

Laboratorio: Firewall Corporativo pfSense

Estudiante: Mauricio Teliz Duche

Objetivo principal del laboratorio:

Implementaremos un firewall corporativo con pfSense en un entorno virtualizado, abarcando desde su instalación y configuración inicial hasta la puesta en marcha de servicios críticos de red DHCP, DNS Resolver/Forwarder, NAT, reglas de firewall y segmentación de interfaces.

Habilitaremos mecanismos de control y filtrado de tráfico (proxy, listas de control de acceso, redirecciones y políticas de seguridad), configuraremos el monitoreo y análisis de logs para registrar y supervisar el tráfico de red, incluyendo la simulación de ataques controlados y la verificación de la efectividad de las reglas y mecanismos de filtrado, buscando establecer una infraestructura segura, funcional y auditable que sirva como base para prácticas avanzadas de ciberseguridad, monitoreo y defensa de redes.

Sección A – Preparación e instalación

Objetivo: Configurar la máquina virtual, instalar pfSense y preparar las interfaces WAN y LAN para el laboratorio, asegurando que la red de pruebas esté aislada y preparada para tráfico controlado.

1. Descarga del ISO

Acciones realizadas paso a paso:

- Accedemos al sitio oficial de Netgate: <https://www.pfsense.org/download/>
- Seleccionamos: Architecture: AMD64 ISO IPMI/VIRTUAL machines

Installer: ISO

Platform: VMware/Virtual Machines

Version: 2.8.1

Guardamos el archivo ISO en nuestro equipo local.

Notas: - Archivo ISO: pfSense-CE-2.8.1-AMD64.iso - Compatible con VMware y VirtualBox.

2. Creación de la VM

- Abrimos VMware y seleccionamos Create New Virtual Machine.
- Seleccionamos la ISO pfSense-CE-2.8.1-AMD64.iso que guardamos en nuestro equipo local.
- Configuramos manualmente sus recursos:

CPU: 2 núcleos

RAM: 4GB

Disco: 20GB (Dinámico)

Notas: - Disco dinámico permite flexibilidad en pruebas.

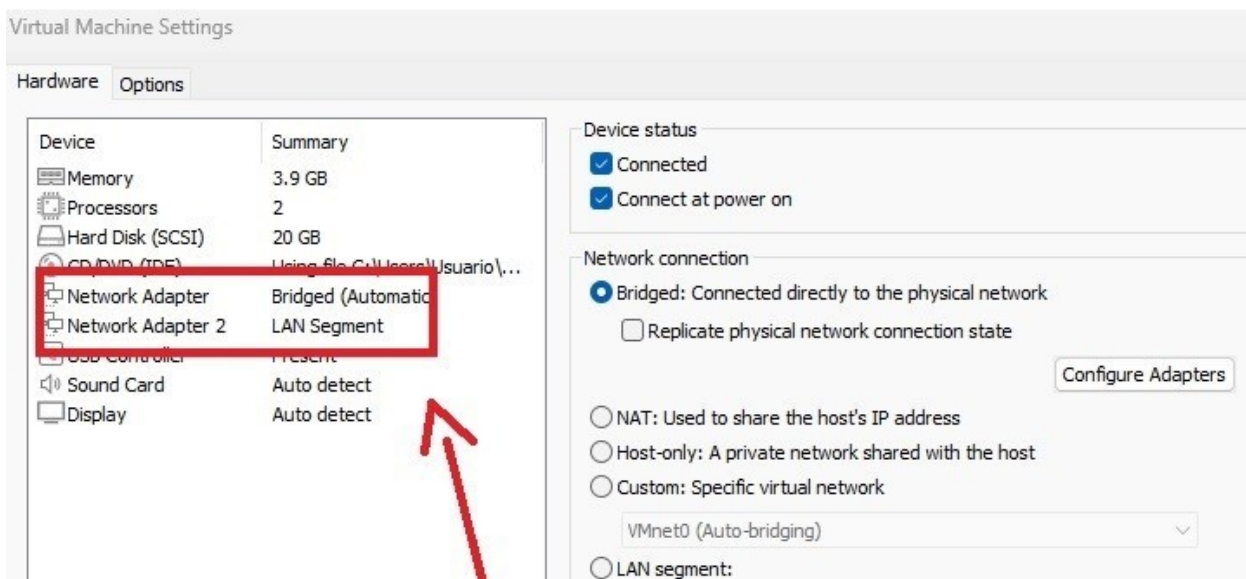
3. Configuraciones de adaptadores de red

Asignamos adaptadores en la VM:

- Adapter 1 (WAN): Bridged (conexión a red física / Internet)

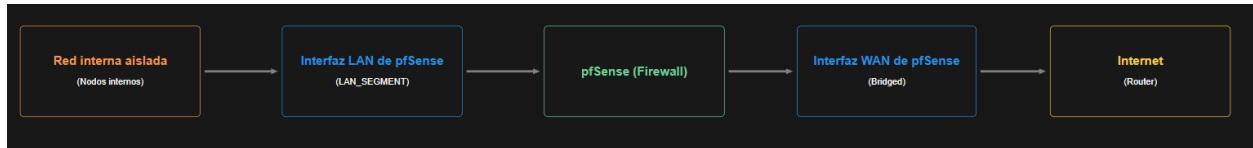
Se desactiva la opción Replicate physical network connection state para garantizar una conectividad estable en el laboratorio.

- Adapter 2 (LAN): LAN Segment (LAN_LAB) para nuestra red interna aislada.



A continuación se presenta un diagrama conceptual que representa el trayecto del tráfico de red desde los nodos internos hasta internet a través del Firewall pfSense.

Diagrama conceptual:



4. Instalación de pfSense

- Iniciamos la VM desde la ISO de pfSense
- Asignamos interfaces WAN y LAN según plan anterior.

Configuramos:

WAN: DHCP → 192.168.1.180/24

LAN: Estática → 192.168.190.1/24

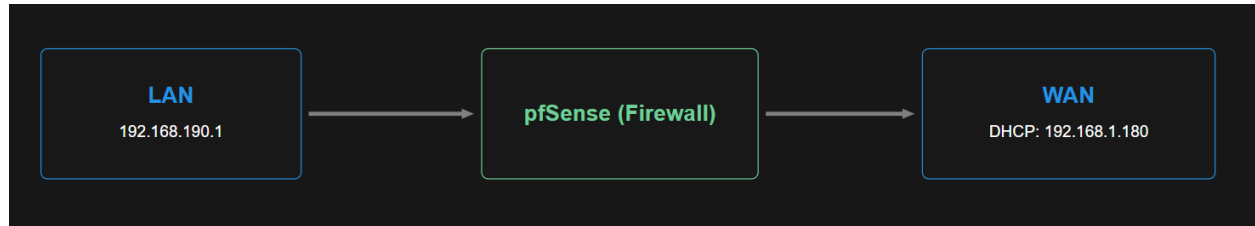
Decidí no habilitar DHCP en LAN para control manual de IPs de clientes.

```
*** Welcome to pfSense 2.8.1-RELEASE (amd64) on pfSense ***

WAN (wan) -> em0 -> v4/DHCP4: 192.168.1.180/24
LAN (lan) -> em1 -> v4: 192.168.190.1/24

0) Logout / Disconnect SSH          9) pfTop
1) Assign Interfaces                10) Filter Logs
2) Set interface(s) IP address     11) Restart GUI
3) Reset admin account and 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
```

Diagrama conceptual de las interfaces establecidas:



Notas: - Preparado para conectividad interna y pruebas de seguridad.

Sección B – Configuración de servicios y reglas de firewall

Objetivo: Verificar la conectividad desde pfSense a internet y desde clientes LAN, comprobando rutas y configuración de red. Vamos a garantizar que la infraestructura básica esté operativa antes de aplicar reglas de firewall o NAT.

1. Verificación desde pfSense

Desde la shell de pfSense:

- Abrimos la shell de pfSense (consola de la VM).

Comandos ejecutados:

ping 8.8.8.8 # Verificar conectividad a Internet

ping www.google.com # Verificar resolución de DNS

ifconfig # Comprobar que la WAN recibió IP correctamente

Respuesta exitosa de los pings:

- **ping 8.8.8.8** (Verificar conectividad a Internet)

```
[2.8.1-RELEASE][root@pfSense.home.arpal]/root: ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=115 time=22.812 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=115 time=23.250 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=115 time=22.297 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=115 time=23.814 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=115 time=22.843 ms
^C
--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 22.297/23.003/23.814/0.506 ms
```

- ping **www.google.com** (Verificar resolución de DNS)

```
[2.8.1-RELEASE][root@pfSense.home.arpal]/root: ping www.google.com
PING www.google.com (142.251.134.68): 56 data bytes
64 bytes from 142.251.134.68: icmp_seq=0 ttl=116 time=22.366 ms
64 bytes from 142.251.134.68: icmp_seq=1 ttl=116 time=22.362 ms
64 bytes from 142.251.134.68: icmp_seq=2 ttl=116 time=23.423 ms
64 bytes from 142.251.134.68: icmp_seq=3 ttl=116 time=22.540 ms
^C
--- www.google.com ping statistics ---
4 packets transmitted, 4 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 22.362/22.673/23.423/0.439 ms
```

- **ifconfig em0** (Comprobar que la WAN recibió IP correctamente)

```
[2.8.1-RELEASE][root@pfSense.home.arpal]/root: ifconfig em0
em0: flags=1008843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST,LOWER_UP> metric 0 mtu
1500
options=4e100bb<RXCSUM,TXCSUM,VLAN_MTU,VLAN_HWTAGGING,JUMBO_MTU,VLAN_HW
SUM,VLAN_HWFILTER,RXCSUM_IPV6,TXCSUM_IPV6,HWSTATS,MEXTPG>
ether 00:0c:29:a9:f4:5e
→ inet 192.168.1.180 netmask 0xfffff00 broadcast 192.168.1.255
inet6 fe80::20c:29ff:fea9:f45e%em0 prefixlen 64 scopeid 0x1
media: Ethernet autoselect (1000baseT <full-duplex>)
status: active
nd6 options=21<PERFORMNUD,AUTO_LINKLOCAL>
```

- WAN con IP asignada correctamente.

2. Verificación desde clientes LAN

Cliente utilizado: Máquina virtual Kali Linux.

Configuración de red estática en Kali Linux (asignada al LAN_SEGMENT):

La máquina Kali Linux conectada al LAN_SEGMENT tiene la interfaz eth0 levantada pero sin IPv4 asignada. A continuación documentamos cómo asignarle una IP estática y configurar la puerta de enlace.

- Asignamos IP estática a eth0 (IPv4)
- Comando utilizado: **sudo ip addr add 192.168.190.10/24 dev eth0**

```

valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
link/ether 00:0c:29:40:99:e0 brd ff:ff:ff:ff:ff:ff
inet 192.168.190.10/24 scope global eth0
valid_lft forever preferred_lft forever

(mauricio@kali)-[~]
$

```

- Configuramos puerta de enlace (gateway) hacia pfSense LAN

Para que la máquina kali pueda comunicarse con redes fuera de su propia subred LAN, se configura la puerta de enlace (gateway) hacia la interfaz LAN del firewall pfSense, cuya IP es **192.168.190.1**. Todo el tráfico saliente desde Kali que no sea dirigido a la subred **192.168.190.0/24** se envía a esta puerta de enlace, de manera que pfSense pueda procesarlo y según sus reglas, decidir si lo entrega a otra máquina de la LAN o hacia la red WAN/Internet.

- Le asignamos la puerta de enlace gateway mediante el siguiente comando:

- Comando utilizado: **sudo ip route add default via 192.168.190.1**

```

(mauricio@kali)-[~]
$ sudo ip route add default via 192.168.190.1
[sudo] contraseña para mauricio:

(mauricio@kali)-[~]
$ ip route
default via 192.168.190.1 dev eth0
192.168.190.0/24 dev eth0 proto kernel scope link src 192.168.190.10

```

- Confirmamos que kali pueda comunicarse correctamente con pfSense mediante la puerta de enlace 192.168.190.1

- Comando utilizado: **ping 192.168.190.1**

```

(mauricio@kali)-[~]
$ ping 192.168.190.1
PING 192.168.190.1 (192.168.190.1) 56(84) bytes of data.
64 bytes from 192.168.190.1: icmp_seq=1 ttl=64 time=0.541 ms
64 bytes from 192.168.190.1: icmp_seq=2 ttl=64 time=0.307 ms
64 bytes from 192.168.190.1: icmp_seq=3 ttl=64 time=0.195 ms
64 bytes from 192.168.190.1: icmp_seq=4 ttl=64 time=0.371 ms
^C
— 192.168.190.1 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3074ms
rtt min/avg/max/mdev = 0.195/0.353/0.541/0.125 ms

```

- Comprobamos que kali tenga salida a internet mediante el firewall pfSense.

- Comando utilizado: **ping 8.8.8.8**

```
(mauricio@kali)-[~]
$ ping 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=114 time=19.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=114 time=19.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=114 time=19.6 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=114 time=19.3 ms
^C
— 8.8.8.8 ping statistics —
4 packets transmitted, 4 received, 0% packet loss, time 3007ms
rtt min/avg/max/mdev = 19.293/19.508/19.606/0.128 ms
```

Establecemos DNS permanente para la resolución de nombres de dominio, para ello editaremos el archivo de conexión /etc/NetworkManager/system-connections/'Wired connection 1' y le asignaremos manualmente las instrucciones para resolver un DNS dentro de nuestra dirección IPV4 para que sea persistente.

- Introducimos las siguientes instrucciones:

- Comandos utilizados:

sudo cat 'Wired connection 1'

```
(mauricio@kali)-[/etc/NetworkManager/system-connections]
$ sudo cat 'Wired connection 1'

[connection]
id=Wired connection 1
uuid=919be524-94ca-472f-b9e8-f5a7c858682d
type=802-3-ethernet

[802-3-ethernet]

[ipv4]
method=manual
address1=192.168.190.10/24,192.168.190.1
dns=8.8.8.8;8.8.4.4;

[ipv6]
method=auto
ip6-privacy=2
```

- Posteriormente le otorgamos permisos al archivo 'Wired connection 1' para evitar problemas de reconocimiento en NetworkManager.

Comandos utilizados:

sudo chmod 600 /etc/NetworkManager/system-connections/'Wired connection 1'

- Activamos la conexión de red 'Wired connection 1'

Comando:

sudo nmcli connection up 'Wired connection 1'

- Le indicamos a NetworkManager que vuelva a leer el archivo 'Wired connection 1' y aplique la configuración.

Comando:

sudo nmcli connection reload

- Probamos la resolución DNS de www.google.com

Comando:

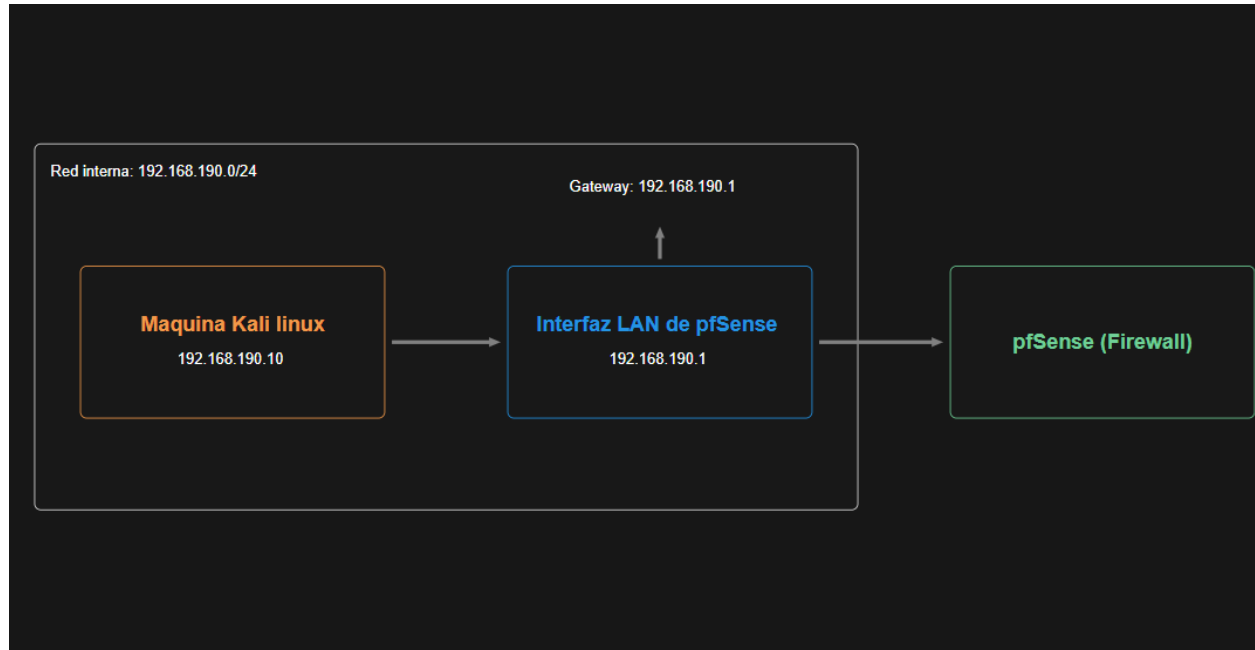
ping www.google.com

- Configuración DNS realizada con éxito.

```
(mauricio@kali)-[/etc/NetworkManager/system-connections]
$ ping www.google.com

PING www.google.com (142.251.129.36) 56(84) bytes of data.
64 bytes from tzezea-ad-in-f4.1e100.net (142.251.129.36): icmp_seq=1 ttl=115 time=19.0 ms
64 bytes from tzezea-ad-in-f4.1e100.net (142.251.129.36): icmp_seq=2 ttl=115 time=20.4 ms
64 bytes from tzezea-ad-in-f4.1e100.net (142.251.129.36): icmp_seq=3 ttl=115 time=19.5 ms
^C
— www.google.com ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 19.028/19.653/20.414/0.573 ms
```


Diagrama conceptual del área interna configurada:



Sección C – Configuración avanzada del firewall

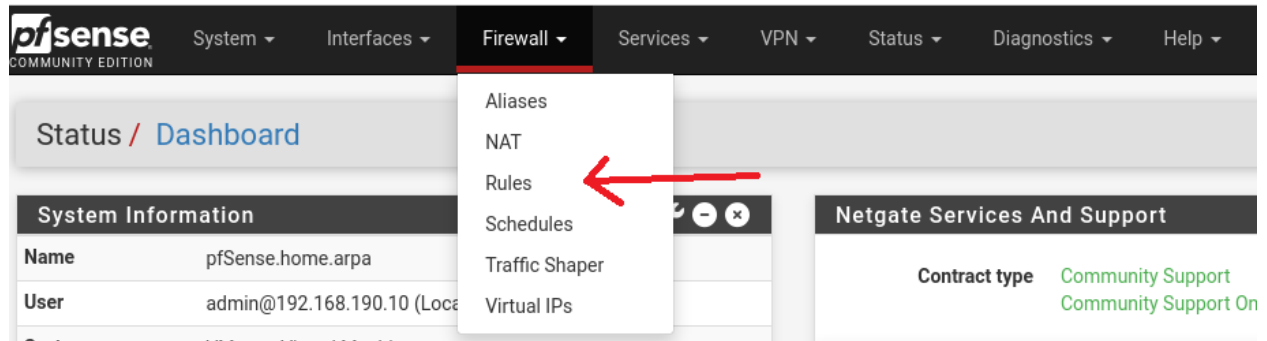
Objetivo: Crear reglas LAN→WAN y WAN→LAN en pfSense, definiendo qué tráfico se permite o bloquea, preparando el escenario para la simulación de ataques controlados y comprobar la efectividad de la defensa del firewall.

1. Accedemos a la interfaz de administración.

URL de acceso: <https://192.168.190.1>

Usuario: Admin

Navegamos a: Firewall → Rules para gestionar reglas por interfaz (LAN, WAN, etc.)



Asignación de reglas entrantes y salientes:

WAN → LAN (tráfico entrante)

Objetivo: Bloquear todo tráfico entrante no solicitado desde Internet.

- Configuración a documentar:

Action: Block

Interface: WAN

Address Family: Ipv4+IPv6

Protocol: Any

Source: Any

Destination: WAN address.

Logging: Marcar para auditar intentos.

Description: Bloquear todo tráfico entrante.

Resultados de la configuración:

- Escaneo de puertos desde VM atacante -> la mayoría de puertos filtrados.
- Intento de conexión a puerto no permitido -> bloqueado.
- Capturas y logs guardados como evidencia.

Bloqueamos tráfico entrante:

Firewall / **Rules** / WAN

Floating **WAN** LAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✗ 0/15 KiB	*	RFC 1918 networks	*	*	*	*	*		Block private networks	
	✗ 0/23 KiB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	
<input type="checkbox"/>	✗ 0/0 B	IPv4+6 *	*	*	WAN address	*	*	none		Bloquear todo tráfico entrante.	

Add Add Delete Toggle Copy Save Separator

LAN → WAN (tráfico saliente)

Objetivo: Permitir todo tráfico saliente a Internet.

- Configuración a documentar:

Action: Pass.

Interface: LAN.

Address Family: Ipv4+IPv6.

Protocol: Any.

Source: Any (Aplica a todas las redes internas, garantizando conectividad saliente a Internet para LAN y VLANs)

Destination: Any.

Logging: Marcar para auditar intentos.

Description: Permitir tráfico LAN a cualquier destino.

Resultados de la configuración:

- Los nodos de las redes internas y VLANs pueden navegar a Internet, hacer pings y usar servicios externos sin problemas.
- Logs muestran tráfico permitido para auditorías.

Permitimos tráfico saliente:

Firewall / Rules / LAN

Floating WAN LAN

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 0/607 KiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	⚙️
<input type="checkbox"/>	✓ 0/34 KiB	IPv4+6 *	LAN subnets	*	*	*	*	none		Permitir tráfico LAN a cualquier destino.	⚓ ✎ 📄 🗑 ✕
<input type="checkbox"/>	✓ 0/1.02 MiB	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

Sección D – NAT y VLANs

Objetivo: Explicaremos el funcionamiento de NAT (Network Address Translation) en pfSense, que permite a las máquinas internas de la LAN salir a Internet a través de la WAN de pfSense. Se menciona también la posibilidad de segmentar la red mediante VLANs para separar distintos servicios o departamentos.

Notas:

* En este laboratorio, la WAN de pfSense no tiene IP pública. Está detrás de un router que provee NAT.

* El tráfico de las VLANs no sale directamente a internet con la IP de pfSense, sino que el tráfico pasa primero por el NAT del router que se conecta a internet.

1. NAT automático (Outbound NAT)

Conceptos:

Outbound NAT: Convierte las direcciones privadas de la LAN en la dirección pública de la WAN al salir a Internet.

Automatic NAT: pfSense maneja la traducción automáticamente sin necesidad de reglas manuales.

Manual/Hybrid NAT: Permite crear reglas específicas para controlar qué hosts o subredes usan qué traducción de IP.

2. Revisión de reglas existentes

Ruta: Firewall → NAT → Outbound

Tipo: Automatic Outbound NAT (ya configurado por defecto):

Firewall / NAT / Outbound

Port Forward
1:1
Outbound
NPT

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)

Save

Mappings

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
<div> Add Add Delete Toggle Save </div>									

Automatic Rules

Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description
✓ WAN	127.0.0.0/8 ::1/128	192.168.190.0/24	*	*	500	WAN address	*	✓ Auto created rule for ISAKMP
✓ WAN	127.0.0.0/8 ::1/128	192.168.190.0/24	*	*	*	WAN address	*	✕ Auto created rule

- Traduce toda la LAN (192.168.190.0/24) a la IP de la WAN al salir a Internet.
- No se crean reglas manuales en este laboratorio, usamos la NAT automática existente.
- Las máquinas de la LAN pueden acceder a recursos fuera de la LAN, sin necesidad de asignar reglas de NAT manuales.

3. VLANS

Objetivo: Explicaremos cómo se pueden segmentar redes internas mediante VLANs en pfSense, creando redes lógicas independientes para distintos servicios o departamentos, y cómo estas VLANs se pueden integrar con la NAT automática.

¿Qué es una VLAN?

VLAN (Virtual LAN): Permite segmentar la misma red en múltiples redes lógicas. Es una segmentación de una red virtual en mas subredes, permitiéndole aplicar a cada una diferentes reglas en función de su contexto.

- Cada VLAN tiene un **ID único** y un **rango de direcciones IP propio**.

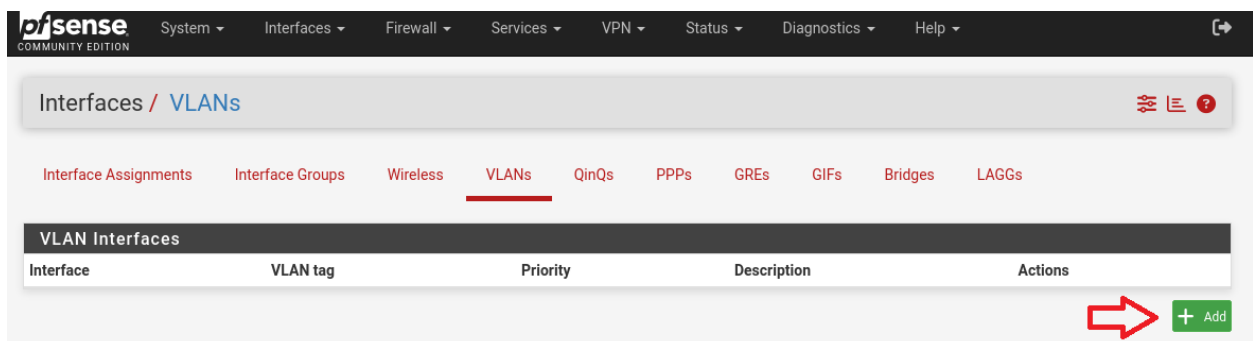
- Ventajas de usar VLANs:

- * Seguridad: aislamiento de tráfico sensible.
- * Organización: separar departamentos o servicios.
- * Control de firewall: reglas específicas por VLAN.

Ejemplo práctico:

Configuración de VLANs en pfSense:

Ruta: Interfaces → Assignments → VLANs → Add



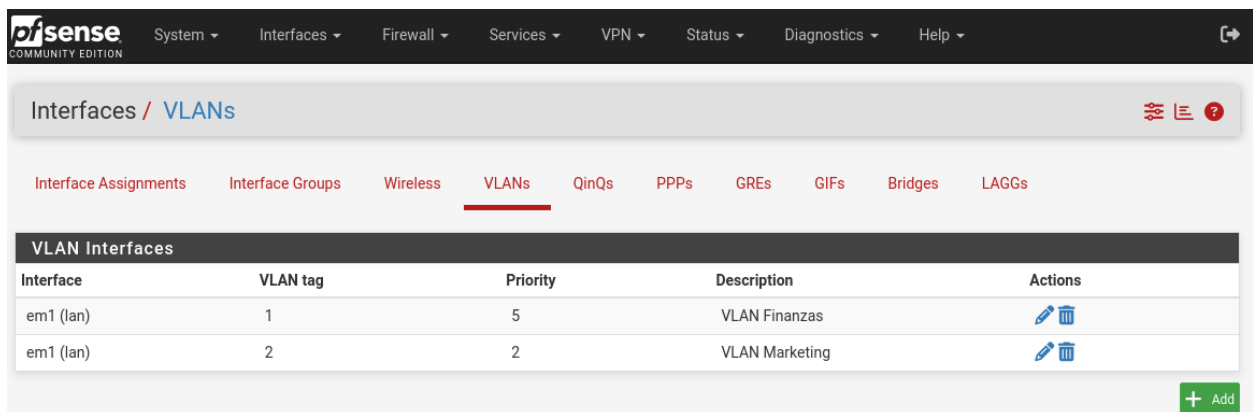
Campos a configurar:

Parent Interface: La interfaz sobre la que se crea la VLAN.





VLAN Tag: Identificador único de cada VLAN.

VLAN Priority: Es un valor de prioridad de tráfico definido en cada paquete de la VLAN, permite dar preferencia a ciertos tipos de tráfico dentro de una red, útil para servicios que necesitan baja latencia.

Description: Breve descripción para referencias administrativas.



The screenshot shows the pfSense web interface. At the top is a navigation bar with the pfSense logo and menu items: System, Interfaces, Firewall, Services, VPN, Status, Diagnostics, and Help. Below this is a breadcrumb trail: Interfaces / VLANs. A secondary navigation bar contains links for Interface Assignments, Interface Groups, Wireless, VLANs (which is highlighted with a red underline), QinQs, PPPs, GREs, GIFs, Bridges, and LAGGs. The main content area is titled 'VLAN Interfaces' and contains a table with the following data:

Interface	VLAN tag	Priority	Description	Actions
em1 (lan)	1	5	VLAN Finanzas	 
em1 (lan)	2	2	VLAN Marketing	 

At the bottom right of the table is a green button with a plus sign and the text 'Add'.

Asignación de interfaces:

- Una vez creadas las VLANS, se asignan como interfaces virtuales en pfSense.

Ruta: Interfaces → Interface Assignments

- Configuramos una IP estática para cada interfaz.

VLANFinanzas → IP: 192.168.30.1/24 → subred proporcionada: 192.168.30.0/24


VLANMarketing → IP: 192.168.40.1/24 → subred proporcionada: 192.168.40.0/24

Notas:

*** La IP asignada en pfSense (.1) en cada subred funciona como una puerta de enlace gateway que proporcionará a los equipos de esa subred conectividad a internet mediante la IP pública de la interfaz WAN de pfSense.**

VLANFinanzas configuración:


- IP proporcionada: 192.168.30.1/24


Enable	<input checked="" type="checkbox"/> Enable interface
Description	<input type="text" value="VLANFinanzas"/>  Enter a description (name) for the interface here.
IPv4 Configuration Type	<input type="text" value="Static IPv4"/>
IPv6 Configuration Type	<input type="text" value="None"/>
MAC Address	<input type="text" value="XXXXXXXXXXXX"/> The MAC address of a VLAN interface must be set on its parent interface
MTU	<input type="text"/> If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	<input type="text"/> If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex	<input type="text" value="Default (no preference, typically autoselect)"/> Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex

Static IPv4 Configuration	
IPv4 Address	<input type="text" value="192.168.30.1"/>  / 24 <input type="text"/>
IPv4 Upstream gateway	<input type="text" value="None"/> + Add a new gateway

VLANMarketing configuración:

- IP proporcionada: 192.168.40.1/24

General Configuration	
Enable	<input checked="" type="checkbox"/> Enable interface
Description	<input type="text" value="VLANMarketing"/>  <small>Enter a description (name) for the interface here.</small>
IPv4 Configuration Type	<input type="text" value="Static IPv4"/>
IPv6 Configuration Type	<input type="text" value="None"/>
MAC Address	<input type="text" value="xx:xx:xx:xx:xx:xx"/> <small>The MAC address of a VLAN interface must be set on its parent interface</small>
MTU	<input type="text"/> <small>If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.</small>
MSS	<input type="text"/> <small>If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.</small>
Speed and Duplex	<input type="text" value="Default (no preference, typically autoselect)"/> <small>Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex mode set.</small>

Static IPv4 Configuration	
IPv4 Address	<input type="text" value="192.168.40.1"/>  / <input type="text" value="24"/>
IPv4 Upstream gateway	<input type="text" value="None"/> <input type="button" value="+ Add a new gateway"/>

Notas sobre gateway y flujo de tráfico:

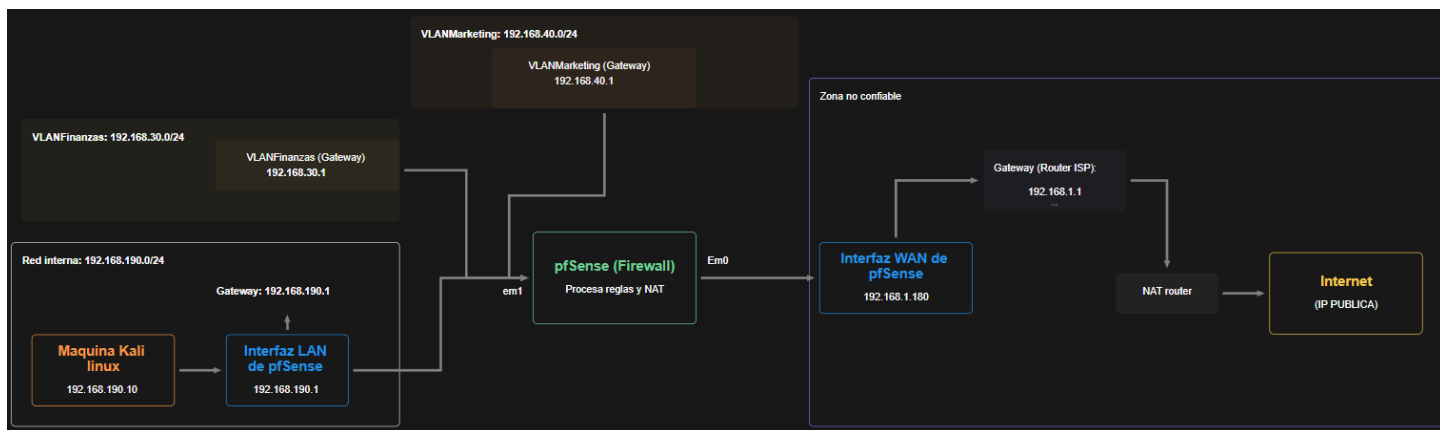
- La IP asignada a cada VLAN funciona como puerta de enlace para los hosts de esa subred.
- Todo el tráfico que no pertenece a la subred se envía al gateway de la VLAN, donde pfSense lo procesa según sus reglas y decide si lo envía a otra subred o a la WAN.
- En este laboratorio, la WAN de pfSense está detrás del router con NAT, generando doble NAT: primero pfSense traduce la subred a su WAN y luego el router traduce la WAN a su IP pública.

NAT (Outbound NAT) se asigna automáticamente para VLANs.

- El Outbound NAT de pfSense se aplica de forma automática a todas las subredes internas, incluyendo las VLANs configuradas, garantizando que el tráfico saliente de cada VLAN utilice la IP de la interfaz WAN para acceder a Internet sin necesidad de reglas NAT adicionales.

Mappings										
<input type="checkbox"/>	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	Actions
<div> <div>↑ Add</div> <div>↓ Add</div> <div>🗑 Delete</div> <div>🔄 Toggle</div> <div>💾 Save</div> </div>										
Automatic Rules										
	Interface	Source	Source Port	Destination	Destination Port	NAT Address	NAT Port	Static Port	Description	
✓	WAN	127.0.0.0/8 ::1/28 192.168.190.0/24 192.168.30.0/24 192.168.40.0/24	*	*	500	WAN address	*	✓	Auto created rule for ISAKMP	
✓	WAN	127.0.0.0/8 ::1/28 192.168.190.0/24 192.168.30.0/24 192.168.40.0/24	*	*	*	WAN address	*	✕	Auto created rule	

Diagrama conceptual:



4. Reglas de Firewall LAN/VLAN → WAN

Objetivo: Permitir el tráfico saliente desde las redes internas (LAN y VLANs) hacia Internet, asegurando conectividad y registro para auditoría.

Configuración de reglas aplicado a VLANFINANZAS:

Action: Pass.

Interface: VLANFINANZAS.

Address Family: IPv4 + Ipv6.

Protocol: Any.

Source: VLANFINANZAS subnet.

Destination: Any.

Logging: Habilitado para auditoría.

Description: Permitir tráfico VLANFINANZAS a internet.

Configuración de reglas aplicado a VLANMARKETING:

Action: Pass.

Interface: VLANMARKETING.

Address Family: IPv4 + Ipv6.

Protocol: Any.

Source: VLANMARKETING subnet.

Destination: Any.

Logging: Habilitado para auditoría.

Description: Permitir tráfico VLANMARKETING a internet.

Notas:

* Ambas VLANs permiten todo el tráfico hacia internet.

* Las reglas LAN por defecto permiten tráfico general, pero las VLANs necesitan reglas propias para poder salir a internet, ya que cada VLAN tiene su propia interfaz conectada a pfSense.

5. Resultados de la configuración

Los hosts de LAN y VLANs pueden:

* Navegar a internet.

* Realizar pings

* Usar servicios externos como HTTP,HTTPS,DNS,etc.

* El NAT automático asegura que las VLANs utilicen la IP de la WAN de pfSense, para dirigir el tráfico al Router con NAT y posteriormente salir a Internet.

6. Captura de logs de VLANs

Objetivo: Documentaremos el tráfico generado por las VLANs hacia Internet, mostrando cómo las reglas de firewall y el NAT automático permiten el acceso.

Resultados de la VLANFINANZAS:

Prueba realizada:

* Ping desde pfSense (VLANFINANZAS IP 192.168.30.1) hacia 8.8.8.8 (DNS público de Google).

* Se verificaron los logs del firewall para registrar la salida.

Resultados del ping:

Diagnostics / Ping

Ping

Hostname

8.8.8.8

IP Protocol

IPv4

Source address

VLANFINANZAS

Select source address for the ping.

Maximum number of pings

5

Select the maximum number of pings.

Seconds between pings

1

Select the number of seconds to wait between pings.

Ping

Results

PING 8.8.8.8 (8.8.8.8) from 192.168.30.1: 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=117 time=17.117 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=117 time=16.075 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=117 time=17.904 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=117 time=16.605 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=117 time=16.227 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 16.075/16.785/17.904/0.665 ms

Resultados de la VLANMARKETING:

Resultados del ping:

Diagnostics / Ping

Ping

Hostname

8.8.8.8

IP Protocol

IPv4

Source address

VLANMARKETING

Maximum number of pings

5

Seconds between pings

1

Select source address for the ping.

Select the maximum number of pings.

Select the number of seconds to wait between pings.

Ping

Results

PING 8.8.8.8 (8.8.8.8) from 192.168.40.1: 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=117 time=18.804 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=117 time=16.380 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=117 time=16.679 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=117 time=17.109 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=117 time=16.038 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 16.038/17.002/18.804/0.967 ms

Conclusión de la configuración de NAT y VLANs

- * Las VLANs fueron configuradas correctamente, cada una con su interfaz y subred propia.
- * El NAT automático permite que el tráfico de cada VLAN utilice la IP de la interfaz WAN de pfSense para salir a Internet, incluso cuando la WAN está detrás de un router con NAT.
- * Las reglas de firewall aplicadas a cada VLAN permiten el tráfico saliente hacia Internet y quedan registradas en los logs para auditoría.
- * Las pruebas de conectividad (ping y tráfico hacia servicios externos) confirman que los hosts virtuales pueden comunicarse correctamente hacia Internet sin necesidad de configuración NAT adicional.
- * El laboratorio demuestra cómo segmentar la red mediante VLANs, manteniendo el control de tráfico con el firewall asegurando que la salida a Internet sea funcional y auditada.

Sección E – Configuración de DNS Resolver y DNS Forwarder en pfSense

Objetivo: Configuraremos y documentaremos el funcionamiento de los dos métodos principales de resolución de nombres en pfSense (DNS Resolver y DNS Forwarder), mostrando cómo los hosts internos pueden resolver dominios a través del firewall.

DNS Resolver

Función: pfSense actúa como servidor recursivo. Consulta directamente a los servidores raíz de Internet y devuelve la respuesta al host interno.

1. Acceso a la interfaz de DNS Resolver

- En la interfaz de pfSense nos dirigimos a Services → DNS Resolver.
- Nos aseguramos que la casilla “Enable DNS Resolver” esté marcada.
- **IP utilizada por los hosts: 192.168.190.1** (IP de pfSense LAN). Los equipos internos usarán como servidor DNS la IP de pfSense en su interfaz LAN 192.168.190.1. De esta forma, cualquier consulta de nombres ejemplo: www.google.com se envía primero a pfSense, que luego resuelve o reenvía la petición a Internet según la configuración (Resolver o Forwarder).

pfSense
COMMUNITY EDITION


System ▾ Interfaces ▾ Firewall ▾ Services ▾ VPN ▾ Status ▾ Diagnostics ▾ Help ▾

Services / DNS Resolver / General Settings

ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit [System > Advanced > Networking](#) to switch DHCP backend.

General Settings Advanced Settings Access Lists

General DNS Resolver Options

Enable	<input checked="" type="checkbox"/> Enable DNS resolver 
Listen Port	<input type="text" value="53"/> The port used for responding to DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 53.
Enable SSL/TLS Service	<input type="checkbox"/> Respond to incoming SSL/TLS queries from local clients Configures the DNS Resolver to act as a DNS over SSL/TLS server which can answer queries from clients which also support DNS over TLS. Activating this option disables automatic interface response routing behavior, thus it works best with specific interface bindings.
SSL/TLS Certificate	<input type="text" value="GUI default (68c7355c76f6a)"/> The server certificate to use for SSL/TLS service. The CA chain will be determined automatically.
SSL/TLS Listen Port	<input type="text" value="853"/> The port used for responding to SSL/TLS DNS queries. It should normally be left blank unless another service needs to bind to TCP/UDP port 853.
Network Interfaces	<div><div>All</div><div>WAN</div><div>LAN</div><div>VLANFINANZAS</div><div>VLANMARKETING</div></div> Interface IP addresses used by the DNS Resolver for responding to queries from clients. If an interface has both IPv4 and IPv6 addresses, both are used. Queries to addresses not selected in this list are discarded. The default behavior is to respond to queries on every available IPv4 and IPv6 address.

DNS Forwarder

Función: pfSense no consulta directamente a los servidores raíz, en su lugar, reenvía la consulta a otro servidor DNS por ejemplo: Google 8.8.8.8 o ISP.


2. Acceso a la interfaz de DNS Forwarder

Activación:

- Ir a **Services** → **DNS Forwarder**.
- Marcamos **Enable DNS Forwarder**.

ISC DHCP has reached end-of-life and will be removed in a future version of pfSense. Visit [System > Advanced > Networking](#) to switch DHCP backend.

General DNS Forwarder Options

Enable	<input type="checkbox"/> Enable DNS forwarder	
DHCP Registration	<input type="checkbox"/> Register DHCP leases in DNS forwarder If this option is set machines that specify their hostname when requesting a DHCP lease will be registered in the DNS forwarder, so that their name can be resolved. The domain in System: General Setup should also be set to the proper value.	
Static DHCP	<input type="checkbox"/> Register DHCP static mappings in DNS forwarder If this option is set, IPv4 DHCP static mappings will be registered in the DNS forwarder so that their name can be resolved. The domain in System: General Setup should also be set to the proper value.	
Prefer DHCP	<input type="checkbox"/> Resolve DHCP mappings first If this option is set DHCP mappings will be resolved before the manual list of names below. This only affects the name given for a reverse lookup (PTR).	
Ignore System DNS	<input type="checkbox"/> Do not use system DNS servers If this option is set the configured system DNS servers will be ignored and custom "server=" options must be used.	
DNS Query Forwarding	<input type="checkbox"/> Query DNS servers sequentially If this option is set pfSense DNS Forwarder (dnsmasq) will query the DNS servers sequentially in the order specified (System - General Setup - DNS Servers), rather than all at once in parallel.	<div><input type="checkbox"/> Require domain If this option is set pfSense DNS Forwarder (dnsmasq) will not forward A or AAAA queries for plain names, without dots or domain parts, to upstream name servers. If the name is not known from /etc/hosts or DHCP then a "not found" answer is returned.</div> <div><input type="checkbox"/> Do not forward private reverse lookups If this option is set pfSense DNS Forwarder (dnsmasq) will not forward reverse DNS lookups (PTR) for private addresses (RFC 1918) to upstream name servers. Any entries in the Domain Overrides section forwarding private</div>

Asignación de servidor DNS en el laboratorio:

-Configuramos la IP de la interfaz LAN de pfSense como servidor DNS para los hosts internos (192.168.190.1).

- Solo se activa uno de los dos (Resolver o Forwarder). En este laboratorio usamos el Resolver para mostrar resolución autónoma.

-En cada host de la red interna se especifica manualmente la IP de pfSense como servidor DNS, asegurando que todas las consultas de nombres de dominio pasen por el firewall y puedan ser registradas en los logs para auditorías.

- En nuestro host indicamos el servidor DNS que usaremos:

Comandos utilizados:

- cd /etc/NetworkManager/system-connections

- sudo nano 'Wired connection 1'

```
(mauricio@kali)-[/etc/NetworkManager/system-connections]
$ sudo nano 'Wired connection 1'
```

```
GNU nano 8.3                               Wired connection 1 *
[connection]
id=Wired connection 1
uuid=919be524-94ca-472f-b9e8-f5a7c858682d
type=802-3-ethernet

[802-3-ethernet]

[ipv4]
method=manual
address1=192.168.190.10/24,192.168.190.1
dns=192.168.190.1;
[ipv6]
method=auto
ip6-privacy=2
```

Prueba de resolución DNS:

Comandos utilizados:

- ping www.google.com

- dig @192.168.190.1 www.google.com


```
(mauricio@kali)-[/etc/NetworkManager/system-connections]
$ ping www.google.com

PING www.google.com (142.251.129.36) 56(84) bytes of data.
64 bytes from tzezea-ad-in-f4.1e100.net (142.251.129.36): icmp_seq=1 ttl=115 time=19.0 ms
64 bytes from tzezea-ad-in-f4.1e100.net (142.251.129.36): icmp_seq=2 ttl=115 time=20.4 ms
64 bytes from tzezea-ad-in-f4.1e100.net (142.251.129.36): icmp_seq=3 ttl=115 time=19.5 ms
^C
— www.google.com ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 19.028/19.653/20.414/0.573 ms
```

```
(mauricio@kali)-[/etc/NetworkManager/system-connections]
$ dig @192.168.190.1 www.google.com

; <<>> DiG 9.20.11-4+b1-Debian <<>> @192.168.190.1 www.google.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; —>HEADER<— opcode: QUERY, status: NOERROR, id: 17688
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL:
0

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1432
;; QUESTION SECTION:
;www.google.com.                IN      A
;; ANSWER SECTION:
www.google.com.                 300     IN      A      142.251.134.196
;; Query time: 443 msec
;; SERVER: 192.168.190.1#53(192.168.190.1) (UDP)
```



1.

Sección F – Monitoreo y análisis de logs en pfSense

Objetivo: Configurar y demostrar el monitoreo de tráfico y análisis de logs en pfSense, incluyendo la captura de eventos legítimos y maliciosos, para evidenciar la funcionalidad del firewall y su capacidad de auditoría.

1. Logs de tráfico permitido y bloqueado

* **Default firewall pass rules:** se refiere a los registros de tráfico que pfSense permite gracias a las reglas implícitas que vienen por defecto (por ejemplo, cuando desde la LAN se puede salir a Internet sin necesidad de crear una regla manual).

* **Default firewall block rules:** son los registros de paquetes que pfSense bloquea automáticamente con sus reglas internas, como suele pasar con intentos de conexión entrantes desde la WAN hacia la red interna.

* **Rule-specific logging:** es el registro que activamos manualmente en reglas concretas. Esto sirve para auditar tráfico específico, por ejemplo, conexiones desde una VLAN en particular hacia Internet.

Configuración:

Accedemos a **Status → System Logs → Settings**.

Activamos las opciones:

- * **Log packets that are allowed by the implicit default pass rule**
- * **Log packets that are blocked by default block rule**

Logging Preferences	
<input checked="" type="checkbox"/>	Default firewall "block" rules Log packets that are blocked by the implicit default block rule.
<input checked="" type="checkbox"/>	Default firewall "pass" rules Log packets that are allowed by the implicit default pass rule. Note: Packets with IP options are not affected by this option and are logged by default .

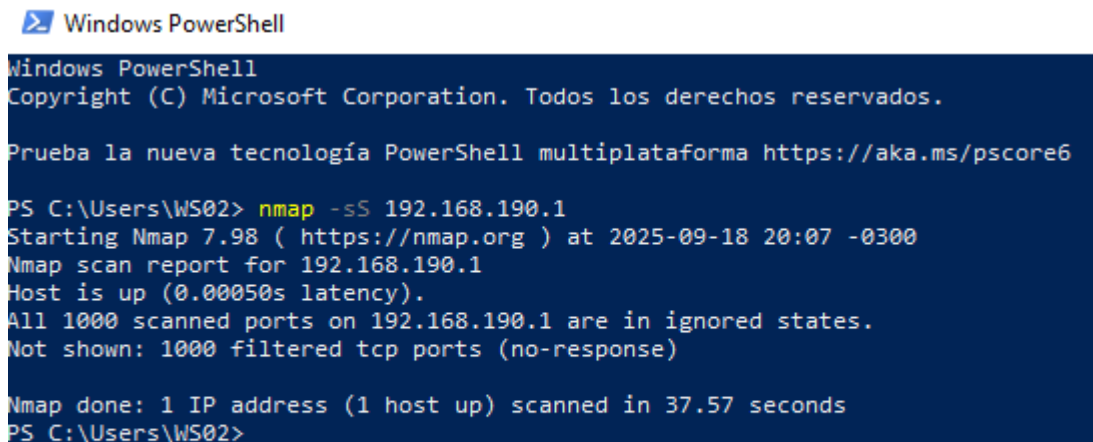
2. Monitoreo de tráfico malicioso con nmap

Objetivo: Verificar que el firewall bloquea tráfico no autorizado y registrar eventos de actividad de red, aunque no se pueda simular un atacante externo real.

Ejemplo: Utilizaremos NMAP para realizar el escaneo de puertos desde un host interno:

Comandos a utilizar:

-nmap -sS 192.168.190.1



```
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos los derechos reservados.

Prueba la nueva tecnología PowerShell multiplataforma https://aka.ms/pscore6

PS C:\Users\WS02> nmap -sS 192.168.190.1
Starting Nmap 7.98 ( https://nmap.org ) at 2025-09-18 20:07 -0300
Nmap scan report for 192.168.190.1
Host is up (0.00050s latency).
All 1000 scanned ports on 192.168.190.1 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 37.57 seconds
PS C:\Users\WS02>
```

Resultados:

- El pfSense bloqueó los intentos de conexión según las reglas configuradas.
- Los logs muestran los paquetes bloqueados por las reglas de “Block private networks” y “Bogon networks”.
- todos los puertos están “filtered/no-response”.

Conclusión: Aunque no se trató de un atacante externo, el laboratorio demuestra la capacidad del firewall para auditar y registrar tráfico sospechoso dentro de la red, mostrando la efectividad de sus reglas de bloqueo y la generación de logs.