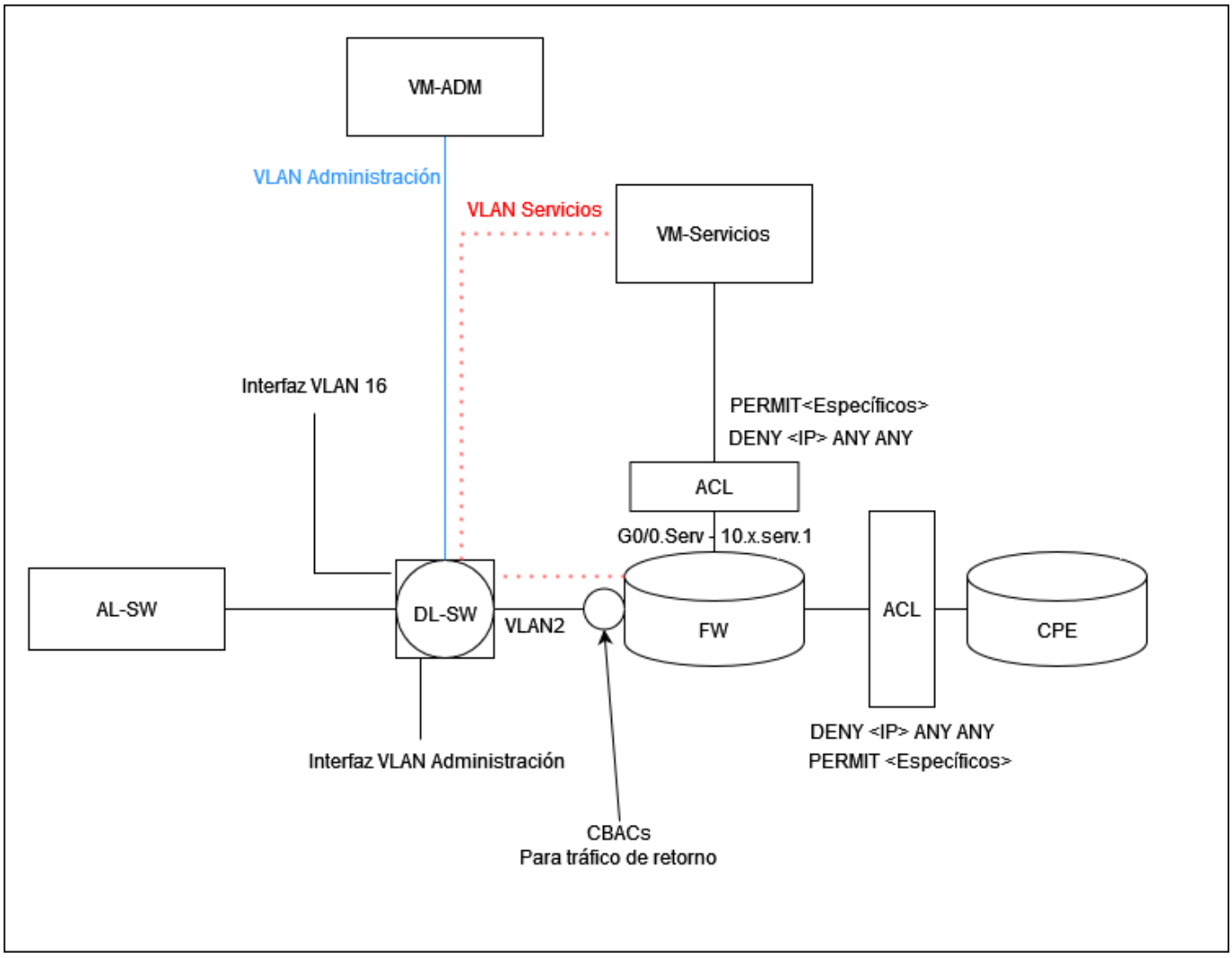
Laboratorio 8: Seguridad Perimetral

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)

El nivel de servicios (Capa 3) se conecta a una subinterfaz del firewall (G0/0.X) siendo la X la Vlan de servicios. La máquina de servicios tiene que ser trasladada al firewall. Dicha máquina entra por el Switch Multicapa, por el cual entra la VLAN de administración (Con una máquina virtual de administración) y la VLAN de servicios que se transporta a nivel de capa 2 hasta el firewall. A nivel de interface VLAN el switch multicapa debe tener Interface VLAN de administración pero NO de servicios. En resumidascuentas, la VM de servicios se conecta por la Vlan de servicios por el switch multicapa y este la pasa al FireWall.



OJO, Sobre el Pin: Mucho ojo, no nos despistemos y nos pongamos a hacer ping donde hay NAT dinámico, que no va a hacer ping Para la VLAN de servicios hacen falta varias Pool de direcciones que no son mencionadas en el enunciado del laboratorio.

Parte 1: Servidores

Servicios HTTP/HTTPS

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>
```

El certificado SSL se puede crear con el siguiente comando:

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/etc/ssl/private/ssl1.key-out /etc/ssl/certs/ssl1.crt
```

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
```

Servicios DNS

Comenzamos instalando el servicio DNS con el siguiente comando:

```
sudo apt install bind9 bind9utils bind9-doc
```

Para configurar el servidor DNS se modifica el archivo /etc/bind/named.conf.options con los servidores a los que se redirigirán las peticiones:

```
options {
...
   forwarders {
      193.144.48.30; 193.144.48.100
   }
}
```

Una vez realizadas las configuraciones se inicia el servicio con el siguiente comando:

```
sudo systemctl enable --now named
```

Tras eso se comprueba que el servicio esté corriendo con el siguiente comnado:

```
sudo systemctl status named
```

Se prueba a hacer una petición desde localhost a google para comprobar que se nos entrega una ip con el siguiente comando:

```
sudo dig @127.0.0.1 google.com
```

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

Las ACL se deben configurar en el CPE ya que son la primera medida de seguridad. En el FW se deben configurar ACL extendidas y complementarlas con CBAC. En el DL-SW se deben usar ACL extendidas. Para comenzar se crea una Acess List estándar con el nombre ISPtoCPE para denegar el tráfico con dirección de origen las ips listadas antes y permitir el tráfico restante.

```
CPE> Enable
CPE# Config Terminal
CPE(config)# ip access-list standar ISPtoCPE
CPE(config-std-nacl)#deny 10.0.0.0 0.255.255.255
CPE(config-std-nacl)#deny 192.168.0.0 0.0.255.255
CPE(config-std-nacl)#deny 172.16.0.0 0.15.255.255
CPE(config-std-nacl)#deny 224.0.0.0 15.255.255.255
CPE(config-std-nacl)#deny 240.0.0.0 15.255.255.255
CPE(config-std-nacl)#deny 127.0.0.0 0.255.255.255
CPE(config-std-nacl)#deny 169.254.0.0 0.0.255.255
CPE(config-std-nacl)#permit any
CPE(config-std-nacl)#exit
CPE(config)# interface g0/1
CPE(config-if)# ip access-group ISPtoCPE in
```

Se crea una ACL a la que llamaremos InternetToCPE que se aplica a la interfaz que conecta el ISP con el CPE (G0/1) en modo in, para bloquear el tráfico entrante proveniente de internet, evitando que este pueda saturar el CPE.

```
ISP(config)#interface g0/1
ISP(config-if)#ip access-group InternetToCPE in
IPS(config-if)#exit
```

Finalmente se aplica una ACL en las “line vty” en cada dispositivo para que solo se permita el envío de tráfico SSH entre los dispositivos que se encuentran en la vLan de Administración (743):

```
AL-SW1>enable
AL-SW1>configure terminal
AL-SW1(config)#access-list 1 permit 10.3.243.9 0.0.0.255
AL-SW1(config)#access-list 1 deny any
AL-SW1(config)#line vty 0 15
AL-SW1(config-line)#access-class 1 in
```

Configuración CBAC en FW

Las ACL estan configuradas para controlar el tráfico entrante en las interfaces del FireWall. El trafico de retorno TCP y UDP se controla con CBAC, mientras que el ICMP será permitido. Interfaz específica: G0/0.744 (Conexión a máquina de servicios), se aplicarán las siguientes reglas a esta interfaz:

- Mombre de ACL: MSStoFW
- Permitir mensajes ICMP de respuesta desde la maquina de servicios a dispositivos de red interna 10.0.0.0/8, incluyendo VLAN actuales y futuras.
- Bloquear tráfico ICMP que no sea una respuesta hacia dichos dispositivos.
- Permitir Tráfico ICMP hacia internet sin restricciones.
- Permitir mensajes de respuesta DHCP (Puerto UDP 67) a los dipositivos de la red interna 10.3.0.0/16 (VLANS actuales)
- Permitir tráfico HTTP (Puerto 80), HTTPS (puerto 443) y DNS (Puerto 53 TCP y UDP) hacia internet
- Bloquear Tráfico HTTP,HTTPS y DNS hacia la red interna.

El tráfico restante será denegado. Se aplican las reglas anteriores, bloqueando cualquier tráfico no especificado: <code> FW(config)#ip access-list extended MSStoFW FW(config-ext-nacl)#remark Control del trafico entre MSS y FW FW(config-ext-nacl)#permit icmp host 10.3.244.254 10.0.0.0 0.255.255.255 echo-reply FW(config-ext-nacl)#permit icmp host 10.3.244.254 10.0.0.0 0.255.255.255 unreachable FW(config-ext-nacl)#deny icmp host 10.3.244.254 10.0.0.0 0.255.255.255 FW(config-ext-nacl)#permit icmp host 10.3.244.254 any FW(config-ext-nacl)#permit udp host 10.3.244.254 eq 67 10.3.0.0 0.0.255.255 FW(config-ext-nacl)#deny tcp host 10.3.244.54 10.0.0.0 0.255.255.255 eq 80 FW(config-ext-nacl)#deny tcp host 10.3.244.54 10.0.0.0 0.255.255.255 eq 443 FW(config-ext-nacl)#deny tcp host 10.3.244.54 10.0.0.0 0.255.255.255 eq 53 FW(config-ext-nacl)#permit tcp host 10.3.244.254 any eq 80 FW(config-ext-nacl)#permit tcp host 10.3.244.254 any eq 443 FW(config-ext-nacl)#permit tcp host 10.3.244.254 any eq 53 FW(config-ext-nacl)# FW(config-ext-nacl)# FW(config-ext-nacl)# FW(config-ext-nacl)# FW(config-ext-nacl)# /code>

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