Yanis HORAIRA

étudiant en BUT Réseaux et télécommunications – IUT Blagnac

Parcours cybersécurité

Projet sécurité réseau

pfsense, dmz & firewalling

**Table des matières**

[**I. Schéma du lab** 3](#_Toc204890790)

[**II. Installation de pfSense** 4](#_Toc204890791)

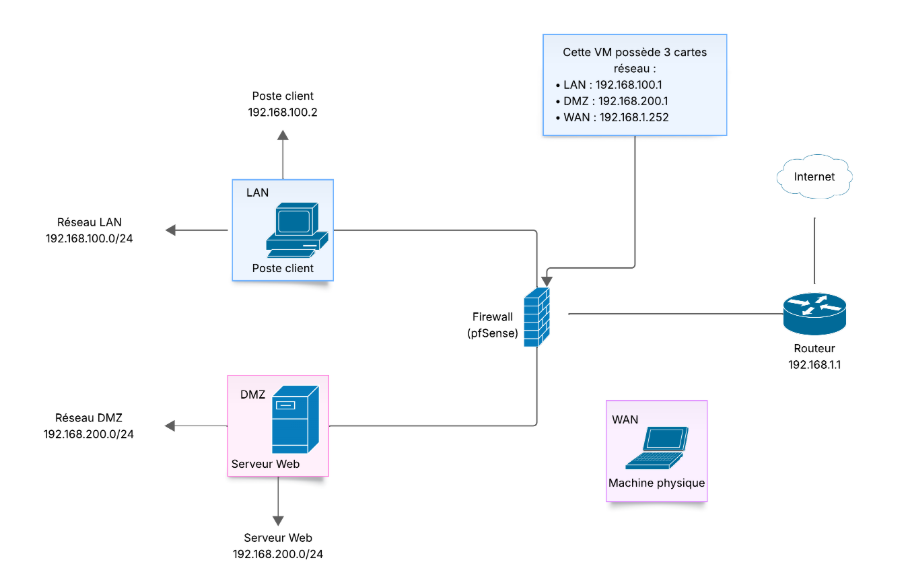
[**III. Configuration de l’interface LAN sur pfSense** 5](#_Toc204890792)

[**IV. Connexion à pfSense et création de la DMZ** 7](#_Toc204890793)

[**VI. Configuration des règles de pare – feu** 11](#_Toc204890794)

[**VII. Configuration des règles de NAT** 15](#_Toc204890795)

# **I. Schéma du lab**



*Figure 1 : Schéma du lab*

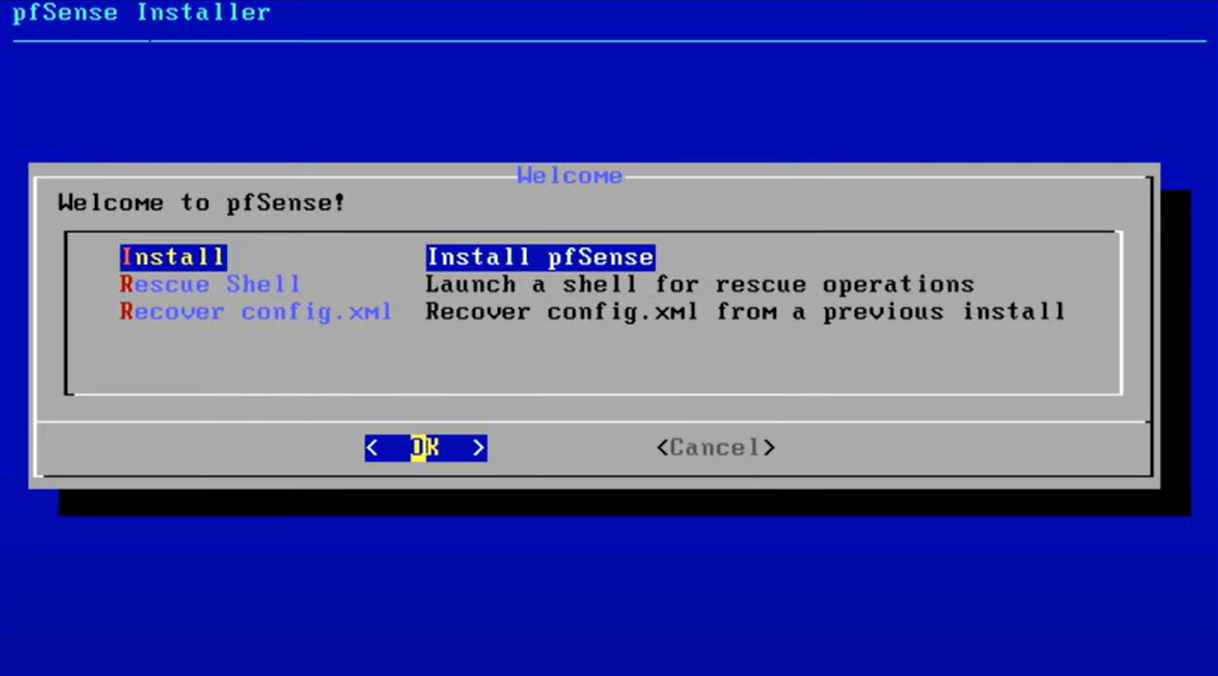
Ce schéma illustre un réseau virtualisé sécurisé basé sur pfSense, configuré comme pare-feu. La VM pfSense dispose de trois cartes réseau : une pour le LAN (poste client), une pour la DMZ (serveur web), et une pour le WAN (accès Internet via la machine physique).

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.

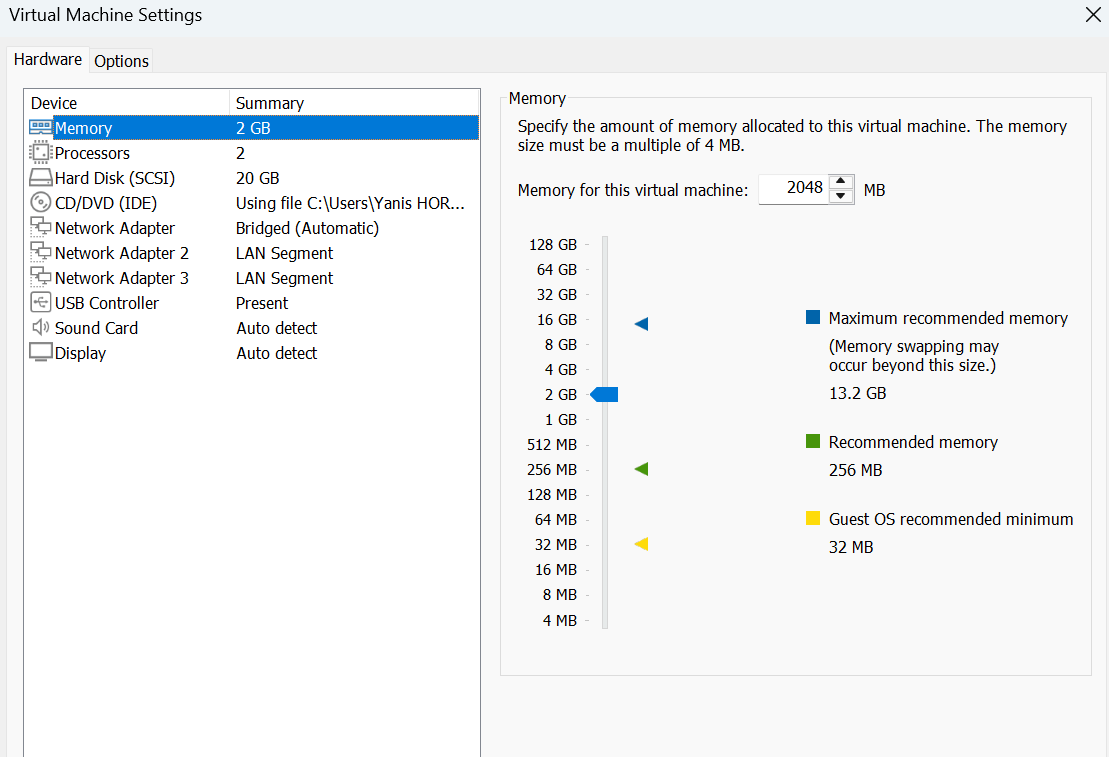
L’interface WAN est en bridge avec la carte réseau physique, ce qui donne un accès réel à Internet. Cela permet aussi de simuler un utilisateur externe accédant au serveur web dans la DMZ.

# **II. Installation de pfSense**

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



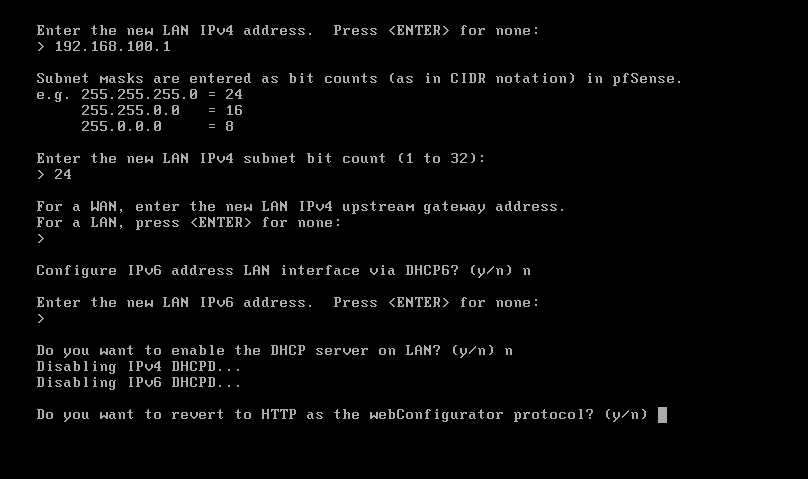
*Figure 2 : Installation de pfSense*



*Figure 3 : Configuration des paramètres de la VM*

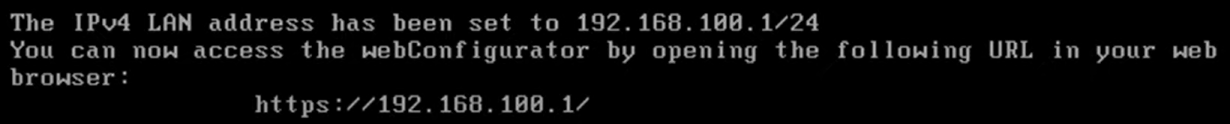
On retrouve bien 3 cartes réseau. La première, étant en bridge, correspond à celle du WAN. La « Network Adapter 2 » est associée au LAN et la « Network Adapter 3 » à la DMZ.

# **III. Configuration de l’interface LAN sur pfSense**



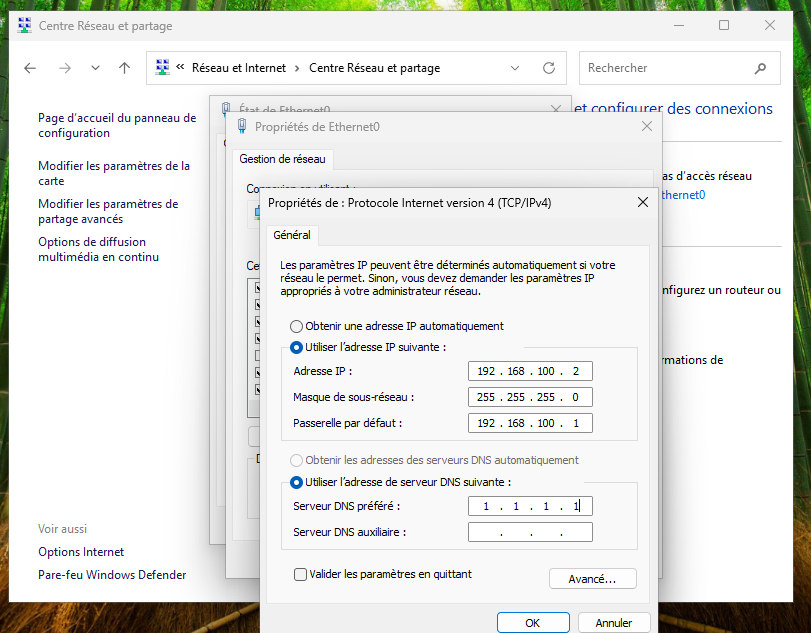
*Figure 4 : Configuration de l’interface LAN*

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



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

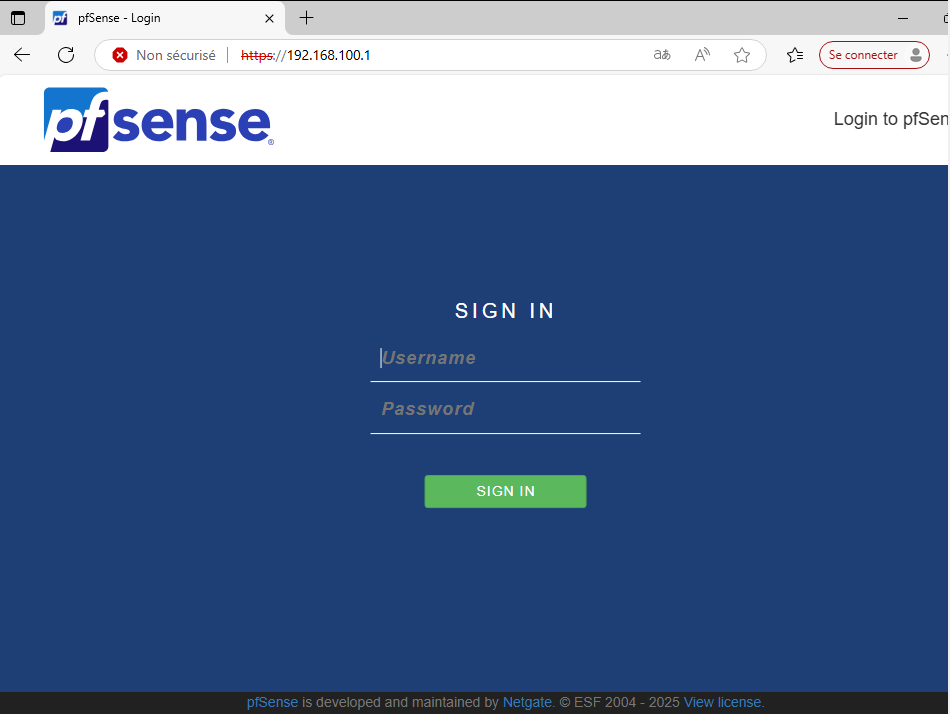
A la fin de notre configuration, on obtient l’URL nous permettant d’accéder à l’interface graphique nous permettant la configuration de notre pare – feu (DMZ, règles de NAT, règles de pare – feu).



*Figure 7 : Configuration du client (Windows 11)*

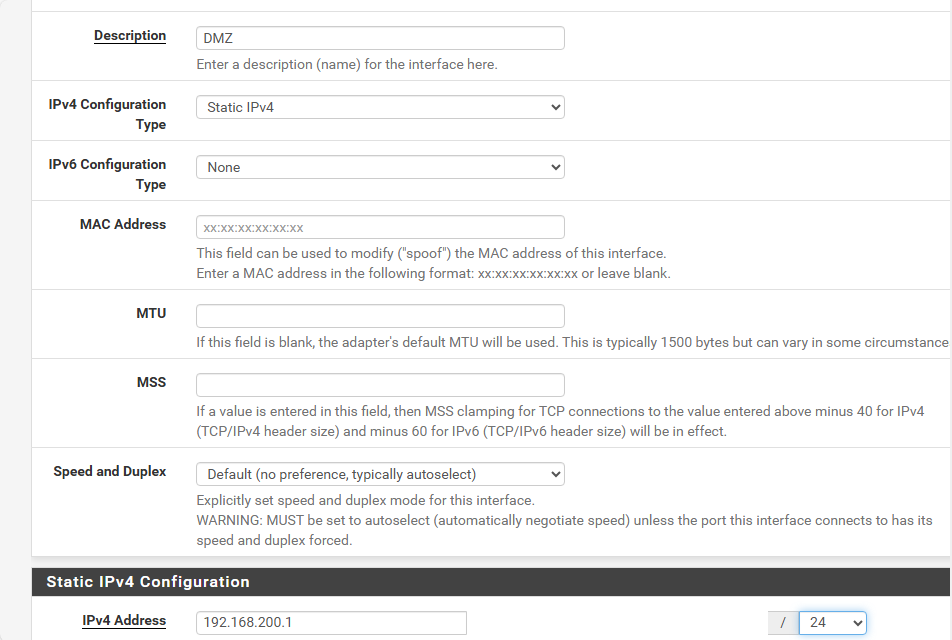
Ci – dessus, nous observons la configuration réseau du client, se trouvant dans le LAN.

# **IV. Connexion à pfSense et création de la DMZ**

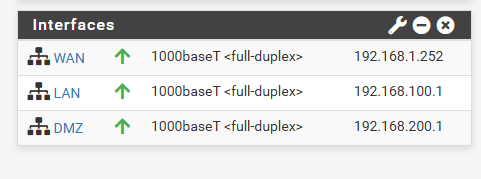


*Figure 8 : Accès à l’interface graphique de pfSense*

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.



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

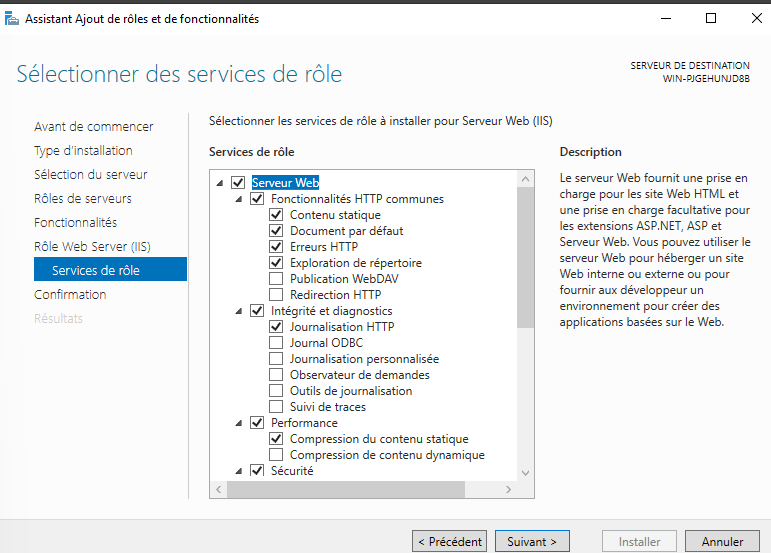


*Figure 10 : Interface configurée sur le pare – feu*

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

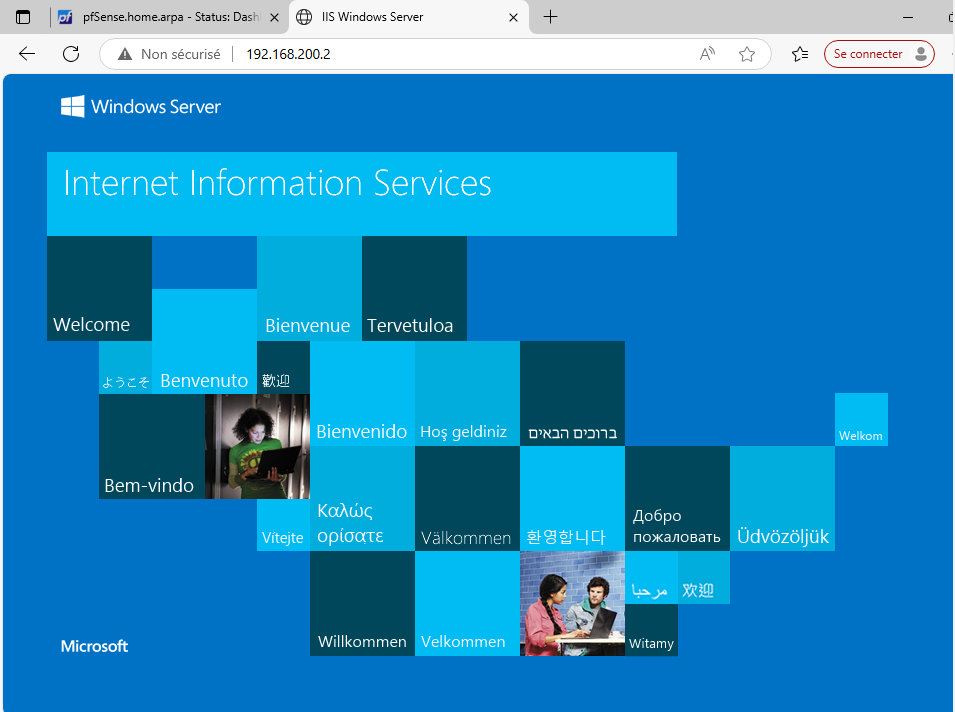
**V. Configuration du serveur web en DMZ**

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



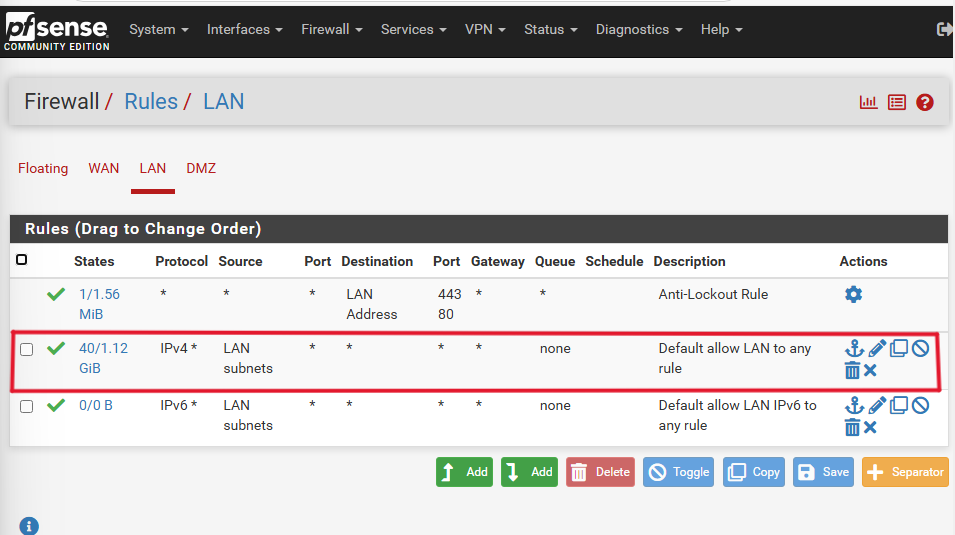
*Figure 11 : Mise en place du serveur web à l’aide de IIS sur le Windows Server 2022*

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



*Figure 12 : Accessibilité du site web*

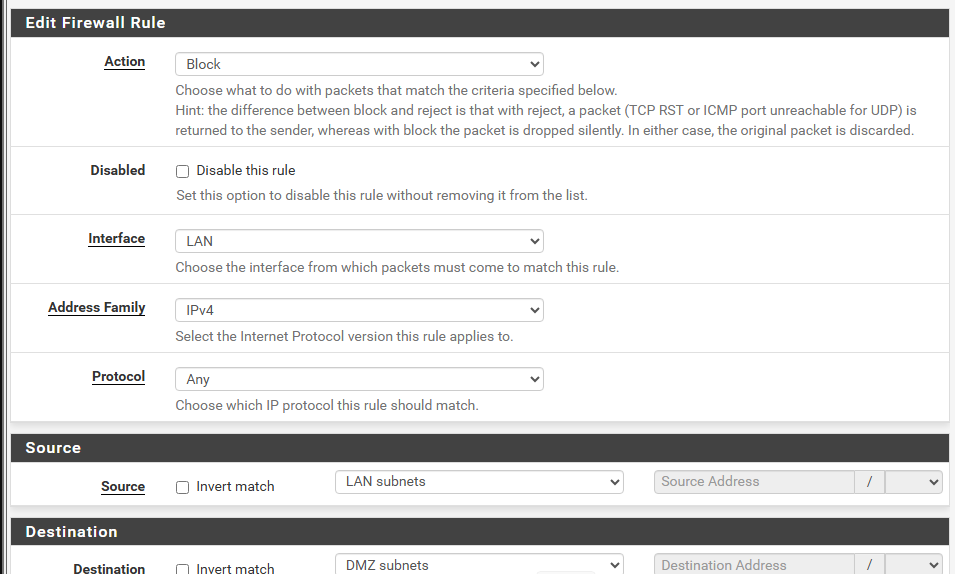
Ceci est normal, d’après la 2e règle de pare – feu pour le LAN, ce dernier peut accéder, pour le moment, à n’importe quel réseau :



*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



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

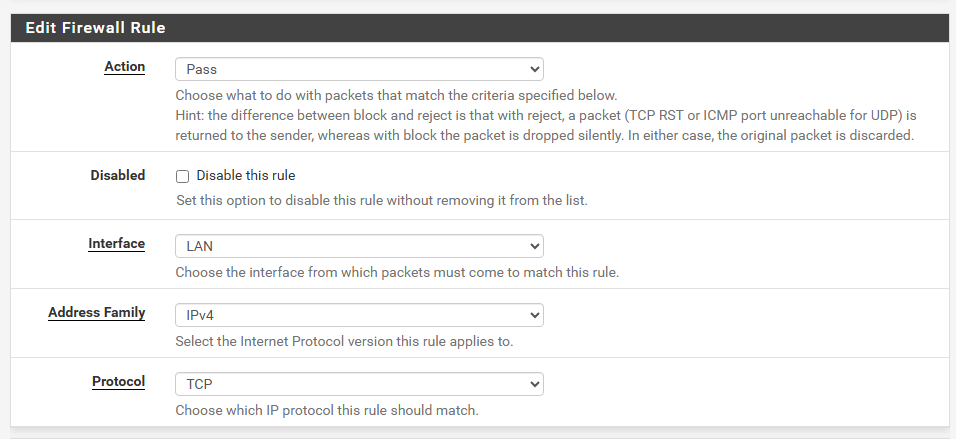
On ajoute une règle de niveau supérieur bloquant le trafic du LAN vers la DMZ.

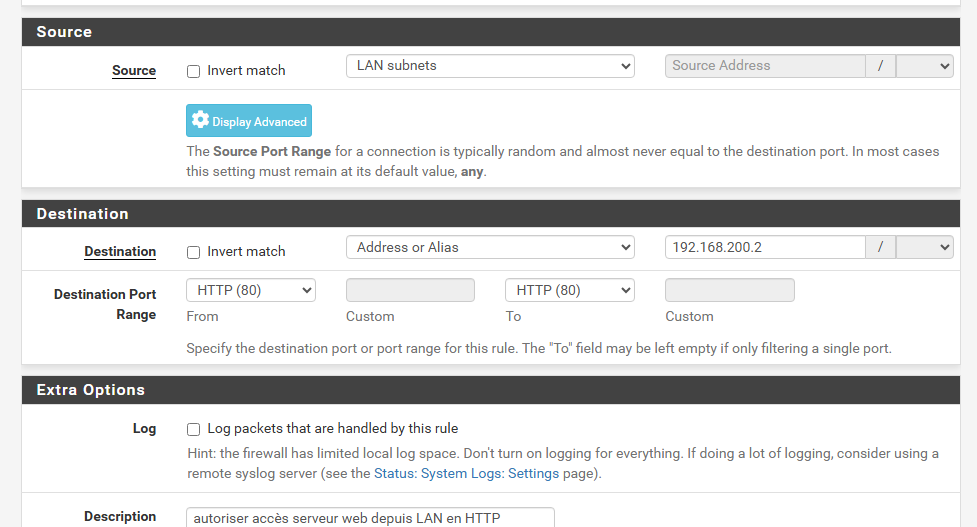
Ainsi, si une machine du LAN est compromise (ex : une attaque par phishing visant un poste de travail dans le LAN a réussi), elle ne pourra pas attaquer notre serveur web se trouvant en DMZ.

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).

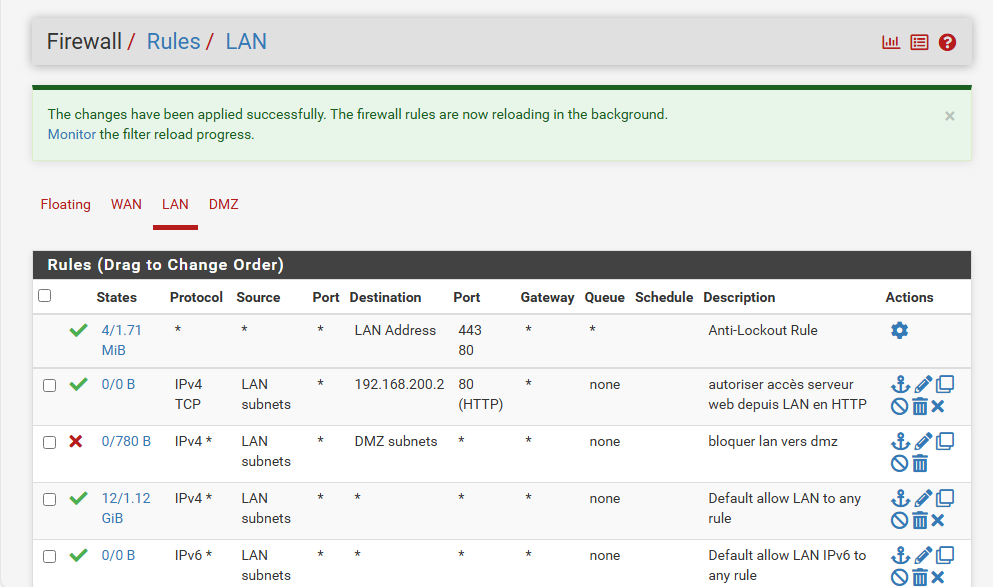
Règle n°2 : Autorisation du trafic en provenance du LAN vers le serveur web





*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.



*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.

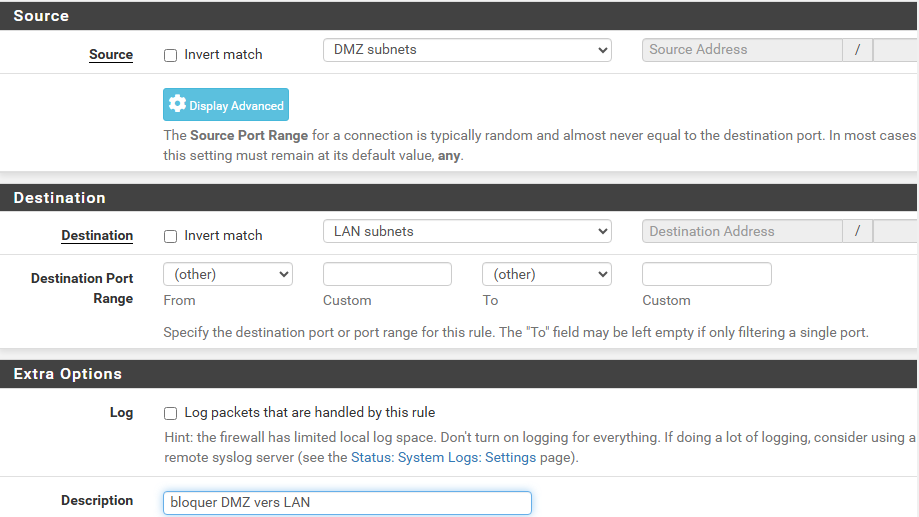
Dans le cas contraire, nous ne pourrons pas accéder au site web.

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.

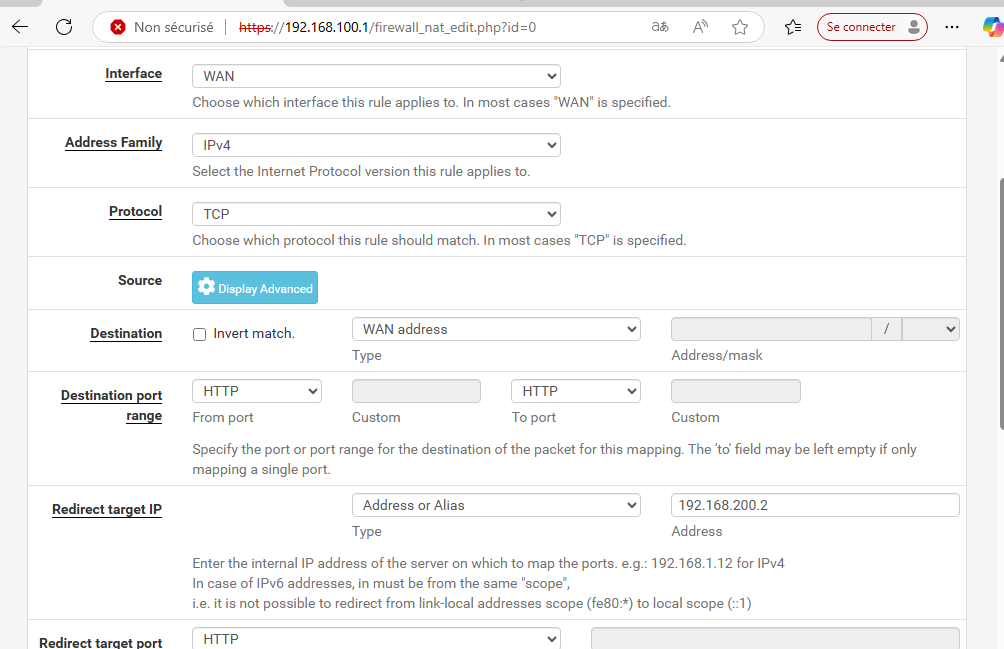
Par conséquent, nous devons ajouter une règle de pare – feu évitant ce type d’attaque (pivoting par exemple).



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

**VII. Configuration des règles de NAT**

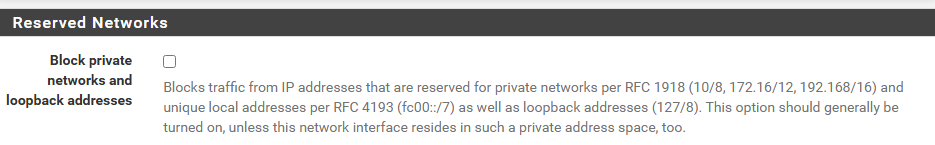
On ajoute une règle de port forwarding sur l’interface WAN pour rediriger le trafic TCP sur le port HTTP vers l’adresse IP du serveur web en DMZ, permettant ainsi l’accès externe au site tout en protégeant le réseau interne.



*Figure 18 : Ajout d’une règle de port forwarding*

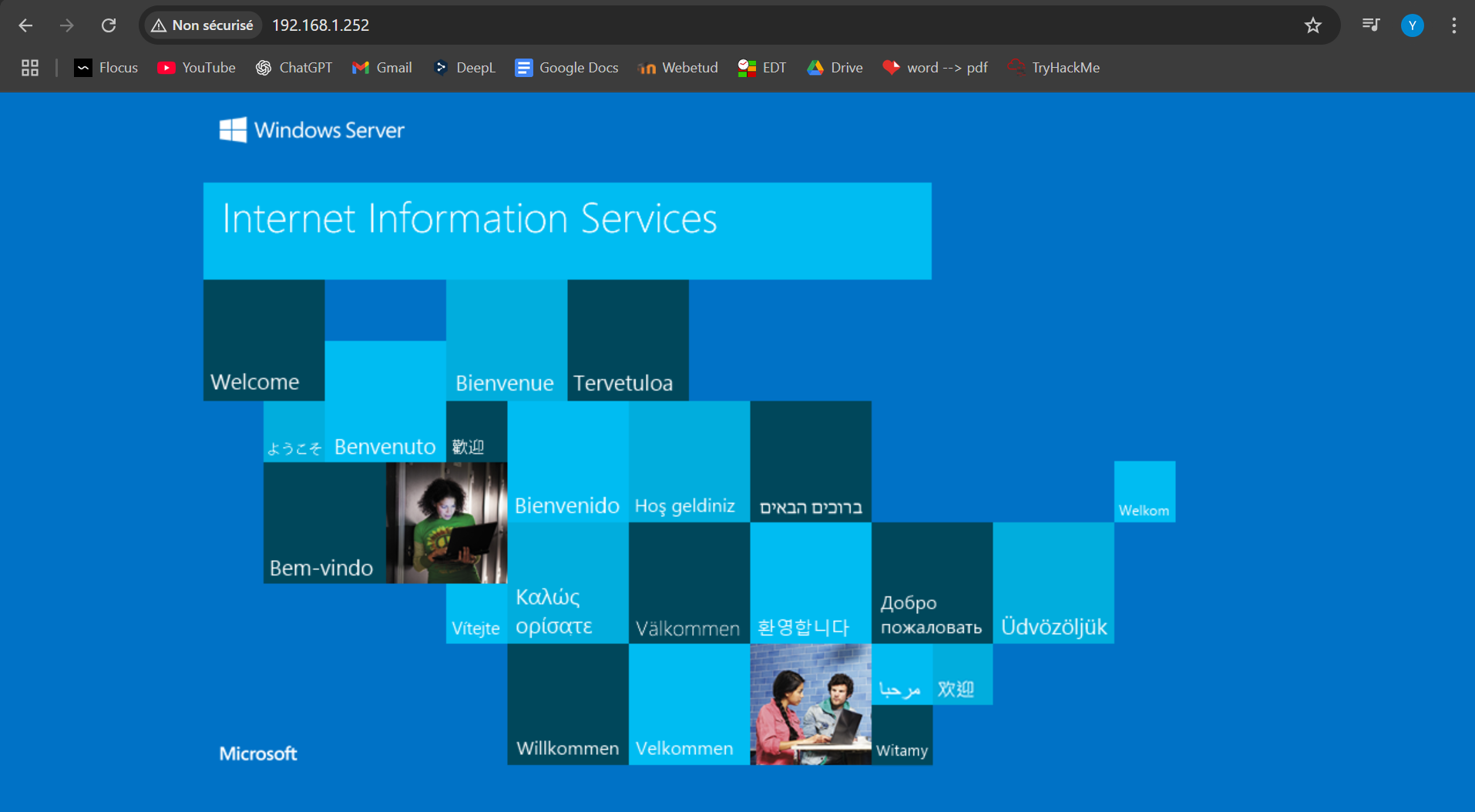
Cependant, nous devons modifier une option se trouvant sur l’interface WAN (cela nous permettra de tester l’accessibilité du site web depuis la machine physique (en effet, son adresse débute par 192.168, elle appartient au RFC 1918).

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.