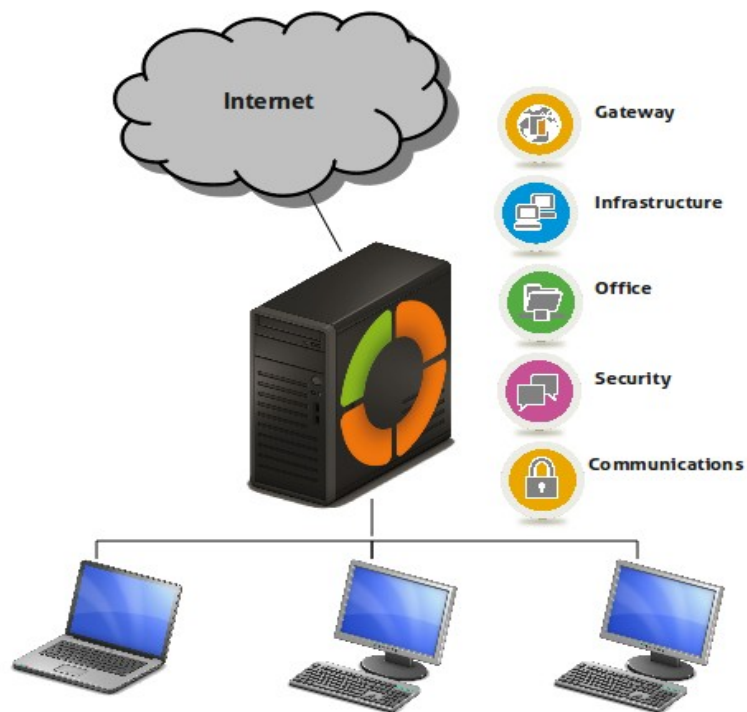


SRC. IES Haría

UT7. Actividad 3

Zentyal gateway/firewall





Este texto se distribuye bajo licencia:

Creative Commons

Reconocimiento-CompartirIgual 3.0

Usted es libre de:

- copiar, distribuir y comunicar públicamente la obra
- hacer obras derivadas

Bajo las condiciones siguientes:



Reconocimiento. Debe reconocer y citar al autor original.



Compartir bajo la misma licencia. Si altera o transforma esta obra, o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta.

Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra.

Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor

Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior.

[<http://creativecommons.org/licenses/by-sa/3.0/es>]

En esta práctica configuraremos Zentyal como puerta de enlace o *gateway* y como *cortafuegos* que nos permite definir reglas para gestionar el tráfico entrante y saliente tanto del servidor como de la red interna. Vamos a empezar viendo como Zentyal organiza la red para a continuación llevar a cabo un caso práctico

Zentyal Gateway. Conceptos

Para ayudar en la configuración del cortafuegos, existen dos módulos que facilitan la gestión de objetos y servicios de red.

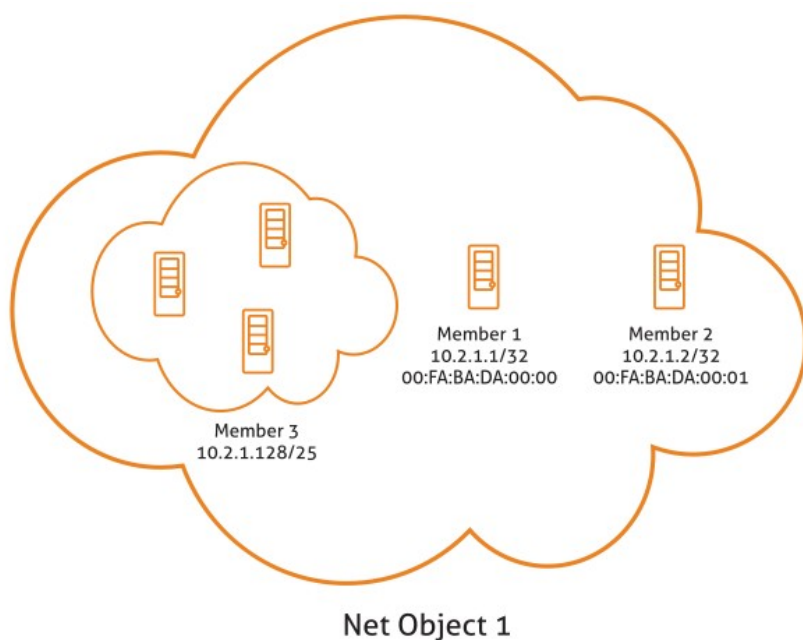
Además Zentyal permite garantizar la calidad del servicio, configurando que tráfico tiene prioridad frente a otro o incluso limitar la velocidad en algún caso, como podría ser el P2P.

Abstracciones de red de alto nivel en Zentyal

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, podemos dar un nombre reconocible a una dirección IP o a un grupo de ellas. En lugar de definir la misma regla en el cortafuegos para cada una de las direcciones IP, simplemente bastaría con **definirla para el objeto** de red que contiene las direcciones.




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

[+ Añade nuevo](#)

Nombre	Miembros	Action
DMZ		 
Guest		 
IT		 
Ventas		 

10 ▼ Página 1    

Objetos de la red

Cada uno de estos **objetos** se compondrá de una serie de **miembros** que podremos modificar en cualquier momento. Los miembros tendrán al menos los siguientes valores: *Nombre*, *Dirección IP* y *Máscara de red*. La *Dirección MAC* es opcional y lógicamente sólo se podrá utilizar para miembros que representen una única máquina.

Objetos ► marketing [\(mostrar ayuda\)](#)

Editando miembro

Nombre:

Dirección IP: CIDR /

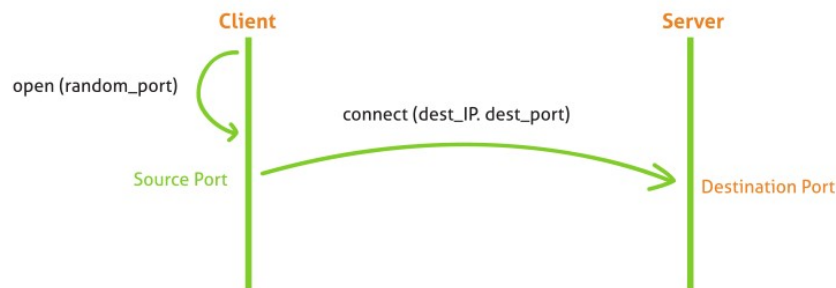
Dirección MAC:
Opcional

En las secciones de la configuración de Zentyal donde podamos usar objetos (como DHCP o Cortafuegos) dispondremos de un menú embebido que nos permitirá crear y configurar objetos sin necesidad de acceder expresamente a esta sección de menú.

Servicios de red

Los **Servicios de red** son la manera de representar los protocolos (TCP, UDP, ICMP, etc) y puertos usados por una aplicación.

La utilidad de los servicios es similar a la de los objetos, nos permitirán en este caso identificar un conjunto de puertos por el nombre de la aplicación que los usa.



Conexión de un cliente a un servidor

Pongamos como ejemplo la **navegación web**. El puerto más habitual es el de HTTP, 80/TCP. Pero además también tenemos que contar con el de HTTPS 443/TCP y el alternativo 8080/TCP.

Si queremos habilitar o denegar el tráfico web no tenemos que aplicar una regla que afecte a la navegación web a **cada uno de los puertos**, sino al **servicio** que la representa y 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 podido definir adicionalmente.

Para cada servicio podemos ver su *Nombre*, *Descripción* y un indicador de si es *Interno* o no. Un servicio es *Interno* si los puertos configurados para dicho servicio se están usando **en el mismo servidor**. Además 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.

El protocolo puede ser TCP, UDP, ESP, GRE o ICMP. También existe un valor TCP/UDP para poder añadir de una sola vez un puerto que se use en ambos protocolos, como en el caso de DNS.

Servicios [\(mostrar ayuda\)](#)

Lista de servicios

[+ Añade nuevo](#)

Nombre del servicio	Descripción	Interno	Configuración	Action
FTP	Zentyal FTP Server	<input checked="" type="checkbox"/>		
RADIUS	Zentyal RADIUS system	<input checked="" type="checkbox"/>		
any	any protocol and port	<input type="checkbox"/>		
any TCP	any TCP port	<input type="checkbox"/>		
any UDP	any UDP port	<input type="checkbox"/>		
dhcp	--	<input checked="" type="checkbox"/>		
dns	Domain Name Service	<input type="checkbox"/>		
eBox administration	Zentyal Administration Web Server	<input checked="" type="checkbox"/>		
http	--	<input checked="" type="checkbox"/>		
ldap	--	<input checked="" type="checkbox"/>		

10 ▼ Página 1 de 2

Encaminamiento

La **puerta de enlace** o *gateway* es el *router* por omisión para las conexiones cuyo destino no está en la red local. Es decir, si el sistema no tiene definidas rutas estáticas o si ninguna de éstas coincide con una transmisión a realizar, ésta se hará a través de la puerta de enlace.

Para configurar una puerta de enlace en Zentyal se utiliza **Red ► Puertas de enlace**, que tiene los siguientes parámetros configurables.

Añadiendo una nueva puerta de enlace

Habilitado: ☒

Nombre:

Dirección IP:

Interfaz: Interfaz conectada a esta puerta de enlace

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

Predeterminado: ☐

Habilitado:

Indica si realmente esta puerta de enlace es efectiva o está desactivada.

Nombre:

Nombre por el que identificaremos a la puerta de enlace.

Dirección IP:

Dirección IP de la puerta de enlace. Esta dirección debe ser directamente accesible desde la máquina que contiene Zentyal, es decir, sin otros enrutamientos intermedios.

Interfaz:

Interfaz de red conectada a la puerta de enlace. Los paquetes que se envíen a la puerta de enlace se enviarán a través de esta interfaz.

Peso

Cuanto mayor sea el peso, más paquetes se enviarán por esa puerta de enlace si activamos el balanceo de tráfico.

Predeterminado

Si esta opción está activada, esta será la puerta de enlace por defecto.

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 la interfaz de red que conecta la máquina con el *router* debe marcarse como **Externo (WAN)** para permitir al cortafuegos establecer unas políticas de filtrado más estrictas para las conexiones procedentes de fuera.

Interfaces de Red [\(mostrar ayuda\)](#)

eth0 eth1 **eth2** eth3

Nombre:

Método:

Externo (WAN): ☒ Comprueba si estás usando Zentyal como gateway y este interfaz está conetado a tu router a Internet

Dirección IP:

Máscara de red:

- La política para las interfaces **externas** es **denegar todo** intento de conexión a Zentyal.
- 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 en Zentyal. Cada vez que añadimos un módulo se añaden, automáticamente, reglas al cortafuegos para permitir estas conexiones, aunque siempre pueden ser modificadas posteriormente por el administrador.
- La configuración predeterminada tanto para la **salida de las redes internas** como **desde el propio servidor** es permitir toda clase de conexiones.



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

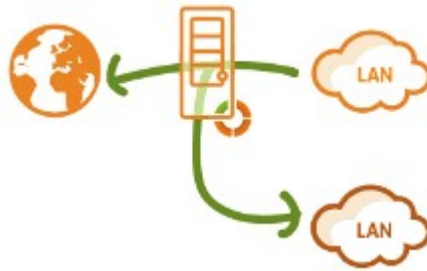
Tipos de reglas

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 en Zentyal desde la red local).



- *Tráfico entre redes internas y de redes internas a Internet* (ejemplo: restringir el acceso a todo Internet o determinadas direcciones a unas direcciones internas o restringir la comunicaciones entre las subredes internas).



- *Tráfico saliente de Zentyal* (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).



- Reglas añadidas por los servicios de Zentyal



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

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 de reglas del cortafuegos

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.

Además cada regla siempre tiene asociado un **Servicio** para especificar el **protocolo** y los **puertos** (o rango de puertos).

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 sobre conexiones se están produciendo.

Las reglas son insertadas en una tabla donde son evaluadas desde el principio hasta el final, aplicándose la primera que se cumpla, por lo que el orden de definición de las reglas es importante.

Añadiendo una nueva regla

The screenshot shows the 'Add new rule' form in Zentyal. It includes the following fields and options:

- Decisión:** A dropdown menu set to 'DENY'.
- Origen:** A dropdown menu set to 'Cualquiera'.
- Destino:** Two dropdown menus, the first set to 'Objeto destino' and the second set to 'IT'.
- Servicio:** A dropdown menu set to 'ssh'.
- Inverse match:** An unchecked checkbox.
- Descripción:** A text input field containing 'No permitir ssh a máquinas de IT'. Below the field is the label 'Opcional'.
- Buttons:** 'Añadir' and 'Cancelar' at the bottom.

Below the 'Inverse match' checkbox, there is a note: 'Si la selección inversa está marcada, la regla será aplicada cualquier servicio excepto el seleccionado'.

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

Redirección de puertos con Zentyal

Las redirecciones de puertos de destino se configuran en **Cortafuegos ▶ Redirecciones de puertos**.

Para configurar una redirección hay que establecer:

- La **Interfaz** donde se **recibe el tráfico** sobre el que se va a hacer la traducción.
- El *Destino original* (que puede ser el servidor Zentyal, una dirección IP o un objeto)
- El *Puerto de destino original* (que puede ser *Cualquiera*, un *Puerto determinado* o un *Rango de puertos*)
- El *Protocolo* y el *Origen* (que también puede ser *Cualquiera*, una *Dirección IP* o un *Objeto*).
- Además estableceremos la dirección IP de *Destino* y finalmente

- El *Puerto* donde la máquina destino recibirá las peticiones, que puede ser el mismo que el original o no.
- Existe también un campo opcional de *Descripción* para aclarar el propósito de la regla.

Redirecciones de puertos

Añadiendo un/a nuevo/a redirección

Interfaz:

Destino original:

Protocolo:

Puerto de destino original:

Origen:

IP Destino:

Puerto:

Remplazar la dirección de origen: ☐

Reemplaza la dirección de origen inicial de la conexión con la dirección de Zentyal. Esto puede ser necesario cuando el destino no tiene una ruta de retorno o tiene reglas de firewall restrictivas

Registro: ☒

Registrar conexiones redirigidas nuevas

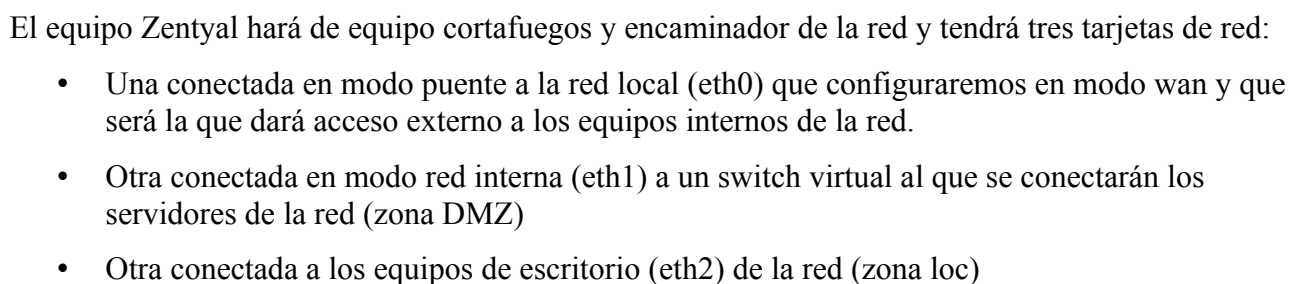
Descripción:

Opcional

En el ejemplo de la imagen se redireccionan las peticiones de cualquier máquina externa a la interfaz externa de Zentyal por el protocolo TCP al puerto 8080 al servidor web de la máquina interna con IP 10.10.10.10

El objetivo de la práctica es simular un caso típico real en el que tenemos una serie de equipos de escritorio de la organización, los servidores de la misma y una máquina que hace de encaminador y cortafuegos de la red local.

Crearemos en nuestro equipo mediante máquinas virtuales el siguiente esquema de red.



1.1. Equipo Zentyal:

Accederemos a **red** → **interfaces** y configuraremos cada una de las tarjetas de red. Suponiendo que **eth0** sea la interfaz configurada en la máquina virtual en modo puente que nos da acceso al exterior aplicaremos la siguiente configuración:

Interfaces de Red [\(mostrar ayuda\)](#)

eth0 **eth1**

Nombre: **eth0**

Método: Estático

Externo (WAN): ☒ Marque aquí si está usando

Dirección IP: 192.168.1

Máscara de red: 255.255.255.0

Cambiar

Habilitaremos **Externo(wan)** de esa forma Zentyal aplicará una configuración predeterminada para dicha interfaz; limitando el tráfico entrante y utilizando dicha interfaz para el acceso externo.

Nota: Al cerrar todo el tráfico entrante no podremos acceder via web a la administración de Zentyal desde nuestro equipo hasta que no habilitemos dicho tráfico en el cortafuegos. De momento accederemos directamente desde la máquina virtual.

El resto de interfaces las configuraremos según los datos del esquema anterior, pero sin habilitar **Externo(WAN)**.

Interfaces de Red [\(mostrar ayuda\)](#)

eth0 **eth1** **eth2**

Nombre: eth2

Método: Estático

Externo (WAN): ☐ Marque aquí si está usando Ze

Dirección IP: 192.168.10.1

Máscara de red: 255.255.255.0

Cambiar

Nota: recuerda hacer clic en guardar cambios para que se aplique la nueva configuración de red.

No olvides configurar la puerta de enlace (**red** → **puerta de enlace:** 192.168.1.1)

Configuración de Puertas de Enlace

Puertas de enlace y Proxy **Balanceo de tráfico**

Editando puerta de enlace

Habilitado: ☒

Nombre: 192.168.1.1

Dirección IP: 192.168.1.254

Interfaz: eth0 Interfaz conectada a esta puerta de

Peso: 1 Este campo solo es útil si tiene ma:

Predeterminado: ☒

Marcando la opción de predeterminada esta puerta de enlace será el destino de todos los paquetes salientes tanto desde Zentyal como desde las redes internas.

Para que Zentyal pueda resolver los nombres de las máquinas hemos de añadirle la IP de un servidor de DNS, podemos utilizar el del aula (**red** → **DNS**: 192.168.1.16)

1.2. Equipo Ubuntu Server

Le asignaremos la IP 192.168.0.2 y como puerta de enlace pondremos la IP de Zentyal en dicha red: 192.168.0.1. Configura como servidor de DNS el de la red del aula (192.168.1.16)

1.3. Equipo de escritorio

De forma análoga al caso anterior le asignaremos la IP 192.168.10.2 y como puerta de enlace pondremos la IP de Zentyal en dicha red: 192.168.10.1. Configura como servidor de DNS el de la red del aula (192.168.1.16)

1.4. Comprobación de la red

Con la configuración actual todos los equipos debería poder acceder a Internet debido a las reglas generadas por defecto que habilitan el tráfico interno hacia afuera y que al haber establecido una puerta de enlace externa predeterminada hacia ella se encaminará todo el tráfico saliente.

Si en este punto tienes alguna dificultad asegúrate de que:

- Todas las interfaces de red de las máquinas virtuales están correctamente interconectadas.
- IP, máscara, puerta de enlace e IP del servidor de DNS están bien configurados.
- Prueba a hacer ping entre las máquinas de cada red.

Si tras hacer estas pruebas sigue sin funcionar la red avisa a un compañero o al profesor.

2. Definiendo los objetos de red

Vamos a crear los diferentes objetos y a incluir sus miembros, lo que nos facilitará la creación de reglas en el cortafuegos. Para ello accedemos a **Red** → **objetos** y vamos a crear un objeto para cada una de las redes internas (**dmz** y **loc**)

The screenshot shows the 'Objetos' (Objects) section of the Zentyal web interface. At the top, there is a link '(mostrar ayuda)'. Below it, the heading 'Añadiendo un/a nuevo/a objeto' is displayed. A form with the label 'Nombre:' contains the text 'loc'. Below the form are two buttons: 'Añadir' and 'Cancelar'. Underneath, the section 'Lista de objetos' is shown, featuring a search bar with a 'Buscar' button. Below the search bar is a table with a single row containing the text 'dmz' under the header 'Nombre'.

Como miembros de la red incluimos todos los miembros de la red **192.168.0.0/24** en el objeto **dmz** y todos los miembros de la red **192.168.10.0/24** en el objeto **loc**.

Para cada objeto hacemos clic en **Miembros** se nos abre una ventana en la que podemos definir los miembros de dos formas, como rango de Ips o en formato CIDR, elegimos este último:

Objetos ► dmz [\(mostrar ayuda\)](#)

Añadiendo un/a nuevo/a miembro

Nombre:

Dirección IP: /

Dirección MAC:

Opcional

En este último formato si quisiéramos especificar una única IP la insertaríamos y pondríamos **32** en el último parámetro, si lo que queremos poner es una red completa ponemos la dirección de red y en el último parámetro el número de bits a 1 de la máscara de subred (8 clase A, 16 clase B y **24** clase C)

De forma análoga definimos la red 192.168.10.0/24 como miembro de la zona **loc**.


3. Accediendo a servicios

3.1. Acceso externo a la web de administración de Zentyal

Con la configuración actual, dado que está restringido todo el tráfico entrante externo a Zentyal no podemos acceder a la web de administración de Zentyal desde nuestro equipo (**a2pcxy**) y en general desde cualquier equipo externo.

Comprueba que en efecto introduciendo en un navegador de tu host la url <https://192.168.1.2xy> no puedes acceder a la administración del equipo.

Para habilitarlo accedemos a **Cortafuegos → Filtrado de paquetes**



Reglas de filtrado desde las redes externas a Zentyal

Estas reglas le permiten controlar el acceso desde redes externas a servicio su máquina Zentyal.

! Debe saber que añadiendo reglas a esta sección puede estar comprometer la seguridad de su red, permitiendo el acceso desde redes no confiables, sólo si sabe lo que está haciendo.

[Configurar reglas](#)

En el apartado **Reglas de filtrado desde las redes externas a Zentyal** hacemos clic en **Configurar reglas**.

Filtrado de paquetes ► Desde redes externas hacia Zentyal

Configure Rules

[+ Añadir nuevo/a](#)

Hacemos clic en **añadir nuevo/a**

Filtrado de paquetes ► Desde redes externas hacia Zentyal

Añadiendo un/a nuevo/a regla

Decisión:

Origen:

Servicio: Coincidencia inversa: ☐

Si la selección inversa está marcada, la regla será aplicada cualquier servi

Descripción:

Opcional

Permitimos que desde cualquier equipo externo podamos acceder a la web de administración. Compruébalo intentando acceder desde un navegador de tu equipo.

3.2. Filtrado de paquetes. Habilitando el acceso por SSH a Ubuntu Server desde la zona/objeto loc

Por defecto Zentyal encamina el tráfico de una red a otra, pero el cortafuegos el único tráfico que permite es el saliente hacia Internet, por lo que si intentamos acceder de un equipo de la zona/objeto **loc** a Ubuntu Server (en dmz) el cortafuegos nos bloqueará el acceso (compruébalo). Debemos crear una regla específica que nos lo permita.

Como vamos a definir una regla para permitir tráfico de una red interna a otra seleccionamos en **Firewall** → **Filtrado de paquetes** la opción **Reglas de filtrado para redes internas**:



Añadimos una nueva regla:

Filtrado de paquetes ► **Redes internas**

Añadiendo un/a nuevo/a regla

Decisión: **ACEPTAR**

Origen: **Objeto origen** loc

Destino: **IP Destino** 192.168.0.2 / 32

Servicio: **ssh** Coincidencia inversa: ☐

Si la selección inversa está marcada, la regla será aplicada

Descripción: **Acceso ssh a Ubuntu server desde loc**

Añadir Cancelar

Si ahora ejecutamos en un terminal del equipo de escritorio:

```
$ ssh usuario@192.168.0.2
```

Deberíamos poder acceder por ssh a ubuntu server. Compruébalo.

Actividad no guiada 1. Habilita el acceso por ssh desde Zentyal a Ubuntu Server.

3.3. Redireccionamiento de puertos. Acceso externo a servidor web en Ubuntu Server

Vamos a redireccionar el puerto 8080 externo en Zentyal de forma que nos redirija al puerto 80 de Ubuntu Server. Accedemos a **Cortafuegos** → **Redirecciones de puertos** y hacemos clic en **Añadir nuevo**.

Se nos abrirá un menú en el que introduciremos las opciones del redireccionamiento de puertos:

Redirecciones de puertos

Añadiendo un/a nuevo/a redirección

Interfaz:

Destino original:

Protocolo:

Puerto de destino original:

Origen:

IP Destino:

Puerto:

Reemplazar la dirección de origen: ☐

Reemplaza la dirección de origen inicial de la < necesario cuando el destino no tiene una ruta

Registro: ☐

Registrar conexiones redirigidas nuevas

Descripción:
Opcional

Después de guardar los cambios, si todo ha ido bien, si desde nuestro equipos accedemos a la URL <http://192.168.1.2xy:8080> deberíamos acceder al servidor web de Ubuntu server.

Actividad no guiada 2. Redirecciona el puerto 2222 al 22 de Ubuntu Server para que podamos acceder por ssh desde nuestro equipo a la máquina interna. Comprueba que funciona.

3.4. Restringiendo el tráfico en la zona/objeto dmz

Por defecto Zentyal habilita todo el tráfico saliente de cualquier red interna, esta no es buena política para la zona desmilitarizado (dmz) en la que se ubican los servidores de las organizaciones, en lugar de eso debería estar denegado todo menos el tráfico estrictamente necesario.

Actividad no guiada 3. Regla 1: Cierra todo el tráfico saliente a los equipos miembros del **dmz**. **Regla 2:** permite en **dmz** el tráfico hacia afuera de DNS necesario para la resolución de nombres. Ten cuidado con el orden en que pones las dos reglas anteriores.

Actividad no guiada 4. Crea el servicio **cpaquetes** y asócialo al puerto **TCP 3142**. Crea una regla que permita a Ubuntu Server acceder al servicio externo cpaquetes del equipo 192.168.1.17 para que pueda actualizar e instalar paquetes. Ten cuidado del orden en que se aplica la regla

Cuando hayas terminado avisa al profesor para que corrija la práctica.