

Firewall

Cuando instalas pfSense y configuras todas sus interfaces, debes crear reglas de firewall. Una regla de firewall permitirá o denegará el tráfico según la fuente de donde proviene ese tráfico. Hay muchas maneras en que puede implementar reglas de firewall en pfSense, y comprender cómo funcionan es un paso importante para garantizar que su red esté configurada correctamente.

Es recomendable leerse la guía de Netgate donde explica cómo se procesan estas reglas de Firewall. ([link](#))

Cómo crear reglas de firewall en pfSense

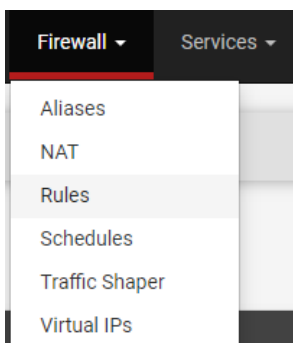
Cuando quieras crear reglas de firewall en pfSense, las reglas deben configurarse en **cada** interfaz. Esto significa que si tiene redes LAN, IoT y de invitados, se deberán crear reglas de firewall en **cada** interfaz para permitir o denegar el tráfico. También debe crear reglas de firewall si está utilizando una VPN como [OpenVPN](#) o [WireGuard](#) (en la interfaz VPN).

Las reglas se crean para cada interfaz solo en la dirección de entrada. Eso no significa que el tráfico de salida no se pueda bloquear, pero el tráfico debe originarse en la dirección de entrada de la interfaz. Un ejemplo se explica más adelante en este documento.

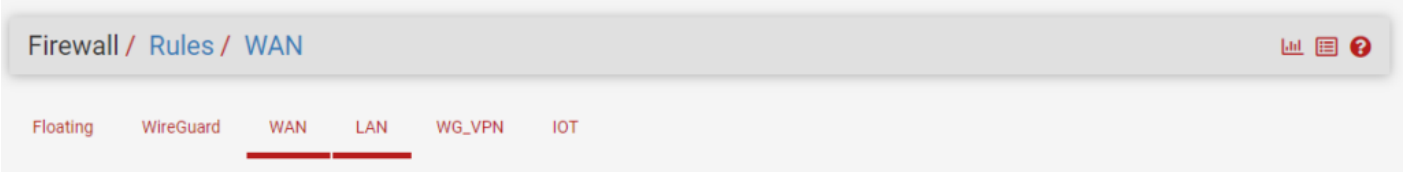
También es importante comprender que, de forma predeterminada, el tráfico se deniega automáticamente. Para permitir el tráfico en una interfaz, primero se debe crear una regla de permiso.

1. Cómo acceder a las reglas del cortafuegos en pfSense

Si deseas configurar reglas de firewall, puedes acceder a la sección de reglas dirigiendote a **Firewall --> Reglas**.



Al hacer click en Rules, te lleva a la pestaña de Rules donde podrás ver los diferentes apartados que utilizas en este momento (WAN, LAN, WireGuard, OpenVPN, Floating, etc.).



Si creas reglas para la interfaz **WAN** , crearás reglas para permitir el tráfico a su red local desde redes externas.

Rules (Drag to Change Order)												
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
<input checked="" type="checkbox"/>	0 / 249 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks		
<input checked="" type="checkbox"/>	0 / 3.81 MIB	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks		
<input checked="" type="checkbox"/>	0 / 4 KIB	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none		OpenVPN OpenVPN Server wizard		
<input checked="" type="checkbox"/>	0 / 0 B	IPv4 UDP	*	*	WAN address	51820	*	none		WireGuard - Allow WAN		

Cualquier otra interfaz enumerada (aparte de la sección flotante) administrará el tráfico para las interfaces internas o para otra categoría (VPN, por ejemplo).

Rules (Drag to Change Order)												
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions	
<input checked="" type="checkbox"/>	2 / 917 KIB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule		
<input type="checkbox"/>	0 / 0 B	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule		
<input type="checkbox"/>	0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule		

Add Add Delete Save Separator

2. Cómo crear reglas de firewall en pfSense

Para crear una regla de firewall en pfSense, ve a la interfaz donde deseas crear la regla y selecciona **Add**. La flecha hacia arriba creará una regla en la parte superior de la lista y la flecha hacia abajo creará una en la parte inferior.

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	2 / 2.68 MIB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0 / 0 B	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	
<input type="checkbox"/>	0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Add
 Add
 Delete
 Save
 Separator

Selecciona en la pestaña **Action** si deseas permitir (aprobar), bloquear o rechazar el tráfico.

Action

Pass

Pass
Block
Reject

TCP RST or ICMP port unreachable for UDP) is returned to the sender, final packet is discarded.

Actualiza la **interfaz** si es necesario, luego cambia la **Address Family** a IPv4, IPv6 o IPv4 + IPv6.

Interface

LAN

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

Address Family

IPv4+IPv6

Select the Internet Protocol version this rule applies to.

En la sección **de Protocol**, selecciona el protocolo correcto para la regla que deseas crear. **Si deseas permitir o denegar todo el tráfico, selecciona cualquiera.**

Según el protocolo que selecciones, aparecerán diferentes opciones debajo de él. Por ejemplo, si seleccionas TCP, deberás especificar el rango de puertos TCP.

Protocol

TCP

Any
TCP
UDP
TCP/UDP
ICMP
ESP
AH
GRE
EoIP
IPv6
IGMP
PIM
OSPF
SCTP
CARP
PFSYNC

Source

Destination

En la sección **de Source**, selecciona la categoría correcta.

Si deseas elegir una red completa (LAN, IoT, invitado, etc.), selecciona "nombre de interfaz + red". Esto utilizará toda la red.

Source

Source ☐ Invert match any Source Address /

Destination

Destination ☐ Invert match any Destination Address /

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).

En la sección de **Destination**, selecciona la opción correcta (igual que la sección de origen).

Destination

Destination ☐ Invert match any Destination Address /

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

Proporciona una **Description** a la regla (no es necesario, pero ayuda a ordenar y comprender la regla por si en un futuro no te acuerdas que hace.) y haz click en **Save**.

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

Save

3. Ejemplo de regla de cortafuegos

Para este ejemplo, se enumera una regla de cortafuegos de ejemplo que bloquea el tráfico de la **red de invitados** a la **red LAN**. Esto significa que cualquier persona conectada a la red de invitados **no** podrá acceder a nada en la red LAN.

- **Acción:** Bloquear
- **Interfaz:** INVITADO
- **Familia de direcciones:** IPv4 + IPv6
- **Protocolo:** Cualquiera
- **Fuente:** Cualquiera
- **Destino:** red LAN
- **Descripción:** Bloquear LAN de Invitado

Edit Firewall Rule

Action

Block

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

GUEST

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

Address Family

IPv4+IPv6

Select the Internet Protocol version this rule applies to.

Protocol

Any

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

any

Source Address

/

Destination

Destination

☐ Invert match

LAN net

Destination Address

/

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

Block LAN from Guest

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

Esta regla bloquea **cualquier tráfico** de la red invitada a la red LAN para el tráfico IPv4 e IPv6. En la interfaz de red LAN, también se puede crear una regla para bloquear el tráfico de la red LAN a la red invitada si no deseas que pase **ningún** tráfico hacia/desde las redes LAN y de invitados.

Tiene que quedar claro que la regla inicial se crea en la interfaz de red para invitados porque las reglas se crean en el nivel de la interfaz solo para el tráfico entrante. El tráfico está bloqueado en la red LAN porque un dispositivo invitado intenta conectarse a un dispositivo LAN y pfSense lo bloquea.

Dispositivo de red invitado > Solicitudes de red LAN > pfSense Firewall > Regla de bloqueo

Revision #5

Created 19 April 2023 16:51:53 by molombo

Updated 19 April 2023 17:21:47 by molombo