CCNA SECURITY 210-260

CAPITULO 1

Conceptos de Seguridad y Red

Comprendiendo la red e información básica de seguridad.

La seguridad es importante, y la ausencia del riesgo financiero, legal, político implica relaciones públicas. Esta sección cubre algunos de estos conceptos, términos y metodología usada en la preparación para trabajar con seguridad de redes.

Objetivos de seguridad de red.

Cuando consideramos redes, usted puede ver entonces desde diferentes perspectivas, por ejemplo, un administrador maestro podría ver la red como una herramienta de negocios para facilitar las metas de la compañía. Técnicas de red podrían considerar sus redes para ser el centro de un universo. Los usuarios finales podrían considerar la red para ser solo una herramienta para ellos hacer su trabajo. O posiblemente como una fuente de recreación.

No todos los usuarios aprecian su roll y mantienen los datos seguros, y desafortunadamente los usuarios de la red representan una vulnerabilidad significante. Y eso que ellos tienen username y password (u otras credenciales, tal como one-time password token generator) eso les permite accesar a la red, si un usuario esta comprometido o no autorizado tiene accesos a los datos, aplicaciones, o dispositivos para los cuales ellos NO DEBERIAN TENER ACCESO, la red podría tener fallas como resultado.

Incluso después de aplicar todos los conceptos que usted aprende en este libro, asi un punto importante para recordar es que el comportamiento de los usuarios pose un riesgo de seguridad y que entrenando a los usuarios es parte de la clave de una comprensiva política de seguridad.

CONFIDENTIALITY, INTEGRITY & AVAILABILITY

(CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD)

El objetivo de la seguridad de redes usualmente involucra 3 conceptos básicos.

Confidentiality: existen dos tipos de datos; datos en movimiento, es decir los que se mueven a través de la red, datos en descanso, es decir los datos que se encuentran almacenados (en servidores, estaciones de trabajo, en la nube etc.). Confidencialidad significa que solo usuarios autorizados puedan ver datos sensibles o información clasificada. Esto también implica que usuarios no autorizados no puedan tener acceso a los datos. Considerando los datos en movimiento, el principal camino para proteger esos datos es cifrárlos antes de enviarlos fuera de la red. Otra opción que usted puede usar con cifrado es para usar en redes separadas para la transmisión de datos confidenciales. Varios capítulos en este libro se concentran en esos dos conceptos.

INTEGRITY: la integridad significa que los cambios hechos a los datos son hechos solo por individuos o sistemas autorizados, la corrupción de datos es una falla para mantener la integridad de datos.

AVAILABILITY: esto aplica para sistemas y datos, si la red o los datos no están disponibles para usuarios no autorizados-quizás porque ataques ***DoS*** (denial of Service) o talvez porque de una falla general de red- el impacto puede ser significante para compañías y usuarios quines confían en esa red como una herramienta de negocios, la falla de un sistema, incluye datos, aplicaciones, dispositivos y redes, generalmente equivalente a la perdida de ingresos.

COSTO BENEFICIO ANALISIS DE SEGURIDAD

Los ingenieros de seguridad deben comprender no solo que es lo que protegen, si no tambien de quien. ***Los riesgos de administracion*** son la frase clave que oira una y otra vez.

Que es un Asset? Es cualquier cosa que es vulnerable para una organización. Esto podria ser un articulo tangible (personas , computadoras, y asi) o articulos intangibles (propiedad intelectual,informacion de bases de datos,lista de contactos, contabilidad) conociendo los assets que usted intenta proteger y su valor, ubicación y exposicion puede ayudar mas efectivamente determinando el tiempo y el dinero para gastar en segurar esos assets.

una vulnerabilidad (***a vulnerability)*** es una debilidad explotable en un sistema o su diseño. Bulnerabilidades pueden ser encontradas en protocolos, sistemas operativos, aplicaciones y sistemas de diseño. Mas vulnerabilidades se descubren cada dia.

Una amenaza (***a threat***) es un daño potencial para un asset, si una vulnerabilidad existe pero no ha sido todavia explotada, mas importante, no es todavia conocida publicamente, la amenaza es latente, si alguien esta activamente lanzando ataques contra sus sistema y exitosamente alcanza alguna cosa o compromete sus seguridad contra un asset, la amenaza es realizada. La entidad que toma ventaja de una vulnerabilidad es conocida como un actor malicioso y la ruta utilizada por este actor para ejecutar el ataque es conocido como actor de amenaza o vector de amenaza (threat actor or threat vector).

Un contramedida (safemeasure) es un salvaguardaque de algun modo mitiga un riesgo potencial, lo hace asi ya sea reduciendo o eliminando la vulneravilidad, o al menos reduciendo la probabilidad del agente amenazante para explotar el riesgo.

Un riesgo (a risk) es el potencial acceso no autorizado para, comprometer, destruir , dañar a un asset, si una amenaza existe, pero las apropiadas contramedidas y protecciones son ubicadas (esta es su meta para prever esta proteccion), el potencial de la amenaza para ser exitosa sera reducida.

LASIFICACION DE LOS ASSETS

Una razon oara clasificar un asset es que pueda tomar acciones especificas, basado en politicas, considerando los assets y dandoles clases, considere VPN, nosotros clasificamos el trafico que debe ser enviado sobre un tunel VPN, para clasicar los datos y etiquetarlo (tal como etiquetar datos TOP SECRET en un disco duro), nosotros podemos concentranos en cantidades apropiadas de proteccion o seguriadad en esos datos: mas seguriada para datos TOP SECRET que para datos sin clasificar. Los beneficios es que cuando nuevos datos estan puestos dentro del sistema, usted pueda clasificarlos como confidenciales o secretos y asi entonces reciviran el mismo nivel de proteccion que las configuraciones para ese tipo de datos.

La tabla siguiente enlista algunas comunes categorias de clasificaciones de assets :

Gouvernamental classification	Unclassified Sensitive but unclassified (SBU) Secret Top Secret
Private Sector Classification	Public Sensitive Private Confidentia
Clasification criterial	Value Age Replacement cost Useful lifetime

Clasification roles	Owner (el ultimo grupo responsable de los datos, usulamente senior management of a company) Custodian (el grupo responsable para implementar la politicacomo es dicatada por el propietario) User (aquellos quienes accesan a los datos y acatan las reglas aceptadas para el uso de los datos)

TLP classification levels (traffic light protocol)

COLOR	WHEN SHOULD IT BE USED?	HOW MAY IT BE SHARED?
RED	FUENTES PUEDEN USAR TLP: RED a información no puede ser eficazmente adoptada por otras partes y podría tener un impacto en la privacidad, reputación u operaciones de una parte si se utiliza indebidamente.	Destinatarios no pueden compartir TLP: RED informacion con cualquier parte fuera del intercambio especifico, encontrandose o conservandose en el cual esta originalmente evelado.
AMBER	Fuentes pueden usar TLP:AMBER la información no puede ser eficazmente aplicada por partes adicionales,	Destinatarios pueden solo compartir: informacion AMBER con miembros de su propia organización quienes necesitan conoser, y solo extendidamente como necesaria para actuar en esa informacion
GREEN	Fuentes pueden usar TLP: GREEN cuando la información es útil para la toma de conciencia de todas las organizaciones participantes, así como con los pares dentro de la comunidad o sector en general	Destinatarios pueen compartir TLP: GREEN la informacion con parejas y organizaciones asociadas dentro de su sector o comunidad, pero no por el camino e la publicidad y los canales accesibles.
WHITE	Fuentes pueden usar TLP: WHITE cuando la informacion lleva minima o tiene riesgos previsiblesde de mal uso, en conformidad con reglas aplicables y procedimientos para lanzamientos publicos.	TLP: informacion WITHE puede ser distribuida sin restricciones, suje a derechos de autor.

Clasificacion de las vulnerabilidades ***(Classifying Vulnerabilities)***

Comprendiendo las vulnerabilidades y debilidades en un sistema o red es un enorme paso hacia corregir la vulnerabilidad o colocando una apropiada contramedida para mitigar ramenazas contra esas vulneravilidades. Potenciales vulneravilidades de red abundan, con muchos resultados de una o mas de las siguientes:

- Policy flaw
- Design errors
- Protocol weaknesses
- Misconfiguration
- Software vulnerabilities
- Human factores
- Malicius software
- Hardware vulnerabilities
- Physycal access to network resource

Cisco y otros han creado bases de datos que categorizan amenazas en el dominio publico. Common vulnerabilities and exposure (CEV) es un diccionario publico de seguridad conociendo vulnerabilidades y exposiciones.

Clasificando contramedidas

Despues de que una compañía a clasificado sus assets y considerado el riesgo involucrado en esos assets de una amenaza contra una vulnrtabilidad, la compañía puede entonces decidir o implementar contramedidas para reducir el riesgo de un ataque exitoso, metodos comununes de control usados para implementar contramedidas incluyen lo siguiente:

- Administrativo (administrative): Esto consiste en escribir politicas, procedimientos, guias, y estandares. Un ejemplo seria un escrito ***acceptable use policy (UAP)***, estar de acuedo para cada uno de los usuarios en la red. Otro ejemplo es cambiar los procesos de control que necesitan ser enviados cuando hacemos cambios en la red. Administrar controles podria involucrer articulos tales como verificar los usuarios a fondo.
- Fisico (phisycal): Control fisico es exactamente como suena. Seguriadad fisica para los servidores de red, equipos, he infraestructura, un ejemplo es proveer puertas cerradas y acceso denegado a personal no autorizado.
- Logico (logical): control logico incluye password, firewall, prevencion de sistemas intrusos, ACL's, VPN's, etc. Los controles logicos son amenudo para los controles tecnico.

QUE HACEMOS CON UN RIESGO? (WHAT DO WE DO WITH THE RISK?)

Puede lidear con un riesgo en varios sentidos, uno de los cuales es eliminarlo, o al menos minimizarlo, una opcion es evitar web service o en conjunto transferir el riesgo a alguien mas, por ejemplo en lugar de alojar su propio servidor en su red, podria subcontratar un service provider, el service provider podria asumir toda la responsabilidad por ataques que podrian ser lanzados

contra su servicio y proveer un nivel de servicio acordado SLA service level agreement para garantizar a los clientes, mantenga en mente, sin embargo, la posibilidad de riesgo debe ser asumida si la entidad del subcontrato no adquiere eliminar el riesgo efectivamente.

Reducir el riesgo implementango contramedidas apropiadas, implementando los debidos parches, y suando un firwall correctamenete en el ISP y otras acciones eso reduce su propio riesgo.

Otras opciones es para una compañía poner su propio web server y solo asumir el riesgo. Desafortunadamenet, si no se toma precaucion de seguridad contramedidas contra amenazas potenciales, el riesgo podria ser alto suficiente para dañar la compañía y ponerlo fuera del negocio. Mas personas estarian deacuerdo que esto no un riesgo aceptable.

RECONOCIENDO AMENAZAS ACTUALES DE RED

Las amenazas estan constantemente cambiando, con nuevas em¡rgiendo, moviendo los objetivos son amenudo dificil concentrarlas, pero comprendiendo la naturaleza general de las amenazas puede preparalo para tratar con nuevas amenazas.

ATACANTES POTENCIALES

- Terrorist
- Criminals
- Goverment agencies
- Nation state
- Hackers
- Disgruntles employees
- Competitors
- Anyone with access a computing device

Diferentes terminos son utilizados para referirse a estos individuos , incluyendo hackers/cracker script-kiddie, bactivist, y la lista sigue, como un practicante de seguridad se debe comprender al enemigo. El unto es que es bueno comprender la motivacion o el intere de las personas involucradas en obtener todas estas cosas que usted busca proteger, tambien se necesita tener una buena compresnsion de sus redes de datos y conocer el ambiente que es vulnerable y que puede ser objetivo por un actor malicioso.

Metodos de ataque (Attack Methods)

Mas atacantes no quieren ser descuviertos y asi ellos usan na variedad de tecnicas para permanecer en las sombras cuando intentan comprometer una red, como describe la siguiente tabla.

Acción	Descripcion
Reconnaissance (reconocimiento)	Este es el proceso para descubrir, usado para encontrar informacion sobre red, podria incluir revizar la red para encontrar algun tipo de IP que responda, y en futuras reviciones ver cuales puertos en el dispositivo que esa esa IP estan abiertos. Este es usualmente el primer paso tomado, para descubrir que esta en la red y para determinar potenciales vulnerabilidades.
Social engineering	Esto es dificil uno por que aprovecha nuestras vulnerabilidades más débiles en un sistema seguro (datos, aplicaciones, dispositivos,redes, ect): el usuario. Si un atacate puede obtener el ususario para revelar informacion, es mucho mas facil para el atacante que usar algun otro metodo de reconocimiento, esto podria ser hecho a tarvez de un E-mail o desconocidas direcciones o paginas web. Las cuales resultan en el momento en que damos click a algunas cosas que conducen a los atacantes ganado esa información, la ingeniaria social tambien puede ser hecha sobre los telefonos. Phishing: se muestra un enlace como un recurso confiable valido para un usuario, cuando el usuario da click, el usuario es colocado para revelar informacion confidencial tal como username/password Pharming: es usado para direccionar a URL de clientes de un recurso valido a uno malicioso uno que podria ser hecho para aparecer como un sitio valido para el usuario. Para alli, intentar extraer informacion confidencial del usuario.
Privilege escalation (escalada de privilegios)	Este es el proceso que toma algunos niveles de acceso (si autoriza o no) y lograr un nivel de acceso muy alto. Un ejemplo es un atacante quien gana el acceso en modo usuariopara un router y entonces usa un ataque de fuerza bruta contra el router, determinado a obtener el nivel de privilegio 15
Back doork (Puerta trasera)	Cuando un ataque gana acceso a un sistema, ellos usualmente quieren acceso futuro, tambien, y ello s lo quieren hacer facil. Una aplicación de backdoor puede ser instalada ya sea para permitir futuros accesos o para recolectar informacion para usar en futuros ataques. Muchas puertas traseras son instaladas por usuarios haciendo click en algunos o sin realizarlo clink en el link de ellos o los archivos pueden ser amenazas, puertas traseras pueden ser resultado de un virus o un gusano (a menudo llmado malware).
Code execition (codigo de ejecucion)	Cuando los atacantes pueden ganar acceso a un dispositivo ellos podrian ser capaces varias acciones, el tipo de accion depende del nivel de acceso que el atacante tiene, o puede alcanzar, uno de los mas debastadores acciones disponibles por un atacante es habilidad de ejecutra codigo con un dispositivo, los codigos de ejecucion podrin resultar en un impacto adverso a la confidencialidad (los atacantes pueden ver informacion en un dispositivo), integridad (los atacantes pueden modificar la configuracion del dispositivo), disponiblilidad (los atacantes pueden crear una negacion de

	servicios a tarvez de la modificacion de codigo) de un dispositivo.

Ataque vector (Attack Vectors)

Los ataques no son solo lanzados desde afuera de la compañía, ellos tambien lanzan ataques desde dispositivos dentro de su compañía quienes tienen actuales y legitimas cuantas de usuarios, este vector es particularmenete preocupante estos dias con la prolifereacion de organizazciones permitiendo empleados traer sus propios equipos (“BYOD” bring your own device) y permitirles el acceso a dispositivos , aplicaciones, datos en la red corporativa, quiza el usuario es curioso, o tal vez un back door es instalado en la computadora en el cual el usuario esta logged in. Ya sea el caso, esto es importante para implementar una politica de seguriadad que nos lleve a garantizar y a estar preparados para mitigar riesgos en varios niveles.

MAN-in-the-Middle Attack

Homnbres en el ataque medio resulta cuando atacantes ubican ellos mismos en linia 2 dispositivos que se estan comunicando, con el intento para ejecutar reconocimiento o para manipular los datos como se mueven entre ellos. Esto puede suceder en capa 2 o 3 , el principal proposito es escuchar, asi que el atacante puede ver el trafico.

Si esto sucede en la capa 2 el atacane burla direcciones MAC de capa 2 para hacer que los dispositivos en la LAN crean que la direccion de la capa 2 del atacante es la direccion de capa 2 de su default gateway. Esto es llamado envenenamiento ARP (ARP poisoning). Las tramas que son supuestas para ir al default gateway son enviadas por el switch a la direccion de capa 2 del atacante en la misma red. como una cortesia, el atacante puede enviar las tramas al correcto destino asi que el cliente tendra la conectividad necesitada y el atacante ahora ve todos los datos entre 2 dispositivos, para mitigar este riesgo, podria usar tecnicas como un *Dynamic Address Resolution Protocol* (***ARP***) inspeccionar (DAI) en switches para impedir spoofing en las direcciones de capa 2.

El atacante podria tambien implementar el ataque para ubicar un switch dentro de la red y manipulando el STP spanning tree protocl para llegar a ser el root switch. Se puede mitigar esto a travez de tecnicas tales como root guard y otros controles de spanning tree discutidos mas tarde.

Un Man-in-the-Middle Attack puede ocurrir en capa 3 cuando un router pillo ubicado en la red y que engañando a otro router dentro creyendo que el nuevo router tiene una mejor ruta, esto podria crear trafico en la red o flujo a tarvez del router pillo y otravez permitir al atacanter robar robar datos de la red. Usted puede mitigar ataques como este en varios sentidos, incluyemdo autenticacion de protocolos y filtrando informacion para ser avisado o aprender de interfaces especidficas.

Para salvaguradar datos en movimiento, una de las mejoras cosas que puede hacer para es usar cifrado para la confidencialidad de datos en transito. Si usted usa protocolos de texto plano para administrar, tal como Telnet o HTTP, un atacante quien a implementado un man-in-the-middle attack puede ver el contenido de sus paquetes de datos en texto claro, y como resultado vera cada cosa que va atarvesando los dispositivos el atacante, incluyendo username y password que son usados. Usando administracion de protocolos que tienen cifrado tal como (SSH) secure shell y hipertext transfer protocol secure (HTTPS), es considerado una mejor parctica, y usando proteccion VPN para datos sensible en texto claro es tambien considerado una mejor practica.

Otros Metodos de Ataque

No existen estabdares para los grupos de atacantes, asi que no todos los ataques se ajustan correctamente en una categoria, de hecho, algunos ataques se ajustan dentro de o mas categorias al mismo tiempo, la tabla describe unos pocos metodos adicionales que atacantes podrian usar.

Metodo	Descripcion
Covert Channel (canal oculto)	Este metodo usa programas o comunicaciones en formas no intencionadas. Por ejemplo, si la politica de seguriadad dice que el trafico web es permitido pero peer to peer no lo es, los usuarios pueden intentar hacer un tunel peer to peer a tarvez de http, un atacante puede usar una tecnica similar para esconder trafico por tuneles dentro de algunos protocolos permitidos para evitar la deteccion. Un ejemplo de esto es una aplicación backdoor recolectando informacion de golpe de teclado de la estacion de trabajo y entonces lentamente enviarlo fuera disfrazado como ICMP (internet control Menssage Protocol), esto es un canal oculto. Un canal oculto es el legitimo uso de un protocolo, tal como un usuario con un buscador web usando http para accesar al servidor web, para propuestas ilegitimas, incluyendo descubrimiento de trafico de red de inspeccion.
Trust explotation (explotacion de confianza)	Si el firewall tiene 3 interfaces, y la interface del lado de afuera permite todo el trafico para el (“DMZ” demilitarized zone) pero no para su red interna, y el DMZ permite acceso a la red interna a el DMZ y usar esa ubicación para lanzar su ataque de alli hacia adentro de la red. Otro modelo de confianza, si configurado correctamente, puede permitir acceso involuntario a un atacante incluyendo directorio y nfc (network file system in UNIX)
Brute-force (password-guessing) attack	Tipos de ataque de fuerza bruta son ejecutados cuando un sistema del atacante intenta cientos de de posibles passwords buscando justo coincidir. Esto está mejor protegido contra límites específicos sobre cuántos intentos de autenticación fallidos pueden ocurrir dentro de un marco de tiempo específico. Ataques de adivinar contraseñas pueden ser hechos atravez de malware, man-in-the-middle attack usando paquetes de sniffers, o usando key loggers.
Botnet	Un botnet es una colección de computadoras infectadas que estan listas para tomar instrucciones del atacante, por ejemplo, si el atacane tiene una maliciosa backdoor software instalado en 10000 computadoras, de su ubicación central, el podria instruir estas computadoras para enviar todo las

	peticiones TCP SYN o ICMP echo request repetidamenete para el mismo destino. El podria tambien falsificar la IP de origen de la que solicita que el trafico responda se envie tambien a otra victima. Los atacadores generalmente usan una canal oculto para administrar dispositivos individuales que maquillan el botnet.
DoS & DDoS	Denial-of-service (DoS) apila ataques distributed denial-of-service (DdoS). Un ejemplo es usar un Botnet para atacar un sistema objetivo. Si un ataque es lanzado desde un solo dispositivo con la intension de causar daño a un asset, el ataque podria ser consderado un intento de DoS, a diferencia de un DDoS. Ambos tipo de ataques intentan el mismo resulatdo, y si es llamado ataque DoS o DDoS solo depende de cuantas fuentes (maquinas) son usadas en el ataque. Una mas avanzada y creciente tipo de DDoS es llamada ataque reflect DDoS (RDDoS). Un RDDoS toma lugar cuando la fuente del paquete inicial (query) esta actualmente suplantada por el atacante. El responde paquetes estan entonces “reflected” atrás del desconocido participante a la victima en el ataque: esos es, el original Spoofed fuente de los paquetes iniciales(query).

Aplicando Fundamentales Principios de Seguridad al Diseño de Red

Lineamientos

Usted quiere algunos principios basicos y lineamientos en ubicar primeras etapas de diseño he implementacion a la red.

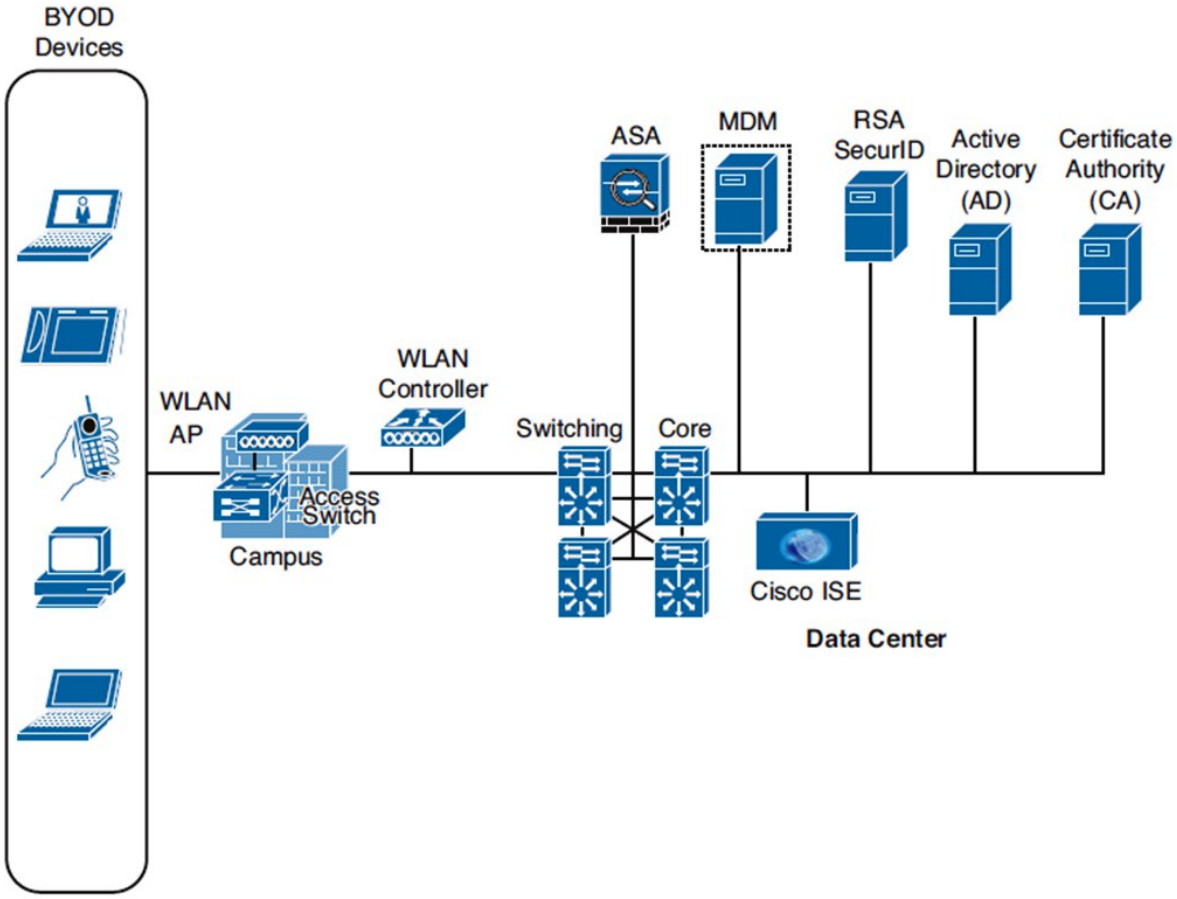
Lineamientos	Explicacion
Rule of least privilege	Estas reglas de estado de minimo acceso es solo proveer recursos de red, y no mas que eso, un ejemplo de esto es un ACL aplicada a una inteface para filtrar que dice el dany all. Anres de esto, entradas especificas podrian ser agregadas solo lo minimo indispensable de protocolos requeridos, y solo entonces entre los correctas fuentes direcciones destino.
Defense in depth	Este concepto sugiere que usted ha imlementado seguridad en lo mas cercano de cada punto de su red. Un ejemplo es filtrando el perimetro del router, filtrando otra vez con un firewall, usando IPSs para analizar trafico antes de alcanzar su servidor, y usando precaucion de seguridad basado en host a el servidor, tambien. Metodos adicionales que pueden ser usados para implementar una defensa profunda incluye un enfoque usando authentication y metodos de authorization, web y seguridad de e-mail, contenido de seguridad, aplicar monitoreo de inspecion, monitorear trafico, y proteccion de malware. El concepto detrás de defensa en profundidad es que si una singular tecnologia de seguridad falla, agregar niveles, o mecanismos de seguridad todavia estan en lugares para proteger datos, aplicaciones, y dispositivos en la red.
Separation of duties	Cuando usted ubica especificaciones individuales con especificos roles, alli puede ser verificado en lugar de considerar la implementacion de las

	politicas de seguriadad. Individuos rotativos dentro de diferentest roles periodicamente asistira tambien en verificacar esas vulnerabilidades estan siendo direccionadas, por que una persona que se mueve dentro de un nuevo giro sera requerido para revizar las politicas en su lugar.
Auditing	Esto se refiere a considerar y mantener archivos sobre que esta ocurriendo en la red. Mas de esto puede ser automatizado a travez de las caracteristicas de authentication, authorization y accounting (AAA).Cuando incluso sucede en al red, los archivos en esos eventos pueden ser enviados a un accounting server. Cuando esta separacion de deveres enfocada es usada, aquellos quienes que estan haciendo cambios en la red que no tienen acceso directo para modificar o eliminar los archivos de administracion que son mantenidos en el accounting server.

TOPOLOGIAS DE RED

Existen un numero de topologias de red que dependen en el tamaño y tipo de cada organización. Algunas organizaciones tienen precencia de cada una de las siguientes topologias, mientras otras solo pueden utilizar un subconjunto de esta lista.

- Campus-Area Network (CAN):es la topologia de red usada para proveer conectividad, datos, aplicaciones, y servicios para usar de una organización que esta fisicamente localizada en la oficina corporativa, el CAN incluye un modulo para construccion en el campus, para el data center, para agregar la WAN, y para el borde de internet.



- Cloud, Wide-Area Networl (WAN):La nuve y el proveedor WAN una logica y ubicación fisica para los datos, y aplicaciones que una organización prefiere tener moviendose fuera del sitio, como ilustra la figura esto a livia a una organización para tener gastos en recursos de operación, matenimiento y administracion de servicios que han sido previstos localizados dentro de la organizacion previamente.

- Data Center: el data center de red contiene el ubificado sistema de computo (UCS) servidores, gateway de voz y CUCM server soportando ambientes de VoIP, todos los cuales proveen conectividad la red por una serie de switches, como ilustra la figura. La entrada al Data Center Network es protegida por un conjunto de firewalls como el borde que filtra todo el trafico entrando y saliendo del data center.

- Small office/home office (SOHO):los remotos sitios SOHO proveran conectividad para los usuarios SOHOa travez del uso de router WAN que encuentran su regreso a los modulos de agregacion WAN en el CAN via MPLS WAN, como muestra la fig. con el SOHO, los usuarios son provistos de conectividad a travez de la precencia de switches de acceso.

Seguridad de Red para amvientes virtuales.

Hoy en dia el ambiente del data center debe ser diseñado para reducir significativamente sobre encabezado administrativo y mejorar la flexibilidad y eficiencia operacional, funciones criticas de seguridad deberian se capaces para dinamicamente escalar para proteger assets como cambio en la demanada de negocio. Cisco ha creado tecnologia y productos tales como ecosistema Application Centric Infraestructure (ACI) y el cisco (ASAv) virtual ASA para proveer soluciones de seguriadad para la demanda del centro de datos de hoy en dia. Por ejemplo ACI provee un nivel de aplicación centralizado ingeniado para control de aplicaciones y servicios con el ambiente virtual.

La figura muestra un alto nivel ambiente data center con multiples conexiones de red.

La figura un data center virtualizado donde multiples aplicaciones de software (tales como VMWare, KVM, Xen) son usadas para dividir un servicio fisico dentro de multiples aislados ambientes virtuales. En este ejemplo firewall fisicos son desplegados para proveer proteccion y segmentacion del data center para el resto de los componentes de red.

CAPITULO 2

Amenazas comunes de seguridad

Network Security Threat Landscape (Seguridad de red escenario de ameza)

Los escenarios y amezas de hoy ambos son complejos siempre cambiando, esto hace trabajar en la seguriada de red un desafio, esta seccion busca proveer la motivacion detrás de atacar una red, quien esta siendo el objetivo, y como las organizaciones pueden protegerse ellas mismas.

Con tantas organizaciones y mas importantemente, dispositivos conectados a internet, no es sorpresa que no hay ausencia de fuentes de amenazas de red y abundantes actores amenazantes maliciosos buscando tomar ventajas de estas amenazas. Asi que, cuales son todas esas motivaciones detrás de estos actores amenazantes.

- Financial(Financiero): hay varios diferentes significados en el cual los atacantes pueden hacer finanzas en contra a traves de sus acciones maliciosas, ellos pueden comprometer un point of sales (PoS) sistema de punto de ventas al por menor o sacar grandes cantidades de milles de tarjestas de credito o debito, las cuales pueden subsecuentemente pueden ser vendids en elinea en el mercado negro, actores amenazantes pueden tambien penetrar en organizaciones financieras por el solo proposito de comprometer cuentas de ususarios y transferir dinero a cuentas que ellos elijan.
- Disruption (Ruptura): desafrtunadamenete muchos individuos o grupos exixten unicamente para causar rupturas en el nucleo de negocios de muchas organizaciones e instituciones. Esta ruptura es creada por varias rasones:

    - Para protestar las acciones, desiciones o comportamiento de una empresa.
    - Para servir como una distraccion mientras el actor malicioso planifica algo en la red para ser apalancado como un punto futuro mas adelante.
    - Una contra medida de atencion para las acciones del grupo malicioso o individu malicioso.

- Geopolitacal: que no nos sorprenda, hay grupos afiliados, con ciertas naciones que apalancan internet para emplear cyber guerra. Sumando, hay grupos de actores malicioso, sin coneccion directa a ninguna nacion individual, quienes usan internet par alanzar ataques contra paises quienes ellos creen no tienen sus mismos intereses.

DDoS Distibuted Denial of Service Attack

- Direct: Direct DDoS attacks ocurren cuando la fuente del ataque genera los paquetes, sin considerar el protocolo, aplicación, y asi, que son enviados directamenet ala victima del ataque.
- Reflected: Reflected DDoS attack ocurre cunado la fuente del ataque es enviar paquetes apocrifos que parecen ser de la victima, y entonces la fuente llega a ser un involuntario participante en el ataque DDoS para enviar de vuelta el trafico de respuesta a la victima destinada. UDP es a menudo usada como el mecanismo de transporte llegando a ser mas facilmente engañado debido a la ausencia de handshake (apreton de manos) three way (usado por TCP).pr ejemplo si el atacante (A) decide atacar a la victima (V), el enviara paquetes (por ejemplo, NTP), request) a la fuente (S) quien piensa ese paquete es legitimo, la fuente (S) entonces responde a la solicitud NTP enviando la respuesta a la victima (V) , quien nunca espero este paquete NTP de la fuente.
- Amplification: amplificacion de ataque son de un ataque reflejado en el cual el trafico de respuesta (enviado por el participante involuntario) esta formado por paquetes que son mucho mas largos que esos que inicialmente fueron inicialmente enviados por el atacante, (spoofing the victim) . un ejemplo de este es cuando solicitudes DNS son enviadas y la respuesta DNS es tan larga dentro del tamaño de los paquetes que los paquetes de consulta iniciales, el resultado final es que la victima termina inundado por los grandes paquetes por los cuales nunca emitio consultas.

Engineering Social Method (Metodos Social de Ingenieria)

Actores maliciosos emplean ingenieria social confiando en el personal humano de redes para encontrar o crear agujeros en la fortaleza conocida como cyber security.

La Ingenieria social esta involucrada asi que rapidamente esas soluciones tecnologicas, politicas de seguridad, y procedimientos operacionales solos no pueden proteger los recursos criticos.

Incluso con esa proteccion, los hackers manipulan comunmente dentro comprometen la seguriadad corporativa. Las victimas podrian sin saberlo revelar la informacion sensible necesaria para pasar la seguridad de la red, o incluso quitar la llave de puertas de estaciones de trabajo para extraños sin identificacion, aunque los ataques al juicio humano son inmunes incluso al mejor sistema de defensa de red, las compañías pueden mitigar el riesgo de la ingeniería social con una cultura activa de seguridad que evoluciona con los cambios de la amenaza.

Social Engineering Tactics:

- Phishing: Fishing provoca que la información segura a través de un mensaje de e-mail que parece venir de una legitima fuente tal como un proveedor de servicios o institución financiera, el mensaje de e-mail puede preguntar el usuario para responder con los datos sensibles, o para accesar a un sitio web para actualizar información tal como un numero de cuenta de un banco.
- Malvertising: es el acto, de incorporar anuncios maliciosos, en websites confiables, el cual resulta dentro de buscador del usuario siendo inadvertidamente redireccionado a sitios alojados de malware.
- Phone scan: esto no es comúnmente alguien llamando a un empleado o intentando convencer a empleados divulgar alguna información sobre ellos mismos u otros dentro de la organización. Un ejemplo es un malvado posando como reclutador preguntando por los nombres, direcciones de e-mail, y asi sucesivamente para los miembros de la organización y entonces usar esa información para empezar a construir bases de datos para aplancar un futuro ataque, misión de reconocimiento, y asi progresivamente.

Defense Againts Social Engineering

Una cultura consistente debe incluir en marcha entrenamiento que consistentemente informe a los empleados sobre las últimas amenazas de seguridad, también políticas y procedimientos que refleje la misión y visión de la empresa en seguridad, este énfasis en seguridad ayuda a los empleados a comprender los potenciales riesgos de las amenazas de ingeniería social, como ellos pueden impedir ataques exitosos, y porque su roll dentro de la cultura de seguridad es vital para un sano comportamiento. Empleados consistentes están mejor preparados para reconocer y evitar rápidamente cambiando e incrementando sofisticados ataques de ingeniería social, y son más complacientes tomando propias responsabilidades de seguridad.

Políticas oficiales de seguridad y procedimientos tomando las conjeturas fuer de operación y ayudar a los empleados tomando decisiones de seguridad altas, tales políticas incluyen lo siguiente.

- Password management: los lineamientos tales como numero y tipos de caracteresque cada password debe incluir como a menudo debe ser cambiado un password, he incluso

una simple declaración que los empleados que los empleados no deben revelar a nadie, ayudara a asegurar la información de los assets.

- Two-factor authentication: la autenticación para altos riesgos de servicios de red tales como un pool del modem y VPN's serían un segundo fator mas bien.
- Antivirus/antiphising defense: multiples capas de defensa de antivirus, tales como un mail, Gateway y máquinas de usuario final, pueden minimizar la amenaza de phising y otros ataques de ingeniería social.
- Information Classification: una política de clasificación debería claramente describir que información es clasificada sensible y como etiquetar y manejarla.
- Document handling and destruction: documentos sensibles deben ser eliminados con seguridad y no simplemente arrojados a la basura de la oficina.
- Physical Security: las organizaciones tendrán efectivos controles de seguridad físicas tales como registro de visor, requerimiento de acompañante, y verificación de fondo.

Malware Identification tools (herramientas de identificación de malware)

Una de las espinas del lado de la conciencia personal de seguridad es tener la habilidad para identificar malware ya sea como un intento para obtener en la red o subsecuentemete para el malware ya estando presente. Varios factores hacen esta identificación particularmente difícil.

- La cantidad de malware que existe y su crecida a la fecha es casi incomprensible, la creación de nuevo malware a menudo resulta en considerar inútil las firmas basadas en herramientas de detección.
- Malware es con frecuencia incrustado en otras maneras de aplicaciones confiables, y enviada sobre protocolos que son tradicionalmente permitidos a través de firewall y acl's.
- Las organizaciones han limitado los recursos (ambos humanos y tecnológicos) para seguir con la cantidad masiva de trafico que atraviesa la red. El volumen de trafico ambos bueno y malo, a llegado a ser tan grande que es tanto para cualquier organización que es tanto para mantenerlo.
- El incremento uso de cifrado, no ha sorprendido, agregando otra capa de complejidad para las organizaciones intentando contra la visibilidad dentro del trafico malicioso residiendo en la red.

Methodos Available for Malware Identification

- Packet capture: recolección, almacenamiento y analizar paquetes que atraviesan la red es cierto un camino para inspeccionar tráfico con presencia de malware, un obstáculo primario en el uso de captura de paquetes para la identificación de malware es el hecho de que usted busca "una aguja en un pajar" debido al volumen de datos generados por la captura de paquetes.
- Snort (bufar): Snorf es una detección de intrusión de fuente abierta y prevención tecnológica desarrollada por el fundador de Sourcefire (ahora parte de cisco). La velocidad, poder, ejecucuion de snorf lo ha hecho el mas popular intrision detection/prevention system (IDS/IPS) tecnology en el mundo. Consiste en identificar

amenazas, detección y componentes de prevencion que se combina para rensamblar trafico, prevenir evaciones, detectar amenazas he información de salida sobre amenazas avanzadas mientras minimiza falsos positivos y pierde legitimas amenazas (falsos negativos).

- NetFlow : captura de paquetes es a menudo referido a un micro análisis en términos de granularidad de datos siendo analizado, pero Netflow es considerado masque un enfoque macro análitico. El uso de netflow recolección de datos consiste de la creación de buckets de flujo de datos que son basados en un conjunto de parámetros predefinidos tal como la fuente IP, fuente del puerto, dirección IP destino, puerto destino, protocolo IP, interface de ingreso y type of service (ToS). En cada uno de estos diferentes parámetros, un nuevo flujo es creado, el flujo es almacenado localmente en el dispositivo para un intervalo de tiempo configurado, después de un tiempo el flujo es exportado a celector externo, a pesar de que los datos netflow no proveen el mismo detalle a veces necesitado para identificar el malware en la red, puede servir como un excelente herramienta en la caja de herramientas para ayudar a rastrear de vuelta evidencia de transigencia una vez algunos de los detalles del malware lleguen a ser conocidos para el administrador de seguridad de red.
- Avanced Malware Protection: Cisco Advanced Malware Protection (AMP) es diseñado por cisco aplicaciones de seguridad de red FirePOWER. Provee visibilidad y control para proteger contra altamente sofisticados, fijados, zero-days, amenazas de malware persistentemente avanzado. AMP ayuda a identificar ataques discretos para analizar continuamente y monitoriar archivos después de que han ingresado a la red, utilizando retrospectivamente alertas de seguridad para ayudar a tomar acciones administrativas durante y después de un ataque.

- NGIPS: el Cisco NGIPS next generation intrusión prevention system (NGIPS) provee multiples soluciones de capa de amenazas de protección avanzada como alta velocidad de rendimiento de inspección. El NGIPS solución de protección de amenaza es administrado centralmente a través de CISCO FireSIGHT managemnet Center y puede ser expandido para incluir adicionales características tales como AMP, visibilidad de aplicación y control y filtrado de URL.

Data Loss and Exfiltration Methods

Mas ataques de red son ahora conducidos por sofisticados, y equipos bien fundamentados que pueden evadir las medidas de seguridad corporativa y robar millones de archivos de todo tipo de organizaciones alrededor del mundo. Las medidas de seguridad tradicionales son buenas como identificar trafico sospechoso que viene hacia adentro, pero muchas organizaciones falta la visibilidad del trafico dentro que es permitido dentro de sus red interna. Este trafico saliente , si es controlado por actores maliciosos con un punto de apoyo dentro de la red corporativa, amenudo incluye tratos secretos de la compañía, datos de clientes, u otra información propietaria que no seria vista por nadie fuera de la organización. Teniendo este tipo de trafico saliendo de la organización, desconociendo a aquellos quienes son responsables para ello, ubicar la organización

como riesgo significativo para comprometer propiedad intelectual, perdida de clientes sensibles y datos financieros, un alto costo de operaciones interrumpidas y esfuerzos de medición.

- Intellectual priety (IP): este consiste en cualquier tipo de datos o ducumento que es propiedad de una organización y ha sido creado o producido por empleados de la organización, IP a menudo se refiere al diseño, bosquejos, y documentos que soporta el desarrollo, ventas y soporte de un producto de una organización.

- Personally identifiable information (PII): Este es el tipo de información que desafortunadamente se ha hablado en la prensa con demasiada frecuencia últimamente escuchamos sobre las violaciones de datos, esta información incluye nombres, fechas de cumpleaños, direcciones y número de seguridad social.

- Credit /debit card: En adición a PII, el cual es con frecuencia robado/comprometido durante la violación de datos, información de tarjetas de crédito y débito es extremadamente deseada por los actores maliciosos.

CAPITULO 3

Implementing AAA in CISCO IOS

Muchas compañías tienen muchos dispositivos de red, un solo administrador necesita acceso a diferentes routers, y usted esta usando localmente la base de datos solo para un username y password de ese administrador, usted debe crear esos mismos usuarios diferentes veces, una vez por cada router, si se necesita cambiara el password, eso también requiere regresar a todos los dispositivos y manualmente hacer los cambios en cada uno. Esta solución no escala bien en ambientes con multiples administradores y muchos dispositivos.

Una solucion a esto es tener una base de datos centralizada donde todos los username y password son mantenidos para la autenticación (authentication) y que cada usuario es permitido para hacerlo (authentication es una porción de AAA). Esto es principalmente el ACS puede proveer. Esto es un proceso de dos partes, la primera parte es configurar un CAS server information sobre los usuarios y los passwords y que usuarios son permitidos, la segunda parte es dicirle al router que debería referir alguna sobre de sus deciciones acerca de autenticación (authentication) o autorización (authorization) al servidos ACS.

Una observación sobre la palabra user: con frecuencia nos referimos al plano de administración , y nos referimos a usuarios (users), aquellos usuarios son muy probablemente administradores quienes necesitan accesar a los comandos del CLI o a la administración web via HTTP, HTTPs, también ser conciente que ususarios finales no necesitan acceso al CLI, pero necesitaran acceso a recursos de red y sus paquetes son permitidos a tarvez del router, se puede usas el ACS para autenticar el tipo de usuario, agregando, se puede usar el ACS como un distino para el inicio de secion (llamado accounting).

Que es ISE?

Un producto llamado Identity Services Engine (ISE) es un identificador y plataforma de políticas de control de acceso que puede validar que una computadora encuentre los requerimientos de una política de la compañía relacionada a archivos de definición de virus, niveles de service pack, y asi mejor permitir los dispositivos en la red. No remplaza al 100% a un ACS, para un futuro cercano, los usuarios quienes quieren las características de ISE probablemente usarn ACS para la autenticación y la autorización y usar ISE para políticas complejas verificando los host.

Protocolos usados entre el ACS y el router

Es necesario comprender el “lenguaje del amor” usado para comunicar el servidor ACS y un router (el router actuando como cliente y el ACS como servidor).

Dos principales protocolos pueden ser usados TACACS+ y RADIUS, TACACS Terminal Access Control Access Control Server, TACACS+ es propiedad de cisco, lo cual significa sus principal uso seria visto como un protocolo usado entre un dispositivo cisco y un server ACS. Si se configura el router y el server ACS paquetes AAA que son enviados entre los dispositivos usan el protocolo TACACS+ los cuales cifran cada paquete antes de ser enviados a la red.

Otro protocolo es RADIUS para el servicio de AAA, el cual es el estándar para Remote Authentication Dial In User Service (RADIUS) es un standard abierto, lo cual significa que no solo ACS lo soporta, si no que otras marcas implementan AAA en sus servicios (tales como Microsoft). RADIUS cifra solo password, pero no todos los paquetes siendo enviados entre el ACS y los dispositivos de red.

	TACACS+	RADIUS
Functionality	Separa funciones AAA dentro de distintos elementos. Authentication es separada de Authorization, y ambos de son separados de Accounting.	Combina muchas de las funciones de Authentication y Authorization junta. Tiene capacidad de cuanta detallada cuando la cuenta esta configurada para sus uso.
Standard	Propiedad de cisco, pero muy bien conocida.	Standard abierto, y soportada por fabricantes cercanos a implementaciones AAA.
L4 Protocol	TCP	UDP
Confidentiality	Todos los paquetes son cifrados entre el ACS server y el router (el cliente).	Solo el password es cifrado entre el ACS y el router.
Granular command by command authorization	Esto es soportado, y las reglas son definidas en el ACS server sobre los cuales los commandos son permitidos o no dermitidos.	No se pueden implementar reglas explicitas de control de autorización de comandos.
Accounting	Provee soporte de Accounting	Provee soporte de accounting, y generalmente acusu de recibo como proveiendo mas información detallada de la cuanta que TACACS+

Configurando un Router para Interoperar con Un ACS server

Una buena noticia es que la más grande diferencia dentro del router es que el método listado, al router se le puede decir para usar la base de datos local (la cual se conoce como running config en el router) para verificar el username y password, o al router se le puede decir para verificar con un ACS server preguntar si o no el username o password son válidos.

En un router, podría usar el CLI o CCP para la configuración, por que usted conocería ambos (y podría necesitar ambos dependiendo de la certificación), ambos métodos son cubiertos aquí. Primero el CLI seguido por el CCP. La configuración esta basada en un router que todavía no ha sido configurado por ningún tipo de AAA. Comentar cada uno de los comandos y sus propósito son incluidos, unos pocos pueden ser una review, del capitulo anterior.

Un factor clave en la implementación es tener un plan, antes de comenzar a configurar el router, asi que el plan es el siguiente.

- Para adminitradores/usuarios quienes están accesando al router via líneas vty, sin considerar si se utiliza telnet o ssh, el router verificara con TACACS+ server (el ACS server usando TACACS* para comunicar con el router) para verificar la authorization (username/password).
- Usuarios Autenticados necesitan ser autorizados para tener acceso al CLI el exec privilegiado, la autorización verifica si debería ser hecha por el router referido al ACS server usando TACACS*.

Ejemplo usando CLI para configurar IOS para usar con ACS.

¡este comando hablita la configuración del resto del AAA, si este esta en la configuración, no se necesita poner otra vez dentro del sistema IOS, por derfecto tiene aaa new-model deshabilitado!

R1(config)#**aaa new-model**

¡este método de autenticación lista, cuando aplicado a una línea tal como la vty diciéndole al router para rápido el usuario quien esta accediendo a esa línea con un username y password en otro para que ese usuario inicie sesión, cuando el usuario provee e username y password para el inicio de sesión rápido el router enviara las credenciales a un servidor TACACS+ configurado y entonces el servidor puede responder con un pass o mensaje de fallo¡

¡este comando indica un grupo TACACS+ como el primer método como ellos podrían ser mas que un servidor configurado. Si no responde el servidos ACS después de un corto tiempo fuera el router entonces intentara un segundo medico el cual es "local" lo cual significa el router entonces verificara el running config para ver si hay username y password coincidente!

R1(config)#**aaa authentication login AUTHEN_via_TACACS group tacacs+ local**

¡El siguiente lista un metodo de autorizacion, cuando aplico a una linea, causara al router Exec. No solo el ACS indicar a el router si o no el usuario esta autorizado, pero puede indicar que nivel de privilegio tiene el usuario, ambos el username y password necesitaran ser creados en el ACS para el método previo de autenticación, y la autorización para el CLI también necesitara ser configurada en aquel ACL SERVER. Esta autorización utilizara uno o mas servidores ACS via TACACS+, y si no hay servidores que respondan , entonces el router verificara localmente reconsiderando si el comando esta autorizado para este usuario basado en nivel de priviegios del usuario y nivel de privilegios del comando siendo intentado.!

R1(config)#**aaa authorization exec Author-Exec_via_TACACS group tacacs+ local**

¡es importante prestart atencion que antes de que apliquemos este listado a la s líneas vty, deberíamos crear al menos un usuario local como respaldo,si el ACS es inalcanzable, o todavía no es configurado. En el ejemplo debajo crearemos un usuario en la base de datos local del router incluyendo username y password, también nivel de privilegios para el usuario esto es altamente recomendable que usted use password fruertes cuando configura cualquier usuario o credenciales en el dispositivo.!

R1(config)#**username admin privilege 15 secret cisco**

¡Siguiendo, necesitamos crear al menos un servidor ACS que el router intentaria usar via TACACS+. Esto es el equivalente de crear un server group. El password es utilizado como parte del cifrado de los paquetes, y si el password se configuro aquí, también necesitamos configurar en el ACS server ¡

R1(config)#**tacacs-server host 192.168.1.252 key cisco123**

¡verificando que la ip es alcanzable puede ser hecho aun antes de las configuraciones totals completadas en el ACS server.!

R1(config)# do ping 192.168.1.252

R1(config)#line vty 0 4

R1(config-line)#authorization exec Author-Exec_via_TACACS

R1(config-line)#login authenticatio AUTHEN_via_TACACS

Con los metodos listados de autenticacion y autorizacion creados y aplicados, podria intentar iniciar cession a travez de una de las 5 lines vty, esto es lo que esperaría: seria rápido el username y password, no podría ser capaz de hacer contacto con el ACS server (por que un no esta configurado) entonces después de un corto tiempo el router usaría un segundo método de sus listas, el cual indica usra la base de datos local para la autenticación y la autorización, por que tendría un usuario local con password y privilegios asignados a un usuario, asi trabajaría.

Task	How to do it
Decide que política seria (ejemplo: líneas vty requieren autorización y autenticación) y cual método (ACS, local o ninguna) seria usado	Este paso es hecho antes incluso de configurar el router, y esta basado en sus políticas de seguridad para su red, es el concepto de que quiere acompletar para autenticar y autorizar.
Habilitar la abilidad para configurar AAA	**aaa new-model** no esta habilitado por defecto,si usted quiere utilizar el servcio de ACS, usted debe habilitar las características de AAA como el primer paso de configuración en un nuevo router.
Especificar la dirección de un ACS SERVER para usar.	Usar el comando tacacs-server host, incluyendo direccion IP del ACS server y el password.
Crear un lista de métodos nombrados para la autenticación y otro para la aoturizacion, basado en su política.	Cada método listado es creado en modo de configuración global, especificando cual método listado utilizara, en orden de izquierda a derecha.
Aplicar el método listado para la ubicación que usaría estos métodos.	Dentro del modo de configuración líneas vty, especificar el método listado de autenticación y atorizacion que usted creo en el paso anterior

CAPITULO 4

Bring Your Own Device (BYOD)

FUNDAMENTOS BYOD

El concepto BYOD trae un desafio para administradores de red, y seguridad asi como para administración e ingenieros. El desafio es proveer la misma conectividad para usuarios que taren su mismo dispositivo mientras mantienen una apropiada postura de seguridad. La organización debe proveer un nivel de seguridad que encuentre las politicas de seguridad de la organizaciony asegurar que los dispositivos de red, sistemas y datos no estén comprometidos a travesde la proliferación de vulnerabilidades con el dispositivo traido por el empleado.

Para habilitar una organización sus usuarios para utilizar la red corporativa y remotamente – casa, hoteles, cafes etc.-a través del uso de VPN. Los empleados no solo demandan hoy en dia indicadores de negocios, legitimammente necesitan ser capaz para usar su propio dispositivo para conectar desde cual ubicación de red conectada en el mundo.

Siguiendo el número de razones de negocios que están manejando la necesidad para soluciones BYOD:

- WIDE VARIETY OF CONSUMER DEVICE: esto parece como cada dia hay nuevos vendors, nuevos dispositivos, o nuevas versiones de un dispositivo ya existente que requiere conectividad a internet. Solo con ver dentro de casa tenemos PC de escritrio, cada uno de os cuales conectan directamente via Ethernet, a la red corporativa. Ahora tenemos laptops, mobiles, tablets, smartphones, todos los cuales requieren conexión a la red.

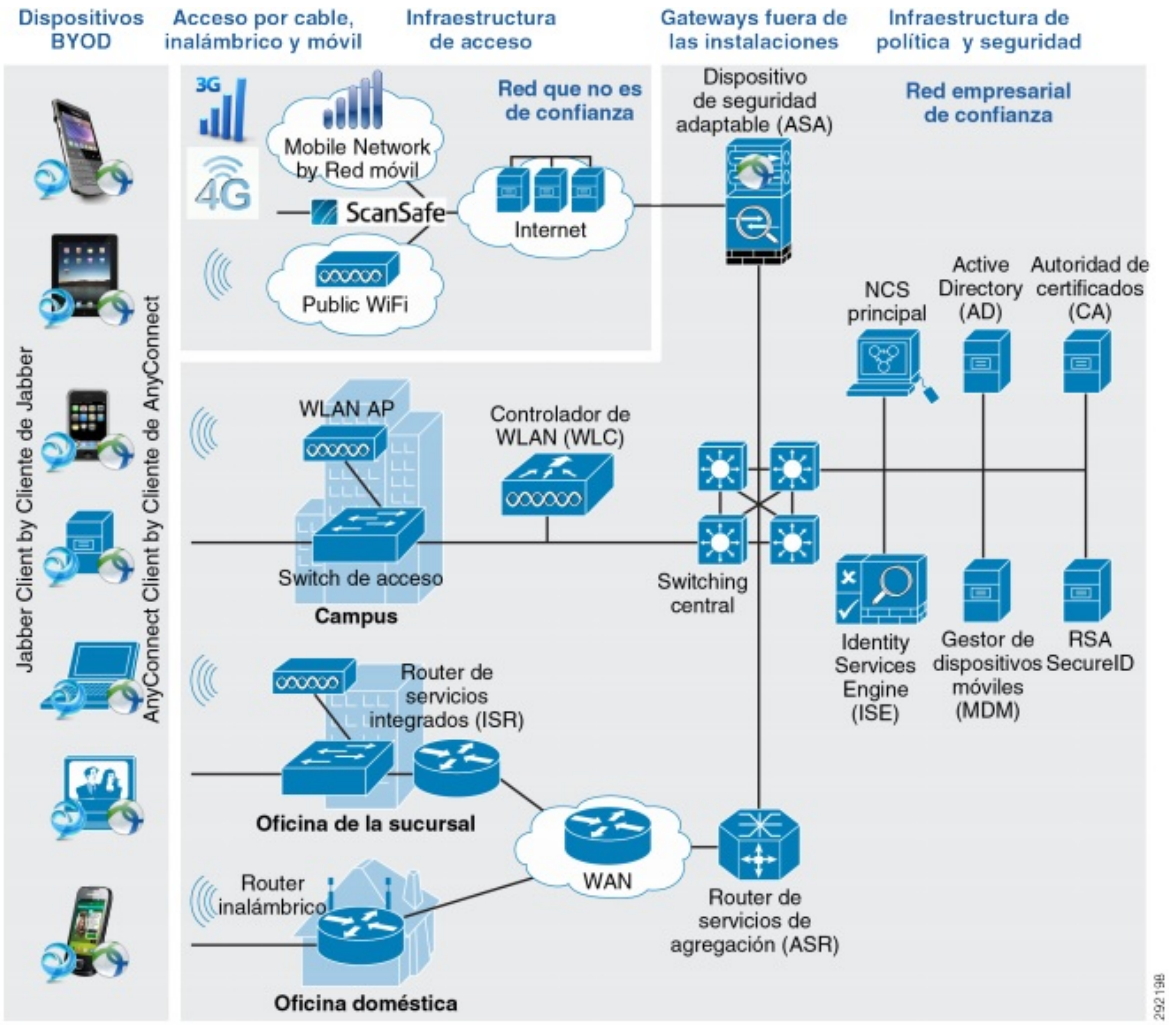
- BLURRED LINES BETWEEN WORK AND PLAY: el termino 9 a 5 usado significativamente el rigido inicio y fin de nuestras tradicionales 8 horas de trabajo hoy en dia. Oviamente los tiempos han cambiado, no solo tenemos que empezar y terminar , pero nosotros incluso no necesariamenet tenemos un trabajo definido “hoy”, trabajamos nuestro trabajo común, trabajamos durante el lanzamiento, trabajamos en casa, trabajamos por la noche, trabajamos mientras miramos a los niñosjugar baseboll, futboll, etc, y los fines de semana, algunos aun trabajan mientras están de vacaciones.

- CONNECT ME ANYTIME, ANYWHERE: usuarios finales esperan ser capaz de comunicar sus dispositivos cuando sea y donde sea.

Arquitectura BYOD

Hay muchos caminos para implementar soluciones a BYOD, en cada una de las organizaciones debe decidirse el nivel de apertura y fexibilidad que se quiere habilitar a sus empleados en términos del tipo de dispositivo que ellos puedan conectar y la cantidad de accesos para cada uno de esos dispositivos será garantizada. Sin embargo las políticas de seguridad de las organizaciones debe ser apalancada para gobernar elnivel de acceso para dispositivos BYOD, y entonces concentrada la tecnología seria usada para asegurar las políticas de seguridad.

Cisco Bordeeless Network Architecture esta basada en asumir best common practice (BCP) es seguida en diseño de red para campus, branch office, internet edge, y home office implementaction.



Componentes de solución BYOD.

- DYOD Device: hay la propiedad corporativa y la propiedad personal, esas terminales requieren acceso a la red corportiva sin considerar su ubicación física. Esta ubicación fisicapuede ser en campus corporativo, la branch office, home office y ubicaciones publicas tales como café, tiendas, hoteles etc. BYOD incluyen laptops, smartphones, tablets, notebooks etc.
- Wireless Access Point (AP): cisco AP provee conectividad de red inalambricapara la red corporativa, para ambas la para propiedad corporativa y para la personal ambientes BYOD o empleados home office.

- Wireless LAN (WLAN) controller: WLC como un sistema centralizado para la configuración, administración y monitoreo, es usado para implementar y reforzar la seguridad para BYOD. WLC trabaja con con el cisco Identity Service Engine (ISE), para reforzar ambos la autorización y la autenticación en cada punto final BYOD que requiere conectividad a la red corporativa, ambos directo y remoto.

- Identity Service Engine: ISE es pieza critica para el cisco BYOD solution. Es la piedra angular de la autenticación , autorización y consideración (authorization, authentication & accounting "AAA") para los requerimientos de acceso de los terminales. El cual esta gobernado por las políticas de seguridad.

- Cisco AnyConnect Secure Mobility Client: para usuarios finales quienes necesitan acceso a la red corporativa, para usar con el campus corporativo, branch, home office, el cliente anyconnect utiliza 802.1X para proveer acceso seguro a la red corporativa, para ususarios quienes están usando internet publico, el AnyConnect Client provee conectividad segura VPN, incluyendo verificación para dispositivos de BYOD.

- Integrate Service Router (ISR): será utilizado en las soluciones BYOD para prover WAN y acceso a internet a las oficinas remotas y acceso a internet par ambientes de home office, agregando, ISR ambos proveerán conectividad a ambos cableado y WLAN y ambientes de oficina remota, finalmente ISR puede ser apalancado para proveer conetividad VPN para dispositivos mobiles que son parte de la solución BYOD.

- Aggregation Service Router(ASR): ASR provee acceso WAN e Internet al campus corporativo y servicio como punto de agregación para todas las oficinas remotas y redes home office conectando de vuelta al campus corporativo para la solución de BYOS Cisco.

- Cloud Web Service. (CWS): provee seguridad mejorada para todas las soluciones BYOD de puntos finales mientras ellos accesan a internet y websites usando los hot spots disponibles 3G, 4G LTE.

- Adaptive Secure Appliance(ASA): provee todos los estándares y funciones de seguridad para las soluciones BYOD en el borde de Internet, agregando un firewall tradicional y funciones de un *intrusión prevention system (IPS)*. El ASA también sirve como un punto terminal VPN para conectar dispositivos mobiles conectando sobre Internet de los hogares, oficinas remotas. Redes inalámbricas publicas y 3G, 4G LTE.

- RSA Secure ID: provee un password temporal (one time password "OTP") para iniciar secion para que aacedan a dispositivos de red y otras aplicaciones las cuales requieren OTP authentication.

- Active Directory: refuerza el control de acceso a la red, a servicios, y aplicaciones. Y restringe acceso a aquellos usuarios con credenciales validas de autenticación.
- Certificate Authority: CA provee entre otras cosas, la incorporación de terminales finales que encuentra requerimientos certificados para accesar a la red corporativa. El CA asegura que solo dispositivos con certificados corporativos puedan accesar a la red corporativa.

Administracion de dispositivos mobiles

También conocido como mobile device management MDM, esto despliega, administra, monitorea los dispositivos mobiles. Esos dispositivos consisten no solo en teléfonos mobiles, smartphones, tablests etc, cualquier otro dispositivo del usuario que conecte de regreso a la red corporativa y que pueda físicamente ser movido de una oficina a casa, hoteles, cafes etc, y otras ubicaciones remotas conectando a internet publico. Funciones especificas que provee el MDM son las siguientes:

- ✓ Aplicación de un PIN lock (que es, echar llave a un dispositivo después de tres intentos fallidos iniciando sesión que intentaron y han sido rechazados)
- ✓ Aplicación de password mas fuestes para todos los dispositivos BYOD. Políticas de password fuertes pueden también ser forzadas po un MDM, reduciendo la probabilidad de un ataque de fuerza bruta.
- ✓ Detección de intentos para un "jailbreak" o "root" en dispositivos BYOD, específicamente smartphones y entonces intentar utilizar estos dispositivos comprometidos en una red corporativa, MDM puede ser usado para detectar este tipo de acciones e inmediataente restringis el acceso a dispositivos a la red u otros assets corporativos.
- ✓ Aplicar requerimiento de cifrado de datos basados en las políticas de seguridad de la organización y requerimientos regulatorios. MDM puede asegurar que solo dispositivos que soportan cifrado de datos y lo tienen habilitado puedan accesar a la red y contenido corporativo.
- ✓ Provee la habilidad de limpiar remotamente un robado o perdido dispositivo BYOD asi que todos los datos son completamente removidos.
- ✓ Administración de ejecución de prevención datos perdidos(data loss prevention "DLP") para BYOD. DLP impide usuarios autorizados hacer descuidado o maliciosamente cosas con datos críticos.

CAPITULO 5

FUNDAMENTOS DE TECNOLOGIA VPN Y CIFRADO

Que es una VPN?

Si descomponemos el termino virtual private network dentro de sus componentes individuales, podríamos decir que la red provee conectividad entre dos dispositivos, aquellos dispositivos podrían ser computadores dentro dela misma LAN o podría ser conectado sobre la WAN . ya sea cualquiera de los casos, la red esta proveindo de conectividad básica entre las dos. La palabra Virtual en VPN se refiere a la conexión lógica entre 2 dispositivos. Por ejemplo, un usuario podría ser conectado a internet en Raleigh, carolina del norte, y otro usuario podría estar conectado en a la internet en NY, y podríamos construir una red lógica, o una red virtual, entre los dos dispositivos usando la internet o sus mecanismos de transporte. La letra P en VPN se refiere a private. La red virtual la podríamos crear entre sus dos usuarios en CAROLINA y NY deveria ser privada entre estas dos partes. Asi que, asi que es lo básico de VPN.

Deafortnadamente si tuviéramos una VPN establecida entre dos dispositivos sobre la internet, que impediría un individuo que tiene acceso a los paquetes de escuchar la conversación? La respuesta es no mucho, por defecto. Asi que en adicion para mas VPN's, agregamos los ingredientes de confidencialidad e integridad de datos, asi que nadie quien este escuchando no puede hacerse con los datos sensible por que están cifrados, y ellos no tienen las llaves requeridas para descifrar o quitar la llave de los datos para ver cuales son los datos actuales. La confidencialidad provista por el cifrado de la nube también representa la P en VPN, asi que usamos verificación de integridad para hacer seguro que nuestra VPN esta viendo correctamente los paquetes como ellos fueron enviados del otro lado de la VPN y que ellos no son alterados o manipulados maliciosamente a lo largo de la ruta.

Usando el ejemplo de usuario en NY y Carolina del norte, por que nosotros quisiéramos siempre querer usar una VPN entre los dos? Nosotros tenemos otras opciones para conectividad. Podríamos programar cada usuario a

conexiones WAN dedicadas de NY a CN, cada usuario podría conectarse a su lado local y comunicar con el otro sobre enlaces dedicados. Uno de los problemas obvios con esto es el costo. Es mucho mas barato conectar el usuario a travez de la internet a un provedor de servicio local, que programar un enlace dedicado para ir solo solo uno al otro lado.

Otro beneficio de usa VPN es la escalabilidad . fi 10 o 20 mas nuevos usuarios necesitan conectar a la sede corporativa, podemos proveer acceso a usuarios a la internet via sus servicio local (DSL digital suscriber line), cablemodem y si. Aprovechando una singular conexión a internet del sitio sede, podría entonces simplificadamente construir VPN's usando la internet para conectar.

Tipos de VPN

Vasado en la definicio VPN, lo siguiente puede ser considerado tecnología VPN:

- IPsec: implementa seguridad de paquetes IP a la capa 3 del modelo OSI y puede ser usado para site-to-site VPN y remote-access VPN.
- SSL: Secure Sockets Layer implementa seguridad de sesiones TCP sobre tuneles cifrados SSLdel modelo OSI, y puede ser usado por Remote-Access VPN's (también es utilizado para asegurar visitas web que lo soportan via HTTPS).
- MPLS: es provisto por un proveedor de servicios para permitir a una compañía con dos o mas sitios tener conectividad lógica entre los sitios usando la red del service provider para transporte. Esto también es un tipo de VPN (llamado MPLSL3VPN) pero no hay cifrado por defecto, IPsec cloud podría usada en lo alto de MPLS para agregar confidencialidad, y el otro veneficio de IPsec para proteger los paquetes de capa 3. MPLS L3VPN no son el principal tipo de VPN en el resto del libro. La principal VPN provee cifrado, integridad de datos, autenticación de quien esta en el otro lado de la VPN.

Dos principales tipos de VPN

Hay dos categorías dentro de las cuales las VPN podrían se ubicadas. : remote-access y site-to-site.

- Remote-access VPN: algunos usuarios podrían necesitar construir conexiones VPN de sus ordenadores individuales a la sede corporativa (o al destino que ellos quieran conectar). Esto es referido como un remote-access VPN conection. Remote-access VPN puede usar tecnología IPsec o SSL para sus VPN's.muchos clientes cisco usan el Cisco anyConnect client para acceso remoto SSL VPN's. SSL VPN prevalece mas, incluso a travez del cisco anyconnect client también soporta IPsec (IKEv2).
- Site-to-site: la otra principal implementación de VPN es para compañías que pueden tener dos o mas sitios que ellos quieren conectar juntas seguramente (probablemente usando la internet) asi que cada lado puede comunicarse con el otro lado o lados. Esta complementación es llamada site-to-site VPN. Site-to-site VPN tradicionalmente usa una colección de tecnollogias VPN llamadas IPsec.

Principales beneficios de las VPN

1. Confidencialidad
2. Integridad de datos
3. Autheticacion
4. Protección antirecepcion

Confidentiality

Significa que solo las partes interesadas pueden comprender los datos enviados. Alguna parte que escucha a escondidas puede ver los paquetes actuales, pero el contenido de los paquetes o la carga util son revueltos y sin sentido para nadie quien no tiene la llave o decifra los datos.

Los algoritmos y formulas de cifrado de datos son publicamente disponibles y bien conocidos , la parte que hace el mensaje secreto es la clave o

“secreto” que es usada para cifrar los datos, si el emisor y el receptor conocen ambos la clave que es usada, ellos pueden cifrar o decifrar la informacion de vuelta y usar la misma clave o claves, y nadie en el medio quienes no conocen la clave que fue usada no puede decifrar.

Data integrity

Si dos dispositivos se estan comunicacndo sobre una vpn , otro importante factor sobre los datos que estan siendo enviados es hacer seguro esto es preciso de terminal a terminal. Si un atacante infiltra bits o datos dentro de los paquetes de una VPN, la integridad de datos podria sufrir si la modificacion de datos va indetectada.

Authentication

Un tunel VPN es fantastico en que se puede cifrar datos y verificar esos datos que no han sido modificados mientras estan en transito, pero que si usted ha establecido una conexión VPN , tambien llamado tunel VPN, directamente a la computadora de un atacante? Seria capaz de validar o autenticar los dispositivos que son conectados esto es un importante aspecto para una VPN. Usted puede autenticar las parejas de los otros terminales del tunel VPN en varias diferentes vias, incluyendo las siguientes:

- Pre-share key usada solo para autenticar
- Public and private key usada solo para autenticar
- User authentication (en combinacion con remote-access VPN)

Antireplay Protection

Si un atacante mira su trafico VPN y lo captura con el intento de responder de vuelta y engañar uno de los pares dentro de la VPN creyendo que el par intentando conectar legitimamente, un atacante podria ser capz de construir una VPN pretendiendo ser un dispositivo diferente. Para solventar eso, mas implementaciones de VPN tienen un funcionalidad antireplay, esto solo significa que una vez una VPN han sido enviados paquetes y contados, esos exactos paquetes VPN no son validos una segunda vez en la sesion VPN.

Componentes basico de Criptografia

"*Definition - What does Hashing mean?*

Hashing is generating a value or values from a string of text using a mathematical function.

Hashing is one way to enable security during the process of message transmission when the message is intended for a particular recipient only. A formula generates the hash, which helps to protect the security of the transmission against tampering.

Hashing is also a method of sorting key values in a database table in an efficient manner When a user sends a secure message, a hash of the intended message is generated and encrypted, and is sent along with the message. When the message is received, the receiver decrypts the hash as well as the message. Then, the receiver creates another hash from the message. If the two hashes are identical when compared, then a secure transmission has occurred. This hashing process ensures that the message is not altered by an unauthorized end user.

Hashing is used to index and retrieve items in a database because it is easier to find the item using the shortened hashed key than using the original value."

Ahora conoce que la confidencialidad esta en funcion del cifrado, la integridad de datos es una funcion del hashing, la autenticacion es el proceso que provee la identidad del otro ladodel tunel, ahora es tiempò de tomar una vista de cómo esos metodos son implementados y la eleccion que tiene para cada uno.

Cipher and keys

CIPHERS (cifrar)

Un cipher es un conjunto de reglas, las cueles pueden tambien ser llamadas algoritmo, sobre como ejecutar cifrado o decifrado. Literalmente cientos de algoritmos de encripcion estan disponibles, y hay muchos mas que probablemente son propietarios y usados para propositos especiales tales como guvernamentales y seguridad nacional.

Metodos comunes que el cifrado usa incluyendo los siguientes:

- Substitution: este tipo de cifrado sustituye un carácter por otro, el exacto metod de substitucion podria ser referido como la clave o llave “key”. Si ambas partes imvolucradas en una VPN comprenden la clave, pueden ambas cifrar y descifrar.
- Polyalphabetic: esto es similar a substitucion, pero en lugar de usar un singular alfabeto, podria usar multiples alfabetos y cambiar entre ellos por algunos caracteres en el mensaje codificado.
- Transposition: este usa muchas diferentes opciones, incuyendo reordenamiento de letras. Por ejemplo , si tiene el mensaje “this is secret”npodriamos escribirlo fuera (top to bottom, left to right) como muestra el ejemplo.

TSSR

HIEE

ISCT

Bloque cifrado

Un bloque cifrado es un ***symmetric key*** (misma clave para cifrar y decifrar) cifras que operan en un grupo de bits llamado a ***block***. Un algoritmo de cifrado ***block cipher*** (bloque cifrado) puede tomar bloques de 64bits de texto plano y generar un bloque de 64 bits de texto cifrado. Con este tipo de

encripcion, la misma clave para cifrar es tambien usada para decifrar. Ejemplos de bloque simetrico cipher algorithms incluyen lo siguiente:

- Avanced Encryption Standard (AES)
- Triple Digital Encryption Standard (3DES)
- Blowfish
- Digital Encryption Standard (DES)
- International Data Encryption Algorithm (IDEA)

Symmetric and Asymmetric Algorithms

Symmetric

Un symmetric encryption algorithm, tambien conocido como un symmetrical cipher, usa las mismas claves de cifrado de datos y decifrados de datos. Dos dispositivos conectados via VPN ambos necesitan la clave o claves para cifrar o decifrar exitosamente los datos que estan protegidos usando un symmetric encryption algorithm. Comunmente ejemplos de cifrado simetrico incluyen los siguientes:

- ♣ DES
- ♣ 3DES
- ♣ AES
- ♣ IDEA
- ♣ RC2,RC4,RC5,RC6
- ♣ Blowfish

Algotritmos de cifrado cimetrico son usados por la mayoria de datos que protegemos en VPN’s hoy en dia. La razon es que es mucho mas rapido para usar algoritmos de cifrado simetrico y toma mens CPU para el mismo algoritmo de cifrado cimetrico que deberia para un algoritmo asimetrico. Como con todos los cifrados, la mayor dificultad la clave, la mayor dificultad para alguien por que no tiene la clave para iterceptar y comprender los datos. Generalmente nos referimos a la clave “key” con VPN’s por su

longitud. Una clave mas larga significa mejor seguridad, una tipica longitud es 112 bits a 256 bits. La minima longitud clave deberia ser al menos 128 bits para algoritmos de cifrado simetrico para ser considerado segura. Otra vez mas grande es mejor.

Asymmetric

Un ejemplo de algoritmo asimetrico es algoritmo de clave publica, hay algo magico sobre aquello, en su lugar de usar una misma clave clave para cifrar o decifrar, usamos dos diferentes claves, que matematicamente trabajan juntas como pareja. Dejeme llamar esas claves la “public kay” & “private key”, juntas ellas hacen una clave en pareja “key pair”.

Imagine un enorme envio que tiene una llave especia con dos cerraduras de lleve (un cerradura grande y una cerradura pequeña), con este contenedor, si usamos la cerradura pequeña con su respectiva llave para cerrar el contenedor, el unicoa manera de desbloquearlo es usar la llave grande y la cerradura grande. Otra opcion es para inicialmente cerrar el contenedor usando la llave grande en la cerradura grande, y entonces la unica manera de desbloquearlo es usar la llave pequeña en la cerradura chica. Esto explica analogicamente la interrelacion entre la clave publica y la privada. (le dejaria decidir cual primero quiere llamar la gran llave y cual la llave pequeña). Hay un muy alto costo de CPU cuando usamos llaves pareja para bloquear y desbloquear datos. Por esta razon usamos escasamente algoritmos asimetricos, en lugar de usarlos para cifrar nuestro bulto de datos, usamos algoritmos asimetricos para cosas tales como autenticar una pareja VPN o generar claves que podrian usar nuestros algoritmos simetricos.

Una razon de esto es llamado ***public key cryptography*** es que nosotros permitimos una de estas llaves para ser publicadas y disponible para cualquiera quien quiere usarlo (the public key). La otra clave dentro del par

de claves es la private kay, y esta clave privada es conocida solo por los dispositivos que pertenecen a la *public-private key pair*. Un ejemplo de usar public-private key pair es visitando un secure website. En el fondo el public-private key pair del servidor esta siendo usado para la seguridad de esta sesion. Su PC tiene acceso a la public key, y el servidor es el unico que conoce

Ejemplos de asymmerical algorithm incluyen los siguientes.

- RSA: llamado asi Rivest, Shamir, y Adleman, quienes crearon el algoritmino, el principal uso de este algoritmo asimetrico hoy es la autenticacion. Es tambien conocido como un public key cryptography standard (PKCS) #1. La logitud de clave puede ser de 512 a 2048, y el tamaño minimo para una buena seguridad es de al menos 1024. Considerando seguridad, entre mayor es mejor.

- DH: Diffie-Hellman key exchange protocol. DH es un algoritmo asimetrico que permite dos dispositivos negociar y establecer material secreto de claves compartidas (keys) sobre una red no confiable. Lo interesante d DH es que a pesar de que el mismo es asimetrico, las claves generadas por el exchange son claves simetricas que pueden entonces ser usadas con algoritmos simetricos tales como 3DES y AES.

- ElGamal (second character is an L) este sistema de cifrado asimetrico es basado en DH exchange.

- DSA: Digital Signature Algorithm fue desarrollado por la Agencia de Seguridad Nacional de U.S

- ECC: Eliptic Curve Cryptogrphy

Los algoritmos asimetricos requieren mas CPU poder de procesado que los algoritmos simetricos. Los algoritmos asimetricos son mas seguros, tipicamente la lungitud de la clave usada en un algoritmo asimetrico puede ser entre 2048 y 4096 bits. La longitud de clave mas corta entonces es de 2048.

Hashes

Hashing es un metodo usado para verificar la integridad de datos, una funcion criptografica hash es un proceso que toma un bloque de datos y crea un pequeño valor hash tamaño-fijo (fixed-sized). Esta es una función de un solo sentido, significa que si dos diferentes computadoras toman los mismos datos y corren la misma función hash, ellos obtendrían el mismo fixed-sized (por ejemplo, quizá un hash de longitud de 12-bit). (Menssage digest 5 altgorithm MD5 es un ejemplo). No es posible generar el mismo hash para diferentes bloques de datos. Esto es referido como collision resistance. El resultado del hash es un fixed-length pequeña cadena de datos. Y es a veces referido como digest, messange digest, o simplemente hash.

Un ejemplo de usar un hash para verificar la integridad es el emisor corriendo un algoritmo hash en cada paquete y adjuntando esos paquetes a el paquete. El emisor corre el mismo hash contra el paquete y compara sus resultados que tiene el emisor (los cuales fueron adjuntados a los paquetes también). Si el hash generado coincide con el hash que fue enviado, conocemos que todos los paquetes están intactos. Si un solo bit de la porción hashed de los paquetes es modificada, el hash calculado por el receptor no coincidiera, el receptor conocería que los paquetes tienen un problema, específicamente con la integridad de los paquetes.

Los tres tipos mas populares de hashe son los siguientes.

- ∑ Message Digest 5 (MD5): este crea un digest 128.bit
- ∑ Secure Hash Altgorithm 1 (SHA-1): este crea un digest 160-bit
- ∑ Secure Hash Altgorithm 2 (SHA-2): incluye opciones a digest entre 224 bits y 512 bits.

Con cifrado y criptografia, y ahora hashing, entre mas grande major, mas bits igual a major seguridad.

Hashed Menssage Authentication Code (HMAC)

HMAC usa el mecanismo de hashing, pero levanta una muesca, en lugar de usar un hash que cualquiera puede calcular, incluye en su calculo una clave secreta de algún tipo. Entonces solo la otra parte quien también conoce la clave secreta y puede calcular el resultado hash puede verificar correctamente el Hash. Cuando este mecanismo es usado, un atacante quien esta escuchando a escondidas y capturando paquetes no puede inyectar o remover datos de esos paquetes sin ser notado por que el no puede recalcular el correcto hash para modificar paquetes por que el no tiene la llave o las llaves usadas por el calculo.

DIGITAL SIGNATURE (firma digital)

Cuando usa alguna firma, a menudo representa un compromiso a seguir, o al menos provee que sea usted quien dice ser. En el mundo de la criptografía, una firma digital provee tres beneficios centrales:

- → Authentication
- → Data integrity
- → Nonrepudation

Digital signature in action

Uno de los mejores caminos para comprender como una firma digital opera es recordar que aprendio en la sección anterior sobre claves privadas y publicas, hashing y cifrado. Las firmas digitales involucra cada uno de esos elementos, aquí esta el play by play. Bob y Lois son dos dispositivos que quieren establecer una VPN uno con el otro, y para hacerlo asi ellos quieren usar una firma digital para verificarse uno al otro y hacer segura la conversación. Ambos dispositivos quieren verificar cada uno al otro, pero por simplicidad concentraran en un dispositivo: Bob buscando proveer su identidad al otro dispositivo Lois (esto podría se también fraseado como Lois preguntando a Bob su identidad).

Cun una pequeña configuración de antemano, usted podría conocer que ambos Bob y Lois han generado public-key pairs, y ha ellos les han sido dados certificados digitales de un común (CA) certificate autority. Un CA es una entidad confiable que entrega certificados digitales. Si usted y yo abrimos un certifcado digital, encontraríamos el nombre de la identiada (por ejemplo Bob). Encontraríamos la clave publica de Bob (la cual Bob da al CA cuando el aplico para su certificado digital). Allí también seria una firma digital del CA, ambos Bob y Lois confiarían en el CA y recibirían sus certificados, muy bie ahora regresemos la historia.

Bob toma un paquete y genera un hash. Bob entonces toma este pequeño paquete hash y lo cifra usando la clave privada. (piense en esto como un contenedor de envio, y nosotros estamos usando la pequeña llave en la cerradura chica para cerrar con llave los datos) adjuntamos este hash cifrado a el paquete y lo envíamos a Lois. Hay un lujoso nombre para este cifrado hash: un digital signature.

Cuando lois recibe el paquete ella busca el cifrado hash que fue enviado y decifrandolo usando la clave publica de Bob. (piense en esto como una gran cerradura y la gran llave siendo usada para desbloquear los datos). Ella entonces configura el descifrado hash fuera del sitio por un momento ella corre el mismo algoritmo hash en el paquete que recivio . si el hash calculado coincide el mismo recibido (después ella lo descifro usando la clave publica enviada). Ella conoce dos cosas, ella conoce solo la persona que podría haber cifrado eso fue Bob, con llave privada de Bob, y que la integridad de los datos en el paquete es solida. Por que si1 bit ha cambiado el has no había coincidido. Este proceso es llamado authentication , usando firma digital, y normalmente sucede en ambas direcciones con un IPsec Tunel VPN si las parejas están usando firmas digitales para autenticar, referido a aun rsa-signature en la configuración.

Uno podría preguntar, esta bien asi como Lois obtuvo la clave de Bob (la clave publica de Bob) para empezar?, la respuesta es que Bob y Lois también intercambian certificados digitales, los cuales contienen cada uno claves publicas del otro. Bob y Lois no solo confían en algún certificado, ellos confían certificados que son digitalmengte firmados por un CA en el que ellos confían. Esto también implica verificar firmas digitales del CA, ambos Bob y lois también necesitaran claves publicas del CA. Mas buscadores hoy en dia tienen incorporado certificados y claves publicas para los principales CA en internet.

KEY MANAGMENT

La clave de administración es enorme en el mundo de la criptografía, tenemos claves simétricas que pueden ser usadas con algoritmos simétricos tales como claves public-private key pair que pueden ser usadas con algoritmos asimétricos tales como firmas digitales, entre otras cosas. Podríamos decir que las claves para seguridad con todos estos algoritmos que tenemos son la clave en si mismo.

Claves de administración trata con generación de claves, verificación de claves, intercambio de claves, almacenamiento de claves, hasta el final de su tiempo de vida, destruyendo claves, un ejemplo de por que esto es critico es si dos dispositivos que quieren establecer una sesión VPN enviar la claves cifradas sobre el inicio de su sesión en texto plano. Si eso sucede, un espia quien ve la clave podría ir derecho a usarlas para cambiar texto cifrado dentro datos incomprendidos, lo cual resultaría en ausencia de confidencialidad con la VPN.

Keyspace se refiere a todos los posibles valores para la clave, la clave mas grande, la mas segura, lo único negativo de tener claves extremadamente grandes es que las claves mas grandes, usan mas CPU para el descifrado y cifrado de datos.

IPsec and SSL

Ip sec usa una suit de protocolos para proteger paquetes IP y ha sido alrededor del mundo. Este es el uso hoy en dia para ambos remote-access VPM y site-to-site VPN, déjeme tomar una mirada mas de cerca para ambas opciones.

IPsec

Es una colección de protocolos y algoritmos usados para proteger paquetes IP de la capa 3 IP Security “IPsec”. IPsec provee el nucleo de beneficios de confidencialidad a travez de cifrado, integridad de datos a travez de hashing y HMAC y autenticación usando firmas digitales o usando un pre-shared key (PSK) que es solo para la autenticación similar al password. IPsec también provee soporte anti respuesta. Tomando una mirada mas cercana de IPsec mas tarde, pero aquí es un buen previo de la atracción que viene:

* ESP & HA: los dos principales métodos de implementación de IPsec, el acrónimo pertenece por Encapsulation Security Payload (ESP), el cual puede hacer todas las características de IPsec, y Authentication Header (AH), el cual puede hacer muchas partes de los objetivos de IPsec, exepto por una importante de cifrado de datos, por esa razón, no vemos frecuentemente AH ser usado.
* Encription Algorithm for Confidentiality: DES, 3DES, AES
* Hashing algorithm for Integrity: MD5, SHA.
* Authentication Algorithm: Pre-shared keys (PSK), RSA digital signatures
* Key Management: un ejemplo podria ser Diffie- Hellman (DH), el cual puede ser usado dinamicamente generando claves simetricas para ser usadas por algoritmos simetricos; PKI, el cual soporta las funciones de certificados digitales mostrados por confiables CA's. e Internet Key Exchange (IKE), el cual hace mucho de la negociación y administración para nosotros para que IPsec opere.

SSL

Trasmitir información sobre la red pública necesita ser asegurado atravesó de cifrado para inpedir acceso no autorizado a esos datos. Un ejemplo es en línea hacer transacciones bancarias. No solo usted no quiere evitar un atacante viendo su username, password y códigos usted también no quiere un atacante que pueda modificar los paquetes en transito durante una transacción con el banco. Podría parecer que esto sería una oportunidad perfecta para IPISEC para ser usado para cifrar los datos y ejecutar la verificación de integridad y verificación de su software actualmente ejecutando en cada una de sus computadoras incluso si hubiera, nadie teniendo un certificado digital o un psk que ellos podrían exitosamente para autenticar.

Usted todavía puede verificarse del concepto descifrado y autenticación para usar un diferente tipo de tecnología. Esta opción adicional es llamada secure sockets layer (SSL). Las cosas convalecientes sobre SSL es que cada buscador web en cada computadora lo soporta así que cualquiera quien tiene una computadora puede usarla.

Para usar SSL, el usuario conecta a un servidor SSL, el cual es una función para decirle al web server que soporta SSL, para usar HTTPS en lugar de http. Una vía fácil para recordar es que la “s” SECURITY o TLS para el usuario final tal como usted y yo. representa una conexión segura al servidor, y al correcto servidor.

Incluso si el usuario no teclea HTTPS, el WEB SITE podría presionar al usuario como regresar a la URL correcta. Una vez allí el buscador solicita el servidor web se identifique así mismo. El servidor envía al buscador una copia de su certificado digital, el cual también puede ser llamado SSL cuando el buscardor recibe el certificado verifica si es un certificado de confianza. El buscador decide si es confiable o bloqueado con la firma digital (CA) está en el certificado; usando el método para verificar la firma digital discutida antes el buscador determina que el certificado es válido basado en la firma del (CA) (o no es válido) si la firma o es válida o al menos si su buscador no piensa que el certificado es válido pop-up es usualmente presentado al usuario preguntando si el usuario quiere procede) esto es cuando el usuario.

Asumiendo que el certificado es verdadero el navegador tiene acceso a la clave pública del servidor contenida en el certificado más de una vez es servidor no requiere del buscador promover quien es. En su lugar el servidor web usa un método de autenticación tal como Pas Word como requisito para verificar quien es el usuario.

Después de que la autenticación haya sido hecha varios cambios ocurren entre el buscador y el servidor, hasta que ellos establecen el algoritmo descifrado la clave que ellos usaran para cifrar y descifrar los datos. Usted aprenderá más sobre esos procesos exactos en el capítulo PKIA

Como mencionamos previamente comprendiendo la terminología es importante para usted un maestro de UBPN. La tabla describe componentes UBPN sus funciones y ejemplos de su implementación algunos de estos términos son de una sobrevista otros son nuevos. Estos conceptos y sus funciones son repetidos a través del capítulo e aquellos TOPIKS para asistirlo en el aprendizaje y en la aplicación de esos conceptos.

Componentes VPN

Componentes	Función	Ejemplos de uso
Algoritmos de cifrado simétrico	Usa la misma clave de cifrado y descifrado de datos	IDE, 3DES, AES, IDEA
Cifrado asimétrico	Usa claves publicas y privadas. Una clave cifra los datos, y la otra clave par es usada para decifrarlos.	RSA, Diffie-Hellman
Firmas Digitales	Cifrado de hash usando clave privada, y descifrado de hash con la clave publica de emisor.	Firma RSA
Diffie-Hellman kay Exchange	Usa una parejas de claves publica-privada de algoritmo asimétrico, pero crea finales claves compartidas secretas que estas entonces son usadas por algoritmos simetricos	Usado como uno de muchos servicios de IPsec
Confidencialidad	Algoritmos de cifrado proveen esto girando texto claro dentro de texto cifrado.	DES, 3DES, AES, RSA, IDEA
Integridad de datos	Valida datos comparando los valores del hash.	MD5, SHA-1

Autenticación	Verifica la identidad de los peer’s	PSKs, RSA firmas

Public Key Infrastructure

Public and Private Key Pair

Una key pair es un conjunto de claves que trabajan en convinacion con cada otra como un equipo. En una típica key pair, usted tiene una clave publica y una clave privada. La clave publica puede ser compsrtida con cualquiera, y la clave privada no es compartida con nadie. Por ejemplo,la clave privada para un web server es conocida solo para ese especifico web server. Si usted usa la clave publica para cifrar datos usando un algoritmo de cifrado asimétrico, la correspondiente clave privada es usada para descifrar los datos. El inverso es también cierto. Si usted cifra con la clave privada, usted entonces descifra con la correspondiente clave publica. Otro nombre para este algoritmo de cifrado asimétrico es public key cryptography o asymmetric key cryptography. Los usos para algoritmos asimétricos no son limitados a solo autenticación como el caso de las firmas digitales discutido en la sección anterior, pero eso es un ejemplo de un algoritmo asimétrico.

RSA ALGORITHM, THE KEY, AND DIGITAL CERTIFICATES

Las claves son el secreto que permite la criptografia para proveer confidencilidad. Dejeme tomar una mirada mas cercana involucrado con RSA y y como es usada:

Como tener claves (Keys) y un certificado digital (Digital Certificate) ?

Con una firma digital RSA, con mabas partes con la intencion en autenticar el otro lado, cada parte tiene una public-private key pair. Regresando a la analogia en la seccion previa, dejeme usar dos computadoras llamadas Bob y Lois. Ellas ambas generando su propia public-private kay pair. Y ambos inscritos con un certificado de autoridad (certificate authority “CA”). Ese CA toma cada una de sus claves publicas (PUBLIC KEY) y sus nombres y direcciones IP y crea individualmente certificados digitales, y el CA emitio esos certificados de regreso a Bob y Lois, respectivamente. El CA tambien digitalmente firmo cada uno de los certificados.

Como dos partes intercambian Public Keys

Cuando bob y louis quieren autenticar cada uno en el otro, ellos envian cada uno al otro sus certificados digitales (o al menos una copia de ellos), sobre recibir de la otra parte el certificado dogital, ellos ambos verifican la autenticidad del certificado para verificar la firma del CA que ellos actualmente confian. (cuando se habla sobre confianza de un certificado de autoridad, eso realmente el medio que usted conoce quien es el CA y puede verificar la firma digital del certificado digital, para conocer la clave de ese CA.)

Ahora que Bob y Lois tienen ambos la clave publica del otro, ellos pueden autenticar cada uno en el otro esto normalmente sucede dentro del tunel VPN en ambas direcciones (cuando las firmas RCA son usadas para autenticar), para el propisito de claridad, nosotros nos concentramos solo en uno de estas partes (por ejemplo, la computadora de Bob) provee su identidad a la computadora de Lois

CREANDO UNA FIRMA DIGITAL

Bob toma algunos datos, genera un hashy entonces cifra el hash con la clave privada de Bob (note que la clave privada no ha sido compartida con nadie mas; incluso los amigos de Bob no la tienen) este hash cifrado es insertado al paquete y enviado a lois este hash cifrado es la firma digital de bob.

Lois habiendo recbido el paquete con la firma digital adjuntada primero decodifica o descifra el hash cifrado usando la clave publica de bob. Ella configura el hash decifrado para su lado por un momento y ejecuta un has contra el mismo dato que bob bob previamente hizo. Si el hash que lois genera coincide al hash descifrado, el cual fue enviado como una firma digital de Bob, ella solo ha autenticado a Bob. La Rason es por que BoB solo tiene una private key usada para la creacion de su firma digital.

CERTIFICATE AUTHORITIES

Un certificado de autoridad es una computadora o una entidad que crea y entrega certificados digitales dentro de un certificado digital esta la información sobre la identidad de un dispositivo tal como su dirección IP, (FQDN) FULLY QUIALIFIELD DOMAIN NAME, la clave pública del dispositivo. Él sea toma solicitudes de dispositivos que suplen toda esta información (incluyendo la clave pública generada por la computadora que está haciendo la solicitud) y genera un certificado digital el cual el CEA asigna un numero serial y una firma de certificado con su propia firma digital (la firma digital del CEA). También influye en el certificado final una URL que otros dispositivos pueden verificar para ver si el certificado ha sido revocado y la validez de datos del certificado (lo cual es similar a la expiración de datos de fecha de caducidad). También en el certificado esta la información sobre el CEA que emite el certificado y varios otros parámetros usados por el PKI.

Para usar una tercera parte confiando en el CEA, la computadora de bob y lois reciben y verifican la identidad del certificado de cada uno del otro (y cientos de otros) tan largo como el certificado es firmado que es CEA que es confiable para bob y lois. Cargar CA´s comerciales una tarifa para mantener certificados digitales. Un beneficio de usar un CA’s comercial para obtener

certificados digitales para sus dispositivos es que más WEB BROUSEN mantienen una lista de los mas comunes servidores CA públicos confiables, y como resultado usando un BROUSEN puede verificar la identidad de su WEB SERVICE por defecto sin tener que modificar todos los WEB BROUSEN. Si una compañía quiere configurar su propio CA interno cada uno de los dispositivos finales para confiar los certificados emitidos por su CA interno, no CA comerciales es requerido, pero el alcance de CCEA es limitado para la compañía de sus dispositivos administrados por que cualquier dispositivo fuera de lugar de la compañía no confiaría en el CEA interno de la compañía por defecto.

ROOT AND IDENTITY CERTIFICATES un certificado digital puede ser a través de un documento electrónico que identifica un dispositivo o persona. Incluye información tal como el nombre de una persona u organización, su dirección, y la clave pública del dispositivo o persona. Hay diferentes tipos de certificados incluyendo ROOT CERTIFICATES “el cual identifica al CEA”, y certificado de identidad, el cual identifica dispositivos tales como un servidor y otros dispositivos que quieren participar dentro de PKI.

ROOT CERTIFICATE

Un certificado raíz contiene la clave pública del servidor CEA y otro detalles sobre el servidor CEA por ejemplo figura siguiente.

La salida de la figura puede ser vista en MAS BROUSEN, apresar de que la ubicación podría diferir un poco dependiendo de su BROUSEN y versión.

Yo recomiendo conocer las partes relevantes de un certificado, que incluye lo siguiente:

- Serial number: emitido y rastreado por el CEA que emitió un certificado.

- Issuer: “emisor” el CEA emitió este certificado. (incluso el certificado raíz necesita tener su certificado emitido por alguien quizá incluso de el mismo).
- Validite dates: el tiempo de ventana durante el cual el certificado podría considerar valido. si una computadora LOCAL es apagada durante un pocos años, esa misma computadora puede considerar el certificado invalido debido a su propio error sobre el tiempo, usar NTP NETWORK TIME PROTOCOL es una buen idea para evitar este problema
- SUBJECTS OF THE CERTIFICATE: esto incluye la OU ORGANIZATIONAL UNIT, organization “O” CONTRY “C”, y otro detalles comúnmente encontrados en un X.500 directorio estructurado. El tema de un certificado raíz es el mismo CEA. El tema para el certificado de identidad para un cliente es el cliente.
- PUBLIC KEY: el contenido de la clave pública y la longitud de la clave son a menudo ambas mostradas. Después de todo la clave públic.
- THUMBPRINT ALGORITHM AND THUMBPRIN: este es el hash para el certificado. En un nuevo certificado raíz o ROOT CERTIFICATE, usted podría usar un teléfono para llamar y preguntar por el valor del HASH y compararlo al valor el hash que usted ve en el certificado. Si coincide, usted solo ha ejecutado OUTE-OFF-BANDS (usando el teléfono) verificación del certificado digital.

IDENTITY CERTIIFCATE

Un certificado de identidad es similar a un certificado raíz pero eso describe el cliente y contiene la llave publica de host individual “EL PUNTO”. Un ejemplo de un cliente está en el WER SERVICE que quiere soportar SSL SOCURETE SOCKET LAYER o un Reuter que quiere usar firmas digitales para la autenticación de un túnel BPN. La figura muestra un ejemplo de un certificado de identidad.

USANDO UN CERTIFICADO DIGITAL PARA OBTENER LA CLAVE O LLAVE PUBLICA DEL PEER

En sus básicos componentes, cualquier dispositivo que quiera verificar una firma digital debe tener la llave pública del emisor. Así que déjeme usar un ejemplo de usted y yo. Si nosotros queremos autenticar cada uno del otro, y nosotros ambos confiamos en un común CEA y HEMOS PREVIAMNETE SOLICITADO Y RECIBIDO el certificado digital "IDENTTY CERTIFICATE DEL SERVIDOR CEA" nosotros intercambiamos nuestros identty certificate, el cual contiene nuestra llave pública. Nosotros solo verificamos las firmas del CEA dentro del certificado digital que nosotros solo recibimos del otro usando la llave pública del CEA. En la práctica esta llave pública para el Cea es construida dentro nuestros BROUSER hoy en día para los servidores públicos CEA. Una vez verificado los certificados de cada uno del otro, podemos entonces confiar su contenido de aquellos certificados (y más importante, la llave publica). Ahora que usted y yo ambos tenemos la llave publica de cada uno del otro, podemos usar aquellas llaves públicas para verificar las firmas digitales de cada uno.

X.500 AND X.509v3 CERTIFICATE

x.500es una serie del estándar concentrado en directorio servicios como esos directorios son organizados. Muchos sistemas operativos oculares de red han sido basados en x.500, incluyendo MICROSOFF ACTIVE DIRECTORY. Este x.500 estructura la fundación de la forma en la cual usted ve comúnmente elementos de directorio tales como CN=BOB (COMMON NAME=CN), OU=ENEGINEERING (ORGANIZATIONAL UNIT=OU), O=CISCO.COM (ORGANIZATION=O), y así dentro de un "ORG-CHART" formado como una pirámide. X.509 versión 3 es un estándar en certificados digitales es ampliamente aceptado e incorpora muchos de los mismos directorios y estándares nombrados. Un protocolo común que es usado para ser LOOKUPS en lugar de hacer búsquedas de un directorio es llamado LIGHTWEIGTH DIRECTORY ACCESS PROTOCOL (LDAP). Un común uso de este es teniendo un certificado digital siendo usado para la autenticación. Y entonces basado en los detalles de ese certificado (por ejemplo, el OU=VENTAS DELMISMO CERTIFICADO), EL USUARIO PODRIA

SER dinámicamente asignado al acceso justo al que está asociado con ese grupo dentro del directorio activo o algunas otras base de datos accesibles LDAP. El concepto es definir el momento justo y entonces aplazarlo una y otra vez. Un ejemplo es configurando el directorio activo para la red y entonces usarlo eso para configurar ya para controlar que acceso está previendo cada usuario después de que él o ella autentica.

Como una revisión, mas certificado digital contiene la siguiente información:

- Serial Number: Asignado por el CA y usado para identificar únicamente el certificado.
- Subjec: la persona o entidad que esta siendo identificado.
- Signature algorithm: el algotitmo especifica que fue usado para firmar el certificado digital.
- Signature: la firma digital del certificado de aoutoridad, el cual es usado por dispositivos que quieren verificar la autenticidad del certificado emitido por el CA.
- Issuer: La entidad o CA que creo y emitio el certificado digital.
- Valid From: la fecha que llega a ser valido
- Valid to: la fecha de expiración del certificado.
- Key usage: la función par la cual la clave publica en el certificado puede ser usada.
- Public key: la porción publica del public and private key pair generada por el host cuyo certificado esta siendo examinado.
- Thumbprint algorithm: el hash algorith usado para la integridad de datos.
- Thumbprint: el actual hash
- Certificate revocation list location: la URL que puede ser verificada para ver si el numero serial de cualquier certificado emitido por el CA ha sido revocado.

Authenticating and enrolling with the CA

Si usted quiere usar un nuevo CA como una entidad confiable, y quiere solicitar y recibir su propia identidad de certificado de esta CA esto es realmente un proceso de dos pasos.

PASO 1. El primer paso es autenticar en el servidor CA, o en otras palabras confiar en el servidor CA. Desafortunadamente si usted no tiene una llave publicapara el servidor CA usted no puee verificar el certificado digital del servidor CA, el cual puede ser encontrado en el certificado raíz del CA, pero no puede verificar la firma de un certificado, hasta que tenga la llave publica.
Obtener el ball Rolling, usted podría descargar el certificado raíz y entonces usar un out-of-band method. Es tal como hacer una llamada telefonica para validar el certificado raíz. Esto puede ser hecho después de descargar el certificado raíz y buscar el valor del hash, llamanado al administrador del CA raíz y preguntándoles verbalmente diciendo usted cual es el hash. Si e hash que ellos le dicen y usted sobre la llamada telefónica coincide el hash que usted ve en el certificado digital, usted entonces conoce que el certificado es valido, y usted entonces podría utilizar la llave publica contenida en el certificado para verificar futuros certificados los cuales son asignados por ese CA, este proceso de la obtención del certificado raíz CA instalado a menudo referido como una autenticación del CA. Actualmente los buscadores web automáticamente este proceso para Cas es bien conocido.

PASO 2. Después de que usted ha autentica la raíz del CA, usted tiene un bien conocido certificado raíz para ese CA, usted puede solicitar su propio certificado de identidad. Esto involucra generar un public-

private key pair he incluirlo en la porción de la llave publica y cualquier solicitud para su propio certificado de identidad. Un certificado de identidad podría ser para un dispositivo o una persona. Una vez que usted hace esta solicitud, el CA puede tomar toda su información y generar un certificado de identidad para usted. El cual incluye su llave publica. Y entonces enviar ese certificado de vuelta a usted, si esto es hecho electrónicamente, ¿Cómo verifica usted el certificado de identidad que obtuvo es realmente del server CA que usted confio? La respuesta es simple por que el CA no solo ha emitido el certificado también firmo el certificado. Por que usted autentico antes en el server CA y usted tiene una copia de su certificado digital con su llave publica, usted ahora puede verificar la firma digital que puso en su propio certificado de identidad. Si la firma del CA es valida, usted también sabe que su certificado es valido y asi usted puede instalarlo y usarlo.

Public Key Cryptography Standards

Muchos standares esta en uso por el PKI, muchos de ellos tienen public key cryptography standard (PKCS). Algunos de estos estándares controlan la forma y uso de certificados, incluyendo solicitudes para nuevos certificados CA, el formato para un archivo que va a ser el nuevo certificado de identidad, y el formato de archivo y acceso de uso para certificados. Teniendo los estándares dentro del lugar con interoperabilidad entre diferentes servers CA y muchos diferentes clientes CA.

Aquí están unos pocos estandars, usted debería llegar a familiarizar con los cuales incluyen protocolos para ellos mismos y protocolos usados para trabajar con certificados digitales.

- PKCS#10: este es un formato de una solicitud de certificado enviado a la CA que quiere recibir su certificado identidad. Este tipo de solicitud incluiría la llave publica para la entidad desiganada a certificar.

- PKCS#7: este es un formato que puede ser usado por un CA como una respuesta para la solicitud PKCS#10. La respuesta misma muy probablemente seria el certificado de identidad que ha sido previamente solicitado.
- PKCS#1: RSA Cryptography Standard
- PKCS#12: un formato para almacenar ambas public y private key usando un symmetric password-based key to “unlook” los datos cuando la llave necesite ser usada o accesada.
- PKCS#3: Diffie-Hellman key Exchange

Simple Certificate Enrollmnete Protocol

El proceso para autenticar un server CA, generando una public private key pair, solicitando un certificado de identidad, y entonces verificando e implementando el certificado de identidad puede ser un proceso de varios pasos. Cisco, en asociación con unos pocos vendors, desarrollaron Simple Certificate Enrollment Protocol (SCEP), el cual puede automatizar mas del proceso para solicitar e instalar un certificado de identidad. A pesar de que no es un standard abierto, es soportado por mas dispositivos cisco y lo hace conveniente para tener e instalar ambos root y identity certificates, como vera en acción mas tarde en el capitulo.

Revoked Certificates

Si usted decomisa un dispositivo que ha sido asignado un certificado de identidad, o si el dispositivo asignado a un certificado de identidad ha sido comprometido y cree que la llave privada no es tan larga o “PRIVADA”, podría solicitar al CA que el certificado previamente emitido sea revocado. Esto posee un único problema. Normalmente cuando dos dispositivos autentican cada uno con el otro, ellos no necesitan contactar al CA para

verificar la identidad de la otra parte. Esto es por que los dispositivos ya tienen la llave publica del CA y pueden validar la firma en un certificado de pareja sin contactar directo al CA. Asi que aquí esta el desafio, si un certificado ha sido revocado por el CA, y el peer no esta verificando con el CA cada momento ellos prueban autenticar al peer, como un peer conoce si el certificado recibido ha sido revocado? La respuesta es simple: esto es verificar y mirar. Un certificado digital contiene información en donde una lista actualizada de certificados revocados pueden ser obtenidos. Esta URL podría señalar el server CA el mismo o algún otro recurso publico disponible en internet. El certificado revocado esta listado basado en el numero de serie del certificado. Y si un peer ha sido configurado para verificar certificados revocados, eso agrega esta verificación antes de completar la autenticación con un peer. Si un CRL (certificate revoked list) es verificada, y el certificado del peer esta en esa lista, la autenticación para en ese momento. Las tres básicas vías para verificar si el certificado ha sido revocado son las siguientes, en el siguiente orden.

- CRL: esta es una lista de certificados, basada en su numero serial que inicialmente ha sido emitida por el CA pero ya que ha sido revocado y como resultado no seria confiable. Un CRL podría ser muy grande, y el cliente tendría que procesar la lista de entrada para verificar el certificado no este dentro de la lista. Este es el protocolo primerio usado para este propósito, comparado a OSCP y AAA. Un CRL podría ser accesado por varios protocolos, incluyendo LDAP y HTTP, un CRL podría también ser obtenido via SCEP.
- Online Certificate Status Protocol (OCSP): este es una alternativa para CLR´s. usando este método, un cliente simplemente envía una solicitud para encontrar el estatus de un certificado y obtener una respuesta sin tener que conocer la lista completa de certfivados revocados.
- Authorization, Authentication and Accounting (AAA): Cisco AAA service también prove soporte para validar certificados digitales, incluyendo una verificación para ver si un certificado ha sido revocado, por que esta es una solucion propiedad, este no es a menudo usado en PKI.

Usos de Certificados Digitales

Pueden ser usados por clientes quienes quieren autenticar un web server para verificar que ellos están conectados al servidor correcto usando HTTP secure (https), TRANSPORT LAYER SECURITY (TLS), o SECURE SOCKET LAYER (SSL), para el promedio de usuarios quienes no tienen que escribir esos protocolos, pero simplememnte se benefician de usarlos, son todos efectivamente los mismos, el cual es HTTP combinado con TLS/SSL para los beneficios de seguridad. Esto significa que los certificados digitales pueden ser usados cuando hace transacciones bancarias en línea de su pc la sitio web del banco. Eso también significa que si usted usa tecnología SSL para su remote-access VPN usted también puede usar certificados digitales para autenticar el peer (en cada lado) de la VPN.

También puede usar certificados digitales con el protocolo family de IPsec, el cual puede tanbien usar certificados digitales para la porción de autenticación.

Los certificados digitales pueden también ser usados con protocolos tales como 802.1x el cual involucra autenticación en el borde de la red antes de permitir paquetes de los usuarios y tramas para progresar a travez de la red. Un ejemplo es una red inalámbrica, controlar el acceso y requerimiento de autenticación, usando certificados digitales para su PC /usuarios, antes de permitirlos dentro de la red.

PKI TOPOLOGIES

No hay una sola talla para todas las soluciones PKI. Una pequeña red, un singular server CA puede ser suficiente, pero en una red con 30000 dispositivos, un solo server no puede proveer la disponibilidad y tolerancia requerida. para contestar a este problema, vamos a investigar la opción disponible para nuestra implementación del PKI, usando varias topologías,

incluyendo singular y jerárquica. Vamos a empezar con un solo CA y expandiendo desde allí.

Single Root CA

Si usted tiene un CA de confianza, y usted tiene 10 o cientos de clientes quienes quieren autenticar ese CA y solicitar su propio certificado de identidad, allí podría ser grande la demanda de un solo server incluso a travez de un solo CA no tiene que ser directamente involucrado en la autenticación dia a dia que sucede entre peers. Para descargar algunas de las cargas de trabajo de un solo server, usted podría publicar URL´s en otro server. Esto hace en un sentido tener al menos alguna tolerancia para su PKI, lo cual significa mas que solo una solo root server.

Hierarchical CA with subordinate CAs

Una de nuestras opciones para suponer falta de tolerancia e incrementar capacidad es para usar intermediarios o subordinados Cas para asistir al CA raíz. El root CA es un tipo de colina. El CA raíz delega la autoridad (para subordinados CAs) para crear y asignar certificados de identidad para clientes. Esto es llamado un herarchical PKI topology. El CA raíz firma el certificado digital de sus sobordinados o intermediarios CAs, y el subordinado CA es el primero para emitir certificados para clientes. Para un cliente verificar el “chain” de autoridad, un cliente necesita ambos los certificados del subordinado y el raíz. El certificado raíz (y su llave publica) es solicitada para verificar la firma digital del CA subordinado, y el certificado del subordinado (y su llave publica) es requerida para para verificar la firma del subordinado CA. Si hay multiples niveles de subordinados de CAs, un cliente necesita certificados de todos los dispositivos en la cadena de todas la vías al CA raíz que emitio los certificados de clientes.

Cross-Certifying CAs

Otro enfoque para PKI jerárquico es llamado cross-certifying. Con cross-certifying usted podría tener un CA con una relación de confianza horizontal sobre un segundo CA asi que los cliente ya sea de CA cloud confían la firma de otro CA.

PUTTING the PIECES of PKI to WORK

Está sección cubre cómo implementar estos componentes en un red de producción actual.

Tomando una mirada de los componentes para el PKI, la infraestructura de llave publica. Ambos el Adaptive Secure Applince (ASA) y routers cisco pueden usar certificados digitales. Permita tomar una mirada como instalar certificados digitales en un ASA, usando el Adaptive Secure Device Manager (ASDM)

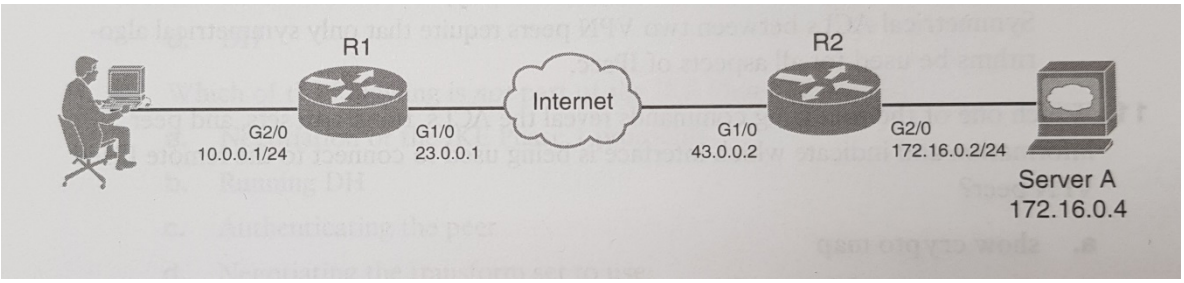
La figura muestra el principal tablero del dispositivo ASDM.

CAPITULO 6

FUNDAMENTALS OF IP SECURITY

IPsec es uno de los mas maduros standards de VPN en la industria, el secreto de IPsec es que no esta encerrado dentro de un especifico protocolo o incluso un conjunto de protocolos. Como tecnología avanzada, asi que pueden los protocolos que están siendo usados por IPsec. La meta de IPsec es bastante simple, proveer cofidencialidad, integridad de datos, y autentiaccion de una VPN. Implementando todo esto en la capa 3 individualmente, protegiendo cada uno de susu envios de una teerminal VPN hasta alcanzar le otra tereminal.

Para comprender mejor como IPsec opera, tomemos una vista de una topología simple que puede ser usada como un marco de este capítulo de entrada, mostrado en la siguiente figura.



Metas de IPsec y métodos usados para implemtarlos.

GOAL	Method that Provides the Feature
Confidentiality	Encryption
Data Integrity	Hashing

Peer Authentication	Pre-shared keys, RSA Digital Signature
Antireplay	Integred into IPsec, basically applying serial number to packets

La metas pueden ser descritas como lo siguiente:

→ Confidetiality: provee a través de cifrado cambiar el texto claro dendro del texto cifrado
→ Data integrity: provee a través del hashing y a través de hashed message authentication code (HMAC) para verificar que los datos no han sido manipulados durante su trancito a trvesando la red.
→ Authentication: provee a través de la autenticación los peer VPN empezando la sesión VPN usanso pre-shared keys (PSK) o firmas dgitales (aprovechando certificados digitales). La autenticación puede también ser hecha continuamente mediante el uso de un HMAC el cual incluye un secreto conocido por los 2 teminales.
→ Antireplay protection: cuando las VPN son establecidas, los peers pueden secuencialmente numerar los paquetes, y si un paquete es intentado ser respondido otra ves (quizá por un atacante), el paquete no será aceptado por que el dispositivo VPN cree que ya ha sido procesado ese paquete.

De nuestra topología, podríamos decidir que cualquier trafico de la red 10.0.0.0 en la izquierda necesita ir a la red 172.16.0.0 a la derecha debería ser primero cifrada por R1, el cual entonces enviaría los paquetes protegidos sobre internet hasta alcanzar R2. La nube entre R1 y R2 representa redes desconocidas, tal como internet. R2 entonces decifra cada paquete y envía el trafico dentro de su destino final, el cual puede ser una PC o un server en la red 172.16.0.0. los paquetes protegidos podrían ser cifrados, hashed, y mantenerlo rastreado los 4 beneficios listados previamente.

The Internet Key Exchange (IKE) Protocol

IPsec usa el internet key exchange (IKE) para negociar y establecer seguridad site-to-site o remote-access VPN´s tunnels. IKE es un marco de referencia que ws provisto por Internet Security Association an Key Management Protocol (ISAKMP) y parte de otros dos protocolos de aadministracion de llaves (claves), llamadas Oakley and Secure key Exchange Mechanism (SKEME).

Hay dos versiones de IKE:

1. IKEv1: definido en el RFC 2409, the internet key Exchange
2. IKE versión 2 (IKEv2): definido en el RFC 4306, Internet Key Exchange (IKEv2) Protocol

KEv2 mejora las funciones de intercambio de llave de ejecución dinámica y autheticacion de peer.

IKE2 simplifica el flujo de intercambio de llave e introduce medidas para solucionar vulnerabilidades presentes en IKEv1. Ambos IKEv1 e IKEv2 operan en dos fases. IKEv2 provee una mayor simpleza y más eficiente intercambio.

Pase 1 en IKEv2 es IKE_SA, consiste del mensaje par IKE_SA_INIT. IKE_SA_INIT es usado para iniciar la negociación IKE. IKE_SA es comparable a IKEv1 fase 1. The Security Association (SA) es la clave material usada para cifrar paquetes sobre el túnel VPN. Los atributos de la fase IKE_SA son definidos en la política de intercambio de llave (clave). La segunda fase en IKEv2 es CHILD_SA. El primer CHILD_SA (Pase 2 SA) es el IKE_AUTH messange pair. Esta fase es

comparable a el IKEv1 fase 2. Adicional CHILD_SA message pairs puede ser enviado para reprogramar y mensajes de información. El atributo CHILD_SA es definido en la política de datos.

Diferencias de IKEv1 incluyen las siguientes:

- IKEv1 fase 1 tiene 2 posibles intercambios: modo principal y modo agresivo. Hay un solo intercambio de message pair para IKEv2 IKE_SA.
- IKEv2 tiene un simple intercambio de dos message pairs para CHILD_SA. IKEv1 usa al menos 3 message pair Exchange para fase 2.

The PLAY by PLAY for IPsec

Dejeme iniciar la discucion del play by play asumiendo que los dos routers han sido correctamente configurados para ser peers vpn y que ellos tienen por defecto rutas apuntando a la internet u que ellos fueron ambos energizados. con una VPN site-to-site, como se muestra en nuestra topología, cada uno de los peers podría también ser llamado GATEWAY VPN, el cual esta sirviendo a los clientes en 10.0.0.0/27 y 172.16.0.0/24. Los dos routers llegaran a ser IPsec peers con cada uno en el túnel IPsec sobre internet.

La primera cosa que el router R1 va hacer, si se le ha sido dicho cifrar y proteger trafico que es la fuente de la red 10.0.0.0/24 y destinado a la 172.16.0.0/24, este espera por ese trafico por aparecer. Un usuario en la red 10.0.0.0 envia paquetes al servidos A en la red 172.16.0.0, y ahora R1 ve estos paquetes y necesita cifrarlos y protegerlos antes de enviarlos. Desafortunadamente el router todavía no ha establecido un túnel VPN entre el y el router a la derecha. Asi que, si el trafico apareció en R1 y necesito ser cifrado basado en políticas, R1 iniciaria la negociación con el router a la derecha, en este caso, R1 seria el iniciador de la VPN.

STEP 1: Negotiate the IKEv1 Phase 1 Tunnel

Cuando estos dos router primero negocian es algo llamado un IKE PHASE 1 TUNNEL, esto puede ser hecho en uno de dos modos: modo principal (main mode) o modo agresivo (aggressive mode). Modo principal usa mas paquetes para el proceso que modo agresivo. Pero modo principal es considerado mas seguro. Mas recientes imolementaciones VPN por defecto usan modo seguro, el primer tunnel (the IKE PHASE 1) es usado entre dos routers para hablar directamente uno con el otro. Este tunel (una vez establecido) no va a ser usado para enviar paquetes del usuario, mas bien solo para proteger trafico relacionado a administración para la VPN entre los dos routers, los paquetes tales como los keepalive message para verificar que el túnel VPN esta todavía trabajando es un ejemplo de trafico que esos dos routers envían a través de IKE PHASE 1 directamente al otro.

Porque R1 primero recibió trafico que necesita ser cifrado y no había IKE PHASE 1 Tunnel en el lugar, el router a la izquierda llega a ser el iniciador para la negociación. El iniciador envía sobre todo su configuración/ parámetros por defecto que usara para IKE PHASE 1. 5 temas basicos necesitan ser agregados entre los dos dispositivos VPN (en este caso los dos routers) para IKE PHASE 1 Tunnel sea exitoso:

→ HASH ALGORITHM: este podría ser MD5 (Message Digest 5 algorithm) o SHA (Secure Hash Algorithm) en la mayoría de los dispositivos.
→ ENCRYPTION ALGORITHM: este podría ser DES (Digital Encryption Standard) “mala idea”, 3DES (Triple Digital Encryption Standard) “mejor idea” o AES (Advanced Encryption Standard) “la mejor idea” con varias longitudes de llave (clave) “mas larga la clave mejor”.
→ Diffie-Hellman (DH) group to use: el DH “group” se refiere al tamaño de modulo (longitude de la llave (clave)) para usar para el intercambio de llave DH. Grupo 1 usa 768 bits, grupo 2 usa 1024 bits, grupo 5 usa

1536. Mas seguro DH group es parte del next-generation encryption (NGE):

* Group 14 o 24: provee 2048 bit DH
* Group 16 y 15: soporta 3072 bit y 4096 bit DH
* Group 19 o 20: soportan 256 y 384 bit ECDH groups,respectivamente
  El propósito de DH es generar material de codificación compartida (llaves (claves) simétricas) que pueen ser usadas por los dos peers VPN para algoritmos simétricos, tales como AES. Es importante notar que el propio intercambio DH es asimétrico y las llaves (claves) resultantes que son generadas son simétricas.

→ Authentication method: usado para verificar la identidad del peer VPN en el otro lado del túnel, la opción incluye un pre-shared key (PSK) usado solo para la autenticacion o firmas RSA (las cuales apalancan la llave publica (clave publica) contenida en el certificado digital).

→ Lifetiem: cuanto tiempo hasta IKE PHASE 1 tunnel seria tornado abajo. (por defecto es un dia listado en segundos) este es el único parámetro que no tiene exacta coincidencia con el otro peer para ser aceptado. Si todos los otros parámetros coinciden y el lifetime es diferente, ellos están deacuerdo en usar el tiempo de vida mas pequeño entre los dos peers. Un tiempo de vida mas corto es considerado mas seguro por que da a un atacante menos tiempo para calcular llaves (claves) usada para el actual túnel.

COMO RECORDAR LAS 5 CLAVES DE NEGOCIACION IKE PHASE 1
Como un practico camino para re-llamar las 5 piezas en la negociación del IKE phase 1 tunnel , podría recordar HAGLE para IKE phase 1
H: hash
A: Authentication
G: DH group
L:Lifetime
E:Encryption

PASO 2: RUN THE DH KEY EXCHANGE

Ahora teniendo agregado la política pase 1 IKE del peer, los dos dispositivos ehecutan DH key Exchange. Ellos usan el DH group (DH key for the Exchange) ellos están de acuerdo durante la negociación, y al final de este intercambio de llave (clave), ellos tienen ambos llaves (claves) simétricas (lo cual es un via para decir que ellos tienen la misma llave (clave) secreta que pueden usar con algoritmos simétricos). DH como usted aprendio en un capitulo previo , permite dos dispositivos que todavía no tienen una coneccion segura para establecer claves secretas compartidas (claves que pueen ser usadas con algoritmos simétricos tales como AES).

PASO 3: AUTHENTICATE THE PEER

La ultima pieza de IKE phase 1 es validar o autenticar al peer del otro lado. Para autenticar, ellos usan lo que sea que estén deacuerdo para iniciar HAGLE, y si ellos exitosamente autentican con el otro, nosotros ahora tenemos un IKE phase 1 tunnel ubicado entre los dos VPN Gateway. Este túnel es bidireccional, significa que el dispositivo puede enviar o recibir dentro de IKE phase 1 tunnel. La utenticacion puede ser hacha ya sea usando PSK o RSA firmas digitales (dependiendo en que ellos estén de acuerdo para usar en el paso 1

Que pasa con los paquetes originales del usuario.

Aquí esta el desafio: después de todo el trabajo que fue para construir el túnel IKE phase 1, este tunes es usado solo como un túnel de administración asi que los dos routers pueden seguramente comunicarse ditectamente uno con el otro. Este túnel IKE phase 1 no es usado para cifrar o proteger los

paquetes del usuario final. Para proteger los paquetes del usuario (lo cual es el objetivo de IPsec), los dos dispositivos VPN construyeron un segundo túnel con el solo propósito de cifrar los paquetes delusuario este segundo túnel es llamado IKE phase 2 tunnel. Es comúnmente referido como (drum roll, phase) IPsec tunnel. Este túnel IKE phase 2 usado para proteger los paquetes del usuario final como aquellos paquetes atravesando la red no confiable entre los peers VPN.

Leveraging what they have already built (aprovechando lo que ya han construido).

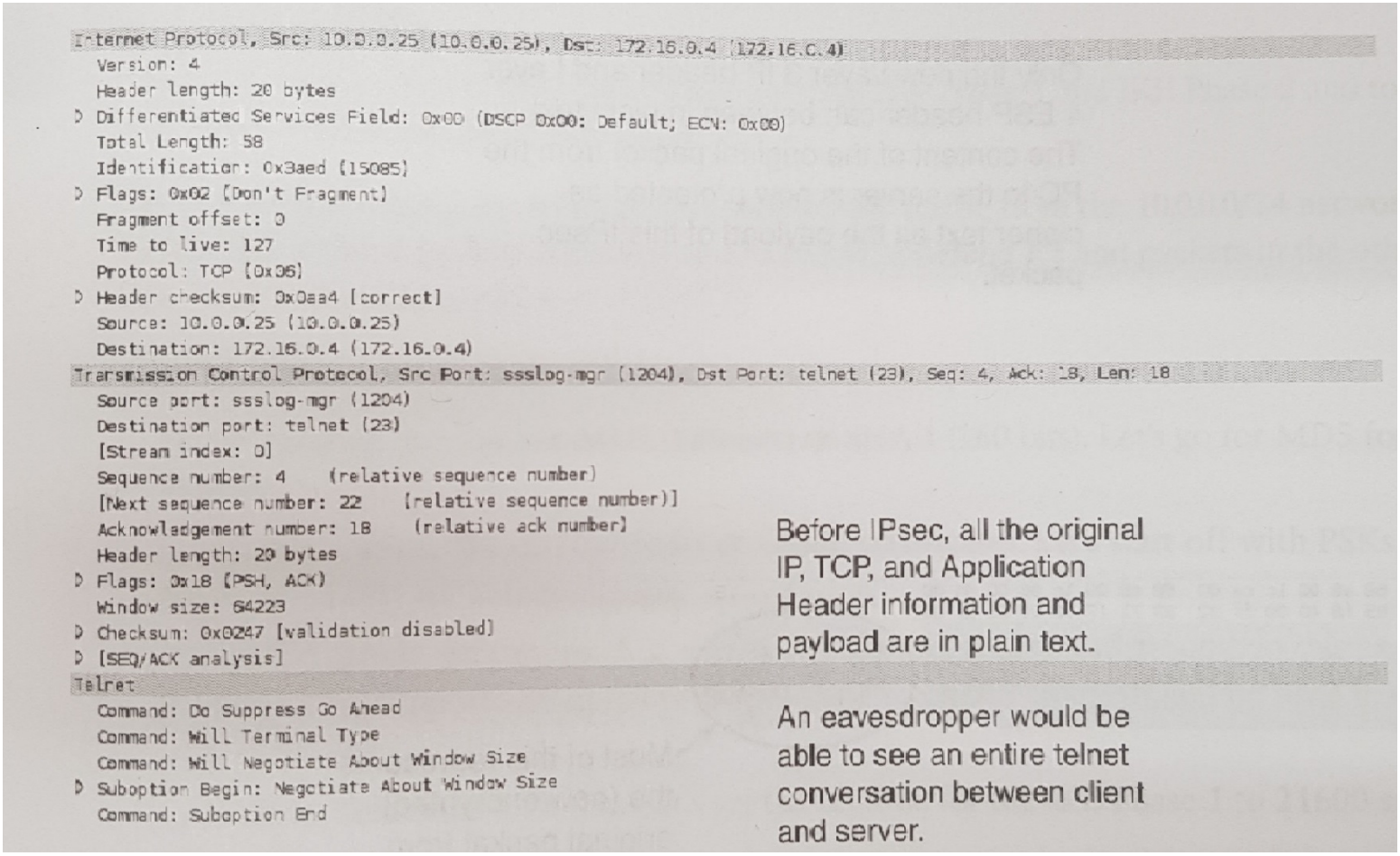
Los dos routers con un hermoso tunel IKE phase 1, pueden usar ese tunel Ike phase 1 para negociar seguro y establecer el IPsec phase 2. En mis años de trabajo con estudiantes, esto es donnde la confusión a veces viene, por que durante la configuración se dicen ellos mismos, “no especifique los detalles para el cifrado y hashing? Porque esta preguntadoles otra vez la configuración?” la respuesta es que nosotros tenemos que instalar comandos específicos para especificar la política de IKE phase 1, y nosotros instalamos un diferente conjunto de similares comandos para especificar IKE phase 2 (incluyendo el componente llamado ***transform set***).

Inmediatamente después de que IKE phase 1 es establecido (los dos diferentes modos para configurar IKE phase 1 son main mod, el cual toma mas paquetes o aggressive mode el cual toma menos paquetes y es considerado menos seguro), los routers inmediatamente empiezan a estableces IKE phase 2 tunnel.

El IKE phase 1 es su túnel de administración, la conversación y negociación completa del IKE phase 2 son completamente hechas en privado por que IKE phase 1 protege el trafico negociado. El túnel IKE phase 2 incluye el hasing y algoritmo de cifrado. El nombre del modo para construir el túnel IKE phase 2 es llamado Quick mode.

Ahora IPsec puede Proteger los paquetes del usuario.

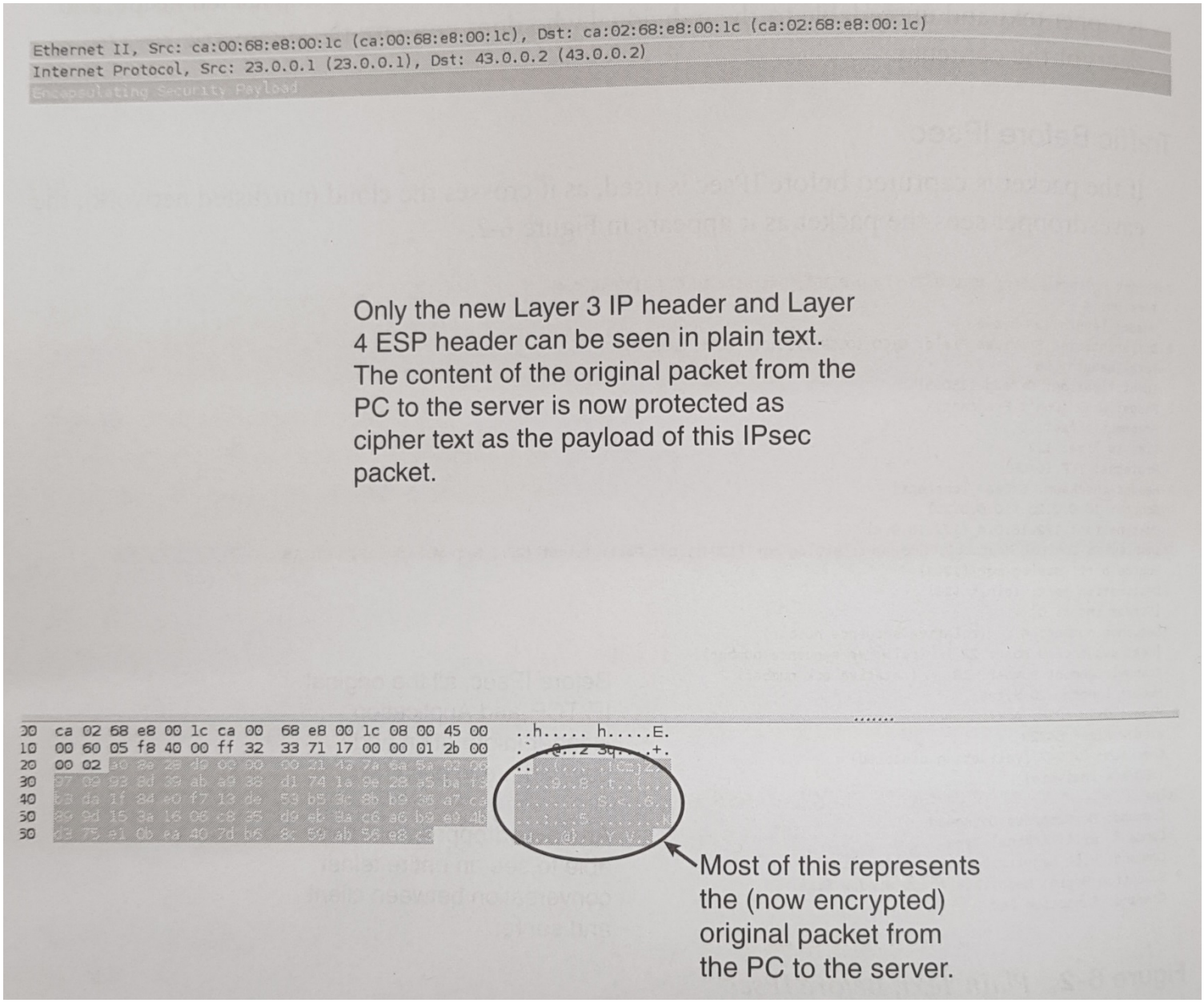
Una ves construido el tune Ike phase 2, el router puede entoces comenzar a cifrar el trafico del usuario y eviar aquellos paquetes cifrados directamente al peer al lado mas lejano. Desde la perspectiva de internet, mira como la afuente de los paquetes IP de R1 estan siendo enviados a la dirección IP de R2. La carga útil cifrada de esos paquetes contiene las originales direcciones IP del usuario quien esta enviando un paquete al server y viceversa. Si esos paquetes son escuchados a escondidas, el escuchador ve las direcciones IP involucradas entre los dos routers; la carga útil (el paquete original) ha sido cifrado y encapsulado dentro , un texto cerrado e inalcanzable para la persona quien no tiene las claves simétricas para descifrar el contenido.



En la figura cualquier escuchante puede ver y determinar la conversación completa entre el cliente y el server. Por que telnet no ofrece capacidad de cifrado. El atacante podría aprender el username y password usado para iniciar telnet y cada comando que el usuario telnet muestre como resultado.

Trafico después de IPsec

Después de configurar R1 y R2 para llegar a ser peers o Gateway VPN, y decirles que todos los paquetes entre entre las dos redes 10.0.0.0 y 172.16.0.0 deberian ser protegidas por IPsec, R1 y R2 negocian y construyen su túnel VPN (IKE phase 1 e IKE phase 2), y entonces cualquier trafico de sus red y destino para el otro es protegido. Permita considerar los paquetes mostrados en la figura anterior . cuando R1 ve este mismo paquete repartiendo a 172.16.0.4 y su fuente esta en la 10.0.0.0/24. R1 usa el IKE phase 2 y cifra los paquetes y encapsula paquetes cifrados con un nuevo



encabezado IP que muestra la fuente ip R1 y destino IP R2. La capa 4

mostraria como esta Encapsulating Security Payload (ESP), el cual esta reflejado en el encabezado como protocol #50. Cualdo R2 recive esto des encapsula los paquetes , ve que es ESP, y entonces procede a descifrar los paquetes originales. Una vez descifrado, R2 envia en texto plano al server 172.16.0.4. el paquete cifrado, como atravesó sobre la no confiable red entre R1 y R2, aparece, como muestra la figura.

CONFIGURANDO Y VERIFICANDO IPsec

Ahora que hemos tomado una mirada como el bloque construido para IPsec, vamos aplicar lo que aprendio para la topologoa introducida al principio del capitulo.

Herramientas para configurar el Tunnel

En el curso CCNA Security, CCP cisco configuration profesional es usado para configurar tuneles VPN, incluyendo ambos IKE phase 1 e IKE phase 2. Nosotros usamos CCP aquí, pero usted también puede aprender el CLI command line interface equivalente para cada comando, los cuales están anotados para dejarle conocer cada comando hecho.

START WITH A PLAN

La primera cosa para planear –es que protocolo a usar para IKE phase 1 e IKE phase 2 e identificar cual trafico será cifrado.

De la topología, vamos a estar de acuerdo para cifrar cualquier trafico de la 10.0.0.0/24 detrás de R1 y aquellos paquetes van a ir a la 172.16.0.0/24 detrás de R2 y viceversa.

Para IKE phase 1 vamos a usar lo siguiente:

H: para HASHING, podemos usar MD5 (128bits) o SHA-1 (160 bits). Vamos ir por MD5 para IKE phase 1

A: Authentication. Podemos usar PSK o certificados digitales. Vamos a empezar con PSK (un password realmente) para autenticar.

G: para Diffi-Helman group, podemos usar 1,2 o 5 en los routers. Usemos grupo 2 en el ejemplo. Si su router soporta grupo 14 o mas altos, los grupos mas altos DH serian usados porque son mas seguros.

L: el tiempo de vida por defecto es de un dia, vamos a configurar el lifetime para IKE phase 1 para 21600 segundos (6 horas).

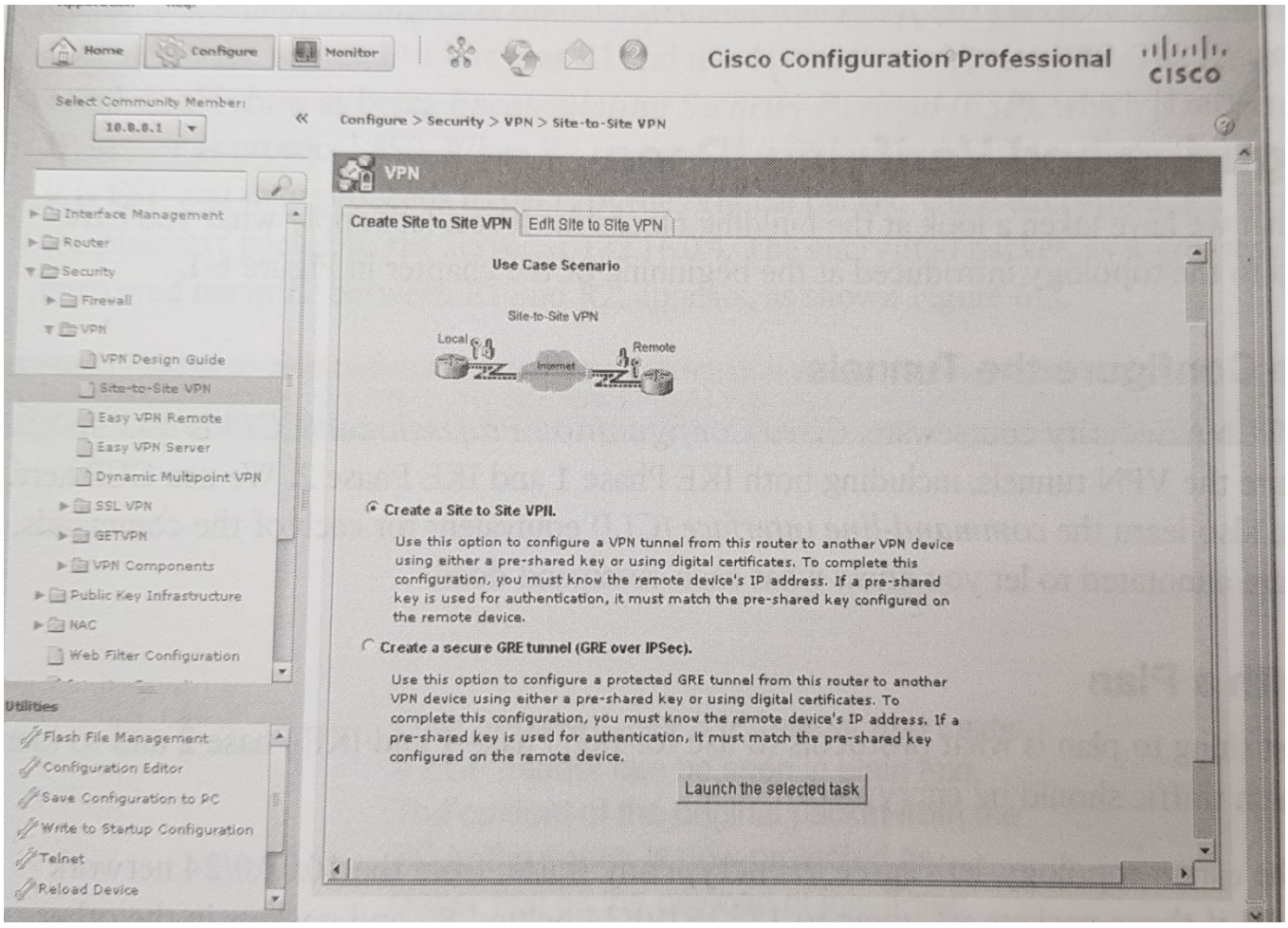
E: “Encryption” cifrado de IKE phase 1 puede ser DES, 3DES o AES. Vamos a usar 128-bit AES.

Ahora para la fase 2, también necesitamos decidir hashing y cifrado (encryption) como minimo. Podemos usar por defecto el lifetime. Para hashing, usemos SHA (solo para ver la diferencia entre hashing aquí y el

hashing IKE phase 1). Vamos también a usar AES-256 en IKE phase 2. Las Politicas usadas para IKE phase 2 son llamadas transform sets.

PLICANDO LA CONFIGURACION

Con todo eso en mente, vamos a empezar la configuración en R1. Usando CCP, seleccionar R1 del menú drop-down y navegando a **Configure > Security > VPN** . De allí verificamos que la opción seleccionada es **Create a Site-to-Site VPN**. Y entonces hacer click en el boton **Launch the Select Task** como muestra la fihura.



Siguiendo, se le indica a cualquiera uasr Quick Setup o Step by Step Wizard. Quick Setup usa los valores por defecto para IKE phase 1 e IKE phase 2 que

son construidos dentro CCP. Usted quiere personalizar las políticas, escoja el Step by Step Wizard, como muestra la figura y entonces hacer click en next.

De la interface drop-down list, seleccione la interface en R1 que será la salida a internet (será también la interface hacia su peer R2), y configure la dirección ip del peer (para alcanzar la dirección del peer en internet). En este caso la dirección de salida de R2 es la 43.0.0.2, seleccione la opción de autenticación usando PSK y configure la llave (clave). (esta necesita ser la misma llave (clave) de ambos lados. Para este ejemplo usamos PSK cisco123 para la autenticación IKE phase 1). Después de ingresar los datos, los revisamos para estar seguros y ser presisos. Como muestra la figura y entonces hacemos click en next.

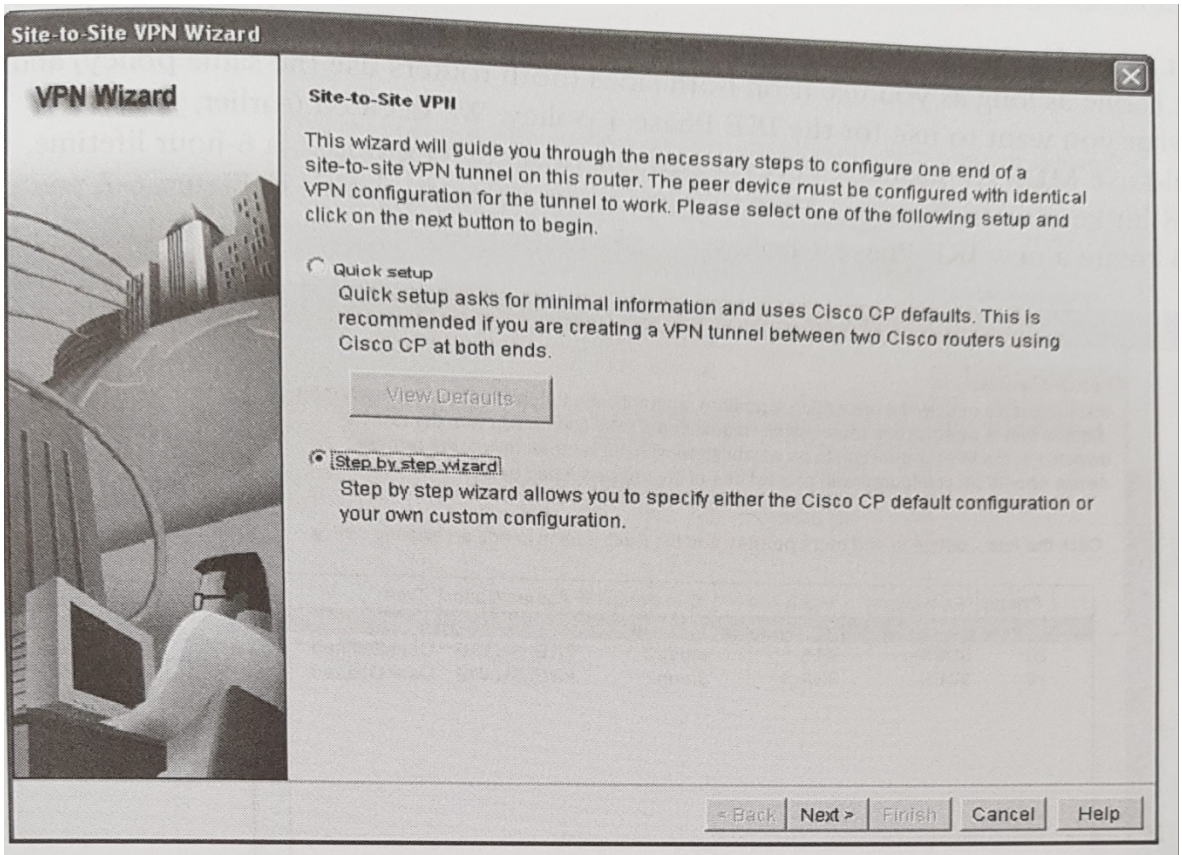
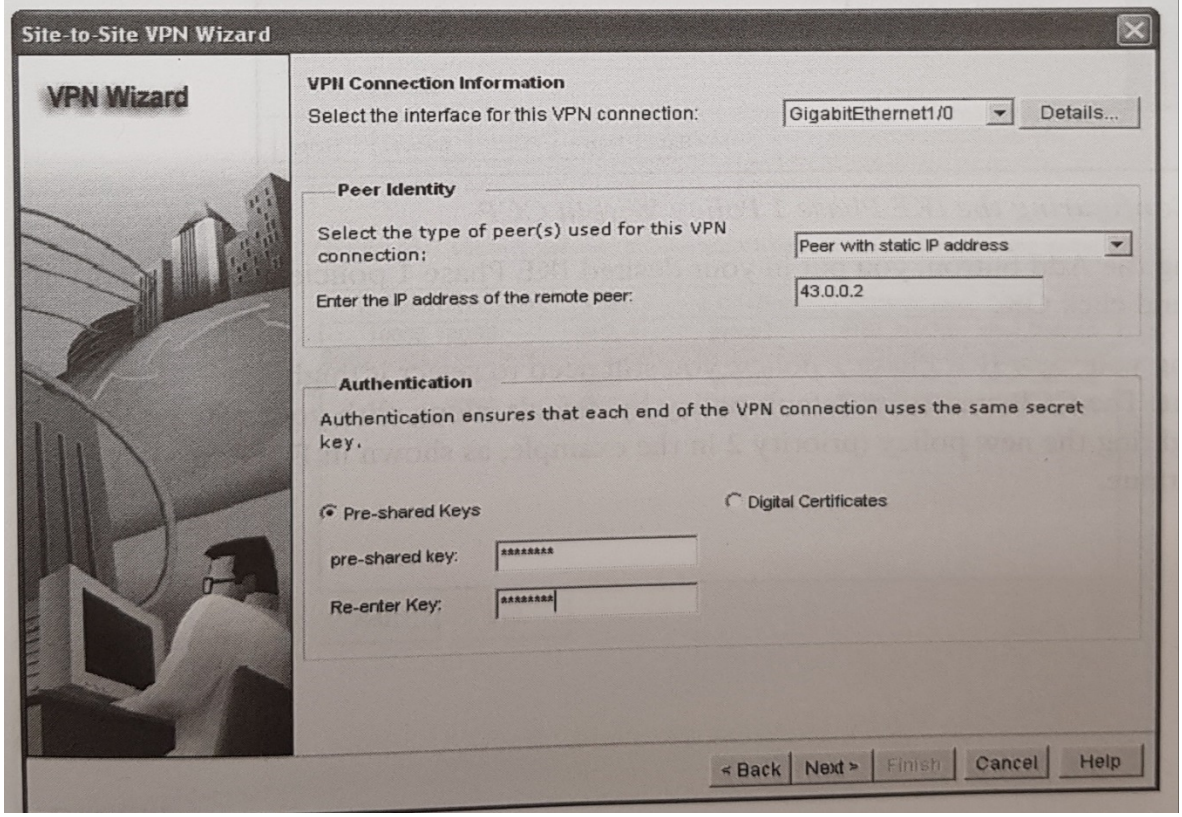
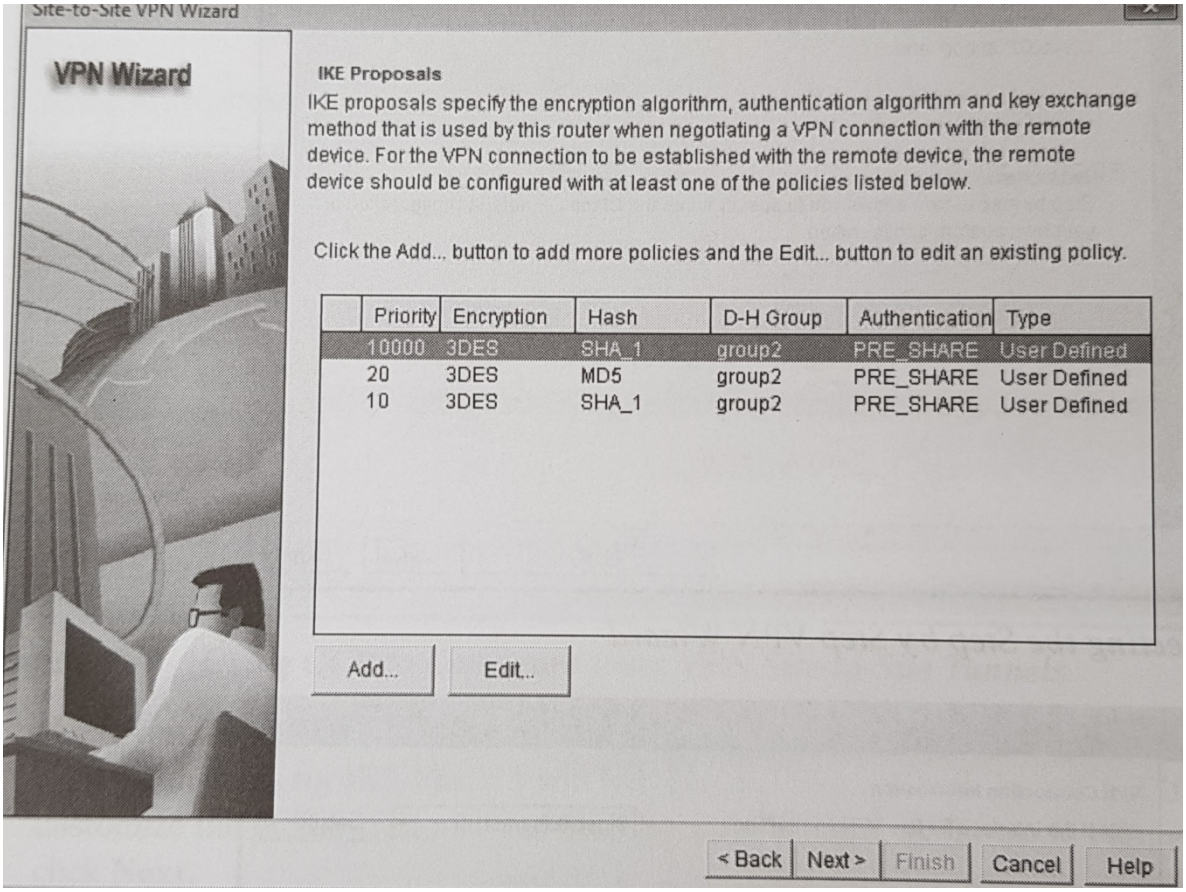


Figure 6-5 *Selecting the Step by Step VPN Wizard*



Usted se esta preguntando por la propuesta IKE phase 1 que quiere usar. Si usted quiere usar el predeterminado, eso es bueno si a lo largo lo usa en ambos lados (ambos routers usan la misma política) coincide con lo que usa para la política IKE phase 1. Nosotros decidimos (usted y yo) que usaríamos MD5 para HAshing. PSK para autenticar. DH group 2, 6 horas de lifetime, y AES 128-bit key para el cifrado. Después de mirar lo predeterminado, muestrado en la figura siguiente, usted selecciona Add para crear una nueva política IKE phase 1.



Después de hacer click en el botón **Add**, usted pone dentro sus políticas deseadas IKE phase 1, como muestra la figura y click en **OK**.

Después de crear su nueva política IKE phase 1, usted todavía necesita selecciónalo (lo mas alto) antes hacer click Next. El CCP crea su política por defecto, con su nueva política. Después destacando la nueva política (priority 2 en el ejemplo, como muestra la figura), hacer click Next para continuar.

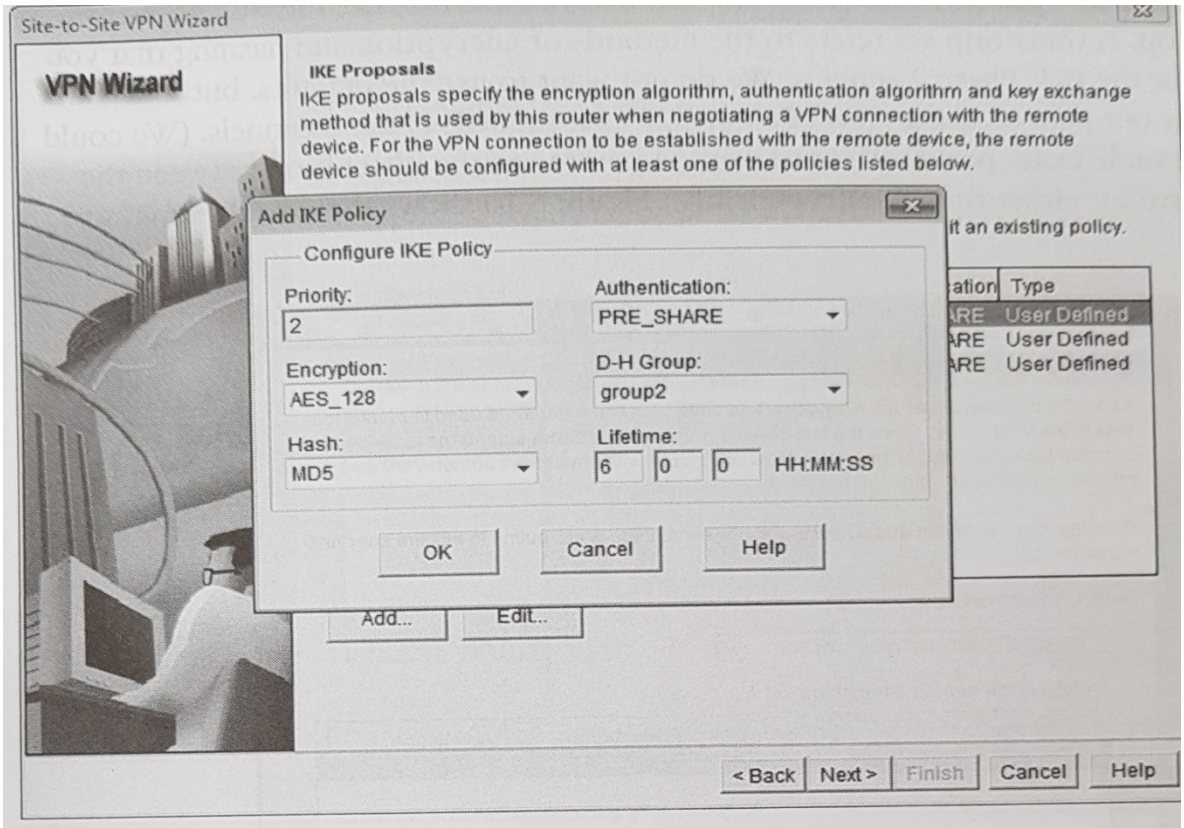
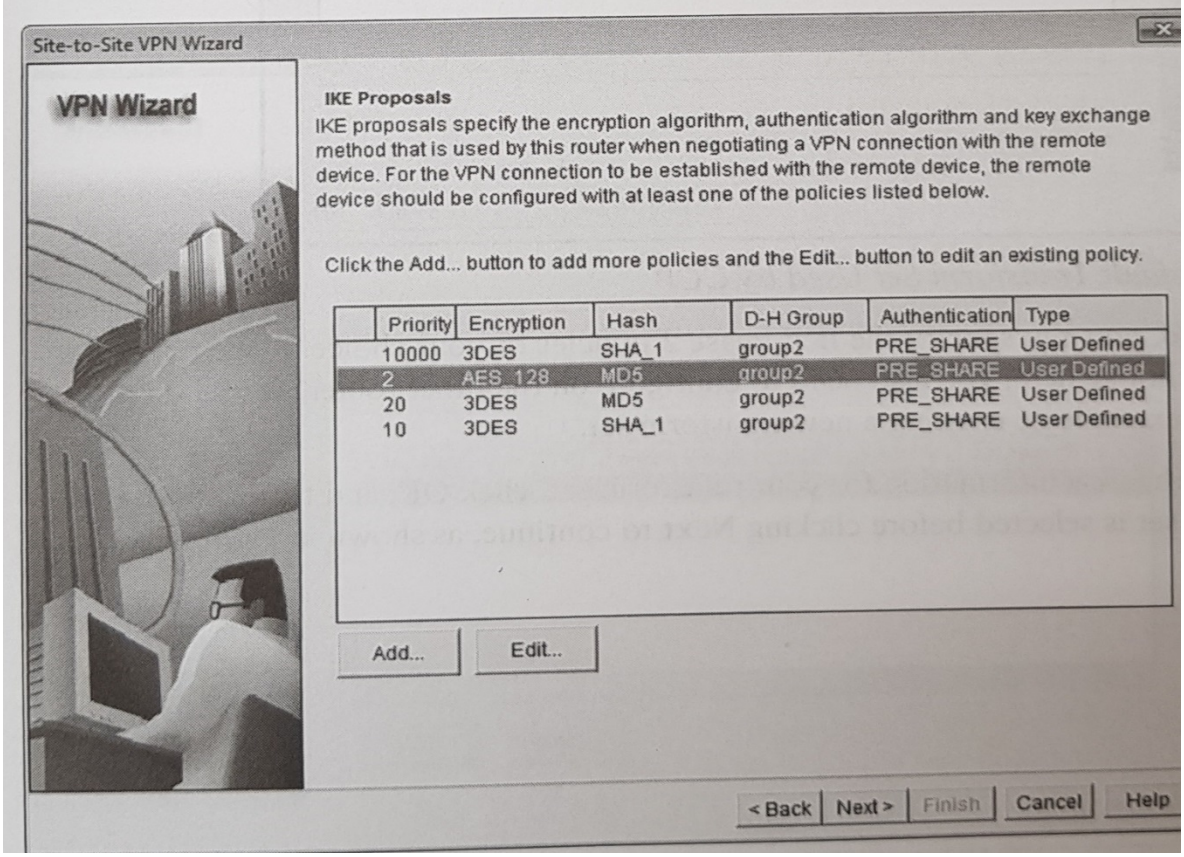
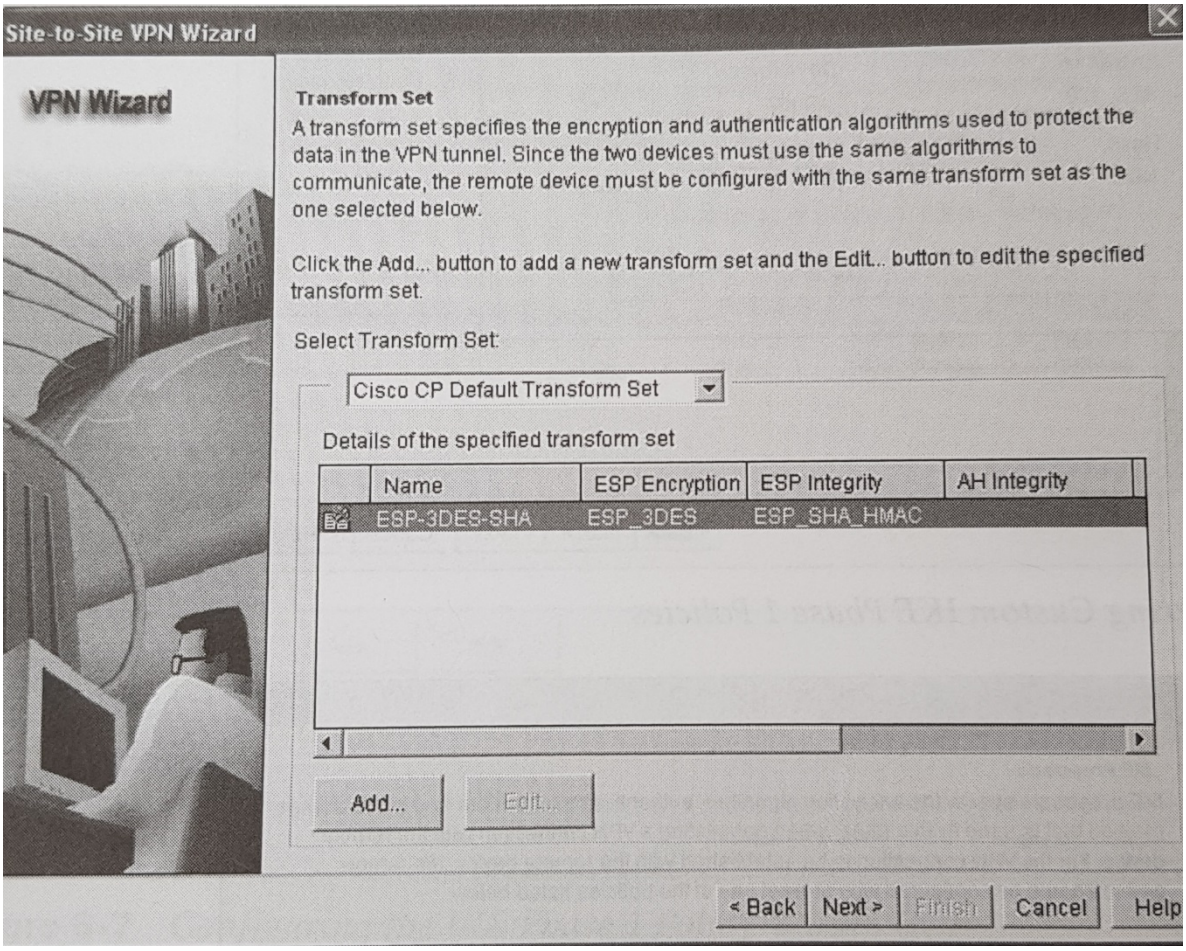


Figure 6-8 *Entering Custom IKE Phase 1 Policies*



La siguiente pantalla que aparece se ve similar a la primera, pero esta caja tiene el titulo Transform Set en la parte de arriba. Un Transform Set se refiere a los métodos de cifrado (encryption) y hashing que usted quiere usar para el IKE phase 2 tunnel. Nosotros no queremos usar las que están por defecto. Pero mas bien nosotros queremos seguir nuestro plan de usar AES-256 y SHA para IKE phase 2. (podríamos haber usado los mismos protocolos exactamente, pero yo quiero que tu veas la distinción entre la opción que tenemos independientemente.) la figura muestra por defecto **Transform Set**.



Haciendo click en **Add**, puede especificar las políticas IKE Phase 2 de su elección, recuerde que si usted elige aquí, usted también necesita configurar en el otro router también. La figura muestra un ejemplo de la creación de un nuevo **Transform Set**.

Después de ingresar la nueva información en su Transform Set, y hacer click en **OK**,y entonces verificar su nuevo Transform Set este seleccionado antes de hacer click en **Next** para continuar, como muestra la figura.

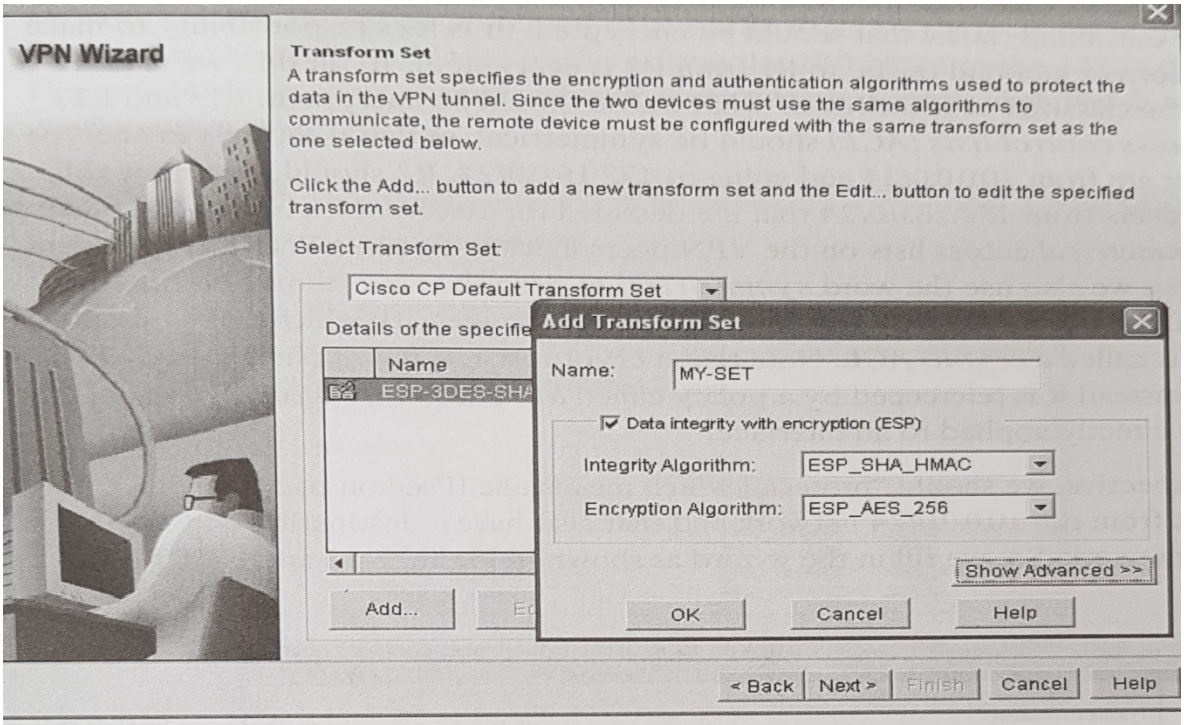
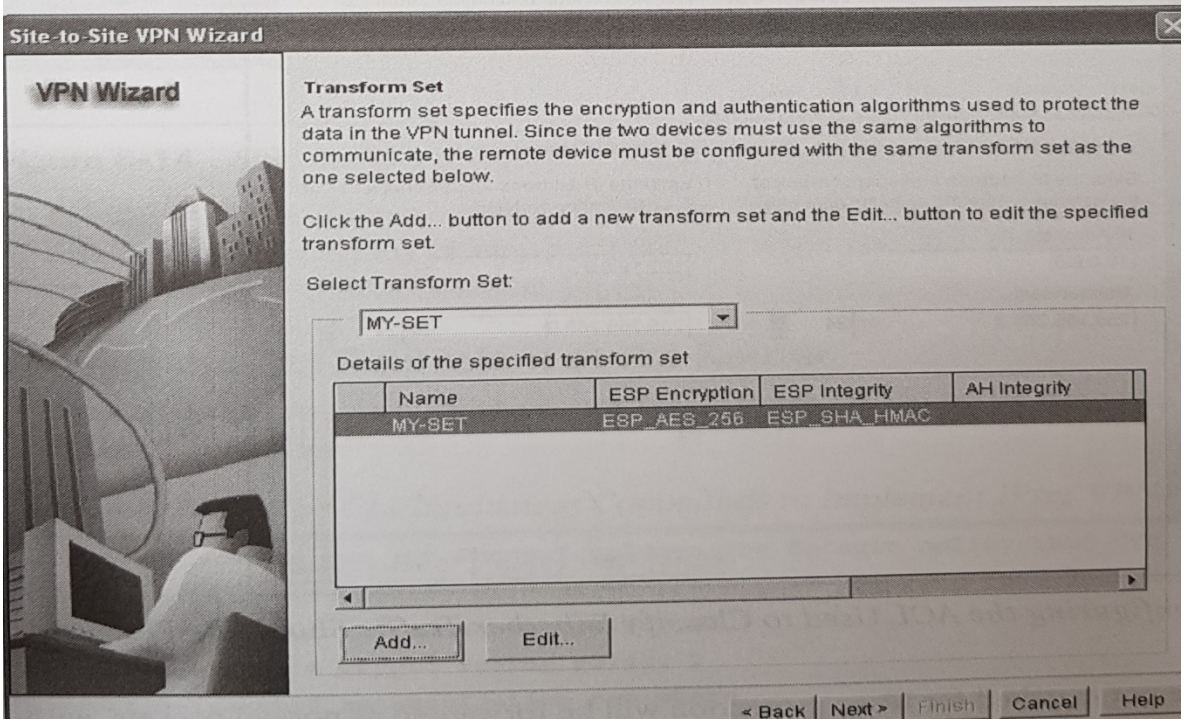
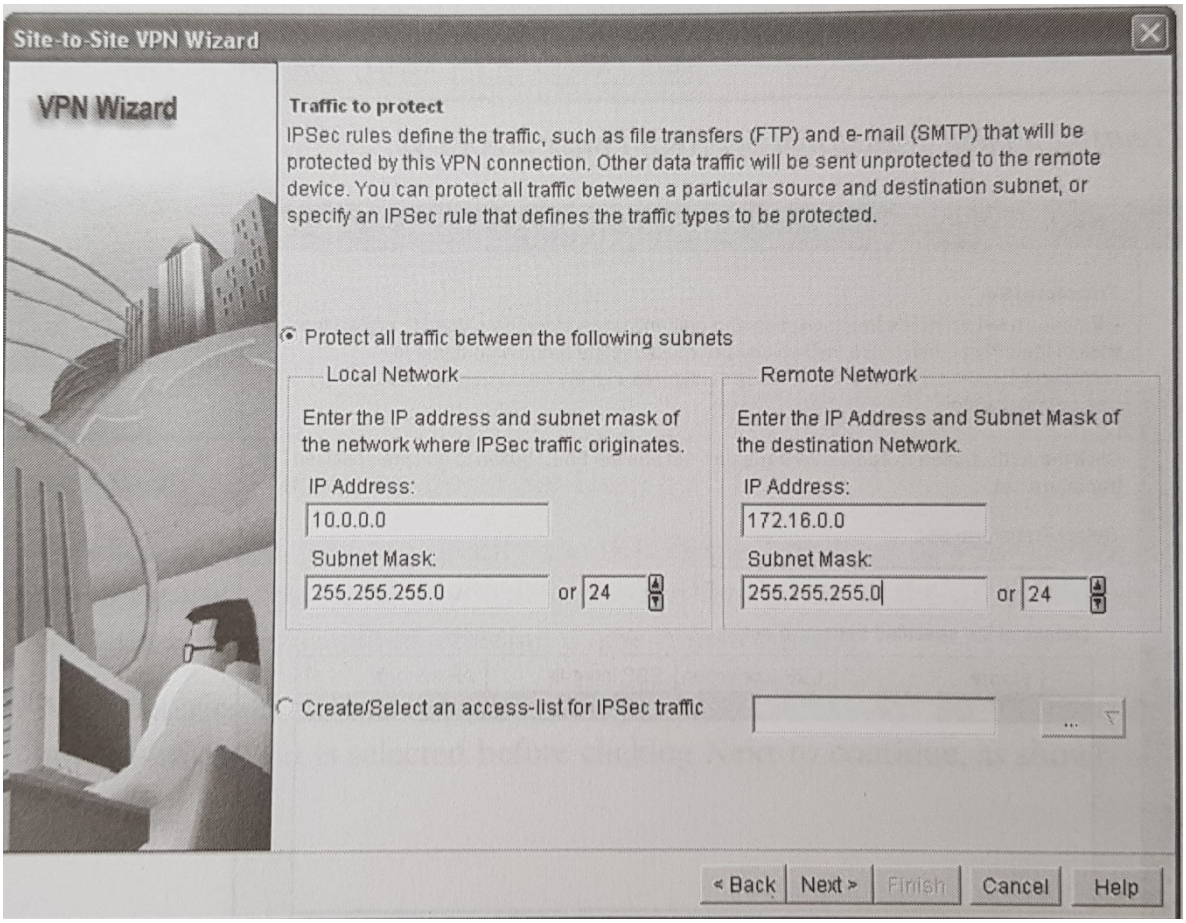


Figure 6-11 *Creating a New Transform Set (IKE Phase 2 Policy)*

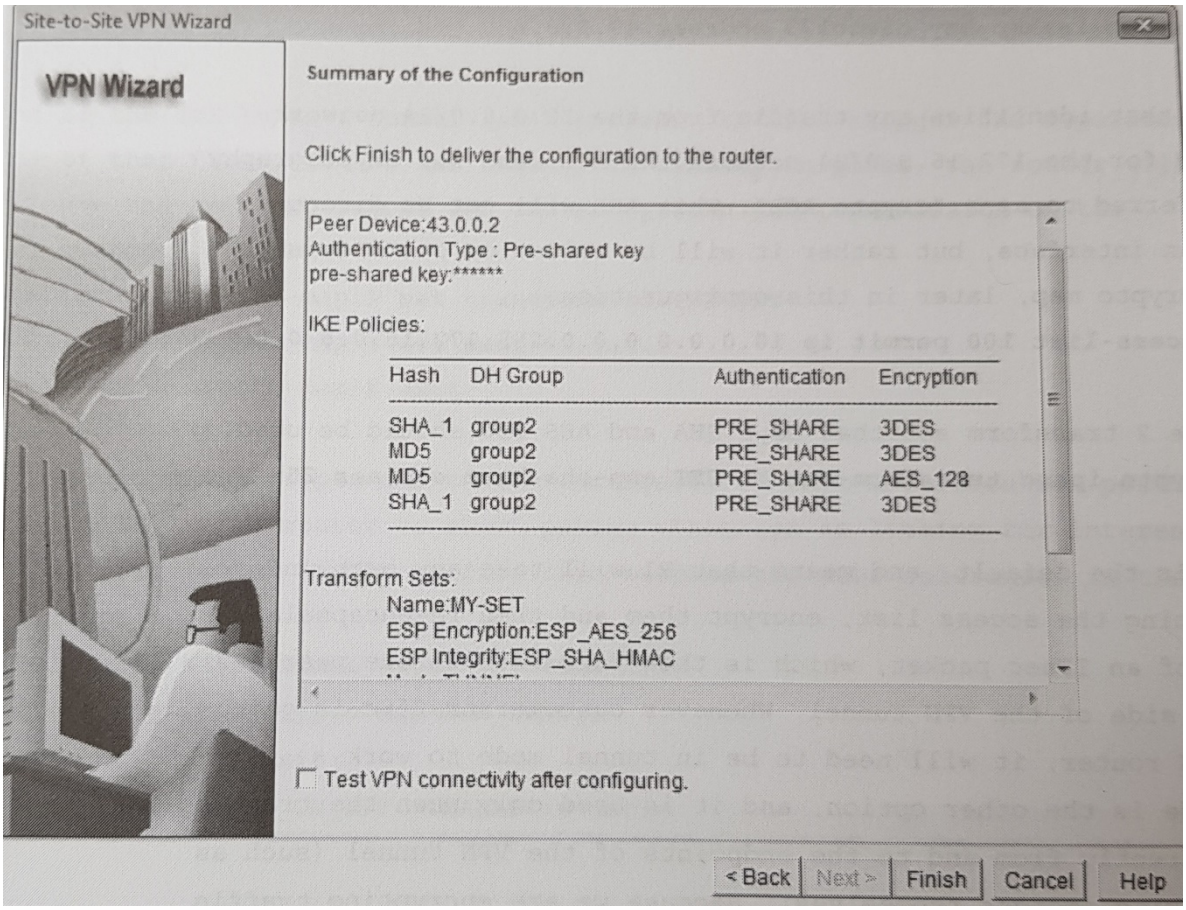


Wizard entonces pregunta que trafico será cifrado. Por que estamos en R1, nosotros deberíamos concentrarnos solo en la salida de tráfico que debería ser cifrado. (esto es la responsabilidad de R2 hacer seguro que la entrada correcta para R1 de R2 es cifrada). Para hacer esto. Nosotros usamos un Access list como el clasificador o filtro de que trafico debería ser cifrado. R1 y R2clasifican ACLs simétricas, si R1 dice cifrar todos los paquetes que están en la 10.0.0.0/24 y van a la 172.16.0.0/24, R2 dice que cifrara todos los paquetes de 172.16.0.0/24 que son destinados a 10.0.0.0/24.esto es lo que significa tener ACL simétricas en los pears VPN dento de un vpn site-to-site.(esto solo es unamala coincidencia que nosotros también usamos la palabra “simétrica” para describir algoritmos como AES que aquel peer estaría usando) Una ACL que ha sido creada para identificar cual trafico debería ser cifrado es llamado un **crypto ACL.** Note que una crypto ACL no es aplicada directamente en cualquier interface, pero en su lugar es referida por una política llamada un **crypto map** (discutido pronto). El crypto map es directamente aplicado a la interface.

Desde laperspectiva de R1, nosotros deberíamos “proteger”, lo cual significa usar IPsec dentro de los paquetes con un dirección fuente de red 10.0.0.0/24 y que también tiene un dirección destino en la red 172.16.0.0/24. Asi que, nosotros llenamos en el wizard como muestra la figura y hacemos click en Next para continuar.



Paquetes que no están coincidiendo por la protección IPsec será enviada como paquetes normales, sin encapsulación IPsec o cifrado aplicado. Cuando usted hace click en el botón Next, un resumen en pantalla de la política IKE (IKE PHASE 1) y Transform Set (IKE PHASE 2) que implementara el router. Note que el CCP como implementa por defecto IKE phase 1, junto con la política personalizada IKE phase 1, asi ambos terminaran en la configuración. la politica también especifica la el método de autenticación que nosotros seleccionamos antes en e wizard (PSK), y cual trafico de red debería ser protegido. (el trafico para proteger es de la perspectiva de salida. En este caso, trafico de salida de R1 es de la red 10.0.0.0/24 a la red 172.16.0.0/24) la figra muestra la tabla de resumen. Si cada cosa es correcta, click en **Finish** para entregar la configuración para el router.



Basado en sus preferencias de configuración, CCP puede mostrarle el equivalente CLI de la configuración sobre lo desplegado o solo desplegarlo cuando hace click en Finish. Puede controlar estas configuraciones en las configuraciones de preferencias para el CCP.

REVISANDO LA EQUIVALENCIA DEL CLI EN EL ROUTER

El ejemplo muestra el CLI equivalente que es implementado en R1 de la configuración hecha en el CCP en R1.

¡ Esta es nuestra implementación de política IKE Phase 1. La política por defecto que CCP

¡ Implementa es sus política #1, (la cual tiene mayor prioridad que la política de mayor numero,

¡ incluyendo nuestra política #2.)

R1(config-isakmp)#**crypto isakmp policy 2**

R1(config-isakmp)#**authentication pre-share**

R1(config-isakmp)#**encryption aes 128**

R1(config-isakmp)#**hash md5**

R1(config-isakmp)#**group 2**

R1(config-isakmp)#**lifetime 22600**

R1(config-isakmp)#**exit**

¡nota: me gusta remover la politica por defecto del CCP para IKE phase 1, y por esa razon, no ¡tengo que aplicarla aquí

¡esto especifica que que el PSK cisco123 sera usada como una lave (clave) para la autentiacacion ¡de IKE Phase 1 con el peer 43.0.0.2

R1(config)# **crypto isakmp key cisco123 address 43.0.0.2**

¡ACL que identifica cualquier trafico de la red 10.0.0.0/24 y destinado para la red 172.16.0.0/24.

¡una ACL usada para cifrar esta amenudo referida como una “crypto ACL”. Esta ACL no será ¡directamente aplicada a la interface, pero mas bien será llamado o “referenciada” con el crypto map, mas tarde aplcada en la configuración.

R1(config)#**access-list 1000 permit ip 10.0.0.0 0.0.0.255 172.16.0.0 0.0.0.255**

¡el IKE Phase 2 Transform Set que dice SHA y AES 256 sera usado

R1(config)#**crypto ipsec transform set MY-SET esp-sha-hmac esp-aes 256**

¡modo tunes esta predeterminado, y significa que R1 tomara cualquier salida los paquetes ¡coincidentes a la ACL, cifrándolos y entonces re-encapsulandolos dentro de un paquete IPsec, los ¡cuales entoneces son enviados al peer (R2) en el otro lado del túnel VPN. Cuando trafico de ¡clientes va a travez de un router VPN, necesitara estar en modo túnel para trabajar. modo ¡transporte is la otra opción, y es usado solo cuando el tráfico de tránsito es directamente ¡desde y hacia el punto final del túnel vpn (tal como R1 y R2 hablando entre ellos mismos). Por ¡que nosotros ciframos trafico para los usuarios finales, modo túnel (es por defecto) será usado.

R1(cfg-crypto-trans)#**mode tunnel**

R1(cfg-crypto-trans)#**exit**

¡el crypto map es una gran afirmacion. Es aplicado para la interface de salida (frente a internet), y ¡entonces mira el trafico. Si el trafico de salida coincide la ACL, entonces el router conoce los ¡paquetes que deberían ser cifrados, encapsulado dentro un encabezado IPsec (usualmente ¡protocolo 50, el cual es ESP y esta para encapsular carga útil asegurada), y entonces enviar a la ¡dirección IP del peer en el otro lado (R2) quien descifrara y enviara paquetes en texto plano al ¡dispositivo en la red 172.16.0.0/24 “ipsec-sakmp” significa que queremos el router para ¡automáticamente negociar el IKE phase 2 , usando isakmp, que representa Internet Security ¡Association Key Management Protocol. En corto, eso significa automatizar el proceso, asi que el ¡administrador no tiene que manualmente configurar todas las claves (llaves) para cifrado. El “1” ¡representa numero de secuencia “1”. Si nosotros tenemos 5vdiferentes peers IPsec, podríamos ¡usar 5 diferentes números de secuenciea en el mismo crypto map para organizar nuestra política ¡basada en el numero de sequencia y correspondiente peer estaríamos usando IPsec.

R1(config)#crypto map SDM_CMAP_1 1 ipsec-isackmp

¡esto dice el crypto map presta atención a la ACL 100 para ver si el trafico seria cifrado o no

R1(config-crypto-map)#match address 100

¡si el trafico coincide la ACL, entonces R1 usaria el transform-set nombrado MY-SET para negociar ¡el IKE phase 2, con el peer 43.0.0.2

¡si el IKE phase 1 no esta preente, eso disparara la negociación de esa primero. Si el IKE phase 2 ¡esta ya ubicada, el router usara el túnel existente para cifrar y transmisión de los paquetes del ¡cliente

R1(config-crypto-map)#set transform-set MY-SET

R1(config-crypto-map)#set peer 43.0.0.2

R1(config-crypto-map)#exit

¡Aplicando el crypto map a la interface, es que active nuestra politica, y le dice al router iniciar ¡poniendo atencion en buscar trafico interesante (el cual es el trafico que coincide la ACL referida ¡en el crypto map).

R1(config)#interface gigabitethernet1/0

R1(config-if)#crypto map SDM_CMAP_1

R1(config-if)#exit

%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ONcom

COMPLETANDO Y VERIFICANDO IPsec

Cuando usted hace click en Finish, el CCP muestra el estatus del tunel VPN, como muestra la figura . la rason el túnel este abajo es porque el otro lado del túnel no ha sido configurado.

Para configurar R2, nosotros podríamos seleccionar R2 con el CCP y seguir el mismo proceso. CCP tiene la habilidad para usar el botón Mirror del CCP de R1, y entonces modificar y aplicar esa imagen espejo de la VPN para R2. La figura muestra el resultado de hacer click en el botón Generate Mirror.

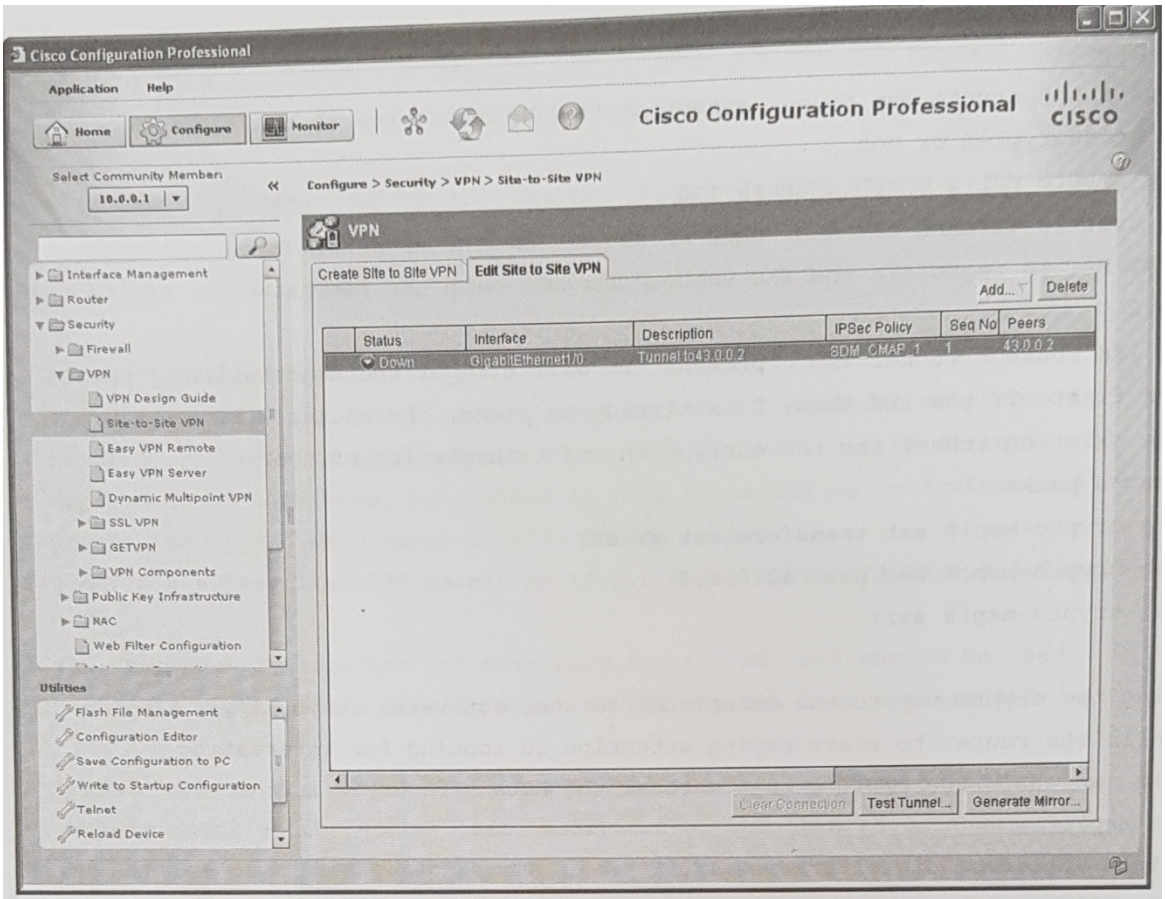
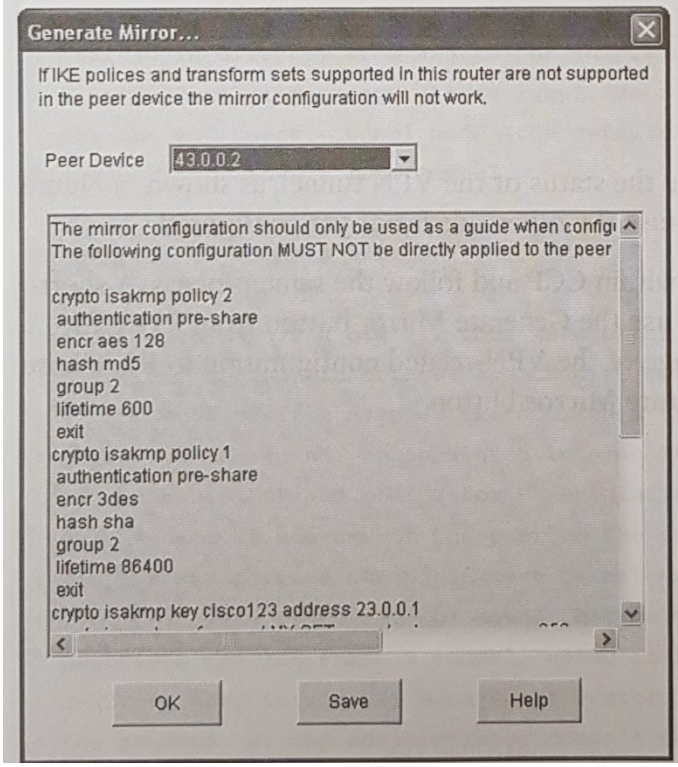


Figure 6-15 *Results of Finishing the VPN Wizard*



Podríamos tomar este archivo, y aplicarlo a R2, mostrando y editando el archivo que es apropiado para R2

```
Crypto isakmp policy 2
Authetication pre-share
Encr aes 128
Group 2
Lifetime 21600
Exit

Crypto isakmp key cisco123 address 23.0.0.1
Crypto ipsec transform-set MY-SET esp-sha-hmac esp-aes 256
Mode tunnel
Exit

Ip access-list extended SDM_1
Permit ip 172.16.0.0 0.0.0.255 10.0.0.0 0.0.0.255
Exit

Crypto map SDM_CMAP_1 1 ipsec-isakmp
Match address SDM_1
Set transform-set mY-SET
Set peer 23.0.0.1
Exit

Interface g1/0
Crypto map SDM_CMAP_1
Exit
```

Verificando IPsec en el CLI

```
! Verify the IKE Phase 1 policies in place on the router
R1# show crypto isakmp policy

Global IKE policy
Protection suite of priority 2
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               21600 seconds, no volume limit

! Show the details of the crypto map, and where it is applied, showing
! the contents of the IKE Phase 2 transform sets, learning the ACLs
! involved for the VPN, who the current peer is, and more.
R1# show crypto map
Crypto Map "SDM_CMAP_1" 1 ipsec-isakmp
        Description: Tunnel to43.0.0.2
        Peer = 43.0.0.2
```

```
        Extended IP access list 100
            access-list 100 permit ip 10.0.0.0 0.0.0.255 172.16.0.0 0.0.0.255
        Current peer: 43.0.0.2
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N): N
        PFS (Y/N): N
        Transform sets={
                MY-SET:  { esp-256-aes esp-sha-hmac  } ,
        }
        Interfaces using crypto map SDM_CMAP_1:
                GigabitEthernet1/0

! See the details for the IKE Phase 1 tunnel that is in place

R1# show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       T - cTCP encapsulation, X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA

C-id  Local       Remote      I-VRF    Status Encr Hash Auth DH Lifetime Cap.

1001  23.0.0.1    43.0.0.2             ACTIVE aes  md5  psk  2  00:04:05
      Engine-id:Conn-id =  SW:1

! See the details for the IKE Phase 2 tunnels that are in place.  There is
! one inbound Security Association (SA) and one outbound. They both have
! different SA numbers used for tracking these sessions.
! ESP is used, and it provides all the services desirable from IPsec.
! The other option is Authentication Header (AH) which isn't used because
! it doesn't support any encryption algorithms.
R1# show crypto ipsec sa
<Note: less relevant content removed>
interface: GigabitEthernet1/0
    Crypto map tag: SDM_CMAP_1, local addr 23.0.0.1
! Shows what traffic is being encrypted.  All IP traffic between
! 10.0.0.0/24 and 172.16.0.0/24
   local  ident (addr/mask/prot/port): (10.0.0.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (172.16.0.0/255.255.255.0/0/0)

! IKE Phase 1 uses UDP port 500 to negotiate and set up the IKE Phase 1
! tunnel
   current_peer 43.0.0.2 port 500
```

```
    #pkts encaps: 29, #pkts encrypt: 29, #pkts digest: 29
    #pkts decaps: 29, #pkts decrypt: 29, #pkts verify: 29

! From R1's perspective, the local side is its G1/0, and R2 is at 43.0.0.2
     local crypto endpt.: 23.0.0.1, remote crypto endpt.: 43.0.0.2
     path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet1/0

! An SPI is a Security Parameter Index.  It is a fancy way of tracking
! a specific Security Association (SA) between itself and a peer.
! Think of it as a serial number (unique) for each SA.
     current outbound spi: 0x48A3CF57(1218694999)
! PFS stands for Perfect Forward Secrecy, and it is the ability for IKE
! Phase 2 to run the DH algorithm again, instead of using the keys
! generated during the DH from IKE Phase 1.   This feature is off by
! default for most platforms.
     PFS (Y/N): N, DH group: none

! The IPsec or IKE Phase 2 is really two tunnels.   There is one for
! traffic from R1 to R2.   There is another from R2 to R1.   They have
! different SPIs, but together, these two unidirectional tunnels make up
! the "IPsec" tunnel.
! Encapsulating Security Payload (ESP) is the primary method used by IPsec.
! The other option is to use Authentication Header (AH), but it doesn't
! have the ability to encrypt, and isn't often used for that reason.   AH
! also breaks when going through Network Address Translation (NAT).
! Here is the inbound SA used by R1 to receive encrypted user packets from
! R2.
     inbound esp sas:
      spi: 0xE732E3A0(3878871968)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 1, flow_id: SW:1, sibling_flags 80000046, crypto map:
         SDM_CMAP_1
        sa timing: remaining key lifetime (k/sec): (4388080/3230)
        IV size: 16 bytes
! Here is the built in anti-replay support
        replay detection support: Y
        Status: ACTIVE
! We aren't using AH, so there are no Security Associations (SAs) for AH.
     inbound ah sas:

! Here is the Outbound SA used by R1 to send encrypted user packets to R2.
     outbound esp sas:
      spi: 0x48A3CF57(1218694999)
        transform: esp-256-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
```

```
        conn id: 2, flow_id: SW:2, sibling_flags 80000046, crypto map: SDM_
         CMAP_1
        sa timing: remaining key lifetime (k/sec): (4388079/3230)
        IV size: 16 bytes
        replay detection support: Y
        Status: ACTIVE

     outbound ah sas:

! Another way of seeing that the encryption and decryption is working.
R1# show crypto engine connections active
Crypto Engine Connections

   ID  Type    Algorithm           Encrypt  Decrypt IP-Address
    1  IPsec   AES256+SHA                0       29 23.0.0.1
    2  IPsec   AES256+SHA               29        0 23.0.0.1
 1001  IKE     MD5+AES                   0        0 23.0.0.1
```

CAPITULO 7

IMPLEMENTANDO IPsec Site-to-Site VPN

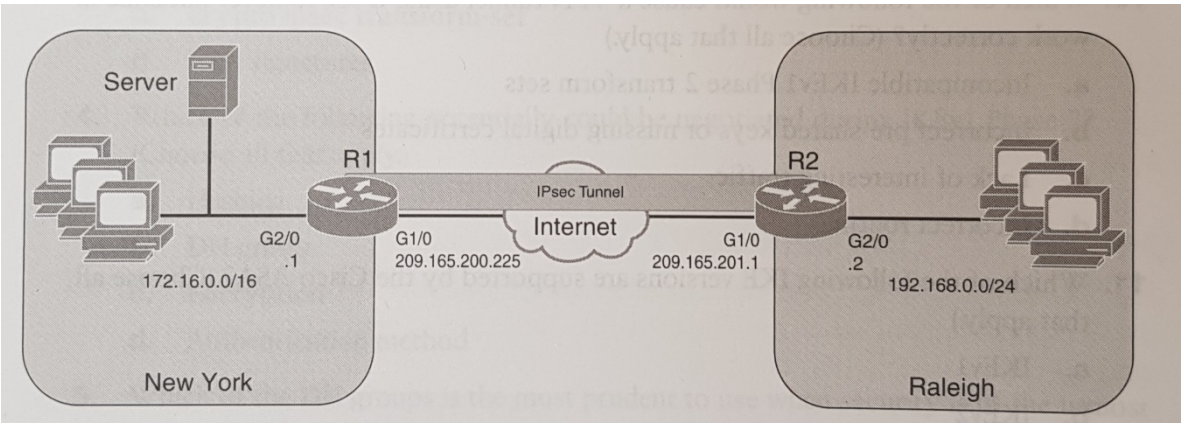
En el capitulo previo, aprendio sobre los beneficios de las VPN y el protocol y metodo usado para implementar aquellos beneficios, tales como cifrado y confidencialidad, hashing para integridad de datos, y authentication para verificacion de peer. Usted también ha visto ejemplos de esos protocolos, tales como 3DES, AES, MD5, SHA, para integridad de datos, y pre-shared key (PSK) o RSA signature (también conocido como firma digital) usada para la autenticación.

Planeando y Preparando una VPN IPsec Site-to-Site

En esta sección usaremos un caso de estudio para identificar las necesidades del cliente VPN y nuestro plan, los detalles para implemetar la VPN. Esta sección integar la información aprendida en el capitulo previo sobre VPNs.

Necesidades del Cliente

Para este escenario, digamos usted y to tenemos un cliente con oficinas en New York y Raleigh Carolina del Norte. La oficina en NY tiene un área local y un solo router, R1 que conecta a internet. Router 2 (R2) es usado para proveer acceso a internet para el sitio en CN, la figura muestra la topología.



El sitio en NY tiene seridores de archivos que contienen datos sensibles de clientes, y los ususarios en el sitio en CN necesitaran accesar a esos datos. En adicion, usuarios en NY necesitan la abilidad para accesar seguramente a algunas de las computadoras en CN que tienen servicos de archivos compartidos habilitado. Ambos sitios están usando direcciones IP privadas para las LAN que no pueden ser enviadas directamente sobre la internet.

Los clientes nos han preguntado por una recomendación para permitir servicios de archivos entre las dos oficinas que pueden ser hechos seguramente. Los clientes también quieren asegurar que los datos como estos esta siendo enviado sobre la red no lleguen a ser alterados o corrompidos en transito. El cliente esta también preocupado sobre posibles atacantes, quienes están en algunas otras ubicaciones que las oficinas de NY y NC siendo capaz de suplantar routers pretendiendo ser el otro router y conectados a la red. En la actualidad, la comapñia no necesita agregar accesos remotos a otra red que directamente entre los dos sitios.

Usted y yo regresamos hasta nuestra oficina y consideramos la red del cliente y requerimientos. Como nosotros consideramos la opción de VPN que provee seguridad, recordamos que IPsec puede ejecutar lo siguiente:

- Confidencialidad: usando algoritmos de cifrado simétrico tales como 3DES, IDEA, AES y asi cifrar datos de texto claro dentro de texto cifrado.
- Integridad de Datos: usando algoritmos de hashing tales como MD5, SHA y hashed message authentication code (HMAC) para verificar esos datos no han sido manipulados durante su transito atraves de la red.
- Autenticación: hecho para autenticar peers VPN, usando PSK o digital signature (aprovechando certificados digitales).
- Escondiendo las direcciones privadas para internet: por que IPsec Encapsulation Security Protocol (ESP) en modo túnel cifra y encapsula los paquetes originales, y entonces ubica un nuevo encabezado IP antes de enviar los paquetes, internet ve solo los paquetes con la global IP de un router y destinado a el global IP del segundo router.

IPsec usa dos métodos para el cifrado: modo túnel y transporte. Si IPsec modo túnel es usado, el encabezado IPsec y la carga útil es cifrada, cuando modo transporte es usado, solo los paquetes con carga útil estan cifrados.

Tecnologia IPesc buscan métodos como un perfecto ajuste para el cliente. Anted de ir tanto al futuro, usted quiere verificar que la conexión a internet para R1 y R2 este trabajando, y que R1 y R2 tengan alcance cada uno con el otro. Usted puede hacerlo asi con un simple ping a la dirección global de R2 desde R1. Si hay filtrado para ICMP, el cual es usado para hacer PING, eso no necesariamente significa que IPsec no trabaje, como el protocolo para IPsec todavía es permitido entre los routers. La Tabla los protocolos críticos que podrimos necesitar entre R1 y R2

PROTOCOLO/ PUERTO	QUIEN LO USA	COMO ES USADO
UDP port 500	IKEv1 Phase 1	IKEv1 Phase 1 UDP:500 para su negociación.
UDP port 4500	NAT-T (NAT Trasversal)	Si ambos peers soportan NAT-T, y si ellos detectan que ellos están conectango cada uno con el otro a través de un dispositivo NAT, ellos pueden negociar que ellos quieran poner un falso encabezado UDP port 4500 en cada uno de los paquetes de IPsec (antes del encabezado ESP) para sobrevivir a un dispositivo NAT que de otra manera podría tener un problema rastreando una sesión ESP (capa 4 protocolo 50)
Layer 4 protocol 50	ESP	Los pauqetes IPsec tienen protocolo de capa 4 ESP (IP Protocol #50). El cual es encapsulado por el emisor para cada paquete IPsec. ESP es normalmente usado en lugar de authentication header “AH”. El encabezado ESP es escondido detrás del un encabezado UDP si NAT T es usado.
Layer 4 protocol 51	AH	Los paquetes AH tienen protocolo de capa 4 AH (ip Protocol #51) nosotros no usamos normalmente AH (opuesto a ESP) por que la ausecncia AH carece de capacidad de cifrado para datos de usuario.

Si R1 y R2 tienen ACL aplicada de entrada en su interface de salida (g1/0), nos gustaría asegurar que estamos permitiendo los protocolos requeridos entre las direcciones IP globales (internet) de los dos routers. Cada router necesita creer alcanzar redes remotas a través de rutas especificas, o como minimo, una default route (ruta por defeto). Si el router no tiene una ruta, no intenatara enviar paquetes, y no disparara ningún crypto map que este buscando filtrar el trafico de interés. La decisión del router sucede antes de que IPsec este implementado.

PLANNING IKEv1 PHASE 1

Con la conectividad verificada, el primer paso del plan es elegir los componentes para usar por IKE phase 1. (recordando HAGLE). La tabla lista alguna de nuestras elecciones para IKEv 1 phase 1.

FUNCION	METODO FUERTE	METODO MAS FUERTE
Hashing	MD5 128 bit	SHA1, 160 bit
Authentication	Pre-Shared Key (PSK)	RSA-Sigs (Digital Signature)
Group # para DH key Exchange	1,2,5	IKE group 14 y 24 usa 2048 bit DH. Group 15 y 16 3072-bit y 4096-bit DH. Group 19 y 20 soporta 256-bit y 384-bit ECDH groups, respectivamente.
Lifetime	86400 segundo = 1 dia (por defecto)	Mas corto que un dia, 3600
Encryption	3DES	AES-128 (o 192 o 256)

Por el cliente, decidimos que usaremos opciones mas fuertes, y usaremos lo siguiente para IKE1 pahse 1:

- Hashing: SHA
- Auyhentication: RSA-sign (el cual requiere PKI para ser usado)
- DH group: 5
- Lifetime: 3600 seconds
- Encryption: AES-256

También notaremos que todo estos parámetros están para ser usados pora políticas IKEv1 Phase 1, el cual nosotros especificamos usar el comando **crypto isakmp policy**.

Planeando IKEv1 phase 2

Para IKEv1 phase 2, el cual es el túnel actual que será usado para proteger los paquetes de los usuarios, nosotros tenemos los elementos listados en la tabla para el plan:

Item to plan	Implemented by	Notes
Peer IP address	Crypto map	Habiendo una dirección IP alcanzable conocida para la VPN peer es critico para los tuneles site-to-site IPsec tradicional para negociar y establecer la VPN (ambas fases)
Traffic to encryption	Crypto ACL, la cual es referida dentro del crypto map	Una ACL extendida que no es aplicada a la inteface pero es referida dentro del crypto map. Esto debería solo referenciar el trafico de salida, el cual debería ser protegido por IPsec. El trafico no coincidente con la ACL no será cifrado, pero será enviado como paquetes normales.
Encryption method	Transform set, el cual es referido dentro del crypto map.	DES, 3DES, AES son todas las opciones. IKEv1 phase 2 no necesita ser el mismo método que IKEv1 Phase. El método necesita coincidir las políticas de los peers (transform sets) para phase 2.
Hashing (HMAC) method	Transform set, el cual es referido dentro del crypto map	MD5 y SHA HMACs puede ser usado, y necesita coincidir la política phase 2 del peer.
Lifetime	Global configuration command: crypto ipsec Security-association lifetime…	Lifetime para phase 2 debera coincidir entre los peers, si ambos usan el tiempo de vida por defecto (pero especifica un tiempo de vida), ambos peers tendrían tiempos de vida compatibles. El tempo de vida puede ser especificado como un numero de segundos o numero de kilobytes.

Perfec forward secrecy (PFS) (run DH otra vez o no)	Crypto map	DH esta corriendo durante IKEv1 Phase 1, y phase 2 reusa esa misma claves que se generaron. Si usted quiere reejecutar Phase 2 el DH, es llamado PFS y usted debe escoger un DH group number 1,2,5 para usar en phase 2
Cual interface uso para el peer con el otro dispositivo VPN	Crypto map aplicado a la salida de la interface	Desde la perspectiva del router, esta es la interface de un peer VPN para el otro peer, donde la salida de los paquetes IPsec son permitidos al router y los paquetes de IPsec de entrada están viniendo dentro del router.

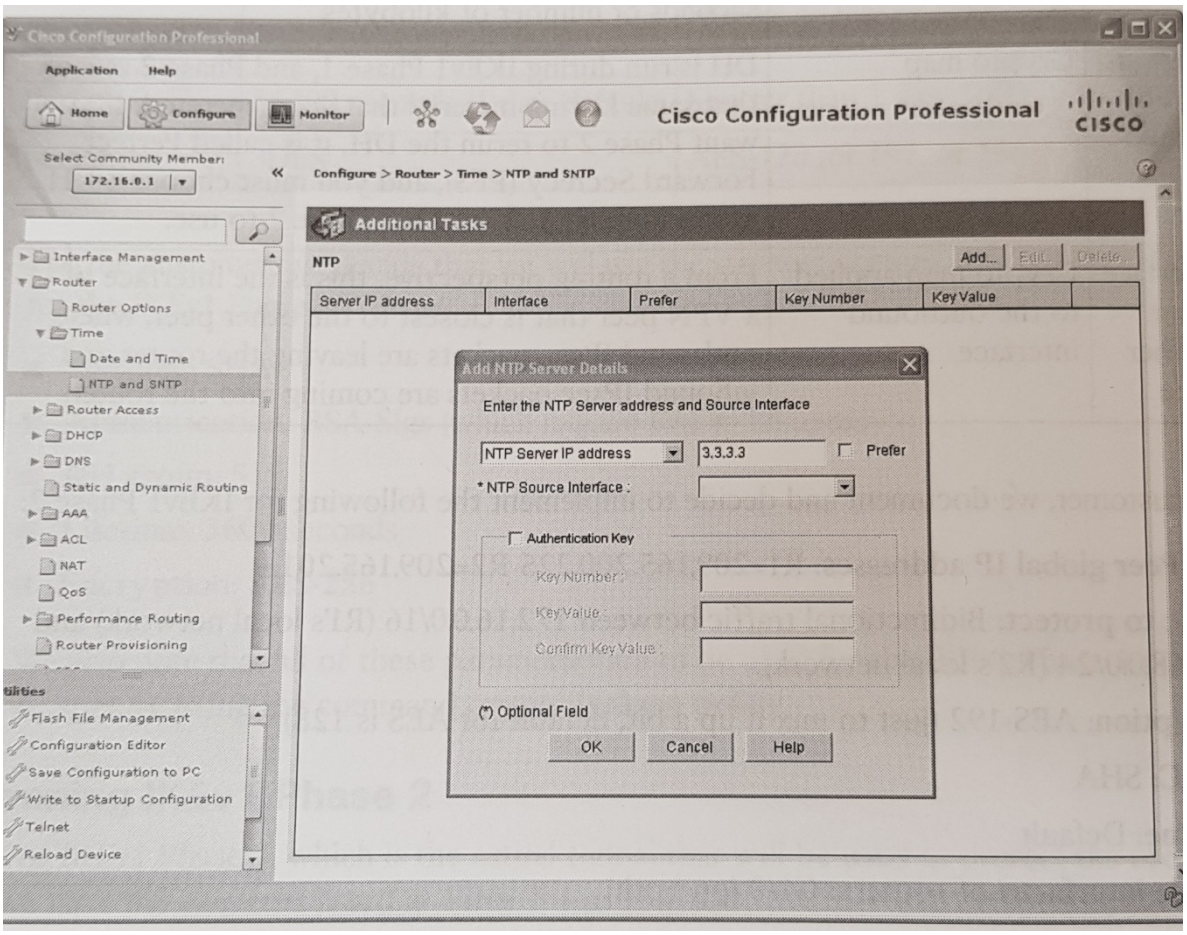
Para nuestros clientes, nosotros documentamos y decidimos implementar lo siguiente para IKEv1 phase 2:

- VPN peer global IP address: R1=209.165.200.225 R2=209.165..201.1
- Traffic to protect: trafico bidireccional entre 172.16.0.0/16 (R1 red local) y 192.168.0.0/24 (R2 red local).
- Encryption: AES-192
- HMAC: SHA
- LIfetime: default
- Outside interfaces del los routers: GI1/0 en ambos
- PFS: Group 2

IMPLEMENTANDO Y VERIFICANDO UNA VPN SITE-TO-SITE EN DISPOSITIVOS CISCO

En esta sección tomaremos la información de nuestro plan en secciones previas para implementar, verificar, y resolver problemas de VPNs usando una configuración de Cisco Configuration Profesional (CCP) y el CLI.

Al principio del los capítulos, discutimos importantes recursos tales como Network Time Protocol (NTP) y Certificate Authorities (CA). Por que nosotros escogimos implementar RSA-signatures para este cliente, nosotros queremos implementar NTP como uno de los primeros paso. Esto es por que cuando intercambiemos certificados durante IKEv1 Phase 1, si R1 piensa en el año 2024, y el certificado que recivio de R2 es listado como valido de 2015 2018, R1 rechazara el certificado como no valido, e IKEv1 Phase 1 no se completara bien. (si IKEv1 Phase1 no trabaja, IKEv1 phase 2 no tendrá oportunidad también.) asi que para esta implementación, usamos un servise provider en internet (en nuestra topología del cliente) que proveerá ambos NTP y servicios CA en la dirección 3.3.3.3 (en la internet simulada). Vamos a sincronizar el tiempo en ambos routers con el SP de NTP como muestra la figura.



El mismo proceso seria repetido para el otro router también. NTP puede tomas 15 min para sincronizar. Otro tema a considerar del NTP sevrver el tiempo entregado basado en coordinate universal time (UTC) y configurar el tiempo local de la zona horaria en su router es importante que ese correcto offset del UTC este reflejado en el router local. Para verificar que el tiempo esta sincronizado con el tiempo del servidor, como el CLI en el router podemos usar el comando mostrado en el ejemplo:

Example 7-1 *Verifying NTP Status*

```
R1# show ntp status
Clock is unsynchronized, stratum 16, no reference clock
nominal freq is 250.0000 Hz, actual freq is 249.9999 Hz, precision is 2**24
reference time is D2C15194.71E5E637 (14:11:32.444 UTC Wed Jan 18 2012)
clock offset is 0.0000 msec, root delay is 0.00 msec
root dispersion is 0.00 msec, peer dispersion is 0.00 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000085 s/s
system poll interval is 64, last update was 1518 sec ago.

! Note the above indicates the time isn't synchronized.
! We can check to see if the router has the NTP server configured with the
! following:


R1# show ntp association

  address         ref clock       st   when   poll reach  delay  offset   disp
 ~3.3.3.3         .INIT.          16      -     64     0  0.000   0.000 16000.
 * sys.peer, # selected, + candidate, - outlyer, x falseticker, ~ configured

! Based on this output, we know that it has information to use the 3.3.3.3
! server
! It may take anywhere from 5 to 15 minutes for
! the synchronization to happen.     After verifying the configuration, and
! waiting about 5 minutes, we can then issue the verification commands
! again and see that the synchronization is complete.
R1# show ntp status
Clock is synchronized, stratum 3, reference is 3.3.3.3
nominal freq is 250.0000 Hz, actual freq is 249.9999 Hz, precision is 2**24
reference time is D2C15854.6F453DAE (14:40:20.434 UTC Wed Jan 18 2012)
clock offset is 0.0029 msec, root delay is 0.01 msec
root dispersion is 0.95 msec, peer dispersion is 0.06 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000000097 s/s
system poll interval is 64, last update was 251 sec ago.
```

Nuestra siguiente tarea, preparar IPsec, es generar las claves pares en R1 y R2, configurarlos para usar CA, tener la autentiaccion del CA (obtener el certificado raíz), y entonces suscribirse con el CA (solicitar su propio certificado de identidad). El CA esta en 3.3.3.3 y soporta Simple Certificate Enrollment Protocol (SCEP). De R1 y R2, el proceso es el mismo, y el comando usado en R1 es mostrado en el ejemplo.

Ejemplo: Preparando por y para obtener certificados digitales

¡especficando el domain-name que será usado incluido con la llave (clave) pareja que usted esta ¡generando

¡nota: si usted ya ha creado una key-pair. Puede usar la misma key-pair para ambos propósitos si desea.

R1(config)**#ip domain name cisco.com**

R1(config)**#crypto key generate rsa**

The name for the key will be: R1.cisco.com

Choose the size of the key modulus in the range of 360 to 2048 for you generate purprose keys. Choosing a key modulus greater than 512 may take a few minutes.

¡una clave larga es major. Usando una longitud minima de 1024 es una mejor practica.

How many bits in the modulus [512]: **1024**

%generating 1024 bit RSA Keys, keys will be non-exportable . . .[OK]

¡especificando el CA que le gustaria usar, y la URL para ser usada para alcanzar ese CA.

R1(config)**#crypto pki trustpoint CA**

R1(ca-trustpoint)**#enrollment URL** http://3.3.3.3

R1(ca-trustpoint)**#exit**

¡solicitor el certificado raiz atraves de “authenticating” al CA

R1(confg)**#crypto pki autheticate CA**

Certificate has the following attributes:

Fingerprint MD5: B1AF5247 s1F35FE3 0200F345 7C20FBA0

Fingerprint SHA1: F5BB33E3 1CB5D633 0DF720DF 8C72CD48 E744CF5B

%Do you accept this certificate? [yes/no]: **yes**

Truspoint CA certificate accepted.

¡solicitor un certificado de identidad para este router, via SCEP y la opción “enroll”

R1(config)**#crypto pki enroll CA**

%

%Start certificate enrollment . . .

%crear un challenge password. You will need to verbally provide this password to the CA administrator in order to revoke your certificate. For security reason your password will not be saved in the configuration. Please make a note of it.

¡especificando el challenge password que sera usado en los eventos que usted necesite preguntar al CA para ¡revocar este certificado en el future.

Password: **SuperSecret!23**

Re-enter password: **SuperSecret!23**

%the subject name in the certificate will include:R1.cisco.com

¡los siguientes dos articulos son elementos opcionales que pueden ser incluidos en el certificado

%Include the router serial number in the subject name:[yes/no]: **no**

%include an IP addess in the subjectname? [yes/no]: **no**

Request certificate from CA? [yes/no]: **yes**

%certificate request sent to Certificate Authority

%the “show crypto pki certificate verbose CA” command will show the fingerprint.

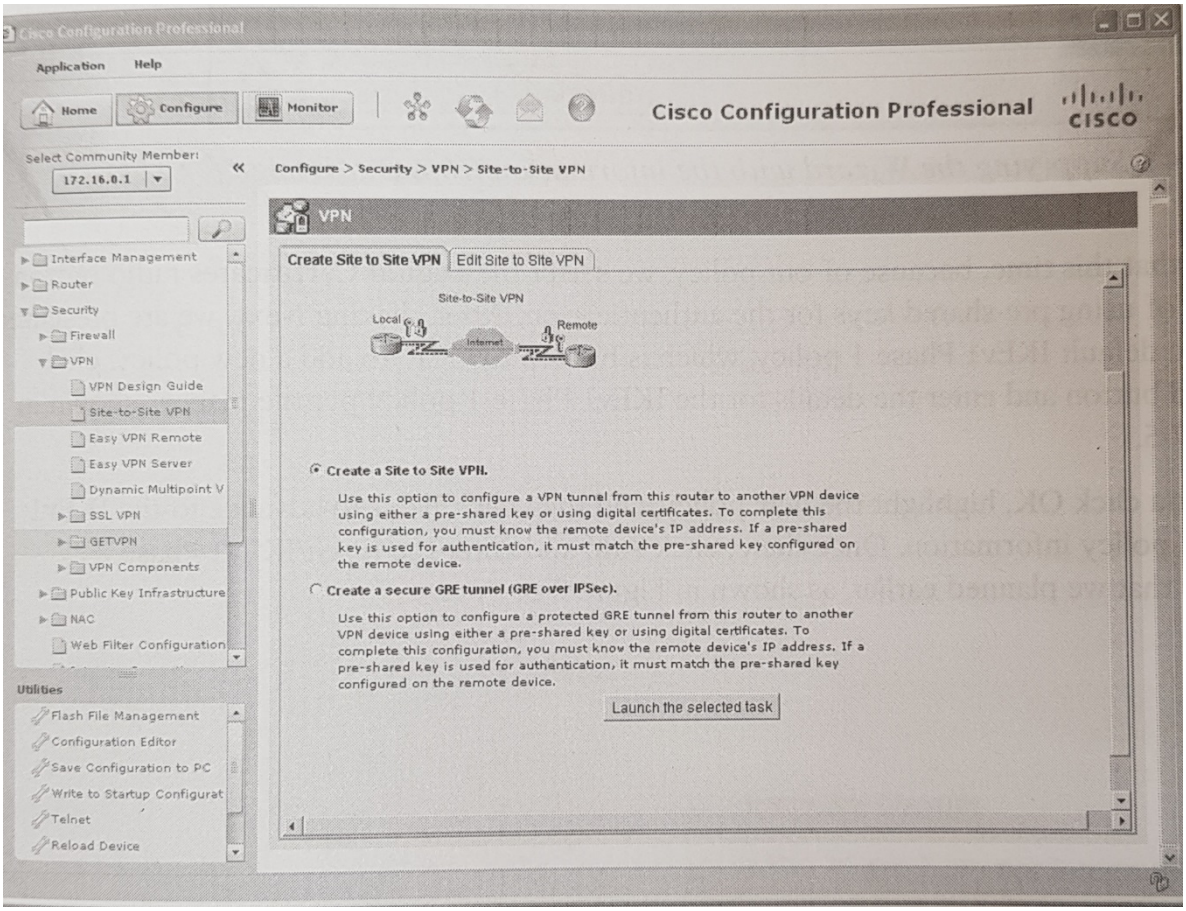
CRYPTO_PKI: Certifiate Request Fingerprint MD5: B1AF5247 s1F35FE3 0200F345 7C20FBA0

CRYPTO_PKI: Certifiate Request Fingerprint SHA1: F5BB33E3 1CB5D633 0DF720DF 8C72CD48 E744CF5B

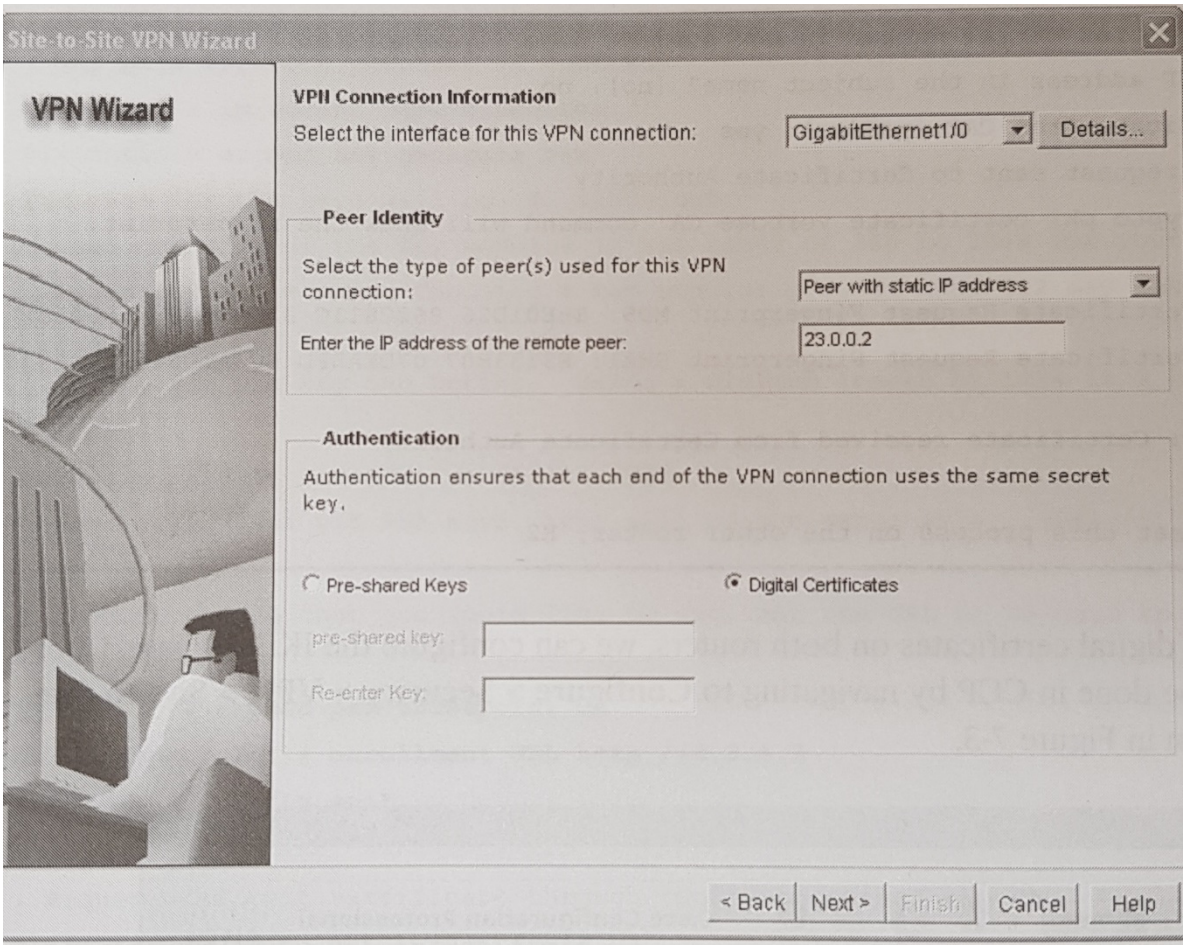
%PKI-6-CERTRET: Certificate received from Certificate Authority

¡podriamos repetir este proceso en el router R2

Despues de que nosotros tenemos el certificado digital en ambos routers, podemos configurar el IKEv1 Phase 1. Esto puede ser hecho en el CCP navegando por Configure>Security>VPN>Site-toSite VPN como muestra la figura.



Usando el botón Launch the Selected Task para continuar, escogemos el Step-by-Step Wizard (dentro encontraras Quick Setup), y entonces hacer click en Next. Tenemos la oportunidad para empezar enterado de la información recolectada antes sobre la interface para usar y las políticas para implementar, como se muestra en la figura.



Supliendo el wizard con la información de nuestro diseño para este cliente.

Preste atención en este momento, por que en nuestra política, selecionamos el Digital Certificates en el circulo en lugar que Pre-Shared Keys para la autenticación. Después hacemos click en Next, nosotros estamos presentando con las políticas poe defecto de IKEv1 Phase 1, que se esta configurando con el CCP. Para agregar nuevas políticas, click en Add he ingresar los detalles para IKEv1 Phase 1 del plan, como muestra la figura.

Después de hacer click en OK, en lo alto de la nueva política, y entonces click en Next para continuar para IKEv1 Phase 2. Una vez allí, click en Add he ingresar IPsec/IKEv1 Phase 2 que planteamos antes , como muestra la figura.

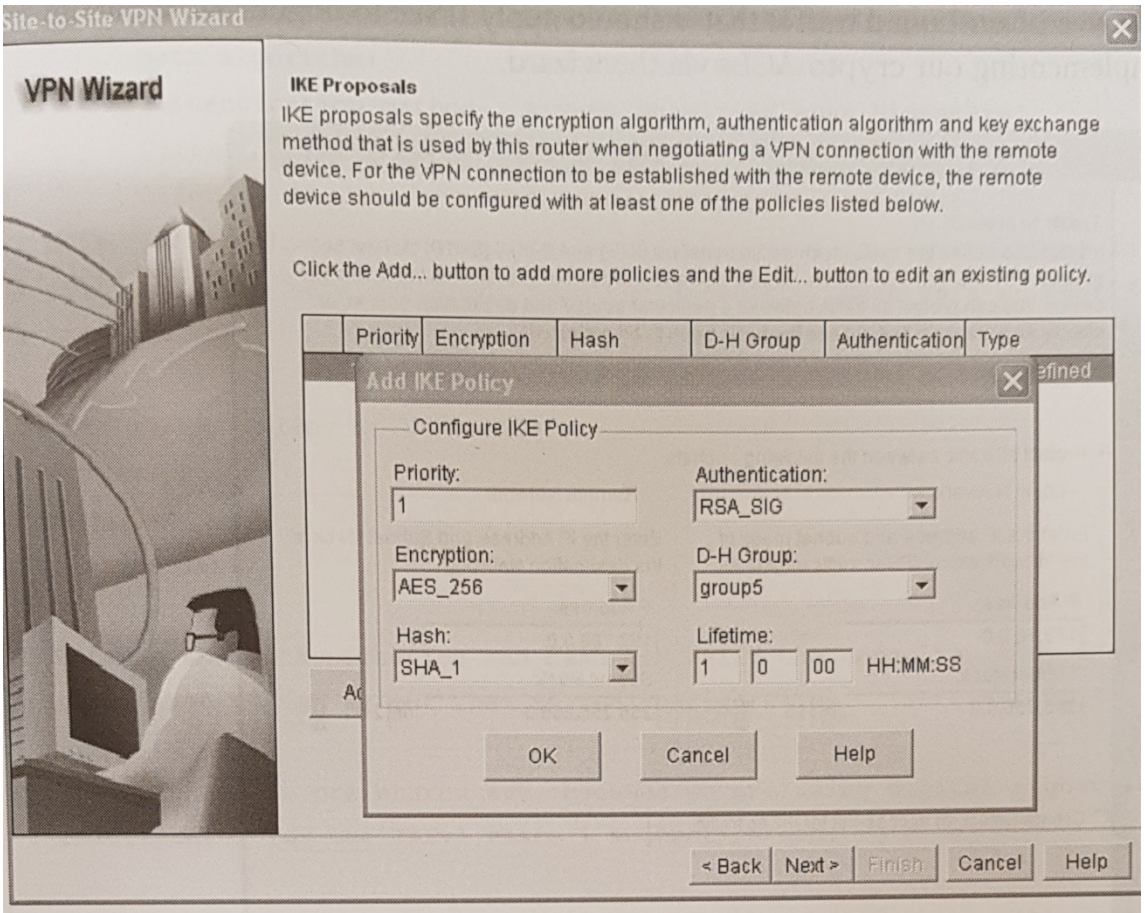
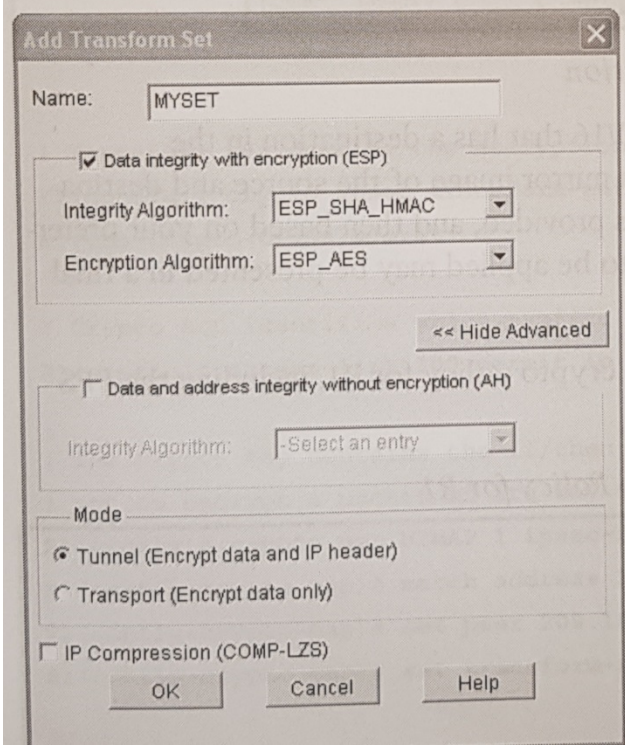
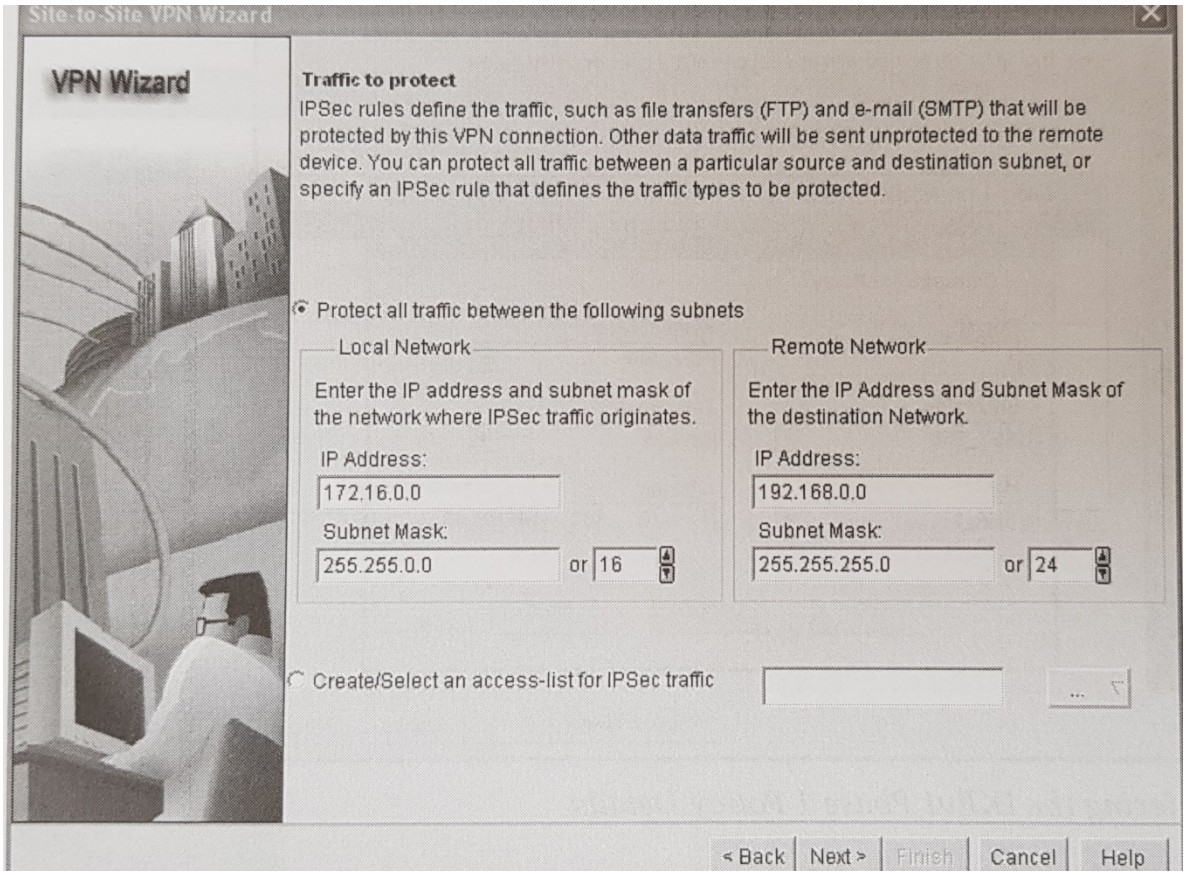


Figure 7-5 *Entering the IKEv1 Phase 1 Policy Details*



Desafortunadamente, la opción para configurar PFS para IKEv1 Phase 2 no esta integrado en el wizard. Vamos a finalizar el wizard, para confirmar la información del ACL, haciendo click en OK para el Transform Set, haciendo clcik en Transform Set para resaltarlo, y haciendo click en Next para continuar. A la siguiente ventana, nosotros especificamos cua trafico para cifrar. Recordar que este es de la perspectiva del router local para la salida del trafico que debería palicar IPsec. La figura muestra un ejemplo de implementación de nuestro crypto ACL via wizard.



En R1, la ACL coincide con el trafico de 172.16.0.0/16 que tiene un destino hacia la 192.168.0.0/24. La ACL en R2 debe ser el espejo imagen de la fuente y destino de red. Cuando usted hace ckick en Next, un resumen es mostrado, y entonces basado en sus preferencias de configuiracion del CCP, el comando para ser aplicada puede ser presentado en el final de la ventana antes de que usted las apruebe para ser entregadas.

Implementacion del Crypto Policy para R1 en el CLI

R1(config)#crypto isakmp policy 1

R1(config-isakmp)#encr aes 256

R1(config-isakmp)#group 5

R1(config-isakmp)#lifetime 3600

R1(config-isakmp)#authentication rsa-sig

R1(config-isakmp)#hash sha

!para verificar la configuracion:

R1# show crypto isakmp policy

Global IKEv1 policy

Protection suite of priority 1

Encryption algorithm:	AES – Advanced Encryption Standard (256 bit keys).
Hash alghorithm:	Secure Hash Standard.
Authentication method:	Rivest-Shamir-Adleman Signature.
Diffiie-Hellman group:	#5 (1536 bit)
Lifetime:	3600 seconds, no volume limit

!Note, que un show running-config, solo mostraria detalles configurados en la politica si ellas ¡fueran diferentes de las que hay por defecto. Aquí hay un pedazo del show runn:

Crypto isakmp policy 1

Encr aes 256

Group 5

Lifetime 3600

!Por que la authentication y el hash estan usando las configuraciones por defecto, ellas no son ¡mostradas incluso auque las pusimos en la configuración. (Interesante para conocer)

¡Nosotros no necesitaremos un PSK pre-shared key, porque estamos usando digital ¡signatures/certificates para IKEv1 phase 1 autenticacion.

¡Lo siguiente nosotros podemos crear nuestro transform –set, y crypto ACL, la cual será ubicada ¡dentro del crypto-map. El crypto map será ubicado en la interface del router.

¡Transform-set detalla el cifrado y HMAC para usar

R1(config)#crypto ipsec transform-set MYSET esp-aes esp-sha-hmac

R1(config-trans)#exit

!Crypto ACL identifica cual trafico de salida sera cifrado.

R1(config)#access-list 100 permit ip 172.16.0.0 0.0.255.255 192.168.0.0 0.0.0.255

!el crypto map contiene la declaración para decidir cifrar o no un paquete en su camino hacia ¡afuera.

R1(config)#crypto map MYSET 1 ipsec-isakmp

R1(config-crypto-map)#match address 100

R1(config-crypto-map)#set peer 209.165.201.1

R1(config-crypto-map)#set transform-set MYSET

!aqui esta el PFS parte que estamos agregando manualmente, como el wizard no soporta esta ¡caracteristica

R1(config-crypto-map)#set pfs group2

R1(config-crypto-map)#exit

!aplicando el crypto map a la interface es que permite la función completa ipsec para ser ¡disparada. Es por eso que es importante que el router tenga al menos una ruta predeterminada

¡(si no es una ruta más específica) fuera de esta interfaz para llegar a la red ¡remota para la cual el ¡enrutador brinda soporte IPsec.

Cuando el router considera enviar trafico fuera de esta interface, es disparada la decisión para cifrar o no, si el trafico coincide con el crypto ACL en el crypto map, el router cifrara los paquetes originales, encapsula los paquetes cifrados dentro de un nuevo paquete con ESP en el encabezado de capa 4, y la dirección IP global del peer con la nueva cabecera de capa 3. Si no IPsec SA (tunnel) no es construido todavía, esto desparara la negociación para construir el túnel, incluyendp IKEv1 phase 1 si no esta ya en el lugar.

R1(config)#interface gigabitethernet 1/0

R1(config-if)#crypto map MYMAP

R1(config-if)#exit

Despues de la apropiada configuracion compatible que ha sido ubicada en R2, deberiamos poder cifrar trafico entre las dos redes usando IPsec.

TROUBLESHOOTING IPsec Site-to-Site VPN en CISCO IOS

Cuando se implementa una nueva VPN, alli puede ser un problema o 2, asi que, vamos atras a traves de la verificacion del tunel, y si lo descubrmos no trabajando, le mostrare alguno de mis commandos favoritos para asistir en el proceso de troubleshooting.

¡esto verifica que IKEv1 Phase 1 policy o políticas se ubique dentro del lugar.

R1#show crypto isakmp policy

Global IKEv1 policy

Proteccion suite of priority 1

Encryption algorithm:	AES -Advances Encryption Standard (256 bit key)
Hash algorithm:	Secure Hash Standard
Authentication method:	Rivest-Shamir-Adleman Signature
Diffie-Hellman group:	#5 (1536 bit)
Lifetime:	3600 seconds, no volume time limit

!el siguiente es mi commando favorite, como lo muestra virtualmente todo el resto de la ¡configuracion incluyendo el transfor set y crypto ACL involucrada, y donde el crypto map esta ¡aplicado.

```
R1#show crypto map
Crypto Map “MYMAP” 1 ipsec-isakmp
        Peer=209.165.201.1
        Extended IP access list 100
            Access-list 100 permit ip 172.16.0.0 0.0.255.255 192.168.0.0 0.0.0.255
        Current peer: 209.165.201.1
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N):  N
        PFS  (Y/N) :  Y
        DH group:          group2
        Transform sets={
                MYSET:         {esp-aes esp-sha-hmac}   ,
         }
        Interface using crypto map MYMAP:
                        GigabitEthernet1/0
```

Armado con esta informacion, un paquete de la red 172.16.0.0 destiando a la red 192.168.0.0 dispara el proceso IPsec. Podemos probar esto sin sacar la consola del router. Porque R1 conectado a la red 172.16.0.0, podemos hacer ping de solicitud generados en la red y destinados a la dirección 192.168.0.2 o R2

Ejemplo:

```
R1#ping 192.168.0.2 source g1/0

Type escape sequence to abort.
Sending 5, 100 byte ICMP Echo to 192.168.0.2, timeout is 2 seconds:
Packet sent with a source address of 209.165.200.225
U.U.U
Source rate is 0 percent (0/5)
R1#
```

Un ping esta siendo respondido con un mensaje U.U.U. La U representa un mensaje ICMP inalcanzable siendo enviado hacia nosotros de uno de los routers de internet (probablemente nuestro router directamente conectado). Si nuestra política no fue aplicada correctamente, puede ser posible que nosotros estemos intentando para enviar paquetes a la 192.169.0.2, y cuando el ISP ve estos paquetes, ellos son denegados por que ellos tienen espacios de direcciones en el RFC 1918 (los cuales no son permitidos en internet). Si los paquetes han sido exitosamente encapsulados dentro de la capa 4 de IPsec protocolo 50 (ESP), la internet habría visto un paquete destiando para la capa 3 direccion global 209.165.201.1, generados de la dirección global de R1.

¡Vamos al troubleshooting! Nosotros podemos querer ir a R2 y hacer el mismo comando show que hicimos en R1. Si R2 no es accesible via CLI al momento, podríamos hacer también algúna prueba a R1 usando debug específicamente para IPsec Phase 1 y Phase 2. Para IKEv1 Phase 1 debugging, podríamos usar el comando mostrado en el ejemplo

¡Proceso de depurar IKEv1 Phase 1!

```
R1#debug crypto isakmp

Crypto ISAKMP debugging is on
```

¡generar trafico interesado que coicidiria la ACL usada en el crypto map

```
R1#ping 192.168.0.2 source gi1/0

Type escape sequence to abort.
Sending 5, 100 byte ICMP Echo to 192.168.0.2, timeout is 2 seconds:
Packet sent with a source address of 209.165.200.225
U.U.U
Source rate is 0 percent (0/5)
```

Con la depuracion de IKEv1 Phase 1 on, y entonces usando el ping otravez, no vemos salida del debug. Esto implica que antes IKEv1 Phase 1 esta ya arriba y no necesita ser negociado, o si este esta actualmente abajo, sin trafico interesante disparándolo. Esto podría ser por una interface abajo, un crypto map mal aplicado, o enrutamiento que no esta tratando de enviar trafico fuera de la interface que tiene el crypto map aplicado, vamos a tomar una mirada mas de cerca, mostrado en el ejemplo.

```
R1#show crypto map
Crypto Map “MYMAP” 1 ipsec-isakmp
        Peer=209.165.201.1
        Extended IP access list 100
            Access-list 100 permit ip 172.16.0.0 0.0.255.255 192.168.0.0 0.0.0.255
        Current peer: 209.165.201.1
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N):  N
        PFS  (Y/N) :  Y
        DH group:          group2
        Transform sets={
                MYSET:         {esp-aes esp-sha-hmac}   ,
         }
        Interface using crypto map MYMAP:
                        GigabitEthernet1/0
```

```
R1#show ip int brief
Interface                  IP-Address   OK? Method  Status                          Protocol
FastEthernet 0/0           unassigned   YES unset   administratively   down          down
GigabitEthernet1/0         209.165.200.225     YES manual              up            up
GigabitEthernet2/0         172.16.0.1   YES manual  up                              up
```

¡solo como antes, el crypto map aparecec para ser aplicado a la interface correcta, y ambas ¡interfaces estan UP. Vamos a la siguiente verificación para ver si hay IKEv1 Phase 1 ya ubicada.

```
R1#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
Dts                        src                         state                       conn-id  status
```

¡la salida del comado arriba indica que no hay IKEv1 Phase 1 tunnel actualmente ubicado. Vamos a verificar el enrutamiento, para ver si R1 intentaria incluso enviar paquetes a 192.168.0.2 a través de la interface g1/0.

```
R1#show ip route

C       172.16.0.0/16 is directly connected, GigabitEthernet 2/0
        209.165.200.0/24 is subnetted, 1 subnets
C       209.165.200.0 is directly connected, GigabitEthernet 1/0
S*    0.0.0.0/0 [1/0] via 209.165.200.226
```

¡La salida del show ip route indica que R1 usara su G1/0 para usar el default gateway ¡209.165.200.226. nosotros recivimos un mensaje U antes de el router por eso.

¡A veces cuando hacemos cambios de configuraciones considerando IPsec, el dispositivo VPN ¡puede llegar a ser confundido si no hay trafico VPN trabajando, tenemos buscar remover y re ¡aplicar el crypto map de la interface es amenudo exitoso y re empezar el proceso IPsec en el ¡router. Vamso a intentarlo a continuación en R1.

```
R1(config)#int gi0/1
R1(config-if)# no crypto map MYMAP
R1(config-if)# crypto map MYMAP
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is OFF
R1(config-if)# crypto map MYMAP
R1(config-if)#
%CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

¡note que ISAKMP giro el mismo abajo, cuando el map fue removido y giro arriba de regreso ¡cuando el map fue reubicado, basado en el mensaje de consola. ISAKMP permanece para ¡Internet Security Association Key Managment Protocol. Ahora vamos intentar el ping de nuevo.

¡debugging esta aun en on

R1#show debug

Cryptographic Subsystem:
  Crypto ISAKMP debbuging is on

R1#ping 192.168.0.2 source gi1/0

Type escape sequence to abort.
Sending 5, 100 byte ICMP Echo to 192.168.0.2, timeout is 2 seconds:
Packet sent with a source address of 209.165.200.225
U.U.U
Source rate is 0 percent (0/5)

R1#

El mismo resultado como antes. Asi que vamos a pensar en el dolor del troubleshooting? Porque esta es una habilidad que usted debe tener, y por que vamos a pensarlo juntos, eso lo hara tener mejores hablidades para el mundo real. Antes de ir tanto al futuro. Vamos a pausar y examinar nuestro ping de test. Un común error en las personas es asumir la VPN debería venir arriba, incluso si no hay trafico de interés (coincidiendo la crypto ACL).

En nuestro ping, en nuestro ping el origen es la interface g1/0 (esta interface no esta en la red 172.16.0.0/16) y por lo tanto como un resultado el paquete no coincide la crypto ACL. El router no lo piensa el debaria aplicar IPsec, asi que envía un ping en texto plano hacia fuera. Las direcciones IP fuente original y destino no están cargadas, lo cual causa que el ISP deniegue el trafico.

Armado con el conocimiento de nuestro ping de test tiene un problema, vamos a depurar e intentar el ping, como muestra el ejemplo.

R1#ping 192.168.0.2 source g2/0

¡A pesar de que hay poco trafico interesante de salida, apuntaremos nuestra información mas ¡relevante considerando nuestro troubleshooting

send 5, 100-byte ICMP Echo to 192.168.0.2, timeout is 2 seconds:

¡Note la direccion Fuente correcta, importa si nosotros queremos coincidir el crypto ACL

Packets sent with a source address of 172.16.0.1

ISAKMP: (0) : SA request profile is (NULL)
ISAKMP: Created a peer struct for 209.165.201.1, peer port 500
ISAKMP: New peer created peer = 0x6A76F70 peer_handle = 0x80000005

ISAKMP: Looking peer struct 0x6A76F70, refcount 1 for isakmp_initiator
ISAKMP: local port 500, remote port 500
ISAKMP: set new mode 0 to QM_IDLE
ISAKMP: (0) : insert sa successfully sa = 66570618
ISAKMP: (0) : Can not start Aggressive mode, trying Main Mode
ISAKMP: (0) : No pre-shared key with 2009.165.201.1!
ISAKMP: (0) : constructed NAT-T vendor-rfc3947 ID
ISAKMP: (0) : constructed NAT-T vendor-07 ID
ISAKMP: (0) : constructed NAT-T vendor-03 ID
ISAKMP: (0) : constructed NAT-T vendor-02 ID
ISAKMP: (0) : Input = IKEv1_MESG_FROM_IPSEC, IKEv1_SA_REQ_MM
ISAKMP: (0) : Old state = IKEv1_READY New State = IKEv1_I_MM1

ISAKMP: (0) : beginning Main Mode Exchange

¡R1 es el iniciador, y asi que el esta enviando el primer paquete, tartando de negociar un ¡compatible IKEv1 Phase 1 policy con R2

ISAKMP: (0) : sending packet to 209.165.201.1 my_port 500 peer_port 500 (I) MM_STATE
ISAKMP: (0) :Sending an IKEv1 IPv4 Packet.
ISAKMP: (0) : received packet from 209.165.201.1 dport 500 sport 500 Global (I) MM_NO_STATE
ISAKMP: (0) :Notify has no hash. Rejected
ISAKMP: (0) : Unknow Input IKEv1_MESG_FROM_PEER, IKEv1_INFO_NOTIFY: statet = IKEv1_I_MM1
ISAKMP: (0) :Input = IKEv1_MESG_FROM_PEER, IKEv1_INFO_NOTIFY
ISAKMP: (0) :Old State = IKEv1_MM1 New State = IKEv1_I_MM1

¡esta linea debajo son malas noticias. IKEv1 Phase 1 fallo

%CRYPTO-6-IKMP_MODE_FAILURE: Processing of Informational mode failed with peer at 209.165.201.1

¡y nuestro ping no lo hizo también (no túnel VPN todavía).

. . . . .

Success rate is 0 percent (0/5)

¡El IKEv1 Phase 1 tunnel tiene un estado de MM_NO_STATE lo cual no es algo bueno nosotros ¡queremos ver el estado de QM_IDLE, significa el IKEv1 Phase 1 esta arriba, en la salida del ¡siguiente comando, que muestra el estado del IKEv1 Phase 1 tunnel.

R1#show crypto isakmp sa
IPv4 Crypto isakmp SA

Dst	src	state	conn-id status
209.165.201.1	209.165.200.225	MM_NO_STATE	0 ACTIVE

Quiza R2 no esta configurado correctamente. Si IKEv1 Phase 1 ha completado, podríamos investigar IKEv1 Phase 2, pero debido a la falla de Phase 1, aquello es lo primero que rivizamos en R2, la IKEv1 Phase 1 policy match en R2, también quisiéramos verificar que R2 tenga un Digital Certificate para usar con RSA-Signature. Vamos a mirar la política de R2, que se muestra en el ejemplo.

R2#show crypto isakmp policy
Global IKEv1 policy
Protection suite of priority 1

Encryption algorithm:	three key triple DES
Hash algorithm:	secure hash standard
Authentication method:	Rives-Shamir-Adleman Signature
Diffie-Hellman group:	#5 (1536 bit)
Lifetime:	3600 seconds, no volume limit

¡basado en la salida, aparece el algoritmo de cifrado para R2 IKEv1 Phase 1 configurado como ¡3DES, y en R1 fue configurado con AES 256, eso es un problema. Vamos hacer los cambios en R2, ¡habilitando la depuración, y ver si obtenemos un mejor resultado.

¡cambiando la política en R2

R2(config)#crypto isakmp policy 1
R2(config-isakmp)#encryption aes 256
R2(config-isakmp)#end

¡abilitando debug de IKEv1 Phase 1 y mostrar el ping de R2 disparando el crypto ACL (el cual esta ¡en el crypto map, el cual esta aplicado en la interface).

R2#debug crypto isakmp
Crypto ISAKMP debugging i son

R2#ping 172.16.0.1 source gi2/0

Type escape sequence to abort.
Sending 5, 100 byte ICMP Echo to 172.16.0.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.0.2

ISAKMP: (0) : SA request profile is (NULL)
ISAKMP: Created a peer struct for 209.165.200.225, peer port 500
ISAKMP: New peer created peer = 0x6816E21C peer_handle = 0x80000006
ISAKMP: Looking peer struct 0x6816E21C, refcount 1 for isakmp_initiator
ISAKMP: local port 500, remote port 500
ISAKMP: set new node 0 to QM_IDLE
ISAKMP: (0) : insert sa successfully sa = 671E34DC

¡los dos modos de IKEv1 Phase 1 es aggressive, o principal. R2 va a usar modo principal.

ISAKMP: (0) : Can not start Aggressive mode, trying Main Mode

¡R2 no necesitara un pre-shared key con R1 para autenticar, debido al uso de digital signature

ISAKMP: (0) : No pre-shared key with 209.165.200.225!
ISAKMP: (0) : constructed NAT-T vendor-rfc3947 ID
ISAKMP: (0) : constructed NAT-T vendor-07 ID
ISAKMP: (0) : constructed NAT-T vendor-03 ID
ISAKMP: (0) : constructed NAT-T vendor-02 ID
ISAKMP: (0) : Input = IKEv1_MESG_FROM_IPSEC, IKEv1_SA_REQ_MM
ISAKMP: (0) : Old state = IKEv1_READY New State = IKEv1_I_MM1
ISAKMP: (0) : beginning Main Mode Exchange
ISAKMP: (0) : sending packet to 209.165.200.225 my_port 500 peer_port 500 (I) MM_STATE
ISAKMP: (0) :Sending an IKEv1 IPv4 Packet.
ISAKMP: (0) : received packet from 209.165.200.225 dport 500 sport 500 Global (I) MM_NO_STATE
ISAKMP: (0) :Input = IKEv1_MESG_FROM_PEER, IKEv1_MM_EXCH
ISAKMP: (0) :Old State = IKEv1_MM1 New State = IKEv1_I_MM2
ISAKMP: (0) : processing SA payload. Message ID = 0
ISAKMP: (0) : processing vendor id payload
ISAKMP: (0) : vendor ID seems Unity/DPD but major 69 mismatch
ISAKMP: (0) : vendor ID is NAT-T RFC 3947
ISAKMP: (0) : Scanning profile for xauth...

¡observe como estos dos peers han encontrado una politica compatible. Eso es contenido de la política que necesita para ser compatible, no la política literal numero de prioridad la compilación muestar la palabra “transform” pero no debe ser confundida con IKEv2 Phase 2 lo cual ocurre solo después de IKEv1 Phase 1 es completado.

ISAKMP: (0) : checking . ISAKMP transform 1 against priority 1 policy
ISAKMP: (0) : encryption AES-CBC
ISAKMP: (0) : keylength of 256
ISAKMP: (0) : hash SHA
ISAKMP: (0) : default group 5
ISAKMP: (0) : auth RSA sig
ISAKMP: (0) : life type in seconds
ISAKMP: (0) : life duration (basic) of 3600

¡los peers han estado deacuerdo en el IKEv1 Phase 1 Policy

ISAKMP: (1004) : SA has been authentication with 209.165.200.225

ISAKMP: (1004) : Old State = IKEv1_I_MM6 New State = IKEv1_P1_COMPLETE

¡ahora que IKEv1 es completado, IKEv1 Phase 2 (quick mode) puede iniciar.

ISAKMP: (1004) : beginning Quick Mode Exchange, M-ID of -534639709

Cuando IKEv1 Phase 1 trabaja, vamos a concentrarnos en IKEv1 Phase 2 y ver si nosotros resolver el problema (por que el ping no lo hizo) para comparar los componentes IKEv1 Phase 2 en ambos R1 y R2.

R1# show crypto map
Crypto Map “MYMAP” 1 ipsec-isakmp
Peer = 209.165.201.1
Extended IP access list 100
Access-list 100 permit ip 172.16.0.0 0.0.255.255 192.168.0.0 0.0.0.255
Current peer: 209.165.201.1
Security association lifetime: 4608000 kilobytes/3600 seconds
Responder-Only (Y/N) : N
PFS (Y/N) : Y
DH group: group2
Transform sets = {
MYSET: { esp-aes esp-sha-hmac}
}
Interface using crypto map MYMAP:
GigabitEthernet1/0

¡vamos verificando el otro router

```
R2#show crypto map
Crypto Map “MYMAP” 1 ipsec-isakmp
        Peer = 209.165.200.225
        Extended IP access list 100
            Access-list 100 permit ip 192.168.0.0 0.0.0.255 172.16.0.0 0.0.255.255
        Current peer: 209.165.200.225
        Security association lifetime: 4608000 kilobytes/3600 seconds
        Responder-Only (Y/N) : N
        PFS (Y/N) : N
        Transform sets = {
                MYSET:    { esp-aes esp-sha-hmac}
        }
        Interface using  crypto map MYMAP:
                GigabitEthernet1/0
```

¡basados en la salida, buscamos como R1 esta configurado para usar PFS group2, y R2 no. Vamos a ¡corregir esto en R2, y re intentar el ping.

```
R2(config)# crypto map MYMAP 1 ipsec-isakmp
R2(config-crypto-map)#set pfs group 2
R2(config-crypto-map)#end
```

¡ahora vamos a intentar ese ping.

```
R2#ping 172.16.0.1 source gi2/0
Type escape sequence to abort.
Sending 5, 100 byte ICMP Echo to 172.16.0.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.0.2
.!!!!
Success rate is 80 porcent (4/5). Round-trip min/avg/max = 32/38/44 ms
R2#
```

¡el primer ping pudo haber estado fuera antes que el túnel (Phase 2) IPsec se estableciera, pero el resto de los ping y futuros pings pueden tomar ventaja del túnel existente y deberían trabajar.

```
R2#ping 172.16.0.1 source gi2/0 repeat 500

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

!!
!!!!!!!!!!!!!!!!

Success rate is 100 porcent (500/500). Round-trip min/avg/max = 32/38/44 ms
R2#

¡para cerificar el IKEv1 Phase 1 y Phase2, podemos usar el commando

R2#show crypto isakmp sa
IPv4 Crypto ISAKMP SA

Dst	src	state	con-id status
209.165.200.225	209.165.201.1	QM_IDLE	1004 ACTIVE

¡QM_IDLE es el estado deseado para la salida del commando arriba

R2#show crypto isakmp sa detail
Code: C – IKEv1 configuration mode, D – Dead Peer Detection
K – Keepalives, N – NAT-Trasversal
T – cTCP encapsulation, X – IKEv1 Extended Authentication
Psk – Preshared key, rsig – RSA signature
Renc – RSA encryption
IPv4 Crypto ISAKMP SA

C-id	Local	Remote	I-VRF	STATUS	Encr	Hash	Auth	DH	Lifetime	Cap.
1004	209.165.201.1	209.165.200.225		ACTIVE	aes	sha	rsig	5	00:55:54	

¡esto verifica la function IKEv1 Phase 1 (QM_IDLE,ACTIVE) y las opciones detalladas revelan que
¡IKEv1 usando RSA signature para la autenticacion, AES para cifrado, SHA para el hashing y DH
¡group 5, con el tiempo de vida restante por que eso fue inicialmente agregado por los peers.

¡para verificar el IPsec (IKEv1 Phase 2) tunnel, podemos hacerlo con el siguiente comando.

R2#show crypto ipsec sa

Interface: GigabitEthernet 1/0
Crypto map tag: MYMAP, local addr 209.165.201.1

Protected crf: (none)
Local idle (addr/mask/prot/port) : (192.168.0.0/255.255.255.0/0/0)

```
      Remote idle (addr/mask/prot/port) : (172.16.0.0/255.255.0.0/0/0)
         Current_peer 209.165.200.225 port 500
            PERMIT, flas={origin_is_acl,}
           #pkts encaps: 504, #pkts ecrypt: 504, #pkts diges: 504
           #pkts decaps: 504, #pkts ecrypt: 504, #pkts diges: 504
           #pkts compressed: 0, #pkts decompressed: 0
           #pkts not compressed: 0, #pkts comp. failed: 0
           #pkts not decompressed: 0, #pkts decompress failed: 0
           #send error 11, #recv error 0


          Local crypto endpt.:  209.165.201.1, remote crypto endpt.: 209.165.200.225
          Phat mtu 1500, ip mtu 1500, ip mtu idl GigabitEthernet1/0
          Current outbound spi: 0x3BE5B517 (1004909847)
          PFS (Y/N) : Y, DH group: group2

¡asociacion  de seguridad de entrada (SA/tunnel) del trafico viniendo del peer


         Inbound esp sas:
            Spi: 0x87F1D10A (2280771850)
                 Transform: esp-aes  esp-sha-hmac   ,
                 In use setting = {Tunnel,    }
                 Con id: 9, flow_id: SW:9, sibling_flag 80000046, crypto map : MYMAP
                 Sa timing: remaining key lifetime (k/sec) :  (4558182/3257)
                 IV size: 16 bytes
                 Replay detection support: y
                 Status: ACTIVE

¡no usa HA, asi que no entarnate  AH SA

            Inbound ah sas:

¡asociacion de seguridad de salida (SA/tunnel) para el trafico que va al otro peer

            Outband esp sas:
                Spi: 0x3BE5B517 (1004909847)
                    Transform: esp-aes esp-sha-hmac
                    In use setting = {Tunnel,    }
                    Con id: 10, flow_id: SW:10, sibling_flag 80000046, crypto map : MYMAP
                  Sa timing: remaining key lifetime (k/sec) :  (4558182/3257)
                  IV size: 16 bytes
                  Replay detection support: y
                  Status: ACTIVE

¡no usando AH, asi que no sale AH SA

             Outband ah sas:
```

¡esta salida ha sido detallada en capítulos previos, pero es relevante conocerque hay 2 SA (Security ¡association) con el IKEv1 Phase 2 (IPsec). Un SA para salir al otro peer, y otro para la entrada del ¡peer. Podemos también ver el cifrado y descifrado para cada uno de los SAs.

¡un comando mas que es usado, y viendo como ojo de alcon la criptografía es este:

R2#show crypto engine connection active
Crypto Engine Connection

ID	Type	Algorithm	Encrypt	Decrypt	IP-Address
9	IPsec	AES+SHA	0	504	209.165.201.1
10	IPsec	AES+SHA	504	0	209.165.201.1
1004	IKEv1	SHA+AES256	0	0	209.165.201.1

Hay otras alternativas de tecnologia VPN SITE-TO-SITE

- Dynamic Multipoint VPN (DMVPN)
- FlexVPN

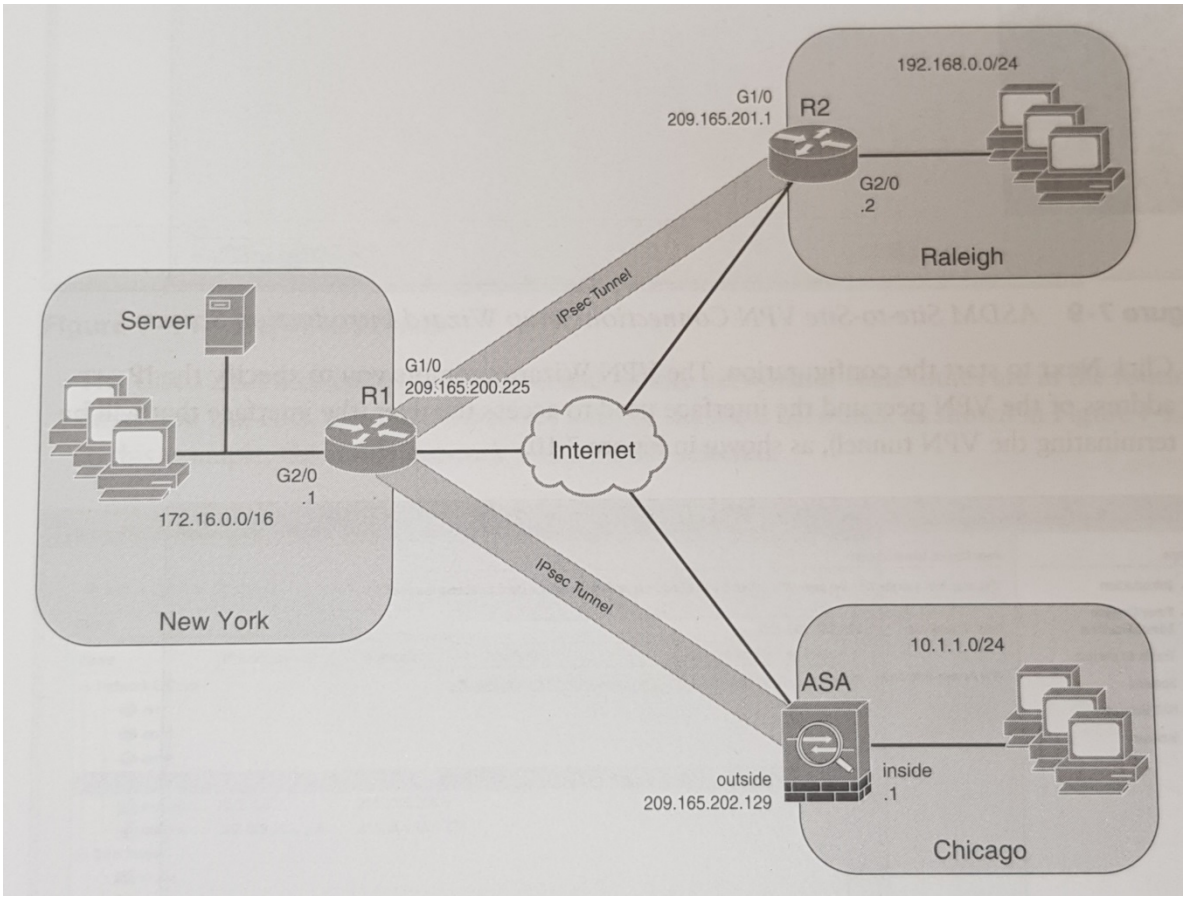
DMVPN es una solucion de cisco para desplegar alta escalabilidad IPsec site-to-siteVPNs. DMVPN usa una arquitectura centralizada para habilitar al administrador de red desplegar control de acceso granular. Permitir ubicaciones remotas para comunicación directa con cada otro sobre internet sin requerir una conexión permanente entre sitios.

FlexVPN es una solucion unificada VPN que puede ser desplegada sobre cualquier conexión de internet publico o redes privadas (MPLS). FlexVPN es diseñada para la concentración de amboas site-to-site y remote Access VPNs. Una FlexVPN puede acepatar ambos tipos de solicitus de coneccion al mismo tiempo. Usa protocolos de enrutamiento para redundancia y selecciona path/head-end.

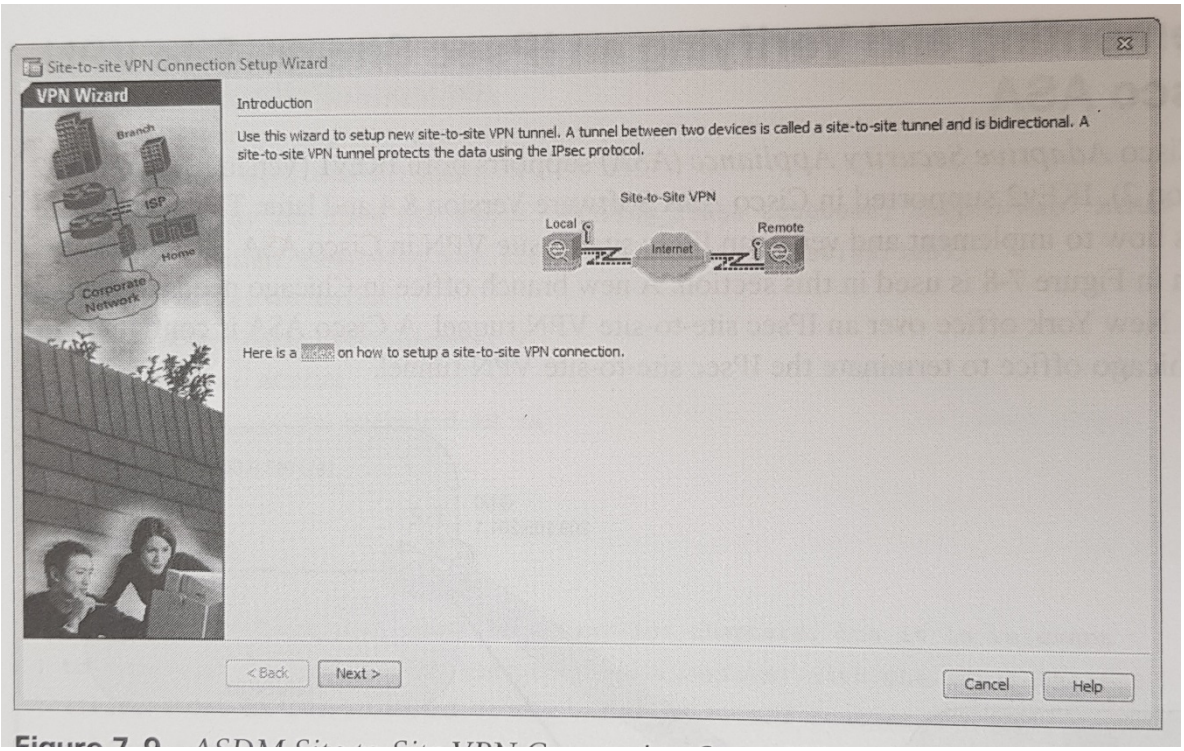
“buscar mas información sobre FlexVPN”

IMPLEMENTANDO Y VERIFICANDO UNA VPN IPsec SITE-TO-SITE EN EL CISCO ASA

El Cisco Adaptative Security Applience (ASA) soporta ambos IKEv1 (versión 1) e IKEv2 (versión 2). IKEv2 soportada software cisco ASA versión de 8.4 y superior. La topología muestra la figura usada en esta sección. Una nueva oficina remota en Chicago necesita conectar a NY sobre el Tunel IPsec VPN site-to-site. Un Cisco ASA es configurado en Chicago como terminal de la VPN site-to-site.

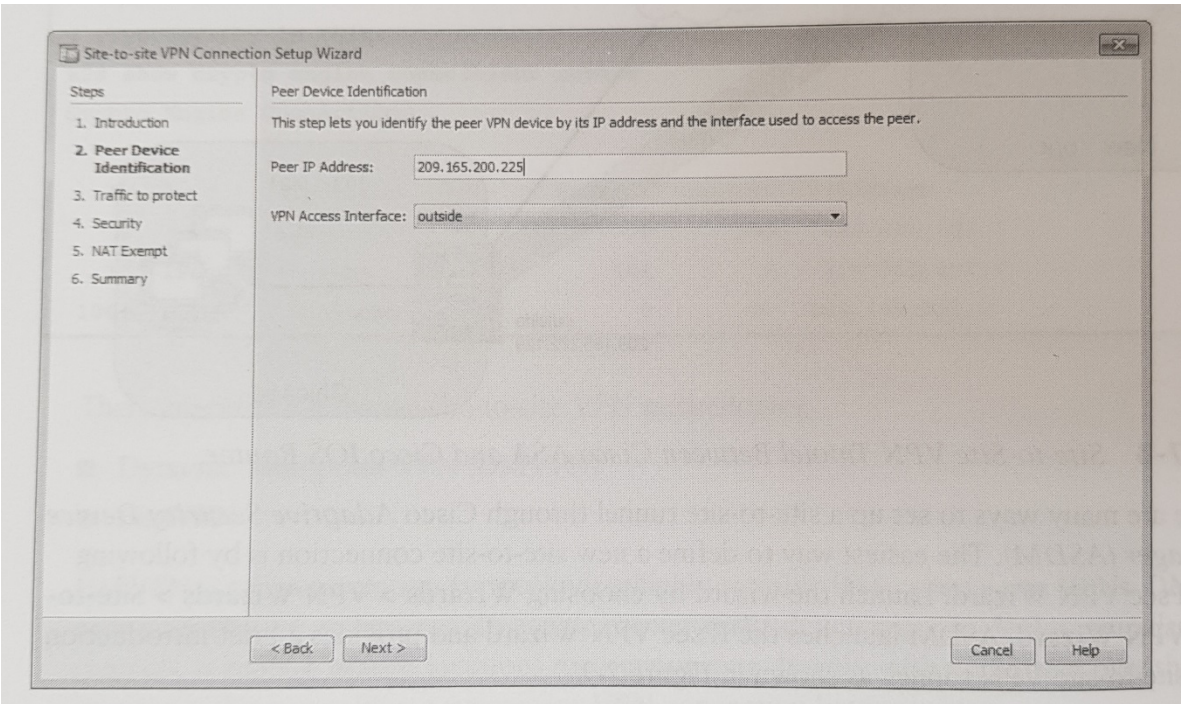


Hay muchos caminos para configurar arriba una VPN site-to-site a través de un Cisco Adaptative Device Manager (ASDM), el camino mas fácil a definir una nueva site-to-site conection es seguir el IPsec VPN Wizard. Lanzar el Wizard para escoger Wizard>VPN Wizard> Site-to-Site VPN Wizard. ASDM lanza el IP sec VPN Wizard y provee una introducción abreviada de un túnel site-to-site. Como muestra la figura.



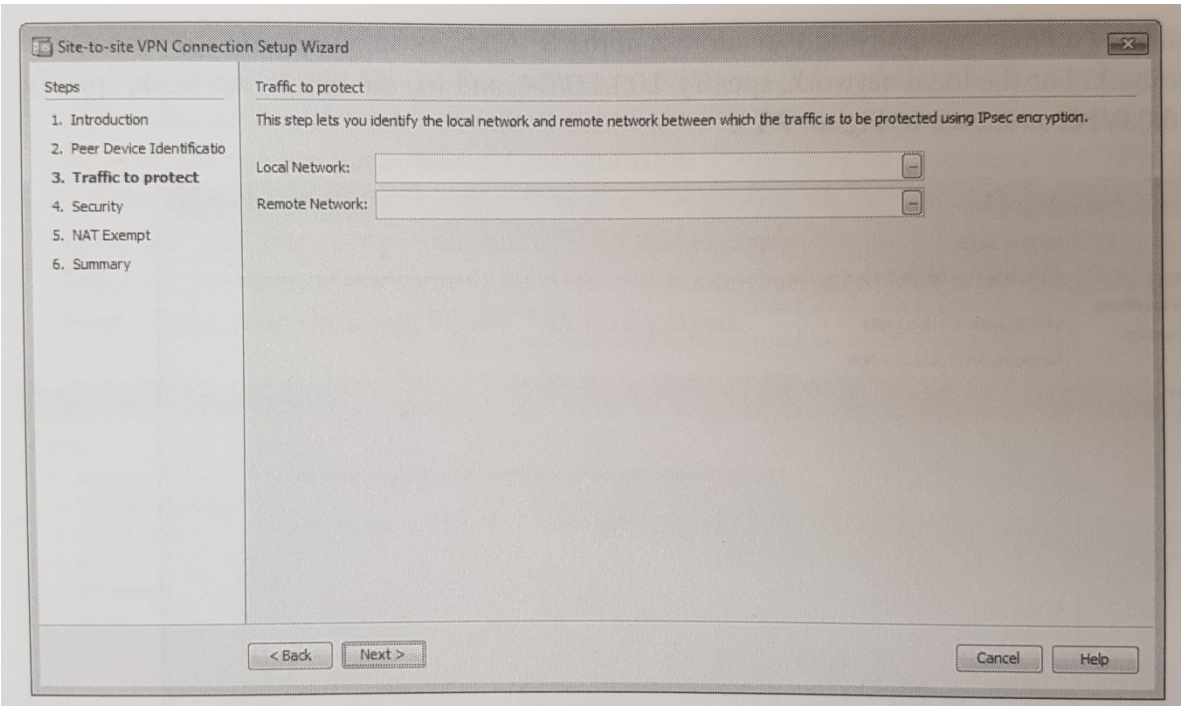
ASMD site-to-site VPN connection setup Wizard Introduction Screen.

Click en NEXT para iniciar la configuracion. En el prompt del Wizard VPN usted puede especificar la dirección IP del peer VPN y la interface usada para accesar al peer (la interface que será la terminación del túnel VPN).

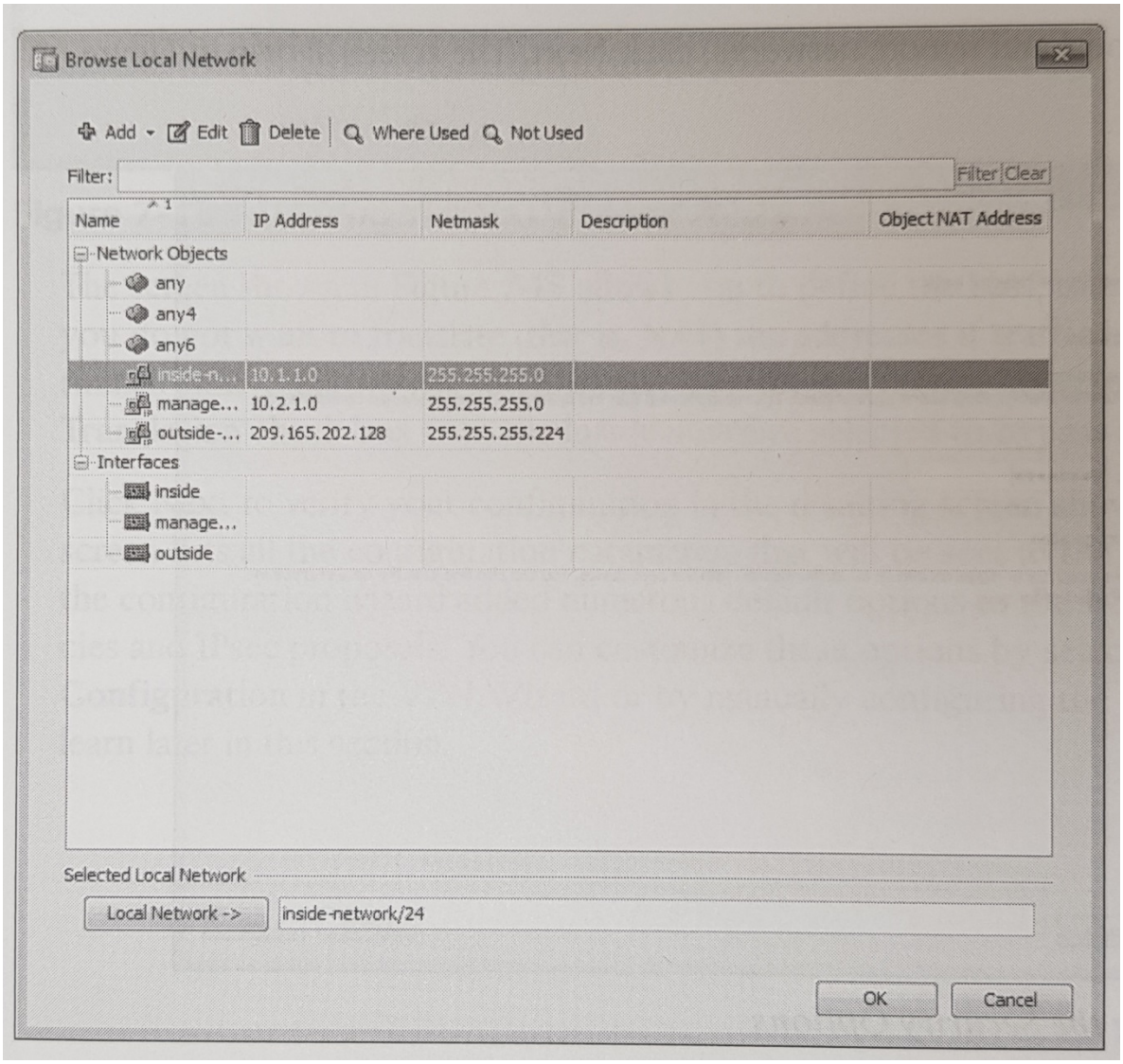


En este ejemplo, la dirección IP del router cisco en NY es 209.165.200.225 la interface de salida es selecionada del VPN ACCESS INTERFACE drop-down menú. Haciendo click en Next.

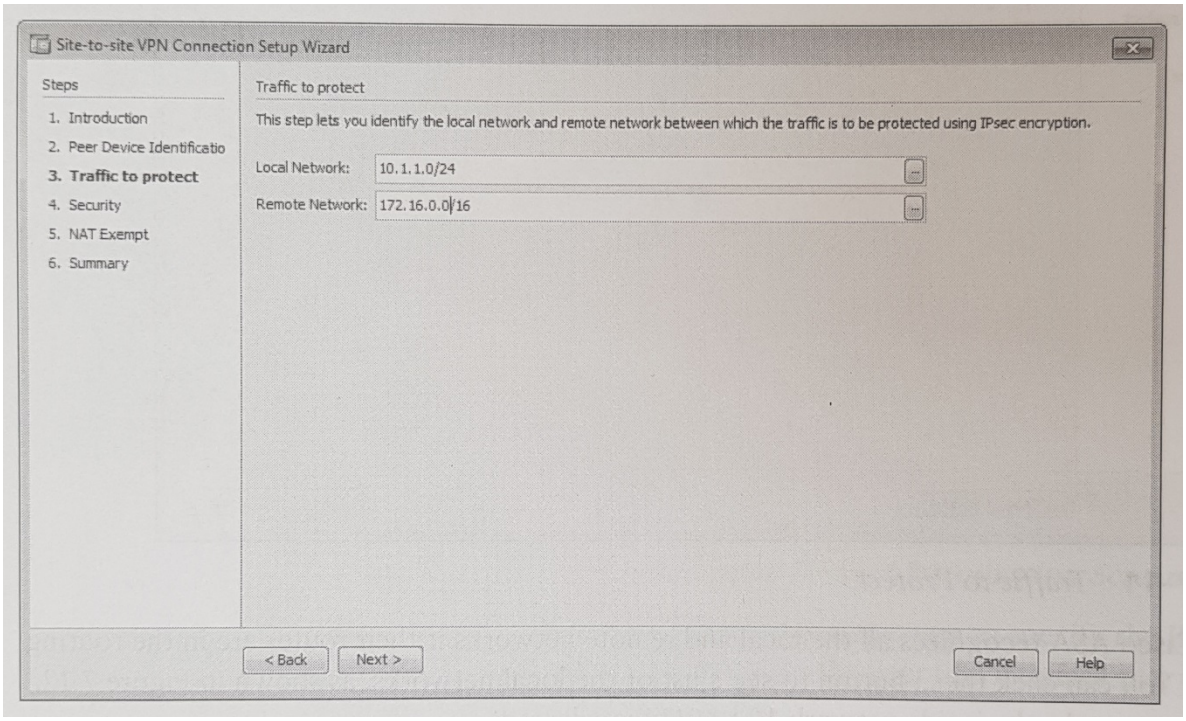
La pantalla muestra dentro de la figura siguiente. Identificando redes locales y remotas. Escogiendo el host/subnets o networks para ser usada como el local y remote proxies durante la negociación IPsec.



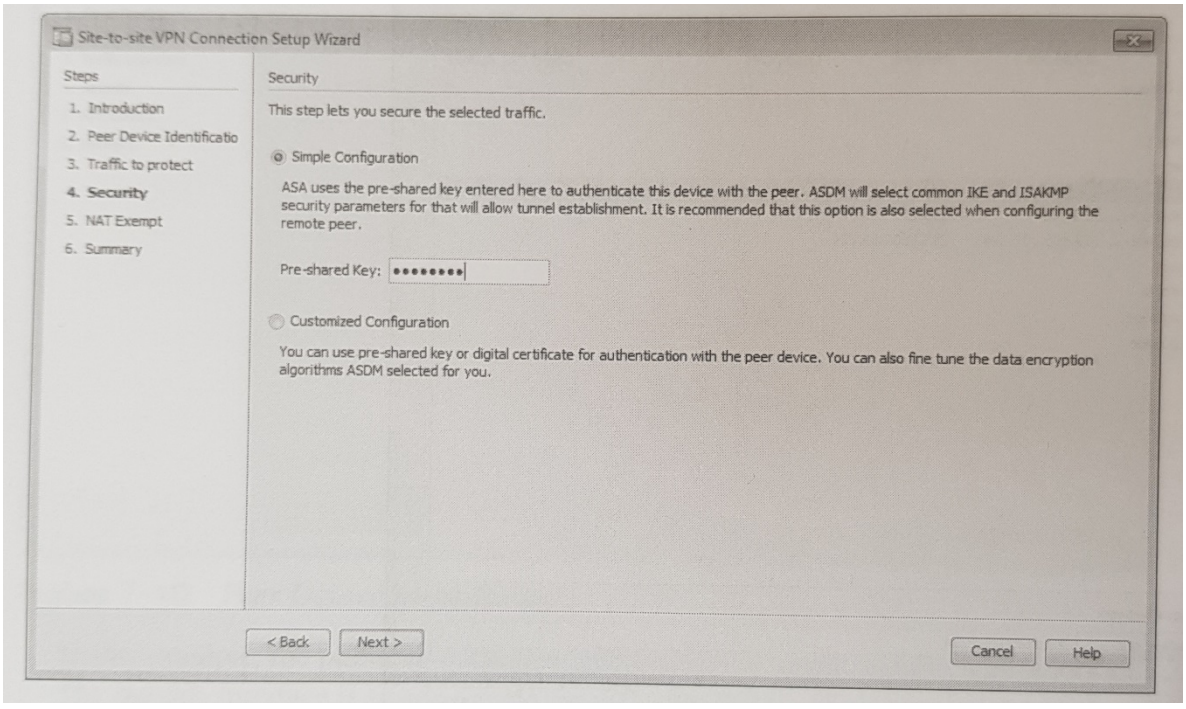
El cisco ASA reconoce todas las redes locales y remotas si sus rutas están dentro de la tabla de enrutamiento. Puede hacer click en el botón para ver la lista de las redes locales, como muestra la figura en este ejemplo. La red dentro es 10.1.1.0/24 seleccionada.



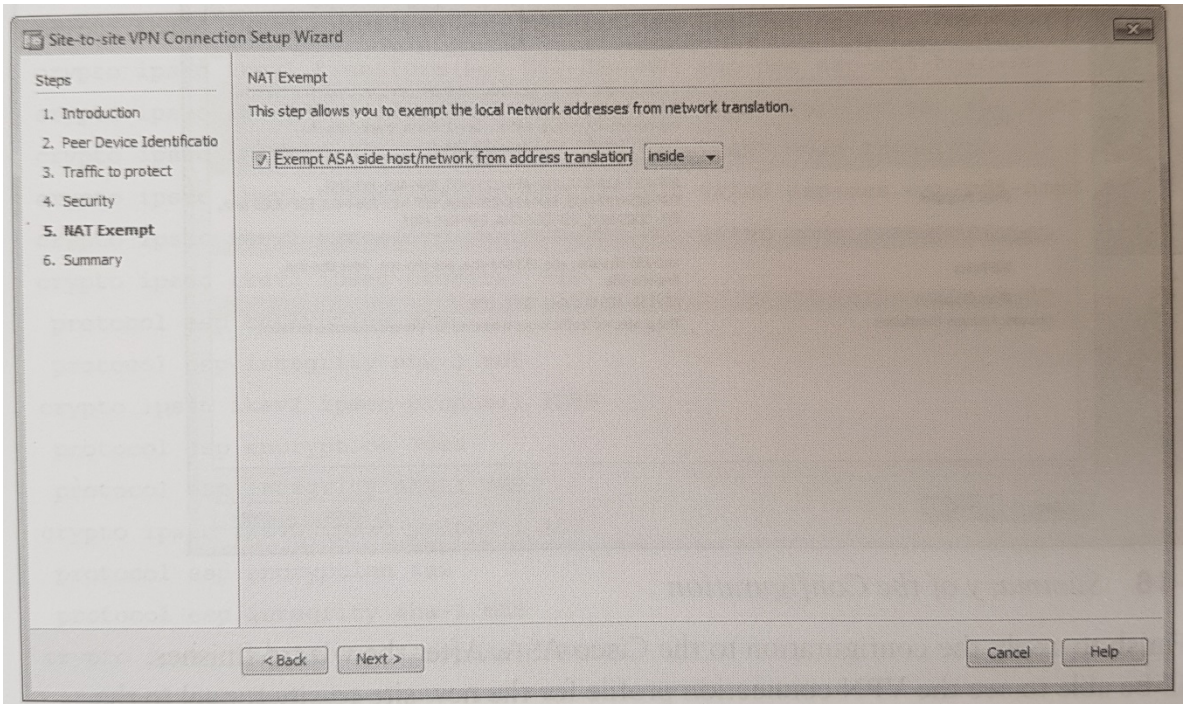
Opcionalmente, usted puede anualmente agregar una dirección en el campo de dirección IP con su apropiada mascara de subred. Para la red local, específicamente 10.1.1.0/24, y para la red remota 172.16.0.0/16 como muestra la figura.



Después de especificar las redes remotas y local. Hacer click en Next. Se mostrara la siguiente pantalla.



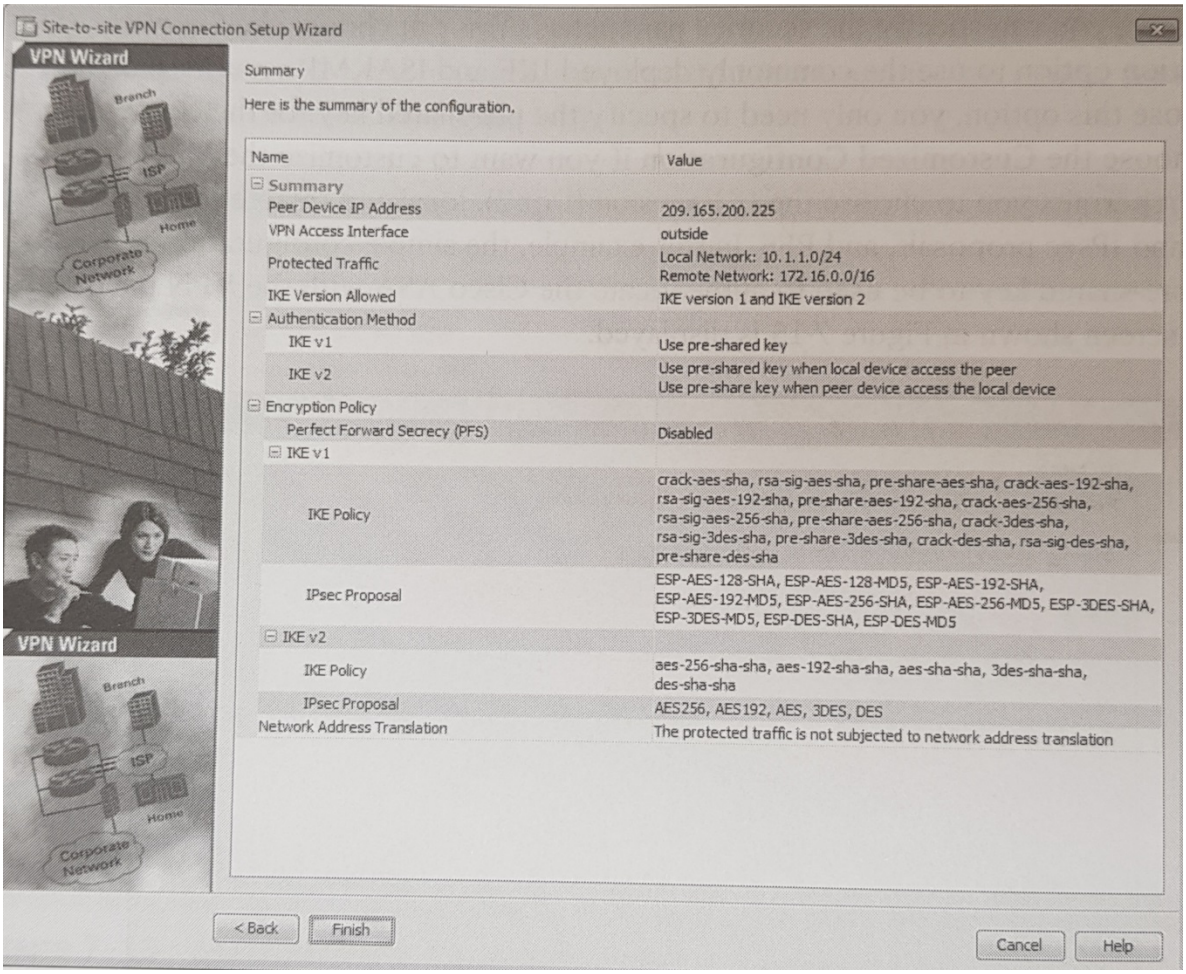
En esta pantalla, usted puede especificar los parámetros de seguridad. Usted puede escoger la configuración simple “simple configuration” opcional para usar comúnmente desplegada en IKE & ISAKMP secure parameters. Si usted elige esta opción, usted solo necesita especificar e pre-shared key para la conexión. Usted puede escoger la configuracionpersonalizada si usted quiere personalizar las políticas de la VPN. ASMD entonces le permite escoger la versión de IKE (versión 1 y 2), local y remote pre-shared keys, propuesta IKE e IPsec y PFS. En este ejemplo, la configuración simple es usada. Ingrese el pre-shared key para ser usado para autenticar el Cisco ASA con la peer VPN. Hacer click en Next. La figura muestra la pantalla desplegada.



Definiendo el NAT ejemplo de política.

La pantalla muestra en la figura anterior seguir para definir el NAT. En muchos casos, usted no quiere traducir las direcciones si el trafico esta viajando en el túnel VPN. ASDM le permite verificar el Exempt ASA Side Host/Network from Address Translation verificar la caja con el Inside interface seleccionada para pasar la traducción de direcciones.

Hacer click en Next para verificar su configuración como resultado la figura mostrada en la pantalla. Esta pantalla lista todo la configuración de parámetros que será enviada al cisco ASA. Desece cuenta que la configuración de Wizard agrego números por defecto opciones para políticas IKEv1 e IKEv2 y propósitos IPsec. Puede personalizar estas opciones selcionando "Customized Configuraction" en el VPN Wizard o para configuraciones de parámetros manuales, como se aprenderá después en esta sección.



Hacer click en Finish para aplicar la configuración al Cisco ASA. Después de finalizar el Wizard, usted seria capaz para ver la coneccion VPN para el nuevo site-to-site a la 209.165.200.225 del peer.

El ejemplo muestra todos los comandos enviados al cisco ASA por el ASDM.

Key Topic

Example 7-11 *Commands Sent to the Cisco ASA by ASDM*

```
! Crypto IPsec (Phase 2) IKEv1 and IKEv2 transform sets.
crypto ipsec ikev1 transform-set ESP-AES-128-SHA esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5 esp-aes esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA esp-aes-192 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5 esp-aes-192 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-SHA esp-aes-256 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-MD5 esp-aes-256 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA-TRANS esp-aes esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-128-MD5-TRANS esp-aes esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-128-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-192-SHA-TRANS esp-aes-192 esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-192-MD5-TRANS esp-aes-192 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-192-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-256-SHA-TRANS esp-aes-256 esp-sha-hmac
```

```
crypto ipsec ikev1 transform-set ESP-AES-256-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-AES-256-MD5-TRANS esp-aes-256 esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-AES-256-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA-TRANS esp-3des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-3DES-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-3DES-MD5-TRANS esp-3des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-3DES-MD5-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-DES-SHA esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5 esp-des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA-TRANS esp-des esp-sha-hmac
crypto ipsec ikev1 transform-set ESP-DES-SHA-TRANS mode transport
crypto ipsec ikev1 transform-set ESP-DES-MD5-TRANS esp-des esp-md5-hmac
crypto ipsec ikev1 transform-set ESP-DES-MD5-TRANS mode transport
crypto ipsec ikev2 ipsec-proposal DES
 protocol esp encryption des
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal 3DES
 protocol esp encryption 3des
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES
 protocol esp encryption aes
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES192
 protocol esp encryption aes-192
 protocol esp integrity sha-1 md5
crypto ipsec ikev2 ipsec-proposal AES256
 protocol esp encryption aes-256
 protocol esp integrity sha-1 md5
!
! ASDM creates an access control list (ACL) named outside_cryptomap used to
! define the local and remote networks.
access-list outside_cryptomap extended permit ip 10.1.1.0 255.255.255.0 172.16.0.0
  255.255.0.0
!The ACL is then applied (matched) the crypto map
crypto map outside_map 1 match address outside_cryptomap
!
!The VPN peer is defined in the crypto map
crypto map outside_map 1 set peer 209.165.200.225
!
! The crypto map is configured with the IKEv1 transform set with several encryption
! algorithms. The highest security algorithm is picked first based on the peers
  proposals.
crypto map outside_map 1 set ikev1 transform-set ESP-AES-128-SHA ESP-AES-128-MD5
  ESP-AES-192-SHA ESP-AES-192-MD5 ESP-AES-256-SHA ESP-AES-256-MD5 ESP-3DES-SHA
```

```
  ESP-3DES-MD5 ESP-DES-SHA ESP-DES-MD5
!
!
! The crypto map is configured with the IKEv2 transform set
crypto map outside_map 1 set ikev2 ipsec-proposal AES256 AES192 AES 3DES DES
!
! the crypto map is applied to the outside interface
crypto map outside_map interface outside
!
!
! ASDM applies numerous default IKEv1 and IKEv2 policies
crypto ikev2 policy 1
 encryption aes-256
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 10
 encryption aes-192
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 20
 encryption aes
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 30
 encryption 3des
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 policy 40
 encryption des
 integrity sha
 group 5 2
 prf sha
 lifetime seconds 86400
crypto ikev2 enable outside
crypto ikev1 enable outside
crypto ikev1 policy 10
 authentication crack
 encryption aes-256
```

```
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 20
 authentication rsa-sig
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 30
 authentication pre-share
 encryption aes-256
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 40
 authentication crack
 encryption aes-192
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 50
 authentication rsa-sig
 encryption aes-192
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 60
 authentication pre-share
 encryption aes-192
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 70
 authentication crack
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 80
 authentication rsa-sig
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 90
```

```
 authentication pre-share
 encryption aes
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 100
 authentication crack
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 110
 authentication rsa-sig
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 120
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 130
 authentication crack
 encryption des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 140
 authentication rsa-sig
 encryption des
 hash sha
 group 2
 lifetime 86400
crypto ikev1 policy 150
 authentication pre-share
 encryption des
 hash sha
 group 2
 lifetime 86400
!
! ASDM creates all the crypto ikev1 policies above by default.
! However, only the one that matches the peer's proposal will be used.
```

```
!
! The group policy for the tunnel is configured. The group policy name is
! GroupPolicy_209.165.200.225.
!
group-policy GroupPolicy_209.165.200.225 internal
group-policy GroupPolicy_209.165.200.225 attributes
 vpn-tunnel-protocol ikev1 ikev2
!
!
! The tunnel group is defined as type ipsec-l2l (which stands for IPsec Lan-to-Lan
! tunnel).
tunnel-group 209.165.200.225 type ipsec-l2l
!
! The group policy is applied to the tunnel group under the tunnel group general
! attributes.
tunnel-group 209.165.200.225 general-attributes
 default-group-policy GroupPolicy_209.165.200.225
!
! The pre-shared key is configured for both IKEv1 and IKEv2 by default.
tunnel-group 209.165.200.225 ipsec-attributes
 ikev1 pre-shared-key *****
 ikev2 remote-authentication pre-shared-key *****
 ikev2 local-authentication pre-shared-key *****
!
! nat is bypassed for the local and remote network communication over the site-to-site
! tunnel
nat (inside,outside) source static NETWORK_OBJ_10.1.1.0_24 NETWORK_OBJ_10.1.1.0_24
  destination static NETWORK_OBJ_172.16.0.0_16 NETWORK_OBJ_172.16.0.0_16 no-proxy-arp
  route-lookup
!
object network NETWORK_OBJ_10.1.1.0_24
 subnet 10.1.1.0 255.255.255.0
object network NETWORK_OBJ_172.16.0.0_16
 subnet 172.16.0.0 255.255.0.0
!
```

Como usted puede ver, ASDM envía numerosas políticas IKEv1 e IKEv2 y transform sets por defecto que pueden hacer la configuración muy complicada. Para evitar esto, puede seleccionar el Customized Configuration en el VPN WIzard o manualmente configurar los parámetros en la pantalla de perfiles de conexión. Como se muestra.

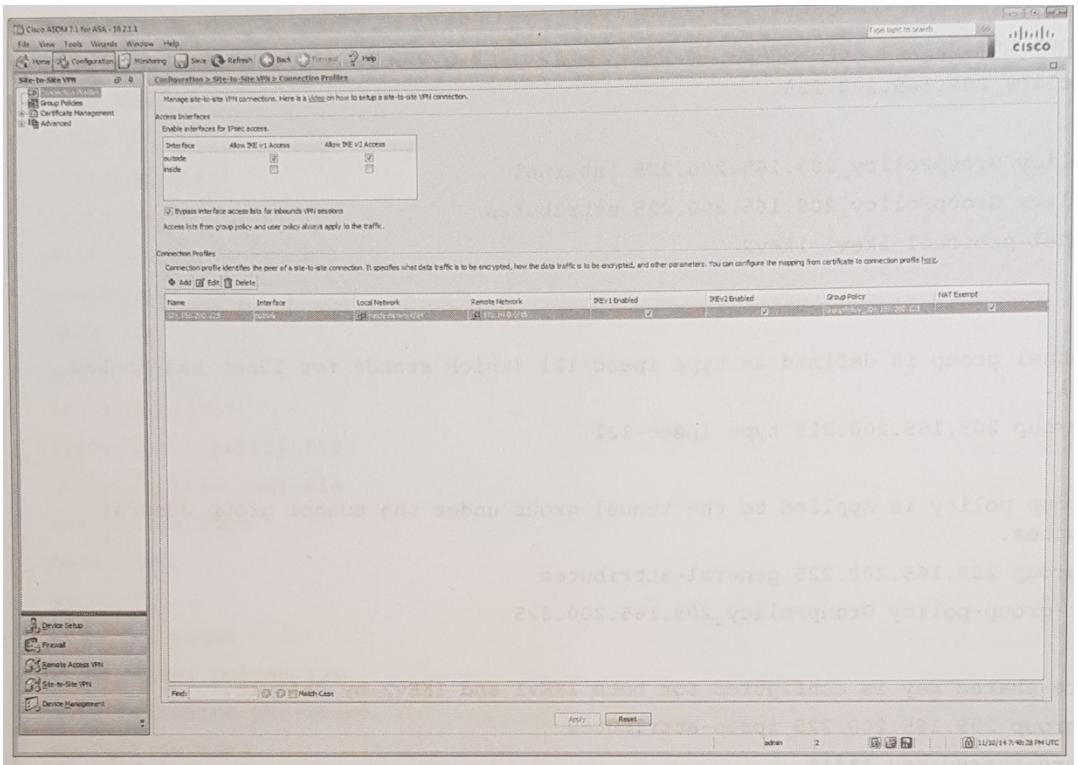
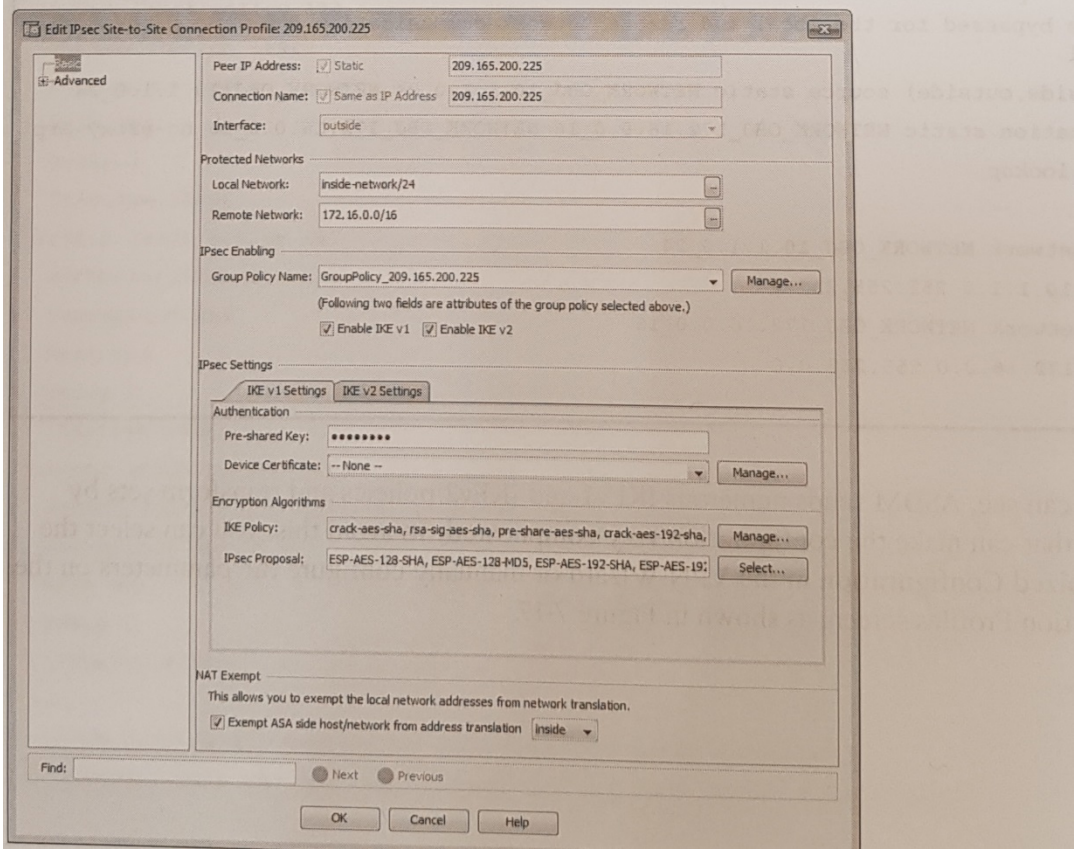


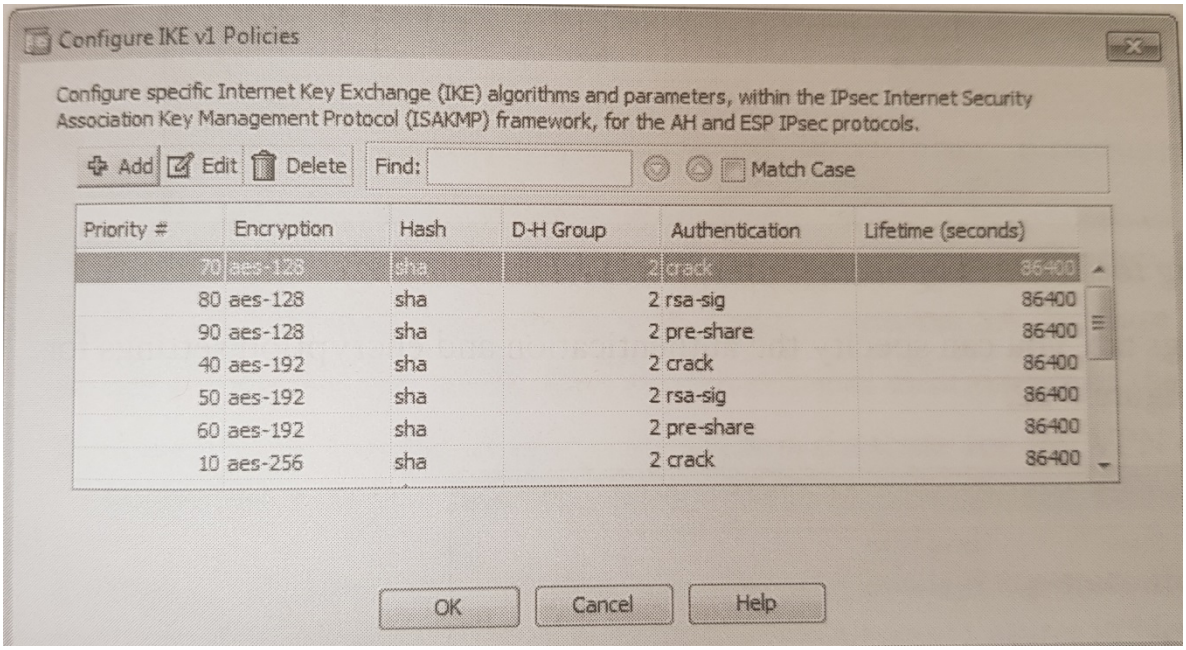
Figure 7-17 *Connection Profiles*

To edit the configuration, click the **Edit** button. The screen in Figure 7-18 is shown.



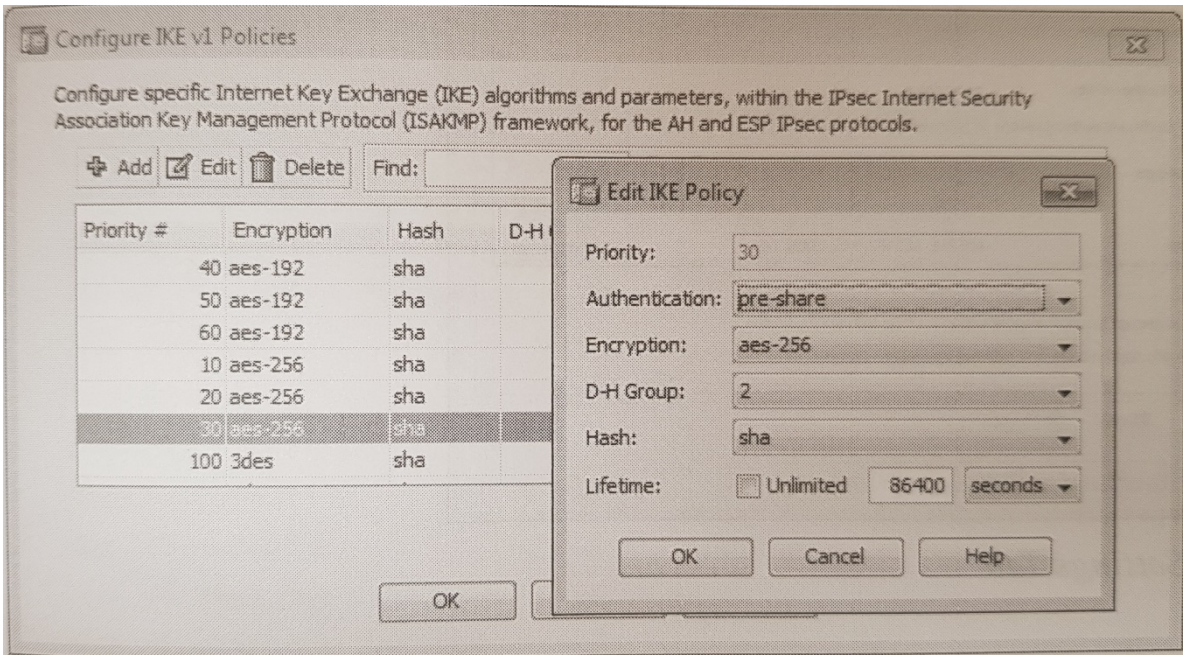
El Edit IPsec Site-oSite conection profile en el box vamos a modificar la conexión IPsec site-to-site. Esta ventana de dialogo le permite especificar la dirección IP del peer, especificando un nombre de política de grupo, seleccionar una interface, especificar IKEv1 & IKEv2 peer y usuario parámetros de autentiaccion, especificar la red protegida, y especificar el algoritmo de cifrado.

Para hacer la configuración mas simple, uede navegar a las configuraciones IPsec, y debajo las tablas de configuraciones IKEv1, puede especificar el algoritmo de cifrado que quiere usar para este tunnel site-to-site, como usted ve, varias políticas de algoritmo de cifrado por defecto IKE e IPsec IKEv1 en la ventana de dialogo, puede hacer click en el botón Manage para abrir la ventana de dialogo de las políticas de configuración IKEv1, mostrado en la figura.

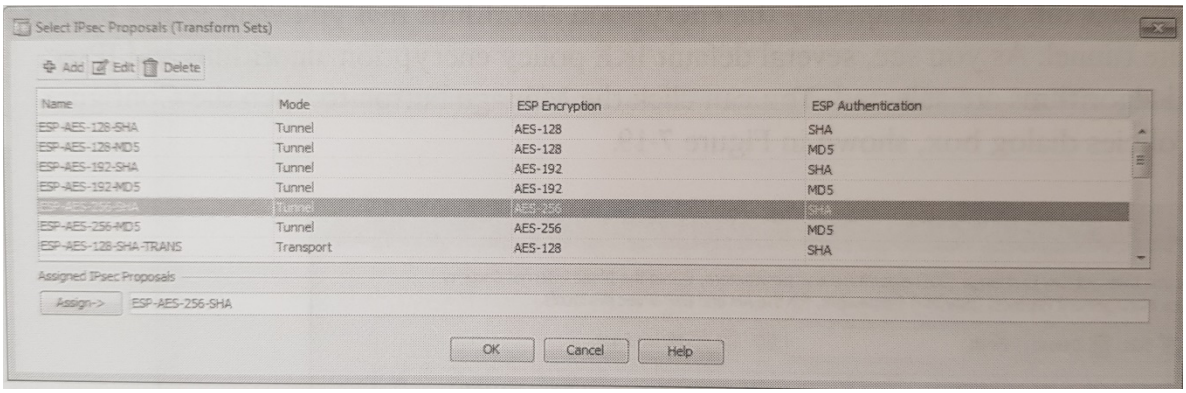


Configuracion Manual de las políticas IKEv1

Esta pantalla permite a usted para agregar manualmente, editar, o eliminar las políticas IKEv1. En este ejemplo, solo queremos tener una sola política IKE para el túnel. La política IKE es configurada con pre-shared key para la autentiaccion, el algoritmo de cifrado es aes 256, Diffie-Hellman Group es configurado para 2, el hashing algorithm es sha, y el lifetime es configurado por defecto 86400 seconds.

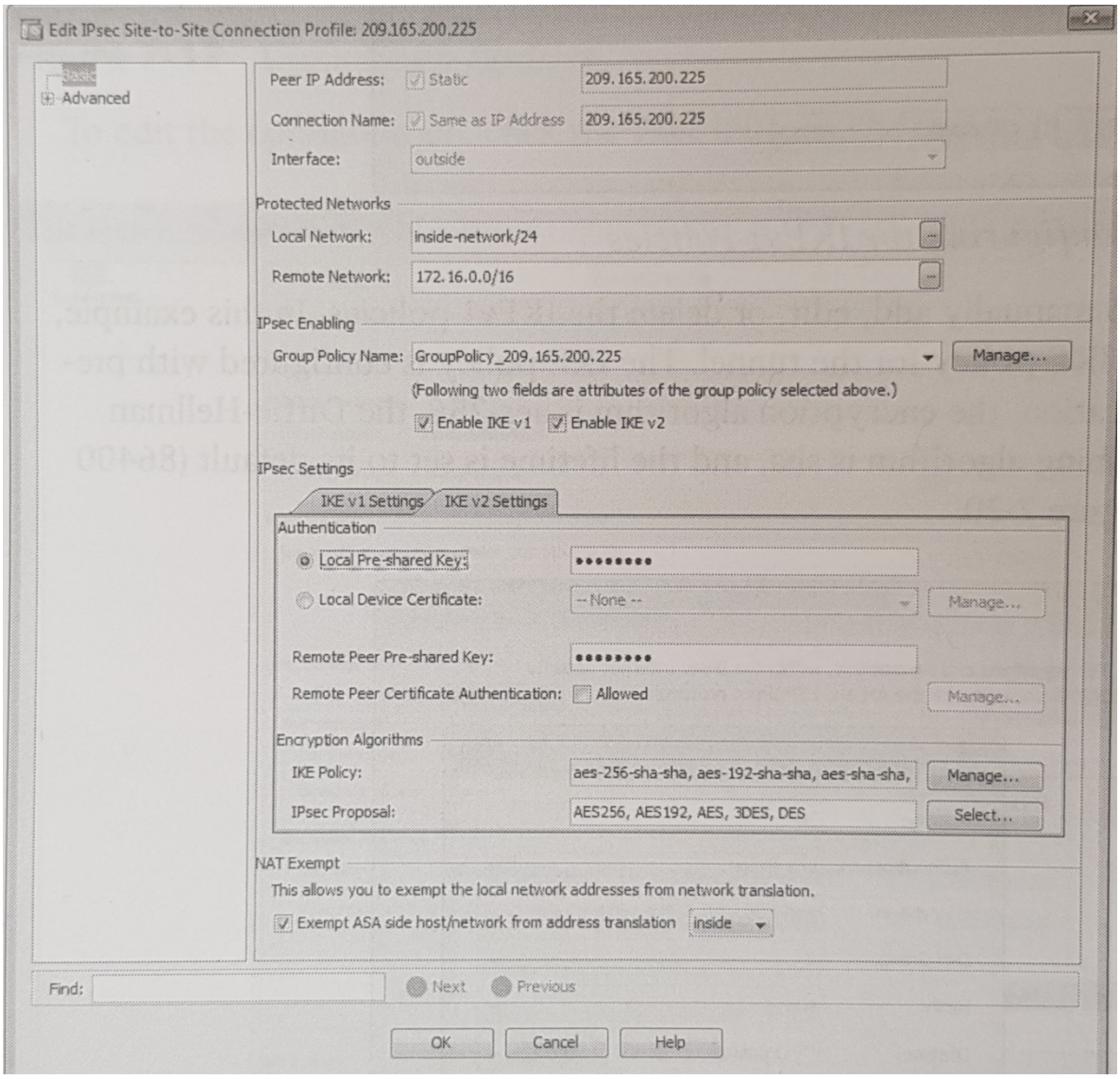


Similarmente, puede editar la propuesta IPsec para especificar una o mas algoritmos de cifrado para usar por IPsec IKEv1 policy. Editar el propósito de IPsec haciendo click en el botón Select. El cudro de dialogo muestra la figura siguiente desplegado. Esta pantalla permite a usted agregar, editar, o eliminar el IPsec (Transform set) para ser usado en el Cisco ASA y para ser asignado al túnel.



Seleccionando IPsec Transform Set

En la tabla de configuraciones IKEv2, puede especificar la authenticacion t configurar el cifrado para IKEv2 como muestra la figura.



Configuracion Tabla IKEv2

TROUBLESHOOTING IPsec Site-to-Site en Cisco ASA

Similar al los dispositivos cisco IOS, el Cisco ASA tiene varios comados show que habilita usted para verificar la configuracion de la informacion de IKE e IPsec. Los siguientes son algunos de los mas usados coamdos “show” para troubleshooting IPsec en Cisco ASA.

- Show crypto isakmp starts: muestra información detallada de ambos IKEv1 e IKEv2 en el CISCO ASA
- Show crypto ikev1 starts: muestra información detallada de IKEv1 en CISCO ASA
- Show crypto ikev2 starts: muestra información detallada de IKEv2 en CISCO ASA
- Show isakmp sa:muestra el runtime ikev1 e ikev2 asociacion de seguridad (SA) de la base de datos
- Show isakmp sa detail: despliega información detallada de los comandos previos.
- Show crypto ipsec sa: despliega el runtime phase 2 SA database
- Show crypto ipsec sa detail: despliega informacion del coamdo previo
- Show vpn-sessiondb: despliega las sesiones de la database para cualquier vpn conection terminal en el Cisco ASA

CAPITULO 9

Securing Layer 2 Tecnologies

Con frecuencia tomar por aceptada la capa 2 en la red por que trabaja sola, ARP en capa 2 trabaja sobre Ethernet con todas las tecnologías probadas que trabajan muy bien. Esta certificación, el CCNA Security, fue construida con la presunción que los candidatos tendrían los conocimientos del CCNA R&S o equivalente. Con estos conocimientos, usted comprendiendo los detalles sobre VLANs, trunking e inter-VLAN routing es presumido, sin embargo, asi que uste absolutamente comprende estos conceptos fundamentales, este capitulo será como un repaso.

Fundamentos de VLAN y TRUNKING

Debe comprender lo básico de como VLANs y TRUNKING operan antes de que pueda aprender a asegurar esasta características. Esta sección repasa como las VLANs y TRUNKING son configurados y como ellos operan.

Topología:

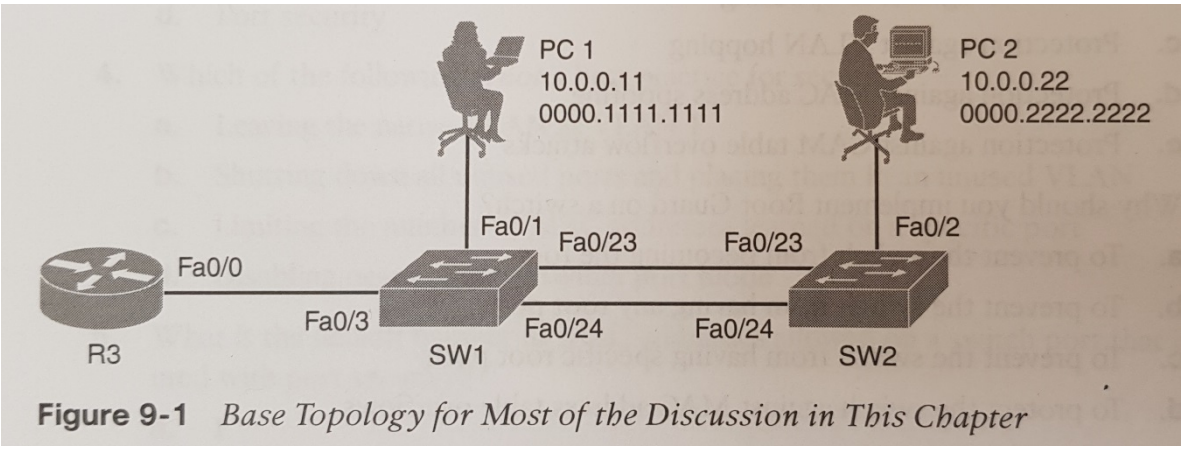


Figure 9-1 *Base Topology for Most of the Discussion in This Chapter*

Que es un Vlan?

Una via para identificar una LAN es decir que todos los dispositivos en esa misma LAN tienen una común dirección IP de la capa 3 en la red y que ellos están todos ubicados en e mismo dominio de broadcast de capa 2. Una VLAN es otro nombre para el dominio de broadcast de capa 2. Las VLAN son controladas por el switch. El switch también controla cuales puertos son asociados con cual VLAN. En la figura anterior esta en sus configuraciones por defecto, todos los puertos por defecto son asiganados a la vlan 1 , y eso significa que todos los dispositivos, incluyendo los dos usuarios y el router, están todos en el mismo dominio de broadcast, o VLAN.

Como usted empieza a agregar cientos de usuarios, usted podría querer separa grupos de usuarios dentro de subredes y asociarlos a grupos de VLANs. Para hacer esto, usted asigna los puertos del switch a la VLAN, y entonces cualquier dispositivo que conecte a un especifico puerto de switch es un miembro de esa VLAN. Ojala todos los dispositivos que conectan a los puertos del switch que están asignados a la VLAN dada también tienen una común dirección IP configurada asi que ellos pueden comunicarse cada uno con el otro dispositivo en la misma VLAN. Con frecuencia, DHCP es usado para asignar direcciones IP de una común subred para los dispositivos dados de la VLAN.

Si quiere mover los dos usuarios en la figura anterior a una nueva VLAN , debe crear la VLAN en el los switches, y entonces asignar el puerto de acceso a esa nueva VLAN.

(generar una vlan 10 en un switch y agregar el “sh vlan brief”)

(agregar “sh vlan id num_VLAN)

TRUNKING con 802.1q

Un problema con tener 2 usuarios en la misma VLAN pero no en el mismo switch es como SW1 le dice a SW2 que las tramas de broadcast o unicast es supuesta para ser de la VLAN 10.

La respuesta es simple. Para conectar entre 2 switches que contienen puertos en la VLAN que existen en ambos switch, se configura un puerto especifico troncal en lugar de configura puertos de acceso. Si los dos puertos de switch son configurados como troncales, ellos incluyen información adicional llamada tag que identifica cada tramade VLAN a la cual pertenece. 802.1q es el standard para este tagging o etiquetado. La pieza mas critica de información (para esta discucuion) en esta etiqueta “tag” es el VLAN ID.

Actualmente, los dos usuarios no pueden comunicarse por que ellos están en la misma VLAN, pero el enlace entre switch no esta configurado como troncal. Para configurar ambos conjuntos de interfaces como troncal, debería especificar el método de troncal 802.1q y entonces levantar esa característica, como se muestra.

(configuar los enlaces como troncales de la topología agregar el screen del show int trunk y show interface x switchport).

SIGUIENDO LA TRAMA PASO A PASO

Una trama de broadcast enviada por PC1 y recibida por SW1 enviaria la trama sobre el troncal etiquetado como perteneciente a la VLAN 10 hacia el SW2. SW2 veria la etiqueta, la conoce, fue un broadcast asociado a la VLAN 10, remueve la etiqueta, y envía el broadcast a todos los puertos con interfaces asocidas con la VLAN 10, incluyendo el puerto de switch que conecta a PC2, esos 2 componentes (puertos asignados a la VLAN, y puertos troncales que etiquetan el trafico, asi que un switch recibiendo el trafico conocido de cual VLAN pertenece la trama) son el nucleo construyendo bloques de capa 2, es allí donde una vlan puede extenderse mas alla de un solo switch.

LA NATIVE VLAN en un TRONCAL

De la saida del ejemplo anterior (show interface fa0/1 switchport), verificamos nuestra interface troncal entre 2 switches. Una opción mostrada en la salida fue una native VLAN. Por defecto, vlan nativa es la VLAN 1. Asi que, que significa esto, y por que nos preocupa? Si un usuario es conecatdo a un puerto de acceso que se le asigno la VLAN 1 en el SW1, y ese usuario envía una trama de broadcast, cuando SW1 envie ese Broadcast a SW2, llegara a ser esa trama perteneciente a l VLAN nativa (y ambos switch están deacuerdo en usar la VLAN native), el 802.1q etiquetando es simplemente excluido. Esto trabaja por que cuando el switch recibe una trama en un puerto troncal, si esa trama esta perdida el 802.1q etiqueta completamente, le switch recibiendo asume que l atrama pertenece a la vlan nativa (en este caso la VLAN 1).

Esto no es un gran problema hasta que alguien intenta tomar ventaja de esto, como se discutirá mas tarde en el capitulo, mientras, solo conocemos que usar una especifica VLAN como nativa VLAN (diferente de la vlan 1 por defecto) y nunca usar una misma vlan para trafico de usuarios es una prudente idea.

Asi que, que quiere usted hacer? (Pregunta el puerto)

Los trocales pueden ser automáticamente negociados entre los switches, o entre un switch y un dispositivo que pueda soportar trunking. Negociación automática para determinar si un puerto será un puerto de acceso o un troncal es un riego por que un atacante podría negociar potencialmente un troncal con un switch, entonces un atacante podría accesar directamente a cualquier VLAN disponible simplemente para ilegalmente etiquetar el tráfico directamente de su PC.

Inter VLAN Routing

Nuestros dos usuarios PC1 y PC2 comunican uno con el otro, y ellos pueden comunicarse con otros dispositivos en la misma VLAN (la cual esta también la misma subred IP), pero ellos no pueden comunicarse con dispositivos fuera de su vlan local sin la asistencia de un defaul Gateway. Un router puede ser imlementado con dos interfaces físicas, una conectada a un puerto de acceso en el switch que ha sido asiganada a la VLAN 10, y otra interface conectada a un diferente puerto que ha sido configurado para una diferente VLAN. Con dos interface físicas y direrecciones IP diferentes en cada una, el router podría ejecutar enrtamiento entre las dos VLANs.

El desafio de usar solo interfaces físicas

Asi que aquí esta el problema: Que si usted tiene 50 VLANs? Programando 50 interfaces físicas para el router seria caro, solo el hecho que usted este usando 50 interfaces físicas en el switch. Una solucion es el uso de una tecnoca lla,ada router-on-a-stick.

Usando “Sub” Interfaces Virtuales

Para usar una interface física, vamos a jugar un juego, vamos a decirle al switch que vamos a hacer un troncal fuera a hacia el router, el cual desde la perspectiva del switch busca exactamente como troncal a otro switch. Y en el router, vamos a decirle al router poner atención en 802.1q tags, y asignando tramas de especificas VLANs, basado en las etiquetas “tags”, para las sub interfaces lógicas. En cada sub interface hay una diferente subred, como se muestra en el ejemplo

(Agregar la configuración de las configuraciones de las sub interfaces y el switch como troncales pag 240).

SPANNING-TREE FUNDAMENTOS

Esta sección discute lo básico de como STP puede evitar loops de capa 2 del modelo OSI. Esto es importante por comprender, como trabajarlo asi que puede comprenderlo completamente corrigiento la técnica de mitigación.

LOOPS en la red usualmente malos.

Sin STP, cuando tenemos enlaces paralelos entre dispositivos de capa 2, tales como la conexión entre SW1 Y SW2, deberíamos tener loops de capa 2. Déjeme tomar una mirada como lo usa la red configurada en la sección previa. STP esta operando por defecto en los demas switches cisc, pero para el propósito de esta discusión, asume que STP no esta corriendo, al menos por ahora.

LA vida de un loop

Si PC1 envia una solicitud ARP dentro de la red. SW1 lo recibe y conoce que esta trama pertenece a la VLAN 10 por que el puerto acceso entro y lo envio fuera a todos los puertos que estos tienen asiganada la VLAN 10, en adicion para cualquier puerto troncal que este permitiendo la VLAN 10. Por defecto, los puertos troncales permiten todas las VLAN. Este broadcast es etiquetado como perteneciente a la VLAN 10, y es enviado abajo por los puertos 23 y 24.

Solo por un momento, vamos siguiendo uno de aquellos puertos. El trafico esta siendo enviado abajao por el puerto 23, y SW2 lo ve y decide necesitar para enviarlo fuera a todos los puertos que están asignados a la VLAN 10, la cual incluye el purto 2 , el cual esta asiganado como puerto e acceso para la VLAN 10, y también el puerto troncal 24. Asi que, ahora SW2 envia el mismo broadcast a SW1 en el puerto 24. SW1 repite el proceso y lo envía fuera del puerto 23, y allí será el loop. El loop sucede en la otra dirección, también. Además teniendo un loop, ambos switch llegan a confundirse sobre cual puerto es asociado con la dirección MAC de la PC1. Por que la trama del loop es visto entrando en ambos puertos 23 y 24, por que el loop va en ambas direcciones, la dirección MAC caen y se levantan esto ocurre en la tabla de direcciones MAC dinámicas aprendidasdel switch. No solo hace esto dirigiendo a execivos e inesesarios envios de solicitudes ARP para los puertos del switch, eso tambia podría presentar una condición DoSsi el switch esta sin poder ejecutar todas sus funciones por los recursos desperdiciados por este loop en la red.

La solucion al LOOP de capa 2

STP, o 802.1D, fue desarrollado para identificar rutas paralelas de capa 2 y bloquear uno de los enlaces redundantes asi que que un loop de capa 2 no ocurrirá. Un solo switch con el mas bajo bridge ID llegara a ser el root bridge, y entonces todos los demás switches noroots determinan si ellos tienen enlaces paralelos al root y bloquean dentro todos pero dejando una ruata. STP se comunica usando bridge protocol data unit (BPDU), y que es ahora quien negocia la detección de loops.

(show spanning-tree vlan 10 en sw1)

(show spanning-tree vlan 10 en sw 2)

STP esta encencdido por defeto, y tendra una instancia separada para cada VLAN. Asi que, si usted tiene 5 VLANs, usted tiene 5 instancias de STP. Cisco llama esta implementación por defecto Per-Vlan Spanning Tree Plus (PVST+).

STP consiste en lo siguiente.

- Root Port: el puerto de switch mas cerca al root bridge en términos de costo de ruta de STP es considerado el root port.
- Designated: el puerto de switch que puede enviar la mejor BPDU para una particular VLAN en un switch es considerado como puerto desigated.
- Nodesignated: hay puertos de switch que no envían paquetes , asi como impiden la existencia de loops dentro de la red.

STP es cauteloso de nuevos puertos.

Cuando una interface se va arriba y recibe un enlace con señal de un dispositivo conectado, tal como una PC o un router, STP es cauteloso antes de permitir tramas en la interface, si outro shitch es adjuntado, hay posibles loops. STP cautelosamente espera 30 segundos (por defecto) en un puerto recientemente up antes de permitir tramas atraves de esa interface; 15 segundos de esos permanece en estado de escucha (listening state), donde STP esta viendo si cualquiera BPDU esta intrando. Durante este tiempo no graba direcciones MAC en su tabla dinámica, la segunda mitad de los 30 segundos, esta todavía buscando por BPDUs, pero STP también empieza a poblar la tabla de direcciones MAC con las direcciones MAC fuente que ve en las tramas, esto es llamado estado de aprendizaje (learning state). Después de escuchar y aprender ha completado los 30 segundos, el switch puede empezar a enviar tramas. Si un puerto esta en estado de bloqueo como al principio, un adicional de 20 segundos de retardo podrían ocurrir como el puerto lo determine que la ruta paralela se ha ido, antes de mover a escucha y aprendizaje.

Para la mayoría de administradores y usuarios, este retardo es largo.

Mejorando el tiempo de envio.

Cisco tiene alguna mejora propiedad de cisco para el 802.1d (STP) que permite convergencia mas rápida en el caso de eventos de una cambio de topología e incluye muchos características tales como PortFast, UplinkFast y BackBoneFast. Muchas de esas características fueron usadas en una nueva versión de STP llamada Rapid Spanning Tree (tambie conocida como 802.1w). habilitando PortFast para tradicionales STP y configurando Rapid Spanning Tree globalmente

Amenazas comunes de capa 2 y como mitigarlas

Esta sección discute muchas amenazas que se concentran en tecnologías de caoa 2, esto es relevante para la porción de “seguridad” del CCNA security.

Cada cosa en lo mas alto de la capa 3 es encapsulado dentro de algún tipo de trama de capa 2 , si el atacante puede interrumpir, copiar, redireccionar, o confundir los datos enviándose en capa 2, el mismo atacnte puede también interrumpir cualquier tipo de protocolo superior que este siendo usado.

MEJORES PRACTICAS DE LA CAPA 2

Vamos a iniciar con las mejores practicas para asegurar sus switches y entonces discutimos con mas detalle las mejores practicas para mitigar tipos de ataques.

- Selecione una VLAN sin usar (otra que la VLAN 1) y use esa para la VLAN nativa para todos los troncales. No usar esta VLAN nativa para cualquiera de sus puertos de acceso habilitados.
- Configurarar administrativamentepuertos como puertos de acceso asi los usuarios no podrán negociar un troncaly deshabilitar la negociación del troncal (no dynamic truncking Protocol {DTP}).
- Limitar el numero de direcciones MAC aprendidas en un puerto dado con port security.
- Control STP para detener usuarios o dispositivos desconocidos para manipular STP, puede hacerlo asi con BPDU Guard y Root Guard.
- Apagar CDP en puertos que no sean de confianza o desconocidos que no requieren CDP.
- En un nuevo switch, apagar todos los puertos y asignarlos a una VLAN que no es usada para cualquier cosa.

(configuración de mode Access, acc vlan x, sw nonegotiation)

(interf x, sw trunk encap dot1q, sw mode trunk, sw trunk nat vlan x, sw nonegotiate)

NO Permitir la Negociacion.

En el ejeplo anterior impide a un usuario para negociar un troncal con el switch, maliciosamente, y entonces acceso total a cada una de las vlans para usar software de cliente en la computadora que pueda ambombos enviar y recibir dot1q tramas etiquetadas. Un usuario con un troncal establecido podría ejecutar “VLAN hopping” para cualquier VLAN, otro truco malicioso podría ser hecho, también, forzando al puerto a un puerto de acceso con no negociación remueve el riesgo.

Layer 2 Security Toolkit

ara proteger la capa 2, incluyendo estas decritas en la siguiente tabla.

Cisco tiene muchas herramientas

TOOL	DESCRIPTION
Port Security	Limita el numero de direcciones MAC para ser aprendidas dentro de un puerto de acceso.
BPDU Guard	Si BPDU se muestra activo, donde ellos no deberían, el switch se protege a si mismo.
Root Guard	Controla que puertos no pueden llegar a ser puertos root a root switches remotos.
Dynamic ARP inspection	Previene spoofing de capa 2 informacion para host.
IP Source Guard	Previene spoofing de capa 3 informacion para host
802.1x	Authetica usaurios antes de permitir sus tramas de datos dentro de la red.
DHCP snooping	Previene servidores DHCP engañosos para impactar la red.
Storm Control	Limita la cantidad de broadcast o milticast trafico fluyendo a través de switches
ACL	ACL para reforzar políticas.

La clave de seguridad en tecnología de capa 2 se concentra en el CCNA Security incluyendo port security, BPDU Guard, Root Guard, DHCP snooping, y ACL. Las otras claves de la tabla usted puede guardarlas para el CCNP Security.

ESPECIFICA MITIGACION DE CAPA 2 para CCNA SECURITY

Cuando uno reviza las tecnologías de switching y como ellas operan ahora en mi mente, voy a tomar una especifica mirada de como implementar características de seguridad nuestros switches.

BPDU Guard

Cuando usted habilita BPDU Guard, un puerto de switch que fue enviado un alto y deshabilitado el puerto si un BPDU es visto en el puerto un usuario jamas seria generador de legitimas BPDUs. Esta configuración, aplicad a puertos que debería solo ser puertos de acceso para estaciones terminales, ayudar a impedir otro switch para ser conectado a la red. Esta nube impide manipulación de su actual topología STP. El ejemplo muestra como implementar BPDU Guard

SW2(config-if)#interface fa0/2

SW2(config-if)#spanning-tree bpduguard enable

SW2((config-if)#end

SW2#show interface fa0/2 staus

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/2		connected	10	a-full	a-100	10/100BaseTX

Un Puerto que ha sido deshabilitado por que de una violacion muestra un status de err-disable. Para traer de vuelta la interface arriba, emitir un shutdown y un no shutdown en el modo de configuración de la interface.

También se puede configurar el switch automáticamente para traer una interface fuera de err-disable state, basado en la razón que fue ubicada y cuanto tiempo ha pasado antes de traerla de vuelta arriba. Para habilitar esto por una característica especifica, siga el ejemplo.

SW2(config)#errdisable recovery cause bpduguard

!err-disabled ports se recuperara despues de 30 segundos de un bpdu violation

SW2(config)#errdisable recovery interval 30

!usted puede ver el timeout para la recuperación

SW2#show errdisable recovery

ErrDisable Reason	Timer Status
Arp-inspection	Disable
Bpduguaerd	enable

<snip>

Timer interval: 30 seconds

Interface that will ve enabled at the next timeout:

SW2#

ROOT Guard

Su switch podria ser conectado a otro switches que usted no administra. Si usted quiere impedir a su switch local de aprender sobre un nuevo root switch atraves de uno de sus puertos locales, usted puede configurar Root Guard en un poerto, como muestra el ejemplo, esto también ayudara en prevenir moderando su topología STP.

```
SW1(config)#interface fa0/24
SW1(config-if)#spanning-tree guard root
%SPANTREE-2-ROOTGUARD_CONFIG_CHANGE: Root guard enable on port
FastEthernet0/24.
```

PORT SECURITY (YA FUE VISTO EN CCNA R&S)

CDP y LLDP

Cisco introduce el CDP en 1994 para proveer un mecanismo del sistema de administración para automaticamnete aprender sobre dispositivos conectados a la red. CDP corre en dispositivos cisco (routers, switches, phones, etc) y es también licenciado para correr en algunos dispositivos de red para otros vendors. Usando CDP, dispositivos de red periódicamente anuncian su propia información a una direcciones multicas en la red, haciéndolo disponible para cualquier dispositivo o aplicación que desee para enlistar o recolectarlo.

Al paso del tiempo, mejoras han sido hechas para protocolos descubridores para proveer mejor disponibilidad. Aplicaciones (tales como la voz) han llegado a ser dependientes en estas disponiblidad para operar apropiadamente, aprendiendo para interoperar entre vendors. Por lo tanto para permitir interoperar entre vendors, ha llegado a ser necesario tener un solo protocolo descubridor estandarizado. Cisco ha estado trabajando con otros lideres en la internet e IEEE community para desarrollar uno nuevo protocolo de descubrimento estandarizado, 802.1AB (station and media Access Control Community Discovery, o Link Layer Discovery Protocol {LLDP}).

LLDP el cual define disponibilidad de descubrimiento básico, fue mejorado para direcciones específicamente de aplicaciones de voz; esta extensión para LLDP es llamada LLDP-MED o LLDP (for Media Endpoint Devices).

Como mencionamos previamente, una mejor paractica recomendada es deshabilitar CDP en cualquier puerto a redes desconocidas que no requieran CDP. CDP opera en la capa 2 y puede proveer a los atacantes con información (por ejemplo, tipos de dispositivos, hardware y software,VLAN eIP address, etc) que usted mas bien no revela, el ejemplo detalla los pasos de la configuración necesaria para deshabilitar CDP en el modo global o por interface.

¡Disable CDP en la interface fa0/24

```
SW2(config)#int fa0/24
SW2(config-if)#no cdp enable
SW2config-if)#exit
!deshabilitando CDP en modo global!
SW2(config)#no cdp run
SW2(config)#exit
```

!Verificando CDP este deshabilitado

```
SW2#shpw cdp
%CDP is not enable
```

!confirmando LLDP este habilitado en el Switch

```
SW2#show lldp

Global LLDP information:
    Status:      ACTIVE
    LLDP advertised are sent every 30 seconds
    LLDP hold time advertised is 120 seconds
    LLDP interface reinitialisation delay is 2 seconds

SW2#
```

!Deshabilitando LLDP en forma global!

```
SW2#conf t
SW2(config)#no lldp run
SW2(config)#exit
SW2#show lldp
%LLDP is not enable
SW2#
```

DHCP Snooping

DHCP snooping es una caracteristica de seguridad que actua como un firewall entre un un host no confiable y un server DHCP de confianza. El DHCP snooping ejecuta las siguientes caractristicas:

- Vlida mensajes recibidos DHCP de fuentes no confiables y filtra los mensajes fuente.
- Límites de velocidad del tráfico de DHCP de fuentes confiables y no confiables
- Contruye y mantiene la base de datos de enlace de indagación DHCP, que contiene información sobre un host no confiable con la menos la dirección IP.
- Utilizar la base de datos DHCP snooping para validar la solicitud posterior desde un host no confiable.

Otra característica de seguridad, tal como Dynamic ARP inspection (DAI), el cual es descrito en la siguiente sección, también usa información almacenada en el DHCP snooping con la base de datos.

DHCP snooping es habilitado por VLAN, la característica esta deshabilitada en todas las VLANs. Usted puede habilitar la característica en una sola VLAN o en un rango de VLANs.

El ataque de indagación DHCP tiene lugar cuando los dispositivos intentan a propósito generar suficiente solicitud DHCP para agotar el número de direcciones IP asignadas al grupo DHCP

Las características de DHCO snooping determinan si el trafico de origen es confiable o no. Una fuente no confiable puede iniciar ataque de trafico u otras acciones ostiles. Para impedir tales ataques, la característica DHCP snooping filtra mensajes y velocidad de trafico de fuentes no confiables.

Los siguientes pasos son requeridos para implementar DHCP snooping en su red:

PASO 1. Definir y configurar el server DHCP.

PASO 2. Habilitar DHCP snooping en almenos una VLAN. Por defecto, DHCP snooping esta inactivo en todas las VLANs.

PASO 3. Asegurarse que DHCP server este conectado a travez de una interface confiable. Por defecto, el estado de confianza de todas las interfaces es de no confianza.

PASO 4. configure el agente de base de datos de indagación DHCP; este paso garantiza que las entradas de la base de datos se restauren después de un reinicio o cambioHabilitar DHCP snooping globalmente.

PASO 5. Habilite DHCP snooping globalmente.

El DHCP snooping no esta activo hasta usted completar estos pasos.

¡habilitando DHCP Snooping Globalmente.

SW2(config)#ip dhcp snooping

¡habilitando DHCP Snooping en la vlan 10

SW2(config)#ip dhcp snooping vlan 10

!configurando la interface fa0/24 como una interface confinable!

SW2(config)#interface fa0/24
SW2(config-if)#ip dhcp trust

!configurar el DHCP Snooping database agent para almacenar la libreta en una ubicación dada.

SW2(config)#ip dhcp snooping database tftp://10.1.1.1/directory/file
SW2(config)#exit
SW2#

!verificando la configuracion DHCP Snooping!

SW2#sh ip dhcp snooping

Switch DHCP snooping is enable
DHCP snooping is configurated on following VLANs.
10
DHCP snooping is operational on following VLANs.
None
DHCP snooping is configurated on the following L3 Interfaces:

Insertion of option 82 is enable

Circuit-id default format: vlan-mod-port
Remote-id: 000f.90df.3400 (MAC)
Option 82 on untrusted port is not allowed
Verification of hwaddr field is enable
Verification of giaddr field is enable
DHCP snooping trust/rate is configurated on the following interface

Interface	Trusted	Allow option	Rate limit (pps)
FastEthernet 0/24	yes	yes	unlimited
Custom circuit-ids:			

Dynamic ARP Inspection

ARP prove comunicacion IP dentro de capa 2 en el dominio de broadcast para mapear una direccion IP a una direccion MAC. Por ejmplo, host B quiere envía información a host A pero no tiene la dirección MAC de host A en su ARP cache. Host B genera un mensaje de broadcast para todos los host dentro del dominio de broadcas para obtener la dirección MAC asociada con la dirección IP de host A. todos los host dentro del dominio de broadcast reciben la solicitud ARP, y host A responde con su dirección MAC.

Ataques de falcificacion ARP y envenenamiento ARP cache pueden ocurrir por que ARP permite una respuesta gratuita de un host incluso si una solicitud ARP no fue recibido, después el ataque, todo trafico de un dispositivo bajo el flujo del ataque atraves de la computadora del atacante y entonces al router, switch o host.

Un ataque de falcificacion ARP puede etiquetar host , switches y routers conectados a su red de capa 2 por envenamiento de de ARP cache del sistema conectado a la subred y para interceptar trafico generado por otros host en la misma subred, el ejemplo muestra envenenamineto de ARP cache.

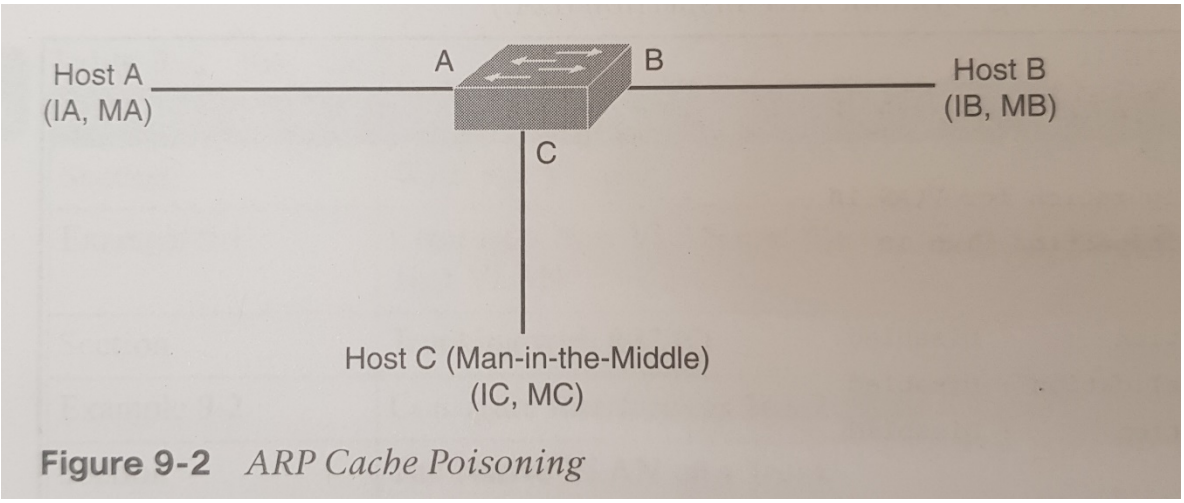


Figure 9-2 *ARP Cache Poisoning*

Host A, B y C están conectados a el mismo switch en interfaces A, B y C todos en la misma subred. Su IP y MAC son mostradas en paréntesis; por ejemplo, host A usa la dirección IP (IA) y MAC (MA). Cunado host A necesita comunicar a host B en la capa 3, unas solicitud ARP broadcast para la dirección asociada MAC con la dirección IP IB. Cuando el switch y el host B reciben la solicitud ARP, ellos difunden su ARP cahe con un ARP binding para un host con la dirección IP IA y una dirección MAC; por ejemplo, una dirección IA esta unido la la dirección MAC MA, cuando host B responde , el switch y el host A divulgan su ARP cache con una entrega para un host co la dirección IP IB y una dirección MAC MB.

Host C puede envenenar el ARP cache del switch para host A, y host B por broadcasting olvido respustas ARP con entregar para un host con una dirección IP IA o IB y dirección MAC de MC. Host con cahe ARP envenenado, usan la dirección MC como el destino MAC para intentar trafico para

IA o IB. Esto significa que host C intercepta ese trafico. Por que host C conoce la verdadera dirección MAC asociada con IA e IB, puede enviar el trafico intercepatado a aquellos host para usar la correcta dirección MAC como el destino. Host C ha insertado el mismo dentro elflujo de trafico desde host A a host B, la cual es la topología clásica de man-in-the-middle attack.

DAI es uan característica de seguridad que valida los paquetes ARP en la red, DAI intercepta, logs, y descarta paquetes ARP con invalid IP-to-MAC addresss entregadas. Esta capacidad protege la red de algunos man-in-the- middle attacks.

DAI determina la validez de un paquete ARP basado en una valida IP-to-MAC entregada y almacenada en una base de datos confiable, el DHCP nooping binding database, como se describió en la sección previa, esta base es construida por DHCP snooping si DHCP snooping esta habilitado en la VLAN y en el switch. Si le paquete ARP es recibido en una interface confiable, el switch envía los paquetes sin ninguna verificación. Una interface no confiable, el switch el switch envía los paquetes solo si es valida.

Usted puede configurar DAI para dejar caer paquetes ARP con la dirección IP en el paquete es invalida o cuando la dirección MAC en el cuerpo del paqute ARP no coincide la dirección especifica en el encabezado Ethetrnet.

Ejemplo, prove la configuración detallada necesaria para implementar DAI para mitigar los efectos de ARP spoofing attacks.

KEY TOPIC ELEMET	DESCRIPTION
Seccion	Que es una VLAN
Ejemplo	Creando una nueva VLAN y ubicar los puertos del SWITCH dentro de esa VLAN
seccion	Trunking con 802.1Q
Ejemplo	Configurar interfaces como puerto troncal
Seccion	La VLAN nativa en un troncal
Seccion	Inter-VLAN Routing
Ejemplo	Configurar Router-on-a-stick y switch support for the router
Ejemplo	Configurar PortFast, Rapid Spanning Tree
List	Mejores practicas de capa 2
Ejemplo	Administrativamente llevar abajo los puertos del switch
Tabla	Toolkit para la seguridad de capa 2
Sección	BPDU Guard
Sección	Root Guard
TEXT	PORT SECURITY
Ejemplo	Implementando Port Security
Sección	CDP y LLDP
Ejemplo	Deshabilitando CDP
Sección	DHCP Snooping
Ejemplo	Configurando DHCP snooping
Sección	Dynamic ARP Inspection
Ejemplo	Configurando DAI

Comando	Descripcion
Switchport mode Access	Asigna un puertò de switch como puerto de acceso
Switchport Access vlan 10	Asocia el dispositivo con una VLAN especifica
Show interface fa0/1 switchport	Verifica la configuración actual y estatus de operación de un puerto de switch
Switchport trunk encapsulation dot1q	Especifica que la encapsilacion del troncal para ser usada, si se hace troncal
Switchport mode trunk	Especifica que este puerto será troncal
Switchport trunk native vlan X	Especifica la vlan native sera X, si el Puerto esta actuando como un Puerto truncal
Switchport nonegotiation	Deshabilita la negociación entre entre el switch y el dispositivo conectado al dispositivo relacionado con el troncal

Spanning-tree bpduguard enable	Protege el puerto del switch contra ser conectado en este puerto otro dispositivo que este generando cualquier tipo de bpdu.
Spanning-tree guard root	Protege este puerto de switch contra creer el root bridge es alcanzable por este puerto
Switchport port-security	Protege el switch (en este puerto al menos) contra una tabla de dirección MAC inundando ataques (tabla CAM con sobreflujo) e impide una inanición de ataque DHCP para ser lanzado del dispositivo conectado a este puerto.
No cdp enable	Des habilita CDP dentro de un interface
No cdp run	Des habilita CDP globalmente en el switch
Ip dhcp snooping	Habilitar DHCP snooping globalmente en el switch
Ip DHCP snooping vlan X	Habilita DHCP snooping en la VLAN X
Ip DHCP snooping trust	Configura en una interface como un interface de confianza DHCP snooping
Ip arp inspection vlan X	Configure VLAN X para DAI
Ip arp inspection trust	Configura una interface como interface confiable DAI

CAPITULO 10

FUNDAMENTOS DE PROTECCION DE RED