

Règles pare-feu

Notre système PfSense peut contenir un ensemble de règles permettant :

- D'autoriser la connexion (Pass) ;
- De bloquer la connexion (Block) ;

De rejeter la demande de connexion avec un message TCP RST ou ICMP port unreachable pour UDP (Reject).

Sous PfSense on **autorise uniquement les communications ayant été explicitement autorisées**. Soit tout ce qui n'est pas explicitement autorisé est interdit.

Exemple :

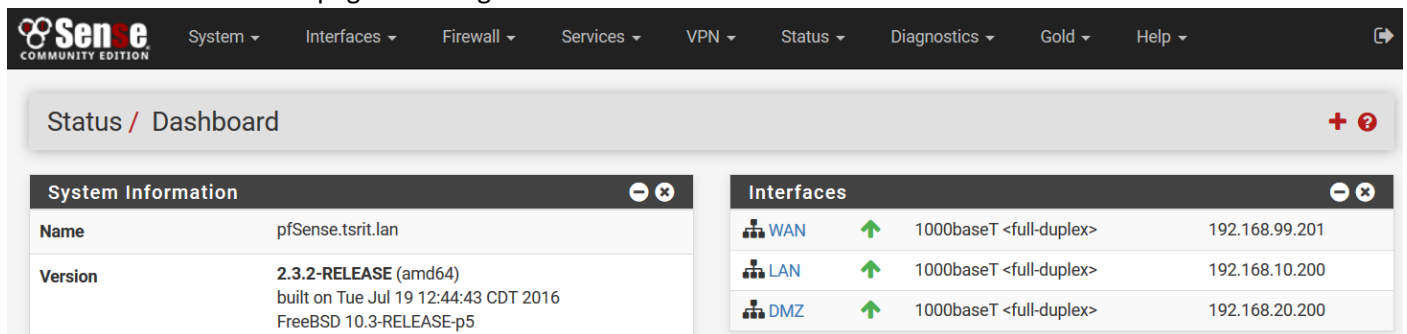
Règle	Action	IP source	IP dest	Protocol	Port source	Port dest
1	Pass	192.168.20.10	tout sauf LAN	udp	any	53
2	Pass	192.168.20.10	tout sauf LAN	tcp	any	80
3	Pass	192.168.20.10	tout sauf LAN	tcp	any	443

La première règle autorise la machine 192.168.20.10 à envoyer des requêtes en UDP pour la résolution DNS vers internet.

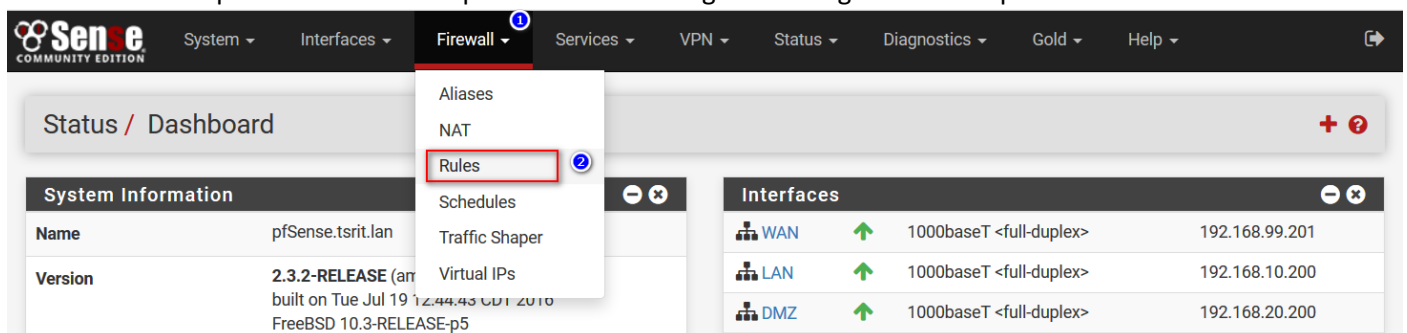
La deuxième et troisième règle autorise la communication http et https depuis la machine 192.168.20.10 vers internet.

Procédure

Connectez-vous sur votre page de configuration PfSense.



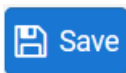
Nous allons nous placer dans le menu permettant de configurer les règles de notre pare-feu :



Puis choisir l'onglet « DMZ » et cliquer sur « Add »

Nous allons autoriser la résolution de nom de domaine (DNS) via le port 53 et le protocole http/https depuis notre serveur Web qui est placé dans la Zone « **DMZ** » pour qu'on puisse le mettre à jours régulièrement avec les commandes « **apt-get update && apt-get upgrade** ».

Puis cliquer sur




On autoriser dorénavant la résolution DNS depuis notre serveur web vers internet.

Procéder comme suit pour autoriser la connexion web :

Cliquez sur le bouton « Copy » sur la règle qu'on viens de crée.

FloatingWANLANDMZ

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/4 KiB	IPv4 UDP	192.168.20.10	*	! LAN net	53 (DNS)	*	none		

↑ Add

↓ Add

Delete

Save

Separator

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

DMZ

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.

Single host or alias

192.168.20.10

Display Advanced

Display Advanced

Destination

Destination

☒ Invert match.

LAN net

Destination Address

Destination port range

HTTP (80)

From


Custom

HTTP (80)

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.

Puis cliquer sur .

Puis le protocole HTTPS :

FloatingWANLANDMZ

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓	0/4 KiB	IPv4 UDP	192.168.20.10	*	! LAN net	53 (DNS)	*	none		
<input type="checkbox"/>	✓	0/0 B	IPv4 TCP	192.168.20.10	*	! LAN net	80 (HTTP)	*	none		

↑ Add

↓ Add

Delete

Save

Separator

Destination

Destination

☒ Invert match.

LAN net

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.

Puis cliquer sur .