Redes Seguras
Prácticas Bloque III
Laboratorio 8: Seguridad Perimetral

Aarón Cela Riveiro
Sergio Vila Riveira
Samuel Fernández Vázquez
Lennart Thiele

1 Servidores HTTP, HTTPS y DNS

Para el despliegue de los servidores web y DNS requeridos en la práctica se ha utilizado la maquina virtual de servicios asignada a POD1 en el laboratorio. Esta máquina virtual dispone por lo tanto (de forma similar a la de administración) de dos interfaces de red, una conectada a la red del campus y otra conectada a la VLAN de servicios de la red de prácticas.

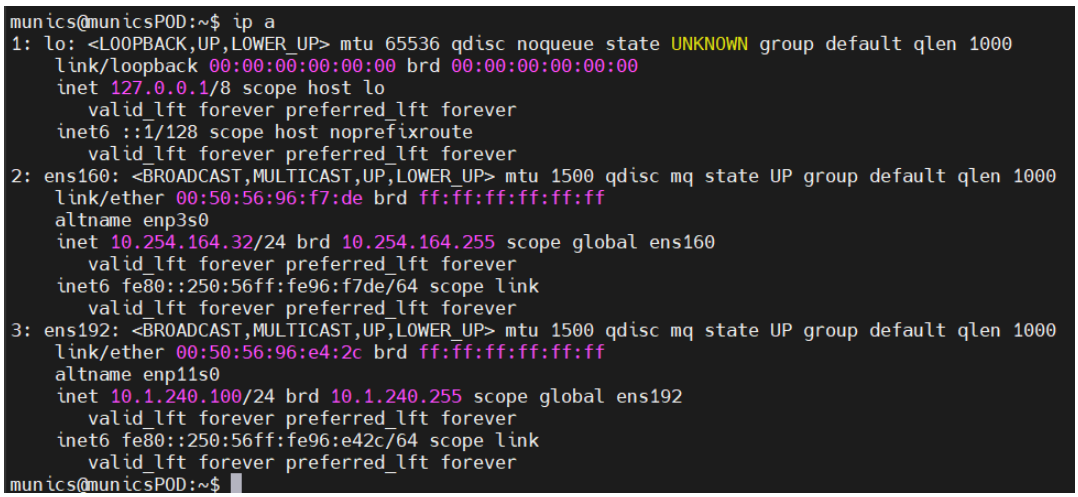

Figure 1: Salida del comando `$ ip a` en la máquina de servicios.

Vista la salida del comando, tenemos:

- **ens192** (`10.1.240.100/24`): interfaz conectada a la VLAN de servicios del escenario de laboratorio.
- **ens160** (`10.254.164.32/24`): interfaz conectada a la red del campus.
- **lo** (`127.0.0.1/8`): interfaz de loopback

1.1 Servidores HTTP y HTTPS

Una vez que se configuraron las interfaces de red de la MV, el siguiente paso fue desplegar un servidor web. PAra ello, se optoó por Apache2 dado que su instalación y configuración básica es muy sencilla.

Tras la instalación se comprobó el estado del servicio para verificar que Apache había quedado activo y habilitado al arranque.

Figure 2: Salida del comando `$ sudo systemctl status apache2.`

.

Para confirmar que el servidor escucha correctamente en el puerto 80/TCP se utilizó el siguiente comando, que nos devolvió la salida esperada.

```
munics@municsPOD:~$ sudo ss -tuln | egrep ':80'
tcp    LISTEN 0      511                *:80              *:*
```

Finalmente verificamos el funcionamiento total del servicio realizando una petición HTTP.

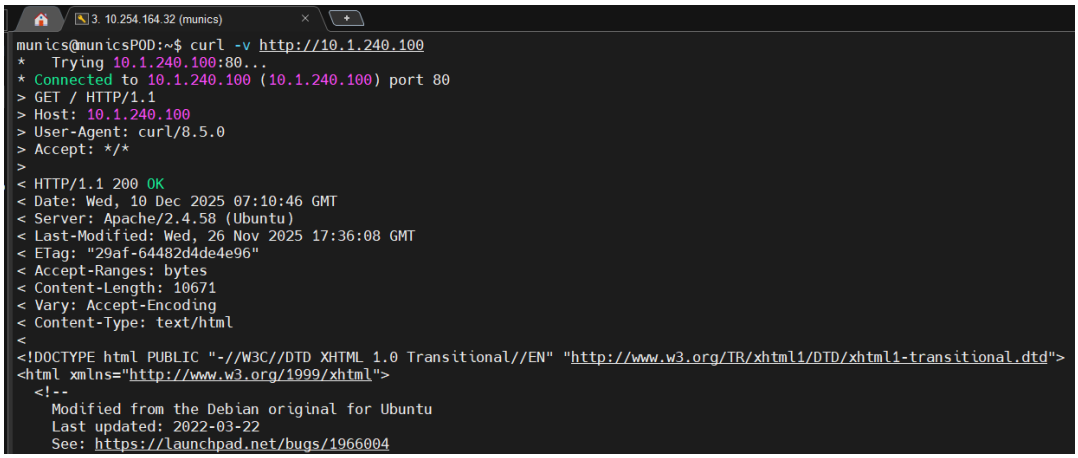

Figure 3: Curl al servidor web HTTP.

Para ofrecer el mismo contenido web de forma cifrada, se habilitó también el servicio HTTPS sobre la misma máquina y dirección IP, de modo que tanto HTTP como HTTPS se sirven desde `10.1.240.100` pero utilizando los puertos 80/TCP y 443/TCP respectivamente.

En primer lugar se activó el módulo SSL de Apache y el sitio virtual seguro por defecto.

```
sudo a2enmod ssl
sudo a2ensite default-ssl
```

A continuación se generó un certificado autofirmado utilizando openssl:

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

Despues, el fichero `/etc/apache2/sites-available/default-ssl.conf` se ajustó para referenciar este certificado y su clave privada mediante las directivas `SSLCertificateFile` y `SSLCertificateKeyFile`.

Tras recargar la configuración del servidor se hicieron las mismas pruebas que con HTTP. La primera, comprobar que Apache estaba escuchando correctamente en el puerto 443/TCP:

```
munics@municsPOD:~$ sudo ss -tuln | egrep ':443'
tcp    LISTEN 0      511                *:443             *:*
```

Y la segunda, comporbar la conectividad a través de un curl con -vk, para que así permita aceptar el certificado autofirmado.

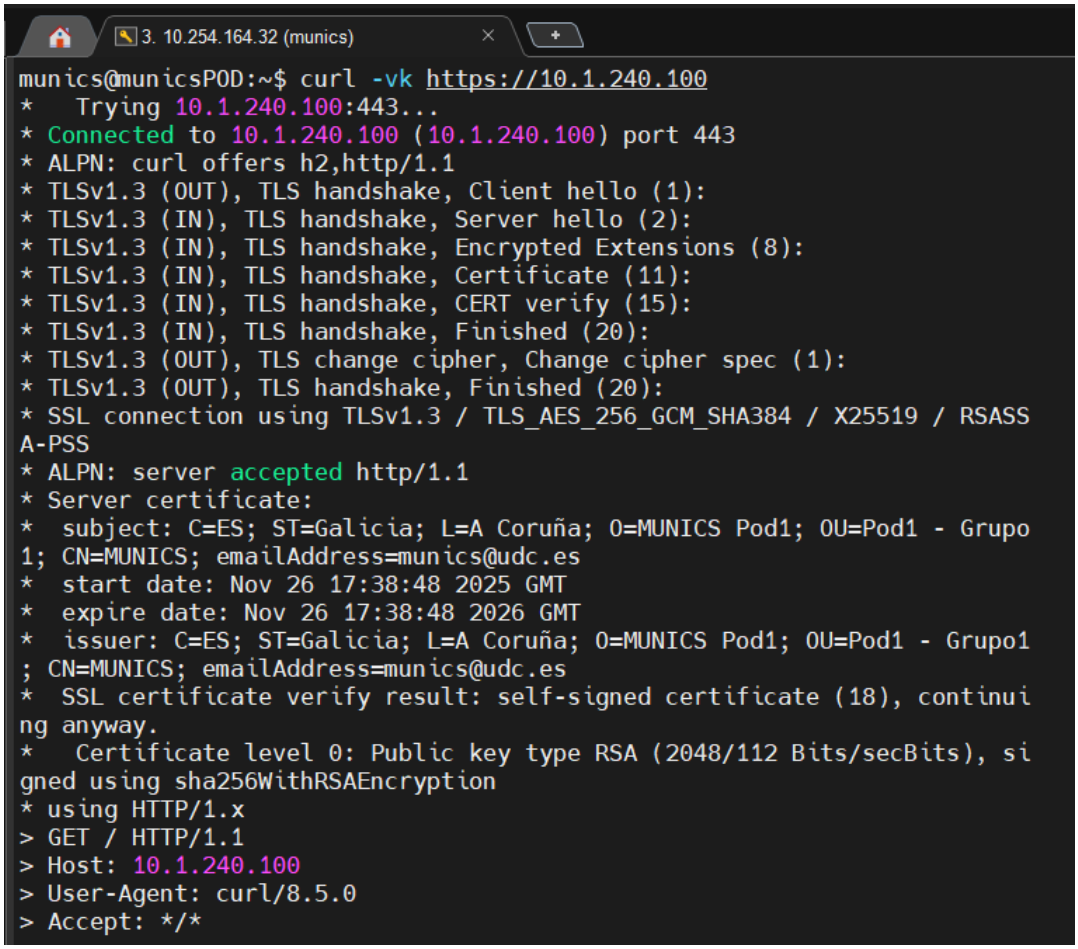

Figure 4: Curl al servidor web HTTPS.

1.2 Servidor DNS

Además de los servicios HTTP y HTTPS, se ha desplegado en la misma máquina virtual de servicios un servidor DNS basado en `BIND9`, de forma que todos los servicios del laboratorio (web y DNS) se ofrecen desde la misma dirección IP `10.1.240.100`. Este servidor actúa como:

- **servidor recursivo** para las estaciones de las VLAN 16, 17 y 18, reenviando las consultas a servidores DNS externos;
- **servidor autoritativo** para el dominio interno `munics.pri` y su zona inversa asociada a la red `10.1.240.0/24`.

1.2.1 Instalación y configuración del servicio DNS

```
sudo systemctl status bind9
```

Lo primero tras instalar BIND9 fue comprobar el estado del servicio.

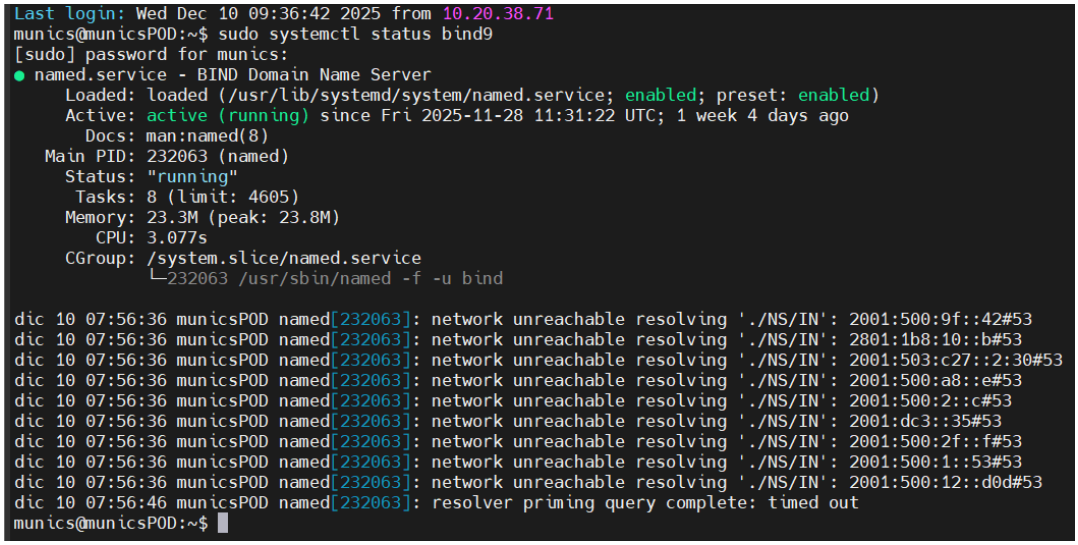

Figure 5: BIND9 activo.

A partir de ahí, comenzamos la configuración del servicio, lo primero con el archivo `/etc/bind/named.conf.options`. En este fichero se han definido los servidores forwarders que se utilizarán para resolver nombres externos y se ha limitado la escucha a la interfaz de servicios.

```

options {
        directory "/var/cache/bind";

        listen-on { 127.0.0.1; 10.1.240.100; };
        listen-on-v6 { none; };

        allow-query { any; };
        recursion yes;

         forwarders {
                193.144.48.30;
                193.144.48.100;
                8.8.8.8;
                8.8.4.4;
         };
```

A continuación, en `/etc/bind/named.conf.local` se han declarado las zonas internas gestionadas por el servidor.

```
// zona directa
 zone "munics.pri" {
     type master;
     file "/etc/bind/munics.db";
 };

// zona inversa
 zone "240.1.10.in-addr.arpa" {
     type master;
     file "/etc/bind/10.1.240.rev";
 };
```

El fichero de zona directa `/etc/bind/munics.db` define los registros del dominio `munics.pri`, asociando el nombre del servidor de servicios a la dirección `10.1.240.100`:

```
;
; Zona directa para munics.pri
;
```

```
$ORIGIN munics.pri.
$TTL 1D

@   IN SOA  munics.pri. root.munics.pri. (
        2025112701 ; Serial
        604800     ; Refresh
        86400      ; Retry
        2419200    ; Expire
        604800 )   ; Default TTL

    IN NS  srv1-deb.munics.pri.

; Alias "dns" apuntando al servidor
dns       IN CNAME srv1-deb

; Servidor de servicios
srv1-deb  IN A     10.1.240.100
```

De este modo, el nombre `srv1-deb.munics.pri` apunta al servidor de servicios donde reside HTTP y HTTPS. Por su parte, el fichero de zona inversa `/etc/bind/10.1.240.rev` permite resolver direcciones IP de la red `10.1.240.0/24` a nombres de dominio.

```
$TTL 1D

@   IN SOA  munics.pri. root.munics.pri. (
        2025112701 ; Serial
        604800
        86400
        2419200
        604800 )

    IN NS  srv1-deb.munics.pri.


100 IN PTR srv1-deb.munics.pri.
```

Finalmente, se ha configurado el propio sistema para utilizar este servidor DNS editando `/etc/resolv.conf` (o el mecanismo equivalente de la distribución), de forma que la VM se resuelve a sí misma.

```
nameserver 127.0.0.1
search munics.pri
```

Una vez aplicada la configuración se ha recargado el servicio.

```
sudo systemctl restart bind9
```

1.2.2 Verificación del servicio DNS

Se ha comprobado el correcto funcionamiento del servidor mediante la herramienta `dig`. En primer lugar, se ha verificado la resolución de nombres externos a través de los forwarders:

Figure 6: Curl al servidor web HTTPS.

La respuesta obtenida presenta código de estado `NOERROR` y un registro de tipo `A` para `google.com`, lo que confirma que el servidor actúa como resolutor recursivo. A continuación, se ha comprobado la zona interna:

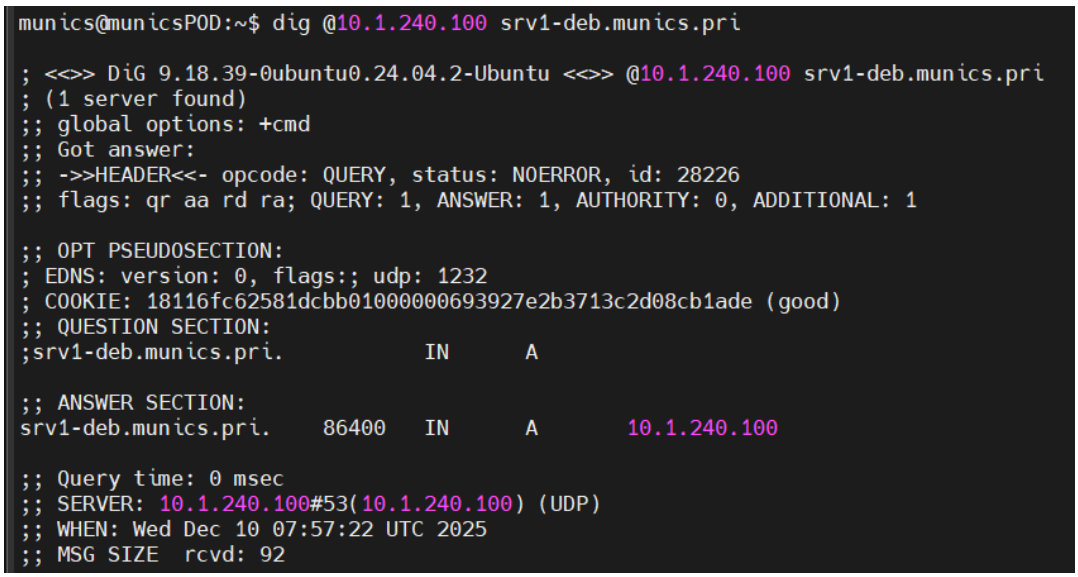

Figure 7: Curl al servidor web HTTPS.

En este caso la respuesta incluye el flag `aa` (authoritative answer) y devuelve la dirección `10.1.240.100`, demostrando que el servidor es autoritativo para el dominio `munics.pri`. Finalmente, se ha verificado la resolución inversa:

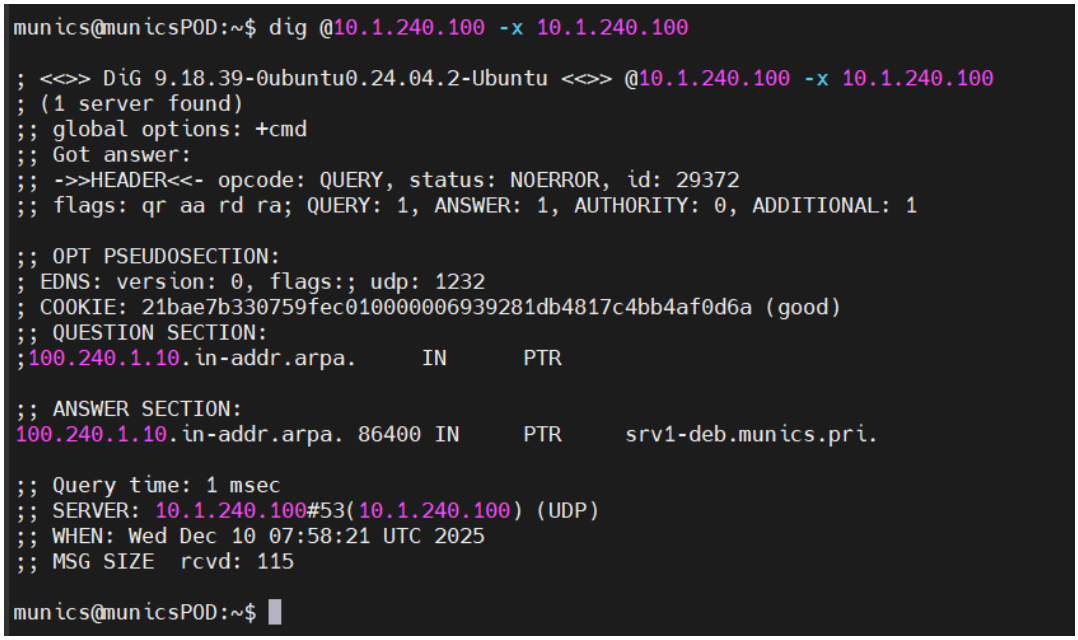

Figure 8: Curl al servidor web HTTPS.

donde se obtiene como resultado el nombre `srv1-deb.munics.pri.`, coherente con la configuración de la zona inversa.

2 Configuración de filtros en los Firewall

En esta sección se muestra la configuración que se ha aplicado para lograr la seguridad permietral con el uso de ACLs y CBACs como elementos de control.

En la figura 9 se ilustra la topología lógica del escenario, junto con sus ACLs y CBACs correspondientes.

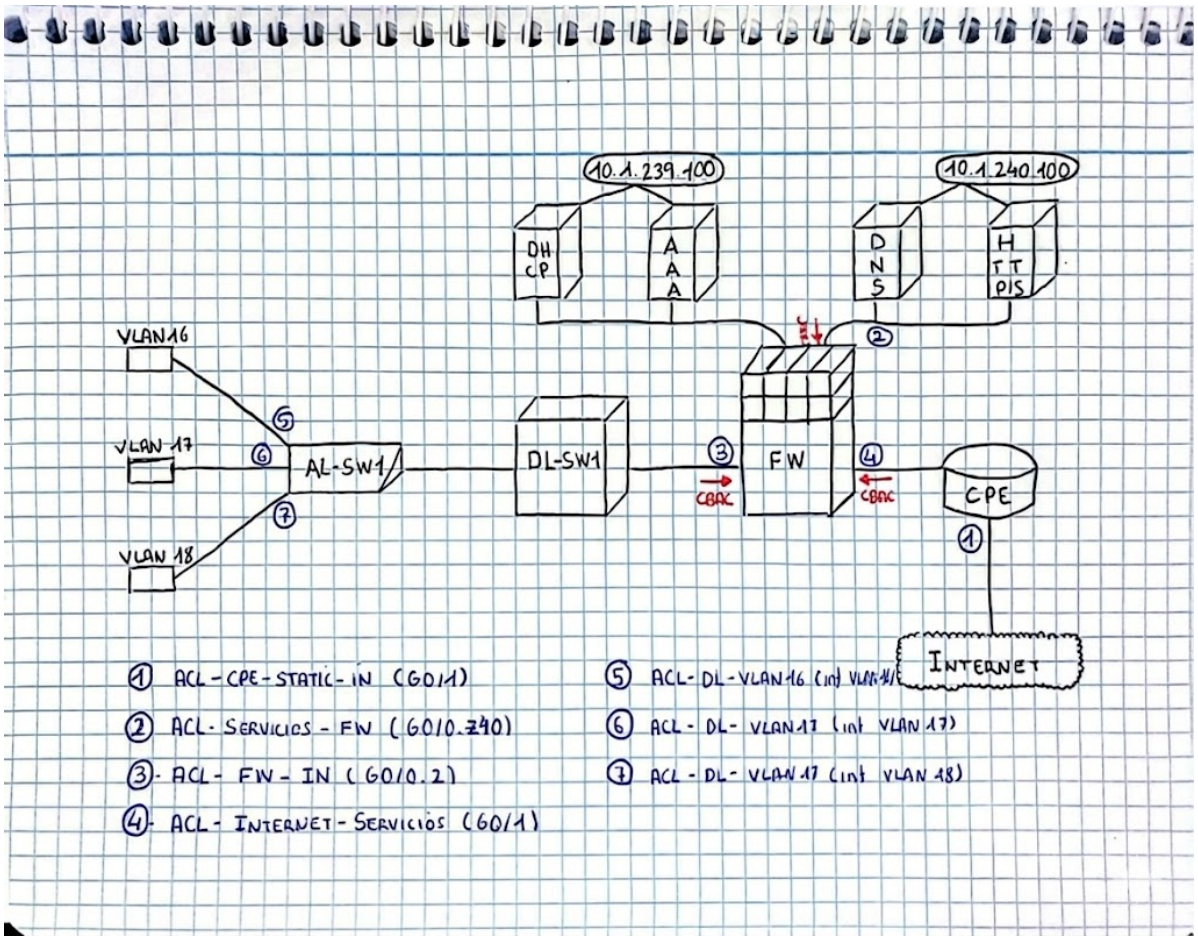

Figure 9: Topología Lógica

2.1 Filtrado estático de paquetes

Como primera medida de seguridad se ha configurado en el CPE un filtrado estático de paquetes de entrada en la interfaz que conecta con el ISP. El objetivo es descartar, lo antes posible, tráfico cuyo origen no puede ser legítimo desde un origen exterior como Internet (direcciones marcianas).

Para ello se ha definido una lista de control de acceso estándar, ACL-CPE-STATIC-IN, que filtra únicamente por dirección de origen.

```
!privadas
access-list 1 deny 10.0.0.0 0.255.255.255
access-list 1 deny 172.16.0.0 0.15.255.255
access-list 1 deny 192.168.0.0 0.0.255.255
!enlace local
access-list 1 deny 169.254.0.0 0.0.255.255
!multicast
access-list 1 deny 224.0.0.0 15.255.255.255
!broadcast
access-list 1 deny host 255.255.255.255
!loopback
access-list 1 deny 127.0.0.0 0.255.255.255
!propio fw
access-list 1 deny host 127.0.0.1
!red actual
access-list 1 deny 0.0.0.0 0.255.255.255
!otras direcciones peligrosas
!testnet1
access-list 1 deny 192.0.2.0 0.0.0.255
!testnet2
access-list 1 deny 198.51.100.0 0.0.0.255
!testnet3
access-list 1 deny 203.0.113.0 0.0.0.255
!usos futuros reservada
access-list 1 deny 240.0.0.0 15.255.255.255
!otras a justificar
!CGNAT Carrier-Grade Nat
access-list 1 deny 100.64.0.0 0.63.255.255
!permitir el resto
access-list 1 permit any
```

La ACL se aplica en sentido de entrada (IN) sobre la interfaz `GigabitEthernet0/1`, que es la que conecta el CPE con el ISP.

```
interface GigabitEthernet0/1
  ip address 192.0.1.1 255.255.255.0
  ip access-group ACL-CPE-STATIC-IN in
  ip nat outside
  ip virtual-reassembly in
  duplex auto
  speed auto
```

De este modo, todo el tráfico que entra en la red corporativa desde Internet debe superar previamente este filtrado estático de orígenes válidos en el CPE.

2.2 Filtrado de conexión entre VLANs - DL

Para limitar el conexión entre VLANs aplicamos una ACL extendida en cada interfaz de la VLAN del DL:

ACLs para el Bloqueo de las VLANs):

```
ip access-list extended ACL-DL-VLAN16-IN
 remark BLOQUEO VLANS 17 y 18
 deny   ip 10.1.16.0 0.0.0.255 10.1.17.0 0.0.0.255
 deny   ip 10.1.16.0 0.0.0.255 10.1.18.0 0.0.0.255
 permit ip any any
 remark DHCP OFFER
ip access-list extended ACL-DL-VLAN17-IN
 remark BLOQUEO VLANS 16 y 17
 deny   ip 10.1.17.0 0.0.0.255 10.1.16.0 0.0.0.255
 deny   ip 10.1.17.0 0.0.0.255 10.1.18.0 0.0.0.255
 remark DHCP OFFER
 permit ip any any
ip access-list extended ACL-DL-VLAN18-IN
 remark BLOQUEO VLANS 16 y 18
 deny   ip 10.1.18.0 0.0.0.255 10.1.16.0 0.0.0.255
 deny   ip 10.1.18.0 0.0.0.255 10.1.17.0 0.0.0.255
 remark DHCP OFFER
 permit ip any any
```

Cada una está aplicada a su interfaz VLAN del DL en sentido entrante: lo que se pretende es denegar todo el tráfico que vaya hacia otras VLANs, y el resto se deja pasar (principalmente para las peticiones DHCP OFFER), aunque se les volverá a aplicar un filtro a la entrada del FW del que hablaremos ahora.

2.3 Filtrado de conexión entre VLANs - DL

Continuando con la explicación, el tráfico VLAN pasará por una segunda línea de defensa a la entrada del FW, lo que queremos es permitir todo el tráfico HTTP, HTTPS, DNS e ICMP tanto hacia la máquina de servicios como hacia fuera (Internet) y denegar el resto. Para ello aplicaremos una ACL extendida dirección **IN**, en la interfaz G0/0.2

```
ip access-list extended ACL-FW-IN
 remark ACCESO DE DISPOSITIVOS AL SERVIDOR DHCP
 permit udp any host 10.1.239.100 eq bootps
 permit udp any host 10.1.239.100 eq bootpc
 remark OSPF
 permit ospf host 10.1.0.1 host 224.0.0.5
 permit ospf host 10.1.0.1 host 10.1.0.2
 permit ospf host 10.1.0.2 host 224.0.0.5
 permit ospf host 10.1.0.2 host 10.1.0.1
 remark ACCESO A SERVICIOS VLAN 16
 permit tcp 10.1.16.0 0.0.0.255 host 10.1.240.100 eq www
 permit tcp 10.1.16.0 0.0.0.255 host 10.1.240.100 eq 443
 permit tcp 10.1.16.0 0.0.0.255 host 10.1.240.100 eq domain
 permit udp 10.1.16.0 0.0.0.255 host 10.1.240.100 eq domain
 permit icmp 10.1.16.0 0.0.0.255 host 10.1.240.100 echo
 remark ACCESO A INTERNET VLAN 16
 permit tcp 10.1.16.0 0.0.0.255 any eq www
 permit tcp 10.1.16.0 0.0.0.255 any eq 443
 permit udp 10.1.16.0 0.0.0.255 any eq domain
 permit icmp 10.1.16.0 0.0.0.255 any echo
 remark ACCESO A SERVICIOS VLAN 17
 permit tcp 10.1.17.0 0.0.0.255 host 10.1.240.100 eq www
 permit tcp 10.1.17.0 0.0.0.255 host 10.1.240.100 eq 443
 permit tcp 10.1.17.0 0.0.0.255 host 10.1.240.100 eq domain
 permit udp 10.1.17.0 0.0.0.255 host 10.1.240.100 eq domain
 permit icmp 10.1.17.0 0.0.0.255 host 10.1.240.100 echo
 remark ACCESO A INTERNET VLAN 17
```

```
 permit tcp 10.1.17.0 0.0.0.255 any eq www
 permit tcp 10.1.17.0 0.0.0.255 any eq 443
 permit udp 10.1.17.0 0.0.0.255 any eq domain
 permit icmp 10.1.17.0 0.0.0.255 any echo
 remark ACCESO A SERVICIOS VLAN 18
 permit tcp 10.1.18.0 0.0.0.255 host 10.1.240.100 eq www
 permit tcp 10.1.18.0 0.0.0.255 host 10.1.240.100 eq 443
 permit tcp 10.1.18.0 0.0.0.255 host 10.1.240.100 eq domain
 permit udp 10.1.18.0 0.0.0.255 host 10.1.240.100 eq domain
 permit icmp 10.1.18.0 0.0.0.255 host 10.1.240.100 echo
 remark ACCESO A INTERNET VLAN 18
 permit tcp 10.1.18.0 0.0.0.255 any eq www
 permit tcp 10.1.18.0 0.0.0.255 any eq 443
 permit udp 10.1.18.0 0.0.0.255 any eq domain
 permit icmp 10.1.18.0 0.0.0.255 any echo
 deny   ip any any
```

A mayores, dejamos unas reglas de inspección CBAC para permitir el tráfico de vuelta generado por estas peticiones, abriendo su propio túnel para las ACLs restrictivas que encuentre por el camino.

```
    ip inspect name CBAC tcp timeout 300
    ip inspect name CBAC udp timeout 30
    ip inspect name CBAC icmp timeout 10
```

2.4 Filtrado de conexión entre Servicio y FW

Queremos que la VLAN de servicios solo pueda acceder a Internet mediante HTTP, HTTPS, ICMP y DNS, denegando explícitamente su conectividad a nuestras VLANs. Para ello aplicamos la siguiente ACL, en la interfaz g0/0.740 del FW, dirección IN:

```
ip access-list extended ACL-SERVICIOS-FW
remark DENEGAR CONEXIONES VLAN
deny ip any 10.1.16.0 0.0.0.255
deny ip any 10.1.17.0 0.0.0.255
deny ip any 10.1.18.0 0.0.0.255

permit tcp 10.1.240.0 0.0.0.255 any eq 80
permit tcp 10.1.240.0 0.0.0.255 any eq 443
permit tcp 10.1.240.0 0.0.0.255 any eq 53
permit udp 10.1.240.0 0.0.0.255 any eq 53
permit icmp 10.1.240.0 0.0.0.255 any

deny ip any any
```

Además también aplicamos la CBAC para permitir conexiones de vuelta.

```
    ip inspect CBAC in
```

2.5 Filtrado de conexión entre Internet y FW

Por último queremos controlar el acceso a nuestra red desde internet. Para ello aplicamos una ACL en la interfaz que comunica el FW con CPE (int g0/1). Con el siguiente contenido:

```
ip access-list extended ACL-INTERNET-FW
 permit ospf host 10.1.0.6 host 224.0.0.5
 permit ospf host 10.1.0.6 host 10.1.0.5
 permit ospf host 10.1.0.5 host 224.0.0.5
 permit ospf host 10.1.0.5 host 10.1.0.6
 permit tcp any host 10.1.240.100 eq 443
 permit icmp any host 10.1.240.100 echo
 deny   ip any 10.1.0.0 0.0.255.255
 deny   ip any any
```

Teniendo cuidado de no cortar el tráfico OSPF y permitiendo solo peticiones HTTPS e ICMP a nuestra VLAN de Servicios. A mayores volvemos a dejar una CBAC para permitir el tráfico de retorno.

3 Configurar Zone-Based Firewall en FW

Para implementar Zone-Based Firewall (ZBFW) en el firewall, se han definido tres zonas de seguridad. En la Figura 10 se muestra el esquema de zonas utilizado.

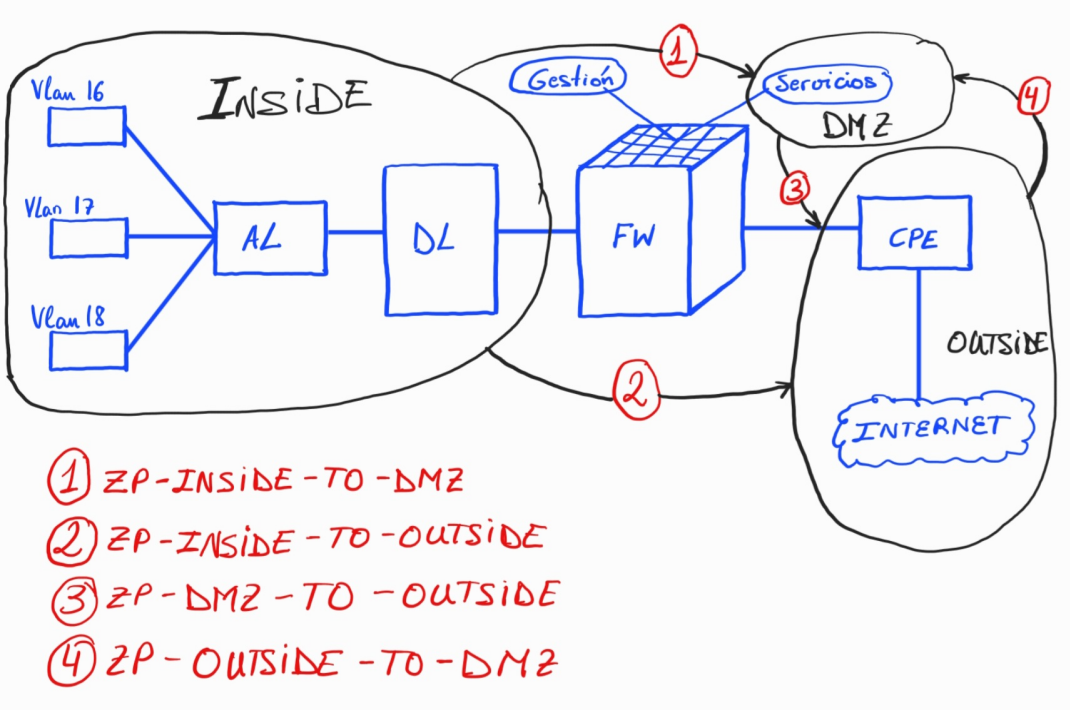

Figure 10: Zonas implementadas

Para llevar a cabo esta implementación se han seguido los siguientes pasos:

1. **Creación de las zonas de seguridad.** Se definen las distintas zonas que agrupan interfaces con el mismo nivel de confianza: red interna, red de servicios (DMZ) y red externa.

```
zone security INSIDE
zone security DMZ
zone security OUTSIDE
```

2. **Asignación de interfaces a cada zona.** Cada interfaz del firewall se asocia a la zona que le corresponde según su función dentro de la topología.

```
interface GigabitEthernet0/0.2
 zone-member security INSIDE
!
interface GigabitEthernet0/0.740
 zone-member security OUTSIDE
!
interface GigabitEthernet0/1
 zone-member security OUTSIDE
```

3. **Creación de listas de control de acceso (ACL).** Se crean ACLs que posteriormente se utilizarán para identificar el tráfico en las *class-map*, permitiendo definir de forma precisa qué flujos serán inspeccionados.

```
ip access-list extended ACL-DHCP
 permit udp any host 10.1.239.100 eq bootps
 permit udp any host 10.1.239.100 eq bootpc
ip access-list extended ACL-DMZ-SERVER
```

```
 permit ip any host 10.1.240.100
ip access-list extended ACL-INSIDE
 permit ip 10.1.16.0 0.0.0.255 any
 permit ip 10.1.17.0 0.0.0.255 any
 permit ip 10.1.18.0 0.0.0.255 any
ip access-list extended ACL-OSPF
 permit ospf any any
!
```

4. **Definición de las class-map.** Se crean las *class-map* para clasificar el tráfico según protocolos y ACLs, identificando los flujos que serán permitidos entre zonas.

```
class-map type inspect match-any CM-DMZ-TO-OUTSIDE
 match access-group name ACL-DMZ-SERVER
 match protocol tcp
 match protocol udp
 match protocol icmp
class-map type inspect match-any CM-OUTSIDE-TO-DMZ
 match access-group name ACL-DMZ-SERVER
 match protocol icmp
 match protocol tcp
class-map type inspect match-any CM-CONTROL
 match access-group name ACL-DHCP
 match access-group name ACL-OSPF
class-map type inspect match-any CM-INSIDE-TO-OUTSIDE
 match access-group name ACL-INSIDE
 match protocol tcp
 match protocol udp
 match protocol icmp
class-map type inspect match-any CM-INSIDE-TO-DMZ
 match access-group name ACL-INSIDE
 match access-group name ACL-DMZ-SERVER
 match protocol tcp
 match protocol udp
 match protocol icmp
!
```

5. **Creación de las policy-map.** Las *policy-map* definen la acción a realizar sobre el tráfico clasificado: inspección del tráfico permitido y bloqueo del resto.

```
policy-map type inspect PM-DMZ-TO-OUTSIDE
 class type inspect CM-DMZ-TO-OUTSIDE
  inspect
 class class-default
  drop
policy-map type inspect PM-INSIDE-TO-OUTSIDE
 class type inspect CM-INSIDE-TO-OUTSIDE
  inspect
 class type inspect CM-CONTROL
  pass
 class class-default
  drop
policy-map type inspect PM-OUTSIDE-TO-DMZ
 class type inspect CM-OUTSIDE-TO-DMZ
  inspect
 class class-default
  drop
policy-map type inspect PM-INSIDE-TO-DMZ
 class type inspect CM-INSIDE-TO-DMZ
  inspect
 class type inspect CM-CONTROL
  pass
```

```
 class class-default
  drop
!
```

6. **Definición de los pares de zonas (zone-pair).** Finalmente, se crean los *zone-pair* que asocian las zonas de origen y destino con su correspondiente política de seguridad.

```
zone-pair security ZP-INSIDE-TO-DMZ source INSIDE destination DMZ
 service-policy type inspect PM-INSIDE-TO-DMZ
zone-pair security ZP-INSIDE-TO-OUTSIDE source INSIDE destination OUTSIDE
 service-policy type inspect PM-INSIDE-TO-OUTSIDE
zone-pair security ZP-DMZ-TO-OUTSIDE source DMZ destination OUTSIDE
 service-policy type inspect PM-DMZ-TO-OUTSIDE
zone-pair security ZP-OUTSIDE-TO-DMZ source OUTSIDE destination DMZ
 service-policy type inspect PM-OUTSIDE-TO-DMZ
```

Finalmente, a continuación se describe el comportamiento de cada par de zonas definido:

- **INSIDE → DMZ**: Se permite el acceso desde la red interna a la red de servicios (DMZ) utilizando los protocolos definidos (HTTP, HTTPS, DNS e ICMP). El tráfico permitido es inspeccionado para permitir el retorno de las conexiones. Cualquier otro tráfico es bloqueado.
- **INSIDE → OUTSIDE**: Se autoriza la salida de tráfico desde la red interna hacia Internet únicamente para los servicios permitidos (HTTP, HTTPS, DNS e ICMP). El resto del tráfico hacia el exterior es denegado.
- **DMZ → OUTSIDE**: Se permite que los servidores ubicados en la DMZ accedan a Internet para los servicios necesarios, inspeccionando el tráfico para permitir las respuestas. Cualquier comunicación no autorizada es descartada.
- **OUTSIDE → DMZ**: Desde la red externa solo se permite el acceso controlado a los servicios publicados en la DMZ (por ejemplo HTTPS), mientras que cualquier otro intento de conexión desde el exterior es bloqueado por defecto.

4 Pruebas

Estas son todas las pruebas que hemos realizado, exceptuando las de NAT, que se describen en secciones posteriores junto con la configuración correspondiente.

4.1 Desde un usuario en la VLAN 18

```
┌──(kali㉿kali)-[~]
└─$ ping 10.1.240.100
PING 10.1.240.100 (10.1.240.100) 56(84) bytes of data.
64 bytes from 10.1.240.100: icmp_seq=1 ttl=62 time=2.06 ms
64 bytes from 10.1.240.100: icmp_seq=2 ttl=62 time=1.47 ms
64 bytes from 10.1.240.100: icmp_seq=3 ttl=62 time=2.06 ms
^C
── 10.1.240.100 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 1.470/1.862/2.062/0.277 ms

┌──(kali㉿kali)-[~]
└─$ curl 10.1.240.100
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/
xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <!--
    Modified from the Debian original for Ubuntu
    Last updated: 2022-03-22
    See: https://launchpad.net/bugs/1966004
  -->
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>Apache2 Ubuntu Default Page: It works</title>
    <style type="text/css" media="screen">
  * {
    margin: 0px 0px 0px 0px;
    padding: 0px 0px 0px 0px;
  }
```

Figure 11: PING y CURL a Servicios

En la Figura 11 se observa cómo un usuario de la VLAN 18 puede comunicarse correctamente con la red de Servicios. El ping confirma conectividad a nivel ICMP y la petición HTTP mediante `curl` devuelve la página del servidor.

```
┌──(kali㉿kali)-[~]
└─$ ping 10.1.16.1
PING 10.1.16.1 (10.1.16.1) 56(84) bytes of data.
From 10.1.18.1 icmp_seq=1 Packet filtered
From 10.1.18.1 icmp_seq=2 Packet filtered
^C
── 10.1.16.1 ping statistics ──
2 packets transmitted, 0 received, +2 errors, 100% packet loss, time 1001ms
```

Figure 12: Ping a otra VLAN

La Figura 12 muestra un intento de comunicación desde la VLAN 18 hacia otra VLAN de usuarios. El tráfico es bloqueado, lo que confirma que el firewall impide el tráfico lateral entre VLANs internas, cumpliendo las restricciones de aislamiento definidas en la política de seguridad.

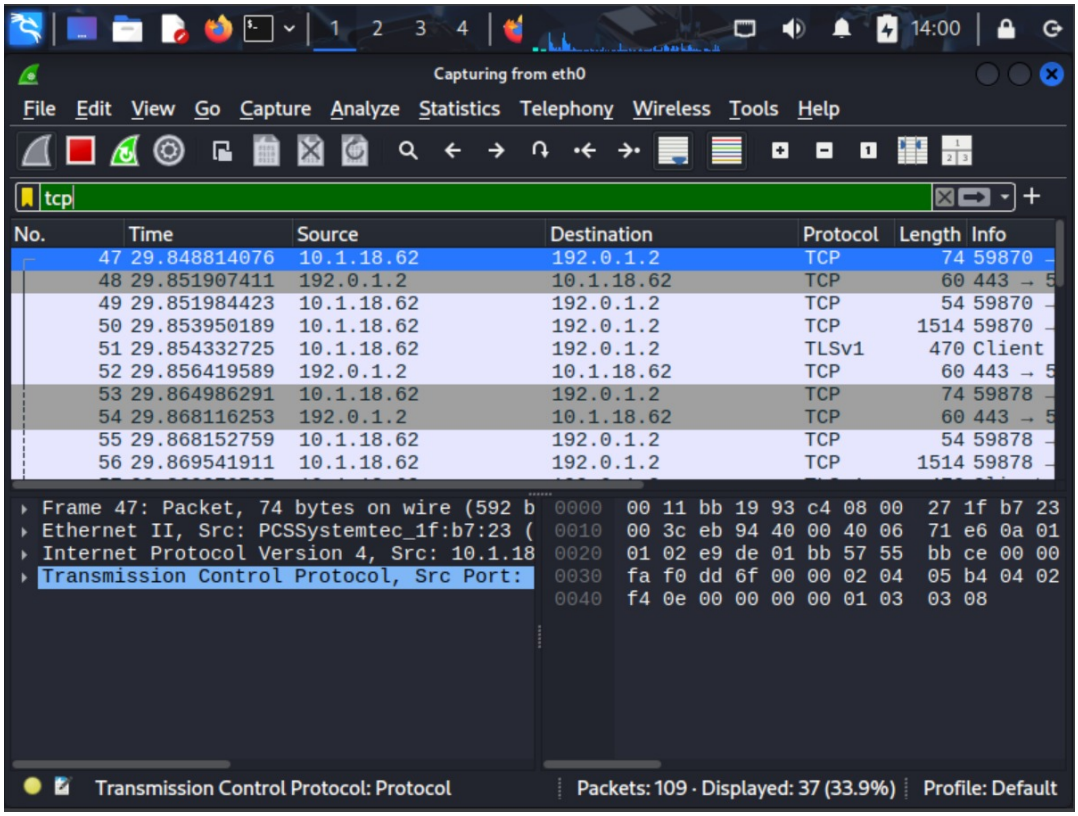

Figure 13: Captura de tráfico hacia el servidor en el ISP

En la Figura 13 se muestra una captura con Wireshark donde se observa que el tráfico generado por el usuario alcanza correctamente el servidor ubicado en el ISP. Esto demuestra que se permite el tráfico saliente hacia Internet para los servicios autorizados.

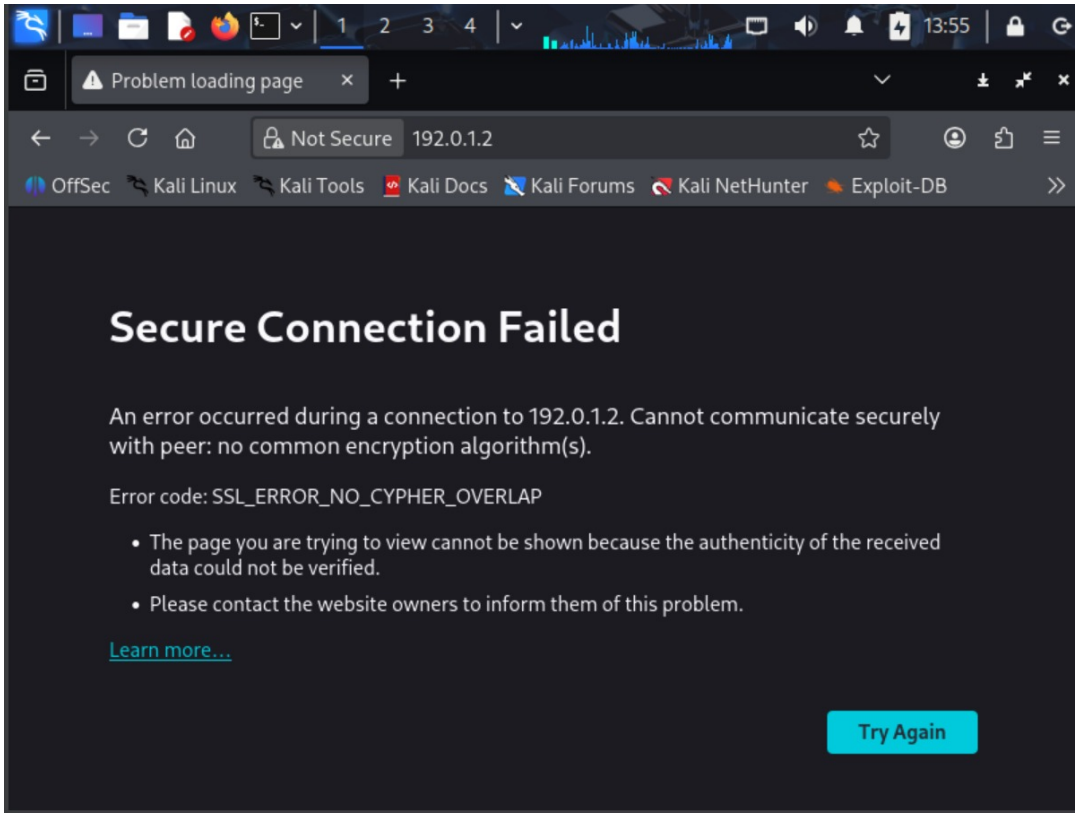

Figure 14: Acceso al servidor del ISP desde el navegador

La Figura 14 confirma el acceso desde el navegador del usuario al servidor HTTPS del ISP. Aunque se muestra un aviso de seguridad debido al uso de un certificado autofirmado, la conexión se establece correctamente.

```
┌──(kali㉿kali)-[~]
└─$ dig @10.1.240.100 srv1-deb.munics.pri

; <<>> DiG 9.20.15-2-Debian <<>> @10.1.240.100 srv1-deb.munics.pri
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19191
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 6224b9e002d1f18c01000000693b0b5aec044d0f15791db7 (good)
;; QUESTION SECTION:
;srv1-deb.munics.pri.           IN      A

;; ANSWER SECTION:
srv1-deb.munics.pri.    86400   IN      A       10.1.240.100

;; Query time: 4 msec
;; SERVER: 10.1.240.100#53(10.1.240.100) (UDP)
;; WHEN: Thu Dec 11 13:19:36 EST 2025
;; MSG SIZE  rcvd: 92
```

Figure 15: Consulta DNS desde la VLAN 18

En la Figura 15 se observa una consulta DNS realizada desde la VLAN 18 al servidor de Servicios.

4.2 Pruebas desde el ISP simulando Internet

En este apartado se muestran las pruebas realizadas desde el ISP, el cual simula una red externa a la organización, con el objetivo de verificar que las políticas de seguridad implementadas permiten únicamente el tráfico autorizado desde Internet hacia la red interna.

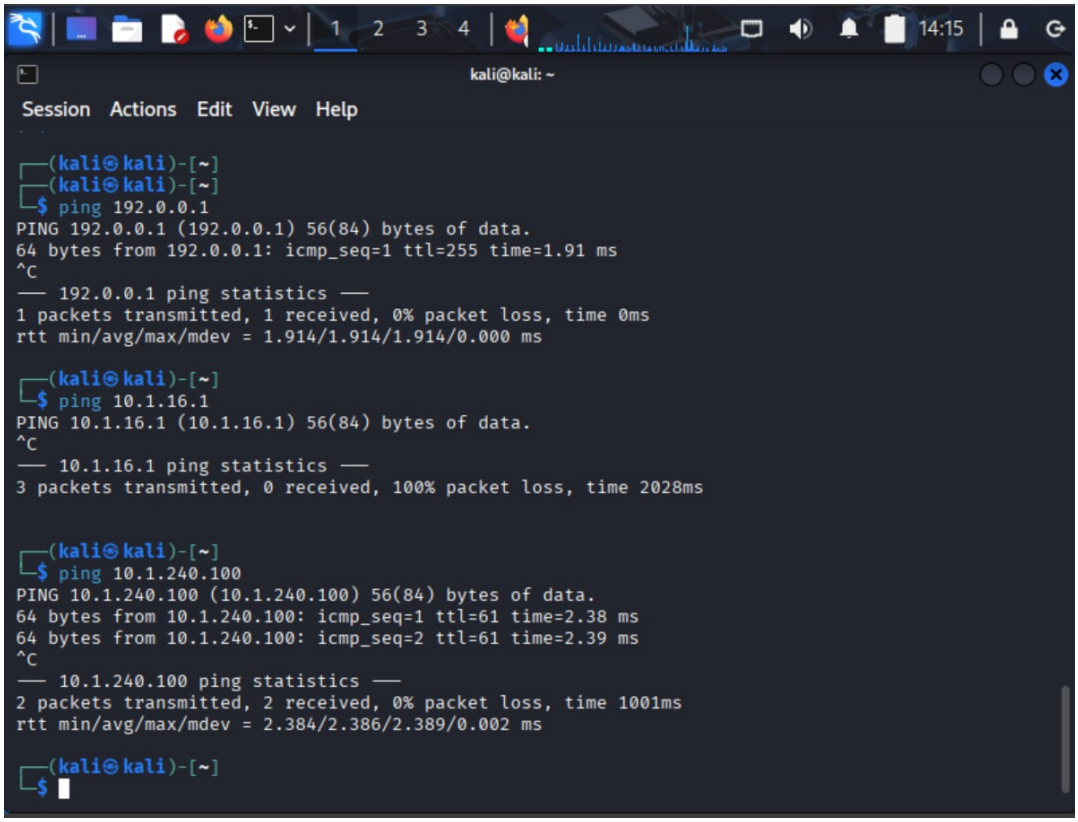

Figure 16: Pruebas de conectividad desde el ISP

En la Figura 16 se observa que desde el ISP se puede alcanzar el servidor de Servicios mediante los protocolos permitidos. El acceso a otros elementos de la red interna, como las VLAN de usuarios o dispositivos de red, no es posible, lo que confirma que se bloquea correctamente cualquier acceso no autorizado desde la red externa.

4.3 Pruebas desde la VLAN de Servicios

Primero vemos como se deniega por completo el acceso a nuestras VLANs:

```
munics@municsPOD:~$ ping 10.1.16.54
PING 10.1.16.54 (10.1.16.54) 56(84) bytes of data.
From 10.1.240.1 icmp_seq=1 Packet filtered
From 10.1.240.1 icmp_seq=2 Packet filtered
From 10.1.240.1 icmp_seq=3 Packet filtered
^C
--- 10.1.16.54 ping statistics ---
3 packets transmitted, 0 received, +3 errors, 100% packet loss, time 2038ms

munics@municsPOD:~$ ping 10.1.18.1
PING 10.1.18.1 (10.1.18.1) 56(84) bytes of data.
From 10.1.240.1 icmp_seq=1 Packet filtered
From 10.1.240.1 icmp_seq=2 Packet filtered
From 10.1.240.1 icmp_seq=3 Packet filtered
^C
--- 10.1.18.1 ping statistics ---
3 packets transmitted, 0 received, +3 errors, 100% packet loss, time 2038ms

munics@municsPOD:~$ ping 10.1.17.33
PING 10.1.17.33 (10.1.17.33) 56(84) bytes of data.
From 10.1.240.1 icmp_seq=1 Packet filtered
From 10.1.240.1 icmp_seq=2 Packet filtered
From 10.1.240.1 icmp_seq=3 Packet filtered
^C
--- 10.1.17.33 ping statistics ---
3 packets transmitted, 0 received, +3 errors, 100% packet loss, time 2036ms
```

Figure 17: Ping hacia VLAN desde VM Servicios

Y ahora comprobamos el acceso a Internet enviando ping, petición HTTP y petición DNS. **Nota**: Tener en cuenta que el curl no devuelve nada debido a un fallo con el certificado, y el nslookup tampoco porque esa IP no tiene ningún nombre asociado, pero ambas peticiones demuestran la conectividad de dichos protocolos.

```
munics@municsPOD:~$ ping 192.0.1.2
PING 192.0.1.2 (192.0.1.2) 56(84) bytes of data.
64 bytes from 192.0.1.2: icmp_seq=1 ttl=253 time=1.73 ms
64 bytes from 192.0.1.2: icmp_seq=2 ttl=253 time=1.38 ms
64 bytes from 192.0.1.2: icmp_seq=3 ttl=253 time=1.33 ms
^C
--- 192.0.1.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 1.325/1.476/1.725/0.177 ms
munics@municsPOD:~$ curl 192.0.1.2
curl: (7) Failed to connect to 192.0.1.2 port 80 after 2 ms: Couldn't connect to server
munics@municsPOD:~$ nslookup 192.0.1.2
** server can't find 2.1.0.192.in-addr.arpa: NXDOMAIN
```

Figure 18: Conectividad a Internet desde Servicios

4.4 Configuración de la interfaz de servicios

Para que estas pruebas pudiesen realizarse correctamente, fue necesario configurar de forma adecuada la conectividad del servidor situado en la red de Servicios, añadiendo rutas estáticas hacia las redes internas y externas correspondientes.

```
munics@municsPOD:~$ sudo cat /etc/netplan/00-installer-config.yaml
[sudo] password for munics:
# This is the network config written by 'subiquity'
network:
  ethernets:
    ens160:
      addresses:
      - 10.254.164.32/24
      dhcp4: false
      gateway4: 10.254.164.1
      nameservers:
        addresses:
        - 193.144.48.30
        - 193.144.48.100
        search: []
    ens192:
      addresses:
        - 10.1.240.100/24
      dhcp4: false
      routes:
        - to: 10.1.0.0/16
          via: 10.1.240.1
        - to: 192.168.0.0/16
          via: 10.1.240.1
        - to: 192.0.0.0/16
          via: 10.1.240.1
  version: 2
```

Figure 19: Configuración de red mediante netplan

La Figura 19 muestra la configuración de `netplan` utilizada. En ella se definen direcciones IP estáticas para ambas interfaces de red y se añaden rutas específicas que permiten alcanzar las redes internas del laboratorio a través del firewall. Esta configuración es necesaria para garantizar la correcta comunicación entre el servidor de Servicios, el firewall y el ISP durante las pruebas.

5 Configuración de NAT

En el escenario propuesto el dispositivo que actúa como *router frontera* es el CPE. Sobre él se ha configurado NAT para:

- Permitir que las VLAN de usuarios (16, 17 y 18) salgan a Internet mediante PAT dinámico, usando una única IP pública por VLAN.
- Publicar los servicios HTTP/HTTPS de la máquina de servicios (`10.1.240.100`) hacia Internet mediante *port-forwarding*.

En primer lugar se marcan las interfaces del CPE como *inside* (hacia la red corporativa) y *outside* (hacia el ISP).

```
interface GigabitEthernet0/0.3
 ip address 10.1.0.6 255.255.255.252
 ip nat inside

interface GigabitEthernet0/1
 ip address 192.0.1.1 255.255.255.0
 ip nat outside
```

5.1 Configuración de PAT dinámico

Para cumplir la política del laboratorio, cada VLAN de usuarios debe utilizar una única dirección IP pública:

- VLAN16 (`10.1.16.0/24`) → `192.0.1.200`
- VLAN17 (`10.1.17.0/24`) → `192.0.1.201`
- VLAN18 (`10.1.18.0/24`) → `192.0.1.202`

Para ello se han definido tres ACL estándar que identifican las redes internas y tres pools de NAT con las IP públicas asociadas. Finalmente, se activa PAT con la opción overload.

```

ip access-list standard NAT-VLAN16
 permit 10.1.16.0 0.0.0.255
ip access-list standard NAT-VLAN17
 permit 10.1.17.0 0.0.0.255
ip access-list standard NAT-VLAN18
 permit 10.1.18.0 0.0.0.255

ip nat pool Vlan16 192.0.1.200 192.0.1.200 netmask 255.255.255.0
ip nat pool Vlan17 192.0.1.201 192.0.1.201 netmask 255.255.255.0
ip nat pool Vlan18 192.0.1.202 192.0.1.202 netmask 255.255.255.0

ip nat inside source list NAT-VLAN16 pool Vlan16 overload
ip nat inside source list NAT-VLAN17 pool Vlan17 overload
ip nat inside source list NAT-VLAN18 pool Vlan18 overload
```

Listing 1: Configuración de PAT dinámico por VLAN en el CPE

Con esta configuración, todas las conexiones salientes desde las VLAN 16, 17 y 18 comparten la misma IP pública correspondiente a su VLAN, diferenciándose mediante números de puerto.

5.2 Configuración de port-forwarding

Además del tráfico saliente, la organización publica hacia Internet los servicios HTTP y HTTPS de la máquina de servicios (`10.1.240.100`) ubicada en la VLAN de servicios. Para ello se ha configurado *NAT estático de puerto* (*port-forwarding*), de forma que las peticiones externas a `192.0.1.203` se traduzcan al servidor interno.

```
ip nat inside source static tcp 10.1.240.100 80  192.0.1.203 80  extendable
ip nat inside source static tcp 10.1.240.100 443 192.0.1.203 443 extendable
```

De este modo:

- Cualquier conexión dirigida a `192.0.1.203:80` se redirige a `10.1.240.100:80` (HTTP).
- Cualquier conexión dirigida a `192.0.1.203:443` se redirige a `10.1.240.100:443` (HTTPS).

5.3 Pruebas para la NAT

5.3.1 Pruebas exterior-interior

En el segmento del ISP no disponemos de una máquina virtual de pruebas y, además, las ACL configuradas en el CPE bloquean cualquier acceso genérico desde Internet. Por ello, la validación de la NAT desde fuera se ha limitado a realizar ping desde el router ISP hacia las direcciones que el CPE expone en su interfaz externa: la propia IP del CPE (`192.0.1.1`) y la dirección pública asociada al servidor de servicios (`192.0.1.203`).

```
ISP# ping 192.0.1.203
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.0.1.203, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
ISP#
ISP# ping 192.0.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.0.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
ISP#
ISP#
ISP#
```

Figure 20: Ping desde ISP a las direcciones públicas del CPE.

Si la configuración de NAT o el direccionamiento en el CPE fueran incorrectos, el router ISP no podría resolver `192.0.1.203` en su segmento ni recibir respuestas ICMP desde esa dirección, y estos ping fallarían sistemáticamente.

5.3.2 Pruebas interior-exterior

Para verificar la conectividad interior–exterior y que la NAT permite el tráfico saliente desde las VLAN de usuarios, se realiza un ping desde una máquina de la VLAN 18 (host 10.1.18.66) hacia la IP del ISP (192.0.1.2).

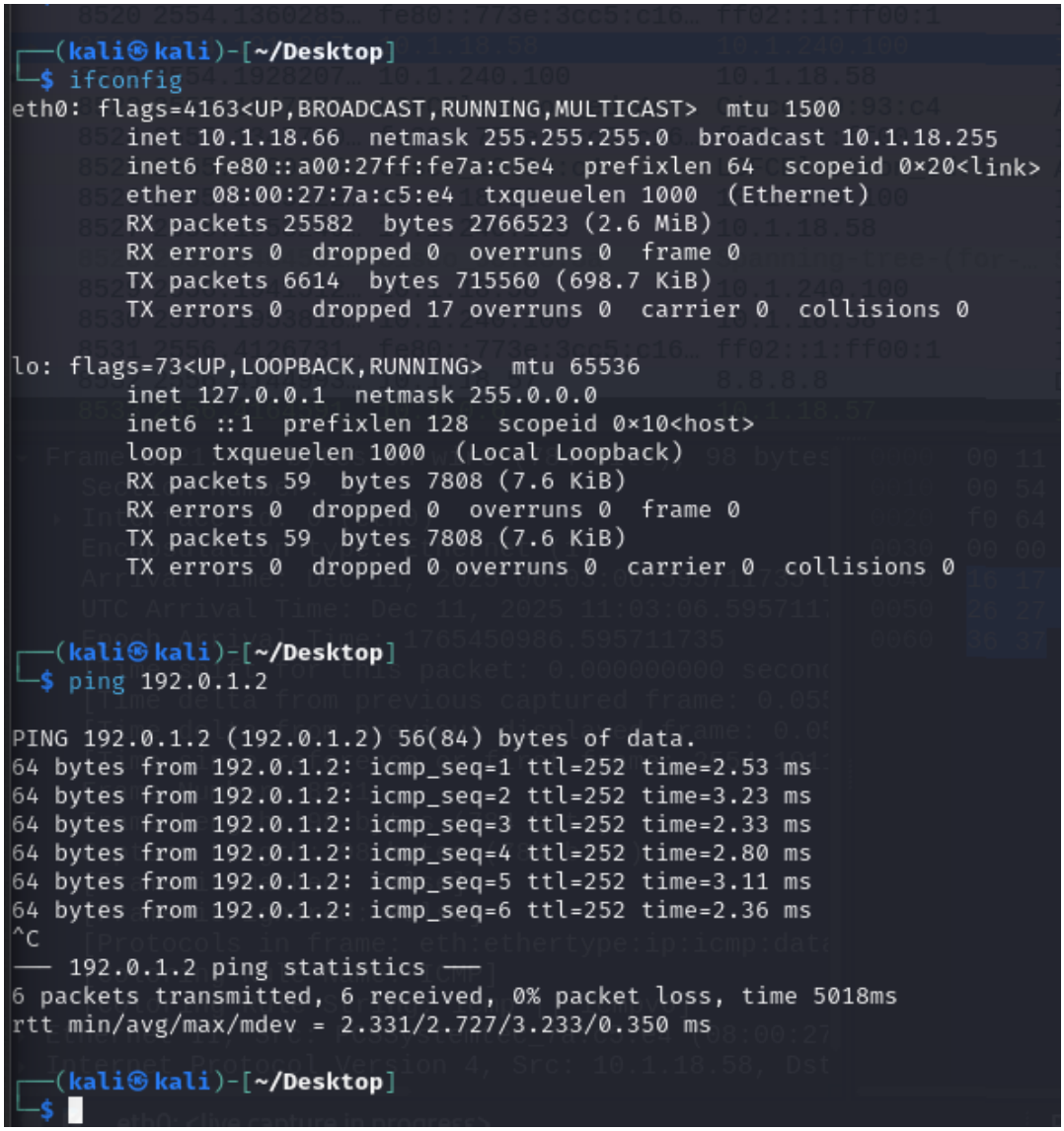

Figure 21: Ping desde Vlan 18 a ISP.

5.3.3 Pruebas desde el router frontera CPE

Dado que en este router se encuentra configurada la NAT, resulta adecuado comprobar la tabla de traducciones y la tabla de estadísticas, verificando que ambas se corresponden con la configuración realizada previamente.

```
CPE#
CPE#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
udp 192.0.1.202:52112  10.1.18.60:52112   8.8.8.8:53         8.8.8.8:53
udp 192.0.1.202:55955  10.1.18.60:55955   8.8.8.8:53         8.8.8.8:53
udp 192.0.1.202:57640  10.1.18.60:57640   8.8.8.8:53         8.8.8.8:53
udp 192.0.1.202:9993   10.1.18.64:9993    79.127.159.187:9993 79.127.159.187:9993
udp 192.0.1.202:9993   10.1.18.64:9993    84.17.53.155:9993  84.17.53.155:9993
udp 192.0.1.202:9993   10.1.18.64:9993    103.195.103.66:9993 103.195.103.66:9993
udp 192.0.1.202:9993   10.1.18.64:9993    185.152.67.145:9993 185.152.67.145:9993
udp 192.0.1.202:53028  10.1.18.64:53028   79.127.159.187:9993 79.127.159.187:9993
udp 192.0.1.202:53028  10.1.18.64:53028   84.17.53.155:9993  84.17.53.155:9993
udp 192.0.1.202:53028  10.1.18.64:53028   103.195.103.66:9993 103.195.103.66:9993
udp 192.0.1.202:53028  10.1.18.64:53028   185.152.67.145:9993 185.152.67.145:9993
udp 192.0.1.202:61837  10.1.18.64:61837   79.127.159.187:9993 79.127.159.187:9993
udp 192.0.1.202:61837  10.1.18.64:61837   84.17.53.155:9993  84.17.53.155:9993
udp 192.0.1.202:61837  10.1.18.64:61837   103.195.103.66:9993 103.195.103.66:9993
udp 192.0.1.202:61837  10.1.18.64:61837   185.152.67.145:9993 185.152.67.145:9993
tcp 192.0.1.203:80     10.1.240.100:80    ---                ---
tcp 192.0.1.203:443    10.1.240.100:443   ---                ---
CPE#
```

Figure 22: Tabla de traducciones.

```
CPE#show ip nat statistics
Total active translations: 16 (2 static, 14 dynamic; 16 extended)
Peak translations: 51, occurred 1d00h ago
Outside interfaces:
  GigabitEthernet0/1
Inside interfaces:
  GigabitEthernet0/0.3
Hits: 1408  Misses: 0
CEF Translated packets: 416, CEF Punted packets: 23758
Expired translations: 192
Dynamic mappings:
-- Inside Source
[Id: 4] access-list NAT-VLAN16 pool Vlan16 refcount 0
 pool Vlan16: netmask 255.255.255.0
        start 192.0.1.200 end 192.0.1.200
        type generic, total addresses 1, allocated 0 (0%), misses 0
[Id: 5] access-list NAT-VLAN17 pool Vlan17 refcount 0
 pool Vlan17: netmask 255.255.255.0
        start 192.0.1.201 end 192.0.1.201
        type generic, total addresses 1, allocated 0 (0%), misses 0
[Id: 6] access-list NAT-VLAN18 pool Vlan18 refcount 14
 pool Vlan18: netmask 255.255.255.0
        start 192.0.1.202 end 192.0.1.202
        type generic, total addresses 1, allocated 1 (100%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
CPE#
```

Figure 23: Tabla de estadísticas.

6 Running-Configs de todo el escenario

6.1 AL-SW1

```
!
! Last configuration change at 21:21:35 UTC Sun Mar 28 1993 by superMunics
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname AL-SW1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$4ggR$iNwcR8H.ugsTaXxgbLjRE0
enable password munics
!
username juniorAdmin secret 5 $1$d7AC$tqsCDMtxIT2qtcTB6Q1e60
username admin privilege 15 secret 5 $1$4JQN$abPigzcy1C8p.ZxNfzcKI.
aaa new-model
!
!
aaa authentication login default group radius local
aaa authentication login AAA-LOGIN group radius local
aaa authorization exec AAA-AUTHZ group radius local if-authenticated
!
!
!
!
!
aaa session-id common
system mtu routing 1500
ip arp inspection vlan 16-18
!
!
ip dhcp snooping vlan 16-18
no ip dhcp snooping information option
ip dhcp snooping
ip domain-name munics.pri
!
!
crypto pki trustpoint TP-self-signed-4271428480
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-4271428480
 revocation-check none
 rsakeypair TP-self-signed-4271428480
!
!
crypto pki certificate chain TP-self-signed-4271428480
 certificate self-signed 01
  30820249 308201B2 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 34323731 34323834 3830301E 170D3933 30333031 30303031
  30395A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D34 32373134
  32383438 3030819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  810085E1 0E0FF69D 55BAA4B8 3242956C 88BA4A20 007F0BAE 7C775218 787A4D1E
  6A592433 AC88CA8D F2E44FA1 8B8061E1 0640595E AB331A30 7231D400 87C14740
```

```
  12109636 B239C3DE AB88408E 9479B0AF 0FE5CCBD 29B2AA25 3092B8C2 4953E0E1
  D0A43208 26766077 ADB9F855 EC64E3EA BE46ACC2 C1683A25 5A016AF6 A6C90A66
  EAFD0203 010001A3 71306F30 0F060355 1D130101 FF040530 030101FF 301C0603
  551D1104 15301382 11414C2D 5357312E 6D756E69 63732E70 7269301F 0603551D
  23041830 16801424 61E8C2FF 22D3F0BC 988C64AA 5150C191 90078430 1D060355
  1D0E0416 04142461 E8C2FF22 D3F0BC98 8C64AA51 50C19190 0784300D 06092A86
  4886F70D 01010405 00038181 003C7B6B BD62DE1F 846CB7BC 2DD4AC14 18346E36
  94077A12 17788E9F 779BDC53 EC20C9E8 76522AF6 3BCB2F13 29B0536B CBDBB47A
  92923AE7 A68A5C1D 240F8583 88A15EE8 336A4BFC 7F51A462 BBDC05DB 4966E706
  3128FD1E 3A7293C8 8E2EF904 05DE8ED6 914029F8 57EC6202 A6C8F86E D18F5A8B
  FF5A5A6A 686C2158 574E7941 F1
    quit
!
!
!
spanning-tree mode pvst
spanning-tree portfast bpduguard default
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
ip ssh time-out 60
ip ssh version 2
!
!
!
!
!
interface GigabitEthernet0/1
 switchport access vlan 739
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet0/2
 switchport access vlan 16
 switchport mode access
 switchport port-security maximum 10
 switchport port-security violation protect
 no cdp enable
 spanning-tree portfast
 ip dhcp snooping limit rate 10
!
interface GigabitEthernet0/3
 switchport access vlan 16
 switchport mode access
 switchport port-security maximum 10
 switchport port-security violation protect
 no cdp enable
 spanning-tree portfast
 ip dhcp snooping limit rate 10
!
interface GigabitEthernet0/4
 switchport access vlan 16
 switchport mode access
 switchport port-security maximum 10
 switchport port-security violation protect
 no cdp enable
 spanning-tree portfast
 ip dhcp snooping limit rate 10
!
interface GigabitEthernet0/5
 switchport access vlan 17
```

```
 switchport mode access
 switchport port-security maximum 10
 switchport port-security violation protect
 no cdp enable
 spanning-tree portfast
 ip dhcp snooping limit rate 10
!
interface GigabitEthernet0/6
 switchport access vlan 17
 switchport mode access
 switchport port-security maximum 10
 switchport port-security violation protect
 no cdp enable
 spanning-tree portfast
 ip dhcp snooping limit rate 10
!
interface GigabitEthernet0/7
 switchport access vlan 17
 switchport mode access
 switchport port-security maximum 10
 switchport port-security violation protect
 no cdp enable
 spanning-tree portfast
 ip dhcp snooping limit rate 10
!
interface GigabitEthernet0/8
 switchport access vlan 18
 switchport mode access
 switchport port-security maximum 10
 switchport port-security violation protect
 no cdp enable
 spanning-tree portfast
 ip dhcp snooping limit rate 10
!
interface GigabitEthernet0/9
 switchport access vlan 18
 switchport mode access
 switchport port-security maximum 10
 switchport port-security violation protect
 no cdp enable
 spanning-tree portfast
 ip dhcp snooping limit rate 10
!
interface GigabitEthernet0/10
 switchport access vlan 18
 switchport mode access
 switchport port-security maximum 10
 switchport port-security violation protect
 no cdp enable
 spanning-tree portfast
 ip dhcp snooping limit rate 10
!
interface GigabitEthernet0/11
 switchport access vlan 88
 switchport mode access
 shutdown
!
interface GigabitEthernet0/12
 switchport access vlan 88
 switchport mode access
 shutdown
!
```

```
interface GigabitEthernet0/13
 switchport access vlan 88
 switchport mode access
 shutdown
!
interface GigabitEthernet0/14
 switchport access vlan 88
 switchport mode access
 shutdown
!
interface GigabitEthernet0/15
 switchport access vlan 88
 switchport mode access
 shutdown
!
interface GigabitEthernet0/16
 switchport access vlan 88
 switchport mode access
 shutdown
!
interface GigabitEthernet0/17
 switchport access vlan 88
 switchport mode access
 shutdown
!
interface GigabitEthernet0/18
 switchport access vlan 88
 switchport mode access
 shutdown
!
interface GigabitEthernet0/19
 switchport access vlan 88
 switchport mode access
 shutdown
!
interface GigabitEthernet0/20
 switchport trunk allowed vlan 16-18,739
 switchport mode trunk
 switchport nonegotiate
 ip arp inspection trust
 ip dhcp snooping trust
!
interface GigabitEthernet0/21
 switchport access vlan 88
 switchport mode access
 shutdown
!
interface GigabitEthernet0/22
 switchport access vlan 88
 switchport mode access
 shutdown
!
interface GigabitEthernet0/23
 switchport access vlan 88
 switchport mode access
 shutdown
!
interface GigabitEthernet0/24
 switchport access vlan 88
 switchport mode access
 shutdown
!
```

```
interface Vlan1
 no ip address
 shutdown
!
interface Vlan739
 ip address 10.1.239.1 255.255.255.0
!
ip http server
ip http secure-server
!
ip access-list standard ACL-MGMT
 remark Solo gestion desde VLAN Pod1-adm
 permit 10.1.239.0 0.0.0.255
 deny   any log
logging esm config
!
radius server RAD1
 address ipv4 10.1.239.100 auth-port 1812 acct-port 1813
 key Bayern_2025
!
!
!
line con 0
 password munics
line vty 0 4
 password munics
 authorization exec AAA-AUTHZ
 login authentication AAA-LOGIN
 transport input ssh
line vty 5 15
!
end
```

Listing 2: Running Config del AL-SW1

6.2 DL-SW1

```
!
version 12.2
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname DL-SW1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$zKX1$6XtnZqAyzRsANPWZbyDWH.
enable password munics
!
!
!
aaa new-model
!
!
aaa authentication login AAA-LOGIN group radius local
aaa authentication login CONSOLE group radius local
aaa authorization exec AAA-AUTHZ group radius local if-authenticated
aaa authorization exec CONSOLE group radius local
!
!
!
aaa session-id common
system mtu routing 1500
ip routing
ip domain-name munics.pri
!
!
!
!
crypto pki trustpoint TP-self-signed-3139015552
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-3139015552
 revocation-check none
 rsakeypair TP-self-signed-3139015552
!
!
crypto pki certificate chain TP-self-signed-3139015552
 certificate self-signed 01
  30820249 308201B2 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
  31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 33313339 30313535 3532301E 170D3933 30333031 30303030
  35365A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
  4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 31333930
  31353535 3230819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
  8100EEF0 77B70D39 C077512A 5E183579 2E051087 D4B06526 22A76CB5 11FCC6EC
  A3F2516A DFBE4837 104CF317 B63576B7 7FE48A7B 2F3F8F01 C095FB6A F3F9A15C
  F3E052FB F2B60124 6A6BF8DD B2C6DD7A 175F496A 3228903B B6288596 B7F15493
  4BFF2578 D16AB815 F61B3253 F8E5B0C9 EC236C7B DBD2802D 5CF30BAB 806A39E8
  54E50203 010001A3 71306F30 0F060355 1D130101 FF040530 030101FF 301C0603
  551D1104 15301382 11444C2D 5357312E 6D756E69 63732E70 7269301F 0603551D
  23041830 168014EB 2849A1D4 49DFF386 2F8F4A87 7DA4977D 18848B30 1D060355
  1D0E0416 0414EB28 49A1D449 DFF3862F 8F4A877D A4977D18 848B300D 06092A86
  4886F70D 01010405 00038181 00307FFD AB23E244 74634FD5 44EB45CC C0211344
  3C00652E 97E7E5CE EA8C42D9 FE518876 D5172237 6090DABE 211B3531 38A323B1
```

```
  D3C37783 BF1CDC40 CFB0AD25 AD830DB0 4B30792F BC6F3D7C E9EC5056 03153280
  6D2B31A0 6DC1BEC7 24691E7D 095F8D2E 98384A30 3DD6DBDD 5E3771FE 454907D6
  C72687DF FB681141 C5E6CD8A FF
  quit
!
!
!
!
spanning-tree mode pvst
spanning-tree extend system-id
spanning-tree vlan 16-18,739,745 priority 24576
!
vlan internal allocation policy ascending
!
ip ssh time-out 60
ip ssh version 2
!
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 16-18,739
 switchport mode trunk
!
interface FastEthernet0/13
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 2,739,740
 switchport mode trunk
!
interface FastEthernet0/14
 switchport access vlan 3
 switchport mode access
!
interface FastEthernet0/15
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 3,739
 switchport mode trunk
!
interface FastEthernet0/16
 switchport access vlan 4
```

```
 switchport mode access
!
interface FastEthernet0/17
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 4,739
 switchport mode trunk
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 739,740
 switchport mode trunk
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan2
 ip address 10.1.0.1 255.255.255.252
 ip ospf network point-to-point
 ip ospf 1 area 0
!
interface Vlan16
 ip address 10.1.16.1 255.255.255.0
 ip access-group ACL-DL-VLAN16-IN in
 ip helper-address 10.1.239.100
 ip ospf 1 area 0
!
interface Vlan17
 ip address 10.1.17.1 255.255.255.0
 ip access-group ACL-DL-VLAN17-IN in
 ip helper-address 10.1.239.100
 ip ospf 1 area 0
!
interface Vlan18
 ip address 10.1.18.1 255.255.255.0
 ip access-group ACL-DL-VLAN18-IN in
 ip helper-address 10.1.239.100
 ip ospf 1 area 0
!
interface Vlan739
 ip address 10.1.239.2 255.255.255.0
!
router ospf 1
 log-adjacency-changes
 passive-interface default
 no passive-interface Vlan2
```

```
 network 10.1.0.0 0.0.0.3 area 0
 network 10.1.16.0 0.0.0.255 area 0
 network 10.1.17.0 0.0.0.255 area 0
 network 10.1.18.0 0.0.0.255 area 0
!
ip classless
ip http server
ip http secure-server
!
!
ip access-list standard ACL-MGMT
 remark Solo gestion desde VLAN Pod1-adm
 permit 10.1.239.0 0.0.0.255
 deny   any log
!
ip access-list extended ACL-DL-VLAN16-IN
 remark BLOQUEO VLANS 17 y 18
 deny   ip 10.1.16.0 0.0.0.255 10.1.17.0 0.0.0.255
 deny   ip 10.1.16.0 0.0.0.255 10.1.18.0 0.0.0.255
 permit ip any any
 remark DHCP OFFER
ip access-list extended ACL-DL-VLAN17-IN
 remark BLOQUEO VLANS 16 y 17
 deny   ip 10.1.17.0 0.0.0.255 10.1.16.0 0.0.0.255
 deny   ip 10.1.17.0 0.0.0.255 10.1.18.0 0.0.0.255
 remark DHCP OFFER
 permit ip any any
ip access-list extended ACL-DL-VLAN18-IN
 remark BLOQUEO VLANS 16 y 18
 deny   ip 10.1.18.0 0.0.0.255 10.1.16.0 0.0.0.255
 deny   ip 10.1.18.0 0.0.0.255 10.1.17.0 0.0.0.255
 remark DHCP OFFER
 permit ip any any
!
ip sla enable reaction-alerts
!
radius-server host 10.1.239.100 auth-port 1812 acct-port 1813 key Bayern_2025
!
!
line con 0
 password munics
line vty 0 4
 access-class ACL-MGMT in
 password munics
 authorization exec AAA-AUTHZ
 login authentication AAA-LOGIN
 transport input ssh
line vty 5 15
!
end
```

Listing 3: Running Config del DL-SW1

6.3 FW (VERSIÓN ACL + CBACs)

```
!
! Last configuration change at 15:18:54 UTC Fri Dec 12 2025 by superMunics
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname FW
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$iaUf$/YbICUZAx7Df3Gwn6CYTC1
enable password munics
!
aaa new-model
!
!
aaa authentication login AAA-LOGIN group radius local
aaa authentication login SSH-LOGIN group radius local
aaa authentication login CONSOLE group radius local
aaa authorization exec AAA-AUTHZ group radius local if-authenticated
aaa authorization exec SSH-LOGIN group radius local
aaa authorization exec CONSOLE group radius local
!
!
!
!
!
aaa session-id common
memory-size iomem 15
!
!
!
!
!
!
!
!
!


!
!
!
!
ip domain name munics.pri
ip inspect name CBAC tcp timeout 300
ip inspect name CBAC udp timeout 30
ip inspect name CBAC icmp timeout 10
ip inspect name CBAC-INTERNET tcp timeout 300
ip inspect name CBAC-INTERNET icmp timeout 10
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
```

```
!
license udi pid CISCO1941/K9 sn FCZ1731609A
license boot c1900 technology-package securityk9
license boot c1900 technology-package datak9
!
!
username juniorAdmin secret 5 $1$7V/v$HXT2XqfZZ1yakmQIW/YxH1
username admin privilege 15 secret 5 $1$XJKK$2EQITMry7Lf7ROhltEAcL.
!
redundancy
!
!
!
!
!
ip ssh time-out 60
ip ssh version 2
!
!
!
!
!
!
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 description Trunk to DL-SW1 F0/13
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.2
 encapsulation dot1Q 2
 ip address 10.1.0.2 255.255.255.252
 ip inspect CBAC in
 ip ospf network point-to-point
!
interface GigabitEthernet0/0.739
 description ADM (Pod1)
 encapsulation dot1Q 739
 ip address 10.1.239.3 255.255.255.0
!
interface GigabitEthernet0/0.740
 encapsulation dot1Q 740
 ip address 10.1.240.1 255.255.255.0
 ip access-group ACL-SERVICIOS-FW in
 ip inspect CBAC in
!
interface GigabitEthernet0/1
 ip address 10.1.0.5 255.255.255.252
 ip access-group ACL-INTERNET-IN in
 ip inspect CBAC in
 ip ospf network point-to-point
 duplex auto
 speed auto
!
```

```
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
router ospf 1
 passive-interface default
 no passive-interface GigabitEthernet0/0.2
 no passive-interface GigabitEthernet0/1
 network 10.1.0.0 0.0.255.255 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
ip access-list standard ACL-MGMT
 remark Solo gestion desde VALN Pod1_adm
 permit 10.1.239.0 0.0.0.255
 deny   any log
!
ip access-list extended ACL-FW-IN
 remark ACCESO DE DISPOSITIVOS AL SERVIDOR DHCP
 permit udp any host 10.1.239.100 eq bootps
 permit udp any host 10.1.239.100 eq bootpc
 remark OSPF
 permit ospf host 10.1.0.1 host 224.0.0.5
 permit ospf host 10.1.0.1 host 10.1.0.2
 permit ospf host 10.1.0.2 host 224.0.0.5
 permit ospf host 10.1.0.2 host 10.1.0.1
 remark ACCESO A SERVICIOS VLAN 16
 permit tcp 10.1.16.0 0.0.0.255 host 10.1.240.100 eq www
 permit tcp 10.1.16.0 0.0.0.255 host 10.1.240.100 eq 443
 permit tcp 10.1.16.0 0.0.0.255 host 10.1.240.100 eq domain
 permit udp 10.1.16.0 0.0.0.255 host 10.1.240.100 eq domain
 permit icmp 10.1.16.0 0.0.0.255 host 10.1.240.100 echo
 remark ACCESO A INTERNET VLAN 16
 permit tcp 10.1.16.0 0.0.0.255 any eq www
 permit tcp 10.1.16.0 0.0.0.255 any eq 443
 permit udp 10.1.16.0 0.0.0.255 any eq domain
 permit icmp 10.1.16.0 0.0.0.255 any echo
 remark ACCESO A SERVICIOS VLAN 17
 permit tcp 10.1.17.0 0.0.0.255 host 10.1.240.100 eq www
 permit tcp 10.1.17.0 0.0.0.255 host 10.1.240.100 eq 443
 permit tcp 10.1.17.0 0.0.0.255 host 10.1.240.100 eq domain
 permit udp 10.1.17.0 0.0.0.255 host 10.1.240.100 eq domain
 permit icmp 10.1.17.0 0.0.0.255 host 10.1.240.100 echo
 remark ACCESO A INTERNET VLAN 17
 permit tcp 10.1.17.0 0.0.0.255 any eq www
 permit tcp 10.1.17.0 0.0.0.255 any eq 443
 permit udp 10.1.17.0 0.0.0.255 any eq domain
 permit icmp 10.1.17.0 0.0.0.255 any echo
 remark ACCESO A SERVICIOS VLAN 18
 permit tcp 10.1.18.0 0.0.0.255 host 10.1.240.100 eq www
 permit tcp 10.1.18.0 0.0.0.255 host 10.1.240.100 eq 443
 permit tcp 10.1.18.0 0.0.0.255 host 10.1.240.100 eq domain
```

```
 permit udp 10.1.18.0 0.0.0.255 host 10.1.240.100 eq domain
 permit icmp 10.1.18.0 0.0.0.255 host 10.1.240.100 echo
 remark ACCESO A INTERNET VLAN 18
 permit tcp 10.1.18.0 0.0.0.255 any eq www
 permit tcp 10.1.18.0 0.0.0.255 any eq 443
 permit udp 10.1.18.0 0.0.0.255 any eq domain
 permit icmp 10.1.18.0 0.0.0.255 any echo
 deny   ip any any
ip access-list extended ACL-INTERNET-FW
 permit ospf host 10.1.0.6 host 224.0.0.5
 permit ospf host 10.1.0.6 host 10.1.0.5
 permit ospf host 10.1.0.5 host 224.0.0.5
 permit ospf host 10.1.0.5 host 10.1.0.6
 permit tcp any host 10.1.240.100 eq 443
 permit icmp any host 10.1.240.100 echo
 deny   ip any 10.1.0.0 0.0.255.255
 deny   ip any any
ip access-list extended ACL-SERVICIOS-FW
remark DENEGAR CONEXIONES VLAN
deny ip any 10.1.16.0 0.0.0.255
deny ip any 10.1.17.0 0.0.0.255
deny ip any 10.1.18.0 0.0.0.255

permit tcp 10.1.240.0 0.0.0.255 any eq 80
permit tcp 10.1.240.0 0.0.0.255 any eq 443
permit tcp 10.1.240.0 0.0.0.255 any eq 53
permit udp 10.1.240.0 0.0.0.255 any eq 53
permit icmp 10.1.240.0 0.0.0.255 any

deny ip any any
!
ip radius source-interface GigabitEthernet0/0.739
!
!
!
radius server RAD1
 address ipv4 10.1.239.100 auth-port 1812 acct-port 1813
 key Bayern_2025
!
!
!
control-plane
!
!
!
line con 0
 password munics
 login authentication CONSOLE
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 access-class ACL-MGMT in
 password munics
 authorization exec AAA-AUTHZ
 login authentication AAA-LOGIN
 transport input ssh
!
```

```
scheduler allocate 20000 1000
!
end
```

Listing 4: Running Config del FW con ACLs y CBACs

6.4 FW (Versión ZBFW)

```
FW#show run
Building configuration...

Current configuration : 5144 bytes
!
! Last configuration change at 16:08:13 UTC Thu Dec 11 2025 by superMunics
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname FW
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$iaUf$/YbICUZAx7Df3Gwn6CYTC1
enable password munics
!
aaa new-model
!
!
aaa authentication login AAA-LOGIN group radius local
aaa authentication login SSH-LOGIN group radius local
aaa authentication login CONSOLE group radius local
aaa authorization exec AAA-AUTHZ group radius local if-authenticated
aaa authorization exec SSH-LOGIN group radius local
aaa authorization exec CONSOLE group radius local
!
!
!
!
!
aaa session-id common
memory-size iomem 15
!
!
!
!
!
!
!
!
!


!
!
!
!
ip domain name munics.pri
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
```

```
license udi pid CISCO1941/K9 sn FCZ1731609A
license boot c1900 technology-package securityk9
license boot c1900 technology-package datak9
!
!
username juniorAdmin secret 5 $1$7V/v$HXT2XqfZZ1yakmQIW/YxH1
username admin privilege 15 secret 5 $1$XJKK$2EQITMry7Lf7ROhltEAcL.
!
redundancy
!
!
!
!
!
ip ssh time-out 60
ip ssh version 2
!
class-map type inspect match-any CM-DMZ-TO-OUTSIDE
 match access-group name ACL-DMZ-SERVER
 match protocol tcp
 match protocol udp
 match protocol icmp
class-map type inspect match-any CM-OUTSIDE-TO-DMZ
 match access-group name ACL-DMZ-SERVER
 match protocol icmp
 match protocol tcp
class-map type inspect match-any CM-CONTROL
 match access-group name ACL-DHCP
 match access-group name ACL-OSPF
class-map type inspect match-any CM-INSIDE-TO-OUTSIDE
 match access-group name ACL-INSIDE
 match protocol tcp
 match protocol udp
 match protocol icmp
class-map type inspect match-any CM-INSIDE-TO-DMZ
 match access-group name ACL-INSIDE
 match access-group name ACL-DMZ-SERVER
 match protocol tcp
 match protocol udp
 match protocol icmp
!
policy-map type inspect PM-DMZ-TO-OUTSIDE
 class type inspect CM-DMZ-TO-OUTSIDE
  inspect
 class class-default
  drop
policy-map type inspect PM-INSIDE-TO-OUTSIDE
 class type inspect CM-INSIDE-TO-OUTSIDE
  inspect
 class type inspect CM-CONTROL
  pass
 class class-default
  drop
policy-map type inspect PM-OUTSIDE-TO-DMZ
 class type inspect CM-OUTSIDE-TO-DMZ
  inspect
 class class-default
  drop
policy-map type inspect PM-INSIDE-TO-DMZ
 class type inspect CM-INSIDE-TO-DMZ
  inspect
 class type inspect CM-CONTROL
```

```
  pass
 class class-default
  drop
!
zone security INSIDE
zone security DMZ
zone security OUTSIDE
zone-pair security ZP-INSIDE-TO-DMZ source INSIDE destination DMZ
 service-policy type inspect PM-INSIDE-TO-DMZ
zone-pair security ZP-INSIDE-TO-OUTSIDE source INSIDE destination OUTSIDE
 service-policy type inspect PM-INSIDE-TO-OUTSIDE
zone-pair security ZP-DMZ-TO-OUTSIDE source DMZ destination OUTSIDE
 service-policy type inspect PM-DMZ-TO-OUTSIDE
zone-pair security ZP-OUTSIDE-TO-DMZ source OUTSIDE destination DMZ
 service-policy type inspect PM-OUTSIDE-TO-DMZ
!
!
!
!
!
!
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 description Trunk to DL-SW1 F0/13
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.2
 encapsulation dot1Q 2
 ip address 10.1.0.2 255.255.255.252
 zone-member security INSIDE
 ip ospf network point-to-point
!
interface GigabitEthernet0/0.739
 description ADM (Pod1)
 encapsulation dot1Q 739
 ip address 10.1.239.3 255.255.255.0
!
interface GigabitEthernet0/0.740
 encapsulation dot1Q 740
 ip address 10.1.240.1 255.255.255.0
 zone-member security OUTSIDE
!
interface GigabitEthernet0/1
 ip address 10.1.0.5 255.255.255.252
 zone-member security OUTSIDE
 ip ospf network point-to-point
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
```

```
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
router ospf 1
 passive-interface default
 no passive-interface GigabitEthernet0/0.2
 no passive-interface GigabitEthernet0/1
 network 10.1.0.0 0.0.255.255 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
!
ip access-list standard ACL-MGMT
 remark Solo gestion desde VALN Pod1_adm
 permit 10.1.239.0 0.0.0.255
 deny   any log
!
ip access-list extended ACL-DHCP
 permit udp any host 10.1.239.100 eq bootps
 permit udp any host 10.1.239.100 eq bootpc
ip access-list extended ACL-DMZ-SERVER
 permit ip any host 10.1.240.100
ip access-list extended ACL-INSIDE
 permit ip 10.1.16.0 0.0.0.255 any
 permit ip 10.1.17.0 0.0.0.255 any
 permit ip 10.1.18.0 0.0.0.255 any
ip access-list extended ACL-OSPF
 permit ospf any any
!
ip radius source-interface GigabitEthernet0/0.739
!
!
!
radius server RAD1
 address ipv4 10.1.239.100 auth-port 1812 acct-port 1813
 key Bayern_2025
!
!
!
control-plane
!
!
!
line con 0
 password munics
 login authentication CONSOLE
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 access-class ACL-MGMT in
 password munics
```

```
 authorization exec AAA-AUTHZ
 login authentication AAA-LOGIN
 transport input ssh
!
scheduler allocate 20000 1000
!
end
```

Listing 5: Running Config del FW con ZBFW

6.5 CPE

```
!
! Last configuration change at 19:46:13 UTC Fri Dec 12 2025 by superMunics
!
version 15.7
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CPE
!
boot-start-marker
boot-end-marker
!
!
enable secret 5 $1$3FPY$n.Qd8MGjf/Gdju/Fd6Ai2.
enable password munics
!
aaa new-model
!
!
aaa authentication login AAA-LOGIN group radius local
aaa authentication login CONSOLE group radius local
aaa authorization exec AAA-AUTHZ group radius local if-authenticated
aaa authorization exec CONSOLE group radius local
!
!
!
!
!
!
aaa session-id common
!
!
!
!
!
!
!
!
!
!
!
!
!
ip domain name munics.pri
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
license udi pid CISCO1941/K9 sn FHK14287AAC
!
!
username admin privilege 15 secret 5 $1$C97z$JGvHtFWUCPaWk9XVeyx310
username juniorAdmin secret 5 $1$Jm7P$ZdkceIBDI6WeyrwRy2DXt1
!
redundancy
!
!
```

```
!
!
!
!
!
!
!
!
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.3
 encapsulation dot1Q 3
 ip address 10.1.0.6 255.255.255.252
 ip nat inside
 ip virtual-reassembly in
 ip ospf network point-to-point
!
interface GigabitEthernet0/0.739
 encapsulation dot1Q 739
 ip address 10.1.239.4 255.255.255.0
!
interface GigabitEthernet0/1
 ip address 192.0.1.1 255.255.255.0
 ip access-group ACL-CPE-STATIC-IN in
 ip nat outside
 ip virtual-reassembly in
 duplex auto
 speed auto
!
router ospf 1
 redistribute static subnets
 passive-interface default
 no passive-interface GigabitEthernet0/0.3
 network 10.1.0.4 0.0.0.3 area 0
 default-information originate
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip nat pool Vlan16 192.0.1.200 192.0.1.200 netmask 255.255.255.0
ip nat pool Vlan17 192.0.1.201 192.0.1.201 netmask 255.255.255.0
ip nat pool Vlan18 192.0.1.202 192.0.1.202 netmask 255.255.255.0
ip nat inside source list NAT-VLAN16 pool Vlan16 overload
ip nat inside source list NAT-VLAN17 pool Vlan17 overload
ip nat inside source list NAT-VLAN18 pool Vlan18 overload
ip nat inside source static tcp 10.1.240.100 80 192.0.1.203 80 extendable
ip nat inside source static tcp 10.1.240.100 443 192.0.1.203 443 extendable
ip route 0.0.0.0 0.0.0.0 192.0.1.2
```

```
ip ssh time-out 60
ip ssh version 2
!
ip access-list standard ACL-CPE-STATIC-IN
 deny   10.0.0.0 0.255.255.255
 deny   172.16.0.0 0.15.255.255
 deny   192.168.0.0 0.0.255.255
 deny   169.254.0.0 0.0.255.255
 deny   192.0.2.0 0.0.0.255
 deny   198.51.100.0 0.0.0.255
 deny   203.0.113.0 0.0.0.255
 deny   100.64.0.0 0.63.255.255
 deny   127.0.0.0 0.255.255.255
 deny   0.0.0.0 0.255.255.255
 deny   224.0.0.0 15.255.255.255
 deny   240.0.0.0 15.255.255.255
 permit any
ip access-list standard ACL-MGMT
 permit 10.1.239.0 0.0.0.255
 deny   any log
ip access-list standard NAT-VLAN16
 permit 10.1.16.0 0.0.0.255
ip access-list standard NAT-VLAN17
 permit 10.1.17.0 0.0.0.255
ip access-list standard NAT-VLAN18
 permit 10.1.18.0 0.0.0.255
!
ip access-list extended ACL-INTERNET-FW
 deny   ip any any
!
!
!
!
radius server RAD1
 address ipv4 10.1.239.100 auth-port 1812 acct-port 1813
 key Bayern_2025
!
!
!
control-plane
!
!
line con 0
 password munics
 login authentication CONSOLE
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 access-class ACL-MGMT in
 password munics
 authorization exec AAA-AUTHZ
 login authentication AAA-LOGIN
 transport input ssh
!
scheduler allocate 20000 1000
!
end
```

Listing 6: Running Config del CPE

6.6 ISP

```
!
! Last configuration change at 18:26:14 UTC Thu Dec 11 2025 by superMunics
!
version 15.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname ISP
!
boot-start-marker
boot-end-marker
!
!
no logging console
enable secret 5 $1$Pyez$rusV3Zwb.xaThFtrZJgsP/
enable password munics
!
aaa new-model
!
!
aaa authentication login SSH-LOGIN group radius local
aaa authentication login CONSOLE group radius local
aaa authorization exec SSH-LOGIN group radius local
aaa authorization exec CONSOLE group radius local
!
!
!
!
!
aaa session-id common
memory-size iomem 15
!
!
!
!
!
!
!
!
!


!
!
!
!
ip domain name munics.pri
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
!
!
license udi pid CISCO1941/K9 sn FCZ1626901Y
license boot c1900 technology-package datak9
!
!
username juniorAdmin secret 5 $1$1n22$4rNzB0PvcUyeIGzyU1h7R0
```

```
username admin privilege 15 secret 5 $1$AgDE$8L9VyE7FY3JaKLgNZMtad.
!
redundancy
!
!
!
!
!
ip ssh version 2
!
!
!
!
!
!
!
!
!
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 description TRUNK link to DL-SW1 F0/17
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.4
 encapsulation dot1Q 4
 ip address 192.0.1.2 255.255.255.0
!
interface GigabitEthernet0/0.739
 description ADM (VLAN 739)
 encapsulation dot1Q 739
 ip address 10.1.239.5 255.255.255.0
!
interface GigabitEthernet0/1
 ip address 192.0.0.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
 clock rate 2000000
!
ip forward-protocol nd
!
no ip http server
ip http secure-server
!
ip route 10.1.0.0 255.255.0.0 192.0.1.1
!
ip access-list standard MGMT-ONLY
 permit 10.1.239.0 0.0.0.255
```

```
 deny   any log
!
ip radius source-interface GigabitEthernet0/0.739
!
!
radius-server host 10.1.239.100 auth-port 1812 acct-port 1813 key Bayern_2025
!
!
!
control-plane
!
!
!
line con 0
 logging synchronous
 login authentication CONSOLE
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 access-class MGMT-ONLY in
 authorization exec SSH-LOGIN
 login authentication SSH-LOGIN
 transport input ssh
!
scheduler allocate 20000 1000
!
end
```

Listing 7: Running Config del ISP