

Proyecto de redes y servicios

Servicios de red y seguridad

Índice

Objetivos de aprendizaje	3
1. Introducción al cortafuegos pfSense.....	3
2. Montaje.....	3
Paso 1. Añadir la plantilla de dispositivo en GNS3 para un cortafuegos pfSense	5
Paso 2. Añadir e instalar el cortafuegos pfSense en el proyecto de GNS3	7
Paso 3. Configuración básica de red del cortafuegos pfSense	9
Paso 4. Acceso a la gestión web del cortafuegos pfSense	11
Paso 5. Configuración básica del cortafuegos pfSense	11
Paso 6. Configuración del servicio DNS.....	13
Paso 7 Configuración del servicio DHCP.....	15
Paso 8. Configuración del NAT Port Forward	19
3. Mejoras a implementar	22
3.1 Despliegue y configuración de la zona DMZ	22
3.2 Mejoras en la política de seguridad	23
3.3 Mejoras en la política de seguridad	23
Referencias.....	23

Objetivos de aprendizaje

El objetivo de esta práctica es familiarizarnos con la configuración básica de un servicio de seguridad perimetral y de algunos de los servicios de red más importantes. En concreto, vamos a trabajar sobre una solución de cortafuegos [5] de uso profesional que nos permitirá desplegar y administrar de forma centralizada tanto la seguridad perimetral como algunos de los servicios de red de la organización (especialmente factible en organizaciones de tamaño pequeño y mediano), describiremos su funcionamiento, y aprenderemos a realizar su manejo básico y emulación.

A la finalización de esta práctica seremos capaces de:

1. Comprender los conceptos básicos asociados a una solución de seguridad perimetral.
2. Comprender los conceptos básicos asociados a los protocolos y servicios de red más habituales.
3. Instalar y configurar una solución de seguridad perimetral.
4. Instalar y configurar los servicios de red más habituales.

1. Introducción al cortafuegos pfSense

El cortafuegos Pfsense [1] es un software de código abierto basado en el proyecto FreeBSD, por lo que hereda muchas de las características básicas de filtrado de paquetes, firewall y gestión de la calidad de servicio (QoS) que ya proporciona FreeDSB, sin embargo, incorpora como valor añadido una administración, monitorización y mantenimiento mucho más sencillo, al añadir una capa de gestión gráfica (GUI) y por línea de comandos (CLI) muy completa.

De esta forma, pfSense se configura como una solución de firewall/router/VPN que es compatible con la mayoría de las funciones que están disponibles en otros firewalls de gama alta, por lo que se encuentra muy extendido en muchas organizaciones públicas y/o privadas que lo utilizan en sus sistemas de producción.

Se trata de un sistema de seguridad muy versátil, que además de implementar las funcionalidades y servicios necesarias para proteger el perímetro de una organización (p.e.: filtrado de tráfico, VPN y NAT), también puede actuar como un elemento de enrutamiento (router), dispone de muchas opciones de configuración avanzadas de servicios de red (p.e.: gestión de VLANs, proxys de navegación, DHCP y DNS), e incluso la posibilidad de instalar software adicional para ampliar sus funcionalidades (p.e.: servicio de detección y prevención de intrusiones IDS/IPS, etc).

2. Montaje

La arquitectura de red que vamos a desplegar y emular (dentro de la solución GNS3) es la que se muestra en la siguiente figura [1].

Se trata de la ampliación de la arquitectura de red que ya hemos trabajado en la primera parte del proyecto y que implementamos bajo la filosofía de una red definida por software (SDN), en concreto vamos a incorporar los elementos resaltados en rojo y que serán los encargados de soportar a los servicios de seguridad y de red que vamos a implementar.

Vamos a incorporar también a la arquitectura de seguridad una zona DMZ en la que alojaremos los servicios de la organización que serán expuestos al exterior.

Como podemos ver en el montaje, y en la tabla [1] que contiene la información ampliada de direccionamiento de la arquitectura, el cortafuegos pfSense tendrá varias interfaces de red, cada una de las cuales se ubicará en las distintas redes que vamos a interconectar (router) y proteger (firewall) en nuestra arquitectura:

- Interfaz em0: WAN, para la conexión con Internet (DHCP).
- Interfaz em1: LAN, para la conexión con la red de USUARIOS (192.168.1.0/24).
- Interfaz em2: MGMT, para la conexión con la red de GESTIÓN (192.168.0.0/24).
- Interfaz em3: DMZ, para la conexión con la red de DMZ (192.168.2.0/24).

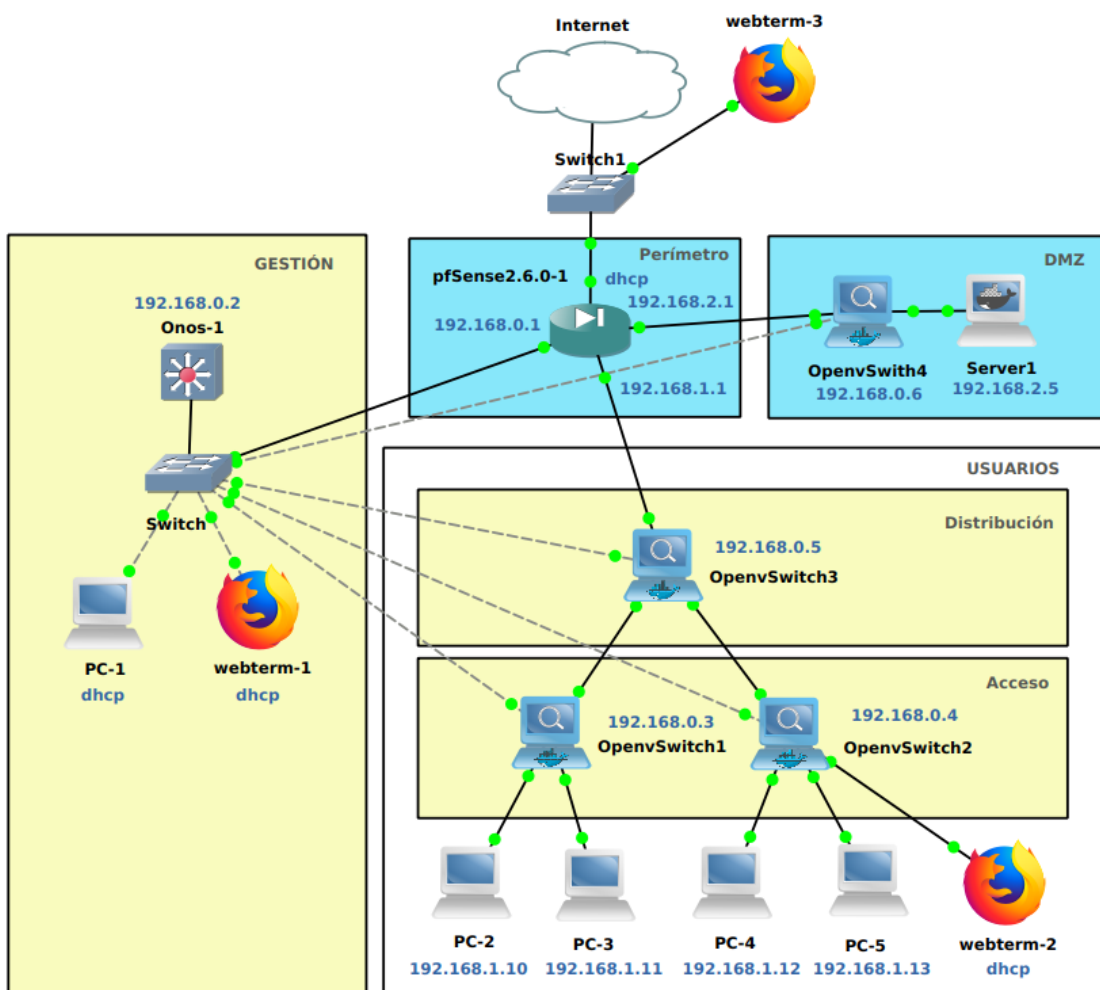


Figura 1. Montaje que se pretende emular en GNS3.

El direccionamiento IP completo que emplearemos es el que se indica en la siguiente tabla (en negrita los cambios con respecto a la práctica anterior):

Red	Equipo	Dirección IP	Descripción
PERÍMETRO	pfSense2.6.0-1	Dinámica	Interfaz WAN (em0) del pfSense2.6.0-1
	webterm-3	Dinámica	Equipo para acceso con navegador desde WAN
DMZ	pfSense2.6.0-1	192.168.2.1/24	Interfaz DMZ (em3) del pfSense2.6.0-1
	Server1	192.168.2.5/24	Servidor de publicación de servicios en Internet
GESTIÓN	pfSense2.6.0-1	192.168.0.1/24	Interfaz MGMT (em2) del pfSense2.6.0-1
	OpenvSwitch1	192.168.0.2/24	CLI del conmutador virtual Open vSwitch de Acceso
	OpenvSwitch2	192.168.0.3/24	CLI del conmutador virtual Open vSwitch de Acceso
	OpenvSwitch3	192.168.0.4/24	CLI del conmutador virtual Open vSwitch de Distribución
	OpenvSwitch4	192.168.0.6/24	CLI del conmutador virtual Open vSwitch de la DMZ
	Onos-1	192.168.0.5/24	Controlador ONOS
	webterm-1	Dinámica	Equipo para acceso con navegador para gestión
	PC-1	Dinámica	Equipo para acceso por SSH para gestión
USUARIOS	pfSense2.6.0-1	192.168.1.1/24	Interfaz LAN (em1) del pfSense2.6.0-1
	PC-2	192.168.1.10/24	Equipo de usuario en OpenvSwitch1
	PC-3	192.168.1.11/24	Equipo de usuario en OpenvSwitch1
	PC-4	192.168.1.12/24	Equipo de usuario en OpenvSwitch2
	PC-5	192.168.1.13/24	Equipo de usuario en OpenvSwitch3
	webterm-2	Dinámica	Equipo para acceso con navegador desde USUARIOS

Tabla 1. Configuración de red a aplicar.

Paso 1. Añadir la plantilla de dispositivo en GNS3 para un cortafuegos pfSense

Antes de nada, vamos a crear la plantilla de dispositivo para un cortafuegos pfSense en GNS3, aunque ya existe una plantilla oficial en los repositorios de GNS3, no está disponible para la última versión de pfSense, así que vamos a partir de esta plantilla oficial (para heredar la configuración de la máquina virtual QEMU), pero la vamos a personalizar instalando la última versión disponible.

Como primer paso vamos a descargar la ISO, de la última versión disponible, del cortafuegos desde su página de descarga: <https://www.pfsense.org/download/>. Seleccionamos la arquitectura AMD y el instalador ISO.



Por defecto, el fichero ISO se descargará comprimido con el comando gzip (extensión *.gz), así que debemos descomprimirlo previamente (para dejarlo en el formato adecuado y con la extensión *.iso):

```
~/Descargas$
~/Descargas$ ls -lrt *.gz
o 437073513 abr 30 13:53 pfSense-CE-2.6.0-RELEASE-amd64.iso.gz
~/Descargas$
~/Descargas$ gunzip pfSense-CE-2.6.0-RELEASE-amd64.iso.gz
~/Descargas$
~/Descargas$
```

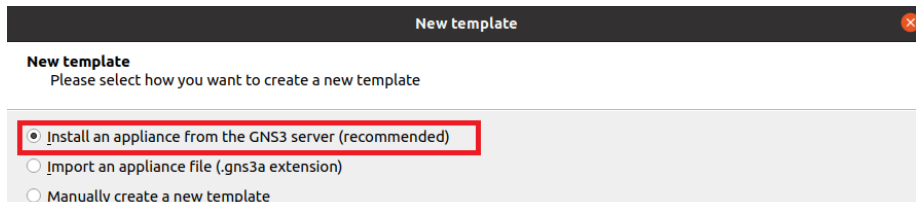
A continuación, descargaremos el fichero imagen de un disco duro virtual vacío de 100GB (plantilla), para un dispositivo en GNS3 que se va desplegar con QEMU (formato qcow2), desde la siguiente URL:

<https://sourceforge.net/projects/gns-3/files/Empty%20Qemu%20disk/empty100G.qcow2/download>

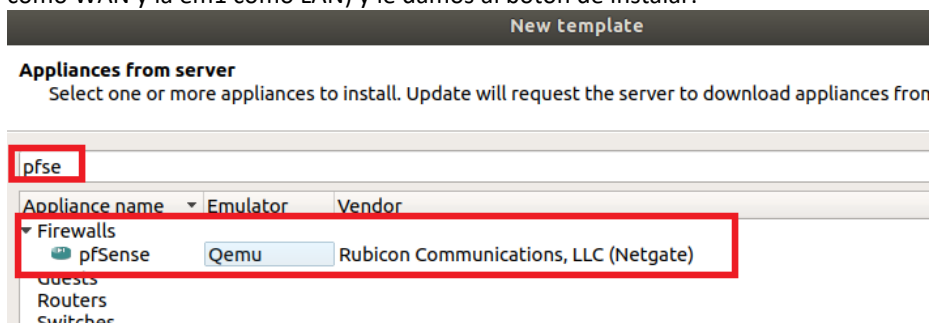
Ahora ya tenemos todo preparado y podemos añadir la plantilla del dispositivo, para ello, nos vamos a la sección de dispositivos de seguridad y le damos a la opción de añadir nueva plantilla:



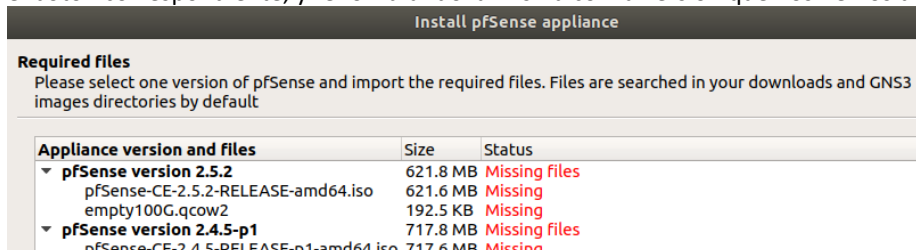
A continuación, indicamos que deseamos realizar la instalación a partir de un appliance disponible en el servidor de GNS3:



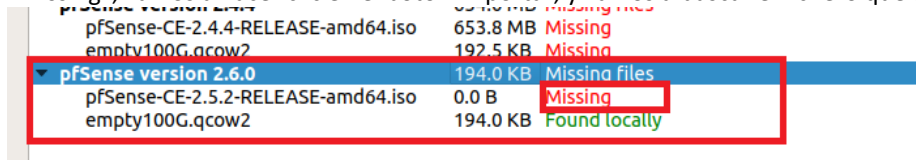
En la siguiente pantalla, ponemos “pfse” en el campo del buscador de appliances, seleccionamos la plantilla denominada “pfSense” (ya viene parametrizada para su emulación en Qemu con la interfaz em0 configurada como WAN y la em1 como LAN) y le damos al botón de instalar:



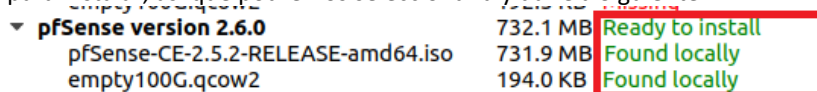
En las siguientes dos pantallas, seleccionamos el despliegue en el equipo local y que use el binario de Qemu de la última versión de 64 bits. Una vez que lleguemos a la pantalla de archivos requeridos para la instalación, vamos a crear una nueva versión (para incorporar la ISO de la última versión que hemos descargado), haciendo clic en el botón correspondiente, y renombrando la misma con la versión que nos hemos descargado previamente:



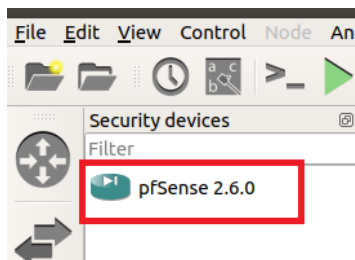
Una vez creada la nueva versión, veremos que algunos de los ficheros necesarios (la imagen ISO de instalación y la imagen del disco duro virtual) no están localizados, así que para cada uno de los ficheros que aparezcan como “Missing”, vamos a hacer clic en el botón Importar, y vamos a buscar el fichero que descargamos previamente:



Cuando ya hayamos importados todos los ficheros necesarios, ya veremos que la versión asociada está disponible para instalar, así que podremos seleccionarla y darle a Siguiente:



A continuación, finalizamos la instalación y ya veremos la plantilla del dispositivo disponible:



Paso 2. Añadir e instalar el cortafuegos pfSense en el proyecto de GNS3

Una vez que tengamos creada la plantilla, ya podemos añadir un dispositivo pfSense en nuestros proyectos, para ello, es recomendable crear un nuevo proyecto, partiendo del finalizado en la práctica 1, de forma que guardemos una copia de todo lo realizado previamente.

En el proyecto, añadiremos un dispositivo de tipo pfSense y otro de tipo Cloud (a este último le cambiaremos el nombre a Internet) y los conectaremos con el resto de los elementos ya existentes de la forma indicada en la figura [2] (analizar y revisar la asignación de puertos en donde corresponda):

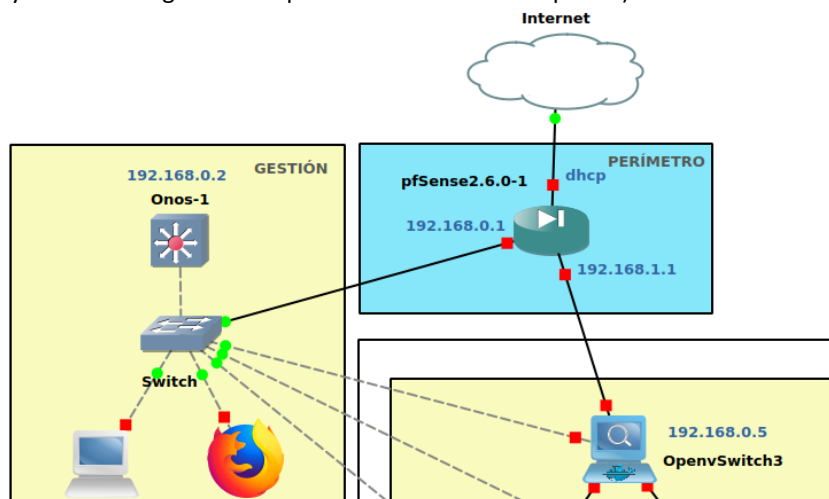
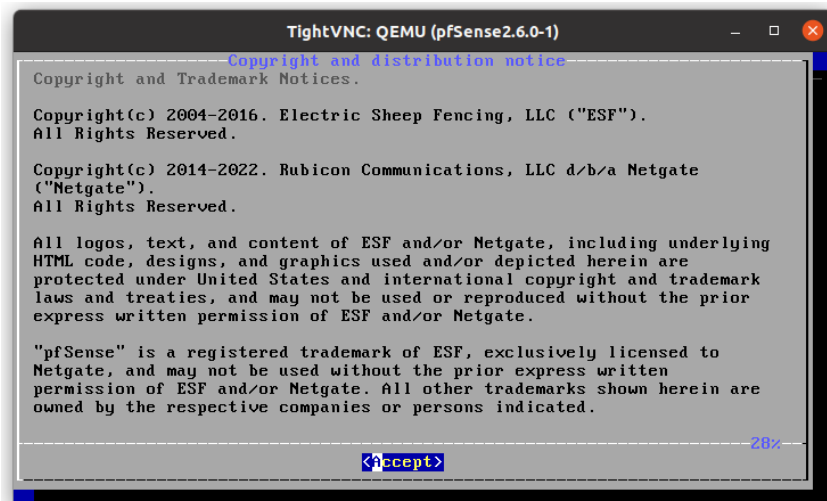


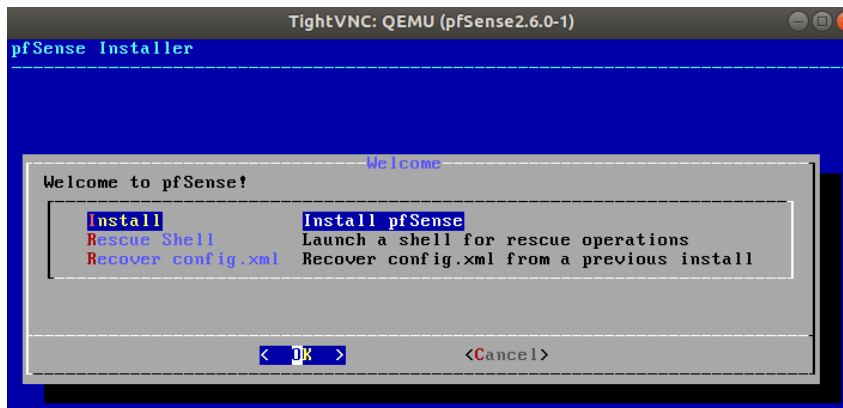
Figura 2. Montaje inicial del cortafuegos sobre lo realizado en la práctica 1.

Una vez añadidos y conectados los dispositivos, arrancaremos el cortafuegos y abriremos su consola para ver el progreso de su arranque inicial.

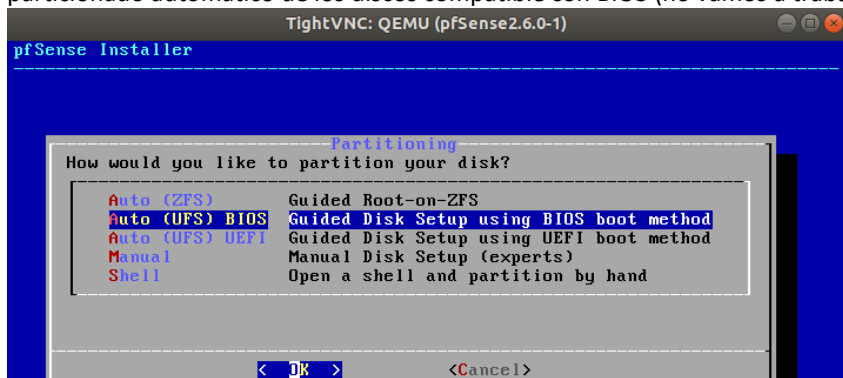
Una vez terminado el arranque inicial, llegaremos a la primera pantalla del asistente de instalación, en donde indicaremos que aceptamos el aviso sobre derechos de autor y de distribución del software pfSense:



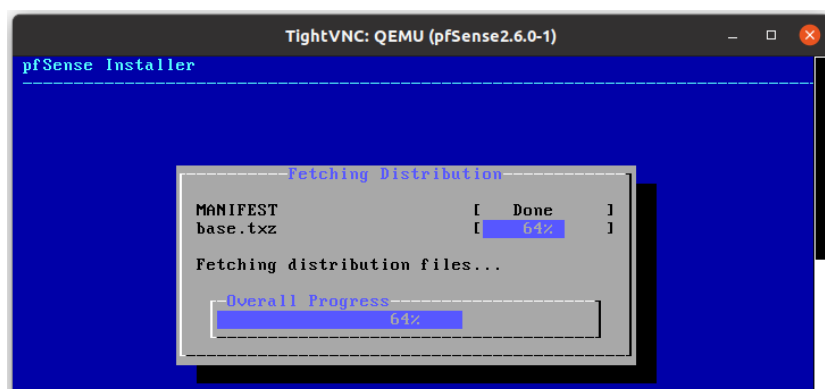
En la siguiente pantalla seleccionamos la opción de instalación:



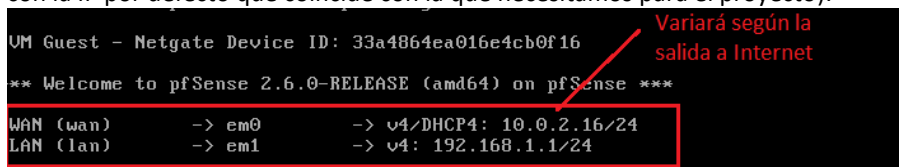
Continuamos con la distribución de teclado por defecto, y seleccionamos la opción de configuración y particionado automático de los discos compatible con BIOS (no vamos a trabajar esta parte):



A continuación, se iniciará el proceso de instalación y deberemos esperar a que finalice:



Una vez finalizado el asistente de instalación, confirmamos el reinicio del cortafuegos. Al terminar el reinicio (tardará algunos minutos en hacerlo) la consola debería tener la siguiente apariencia (la interfaz WAN debería haber recibido una IP por DHCP desde la interfaz de red del equipo y la interfaz LAN se debe haber configurado con la IP por defecto que coincide con la que necesitamos para el proyecto):



Paso 3. Configuración básica de red del cortafuegos pfSense

Hasta este momento solamente tenemos asignadas y configuradas las interfaces em0 (WAN) y em1 (LAN), vamos a añadir ahora, desde la consola, las dos interfaces adicionales que vamos a necesitar: em2 (MGMT) y em3 (DMZ). Para ello, en el menú inicial, elegimos la opción “1 Assign Interfaces”, y a continuación repasamos la asignación:

```
TightVNC: QEMU (pfSense2.6.0-1)
Do VLANs need to be set up first?
If VLANs will not be used, or only for optional interfaces, it is typical to
say no here and use the webConfigurator to configure VLANs later, if required.
should VLANs be set up now [y/n]? n      No configuramos VLAN

If the names of the interfaces are not known, auto-detection can
be used instead. To use auto-detection, please disconnect all
interfaces before pressing 'a' to begin the process.

Enter the WAN interface name or 'a' for auto-detection      WAN -> em0
(em0 em1 em2 em3 em4 em5 or a): em0

Enter the LAN interface name or 'a' for auto-detection      LAN -> em1
NOTE: this enables full Firewalling/NAT mode.
(em1 em2 em3 em4 em5 a or nothing if finished): em1

Enter the Optional 1 interface name or 'a' for auto-detection      MGMT -> em2
(em2 em3 em4 em5 a or nothing if finished): em2

Enter the Optional 2 interface name or 'a' for auto-detection      DMZ -> em3
(em3 em4 em5 a or nothing if finished): em3

Enter the Optional 3 interface name or 'a' for auto-detection
(em4 em5 a or nothing if finished):
```

Una vez configuradas las cuatro interfaces que necesitamos, paramos el proceso de configuración pulsando la tecla Enter/Intro sin haber escrito nada.

```
Enter the Optional 3 interface name or 'a' for auto-detection
(em4 em5 a or nothing if finished):

The interfaces will be assigned as follows:
WAN -> em0
LAN -> em1
OPT1 -> em2
OPT2 -> em3

Do you want to proceed [y/n]? y
```

Una vez recargada la configuración, ya veremos las 4 interfaces por la consola:

```
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
KVM Guest - Netgate Device ID: 33a4864ea016e4cb0f16
*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan) -> em0 -> v4/DHCP4: 10.0.2.16/24
LAN (lan) -> em1 -> v4: 192.168.1.1/24
OPT1 (opt1) -> em2 ->
OPT2 (opt2) -> em3 ->
```

Ahora vamos a configurar el direccionamiento IP de las interfaces (la em3 (DMZ) la dejaremos para luego):

- em0 (WAN): lo vamos a dejar por DHCP (no modificamos nada).
- em1 (LAN): vamos a dejar la IP 192.168.1.1/24 que nos vale para el proyecto (no modificamos nada).
- em2 (MGMT): vamos a asignar la IP 192.168.0.1/24 (desde esta interfaz administraremos el cortafuegos desde la red de GESTIÓN).

Para realizar la configuración de las direcciones IP por la consola, seleccionamos la opción 2 “Set Interface(s) IP address”:

```

0) Logout (SSH only)
1) Assign Interfaces
2) Set interface(s) IP address
3) Reset webConfigurator password
4) Reset to factory defaults
5) Reboot system
6) Halt system
7) Ping host
8) Shell
9) pfTop
10) Filter Logs
11) Restart webConfigurator
12) PHP shell + pfSense tools
13) Update from console
14) Enable Secure Shell (sshd)
15) Restore recent configuration
16) Restart PHP-FPM
Enter an option:

```

Seleccionamos la opción 3, para configurar la interfaz em2 (MGMT), y ponemos la dirección IP y la máscara en notación CIDR (indicamos 24):

```

Available interfaces:
1 - WAN (em0 - dhcp, dhcp6)
2 - LAN (em1 - static)
3 - OPT1 (em2)
4 - OPT2 (em3)
Enter the number of the interface you wish to configure: 3
Enter the new OPT1 IPv4 address. Press <ENTER> for none:
192.168.0.1
Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8
Enter the new OPT1 IPv4 subnet bit count (1 to 32):
24

```

La configuramos como interfaz interna (de tipo LAN sin gateway), de momento no activamos un servidor DHCP en esta interfaz (lo haremos por la GUI) y marcamos que es posible el acceso HTTP al webConfigurator (la interfaz GUI por web) para simplificar (no es lo recomendable desde el punto de vista de seguridad):

```

For a WAN, enter the new OPT1 IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>
Enter the new OPT1 IPv6 address. Press <ENTER> for none:
>
Do you want to enable the DHCP server on OPT1? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) y
Please wait while the changes are saved to OPT1...
Reloading filter...

```

A continuación, comprobaremos que las interfaces tienen asignadas sus direcciones IP de forma correcta:

```

FreeBSD/amd64 (pfSense.localdomain) (ttyv0)
VM Guest - Netgate Device ID: fec0b82b1a33ec9461b7
** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense **

WAN (wan)      -> em0      -> v4/DHCP4: 10.0.2.16/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24
MGMT (opt1)    -> em2      -> v4: 192.168.0.1/24
DMZ (opt2)     -> em3      ->

```

La IP WAN dependerá del acceso a Internet

Por último, verificamos que es posible el acceso a Internet desde el cortafuegos, para ello nos vamos a la opción 8 de la consola "Shell", y lanzamos un ping contra un servidor en Internet (si hubiese algún fallo revisarlo y solventarlo):

```

8) Shell

Enter an option 8

2.6.0-RELEASE[root@pfSense.localdomain]/root: ping www.google.es
PING www.google.es (216.58.209.67): 56 data bytes
4 bytes from 216.58.209.67: icmp_seq=0 ttl=114 time=68.732 ms
4 bytes from 216.58.209.67: icmp_seq=1 ttl=114 time=50.063 ms
4 bytes from 216.58.209.67: icmp_seq=2 ttl=114 time=59.475 ms
4 bytes from 216.58.209.67: icmp_seq=3 ttl=114 time=46.399 ms

```

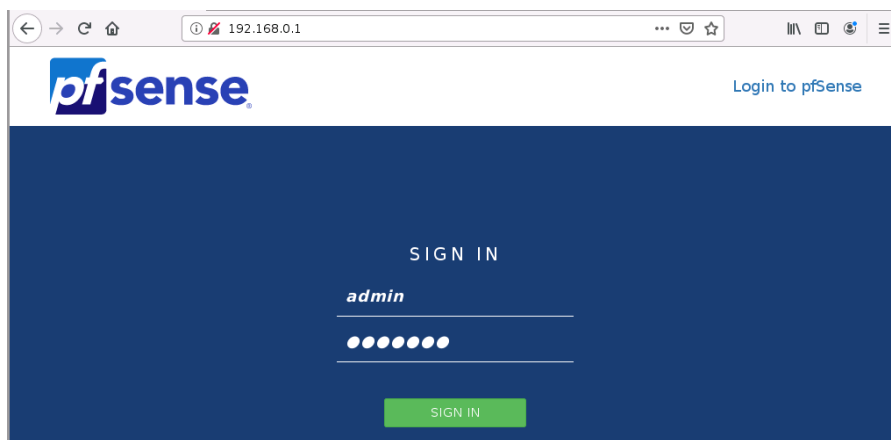
Paso 4. Acceso a la gestión web del cortafuegos pfSense

Por defecto, el acceso web a la gestión del cortafuegos se habilita solamente desde la interfaz LAN (em2), pero en nuestro caso necesitamos habilitarlo desde la red de GESTIÓN, de manera que podamos conectarnos desde webterm-1 y realizar las tareas de administración (es muy recomendable que no se pueda acceder desde la red de USUARIOS).

Para activar el acceso a la gestión web desde la interfaz em2 (ahora OPT1, pero que más adelante llamaremos MGMT), vamos a la consola del pfSense, elegimos la opción 8 "Shell", y a continuación lanzamos los siguientes comandos para establecer reglas rápidas desde la consola (dejar pasar en la interfaz de gestión el tráfico TCP al puerto 80 desde cualquier origen y a cualquier destino, esta regla es recomendable restringirla más adelante en cuando podamos):

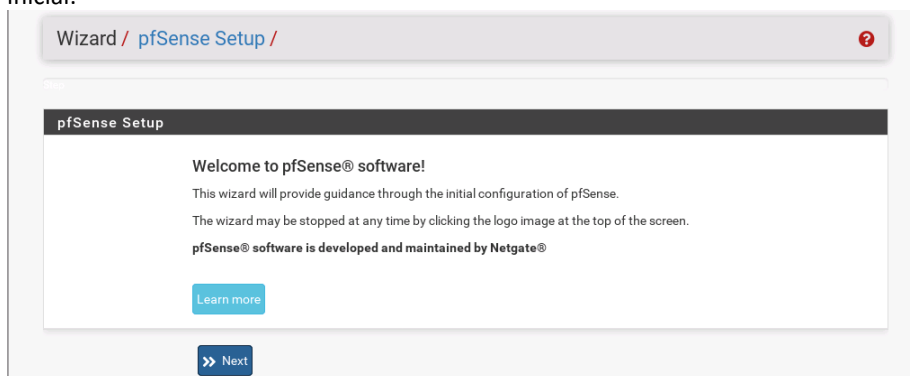
```
# easyrule pass mgmt tcp any any 80
```

A continuación, arrancamos webterm-1 y desde su navegador web accedemos a la dirección de la interfaz em2 (OPT1 o MGMT) del cortafuegos, esto es <https://192.168.0.1>, y nos validamos con las credenciales por defecto (nombre de usuario «admin» y clave «pfsense»).



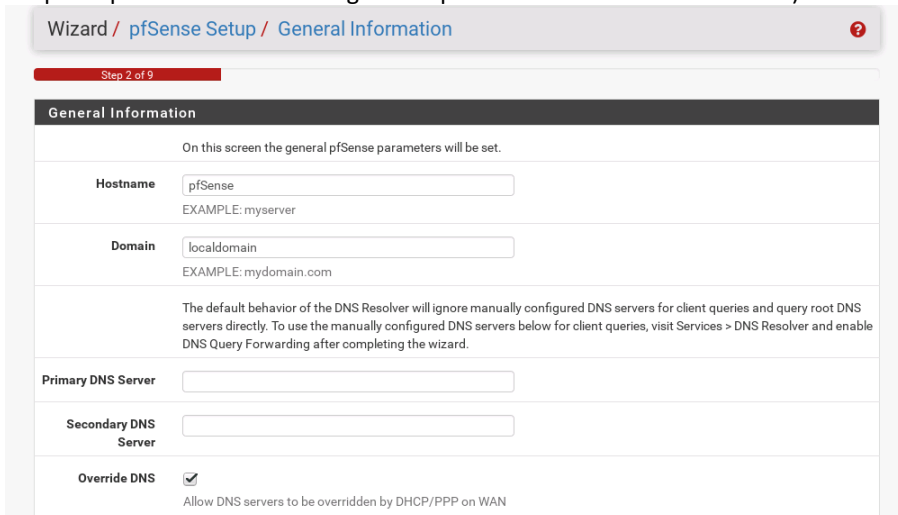
Paso 5. Configuración básica del cortafuegos pfSense

Cuando accedamos por primera vez a la interfaz web de gestión se nos mostrará un asistente de configuración inicial:



Iremos dando a siguiente en cada pantalla, y dejaremos la mayoría de las opciones en sus valores por defecto, salvo las siguientes:

Configuraremos el nombre, el dominio y los servidores DNS (no indicaremos algunos específicos y marcaremos la opción para heredar los configurados por DHCP desde la interfaz WAN):



Wizard / pfSense Setup / General Information

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname
EXAMPLE: myserver

Domain
EXAMPLE: mydomain.com

The default behavior of the DNS Resolver will ignore manually configured DNS servers for client queries and query root DNS servers directly. To use the manually configured DNS servers below for client queries, visit Services > DNS Resolver and enable DNS Query Forwarding after completing the wizard.

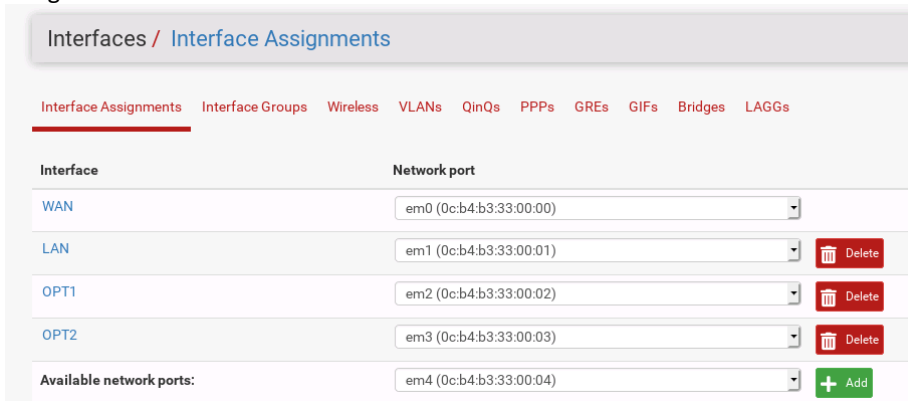
Primary DNS Server

Secondary DNS Server

Override DNS ☒
Allow DNS servers to be overridden by DHCP/PPP on WAN

Por último, cambiamos la contraseña del administrador (usuario admin) y recargamos la configuración.

A continuación, completamos la configuración de las interfaces de red, y para ello nos vamos a Interfaces -> Assignments:



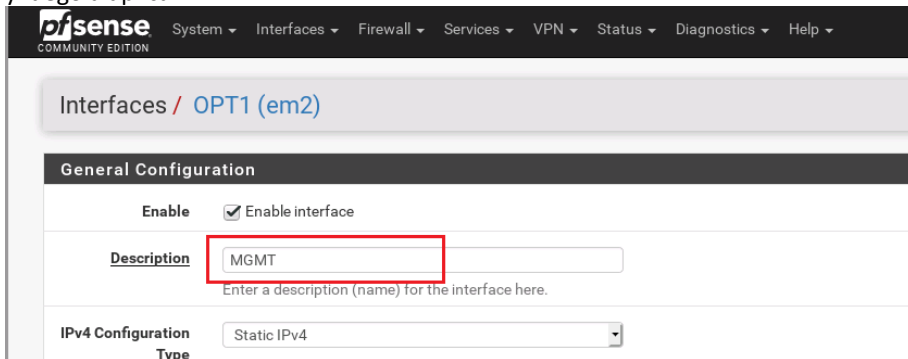
Interfaces / Interface Assignments

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

Interface	Network port	
WAN	em0 (0c:b4:b3:33:00:00)	
LAN	em1 (0c:b4:b3:33:00:01)	Delete
OPT1	em2 (0c:b4:b3:33:00:02)	Delete
OPT2	em3 (0c:b4:b3:33:00:03)	Delete
Available network ports:	em4 (0c:b4:b3:33:00:04)	Add

Accedemos a las interfaces OPT1 y OPT2 (haciendo clic sobre cada una) y reconfiguramos su nombre y otros parámetros:

Para OPT1, vamos a cambiar el nombre a MGMT (la IP ya la habíamos configurado por CLI), le damos a guardar y luego a aplicar:



pfSense COMMUNITY EDITION

System Interfaces Firewall Services VPN Status Diagnostics Help

Interfaces / OPT1 (em2)

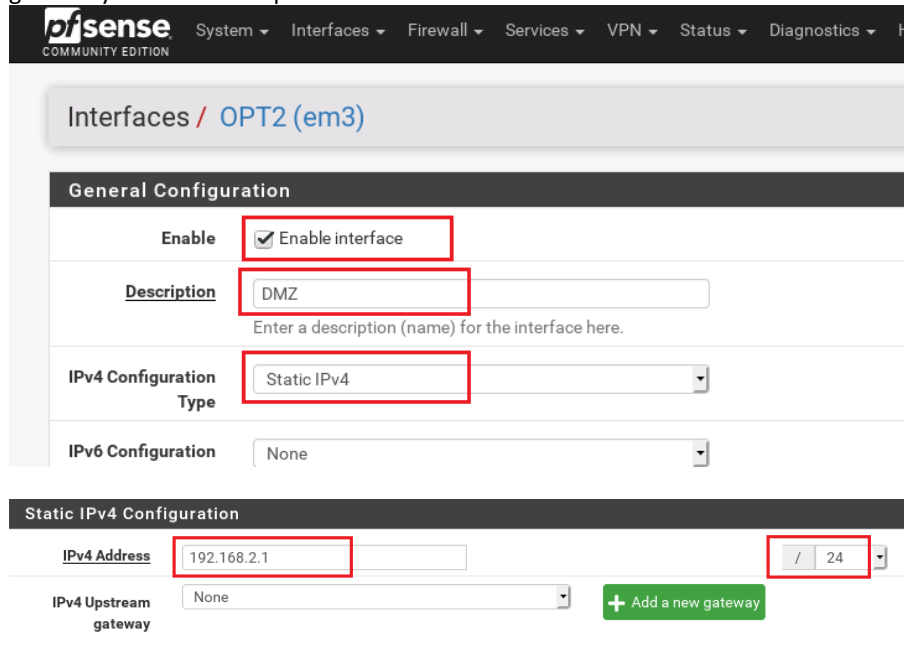
General Configuration

Enable ☒ Enable interface

Description
Enter a description (name) for the interface here.

IPv4 Configuration Type

Para OPT2, vamos a cambiar el nombre a DMZ y configuraremos el direccionamiento IP, luego le daremos a guardar y finalmente a aplicar:



Interfaces / OPT2 (em3)

General Configuration

Enable ☒ Enable interface

Description DMZ
Enter a description (name) for the interface here.

IPv4 Configuration Type Static IPv4

IPv6 Configuration None

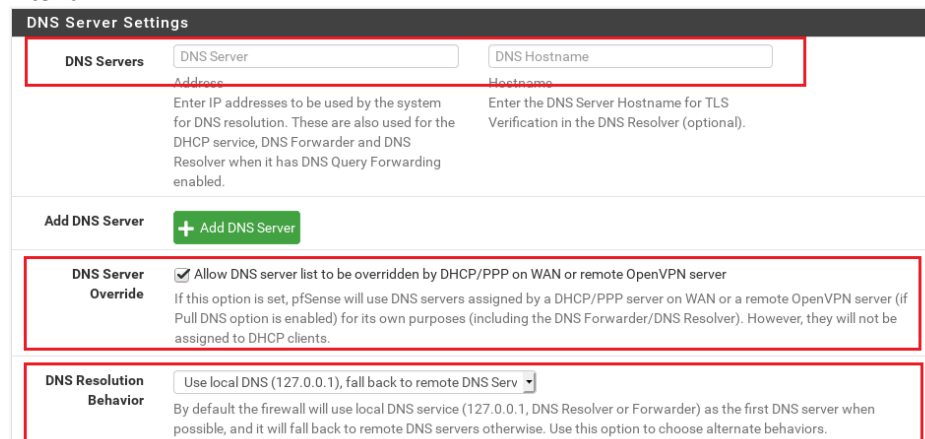
Static IPv4 Configuration

IPv4 Address 192.168.2.1 / 24

IPv4 Upstream gateway None [+ Add a new gateway](#)

Paso 6. Configuración del servicio DNS

A través del asistente de configuración inicial, ya hemos establecido en System -> General Setup, para la configuración DNS [2], que no vamos a forzar el uso de servidores DNS específicos, sino que hemos marcado la opción para dar prioridad a los servidores DNS que el DHCP de la interfaz WAN nos indique (en nuestro caso, el cortafuegos usará la interfaz de nuestro equipo, y lo normal es que obtenga su configuración de red de forma dinámica a través de DHCP). También hemos establecido como comportamiento por defecto el uso en primer lugar del DNS local (los equipos internos deberán usar como servidor DNS la interfaz del cortafuegos en su red) y luego el fallback (si no se puede resolver en local) sobre los servidores DNS obtenidos por el cliente DHCP de la interfaz WAN.



DNS Server Settings

DNS Servers

DNS Server Address
Enter IP addresses to be used by the system for DNS resolution. These are also used for the DHCP service, DNS Forwarder and DNS Resolver when it has DNS Query Forwarding enabled.

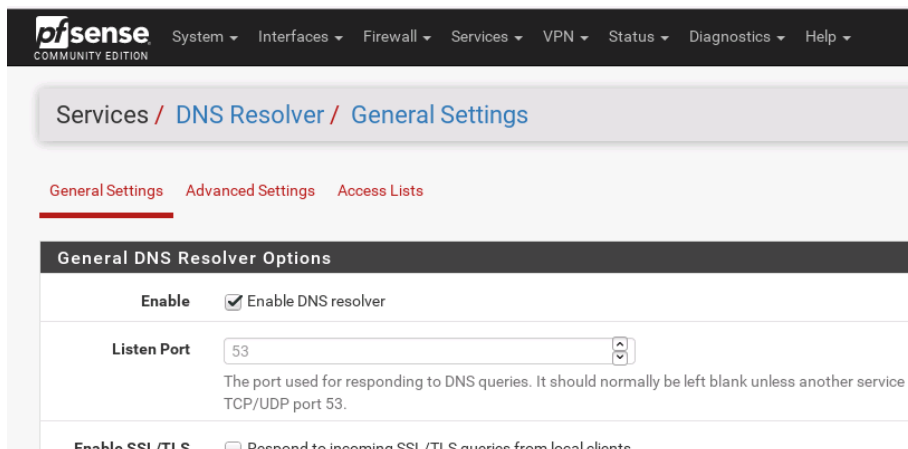
DNS Server Hostname
Enter the DNS Server Hostname for TLS Verification in the DNS Resolver (optional).

Add DNS Server [+ Add DNS Server](#)

DNS Server Override ☒ Allow DNS server list to be overridden by DHCP/PPP on WAN or remote OpenVPN server
If this option is set, pfSense will use DNS servers assigned by a DHCP/PPP server on WAN or a remote OpenVPN server (if Pull DNS option is enabled) for its own purposes (including the DNS Forwarder/DNS Resolver). However, they will not be assigned to DHCP clients.

DNS Resolution Behavior Use local DNS (127.0.0.1), fall back to remote DNS Serv
By default the firewall will use local DNS service (127.0.0.1, DNS Resolver or Forwarder) as the first DNS server when possible, and it will fall back to remote DNS servers otherwise. Use this option to choose alternate behaviors.

A continuación, debemos verificar que el DNS Resolver o el DNS Forwarder esté activo, ya que para poder gestionar el fallback sobre los DNS externos al menos uno de los dos debe estar activo (no pueden estarlo los dos al mismo tiempo). Para ello, nos vamos a Services -> DNS Resolver y comprobamos (lo normal es que esté activo):



Ahora vamos a configurar y probar la resolución DNS en webterm-1 contra la interfaz del cortafuegos en su red, para ello editamos su configuración de red, e indicamos que su servidor DNS será la interfaz del cortafuegos en la red MGMT:

```
# Static config for eth0
auto eth0
iface eth0 inet static
    address 192.168.0.100
    netmask 255.255.255.0
    gateway 192.168.0.1
    up echo nameserver 192.168.0.1 > /etc/resolv.conf
```

Si ahora probamos la resolución DNS desde webterm-1, abriendo un terminal con el comando host, veremos que aún no es posible (pero si observamos que las peticiones se remiten al cortafuegos):

```
LXTerminal
File Edit Tabs Help

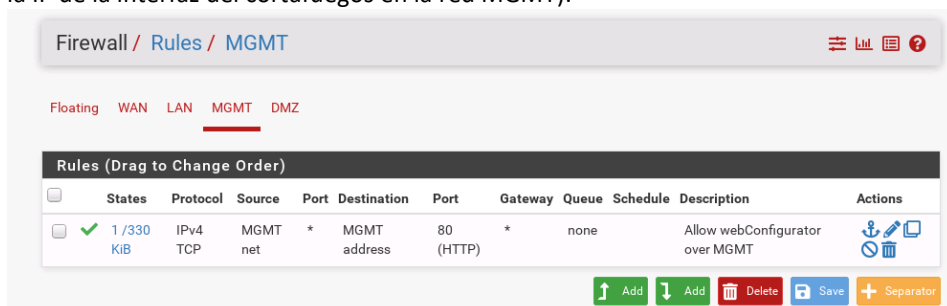
root@webterm-1:~#
root@webterm-1:~#
root@webterm-1:~# host www.google.es
; Warning: response timeout for 192.168.0.1@53(UDP)

; Warning: response timeout for 192.168.0.1@53(UDP)
; Warning: failed to query server 192.168.0.1@53(UDP)
; Warning: response timeout for 192.168.0.1@53(UDP)

; Warning: response timeout for 192.168.0.1@53(UDP)
; Warning: failed to query server 192.168.0.1@53(UDP)
; Warning: response timeout for 192.168.0.1@53(UDP)

; Warning: response timeout for 192.168.0.1@53(UDP)
; Warning: failed to query server 192.168.0.1@53(UDP)
root@webterm-1:~# ^C
```

¿Qué puede estar ocurriendo?, pues lo más habitual en estos casos es que nos falte habilitar el tráfico en el cortafuegos. Si vamos a Firewall -> Rules -> MGMT, veremos que solamente tenemos creada la regla que habilitamos desde consola para permitir el acceso a la interfaz web de gestión (aprovechamos para restringirla a la IP de la interfaz del cortafuegos en la red MGMT):



Esta regla significa que el tráfico IPv4 que contenga el protocolo TCP, con origen en cualquier IP de la red MGMT, y desde cualquier puerto, puede iniciar sesiones a la IP del pfSense en esa red, y sobre el puerto 80.

Nota: las reglas se definen pensando en tratar el tráfico de inicio de una comunicación, pero al mismo tiempo se aplican sobre el tráfico de respuesta relacionado (el cortafuegos detecta y mantiene las sesiones activas y es capaz de identificar todo el tráfico asociado y de aplicarle la misma regla que definimos para el inicio), por tanto, no es necesario crear otra regla para habilitar el tráfico de respuesta en el sentido contrario.

El cortafuego pfSense se comporta en modo “Explicit Deny”, es decir, que si el tráfico recibido no hace match (sus características no coinciden con los criterios definidos) en ninguna de las reglas establecidas (se van evaluando en orden de arriba a abajo), el mismo se deniega a través de la regla por defecto (“Default deny rule”). Si, por el contrario, hace match en alguna regla, se ejecuta la acción establecida y no se evalúan el resto de reglas. En este sentido, podemos comprobar en Status -> System Logs -> Firewall (los logs de filtrado de paquetes del cortafuegos) que el tráfico DNS generado por webterm-1 a la interfaz MGMT del cortafuegos sobre el puerto UDP 53 aparece como denegado por la Default deny rule (no había ninguna regla que habilitase el tráfico):

Nota: Ante cualquier problema es muy importante siempre indagar primero en los logs de eventos de filtrado del cortafuegos, es decir en Status -> System Logs -> Firewall, para comprobar si la causa del mismo puede ser un bloqueo de tráfico.

Status / System Logs / Firewall / Normal View

System Firewall DHCP Authentication IPsec PPP PPPoE/L2TP Server OpenVPN NTP Packages Settings

Normal View Dynamic View Summary View

Last 500 Firewall Log Entries. (Maximum 500)

Action	Time	Interface	Rule	Source	Destination	Protocol
✗	Apr 30 19:23:17	MGMT	Default deny rule IPv4 (1000000103)	192.168.0.100:43005	192.168.0.1:53	UDP

Vamos entonces a añadir una regla para permitir el tráfico DNS, quedando la configuración de la siguiente forma:

Firewall / Rules / MGMT

Floating WAN LAN MGMT DMZ

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	IPv4 UDP	MGMT net	*	MGMT address	53 (DNS)	*	none			
<input type="checkbox"/>	✓ 1/37 KIB	IPv4 TCP	MGMT net	*	MGMT address	80 (HTTP)	*	none		Allow webConfigurator over MGMT	

Add Add Delete Save Separator

Ahora, si volvemos a comprobar la realización de consultas DNS, ya veremos que es posible:

```
root@webterm-1:~#
root@webterm-1:~#
root@webterm-1:~# host www.google.es
www.google.es. has IPv4 address 142.250.178.163
www.google.es. has IPv6 address 2a00:1450:4003:807::2003
Host www.google.es. has no MX record
root@webterm-1:~#
```

Paso 7 Configuración del servicio DHCP

El Servicio DHCP se encarga de gestionar, para cada interfaz, la asignación de direcciones IP, dentro de un rango preconfigurado, a los equipos locales que lo soliciten. Esta asignación puede ser dinámica (va cambiando) o estática (asignamos siempre a un equipo la misma dirección IP en función de su MAC).

En nuestro caso vamos a tener tres servidores DHCP, uno por cada subred interna (interfaz del cortafuegos), y en cada uno tendremos definido un rango de direcciones IP diferente, dejando el resto de los parámetros de configuración a los valores por defecto.

Para realizar la configuración DHCP nos vamos a ir a la opción de menú Services -> DHCP Server, y luego en cada interfaz haremos lo siguiente:

En MGMT, activaremos el servidor DHCP:

Services / DHCP Server / MGMT

LAN **MGMT** DMZ

General Options

Enable ☒ Enable DHCP server on MGMT interface

BOOTP ☐ Ignore BOOTP queries

Indicaremos el siguiente rango de direcciones IP a servir (un rango alto y dejamos las direcciones bajas para las reservas estáticas):

Subnet 192.168.0.0

Subnet mask 255.255.255.0

Available range 192.168.0.1 - 192.168.0.254

Range

From To

Additional Pools

Todas las demás opciones las dejamos por defecto (el servidor DNS y la puerta de enlace a configurar por DHCP en los equipos será la propia interfaz del cortafuegos en la subred) y le damos a guardar.

Si ahora modificamos la configuración de red de webterm-1 para que se obtenga por DHCP desde el cortafuegos:

```
# Static config for eth0
#auto eth0
#iface eth0 inet static
#    address 192.168.0.100
#    netmask 255.255.255.0
#    gateway 192.168.0.1
#    up echo nameserver 192.168.0.1 > /etc/resolv.conf

# DHCP config for eth0
auto eth0
iface eth0 inet dhcp
```

Y reiniciamos el equipo, podremos comprobar, iniciando previamente una captura de paquetes en la interfaz de webterm-1, el intercambio de mensajes DHCP y la configuración enviada al equipo:

No.	Time	Source	Destination	Protocol	Length	Info
2	0.019911	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Tr
5	1.052803	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Tr
6	1.059951	192.168.0.1	192.168.0.101	DHCP	342	DHCP Offer - Tr
7	1.064582	192.168.0.1	192.168.0.101	DHCP	342	DHCP Offer - Tr
8	1.079944	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Tr
9	1.088130	192.168.0.1	192.168.0.101	DHCP	342	DHCP ACK - Tr

```
Client IP address: 0.0.0.0
Your (client) IP address: 192.168.0.101
Next server IP address: 0.0.0.0
Relay agent IP address: 0.0.0.0
Client MAC address: 6a:a2:cf:b6:98:89 (6a:a2:cf:b6:98:89)
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
Option: (53) DHCP Message Type (ACK)
Option: (54) DHCP Server Identifier (192.168.0.1)
Option: (51) IP Address Lease Time
Option: (1) Subnet Mask (255.255.255.0)
Length: 4
Subnet Mask: 255.255.255.0
Option: (3) Router
Length: 4
Router: 192.168.0.1
Option: (6) Domain Name Server
Length: 4
Domain Name Server: 192.168.0.1
Option: (15) Domain Name
```


Nota: una herramienta muy útil para el diagnóstico de problemas son las capturas de tráfico, que además podemos hacer de forma integrada en GNS3, para ello solamente debemos hacer clic con el botón derecho sobre el enlace que queremos analizar (cuando se ponga de color rojo) y le damos a la opción de iniciar captura (esto nos abrirá una ventana de Wireshark).

Podemos comprobar también en webterm-1 la aplicación de la configuración de red obtenida por DHCP:

```

LXTerminal
File Edit Tabs Help

root@webterm-1:~# ifconfig eth0
eth0      Link encap:Ethernet  Hwaddr 6a:a2:cf:b6:98:89
          inet addr:192.168.0.101 Bcast:0.0.0.0 Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
          RX packets:157 errors:0 dropped:0 overruns:0 frame:0
          TX packets:548 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:84265 (82.2 KiB)  TX bytes:43512 (42.4 KiB)

root@webterm-1:~# cat /etc/resolv.conf
search localdomain
nameserver 192.168.0.1
root@webterm-1:~#
root@webterm-1:~# route
Kernel IP routing table
Destination Gateway      Genmask         Flags Metric Ref    Use Iface
default     192.168.0.1    0.0.0.0         UG        208    0      0 eth0
192.168.0.0 *            255.255.255.0   U         0       0      0 eth0
root@webterm-1:~#

```

A continuación, vamos a realizar una asignación DHCP estática al servidor onos-1. Previamente necesitamos obtener su dirección MAC, así que una de las formas de hacerlo es haciendo una captura de tráfico en su interfaz de red, realizando por ejemplo un ping desde webterm-1, buscando los mensajes intercambiados por la dirección 192.168.0.2, y comprobando la dirección MAC en la captura:

```

15 31.365185 192.168.0.2 192.168.0.114 ICMP 98 Echo (ping) reply id=0x051
16 32.379903 192.168.0.114 192.168.0.2 ICMP 98 Echo (ping) request id=0x051
17 32.380160 192.168.0.2 192.168.0.114 ICMP 98 Echo (ping) reply id=0x051
18 33.404154 192.168.0.114 192.168.0.2 ICMP 98 Echo (ping) request id=0x051
+ 19 33.404544 192.168.0.2 192.168.0.114 ICMP 98 Echo (ping) reply id=0x051
20 34.405371 192.168.0.114 192.168.0.2 ICMP 98 Echo (ping) request id=0x051
21 34.405691 192.168.0.2 192.168.0.114 ICMP 98 Echo (ping) reply id=0x051

Frame 19: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
Ethernet II, Src: f6:b5:cf:76:3c:15 (f6:b5:cf:76:3c:15), Dst: 72:b1:88:74:e4:32 (72:b1:88:74:e4:32)
  Destination: 72:b1:88:74:e4:32 (72:b1:88:74:e4:32)
    Address: 72:b1:88:74:e4:32 (72:b1:88:74:e4:32)
      ....1. .... = LG bit: Locally administered address (this is NOT the factory default)
      ....0. .... = IG bit: Individual address (unicast)
  - Source: f6:b5:cf:76:3c:15 (f6:b5:cf:76:3c:15)
    Address: f6:b5:cf:76:3c:15 (f6:b5:cf:76:3c:15)
      ....1. .... = LG bit: Locally administered address (this is NOT the factory default)

```

Vamos a crear la asignación estática en el DHCP a partir de esta MAC, y para ello vamos a la opción de menú Services -> DHCP Server -> MGMT, y al final del todo, le damos a añadir un mapeo de DHCP estático nuevo, ponemos los datos del servidor onos-1, le damos a guardar y finalmente a aplicar:

Save

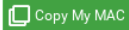
DHCP Static Mappings for this Interface

Static ARP	MAC address	IP address	Hostname	Description

+ Add

Services / DHCP Server / MGMT / Edit Static Mapping

Static DHCP Mapping on MGMT

MAC Address	<input type="text" value="f6:b5:cf:76:3c:15"/>	
MAC address (6 hex octets separated by colons)		
Client Identifier	<input type="text" value="onos-1"/>	
IP Address	<input type="text" value="192.168.0.2"/>	
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. The same IP address may be assigned to multiple mappings.		
Hostname	<input type="text" value="onos-1"/>	
Name of the host, without domain part.		
Description	<input type="text" value="SDN Controller"/>	
A description may be entered here for administrative reference (not parsed).		

El problema que tenemos con esta configuración en nuestro caso, es que como onos-1 está desplegado sobre Docker, y por defecto, en cada reinicio se genera una nueva MAC dinámica, necesitamos forzar el uso de una MAC determinada en su configuración de red, además de activar el cliente DHCP, aplicando la siguiente configuración en onos-1 (y realizando un reinicio):

```
# Static config for eth0
#auto eth0
#iface eth0 inet static
#    address 192.168.0.2
#    netmask 255.255.255.0
#    gateway 192.168.0.1
#    up echo nameserver 192.168.0.1 > /etc/resolv.conf

# DHCP config for eth0
auto eth0
iface eth0 inet dhcp
    hwaddress ether f6:b5:cf:76:3c:15
```

Comprueba con una captura que se ha asignado de forma correcta la MAC y la dirección adecuada por DHCP en onos-1.

A continuación, vamos a crear, añadir y configurar el dispositivo webterm-2 que vamos a incorporar en la red de USUARIOS de acuerdo con lo que se indica en la figura [1]. Vamos a configurar tanto en PC-1 como en webterm-2 la configuración de red de forma dinámica con el DHCP. Para ello, revisa que para la red LAN (USUARIOS), esté activado el servidor DHCP, y que la asignación dinámica se realice sobre el rango mostrado en la siguiente figura:

Subnet	192.168.1.0	
Subnet mask	255.255.255.0	
Available range	192.168.1.1 - 192.168.1.254	
Range	<input type="text" value="192.168.1.100"/>	<input type="text" value="192.168.1.200"/>
	From	To

Por último, vamos a revisar las reglas en la interfaz LAN, para evitar el acceso a la consola y permitir además el tráfico de navegación (y otros). Para quitar la regla por defecto de Anti-Lockout (la que habilita el acceso a la consola desde la red LAN) debemos ir a System -> Advanced -> Admin Access y marcar esta opción (y aplicar luego):

Anti-lockout ☒ Disable webConfigurator anti-lockout rule

When this is unchecked, access to the webConfigurator on the LAN interface is always permitted, regardless of the user-defined firewall rule set. Check this box to disable this automatically added rule, so access to the webConfigurator is controlled by the user-defined firewall rules (ensure a firewall rule is in place that allows access, to avoid being locked out!)
Hint: the "Set interface(s) IP address" option in the console menu resets this setting as well.

Revisa y actualiza las reglas en la interfaz LAN para que queden de esta forma (no permite la conexión a la consola y habilita el tráfico de navegación y DNS, lo recomendable sería restringir la segunda regla):

Firewall / Rules / LAN

Floating WAN LAN MGMT DMZ

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 TCP	LAN net	*	LAN address	80 (HTTP)	*	none			
5/5 KiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	

↑ Add ↓ Add Delete Save + Separator

Por último, verifica que desde webterm-2 no puedes acceder a la gestión web del cortafuegos y que además puedes navegar (por ejemplo, a la página <http://hipertexto.info> cuyo contenido es pequeño para que se pueda abrir desde el emulador).

IMPORTANTE: a partir del momento en el que configuremos algún servidor para obtener su configuración de red a través de DHCP estático, es muy importante que prestemos atención al orden de arranque, de forma que siempre debería arrancar primero el cortafuegos, para asegurar la disponibilidad del servidor DHCP de forma previa al arranque de cualquier equipo para que pueda obtener su configuración de red.



Paso 8. Configuración del NAT Port Forward

En este apartado vamos a aplicar la configuración necesaria para poder publicar servicios de nuestra red, desde la DMZ, hacia el exterior, empleando la funcionalidad de NAT Port Forward [3] que se encarga de redireccionar determinados puertos o rangos que hemos elegido de la IP pública del cortafuegos a máquinas internas.

Vamos a aprovechar para introducir el uso de los Alias, como una de las buenas prácticas a seguir en la configuración de cortafuegos, ya que nos permite incrementar la legibilidad y la facilidad de modificación de la información de configuración. En este caso, los vamos a usar para crear grupos de puertos y de servidores (y así evitar la duplicación de reglas al manejar varios de estos elementos).

Para crear un alias para los servidores web de la DMZ, nos vamos a Firewall -> Aliases -> IP, le damos a añadir y luego a guardar:

Ahora vamos a crear un alias para todos los puertos de acceso web que voy a emplear, a través de los cuales voy a recibir peticiones desde el exterior, y para ello nos vamos a Firewall -> Aliases → Ports, le damos a añadir y luego a guardar:

Una vez creados los alias que vamos a usar para facilitar la configuración de la redirección de puertos para el tráfico entrante (el que se recibe por la interfaz WAN, para que se reenvíe haciendo NAT a una dirección IP interna de la DMZ) nos vamos a la opción de menú Firewall -> NAT -> Port Forward, y le damos a añadir:

Configuramos los siguientes campos, le damos a guardar y finalmente a aplicar:

Firewall / NAT / Port Forward / Edit

Edit Redirect Entry

Disabled ☐ Disable this rule

No RDR (NOT) ☐ Disable redirection for traffic matching this rule
This option is rarely needed. Don't use this without thorough knowledge of the implications.

Interface WAN
Choose which interface this rule applies to. In most cases "WAN" is specified.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

Protocol TCP
Choose which protocol this rule should match. In most cases "TCP" is specified.

Source Display Advanced

Destination ☐ Invert match. WAN address Address/mask

Destination port range Other Web_Ports Other Web_Ports
Specify the port or port range for the destination of the packet for this mapping. The "to" field may be left empty if only mapping a

Redirect target IP Single host Server1
Specify the IP address of the destination of the packet for this mapping. The "to" field may be left empty if only mapping a

Redirect target port Other Web_Ports
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of

Description Port forward to web servers in DMZ
A description may be entered here for administrative reference (not parsed).

No XMLRPC Sync ☐ Do not automatically sync to other CARP members
This prevents the rule on Master from automatically syncing to other CARP members. This does NOT prevent the rule fr

NAT reflection Use system default

Filter rule association Rule NAT Port forward to web server in DMZ
[View the filter rule](#)

El significado de estos campos es el siguiente:




- Interfaz: WAN (es la interfaz externa por la que me van a llegar las peticiones cuyas direcciones externas voy a traducir por las internas).
- Destino: la dirección WAN del cortafuegos.
- Intervalo de puertos de destino: usamos el alias de puertos que hemos creado.
- Redirigir IP de destino: indicamos que un host y ponemos el alias de host que hemos creado.
- Redirigir el puerto de destino: usamos el alias de puertos que hemos creado.
- Descripción: Port forward to web servers in DMZ.

Nota: una buena práctica fundamental es describir de forma muy concreta y resumida la función de cada una de las reglas que configuramos haciendo uso del campo Descripción. Esto facilita la legibilidad y por tanto la administración de las mismas.

Firewall / NAT / Port Forward

Port Forward 1:1 Outbound NAT

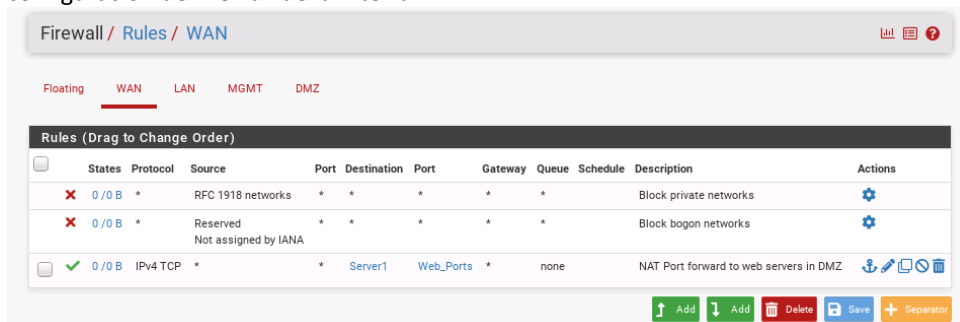
Rules

	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input checked="" type="checkbox"/>	WAN	TCP	*	*	WAN address	Web_Ports	Server1	Web_Ports	Port forward to web servers in DMZ	  

Add
Add
Delete
Save
Separator

Esta configuración NAT nos crea automáticamente una regla de acceso para el tráfico correspondiente en la

configuración de firewall de la interfaz WAN:



3. Mejoras a implementar

3.1 Despliegue y configuración de la zona DMZ

En este apartado debe configurar los elementos necesarios para montar y verificar la zona DMZ [4].

Deberá activar y configurar el DHCP Server de la DMZ de una forma similar a la realizada en la práctica.

Deberá incorporar y configurar en la DMZ un OpenvSwitch integrado en Onos-1 para la conectividad con el cortafuegos de los equipos en la DMZ. Revise y aplique la configuración necesaria.

Luego debe incorporar un equipo (Server1) con un servidor web NGINX, y que debe desplegar containerizado a partir de la imagen ajnouri/nginx (una de las preparadas para su uso en GNS3). Como siempre vamos a crear primero una nueva plantilla para este tipo de dispositivo. A continuación, vamos a incorporar un dispositivo y lo vamos a configurar para que se llame Server1 y use DHCP, creando previamente en el cortafuegos una reserva estática con su MAC (definimos una y la forzamos como parte de la configuración de red del equipo, de una forma similar a la que aplicamos para Onos-1).

Para las pruebas de conexión desde el exterior vamos a desplegar y configurar un Switch y el webterm-3.

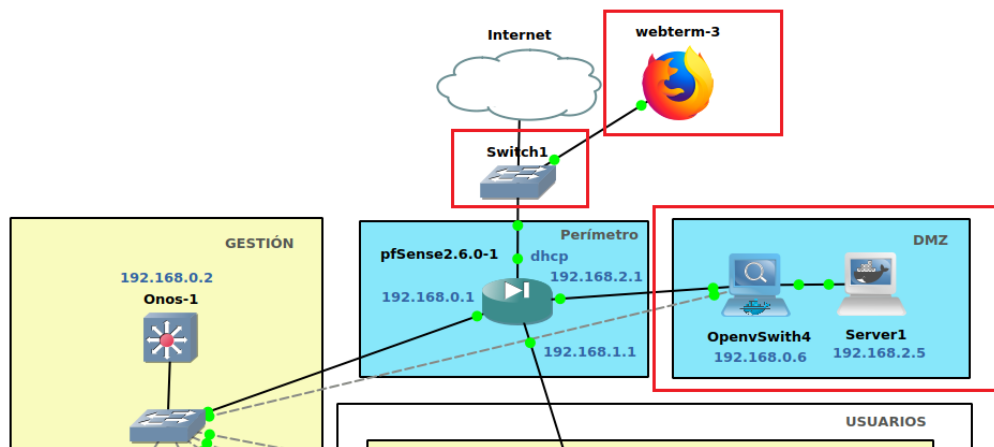
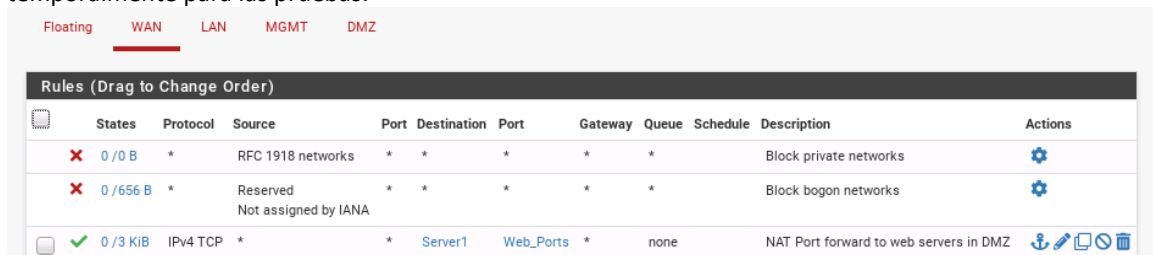
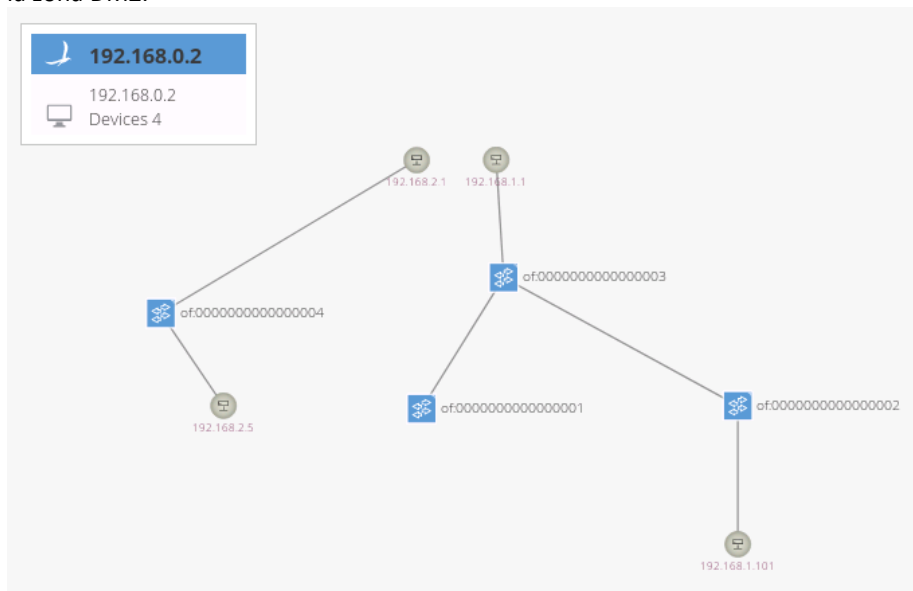


Figura 4. Detalle despliegue en zona DMZ y Perímetro

Tener en cuenta para las pruebas de acceso desde webterm-3, que pfSense activa por defecto dos reglas en las interfaces externas (WAN) para evitar los ataques de IP Spoofing (suplantación de identidad), en las que se deniega por defecto las peticiones con rangos de direcciones privadas, así que debemos desactivarla temporalmente para las pruebas:



Incorporar y analizar la información que se muestra en el controlador ONOS al descubrir la nueva topología en la zona DMZ:



Finalmente debemos comprobar que desde el exterior se pueda acceder al servidor Web existente en Server1. Realizar los ajustes y comprobaciones que estime necesarios.

3.2 Mejoras en la política de seguridad

Estudiar, aplicar y documentar las siguientes mejoras en la configuración de seguridad:

- Admitir solamente la conexión HTTPS a la interfaz de gestión del cortafuegos (no admitir HTTP).
- El acceso HTTPS a la interfaz de gestión del cortafuegos solamente debe ser posible desde la red de GESTIÓN/MGMT.
- 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.
- 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.
- El acceso desde la WAN solamente debe ser posible para las conexiones relacionadas iniciadas desde dentro y para la configuración NAT Port Forward realizada.
- 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.
- Proponga y aplique todas las reglas adicionales o mejoras que estime para mejorar la seguridad.

3.3 Mejoras en la política de seguridad

Integrar la configuración de VLAN propuesta como mejora en la práctica 1.

Referencias

- [1] Portal de documentación de pfSense: <https://docs.netgate.com/pfsense/en/latest/>
- [2] Opciones de configuración DNS de pfSense: <https://docs.netgate.com/pfsense/en/latest/services/dns/index.html>
- [3] Opciones de configuración NAT de pfSense: <https://docs.netgate.com/pfsense/en/latest/nat/index.html>
- [4] Receta de configuración VLAN en pfSense: <https://docs.netgate.com/pfsense/en/latest/recipes/switch-vlan-configuration.htm>
- [5] Guía de seguridad de cortafuegos del CCN: <https://www.ccn-cert.cni.es/series-ccn-stic/guias-de-acceso-publico-ccn-stic/74-ccn-stic-408-seguridad-perimetral-cortafuegos/file.html>