Laboratorio 8

La VLAN de servicios no tienen interfaz SVI, se propaga al firewall. Esa VLAN va a una interfaz gigabit con encapsulamiento de VLAN de servicios, el switch multicapa no la enruta, la deja pasar hasta el firewall. El control de la VLAN de servicios se hace en el firewall. La Vlan de servicios esta conectada a nivel de capa 3 al firewall. Fisicamente cuando se piensa en las VLANS de administración y gestión se piensa que vienen por dos sitios diferentes, pero en este caso vienen por el mismo cable y se inyectan en el switch multicapa, donde se crean 2 vlans. A nivel 3 no se crea nada. A nivel lógico la subred de servicios está conectada al firewall (Lo que sería una DMZ).

Sobre los ACL: Las ACL SOLO aplican a interfaces de CAPA 3 como los routers (Si no tienen subinterfaces) y en los switches (Interfaces enrutadas o svis). OJO esto no se puede aplicar a troncales (capa 2). (Mucho ojo, puede caer en el examen y si se mete la pata un 0)

Parte 1: Servidores

Primero se necesita Apache para montar el servicio Web:

```
sudo apt install apache2
```

Tras eso se debe configurar apache creando el archivo “redesMunics.conf” /etc/apache2/sites-avaliable, donde estableceremos la configuración para http (puerto 80) y https (puerto 443), que necesitará de certificado SSL.

```
<VirtualHost *:80>
  ServerName munics
  DocumentRoot /var/www/html
</VirtualHost>

<VirtualHost *:443>
  ServerName munics
  DocumentRoot /var/www/html

  SSLEngine on
  SSLCertificateFile /etc/ssl/certs/ssl1.crt
  SSLCertificateKeyFile /etc/ssl/private/ssl1.key
</VirtualHost>
```

Para habilitar SSL utilizamos “a2enmod” con los siguientes comandos:

```
sudo a2enmod ssl
sudo systemctl restart apache2
```

Tras eso debemos aplicar la configuración (desde el directorio /etc/apache2/sites-avaliable) con los siguientes comandos:

```
sudo a2ensite redesMunics.conf
```

```
sudo systemctl restart apache2
```

Parte 2: Configuración de los filtros del firewall

Configuración de filtrado estático de paquetes

Se debe usar una ACL estándar para bloquear tráfico procedente de IPs no permitidas o no validas. Se deben prohibir:

- Direcciones privadas
- Direcciones de enlace local
- Direcciones de multicast
- Direcciones de broadcast
- Direcciones que nunca puedan ser de origen (ej. 127.0.0.0/8)
- Direcciones potencialmente peligrosas

Configuración CBAC en FW

Configurar Zone-Based Firewal en FW

Configurar filtrado en DL-SW1

Parte 3: Configuración de NAT

Configuración de PAT dinámico para el tráfico saliente

Configuración de port forwarding para acceso desde internet a los servicios publicados por la organización