

Administración Zentyal



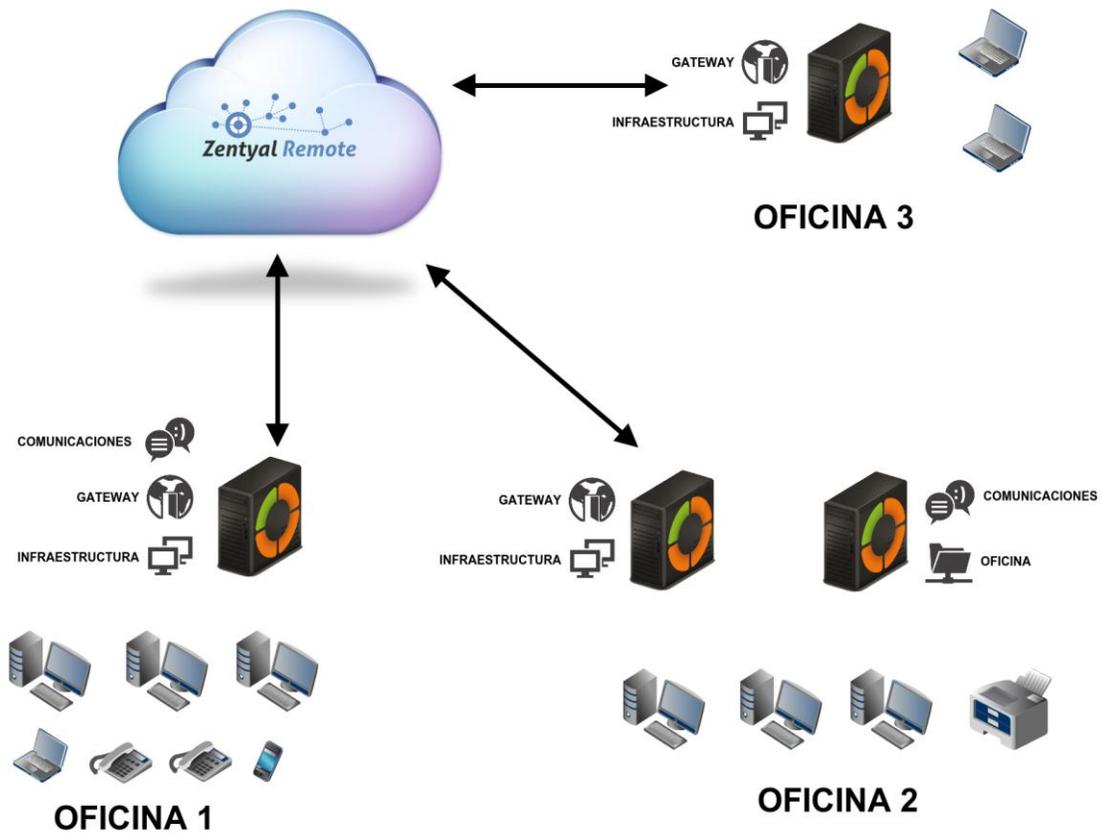
MANUAL DE MANEJO DE ZENTYAL

Contenido

1. Introducción	3
2. Instalación	4
3. Configuración inicial	12
4. Administración Web.....	18
5. Dashboard	20
6. Configuración del estado de los módulos	22
Aplicando los cambios en la configuración	23
7. Configuración general	24
8. Configuración de red en Zentyal	25
9. Objetos de red.....	34
10. Gestión de los Objetos de red con Zentyal	34
11. Servicios de red	37
12. Zentyal Gateway.....	39
13. Cortafuegos.....	39

1. Introducción

Por medio del presente manual se espera dar a entender a un usuario informático el uso adecuado de Zentyal para el rol de servidor dentro de una organización, en el manejo tanto desde la instalación, y la configuración del mismo para funcionar como firewall y la habilitación de Proxy dentro del mismo.



El grafico anteriormente descrito muestra la estructura funcional de Zentyal como servidor de una organización.

2. Instalación

2.1. El instalador de Zentyal

El instalador de Zentyal está basado en el instalador de *Ubuntu Server* así que el proceso de instalación resultará muy familiar a los usuarios de dicha distribución.

En primer lugar seleccionaremos el lenguaje de la instalación, para este ejemplo usaremos *Español*.



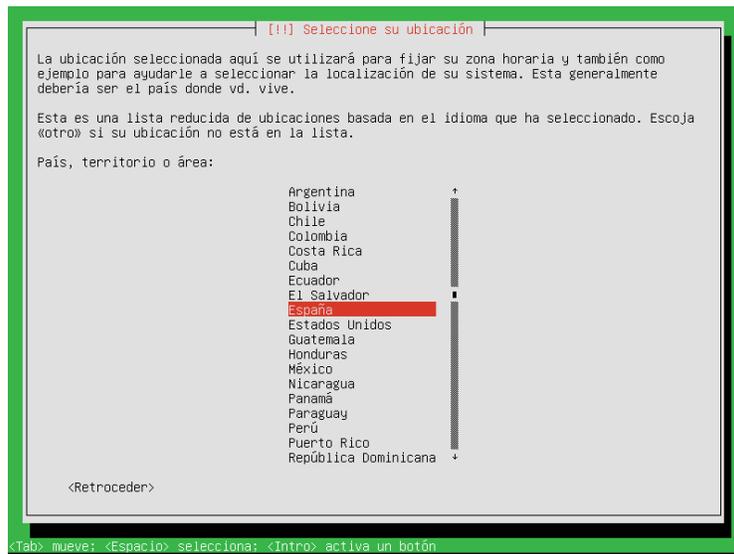
Selección del idioma

Podemos instalar utilizando la opción por omisión que elimina todo el contenido del disco duro y crea las particiones necesarias para Zentyal usando *LVM* o podemos seleccionar la opción *expert mode* que permite realizar un particionado personalizado. La mayoría de los usuarios deberían elegir la opción por omisión a no ser que estén instalando en un servidor con RAID por software o quieran hacer un particionado más específico a sus necesidades concretas.



Inicio del instalador

En el siguiente paso elegiremos el lenguaje que usará la interfaz de nuestro sistema una vez instalado, para ello nos pregunta por el país donde nos localizamos, en este caso *Ecuador*.

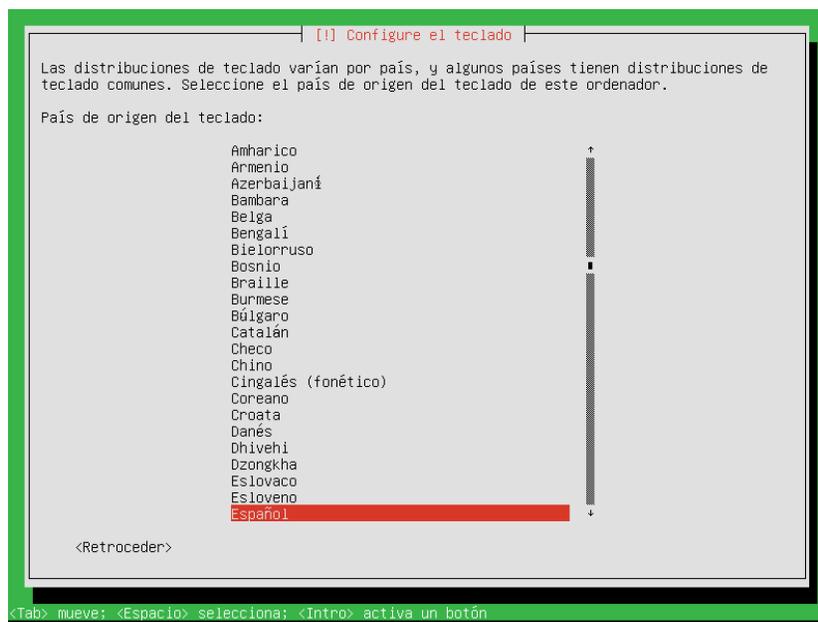


Localización geográfica

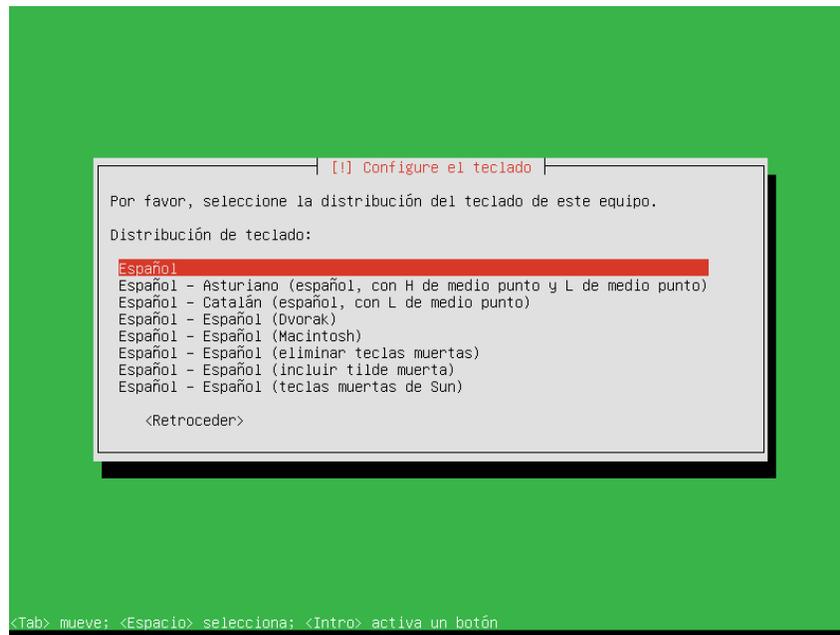
Podemos usar la detección de automática de la distribución del teclado, que hará unas cuantas preguntas para asegurarse del modelo que estamos usando o podemos seleccionarlo manualmente escogiendo *No*.



Auto detección del teclado

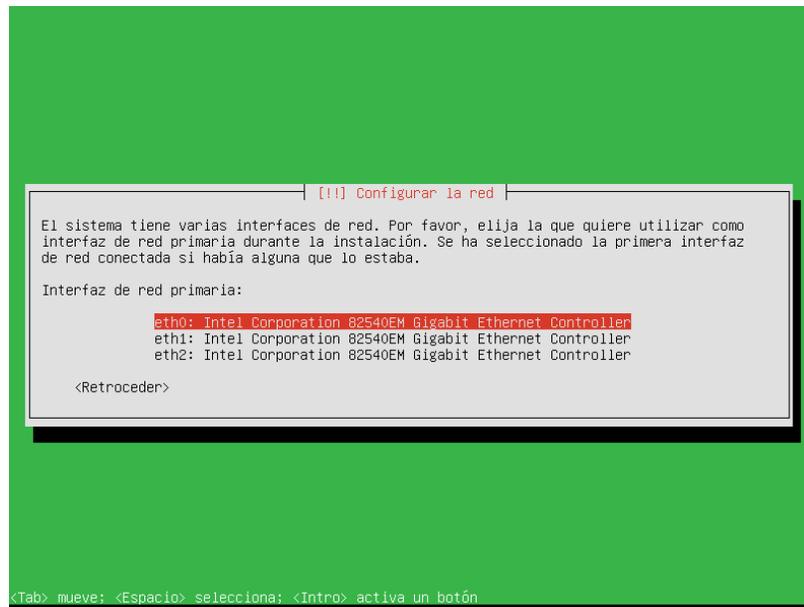


Selección del teclado 1



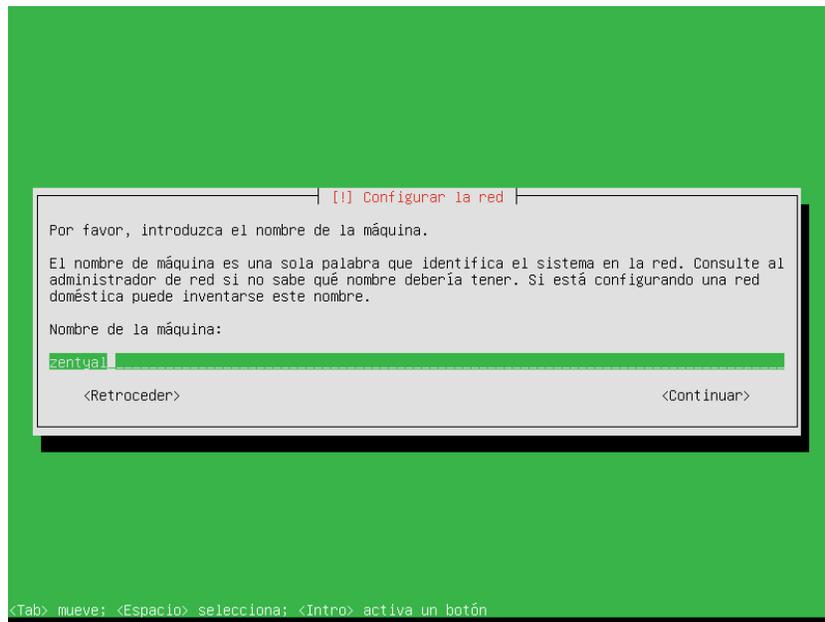
Selección del teclado 2

En caso de que dispongamos de más de una interfaz de red, el sistema nos preguntará cuál usar durante la instalación (por ejemplo para descargar actualizaciones). Si tan solo tenemos una, no habrá pregunta.



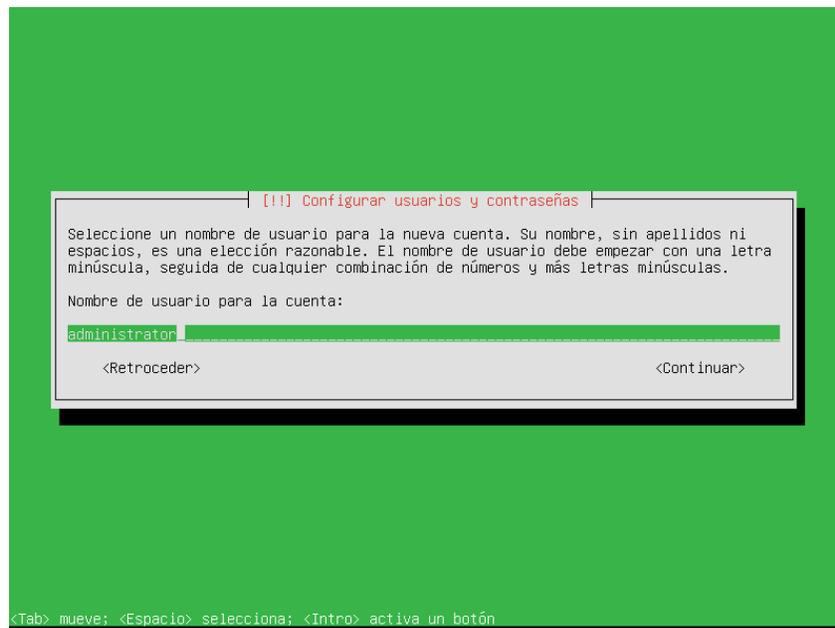
Selección de interfaz de red

Después elegiremos un nombre para nuestro servidor; este nombre es importante para la identificación de la máquina dentro de la red. El servicio de *DNS* registrará automáticamente este nombre, *Samba* también lo usará de identificador como podremos comprobar más adelante.



Nombre de la máquina

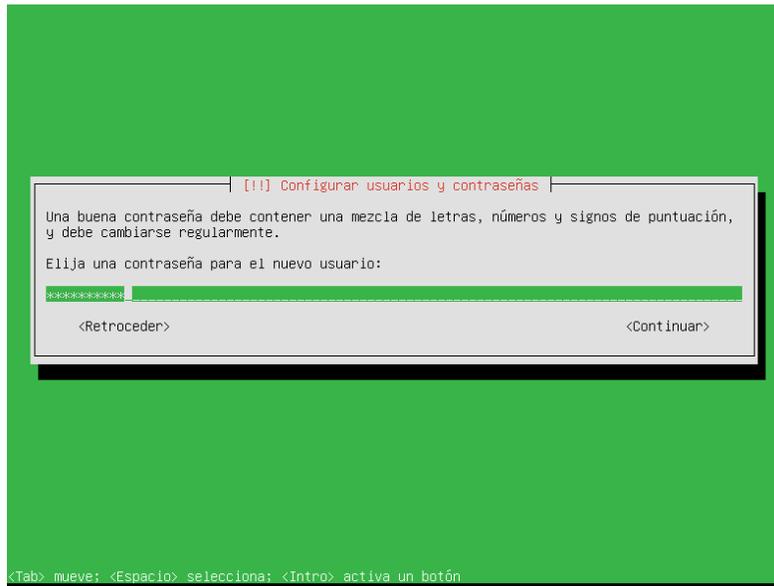
Para continuar, habrá que indicar el nombre de usuario o *login* usado para identificarse ante el sistema. Este usuario tendrá privilegios de administración y además será el utilizado para acceder a la interfaz de Zentyal.



Usuario qhcalinux

En el siguiente paso nos pedirá la contraseña para el usuario. Cabe destacar que el anterior usuario con esta contraseña podrá acceder tanto al sistema (mediante SSH o *login* local) como a la interfaz web de Zentyal, por lo que seremos especialmente

cuidadosos en elegir una contraseña segura (más de 12 caracteres incluyendo letras, cifras y símbolos de puntuación).



[!!] Configurar usuarios y contraseñas

Una buena contraseña debe contener una mezcla de letras, números y signos de puntuación, y debe cambiarse regularmente.

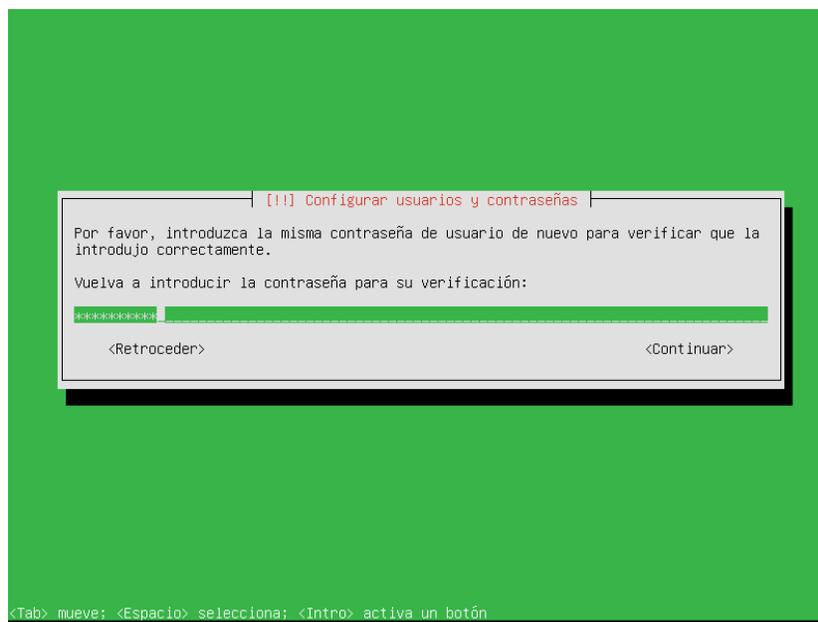
Elija una contraseña para el nuevo usuario:

<Retroceder> <Continuar>

<Tab> mueve: <Espacio> selecciona: <Intro> activa un botón

Contraseña:

E introduciremos de nuevo la contraseña para su verificación.



[!!] Configurar usuarios y contraseñas

Por favor, introduzca la misma contraseña de usuario de nuevo para verificar que la introdujo correctamente.

Vuelva a introducir la contraseña para su verificación:

<Retroceder> <Continuar>

<Tab> mueve: <Espacio> selecciona: <Intro> activa un botón

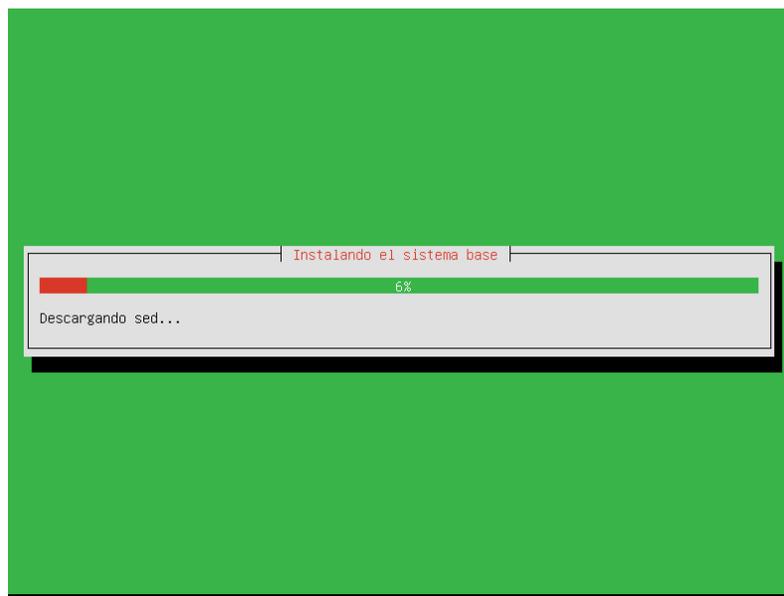
Confirmar contraseña

En el siguiente paso, se nos pregunta por nuestra zona horaria, que se auto configurará dependiendo del país de origen que hayamos seleccionado anteriormente, pero se puede modificar en caso de que sea errónea.



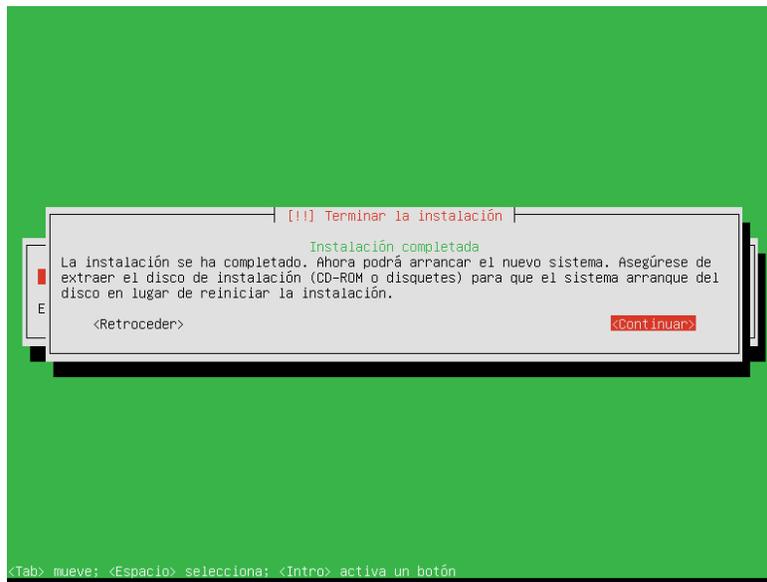
Zona horaria

Esperaremos a que nuestro sistema básico se instale, mientras muestra una barra de progreso. Este proceso puede durar unos 20 minutos aproximadamente, dependiendo del servidor en cada caso.



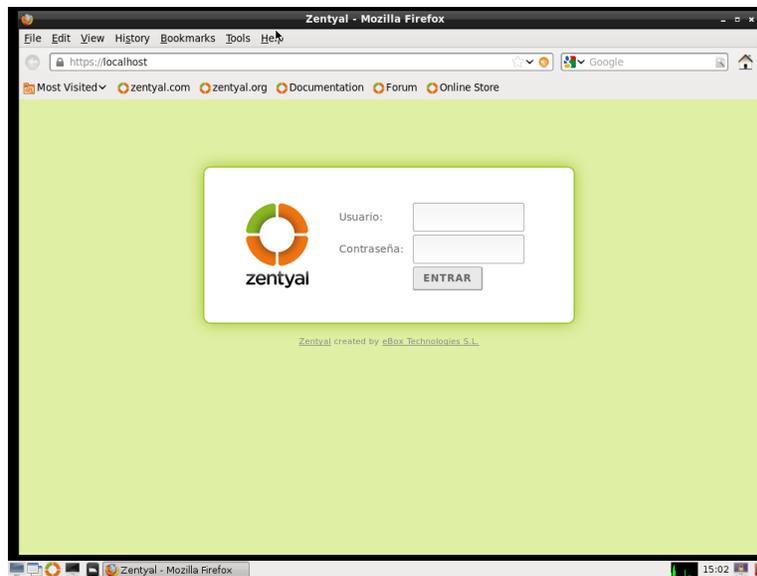
Instalación del sistema base

La instalación del sistema base está completada; ahora podremos extraer el disco de instalación y reiniciar.



Reiniciar

El sistema arrancará un interfaz gráfico con un navegador que permite acceder a la interfaz de administración, y, aunque tras este primer reinicio el sistema haya iniciado la sesión de usuario automáticamente, de aquí en adelante, necesitará autenticarse antes de hacer login en el sistema. El primer arranque tomará algo más de tiempo, ya que necesita configurar algunos paquetes básicos de software.



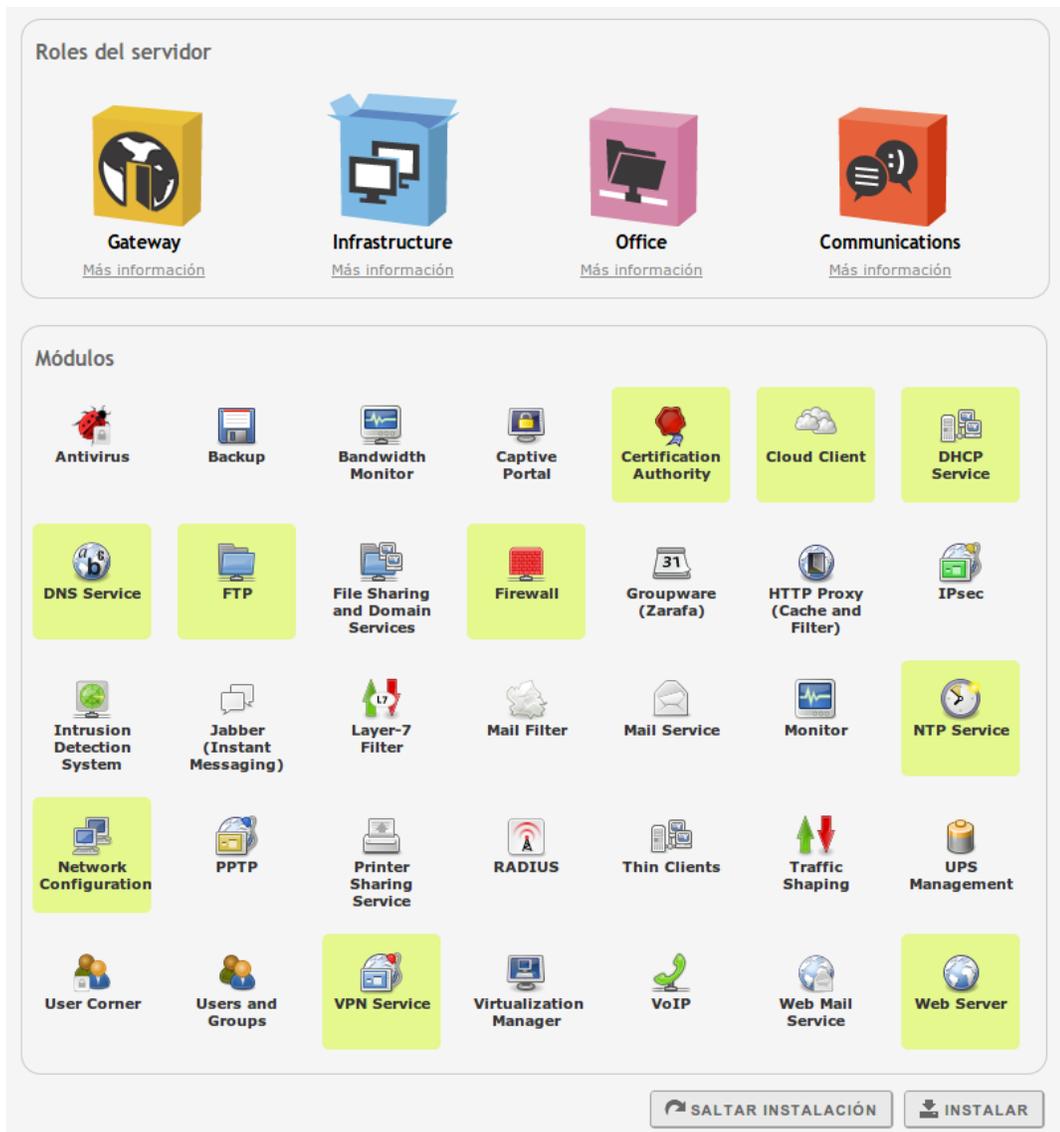
Entorno gráfico con el interfaz de administración

Para comenzar a configurar los perfiles o módulos de Zentyal, usaremos el usuario y contraseña indicados durante la instalación. Cualquier otro usuario que añadamos posteriormente al grupo *sudo* podrá acceder al interfaz de Zentyal al igual que tendrá privilegios de superusuario en el sistema.

3. Configuración inicial

Una vez autenticado por primera vez en la interfaz web comienza un asistente de configuración, en primer lugar podremos seleccionar qué funcionalidades queremos incluir en nuestro sistema.

Para simplificar nuestra selección, en la parte superior de la interfaz contamos con unos perfiles prediseñados.



Perfiles y paquetes instalables

3.1. Perfiles de Zentyal que podemos instalar:

3.1.1. Zentyal Gateway:

Zentyal actúa como la puerta de enlace de la red local ofreciendo un acceso a Internet seguro y controlado. Zentyal protege la red local contra ataques externos, intrusiones, amenazas a la seguridad interna y posibilita la interconexión segura entre redes locales a través de Internet u otra red externa.

3.1.2. Zentyal Infrastructure:

Zentyal gestiona la infraestructura de la red local con los servicios básicos: DHCP, DNS, NTP, servidor HTTP, etc.

3.1.3. Zentyal Office:

Zentyal actúa como servidor de recursos compartidos de la red local: ficheros, impresoras, calendarios, contactos, perfiles de usuarios y grupos, etc.

3.1.4. Zentyal Unified Communications:

Zentyal se convierte en el centro de comunicaciones de la empresa, incluyendo correo, mensajería instantánea y Voz IP. Podemos seleccionar varios perfiles para hacer que Zentyal tenga, de forma simultánea, diferentes roles en la red.

También podemos instalar un conjunto manual de servicios simplemente clicando sobre sus respectivos iconos sin necesidad de amoldarnos a los perfiles, o bien, instalar un perfil más unos determinados paquetes que también nos interesen.

Para nuestro ejemplo usaremos una instalación del perfil de Infraestructura únicamente. Los *wizards* que aparecerán en nuestra instalación dependen de los paquetes que hayamos escogido en este paso.

Al terminar la selección, se instalarán también los paquetes adicionales necesarios y además si hay algún complemento recomendado se preguntará si lo queremos instalar. Esta selección no es definitiva, ya que posteriormente podremos instalar y desinstalar el resto de módulos de Zentyal a través de la gestión de software.



Paquetes adicionales

El sistema comenzará con el proceso de instalación de los módulos requeridos, mostrando una barra de progreso donde además podemos leer una breve introducción sobre las funcionalidades y servicios adicionales disponibles en Zentyal Server y los paquetes comerciales asociados.

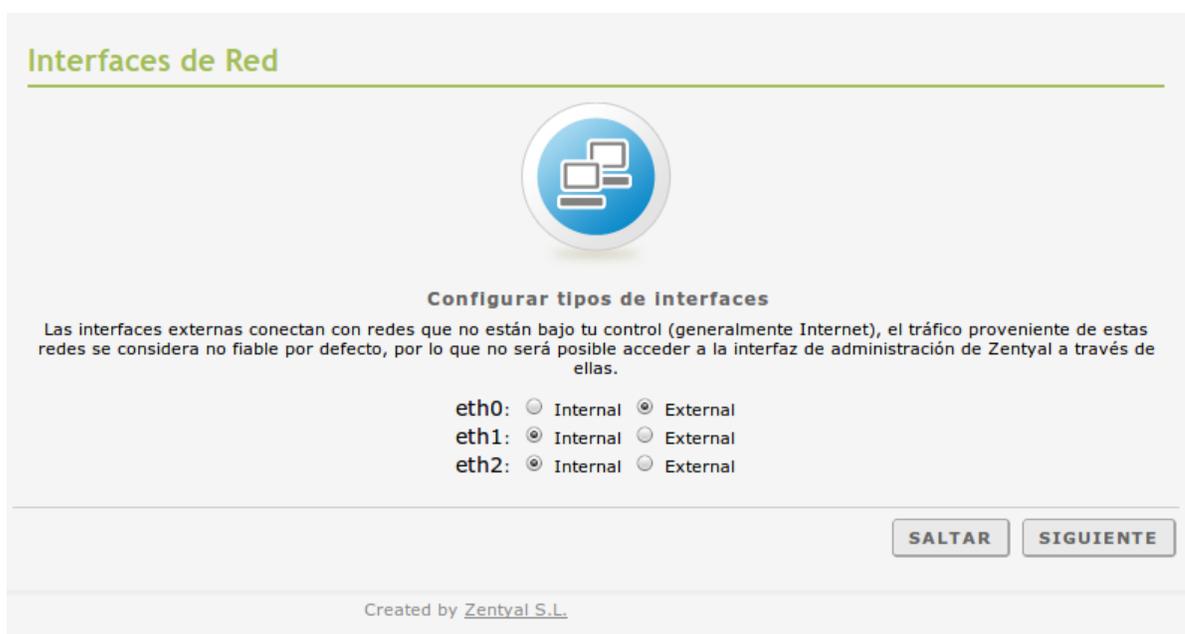


Instalación e información adicional

Una vez terminado el proceso de instalación el asistente configurará los nuevos módulos realizando algunas preguntas. Cuando instalemos módulos de Zentyal más adelante, pueden llevar asociados *wizards* de configuración similares.

En primer lugar se solicitará información sobre la configuración de red, definiendo para cada interfaz de red si es interna o externa, es decir, si va a ser utilizada para conectarse a Internet u otras redes externas, o bien, si está conectada a la red local. Se aplicarán políticas estrictas en el cortafuego para todo el tráfico entrante a través de interfaces de red externas.

Posteriormente, podemos configurar el método y parámetros de configuración (DHCP, estática, IP asociada, etc.). De nuevo, si nos equivocamos en cualquiera de estos parámetros no es crítico dado que los podremos modificar desde el interfaz de Zentyal en cualquier otro momento.



The screenshot shows a configuration window titled "Interfaces de Red". At the top center is a blue circular icon with a white computer monitor and network cables. Below the icon is the heading "Configurar tipos de interfaces". A paragraph of text explains that external interfaces connect to networks not under the user's control (like Internet), and traffic from these networks is considered unreliable by default, meaning access to the Zentyal administration interface will not be possible through them. Below this text are three rows of radio button options for interfaces eth0, eth1, and eth2. For each interface, there are two options: "Internal" and "External". In the screenshot, eth0 is set to "External", eth1 is set to "Internal", and eth2 is set to "Internal". At the bottom right of the window are two buttons: "SALTAR" and "SIGUIENTE". At the bottom center, it says "Created by Zentyal S.L."

Seleccionar modo de las interfaces de red

A continuación, tendremos que elegir el dominio asociado a nuestro servidor, si hemos configurado nuestra(s) interfaz externa por DHCP, es posible que el campo aparezca ya rellenado. Como hemos comentado anteriormente, nuestro *hostname* se registrará como un *host* perteneciente a este dominio. El dominio de autenticación para los usuarios tomará también este identificador. Más adelante podremos configurar otros dominios y su configuración asociada, pero éste es el único que vendrá pre configurado para que nuestros clientes de LAN encuentren los servicios de autenticación necesarios.

Usuarios y Grupos



Seleccionar nombre del dominio del servidor
 Esto será usado como dominio de autenticación de Kerberos para sus usuarios.

Nombre del dominio para esta máquina

SALTAR **SIGUIENTE**

Configurar dominio local del servidor

El último asistente permite suscribir nuestro servidor. En caso de tener una suscripción ya registrada, tan sólo es necesario introducir los credenciales. Si todavía no has suscrito el servidor, es posible obtener una suscripción básica gratuita usando este mismo formulario.

Registra tu servidor Zentyal GRATIS y obtén las siguientes ventajas

- Backup de la configuración **en el cloud**
- **subdominio zentyal.me** para tu servidor
- ¡Y mucho más a punto de llegar!



Registra este servidor

Nombre del servidor*

Tu cuenta Zentyal

Registrar con una cuenta existente
 Crear una cuenta Zentyal

Correo Electrónico*

Contraseña*

* Campos obligatorios

REGISTRAR

Suscribir el servidor

En ambos casos el formulario solicita un nombre para el servidor. Una vez hayan sido respondidas estas cuestiones, se procederá a la configuración de cada uno de los módulos instalados.

Pasos de la Instalación

- ✓ Selección de paquetes
- ✓ Confirmación
- ✓ Instalación
- ✓ Configuración inicial
- Guardar los cambios**
- Finalizar

Guardando cambios

Guardando cambios en los módulos

Operación actual: **Habilitando módulo users**

38%

13 de 35 operaciones efectuadas

Configuración inicial finalizada

El instalador nos avisará cuando se haya terminado el proceso.



Guardando cambios

Ya podemos acceder al Dashboard.

The dashboard displays the following information:

- Información general:**
 - Hora: Jue sep 13 16:14:31 CEST 2012
 - Nombre de máquina: zentyal
 - Versión de la plataforma: 3.0
 - Software: 5 actualizaciones del sistema
 - Carga del sistema: 0.14, 0.13, 0.22
 - Tiempo de funcionamiento sin interrupciones: 53 min
 - Usuarios: 0
- Interfases de Red:**
 - eth0:** Estado: activado, externo, enlace ok; Dirección MAC: 08:00:27:f7:11:7f; Dirección IP: 10.0.2.15. Includes graphs for Bytes Tx and Bytes Rx.
 - eth1:** Estado: activado, interno, enlace ok; Dirección MAC: 08:00:27:50:91:1d; Dirección IP: 192.168.56.254. Includes graphs for Bytes Tx and Bytes Rx.
 - eth2:** Estado: activado, interno, enlace ok; Dirección MAC: 08:00:27:f4:13:9b; Dirección IP: 192.168.200.254. Includes graphs for Bytes Tx and Bytes Rx.
- Recursos:**
 - Comunidad: [¡Regístrate Gratis!](#), [Documentación](#), [Foro](#), [Reportar un bug](#)
 - Negocio: [Edición Small Business](#), [Edición Enterprise](#), [Formación Certificada](#), [Manual Oficial](#)
- IPs asignadas con DHCP:** No hay entradas en la lista
- Estado de los Módulos:**
 - Red: Ejecutándose
 - Cortafuegos: Ejecutándose
 - Autoridad de certificación: No creada
 - DHCP: Deshabilitado
 - DNS: Ejecutándose (Reiniciar)
 - Eventos: Ejecutándose (Reiniciar)
 - FTP: Ejecutándose (Reiniciar)
 - Registros: Ejecutándose (Reiniciar)
 - Monitorización: Ejecutándose (Reiniciar)
 - NTP: Ejecutándose (Reiniciar)
 - VPN: Ejecutándose (Reiniciar)
 - Cliente de Zentyal Remote: Suscrito
 - Usuarios y Grupos: Ejecutándose
 - Servidor Web: Ejecutándose (Reiniciar)

Created by Zentyal S.L.

4. Administración Web

Una vez instalado Zentyal, podemos acceder al interfaz web de administración tanto a través del propio entorno gráfico que incluye el instalador como desde cualquier lugar de la red interna, mediante la dirección: <https://172.16.27.254> . Dado que el acceso es mediante HTTPS, la primera vez el navegador nos pedirá si queremos confiar en este sitio, aceptaremos el certificado autogenerado.

La primera pantalla solicita el nombre de usuario y la contraseña, podrán autenticarse como administradores tanto el usuario creado durante la instalación como cualquier otro perteneciente al grupo *sudo*.

The image shows the Zentyal login interface. On the left is the Zentyal logo, which consists of a circular icon with green and orange segments and the word "zentyal" below it. To the right of the logo are two input fields: "Usuario:" with the text "administrator" and "Contraseña:" with a masked password of seven dots. Below these fields is a button labeled "ENTRAR". At the bottom of the interface, there is a footer that reads "Zentyal created by eBox Technologies S.L.".

Usuario: administrator

Contraseña:

ENTRAR

Zentyal created by eBox Technologies S.L.

Login

Una vez autenticados, aparecerá la interfaz de administración que se encuentra dividida en tres partes fundamentales:

Menú lateral izquierdo:

Contiene los enlaces a todos los **servicios** que se pueden configurar mediante Zentyal, separados por categorías. Cuando se ha seleccionado algún servicio en este menú puede aparecer un submenú para configurar cuestiones particulares de dicho servicio.



Menú lateral

Menú superior:

Contiene las **acciones**: guardar los cambios realizados en el contenido y hacerlos efectivos, así como el cierre de sesión.



Menú superior

Contenido principal:

El contenido, que ocupa la parte central, comprende uno o varios formularios o tablas con información acerca de la **configuración del servicio** seleccionado a través del menú lateral izquierdo y sus submenús. En ocasiones, en la parte superior, aparecerá una barra de pestañas en la que cada pestaña representará una subsección diferente dentro de la sección a la que hemos accedido.

Consulta registros Configurar los registros

Consulta registros

BUSCAR

Dominio	Informe completo	Informe resumido	Acción
Cortafuegos			
Cambios en la configuración		--	
Sesiones del administrador		--	
Eventos		--	
VPN		--	

10 Página 1

Contenido de un formulario

5. Dashboard

El *Dashboard* es la pantalla inicial de la interfaz. Contiene una serie de *widjets* configurables. Podemos reorganizarlos pulsando en los títulos y arrastrando con el ratón.

Pulsando en *Configurar Widjets* la interfaz cambia, permitiendo retirar y añadir nuevos *widjets*. Para añadir uno nuevo, se busca en el menú superior y se arrastra a la parte central. Para eliminarlos, se usa la cruz situada en la esquina superior derecha de cada uno de ellos.

Configurar widjets

Información de sistema | Red | DHCP | VPN

Dashboard

Configurar widjets

Core

- Dashboard
- Estado de los Módulos
- Sistema
- Red
- Mantenimiento

Información general

Hora: lun sep 10 18:33:32 CEST 2012

Nombre de máquina: zentyaldos

Versión de la plataforma: 2.3.23

Software: **7 actualizaciones del sistema**

Carga del sistema: 0.15, 0.13, 0.11

Tiempo de

Recursos

Comunidad

- [Suscripción Básica GRATIS](#)
- [Documentación](#)
- [Foro](#)
- [Reportar un bug](#)

Negocio

- [Edición Small Business](#)
- [Edición Enterprise](#)
- [Formación Certificada](#)
- [Manual Oficial](#)

IPs asignadas con DHCP

No hay entradas en la lista

Configuración del *Dashboard*

Hay un *widjet* importante dentro del *Dashboard* que muestra el estado de los módulos de Zentyal asociados a *daemons*.

Estado de los Módulos		
Red	Ejecutándose	
Cortafuegos	Ejecutándose	
Autoridad de certificación	No creada	
DHCP	Deshabilitado	
DNS	Ejecutándose	Reiniciar
Eventos	Ejecutándose	Reiniciar
FTP	Ejecutándose	Reiniciar
Registros	Ejecutándose	Reiniciar
NTP	Ejecutándose	Reiniciar
VPN	Ejecutándose	Reiniciar
Usuarios y Grupos	Ejecutándose	
Servidor Web	Ejecutándose	Reiniciar

Widget de estado de los módulos

La imagen muestra el estado para un servicio y la acción que se puede ejecutar sobre él. Los estados disponibles son los siguientes:

Ejecutándose:

El servicio se está ejecutando aceptando conexiones de los clientes. Se puede reiniciar el servicio usando *Reiniciar*.

Ejecutándose sin ser gestionado:

Si no se ha activado todavía el módulo, se ejecutará con la configuración por defecto de la distribución.

Parado:

El servicio está parado bien por acción del administrador o porque ha ocurrido algún problema. Se puede iniciar el servicio mediante *Arrancar*.

Deshabilitado:

El módulo ha sido deshabilitado explícitamente por el administrador.

6. Configuración del estado de los módulos

Zentyal tiene un diseño modular, en el que cada módulo gestiona un servicio distinto. Para poder configurar cada uno de estos servicios se ha de habilitar el módulo correspondiente desde Estado del módulo. Todas aquellas funcionalidades que hayan sido seleccionadas durante la instalación se habilitan automáticamente.

Módulo	Depende	Estado
Red		<input checked="" type="checkbox"/>
Cortafuegos	Red	<input checked="" type="checkbox"/>
DHCP	Red	<input type="checkbox"/>
DNS		<input checked="" type="checkbox"/>
Eventos		<input checked="" type="checkbox"/>
Registros		<input checked="" type="checkbox"/>
NTP		<input checked="" type="checkbox"/>
VPN	Red	<input checked="" type="checkbox"/>
Usuarios y Grupos	DNS, NTP	<input checked="" type="checkbox"/>
Servidor Web		<input checked="" type="checkbox"/>
FTP	Usuarios y Grupos	<input checked="" type="checkbox"/>

Configuración del estado del módulo

Cada módulo puede depender de otros módulos para su funcionamiento. Por ejemplo, el módulo DHCP necesita que el módulo de red esté habilitado para que pueda ofrecer direcciones IP a través de las interfaces de red configuradas. Las dependencias se muestran en la columna Dependencia y hasta que estas no se habiliten, no se puede habilitar tampoco el módulo.

NOTA: Es importante recordar que hasta que no habilitemos un módulo, este no estará funcionando realmente. Así mismo, podemos hacer diferentes cambios en la configuración de un módulo que no se aplicarán hasta que no guardemos cambios. Este comportamiento es intencional y nos sirve para poder revisar detenidamente la configuración antes de hacerla efectiva.

La primera vez que se habilita un módulo, se pide confirmación de las acciones que va a realizar en el sistema así como los ficheros de configuración que va a sobrescribir. Tras aceptar cada una de las acciones y ficheros, habrá que guardar cambios para que la configuración sea efectiva.



Confirmación para habilitar un módulo

Aplicando los cambios en la configuración

Una particularidad importante del funcionamiento de Zentyal es su forma de hacer efectivas las configuraciones que hagamos en la interfaz. Para ello, primero se tendrán que aceptar los cambios en el formulario actual, pero para que estos cambios sean efectivos y se apliquen de forma permanente se tendrá que Guardar Cambios en el menú superior. Este botón cambiará a color rojo para indicarnos que hay cambios sin guardar. Si no se sigue este procedimiento se perderán todos los cambios que se hayan realizado a lo largo de la sesión al finalizar ésta. Una excepción a este funcionamiento es la gestión de usuarios y grupos, dónde los cambios se efectúan directamente.



Guardar Cambios

Advertencia: Si se cambia la configuración de las interfaces de red, el cortafuegos o el puerto del interfaz de administración, se podría perder la conexión teniendo que cambiar la URL en el navegador o reconfigurar a través del entorno gráfico en local.

7. Configuración general

Hay varios parámetros de la configuración general de Zentyal que se pueden modificar en Sistema
▸ General.

Configuración general mostrar ayuda

Cambiar contraseña del administrador

Nombre de usuario:

Contraseña actual:

Nueva contraseña:

Confirmar contraseña:

La contraseña debe tener al menos 6 caracteres.

Selección de idioma

es_EC.UTF-8

Zona Horaria

Zona Horaria: /

Es probable que necesite reiniciar algunos servicios tras cambiar la zona horaria.

Fecha y Hora

i Dado que la sincronización con servidor NTP externo está habilitada, no puede cambiar la fecha u hora.

23/7/2013
11:59:09
Un cambio en la fecha u hora provocará que se reinicien todos los servicios de Zentyal.

Puerto TCP de la interfaz de administración

Nombre de máquina y Dominio

Nombre de máquina:

Dominio:

Se necesitará reiniciar todos los servicios o reiniciar el sistema para aplicar el cambio de nombre.

Configuración general

Contraseña:

Podemos cambiar la contraseña de un usuario. Será necesario introducir su nombre de Usuario, la Contraseña actual, la Nueva contraseña y confirmarla de nuevo en la sección Cambiar contraseña.

Idioma:

Podemos seleccionar el idioma de la interfaz mediante Selección de idioma.

Zona Horaria:

Aquí podemos especificar nuestra ciudad y país para configurar el ajuste horario.

Fecha y Hora:

Podemos especificar la fecha y hora del servidor, siempre y cuando no estemos sincronizando con un servidor de hora exterior (ver NTP).

Puerto del interfaz de administración:

Por defecto es el 443/HTTPS, pero si queremos este puerto para el servidor web, habrá que cambiar la administración de Zentyal a otro distinto y especificarlo en la URL a la hora de acceder: <https://172.16.27.254:443/>.

Nombre de la máquina y dominio:

Es posible cambiar el hostname o nombre de la máquina, así como el dominio asociado, estos parámetros corresponden con los que configuramos en la instalación.

8. Configuración de red en Zentyal

A través de Red ▶ Interfaces se puede acceder a la configuración de cada una de las tarjetas de red detectadas por el sistema y se pueden establecer como dirección de red estática (configurada manualmente), dinámica (configurada mediante DHCP), VLAN (802.1Q) trunk, PPPoE o bridged.

Además cada interfaz puede definirse como Externa si está conectada a una red externa (esto se refiere generalmente a Internet) para aplicar políticas más estrictas en el cortafuegos. En caso contrario se asumirá interna, conectada a la red local.

Cuando se configure como DHCP, no solamente se configurará la dirección IP sino también los servidores DNS y la puerta de enlace. Esto es habitual en máquinas dentro de la red local o en las interfaces externas conectadas a los routers ADSL.

Interfaces de Red

eth0 eth1

Nombre:

Método:

Externo (WAN): Marque aquí si está usando Zentyal como gateway y este interfaz está conetado a su router a Internet

CAMBIAR

Configuración DHCP de la interfaz de red

Si configuramos la interfaz como estática especificaremos la dirección IP, la máscara de red y además podremos asociar una o más Interfaces Virtuales a dicha interfaz real para disponer de direcciones IP adicionales.

Estas direcciones adicionales son útiles para ofrecer un servicio en más de una dirección IP o subred, para facilitar la migración desde un escenario anterior o para tener diferentes dominios en un servidor web usando certificados SSL.

Interfaces de Red

eth0 eth1

Nombre:

Método:

Externo (WAN): Marque aquí si está usando Zentyal como gateway y este interfaz está conetado a su router a Internet

Dirección IP:

Máscara de red:

CAMBIAR

Interfaces Virtuales

Nombre	Dirección IP	Máscara de red	Acción
<input type="text"/>	<input type="text"/>	<input type="text" value="255.255.255.0"/>	<input style="border: 1px solid #ccc; padding: 2px 5px;" type="button" value="+"/>

Configuración estática de la interfaz de red

Si se dispone de un router ADSL PPPoE (un método de conexión utilizado por algunos proveedores de Internet), podemos configurar también este tipo de conexiones. Para ello, sólo hay que seleccionar PPPoE e introducir el Nombre de usuario y Contraseña proporcionado por el proveedor.

Configuración PPPoE de la interfaz de red

En caso de tener que conectar el servidor a una o más redes VLAN, seleccionaremos Trunk (802.11q). Una vez seleccionado este método podremos crear tantas interfaces asociadas al tagdefinido como queramos y las podremos tratar como si de interfaces reales se tratase.

La infraestructura de red VLAN permite segmentar la red local para mejor rendimiento y mayor seguridad sin la inversión en hardware físico que sería necesaria para cada segmento.

Identificador de VLAN	Descripción	Acción
<input type="text"/>	<input type="text"/>	<input data-bbox="1214 1213 1247 1255" type="button" value="+"/>
6	DMZ	<input data-bbox="1214 1266 1247 1308" type="button" value="✖"/>
5	Marketing	<input data-bbox="1214 1318 1247 1360" type="button" value="✖"/>

Configuración VLAN de interfaces de red

El modo puente o bridged consiste en asociar dos interfaces de red físicas de nuestro servidor conectadas a dos redes diferentes. Por ejemplo, una tarjeta conectada al router y otra tarjeta conectada a la red local. Mediante esta asociación podemos conseguir que el tráfico de la red conectada a una de las tarjetas se redirija a la otra de modo transparente.

Esto tiene la principal ventaja de que las máquinas clientes de la red local no necesitan modificar absolutamente ninguna de sus configuraciones de red cuando instalemos un servidor Zentyal como puerta de enlace, y sin embargo, podemos gestionar el tráfico que efectivamente pasa a través de nuestro servidor con el cortafuegos, filtrado de contenidos o detección de intrusos. Esta asociación se crea cambiando el método de las interfaces a En puente de red. Podemos ver como al seleccionar esta opción nos aparece un nuevo selector, Puente de red para que seleccionemos a qué grupo de interfaces queremos asociar esta interfaz.

Interfaces de Red

eth0 eth1 vlan6 vlan5 br1

Nombre:

Método:

Externo (WAN): Marque aquí si está usando Zentyal como gateway y este interfaz está conectado a su router a Internet

Puente de red:

Creación de un bridge

Esto creará una nueva interfaz virtual bridge que tendrá su propia configuración como una interfaz real, por lo cual aunque el tráfico la atraviere transparentemente, puede ser utilizado para ofrecer otros servicios como podría ser el propio interfaz de administración de Zentyal o un servidor de ficheros.

Interfaces de Red

eth0 eth1 vlan6 vlan5 br1

Nombre:

Método:

Dirección IP:

Máscara de red:

Configuración de interfaces bridged

En el caso de configurar manualmente la interfaz de red será necesario definir la puerta de enlace de acceso a Internet en Red > Puertas de enlace. Normalmente esto se hace automáticamente si usamos DHCP o PPPoE pero no en el resto de opciones. Para cada uno podremos indicar Nombre, Dirección IP, Interfaz a la que está conectada, su Peso que sirve para indicar la prioridad respecto a otros gateways y si es el Predeterminado de todos ellos.

Además, si es necesario el uso de un proxy HTTP para el acceso a Internet, podremos configurarlo también en esta sección. Este proxy será utilizado por Zentyal para conexiones como las de actualización e instalación de paquetes o la actualización del antivirus.

Habilitado	Nombre	Dirección IP	Interfaz	Peso	Predeterminado	Acción
<input checked="" type="checkbox"/>	adsl1	10.0.2.2	eth0	3	<input checked="" type="checkbox"/>	 
<input checked="" type="checkbox"/>	adsl2	10.0.5.2	eth3	1	<input type="checkbox"/>	 

Configuración de las puertas de enlace

Para que el sistema sea capaz de resolver nombres de dominio debemos indicarle la dirección de uno o varios servidores de nombres en Red ▶ DNS. En caso de que tengamos un servidor DNS configurado en la propia máquina, el primer servidor estará fijado al local 127.0.0.1.



The screenshot shows a web interface for configuring DNS servers. At the top, there is a search bar with a 'BUSCAR' button. Below it is a table with two columns: 'Servidor de nombres de dominio' and 'Acción'. The table contains two entries: 127.0.0.1 and 10.0.2.2. The 10.0.2.2 entry is highlighted in green. Below the table, there is a pagination control showing '10' and 'Página 1' with navigation arrows.

Servidor de nombres de dominio	Acción
127.0.0.1	[X] [Edit] [Down Arrow]
10.0.2.2	[X] [Edit] [Up Arrow]

Configuración de los servidores DNS

Si la conexión a Internet asigna una dirección IP dinámica y queremos que un nombre de dominio apunte a ella, se necesita un proveedor de DNS dinámico. Utilizando Zentyal se puede configurar alguno de los proveedores de DNS dinámico más populares.

Para ello iremos a Red ▶ DynDNS y seleccionaremos el proveedor, del Servicio, Nombre de usuario, Contraseña y Nombre de máquina que queremos actualizar cuando la dirección pública cambie, sólo resta Habilitar DNS dinámico.



The screenshot shows the 'Habilitar DNS dinámico' configuration form. The 'Habilitar DNS dinámico' checkbox is checked. The 'Servicio' dropdown is set to 'DynDNS'. The 'Usuario' field is 'zentyal', the 'Contraseña' field is masked with dots, and the 'Nombre de máquina' field is 'servidor.dyndns.org'. There is a 'CAMBIAR' button at the bottom.

Habilitar DNS dinámico:

Servicio: DynDNS

Usuario: zentyal

Contraseña:

Nombre de máquina: servidor.dyndns.org

CAMBIAR

Configuración de DNS Dinámico

Zentyal se conecta al proveedor para conseguir la dirección IP pública evitando cualquier traducción de dirección red (NAT) que haya entre el servidor e Internet. Si estamos utilizando esta funcionalidad en un escenario con multirouter, no hay que olvidar crear una regla que haga que las conexiones al proveedor usen siempre la misma puerta de enlace.

Diagnóstico de red

Para ver si hemos configurado bien nuestra red podemos utilizar las herramientas de Red ▶ Herramientas.

ping es una herramienta que utiliza el protocolo de diagnóstico de redes ICMP (Internet Control Message Protocol) para comprobar la conectividad hasta una máquina remota mediante una sencilla conversación entre ambas.



Ping

Host:

Traceroute

Host:

Resolución de Nombre de Dominio

Nombre de dominio:

Wake On LAN

Dirección MAC:

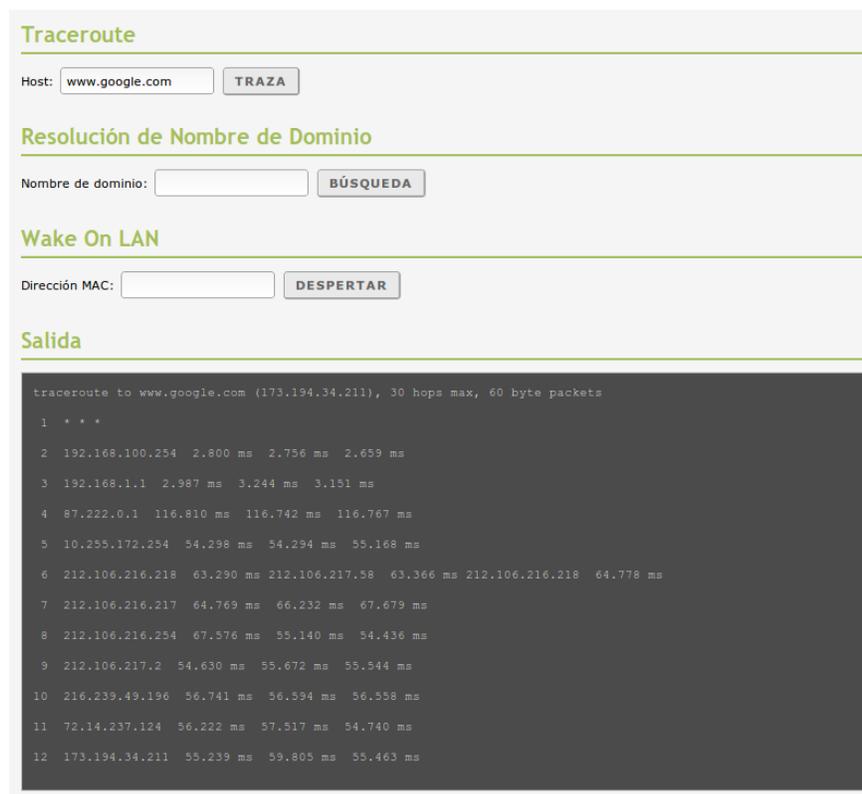
Salida

```
PING zentyal.org (92.243.17.196) 56(84) bytes of data:
64 bytes from slurm.zentyal.com (92.243.17.196): icmp_req=1 ttl=63 time=186 ms
64 bytes from slurm.zentyal.com (92.243.17.196): icmp_req=2 ttl=63 time=207 ms
64 bytes from slurm.zentyal.com (92.243.17.196): icmp_req=3 ttl=63 time=118 ms

--- zentyal.org ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2000ms
rtt min/avg/max/mdev = 118.914/171.044/207.719/37.867 ms
```

Herramientas de diagnóstico de redes, ping

También disponemos de la herramienta traceroute que se encarga de mostrar la ruta que toman los paquetes hasta llegar a la máquina remota determinada.



Traceroute

Host:

Resolución de Nombre de Dominio

Nombre de dominio:

Wake On LAN

Dirección MAC:

Salida

```
traceroute to www.google.com (173.194.34.211), 30 hops max, 60 byte packets
 1 * * *
 2 192.168.100.254 2.800 ms 2.756 ms 2.659 ms
 3 192.168.1.1 2.987 ms 3.244 ms 3.151 ms
 4 87.222.0.1 116.810 ms 116.742 ms 116.767 ms
 5 10.255.172.254 54.298 ms 54.294 ms 55.168 ms
 6 212.106.216.218 63.290 ms 212.106.217.58 63.366 ms 212.106.216.218 64.778 ms
 7 212.106.216.217 64.769 ms 66.232 ms 67.679 ms
 8 212.106.216.254 67.576 ms 55.140 ms 54.436 ms
 9 212.106.217.2 54.630 ms 55.672 ms 55.544 ms
10 216.239.49.196 56.741 ms 56.594 ms 56.558 ms
11 72.14.237.124 56.222 ms 57.517 ms 54.740 ms
12 173.194.34.211 55.239 ms 59.805 ms 55.463 ms
```

Herramienta Traceroute

La herramienta de resolución de nombres de dominio se utiliza para comprobar el correcto funcionamiento del servicio DNS.



The screenshot shows a web interface for DNS resolution. At the top, there is a section titled "Resolución de Nombre de Dominio" with a text input field containing "www.facebook.com" and a "BÚSQUEDA" button. Below this is a section titled "Wake On LAN" with a "Dirección MAC:" label and an empty text input field, followed by a "DESPERTAR" button. The main content area is titled "Salida" and displays a dark-themed terminal window with the following text:

```
>>> Dig 9.8.1-P1 <<> +time=3 www.facebook.com
;; global options: +cmd
;; Got answer:
;; -->HEADER<<- opcode: QUERY, status: NOERROR, id: 1249
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2

;; QUESTION SECTION:
;www.facebook.com.          IN      A

;; ANSWER SECTION:
www.facebook.com.         120     IN      A       69.171.242.74

;; AUTHORITY SECTION:
www.facebook.com.         1487    IN      NS      gbl1.facebook.com.
www.facebook.com.         1487    IN      NS      gbl2.facebook.com.

;; ADDITIONAL SECTION:
gbl1.facebook.com.        3341    IN      A       69.171.239.10
gbl2.facebook.com.        3341    IN      A       69.171.255.10

;; Query time: 167 msec
;; SERVER: 10.0.2.2#53(10.0.2.2)
;; WHEN: Mon Sep 10 20:46:45 2012
;; MSG SIZE  rcvd: 120
```

Resolución de nombres de dominio

Por último, usando Wake On Lan podemos activar una máquina por su dirección MAC, si la característica se encuentra activada en la misma.

Una vez revisada los diferentes tipos de configuraciones que nos facilita Zentyal, se ha elegido dos de estas para el uso de la CMLCC en las cuales se detallan a continuación.

Enlace LAN



The screenshot shows the "Interfaces de Red" configuration page in Zentyal. The "LAN" tab is selected. The configuration for the LAN interface is as follows:

- Nombre: LAN
- Método: Estático
- Externo (WAN): (unchecked)
- Dirección IP: 172.16.27.254
- Máscara de red: 255.255.255.0

There is a "CAMBIAR" button below the configuration fields. Below the configuration is a section titled "Interfaces Virtuales" with a table:

Nombre	Dirección IP	Máscara de red	Acción
<input type="text"/>	<input type="text"/>	255.255.255.0	<input data-bbox="1104 1722 1128 1753" type="button" value="+"/>

Al poseer dos tarjetas de red usamos el método estático, en el cual asignamos la dirección IP que nos sirve de Gateway dentro de la red de la organización.

Enlace WAN

Interfaces de Red

mostrar ayuda

LAN **WAN**

Nombre:

Método:

Externo (WAN):
Marque aquí si está usando Zentyal como gateway y este interfaz está conetado a su router a Internet

Dirección IP:

Máscara de red:

Interfaces Virtuales

Nombre	Dirección IP	Máscara de red	Acción
<input type="text"/>	<input type="text"/>	<input type="text" value="255.255.255.0"/>	<input type="button" value="+"/> <input type="button" value="x"/>

Una vez establecido el enlace LAN necesitamos establecer el WAN ubicando la IP que nos permite la salida hacia el Internet con la máscara de red designada por nuestro proveedor de servicios.

Puerta de Enlace

Editando puerta de enlace

Habilitado:

Nombre:

Dirección IP:

Peso:

Este campo solo es útil si tiene mas de un router y la función de balanceo de tráfico esta habilitada.

Predeterminado:

Ponemos añadir nuevo e ingresamos la puerta de enlace de nuestra salida a Internet que responde a la interfaz eth1 correspondiente a la salida WAN habilitamos la misma y la Predeterminamos.

Configuración de Puertas de Enlace

mostrar ayuda

Puertas de enlace y Proxy | Balanceo de tráfico | WAN failover

Lista de Puertas de Enlace

+ Añadir nuevo/a

BUSCAR

Habilitado	Nombre	Dirección IP	Interfaz	Peso	Predeterminado	Acción
<input checked="" type="checkbox"/>	wan	200.105.236.233	eth1	1	<input checked="" type="checkbox"/>	 

10 | Página 1 |    

Proxy

Usuario: Opcional

Contraseña: Opcional

Servidor proxy: Opcional

Puerto del proxy:

DNS

Para el funcionamiento correcto de nuestra red necesitamos establecer los DNS de nuestro proveedor los que responde a nuestra IP, para ello los establecemos de la siguiente manera.

Traductor de Servidores de Nombres de Dominio

mostrar ayuda

Lista de traductores de servidores de nombres de dominio

+ Añadir nuevo/a

BUSCAR

Servidor de nombres de dominio	Acción
127.0.0.1	   
200.105.225.2	   
200.105.225.4	   

10 | Página 1 |    

Dominio de búsqueda

Dominio: Opcional

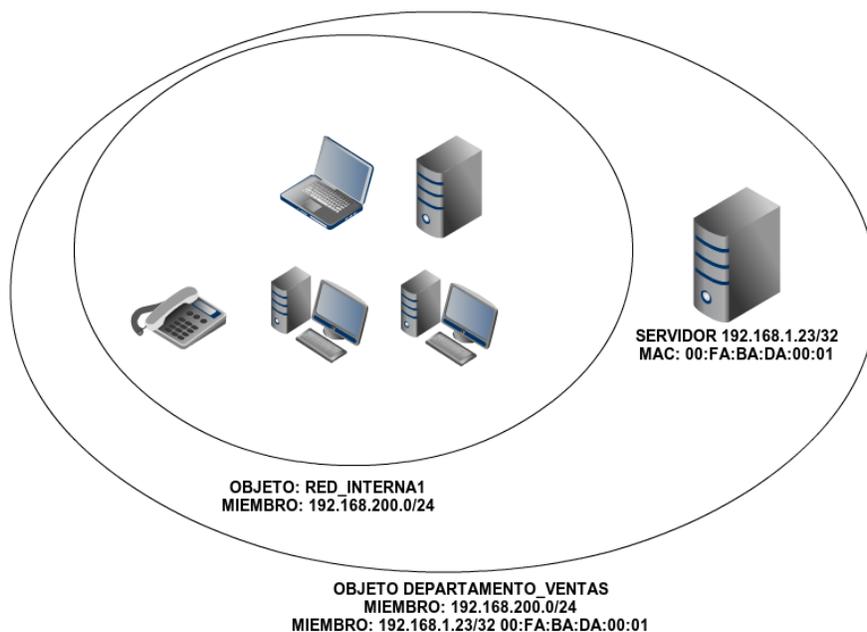
CAMBIAR

Ya establecidos los parámetros de la red podemos generar objetos para dividir de acuerdo a nuestras necesidades por lo cual se ha establecido un rango de IPs para cada uno de los departamentos y áreas de la CMLCC.

9. Objetos de red

Los **Objetos de red** son una manera de representar un elemento de la red o a un conjunto de ellos. Sirven para simplificar y consecuentemente facilitar la gestión de la configuración de la red, pudiendo dotar de un nombre fácilmente reconocible al elemento o al conjunto y aplicar la misma configuración a todos ellos.

Por ejemplo, en lugar de definir la misma regla en el cortafuegos para cada una de las direcciones IP de una subred, simplemente bastaría con definirla para el objeto de red que contiene las direcciones.



Un objeto está compuesto por cualquier cantidad de miembros, cada uno de los cuales está a su vez compuesto por un rango de red o un host específico.

10. Gestión de los Objetos de red con Zentyal

Para empezar a trabajar con los objetos en Zentyal, accederemos la sección *Red* ▶ *Objetos*, allí podremos ver una lista inicialmente vacía, con el nombre de cada uno de los objetos y una serie de acciones a realizar sobre ellos. Se pueden crear, editar y borrar objetos que serán usados más tarde por otros módulos.

Objetos

mostrar ayuda

Lista de objetos

+ Añadir nuevo/a

BUSCAR

Nombre	Miembros	Acción
Administrativo Financiero		
Celulares		
Comunicacion Social		
DominoFacebookHTTPS		
Investigacion		
Juridico		
Presidencia		
Prevencion		
Secretaria Pleno		

10 | Página 1

Para agregar un objeto de red simplemente seleccionamos **Agregar nuevo/a** y procedemos a la configuración.

Añadiendo un/a nuevo/a objeto

Nombre:

AÑADIR **CANCELAR**

Le asignamos un nombre al objeto para caso de demostración agregaremos Pruebas y ponemos añadir el mismo se despliega en el menú inferior

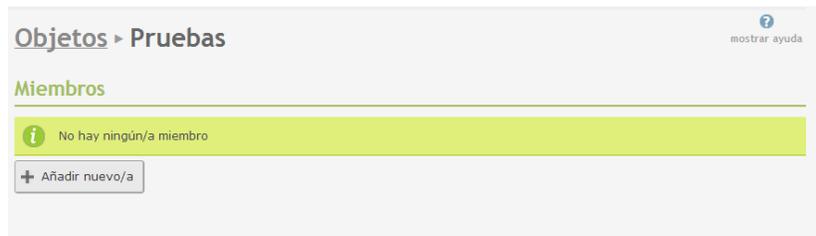
Lista de objetos

BUSCAR

Nombre	Miembros	Acción
Administrativo Financiero		
Celulares		
Comunicacion Social		
DominoFacebookHTTPS		
Investigacion		
Juridico		
Presidencia		
Prevencion		
Pruebas		
Secretaria Pleno		

10 | Página 1

Para editar el objeto simplemente hacemos un clic sobre el engrane a la altura del nombre del objeto



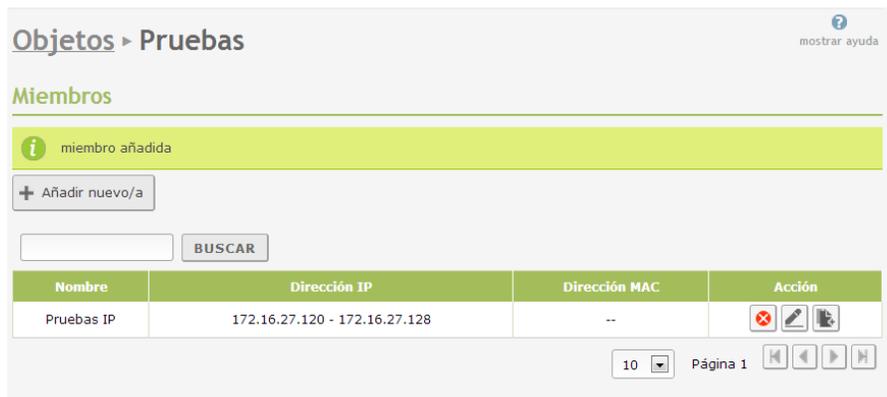
En la parte superior aparece el nombre del objeto y un botón que nos permite agregar los miembros del mismo hacemos clic en **Añadir nuevo/a**



Se nos despliega un menú el cual nos pide un nombre para identificar al miembro del objeto y nos da dos opciones CIDR que es una IP para englobar todo un sector de una red o podemos agregar la opción de rango para determinar desde cual IP hasta cual IP deseamos que se encuentre dentro del objeto para la demostración usaremos la opción de rango.



Elegido el rango de IP simplemente hacemos un clic en **AÑADIR** y esto guardará el cambio realizado a nuestro objeto.



Ya agregada nos da la opción de eliminar, editar y clonar la configuración del mismo.

Para guardar estos cambios buscaremos la opción en el menú superior de **Guardar Cambios**

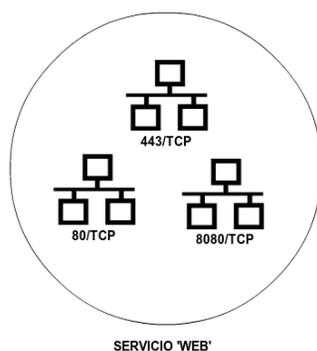


Y esta creado nuestro objeto para usarlo más adelante en el resto de los módulos.

11. Servicios de red

Los **Servicios de red** son la manera de representar los protocolos (TCP, UDP, ICMP, etc.) y puertos usados por una aplicación o conjunto de aplicaciones relacionadas. La utilidad de los servicios es similar a la de los objetos: si con los objetos se puede hacer referencia a un conjunto de direcciones IP usando un nombre significativo, podemos así mismo identificar un conjunto de puertos por el nombre de la aplicación que los usa.

Pongamos como ejemplo la navegación web. El puerto más habitual es el de HTTP, 80/TCP. Pero además también tenemos que contar con el HTTPS 443/TCP y el alternativo 8080/TCP. De nuevo, no tenemos que aplicar una regla que afecte a la navegación web a cada uno de los puertos, sino al servicio que la representa que contiene estos tres puertos. Otro ejemplo puede ser la compartición de ficheros en redes Windows, donde el servidor escucha en los puertos 137/TCP, 138/TCP, 139/TCP y 445/TCP.



Gestión de los Servicios de red con Zentyal

Para trabajar con los servicios en Zentyal se debe ir al menú *Red* ▶ *Servicios* donde se listan los servicios existentes creados por cada uno de los módulos que se hayan instalado y los que hayamos podidos definir adicionalmente. Para cada servicio podemos ver su *Nombre*, *Descripción* así como acceder a su *Configuración*. Cada servicio tendrá una serie de miembros, cada uno de estos miembros tendrá los valores: *Protocolo*, *Puerto origen* y *Puerto destino*. En todos estos

campos podemos introducir el valor *Cualquiera*, por ejemplo, para especificar servicios en los que sea indiferente el puerto origen, o un *Rango de puertos*.

El protocolo puede ser TCP, UDP, ESP, GRE o ICMP. También existe un valor TCP/UDP para evitar tener que añadir dos veces un mismo puerto que se use en ambos protocolos, como en el caso de DNS.

Lista de servicios

+ Añadir nuevo/a

BUSCAR

Nombre del servicio	Descripción	Configuración	Acción
Correo Entrante	Protocolos POP, IMAP y SIEVE		
Envío de Correo	Correo saliente (Protocolo de envío).		
FTP	Servidor FTP de Zentyal		
HTTP	Protocolo de Transporte de hipertexto		
SMTP	Correo saliente (protocolo SMTP).		
Voz IP	Sistema Voz IP de Zentyal		
Administración de Zentyal	Servidor web de administración de Zentyal		
Cualquier TCP	Cualquier puerto TCP		
Cualquier UDP	Cualquier puerto UDP		
Cualquiera	Cualquier protocolo y puerto		

10

12. Zentyal Gateway

En el caso de nuestro servidor se trabaja el mismo como un Gateway dentro de la red interna de la CMLCC, para lo cual deberemos habilitar tanto el firewall como el proxy del mismo, de esta manera podremos tener control sobre la red y gestionar la misma de una manera fiable y segura, lograr el control del ancho de banda y definir las políticas para la navegación y contenidos visitados por nuestros usuarios.

En esta parte del manual igualmente nos centraremos fundamentalmente en el módulo del cortafuegos, lo que nos permitirá controlar el tráfico tanto entrante como saliente de nuestro servidor como de la red interna.

Otro servicio necesario es el despliegue de un Proxy HTTP. El cual nos permite acelerar el acceso a internet, almacenando un cache de la navegación y estableciendo reglas de contenidos.

13. Cortafuegos

Configuración de un cortafuegos con Zentyal

El modelo de seguridad de Zentyal se basa en intentar proporcionar la máxima seguridad posible en su configuración predeterminada, intentando a la vez minimizar los esfuerzos a realizar tras añadir un nuevo servicio.

Cuando Zentyal actúa de cortafuegos, normalmente se instala entre la red interna y el *router* conectado a Internet. La interfaz de red que conecta la máquina con el *router* debe marcarse como *Externo en Red* -> *Interfaces* para permitir al cortafuegos establecer unas políticas de filtrado más estrictas para las conexiones procedentes de fuera.



The screenshot shows the 'Interfaces de Red' configuration page in Zentyal. It features two tabs: 'LAN' and 'WAN', with 'WAN' selected. The configuration fields are as follows:

- Nombre: WAN
- Método: Estático
- Externo (WAN): (with a note: 'Marque aquí si está usando Zentyal como gateway y este interfaz está conectado a su router a Internet')
- Dirección IP: 200.105.236.234
- Máscara de red: 255.255.255.252
- A 'CAMBIAR' button is located at the bottom of the form.

Interfaz externa

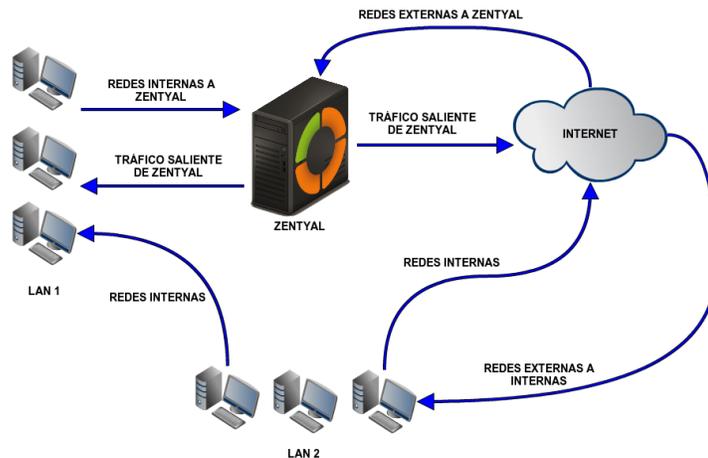
La política por defecto para las interfaces externas es denegar todo intento de nueva conexión a Zentyal, mientras que para las interfaces internas se deniegan todos los intentos de conexión a Zentyal excepto los que se realizan a servicios definidos por los módulos instalados. Los módulos añaden reglas al cortafuegos para permitir estas conexiones, aunque siempre pueden ser modificadas posteriormente por el administrador. Una excepción a esta norma son las conexiones al servidor LDAP, que añaden la regla pero configurada para denegar las conexiones por motivos de seguridad. La configuración predeterminada tanto para la salida de las redes internas como desde del propio servidor es permitir toda clase de conexiones.

La definición de las políticas del cortafuegos se hace desde *Cortafuegos* ▶ *Filtrado de paquetes*.

Se pueden definir reglas en 5 diferentes secciones según el flujo de tráfico sobre el que serán aplicadas:

- *Tráfico de redes internas a Zentyal* (ejemplo: permitir acceso al servidor de ficheros desde la red local).
- *Tráfico entre redes internas y de redes internas a Internet* (ejemplo: restringir el acceso a todo Internet a unas direcciones internas o restringir las comunicaciones entre las subredes internas).
- *Tráfico de Zentyal a redes externas* (ejemplo: permitir descargar ficheros por HTTP desde el propio servidor).
- *Tráfico de redes externas a Zentyal* (ejemplo: permitir que el servidor de correo reciba mensajes de Internet).
- *Tráfico de redes externas a redes internas* (ejemplo: permitir acceso a un servidor interno desde Internet).

Hay que tener en cuenta que los dos últimos tipos de reglas pueden crear un compromiso en la seguridad de Zentyal y la red, por lo que deben utilizarse con sumo cuidado.



Esquema de los diferentes flujos de tráfico en el cortafuegos

Estudiando el esquema, podemos determinar en qué sección se encontraría cualquier tipo de tráfico que deseemos controlar en nuestro cortafuegos. Las flechas sólo indican origen y destino, como es natural, todo el tráfico debe atravesar el cortafuegos de Zentyal para poder ser procesado. Por ejemplo, la flecha *Redes Internas* que va de la *LAN 2* hasta *Internet*, representa que uno de los equipos de la LAN es el origen y una máquina en Internet el destino, pero la conexión será procesada por Zentyal, que es la puerta de enlace para esa máquina.

Zentyal provee una forma sencilla de definir las reglas que conforman la política de un cortafuegos. La definición de estas reglas usa los conceptos de alto nivel introducidos anteriormente: los **Servicios de red** para especificar a qué protocolos y puertos se aplican las reglas y los **Objetos de red** para especificar sobre qué direcciones IP de origen o de destino se aplican.

Configuración general del Proxy HTTP con Zentyal

Para configurar el proxy HTTP iremos a *Proxy HTTP* ▶ *General*. Podremos definir si el proxy funciona en modo *Proxy Transparente* para forzar la política establecida o si por el contrario requerirá configuración manual. En cualquier caso, en *Puerto* estableceremos dónde escuchará el servidor conexiones entrantes. El puerto preseleccionado es el 3128, otros puertos típicos son el 8000 y el 8080. El proxy de Zentyal únicamente acepta conexiones provenientes de las interfaces de red internas, por tanto, se debe usar una dirección interna en la configuración del navegador.

El tamaño de la caché define el espacio en disco máximo usado para almacenar temporalmente contenidos web. Se establece en *Tamaño de caché* y corresponde a cada administrador decidir cuál es el tamaño óptimo teniendo en cuenta las características del servidor y el tráfico esperado.

The screenshot shows the 'Proxy HTTP' configuration page in Zentyal. The main heading is 'Configuración General'. Below it, there is an information icon and a message: '¿Quieres eliminar los anuncios de la navegación de tus usuarios? Obtén la edición Small Business o Enterprise que mantendrán tus reglas de Bloqueo de Anuncios siempre actualizadas.' The configuration options are: 'Proxy Transparente' (checked), 'Habilitar Single Sign-On (Kerberos)' (unchecked), and 'Bloqueo de Anuncios' (checked). Below these, there is a link 'Quitar anuncios de todo el tráfico HTTP'. The 'Puerto' field is set to '3128' and the 'Tamaño de los ficheros de caché (MB)' field is set to '10000'. A 'CAMBIAR' button is located below the cache size field. The 'Excepciones en la caché' section shows 'No hay ningún/a nombre de dominio' and a '+ Añadir nuevo/a' button. The 'Excepciones del Proxy Transparente' section also shows 'No hay ningún/a nombre de dominio' and a '+ Añadir nuevo/a' button.

Proxy HTTP

Es posible indicar que dominios no serán almacenados en caché. Por ejemplo, si tenemos servidores web locales, no se acelerará su acceso usando la caché y se desperdiciaría memoria que podría ser usada por elementos de servidores remotos. Si un dominio está exento de la caché, cuando se reciba una petición con destino a dicho dominio se ignorará la caché y se devolverán directamente los datos recibidos desde el servidor sin almacenarlos. Estos dominios se definen en *Excepciones a la caché*.

A su vez, puede interesarnos que ciertas páginas no se sirvan a través del proxy, sino que se conecte directamente desde el navegador del cliente, ya sea por cuestiones de funcionamiento incorrecto o de privacidad de los usuarios. En esos casos, podemos añadir una excepción en *Excepciones del Proxy Transparente*.

La característica *Activar Single Sign-On (Kerberos)* sirve para validar el usuario automáticamente usando el ticket de *Kerberos* creado al inicio de sesión, por lo tanto nos puede ser útil si estamos usando proxy *No Transparente*, políticas de acceso por grupos y, por supuesto, un esquema de autorizaciones basado en *Kerberos*. El funcionamiento del esquema mencionado se desarrollará en el capítulo ***Servicio de compartición de ficheros y de autenticación***.

Advertencia: Si vamos a usar autenticación automática con Kerberos, al configurar el navegador cliente tendremos que especificar nuestro proxy (el servidor zentyal) por su nombre en el dominio local, nunca por IP.

El proxy HTTP puede eliminar anuncios de las páginas web. Esto ahorrara ancho de banda y reducirá distracciones e incluso riesgos de seguridad para los usuarios. Para usar esta característica, debemos activar la opción Bloqueo de Anuncios.

Reglas de acceso

Una vez hayamos decidido nuestra configuración general, tendremos que definir reglas de acceso. Por defecto, la sección *Proxy HTTP* ▶ *Reglas de acceso* contiene una regla permitiendo todo acceso. Al igual que en el *Cortafuegos*, la política por omisión de regla siempre será denegar y la regla que tendrá preferencia en caso de que varias sean aplicables será la que se encuentre más arriba.



Añadiendo un/a nuevo/a regla

Período de tiempo: De Para Días de la semana L M X J V S D

Período de tiempo en el cual se aplicará esta regla

Origen: Objeto de red Ventas

Decisión: Aplicar perfil de filtrado filtro_estricto

Nueva regla de acceso al proxy

Mediante el *Período de tiempo* podemos definir en que momento se tendrá en consideración esta regla, tanto las horas como los días. Por defecto se aplica en todo momento.

El *Origen* es un parámetro muy flexible, ya que nos permite definir si esta regla se aplicará a los miembros de un *Objeto* de Zentyal o a los usuarios de un determinado *Grupo* (recordemos que las restricciones por grupo sólo están disponibles para el modo de Proxy **no** transparente). La tercera opción es aplicar la regla sobre cualquier tipo de tráfico que atraviese el proxy.

Advertencia Por limitaciones de DansGuardian no son posibles ciertas combinaciones de reglas basadas en grupo y reglas basadas en objeto. La interfaz de Zentyal avisará al usuario cuando se de uno de estos casos.

De forma similar al *Cortafuegos*, una vez Zentyal haya decidido que el tráfico coincide con una de las reglas definidas, debemos indicarle una *Decisión*, en el caso del Proxy hay tres opciones:

- Permitir todo: Permite todo el tráfico sin hacer ninguna comprobación, nos permite aún así, seguir disfrutando de caché de contenidos web y registros de accesos.
- Denegar todo: Deniega la conexión web totalmente.
- Aplicar perfil de filtrado: Para cada petición, comprobará que los contenidos no incumplen ninguno de los filtros definidos en el perfil, se desarrollarán los perfiles de filtrado en el siguiente apartado.

Observemos el siguiente ejemplo:



The screenshot shows the 'Proxy HTTP' configuration page with the 'Reglas de acceso' section. It features a '+ Añadir nuevo/a' button, a search bar with a 'BUSCAR' button, and a table of rules. The table has four columns: 'Período de tiempo', 'Origen', 'Decisión', and 'Acción'. The rules are as follows:

Período de tiempo	Origen	Decisión	Acción
08:00-16:00 Días laborables	Objeto: Celulares	Aplicar el perfil 'Oficina'	[Icons: delete, edit, refresh, up, down]
08:00-16:00 Días laborables	Objeto: Administrativo Financiero	Aplicar el perfil 'Oficina'	[Icons: delete, edit, refresh, up, down]
08:00-16:00 Toda la semana	Objeto: Investigacion	Aplicar el perfil 'Oficina'	[Icons: delete, edit, refresh, up, down]
08:00-16:00 Toda la semana	Objeto: Secretaria Pleno	Aplicar el perfil 'Oficina'	[Icons: delete, edit, refresh, up, down]
08:00-16:00 Días laborables	Objeto: Juridico	Aplicar el perfil 'Oficina'	[Icons: delete, edit, refresh, up, down]
08:00-16:00 Días laborables	Objeto: Prevencion	Aplicar el perfil 'Oficina'	[Icons: delete, edit, refresh, up, down]
Siempre	Cualquiera	Permitir todo	[Icons: delete, edit, refresh, up, down]

At the bottom right of the table, there is a dropdown menu set to '10', the text 'Página 1', and navigation icons for back, forward, and search.

Ejemplo configuración de acceso al proxy

Cualquiera podrá acceder sin restricciones durante el fin de semana, ya que se ha establecido dentro de las reglas de acceso la opción de la misma para que solo actúe de lunes a viernes en horario de oficina, se aplicado el perfil oficina a cada uno de los objetos de la red el cual se describirá más adelante.

Filtrado de contenidos con Zentyal

Zentyal permite el filtrado de páginas web en base a su contenido. Se pueden definir múltiples perfiles de filtrado en *Proxy HTTP* > *Perfiles de Filtrado*.

Proxy HTTP

Perfiles de Filtrado

¿Quieres evitar amenazas como el malware, phishing y los bots? Obtén la edición [Small Business](#) o [Enterprise](#) que mantendrán tus reglas de Filtrado de Contenidos siempre actualizadas.

+ Añadir nuevo/a

BUSCAR

Nombre	Configuración	Acción
defecto		
lan		
dmz		
Oficina		

10

Perfiles de filtrado para los diferentes objetos de red o grupos de usuarios

Accediendo a la *Configuración* de estos perfiles, podremos especificar diversos criterios para ajustar el filtro a nuestros certificados. En la primera pestaña podemos encontrar los *Umbral de contenido* y el filtro del antivirus. Para que aparezca la opción de antivirus, el módulo *Antivirus* debe estar instalado y activado.

Perfiles de Filtrado > Oficina

Configuración Reglas de dominios y URLs Categorías de dominios Tipos MIME Extensiones de archivo

Umbral de filtrado de contenido

Umbral:
Esto especifica cuan estricto es el filtro

Filtrar virus

Usar antivirus:

Configuración del perfil

Estos dos filtros son dinámicos, es decir analizarán cualquier página en busca de palabras inapropiadas o virus. El umbral de contenidos puede ser ajustado para ser más o menos estricto, esto influirá en la cantidad de palabras inapropiadas que permitirá antes de rechazar una página.

En la siguiente pestaña *Reglas de dominios y URLs* podemos decidir de forma estática que dominios estarán permitidos en este perfil. Podemos decidir *Bloquear sitios especificados sólo como IP*, para evitar que alguien pueda evadir los filtros de dominios aprendiendo las direcciones IP asociadas. Así mismo con la opción *Bloquear dominios y URLs no listados* podemos decidir si la lista de dominios más abajo se comporta como una *blacklist* o una *whitelist*, es decir, si el comportamiento por defecto será aceptar o denegar una página no listada.

Perfiles de Filtrado > Oficina

Configuración **Reglas de dominios y URLs** Categorías de dominios Tipos MIME Extensiones de archivo

Configuración del filtrado de dominio

Bloquear dominios y URLs no listados:
Si esta opción está habilitada, cualquier dominio o URL que no esté en la sección *Reglas de dominios*, ni en *Ficheros de listas de dominios* debajo será prohibido.

Bloquear sitios especificados sólo como IP:

CAMBIAR

Reglas de dominios y URLs

+ Añadir nuevo/a

BUSCAR

Dominio o URL	Decisión	Acción
farolatino.com	Denegar	   
mixplay.tv	Denegar	   
zgncdn.com	Denegar	   
farmville.com	Denegar	   
sambatech.com.br	Denegar	   
liquidplatform.com	Denegar	   
verisign.com	Denegar	   
sinmiedosec.com	Denegar	   
20minutos.es/	Denegar	   
facebook.net	Denegar	   

10 Página 1 de 3    

Reglas de dominios y URLs

Finalmente, en la parte inferior, tenemos la lista de reglas, donde podremos especificar los dominios que queremos aceptar o denegar.

Para usar los filtros por *Categorías de dominios* debemos, en primer lugar, cargar una lista de dominios por categorías. Configuraremos la lista de dominios para el Proxy desde *Proxy HTTP > Listas por categorías*.

Nombre	Archivo	Acción
shallalist	shallalist	

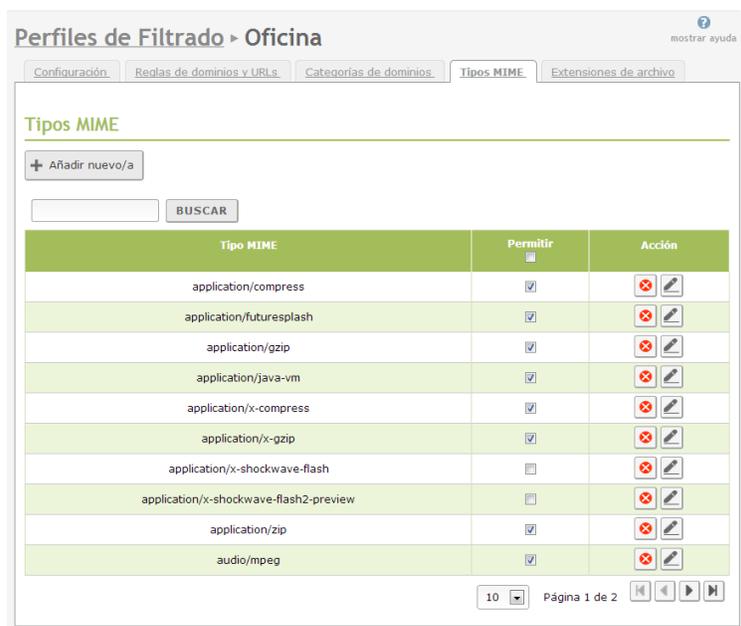
Lista por categorías

Una vez hayamos configurado la lista, podemos seleccionar que categoría en concreto deseamos permitir o denegar desde la pestaña *Categorías de dominios* del filtro.

Categoría	Fichero de listas	Fichero presente	Decisión	Acción
socialnet	shallalist	✓	Denegar todo	

Denegando toda la categoría de redes sociales

En las dos pestañas restantes podemos decidir los tipos de contenido o ficheros que serán aceptados por este perfil, ya sea por tipo MIME o por extensión de fichero. Los tipos MIME son un identificador de formato en Internet, por ejemplo *application/pdf*.



Filtro de tipos MIME

Como podemos ver en la imagen, la propia columna *Permitir* tiene una casilla donde podremos elegir si el comportamiento por defecto será denegar todos o aceptar todos los tipos.

http://en.wikipedia.org/wiki/Mime_type

Contamos con una interfaz similar para las extensiones de ficheros descargados mediante nuestro proxy:



Permitiendo los ficheros con las extensiones descritas.

Normalmente cada regla tiene un *Origen* y un *Destino* que pueden ser *Cualquiera*, una *Dirección IP* o un *Objeto* en el caso que queramos especificar más de una dirección IP o direcciones MAC. En determinadas secciones el *Origen* o el *Destino* son omitidos ya que su valor es conocido *a priori*; será siempre Zentyal tanto el *Destino* en *Tráfico de redes internas a Zentyal* y *Tráfico de redes externas a Zentyal* como el *Origen* en *Tráfico de Zentyal a redes externas*.

Además cada regla siempre tiene asociado un *Servicio* para especificar el protocolo y los puertos (o rango de puertos). Los servicios con puertos de origen son útiles para reglas de tráfico saliente de servicios internos, por ejemplo un servidor HTTP interno, mientras que los servicios con puertos de destino son útiles para reglas de tráfico entrante a servicios internos o tráfico saliente a servicios externos. Cabe destacar que hay una serie de servicios genéricos que son muy útiles para el cortafuegos como *Cualquiera* para seleccionar cualquier protocolo y puertos, *Cualquiera TCP* o *Cualquiera UDP* para seleccionar cualquier protocolo TCP o UDP respectivamente.

El parámetro de mayor relevancia será la *Decisión* a tomar con las conexiones nuevas. Zentyal permite tomar tres tipos distintos de decisiones:

- Aceptar la conexión.
- Denegar la conexión ignorando los paquetes entrantes y haciendo suponer al origen que no se ha podido establecer la conexión.
- Registrar la conexión como un evento y seguir evaluando el resto de reglas. De esta manera, a través de *Mantenimiento* > *Registros* -> *Consulta registros* -> *Cortafuegos* podemos ver las conexiones que se están produciendo.

Las reglas son insertadas en una tabla donde son evaluadas desde el principio hasta el final (desde arriba hacia abajo), una vez que una regla acepta una conexión, no se sigue evaluando el resto. Una regla genérica al principio, puede hacer que otra regla más específica posterior no sea evaluada. Es por esto por lo que el orden de las reglas en las tablas es muy importante. Existe la opción de aplicar un *no lógico* a la evaluación de miembros de una regla con *Coincidencia Inversa* para la definición de políticas más avanzadas.

Añadiendo un/a nuevo/a regla

Decisión:

Origen: Coincidencia inversa:

Servicio: Coincidencia inversa:

Si la selección inversa está marcada, la regla será aplicada cualquier servicio excepto el seleccionado

Descripción: Opcional

Creando una nueva regla en el firewall

Por ejemplo, si queremos registrar las conexiones a un servicio, primero tendremos la regla que registra la conexión y luego la regla que acepta la conexión. Si estas dos reglas están en el orden inverso, no se registrará nada ya que la regla anterior ya acepta la conexión. Igualmente, si queremos restringir la salida a Internet, primero denegaremos explícitamente los sitios o los clientes y luego permitiremos la salida al resto, invertir el orden daría acceso a todos los sitios a todos los *hosts*.

Por omisión, la decisión es siempre denegar las conexiones y tendremos que añadir reglas que las permitan explícitamente. Hay una serie de reglas que se añaden automáticamente durante la instalación para definir una primera versión de la política del cortafuegos: se permiten todas las conexiones salientes hacia las redes externas, Internet, desde el servidor Zentyal (en *Tráfico de Zentyal a redes externas*) y también se permiten todas las conexiones desde las redes internas hacia las externas (en *Tráfico entre redes internas y de redes internas a Internet*). Además cada módulo instalado añade una serie de reglas en las secciones *Tráfico de redes internas a Zentyal* y *Tráfico de redes externas a Zentyal* normalmente permitiendo las conexiones desde las redes internas pero denegándola desde las redes externas. Esto ya se hace implícitamente, pero facilita la gestión del cortafuegos puesto que de esta manera para permitir el servicio solamente hay que cambiar el parámetro *Decisión* y no es necesario crear una regla nueva. Destacar que estas reglas solamente son añadidas durante el proceso de instalación de un módulo por primera vez y no son modificadas automáticamente en el futuro.

Finalmente, existe un campo opcional *Descripción* para comentar el objetivo de la regla dentro de la política global del cortafuegos.