

1x Router: CISCO C8200L-1N-4T



1x FW: pfSense-CE-2.7.2



1x Router: CISCO 7200
12.4(24)T5



1x Switch: CISCO IOS-XE
15.4.1T - IOU L3



2x PCs cliente: Debian 12



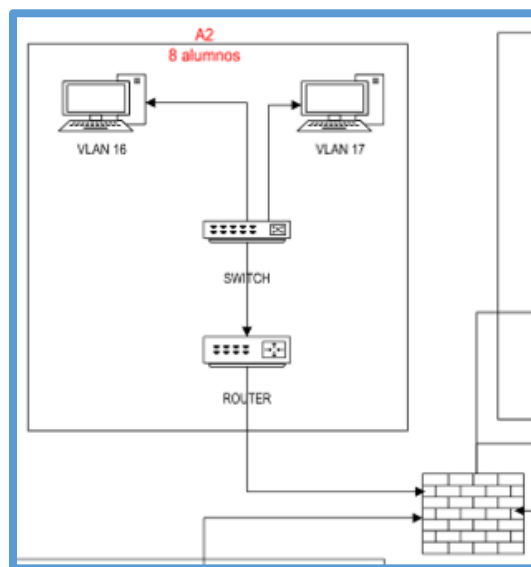
Tabla de Direcccionamiento
realitzada con draw.io



GNS3
Graphical Network Simulator

Entrega -
"ACT 2 – FW"

Tema 1 : Perímetro de la red



Explicar como hacer una configuración básica para crear una red segura con clientes, switch, **FW**, router con VLANs en GNS-3 (Graphical Network Simulator)

Joan Puig, Albert Rodríguez,
1r Curso Grado de Ciber – ENTI-UB

ÍNDIX

1.	INTRODUCCIÓ – ACT 2.1 EN GNS3 & ACT 2.2 EN LAB.....	4
1.1	Act2.2 – Parte 1 -> Router : Cisco modelo C8200L-1N-4T	4
1.2	Act2.2 – Parte 2 -> Switch : Cisco.....	4
1.1	Act2.3 – Parte 3 -> FW : Fortinet	4
1.2	Diagrama de la topología inicial	5
1.3	Configuración básica e incidencias técnicas	5
1.4	Archivos de configuraciones de los dispositivos.....	5
2.	VOCABULARIO	6
2.1	¿Qué es un FW?.....	6
2.2	FW vs NGFW (Next Generation Firewall)	6
2.3	¿Qué es pfSense?	6
2.4	¿Qué es SCP (Secure Copy)?	7
2.5	Aplicación de ACLs : ¿Router o Switch?	7
3.	DIAGRAMA DE TOPOLOGÍA INICIAL – ACT 2.1 & ACT 2.2	7
3.1	Introducción: Implementar configuración inicial y avanzada en la Act.2.1	8
3.1.1	Act.2.1 vs Act.1: la inclusión de un firewall pfSense entre R1 y la nube NAT de GNS3.....	8
3.1.2	Estructura del escenario actual y flujo de tráfico	8
3.1.3	Gestión del firewall y separación de planos	8
3.2	Crear un nuevo “Appliance” de PfSense en GNS3.....	8
3.3	Instalar PfSense en GNS3	9
3.3.1	Pantalla de bienvenida y aceptación de condiciones	10
3.3.2	Selección del modelo de instalación	10
3.3.3	Instalación automática con valores por defecto y ZFS	10
3.3.4	Confirmación de “Proceed with Installation” & Disco sin redundancia (stripe)	11
3.3.5	Selección del disco de destino: vtbd0 (VirtIO Block Device) & Confirmación final	11
3.4	Configurar las 3 tarjetas de red de PFSense (en0: WAN, en1:LAN, en2: OPT1)	12
3.4.1	Identificación de interfaces disponibles.....	12
3.4.2	Asignación de interfaces a WAN, LAN y OPT1	12
	13
3.4.3	Configuración IPv4 de la LAN como enlace de tránsito hacia R1	13
3.4.4	Configuración de OPT1 (em2) mediante DHCP para la red host-only	14
3.4.5	Resultado final y coherencia con la topología.....	15
3.5	Wizard de instalación de PFSense mediante GUI	16
3.5.1	Sección de bienvenida & Información general	16

3.5.2	Time Server Information & Configure WAN Interface	18
3.5.3	Configure LAN interface & Set Admin WebGUI Password & Reload Configuration	19
3.6	Quitar el protocolo NAT de R1	20
3.6.1	Ejecución del script “1_R1_Remove_NAT” y verificación del estado de enrutamiento	20
3.6.2	Definición del gateway de tránsito hacia R1 en pfSense	21
3.6.3	Preparación de rutas estáticas en pfSense hacia VLAN 10 y VLAN 11	21
3.6.4	Creación de la ruta estática hacia la red de la VLAN 10 & VLAN 11	22
3.6.5	Ambas rutas estáticas definidas y configuración lista para operar sin NAT en R1.....	23
3.7	Verificación del estado de NAT de salida en pfSense	24
3.7.1	Estado inicial del cortafuegos en la interfaz LAN.....	25
3.7.2	Alta de la normativa para permitir salida a Internet desde VLAN 10	25
3.7.3	Resultado final tras añadir las reglas de VLAN 10 y VLAN 11.....	26
3.8	Verificar que los clientes Debian tienen acceso a Internet a través de PFSENSE.....	27
3.8.1	Comprobación de conectividad desde R1 hacia pfSense y hacia Internet	27
3.8.2	Renovación de DHCP en el cliente de VLAN 10 y verificación de direccionamiento.....	27
3.8.3	Prueba de salida a Internet desde el cliente de VLAN 10 por IP y por nombre	28
3.9	Permitir acceder a la interfaz web de PFSENSE sin tener que desactivar el firewall	28
3.9.1	Creación de la regla de acceso al WebGUI por HTTPS.....	29
3.10	Permitir acceder por SSH a PfSense solo a través de 192.168.10.21 /24	30
3.10.1	Activación del servicio SSH en pfSense	30
3.10.2	Creación de la regla LAN que permite SSH únicamente desde 192.168.10.21.....	31
3.11	Desactivar normativa “Anti-lockout”	33
3.11.1	Acceso a la configuración avanzada de administración.....	33
3.11.2	Revisión del conjunto de normativas en LAN tras el cambio	33
3.11.3	Sustitución de permisos genéricos por reglas explícitas ICMP y UDP	34
3.11.4	Validación desde cliente autorizado: conectividad e inicio de sesión por SSH.....	34
3.11.5	Confirmación en pfSense: estado de sesión SSH establecido && No establecido.....	35
4.	LOGGING Y MONITOREO BÁSICO	35
4.1	Revisión de eventos en los logs del firewall	35
4.2	Monitorización rápida de actividad con el Traffic Graph	36
4.3	Correlación de estados con pfTop	37
5.	EXTRAS: MANUAL OUTBOUND NAT & DNS ENFORCEMENT	38
5.1	¿Qué es el Manual Outbound NAT?	38
5.2	¿Qué es el DNS Enforcement?	38
5.3	Activar Manual OutBound NAT	38
5.3.1	Borrar normativas NAT creadas automáticamente	39
5.4	Evitar bypass de DNS (DNS enforcement)	40
5.4.1	Activar “DNS Resolver” y justificación de interfaces de red	41
5.4.2	Cambiamos el DNS por defecto a los clientes	41
5.4.3	Creación del alias de redes internas (VLAN 10 y VLAN 11)	42
5.4.4	DNS Enforcement mediante NAT Port Forward interno.....	43

5.4.1	Control de acceso al DNS Resolver con Access Lists por VLAN	45
5.4.2	Prueba desde el cliente (forzando DNS externo y DNS corporativo)	46
5.4.3	Evidencia en pfSense: confirmación del DNS realmente utilizado	47
5.4.4	Normativas en Firewall LAN que permiten el control y justifican el diseño	47
5.4.4.1	1ra normativa: DNS Whitelist	47
5.4.4.2	2nda normativa: SSH administración -> Solo 192.168.10.21/24	48
5.4.4.1	3ra normativa: Excepción: R1 permitir ICMP desde R1 (10.0.0.2) hacia Internet	48
5.4.4.1	4ta normativa: Diagnóstico: R1: Permitir ICMP desde VLAN10 y 11 hacia Internet	48
5.4.4.2	5na normativa: DNS Hijacking: forzar DNS a 10.0.0.1	48

1. Introducción – Act 2.1 en GNS3 & Act 2.2 en LAB

¡IMPORTANTE! Se debe realizar el escenario de la ficha “ACT1 – VLAN” antes de realizar los dos escenarios que narraremos a continuación (ACT2 - FW).

En la Act 2.1, presentaremos como realizar un conjunto de configuraciones básicas para crear una red segura muy simple. De hecho, bastará solo con añadir 5 máquinas virtuales a nuestro escenario de GNS3 junto a los siguientes dispositivos con sus modelos e imágenes.

Dispositivo	Modelo	Imagen IOS
1x Firewall	pfSENSE-2.7.2	pfSense-CE-2.7.2
1x Router	Cisco 7200 124-24.T5	c7200-adventerprisek9-mz.124-24.T5.image
1x Switch	Cisco IOU Switch L2	i86bi-linux-l2-adventerprisek9-15.2d.bin
2x Cliente Debian 12.6	Debian 12.6	debian.gns3a

En cambio, en la actividad 2.2: procederemos en el laboratorio de ENTI a utilizar hardware físico real para montar un nuevo escenario de red. Para ello, tendremos a disposición un PC cliente con Kali Linux que podrá acceder a Internet a través de un router de Cisco modelo C8200L-1N-4T.

Dispositivo	Modelo
1x PC	Kali Linux
1x Router (1ra parte)	Cisco C8200L-1N-4T
1x Switch (2na parte)	Cisco
1x FW (3ra parte)	Fortinet

1.1 Act2.2 – Parte 1 -> Router : Cisco modelo C8200L-1N-4T

De este modo, en el router activaremos el servicio d'SSH (TCP/22), el servicio de DHCP para que pueda recibir una IP automática a través del servidor DHCP de la universidad (IP de red: 192.168.223.0/24), ACLs (Access Control List) para habilitar el protocolo NAT (para permitir acceder a Internet al PC cliente), el servicio web HTTPS de CISCO para monitorizar el dispositivo a través del front-end de nuestro navegador web, y finalmente: activamos el protocolo SCP (Secure Copy Protocol) para poder transferir ficheros entre el router y nuestro cliente Kali Linux.

1.2 Act2.2 – Parte 2 -> Switch : Cisco

Una vez nuestro router Cisco nos brinde acceso a Internet a través de nuestro PC de Kali Linux: conectaremos un Switch entre estos dos dispositivos para implementar una VLAN. De este modo, aprenderemos a través de un escenario con Hardware real como actúa esta segmentación lógica.

1.1 Act2.3 – Parte 3 -> FW : Fortinet

Activadas las VLANs a través del Switch, conectaremos a este dispositivo un FW de Fortinet para activar reglas básicas de filtrado (normas de Inbound = Entrada & Outbound = Salida) e implementación de políticas de seguridad (Ej. denegar acceso al entorno web y al protocolo SSH del router de Cisco a través de WAN para que solo LAN pueda, permitir que solo desde la DMZ y LAN se pueda usar SCP).

Finalmente, se mencionaran capturas de pantalla de los logs producidos tanto en el router, switch y firewall donde constan en acta de acciones permitidas (Allowed) y denegadas (Denied).

1.2 Diagrama de la topología inicial

Seguidamente, procederemos a crear con draw.io un diagrama de la topología de red junto a su plan de direccionamiento. En este, se reflejarán según su escenario cada una de las credenciales de red que irán asignadas a cada una de las tarjetas de red de cada dispositivo.

Por ejemplo, se explicará cada una de las VLANs que debemos crear (VLAN 10 y 11) juntos a sus credenciales de red (ID y Nombre de la VLAN, IP de la red, Subnet Mask, Gateway y Broadcast), además del rango de direccionamiento de la DHCP Pool de cada VLAN, etc.

Pero sobre todo, en el diagrama quedara claro el flujo de red que hay entre los dispositivos para entender con mayor exactitud el escenario a montar luego en GNS3.

1.3 Configuración básica e incidencias técnicas

Además, redactaremos paso por paso de principio a fin como llevar a cabo cada una de las configuraciones necesarias en los dispositivos de GNS3 (Act2.1) y los del LAB (2.2). Esto incluye obviamente narrar como hemos conseguido que los clientes tengan acceso a Internet a través del FW de PFSENSE (Act 2.1), y como lo hemos conseguido también con un Switch y un Forti (2.2) en el LAB.

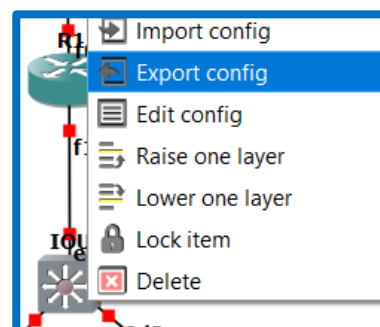
Después, nos aseguraremos de añadir medidas de seguridad en el Switch como VLANs, Port Security (permitir solo una dirección MAC en ese puerto) y el DHCP Snooping (evitar servidores DHCP falsos), además de las ACL en el router, y las medidas de seguridad aplicadas al FW para regular el acceso al SSH solo a la VLAN10, y que solo se acceda al portal web de PFsense a través de 192.168.56.0/24.

Cabe resaltar, que también redactaremos todas aquellas configuraciones que no hemos podido llevar a cabo con éxito, como (redactar de la parte 2 y parte 3 todo)

1.4 Archivos de configuraciones de los dispositivos

Finalmente, subiremos a la entrega de esta tarea este documento en formato PDF, el proyecto GNS3 en modo portable (extensión “.gns3”) y los ficheros de configuración del router y switch CISCO.

Para ello, iremos a uno de estos dispositivos (exceptuando los clientes) y haremos click derecho > Export Config > Guardar.



2. Vocabulario

A continuación, definiremos un conjunto de vocabulario básico esencial para entender con mayor profundidad el escenario de red que montaremos en GNS3.

2.1 ¿Qué es un FW?

Un firewall es un sistema de seguridad que monitoriza, controla y filtra el tráfico de red que entra (Inbound) y sale (Outbound) entre una red interna (LAN) y una red externa (Internet) para definir si las peticiones que posee ese tráfico quedan denegadas (Denied) o permitidas (Allowed).

Un firewall puede existir como dispositivo de hardware (Ej. Cisco, Palo Alto, Checkpoint, Fortinet) o de software (Ej. PFsense, IPtables, Windows Firewall, etc) e incluso integrar reglas de filtrado en un router (ACL = Access Control List) para tomar decisiones basadas en reglas (Ej. Permitir HTTP/HTTPS hacia Internet, bloquear accesos entrantes no solicitados, filtrar la comunicación entre los clientes, etc).

2.2 FW vs NGFW (Next Generation Firewall)

Un firewall “clásico” suele centrarse en filtrar tráfico basándose en criterios de red más tradicionales: direcciones IP, puertos, protocolos y, en muchos casos, el estado de la conexión (stateful).

Esto es útil y sigue siendo necesario. Sin embargo, hoy en día las funcionalidades de un dispositivo como el FW aumentan, y es por eso: que actualmente se queda corto cuando queremos controlar aplicaciones modernas, o amenazas que viajan dentro de tráfico permitido.

Para ello, un NGFW (Next Generation Firewall) amplía ese enfoque. Además de todo lo anterior, incorpora inspección más profunda y funciones avanzadas como identificación de aplicaciones (no solo por puertos), filtrado por usuario/identidad en algunos entornos, análisis de contenido, integración con sistemas de detección y prevención (IDS/IPS), y capacidades para aplicar políticas más “inteligentes” frente a amenazas actuales.

Dicho de forma directa: ambos filtran, pero el NGFW entiende mejor qué está pasando dentro del tráfico y puede tomar decisiones más profundas y certeras al poder trabajar de la capa 2 a la 7, mientras que el FW tradicional trabaja de capa 3 a la 4.

2.3 ¿Qué es pfSense?

pfSense es una plataforma de firewall y router basada en FreeBSD, muy utilizada en laboratorios y también en entornos reales. De hecho, se instala como sistema operativo en un PC o máquina virtual y ofrece una interfaz web para configurar servicios típicos de red: reglas de firewall, NAT, DHCP, DNS, VPN (como IPsec u OpenVPN), VLANs y monitorización.

Por eso mismo, su valor didáctico es alto porque permite montar escenarios completos de seguridad y enrutamiento sin depender de hardware propietario. De este modo, PFsense puede actuar como firewall perimetral con funciones avanzadas si el hardware lo soporta.

2.4 ¿Qué es SCP (Secure Copy)?

SCP (Secure Copy) es un protocolo de red basado en el protocolo SSH (encriptación Diffie-Hellman) que permite copiar archivos entre dos equipos de forma segura.. De este modo, su transferencia de ficheros (Ej. configuraciones, backups o imágenes) viajan bajo un túnel cifrado y autenticado con el objetivo que se puedan interceptar o modificar en tránsito.

En un laboratorio con routers Cisco, el comando **ip scp server enable** permite que desde un cliente como Kali Linux: podamos subir o bajar ficheros del router con comandos **scp** siempre y cuando nos autenticamos con el usuario y contraseña permitido para el dispositivo receptor.

2.5 Aplicación de ACLs : ¿Router o Switch?

Las ACL se aplican preferentemente en dispositivos de capa 3 al poder estos filtrar tráfico por IP, protocolos y puertos (capa 3/4). Por eso, en un escenario clásico se colocan en el router, ya que es el equipo que enruta entre redes y controla el acceso cuando el tráfico pasa de una red a otra.

No obstante, las ACL también son compatibles en switches, especialmente en switches multicapa (L3) para aplicar interfaces VLAN (SVI = Switched Virtual Interface) o en puertos enrutados (Port Forwarding). De hecho, puede ser incluso mejor aplicarlas en el switch L3 cuando este realiza el enrutamiento inter-VLAN, o cuando se quiera bloquear el tráfico lo antes posible (cerca del origen) para mejorar el rendimiento y la segmentación interna.

Sin embargo, en un switch de capa 2 se limita a conmutar por MAC dentro de la VLAN y no es el punto natural para políticas entre redes.

Como norma general, el filtrado debe colocarse donde se produce el cambio de red (punto de enrutamiento) y siguiendo buenas prácticas como mínimo privilegio, denegar por defecto y segmentación por VLAN/zonas, dejando al firewall el control del perímetro y políticas avanzadas

3. Diagrama de topología inicial – Act 2.1 & Act 2.2

Si queremos acceder al diagrama de la topología inicial de las dos actividades, hacemos click encima de la URL de la topología de red que queramos visitar.

ACT 2.1:

<https://drive.google.com/file/d/1EWtqjvkYynzZX3Q9x9eZGoF1wKxCtHWQ/view?usp=sharing>

ACT 2.2:

<https://drive.google.com/file/d/17LD131 - xeeBpQVvOkq6WbProJHFD3i/view?usp=sharing>

3.1 Introducció: Implementar configuració inicial y avanzada en la Act.2.1

Teniendo como base el escenario de la Act.1, en la Act2.1 mantendremos la segmentación por VLAN 10 ('Cliente A' Debian) y VLAN 11 ('Cliente B' Debian) gracias al enlace trunk 802.1Q entre switch y nuestro 'router-on-a-stick'. Además, la asignación dinámica de IPs mediante DHCP desde R1 nos seguirá brindando IPs a los clientes Debian a parte de un gateway y DNS de forma automática.

Es decir, a nivel funcional: la red interna continúa organizada en 192.168.10.0/24 (VLAN 10) y 192.168.11.0/24 (VLAN 11), siendo R1 el gateway de cada VLAN mediante subinterfaces.

3.1.1 Act.2.1 vs Act.1: la inclusión de un firewall pfSense entre R1 y la nube NAT de GNS3

En la Act.1, la salida a Internet y la traducción NAT/PAT se resolvían directamente desde el router de R1. En cambio, en la Act.2.1 el perímetro pasa a externalizarse a través de un FW de pfSense ubicado entre el Router R1 y la nube NAT de GNS3, ya que de este modo: nuestro pfSense brindará a nuestros clientes acceso hacia el exterior (Internet) gracias a la resolución de direcciones IP mediante el protocolo NAT/PAT. En cambio, el router de R1 queda centrado exclusivamente en el enrutamiento interno y los servicios de LAN (VLANs y DHCP). Por lo tanto, se deberá desactivar el protocolo de NAT en este dispositivo de enrutamiento para no interferir con nuestro firewall.

3.1.2 Estructura del escenario actual y flujo de tráfico

El tráfico de usuario para que un cliente pueda acceder a Internet empieza a través de las VLANs (e0/0) configuradas en el Switch (VLAN 10 o 11). Luego, el router enruta entre VLAN 10 y VLAN 11 (fa0/0) para reenviar el tráfico de la LAN hacia pfSense (fa0/1 -> em1) a través de un enlace de tránsito punto a punto (IP de red 10.0.0.0/30).

A continuación, pfSense conecta su WAN (em0) al NAT1 de GNS3 (nat0) dentro de 192.168.122.0/24, utilizando ese salto para proporcionar salida real a Internet mediante NAT/PAT.

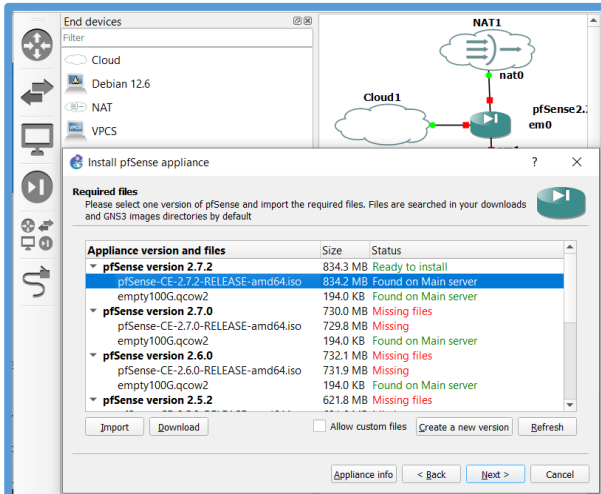
3.1.3 Gestión del firewall y separación de planos

Para administrar pfSense sin depender de la WAN ni interferir con el tráfico de datos, se incorpora una red de gestión independiente mediante una interfaz host-only (em2) en 192.168.56.0/24 para acceder al portal web de PfSense. De este modo, toda el plano de datos queda dedicado a la conectividad de usuarios y salida a Internet, y así: nuestro plano de gestión queda completamente aislado para poder así acceder a la versión web del Firewall sin interferir en el flujo de datos entre los clientes e Internet.

3.2 Crear un nuevo "Appliance" de PfSense en GNS3

Empezaremos por añadir un nuevo dispositivo a nuestro escenario llamado "PfSense-Ce-2.7.2". Para ello, nos iremos al apartado de "End Devices" y pulsaremos en "New Template". Luego, mencionaremos que la plantilla es para nuestro servidor GNS3, y seleccionamos del apartado de "Firewall" la opción de PFSense.

Más adelante, en el apartado de "Required Files", mencionamos que la ISO que vamos a implementar es la versión 2.7.2 al igual que su fichero ".qcow2".



Index of /mirror/downloads/

../old/	06-Jun-2024 19:18
pfSense-CE-2.6.0-RELEASE-amd64.iso.gz	31-Jan-2022 20:31
pfSense-CE-2.6.0-RELEASE-amd64.iso.gz.sha256	31-Jan-2022 20:32
pfSense-CE-2.7.0-RELEASE-amd64.iso.gz	29-Jun-2023 20:11
pfSense-CE-2.7.0-RELEASE-amd64.iso.gz.sha256	29-Jun-2023 20:11
pfSense-CE-2.7.1-RELEASE-amd64.iso.gz	17-Nov-2023 00:47
pfSense-CE-2.7.1-RELEASE-amd64.iso.gz.sha256	17-Nov-2023 00:47
pfSense-CE-2.7.2-RELEASE-amd64.iso.gz	08-Dec-2023 18:27
pfSense-CE-2.7.2-RELEASE-amd64.iso.gz.sha256	08-Dec-2023 18:27

Descarga de la ISO de PFSENSE:

<https://atxfiles.netgate.com/mirror/downloads/>

Descarga directa de la ISO de PFSENSE:

<https://atxfiles.netgate.com/mirror/downloads/pfSense-CE-2.7.2-RELEASE-amd64.iso.gz>

Descarga del fichero “.qcow2”

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

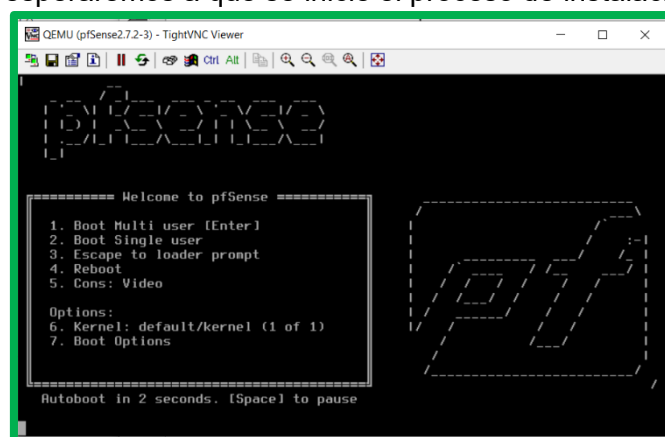
Una vez hechos estos pasos, podremos observar que podemos arrastrar a nuestro escenario un “appliance” llamado “pfSENSE 2.7.2”, que este: lo ubicaremos entre R1 y la nube de NAT de GNS3.

3.3 Instalar PFsense en GNS3

Una vez creadas y configuradas las máquinas virtuales con cada uno de los apartados nombrados anteriormente, añadiremos la ISO descargada anteriormente a la máquina del PFSENSE y la arrancaremos.

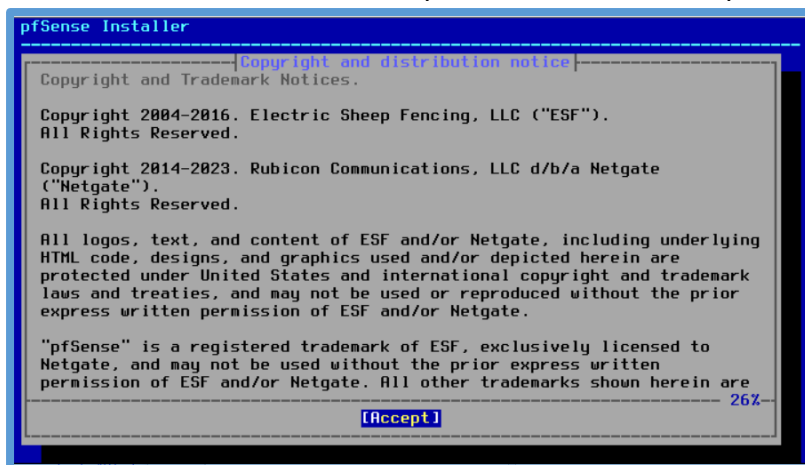
Una vez iniciada la máquina, si el contenido de la ISO ha sido leído correctamente, debería aparecer por pantalla el siguiente menú que aparece debajo.

De hecho, con una captura del menú podemos conocer PFSENSE de forma más detallada. Sin embargo, de momento esperaremos a que se inicie el proceso de instalación automáticamente.



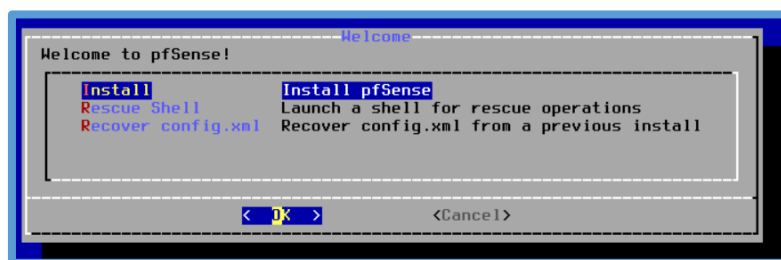
3.3.1 Pantalla de bienvenida y aceptación de condiciones

A continuación, nos aparecerá el mensaje de bienvenida a PFSense. Pasamos al siguiente paso, clicando la tecla “Intro/Enter” de nuestro teclado para accionar en “Accept”.



3.3.2 Selección del modelo de instalación

Seguidamente seleccionamos la opción “Install”, que inicia el asistente de instalación del sistema en el disco. Con esta elección, indicamos que el objetivo es desplegar pfSense como sistema operativo instalado (no únicamente como entorno live).



3.3.3 Instalación automática con valores por defecto y ZFS

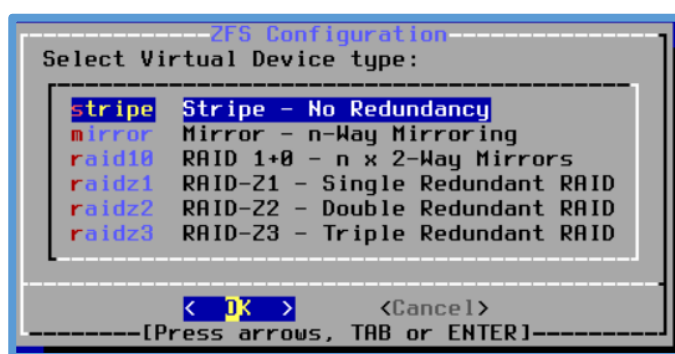
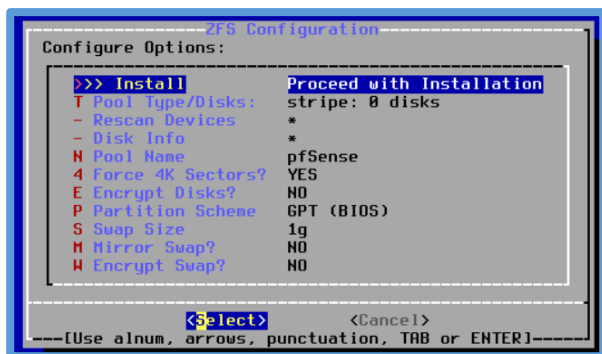
En el siguiente paso optamos por realizar una instalación con valores por defecto y de forma automática, lo que implica que el instalador organizará el disco sin necesidad de definir particiones manualmente. Para ello, escogemos “Auto (ZFS)”, de manera que pfSense utilice ZFS como sistema de ficheros y automatice la creación de la estructura necesaria sobre el disco.



3.3.4 Confirmación de “Proceed with Installation” & Disco sin redundancia (stripe)

Seguidamente, escogeremos la opción “Install” para proceder con la instalación de PFsense (Proceed with Installation). De hecho, en esta pantalla se fija la lógica general del almacenamiento donde se va a crear un pool ZFS llamado ‘pfSense’ con el esquema de particionado GPT (BIOS) con un tamaño de swap de 1 GB. Dicho de otra manera, escogeremos crear un tipo de pool equivalente a “un solo disco”.

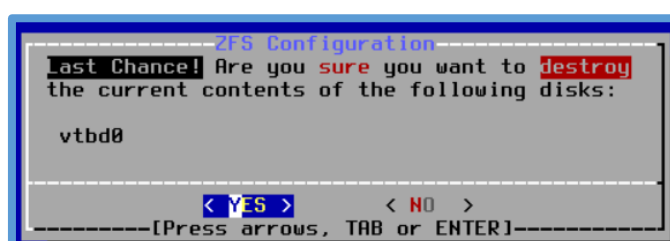
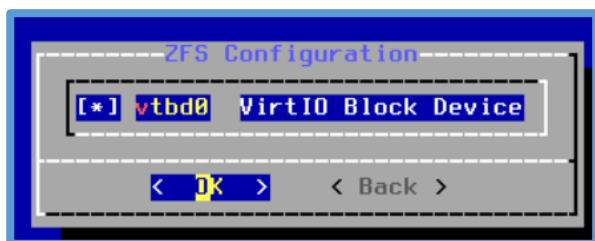
Posteriormente, en la pantalla “Select Virtual Device type” seleccionamos **stripe**. A nivel técnico, esto significa que el pool ZFS se construye sin espejo ni paridad: no hay tolerancia a fallos de disco, porque el objetivo es simplicidad y rapidez en entorno virtual. En un escenario real con varios discos, aquí podríamos escoger mirror o RAIDZ, pero en GNS3/VM usamos stripe al tener solo un disco.



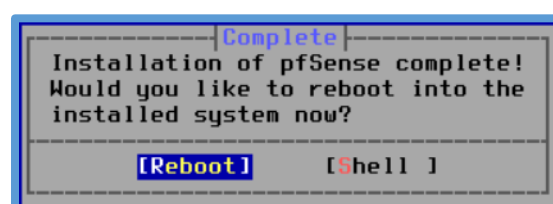
3.3.5 Selección del disco de destino: vtbd0 (VirtIO Block Device) & Confirmación final

Después, el instalador muestra el dispositivo virtual detectado como **vtbd0**, identificado como **VirtIO Block Device**. Esta parte es clave porque confirma dos cosas: que el sistema ha reconocido correctamente el almacenamiento virtual y que el backend es VirtIO (habitual en QEMU/KVM). Luego, marcamos vtbd0 como disco destino y confirmamos con “OK”.

Finalmente, antes de escribir nada, el instalador lanza una advertencia explícita: “Last Chance! Are you sure you want to destroy the current contents...”. Aquí validamos que el disco seleccionado es el correcto (vtbd0) y aceptamos con **YES**. Técnicamente, esto autoriza al instalador a sobrescribir la tabla de particiones y crear desde cero el esquema GPT, el pool ZFS y los datasets necesarios para pfSense. Cabe resaltar, que esta confirmación es el último punto de control para evitar borrar un disco equivocado, especialmente importante cuando hay más de una unidad conectada.



Entonces, una vez finalizada la instalación de PFsense, marcamos la opción de “Reboot” para reiniciar el SO y poder por fin empezar a usar PFsense en nuestro dispositivo (FW) de GNS3.



3.4 Configurar las 3 tarjetas de red de PFSense (en0: WAN, en1: LAN, en2: OPT1)

Como podremos observar, a pesar de tener 3 tarjetas de red conectadas a nuestro PFSense, solo dos interfaces están activas como WAN (en0) y como LAN (en1). Sin embargo, podremos levantar la 3ra tarjeta de red y asignar una IP si seguimos los siguientes pasos.

```
FreeBSD/amd64 (pfSense.home.arpa) (ttyv0)
QEMU Guest - Netgate Device ID: cae68cfbde2da6db651e

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.122.215/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24

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

3.4.1 Identificación de interfaces disponibles

En la consola de pfSense, al acceder a la opción de asignación de interfaces (1 = Assign interfaces), el sistema muestra el listado de interfaces de red detectadas (em0, em1, em2, etc.) junto con su estado (up/down). Es importante entender que en entornos virtualizados como GNS3: una interfaz puede aparecer como “down” aunque este realmente conectada al dispositivo. Lo mas probable, es que en el S.O que estemos usando nos exija levantar esa interfaz de red manualmente para así poder usarla.

3.4.2 Asignación de interfaces a WAN, LAN y OPT1

A continuación, cuando el asistente pregunta si es necesario configurar VLANs antes (“Do VLANs need to be set up first?”), se responde “n” para negar esta configuración, ya que cabe resaltar: que en esta topología no es necesario crear VLANs en pfSense al tener la segmentación de VLAN 10 (Fa0/0.10) y VLAN 11 (Fa0/0.11) en R1 mediante las subinterfaces de Fa0/0).

A continuación se asigna WAN a em0, LAN a em1 y OPT1 a em2 para que la conexión “Host-Only Adapter” nos brinde conectividad al portal web de PFSense a través de nuestro PC local.

Con esto, pfSense queda estructurado con un interfaz de salida hacia Internet (WAN), un interfaz de tránsito interno (LAN), y un tercer interfaz (OPT 1) adicional reservado para administración.

```
Enter an option: 1

Valid interfaces are:

em0      0c:83:ac:04:00:00 (up) Intel(R) Legacy PRO/1000 MT 82540EM
em1      0c:83:ac:04:00:01 (down) Intel(R) Legacy PRO/1000 MT 82540EM
em2      0c:83:ac:04:00:02 (down) Intel(R) Legacy PRO/1000 MT 82540EM
em3      0c:83:ac:04:00:03 (down) Intel(R) Legacy PRO/1000 MT 82540EM
em4      0c:83:ac:04:00:04 (down) Intel(R) Legacy PRO/1000 MT 82540EM
em5      0c:83:ac:04:00:05 (down) Intel(R) Legacy PRO/1000 MT 82540EM

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 [yn]? n

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
(em0 em1 em2 em3 em4 em5 or a): em0
```

```
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
(em0 em1 em2 em3 em4 em5 or a): em0

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

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

The interfaces will be assigned as follows:

WAN -> em0
LAN -> em1
OPT1 -> em2

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

3.4.3 Configuración IPv4 de la LAN como enlace de tránsito hacia R1

Una vez asignadas las interfaces, se configura la dirección IP de la LAN entrando en “Set interface(s) IP address” (opción 2) y seleccionando la LAN (em1). Luego, se indica que no se desea usar DHCP en la LAN porque la dirección debe ser estática, es decir: 10.0.0.1 con prefijo /30 (255.255.255.252).

Esta máscara la usaremos al tratarse de un enlace punto a punto entre dos equipos, ya que un /30 proporciona exactamente dos direcciones útiles para así delimitar el tráfico. Después, cuando el asistente pregunta por un gateway “upstream” para la LAN: se deja en blanco porque la puerta de enlace por defecto de pfSense debe estar en la WAN y no en una red interna.

Seguidamente, se desactiva “IPv6” al estar usando “IPv4”, y se responde que no se habilite el servidor DHCP en LAN, ya que el DHCP: lo gestiona R1 para las redes de clientes. Finalmente, se mantiene el acceso al webConfigurator en HTTPS, evitando revertir a HTTP.

```
Enter an option: 2

Available interfaces:

1 - WAN (em0 - dhcp)
2 - LAN (em1)
3 - OPT1 (em2)

Enter the number of the interface you wish to configure: 2

Configure IPv4 address LAN interface via DHCP? (y/n) n

Enter the new LAN IPv4 address. Press <ENTER> for none:
> 10.0.0.1

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 LAN IPv4 subnet bit count (1 to 32):
> 255.255.255.252

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 30
```

```
For a WAN, enter the new LAN IPv4 upstream gateway address.  
For a LAN, press <ENTER> for none:  
>  
  
Configure IPv6 address LAN interface via DHCP6? (y/n) n  
  
Enter the new LAN IPv6 address. Press <ENTER> for none:  
>  
  
Do you want to enable the DHCP server on LAN? (y/n) n  
Disabling IPv4 DHCPD...  
Disabling IPv6 DHCPD...  
  
Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n
```

Tras aplicar los cambios, pfSense confirma que la LAN queda configurada como 10.0.0.1/30 y suele indicar que el webConfigurator está disponible en <https://10.0.0.1/>, lo cual sirve como verificación inmediata de que el direccionamiento interno se ha aplicado correctamente.

```
Please wait while the changes are saved to LAN...  
Reloading filter...  
Reloading routing configuration...  
DHCPD...  
  
The IPv4 LAN address has been set to 10.0.0.1/30  
You can now access the webConfigurator by opening the following URL in your web  
browser:  
  
https://10.0.0.1/  
  
Press <ENTER> to continue.
```

```
*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***  
  
WAN (wan)      -> em0      -> v4/DHCP4: 192.168.122.215/24  
LAN (lan)      -> em1      -> v4: 10.0.0.1/30  
OPT1 (opt1)    -> em2      ->  
  
0) Logout (SSH only)          9) pfTop  
1) Assign Interfaces          10) Filter Logs  
2) Set interface(s) IP address 11) Restart webConfigurator  
3) Reset webConfigurator password 12) PHP shell + pfSense tools  
4) Reset to factory defaults    13) Update from console  
5) Reboot system              14) Enable Secure Shell (sshd)  
6) Halt system                15) Restore recent configuration  
7) Ping host                  16) Restart PHP-FPM  
8) Shell  
  
Enter an option: 2
```

3.4.4 Configuración de OPT1 (em2) mediante DHCP para la red host-only

Para configurar la tarjeta de red OPT1 volvemos a seleccionar la opción 2 (Set interface IP address) para añadir credenciales de red a esta tarjeta. Luego, se selecciona la interfaz 3 (OPT1) y se decide que obtenga dirección IPv4 por DHCP, lo cual tiene sentido cuando OPT1 está conectada a una red host-only gestionada por el propio entorno de virtualización (por ejemplo, VirtualBox o GNS3).

A continuación, se desactiva DHCPv6 y no se configura IPv6 manual, manteniendo el escenario centrado en IPv4 para simplificar la práctica. Finalmente, se conserva HTTPS como protocolo del webConfigurator (no se revierte a HTTP), garantizando que la administración web se realiza cifrada. Tras guardar, pfSense confirma que la dirección IPv4 de OPT1 queda establecida por DHCP y sugiere una URL de acceso, lo que en la práctica equivale a acceder por la IP que haya recibido la interfaz en esa red host-only (por ejemplo, 192.168.56.102/24).

```

Enter the number of the interface you wish to configure: 3
Configure IPv4 address OPT1 interface via DHCP? (y/n) y
Configure IPv6 address OPT1 interface via DHCP6? (y/n) n
Enter the new OPT1 IPv6 address. Press <ENTER> for none:
>
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) n

Please wait while the changes are saved to OPT1...
Reloading filter...
Reloading routing configuration...
DHCPD...

The IPv4 OPT1 address has been set to dhcp
You can now access the webConfigurator by opening the following URL in your web
browser:
        https://dhcp/

Press <ENTER> to continue.

```

3.4.5 Resultado final y coherencia con la topología

De este modo, con esta estructura WAN (em0) queda como interfaz de salida a Internet, LAN (em1) funciona como enlace de tránsito hacia R1, y OPT1 (em2) se reserva para la red host-only de administración (por ejemplo 192.168.56.0/24). Esto ofrece como resultado un flujo lógico limpio en el que los clientes de VLAN 10 y VLAN 11 salen hacia R1, R1 reenvía el tráfico hacia pfSense por el enlace 10.0.0.0/30, y pfSense centraliza las políticas de seguridad y el NAT hacia Internet, evitando doble traducción y concentrando el control y la trazabilidad en el firewall.

Nº interficie	Interficie a assignar	IP host	Nom Targeta
1	em0	192.168.122.215/24	WAN
2	em1	10.0.0.1/30	LAN
3	em2	192.168.56.102/24	OPT1

```

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.122.215/24
LAN (lan)      -> em1      -> v4: 10.0.0.1/30
OPT1 (opt1)    -> em2      -> v4/DHCP4: 192.168.56.102/24

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

Enter an option: 8

[2.7.2-RELEASE][root@pfSense.home.arpal]/root: pfctl -d
pf disabled
[2.7.2-RELEASE][root@pfSense.home.arpal]/root:

```

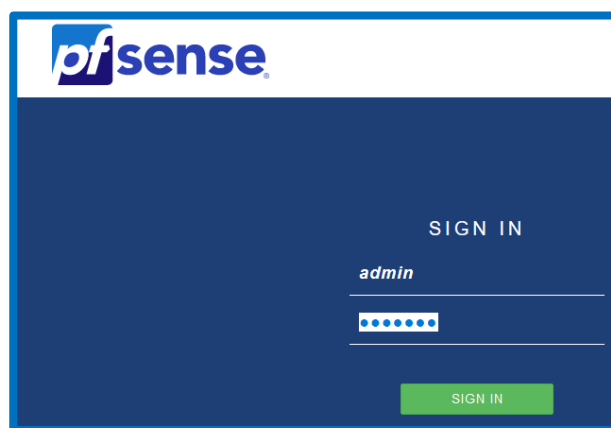
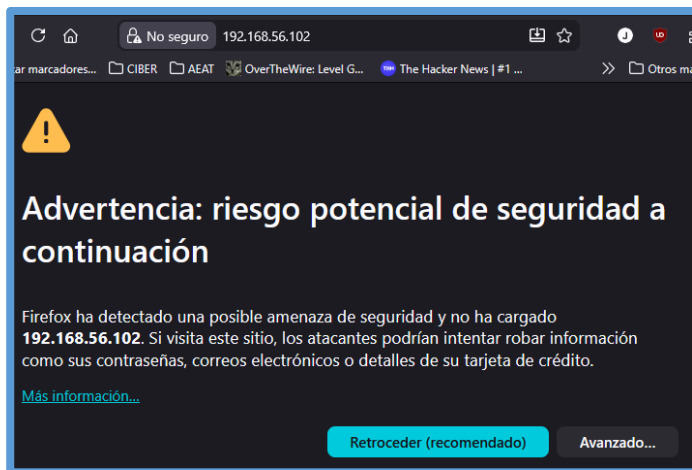
Finalmente, entraremos en al terminal con la opción “8” (Shell) para ejecutar el comando “pfctl -d” para desactivar el FW. Así, accederemos a la interfaz web de PFsense a través de <https://192.168.56.102>

3.5 Wizard de instalación de PFSense mediante GUI

Una vez desactivado el Firewall, podremos observar que si refrescamos la pagina, ya nuestro PC host y la máquina virtual del PFSense se podrán comunicar correctamente.

Lo sabremos, porque Firefox del PC físico, nos preguntará si estamos seguros de acceder a un contenido web donde posee un certificado auto-firmado del servidor que nos queremos conectar.

Aceptaremos la advertencia, pulsando en Avanzado... > Aceptar el riesgo y continuar .

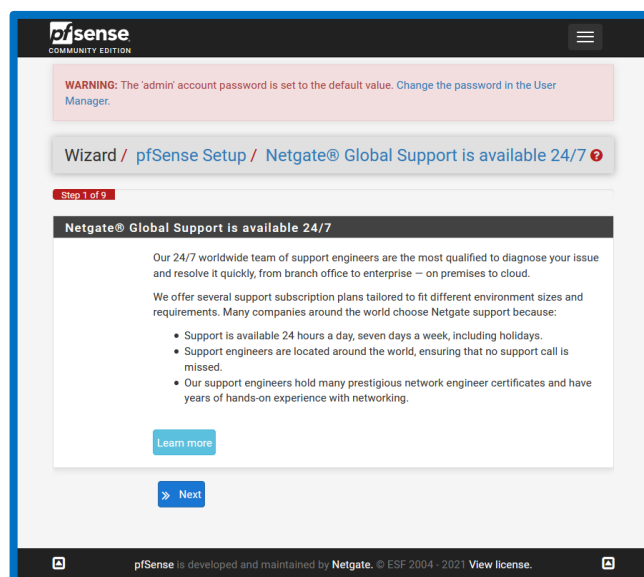
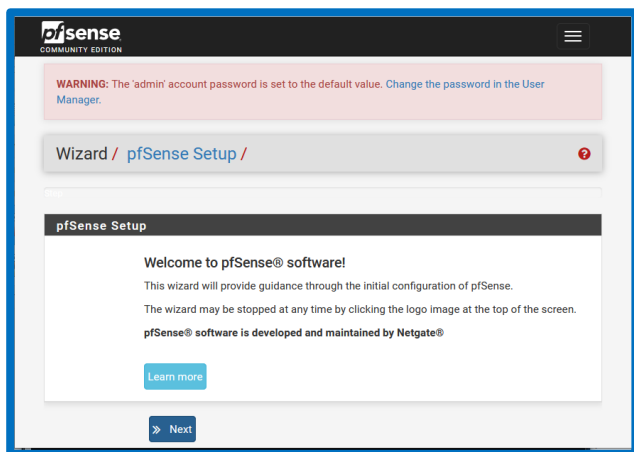


Como podemos ver, la página para validarnos en el PFSense de nuestro MV ya es visible. Ahora, sólo debemos validarnos con el usuario “admin” y con la contraseña “pfsense” para empezar el proceso de configuración de dicho software a través del entorno web.

3.5.1 Sección de bienvenida & Información general

A continuación, procederemos con la configuración de PFSense vía web, donde podremos observar en "Wizard / pfSense Setup" el mensaje de bienvenida.

Pasamos al siguiente paso clicando en “Next”.



Luego, en "Wizard / pfSense Setup / Support 24" nos recuerda que dicha compañía posee un servicio de ayuda a la hora de configurar y administrar este software, mediante el servicio de contratación.

Entonces, en "Wizard / pfSense Setup / General Information" añadiremos un hostname / nombre del equipo para poder identificar dicha máquina del resto de dispositivos que tengamos en nuestra red.

A continuación, añadiremos un SLD (Second-Level Domain) y un TLD (Top Level Domain) para identificar un dominio. En mi caso, he escogido como dominio: puig.rodriguez, para luego añadir como DNS primario (8.8.8.8) y uno de secundario (8.8.4.4).

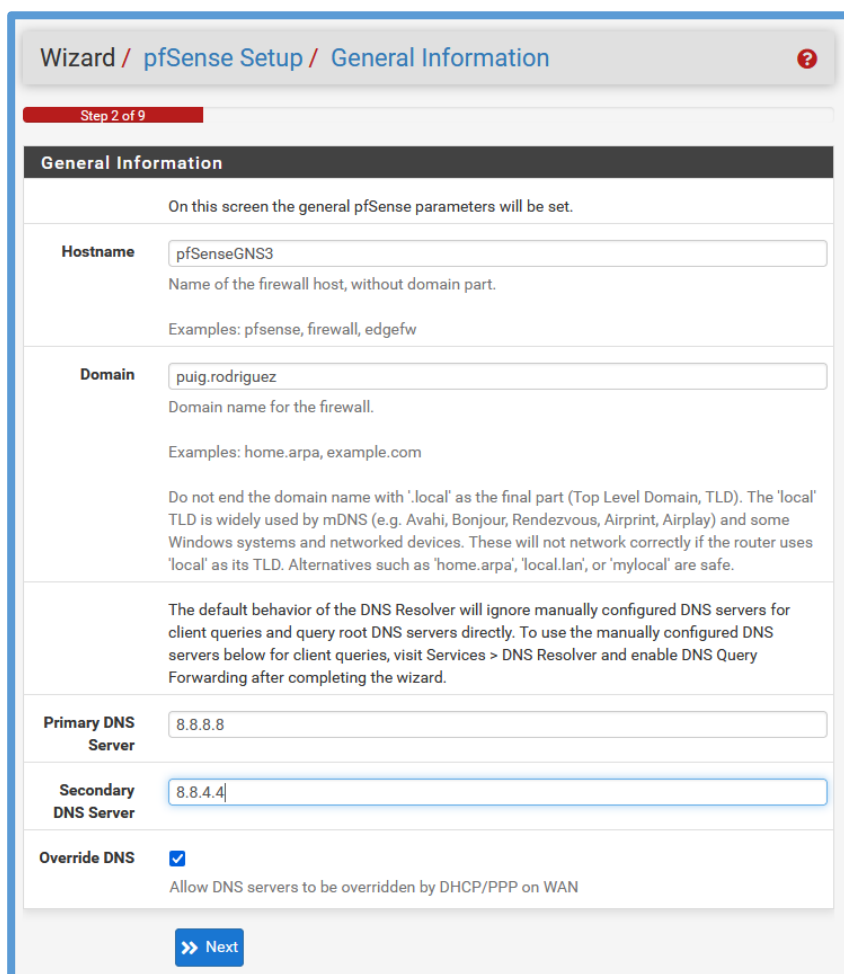
Por último, marcaremos la opción "Override DNS" en el caso de haber escogido dos DNS o bien escogido como DNS primario una IP que no corresponde al DNS de nuestro Router (192.168.1.1).

¡RECUERDA! Override DNS es una función de los Domain Name System que consiste en asignar a nombres de dominio IPs que asignamos nosotros mismos. De esta forma, podemos escoger la ruta completa de resolución de nombres sin la necesidad de utilizar el DNS de nuestro ISP.

Más información

<https://gtmetrix.com/blog/how-to-override-your-dns-with-gtmetrix/>

¡Seguimos! Una vez añadidos los datos anteriores, clicamos en "NEXT".



Wizard / pfSense Setup / General Information

Step 2 of 9

General Information

On this screen the general pfSense parameters will be set.

Hostname
Name of the firewall host, without domain part.
Examples: pfsense, firewall, edgefw

Domain
Domain name for the firewall.
Examples: home.arpa, example.com

Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.

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

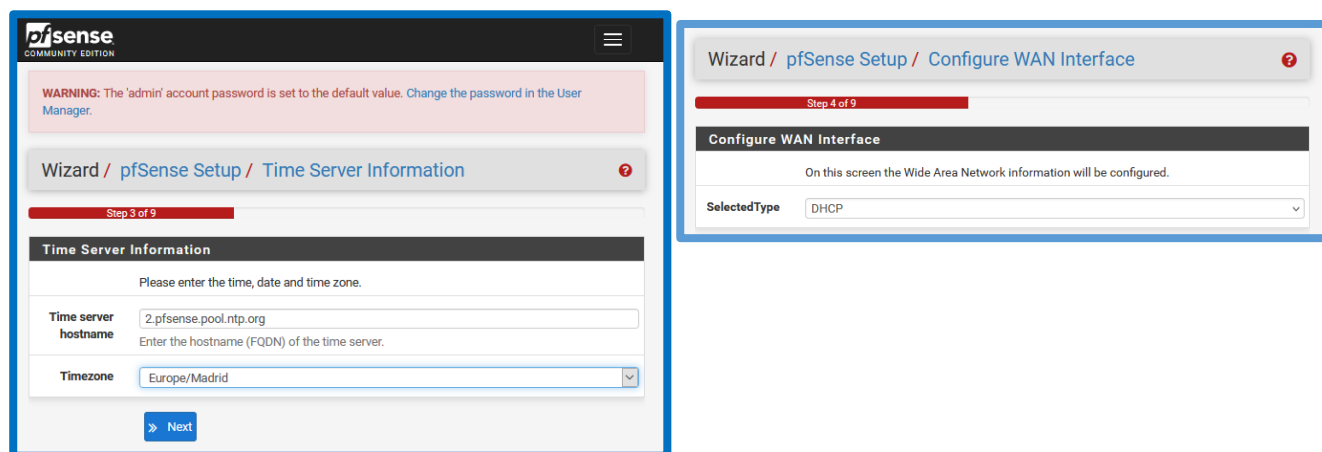
Override DNS ☒
Allow DNS servers to be overridden by DHCP/PPP on WAN

[Next](#)

3.5.2 Time Server Information & Configure WAN Interface

Seguidamente, en “Time Server Information”, dejaremos el hostname por defecto que aparece por pantalla. A continuación, escogeremos la zona horaria de “Europe/Madrid” para tener la hora UTC+1. Por último, clicamos en “Next”.

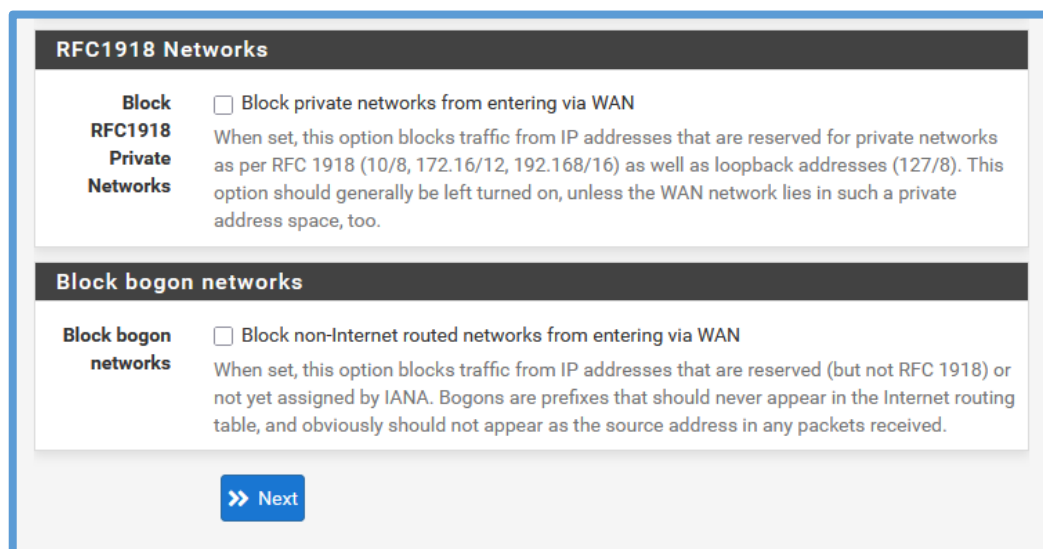
Luego, en “Configure WAN Interface”, escogeremos en “SelectType” > DHCP, para recolectar una IP automática de la nube de GNS3. En este caso, 192.168.122.215 /24.



Después, desmarcaremos las casillas de “Block RFC1918 Private Networks” y “Block bogon networks”, donde la primera opción, si la dejamos marcada, bloqueará todo ese ping que venga de cualquier IP privada que quiera contactar con nuestro PfSense.

Además, la segunda opción, al estar activada, bloqueará todo ese ping procedente de una IP que esté reservada, pero no dentro del RFC 1918, y además, bloqueo de capa 3 de toda aquella dirección de Internet Protocol que no esté dentro de IANA.

Como nosotros no queremos tener complicaciones con el tema de dejar entrar y bloquear paquetes de capa 3 a la hora de gestionar Firewall, desmarcaremos estas dos casillas para obtener un mayor control del cortafuegos. Por último, clicamos en “Next”.

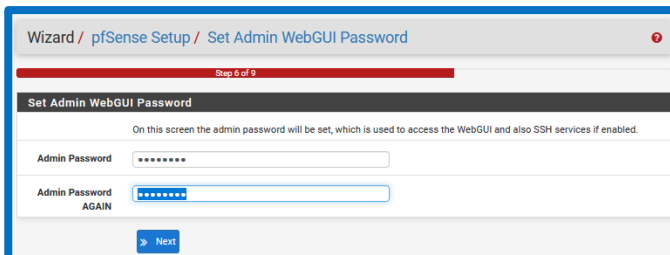
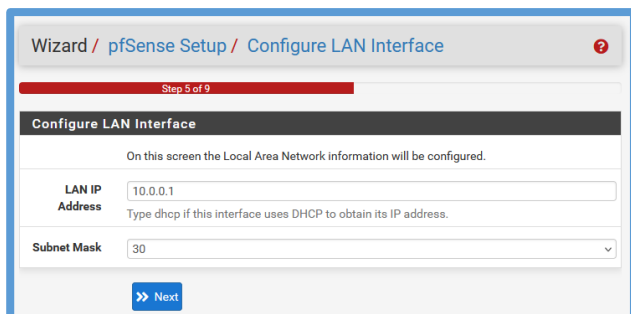


3.5.3 Configure LAN interface & Set Admin WebGUI Password & Reload Configuration

De lo contrario, en “Configure LAN Interface”, especificaremos la IP host manual de nuestra tarjeta LAN, donde podremos añadir dicha dirección a “LAN IP Address”. En nuestro caso, la IP que debemos añadir será la 10.0.0.1 de acuerdo a nuestro esquema.

Por último, la "Subnet Mask" de la dirección de "LAN IP Address" será 255.255.255.252 con /30.

Acabamos esta configuración clicando en “Next”.

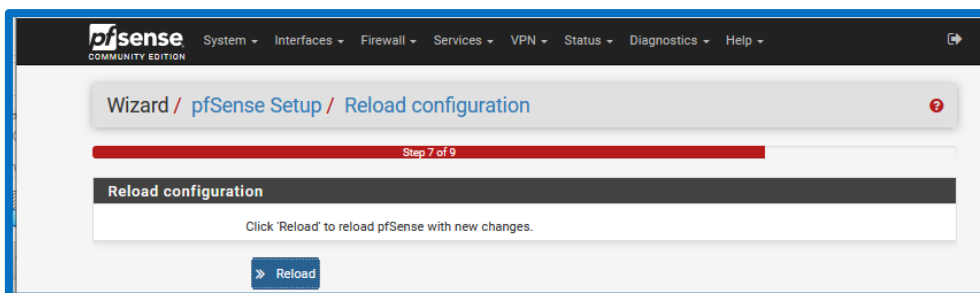


Después, añadiremos una nueva contraseña a nuestro usuario “admin”, donde deberemos añadirla dos veces para asegurarnos que hemos escrito correctamente la contraseña.

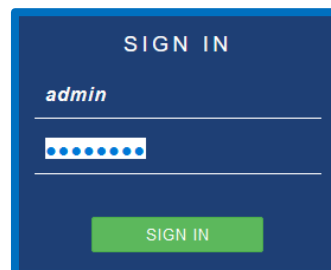
Vamos a la siguiente sección, clicando en “Next”.

Aparte de los pasos anteriores, necesitaremos clicar en el botón “Reload” para acabar de instalar correctamente los datos que hemos añadido anteriormente.

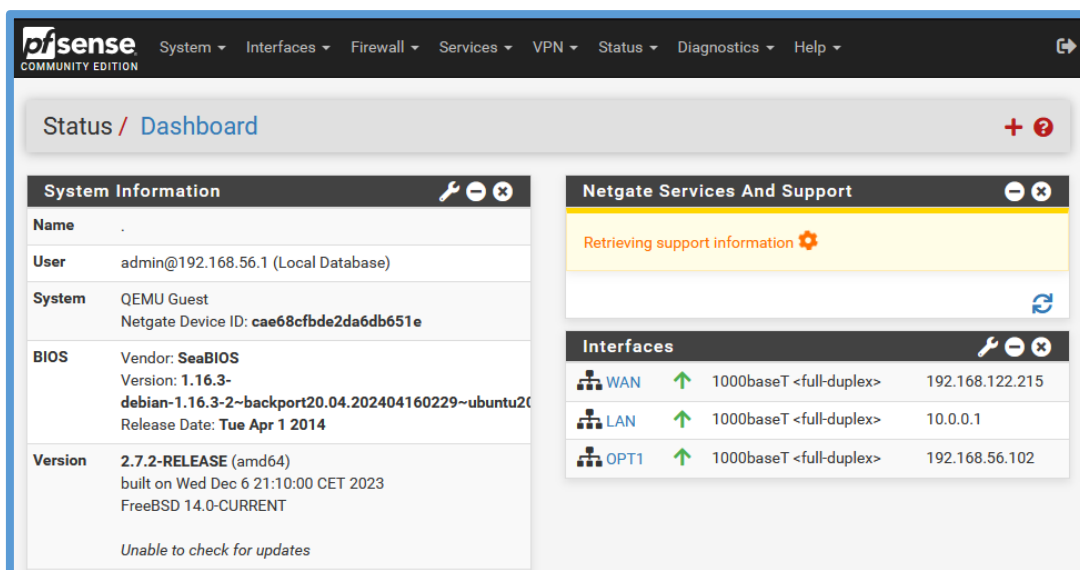
Asimismo, volveremos a la terminal de PFSense, y volveremos a ejecutar el comando “pfctl -d” para desactivar de nuevo el FW. Luego, deberemos esperar a que se recargue la pagina para que Pfsense nos indique que ha terminado de cargar la información anterior correctamente.



```
[2.7.2-RELEASE][root@.]/root: pfctl -d
pf disabled
[2.7.2-RELEASE][root@.]/root: █
```



Como podemos observar, si introducimos de nuevo las nuevas credenciales con nuestro nuevo usuario y contraseña: ya deberíamos poder ver el menú de PFSense donde refleje en la sección “Interfaces” las credenciales de red de nuestras tarjetas (WAN, LAN y OPT1).



3.6 Quitar el protocolo NAT de R1

Al definir que el FW de PFSense va a ser el encargado de usar el protocolo NAT, y así: permitir resolver las direcciones IP de los clientes para poder acceder a Internet, deshabilitaremos entonces el ‘NAT’ que hemos puesto en el router R1 para evitar interferencias.

3.6.1 Ejecución del script “1_R1_Remove_NAT” y verificación del estado de enrutamiento

Tras ejecutar en R1 el script “1_R1_Remove_NAT”, se realiza una comprobación inmediata del estado de las interfaces y de la tabla de rutas para confirmar que el router sigue desempeñando su función de encaminamiento entre VLAN 10, VLAN 11 y el enlace de tránsito hacia pfSense.

Por eso mismo, se observa que R1 mantiene operativas las subinterfaces de VLAN (192.168.10.1 y 192.168.11.1) y el enlace hacia pfSense (10.0.0.2), así como la ruta por defecto apuntando a 10.0.0.1, que es la IP del lado LAN de pfSense en el enlace /30.

```
R1#show ip interface brief
Interface                IP-Address      OK? Method Status      Protocol
FastEthernet0/0          10.0.0.2        YES manual  up           up
FastEthernet1/0          unassigned      YES NVRAM   up           up
FastEthernet1/0.10       192.168.10.1    YES NVRAM   up           up
FastEthernet1/0.11       192.168.11.1    YES NVRAM   up           up
NVI0                      unassigned      YES unset   administratively down down

R1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

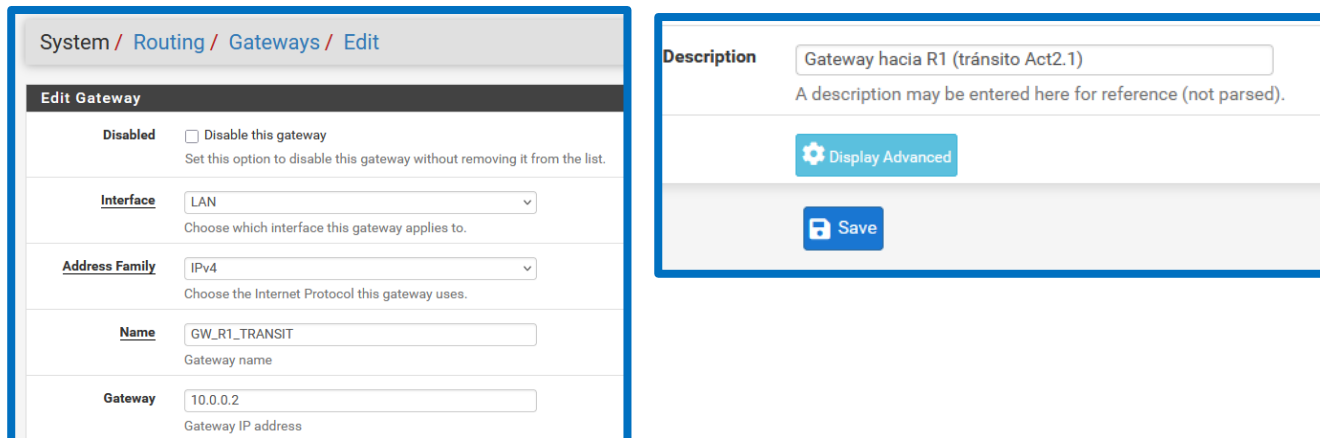
Gateway of last resort is 10.0.0.1 to network 0.0.0.0

C    192.168.10.0/24 is directly connected, FastEthernet1/0.10
C    192.168.11.0/24 is directly connected, FastEthernet1/0.11
     10.0.0.0/30 is subnetted, 1 subnets
C      10.0.0.0 is directly connected, FastEthernet0/0
S*   0.0.0.0/0 [1/0] via 10.0.0.1
R1#
```

3.6.2 Definición del gateway de tránsito hacia R1 en pfSense

Una vez R1 queda funcionando únicamente como router de interconexión interna, el siguiente paso consiste en definir en pfSense un gateway explícito hacia R1 sobre la interfaz LAN (la red de tránsito 10.0.0.0/30). Este gateway permite a pfSense conocer el siguiente salto válido (10.0.0.2) para devolver tráfico hacia las redes de clientes que cuelgan de R1.

Por eso mismo, el gateway “GW_R1_TRANSIT”, se asigna a la interfaz LAN y con dirección de gateway 10.0.0.2, documentado con una descripción para dejar constancia de su función dentro del escenario.



System / Routing / Gateways / Edit

Edit Gateway

Disabled ☐ Disable this gateway
Set this option to disable this gateway without removing it from the list.

Interface LAN
Choose which interface this gateway applies to.

Address Family IPv4
Choose the Internet Protocol this gateway uses.

Name GW_R1_TRANSIT
Gateway name

Gateway 10.0.0.2
Gateway IP address

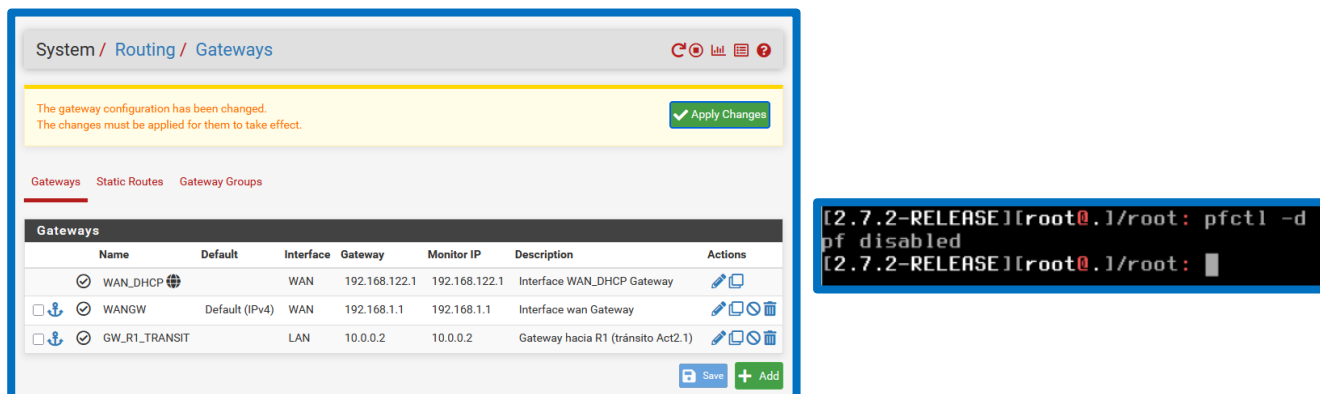
Description Gateway hacia R1 (tránsito Act2.1)
A description may be entered here for reference (not parsed).

[Display Advanced](#)

[Save](#)

Después de guardar el gateway, pfSense notifica que existe una modificación pendiente de aplicar. Este paso es importante porque, hasta que se aplican los cambios, el gateway puede aparecer en la lista pero no quedar operativo en el sistema de enrutamiento. Por eso mismo, el gateway “GW_R1_TRANSIT” ya está presente en el listado de gateways.

Finalmente, al haber aplicado un cambio de configuración de red en PFSENSE, desactivaremos de nuevo el Firewall para poder volver acceder la interfaz web.



System / Routing / Gateways

The gateway configuration has been changed.
The changes must be applied for them to take effect. [Apply Changes](#)

[Gateways](#) [Static Routes](#) [Gateway Groups](#)

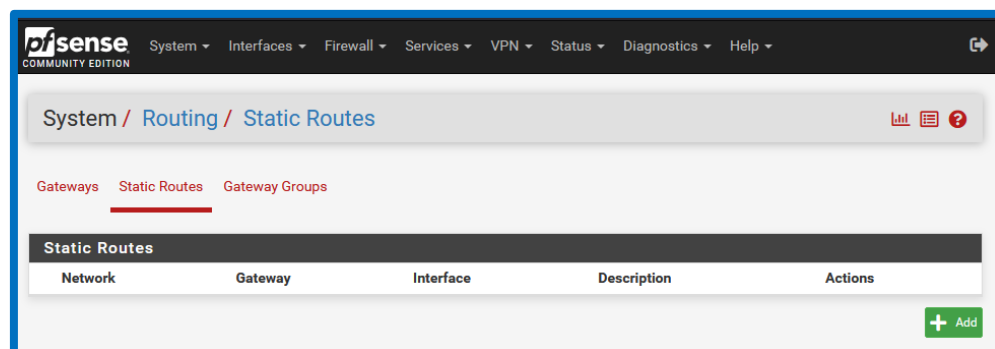
Name	Default	Interface	Gateway	Monitor IP	Description	Actions
<input checked="" type="checkbox"/> WAN_DHCP		WAN	192.168.122.1	192.168.122.1	Interface WAN_DHCP Gateway	Edit Delete
<input checked="" type="checkbox"/> WANGW	Default (IPv4)	WAN	192.168.1.1	192.168.1.1	Interface wan Gateway	Edit Delete
<input checked="" type="checkbox"/> GW_R1_TRANSIT		LAN	10.0.0.2	10.0.0.2	Gateway hacia R1 (tránsito Act2.1)	Edit Delete

[Save](#) [Add](#)

```
[2.7.2-RELEASE][root@.]/root: pfctl -d  
pf disabled  
[2.7.2-RELEASE][root@.]/root: 
```

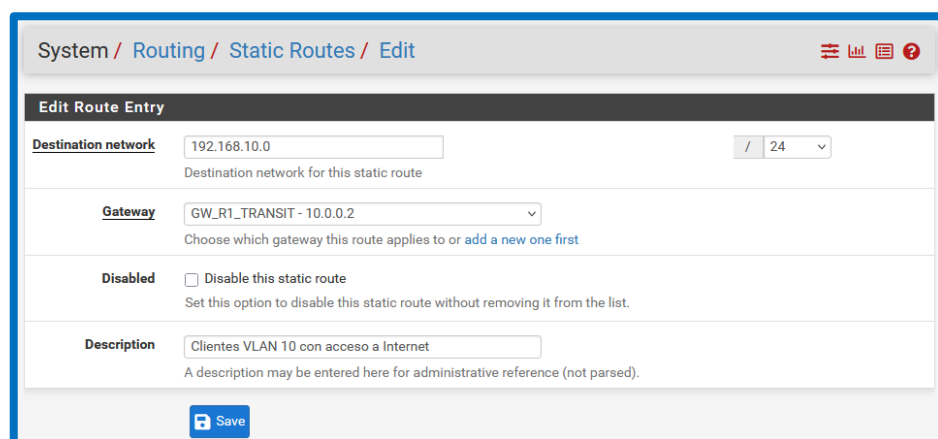
3.6.3 Preparación de rutas estáticas en pfSense hacia VLAN 10 y VLAN 11

Con el gateway de tránsito definido, se procede a crear rutas estáticas para que pfSense conozca que las redes 192.168.10.0/24 y 192.168.11.0/24 no son redes directamente conectadas a pfSense, sino que deben alcanzarse a través de R1. Antes de añadirlas, es útil mostrar que el apartado de rutas estáticas estaba vacío, ya que esto contextualiza la necesidad de crearlas. En la Figura 3.6.4 se muestra el estado inicial sin rutas estáticas configuradas.



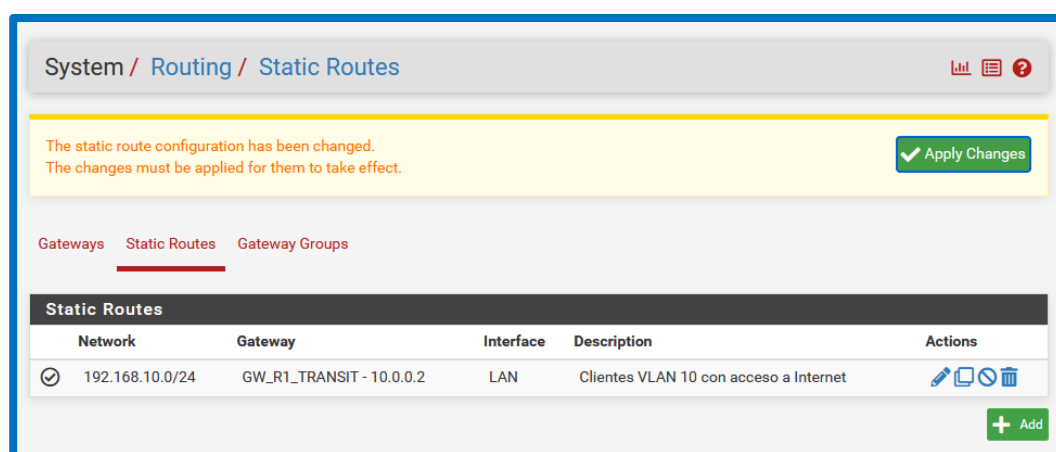
3.6.4 Creación de la ruta estática hacia la red de la VLAN 10 & VLAN 11

Se añade la primera ruta estática indicando como destino la red 192.168.10.0/24 y seleccionando como gateway “GW_R1_TRANSIT (10.0.0.2)”. Con ello, cualquier respuesta o tráfico dirigido a esa red desde pfSense se encaminará correctamente hacia R1. Por eso mismo, se observa en el formulario la ruta con el destino 192.168.10.0/24 y el gateway de tránsito seleccionado (10.0.0.2).

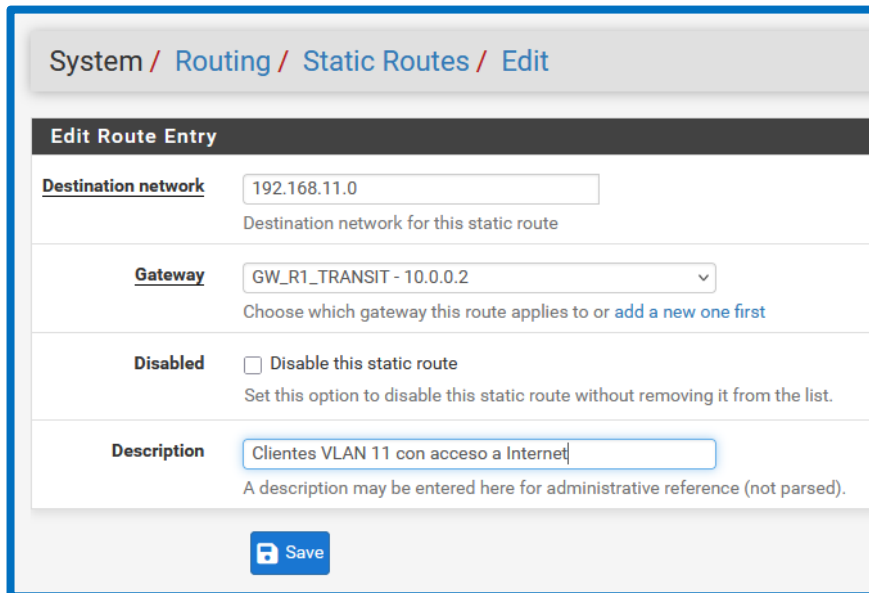


Tras guardar la ruta, pfSense la refleja en el listado de rutas estáticas y vuelve a indicar que hay cambios pendientes de aplicar. De este modo, este punto sirve como evidencia de que la ruta ya está registrada en la configuración y lista para entrar en vigor tras aplicar.

Como podemos observar, al final la ruta de VLAN 10 añadida correctamente.

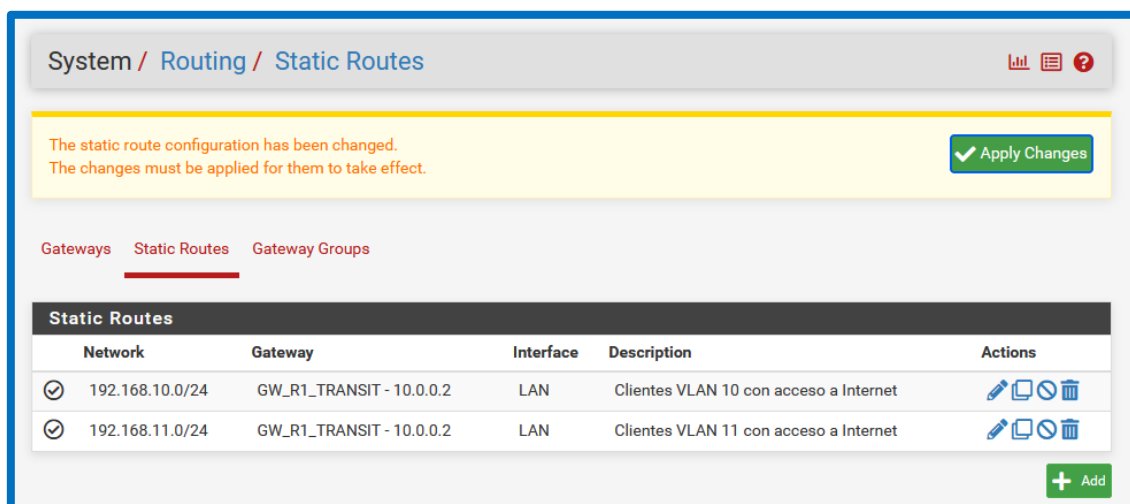








Entonces, se repite el procedimiento para la VLAN 11, donde añadiremos una ruta estática cuyo destino es 192.168.11.0/24 y utilizando el mismo gateway de tránsito hacia R1. Esto garantiza que pfSense dispone de caminos de retorno consistentes para ambas VLAN. Es decir, se debe ver el formulario de la ruta con el destino 192.168.11.0/24 y el gateway “GW_R1_TRANSIT”.



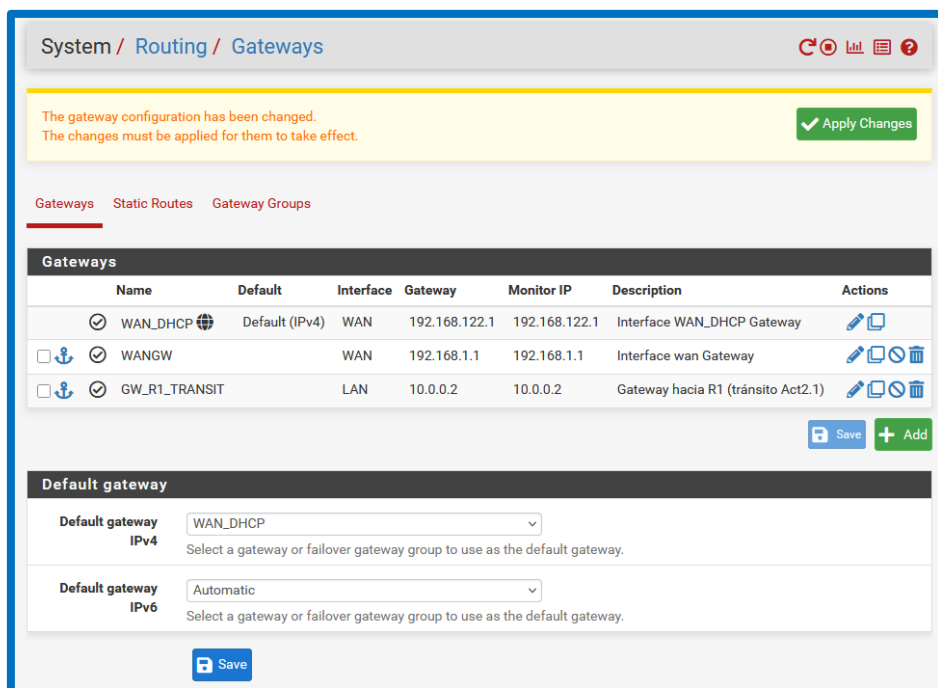
3.6.5 Ambas rutas estáticas definidas y configuración lista para operar sin NAT en R1

Finalmente, el listado de rutas estáticas muestra las dos redes de clientes (VLAN 10 y VLAN 11) apuntando a R1 como siguiente salto. Con esta configuración, el flujo queda correctamente establecido, ya que los clientes salen por R1, R1 reenvía hacia pfSense por el enlace 10.0.0.0/30, pfSense aplica NAT hacia WAN y, gracias a las rutas estáticas, cualquier tráfico de retorno vuelve a las VLAN a través de R1.



Network	Gateway	Interface	Description	Actions
192.168.10.0/24	GW_R1_TRANSIT - 10.0.0.2	LAN	Clientes VLAN 10 con acceso a Internet	  
192.168.11.0/24	GW_R1_TRANSIT - 10.0.0.2	LAN	Clientes VLAN 11 con acceso a Internet	  

Una vez aplicados los cambios en “Apply Changes”, debemos asegurarnos que en el apartado de “Gateways”, se muestra “WAN_DHCP” como gateway por defecto, al ser este el salto entre PFsense y la nube de GNS3 que nos va a brindar conexión a Internet.



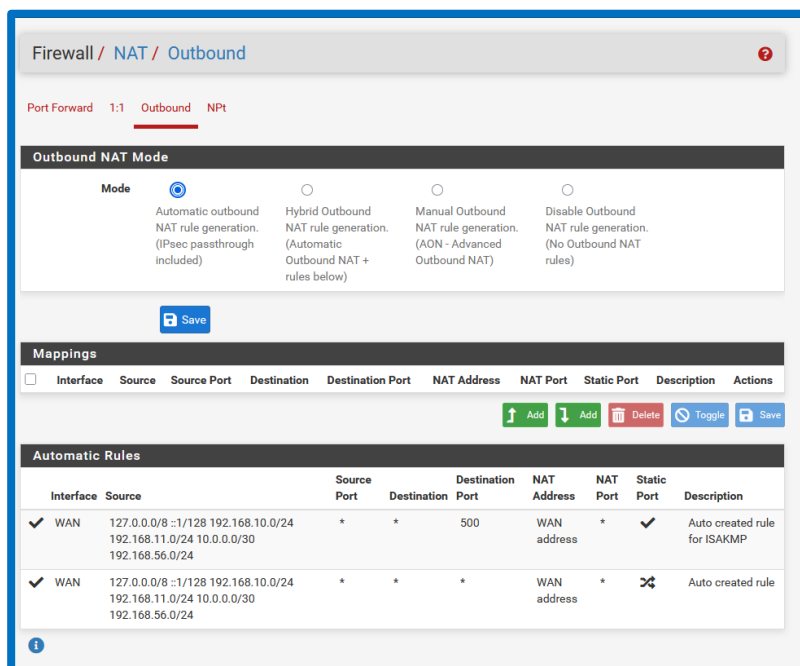
3.7 Verificación del estado de NAT de salida en pfSense

En este punto se revisa el estado del NAT de salida en pfSense para identificar el comportamiento de partida del sistema. pfSense suele trabajar inicialmente con reglas automáticas de traducción, lo cual es suficiente para conectividad bàsica.

Por eso mismo, esta verificación permite ver qué redes están siendo consideradas por las reglas generades, y sirve como referencia antes de dejar el NAT definido de forma manual o con reglas específicas por red, ya que de este modo: se garantiza que la traducción final a Internet se realiza únicamente en el Firewall.

¡IMPORTANTE! Con el modo NAT automático, en la sección de “Automatic Rules” se irán añadiendo cada una de las normativas NAT creadas para permitir que nuestros clientes Debian puedan conectarse a Internet desde el primer ‘ping’ que reciba PFsense de estos equipos.

Si en cambio, lo tenemos en modo manual: nosotros mismos debemos crear esas normativas NAT para brindarles la conectividad a Internet.

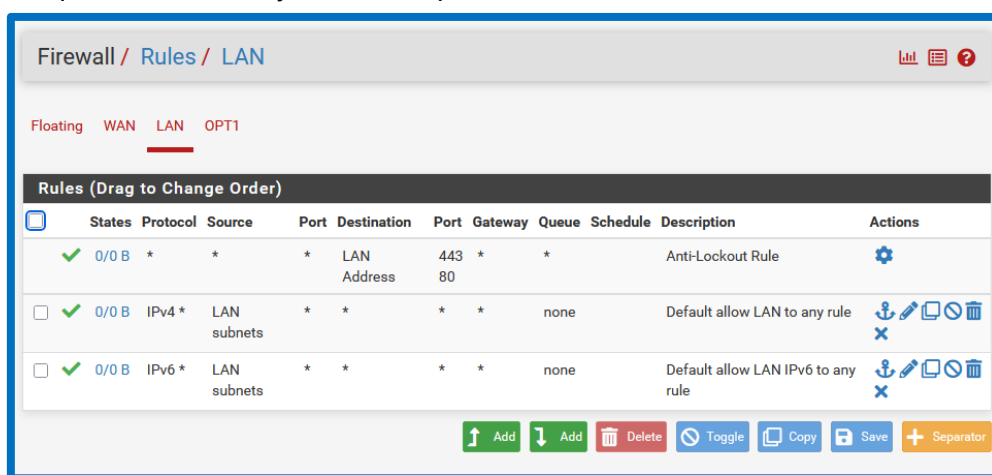


3.7.1 Estado inicial del cortafuegos en la interfaz LAN

Antes de añadir reglas específicas, se observa el conjunto de reglas base en la interfaz **LAN**. pfSense incluye normalmente la regla anti-bloqueo (para evitar perder el acceso a la administración web) y reglas genéricas desde la LAN.

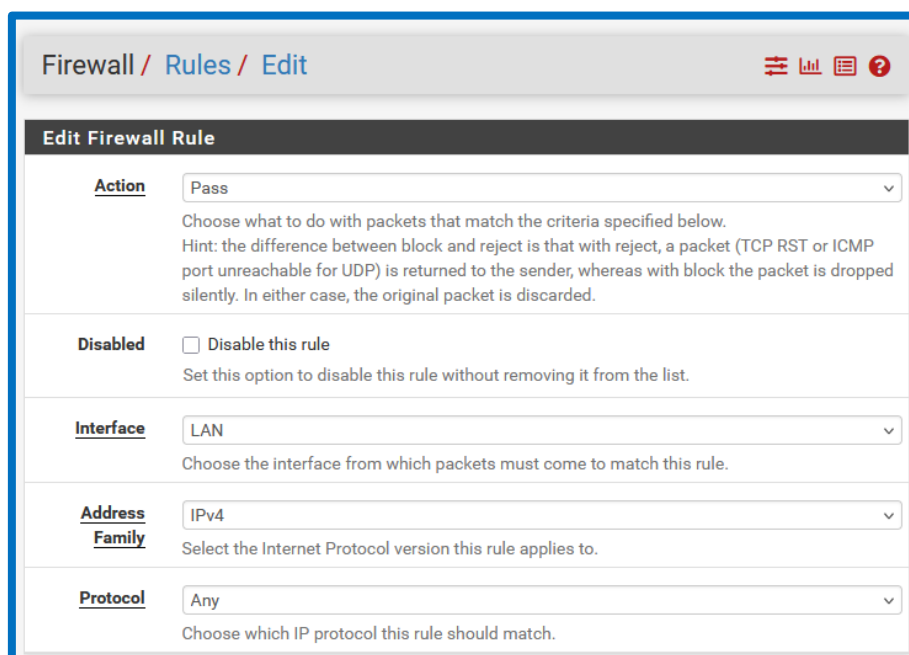
Sin embargo, en este escenario la LAN no representa una “LAN de usuarios”, sino un enlace de tránsito hacia R1 (10.0.0.0/30) por el que entra tráfico con origen real en **192.168.10.0/24** y **192.168.11.0/24**.

Por ello, en lugar de depender únicamente de reglas genéricas, se procede a crear reglas explícitas por subred que documenten y controlen qué redes internas están autorizadas a salir a Internet.

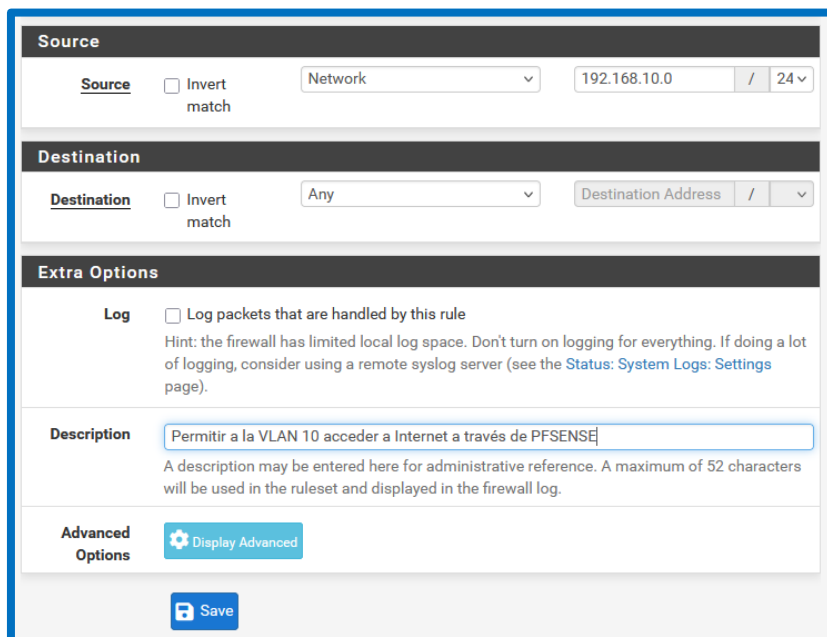


3.7.2 Alta de la normativa para permitir salida a Internet desde VLAN 10

En la creación de la normativa, se define una política de tipo **Pass** aplicada a la interfaz **LAN**, ya que es por esta interfaz por donde pfSense recibe el tráfico reenviado desde R1. De este modo, se limita la regla a **IPv4** y se deja el protocolo en **Any** para permitir el flujo normal de navegación (ICMP para pruebas, TCP/UDP para servicios web y demás tráfico necesario), evitando bloqueos involuntarios durante la validación inicial de conectividad.

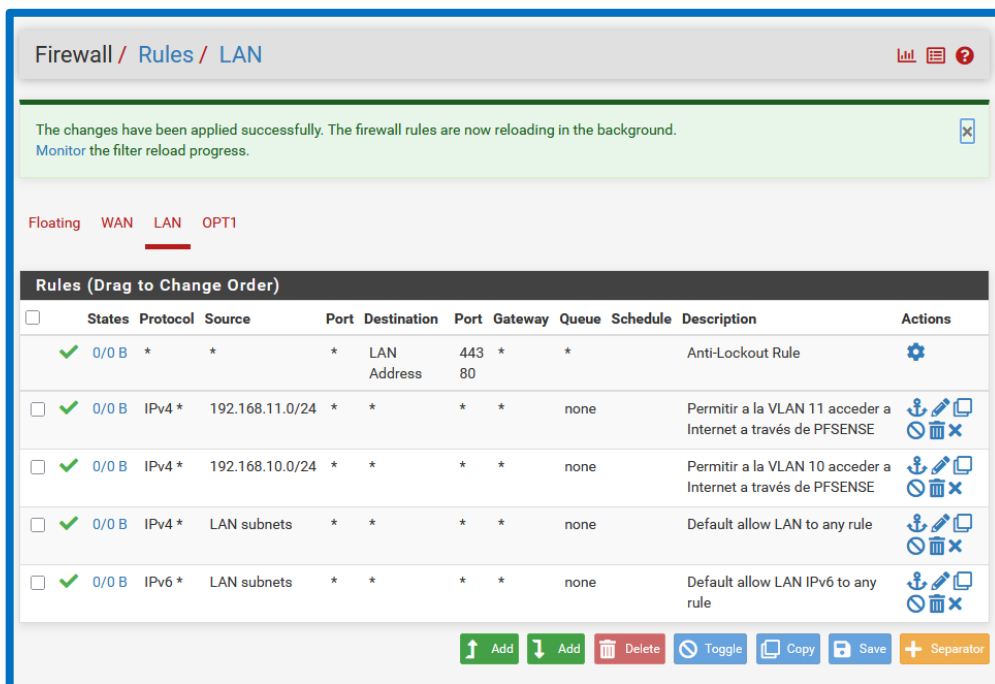


A continuació se concreta el origen como la red **192.168.10.0/24**, que corresponde a la **VLAN 10** detrás de R1, y se establece el destino como **Any**, ya que el objetivo de esta regla es permitir que los clientes de esa VLAN alcancen Internet pasando por el FW. Finalmente, creamos otra para VLAN 11.



3.7.3 Resultado final tras añadir las reglas de VLAN 10 y VLAN 11

Tras guardar y aplicar los cambios, la lista de reglas refleja ya una política explícita por subred, donde se autoriza la salida a Internet de **VLAN 10 (192.168.10.0/24)** y **VLAN 11 (192.168.11.0/24)** a través de pfSense.



Firewall / Rules / LAN											
The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress.											
Floating WAN LAN OPT1											
Rules (Drag to Change Order)											
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/0 B	*	*	*	LAN Address	443	*	*	Anti-Logout Rule	
<input type="checkbox"/>	✓	0/0 B	IPv4 *	192.168.11.0/24	*	*	*	*	none	Permitir a la VLAN 11 acceder a Internet a través de PFSENSE	
<input type="checkbox"/>	✓	0/0 B	IPv4 *	192.168.10.0/24	*	*	*	*	none	Permitir a la VLAN 10 acceder a Internet a través de PFSENSE	
<input type="checkbox"/>	✓	0/0 B	IPv4 *	LAN subnets	*	*	*	*	none	Default allow LAN to any rule	
<input type="checkbox"/>	✓	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none	Default allow LAN IPv6 to any rule	

Add Add Delete Toggle Copy Save Separator

3.8 Verificar que los clientes Debian tienen acceso a Internet a través de PFSENSE

3.8.1 Comprobación de conectividad desde R1 hacia pfSense y hacia Internet

Para ello, desde R1 se lanza un ping a **10.0.0.1** (interfaz LAN de pfSense en el enlace 10.0.0.0/30) y se confirma respuesta correcta, lo que demuestra que la conectividad L3 del tránsito está estable. A continuación, se realiza un ping a **8.8.8.8** y también se obtiene respuesta, confirmando que R1 dispone de salida real a Internet a través de pfSense y que el enrutamiento por defecto hacia **10.0.0.1** está funcionando correctamente después de retirar el NAT del router.

```
R1#ping 10.0.0.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 44/65/84 ms
R1#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/24/40 ms
```

3.8.2 Renovación de DHCP en el cliente de VLAN 10 y verificación de direccionamiento

Tras confirmar que R1 puede alcanzar pfSense e Internet, se fuerza la actualización de configuración de red en el cliente para asegurar que no quedan parámetros antiguos (por ejemplo, DNS o gateway heredados de pruebas previas). De este modo, en el cliente A se libera la concesión DHCP y se solicita una nueva, observándose el proceso completo de descubrimiento, oferta, petición y confirmación, recibiendo la IP **192.168.10.21** desde el servidor DHCP de la VLAN 10 (gateway **192.168.10.1**).

Finalmente, se comprueba que la interfaz de red está en estado operativo y que la IP asignada es la esperada en la subred /24, lo que confirma que el cliente se encuentra correctamente dentro de la VLAN 10 y con parámetros coherentes para la salida a través de R1 y pfSense.

```
debian@clienteA:~$ sudo dhclient -v ens4
Internet Systems Consortium DHCP Client 4.4.3-P1
Copyright 2004-2022 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/ens4/0c:36:ae:33:00:00
Sending on   LPF/ens4/0c:36:ae:33:00:00
Sending on   Socket/fallback
DHCPDISCOVER on ens4 to 255.255.255.255 port 67 interval 4
DHCPOFFER of 192.168.10.21 from 192.168.10.1
DHCPREQUEST for 192.168.10.21 on ens4 to 255.255.255.255 port 67
DHCPACK of 192.168.10.21 from 192.168.10.1
bound to 192.168.10.21 -- renewal in 40140 seconds.
debian@clienteA:~$ ip link show ens4
2: ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP mode
  DEFAULT group default qlen 1000
    link/ether 0c:36:ae:33:00:00 brd ff:ff:ff:ff:ff:ff
    altname enp0s4
debian@clienteA:~$ ip a | grep -i ens4
2: ens4: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group
  default qlen 1000
    inet 192.168.10.21/24 brd 192.168.10.255 scope global dynamic ens4
debian@clienteA:~$
```

3.8.3 Prueba de salida a Internet desde el cliente de VLAN 10 por IP y por nombre

Con el direccionamiento validado, se realizan pruebas de conectividad desde el cliente A. Primero se comprueba el acceso a Internet mediante ping a **8.8.8.8**, lo que confirma que la cadena de encaminamiento funciona extremo a extremo y que la traducción NAT necesaria para salir a Internet se está aplicando donde corresponde (en pfSense).

A continuación, se prueba el ping a **google.com**, y al resolverse correctamente el nombre y responder el destino, queda verificado que la resolución DNS también está funcionando y que el cliente puede navegar por nombre de dominio, no solo por IP. Este doble test permite distinguir claramente entre un problema de conectividad pura y un problema de DNS.

Finalmente, se repiten los mismos pasos de esta sección y de la anterior pero con el otro cliente..

```
debian@clienteA:~$ ping -c3 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=113 time=30.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=113 time=29.2 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=113 time=26.6 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2006ms
rtt min/avg/max/mdev = 26.613/28.815/30.614/1.658 ms
debian@clienteA:~$ ping -c3 google.com
PING google.com (142.250.178.174) 56(84) bytes of data.
64 bytes from mad41s08-in-f14.1e100.net (142.250.178.174): icmp_
=24.8 ms
64 bytes from mad41s08-in-f14.1e100.net (142.250.178.174): icmp_
=26.0 ms
64 bytes from mad41s08-in-f14.1e100.net (142.250.178.174): icmp_
=31.9 ms

--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 24.767/27.551/31.874/3.098 ms
debian@clienteA:~$
```

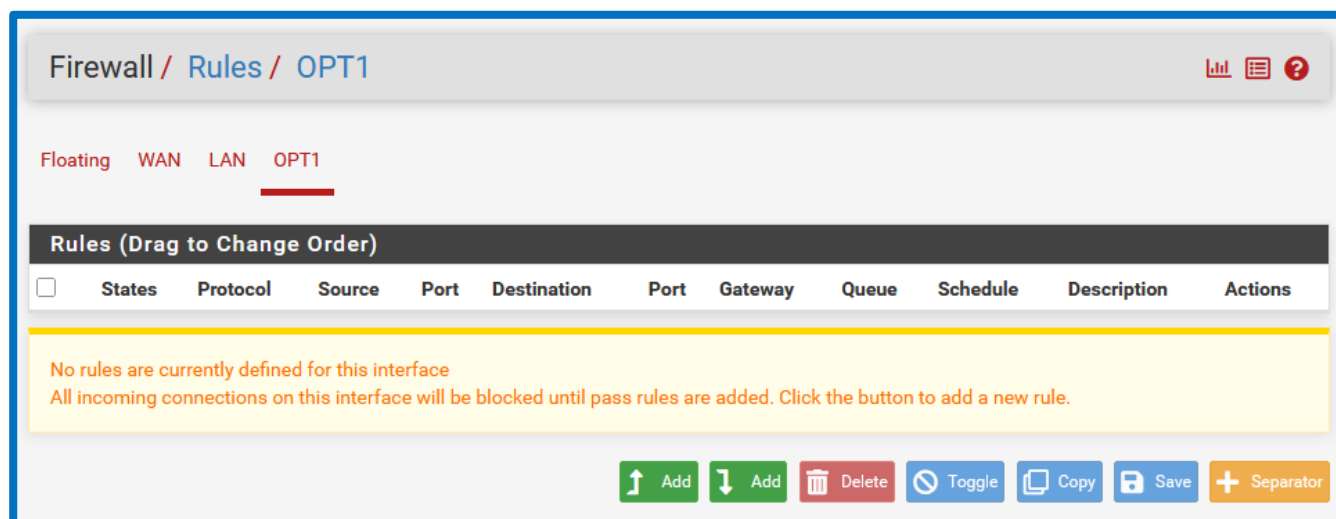
```
debian@clienteB:~$ ping -c3 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=113 time=25.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=113 time=30.6 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=113 time=31.8 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 25.608/29.350/31.840/2.693 ms
debian@clienteB:~$ ping -c3 google.com
PING google.com (142.250.200.110) 56(84) bytes of data.
64 bytes from mad41s13-in-f14.1e100.net (142.250.200.110): icmp_seq=1 ttl=113 ti
me=31.9 ms
64 bytes from mad41s13-in-f14.1e100.net (142.250.200.110): icmp_seq=2 ttl=113 ti
me=31.6 ms
64 bytes from mad41s13-in-f14.1e100.net (142.250.200.110): icmp_seq=3 ttl=113 ti
me=23.4 ms

--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 23.384/28.958/31.889/3.943 ms
debian@clienteB:~$
```

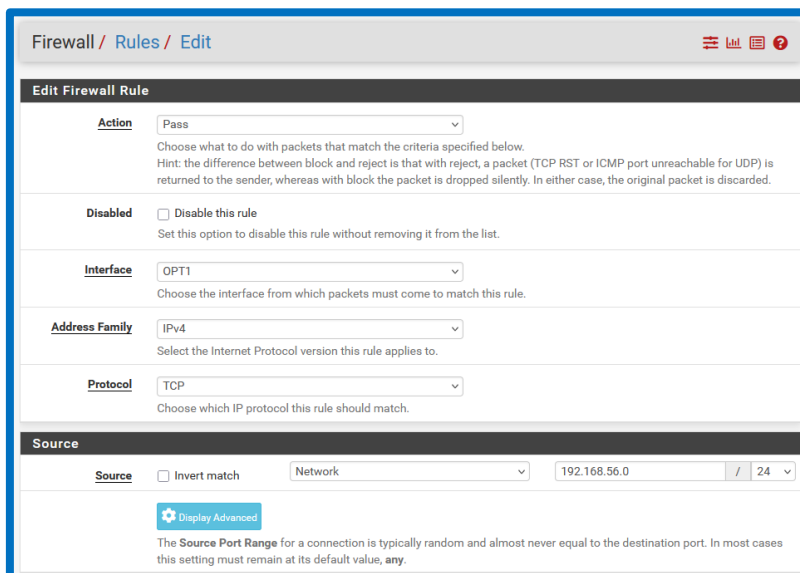
3.9 Permitir acceder a la interfaz web de PFSense sin tener que desactivar el firewall

En este punto se comprueba que la interfaz OPT1 no tiene reglas definidas. En pfSense esto significa que, por defecto, todo el tráfico entrante por OPT1 queda bloqueado hasta que se creen reglas explícitas de tipo pass. Entonces, como OPT1 la estamos usando como red de administración (host-only, por ejemplo 192.168.56.0/24), para poder gestionar el firewall desde esa red.

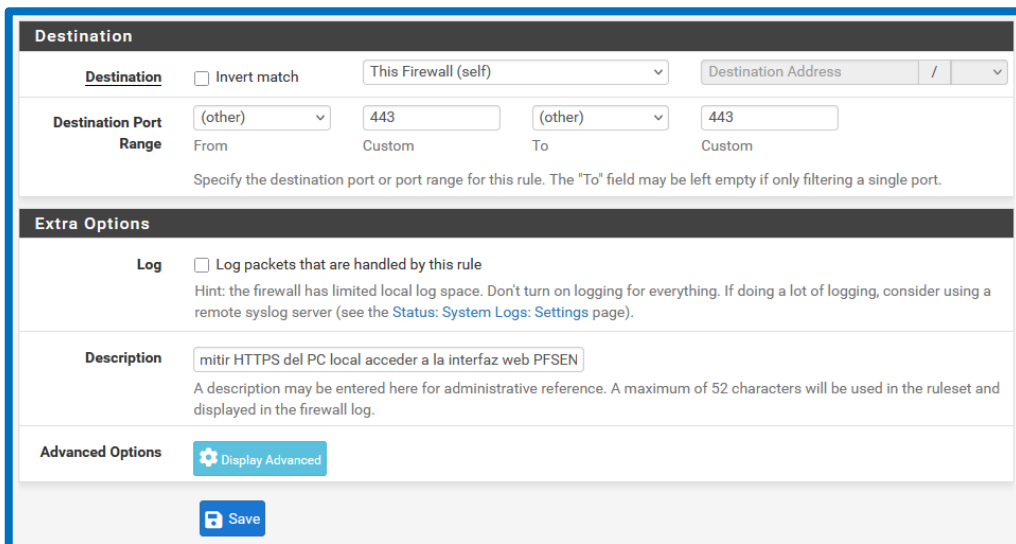


3.9.1 Creación de la regla de acceso al WebGUI por HTTPS

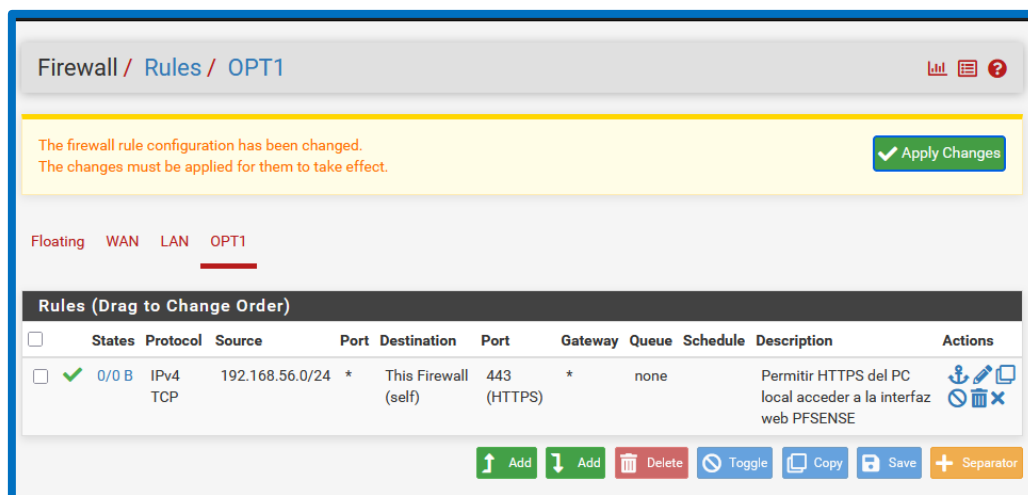
Para habilitar el acceso a la interfaz web, se crea una regla en OPT1 con acción Pass, familia IPv4 y protocolo TCP, porque el panel web se sirve por HTTPS sobre TCP. El origen se restringe a la red de administración 192.168.56.0/24, evitando que otras redes internas (como las VLAN de usuarios) puedan alcanzar la consola de gestión.



A continuación se define el destino como “This Firewall (self)”, porque lo que se pretende es llegar a la propia interfaz de pfSense, y se acota el puerto de destino a 443 para permitir exclusivamente HTTPS. En el campo de descripción conviene dejar un comentario claro y correcto para que el lector entienda exactamente qué se está permitiendo y desde dónde.



Tras guardar la normativa, la interfaz muestra la nueva entrada y solicita aplicar cambios. Al aplicar, la regla queda activa y desde la red 192.168.56.0/24 ya se puede acceder al WebGUI mediante HTTPS sin deshabilitar el firewall.

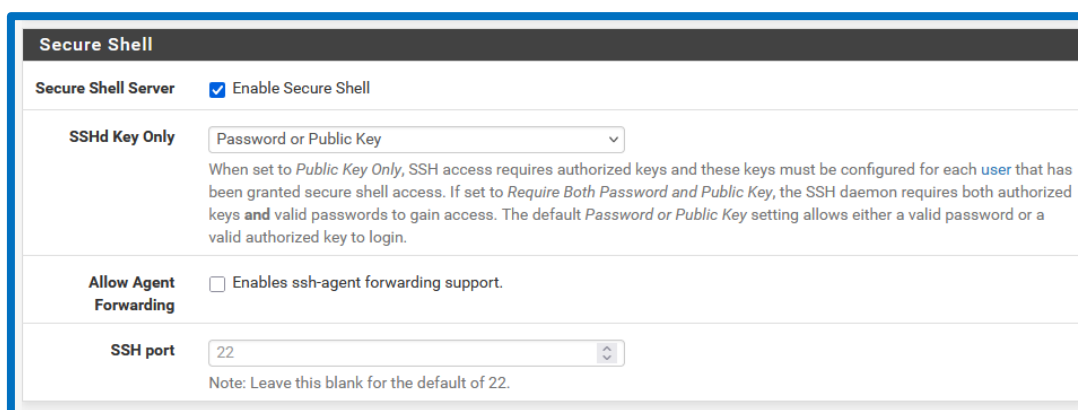
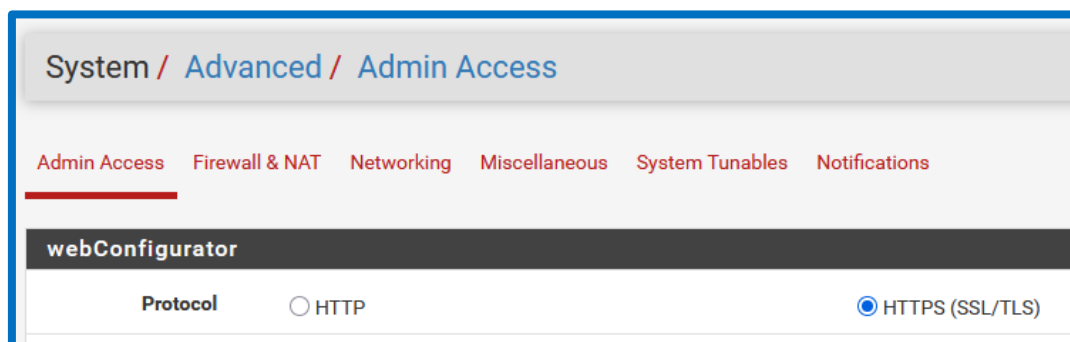


3.10 Permitir acceder por SSH a PFsense solo a través de 192.168.10.21 /24

Adicionalmente, se podemos activar el Secure Shell para conectarnos remotamente al FW mediante nuestra Terminal. Sin embargo, como normativa de seguridad: solo podrá acceder 192.168.10.21/24.

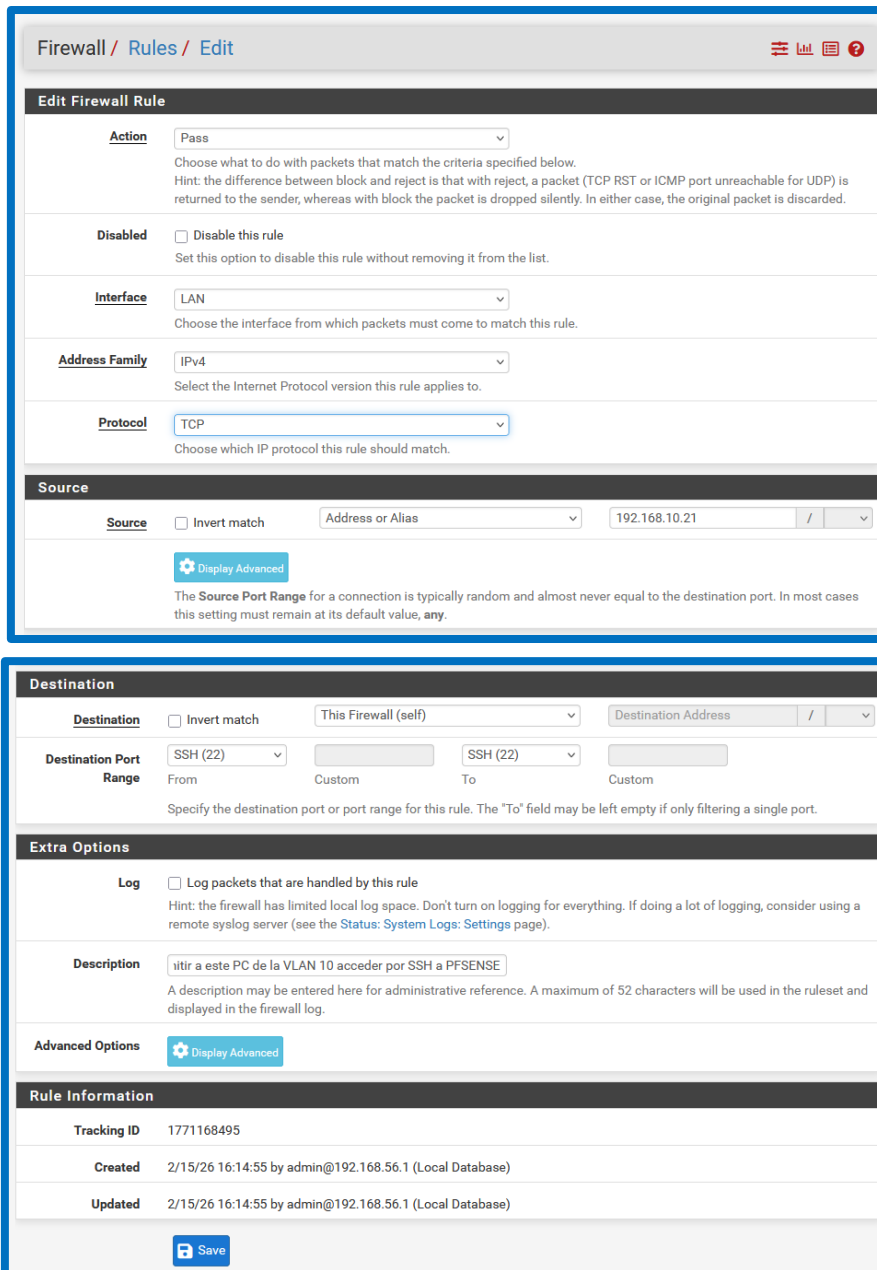
3.10.1 Activación del servicio SSH en pfSense

Entonces, en System / Advanced / Admin Access, se activa Enable Secure Shell para permitir administración remota por consola. Este paso es imprescindible: si el demonio SSH no está habilitado, aunque existan reglas de firewall permitiendo el puerto 22, no habrá un servicio escuchando y las conexiones fallarán igualmente.



3.10.2 Creación de la regla LAN que permite SSH únicamente desde 192.168.10.21

Luego, se define la autorización de acceso de forma explícita mediante una regla en Firewall / Rules / LAN. La regla se configura como Pass, con Interface: LAN, Address Family: IPv4 y Protocol: TCP. El origen se restringe a la IP del equipo administrador 192.168.10.21, y el destino se fija como This Firewall (self), seleccionando el puerto SSH (22). Con esta combinación, la intención queda clara: permitir que únicamente ese host concreto de la VLAN 10 pueda abrir sesiones SSH contra pfSense.



Firewall / Rules / Edit

Edit Firewall Rule

Action
Choose what to do with packets that match the criteria specified below.
Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled ☐ Disable this rule
Set this option to disable this rule without removing it from the list.

Interface
Choose the interface from which packets must come to match this rule.

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

Protocol
Choose which IP protocol this rule should match.

Source

Source ☐ Invert match /

[Display Advanced](#)

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

Destination

Destination ☐ Invert match /

Destination Port Range
From Custom To Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log ☐ Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the [Status: System Logs: Settings](#) page).

Description
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.

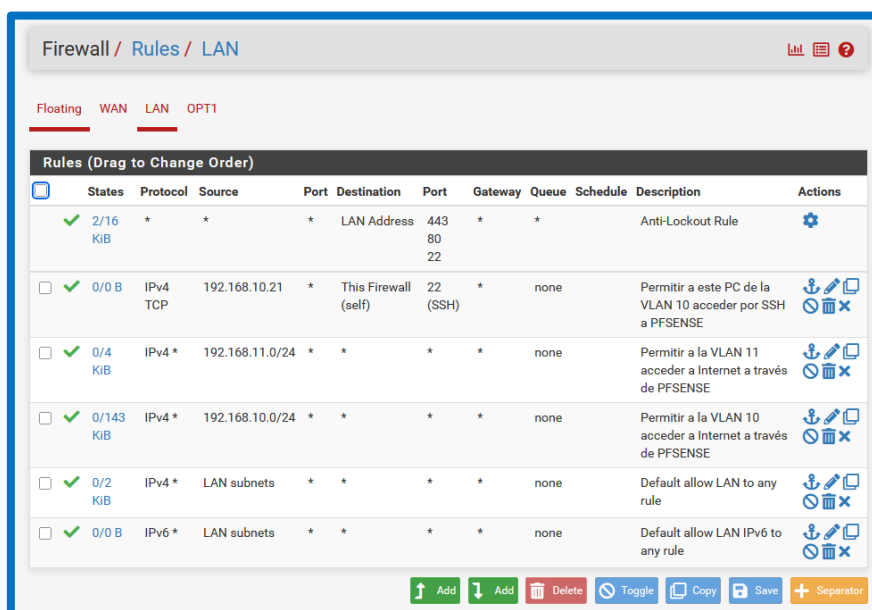
Advanced Options [Display Advanced](#)

Rule Information

Tracking ID	1771168495
Created	2/15/26 16:14:55 by admin@192.168.56.1 (Local Database)
Updated	2/15/26 16:14:55 by admin@192.168.56.1 (Local Database)

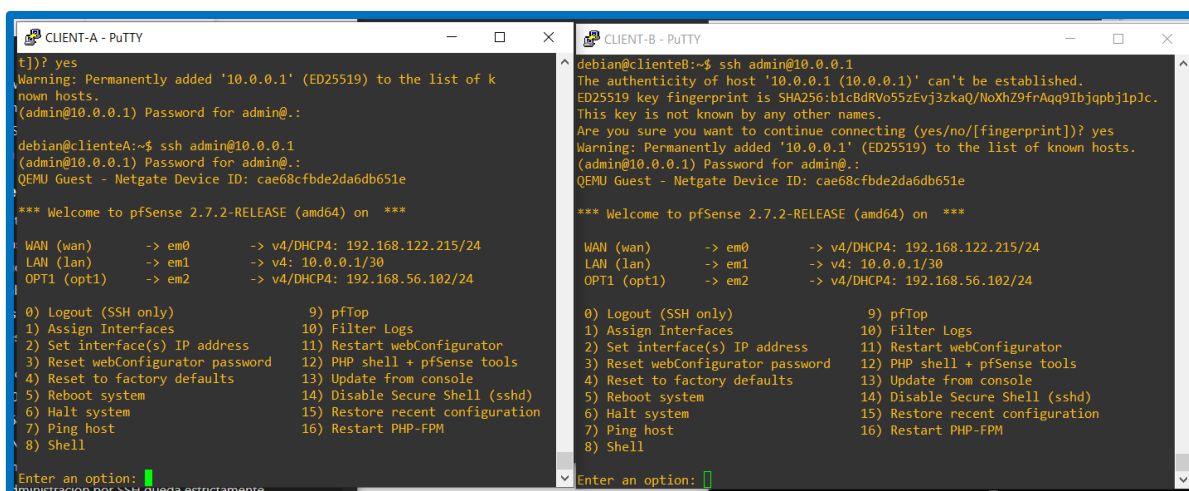
[Save](#)

Tras guardar la regla, se comprueba en el listado de reglas de LAN que la entrada aparece con su descripción, y se aplican los cambios. En este punto ya existe una regla que autoriza el SSH desde 192.168.10.21 hacia pfSense.



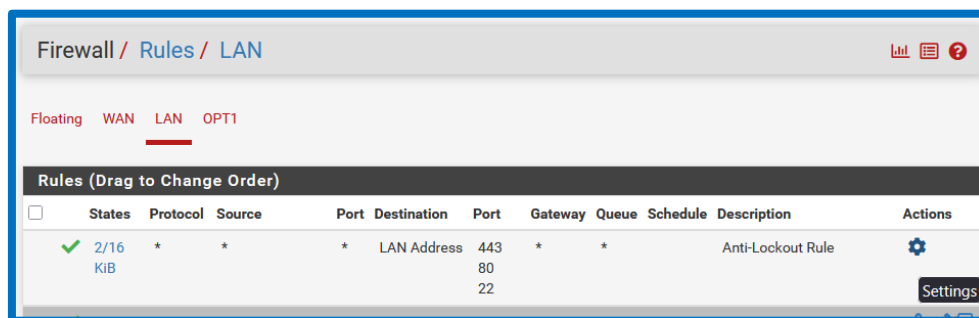
Pero sin embargo como podemos observar, a pesar de la normativa limitando únicamente a que 192.168.10.21 /24 sea el único PC que puede acceder por SSH al FW, si nos conectamos con este protocolo a PFSense observaremos que podemos acceder con ambas maquinas.

Esto se debe a la normativa “Anti-Lockout Rule” de la sección “LAN”, donde se permite el tráfico de cualquier petición que lleve como destino la “LAN Address” si se solicitan los puertos 22,80 y 443.



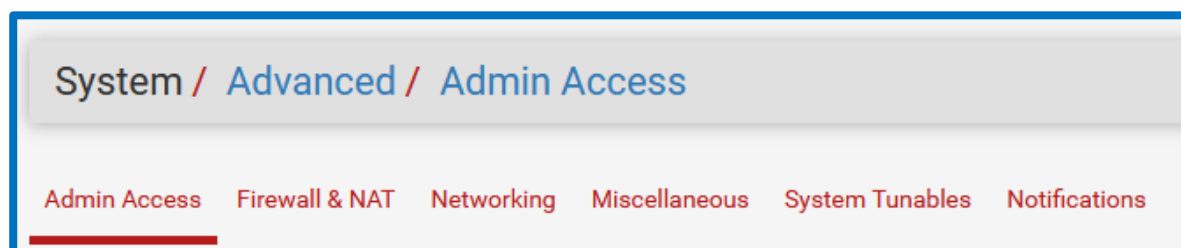
3.11 Desactivar normativa “Anti-lockout”

Antes de endurecer el filtrado, se comprueba la presencia de la regla automática Anti-Lockout Rule en Firewall > Rules > LAN. Esta normativa aparece como una regla de tipo “pass” que permite acceso a la LAN Address en los puertos típicos de administración (HTTP/HTTPS y SSH), con el objetivo de evitar que el administrador se quede sin acceso al webConfigurator por un error de configuración.

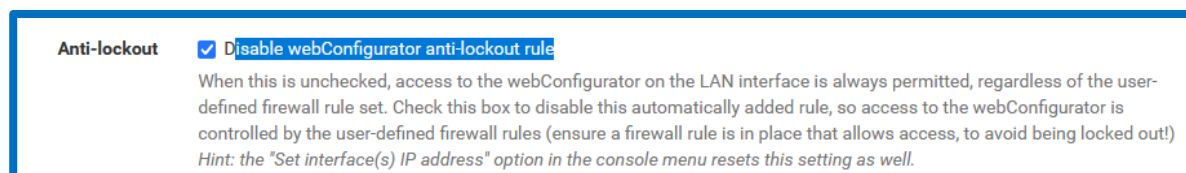


3.11.1 Acceso a la configuración avanzada de administración

Para poder controlar completamente el acceso a la administración mediante reglas propias, se accede al apartado **System > Advanced > Admin Access**, donde pfSense centraliza los parámetros de publicación del webConfigurator y opciones relacionadas con el acceso administrativo.



Dentro de **Admin Access**, se localiza la opción **Disable webConfigurator anti-lockout rule** y se activa. A partir de este momento, el acceso a la interfaz web deja de estar garantizado por una excepción automática y pasa a depender exclusivamente de las reglas definidas en el firewall.



3.11.2 Revisión del conjunto de normativas en LAN tras el cambio

Tras desactivar la normativa anti-lockout, se vuelve a Firewall > Rules > LAN para verificar que la política de acceso queda bajo control explícito. En este punto ya se observa el enfoque de reglas específicas: por un lado, se mantiene una normativa concreta para permitir SSH a pfSense únicamente desde el host autorizado (por ejemplo, el equipo de administración).

Por otro lado aprovechemos para eliminar las reglas de “LAN Subnets” de IPv4 y “IPv6” para evitar depender de normativas de FW demasiado amplias.

3.11.3 Sustitución de permisos genéricos por reglas explícitas ICMP y UDP

Una vez eliminada la excepción automática, se refuerza el control sustituyendo permisos amplios por reglas explícitas por protocolo. En la captura se aprecia el ajuste de normativas donde se destacan **ICMP** y **UDP** para las redes **192.168.10.0/24 (VLAN 10)** y **192.168.11.0/24 (VLAN 11)**.

De este modo, este paso permite conservar conectividad operativa mínima y verificable, ya que ICMP facilita comprobaciones de alcance (por ejemplo, ping a Internet) y UDP habilita el tráfico necesario para servicios básicos como resoluciones DNS.

Firewall / Rules / LAN

Floating WAN LAN OPT1

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP	192.168.10.21	*	This Firewall (self)	22 (SSH)	*	none		Permitir a este PC de la VLAN 10 acceder por SSH a PFSENSE	
<input type="checkbox"/>	✓ 0/4 KiB	IPv4 *	192.168.11.0/24	*	*	*	*	none		Permitir a la VLAN 11 acceder a Internet a través de PFSENSE	
<input type="checkbox"/>	✓ 0/143 KiB	IPv4 *	192.168.10.0/24	*	*	*	*	none		Permitir a la VLAN 10 acceder a Internet a través de PFSENSE	
<input checked="" type="checkbox"/>	✓ 0/2 KiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input checked="" type="checkbox"/>	✓ 0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	Disable

Add Add Delete Toggle Copy Save Separator

Floating WAN LAN OPT1

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/41 KiB	IPv4 TCP	192.168.10.21	*	This Firewall (self)	22 (SSH)	*	none		Permitir a este PC de la VLAN 10 acceder por SSH a PFSENSE	
<input type="checkbox"/>	✓ 0/840 B	IPv4 ICMP any	192.168.11.0/24	*	*	*	*	none		Permitir a la VLAN 11 acceder a Internet a través de PFSENSE	
<input type="checkbox"/>	✓ 0/1 KiB	IPv4 UDP	192.168.11.0/24	*	*	*	*	none		Permitir a la VLAN 11 acceder a Internet a través de PFSENSE	
<input type="checkbox"/>	✓ 0/0 B	IPv4 UDP	192.168.10.0/24	*	*	*	*	none		Permitir a la VLAN 10 acceder a Internet a través de PFSENSE	
<input type="checkbox"/>	✓ 0/0 B	IPv4 ICMP any	192.168.10.0/24	*	*	*	*	none		Permitir a la VLAN 10 acceder a Internet a través de PFSENSE	

3.11.4 Validación desde cliente autorizado: conectividad e inicio de sesión por SSH

Desde el equipo autorizado de la **VLAN 10** se verifica que la conectividad general sigue operativa mediante una prueba de alcance a un dominio público y, a continuación, se comprueba el acceso por **SSH** hacia la IP de pfSense en el enlace de tránsito (**10.0.0.1**). De este modo, el resultado confirma que la desactivación de la regla anti-lockout no ha roto la administración remota porque existe una normativa específica que permite el acceso únicamente a ese host.

3.11.5 Confirmación en pfSense: estado de sesión SSH establecido && No establecido

De hecho, si vamos a **Diagnostics > States** filtrando por la regla correspondiente. La tabla de estados muestra una sesión **TCP establecida** desde **192.168.10.21** hacia **10.0.0.1:22**, lo que valida que la política aplicada está funcionando como se diseñó: el firewall permite y mantiene la sesión únicamente para el origen autorizado.

```
debian@clienteA:~$ ping -c4 google.com
PING google.com (142.251.140.238) 56(84) bytes of data.
64 bytes from dia01s03-in-f14.1e100.net (142.251.140.238): icmp_seq=1 ttl=114 time=28.6 ms
64 bytes from dia01s03-in-f14.1e100.net (142.251.140.238): icmp_seq=2 ttl=114 time=24.9 ms
64 bytes from lcmda-ab-in-f14.1e100.net (142.251.140.238): icmp_seq=3 ttl=114 time=25.1 ms
64 bytes from dia01s03-in-f14.1e100.net (142.251.140.238): icmp_seq=4 ttl=114 time=29.9 ms

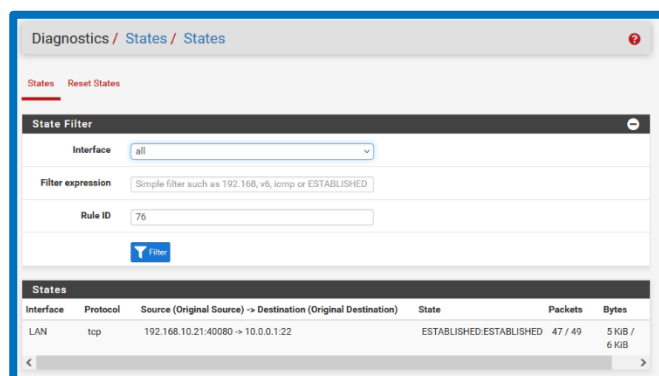
--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 24.936/27.137/29.915/2.175 ms
debian@clienteA:~$ ssh admin@10.0.0.1
(admin@10.0.0.1) Password for admin@.:
QEMU Guest - Netgate Device ID: cae68cfbde2da6db651e

*** Welcome to pfSense 2.7.2-RELEASE (amd64) on ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.122.215/24
LAN (lan)      -> em1      -> v4: 10.0.0.1/30
OPT1 (opt1)    -> em2      -> v4/DHCP4: 192.168.56.102/24

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

Enter an option: █
```



```
debian@clienteB:~$ ping -c3 google.com
PING google.com (142.250.200.110) 56(84) bytes of data.
64 bytes from mad41s13-in-f14.1e100.net (142.250.200.110): icmp_seq=1 ttl=113 time=25.1 ms
64 bytes from mad41s13-in-f14.1e100.net (142.250.200.110): icmp_seq=2 ttl=113 time=29.3 ms
64 bytes from mad41s13-in-f14.1e100.net (142.250.200.110): icmp_seq=3 ttl=113 time=25.9 ms

--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2004ms
rtt min/avg/max/mdev = 25.148/26.767/29.261/1.789 ms
debian@clienteB:~$ ssh admin@10.0.0.1
ssh: connect to host 10.0.0.1 port 22: Connection timed out
debian@clienteB:~$ █
```

Finalmente, se repite la prueba desde un segundo cliente que no está autorizado para administrar pfSense por SSH. En este caso se comprueba primero que el cliente mantiene salida a Internet (la conectividad ICMP funciona), pero el intento de conexión **SSH a 10.0.0.1:22** expira por **timeout**, confirmando que la restricción por origen es efectiva.

Con ello se demuestra el objetivo principal de esta fase: desactivar el mecanismo anti-lockout sin perder control administrativo, sustituyéndolo por reglas explícitas que permiten operación normal de los clientes y, al mismo tiempo, limitan la administración a un único punto autorizado.

4. Logging y monitoreo básico

4.1 Revisión de eventos en los logs del firewall

Para validar que las políticas del cortafuegos se están aplicando como se espera, el primer punto de control es el registro de eventos en Status > System Logs > Firewall. En este caso, el log muestra intentos de conexión que han sido denegados por la regla implícita "Default deny rule IPv4" en la interfaz OPT1, con tráfico desde 192.168.56.1 hacia la propia interfaz de administración en 192.168.56.102:443, lo que confirma que, mientras no existan reglas explícitas de paso en OPT1, el firewall bloqueará cualquier entrada por defecto.

A continuació, el log també permet comprovar controls més fins a nivell de LAN, on es observa un esdevençament permès per SSH des de 192.168.10.21 cap a 10.0.0.1:22, associat a una regla específica (la que autoritza aquest origen), i just a sota un intent equivalent des de 192.168.11.21 que cau en “Default deny rule IPv4”.

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

Advanced Log Filter

Last 500 Firewall Log Entries. (Maximum 500)

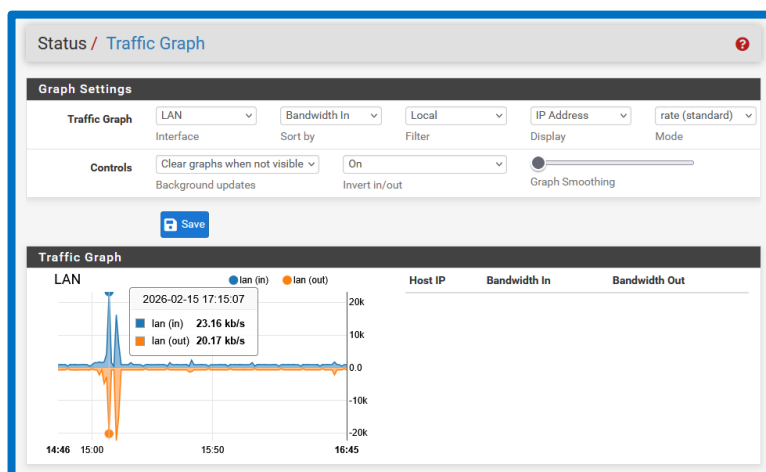
Action	Time	Interface	Rule	Source	Destination	Protocol
✗	Feb 15 00:43:16	OPT1	Default deny rule IPv4 (1000000103)	192.168.56.1:50667	192.168.56.102:443	TCP:PA
✗	Feb 15 00:43:16	OPT1	Default deny rule IPv4 (1000000103)	192.168.56.1:50667	192.168.56.102:443	TCP:RA

Aquesta comparació en el propi registre és especialment útil perquè demostra, amb evidències, que el accés per SSH se està restringint exactament al host autoritzat i que el rest dels orígens queden les seues peticions denegades.

✓	Feb 15 17:11:28	LAN	Permitir a este PC de la VLAN 10 acceder por SSH ... (1771168495)	192.168.10.21:46438	10.0.0.1:22	TCP:S
✗	Feb 15 17:11:36	LAN	Default deny rule IPv4 (1000000103)	192.168.11.21:42670	10.0.0.1:22	TCP:S

4.2 Monitorización rápida de actividad con el Traffic Graph

Una vegada verificat el comportament per regles en els logs, una comprovació ràpida de “salut” del tràfic se pot fer des de **Status > Traffic Graph**, seleccionant la interfaz a observar (en aquest cas, **LAN**) i visualitzant l'amplada de banda d'entrada i sortida. És a dir, el gràfic reflecteix pics puntuals de tràfic (per exemple, un increment al voltant de les 17:15), que sol coincidir amb proves de connectivitat, consultes DNS o sessions iniciades (ICMP, HTTP/HTTPS o SSH).



4.3 Correlación de estados con pfTop

Finalmente, para una visión más “en vivo” de qué flujos están activos y consumiendo más, Diagnostics > pfTop permite listar estados ordenados por bytes y ver rápidamente origen, destino, protocolo y estado de cada conexión. En la salida se aprecian, por ejemplo, estados TCP hacia 192.168.56.102:443 (sesión HTTPS de administración) y tráfico ICMP y UDP asociado a pruebas y servicios (incluyendo consultas DNS).

```
debian@clienteA:~$ ping -c4 google.com
PING google.com (142.251.140.238) 56(84) bytes of data.
64 bytes from dia01s03-in-f14.1e100.net (142.251.140.238): icmp_seq=1 ttl=114 time=28.8 ms
64 bytes from lcmada-ab-in-f14.1e100.net (142.251.140.238): icmp_seq=2 ttl=114 time=23.0 ms
64 bytes from lcmada-ab-in-f14.1e100.net (142.251.140.238): icmp_seq=3 ttl=114 time=24.9 ms
64 bytes from lcmada-ab-in-f14.1e100.net (142.251.140.238): icmp_seq=4 ttl=114 time=22.0 ms

--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 22.029/24.697/28.822/2.599 ms
debian@clienteA:~$
```

De este modo, esta vista es útil para correlacionar lo que aparece en logs con lo que realmente está establecido en ese momento, y para detectar de inmediato si hay conexiones inesperadas o si un flujo que debería existir no llega a crearse.

Diagnostics / pfTop?

pfTop Configuration

View

default

Filter expression

e.g. tcp, ip6 or dst net 208.123.73.0/24

click for filter help ⓘ

Sort by

Bytes

Maximum # of States

100

Output

pfTop: Up State 1-17/17, View: default, Order: bytes

PR	DIR	SRC	DEST	STATE	AGE	EXP	PKTS	
tcp	In	192.168.56.1:51607	192.168.56.102:443	ESTABLISHED:ESTABLISHED	00:06:12	24:00:00	2944	1
icmp	Out	10.0.0.1:28739	10.0.0.2:28739	0:0	00:38:13	00:00:10	8654	:
icmp	Out	192.168.122.215:27923	192.168.122.1:27923	0:0	00:38:13	00:00:10	8654	:
icmp	Out	192.168.122.215:28437	192.168.1.1:28437	0:0	00:38:13	00:00:10	8654	:
tcp	In	192.168.10.21:59574	10.0.0.1:22	FIN_WAIT_2:FIN_WAIT_2	00:05:06	00:00:18	116	
icmp	In	192.168.10.21:5937	142.251.140.238:5937	0:0	00:00:13	00:00:00	8	
icmp	Out	192.168.122.215:35399	142.251.140.238:35399	0:0	00:00:13	00:00:00	8	
udp	In	192.168.10.21:50210	1.1.1.1:53	SINGLE:MULTIPLE	00:00:13	00:00:17	4	
udp	Out	192.168.122.215:6686	1.1.1.1:53	MULTIPLE:SINGLE	00:00:13	00:00:17	4	
udp	In	192.168.10.21:53083	1.1.1.1:53	SINGLE:MULTIPLE	00:00:13	00:00:17	2	
udp	Out	192.168.122.215:8119	1.1.1.1:53	MULTIPLE:SINGLE	00:00:13	00:00:17	2	
udp	In	192.168.10.21:46254	1.1.1.1:53	SINGLE:MULTIPLE	00:00:12	00:00:18	2	
udp	Out	192.168.122.215:54485	1.1.1.1:53	MULTIPLE:SINGLE	00:00:12	00:00:18	2	
udp	In	192.168.10.21:56299	1.1.1.1:53	SINGLE:MULTIPLE	00:00:11	00:00:19	2	
udp	Out	192.168.122.215:29184	1.1.1.1:53	MULTIPLE:SINGLE	00:00:11	00:00:19	2	
udp	In	192.168.10.21:35169	1.1.1.1:53	SINGLE:MULTIPLE	00:00:10	00:00:20	2	
udp	Out	192.168.122.215:38539	1.1.1.1:53	MULTIPLE:SINGLE	00:00:10	00:00:20	2	

5. EXTRAS: Manual Outbound NAT & DNS Enforcement

5.1 ¿Qué es el Manual Outbound NAT?

En pfSense, el “Outbound NAT” es el conjunto de reglas que traducen las IP privadas de tus redes internas a una IP de salida válida cuando los equipos acceden a Internet. Por defecto, pfSense suele trabajar en modo automático generando reglas de manera dinámica según las redes y la interfaz WAN.

De hecho, cuando se habla de “Manual Outbound NAT” significa que desactivas esa generación automática y pasas a definir tú, una por una, las reglas de traducción (qué redes salen, por qué interfaz, con qué IP se “enmascaran” y bajo qué condiciones).

Esto se usa cuando necesitas control total: por ejemplo, si quieres que solo ciertas subredes hagan NAT, si quieres aplicar NAT distinto según origen, si tienes varias WAN, si haces policy routing, o si necesitas evitar conflictos cuando hay más de un salto de routing y no quieres que pfSense “adivine” reglas que no encajan con tu diseño.

5.2 ¿Qué es el DNS Enforcement?

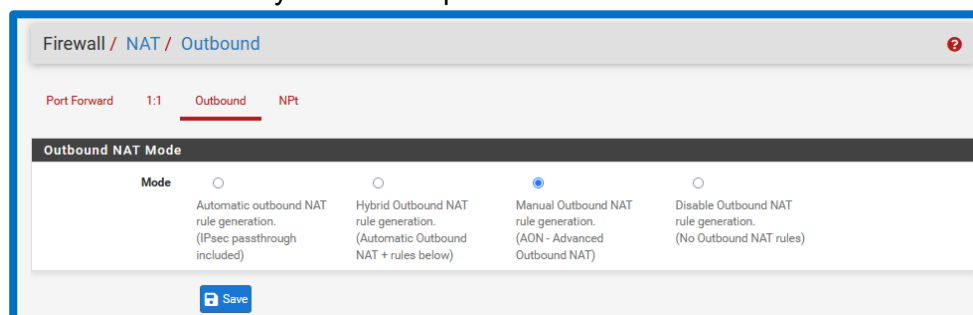
El “DNS Enforcement” es un término práctico para describir una política que obliga a que los clientes usen el DNS que tú defines (normalmente el DNS Resolver/Forwarder de pfSense) y evitar que se “salten” esa política apuntando a DNS externos como 8.8.8.8, 1.1.1.1, etc.

A nivel técnico, se implementa con reglas de firewall y, muchas veces, con un NAT Redirect (port forward interno) que intercepta cualquier tráfico DNS saliente (puerto 53 TCP/UDP, y a veces DoT 853) y lo redirige al DNS permitido. Es decir, la idea es que los clientes solo usen el DNS que quiere la empresa para aplicar filtrado, trazabilidad, logging, control por VLAN, bloqueo de dominios, etc.

El DNS Enforcement, nos evita el DNS Hijacking, que es cuando un cliente acaba usando un DNS diferente al que teníamos planeado. Si esto ocurre, al no ser nuestro DNS quien se encarga de resolverlo o redireccionarla: no queda constancia en la caché de nuestro DNS de dicha resolución.

5.3 Activar Manual OutBound NAT

Para activar el NAT de manera manual, simplemente iremos a “Firewall / NAT / Outbound” para ir a la sección “Outbound” y marcar la opción “Manual NAT” > SAVE.



5.3.1 Borrar normativas NAT creadas automaticamente

Como podemos observar, estas son las normativas que ha creado PFsense automáticamente. Al tener ahora mismo el control de NAT, veremos que muchas de estas normativas simplemente son “ruido”, y es por eso: que únicamente mantendremos las normativas de la VLAN 10 (192.168.10.0/24), la de la VLAN 11 (192.168.11.0/24), y finalmente: la de 10.0.0.0/30 para que R1 tenga Internet.

Mappings										
<input type="checkbox"/>	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
<input checked="" type="checkbox"/>	WAN	127.0.0.0/8	*	*	500 (ISAKMP)	WAN address	*	<input checked="" type="checkbox"/>	Auto created rule for ISAKMP - localhost to WAN	
<input checked="" type="checkbox"/>	WAN	127.0.0.0/8	*	*	*	WAN address	*	<input checked="" type="checkbox"/>	Auto created rule - localhost to WAN	
<input checked="" type="checkbox"/>	WAN	::1/128	*	*	500 (ISAKMP)	WAN address	*	<input checked="" type="checkbox"/>	Auto created rule for ISAKMP - localhost to WAN	
<input checked="" type="checkbox"/>	WAN	::1/128	*	*	*	WAN address	*	<input checked="" type="checkbox"/>	Auto created rule - localhost to WAN	
<input checked="" type="checkbox"/>	WAN	192.168.10.0/24	*	*	500 (ISAKMP)	WAN address	*	<input checked="" type="checkbox"/>	Auto created rule for ISAKMP - static route to WAN	
<input type="checkbox"/>	WAN	192.168.10.0/24	*	*	*	WAN address	*	<input checked="" type="checkbox"/>	Auto created rule - static route to WAN	
<input checked="" type="checkbox"/>	WAN	192.168.11.0/24	*	*	500 (ISAKMP)	WAN address	*	<input checked="" type="checkbox"/>	Auto created rule for ISAKMP - static route to WAN	
<input type="checkbox"/>	WAN	192.168.11.0/24	*	*	*	WAN address	*	<input checked="" type="checkbox"/>	Auto created rule - static route to WAN	
<input checked="" type="checkbox"/>	WAN	10.0.0.0/30	*	*	500 (ISAKMP)	WAN address	*	<input checked="" type="checkbox"/>	Auto created rule for ISAKMP - LAN to WAN	
<input type="checkbox"/>	WAN	10.0.0.0/30	*	*	*	WAN address	*	<input checked="" type="checkbox"/>	Auto created rule - LAN to WAN	
<input checked="" type="checkbox"/>	WAN	192.168.56.0/24	*	*	500 (ISAKMP)	WAN address	*	<input checked="" type="checkbox"/>	Auto created rule for ISAKMP - OPT1 to WAN	
<input checked="" type="checkbox"/>	WAN	192.168.56.0/24	*	*	*	WAN address	*	<input checked="" type="checkbox"/>	Auto created rule - OPT1 to WAN	

Finalmente, una vez guardados los cambios: crearemos una nueva normativa del FW para que R1 pueda acceder a Internet, y volveremos a comprobar des de la VLAN 10 y 11 que tengan comunicación con el exterior.

Firewall / NAT / Outbound

Port Forward 1:1 Outbound NAT

Outbound NAT Mode

Mode

☐ Automatic outbound NAT rule generation. (IPsec passthrough included)
☐ Hybrid Outbound NAT rule generation. (Automatic Outbound NAT + rules below)
☒ Manual Outbound NAT rule generation. (AON - Advanced Outbound NAT)
☐ Disable Outbound NAT rule generation. (No Outbound NAT rules)

Mappings

<input type="checkbox"/>	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
<input type="checkbox"/>	WAN	192.168.10.0/24	*	*	*	WAN address	*	<input checked="" type="checkbox"/>	Auto created rule - static route to WAN	
<input type="checkbox"/>	WAN	192.168.11.0/24	*	*	*	WAN address	*	<input checked="" type="checkbox"/>	Auto created rule - static route to WAN	
<input type="checkbox"/>	WAN	10.0.0.0/30	*	*	*	WAN address	*	<input checked="" type="checkbox"/>	Auto created rule - LAN to WAN	

```
R1#ping 8.8.8.8
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/25/52 ms
R1#
```

```
debian@clienteA:~$ ping -c4 google.com
PING google.com (142.250.200.142) 56(84) bytes of data.
64 bytes from mad41s14-in-f14.1e100.net (142.250.200.142): icmp
_seq=1 ttl=113 time=30.7 ms
64 bytes from mad41s14-in-f14.1e100.net (142.250.200.142): icmp
_seq=2 ttl=113 time=27.7 ms
64 bytes from mad41s14-in-f14.1e100.net (142.250.200.142): icmp
_seq=3 ttl=113 time=25.8 ms
64 bytes from mad41s14-in-f14.1e100.net (142.250.200.142): icmp
_seq=4 ttl=113 time=23.0 ms

--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3010ms
rtt min/avg/max/mdev = 22.997/26.788/30.665/2.800 ms
debian@clienteA:~$
```

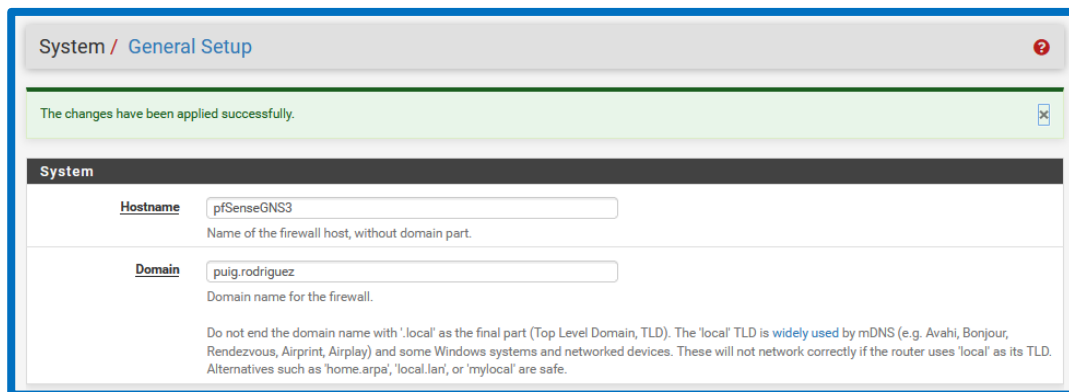
```
debian@clienteB:~$ ping -c3 google.com
PING google.com (142.251.140.238) 56(84) bytes of data.
64 bytes from dia01s03-in-f14.1e100.net (142.251.140.238): icmp_seq=1 ttl=114 ti
me=31.4 ms
64 bytes from lcmada-ab-in-f14.1e100.net (142.251.140.238): icmp_seq=2 ttl=114 t
ime=31.0 ms
64 bytes from dia01s03-in-f14.1e100.net (142.251.140.238): icmp_seq=3 ttl=114 ti
me=36.2 ms

--- google.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2007ms
rtt min/avg/max/mdev = 30.973/32.864/36.195/2.362 ms
debian@clienteB:~$
```

5.4 Evitar bypass de DNS (DNS enforcement)

Para aplicar normativas de DNS en PFsense, primero de todos debemos comprobar si en “System / General Setup” figuran nuestro “Hostname” y nuestro “Dominio”. En el caso que estén vacías, aprovechamos ahora para rellenarlas.

De hecho, si no lo hacemos: nos dará error a la hora de iniciar el servicio de DNS de PFsense.



System / General Setup

The changes have been applied successfully.

System

Hostname pfSenseGNS3
Name of the firewall host, without domain part.

Domain puig.rodriguez
Domain name for the firewall.

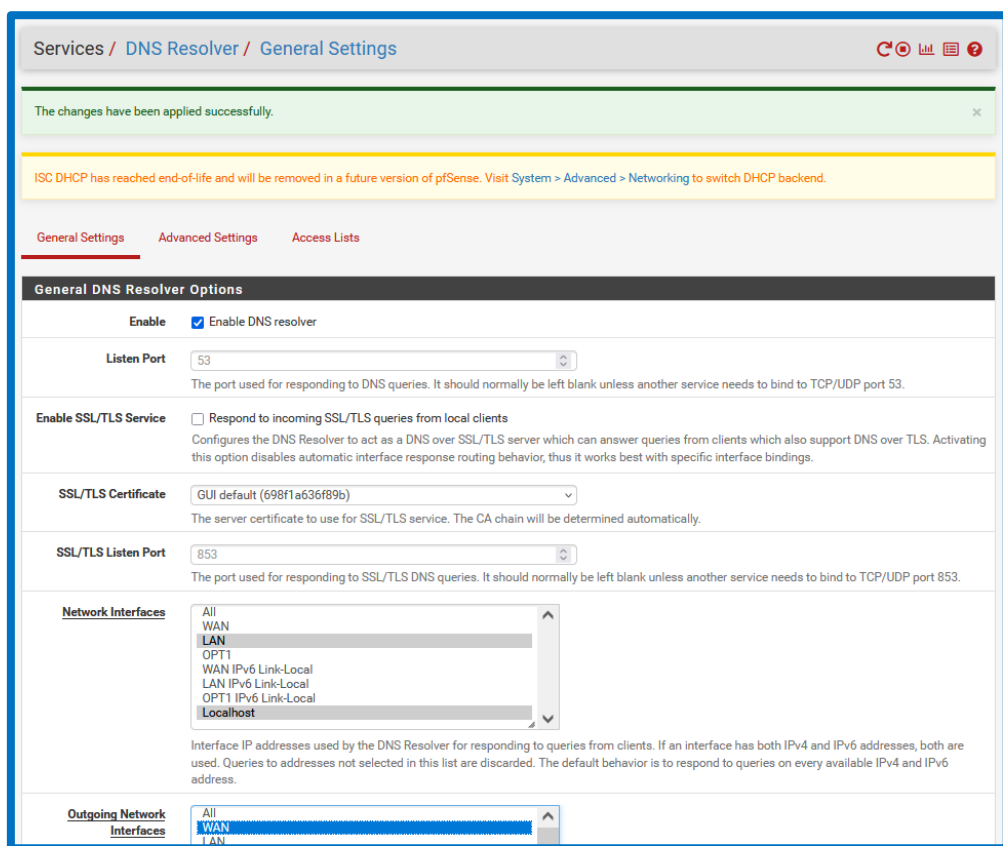
Do not end the domain name with '.local' as the final part (Top Level Domain, TLD). The 'local' TLD is widely used by mDNS (e.g. Avahi, Bonjour, Rendezvous, Airprint, Airplay) and some Windows systems and networked devices. These will not network correctly if the router uses 'local' as its TLD. Alternatives such as 'home.arpa', 'local.lan', or 'mylocal' are safe.

5.4.1 Activar “DNS Resolver” y justificación de interfaces de red

En esta pantalla se valida la configuración del servicio DNS Resolver para que actúe como “DNS Resolver” interno, evitando así que cada cliente resuelva nombres con un DNS no corporativo.

De este modo, se mantiene habilitado el servicio y se confirma el puerto 53, que es el estándar para consultas DNS, de forma que cualquier equipo de las redes internas pueda consultar.

Entonces, en el apartado Network Interfaces se seleccionan LAN y Localhost por un motivo funcional y de seguridad. Al incluir LAN, se garantiza que el DNS Resolver escuche y responda consultas desde la red de tránsito interna donde llegan las redes de usuarios (las VLANs que cuelgan de R1 terminan alcanzando pfSense por el enlace hacia LAN).



Dicho de otro modo, si el resolver no escucha en LAN, los clientes no podrían utilizar pfSense como DNS y se perdería la base del “DNS Enforcement”. Por su parte, Localhost se mantiene seleccionado porque el propio pfSense también necesita resolver nombres para tareas internas y de mantenimiento, como comprobar actualizaciones, resolver hostnames configurados, validar servicios, o incluso permitir que componentes locales consulten DNS sin depender de que la interfaz LAN esté operativa.

A continuación, en el apartado Outgoing Network Interfaces se marca WAN para forzar que las consultas salgan únicamente por la interfaz de salida a Internet.

5.4.2 Cambiamos el DNS por defecto a los clientes

Ejecutamos el contenido del script 2_R1_DNS_is_PFSENSE.txt en R1 para que los DNS pasen de ser 8.8.8.8 a 10.0.0.1 (DNS Resolver de PFSENSE en la tarjeta LAN).

Obviamente, al recibir los Debian sus IPs a través de DHCP, en esos clientes deberemos solicitar los últimos cambios de DHCP de R1 con el comando `dhclient -r` y `dhclient -v` para tener el cambio de DNS. De hecho, si ejecutamos “`cat /etc/resolv.conf`” una vez renovadas las IPs por DHCP. El DNS de estos equipos pasará a ser 10.0.0.1.

```
debian@clienteA:~$ sudo dhclient -r
Killed old client process
debian@clienteA:~$ sudo dhclient -v
Internet Systems Consortium DHCP Client 4.4.3-P1
Copyright 2004-2022 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/ens4/0c:36:ae:33:00:00
Sending on   LPF/ens4/0c:36:ae:33:00:00
Sending on   Socket/fallback
DHCPDISCOVER on ens4 to 255.255.255.255 port 67 interval 6
DHCPOFFER of 192.168.10.21 from 192.168.10.1
DHCPREQUEST for 192.168.10.21 on ens4 to 255.255.255.255 port 67
DHCPACK of 192.168.10.21 from 192.168.10.1
bound to 192.168.10.21 -- renewal in 40587 seconds.
debian@clienteA:~$ cat /etc/resolv.conf | grep -i nameserver
# run "resolvectl status" to see details about the actual nameservers.
nameserver 10.0.0.1
debian@clienteA:~$
```

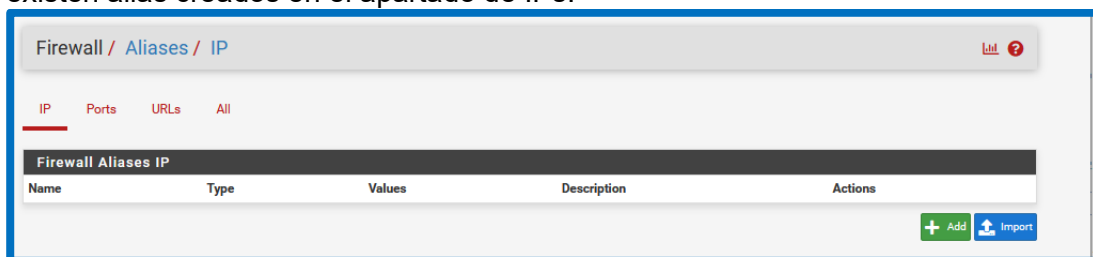
```
debian@clienteB:~$ sudo dhclient -r
Killed old client process
debian@clienteB:~$ sudo dhclient -v
Internet Systems Consortium DHCP Client 4.4.3-P1
Copyright 2004-2022 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/ens4/0c:12:15:36:00:00
Sending on   LPF/ens4/0c:12:15:36:00:00
Sending on   Socket/fallback
DHCPDISCOVER on ens4 to 255.255.255.255 port 67 interval 8
DHCPOFFER of 192.168.11.21 from 192.168.11.1
DHCPREQUEST for 192.168.11.21 on ens4 to 255.255.255.255 port 67
DHCPACK of 192.168.11.21 from 192.168.11.1
bound to 192.168.11.21 -- renewal in 40305 seconds.
debian@clienteB:~$ cat /etc/resolv.conf
# Dynamic resolv.conf(5) file for glibc resolver(3) generated by resolvconf(8)
# DO NOT EDIT THIS FILE BY HAND -- YOUR CHANGES WILL BE OVERWRITTEN
# 127.0.0.53 is the systemd-resolved stub resolver.
# run "resolvectl status" to see details about the actual nameservers.

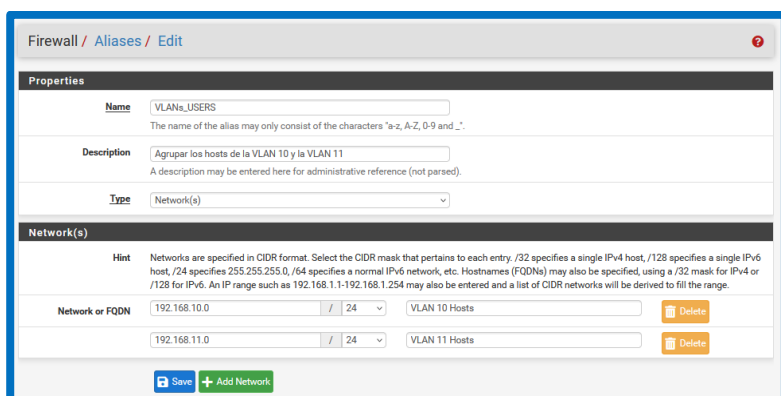
nameserver 10.0.0.1
search lab.local
debian@clienteB:~$
```

5.4.3 Creación del alias de redes internas (VLAN 10 y VLAN 11)

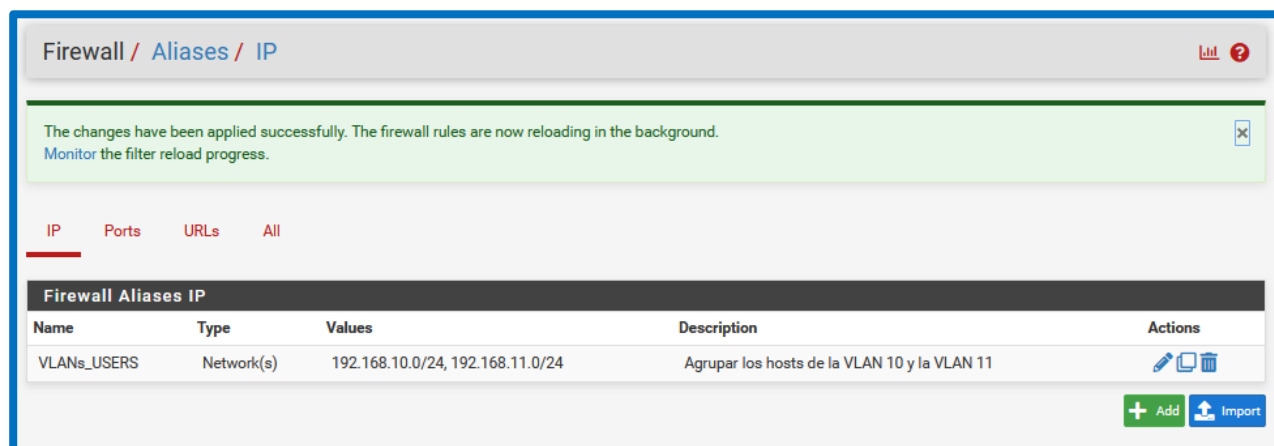
A continuación, se prepara un alias que agrupe las redes de usuarios que van a compartir políticas comunes (por ejemplo, reglas de acceso a Internet, restricciones DNS o trazabilidad). Para ello se accede a la sección de Aliases en el firewall y se verifica el punto de partida, donde todavía no existen alias creados en el apartado de IPs.



Con el formulario de creación/edición se define el alias con un nombre representativo y una descripción administrativa que explica su propósito. Se selecciona el tipo “Network(s)” para poder incluir subredes completas y se añaden explícitamente las dos redes del laboratorio asociadas a los usuarios, identificándolas como VLAN 10 y VLAN 11. De este modo, el alias queda preparado para ser usado como “origen” o “conjunto de redes” en reglas de firewall y NAT, reduciendo duplicidades y evitando errores por repetición manual de subredes.

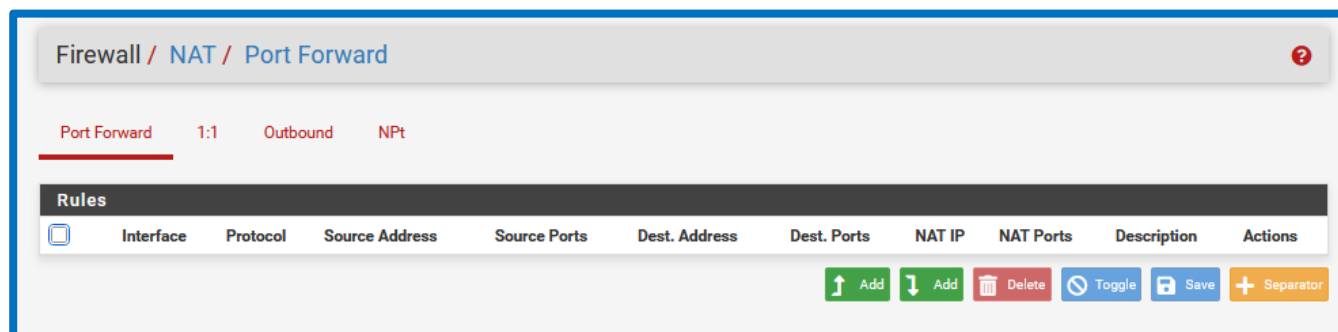


Finalmente se observa el alias ya creado en el listado (VLANs users), mostrando las dos redes incluidas y la descripción definida. En este punto pfSense confirma la aplicación correcta de cambios y la recarga del conjunto de reglas en segundo plano, lo que deja el sistema listo para continuar con la parte operativa de esta sección: aplicar Manual Outbound NAT y reglas de DNS Enforcement apoyándose en el alias para que el control sea consistente en VLAN 10 y VLAN 11.



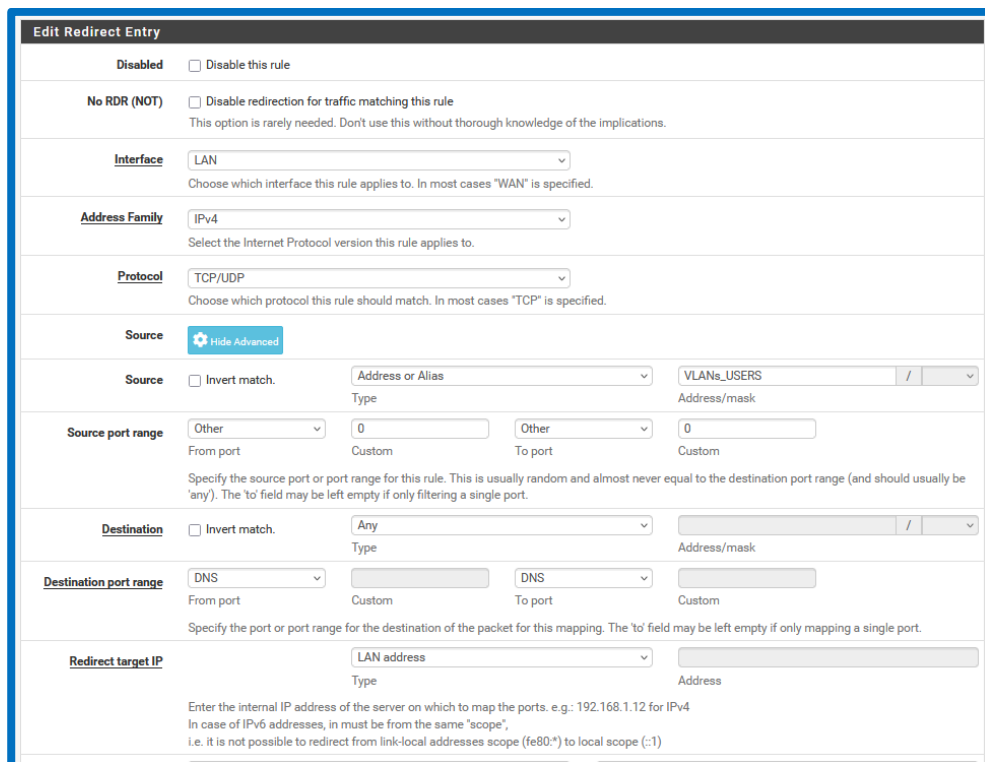
5.4.4 DNS Enforcement mediante NAT Port Forward interno

En el apartado de pfSense en Firewall / NAT / Port Forward, usaremos el mecanismo de reenvío de puertos para forzar el uso del DNS corporativo de manera interna en la LAN. En otras palabras, no se está abriendo nada desde el exterior, sino redirigiendo tráfico DNS que nace en las VLAN de usuarios para que no pueda “saltarse” el resolutor del firewall.



A continuación, crearemos una regla de redirección (Edit Redirect Entry) con los parámetros clave.

Para ello, seleccionaremos la interfaz LAN porque es el punto por el que pfSense recibe el tráfico procedente de las redes de usuarios que cuelgan de R1 (VLAN 10 y VLAN 11) y que llegan al firewall a través del enlace de tránsito. Luego, fijaremos el Address Family en IPv4 para aplicar la medida a las redes IPv4 del escenario. Después, se define el protocolo como TCP/UDP porque DNS opera principalmente por UDP/53, y finalmente: mencionaremos como alias a VLANs_USERS.



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

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

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

Source

Source ☐ Invert match. /
Type Address/mask

Source port range
From port Custom To port Custom
Specify the source port or port range for this rule. This is usually random and almost never equal to the destination port range (and should usually be 'any'). The 'to' field may be left empty if only filtering a single port.

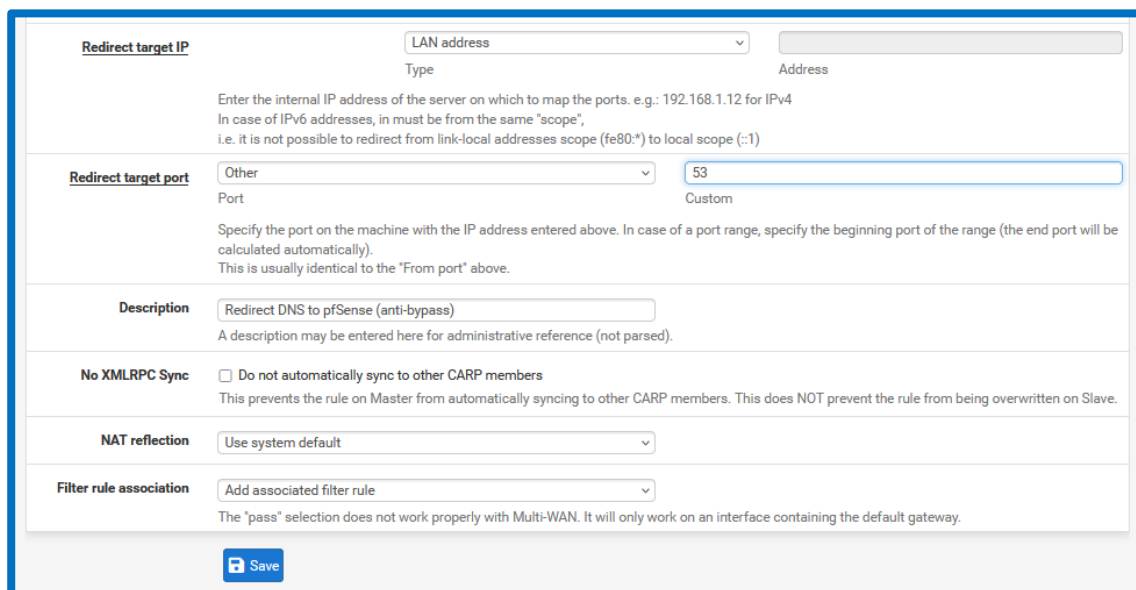
Destination ☐ Invert match. /
Type Address/mask

Destination port range
From port Custom To port Custom
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 single port.

Redirect target IP
Type Address
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4
In case of IPv6 addresses, it must be from the same "scope",
i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)

Después, el destino se deja en Any, y el Destination port range se fija a DNS (53). Esto es precisamente lo que permite el “anti-bypass”: aunque un cliente configure manualmente 8.8.8.8, 1.1.1.1 u otro servidor DNS externo, cualquier intento de consultar por el puerto 53 seguirá coincidiendo con la regla y se interceptará. Luego, el Redirect target IP se establece como LAN address porque el objetivo es que el propio pfSense actúe como destino final del DNS, centralizando resolución, trazabilidad y políticas.

Seguidamente, el Redirect target port se fija en 53 para que la consulta termine realmente en el servicio DNS local del firewall. La descripción “Redirect DNS to pfSense (anti-bypass)” documenta la intención operativa: no es una redirección para publicar un servicio, sino una medida de cumplimiento para impedir el uso de DNS no autorizado.



Redirect target IP
Type Address
Enter the internal IP address of the server on which to map the ports. e.g.: 192.168.1.12 for IPv4
In case of IPv6 addresses, it must be from the same "scope",
i.e. it is not possible to redirect from link-local addresses scope (fe80:*) to local scope (::1)

Redirect target port
Port Custom
Specify the port on the machine with the IP address entered above. In case of a port range, specify the beginning port of the range (the end port will be calculated automatically).
This is usually identical to the "From port" above.

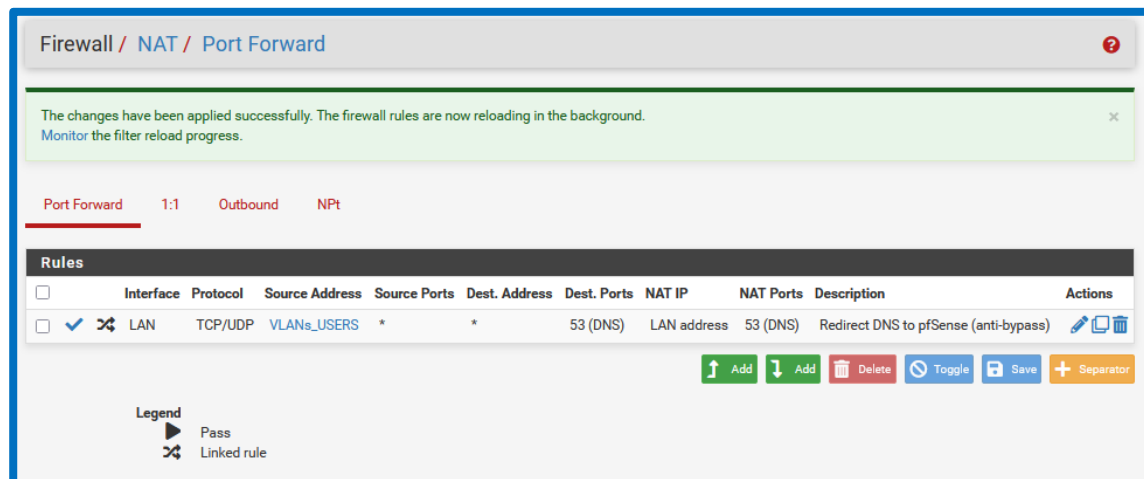
Description
A description may be entered here for administrative reference (not parsed).

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 from being overwritten on Slave.

NAT reflection

Filter rule association
The "pass" selection does not work properly with Multi-WAN. It will only work on an interface containing the default gateway.

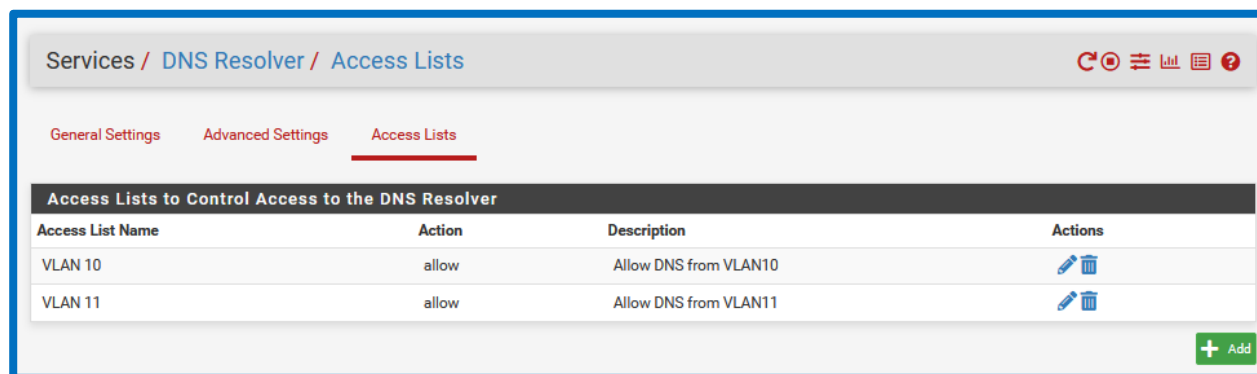
Finalmente, la regla queda creada en la tabla de Port Forward, aplicando a la interfaz LAN, protocolo TCP/UDP, con origen VLANs_USERS y destino DNS (53), redirigido al propio firewall (LAN address:53). Con esto se fuerza que las VLAN de usuarios resuelvan nombres a través de pfSense, lo que ayuda a reducir riesgos de DNS hijacking por cambios de DNS en el cliente.



5.4.1 Control de acceso al DNS Resolver con Access Lists por VLAN

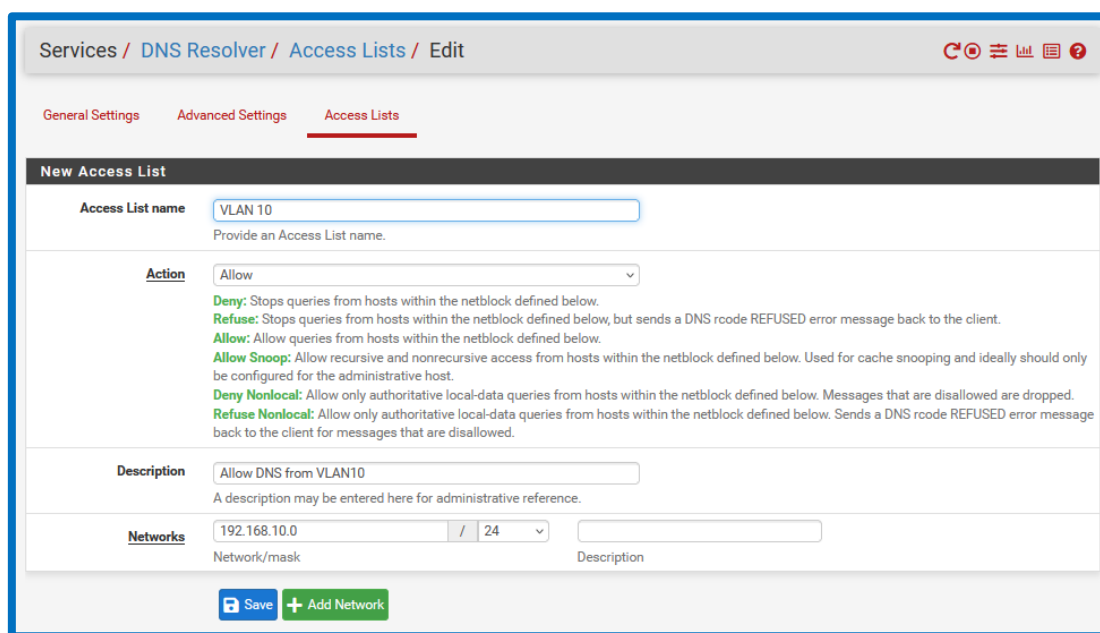
Para añadir ACLs al DNS Resolver, y permitir así que nuestros clientes estén forzados a usar nuestro DNS (10.0.0.1) vamos al menú Services / DNS Resolver / Access Lists con dos listas definidas: VLAN 10 y VLAN 11, ambas con acción allow.

De hecho, estas listas son necesarias para complementar el enforcement anterior con un control explícito de quién puede usar el resolutor de pfSense. Por eso mismo, la redirección NAT enruta las consultas al firewall, y resta a la espera que las ACL dicten qué redes están autorizadas a obtener respuesta del DNS Resolver, y cuales no.



Si queremos crear una Access List para VLAN 10: se define un nombre identificativo (VLAN 10), la acción Allow y se asocia la red 192.168.10.0/24. De hecho, esta granularidad por VLAN aporta control y claridad: permitiendo así aplicar políticas diferenciadas si más adelante se desea, facilita el diagnóstico (porque se define qué segmento está autorizado) y evita sobredimensionar permisos.

Luego, la misma lógica se replica para VLAN 11 con su red correspondiente (192.168.11.0/24), de forma que únicamente los hosts de VLAN 10 y VLAN 11 queden habilitados para resolver DNS a través de pfSense, manteniendo el servicio acotado a los clientes previstos y reforzando el objetivo de evitar bypass y manipulación de DNS desde los endpoints.



The screenshot shows the 'New Access List' configuration page in pfSense. The breadcrumb trail is 'Services / DNS Resolver / Access Lists / Edit'. There are three tabs: 'General Settings', 'Advanced Settings', and 'Access Lists' (which is selected). The form includes:

- Access List name:** A text field containing 'VLAN 10'.
- Action:** A dropdown menu set to 'Allow'. Below it, a list of actions with descriptions: 'Deny', 'Refuse', 'Allow', 'Allow Snoop', 'Deny Nonlocal', and 'Refuse Nonlocal'.
- Description:** A text field containing 'Allow DNS from VLAN10'.
- Networks:** A section with a text field containing '192.168.10.0', a dropdown for '24', and a 'Description' field.

At the bottom, there are 'Save' and '+ Add Network' buttons.

5.4.2 Prueba desde el cliente (forzando DNS externo y DNS corporativo)

En esta primera captura se valida el comportamiento de resolución DNS desde el equipo clienteA forzando explícitamente dos servidores distintos. En primer lugar se ejecuta la resolución con host google.com 8.8.8.8, es decir, intentando usar un DNS público (no corporativo). A continuación se repite la prueba con host google.com 10.0.0.1, que corresponde al DNS corporativo gestionado por pfSense.

El objetivo de esta comprobación es demostrar que un usuario puede intentar utilizar manualmente un DNS externo, pero que la infraestructura está preparada para impedir que ese DNS externo sea el que realmente determine la resolución final. Esta prueba sirve como “intento de bypass” controlado, previo a la verificación en pfSense.

```
debian@clienteA:~$ host google.com 8.8.8.8
Using domain server:
Name: 8.8.8.8
Address: 8.8.8.8#53
Aliases:

google.com has address 142.250.200.110
google.com has IPv6 address 2a00:1450:4003:80e::200e
google.com mail is handled by 10 smtp.google.com.
debian@clienteA:~$ host google.com 10.0.0.1
Using domain server:
Name: 10.0.0.1
Address: 10.0.0.1#53
Aliases:

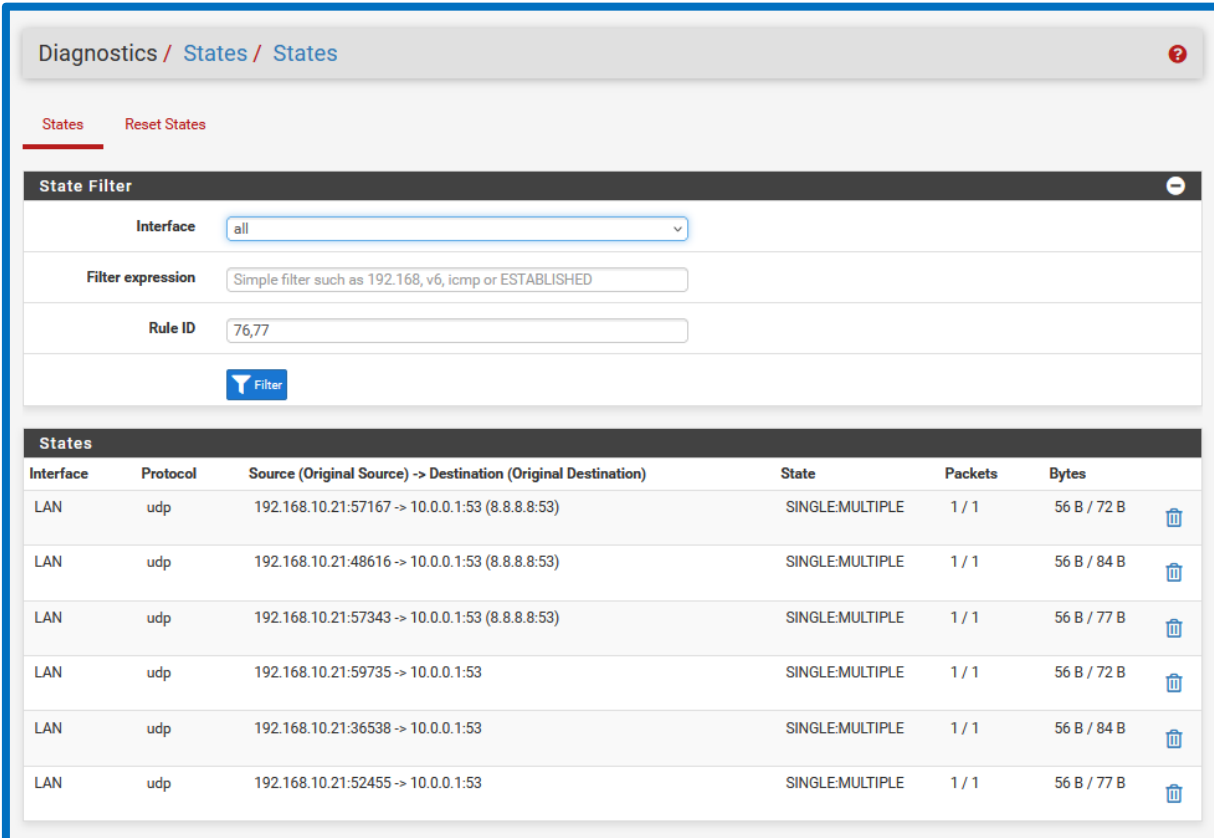
google.com has address 142.250.200.110
google.com has IPv6 address 2a00:1450:4003:80e::200e
google.com mail is handled by 10 smtp.google.com.
debian@clienteA:~$
```

5.4.3 Evidencia en pfSense: confirmación del DNS realmente utilizado

En esta segunda captura se comprueba el resultado real desde pfSense consultando el apartado Diagnostics / States. En la tabla de estados se observa que el tráfico DNS del cliente termina efectivamente contra 10.0.0.1:53, lo que indica que la resolución se está gestionando por el DNS corporativo alojado en el firewall.

Además, en esos mismos estados se muestra el destino original que el cliente intentó usar entre paréntesis, por ejemplo (8.8.8.8:53). Esto es clave porque evidencia que el cliente intentó enviar la consulta a un DNS público, pero pfSense interceptó esa petición y la redirigió hacia 10.0.0.1:53, evitando así el bypass y aplicando la política corporativa de DNS.

En otras palabras: aunque la petición “salga” del cliente apuntando a un DNS externo, el flujo queda forzado para que el resolovedor real sea el corporativo.



The screenshot shows the pfSense web interface for the 'States' tab. It includes a 'State Filter' section with fields for 'Interface' (set to 'all'), 'Filter expression' (with a hint: 'Simple filter such as 192.168, v6, icmp or ESTABLISHED'), and 'Rule ID' (set to '76,77'). Below the filter is a 'Filter' button. The main part of the image is a table titled 'States' with the following columns: Interface, Protocol, Source (Original Source) -> Destination (Original Destination), State, Packets, and Bytes. The table contains six rows of data, all showing UDP traffic on the LAN interface from various source IPs to 10.0.0.1:53, with the original destination in parentheses. Each row also shows '1 / 1' packets and a specific byte count, and has a trash icon for deletion.

Interface	Protocol	Source (Original Source) -> Destination (Original Destination)	State	Packets	Bytes
LAN	udp	192.168.10.21:57167 -> 10.0.0.1:53 (8.8.8.8:53)	SINGLE:MULTIPLE	1 / 1	56 B / 72 B
LAN	udp	192.168.10.21:48616 -> 10.0.0.1:53 (8.8.8.8:53)	SINGLE:MULTIPLE	1 / 1	56 B / 84 B
LAN	udp	192.168.10.21:57343 -> 10.0.0.1:53 (8.8.8.8:53)	SINGLE:MULTIPLE	1 / 1	56 B / 77 B
LAN	udp	192.168.10.21:59735 -> 10.0.0.1:53	SINGLE:MULTIPLE	1 / 1	56 B / 72 B
LAN	udp	192.168.10.21:36538 -> 10.0.0.1:53	SINGLE:MULTIPLE	1 / 1	56 B / 84 B
LAN	udp	192.168.10.21:52455 -> 10.0.0.1:53	SINGLE:MULTIPLE	1 / 1	56 B / 77 B

5.4.4 Normativas en Firewall LAN que permiten el control y justifican el diseño

Las reglas aplicadas en Firewall / Rules / LAN son las responsables de implementar el control de DNS y, además, limitar los accesos de administración y habilitar diagnósticos mínimos. A continuación, se justifica la creación de cada normativa utilizando la descripción visible en la captura.

5.4.4.1 1ra normativa: DNS Whitelist

En primer lugar aparece la regla “DNS whitelist: permitir consultas DNS solo a pfSense (10.0.0.1:53)”. Esta normativa se crea para centralizar la resolución DNS en un único punto controlado (pfSense), garantizando que los clientes de las VLAN no dependan de resolutores arbitrarios.

Esta centralización permite aplicar políticas corporativas (registro, filtrado, control de seguridad) desde el firewall y simplifica el monitoreo.

5.4.4.2 2nda normativa: SSH administración -> Solo 192.168.10.21/24

A continuación se observa la regla “SSH administración: solo PC10 (192.168.10.21) puede acceder por SSH a pfSense (10.0.0.1:22)”. Esta normativa existe para restringir la administración remota del firewall únicamente al host autorizado, evitando que otros dispositivos de la red interna puedan intentar conexiones SSH. Con ello se reduce la superficie de ataque y se aplica el principio de mínimo privilegio: solo el equipo designado para administración puede acceder.

5.4.4.1 3ra normativa: Excepción: R1 permitir ICMP desde R1 (10.0.0.2) hacia Internet

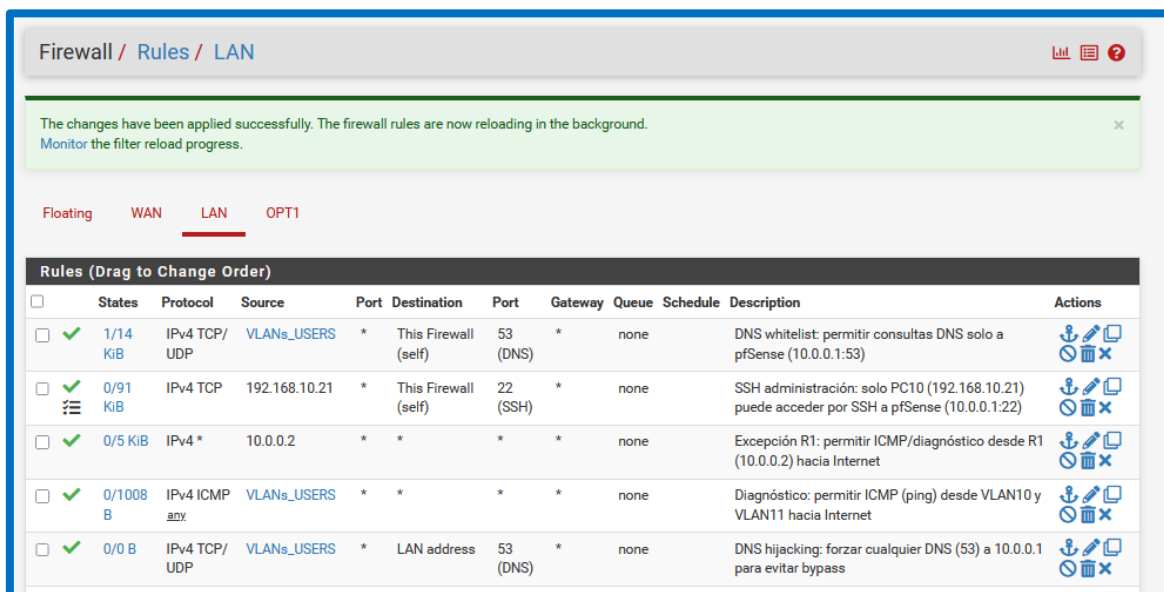
Después se incluye la regla “**Excepción R1: permitir ICMP/diagnóstico desde R1 (10.0.0.2) hacia Internet**”. Esta excepción se justifica porque R1 puede necesitar comprobaciones operativas de conectividad (por ejemplo, verificaciones de tránsito o troubleshooting) sin tener que abrir permisos de diagnóstico para toda la red.

5.4.4.1 4rta normativa: Diagnóstico: R1: Permitir ICMP desde VLAN10 y 11 hacia Internet

Seguidamente aparece la regla “Diagnóstico: permitir ICMP (ping) desde VLAN10 y VLAN11 hacia Internet”. Esta normativa se utiliza para permitir pruebas básicas de conectividad desde los clientes (latencia, reachability) sin habilitar otros protocolos más amplios. Permitir ICMP controlado facilita el diagnóstico sin comprometer la política del firewall.

5.4.4.2 5na normativa: DNS Hijacking: forzar DNS a 10.0.0.1

Finalmente se muestra la regla “**DNS Hijacking: forzar cualquier DNS (53) a 10.0.0.1 para evitar bypass**”. Esta es la normativa que garantiza el DNS Enforcement. Su función es que cualquier intento de usar DNS externos por el puerto 53 quede redirigido hacia el DNS corporativo (10.0.0.1). La prueba queda respaldada por la captura de **States**, donde se aprecia que el usuario intentó resolver contra **(8.8.8.8:53)**, pero el estado real termina en **10.0.0.1:53**, confirmando que el bypass no se produce aunque el cliente lo intente.



Rules (Drag to Change Order)	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 1/14 KiB	IPv4 TCP/UDP	VLANs_USERS	*	This Firewall (self)	53 (DNS)	*	none		DNS whitelist: permitir consultas DNS solo a pfSense (10.0.0.1:53)	
<input type="checkbox"/>	✓ 0/91 KiB	IPv4 TCP	192.168.10.21	*	This Firewall (self)	22 (SSH)	*	none		SSH administración: solo PC10 (192.168.10.21) puede acceder por SSH a pfSense (10.0.0.1:22)	
<input type="checkbox"/>	✓ 0/5 KiB	IPv4 *	10.0.0.2	*	*	*	*	none		Excepción R1: permitir ICMP/diagnóstico desde R1 (10.0.0.2) hacia Internet	
<input type="checkbox"/>	✓ 0/1008 B	IPv4 ICMP any	VLANs_USERS	*	*	*	*	none		Diagnóstico: permitir ICMP (ping) desde VLAN10 y VLAN11 hacia Internet	
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP/UDP	VLANs_USERS	*	LAN address	53 (DNS)	*	none		DNS hijacking: forzar cualquier DNS (53) a 10.0.0.1 para evitar bypass	