

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

Quitamos puerto 80 y pusimos la 443.

Quitamos todo de la LAN

- 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.

Para poder conectarnos por ssh a los equipos necesitamos instalar en los pcs un paquete que convierta los equipos también en servidores.

```

openssh-blacklist-extra openssh-known-hosts
root@Debian:~# sudo apt-get install openssh-server
sudo: unable to resolve host Debian
Reading package lists... Done

```

Esto en todos los equipos.

- 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.

Reglas antispoofing internas

// Mejorar seguridad de las VLAN

// Asegurarse de que en las interfaces virtuales entran la red de la vlan correspondiente.

// En la LAN no se pueden hacer pasar por alguien que no sea de la lan

/ip firewall filter

//Admitir solamente conexión HTTPS a la interfaz de gestión del cortafuegos (no admitirHTTP)

add chain=input dst-port=443 protocol=tcp in-interface=em2 action=accept

add chain=input action=drop

//Garantiza que la redes de USUARIOS/LAN solamente pueda acceder a los servicios de red que necesita, a Internet y a los servicios en la DMZ

add chain=forward in-interface=em1 dst-port=443 dst-address=192.168.2.5 action=accept

add chain=forward in-interface=em1 out-interface=em0 action=accept

add chain=forward in-interface=em1 action=drop

//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.

add chain=forward in-interface=em2 dst-port=443 dst-address=192.168.2.5 action=accept

add chain=forward in-interface=em2 out-interface=em0 action=accept

add chain=forward in-interface=em2 protocol=tcp dst-port=22,23 out-interface=em3
action=accept

add chain=forward in-interface=em2 protocol=tcp dst-port=22,23 out-interface=em1
action=accept

add chain=forward in-interface=em2 action=drop

add chain=input in-interface=em2 protocol=tcp dst-port=22,23 out-interface=em3
action=accept

add chain=input in-interface=em2 protocol=tcp dst-port=22,23 out-interface=em1
action=accept

add chain=input in-interface=em2 action=drop

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

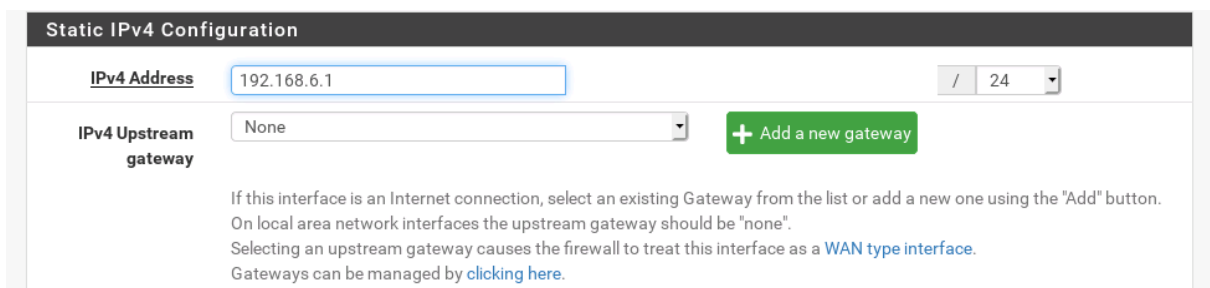
add chain=forward connection-state=established,related in-interface=em0 action=accept

regla hecha si no pregunta lo de la NAT

//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.
 add chain=forward connection-state=established,related in-interface=em3 action=accept
 add chain=forward in-interface=em3 action=drop

// Mejorar seguridad de las VLAN
 // Asegurarse de que en las interfaces virtuales entran la red de la vlan correspondiente.
 // En la LAN no se pueden hacer pasar por alguien que no sea de la lan

Hay que poner el DNS Resolver
 Buscar por que ese y no forwarder.
 Diferencia entre DNS Resolver y Forwarder



Cambiar la ip de la lan porque coincide con la del router

En casa no funcionaba el entrar al servidor desde fuera porque la interfaz de la lan coincidía con el gateway del pfsense (la entrada de nuestro propio router). El problema era la respuesta.

Router casero

configuración de DHCP

servidor DHCP IPv4	<input checked="" type="radio"/> activar	<input type="radio"/> desactivar
dirección IP del Router en la LAN	192 . 168 . 1 . 1	
máscara de subred LAN	255.255.255.0	
dirección IP inicial	192 . 168 . 1 . 10	
dirección IP final	192 . 168 . 1 . 150	
servidor IPv6 DHCP	<input type="radio"/> activar	<input checked="" type="radio"/> desactivar

Como coincide con la de la lan hemos realizado una reasignación de redes para también así favorecer la sumarización de rutas.

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

```
# Static config for eth0
#auto eth0
#iface eth0 inet static
#    address 192.168.0.2
#    netmask 255.255.255.0
```

```
# DHCP config for eth0
auto eth0
iface eth0 inet dhcp
    hwaddress ether 3e:27:34:3c:24:16
```

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 / 11 KiB	IPv4 *	LAN net	*	LAN_zone	*	*	none		LAN conectivity	<div></div> <div></div> <div></div> <div></div>
<div>Server</div> <div></div>											
<input type="checkbox"/>	✓ 0 / 6 KiB	IPv4 TCP	*	*	Server1	web_ports	*	none			<div></div> <div></div> <div></div> <div></div>
<div>Internet</div> <div></div>											
<input type="checkbox"/>	✓ 0 / 10.54 MiB	IPv4 *	*	*	! 192.168.0.0/16	*	*	none			<div></div> <div></div> <div></div> <div></div>

↑ Add

↓ Add

Delete

Save

+ Separator