Guía 4 – Instalación y configuración de los servicios de ruteo y firewall

Contenido de la Guía

Objetivo general de la guía.

- Activar la función de ruteo de paquetes entre las interfaces de red eth0, eth1 y eth2
- Crear reglas de filtrado de paquetes en el firewall para controlar el tráfico de red generado por los protocolos ICMP, TCP y UDP

Objetivos específicos.

- Crear servicios para aplicar reglas de filtrado a servicios de red LAN
    - Servicio con un solo protocolo y un solo puerto, (Ejemplo SSH)
    - Servicio con un solo protocolo y varios puertos. (Ejemplo FTP)
    - Servicio de un solo protocolo y un rango de puertos (Ejemplo VNC)
    - Servicio con dos protocolos y cada uno con un solo puerto (Ejemplo DNS)
    - Servicio con varios protocolos y cada una con un solo puerto (Ejemplo SMB, AD)
- Definir las reglas de filtrado para el tráfico que llega al servidor srvext. (ACCEPT – DENY)
- Escribir el orden de ejecución de reglas de filtrado, usando al final bloqueo de todo el resto de paquetes
- Definir las reglas de filtrado para el tráfico que existirán entre las redes LAN1 y LAN2

Nomenclatura de la guía:

En esta guía se ha utilizado el siguiente formato:

- Fuente courrier en negrita para los comandos que deben digitarse, por ejemplo:
  `root@front-end:~# ps aux |grep sshd`
- Texto con resaltado en amarillo, para la información que debe visualizar cuando realice algún procedimiento o comando. Puede contener color rojo dentro del fondo amarillo.

```
root@front-end:~# mcedit /etc/resolv.conf
search empresay.com.sv
nameserver   192.168.60.2
```

- Las notas o consideraciones se destacan con: **Nota:**

La información aquí presentada ha sido creada por Víctor Cuchillac (padre), cualquier uso o referencia debe citarse al autor.

I. Indicaciones sobre la guía

1.1 Descripción del escenario global.

Usted y su equipo de trabajo han sido contratados para instalar y configurar varios servicios de infraestructura de forma que los usuarios de la EMPRESAY puedan acceder de forma segura a los servicios de la red (Intranet, BD, Servidor de archivos, etc.), utilizando el Appliance Zentyal 4.X más estable.

Para realizar el macro proyecto se realizarán las siguientes tareas.

- Instalación del appliance Zentyal 4.X (versión más reciente)
- Diseño de la red IPv4.
- Consideraciones de asignación dinámica para los clientes y servidores
- Instalación y configuración del servicio DHCP
- Crear pool para clientes (estará desactivado después de las pruebas)
- Configuración de los clientes.
- Verificación de la configuración.

Nota: Por aspectos de aprendizaje se utilizarán en esta guía direcciones IPv4 dinámicas tipo reservadas para los equipos de la red LAN1. En las empresas de la vida real los servidores poseen direcciones IP estáticas.

En la siguiente figura se ilustra el escenario de red para la guía

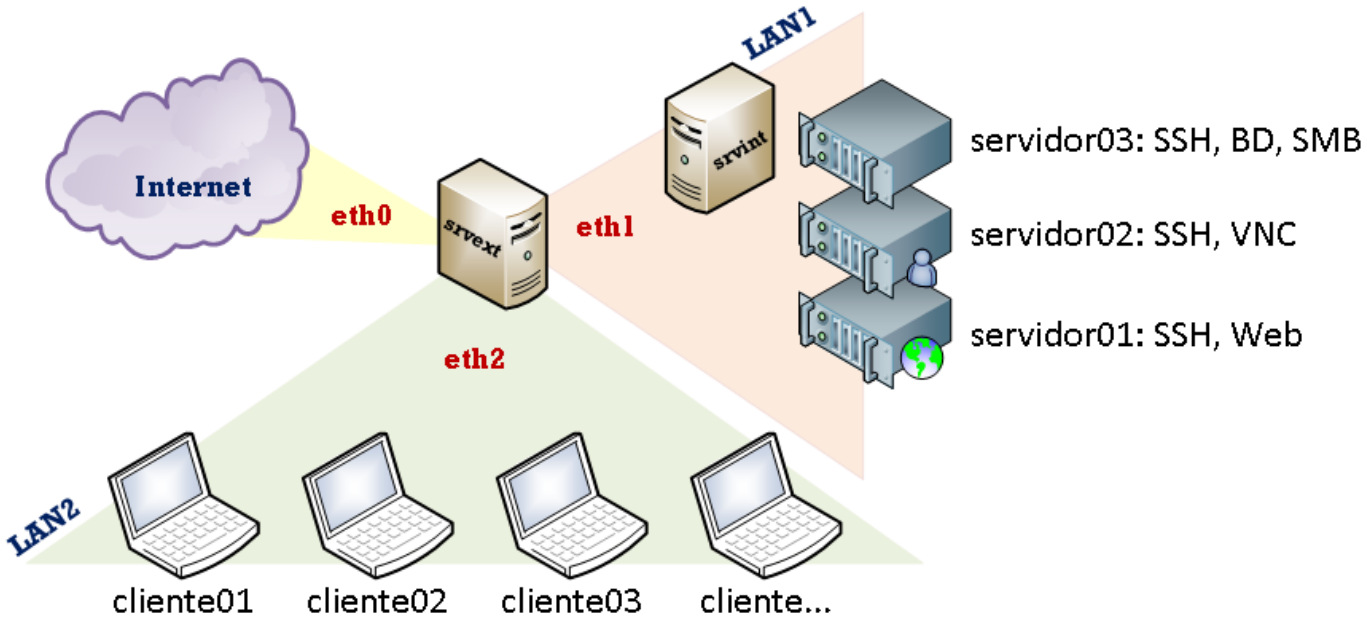


Figura 1 – Diagrama del escenario de la nube privada y pública de la EMPRESAY.

Servicios y clientes en los equipos a utilizar			
ID	**Nombre Equipo**	**Servicios / Software**	**S.O.**

1	srvext	DHCP, Router, Firewall, NAT, VPN	Zentyal 4.X
2	servint	DNS, AD, FS	Zentyal 4.X
3	servidor01	Servidor SSH, Servidor Web	CorePlus 7.X (Plus)
4	servidor02	Servidor SSH, Servidor VNC,	CorePlus 7.X (Plus)
5	servidor03	Servidor SSH, Servidos SMB, Servidor MySQL	CorePlus 7.X (Plus)
6	cliente01	Cliente SSH, Cliente SCP, Cliente VNC, Cliente Web, Cliente MySQL, Cliente SMB	CorePlus 7.X (Plus)
7	cliente02	Cliente SSH, Cliente SCP, Cliente VNC, Cliente Web, Cliente MySQL, Cliente SMB	CorePlus 7.X (Plus)
8	cliente03	Cliente SSH, Cliente SCP, Cliente VNC, Cliente Web, Cliente MySQL, Cliente SMB	CorePlus 7.X (Plus)
9	cliente04	Cliente SSH, Cliente SCP, Cliente VNC, Cliente Web, Cliente MySQL, Cliente SMB	CorePlus 7.X (Plus)
10	cliente05	Cliente SSH, Cliente SCP, Cliente VNC, Cliente Web, Cliente MySQL, Cliente SMB	Windows 7, 8, 10
11	cliente06	Cliente SSH, Cliente SCP, Cliente VNC, Cliente Web, Cliente MySQL, Cliente SMB	Windows 7, 8, 10
12	cliente07	Cliente SSH, Cliente SCP, Cliente VNC, Cliente Web, Cliente SMB	Android x86

Cuadro 1 – Descripción de los equipos del escenario de la EMPRESAY

La red IPv4 de la EMPRESAY para cada equipo se detalla en el siguiente cuadro:

Direcciones MAC e IPv4 para los equipos de la EMPRESAY				
ID	**Equipo**	**Dirección MAC**	**Tipo IPv4**	**IPv4**
1	serext	02:AA:E0:Y:X:01	Dinámica	La del ISP
		02:AA:E1:Y:X:02	Estática	192.168.**60+Y**.1
		02:AA:E2:Y:X:03	Estática	192.168.**50**+Y.1
2	srvint	02:BB:00:Y:X:00	Estática	192.168.**60**+Y.2
3	servidor01	02:BB:00:Y:X:01	Reservada	192.168. **60+Y**.11
4	servidor02	02:BB:00:Y:X:02	Reservada	192.168. **60+Y**.12
5	servidor03	02:BB:00:Y:X:03	Reservada	192.168. **60+Y**.13
6	cliente01	02:CC:00:Y:X:01	Reservada	192.168.**50**+Y.11
7	cliente02	02:CC:00:Y:X:02	Dinámica	192.168.**50**+Y.12
8	cliente03	02:CC:00:Y:X:03	Dinámica	192.168.**50**+Y.13
9	cliente04	02:CC:00:Y:X:04	Dinámica	192.168.**50**+Y.14
10	cliente05	02:CC:00:Y:X:05	Dinámica	192.168.**50**+Y.15
11	cliente06	02:CC:00:Y:X:06	Dinámica	192.168.**50**+Y.16
12	cliente07	02:CC:00:Y:X:06	Dinámica	192.168.**50**+Y.17

Cuadro 2 – Datos generales de red para el escenario de la EMPRESAY según equipo de trabajo

Nota: Para garantizar que no exista una dirección MAC, una IPv4, un host y un dominio duplicado en la red del laboratorio, se utilizará la siguiente nomenclatura:

- Y = representa el número del grupo de trabajo, y se utilizan dos dígitos

- X = representa el número del estudiante, se utilizan dos dígitos

Ejemplos:	**Grupo 7 y estudiante 1**	**Grupo 05 y estudiante 2**	**Grupo 11 y estudiante 3**
02:BB:00:**Y**:**X**:01	02:BB:00:**07**:**01**:01	02:BB:00:**05**:**02**:01	02:BB:00:**11**:**03**:01
empresa**Y**.com.sv	empresa**07**.com.sv	empresa**05**.com.sv	empresa**11**.com.sv
192.168.**50+Y**.3	192.168.5**7**.3	192.168.5**5**.3	192.168.**61**.3

Nota: Imprima o elabore en una hoja con los datos de grupo y número de alumno, de forma que no halla consultas redundantes, pérdida de tiempo o errores ocasionados por la mala configuración de la red en el laboratorio.

Servicios y clientes en los equipos a utilizar				
ID	**Equipo / Nombre de host**	**Dirección IPv4**	**Alias**	**FQDN**
1	srvext	192.168.50+Y.1 192.168.60+Y.1	router01	srvext.empresay.com.sv
2	servint	192.168.**60+Y**.2	fs01	servint.empresay.com.sv
3	servidor01	192.168. **60+Y**.11	www	servidor01.empresay.com.sv
4	servidor02	192.168. **60+Y**.12	bd01	servidor02.empresay.com.sv
5	servidor03	192.168. **60+Y**.13	fs02	servidor03.empresay.com.sv

Cuadro 3 – Datos de resolución para equipos

Servicios y clientes en los equipos a utilizar			
ID	**Equipo**	**FQDN**	**Alias**
1	srvext	srvext.empresay.com.sv	router01
2	servint	servint.empresay.com.sv	fs01
3	servidor01	servidor01.empresay.com.sv	www
4	servidor02	servidor02.empresay.com.sv	vnc
5	servidor03	servidor03.empresay.com.sv	fs02

Cuadro 4 – Datos de resolución para equipos

1.2 Consideraciones Previas

Recursos requeridos:

- Un equipo o MV con servidor **srvext**.
- Un equipo o MV con servidor **srvint**.
- Tres servidores TinyCore 7.X o superior con servicios
- Cuatro clientes TinyCore 7.X o superior con aplicaciones cliente
- Conexión a Internet.
- El servidor srvext deberá tener salida a Internet
- Los servicios DHCP y DNS deberán estar bien configurados, proveyendo todos los datos de la red de la empresa EMPRESAY (sustituir Y por el número de grupo)
- KiTTY para Windows.
- WinSCP o FileZilla para Windows.
- Notepad+++ para Windows (opcional)
- MaSSHandra para Windows (opcional)

Consideraciones:

- Si utiliza máquinas virtuales se utilizará VirtualBox versión 5.X (De preferencia), y para cada equipo se utilizarán las direcciones físicas del cuadro 2.
- Escriba en un papel todas las direcciones IPv4 de su red, utilice el valor de Y con el número de grupo asignado, por ejemplo: Y=grupo01 192.168.50+**Y**.1 = 192.168.168.51.1 (ver cuadro 2)
- La máquina virtual del servidor01 se puede clonar seis veces para obtener de este modo los tres servidores de la red LAN01 y los cuatro clientes de la red LAN02 para el escenario de la EMPRESAY.
- Utilice un fondo de escritorio con el nombre de cada servidor y cliente para identificar mejor cada equipo.
- Verifique que utiliza la dirección MAC para cada grupo y alumno.
- El equipo **srvext** tendrá tres interfaces y Puede configurarse de la siguiente manera:

Configuración 01 para tarjetas en VirtualBox		
Adaptador en VirtualBox	**Alias NIC en Linux**	**Tipo conexión VirtualBox**
Adaptador 1	eth0	Bridge a la tarjeta Ethernet de la computadora
Adaptador 2	eth1	Bridge a una loopback de Micrososft
Adaptador 3	eth2	Bridge a una loopback de Micrososft
• Este escenario es útil si hay un DHCP en la tarjeta Ethernet de la computadora, también se puede utilizar una tarjeta Wi-Fi, si no existe un portal cautivo (es decir sin que haya necesidad de validarse en una página Web). • Se debe crear una loopback para micrososoft: Win + R, hdwwiz, seleccionar hardware manual, NIC, Seleccionar Microsft, loopback KM-Test • Se debe crear una loopback para Linux (tap0)		

Configuración 02 para tarjetas en VirtualBox		
Adaptador en VirtualBox	**Alias NIC en Linux**	**Tipo conexión VirtualBox**
Adaptador 1	eth0	NAT
Adaptador 2	eth1	Bridge a una loopback de Micrososft
Adaptador 3	eth2	Bridge a una loopback de Micrososft
• Este escenario es útil si hay una configuración de portal cautivo en la red Wifi, o si la comunicación es complicada de realizar • Se debe crear una loopback para micrososoft: Win + R, hdwwiz, seleccionar hardware manual, NIC, Seleccionar Microsft, loopback KM-Test		

• Se debe crear una loopback para Linux (tap0)

Configuración 03 para tarjetas en VirtualBox		
Adaptador en VirtualBox	**Alias NIC en Linux**	**Tipo conexión VirtualBox**
Adaptador 1	eth0	Bridge o NAT
Adaptador 2	eth1	Conexión a LAN interna (lan01)
Adaptador 3	eth2	Conexión a LAN interna (lan02)
• Este escenario es útil si se utiliza una laptop o computadora de escritorio que necesite permisos para instalar dispositivos. • No necesita crear interfaces loopback		

Nota: Si se utilizan el escenario 01 o el escenario 02 se debe crear una interfaz loopback con las direcciones para la red LAN01 y LAN02

Por ejemplo:

```
C:\Users\cuchillac>ipconfig

Configuración IP de Windows

Adaptador de LAN inalámbrica Wi-Fi:

   Sufijo DNS específico para la conexión. . : uni.edu.sv
   Dirección IPv4. . . . . . . . . . . . . . : 10.10.3.223
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . : 10.10.3.254

Adaptador de Ethernet loopback:

   Sufijo DNS específico para la conexión. . :
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.50.155
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Dirección IPv4. . . . . . . . . . . . . . : 192.168.60.155
   Máscara de subred . . . . . . . . . . . . : 255.255.255.0
   Puerta de enlace predeterminada . . . . . :
```

1.3 Escenario de la guía

Usted y su equipo de trabajo han sido contratados para instalar y configurar en la EMPRESAY los servicios de encaminimaiento IP (ruteo) y cortafuegos (firewall). Con el servicio de ruteo se permitirá el tráfico entre las dos redes LAN de la empresa y la Internet, y con el servicio de firewall se cotrolará el tráfico entre las redes de la empresa, proveyedo con esto dos aspectos, El control del ancho de banda de la red y uso efectivo de las comunicaciones y el acceso seguro a los servicios de la LAN1

Para lograr lo anterior será necesario configurar políticas de seguridad basadas en reglas para el filtrado del tráfico de los protocolos ICMP, TCP y UDP para todas las redes LAN de la EMPRESAY. La configuración de las políticas de seguridad relacionadas con las reglas de filtrado se realizará en dos fases:

Primera Fase: Configuración del bloqueo del tráfico y habilitación de los servicios básicos

A. El servidor srvext podrá recibir el siguiente tráfico, caso contrario se bloquearán los paquetes.

- ICMP (ping) desde los servidores de la red LAN1 (sólo los servidores de la empresa).
- ICMP (ping) desde los clientes de la red LAN1 (sólo los autorizados).
- Peticiones DHCP de los servidores de la LAN1
- Peticiones DHCP de los clientes de la LAN2

B. El servidor srvext podrá generar (enviar, comunicarse o utilizar) el siguiente tráfico. Caso contrario se debe bloquear todos los paquetes.

- ICMP (ping) a cualquier red por cualquier NIC.
- Navegar en sitios Web de la Internet utilizando HTTP (salida a Internet)
- Navegar en sitios Web de la Internet utilizando HTTPS (salida a Internet)

C. El servidor srvext podrá permitir el tráfico bidireccional entre las redes LAN1 y LAN2 para los siguientes servicios. Caso contrario bloqueará los paquetes.

- Los servidores de la red LAN1 podrá hacer ping hacia la red LAN2 y equipos fuera de la EMPRESAY.
- Los clientes de la red LAN podrán hacer ping hacia los servidores de la red LAN1.
- Los servidores de la red LAN1 podrá hacer consultas al servidor DNS de la EMPRESAY
- Los clientes de la red LAN2 podrá hacer consultas al servidor DNS de la EMPRESAY
- Los servidores de la red LAN1 podrán navegar en sitios Web fuera de la EMPRESAY
- Los clientes de la red LAN2 podrán navegar en sitios Web externos a la EMPRESAY

D. El servidor srvext no permitirá el tráfico que provenga desde cualquier equipo fuera de la EMPRESAY

En los cuadros No. 5 se muestran las reglas recomendadas.

Segunda Fase: Configuración del bloqueo del tráfico y habilitación de los servicios básicos

E. El servicio web del servidor01 sólo será accedido por el cliente01 y el cliente02. Utilizar el navegador opera. Los demás clientes no podrán ver el contenido de dicho equipo.

F. El servicio SCP (SSH) del servidor01 sólo será accedido por el cliente01 y el cliente02. Utilizar el cliente Filezilla. Los demás clientes no podrán ver el contenido de dicho equipo.

G. El servicio VNC del servidor02 sólo será accedido por el cliente03 y el cliente04. Utilizar el cliente Tiger VNC Viewer. Los demás clientes no podrán ver el contenido de dicho equipo.

H. La base de datos MySQL o mariaDB que se ejecuta en el serviodor03 sólo serán accedidos por el cliente01 y el cliente02. Utilizar el cliente de consola mysql. Los demás clientes no podrán ver el contenido de dicho equipo.

I. El servicio SAMBA (servidor SMB) que se ejecuta en el serviodor03 sólo serán accedidos por el cliente03 y el cliente04. Utilizar el cliente de consola smbclient. Los demás clientes no podrán ver el contenido de dicho equipo.

Las reglas de filtrado se muestran en los siguientes cuadros:

Cuadro 5.1 Reglas de filtrado desde las redes internas a Zentyal (para literal A)				
ID	**Origen**	**Destino**	**Servicio**	**Acción**
a.	Servidores desde la LAN1	srvext	ICMP	Permitir
b.	Clientes desde la LAN2	srvext	ICMP	Permitir
c.	Servidores desde la LAN1	srvext	DHCP	Permitir
d.	Clientes desde la LAN2	srvext	DHCP	Permitir
e.	Cualquier equipo de la red 192.168.60.0	srvext	Web de Zentyal (8443)	Permitir
f.	Cualquier origen	srvext	Cualquier servicio	**Denegar**

Cuadro 5.2 Reglas de filtrado para el tráfico saliente de Zentyal (para literal B)				
ID	**Origen**	**Destino**	**Protocolo/Servicio**	**Acción**
a.	srvext	Cualquier destino	ICMP	Permitir
b.	srvext	Cualquier destino	HTTP	Permitir
c.	srvext	Cualquier destino	HTTPS	Permitir
d.	srvext	Cualquier destino	DHCP	Permitir
e.	srvext	Cualquier destino	Cualquier servicio	**Denegar**

Cuadro 5.3 Reglas de filtrado para el tráfico saliente de Zentyal (para literal C)				
ID	**Origen**	**Destino**	**Protocolo/Servicio**	**Acción**
a.	Servidores LAN1	Cualquier destino	ICMP	Permitir
b.	Servidores LAN1	Clientes LAN2	ICMP	Permitir
c.	Clientes LAN2	Servidores LAN1	ICMP	Permitir
d.	Servidores LAN1	srvint	DNS	Permitir
e.	Clientes LAN2	srvint	DNS	Permitir
f.	Servidores LAN1	Cualquier destino	HTTP	Permitir
g.	Clientes LAN2	Cualquier destino	HTTP	Permitir
h.	Servidores LAN1	Cualquier destino	HTTPS	Permitir
i.	Clientes LAN2	Cualquier destino	HTTPS	Permitir
j.	Cualquier origen	Cualquier destino	Cualquier servicio	**Denegar**

Cuadro 5.4 Reglas de filtrado desde las redes externas a Zentyal (para literal D)				
ID	**Origen**	**Destino**	**Servicio**	**Acción**
a.	Cualquier dirección externa	srvext	Cualquier servicio	**Denegar**

Cuadros No. 5 – Reglas de filtrado para la primera fase del router01

Vea la sección 2.1 de la guía No. 2 para la configuración de las tarjetas de red en Virtualbox

II. Desarrollo de la guía.

1. Verificación de la comunicación en las redes previo al filtrado

Comprobar que exista comunicación entre el srvint y el srvext en la LAN1 en ambos sentidos

```
root@srvext:/home/usuario1# ping 192.168.60.2 -c 3

PING 192.168.60.2 (192.168.60.2) 56(84) bytes of data.
64 bytes from 192.168.60.2: icmp_seq=1 ttl=64 time=1.03 ms
64 bytes from 192.168.60.2: icmp_seq=2 ttl=64 time=0.772 ms
64 bytes from 192.168.60.2: icmp_seq=3 ttl=64 time=0.846 ms

--- 192.168.60.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 0.772/0.883/1.032/0.112 ms

root@srvint:/home/usuario1# ping -c 3 192.168.60.1
PING 192.168.60.1 (192.168.60.1) 56(84) bytes of data.
64 bytes from 192.168.60.1: icmp_seq=1 ttl=64 time=0.832 ms
64 bytes from 192.168.60.1: icmp_seq=2 ttl=64 time=0.891 ms
64 bytes from 192.168.60.1: icmp_seq=3 ttl=64 time=0.834 ms

--- 192.168.60.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 0.832/0.852/0.891/0.036 ms
root@srvint:/home/usuario1#
```

Comprobar que exista comunicación entre el **srvint** y un equipo de la LAN2 en ambos sentidos

```
root@srvext:/home/usuario1# ping 192.168.60.11 -c 3

PING 192.168.50.11 (192.168.50.11) 56(84) bytes of data.
64 bytes from 192.168.50.11: icmp_seq=1 ttl=64 time=1.00 ms
64 bytes from 192.168.50.11: icmp_seq=2 ttl=64 time=0.819 ms
64 bytes from 192.168.50.11: icmp_seq=3 ttl=64 time=0.815 ms

--- 192.168.50.11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 0.815/0.881/1.009/0.090 ms


root@cliente02:/home/tc# ping -c 3 192.168.60.1

PING 192.168.50.1 (192.168.50.1): 56 data bytes
64 bytes from 192.168.50.1: seq=0 ttl=64 time=0.993 ms
64 bytes from 192.168.50.1: seq=1 ttl=64 time=0.803 ms
64 bytes from 192.168.50.1: seq=2 ttl=64 time=1.153 ms

--- 192.168.50.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.803/0.983/1.153 ms
```

Comprobar que exista comunicación entre el **srvint** y un host en Internet

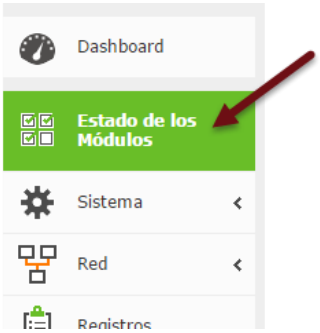
```
root@srvext:/home/usuario1# apt-get install lynx

Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes extras:
  lynx-cur
Se instalarán los siguientes paquetes NUEVOS:
  lynx lynx-cur
0 actualizados, 2 se instalarán, 0 para eliminar y 111 no actualizados.
Necesito descargar 960 kB de archivos.
Se utilizarán 2,570 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] s
Des:1 http://sv.archive.ubuntu.com/ubuntu/ trusty/main lynx-cur amd64 2.8.8pre4-1 [956
kB]
. . .
. . .

Configurando lynx (2.8.8pre4-1) ...
```

El paquete lynx se debe instalar, (Lynx es un navegador Web para consola)

2. Configuración del Firewall

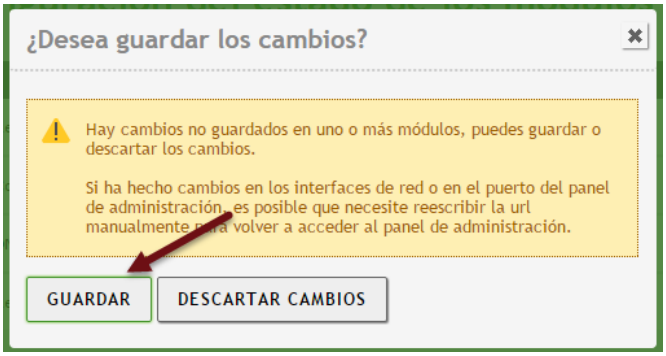
2.1 Activar el Firewall

2.1.1 Seleccionar el menú "Estado de los módulos"

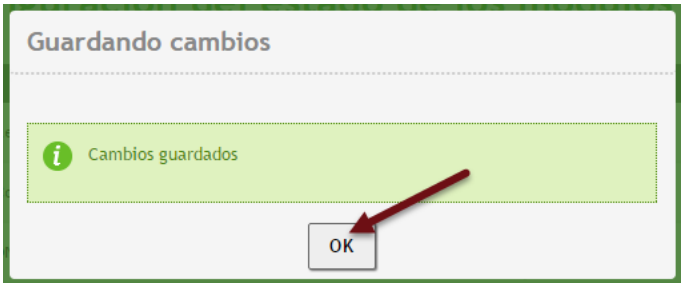


2.1.2 Seleccionar Cortafuegos.

2.1.3 Dar clic en el botón “Guardar”



2.1.4 Confirmar guardar los cambios



2.2 Verificar la comunicación entre redes.

Al activarse el módulo de firewall se han habilitados dos funciones:

- El ruteo, función para permitir el reenvío de paquetes desde una tarjeta de red a otra.
- El firewall, función para bloquear o permitir

2.2.1 Prueba de mensajes ICMP

```
tc@cliente01:~$ ping 192.168.50.1 -c 3
PING 192.168.50.1 (192.168.50.1): 56 data bytes
64 bytes from 192.168.50.1: seq=0 ttl=64 time=0.341 ms
64 bytes from 192.168.50.1: seq=1 ttl=64 time=0.871 ms
64 bytes from 192.168.50.1: seq=2 ttl=64 time=0.918 ms

--- 192.168.50.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.341/0.710/0.918 ms

tc@cliente01:~$ ping 192.168.60.1 -c 3
PING 192.168.60.1 (192.168.60.1): 56 data bytes
64 bytes from 192.168.60.1: seq=0 ttl=64 time=0.363 ms
64 bytes from 192.168.60.1: seq=1 ttl=64 time=0.942 ms
64 bytes from 192.168.60.1: seq=2 ttl=64 time=0.939 ms

--- 192.168.60.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.363/0.748/0.942 ms

tc@cliente01:~$ ping 192.168.60.2 -c 3
PING 192.168.60.2 (192.168.60.2): 56 data bytes
64 bytes from 192.168.60.2: seq=0 ttl=63 time=0.585 ms
64 bytes from 192.168.60.2: seq=1 ttl=63 time=1.503 ms
64 bytes from 192.168.60.2: seq=2 ttl=63 time=1.538 ms
```

```
--- 192.168.60.2 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.585/1.208/1.538 ms

tc@cliente01:~$ ping 10.0.2.15 -c 3
PING 10.0.2.15 (10.0.2.15): 56 data bytes
64 bytes from 10.0.2.15: seq=0 ttl=64 time=0.338 ms
64 bytes from 10.0.2.15: seq=1 ttl=64 time=0.898 ms
64 bytes from 10.0.2.15: seq=2 ttl=64 time=0.866 ms

--- 10.0.2.15 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.338/0.700/0.898 ms

tc@cliente01:~$ ping cuchillac.net -c 3
PING cuchillac.net (50.87.152.212): 56 data bytes
64 bytes from 50.87.152.212: seq=0 ttl=48 time=109.975 ms
64 bytes from 50.87.152.212: seq=1 ttl=48 time=115.812 ms
64 bytes from 50.87.152.212: seq=2 ttl=48 time=116.996 ms

--- cuchillac.net ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 109.975/114.261/116.996 ms
```

2.2.2 Comprobar que se puede navegar en Internet desde el cliente01

Nota: Si no puede navegar en Internet, debe verificar:
En srvext: IPv4 → [eth0] Automática, GW → ISP, DNS → 192.168.60+Y.2
En srvint: IPv4 → 192.168.60+Y.2, GW → 192.168.60.1, DNS → localhost, Reenviador [En el DNS] → DNS ISP
En cliente01: IPv4 → [eth0] Automática, GW → 192.168.50+Y.1 → 192.168.60+Y.2

2.2.3 Comprobación de comunicación de los servicios de red de los clientes

Verifique que funciona el servicio HTTP del servidor01, se debe utilizar http://www.empresay.com.sv


```
tc@cliente02:~$ mysql -h bd01 -u usuario01 -p
Enter password: 123456

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 3
Server version: 10.0.17-MariaDB Source distribution

Copyright (c) 2000, 2015, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| empresay           |
| information_schema |
| test               |
+--------------------+
3 rows in set (0.00 sec)

MariaDB [(none)]>
```

Recuerde que el usuario01 tiene permiso para ingresar desde la red, la contraseña del usuario01 es 123456

3.3 Verificar la comunicación entre redes.

Zentyal tiene cuatro conjuntos de reglas para el filtrado de paquetes IPv4

1. Reglas de filtrado desde las redes internas a Zentyal
2. Reglas de filtrado para las redes internas
3. Reglas de filtrado desde las redes externas a Zentyal
4. Reglas de filtrado para el tráfico saliente de Zentyal

Estos cuatro conjuntos de reglas permiten la comunicación entre la red IPv4 192.168.60.0 y la red IPv4 192.168.50.0
Digite los siguientes comandos para comprobar la comunicación ICMP

```
tc@cliente01:~$ ping 192.168.50.1 -c 3
PING 192.168.50.1 (192.168.50.1): 56 data bytes
64 bytes from 192.168.50.1: seq=0 ttl=64 time=0.341 ms
64 bytes from 192.168.50.1: seq=1 ttl=64 time=0.871 ms
64 bytes from 192.168.50.1: seq=2 ttl=64 time=0.918 ms

--- 192.168.50.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.341/0.710/0.918 ms

tc@cliente01:~$ ping 192.168.60.1 -c 3
PING 192.168.60.1 (192.168.60.1): 56 data bytes
64 bytes from 192.168.60.1: seq=0 ttl=64 time=0.363 ms
64 bytes from 192.168.60.1: seq=1 ttl=64 time=0.942 ms
64 bytes from 192.168.60.1: seq=2 ttl=64 time=0.939 ms

--- 192.168.60.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.363/0.748/0.942 ms

tc@cliente01:~$ ping 192.168.60.2 -c 3
PING 192.168.60.2 (192.168.60.2): 56 data bytes
64 bytes from 192.168.60.2: seq=0 ttl=63 time=0.585 ms
64 bytes from 192.168.60.2: seq=1 ttl=63 time=1.503 ms
64 bytes from 192.168.60.2: seq=2 ttl=63 time=1.538 ms

--- 192.168.60.2 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.585/1.208/1.538 ms

tc@cliente01:~$ ping 10.0.2.15 -c 3
PING 10.0.2.15 (10.0.2.15): 56 data bytes
64 bytes from 10.0.2.15: seq=0 ttl=64 time=0.338 ms
64 bytes from 10.0.2.15: seq=1 ttl=64 time=0.898 ms
64 bytes from 10.0.2.15: seq=2 ttl=64 time=0.866 ms

--- 10.0.2.15 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.338/0.700/0.898 ms

tc@cliente01:~$ ping cuchillac.net -c 3
PING cuchillac.net (50.87.152.212): 56 data bytes
64 bytes from 50.87.152.212: seq=0 ttl=48 time=109.975 ms
64 bytes from 50.87.152.212: seq=1 ttl=48 time=115.812 ms
64 bytes from 50.87.152.212: seq=2 ttl=48 time=116.996 ms

--- cuchillac.net ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 109.975/114.261/116.996 ms
```

3.1 Comprobar que se puede navegar en Internet desde el cliente01

Nota: Si no puede navegar en Internet, debe verificar:
En srvext: IPv4 → [eth0] Automática, GW → ISP, DNS → 192.168.60+Y.2
En srvint: IPv4 → 192.168.60+Y.2, GW → 192.168.60.1, DNS → localhost, Reenviador [En el DNS] → DNS ISP
En cliente01: IPv4 → [eth0] Automática, GW → 192.168.50+Y.1 → 192.168.60+Y.2

3.2 Comprobación de comunicación de los servicios de red de los clientes

Verifique que funciona el servicio HTTP del servidor01, se debe utilizar http://www.empresay.com.sv


```
tc@cliente02:~$ mysql -h bd01 -u usuario01 -p
Enter password: 123456

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 3
Server version: 10.0.17-MariaDB Source distribution

Copyright (c) 2000, 2015, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| empresay           |
| information_schema |
| test               |
+--------------------+
3 rows in set (0.00 sec)

MariaDB [(none)]>
```

Recuerde que el usuario01 tiene permiso para ingresar desde la red, la contraseña del usuario01 es 123456

3. Reglas de filtrado para la primera fase.

El módulo de firewall que provee Zentyal tiene cuatro conjuntos de reglas para el filtrado del tráfico de paquetes IPv4

1. Reglas de filtrado desde las redes internas a Zentyal
2. Reglas de filtrado para las redes internas
3. Reglas de filtrado desde las redes externas a Zentyal
4. Reglas de filtrado para el tráfico saliente de Zentyal

Estos cuatro conjuntos de reglas permiten la comunicación entre la red IPv4 192.168.60.0 y la red IPv4 192.168.50.0 Digite los siguientes comandos para comprobar la comunicación ICMP

3.1 Bloqueo de todo el tráfico.

Para mantener todo el control y aplicar de forma clara las reglas descritas en los cuadros No. 5, será necesario eliminar todas las “cadenas” o expresiones que permiten o deniegan el tráfico.

3.1.1 Ingrese a Cortafuegos.

3.1.2 Seleccione filtrado de paquetes.

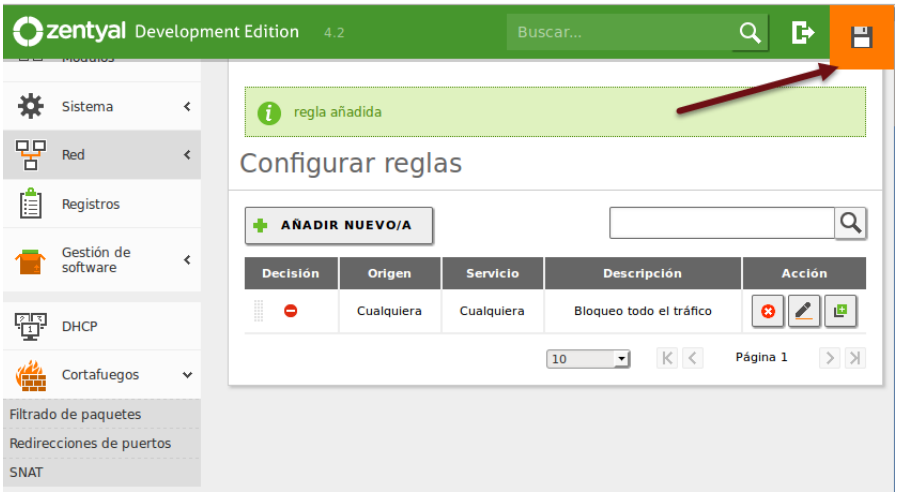
3.1.3 Ingrese a cada conjunto de reglas y elimine todas las líneas que hayan

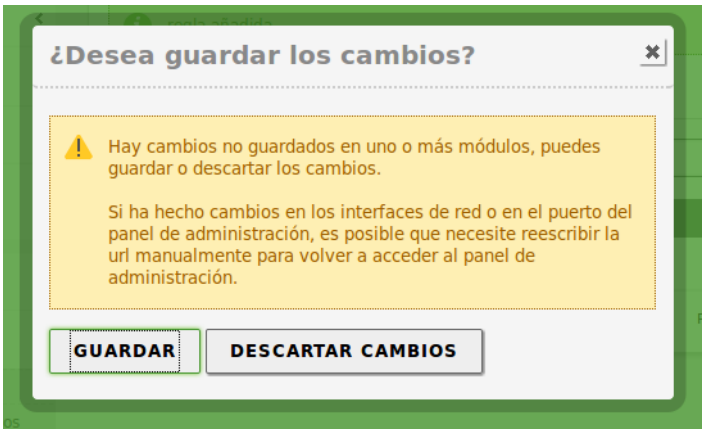
3.1.4 Guarde los cambios para cada conjunto de reglas.

3.1.5 Crear reglas de bloqueo “Any to Any”

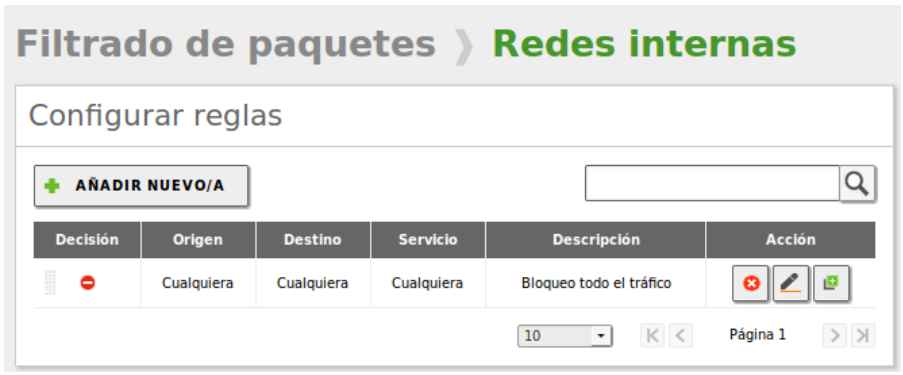
Se debe agregar una regla que boque cualquier origen a cualquier destino con cualquier servicio para cada conjunto de reglas

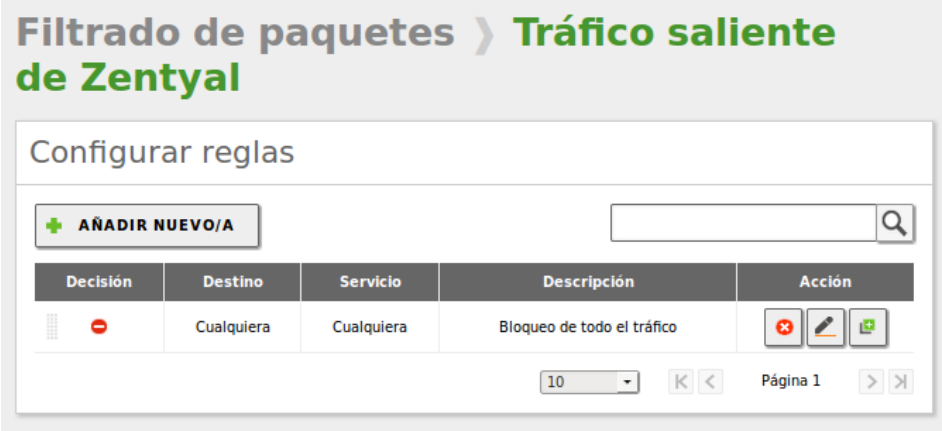
A continuación, se presentan un conjunto de pantallas que muestran lo fácil de elaborar las reglas para denegar tráfico.





Dar clic en botón aplicar los cambios





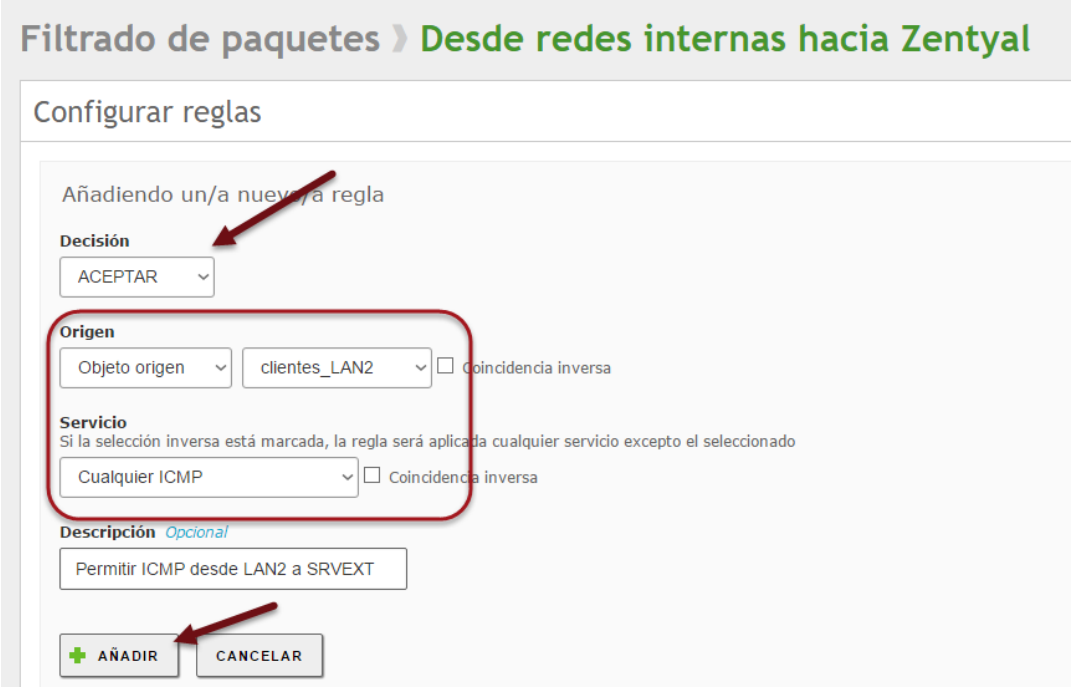
3.2 Aplicar las políticas de seguridad de la primera fase

3.2.1 Permitir hacer ping al srvext desde ambas redes LAN

Para esto es necesario crear dos reglas
Permitir(Aceptar) el tráfico ICMP desde la red LAN2
Permitir(Aceptar) el tráfico ICMP desde la red LAN1

3.2.2 Seleccionar las reglas "Desde redes internas hacia Zentyal"

Utilice los cuadros No. 5 para llenar las pantallas del asistente de configuración.



3.2.3 Verificación de las reglas creadas

3.2.4 Comprobación del envío de mensajes ICMP

```
tc@servidor01:~$ ping 192.168.60.1 -c 3
PING 192.168.60.1 (192.168.60.1): 56 data bytes
64 bytes from 192.168.60.1: seq=0 ttl=64 time=0.371 ms
64 bytes from 192.168.60.1: seq=1 ttl=64 time=0.845 ms
64 bytes from 192.168.60.1: seq=2 ttl=64 time=0.926 ms

--- 192.168.60.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.371/0.714/0.926 ms
tc@servidor01:~$

tc@cliente01:~$ ping 192.168.50.1 -c 3
PING 192.168.50.1 (192.168.50.1): 56 data bytes
```

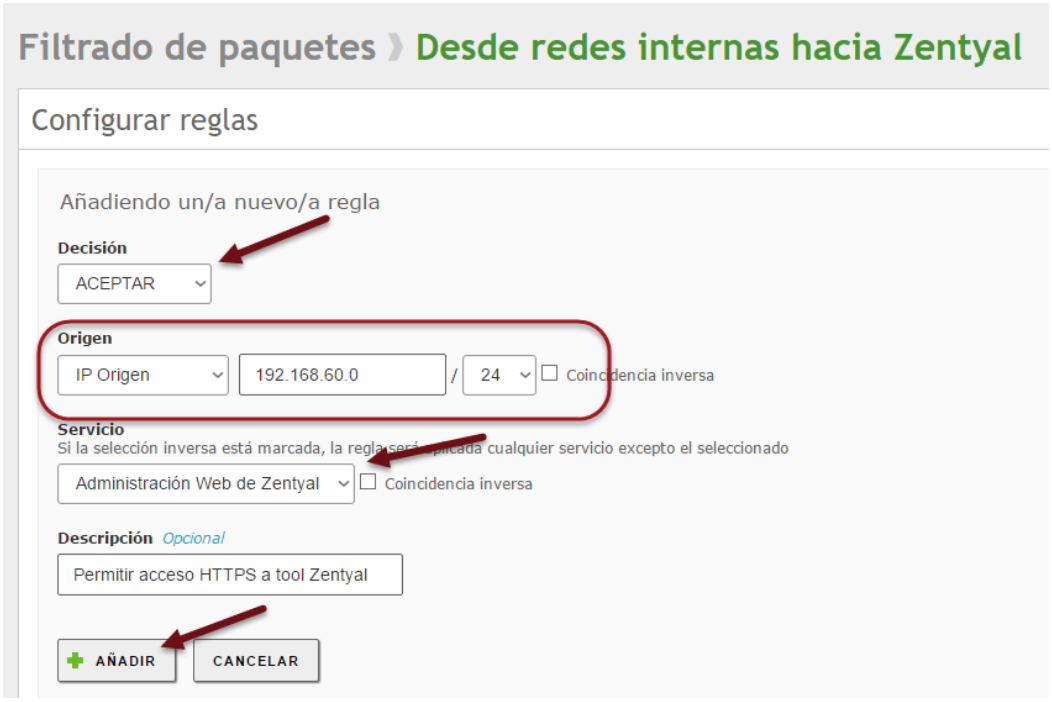
```
64 bytes from 192.168.50.1: seq=0 ttl=64 time=0.362 ms
64 bytes from 192.168.50.1: seq=1 ttl=64 time=0.959 ms
64 bytes from 192.168.50.1: seq=2 ttl=64 time=0.950 ms

--- 192.168.50.1 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.362/0.757/0.959 ms
```

3.2.5 Permitir ICMP entre las redes internas LAN1 y LAN2


```
tc@servidor01:~$ ping 192.168.50.11 -c 3
PING 192.168.50.11 (192.168.50.11): 56 data bytes
64 bytes from 192.168.50.11: seq=0 ttl=63 time=0.535 ms
64 bytes from 192.168.50.11: seq=1 ttl=63 time=1.545 ms
64 bytes from 192.168.50.11: seq=2 ttl=63 time=1.552 ms

--- 192.168.50.11 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.535/1.210/1.552 ms


tc@cliente01:~$ ping 192.168.60.11 -c 3
PING 192.168.60.11 (192.168.60.11): 56 data bytes
64 bytes from 192.168.60.11: seq=0 ttl=63 time=0.913 ms
64 bytes from 192.168.60.11: seq=1 ttl=63 time=1.434 ms
```

```
64 bytes from 192.168.60.11: seq=2 ttl=63 time=0.841 ms

--- 192.168.60.11 ping statistics ---
3 packets transmitted, 3 packets received, 0% packet loss
round-trip min/avg/max = 0.841/1.062/1.434 ms
```

3.2.6 Permitir la administración a Zentyal desde la red de servidores



3.3 Resumen de reglas de filtrado:

Filtrado de paquetes › Redes internas

Configurar reglas

AÑADIR NUEVO/A

Decisión	Origen	Destino	Servicio	Descripción	Acción
↑	servidores_LAN1	192.168.60.2/32	DNS	--	
↑	clientes_LAN2	192.168.60.2/32	DNS	Permitir consultas al DNS interno desde LAN2	
↑	clientes_LAN2	Cualquiera	HTTPS	Permitir a redes LAN2 acceso a sitios HTTPS	
↑	clientes_LAN2	Cualquiera	HTTP	Permitir a redes LAN2 acceso a sitios HTTP	
↑	servidores_LAN1	Cualquiera	HTTPS	Permitir a redes LAN1 acceso a sitios HTTPS	
↑	servidores_LAN1	Cualquiera	HTTP	Permitir a redes LAN1 acceso a sitios HTTP	
↑	clientes_LAN2	servidores_LAN1	Cualquier ICMP	Establcer ICMP desde LAN2 a LAN1	
↑	servidores_LAN1	Cualquiera	Cualquier ICMP	Permitir hacer ICMP a servidores públicos	
⛔	Cualquiera	Cualquiera	Cualquiera	Bloqueo todo el tráfico	

Filtrado de paquetes › Tráfico saliente de Zentyal

Configurar reglas

AÑADIR NUEVO/A

Decisión	Destino	Servicio	Descripción
↑	Cualquiera	HTTPS	Permitir a SRVEXT acceder a sitios HTTPS
↑	Cualquiera	HTTP	Permitir a SRVEXT acceder a HTTP
↑	Cualquiera	Cualquier ICMP	Permitir el ICMP a las redes LAN1 y LAN2
⛔	Cualquiera	Cualquiera	Bloqueo de todo el tráfico

3.4 Realizar respaldo de los archivos de configuración

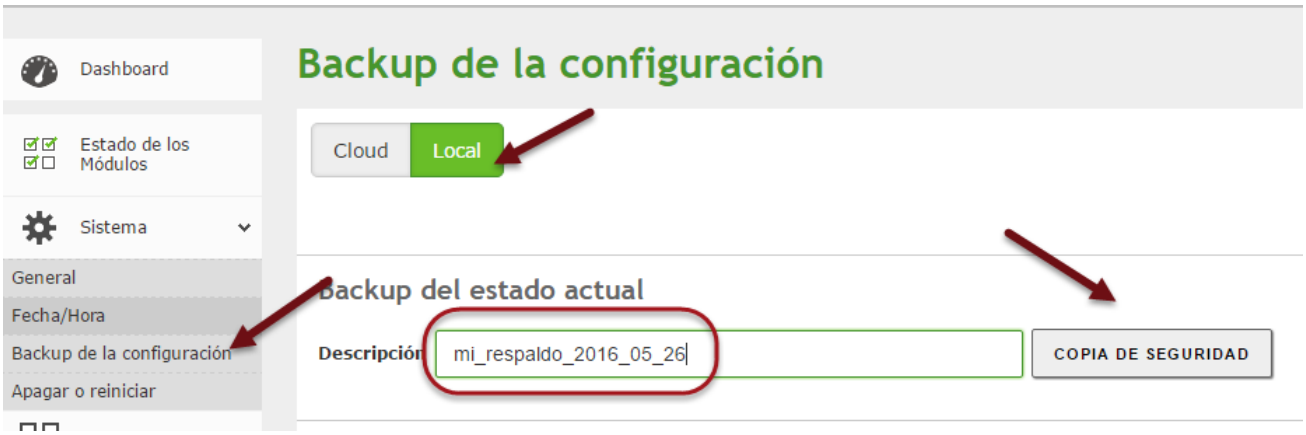
Hacer respaldo de la configuración de los archivos de servicios

3.4.1 Seleccionar Menú Sistema

3.4.2 Seleccionar Backup de la configuración

3.4.3 Seleccionar Local

3.4.4 Definir nombre del archivo de configuración



4. Pruebas de comunicación en los clientes

Verificar que:

- El **servint** pueda realizar consultas iterativas.
- Los clientes de la red LAN2 no puedan enviar mensajes ICMP a los servidores de la red LAN1
- Los servidores de la red LAN1 puedan enviar mensajes ICMP usando direcciones IPv4 y FQDN.
- Los servidores y los clientes puedan realizar consultas iterativas.
- Los servidores y los clientes puedan realizar consultas interactivas.
- Tanto los servidores como los clientes puedan visitar sitios HTTP en Internet.
- Tanto los servidores como los clientes puedan visitar sitios HTTPS en Internet.

5. Reglas de filtrado para la segunda FASE

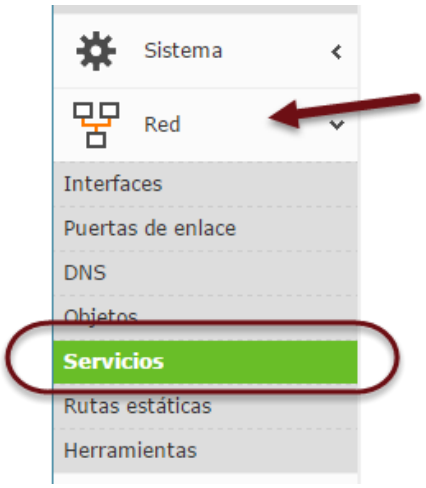
5.1 Creación de los objetos servicios en Zentyal

Similar al concepto de objetos de red, en el Appliance Zentyal se deben crean objetos para definir de una manera más sencilla los protocolos de los servicios que se requieren utilizar y que no están creados dentro de los servicios del Appliancede Zentyal. Esto es útil cuando un servicio como el DNS utiliza varios protocolos (TCP y UDP), o en servicios que se utilizan varios puertos como el FTP o SMB/CIFS

Nota: Se deben crear los servicios que no se tengan acorde a los cuadros No. 5

5.1.1 Seleccionar el menú Red

5.1.2 Seleccionar la opción "Servicios"

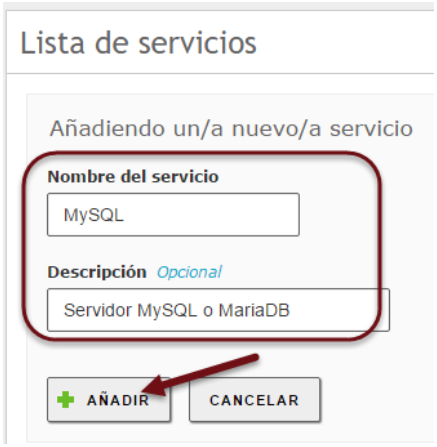


5.1.3 Dar clic en el botón "Añadir nuevo"

5.1.4 Definir el identificador del servicio

Utilice los siguientes valores:

- Nombre del servicio: **MySQL**
- Descripción: Servidor **MySQL** o **MariaDB**



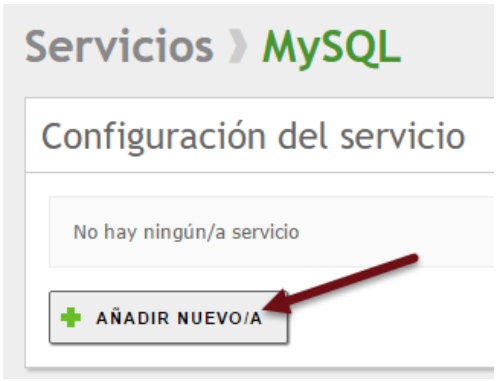
Dar clic en el botón "Añadir"

5.1.5 Definir los valores del objeto servicio creado

Dar clic en el botón "Configuración"

5.1.6 Configurar los valores del servicio

A. Dar clic en el botón "**Añadir nuevo**"

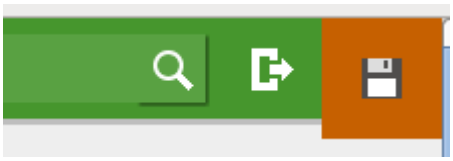


B. Defina los valores

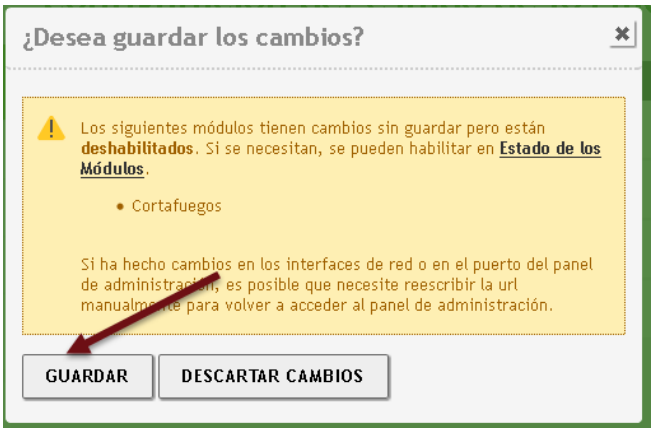
- Protocolo: **TCP**
- Puerto de origen: **Cualquiera**
- Puerto destino: "**Puerto único**" → **3306**

5.1.7 Aplicar los cambios

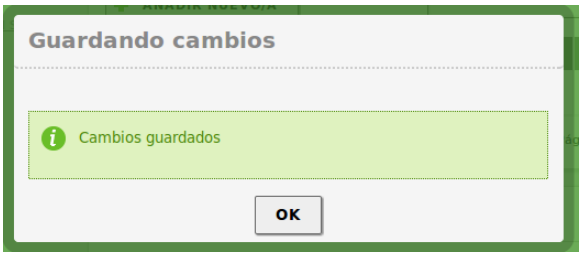
A. Dar clic en el botón guardar



B. Dar clic en botón “Guardar”



C Verificar los cambios



5.2 Repetir mismo procedimiento para crear los otros servicios.

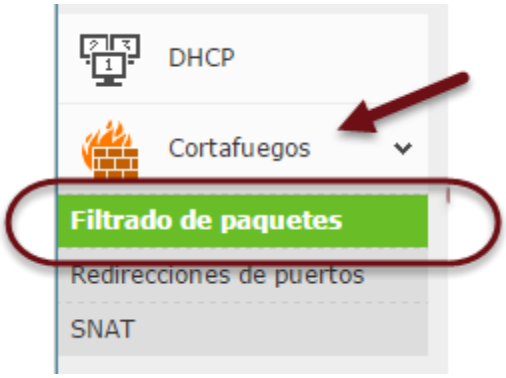
Realice el mismo procedimiento para los servicios:

- VNC, recuerde que se utiliza un puerto por cada conexión y generalmente se inicia desde el 5800 o 5900.
- SMB, Recuerde que existen varios protocolos asociados a este servicio, en UDP y TCP.

5.3 Configuración de las reglas de filtrado

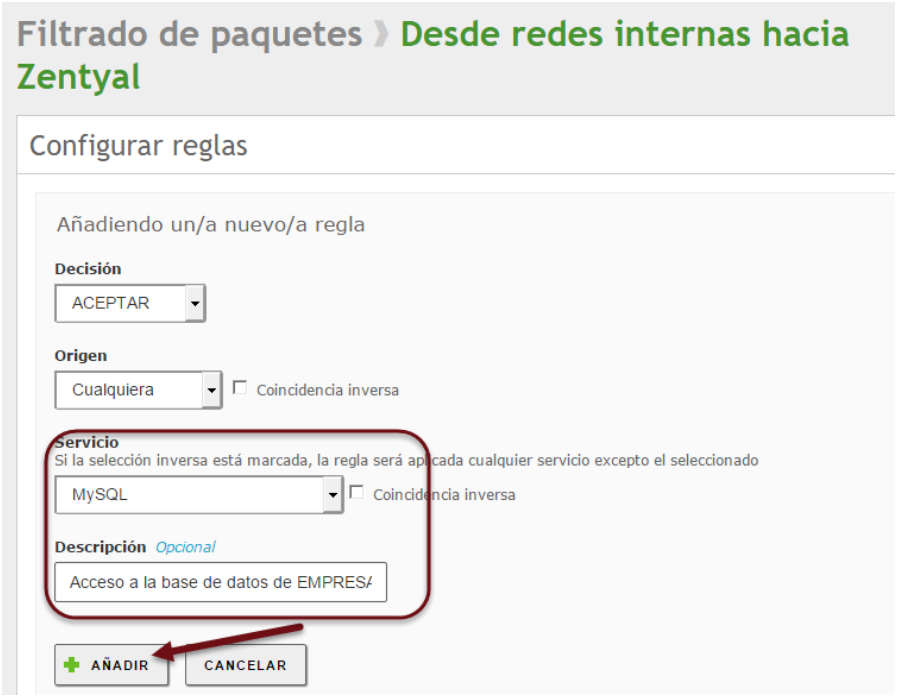
5.3.1 Seleccionar el menú Cortafuegos

5.3.2 Seleccionar la opción "Filtrado de paquetes"



5.3.3 Agregar las reglas de filtrados de las redes internas

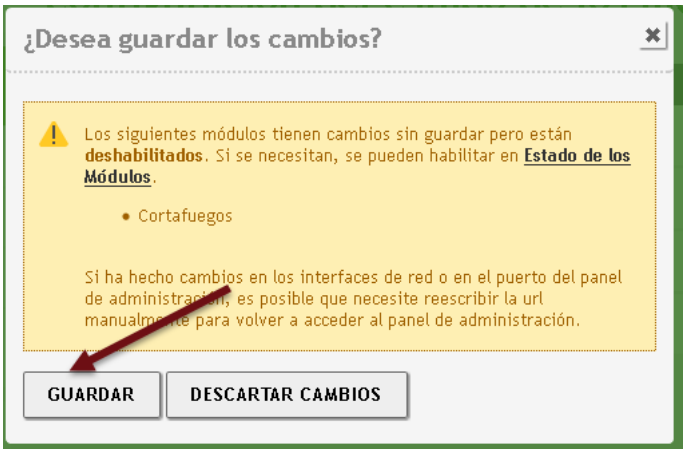
5.3.4 Definir la identificación de la regla



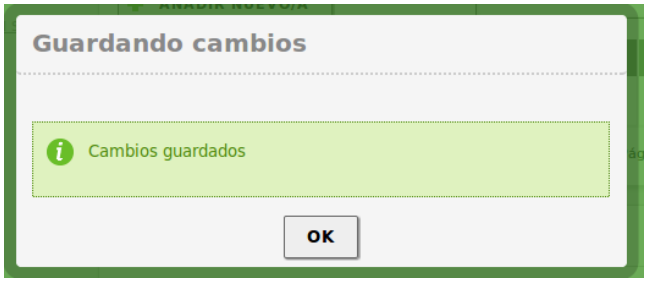
5.3.5 Aplicar los cambios

A. Dar clic en el botón guardar

B. Dar clic en botón “Guardar”



C Verificar los cambios



6. Realizar pruebas de comunicación con servicios

Verifique que se han cumplido las restricciones que se definen en los cuadros No. 5

Material bibliográfico

Para mayor información sobre el firewall puede consultar:

https://wiki.zentyal.org/wiki/En/3.5/Firewall

Anexos

Salida del archivo de configuración de iptables

```
root@srvext:~# iptables -L

Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
preinput   all  --  anywhere             anywhere
idrop      all  --  anywhere             anywhere             state INVALID
iaccept    all  --  anywhere             anywhere             state RELATED,ESTABLISHED
inospoof   all  --  anywhere             anywhere
iexternalmodules  all  --  anywhere      anywhere
iexternal  all  --  anywhere             anywhere
inoexternal  all  --  anywhere           anywhere
imodules   all  --  anywhere             anywhere
iglobal    all  --  anywhere             anywhere
iaccept    icmp !f  anywhere             anywhere             icmp echo-request state NEW
iaccept    icmp !f  anywhere             anywhere             icmp echo-reply state NEW
iaccept    icmp !f  anywhere             anywhere             icmp destination-unreachable state NEW
iaccept    icmp !f  anywhere             anywhere             icmp source-quench state NEW
iaccept    icmp !f  anywhere             anywhere             icmp time-exceeded state NEW
iaccept    icmp !f  anywhere             anywhere             icmp parameter-problem state NEW
idrop      all  --  anywhere             anywhere

Chain FORWARD (policy DROP)
target     prot opt source               destination
preforward  all  --  anywhere             anywhere
fdrop      all  --  anywhere             anywhere             state INVALID
faccept    all  --  anywhere             anywhere             state RELATED,ESTABLISHED
fnospoof   all  --  anywhere             anywhere
fredirects  all  --  anywhere             anywhere
fmodules   all  --  anywhere             anywhere
ffwdrules  all  --  anywhere             anywhere
fnoexternal  all  --  anywhere           anywhere
fdns       all  --  anywhere             anywhere
fglobal    all  --  anywhere             anywhere
faccept    icmp !f  anywhere             anywhere             icmp echo-request state NEW
faccept    icmp !f  anywhere             anywhere             icmp echo-reply state NEW
faccept    icmp !f  anywhere             anywhere             icmp destination-unreachable state NEW
faccept    icmp !f  anywhere             anywhere             icmp source-quench state NEW
faccept    icmp !f  anywhere             anywhere             icmp time-exceeded state NEW
```

```
faccept    icmp !f  anywhere             anywhere             icmp parameter-problem state NEW
fdrop      all  --  anywhere             anywhere

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere
preoutput  all  --  anywhere             anywhere
odrop      all  --  anywhere             anywhere             state INVALID
oaccept    all  --  anywhere             anywhere             state RELATED,ESTABLISHED
ointernal  all  --  anywhere             anywhere
omodules   all  --  anywhere             anywhere
oglobal    all  --  anywhere             anywhere
oaccept    icmp !f  anywhere             anywhere             icmp echo-request state NEW
oaccept    icmp !f  anywhere             anywhere             icmp echo-reply state NEW
oaccept    icmp !f  anywhere             anywhere             icmp destination-unreachable state NEW
oaccept    icmp !f  anywhere             anywhere             icmp source-quench state NEW
oaccept    icmp !f  anywhere             anywhere             icmp time-exceeded state NEW
oaccept    icmp !f  anywhere             anywhere             icmp parameter-problem state NEW
odrop      all  --  anywhere             anywhere

Chain drop (7 references)
target     prot opt source               destination
DROP       all  --  anywhere             anywhere

Chain faccept (194 references)
target     prot opt source               destination
ACCEPT     all  --  anywhere             anywhere

Chain fdns (1 references)
target     prot opt source               destination
faccept    udp  --  anywhere             srvint.empresay.com.sv  state NEW udp dpt:domain
faccept    tcp  --  anywhere             srvint.empresay.com.sv  state NEW tcp dpt:domain
faccept    udp  --  anywhere             192.168.5.19         state NEW udp dpt:domain
faccept    tcp  --  anywhere             192.168.5.19         state NEW tcp dpt:domain
faccept    udp  --  anywhere             google-public-dns-a.google.com  state NEW udp dpt:domain
faccept    tcp  --  anywhere             google-public-dns-a.google.com  state NEW tcp dpt:domain

Chain fdrop (16 references)
target     prot opt source               destination
drop       all  --  anywhere             anywhere

Chain ffwdrules (1 references)
target     prot opt source               destination
RETURN     all  --  anywhere             anywhere
RETURN     all  --  anywhere             anywhere
```

```
Chain fglobal (1 references)
target     prot opt source               destination
faccept    udp  --  192.168.50.11        srvint.empresay.com.sv  udp dpt:domain
faccept    tcp  --  192.168.50.11        srvint.empresay.com.sv  tcp dpt:domain
faccept    udp  --  192.168.50.12        srvint.empresay.com.sv  udp dpt:domain
faccept    tcp  --  192.168.50.12        srvint.empresay.com.sv  tcp dpt:domain
faccept    udp  --  192.168.50.13        srvint.empresay.com.sv  udp dpt:domain
faccept    tcp  --  192.168.50.13        srvint.empresay.com.sv  tcp dpt:domain
faccept    udp  --  192.168.50.14        srvint.empresay.com.sv  udp dpt:domain
faccept    tcp  --  192.168.50.14        srvint.empresay.com.sv  tcp dpt:domain
faccept    udp  --  192.168.50.15        srvint.empresay.com.sv  udp dpt:domain
faccept    tcp  --  192.168.50.15        srvint.empresay.com.sv  tcp dpt:domain
faccept    udp  --  192.168.50.16        srvint.empresay.com.sv  udp dpt:domain
faccept    tcp  --  192.168.50.16        srvint.empresay.com.sv  tcp dpt:domain
faccept    udp  --  servidor01.empresay.com.sv  srvint.empresay.com.sv  udp dpt:domain
faccept    tcp  --  servidor01.empresay.com.sv  srvint.empresay.com.sv  tcp dpt:domain
faccept    udp  --  servidor02.empresay.com.sv  srvint.empresay.com.sv  udp dpt:domain
faccept    tcp  --  servidor02.empresay.com.sv  srvint.empresay.com.sv  tcp dpt:domain
faccept    udp  --  servidor03.empresay.com.sv  srvint.empresay.com.sv  udp dpt:domain
faccept    tcp  --  servidor03.empresay.com.sv  srvint.empresay.com.sv  tcp dpt:domain
faccept    udp  --  srvint.empresay.com.sv  srvint.empresay.com.sv  udp dpt:domain
faccept    tcp  --  srvint.empresay.com.sv  srvint.empresay.com.sv  tcp dpt:domain
faccept    tcp  --  192.168.50.11        anywhere             tcp dpt:https
faccept    tcp  --  192.168.50.12        anywhere             tcp dpt:https
faccept    tcp  --  192.168.50.13        anywhere             tcp dpt:https
faccept    tcp  --  192.168.50.14        anywhere             tcp dpt:https
faccept    tcp  --  192.168.50.15        anywhere             tcp dpt:https
faccept    tcp  --  192.168.50.16        anywhere             tcp dpt:https
faccept    tcp  --  servidor01.empresay.com.sv  anywhere             tcp dpt:https
faccept    tcp  --  servidor02.empresay.com.sv  anywhere             tcp dpt:https
faccept    tcp  --  servidor03.empresay.com.sv  anywhere             tcp dpt:https
faccept    tcp  --  srvint.empresay.com.sv  anywhere             tcp dpt:https
faccept    tcp  --  192.168.50.11        anywhere             tcp dpt:http
faccept    tcp  --  192.168.50.12        anywhere             tcp dpt:http
faccept    tcp  --  192.168.50.13        anywhere             tcp dpt:http
faccept    tcp  --  192.168.50.14        anywhere             tcp dpt:http
faccept    tcp  --  192.168.50.15        anywhere             tcp dpt:http
faccept    tcp  --  192.168.50.16        anywhere             tcp dpt:http
faccept    tcp  --  servidor01.empresay.com.sv  anywhere             tcp dpt:http
faccept    tcp  --  servidor02.empresay.com.sv  anywhere             tcp dpt:http
faccept    tcp  --  servidor03.empresay.com.sv  anywhere             tcp dpt:http
faccept    tcp  --  srvint.empresay.com.sv  anywhere             tcp dpt:http
faccept    icmp !f  192.168.50.11        servidor01.empresay.com.sv  icmp echo-request
faccept    icmp !f  192.168.50.11        servidor01.empresay.com.sv  icmp echo-reply
faccept    icmp !f  192.168.50.11        servidor01.empresay.com.sv  icmp destination-unreachable
faccept    icmp !f  192.168.50.11        servidor01.empresay.com.sv  icmp source-quench
```

```
faccept    icmp !f  192.168.50.11        servidor01.empresay.com.sv  icmp parameter-problem
faccept    icmp !f  192.168.50.11        servidor02.empresay.com.sv  icmp echo-request
faccept    icmp !f  192.168.50.11        servidor02.empresay.com.sv  icmp echo-reply
faccept    icmp !f  192.168.50.11        servidor02.empresay.com.sv  icmp destination-unreachable
faccept    icmp !f  192.168.50.11        servidor02.empresay.com.sv  icmp source-quench
faccept    icmp !f  192.168.50.11        servidor02.empresay.com.sv  icmp parameter-problem
faccept    icmp !f  192.168.50.11        servidor03.empresay.com.sv  icmp echo-request
faccept    icmp !f  192.168.50.11        servidor03.empresay.com.sv  icmp echo-reply
faccept    icmp !f  192.168.50.11        servidor03.empresay.com.sv  icmp destination-unreachable
faccept    icmp !f  192.168.50.11        servidor03.empresay.com.sv  icmp source-quench
faccept    icmp !f  192.168.50.11        servidor03.empresay.com.sv  icmp parameter-problem
faccept    icmp !f  192.168.50.11        srvint.empresay.com.sv  icmp echo-request
faccept    icmp !f  192.168.50.11        srvint.empresay.com.sv  icmp echo-reply
faccept    icmp !f  192.168.50.11        srvint.empresay.com.sv  icmp destination-unreachable
faccept    icmp !f  192.168.50.11        srvint.empresay.com.sv  icmp source-quench
faccept    icmp !f  192.168.50.11        srvint.empresay.com.sv  icmp parameter-problem
faccept    icmp !f  192.168.50.12        servidor01.empresay.com.sv  icmp echo-request
faccept    icmp !f  192.168.50.12        servidor01.empresay.com.sv  icmp echo-reply
faccept    icmp !f  192.168.50.12        servidor01.empresay.com.sv  icmp destination-unreachable
faccept    icmp !f  192.168.50.12        servidor01.empresay.com.sv  icmp source-quench
faccept    icmp !f  192.168.50.12        servidor01.empresay.com.sv  icmp parameter-problem
faccept    icmp !f  192.168.50.12        servidor02.empresay.com.sv  icmp echo-request
faccept    icmp !f  192.168.50.12        servidor02.empresay.com.sv  icmp echo-reply
faccept    icmp !f  192.168.50.12        servidor02.empresay.com.sv  icmp destination-unreachable
faccept    icmp !f  192.168.50.12        servidor02.empresay.com.sv  icmp source-quench
faccept    icmp !f  192.168.50.12        servidor02.empresay.com.sv  icmp parameter-problem
faccept    icmp !f  192.168.50.12        servidor03.empresay.com.sv  icmp echo-request
faccept    icmp !f  192.168.50.12        servidor03.empresay.com.sv  icmp echo-reply
faccept    icmp !f  192.168.50.12        servidor03.empresay.com.sv  icmp destination-unreachable
faccept    icmp !f  192.168.50.12        servidor03.empresay.com.sv  icmp source-quench
faccept    icmp !f  192.168.50.12        servidor03.empresay.com.sv  icmp parameter-problem
faccept    icmp !f  192.168.50.12        srvint.empresay.com.sv  icmp echo-request
faccept    icmp !f  192.168.50.12        srvint.empresay.com.sv  icmp echo-reply
faccept    icmp !f  192.168.50.12        srvint.empresay.com.sv  icmp destination-unreachable
faccept    icmp !f  192.168.50.12        srvint.empresay.com.sv  icmp source-quench
faccept    icmp !f  192.168.50.12        srvint.empresay.com.sv  icmp parameter-problem
faccept    icmp !f  192.168.50.13        servidor01.empresay.com.sv  icmp echo-request
faccept    icmp !f  192.168.50.13        servidor01.empresay.com.sv  icmp echo-reply
faccept    icmp !f  192.168.50.13        servidor01.empresay.com.sv  icmp destination-unreachable
faccept    icmp !f  192.168.50.13        servidor01.empresay.com.sv  icmp source-quench
faccept    icmp !f  192.168.50.13        servidor01.empresay.com.sv  icmp parameter-problem
faccept    icmp !f  192.168.50.13        servidor02.empresay.com.sv  icmp echo-request
faccept    icmp !f  192.168.50.13        servidor02.empresay.com.sv  icmp echo-reply
faccept    icmp !f  192.168.50.13        servidor02.empresay.com.sv  icmp destination-unreachable
faccept    icmp !f  192.168.50.13        servidor02.empresay.com.sv  icmp source-quench
faccept    icmp !f  192.168.50.13        servidor02.empresay.com.sv  icmp parameter-problem
```

```
faccept    icmp !f  192.168.50.13        servidor03.empresay.com.sv  icmp echo-request
faccept    icmp !f  192.168.50.13        servidor03.empresay.com.sv  icmp echo-reply
faccept    icmp !f  192.168.50.13        servidor03.empresay.com.sv  icmp destination-unreachable
faccept    icmp !f  192.168.50.13        servidor03.empresay.com.sv  icmp source-quench
faccept    icmp !f  192.168.50.13        servidor03.empresay.com.sv  icmp parameter-problem
faccept    icmp !f  192.168.50.13        srvint.empresay.com.sv  icmp echo-request
faccept    icmp !f  192.168.50.13        srvint.empresay.com.sv  icmp echo-reply
```