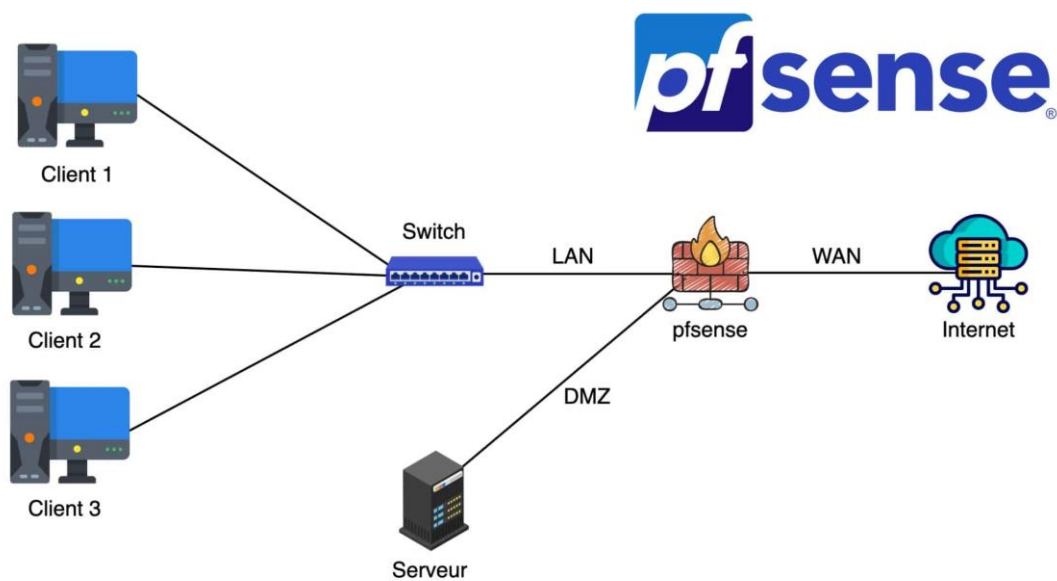


PROJET : DÉPLOIEMENT D'UNE DMZ AVEC PFSENSE



MANANTSOA Georges Iovatiana

I) Télécharger et Installer de pfSense

- ✓ Configuration de pfSense pour avoir 3 cartes réseaux (WAN, LAN, DMZ)
 - WAN en dhcp

- LAN en static
- Modifier le nom de OPT 1 par DMZ

```
Reloading routing configuration...
Restarting webConfigurator...

The IPv4 OPT1 address has been set to 192.168.2.1/24

Press <ENTER> to continue.
VMware Virtual Machine - Netgate Device ID: d67d64d77414496edacf

*** Welcome to pfSense 2.6.0-RELEASE (amd64) on pfSense ***

WAN (wan)      -> em0      -> v4/DHCP4: 192.168.117.139/24
LAN (lan)      -> em1      -> v4: 192.168.1.1/24
OPT1 (opt1)    -> em2      -> v4: 192.168.2.1/24
```

II) Accès à l'interface web de Pfsense

Connexion d'une machine debian à Pfsense pour pouvoir accéder à l'interface web de Pfsense et vérifier sur un navigateur de la machine qu'on a accès à internet.

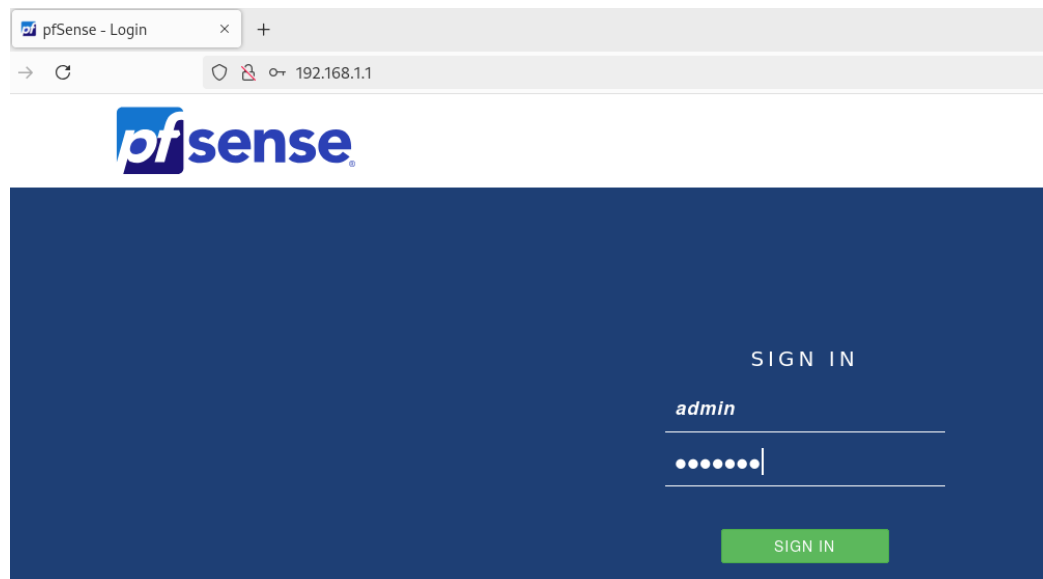
- ✓ Ping le poste vm debian avec le LAN du pfsense

```
root@debian:/home/lovatiana# 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=128 time=27.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=25.7 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=26.3 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=128 time=27.7 ms
^C
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 25.652/26.687/27.679/0.781 ms
```

- ✓ Accès à internet

```
root@debian:/home/tiana# 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=127 time=24.4 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=127 time=40.3 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=127 time=23.2 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=127 time=21.0 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=127 time=22.0 ms
64 bytes from 8.8.8.8: icmp_seq=6 ttl=127 time=25.1 ms
^C
--- 8.8.8.8 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5009ms
```

- ✓ Ouvrir un navigateur web sur la machine Debian, puis entrez l'adresse IP de l'interface LAN de pfSense dans la barre d'adresse du navigateur. Par défaut, cette adresse est généralement 192.168.1.1



Se connecter avec les accès par défaut : admin, mot de passe : pfsense
Puis il faut changer le mot de passe admin

III) Déploiement

1. Vérification et Configuration des Interfaces Réseau

Assurez que vos interfaces WAN, LAN et DMZ sont correctement configurées.

- WAN : Vérifiez que l'interface est configurée pour obtenir une adresse IP via DHCP ou configurez-la avec une adresse IP statique si nécessaire.

General Configuration	
Enable	<input checked="" type="checkbox"/> Enable interface
Description	<input type="text" value="WAN"/> <small>Enter a description (name) for the interface here.</small>
IPv4 Configuration Type	<input type="text" value="DHCP"/>
IPv6 Configuration Type	<input type="text" value="DHCP6"/>

- LAN :

Enable	<input checked="" type="checkbox"/> Enable interface
Description	<input type="text" value="LAN"/> <p>Enter a description (name) for the interface here.</p>
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	Track Interface
MAC Address	<input type="text" value="xxxxxxxxxxxx"/> <p>This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xxxxxxxx:xxxx:xx or leave blank.</p>
MTU	<input type="text"/> <p>If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.</p>
MSS	<input type="text"/> <p>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.</p>
Speed and Duplex	<input type="text" value="Default (no preference, typically autoselect)"/> <p>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 forced.</p>
Static IPv4 Configuration	
IPv4 Address	<input type="text" value="192.168.1.1"/> <input type="text" value="24"/>

- DMZ :

General Configuration	
Enable	<input checked="" type="checkbox"/> Enable interface
Description	<input type="text" value="DMZ"/> <p>Enter a description (name) for the interface here.</p>
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	<input type="text" value="xxxxxxxxxxxx"/> <p>This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xxxxxxxx:xxxx:xx or leave blank.</p>
MTU	<input type="text"/> <p>If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.</p>
MSS	<input type="text"/> <p>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.</p>
Speed and Duplex	<input type="text" value="Default (no preference, typically autoselect)"/> <p>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 forced.</p>
Static IPv4 Configuration	
IPv4 Address	<input type="text" value="192.168.2.1"/> <input type="text" value="24"/>

2. Activation du Serveur DHCP sur le LAN :

Si on souhaite que les appareils du réseau local obtiennent automatiquement des adresses IP il nous faut faire :

Services / DHCP Server / LAN

LAN DMZ

General Options

Enable ☒ Enable DHCP server on LAN interface

BOOTP ☐ Ignore BOOTP queries

Deny unknown clients Allow all clients

When set to **Allow all clients**, any DHCP client will get an IP address within this scope/range on this interface. If set to **Allow known clients from any interface**, any DHCP client with a MAC address listed on **any** scope(s)/interface(s) will get an IP address. If set to **Allow known clients from only this interface**, only MAC addresses listed below (i.e. for this interface) will get an IP address within this scope/range.

Ignore denied clients ☐ Denied clients will be ignored rather than rejected.
This option is not compatible with failover and cannot be enabled when a Failover Peer IP address is configured.

Ignore client identifiers ☐ If a client includes a unique identifier in its DHCP request, that UID will not be recorded in its lease.
This option may be useful when a client can dual boot using different client identifiers but the same hardware (MAC) address. Note that the resulting server behavior violates the official DHCP specification.

Subnet 192.168.1.0

Subnet mask 255.255.255.0

Available range 192.168.1.1 - 192.168.1.254

Range 192.168.1.100 192.168.1.254
From To

3. Configuration des Règles de Pare-feu

- ✓ Pour permettre aux appareils du réseau local d'accéder à Internet et pour gérer le trafic entre les interfaces :

Floating WAN LAN DMZ

Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/0 B	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	<input checked="" type="checkbox"/> 0/0 B	IPv4 TCP	LAN net	*	*	*	*	none		reseau local à accéder à inernet	

4. Étapes pour Établir les Règles de Pare-feu

- ✓ Règle pour le LAN vers la DMZ

Firewall / Rules / LAN

Floating WAN LAN DMZ

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	0/0 B	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	0/0 B	IPv4 TCP	LAN net	*	DMZ net	*	*	none		Allow LAN access to Debian server in DMZ	

Cette règle permettra aux appareils du réseau LAN d'accéder aux services hébergés dans la DMZ.

✓ Règle pour la DMZ

Firewall / Rules / DMZ

Floating WAN LAN DMZ

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	0 / 1008 B	IPv4 ICMP any	*	*	*	*	*	none			
<input type="checkbox"/>	0 / 0 B	IPv4 ICMP any	LAN net	*	DMZ net	*	*	none			
<input type="checkbox"/>	1 / 78.86 MiB	IPv4 TCP	DMZ net	*	*	*	*	none		Allow DMZ to access the internet	

✓ Règle pour le WAN vers la DMZ (si nécessaire)

Si vous souhaitez que des utilisateurs externes puissent accéder à un service spécifique dans la DMZ (comme un serveur web), vous devez configurer une règle NAT et une règle de pare-feu.

Firewall / Rules / WAN

Floating

WAN

LAN

DMZ

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<div></div>	<div></div> 0 / 0 B	*	RFC 1918 networks	*	*	*	*	*		Block private networks	<div></div>
<div></div>	<div></div> 0 / 0 B	*	Reserved Not assigned by IANA	*	*	*	*	*		Block bogon networks	<div></div>
<div><div></div></div>	<div></div> 0 / 0 B	IPv4 TCP	*	*	WAN address	80 (HTTP)	*	none		allow external access to DMZ web server	<div></div> <div></div> <div></div> <div></div>

✓ Configurer le NAT pour rediriger le trafic vers la DMZ

Si on a configuré un serveur web dans la DMZ et que l'on souhaite qu'il soit accessible depuis Internet

Firewall / NAT / Port Forward										
The changes have been applied successfully. The firewall rules are now reloading in the background. Monitor the filter reload progress.										
Port Forward <u>1:1</u> Outbound NPt										
Rules										
<input type="checkbox"/>	Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
<input type="checkbox"/>	<input checked="" type="checkbox"/> WAN	TCP	*	*	WAN address	80 (HTTP)	DMZ address	80 (HTTP)	NAT redirection dmz	

IV) Testes

✓ Tester la Connectivité Interne

Diagnostics / Ping

Ping


Hostname

IP Protocol

Source address
Select source address for the ping.

Maximum number of pings
Select the maximum number of pings.

Seconds between pings
Select the number of seconds to wait between pings.

 Ping

Results

```
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=128 time=19.860 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=21.337 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=22.355 ms

--- 8.8.8.8 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 19.860/21.184/22.355/1.025 ms
```

✓ Teste avec le serveur web

Installer d'un serveur web sur la VM Debian

1. Connectez-vous à votre VM Debian.

2. Ouvrez un terminal.

3. Tapez ces commandes :

...

sudo apt update

sudo apt install apache2

...

4. Apache devrait maintenant être installé et fonctionnel.

Puis creer un site avec debian

Étape 10 : Test

1. Sur un ordinateur connecté au réseau LAN, ouvrez un navigateur.

2. Essayez d'accéder à l'adresse IP publique de votre pfSense.
3. Vous devriez voir la page par défaut d'Apache.

Objectif

L'objectif est de s'assurer que le serveur web dans la DMZ peut accéder à Internet. Si les pings réussissent, cela signifie que la configuration est correcte.

Serveur lan elle doit héberger le serveur web et le ftp