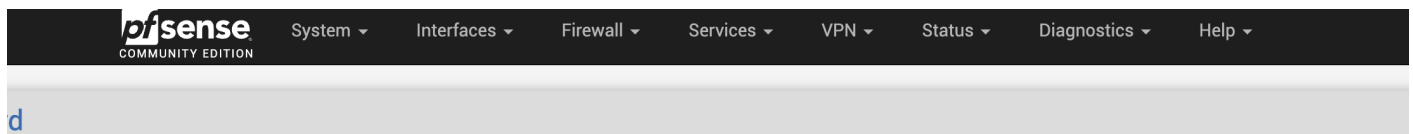


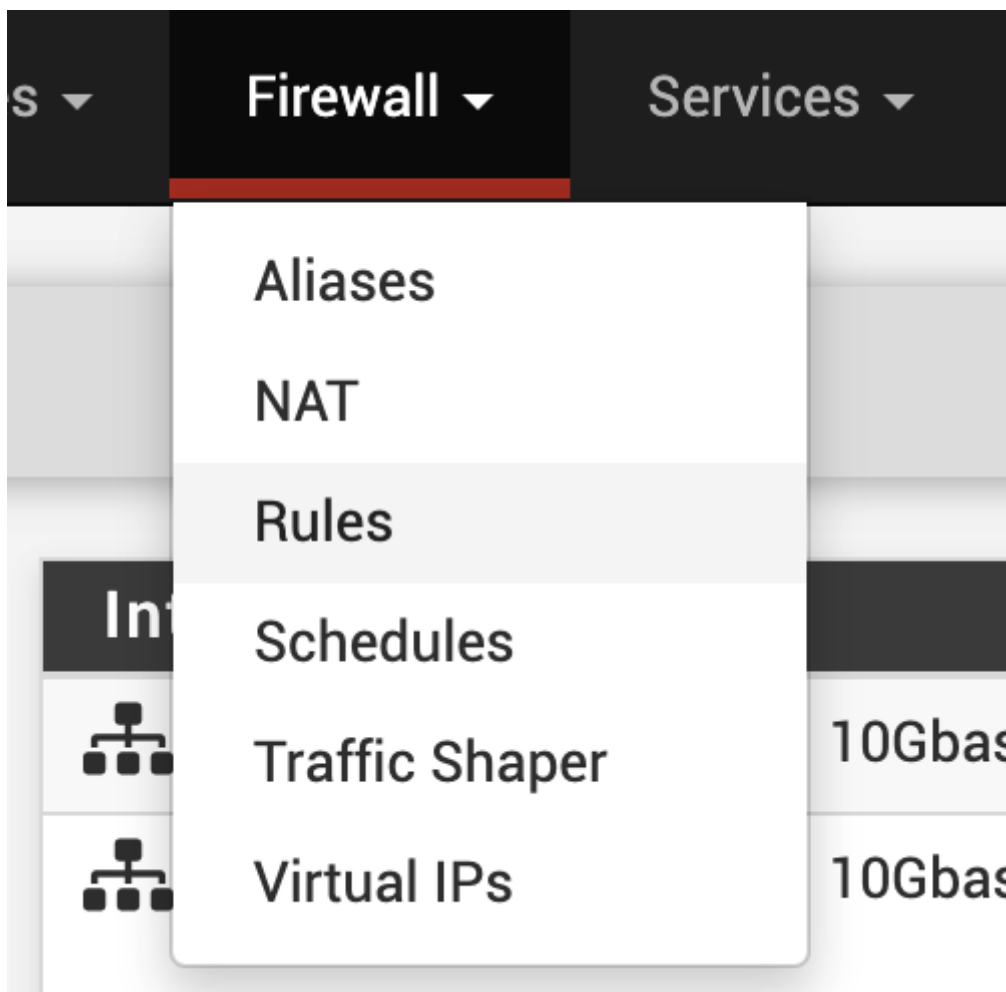
Restringir el acceso a administración en PFSense

Dejar accesible la administración de un PFSense es un riesgo de seguridad, por eso te aconsejamos (si tienes una IP fija) restringir el acceso a esa IP o rango

para ello una vez accedemos al PFSense, vamos a la opción Firewall



En la opción Rules



Creamos una nueva regla

En primer lugar habilitamos SSH. A.B.C.D será nuestra IP y la máscara correspondiente (si es una sola IP será /32)

La regla será Pass , Interface WAN, protocolo TCP desde la fuente (nuestra IP que queremos que acceda) a destino WAN Address.

Firewall / Rules / Edit

Firewall Rule

Action

Pass

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

WAN

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

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which IP protocol this rule should match.

Source

Source

☐ Invert match

Network

A.B.C.D

/

24

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

WAN address

Destination Address

/

Destination Port Range

SSH (22)

From

Custom

To

SSH (22)

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

Https Admin

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

Y luego https y/o http

Edit Firewall Rule

Action

Pass

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

WAN

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

Address Family

IPv4

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which IP protocol this rule should match.

Source

Source☐ Invert match

Network

A.B.C.D

/

24

 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

WAN address

Destination Address

/

Destination Port Range

HTTPS (443)

From

Custom

HTTPS (443)

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

Https Admin

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

Revision #4

Created 9 September 2022 08:16:43 by Admin

Updated 9 September 2022 09:27:05 by Admin