



PROJET SECURITE RESEAU

PFSENSE, DMZ & FIREWALLING

YANIS HORAIRA

ETUDIANT EN BUT RESEAUX ET TELECOMMUNICATIONS – IUT BLAGNAC
Parcours cybersécurité



Table des matières

I. Schéma du lab	3
II. Installation de pfSense	4
III. Configuration de l'interface LAN sur pfSense	5
IV. Connexion à pfSense et création de la DMZ	7
VI. Configuration des règles de pare – feu	11
VII. Configuration des règles de NAT	15

I. Schéma du lab

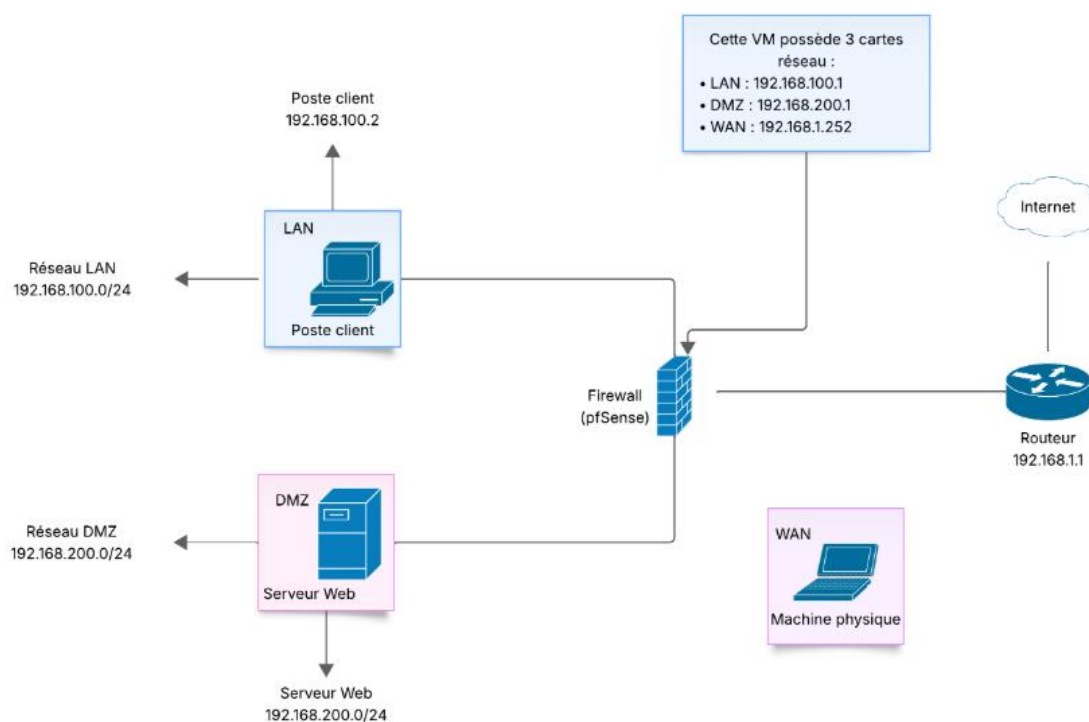


Figure 1 : Schéma du lab

Ce schéma illustre un réseau virtualisé sécurisé basé sur pfSense, configuré comme pare-feu. La VM pfSense dispose de trois cartes réseau : une pour le LAN (poste client), une pour la DMZ (serveur web), et une pour le WAN (accès Internet via la machine physique).

L'utilisation de trois cartes réseau permet d'isoler les flux entre les différentes zones. Le LAN est dédié aux postes clients internes, la DMZ héberge un serveur web, et le WAN assure la liaison avec Internet via le routeur de la machine physique.

L'interface WAN est en bridge avec la carte réseau physique, ce qui donne un accès réel à Internet. Cela permet aussi de simuler un utilisateur externe accédant au serveur web dans la DMZ.

II. Installation de pfSense

Au cours de ce projet, nous utiliserons la version 2.7.2 de pfSense.

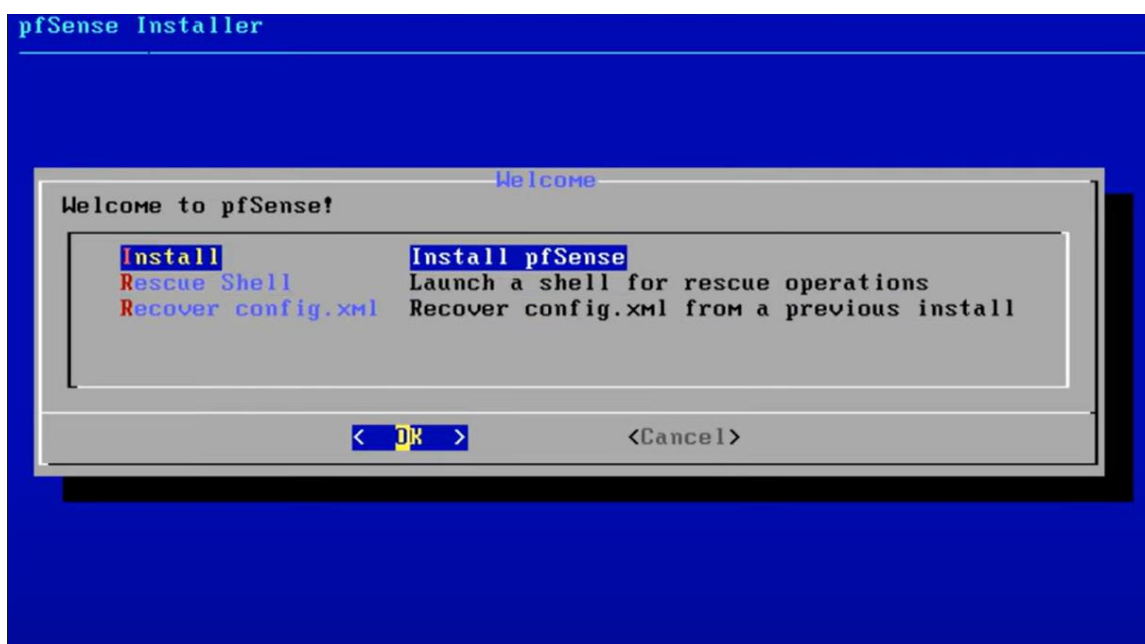


Figure 2 : Installation de pfSense

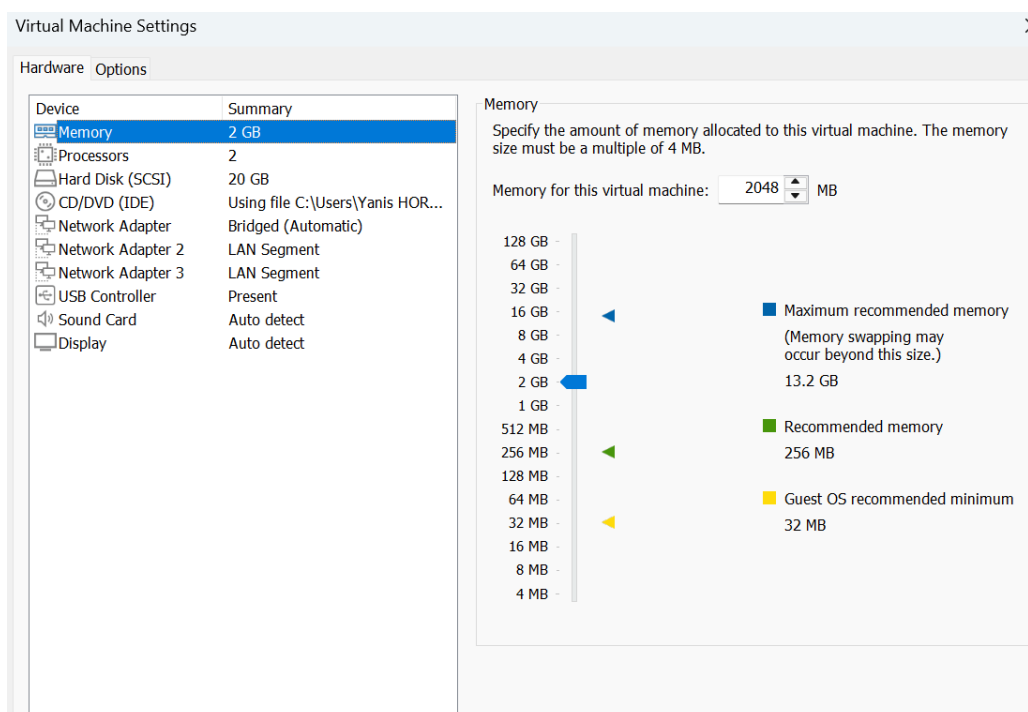


Figure 3 : Configuration des paramètres de la VM

On retrouve bien 3 cartes réseau. La première, étant en bridge, correspond à celle du WAN. La « Network Adapter 2 » est associée au LAN et la « Network Adapter 3 » à la DMZ.

III. Configuration de l'interface LAN sur pfSense

```
Enter the new LAN IPv4 address. Press <ENTER> for none:
> 192.168.100.1

Subnet masks are entered as bit counts (as in CIDR notation) in pfSense.
e.g. 255.255.255.0 = 24
     255.255.0.0   = 16
     255.0.0.0     = 8

Enter the new LAN IPv4 subnet bit count (1 to 32):
> 24

For a WAN, enter the new LAN IPv4 upstream gateway address.
For a LAN, press <ENTER> for none:
>

Configure IPv6 address LAN interface via DHCP6? (y/n) n

Enter the new LAN IPv6 address. Press <ENTER> for none:
>

Do you want to enable the DHCP server on LAN? (y/n) n
Disabling IPv4 DHCPD...
Disabling IPv6 DHCPD...

Do you want to revert to HTTP as the webConfigurator protocol? (y/n) █
```

Figure 4 : Configuration de l'interface LAN

Au cours de cette étape, nous configurons les paramètres IP relatifs à l'interface LAN, conformément à ceux se trouvant sur le schéma réseau.

```
The IPv4 LAN address has been set to 192.168.100.1/24
You can now access the webConfigurator by opening the following URL in your web
browser:
      https://192.168.100.1/
```

Figure 6 : URL pour accéder à l'interface graphique de pfSense

A la fin de notre configuration, on obtient l'URL nous permettant d'accéder à l'interface graphique nous permettant la configuration de notre pare – feu (DMZ, règles de NAT, règles de pare – feu).

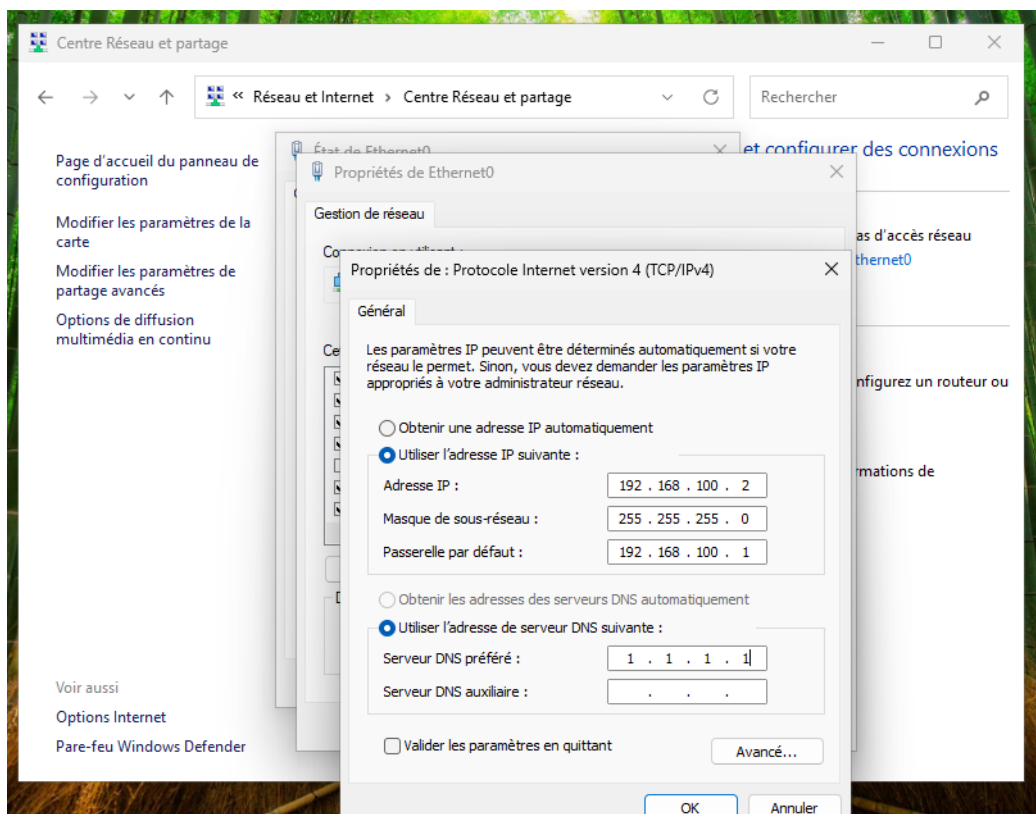


Figure 7 : Configuration du client (Windows 11)

Ci – dessus, nous observons la configuration réseau du client, se trouvant dans le LAN.

IV. Connexion à pfSense et création de la DMZ

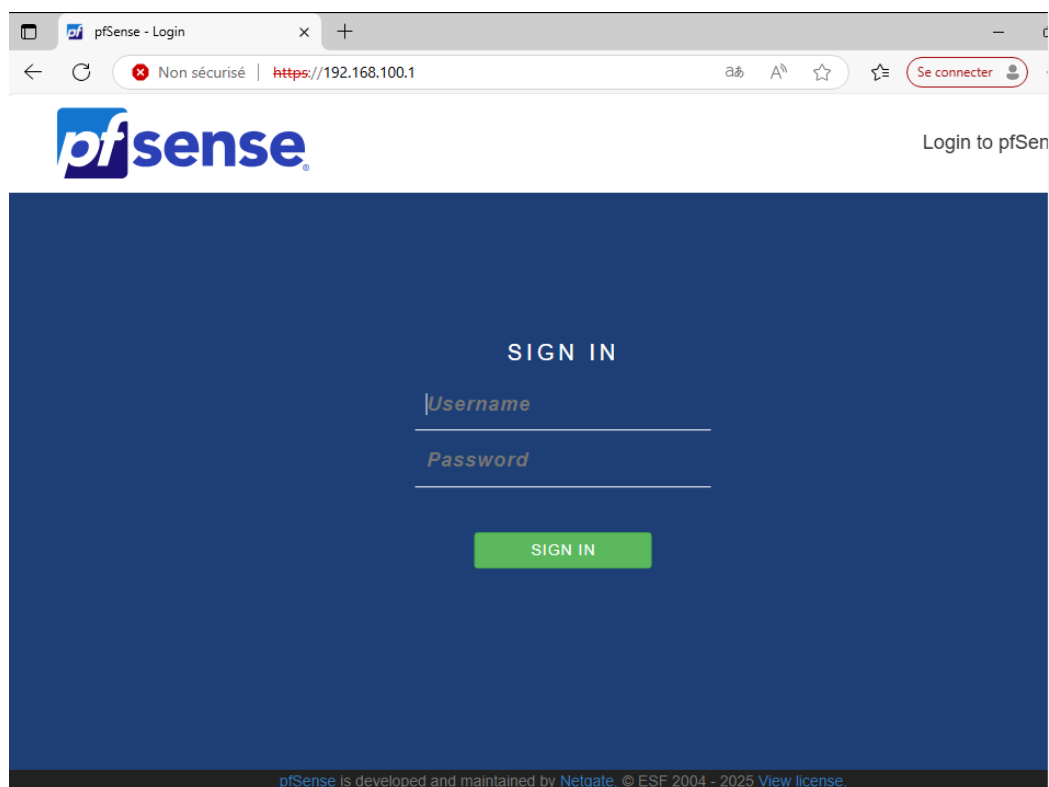


Figure 8 : Accès à l'interface graphique de pfSense

Une fois le poste client configuré, nous pouvons désormais accéder, depuis ce dernier, à l'interface graphique de pfSense, en utilisant l'URL qui nous a précédemment été fournie au cours de l'étape III.

Description
Enter a description (name) for the interface here.

IPv4 Configuration Type

IPv6 Configuration Type

MAC Address
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

MTU
If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstance

MSS
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) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex
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.

Static IPv4 Configuration

IPv4 Address /

Figure 9 : Création de la DMZ depuis l'interface graphique de pfSense




Interfaces ⚙️ ⌵ ✕			
 WAN	↑	1000baseT <full-duplex>	192.168.1.252
 LAN	↑	1000baseT <full-duplex>	192.168.100.1
 DMZ	↑	1000baseT <full-duplex>	192.168.200.1

Figure 10 : Interface configurée sur le pare – feu

Ainsi, nous obtenons, conformément au schéma réseau, les trois interfaces étant chacune associées à leurs adresses IP respectives.

V. Configuration du serveur web en DMZ

Une fois la DMZ configurée, on peut désormais mettre en place le serveur web à l'aide de l'outil IIS :

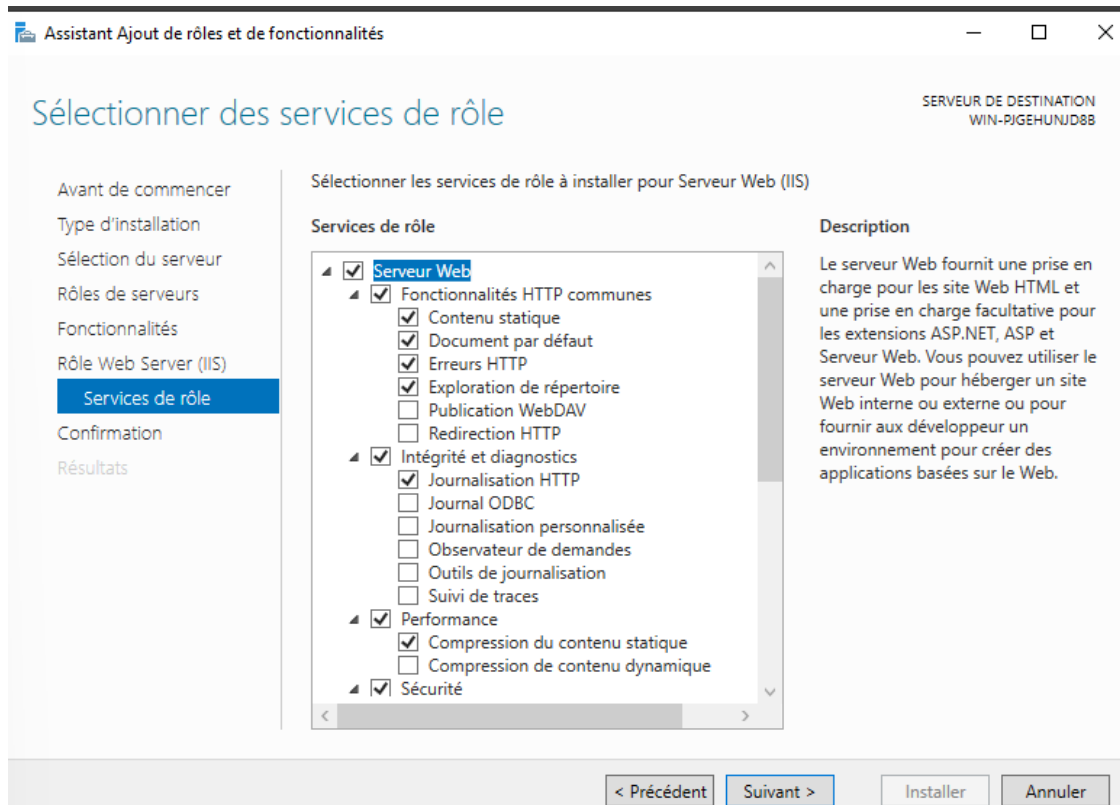


Figure 11 : Mise en place du serveur web à l'aide de IIS sur le Windows Server 2022

Le site web est désormais accessible, en local, mais également depuis le LAN :

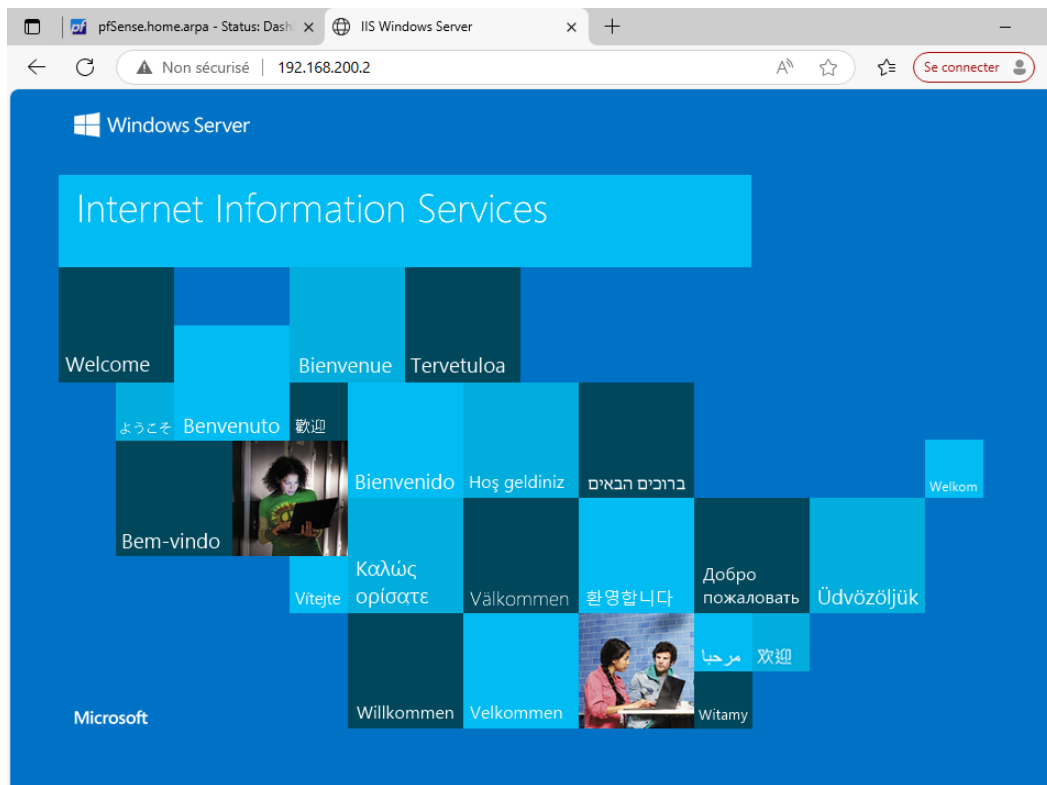


Figure 12 : Accessibilité du site web

Ceci est normal, d'après la 2^e règle de pare – feu pour le LAN, ce dernier peut accéder, pour le moment, à n'importe quel réseau :

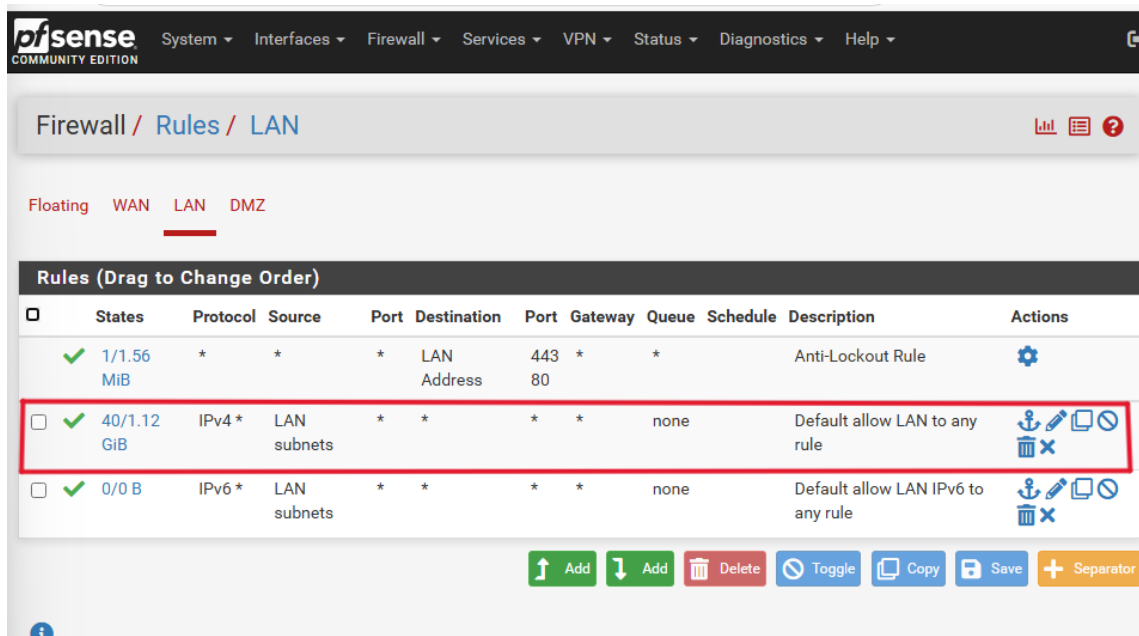


Figure 13 : Règle de pare – feu du LAN autorisant l'accès à tous les réseaux

VI. Configuration des règles de pare – feu

Règle n°1 : Blocage du trafic en provenance du LAN vers la DMZ

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 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 LAN subnets Source Address /

Destination

Destination ☐ Invert match DMZ subnets Destination Address /

Figure 14 : Règle de pare – feu bloquant le trafic du LAN vers la DMZ

On ajoute une règle de niveau supérieur bloquant le trafic du LAN vers la DMZ.

Ainsi, si une machine du LAN est compromise (ex : une attaque par phishing visant un poste de travail dans le LAN a réussi), elle ne pourra pas attaquer notre serveur web se trouvant en DMZ.

Cependant, dans ce cas, on ne pourra plus accéder au site web (se trouvant dans la DMZ) depuis le LAN.

Ainsi, nous devons créer une règle de niveau supérieur autorisant le trafic du LAN vers l'adresse IP du serveur web (192.168.200.2), sur le port 80 (HTTP).

Règle n°2 : Autorisation du trafic en provenance du LAN vers le serveur web

Edit Firewall Rule

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

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

Protocol
 Choose which IP protocol this rule should match.

Source

Source ☐ Invert match /
 [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 /
 Destination Port Range
 From Custom 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

Figure 15 : Règle de pare – feu autorisant le trafic du LAN vers la DMZ

Désormais, nous pouvons de nouveau accéder au site web tout en limitant le risque d'intrusion dans la DMZ via le LAN.

Firewall / Rules / LAN

The changes have been applied successfully. The firewall rules are now reloading in the background.
[Monitor the filter reload progress.](#)

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"/>	4/1.71 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
<input checked="" type="checkbox"/>	0/0 B	IPv4 TCP	LAN subnets	*	192.168.200.2	80 (HTTP)	*	none		autoriser accès serveur web depuis LAN en HTTP	
<input checked="" type="checkbox"/>	0/780 B	IPv4 *	LAN subnets	*	DMZ subnets	*	*	none		bloquer lan vers dmz	
<input checked="" type="checkbox"/>	12/1.12 GiB	IPv4 *	LAN subnets	*	*	*	*	none		Default allow LAN to any rule	
<input checked="" type="checkbox"/>	0/0 B	IPv6 *	LAN subnets	*	*	*	*	none		Default allow LAN IPv6 to any rule	

Figure 16 : Ordre des règles de pare – feu concernant le LAN

Nous devons faire attention à l'ordre des règles du pare – feu. La règle autorisant le trafic allant du LAN vers le serveur web doit être « au – dessus » (de niveau supérieur) de celle bloquant le trafic du LAN vers la DMZ.

Dans le cas contraire, nous ne pourrions pas accéder au site web.

Règle n°3 : Blocage des flux en provenance de la DMZ vers le LAN

La DMZ occupe un rôle de « tampon » entre l'extérieur (Internet) et l'intérieur (LAN), ainsi, notre serveur web est exposé aux attaques.

Cela signifierait que si un attaquant a réussi à s'introduire dans la DMZ, il pourrait accéder au LAN.

Par conséquent, nous devons ajouter une règle de pare – feu évitant ce type d'attaque (pivoting par exemple).

The screenshot shows a firewall rule configuration interface with three main sections: Source, Destination, and Extra Options.

- Source:** The 'Source' dropdown is set to 'DMZ subnets'. There is an 'Invert match' checkbox and a 'Source Address' field.
- Destination:** The 'Destination' dropdown is set to 'LAN subnets'. There is an 'Invert match' checkbox and a 'Destination Address' field. Below this, the 'Destination Port Range' is configured with 'From' and 'To' dropdowns set to '(other)', and 'Custom' input fields for each.
- Extra Options:** The 'Log' checkbox is unchecked. A hint states: '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:** The description field contains the text 'bloquer DMZ vers LAN'.

Figure 17 : Règle de pare – feu bloquant le trafic de la DMZ vers le LAN

VII. Configuration des règles de NAT

On ajoute une règle de port forwarding sur l'interface WAN pour rediriger le trafic TCP sur le port HTTP vers l'adresse IP du serveur web en DMZ, permettant ainsi l'accès externe au site tout en protégeant le réseau interne.

The screenshot shows a web browser window with the URL https://192.168.100.1/firewall_nat_edit.php?id=0. The page is titled "Non sécurisé" and has a "Se connecter" button. The configuration form is as follows:

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	<input type="checkbox"/> Invert match.	WAN address	
		Type	Address/mask
Destination port range	From port	Custom	To port
		HTTP	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	Address or Alias		192.168.200.2
	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		

Figure 18 : Ajout d'une règle de port forwarding

Cependant, nous devons modifier une option se trouvant sur l'interface WAN (cela nous permettra de tester l'accessibilité du site web depuis la machine physique (en effet, son adresse débute par 192.168, elle appartient au RFC 1918).

Nous devons décocher l'option ci – dessous (cette dernière est initialement cochée).

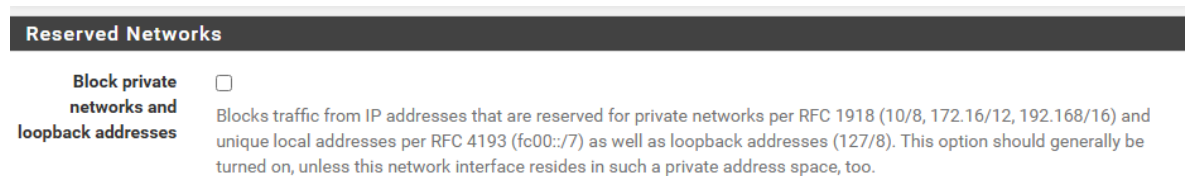


Figure 19 : Option à décocher

Nous pouvons ainsi accéder au site web depuis la machine physique :

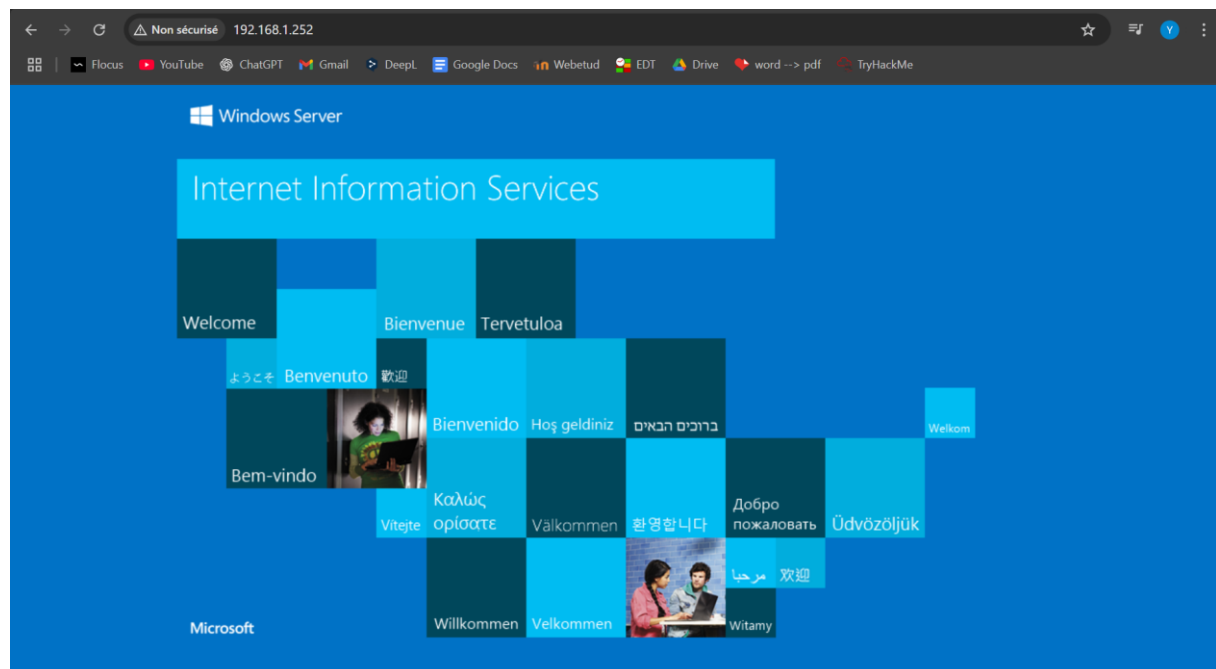


Figure 20 : Accès au site web grâce à la redirection

On remarque que la redirection a bien eu lieu (l'adresse IP entrée correspond à l'interface WAN du pare – feu).

Nous avons finalement réussi à mettre en place notre architecture sécurisée.

