad de las computadoras.


From: IT department

To: All Employees

Subject: Course Offerings

We are currently offering several training opportunities. Please see the list below and contact your manager regarding availability.

Computer Security. This one-hour mandatory session is presented during orientation week and details user account security and password guidelines, network security and bandwidth guidelines, early recognition of potential virus attacks and phishing attacks, and protection from identity theft.

Networking. Four classes are devoted to Carnegie Mellon-specific networking information: Introduction to Andrew File Space, MyFiles, UNIX, and FTP.

Responsible Computing. Bandwidth, academic integrity, and copyright guidelines are covered in this session. It includes a section that explains safe and secure use of social networking sites such as Facebook. We present recorded case scenarios, review related policies and

La educación integra todas las habilidades y competencias de seguridad de las especialidades funcionales a un corpus común de conocimientos, agrega un estudio multidisciplinario de conceptos, problemas y principios (tecnológicos y sociales) y busca producir especialistas y profesionales de la seguridad informática capaces de visión y respuesta proactiva.

Un ejemplo de un programa educativo es una carrera terciaria o universitaria. Algunas personas cursan uno o varios cursos para desarrollar o mejorar sus habilidades en una disciplina particular. Esto es lo que se llama capacitación, en contraste con la educación. Muchos institutos terciarios y universidades ofrecen programas de certificación, en los que el estudiante puede tomar una o dos clases relacionadas con su disciplina y obtener un certificado. Generalmente, estos programas de certificación son colaboraciones entre las escuelas y los proveedores de hardware y software. Estos programas son más

característicos de la capacitación que de la educación. Los responsables de la capacitación de seguridad deben evaluar ambos tipos de programas y decidir cuál satisface mejor sus necesidades identificadas.

Un programa de concientización en seguridad exitosamente implementado reduce considerablemente las acciones no autorizadas de los usuarios, mejora la efectividad de los controles existentes y ayuda a combatir el desperdicio, fraude y abuso de recursos de sistemas de información.



9.7.6 Leyes y ética

Leyes

En muchas de las empresas de hoy en día, una de las consideraciones más importantes en el establecimento de políticas de seguridad y la implementación de programas de concientización es el cumplimiento de la ley. Los profesionales de la seguridad en redes deben estar familiarizados con las leyes y los códigos de ética que son vinculantes para los profesionales de la seguridad de los sistemas de información. La mayoría de los países tienen tres tipos de leyes: criminales, civiles (también llamadas tort) y administrativas.

Las leyes criminales están relacionadas con los crímenes y sus penas generalmente involucran multas o prisión, o ambas.

Las leyes civiles se concentran en corregir las situaciones en las que las entidades han sido dañadas y una compensación económica puede ayudar. La prisión no es posible en la ley civil. Un ejemplo de una ley civil es el caso en el que una empresa demanda a otra empresa por infringir una patente. La pena en la ley civil es generalmente monetaria, aunque también puede haber requisitos de actuación, como dejar de infringir la patente.

Las leyes administrativas guardan relación con la aplicación de las regulaciones por parte de las agencias gubernamentales. Por ejemplo, una empresa puede deber a sus empleados el pago de sus vacaciones. La corte administrativa puede forzar a la empresa a pagar a sus empleados y elevar una multa pagable a la corte.

No todos los gobiernos aceptan o clasifican sus leyes de la misma manera. Esto puede impedir llevar a juicio a los criminales de computadoras o redes que crucen fronteras internacionales.

Ética

La ética es un estándar que rige por sobre la ley. Es un grupo de principios morales que gobiernan el comportamiento civil. Los principios éticos generalmente son la base de muchas de las leyes que están actualmente vigentes. Estos principios generalmente se formalizan en códigos de ética. Los individuos que violen los códigos de ética pueden enfrentar consecuencias como pérdidas de certificaciones, pérdida de su empleo o incluso jucios en cortes criminales o civiles. La profesión de la seguridad de la información tiene un códigos formalizados, como:

- Código de Ética del International Information Systems Security Certification Consortium, Inc (ISC)2
- Computer Ethics Institute (CEI)
- Internet Activities Board (IAB)
- Generally Accepted System Security Principles (GASSP)

Código de Ética del (ISC)2

El código de ética del (ISC)2 consiste en el preámbulo y los cánones de ética. Los cánones se explican con mucho más detalle en el sitio web del (ISC)2. El siguiente contenido es una traducción del original en inglés, disponible en formato pdf en la página del (ISC)2

Preámbulo del código de ética

La seguridad de la mancomunidad y el deber a nuestros principios y a nosotros mismos requiere que adheramos a los estándares éticos de comportamiento más altos y que nuestra adherencia sea pública. Por lo tanto, la adherencia a este Código es una condición necesaria para la certificación.

Cánones del código de ética
Proteger a la sociedad, la mancomunidad y la infraestructura.
Actuar con honor, honestidad, justicia, responsabilidad y legalidad.
Proporcionar un servicio diligente y competente a los principals.
Mejorar y proteger la profesión.

Código de Ética del Computer Ethics Institute

El CEI formalizó su código de ética en la forma de los Diez Mandamientos de la Ética Informática (el original está disponible en formato pdf en la página del Computer Ethics Institute):

1. No usarás una computadora para hacer daño a otros.

2. No interferirás con el trabajo ajeno.

3. No indagarás en los archivos ajenos.

4. No usarás una computadora para robar.

5. No usarás una computadora para dar falso testimonio.

6. No copiarás o usarás software propietario que no hayas pagado.

7. No usarás los recursos informáticos ajenos sin la debida autorización.

8. No te apropiarás de los derechos intelectuales ajenos.

9. Deberás considerar las consecuencias sociales de escribir tu programa o diseñar tu sistema.

10. Deberás siempre usar una computadora en formas que aseguren la consideración y el respeto por otros seres humanos.

Código de ética IAB

El IAB emitió una declación que constituye su código de ética (el original en inglés está disponible en texto plano aquí):

Internet es un complejo nacional cuya utilidad es mayormente consecuencia de su gran disponibilidad y accesibilidad. El uso irresponsable de este recurso crítico representa una amenaza enorme a la continuidad de su disponibilidad a la comunidad técnica. El gobierno de los Estados Unidos de América, patrocinador de este sistema, sufre cuando ocurren abusos que producen interrupciones significativas. El acceso a y uso de Internet es un privilegio que debe ser tratado como tal por todos los usuarios del sistema. El IAB apoya firmemente el enfoque del Division Advisory Panel de la National Science Foundation Division of Network, Communications Research and Infrastructure que, parafraseando, caracterizó como poco ética e inaceptable cualquier actividad que busque:

- Ganar acceso no autorizado a los recursos de Internet
- Interrumpir el uso de Internet
- Desperdiciar recursos, como personas, capacidad y computadoras, a través de tales acciones
- Destruir la integridad de la información basada en computadoras
- Comprometer la privacidad de los usuarios

Código de ética GASSP

El código de ética GASSP establece que los sistemas de información y su seguridad deben ser provistos y utilizados de conformidad con el Código de Conducta Ética (Code of Ethical Conduct) de los profesionales de la seguridad informática. El Código de Conducta Ética prescribe las relaciones entre la ética, la moral y la información.

A medida que las normas sociales para el uso de sistemas informáticos evolucione, el Código de Conducta Ética cambiará y los profesionales de seguridad de la información esparcirán los nuevos conceptos en sus organizaciones y productos. Las precauciones pueden requerir un juicio ético para el uso o la determinación de los límites o controles. Por ejemplo, el "entrapment" es un proceso por el cual se incita a alguien a realizar un acto ilegal o abusivo. Como precaución de seguridad, el profesional de seguridad puede

establecer una brecha fácil de comprometer en el sistema de contorl de acceso, y luego monitorear los intentos para explotar la brecha. Esta forma de "entrapment" es útil como advertencia de que se ha penetrado en el sistema. También puede proporcionar información suficiente para identificar al autor. Debido a las leyes, regulaciones o estándares éticos, puede ser poco ético usar datos recolectados por medio del "entrapment" en un juicio, pero puede ser ético usar el "entrapment" como estrategia de detección y prevención. Pueden buscarse consejos legales y éticos al diseñar la seguridad de la red.

9.7.7 Respuesta a una brecha de seguridad

Las leyes y los códigos de ética existen para permitir a las organizaciones e individuos un medio para reclamar los bienes perdidos y prevenir crímenes. Cada país tiene diferentes estándares legales. En la mayoría de los países y cortes, para procesar exitosamente a un individuo, es necesario establecer motivo, oportunidad y medios.

El motivo responde a la pregunta de por qué la persona efectuó el acto ilegal. Cuando se investiga el crimen, es importante empezar por los individuos que pueden haber tenido motivos para cometerlo. Por ejemplo, los empleados que creen que han sido pasados por alto en aumentos o ascensos pueden tener motivación suficiente para vender datos confidenciales de la empresa a la competencia. Una vez identificados los sospechosos probables, lo siguiente a considerar es si los sospechosos tuvieron la oportunidad de cometer el crimen.

La oportunidad responde a la pregunta de cuándo y dónde la persona cometió el crimen. Por ejemplo, si puede establecerse que tres de los sospechosos estaban en una boda cuando ocurrió la brecha de seguridad, pueden haber tenido motivos, pero no pueden haber tenido oportunidad porque estaban ocupados con otra cosa.

Los medios responden a la pregunta de cómo se cometió el crimen. Será infructuoso acusar a alguien que no posee el conocimiento, habilidades, capacidad o acceso para llevar el crimen a cabo.

Aunque establecer motivo, oportunidad y medios es un estándar para encontrar y procesar por todo tipo de crímenes, en los crímenes informáticos es bastante fácil manipular y encubrir la evidencia por la complejidad de los sistemas de computación, la accesibilidad global por medio de Internet y el conocimiento de los atacantes. Por esta razón, es necesario tener protocolos estrictos en relación con las brechas de seguridad. Estos protocolos deben ser incluidos en la política de seguridad de la organización.

Los datos de computadoras son datos virtuales, lo cual significa que raramente hay representaciones físicas tangibles. Por esta razon, los datos pueden ser fácilmente dañados o modificados. Al trabajar con datos de computadoras en un caso forense, la integridad de los datos debe mantenerse si deben ser utilizados como evidencia en una corte de justicia. Por ejemplo, el cambio de un solo bit de datos puede cambiar la marca de tiempo de 2 de agosto de 2001 a 3 de agosto de 2001. El perpetrador puede ajustar fácilmente los datos para establecer una coartada falsa. Por lo tanto, deben seguirse procedimientos estrictos para garantizar la integridad de los datos forenses que forman parte de una investigación. Algunos de los procedimientos que deben ser establecidos

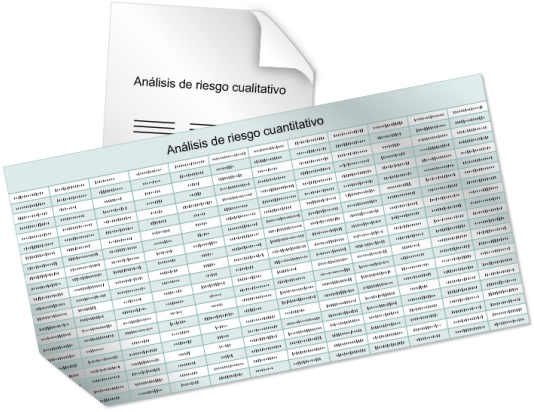
son el de recolección apropiada, la cadena de custodia, el almacenamiento y la creación copias de resguardo de los datos.

El proceso de recolección de datos debe ser efectuado precisa y rápidamente. Cuando toma lugar una brecha de seguridad, es necesario aislar inmediatamente el sistema infectado. Los sistemas no deben ser apagados o reiniciados antes de que la memoria sea volcada en un archivo, ya que el sistema vacía la memoria cada vez que el dispositivo se apaga. Además, debe tomarse una imagen del disco antes de trabajar con los datos en el disco duro. Generalmente se hacen varias copias del disco duro antes de apagar el dispositivo para establecer copias maestras. Estas copias maestras generalmente se almacenan en una caja fuerte y los investigadores usan las copias de trabajo tanto para la fiscalía como para la defensa. Los investigadores pueden determinar si los datos han sido manipulados comparando las copias de trabajo con la copia maestra que ha sido asegurada y por lo tanto no ha sido tocada desde el principio de la investigación.

Luego de la recolección de los datos pero antes de desconectar el equipo, es neceario fotografiar el equipo en el lugar. Toda la evidencia debe ser tratada con una cadena de custodia apropiada, lo cual significa que solo los individuos autorizados deben tener acceso a la evidencia y todos los accesos deben ser documentados.

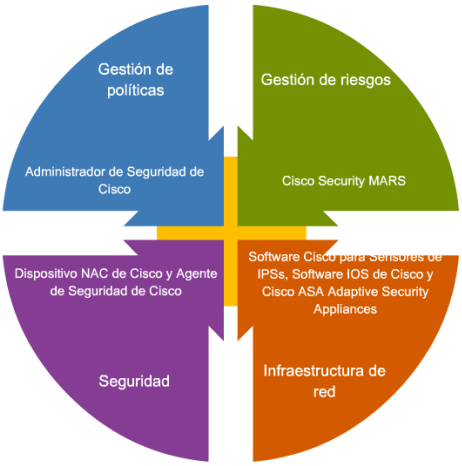
Si se establecen y se siguen protocolos de seguridad, las organizaciones pueden minimizar la pérdida y daños resultantes de los ataques.

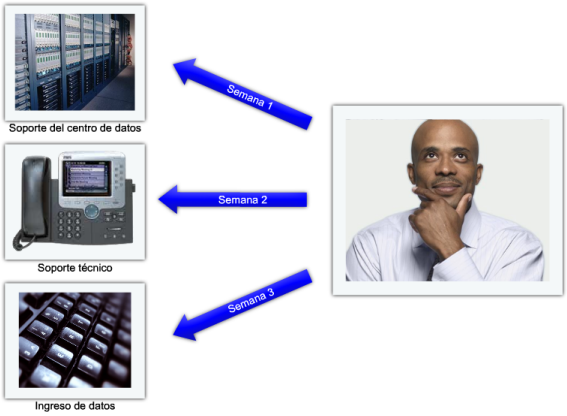
9.8.1 Resumen del capitulo



- La mitigación de ataques de red requiere un enfoque exhaustivo de extremo a extremo.
- La identificación de amenazas y el análisis de riesgos son los primeros pasos en la creaciónde la estrategia de protección.
- La gestión y la evasión de riesgos son dos enfoques distintos sobre los riesgos.

- La Red Autodefensiva de Cisco proporciona una solución exhaustiva de extremo a extremo para la seguridad de la red.
- Las soluciones CSDN incluyen control y contención de amenazas, comunicaciones seguras y control operativo y administración de políticas.
- Administrador de Seguridad de Cisco y Cisco MARS proporcionan soluciones de administración para CSDN.
- El Portfolio de Seguridad Integrado de Cisco ha sido diseñado para cumplir los requisitos y diversos modelos de despliegue de cualquier ambiente de red.

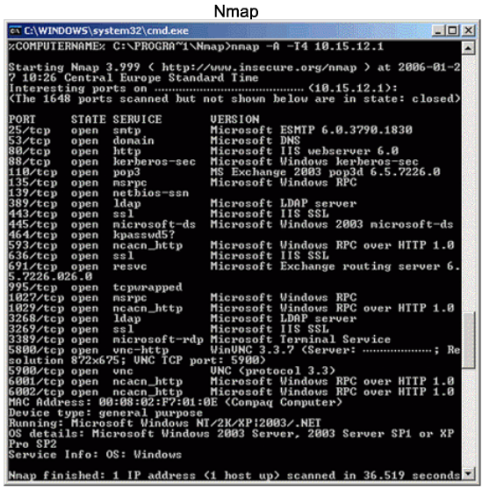




- La seguridad de las operaciones es una parte importante de la administración de una red segura.
- La separación de las tareas establece que ningún individuo debe tener control sobre dos o más fases de una transacción u operación.
- La rotación de tareas es una medida de seguridad en la que se asigna a cada individuo una tarea por un cierto tiempo antes de moverlos a otra tarea.
- La recuperación confiable es un principio importante de la seguridad de las operaciones.

- Las pruebas de seguridad en red son un proceso crítico para mantener a la red segura.
- Nmap y SuperScan son dos herramientas útiles para la realización de pruebas de seguridad en la red.
- Las pruebas incluyen el escaneo de redes, el escaneo de vulnerabilidades, el cracking de contraseñas, la revisión de registros, el chequeo de integridad, la detección de virus, el wardriving y las pruebas de penetración.

Nmap

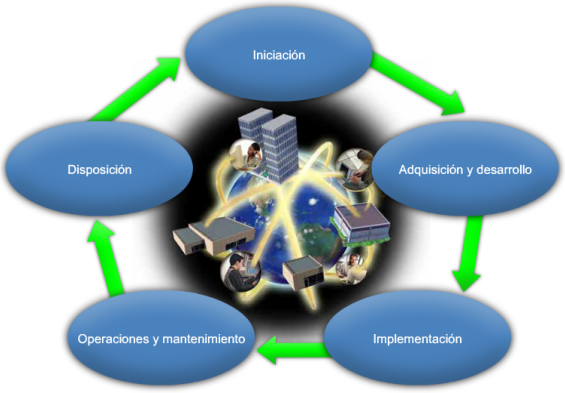




- La planeación de la continuidad de los negocios trata la continuación de las operaciones de una empresa si ocurriera un desastre o interrupción momentánea o continuada que afecte la misión de la organización.
- Primero deben identificarse los tipos posibles de interrupciones. La magnitud de la interrupción determina la respuesta.
- La redundancia garantiza la continuidad de las operaciones de negocios. Los SLAs deben incluir información de redundancia.

- El ciclo de vida de desarrollo de sistemas (system development life cycle - SDLC) implica la evaluación de cambios en el sistema y el ajuste de los planes como corresponde.
- El SDLC consiste en 5 fases.

Ciclo de vida de desarrollo de sistemas





La política de seguridad es un componente integral del diseño e implementación de la seguridad en la red de una empresa. Responde preguntas sobre qué activos deben ser protegidos y cómo protegerlos.

La política de seguridad típicamiente consiste en una política gobernante, una política técnica y una política de usuario final.

Los estándares, las guías y los procedimientos contienen los detalles definidos en las políticas.

La política debe establecer los roles y responsabilidades de los profesionales informáticos.

Es necesario un programa de concientización en seguridad para asegurarse de que todos los empleados de una empresa estén conscientes de y adhieran a las políticas de seguridad.

Los profesionales de la seguridad en red deben estar conscientes de todas las leyes y éticas relacionadas con la seguridad de las redes.