

# Proyecto de redes y servicios (IC)

**Realizado por:**

Anabel Díaz Labrador

Cheuk Kelly Ng Pante

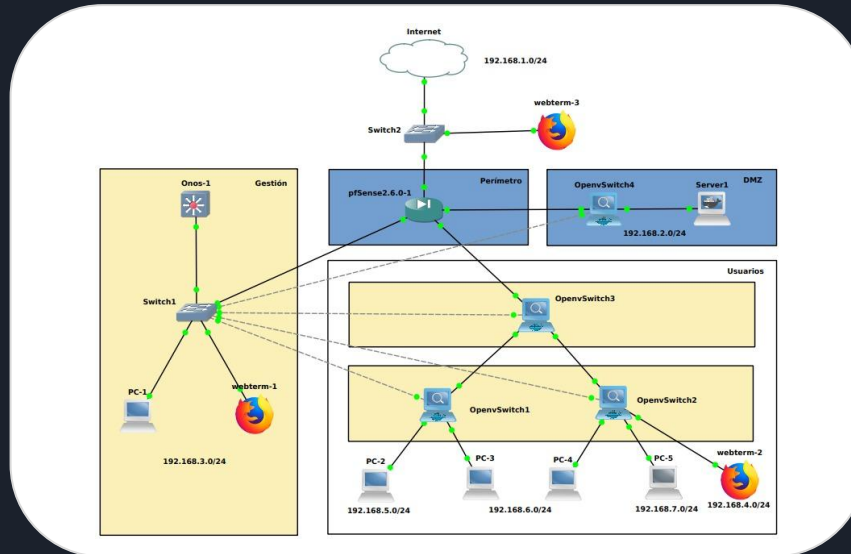
Jaime Pablo Pérez Moro

Carmen Clara Rocío Machado

# Índice

- Planteando un nuevo esquema de direccionamiento para la red
- Segmentación de redes (VLAN)
- Esquema alternativo de flujos
- Despliegue y configuración de la zona DMZ
- Mejoras en la política de seguridad
- Mejoras generales

1  
2  
6  
9  
16  
23




# Planteando un nuevo esquema de direccionamiento para la red

| Red  | Equipo          | Interfaz   | Dirección IP                                    |
|------|-----------------|------------|---|
| -    | pfSense 2.6.0-1 | WAN (em0)  | WAN DHCP  |
| -    | pfSense 2.6.0-1 | LAN (em1)  | 192.168.4.1/24                                  |
| -    | pfSense 2.6.0-1 | MGMT (em2) | 192.168.3.1/24                                  |
| -    | pfSense 2.6.0-1 | DMZ (em3)  | 192.168.2.1/24                                  |
| WAN  | webterm-3       | eth0       | WAN DHCP  |
| MGMT | Onos-1          | eth0       | local DHCP<br>MAC reservation<br>192.168.3.2/24 |
|      | webterm-1       | eth0       | local DHCP                                      |
|      | PC-1            | eth0       | local DHCP                                      |
| DMZ  | OpenvSwitch 4   | -          | 192.168.3.6/24                                  |
|      | Server1         | eth0       | local DHCP<br>MAC reservation<br>192.168.2.5/24 |

| Red | Equipo        | Interfaz | Dirección IP    |
|-----|---------------|----------|-----------------|
| LAN | OpenvSwitch 1 | -        | 192.168.3.3/24  |
|     | OpenvSwitch 2 | -        | 192.168.3.4/24  |
|     | OpenvSwitch 3 | -        | 192.168.3.5/24  |
|     | PC-2          | eth0     | 192.168.5.10/24 |
|     | PC-3          | eth0     | 192.168.6.11/24 |
|     | PC-4          | eth0     | 192.168.6.12/24 |
|     | PC-5          | eth0     | 192.168.7.13/24 |
|     | webterm-2     | eth0     | local DHCP      |

- DMZ: 192.168.2.100 - 192.168.2.200
- MGMT: 192.168.3.100 - 192.168.3.200
- LAN: 192.168.4.100 - 192.168.4.200

# Segmentación de redes (VLAN)



| VLAN | Nombre    | Dirección de red | Descripción                      |
|------|-----------|------------------|----------------------------------|
| 10   | Centrales | 192.168.5.0/24   | Personal de servicios centrales. |
| 20   | Oficina   | 192.168.6.0/24   | Personal de oficinas.            |
| 30   | CPD       | 192.168.7.0/24   | Equipamiento en CPD.             |

| Red      | Equipo | VLAN | Dirección de red | Descripción                                    |
|----------|--------|------|------------------|--|
| Usuarios | PC-2   | 10   | 192.168.5.10     | Equipo en OpenvSwitch1 de servicios centrales. |
|          | PC-3   | 20   | 192.168.6.11     | Equipo en OpenvSwitch1 de oficinas.            |
|          | PC-4   | 20   | 192.168.6.12     | Equipo en OpenvSwitch2 de oficinas.            |
|          | PC-5   | 30   | 192.168.7.13     | Equipo en OpenvSwitch2 del CPD.                |

# Segmentación de redes (VLAN)

```
OpenvSwitch2 — Konsole
Archivo  Editar  Ver  Marcadores  Complementos  Preferencias  Ayuda

/ # ovs-vsctl set port eth1 tag=20
/ # ovs-vsctl set port eth2 tag=30
/ # ovs-vsctl set port eth3 trunk=10,20,30
/ # ovs-vsctl show
ea2beba3-c97b-44c8-98f5-b781e0ac3455
  Bridge "br0"
    Controller "tcp:192.168.0.2:6633"
      is_connected: true
    fail_mode: secure
    Port "eth2"
      tag: 30
    Interface "eth2"
    Port "eth3"
      trunks: [10, 20, 30]
    Interface "eth3"
    Port "eth1"
      tag: 20
    Interface "eth1"
    Port "br0"
      Interface "br0"
      type: internal
```

```
PC-2
Loading Linux 3.16.0-4-686-pae ...
root@Debian:~# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 0c:c5:fc:82:00:00
          inet6 addr: fe80::ec5:fcff:fe82:0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:16 errors:0 dropped:7 overruns:0 frame:0
          TX packets:16 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2378 (2.3 KiB)  TX bytes:1696 (1.6 KiB)

eth0.10    Link encap:Ethernet  HWaddr 0c:c5:fc:82:00:00
          inet addr:192.168.1.10 Bcast:192.168.1.255 Mask:255.255.255.0
          inet6 addr: fe80::ec5:fcff:fe82:0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:8 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:808 (808.0 B)







lo         Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
```

# Segmentación de redes (VLAN)

```
PC-3
root@Debian:~# ping 192.168.1.12
PING 192.168.1.12 (192.168.1.12) 56(84) bytes of data.
64 bytes from 192.168.1.12: icmp_seq=1 ttl=64 time=18.9 ms
64 bytes from 192.168.1.12: icmp_seq=2 ttl=64 time=1.35 ms
64 bytes from 192.168.1.12: icmp_seq=3 ttl=64 time=1.50 ms
64 bytes from 192.168.1.12: icmp_seq=4 ttl=64 time=1.09 ms
^C
--- 192.168.1.12 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 300 ms
rtt min/avg/max/mdev = 1.096/5.737/18.992/7.654 ms
root@Debian:~# ping 192.168.1.10
PING 192.168.1.10 (192.168.1.10) 56(84) bytes of data.
From 192.168.1.11 icmp_seq=1 Destination Host Unreachable
From 192.168.1.11 icmp_seq=2 Destination Host Unreachable
From 192.168.1.11 icmp_seq=3 Destination Host Unreachable
^C
--- 192.168.1.10 ping statistics ---
6 packets transmitted, 0 received, +3 errors, 100% packet loss
pipe 3
```


Interfaces / VLANs

Interface Assignments Interface Groups Wireless **VLANs** QinQs PPPs GREs GIFs Bridges LAGGs







| VLAN Interfaces |          |          |                      |   |
|-----------------|----------|----------|----------------------|---|
| Interface       | VLAN tag | Priority | Description          | Actions   |
| em1 (lan)       | 10       |          | Contains PC2         |   |
| em1 (lan)       | 20       |          | Contains PC3 and PC4 |   |
| em1 (lan)       | 30       |          | Contains PC5         |   |

+ Add

# Segmentación de redes (VLAN)

Interfaces / Interface Assignments 

Interface Assignments Interface Groups Wireless VLANs QinQs PPPs GREs GIFs Bridges LAGGs

| Interface | Network port  |
|-----------|---|
| WAN       | em0 (0c:0c:5d:e0:00:00)   |
| LAN       | em1 (0c:0c:5d:e0:00:01)                      |
| MGMT      | em2 (0c:0c:5d:e0:00:02)                      |
| DMZ       | em3 (0c:0c:5d:e0:00:03)                      |
| VLAN10    | VLAN 10 on em1 - lan (Contains PC2)          |
| VLAN20    | VLAN 20 on em1 - lan (Contains PC3 and PC4)  |
| VLAN30    | VLAN 30 on em1 - lan (Contains PC5)          |





PC-5 — Konsole






Archivo Editar Ver Marcadores Complementos Preferencias Ayuda


```
root@Debian:~# ping 192.168.3.10
PING 192.168.3.10 (192.168.3.10) 56(84) bytes of data:
64 bytes from 192.168.3.10: icmp_seq=1 ttl=63 time=12.4 ms
64 bytes from 192.168.3.10: icmp_seq=2 ttl=63 time=5.28 ms
64 bytes from 192.168.3.10: icmp_seq=3 ttl=63 time=4.20 ms
^C
--- 192.168.3.10 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 4.204/7.300/12.415/3.643 ms
root@Debian:~# ping 192.168.4.11
PING 192.168.4.11 (192.168.4.11) 56(84) bytes of data:
64 bytes from 192.168.4.11: icmp_seq=1 ttl=63 time=5.29 ms
64 bytes from 192.168.4.11: icmp_seq=2 ttl=63 time=4.42 ms
64 bytes from 192.168.4.11: icmp_seq=3 ttl=63 time=4.13 ms
^C
--- 192.168.4.11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 4.138/4.620/5.297/0.492 ms
root@Debian:~# ping 192.168.4.12
PING 192.168.4.12 (192.168.4.12) 56(84) bytes of data:
64 bytes from 192.168.4.12: icmp_seq=1 ttl=63 time=6.08 ms
64 bytes from 192.168.4.12: icmp_seq=2 ttl=63 time=4.11 ms
64 bytes from 192.168.4.12: icmp_seq=3 ttl=63 time=2.45 ms
^C
--- 192.168.4.12 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 2.450/4.883/8.082/2.363 ms
```

Floating WAN LAN MGMT DMZ VLAN10 VLAN20 VLAN30

Rules (Drag to Change Order)

|                          | States | Protocol | Source | Port | Destination | Port | Gateway | Queue | Schedule | Description | Actions   |
|--------------------------|--------|----------|--------|------|-------------|------|---------|-------|----------|-------------|---|
| <input type="checkbox"/> | ✓      | 0 / 0 B  | IPv4 * | *    | *           | *    | *       | none  |          |             |     |

 Add  Add  Delete  Save  Separator



# Esquema alternativo de flujos

Reactive Forwarding off

```
PC-2 — Konsole
Archivo  Editar  Ver  Marcadores  Complementos  Preferencias  Ayuda

root@Debian:~# ping 192.168.4.12
PING 192.168.4.12 (192.168.4.12) 56(84) bytes of data.
From 192.168.3.10 icmp_seq=1 Destination Host Unreachable
From 192.168.3.10 icmp_seq=2 Destination Host Unreachable
From 192.168.3.10 icmp_seq=3 Destination Host Unreachable
^C
--- 192.168.4.12 ping statistics ---
5 packets transmitted, 0 received, +3 errors, 100% packet loss, time 4000ms
pipe 3
```

intents



# Esquema alternativo de flujos

```
PC-1 — Konsole
Archivo  Editar  Ver  Marcadores  Complementos  Preferencias  Ayuda
karaf@root > hosts
15:51:38
id=0C:0C:5D:E0:00:01/10, mac=0C:0C:5D:E0:00:01, locations=[of:0000000000000002/2], auxLocations=null, vlan=10, ip(s)=[192.168.3.1, 192.168.5.1], innerVlan=None, outerTPID=unknown, provider=of:
id=0C:0C:5D:E0:00:01/20, mac=0C:0C:5D:E0:00:01, locations=[of:0000000000000003/1], auxLocations=null, vlan=20, ip(s)=[192.168.4.1], innerVlan=None, outerTPID=unknown, provider=of:
id=0C:0C:5D:E0:00:01/30, mac=0C:0C:5D:E0:00:01, locations=[of:0000000000000003/1], auxLocations=null, vlan=30, ip(s)=[192.168.5.1], innerVlan=None, outerTPID=unknown, provider=of:
id=0C:0C:5D:E0:00:01/None, mac=0C:0C:5D:E0:00:01, locations=[of:0000000000000003/1], auxLocations=null, vlan=None, ip(s)=[192.168.1.1], innerVlan=None, outerTPID=unknown, provider=of:
id=0C:14:56:91:00:00/30, mac=0C:14:56:91:00:00, locations=[of:0000000000000002/3], auxLocations=null, vlan=30, ip(s)=[192.168.5.13], innerVlan=None, outerTPID=unknown, provider=of:
id=0C:BD:92:3A:00:00/20, mac=0C:BD:92:3A:00:00, locations=[of:0000000000000002/4], auxLocations=null, vlan=20, ip(s)=[192.168.1.12, 192.168.4.12], innerVlan=None, outerTPID=unknown, provider=of:
id=0C:C5:FC:82:00:00/10, mac=0C:C5:FC:82:00:00, locations=[of:0000000000000001/1], auxLocations=null, vlan=10, ip(s)=[192.168.3.10, 192.168.1.10], innerVlan=None, outerTPID=unknown, provider=of:
id=0C:F8:9D:4C:00:00/20, mac=0C:F8:9D:4C:00:00, locations=[of:0000000000000002/2], auxLocations=null, vlan=20, ip(s)=[192.168.4.11, 192.168.1.11], innerVlan=None, outerTPID=unknown, provider=of:
id=22:4C:9B:21:AE:2F/None, mac=22:4C:9B:21:AE:2F, locations=[of:0000000000000002/1], auxLocations=null, vlan=None, ip(s)=[192.168.1.113], innerVlan=None, outerTPID=unknown, provider=of:
id=4E:9A:03:CC:B8:B5/None, mac=4E:9A:03:CC:B8:B5, locations=[of:0000000000000002/1], auxLocations=null, vlan=None, ip(s)=[192.168.1.111], innerVlan=None, outerTPID=unknown, provider=of:
id=62:83:BE:3E:41:5E/None, mac=62:83:BE:3E:41:5E, locations=[of:0000000000000002/1], auxLocations=null, vlan=None, ip(s)=[192.168.1.110], innerVlan=None, outerTPID=unknown, provider=of:
id=9A:30:13:60:3E:EF/None, mac=9A:30:13:60:3E:EF, locations=[of:0000000000000002/1], auxLocations=null, vlan=None, ip(s)=[192.168.1.114], innerVlan=None, outerTPID=unknown, provider=of:
id=AA:27:3E:72:74:F6/None, mac=AA:27:3E:72:74:F6, locations=[of:0000000000000002/1], auxLocations=null, vlan=None, ip(s)=[192.168.1.109], innerVlan=None, outerTPID=unknown, provider=of:
id=DA:DD:34:E4:25:61/None, mac=DA:DD:34:E4:25:61, locations=[of:0000000000000002/1], auxLocations=null, vlan=None, ip(s)=[192.168.1.112], innerVlan=None, outerTPID=unknown, provider=of:
```

Identificación de los PCs es la siguiente:




- PC2: id=0C:C5:FC:82:00:00/10
- PC4: id=0C:BD:92:3A:00:00/20
- Interfaz virtual pfSense VLAN10: id=0C:0C:5D:E0:00:01/10
- Interfaz virtual pfSense VLAN20: id=0C:0C:5D:E0:00:01/20

```
PC-1 — Konsole
Archivo  Editar  Ver  Marcadores  Complementos  Preferencias  Ayuda
karaf@root > add-host-intent 0C:C5:FC:82:00:00/10 0C:0C:5D:E0:00:01/10 16:55:08
Host to Host intent submitted:
HostToHostIntent{id=0x1db, key=0x1db, appId=DefaultApplicationId{id=2, name=org.onosproject.cli}, priority=100, resources=[0C:C5:FC:82:00:00/10]}
karaf@root > add-host-intent 0C:BD:92:3A:00:00/20 0C:0C:5D:E0:00:01/20 16:55:11
Host to Host intent submitted:
HostToHostIntent{id=0x1e0, key=0x1e0, appId=DefaultApplicationId{id=2, name=org.onosproject.cli}, priority=100, resources=[0C:BD:92:3A:00:00/20]}
```


# Esquema alternativo de flujos

Applications (169 Total)

arp All Fields ▾

| ▼ | Title   | App ID                       |
|---|---|------------------------------|
| ✓ |  Host Location Provider  | org.onosproject.hostprovider |
| ✓ |  OpenFlow Provider Suite | org.onosproject.openflow     |
| ✓ |  Proxy ARP/NDP           | org.onosproject.proxyarp     |

### Proxy ARP/NDP



**App ID** org.onosproject.proxyarp  
**State** ACTIVE  
**Category** Traffic Engineering  
**Version** 3.0.0.SNAPSHOT  
**Origin** ONOS Community  
**Role** UNSPECIFIED

<http://onosproject.org>

Proxy ARP/NDP application.

**FEATURES**

onos-apps-proxyarp

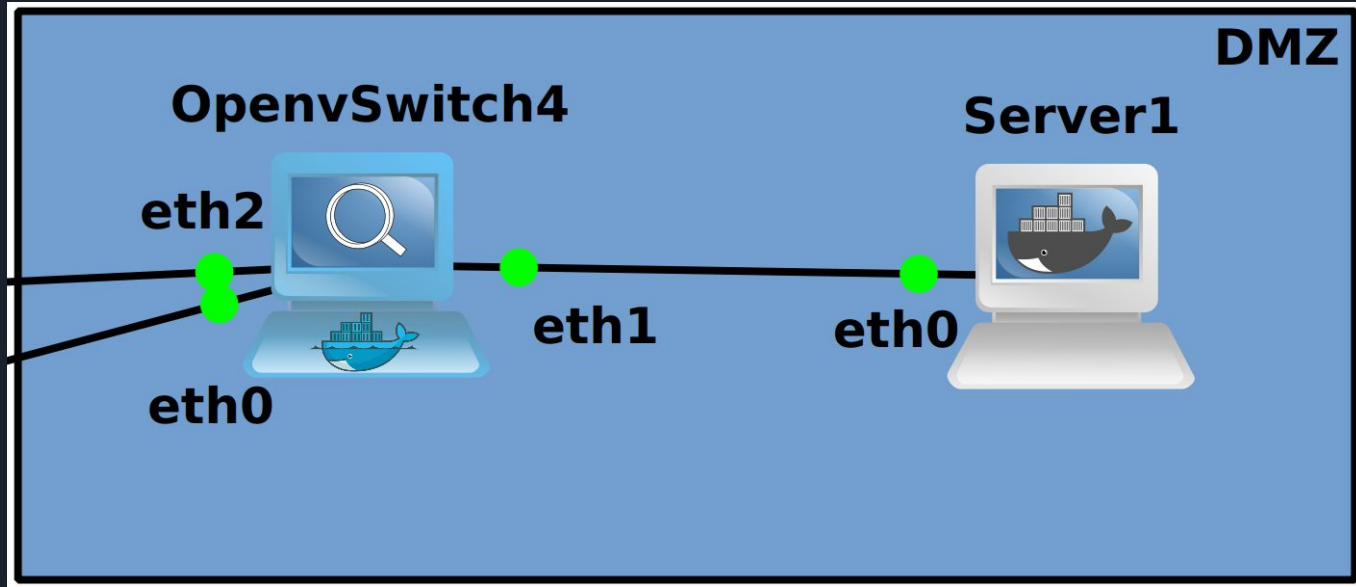
**REQUIRED APPS**

PC-2 — Konsole

Archivo Editar Ver Marcadores Complementos Preferencias Ayuda

```
PING 192.168.4.12 (192.168.4.12) 56(84) bytes of data.  
64 bytes from 192.168.4.12: icmp_seq=1 ttl=63 time=2.52 ms  
64 bytes from 192.168.4.12: icmp_seq=2 ttl=63 time=4.47 ms  
64 bytes from 192.168.4.12: icmp_seq=3 ttl=63 time=4.48 ms  
64 bytes from 192.168.4.12: icmp_seq=4 ttl=63 time=4.19 ms  
^C  
--- 192.168.4.12 ping statistics ---  
4 packets transmitted, 4 received, 0% packet loss, time 3004ms  
rtt min/avg/max/mdev = 2.523/3.918/4.481/0.815 ms
```

# Despliegue y configuración de la zona DMZ



# Instalación del paquete ajnouri/nginx



ajnouri/nginx ☆

By [ajnouri](#) • Updated 4 years ago

Docker container nginx server container + php5-fpm

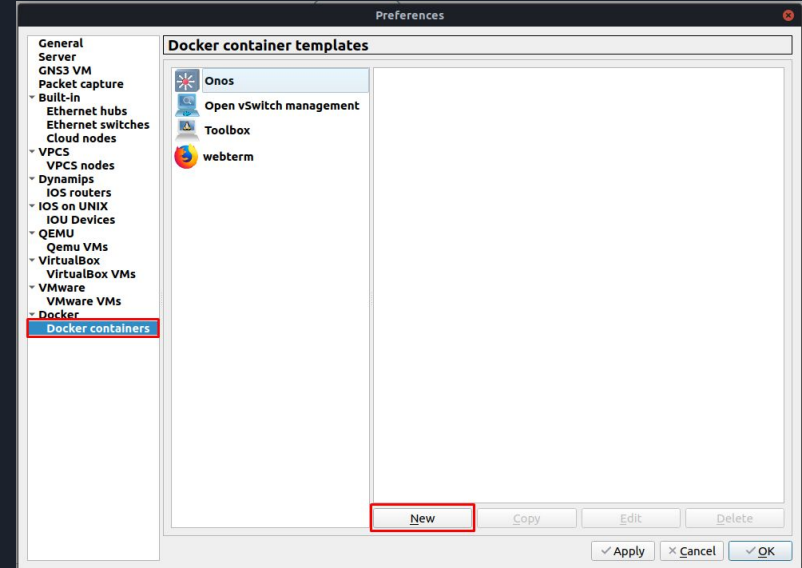
Container

New Docker container template

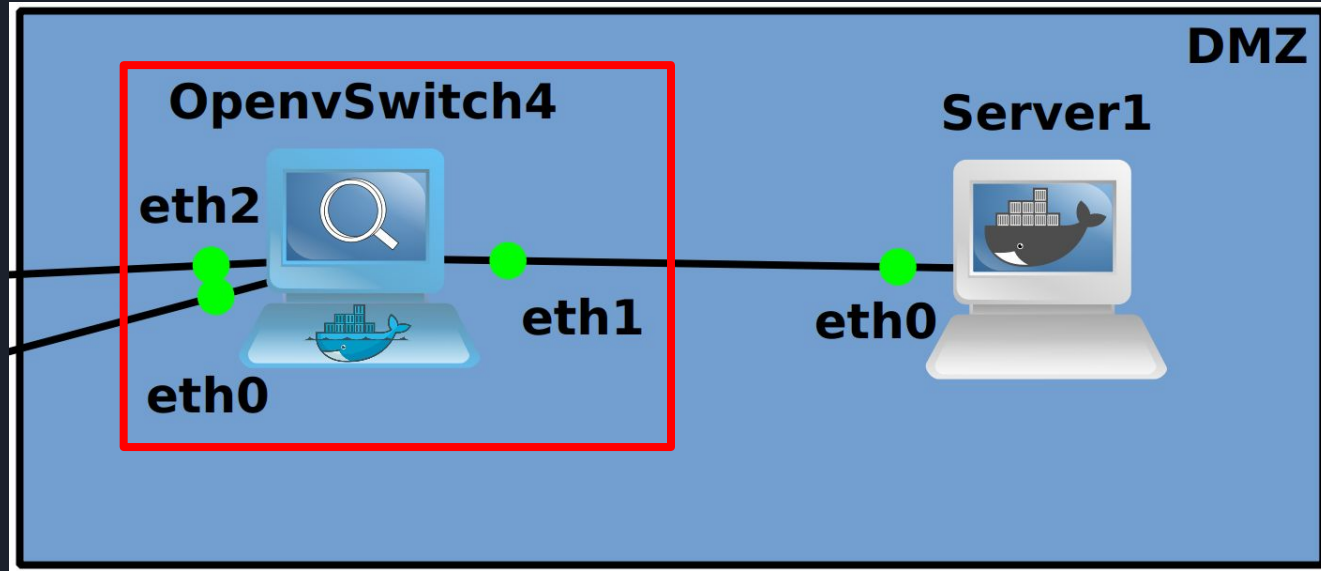
**Docker Virtual Machine**  
Please choose a Docker virtual machine from the list or provide an image name on Docker hub.

☐ Existing image ☒ New image

Image name:



# Configuración del OpenvSwitch4 de la DMZ



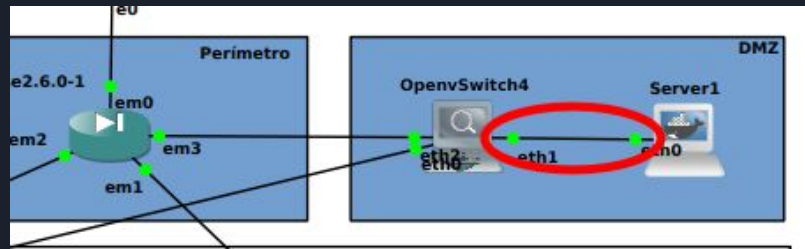
# Configuración del OpenvSwitch4 de la DMZ

```
/ # ovs-vsctl del-br br0
/ # ovs-vsctl del-br br1
/ # ovs-vsctl del-br br2
/ # ovs-vsctl del-br br3
/ # ovs-vsctl add-br br0
/ # ovs-vsctl add-port br0 eth1
/ # ovs-vsctl add-port br0 eth2
/ # ovs-vsctl add-port br0 eth3
/ # ovs-vsctl show
40db1b69-bf87-404a-8f43-ad191b9ff6c6
    Bridge "br0"
        Port "eth2"
            Interface "eth2"
        Port "eth3"
            Interface "eth3"
        Port "br0"
            Interface "br0"
            type: internal
        Port "eth1"
            Interface "eth1"
```

```
/ # ovs-vsctl set bridge br0 other-config:datapath-id=0000000000000004 \
> -- set bridge br0 protocols=OpenFlow13 \
> -- set bridge br0 fail_mode=secure \
> -- set-controller br0 tcp:192.168.0.2:6633 \
> -- set controller br0 connection-mode=out-of-band
/ # ovs-vsctl show
40db1b69-bf87-404a-8f43-ad191b9ff6c6
    Bridge "br0"
        Controller "tcp:192.168.0.2:6633"
        fail_mode: secure
        Port "eth2"
            Interface "eth2"
        Port "eth3"
            Interface "eth3"
        Port "br0"
            Interface "br0"
            type: internal
        Port "eth1"
            Interface "eth1"
```

# Configuración de una reserva estática con la MAC

```
# Static config for eth0
auto eth0
iface eth0 inet static
    address 192.168.2.5
    netmask 255.255.255.0
    gateway 192.168.2.1
#
# up echo nameserver 192.168.0.1 > /etc/resolv.conf
```



```
[2.6.0-RELEASE][root@myPistolones.Pistolones4k]/root: ping 192.168.2.5
PING 192.168.2.5 (192.168.2.5): 56 data bytes
64 bytes from 192.168.2.5: icmp_seq=0 ttl=64 time=32.961 ms
64 bytes from 192.168.2.5: icmp_seq=1 ttl=64 time=1.268 ms
64 bytes from 192.168.2.5: icmp_seq=2 ttl=64 time=1.541 ms
64 bytes from 192.168.2.5: icmp_seq=3 ttl=64 time=1.767 ms
^C
--- 192.168.2.5 ping statistics ---
5 packets transmitted, 4 packets received, 20.0% packet loss
round-trip min/avg/max/stddev = 1.268/9.384/32.961/13.613 ms
```



# Configuración de una reserva estática con la MAC

|    |           |                   |                   |
|----|-----------|-------------------|-------------------|
| 26 | 24.801876 | 192.168.2.5       | 192.168.2.1       |
| 27 | 25.875537 | 192.168.2.1       | 192.168.2.5       |
| 28 | 25.875804 | 192.168.2.5       | 192.168.2.1       |
| 29 | 26.897819 | 192.168.2.1       | 192.168.2.5       |
| 30 | 26.898175 | 192.168.2.5       | 192.168.2.1       |
| 31 | 27.805786 | 9e:65:67:10:92:da | 0c:0c:5d:e0:00:03 |
| 32 | 27.811093 | 0c:0c:5d:e0:00:03 | 9e:65:67:10:92:da |
| 33 | 27.899010 | 02:eb:9f:67:c9:42 | LLDP_Multicast    |
| 34 | 27.899083 | 02:eb:9f:67:c9:42 | Broadcast         |
| 35 | 27.961137 | 192.168.2.1       | 192.168.2.5       |
| 36 | 27.961566 | 192.168.2.5       | 192.168.2.1       |
| 37 | 28.978065 | 192.168.2.1       | 192.168.2.5       |

Frame 26: 98 bytes on wire (784 bits), 98 bytes captured (784) on interface 0  
Ethernet II, Src: 9e:65:67:10:92:da (9e:65:67:10:92:da), Dst: 0c:0c:5d:e0:00:03 (0c:0c:5d:e0:00:03)  
Destination: 0c:0c:5d:e0:00:03 (0c:0c:5d:e0:00:03)  
Source: 9e:65:67:10:92:da (9e:65:67:10:92:da)  
Address: 9e:65:67:10:92:da (9e:65:67:10:92:da)  
.....1..... = LG bit: Locally administered  
.....0..... = IG bit: Individual address  
Type: IPv4 (0x0800)  
Internet Protocol Version 4, Src: 192.168.2.5, Dst: 192.168.2.1

## Services / DHCP Server / DMZ / Edit Static Mapping

### Static DHCP Mapping on DMZ

MAC Address

9e:65:67:10:92:da

Copy My MAC

MAC address (6 hex octets separated by colons)

Client Identifier

Server1

IP Address

192.168.2.5

If an IPv4 address is entered, the address must be outside of the pool.

If no IPv4 address is given, one will be dynamically allocated from the pool.



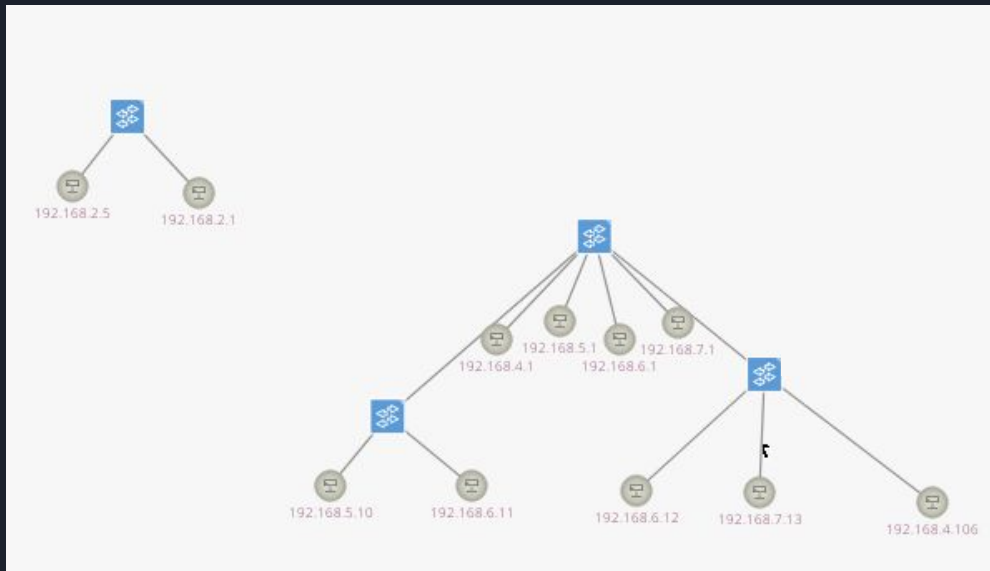
# Configuración de una reserva estática con la MAC

## Server1 interfaces

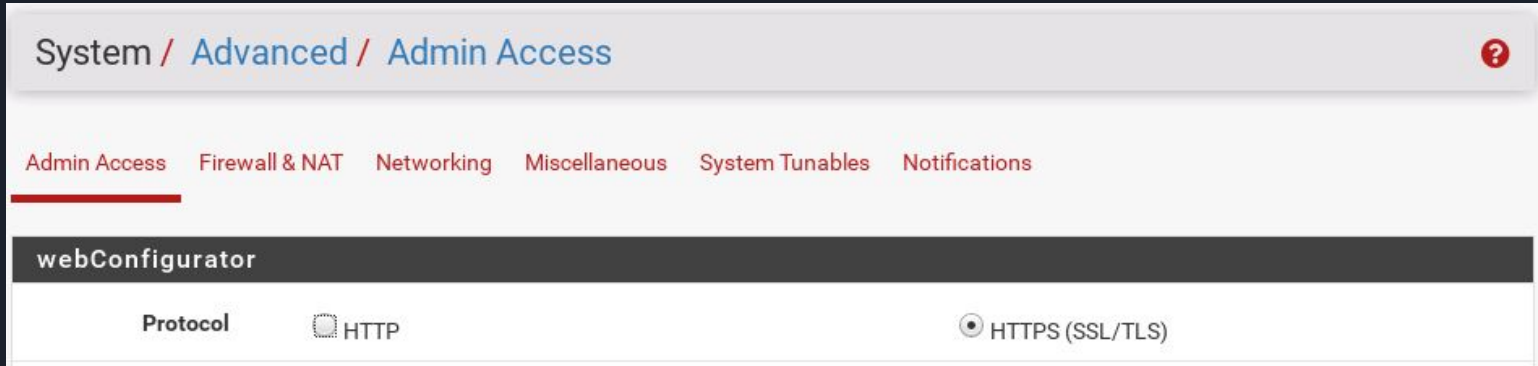
```
#
# This is a sample network config uncomment lines to configure the network
#

# Static config for eth0
#auto eth0
#iface eth0 inet static
#    address 192.168.2.5
#    netmask 255.255.255.0
#    gateway 192.168.2.1
#    up echo nameserver 192.168.0.1 > /etc/resolv.conf

# DHCP config for eth0
auto eth0
iface eth0 inet dhcp
    hwaddress ether 9e:65:67:10:92:da
```



# Mejoras de política de seguridad



Admitir solamente la conexión HTTPS a la interfaz de gestión del cortafuegos (no admitir HTTP).

# Mejoras de política de seguridad

| Access to firewall       |   |                |             |   |   |               |                |   |      |    |
|--------------------------|---|----------------|-------------|---|---|---------------|----------------|---|------|---|
| <input type="checkbox"/> |  | 1 / 551<br>KiB | IPv4<br>TCP | * | * | This Firewall | 443<br>(HTTPS) | * | none | <br><br><br><br> |
| <input type="checkbox"/> |  | 0 / 7<br>KiB   | IPv4<br>UDP | * | * | This Firewall | 53 (DNS)       | * | none | <br><br><br><br> |


















El acceso HTTPS a la interfaz de gestión del cortafuegos solamente debe ser posible desde la red de GESTIÓN/MGMT.

# Mejoras de política de seguridad

Firewall / Rules / LAN

















Floating WAN LAN MGMT DMZ VLAN10 VLAN20 VLAN30






Rules (Drag to Change Order)

|                            | States     | Protocol | Source  | Port | Destination      | Port      | Gateway | Queue | Schedule | Description     | Actions   |
|----------------------------|------------|----------|---------|------|------------------|-----------|---------|-------|----------|-----------------|---|
| <input type="checkbox"/> ✓ | 0 / 2 KiB  | IPv4 *   | LAN net | *    | LAN_zone         | *         | *       | none  |          | LAN conectivity |      |
| Server                     |            |          |         |      |                  |           |         |       |          |                 |    |
| <input type="checkbox"/> ✓ | 0 / 3 KiB  | IPv4 TCP | LAN net | *    | Server1          | web_ports | *       | none  |          |                 |      |
| Internet                   |            |          |         |      |                  |           |         |       |          |                 |    |
| <input type="checkbox"/> ✓ | 2 / 41 KiB | IPv4 TCP | LAN net | *    | ! 192.168.0.0/21 | *         | *       | none  |          |                 |      |

Garantizar que la red de USUARIOS/LAN solamente pueda acceder a los servicios de red que necesita, a Internet y a los servidores en la DMZ.

Floating WAN LAN MGMT DMZ VLAN10 VLAN20 VLAN30

| Rules (Drag to Change Order)  |           |          |            |      |                  |           |         |       |          |                  |   |
|---|-----------|----------|------------|------|------------------|-----------|---------|-------|----------|------------------|---|
|  | States    | Protocol | Source     | Port | Destination      | Port      | Gateway | Queue | Schedule | Description      | Actions   |
| <input type="checkbox"/>  | ✓ 0/672 B | IPv4 *   | VLAN10 net | *    | LAN_zone         | *         | *       | none  |          | LAN connectivity |      |
| <input type="checkbox"/>  | ✓ 0/0 B   | IPv4 TCP | VLAN10 net | *    | Server1          | web_ports | *       | none  |          |                  |      |
| <input type="checkbox"/>  | ✓ 0/0 B   | IPv4 *   | VLAN10 net | *    | ! 192.168.0.0/21 | *         | *       | none  |          |                  |      |

 Add
  Add
  Delete
  Save
  Separator

Ejemplo de reglas en VLAN 10

# Mejoras de política de seguridad





|                          |   |       |             |             |   |               |                   |   |      |   |  |
|--------------------------|---|-------|-------------|-------------|---|---------------|-------------------|---|------|---|--|
| <input type="checkbox"/> | ✓ | 0/0 B | IPv4<br>TCP | MGMT<br>net | * | OpenvSwitches | remote_<br>access | * | none | Access to OpenvSwitches<br>through SSH and Telnet |  |
| <input type="checkbox"/> | ✓ | 0/0 B | IPv4<br>TCP | MGMT<br>net | * | LAN net       | remote_<br>access | * | none | Only allow SSH and telnet<br>to LAN net           |  |






Desde la red GESTIÓN/MGMT debe ser posible la navegación en Internet y en Server1. Además, debe ser posible el acceso por SSH y Telnet a todos los equipos de la red.

# Mejoras de política de seguridad

Floating WAN LAN MGMT DMZ VLAN10 VLAN20 VLAN30

Rules (Drag to Change Order)






|                          | States      | Protocol | Source | Port | Destination | Port      | Gateway | Queue | Schedule | Description                            | Actions   |
|--------------------------|-------------|----------|--------|------|-------------|-----------|---------|-------|----------|--|---|
| <input type="checkbox"/> | ✓ 0 / 4 KiB | IPv4 TCP | *      | *    | Server1     | 80 (HTTP) | *       | none  |          | NAT Port forward to web servers in DMZ |     |






 Add  Add  Delete  Save  Separator

Firewall / NAT / Port Forward

Port Forward 1:1 Outbound NPt









Rules

|                          | Interface   | Protocol | Source Address | Source Ports | Dest. Address | Dest. Ports | NAT IP  | NAT Ports | Description                        | Actions   |
|--------------------------|---|----------|----------------|--------------|---------------|-------------|---------|-----------|------------------------------------|---|
| <input type="checkbox"/> | ✓  WAN | TCP      | *              | *            | WAN address   | 80 (HTTP)   | Server1 | 80 (HTTP) | Port forward to web servers in DMZ |     |

 Add  Add  Delete  Save  Separator

El acceso desde la WAN solamente debe ser posible para las conexiones relacionadas iniciadas desde dentro y para la configuración NAT Port Forward realizada.

# Mejoras de política de seguridad

|  |   |         |             |             |   |         |                   |   |      |   |
|--|---|---------|-------------|-------------|---|---------|-------------------|---|------|---|
| Misc.  |   |         |             |             |   |         |                   |   |      |    |
|  |  | 0 / 0 B | IPv4<br>TCP | MGMT<br>net | * | DMZ net | remote_<br>access | * | none | <br><br><br><br> |

Desde la DMZ se debe poder acceder a los servicios de la red que necesite. No debe ser posible la navegación a Internet. El acceso para administración (SSH o Telnet) a los equipos de la DMZ solamente debe ser posible desde la red de GESTIÓN/MGMT.



# Mejoras generales

**Host Override Options**

**Host**

server1

Name of the host, without the domain part  
e.g. enter 'myhost' if the full domain name is 'myhost.example.com'

**Domain**

Pistolones4k.com

Parent domain of the host  
e.g. enter 'example.com' for 'myhost.example.com'

**IP Address**

192.168.2.5

IPv4 or IPv6 comma-separated addresses to be returned for the host  
e.g.: 192.168.100.100 or fd00:abcd:  
or list 192.168.1.3,192.168.4.5,fd00:123:3



**Description**

Server1


A description may be entered here for administrative reference (not parsed).

This page is used to override the usual lookup process for a specific host. A host is defined by its name and parent domain (e.g., 'somesite.google.com' is entered as host='somesite' and parent domain='google.com'). Any attempt to lookup that host will automatically return the given IP address, and any usual external lookup server for the domain will not be queried. Both the name and parent domain can contain 'non-standard', 'invalid' and 'local' domains such as 'test', 'nas.home.arpa', 'mycompany.localdomain', or '1.168.192.in-addr.arpa', as well as usual publicly resolvable names such as 'www' or 'google.co.uk'.



| Host Overrides |                       |                       |             |   |
|----------------|-----------------------|-----------------------|-------------|---|
| Host           | Parent domain of host | IP to return for host | Description | Actions   |
| server1        | Pistolones4k.com      | 192.168.2.5           | Server1     |   |

Enter any individual hosts for which the resolver's standard DNS lookup process should be overridden and a specific IPv4 or IPv6 address should automatically be returned by the resolver. Standard and also non-standard names and parent domains can be entered, such as 'test', 'nas.home.arpa', 'mycompany.localdomain', '1.168.192.in-addr.arpa', or 'somesite.com'. Any lookup attempt for the host will automatically return the given IP address, and the usual lookup server for the domain will not be queried for the host's records.

 Add



¡Gracias por su atención!