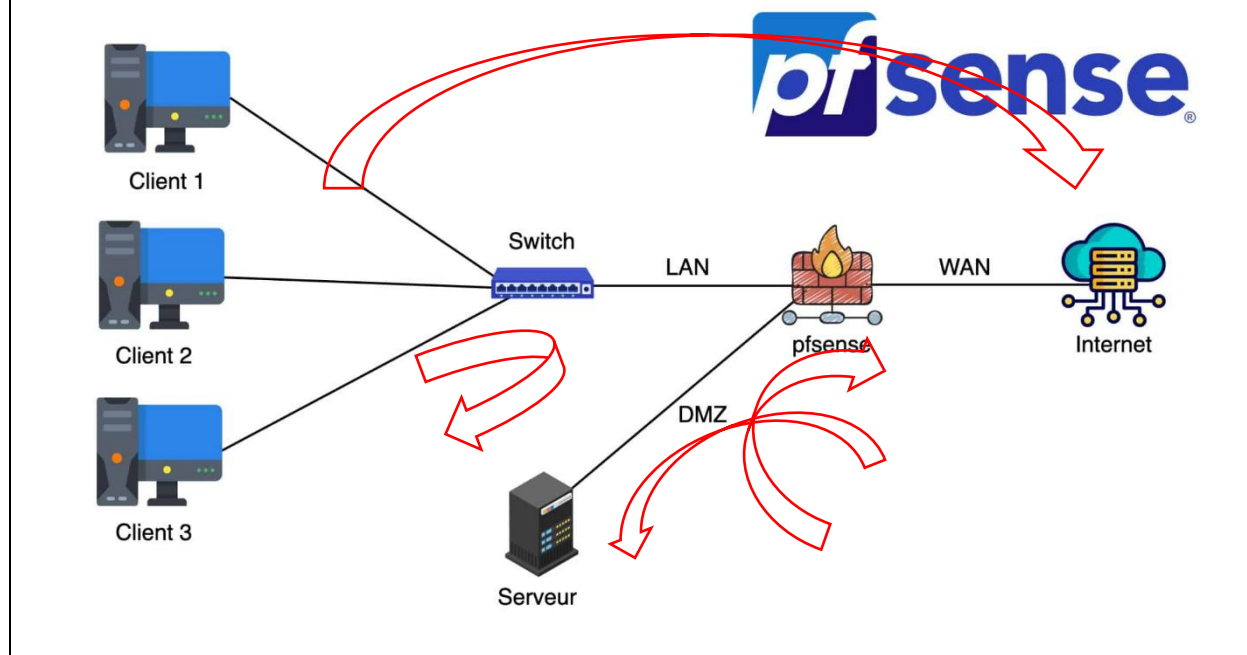


Configuration du pare-feu pfSense et gestion des règles de filtrage



1. Introduction

Dans ce tutoriel, nous allons configurer les **règles de pare-feu** sur pfSense afin de permettre et de contrôler la communication entre les différents réseaux de notre infrastructure. Cette configuration vise à assurer la **sécurité et l'isolation des flux** entre la DMZ, le réseau interne (LAN) et Internet (WAN).

Définition de quelques notions :

Qu'est-ce que pfSense ?

pfSense est un **pare-feu open-source et une solution de routage avancée** basée sur FreeBSD. Il permet de sécuriser un réseau en contrôlant le trafic entrant et sortant à travers des règles personnalisables. Il est couramment utilisé pour gérer les réseaux d'entreprise grâce à ses fonctionnalités telles que le filtrage de paquets, le VPN, la gestion des VLANs et la détection d'intrusions.

Qu'est-ce qu'une DMZ ?

Une **DMZ (Demilitarized Zone)** est un sous-réseau isolé du réseau interne (LAN) et accessible depuis l'extérieur. Elle est utilisée pour héberger des serveurs accessibles publiquement (serveurs web, serveurs de messagerie, etc.) tout en protégeant le réseau interne contre les attaques potentielles. L'objectif principal de la DMZ est de minimiser les risques d'intrusion dans le LAN en maintenant une séparation stricte entre les zones sensibles et les services exposés.

Qu'est-ce qu'un LAN ?

Le **LAN (Local Area Network)** représente le réseau interne d'une organisation. Il est constitué des postes de travail, des imprimantes, des serveurs internes et d'autres équipements connectés. Contrairement à la DMZ, le LAN est destiné aux utilisateurs internes et est généralement protégé contre l'accès extérieur grâce à un pare-feu comme pfSense.

2. Objectifs

L'objectif principal est de définir des règles de filtrage pour :

- Autoriser l'accès à Internet depuis le LAN et la DMZ
- Bloquer l'accès direct de la DMZ vers le LAN
- Autoriser l'accès au serveur web situé en DMZ depuis le LAN
- Configurer le NAT pour permettre l'accès à un service depuis l'extérieur

3. Configuration des règles de pare-feu

3.1 Autoriser le LAN à accéder à Internet

1. Connectez-vous à l'interface web de pfSense.
2. Accédez à **Firewall > Rules > LAN > Add** pour créer une nouvelle règle.
3. Configurez la règle comme suit :

The first screenshot shows the pfSense dashboard with the 'Firewall' menu open and 'Rules' selected. A red box highlights the 'Rules' option, and a red arrow points to it.

The second screenshot shows the 'Firewall / Rules / LAN' page. A red box highlights the 'LAN' interface, and a red arrow points to it. Below the interface selection, there is a table of existing rules. At the bottom, a red box highlights the 'Add' button, and a red arrow points to it.

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
✓ 4 / 118 KiB	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	⚙️
✓ 61 / 99 KiB	IPv4 *	LAN net	*	*	*	*	none		Default allow LAN to any rule	🔗 📄 🗑️
✓ 0 / 0 B	IPv6 *	LAN net	*	*	*	*	none		Default allow LAN IPv6 to any rule	🔗 📄 🗑️

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 LAN
 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 Any
 Choose which IP protocol this rule should match.

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).

Description accès internet depuis le LAN
 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

3.2 Bloquer l'accès de la DMZ vers le LAN

1. Rendez-vous dans **Firewall > Rules > DMZ > Add** et créez une règle avec les paramètres suivants :

- **Action** : Block
- **Interface** : DMZ
- **Protocol** : Any
- **Source** : DMZ net
- **Destination** : LAN net

▲ Non sécurisé | 192.168.10.1/firewall_rules_edit.php?fr=opt1&after=-1

Firewall / Rules / Edit

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 Any
 Choose which IP protocol this rule should match.

Source

Source ☐ Invert match DMZ net 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 Bloquer l'accès de la DMZ vers le LAN
 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

2. Enregistrez la règle et appliquez les changements.

3.3 Autoriser le LAN à accéder au serveur web en DMZ

4 Toujours dans **Firewall > Rules**, sélectionnez **LAN>Add** et configurez la règle comme suit :

4.2 Action : Pass

4.3 Interface : LAN

4.4 Protocol : TCP

4.5 Source : LAN net

4.6 Destination : IP du serveur web en DMZ

4.7 Port destination : 80 (HTTP) ou 443 (HTTPS)

Firewall / Rules / Edit

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 LAN
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 LAN net Source Address /

[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 DMZ net Destination Address /

Destination Port Range HTTP (80) From Custom To Custom HTTPS (443) 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 accès serveur web dans la DMZ depuis le LAN
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

5 Enregistrez et appliquez la règle.

3.4 CONFIGURER LE NAT OUTBOUND POUR AUTORISER LA DMZ A UTILISER LA WAN

Cette règle permettra au réseau DMZ de « sortir » sur Internet via l'interface WAN.

Pour cela, effectuez les manipulations suivantes :

- Cliquez sur « **Firewall** » - « **NAT** » « **Outbound** » « **Add** » et configurez votre règle ainsi :

Firewall / NAT / Outbound / Edit

Edit Advanced Outbound NAT Entry

Disabled ☐ Disable this rule

Do not NAT ☐ Enabling this option will disable NAT for traffic matching this rule and stop processing Outbound NAT rules. In most cases this option is not required.

Interface WAN
The interface on which traffic is matched as it exits the firewall. In most cases this is "WAN" or another externally-connected interface.

Address Family IPv4
Select the Internet Protocol version this rule applies to.

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

Source Any / 24
Type: Source network for the outbound NAT mapping. Port or Range

Destination Any / 24
Type: Destination network for the outbound NAT mapping. Port or Range

3.5 Configurer le NAT pour un accès externe au serveur web en DMZ

1. Allez dans **Firewall > NAT > Port Forward**.
2. Cliquez sur **Add** et configurez la redirection comme suit :
 - **Interface** : WAN
 - **Protocol** : TCP
 - **Destination** : WAN Address
 - **Port destination** : 80 (HTTP) ou 443 (HTTPS)
 - **Redirect Target IP** : IP du serveur web en DMZ
 - **Redirect Target Port** : 80 ou 443

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

Address Family IPv4
Select the Internet Protocol version this rule applies to.

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

Source Display Advanced

Destination ☐ Invert match. WAN address
Type: Address/mask

Destination port range HTTP
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 Single host
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 HTTP
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.

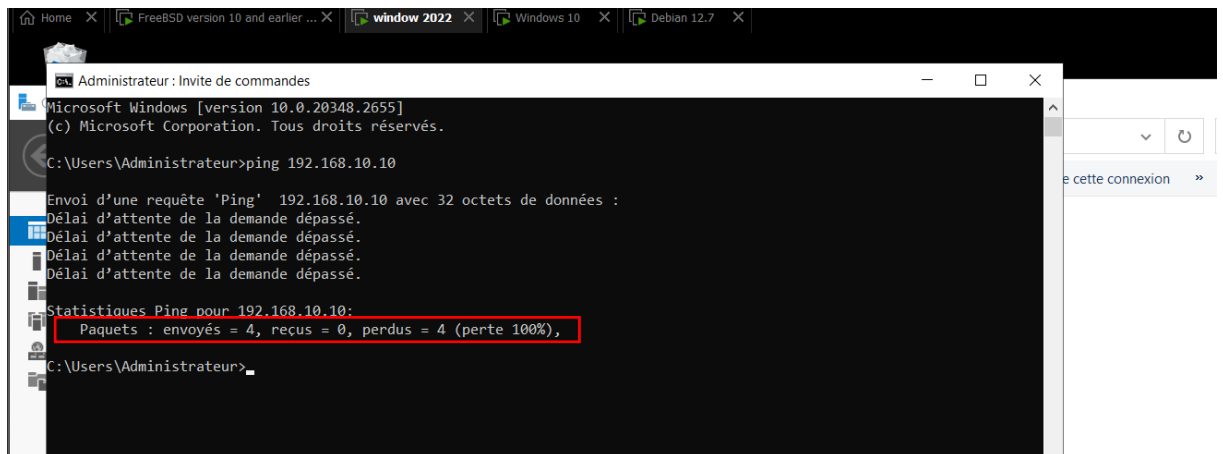
Description Accès serveur web depuis le WAN
A description may be entered here for administrative reference (not parsed).

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 Use system default

3. Enregistrez et appliquez la règle.

- Depuis une machine en DMZ, essayez de **pinger** une machine en LAN.



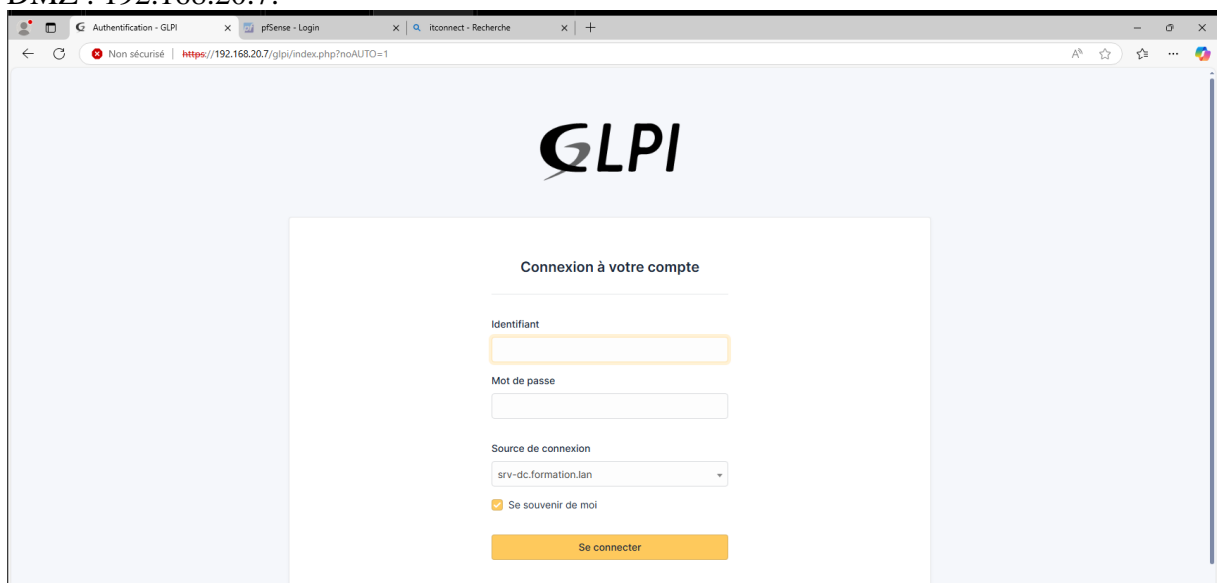
- La connexion doit être bloquée.

```

root@srv-web:~# ping 192.168.10.10
PING 192.168.10.10 (192.168.10.10) 56(84) bytes of data.
^C
--- 192.168.10.10 ping statistics ---
55 packets transmitted, 0 received, 100% packet loss, time 55328ms
  
```

4.3 Accéder au serveur web depuis le LAN

- Depuis une machine en LAN, ouvrez un navigateur et entrez l'IP du serveur web en DMZ : 192.168.20.7.



4.4 Tester l'accès externe au serveur web en DMZ

- Depuis une connexion externe, tentez d'accéder à l'IP publique de pfSense.

5. Conclusion

Nous avons mis en place un système de filtrage des flux réseau permettant de sécuriser les accès entre les différentes zones de l'infrastructure. Cette configuration garantit un cloisonnement efficace tout en permettant les communications essentielles.