



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 máquina 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.

```
munics@municsPOD:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
            inet6 ::1/128 scope host noprefixroute
                valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:96:f7:de brd ff:ff:ff:ff:ff:ff
        altname enp3s0
        inet 10.254.164.32/24 brd 10.254.164.255 scope global ens160
            valid_lft forever preferred_lft forever
            inet6 fe80::250:56ff:fe96:f7de/64 scope link
                valid_lft forever preferred_lft forever
3: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:96:e4:2c brd ff:ff:ff:ff:ff:ff
        altname enp11s0
        inet 10.1.240.100/24 brd 10.1.240.255 scope global ens192
            valid_lft forever preferred_lft forever
            inet6 fe80::250:56ff:fe96:e42c/64 scope link
                valid_lft forever preferred_lft forever
munics@municsPOD:~$
```

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 optó 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.

```
lines 1-24/24 (END)
● apache2.service - The Apache HTTP Server
  Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
  Active: active (running) since Wed 2025-11-26 17:36:09 UTC; 1 week 6 days ago
    Docs: https://httpd.apache.org/docs/2.4/
  Process: 255401 ExecReload=/usr/sbin/apachectl graceful (code=exited, status=0/SUCCESS)
 Main PID: 172013 (apache2)
   Tasks: 55 (limit: 4605)
  Memory: 6.8M (peak: 10.2M)
     CPU: 1min 33.005s
    CGroup: /system.slice/apache2.service
            └─172013 /usr/sbin/apache2 -k start
              ├─255406 /usr/sbin/apache2 -k start
              └─255407 /usr/sbin/apache2 -k start
```

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.

```

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

```

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

```

munics@municsPOD:~$ curl -v http://10.1.240.100
* Trying 10.1.240.100:80...
* Connected to 10.1.240.100 (10.1.240.100) port 80
> GET / HTTP/1.1
> Host: 10.1.240.100
> User-Agent: curl/8.5.0
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Wed, 10 Dec 2025 07:10:46 GMT
< Server: Apache/2.4.58 (Ubuntu)
< Last-Modified: Wed, 26 Nov 2025 17:36:08 GMT
< ETag: "29af-64482dd4de4e96"
< Accept-Ranges: bytes
< Content-Length: 10671
< Vary: Accept-Encoding
< Content-Type: text/html
<
<!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

```

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.

```

1 sudo a2enmod ssl
2 sudo a2ensite default-ssl

```

A continuación se generó un certificado autofirmado utilizando openssl:

```

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

```

Después, 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:

```

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

```

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

```

3. 10.254.164.32 (munics) × +
munics@municsPOD:~$ curl -vk https://10.1.240.100
*   Trying 10.1.240.100:443...
* Connected to 10.1.240.100 (10.1.240.100) port 443
* ALPN: curl offers h2,http/1.1
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.3 (IN), TLS handshake, Encrypted Extensions (8):
* TLSv1.3 (IN), TLS handshake, Certificate (11):
* TLSv1.3 (IN), TLS handshake, CERT verify (15):
* TLSv1.3 (IN), TLS handshake, Finished (20):
* TLSv1.3 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.3 (OUT), TLS handshake, Finished (20):
* SSL connection using TLSv1.3 / TLS_AES_256_GCM_SHA384 / X25519 / RSASSA-PSS
* ALPN: server accepted http/1.1
* Server certificate:
*   subject: C=ES; ST=Galicia; L=A Coruña; O=MUNICS Pod1; OU=Pod1 - Grupo 1; CN=MUNICS; emailAddress=munics@udc.es
*   start date: Nov 26 17:38:48 2025 GMT
*   expire date: Nov 26 17:38:48 2026 GMT
*   issuer: C=ES; ST=Galicia; L=A Coruña; O=MUNICS Pod1; OU=Pod1 - Grupo 1; CN=MUNICS; emailAddress=munics@udc.es
*   SSL certificate verify result: self-signed certificate (18), continuing anyway.
*   Certificate level 0: Public key type RSA (2048/112 Bits/secBits), signed using sha256WithRSAEncryption
*   using HTTP/1.x
> GET / HTTP/1.1
> Host: 10.1.240.100
> User-Agent: curl/8.5.0
> Accept: */*

```

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

```
1 sudo systemctl status bind9
```

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

```
Last login: Wed Dec 10 09:36:42 2025 from 10.20.38.71
munics@municsPOD:~$ sudo systemctl status bind9
[sudo] password for munics:
● named.service - BIND Domain Name Server
    Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; preset: enabled)
      Active: active (running) since Fri 2025-11-28 11:31:22 UTC; 1 week 4 days ago
        Docs: man:named(8)
     Main PID: 232063 (named)
       Status: "running"
        Tasks: 8 (limit: 4605)
      Memory: 23.3M (peak: 23.8M)
         CPU: 3.077s
      CGroup: /system.slice/named.service
              └─232063 /usr/sbin/named -f -u bind

dic 10 07:56:36 municsPOD named[232063]: network unreachable resolving './NS/IN': 2001:500:9f::42#53
dic 10 07:56:36 municsPOD named[232063]: network unreachable resolving './NS/IN': 2001:1b8:10::b#53
dic 10 07:56:36 municsPOD named[232063]: network unreachable resolving './NS/IN': 2001:503:c27::2:30#53
dic 10 07:56:36 municsPOD named[232063]: network unreachable resolving './NS/IN': 2001:500:a8::e#53
dic 10 07:56:36 municsPOD named[232063]: network unreachable resolving './NS/IN': 2001:500:2::c#53
dic 10 07:56:36 municsPOD named[232063]: network unreachable resolving './NS/IN': 2001:dc3::35#53
dic 10 07:56:36 municsPOD named[232063]: network unreachable resolving './NS/IN': 2001:500:2f::f#53
dic 10 07:56:36 municsPOD named[232063]: network unreachable resolving './NS/IN': 2001:500:1::53#53
dic 10 07:56:46 municsPOD named[232063]: network unreachable resolving './NS/IN': 2001:500:12::d0d#53
dic 10 07:56:46 municsPOD named[232063]: resolver printing query complete: timed out
munics@municsPOD:~$
```

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.

```
1
2 options {
3   directory "/var/cache/bind";
4
5   listen-on { 127.0.0.1; 10.1.240.100; };
6   listen-on-v6 { none; };
7
8   allow-query { any; };
9   recursion yes;
10
11  forwarders {
12    193.144.48.30;
13    193.144.48.100;
14    8.8.8.8;
15    8.8.4.4;
16  };
}
```

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

```
1 // zona directa
2 zone "munics.pri" {
3   type master;
4   file "/etc/bind/munics.db";
5 };
6
7 // zona inversa
8 zone "240.1.10.in-addr.arpa" {
9   type master;
10  file "/etc/bind/10.1.240.rev";
11};
```

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:

```
1 ;
2 ; Zona directa para munics.pri
3 ;
```

```

4 $ORIGIN munics.pri.
5 $TTL 1D
6
7 @ IN SOA munics.pri. root.munics.pri. (
8     2025112701 ; Serial
9     604800    ; Refresh
10    86400     ; Retry
11    2419200   ; Expire
12    604800 )  ; Default TTL
13
14    IN NS    srv1-deb.munics.pri.
15
16 ; Alias "dns" apuntando al servidor
17 dns      IN CNAME srv1-deb
18
19 ; Servidor de servicios
20 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.

```

1 $TTL 1D
2
3 @ IN SOA munics.pri. root.munics.pri. (
4     2025112701 ; Serial
5     604800
6     86400
7     2419200
8     604800 )
9
10    IN NS    srv1-deb.munics.pri.
11
12
13 100 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.

```

1 nameserver 127.0.0.1
2 search munics.pri

```

Una vez aplicada la configuración se ha recargado el servicio.

```

1 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:

```

munics@municsPOD:~$ dig @10.1.240.100 google.com

; <>> DiG 9.18.39-0ubuntu0.24.04.2-Ubuntu <>> @10.1.240.100 google.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 13888
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: ffc93fbdc148d25901000000693927b496e245b48f4d2be5 (good)
;; QUESTION SECTION:
;google.com.           IN      A

;; ANSWER SECTION:
google.com.        19      IN      A      142.250.185.14

;; Query time: 77 msec
;; SERVER: 10.1.240.100#53(10.1.240.100) (UDP)
;; WHEN: Wed Dec 10 07:56:36 UTC 2025
;; MSG SIZE rcvd: 83

munics@municsPOD:~$ █

```

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:

```

munics@municsPOD:~$ dig @10.1.240.100 srv1-deb.munics.pri

; <>> DiG 9.18.39-0ubuntu0.24.04.2-Ubuntu <>> @10.1.240.100 srv1-deb.munics.pri
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 28226
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: 18116fc62581dcbb01000000693927e2b3713c2d08cb1ade (good)
;; QUESTION SECTION:
;srv1-deb.munics.pri.       IN      A

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

;; Query time: 0 msec
;; SERVER: 10.1.240.100#53(10.1.240.100) (UDP)
;; WHEN: Wed Dec 10 07:57:22 UTC 2025
;; MSG SIZE rcvd: 92

```

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:

```
munics@municsPOD:~$ dig @10.1.240.100 -x 10.1.240.100
; <>> DiG 9.18.39-0ubuntu0.24.04.2-Ubuntu <>> @10.1.240.100 -x 10.1.240.100
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29372
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: 21bae7b330759fec010000006939281db4817c4bb4af0d6a (good)
;; QUESTION SECTION:
;100.240.1.10.in-addr.arpa. IN PTR
;; ANSWER SECTION:
100.240.1.10.in-addr.arpa. 86400 IN PTR srv1-deb.munics.pri.
;; Query time: 1 msec
;; SERVER: 10.1.240.100#53(10.1.240.100) (UDP)
;; WHEN: Wed Dec 10 07:58:21 UTC 2025
;; MSG SIZE rcvd: 115
munics@municsPOD:~$
```

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 permitral 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.

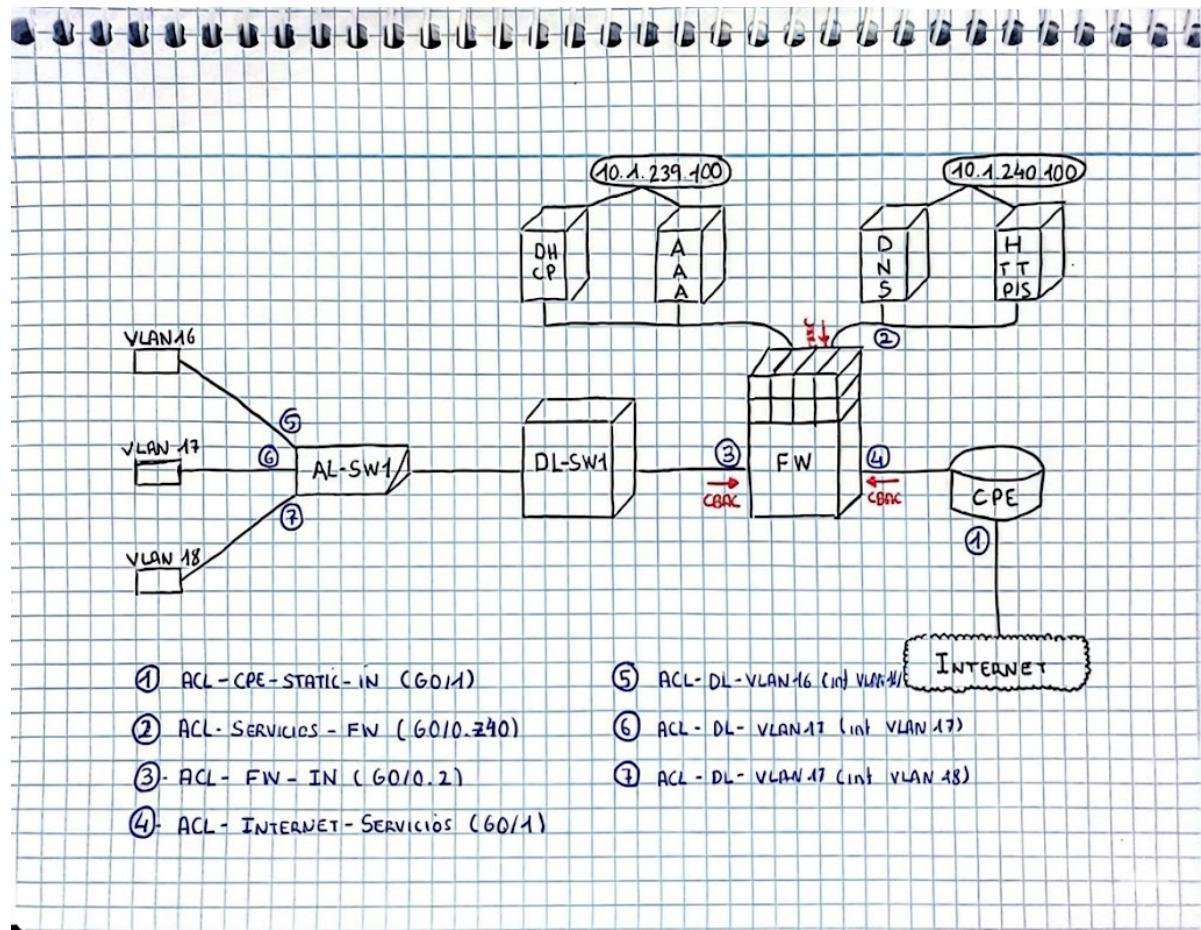


Figure 9: Topología Lógica

## 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.

```
1 !privadas
2 access-list 1 deny 10.0.0.0 0.255.255.255
3 access-list 1 deny 172.16.0.0 0.15.255.255
4 access-list 1 deny 192.168.0.0 0.0.255.255
5 !enlace local
6 access-list 1 deny 169.254.0.0 0.0.255.255
7 !multicast
8 access-list 1 deny 224.0.0.0 15.255.255.255
9 !broadcast
10 access-list 1 deny host 255.255.255.255
11 !loopback
12 access-list 1 deny 127.0.0.0 0.255.255.255
13 !propio fw
14 access-list 1 deny host 127.0.0.1
15 !red actual
16 access-list 1 deny 0.0.0.0 0.255.255.255
17 !otras direcciones peligrosas
18 !testnet1
19 access-list 1 deny 192.0.2.0 0.0.0.255
20 !testnet2
21 access-list 1 deny 198.51.100.0 0.0.0.255
22 !testnet3
23 access-list 1 deny 203.0.113.0 0.0.0.255
24 !usos futuros reservada
25 access-list 1 deny 240.0.0.0 15.255.255.255
26 !otras a justificar
27 !CGNAT Carrier-Grade Nat
28 access-list 1 deny 100.64.0.0 0.63.255.255
29 !permitir el resto
30 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.

```
1 interface GigabitEthernet0/1
2   ip address 192.0.1.1 255.255.255.0
3   ip access-group ACL-CPE-STATIC-IN in
4   ip nat outside
5   ip virtual-reassembly in
6   duplex auto
7   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):

```
1 ip access-list extended ACL-DL-VLAN16-IN
2 remark BLOQUEO VLANS 17 y 18
3 deny ip 10.1.16.0 0.0.0.255 10.1.17.0 0.0.0.255
4 deny ip 10.1.16.0 0.0.0.255 10.1.18.0 0.0.0.255
5 permit ip any any
6 remark DHCP OFFER
7 ip access-list extended ACL-DL-VLAN17-IN
8 remark BLOQUEO VLANS 16 y 17
9 deny ip 10.1.17.0 0.0.0.255 10.1.16.0 0.0.0.255
10 deny ip 10.1.17.0 0.0.0.255 10.1.18.0 0.0.0.255
11 remark DHCP OFFER
12 permit ip any any
13 ip access-list extended ACL-DL-VLAN18-IN
14 remark BLOQUEO VLANS 16 y 18
15 deny ip 10.1.18.0 0.0.0.255 10.1.16.0 0.0.0.255
16 deny ip 10.1.18.0 0.0.0.255 10.1.17.0 0.0.0.255
17 remark DHCP OFFER
18 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

```
1 ip access-list extended ACL-FW-IN
2 remark ACCESO DE DISPOSITIVOS AL SERVIDOR DHCP
3 permit udp any host 10.1.239.100 eq bootps
4 permit udp any host 10.1.239.100 eq bootpc
5 remark OSPF
6 permit ospf host 10.1.0.1 host 224.0.0.5
7 permit ospf host 10.1.0.1 host 10.1.0.2
8 permit ospf host 10.1.0.2 host 224.0.0.5
9 permit ospf host 10.1.0.2 host 10.1.0.1
10 remark ACCESO A SERVICIOS VLAN 16
11 permit tcp 10.1.16.0 0.0.0.255 host 10.1.240.100 eq www
12 permit tcp 10.1.16.0 0.0.0.255 host 10.1.240.100 eq 443
13 permit tcp 10.1.16.0 0.0.0.255 host 10.1.240.100 eq domain
14 permit udp 10.1.16.0 0.0.0.255 host 10.1.240.100 eq domain
15 permit icmp 10.1.16.0 0.0.0.255 host 10.1.240.100 echo
16 remark ACCESO A INTERNET VLAN 16
17 permit tcp 10.1.16.0 0.0.0.255 any eq www
18 permit tcp 10.1.16.0 0.0.0.255 any eq 443
19 permit udp 10.1.16.0 0.0.0.255 any eq domain
20 permit icmp 10.1.16.0 0.0.0.255 any echo
21 remark ACCESO A SERVICIOS VLAN 17
22 permit tcp 10.1.17.0 0.0.0.255 host 10.1.240.100 eq www
23 permit tcp 10.1.17.0 0.0.0.255 host 10.1.240.100 eq 443
24 permit tcp 10.1.17.0 0.0.0.255 host 10.1.240.100 eq domain
25 permit udp 10.1.17.0 0.0.0.255 host 10.1.240.100 eq domain
26 permit icmp 10.1.17.0 0.0.0.255 host 10.1.240.100 echo
27 remark ACCESO A INTERNET VLAN 17
```

```

28  permit tcp 10.1.17.0 0.0.0.255 any eq www
29  permit tcp 10.1.17.0 0.0.0.255 any eq 443
30  permit udp 10.1.17.0 0.0.0.255 any eq domain
31  permit icmp 10.1.17.0 0.0.0.255 any echo
32  remark ACCESO A SERVICIOS VLAN 18
33  permit tcp 10.1.18.0 0.0.0.255 host 10.1.240.100 eq www
34  permit tcp 10.1.18.0 0.0.0.255 host 10.1.240.100 eq 443
35  permit tcp 10.1.18.0 0.0.0.255 host 10.1.240.100 eq domain
36  permit udp 10.1.18.0 0.0.0.255 host 10.1.240.100 eq domain
37  permit icmp 10.1.18.0 0.0.0.255 host 10.1.240.100 echo
38  remark ACCESO A INTERNET VLAN 18
39  permit tcp 10.1.18.0 0.0.0.255 any eq www
40  permit tcp 10.1.18.0 0.0.0.255 any eq 443
41  permit udp 10.1.18.0 0.0.0.255 any eq domain
42  permit icmp 10.1.18.0 0.0.0.255 any echo
43  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.

```

1  ip inspect name CBAC tcp timeout 300
2  ip inspect name CBAC udp timeout 30
3  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:

```

1  ip access-list extended ACL-SERVICIOS-FW
2  remark DENEGAR CONEXIONES VLAN
3  deny ip any 10.1.16.0 0.0.0.255
4  deny ip any 10.1.17.0 0.0.0.255
5  deny ip any 10.1.18.0 0.0.0.255
6
7  permit tcp 10.1.240.0 0.0.0.255 any eq 80
8  permit tcp 10.1.240.0 0.0.0.255 any eq 443
9  permit tcp 10.1.240.0 0.0.0.255 any eq 53
10  permit udp 10.1.240.0 0.0.0.255 any eq 53
11  permit icmp 10.1.240.0 0.0.0.255 any
12
13  deny ip any any

```

Además también aplicamos la CBAC para permitir conexiones de vuelta.

```

1  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:

```

1  ip access-list extended ACL-INTERNET-FW
2  permit ospf host 10.1.0.6 host 224.0.0.5
3  permit ospf host 10.1.0.6 host 10.1.0.5
4  permit ospf host 10.1.0.5 host 224.0.0.5
5  permit ospf host 10.1.0.5 host 10.1.0.6
6  permit tcp any host 10.1.240.100 eq 443
7  permit icmp any host 10.1.240.100 echo
8  deny ip any 10.1.0.0 0.0.255.255
9  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.

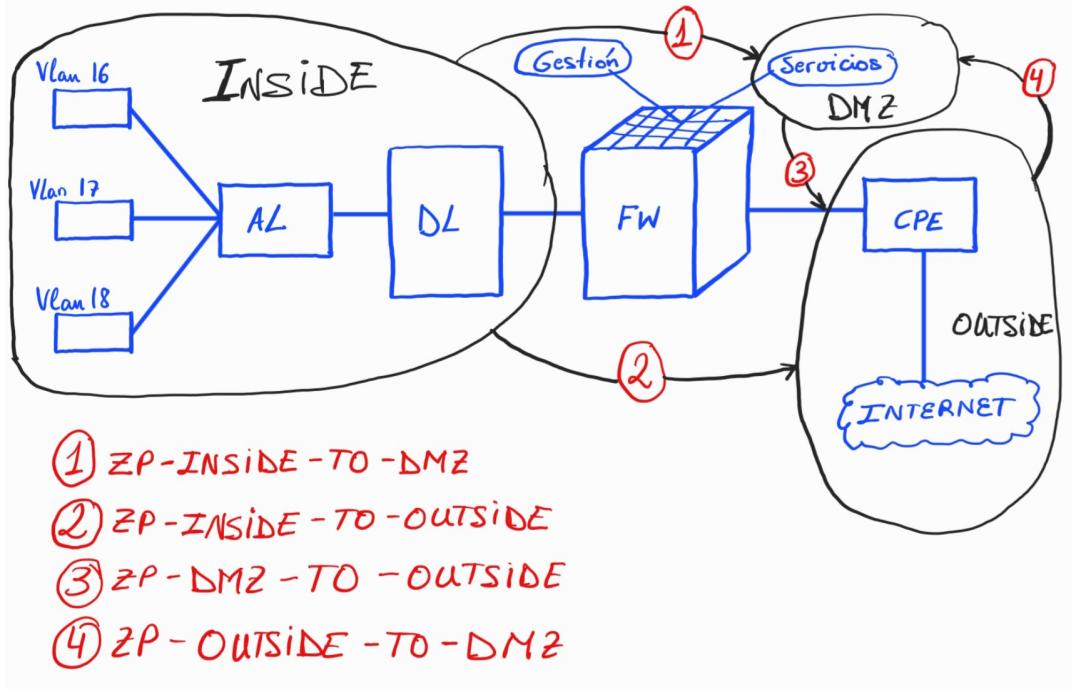


Figure 10: Zonas implementadas

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.

```

1 zone security INSIDE
2 zone security DMZ
3 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.

```

1 interface GigabitEthernet0/0.2
2 zone-member security INSIDE
3 !
4 interface GigabitEthernet0/0.740
5 zone-member security OUTSIDE
6 !
7 interface GigabitEthernet0/1
8 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.

```

1 ip access-list extended ACL-DHCP
2 permit udp any host 10.1.239.100 eq bootps
3 permit udp any host 10.1.239.100 eq bootpc
4 ip access-list extended ACL-DMZ-SERVER

```

```

5  permit ip any host 10.1.240.100
6  ip access-list extended ACL-INSIDE
7    permit ip 10.1.16.0 0.0.0.255 any
8    permit ip 10.1.17.0 0.0.0.255 any
9    permit ip 10.1.18.0 0.0.0.255 any
10   ip access-list extended ACL-OSPF
11     permit ospf any any
12 !

```

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.

```

1  class-map type inspect match-any CM-DMZ-TO-OUTSIDE
2    match access-group name ACL-DMZ-SERVER
3    match protocol tcp
4    match protocol udp
5    match protocol icmp
6  class-map type inspect match-any CM-OUTSIDE-TO-DMZ
7    match access-group name ACL-DMZ-SERVER
8    match protocol icmp
9    match protocol tcp
10   class-map type inspect match-any CM-CONTROL
11     match access-group name ACL-DHCP
12     match access-group name ACL-OSPF
13   class-map type inspect match-any CM-INSIDE-TO-OUTSIDE
14     match access-group name ACL-INSIDE
15     match protocol tcp
16     match protocol udp
17     match protocol icmp
18   class-map type inspect match-any CM-INSIDE-TO-DMZ
19     match access-group name ACL-INSIDE
20     match access-group name ACL-DMZ-SERVER
21     match protocol tcp
22     match protocol udp
23     match protocol icmp
24 !

```

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.

```

1  policy-map type inspect PM-DMZ-TO-OUTSIDE
2    class type inspect CM-DMZ-TO-OUTSIDE
3      inspect
4    class class-default
5      drop
6  policy-map type inspect PM-INSIDE-TO-OUTSIDE
7    class type inspect CM-INSIDE-TO-OUTSIDE
8      inspect
9    class type inspect CM-CONTROL
10      pass
11    class class-default
12      drop
13  policy-map type inspect PM-OUTSIDE-TO-DMZ
14    class type inspect CM-OUTSIDE-TO-DMZ
15      inspect
16    class class-default
17      drop
18  policy-map type inspect PM-INSIDE-TO-DMZ
19    class type inspect CM-INSIDE-TO-DMZ
20      inspect
21    class type inspect CM-CONTROL
22      pass

```

```

23 class class-default
24   drop
25 !

```

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.

```

1 zone-pair security ZP-INSIDE-TO-DMZ source INSIDE destination DMZ
2   service-policy type inspect PM-INSIDE-TO-DMZ
3 zone-pair security ZP-INSIDE-TO-OUTSIDE source INSIDE destination OUTSIDE
4   service-policy type inspect PM-INSIDE-TO-OUTSIDE
5 zone-pair security ZP-DMZ-TO-OUTSIDE source DMZ destination OUTSIDE
6   service-policy type inspect PM-DMZ-TO-OUTSIDE
7 zone-pair security ZP-OUTSIDE-TO-DMZ source OUTSIDE destination DMZ
8   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.

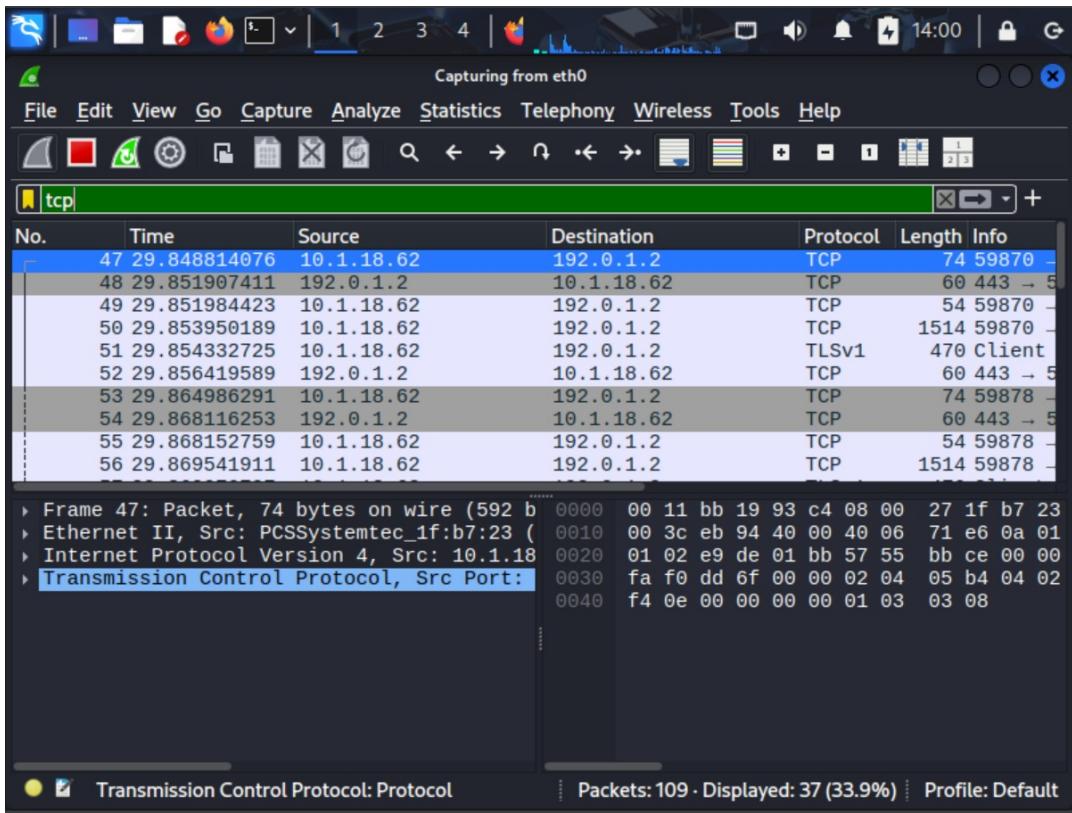


Figure 13: Captura de tráfico hacia el servidor en el ISP

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.

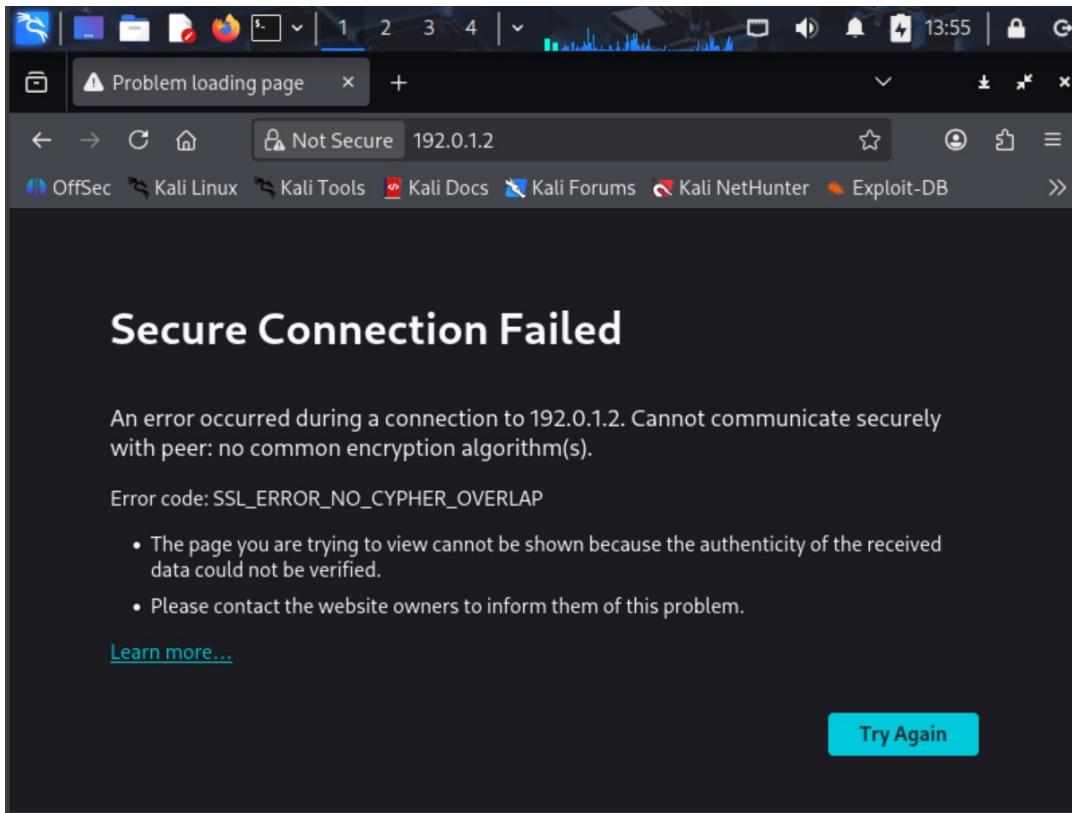


Figure 14: Acceso al servidor del ISP desde el navegador

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

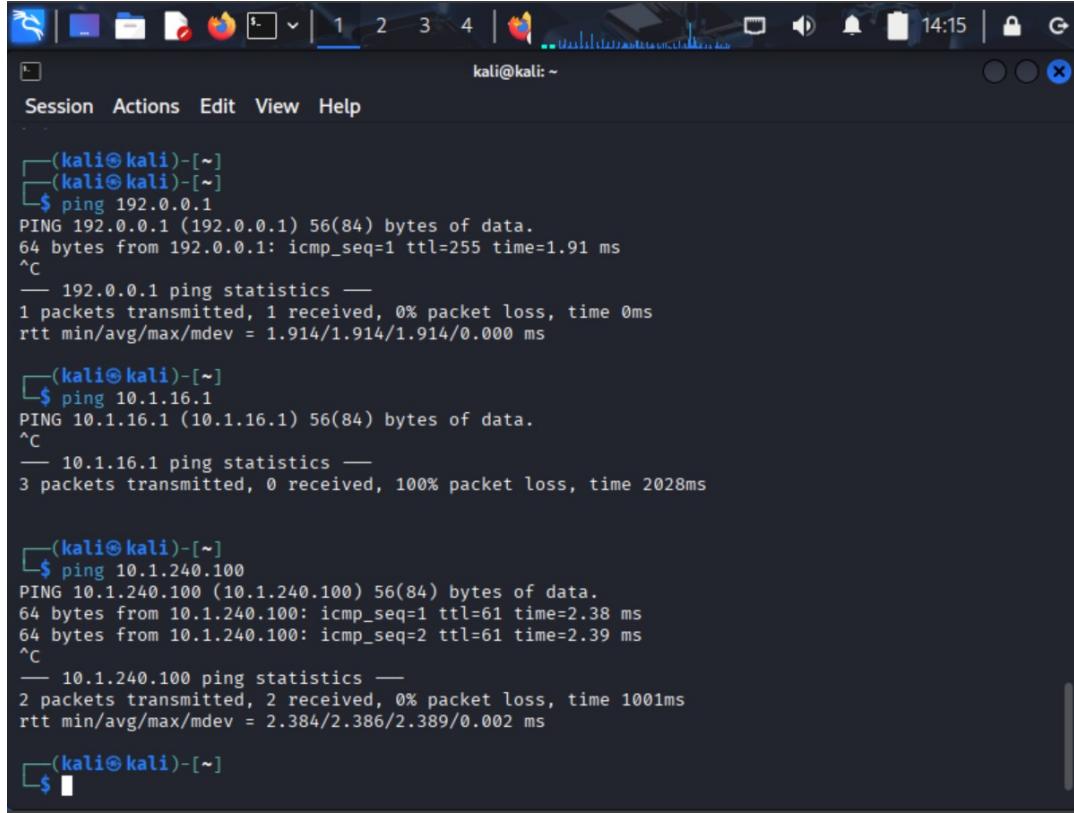
;; Query time: 4 msec
;; SERVER: 10.1.240.100#53(10.1.240.100) (UDP)
;; WHEN: Thu Dec 11 13:19:36 EST 2025
;; MSG SIZE  rcvd: 92
```

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.



The screenshot shows a terminal window titled 'kali@kali: ~' with a dark theme. It displays three separate ping commands:

- The first command pings the gateway at 192.0.0.1, showing successful results with 1 packet transmitted, 1 received, 0% loss, and a round-trip time of 1.91 ms.
- The second command pings a host at 10.1.16.1, showing 3 packets transmitted, 0 received, and 100% packet loss.
- The third command pings a host at 10.1.240.100, showing 2 packets transmitted, 2 received, 0% loss, and a round-trip time of 1001ms.

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).

```
1 interface GigabitEthernet0/0.3
2   ip address 10.1.0.6 255.255.255.252
3   ip nat inside
4
5 interface GigabitEthernet0/1
6   ip address 192.0.1.1 255.255.255.0
7   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.

```
1
2 ip access-list standard NAT-VLAN16
3   permit 10.1.16.0 0.0.0.255
4 ip access-list standard NAT-VLAN17
5   permit 10.1.17.0 0.0.0.255
6 ip access-list standard NAT-VLAN18
7   permit 10.1.18.0 0.0.0.255
8
9 ip nat pool Vlan16 192.0.1.200 192.0.1.200 netmask 255.255.255.0
10 ip nat pool Vlan17 192.0.1.201 192.0.1.201 netmask 255.255.255.0
11 ip nat pool Vlan18 192.0.1.202 192.0.1.202 netmask 255.255.255.0
12
13 ip nat inside source list NAT-VLAN16 pool Vlan16 overload
14 ip nat inside source list NAT-VLAN17 pool Vlan17 overload
15 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.

```

1 ip nat inside source static tcp 10.1.240.100 80 192.0.1.203 80 extendable
2 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).

```

 8520 2554.1360285... fe80::73e:3cc5:c16... ff02::1:ff00:1
└─(kali㉿kali)-[~/Desktop] 10.1.18.58 10.1.240.100
$ ifconfig
 8521 54.1928207... 10.1.240.100 10.1.18.58
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 193:c4
 8522     inet 10.1.18.66 netmask 255.255.255.0 broadcast 10.1.18.255
 8523     inet6 fe80::a00:27ff:fe7a:c5e4 prefixlen 64 scopeid 0x20<link>
 8524     ether 08:00:27:7a:c5:e4 txqueuelen 1000 (Ethernet) 10.1.18.58
 8525     RX packets 25582 bytes 2766523 (2.6 MiB) 10.1.18.58
 8526     RX errors 0 dropped 0 overruns 0 frame 0
 8527     TX packets 6614 bytes 715560 (698.7 KiB) 10.1.240.100
 8528     TX errors 0 dropped 17 overruns 0 carrier 0 collisions 0
 8529
 8530 2556.4126731... fe80::773e:3cc5:c16... ff02::1:ff00:1
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536 8.8.8.8
 8531     inet 127.0.0.1 netmask 255.0.0.0
 8532     inet6 ::1 prefixlen 128 scopeid 0x10<host>
 8533     loop txqueuelen 1000 (Local Loopback)
 8534     RX packets 59 bytes 7808 (7.6 KiB)
 8535     RX errors 0 dropped 0 overruns 0 frame 0
 8536     TX packets 59 bytes 7808 (7.6 KiB)
 8537     TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
 8538
 8539 UTC Arrival Time: Dec 11, 2025 11:03:06.5957111 0050 26 27
 8540 Ethernet Arrival Time: 1765450986.595711735 0060 36 37
└─(kali㉿kali)-[~/Desktop]
$ ping 192.0.1.2
 8541     for this packet: 0.000000000 seconds
 8542     Time delta from previous captured frame: 0.055
 8543     [Protocols in frame: eth:ethertype:ip:icmp:data]
PING 192.0.1.2 (192.0.1.2) 56(84) bytes of data.
 8544 64 bytes from 192.0.1.2: icmp_seq=1 ttl=252 time=2.53 ms
 8545 64 bytes from 192.0.1.2: icmp_seq=2 ttl=252 time=3.23 ms
 8546 64 bytes from 192.0.1.2: icmp_seq=3 ttl=252 time=2.33 ms
 8547 64 bytes from 192.0.1.2: icmp_seq=4 ttl=252 time=2.80 ms
 8548 64 bytes from 192.0.1.2: icmp_seq=5 ttl=252 time=3.11 ms
 8549 64 bytes from 192.0.1.2: icmp_seq=6 ttl=252 time=2.36 ms
^C
 8550     — 192.0.1.2 ping statistics —
 8551 6 packets transmitted, 6 received, 0% packet loss, time 5018ms
 8552 rtt min/avg/max/mdev = 2.331/2.727/3.233/0.350 ms
 8553
 8554 Internet Protocol Version 4, Src: 10.1.18.58, Dst:
└─(kali㉿kali)-[~/Desktop]
$ █

```

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# 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

```
1 !
2 ! Last configuration change at 21:21:35 UTC Sun Mar 28 1993 by superMunics
3 !
4 version 12.2
5 no service pad
6 service timestamps debug datetime msec
7 service timestamps log datetime msec
8 no service password-encryption
9 !
10 hostname AL-SW1
11 !
12 boot-start-marker
13 boot-end-marker
14 !
15 enable secret 5 $1$4ggR$iNwcR8H.ugsTaXxgbLjRE0
16 enable password munics
17 !
18 username juniorAdmin secret 5 $1$d7AC$tqsCDMtxIT2qtcTB6Q1e60
19 username admin privilege 15 secret 5 $1$4JQN$abPigzcy1C8p.ZxNfzcKI.
20 aaa new-model
21 !
22 !
23 aaa authentication login default group radius local
24 aaa authentication login AAA-LOGIN group radius local
25 aaa authorization exec AAA-AUTHZ group radius local if-authenticated
26 !
27 !
28 !
29 !
30 !
31 aaa session-id common
32 system mtu routing 1500
33 ip arp inspection vlan 16-18
34 !
35 !
36 ip dhcp snooping vlan 16-18
37 no ip dhcp snooping information option
38 ip dhcp snooping
39 ip domain-name munics.pri
40 !
41 !
42 crypto pki trustpoint TP-self-signed-4271428480
43 enrollment selfsigned
44 subject-name cn=IOS-Self-Signed-Certificate-4271428480
45 revocation-check none
46 rsakeypair TP-self-signed-4271428480
47 !
48 !
49 crypto pki certificate chain TP-self-signed-4271428480
50 certificate self-signed 01
51 30820249 308201B2 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
52 31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
53 69666963 6174652D 34323731 34323834 3830301E 170D3933 30333031 30303031
54 30395A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
55 4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D34 32373134
56 32383438 3030819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
57 810085E1 0E0FF69D 55BAA4B8 3242956C 88BA4A20 007F0BAE 7C775218 787A4D1E
58 6A592433 AC88CA8D F2E44FA1 8B8061E1 0640595E AB331A30 7231D400 87C14740
```

```

59  12109636 B239C3DE AB88408E 9479B0AF OFE5CCBD 29B2AA25 3092B8C2 4953E0E1
60  D0A43208 26766077 ADB9F855 EC64E3EA BE46ACC2 C1683A25 5A016AF6 A6C90A66
61  EAFD0203 010001A3 71306F30 0F060355 1D130101 FF040530 030101FF 301C0603
62  551D1104 15301382 11414C2D 5357312E 6D756E69 63732E70 7269301F 0603551D
63  23041830 16801424 61E8C2FF 22D3F0BC 988C64AA 5150C191 90078430 1D060355
64  1D0E0416 04142461 E8C2FF22 D3F0BC98 8C64AA51 50C19190 0784300D 06092A86
65  4886F70D 01010405 00038181 003C7B6B BD62DE1F 846CB7BC 2DD4AC14 18346E36
66  94077A12 17788E9F 779BDC53 EC20C9E8 76522AF6 3BCB2F13 29B0536B CBDDBB47A
67  92923AE7 A68A5C1D 240F8583 88A15EE8 336A4BFC 7F51A462 BBDC05DB 4966E706
68  3128FD1E 3A7293C8 8E2EF904 05DE8ED6 914029F8 57EC6202 A6C8F86E D18F5A8B
69  FF5A5A6A 686C2158 574E7941 F1
70  quit
71 !
72 !
73 !
74 spanning-tree mode pvst
75 spanning-tree portfast bpduguard default
76 spanning-tree extend system-id
77 !
78 vlan internal allocation policy ascending
79 !
80 ip ssh time-out 60
81 ip ssh version 2
82 !
83 !
84 !
85 !
86 !
87 interface GigabitEthernet0/1
88 switchport access vlan 739
89 switchport mode access
90 spanning-tree portfast
91 !
92 interface GigabitEthernet0/2
93 switchport access vlan 16
94 switchport mode access
95 switchport port-security maximum 10
96 switchport port-security violation protect
97 no cdp enable
98 spanning-tree portfast
99 ip dhcp snooping limit rate 10
100 !
101 interface GigabitEthernet0/3
102 switchport access vlan 16
103 switchport mode access
104 switchport port-security maximum 10
105 switchport port-security violation protect
106 no cdp enable
107 spanning-tree portfast
108 ip dhcp snooping limit rate 10
109 !
110 interface GigabitEthernet0/4
111 switchport access vlan 16
112 switchport mode access
113 switchport port-security maximum 10
114 switchport port-security violation protect
115 no cdp enable
116 spanning-tree portfast
117 ip dhcp snooping limit rate 10
118 !
119 interface GigabitEthernet0/5
120 switchport access vlan 17

```

```

121 switchport mode access
122 switchport port-security maximum 10
123 switchport port-security violation protect
124 no cdp enable
125 spanning-tree portfast
126 ip dhcp snooping limit rate 10
127 !
128 interface GigabitEthernet0/6
129   switchport access vlan 17
130   switchport mode access
131   switchport port-security maximum 10
132   switchport port-security violation protect
133   no cdp enable
134   spanning-tree portfast
135   ip dhcp snooping limit rate 10
136 !
137 interface GigabitEthernet0/7
138   switchport access vlan 17
139   switchport mode access
140   switchport port-security maximum 10
141   switchport port-security violation protect
142   no cdp enable
143   spanning-tree portfast
144   ip dhcp snooping limit rate 10
145 !
146 interface GigabitEthernet0/8
147   switchport access vlan 18
148   switchport mode access
149   switchport port-security maximum 10
150   switchport port-security violation protect
151   no cdp enable
152   spanning-tree portfast
153   ip dhcp snooping limit rate 10
154 !
155 interface GigabitEthernet0/9
156   switchport access vlan 18
157   switchport mode access
158   switchport port-security maximum 10
159   switchport port-security violation protect
160   no cdp enable
161   spanning-tree portfast
162   ip dhcp snooping limit rate 10
163 !
164 interface GigabitEthernet0/10
165   switchport access vlan 18
166   switchport mode access
167   switchport port-security maximum 10
168   switchport port-security violation protect
169   no cdp enable
170   spanning-tree portfast
171   ip dhcp snooping limit rate 10
172 !
173 interface GigabitEthernet0/11
174   switchport access vlan 88
175   switchport mode access
176   shutdown
177 !
178 interface GigabitEthernet0/12
179   switchport access vlan 88
180   switchport mode access
181   shutdown
182 !

```

```

183 interface GigabitEthernet0/13
184   switchport access vlan 88
185   switchport mode access
186   shutdown
187 !
188 interface GigabitEthernet0/14
189   switchport access vlan 88
190   switchport mode access
191   shutdown
192 !
193 interface GigabitEthernet0/15
194   switchport access vlan 88
195   switchport mode access
196   shutdown
197 !
198 interface GigabitEthernet0/16
199   switchport access vlan 88
200   switchport mode access
201   shutdown
202 !
203 interface GigabitEthernet0/17
204   switchport access vlan 88
205   switchport mode access
206   shutdown
207 !
208 interface GigabitEthernet0/18
209   switchport access vlan 88
210   switchport mode access
211   shutdown
212 !
213 interface GigabitEthernet0/19
214   switchport access vlan 88
215   switchport mode access
216   shutdown
217 !
218 interface GigabitEthernet0/20
219   switchport trunk allowed vlan 16-18,739
220   switchport mode trunk
221   switchport nonegotiate
222   ip arp inspection trust
223   ip dhcp snooping trust
224 !
225 interface GigabitEthernet0/21
226   switchport access vlan 88
227   switchport mode access
228   shutdown
229 !
230 interface GigabitEthernet0/22
231   switchport access vlan 88
232   switchport mode access
233   shutdown
234 !
235 interface GigabitEthernet0/23
236   switchport access vlan 88
237   switchport mode access
238   shutdown
239 !
240 interface GigabitEthernet0/24
241   switchport access vlan 88
242   switchport mode access
243   shutdown
244 !

```

```

245 interface Vlan1
246   no ip address
247   shutdown
248 !
249 interface Vlan739
250   ip address 10.1.239.1 255.255.255.0
251 !
252 ip http server
253 ip http secure-server
254 !
255 ip access-list standard ACL-MGMT
256   remark Solo gestion desde VLAN Pod1-adm
257   permit 10.1.239.0 0.0.0.255
258   deny   any log
259 logging esm config
260 !
261 radius server RAD1
262   address ipv4 10.1.239.100 auth-port 1812 acct-port 1813
263   key Bayern_2025
264 !
265 !
266 !
267 line con 0
268   password munics
269 line vty 0 4
270   password munics
271   authorization exec AAA-AUTHZ
272   login authentication AAA-LOGIN
273   transport input ssh
274 line vty 5 15
275 !
276 end

```

Listing 2: Running Config del AL-SW1

## 6.2 DL-SW1

```
1 !
2 version 12.2
3 no service pad
4 service timestamps debug datetime msec
5 service timestamps log datetime msec
6 no service password-encryption
7 !
8 hostname DL-SW1
9 !
10 boot-start-marker
11 boot-end-marker
12 !
13 enable secret 5 $1$zKX1$6XtnZqAyzRsANPWZbyDWH.
14 enable password munics
15 !
16 !
17 !
18 aaa new-model
19 !
20 !
21 aaa authentication login AAA-LOGIN group radius local
22 aaa authentication login CONSOLE group radius local
23 aaa authorization exec AAA-AUTHZ group radius local if-authenticated
24 aaa authorization exec CONSOLE group radius local
25 !
26 !
27 !
28 aaa session-id common
29 system mtu routing 1500
30 ip routing
31 ip domain-name munics.pri
32 !
33 !
34 !
35 !
36 crypto pki trustpoint TP-self-signed-3139015552
37 enrollment selfsigned
38 subject-name cn=IOS-Self-Signed-Certificate-3139015552
39 revocation-check none
40 rsakeypair TP-self-signed-3139015552
41 !
42 !
43 crypto pki certificate chain TP-self-signed-3139015552
44 certificate self-signed 01
45 30820249 308201B2 A0030201 02020101 300D0609 2A864886 F70D0101 04050030
46 31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
47 69666963 6174652D 33313339 30313535 3532301E 170D3933 30333031 30303030
48 35365A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
49 4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D33 31333930
50 31353535 3230819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
51 8100EEF0 77B70D39 C077512A 5E183579 2E051087 D4B06526 22A76CB5 11FCC6EC
52 A3F2516A DFBE4837 104CF317 B63576B7 7FE48A7B 2F3F8F01 C095FB6A F3F9A15C
53 F3E052FB F2B60124 6A6BF8DD B2C6DD7A 175F496A 3228903B B6288596 B7F15493
54 4BFF2578 D16AB815 F61B3253 F8E5B0C9 EC236C7B DBD2802D 5CF30BAB 806A39E8
55 54E50203 010001A3 71306F30 0F060355 1D130101 FF040530 030101FF 301C0603
56 551D1104 15301382 11444C2D 5357312E 6D756E69 63732E70 7269301F 0603551D
57 23041830 168014EB 2849A1D4 49DFF386 2F8F4A87 7DA4977D 18848B30 1D060355
58 1D0E0416 0414EB28 49A1D449 DFF3862F 8F4A877D A4977D18 848B300D 06092A86
59 4886F70D 01010405 00038181 00307FFD AB23E244 74634FD5 44EB45CC C0211344
60 3C00652E 97E7E5CE EA8C42D9 FE518876 D5172237 6090DABE 211B3531 38A323B1
```

```

61 D3C37783 BF1CDC40 CFBOAD25 AD830DB0 4B30792F BC6F3D7C E9EC5056 03153280
62 6D2B31A0 6DC1BEC7 24691E7D 095F8D2E 98384A30 3DD6DBDD 5E3771FE 454907D6
63 C72687DF FB681141 C5E6CD8A FF
64 quit
65 !
66 !
67 !
68 !
69 spanning-tree mode pvst
70 spanning-tree extend system-id
71 spanning-tree vlan 16-18,739,745 priority 24576
72 !
73 vlan internal allocation policy ascending
74 !
75 ip ssh time-out 60
76 ip ssh version 2
77 !
78 !
79 !
80 interface FastEthernet0/1
81 !
82 interface FastEthernet0/2
83 !
84 interface FastEthernet0/3
85 !
86 interface FastEthernet0/4
87 !
88 interface FastEthernet0/5
89 !
90 interface FastEthernet0/6
91 !
92 interface FastEthernet0/7
93 !
94 interface FastEthernet0/8
95 !
96 interface FastEthernet0/9
97 !
98 interface FastEthernet0/10
99 !
100 interface FastEthernet0/11
101 !
102 interface FastEthernet0/12
103   switchport trunk encapsulation dot1q
104   switchport trunk allowed vlan 16-18,739
105   switchport mode trunk
106 !
107 interface FastEthernet0/13
108   switchport trunk encapsulation dot1q
109   switchport trunk allowed vlan 2,739,740
110   switchport mode trunk
111 !
112 interface FastEthernet0/14
113   switchport access vlan 3
114   switchport mode access
115 !
116 interface FastEthernet0/15
117   switchport trunk encapsulation dot1q
118   switchport trunk allowed vlan 3,739
119   switchport mode trunk
120 !
121 interface FastEthernet0/16
122   switchport access vlan 4

```

```

123  switchport mode access
124 !
125 interface FastEthernet0/17
126   switchport trunk encapsulation dot1q
127   switchport trunk allowed vlan 4,739
128   switchport mode trunk
129 !
130 interface FastEthernet0/18
131 !
132 interface FastEthernet0/19
133 !
134 interface FastEthernet0/20
135 !
136 interface FastEthernet0/21
137 !
138 interface FastEthernet0/22
139 !
140 interface FastEthernet0/23
141 !
142 interface FastEthernet0/24
143   switchport trunk encapsulation dot1q
144   switchport trunk allowed vlan 739,740
145   switchport mode trunk
146 !
147 interface GigabitEthernet0/1
148 !
149 interface GigabitEthernet0/2
150 !
151 interface Vlan1
152   no ip address
153   shutdown
154 !
155 interface Vlan2
156   ip address 10.1.0.1 255.255.255.252
157   ip ospf network point-to-point
158   ip ospf 1 area 0
159 !
160 interface Vlan16
161   ip address 10.1.16.1 255.255.255.0
162   ip access-group ACL-DL-VLAN16-IN in
163   ip helper-address 10.1.239.100
164   ip ospf 1 area 0
165 !
166 interface Vlan17
167   ip address 10.1.17.1 255.255.255.0
168   ip access-group ACL-DL-VLAN17-IN in
169   ip helper-address 10.1.239.100
170   ip ospf 1 area 0
171 !
172 interface Vlan18
173   ip address 10.1.18.1 255.255.255.0
174   ip access-group ACL-DL-VLAN18-IN in
175   ip helper-address 10.1.239.100
176   ip ospf 1 area 0
177 !
178 interface Vlan739
179   ip address 10.1.239.2 255.255.255.0
180 !
181 router ospf 1
182   log-adjacency-changes
183   passive-interface default
184   no passive-interface Vlan2

```

```

185 network 10.1.0.0 0.0.0.3 area 0
186 network 10.1.16.0 0.0.0.255 area 0
187 network 10.1.17.0 0.0.0.255 area 0
188 network 10.1.18.0 0.0.0.255 area 0
189 !
190 ip classless
191 ip http server
192 ip http secure-server
193 !
194 !
195 ip access-list standard ACL-MGMT
196 remark Solo gestion desde VLAN Pod1-adm
197 permit 10.1.239.0 0.0.0.255
198 deny any log
199 !
200 ip access-list extended ACL-DL-VLAN16-IN
201 remark BLOQUEO VLANS 17 y 18
202 deny ip 10.1.16.0 0.0.0.255 10.1.17.0 0.0.0.255
203 deny ip 10.1.16.0 0.0.0.255 10.1.18.0 0.0.0.255
204 permit ip any any
205 remark DHCP OFFER
206 ip access-list extended ACL-DL-VLAN17-IN
207 remark BLOQUEO VLANS 16 y 17
208 deny ip 10.1.17.0 0.0.0.255 10.1.16.0 0.0.0.255
209 deny ip 10.1.17.0 0.0.0.255 10.1.18.0 0.0.0.255
210 remark DHCP OFFER
211 permit ip any any
212 ip access-list extended ACL-DL-VLAN18-IN
213 remark BLOQUEO VLANS 16 y 18
214 deny ip 10.1.18.0 0.0.0.255 10.1.16.0 0.0.0.255
215 deny ip 10.1.18.0 0.0.0.255 10.1.17.0 0.0.0.255
216 remark DHCP OFFER
217 permit ip any any
218 !
219 ip sla enable reaction-alerts
220 !
221 radius-server host 10.1.239.100 auth-port 1812 acct-port 1813 key Bayern_2025
222 !
223 !
224 line con 0
225 password munics
226 line vty 0 4
227 access-class ACL-MGMT in
228 password munics
229 authorization exec AAA-AUTHZ
230 login authentication AAA-LOGIN
231 transport input ssh
232 line vty 5 15
233 !
234 end

```

Listing 3: Running Config del DL-SW1

### 6.3 FW (VERSIÓN ACL + CBACs)

```
1 !
2 ! Last configuration change at 15:18:54 UTC Fri Dec 12 2025 by superMunics
3 !
4 version 15.4
5 service timestamps debug datetime msec
6 service timestamps log datetime msec
7 no service password-encryption
8 !
9 hostname FW
10 !
11 boot-start-marker
12 boot-end-marker
13 !
14 !
15 enable secret 5 $1$iaUf$/YbICUZAx7Df3Gwn6CYTC1
16 enable password munics
17 !
18 aaa new-model
19 !
20 !
21 aaa authentication login AAA-LISTEN group radius local
22 aaa authentication login SSH-LISTEN group radius local
23 aaa authentication login CONSOLE group radius local
24 aaa authorization exec AAA-AUTHZ group radius local if-authenticated
25 aaa authorization exec SSH-LISTEN group radius local
26 aaa authorization exec CONSOLE group radius local
27 !
28 !
29 !
30 !
31 !
32 aaa session-id common
33 memory-size iomem 15
34 !
35 !
36 !
37 !
38 !
39 !
40 !
41 !
42 !
43
44 !
45 !
46 !
47 !
48 !
49 ip domain name munics.pri
50 ip inspect name CBAC tcp timeout 300
51 ip inspect name CBAC udp timeout 30
52 ip inspect name CBAC icmp timeout 10
53 ip inspect name CBAC-INTERNET tcp timeout 300
54 ip inspect name CBAC-INTERNET icmp timeout 10
55 ip cef
56 no ipv6 cef
57 !
58 multilink bundle-name authenticated
59 !
60 !
```

```

61 !
62 license udi pid CISCO1941/K9 sn FCZ1731609A
63 license boot c1900 technology-package securityk9
64 license boot c1900 technology-package datak9
65 !
66 !
67 username juniorAdmin secret 5 $1$7V/v$HXT2XqfZZ1yakmQIW/YxH1
68 username admin privilege 15 secret 5 $1$XJKK$2EQITMry7Lf7R0hltEAcl.
69 !
70 redundancy
71 !
72 !
73 !
74 !
75 !
76 ip ssh time-out 60
77 ip ssh version 2
78 !
79 !
80 !
81 !
82 !
83 !
84 !
85 !
86 !
87 !
88 interface Embedded-Service-Engine0/0
89   no ip address
90   shutdown
91 !
92 interface GigabitEthernet0/0
93   description Trunk to DL-SW1 F0/13
94   no ip address
95   duplex auto
96   speed auto
97 !
98 interface GigabitEthernet0/0.2
99   encapsulation dot1Q 2
100  ip address 10.1.0.2 255.255.255.252
101  ip inspect CBAC in
102  ip ospf network point-to-point
103 !
104 interface GigabitEthernet0/0.739
105  description ADM (Pod1)
106  encapsulation dot1Q 739
107  ip address 10.1.239.3 255.255.255.0
108 !
109 interface GigabitEthernet0/0.740
110  encapsulation dot1Q 740
111  ip address 10.1.240.1 255.255.255.0
112  ip access-group ACL-SERVICIOS-FW in
113  ip inspect CBAC in
114 !
115 interface GigabitEthernet0/1
116  ip address 10.1.0.5 255.255.255.252
117  ip access-group ACL-INTERNET-IN in
118  ip inspect CBAC in
119  ip ospf network point-to-point
120  duplex auto
121  speed auto
122 !

```

```

123 interface Serial0/0/0
124 no ip address
125 shutdown
126 clock rate 2000000
127 !
128 interface Serial0/0/1
129 no ip address
130 shutdown
131 clock rate 2000000
132 !
133 router ospf 1
134 passive-interface default
135 no passive-interface GigabitEthernet0/0.2
136 no passive-interface GigabitEthernet0/1
137 network 10.1.0.0 0.0.255.255 area 0
138 !
139 ip forward-protocol nd
140 !
141 no ip http server
142 no ip http secure-server
143 !
144 !
145 ip access-list standard ACL-MGMT
146 remark Solo gestion desde VALN Pod1_adm
147 permit 10.1.239.0 0.0.0.255
148 deny   any log
149 !
150 ip access-list extended ACL-FW-IN
151 remark ACCESO DE DISPOSITIVOS AL SERVIDOR DHCP
152 permit udp any host 10.1.239.100 eq bootps
153 permit udp any host 10.1.239.100 eq bootpc
154 remark OSPF
155 permit ospf host 10.1.0.1 host 224.0.0.5
156 permit ospf host 10.1.0.1 host 10.1.0.2
157 permit ospf host 10.1.0.2 host 224.0.0.5
158 permit ospf host 10.1.0.2 host 10.1.0.1
159 remark ACCESO A SERVICIOS VLAN 16
160 permit tcp 10.1.16.0 0.0.0.255 host 10.1.240.100 eq www
161 permit tcp 10.1.16.0 0.0.0.255 host 10.1.240.100 eq 443
162 permit tcp 10.1.16.0 0.0.0.255 host 10.1.240.100 eq domain
163 permit udp 10.1.16.0 0.0.0.255 host 10.1.240.100 eq domain
164 permit icmp 10.1.16.0 0.0.0.255 host 10.1.240.100 echo
165 remark ACCESO A INTERNET VLAN 16
166 permit tcp 10.1.16.0 0.0.0.255 any eq www
167 permit tcp 10.1.16.0 0.0.0.255 any eq 443
168 permit udp 10.1.16.0 0.0.0.255 any eq domain
169 permit icmp 10.1.16.0 0.0.0.255 any echo
170 remark ACCESO A SERVICIOS VLAN 17
171 permit tcp 10.1.17.0 0.0.0.255 host 10.1.240.100 eq www
172 permit tcp 10.1.17.0 0.0.0.255 host 10.1.240.100 eq 443
173 permit tcp 10.1.17.0 0.0.0.255 host 10.1.240.100 eq domain
174 permit udp 10.1.17.0 0.0.0.255 host 10.1.240.100 eq domain
175 permit icmp 10.1.17.0 0.0.0.255 host 10.1.240.100 echo
176 remark ACCESO A INTERNET VLAN 17
177 permit tcp 10.1.17.0 0.0.0.255 any eq www
178 permit tcp 10.1.17.0 0.0.0.255 any eq 443
179 permit udp 10.1.17.0 0.0.0.255 any eq domain
180 permit icmp 10.1.17.0 0.0.0.255 any echo
181 remark ACCESO A SERVICIOS VLAN 18
182 permit tcp 10.1.18.0 0.0.0.255 host 10.1.240.100 eq www
183 permit tcp 10.1.18.0 0.0.0.255 host 10.1.240.100 eq 443
184 permit tcp 10.1.18.0 0.0.0.255 host 10.1.240.100 eq domain

```

```

185  permit udp 10.1.18.0 0.0.0.255 host 10.1.240.100 eq domain
186  permit icmp 10.1.18.0 0.0.0.255 host 10.1.240.100 echo
187  remark ACCESO A INTERNET VLAN 18
188  permit tcp 10.1.18.0 0.0.0.255 any eq www
189  permit tcp 10.1.18.0 0.0.0.255 any eq 443
190  permit udp 10.1.18.0 0.0.0.255 any eq domain
191  permit icmp 10.1.18.0 0.0.0.255 any echo
192  deny ip any any
193 ip access-list extended ACL-INTERNET-FW
194  permit ospf host 10.1.0.6 host 224.0.0.5
195  permit ospf host 10.1.0.6 host 10.1.0.5
196  permit ospf host 10.1.0.5 host 224.0.0.5
197  permit ospf host 10.1.0.5 host 10.1.0.6
198  permit tcp any host 10.1.240.100 eq 443
199  permit icmp any host 10.1.240.100 echo
200  deny ip any 10.1.0.0 0.0.255.255
201  deny ip any any
202 ip access-list extended ACL-SERVICIOS-FW
203  remark DENEGAR CONEXIONES VLAN
204  deny ip any 10.1.16.0 0.0.0.255
205  deny ip any 10.1.17.0 0.0.0.255
206  deny ip any 10.1.18.0 0.0.0.255
207
208  permit tcp 10.1.240.0 0.0.0.255 any eq 80
209  permit tcp 10.1.240.0 0.0.0.255 any eq 443
210  permit tcp 10.1.240.0 0.0.0.255 any eq 53
211  permit udp 10.1.240.0 0.0.0.255 any eq 53
212  permit icmp 10.1.240.0 0.0.0.255 any
213
214  deny ip any any
215 !
216 ip radius source-interface GigabitEthernet0/0.739
217 !
218 !
219 !
220 radius server RAD1
221  address ipv4 10.1.239.100 auth-port 1812 acct-port 1813
222  key Bayern_2025
223 !
224 !
225 !
226 control-plane
227 !
228 !
229 !
230 line con 0
231  password munics
232  login authentication CONSOLE
233 line aux 0
234 line 2
235  no activation-character
236  no exec
237  transport preferred none
238  transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
239  stopbits 1
240 line vty 0 4
241  access-class ACL-MGMT in
242  password munics
243  authorization exec AAA-AUTHZ
244  login authentication AAA-LOGIN
245  transport input ssh
246 !

```

```
247 scheduler allocate 20000 1000
248 !
249 end
```

Listing 4: Running Config del FW con ACLs y CBACs

## 6.4 FW (Versión ZBFW)

```
1 FW#show run
2 Building configuration...
3
4 Current configuration : 5144 bytes
5 !
6 ! Last configuration change at 16:08:13 UTC Thu Dec 11 2025 by superMunics
7 !
8 version 15.4
9 service timestamps debug datetime msec
10 service timestamps log datetime msec
11 no service password-encryption
12 !
13 hostname FW
14 !
15 boot-start-marker
16 boot-end-marker
17 !
18 !
19 enable secret 5 $1$iaUf$/YbICUZAx7Df3Gwn6CYTC1
20 enable password munics
21 !
22 aaa new-model
23 !
24 !
25 aaa authentication login AAA-LIST group radius local
26 aaa authentication login SSH-LIST group radius local
27 aaa authentication login CONSOLE group radius local
28 aaa authorization exec AAA-AUTHZ group radius local if-authenticated
29 aaa authorization exec SSH-LIST group radius local
30 aaa authorization exec CONSOLE group radius local
31 !
32 !
33 !
34 !
35 !
36 aaa session-id common
37 memory-size iomem 15
38 !
39 !
40 !
41 !
42 !
43 !
44 !
45 !
46 !
47 !
48 !
49 !
50 !
51 !
52 !
53 ip domain name munics.pri
54 ip cef
55 no ipv6 cef
56 !
57 multilink bundle-name authenticated
58 !
59 !
60 !
```

```

61 license udi pid CISCO1941/K9 sn FCZ1731609A
62 license boot c1900 technology-package securityk9
63 license boot c1900 technology-package datak9
64 !
65 !
66 username juniorAdmin secret 5 $1$7V/v$HXT2XqfZZ1yakmQIW/YxH1
67 username admin privilege 15 secret 5 $1$XJKK$2EQITMry7Lf7R0hltEAcL.
68 !
69 redundancy
70 !
71 !
72 !
73 !
74 !
75 ip ssh time-out 60
76 ip ssh version 2
77 !
78 class-map type inspect match-any CM-DMZ-TO-OUTSIDE
79   match access-group name ACL-DMZ-SERVER
80   match protocol tcp
81   match protocol udp
82   match protocol icmp
83 class-map type inspect match-any CM-OUTSIDE-TO-DMZ
84   match access-group name ACL-DMZ-SERVER
85   match protocol icmp
86   match protocol tcp
87 class-map type inspect match-any CM-CONTROL
88   match access-group name ACL-DHCP
89   match access-group name ACL-OSPF
90 class-map type inspect match-any CM-INSIDE-TO-OUTSIDE
91   match access-group name ACL-INSIDE
92   match protocol tcp
93   match protocol udp
94   match protocol icmp
95 class-map type inspect match-any CM-INSIDE-TO-DMZ
96   match access-group name ACL-INSIDE
97   match access-group name ACL-DMZ-SERVER
98   match protocol tcp
99   match protocol udp
100  match protocol icmp
101 !
102 policy-map type inspect PM-DMZ-TO-OUTSIDE
103   class type inspect CM-DMZ-TO-OUTSIDE
104     inspect
105     class class-default
106       drop
107 policy-map type inspect PM-INSIDE-TO-OUTSIDE
108   class type inspect CM-INSIDE-TO-OUTSIDE
109     inspect
110     class type inspect CM-CONTROL
111       pass
112     class class-default
113       drop
114 policy-map type inspect PM-OUTSIDE-TO-DMZ
115   class type inspect CM-OUTSIDE-TO-DMZ
116     inspect
117     class class-default
118       drop
119 policy-map type inspect PM-INSIDE-TO-DMZ
120   class type inspect CM-INSIDE-TO-DMZ
121     inspect
122     class type inspect CM-CONTROL

```

```

123  pass
124  class class-default
125  drop
126 !
127 zone security INSIDE
128 zone security DMZ
129 zone security OUTSIDE
130 zone-pair security ZP-INSIDE-TO-DMZ source INSIDE destination DMZ
131   service-policy type inspect PM-INSIDE-TO-DMZ
132 zone-pair security ZP-INSIDE-TO-OUTSIDE source INSIDE destination OUTSIDE
133   service-policy type inspect PM-INSIDE-TO-OUTSIDE
134 zone-pair security ZP-DMZ-TO-OUTSIDE source DMZ destination OUTSIDE
135   service-policy type inspect PM-DMZ-TO-OUTSIDE
136 zone-pair security ZP-OUTSIDE-TO-DMZ source OUTSIDE destination DMZ
137   service-policy type inspect PM-OUTSIDE-TO-DMZ
138 !
139 !
140 !
141 !
142 !
143 !
144 !
145 !
146 !
147 !
148 interface Embedded-Service-Engine0/0
149   no ip address
150   shutdown
151 !
152 interface GigabitEthernet0/0
153   description Trunk to DL-SW1 F0/13
154   no ip address
155   duplex auto
156   speed auto
157 !
158 interface GigabitEthernet0/0.2
159   encapsulation dot1Q 2
160   ip address 10.1.0.2 255.255.255.252
161   zone-member security INSIDE
162   ip ospf network point-to-point
163 !
164 interface GigabitEthernet0/0.739
165   description ADM (Pod1)
166   encapsulation dot1Q 739
167   ip address 10.1.239.3 255.255.255.0
168 !
169 interface GigabitEthernet0/0.740
170   encapsulation dot1Q 740
171   ip address 10.1.240.1 255.255.255.0
172   zone-member security OUTSIDE
173 !
174 interface GigabitEthernet0/1
175   ip address 10.1.0.5 255.255.255.252
176   zone-member security OUTSIDE
177   ip ospf network point-to-point
178   duplex auto
179   speed auto
180 !
181 interface Serial0/0/0
182   no ip address
183   shutdown
184   clock rate 2000000

```

```

185 !
186 interface Serial0/0/1
187   no ip address
188   shutdown
189   clock rate 2000000
190 !
191 router ospf 1
192   passive-interface default
193   no passive-interface GigabitEthernet0/0.2
194   no passive-interface GigabitEthernet0/1
195   network 10.1.0.0 0.0.255.255 area 0
196 !
197 ip forward-protocol nd
198 !
199 no ip http server
200 no ip http secure-server
201 !
202 !
203 ip access-list standard ACL-MGMT
204   remark Solo gestion desde VALN Pod1_adm
205   permit 10.1.239.0 0.0.0.255
206   deny   any log
207 !
208 ip access-list extended ACL-DHCP
209   permit udp any host 10.1.239.100 eq bootps
210   permit udp any host 10.1.239.100 eq bootpc
211 ip access-list extended ACL-DMZ-SERVER
212   permit ip any host 10.1.240.100
213 ip access-list extended ACL-INSIDE
214   permit ip 10.1.16.0 0.0.0.255 any
215   permit ip 10.1.17.0 0.0.0.255 any
216   permit ip 10.1.18.0 0.0.0.255 any
217 ip access-list extended ACL-OSPF
218   permit ospf any any
219 !
220 ip radius source-interface GigabitEthernet0/0.739
221 !
222 !
223 !
224 radius server RAD1
225   address ipv4 10.1.239.100 auth-port 1812 acct-port 1813
226   key Bayern_2025
227 !
228 !
229 !
230 control-plane
231 !
232 !
233 !
234 line con 0
235   password munics
236   login authentication CONSOLE
237 line aux 0
238 line 2
239   no activation-character
240   no exec
241   transport preferred none
242   transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
243   stopbits 1
244 line vty 0 4
245   access-class ACL-MGMT in
246   password munics

```

```
247 authorization exec AAA-AUTHZ
248 login authentication AAA-LGIN
249 transport input ssh
250 !
251 scheduler allocate 20000 1000
252 !
253 end
```

Listing 5: Running Config del FW con ZBFW

## 6.5 CPE

```
1 !
2 ! Last configuration change at 19:46:13 UTC Fri Dec 12 2025 by superMunics
3 !
4 version 15.7
5 service timestamps debug datetime msec
6 service timestamps log datetime msec
7 no service password-encryption
8 !
9 hostname CPE
10 !
11 boot-start-marker
12 boot-end-marker
13 !
14 !
15 enable secret 5 $1$3FPY$n.Qd8MGjf/Gdju/Fd6Ai2.
16 enable password munics
17 !
18 aaa new-model
19 !
20 !
21 aaa authentication login AAA-LOGIN group radius local
22 aaa authentication login CONSOLE group radius local
23 aaa authorization exec AAA-AUTHZ group radius local if-authenticated
24 aaa authorization exec CONSOLE group radius local
25 !
26 !
27 !
28 !
29 !
30 !
31 aaa session-id common
32 !
33 !
34 !
35 !
36 !
37 !
38 !
39 !
40 !
41 !
42 !
43 !
44 ip domain name munics.pri
45 ip cef
46 no ipv6 cef
47 !
48 multilink bundle-name authenticated
49 !
50 !
51 !
52 license udi pid CISCO1941/K9 sn FHK14287AAC
53 !
54 !
55 username admin privilege 15 secret 5 $1$C97z$JGvHtFWUCPaWk9XVeYx310
56 username juniorAdmin secret 5 $1$Jm7P$ZdkceIBDI6WeyrwRy2DXt1
57 !
58 redundancy
59 !
60 !
```

```

61 !
62 !
63 !
64 !
65 !
66 !
67 !
68 !
69 !
70 !
71 !
72 !
73 !
74 interface Embedded-Service-Engine0/0
75   no ip address
76   shutdown
77 !
78 interface GigabitEthernet0/0
79   no ip address
80   duplex auto
81   speed auto
82 !
83 interface GigabitEthernet0/0.3
84   encapsulation dot1Q 3
85   ip address 10.1.0.6 255.255.255.252
86   ip nat inside
87   ip virtual-reassembly in
88   ip ospf network point-to-point
89 !
90 interface GigabitEthernet0/0.739
91   encapsulation dot1Q 739
92   ip address 10.1.239.4 255.255.255.0
93 !
94 interface GigabitEthernet0/1
95   ip address 192.0.1.1 255.255.255.0
96   ip access-group ACL-CPE-STATIC-IN in
97   ip nat outside
98   ip virtual-reassembly in
99   duplex auto
100  speed auto
101 !
102 router ospf 1
103   redistribute static subnets
104   passive-interface default
105   no passive-interface GigabitEthernet0/0.3
106   network 10.1.0.4 0.0.0.3 area 0
107   default-information originate
108 !
109 ip forward-protocol nd
110 !
111 no ip http server
112 no ip http secure-server
113 !
114 ip nat pool Vlan16 192.0.1.200 192.0.1.200 netmask 255.255.255.0
115 ip nat pool Vlan17 192.0.1.201 192.0.1.201 netmask 255.255.255.0
116 ip nat pool Vlan18 192.0.1.202 192.0.1.202 netmask 255.255.255.0
117 ip nat inside source list NAT-VLAN16 pool Vlan16 overload
118 ip nat inside source list NAT-VLAN17 pool Vlan17 overload
119 ip nat inside source list NAT-VLAN18 pool Vlan18 overload
120 ip nat inside source static tcp 10.1.240.100 80 192.0.1.203 80 extendable
121 ip nat inside source static tcp 10.1.240.100 443 192.0.1.203 443 extendable
122 ip route 0.0.0.0 0.0.0.0 192.0.1.2

```

```

123 ip ssh time-out 60
124 ip ssh version 2
125 !
126 ip access-list standard ACL-CPE-STATIC-IN
127 deny 10.0.0.0 0.255.255.255
128 deny 172.16.0.0 0.15.255.255
129 deny 192.168.0.0 0.0.255.255
130 deny 169.254.0.0 0.0.255.255
131 deny 192.0.2.0 0.0.0.255
132 deny 198.51.100.0 0.0.0.255
133 deny 203.0.113.0 0.0.0.255
134 deny 100.64.0.0 0.63.255.255
135 deny 127.0.0.0 0.255.255.255
136 deny 0.0.0.0 0.255.255.255
137 deny 224.0.0.0 15.255.255.255
138 deny 240.0.0.0 15.255.255.255
139 permit any
140 ip access-list standard ACL-MGMT
141 permit 10.1.239.0 0.0.0.255
142 deny any log
143 ip access-list standard NAT-VLAN16
144 permit 10.1.16.0 0.0.0.255
145 ip access-list standard NAT-VLAN17
146 permit 10.1.17.0 0.0.0.255
147 ip access-list standard NAT-VLAN18
148 permit 10.1.18.0 0.0.0.255
149 !
150 ip access-list extended ACL-INTERNET-FW
151 deny ip any any
152 !
153 !
154 !
155 !
156 radius server RAD1
157 address ipv4 10.1.239.100 auth-port 1812 acct-port 1813
158 key Bayern_2025
159 !
160 !
161 !
162 control-plane
163 !
164 !
165 line con 0
166 password munics
167 login authentication CONSOLE
168 line aux 0
169 line 2
170 no activation-character
171 no exec
172 transport preferred none
173 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
174 stopbits 1
175 line vty 0 4
176 access-class ACL-MGMT in
177 password munics
178 authorization exec AAA-AUTHZ
179 login authentication AAA-LOGIN
180 transport input ssh
181 !
182 scheduler allocate 20000 1000
183 !
184 end

```

---

Listing 6: Running Config del CPE

## 6.6 ISP

```
1 !
2 ! Last configuration change at 18:26:14 UTC Thu Dec 11 2025 by superMunics
3 !
4 version 15.4
5 service timestamps debug datetime msec
6 service timestamps log datetime msec
7 no service password-encryption
8 !
9 hostname ISP
10 !
11 boot-start-marker
12 boot-end-marker
13 !
14 !
15 no logging console
16 enable secret 5 $1$Pyez$rusV3Zwb.xaThFtrZJgsP/
17 enable password munics
18 !
19 aaa new-model
20 !
21 !
22 aaa authentication login SSH-LOGIN group radius local
23 aaa authentication login CONSOLE group radius local
24 aaa authorization exec SSH-LOGIN group radius local
25 aaa authorization exec CONSOLE group radius local
26 !
27 !
28 !
29 !
30 !
31 aaa session-id common
32 memory-size iomem 15
33 !
34 !
35 !
36 !
37 !
38 !
39 !
40 !
41 !
42 !
43 !
44 !
45 !
46 !
47 !
48 ip domain name munics.pri
49 ip cef
50 no ipv6 cef
51 !
52 multilink bundle-name authenticated
53 !
54 !
55 !
56 license udi pid CISCO1941/K9 sn FCZ1626901Y
57 license boot c1900 technology-package datak9
58 !
59 !
60 username juniorAdmin secret 5 $1$1n22$4rNzBOPvcUyeIGzyU1h7R0
```

```

61 username admin privilege 15 secret 5 $1$AgDE$8L9VyE7FY3JaKLgNZMtad.
62 !
63 redundancy
64 !
65 !
66 !
67 !
68 !
69 ip ssh version 2
70 !
71 !
72 !
73 !
74 !
75 !
76 !
77 !
78 !
79 !
80 interface Embedded-Service-Engine0/0
81   no ip address
82   shutdown
83 !
84 interface GigabitEthernet0/0
85   description TRUNK link to DL-SW1 F0/17
86   no ip address
87   duplex auto
88   speed auto
89 !
90 interface GigabitEthernet0/0.4
91   encapsulation dot1Q 4
92   ip address 192.0.1.2 255.255.255.0
93 !
94 interface GigabitEthernet0/0.739
95   description ADM (VLAN 739)
96   encapsulation dot1Q 739
97   ip address 10.1.239.5 255.255.255.0
98 !
99 interface GigabitEthernet0/1
100  ip address 192.0.0.1 255.255.255.0
101  duplex auto
102  speed auto
103 !
104 interface Serial0/0/0
105  no ip address
106  shutdown
107  clock rate 2000000
108 !
109 interface Serial0/0/1
110  no ip address
111  shutdown
112  clock rate 2000000
113 !
114 ip forward-protocol nd
115 !
116 no ip http server
117 ip http secure-server
118 !
119 ip route 10.1.0.0 255.255.0.0 192.0.1.1
120 !
121 ip access-list standard MGMT-ONLY
122  permit 10.1.239.0 0.0.0.255

```

```

123  deny    any  log
124 !
125 ip radius source-interface GigabitEthernet0/0.739
126 !
127 !
128 radius-server host 10.1.239.100 auth-port 1812 acct-port 1813 key Bayern_2025
129 !
130 !
131 !
132 control-plane
133 !
134 !
135 !
136 line con 0
137   logging synchronous
138   login authentication CONSOLE
139 line aux 0
140 line 2
141   no activation-character
142   no exec
143   transport preferred none
144   transport output lat pad telnet rlogin lapb-ta mop udptn v120 ssh
145   stopbits 1
146 line vty 0 4
147   access-class MGMT-ONLY in
148   authorization exec SSH-LGIN
149   login authentication SSH-LGIN
150   transport input ssh
151 !
152 scheduler allocate 20000 1000
153 !
154 end

```

Listing 7: Running Config del ISP