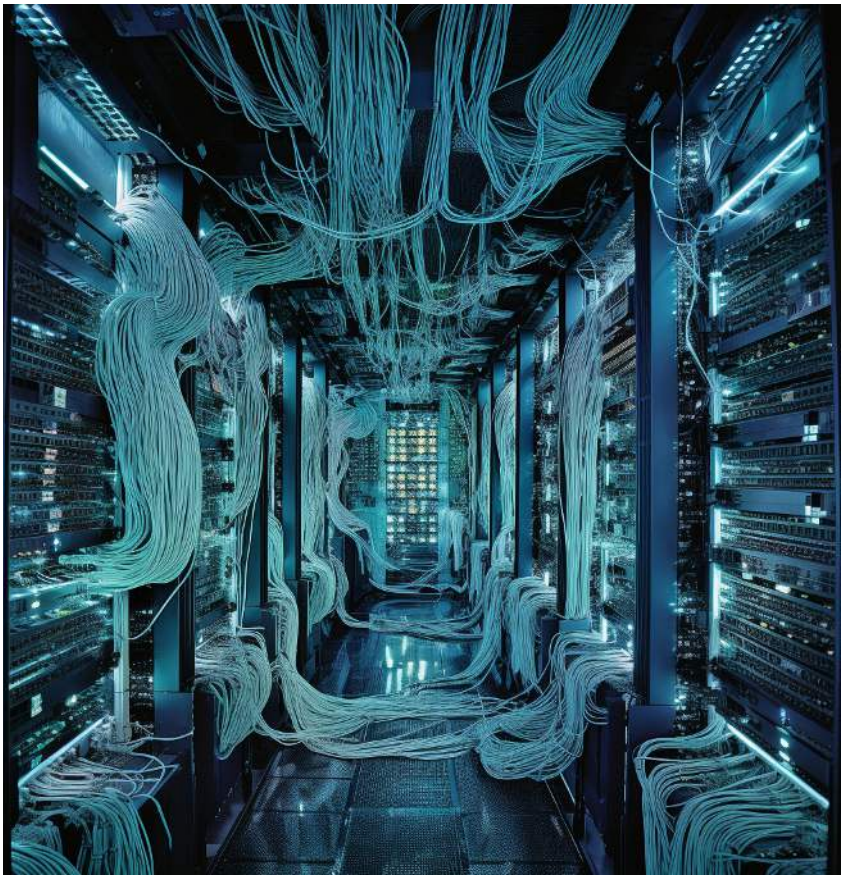
Dossier Technique Infrastructure et Réseau



Fait par :
SCHELLENS Kylian

Introduction

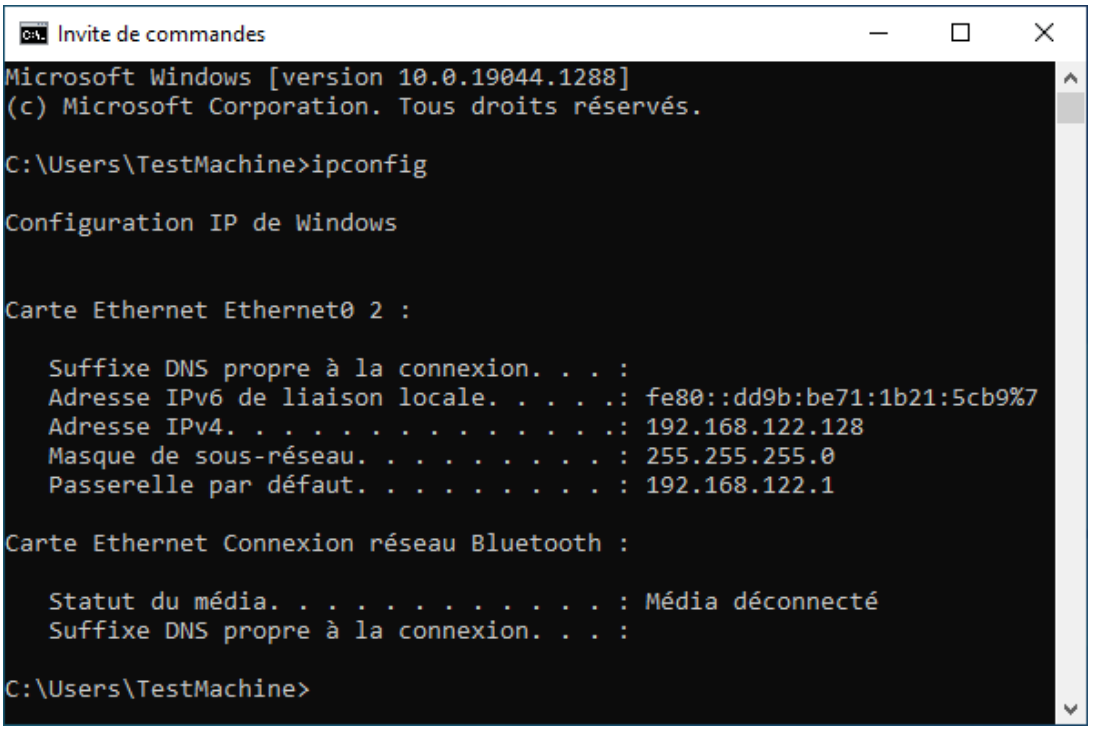
Ce dossier détaille l'architecture et la configuration d'une infrastructure réseau sophistiquée développée dans l'environnement de simulation GNS3. Le pivot de cette infrastructure est le routeur firewall pfSense, qui gère trois interfaces réseau distinctes : LAN, WAN et DMZ.

Description et Configuration du Réseau

Notre réseau est conçu pour optimiser la sécurité, la flexibilité et l'efficacité opérationnelle. Le routeur firewall pfSense, au centre de notre architecture, offre une sécurité de pointe et un contrôle précis du trafic réseau.

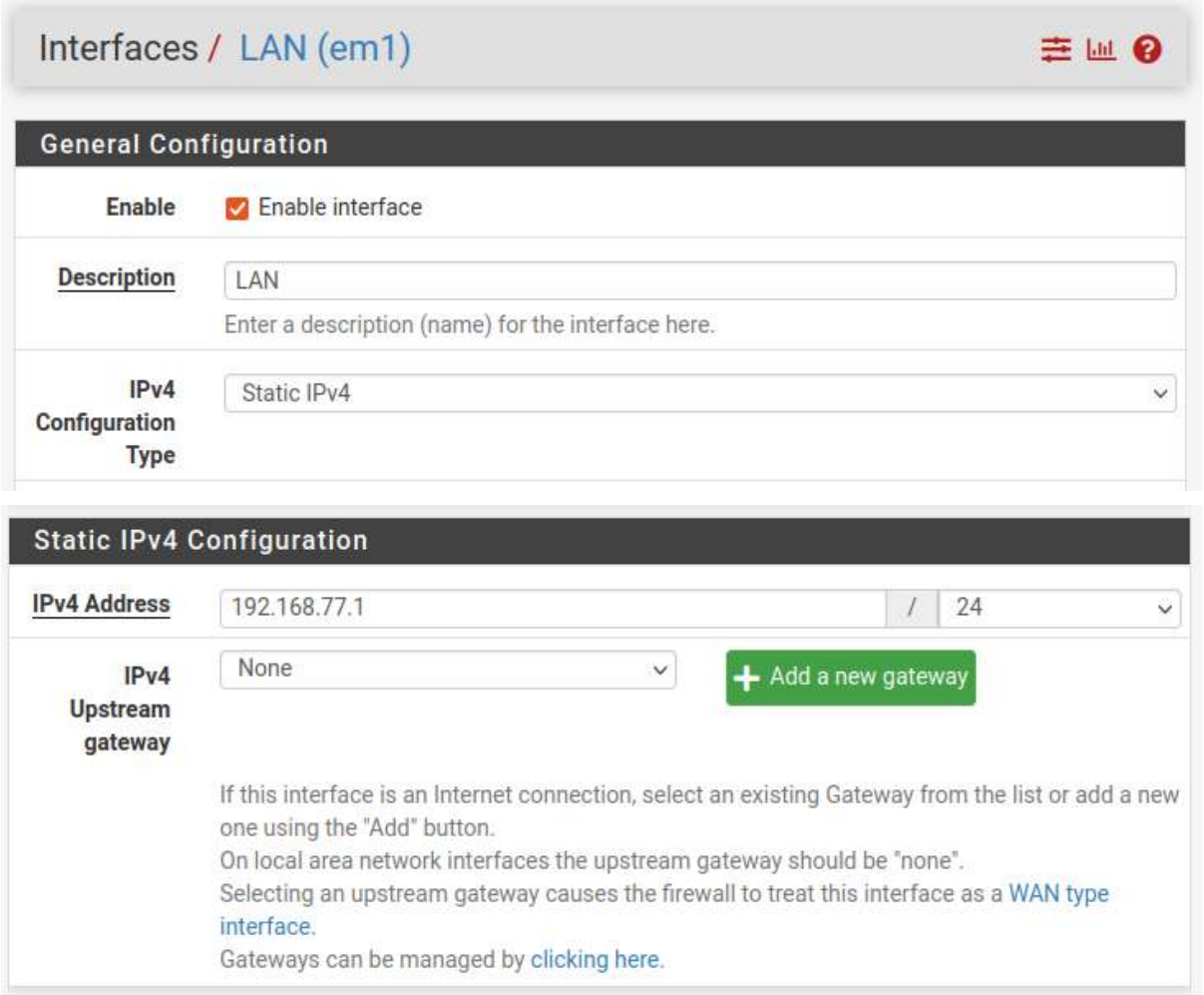
1. **Interface WAN** :

L'interface WAN, avec l'adresse IP statique `192.168.122.149`, est reliée à un switch qui gère le trafic vers un PC Windows 10 et un dispositif NAT, agissant comme passerelle vers Internet.



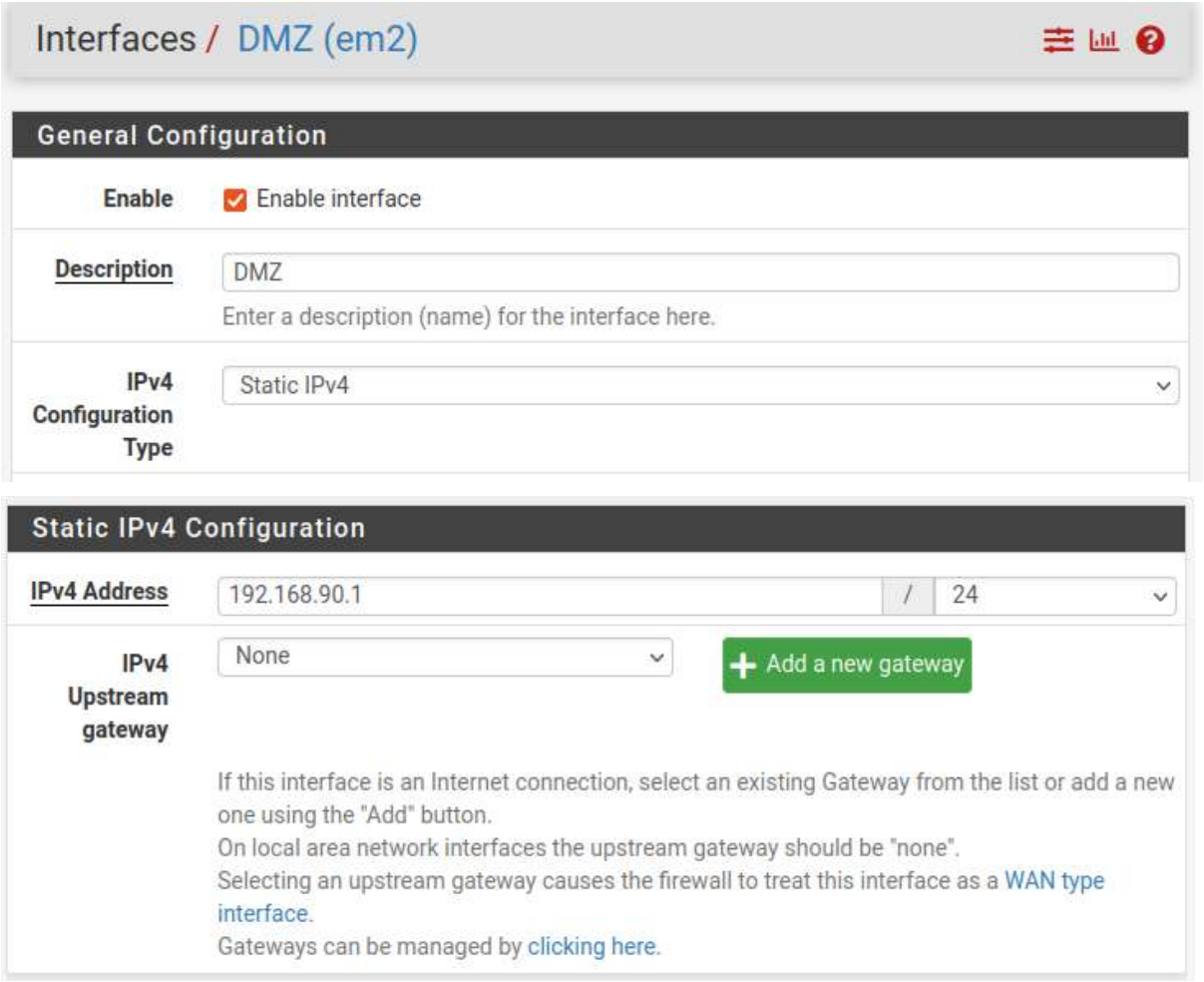
2. Interface LAN:

Cette interface, configurée avec l'adresse IP statique `192.168.77.1`, est connectée à un switch dédié qui dessert deux PC clients



3. Interface DMZ :

L'interface DMZ, ayant l'adresse IP statique `192.168.90.1`, est connectée à un switch séparé qui est ensuite relié à un serveur Ubuntu, établissant ainsi une zone démilitarisée pour minimiser les risques de sécurité.



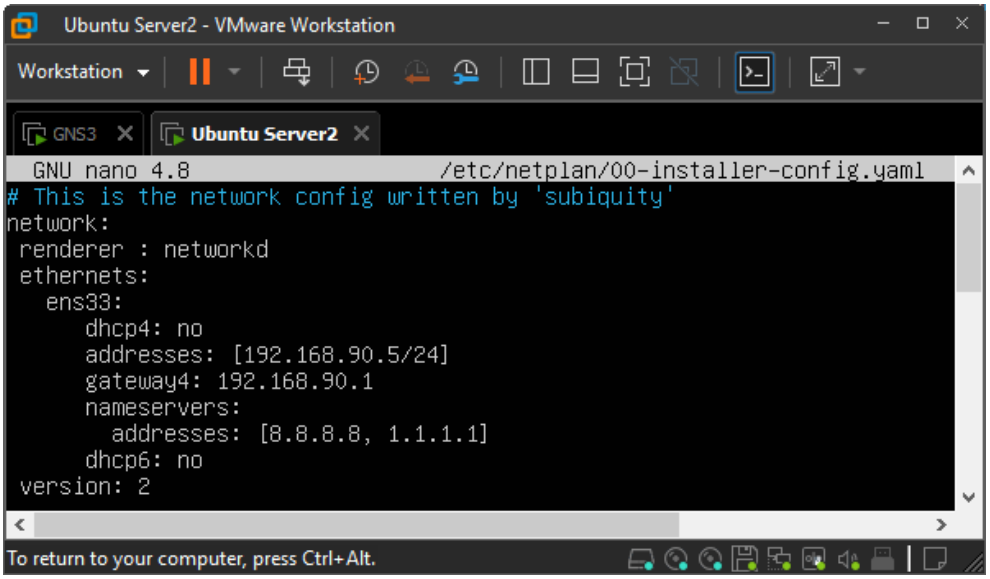
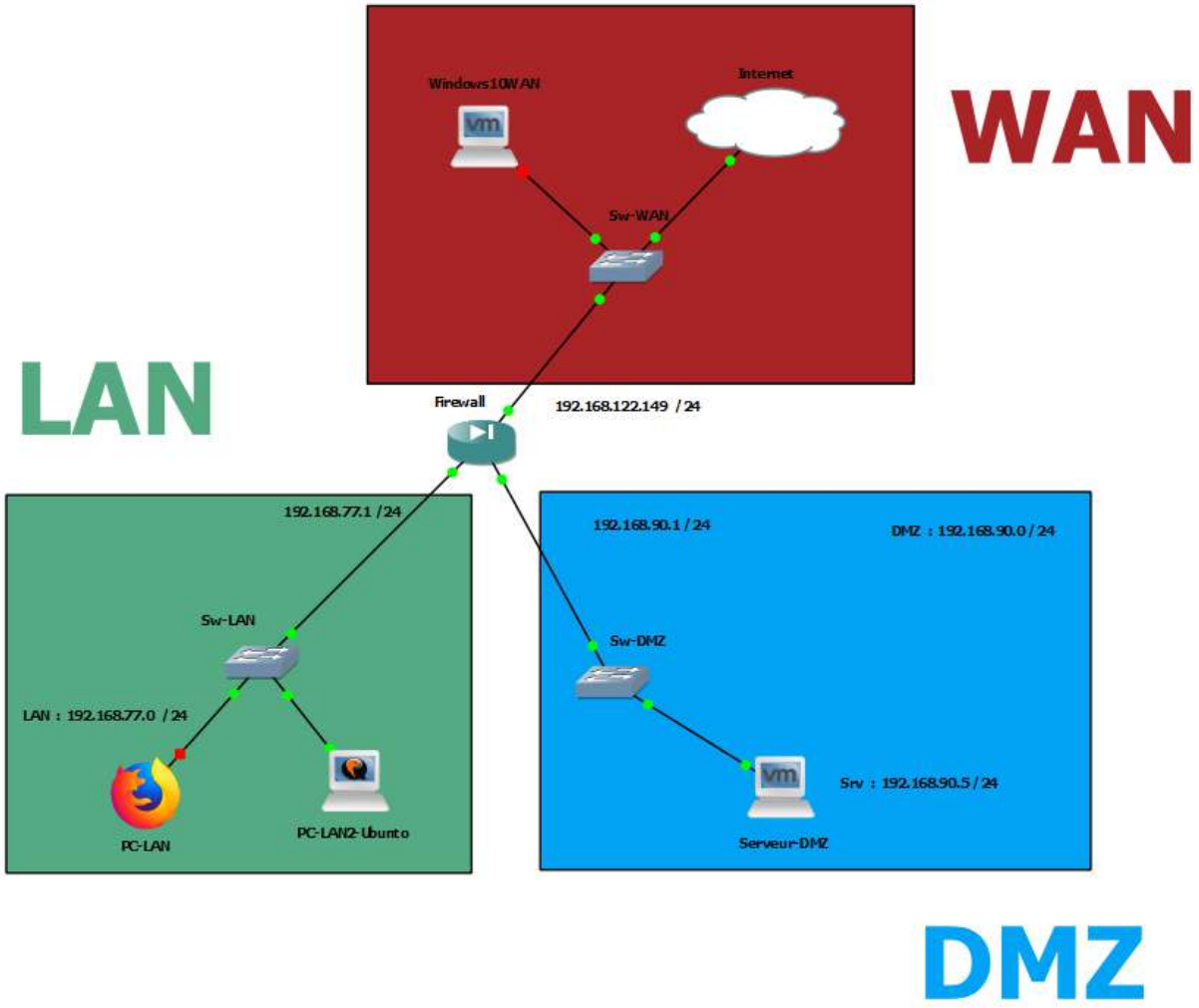


Diagramme du Réseau

Le diagramme de réseau visuel donne une représentation claire de l'architecture globale du réseau, montrant comment chaque composant est interconnecté pour fournir un système réseau solide et sécurisé.

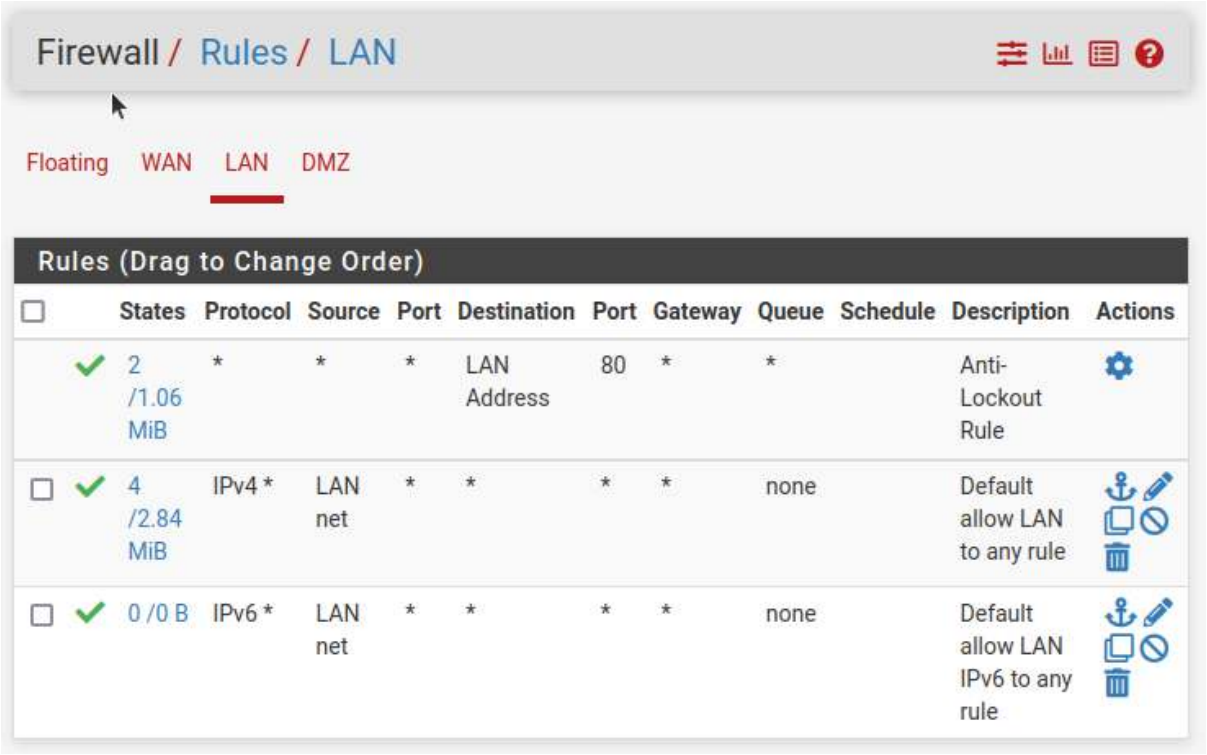


Stratégies de Sécurité du Réseau

Un aspect critique de notre réseau est sa robustesse en matière de sécurité. Nous avons mis en place des politiques de sécurité spécifiques pour chaque segment du réseau :

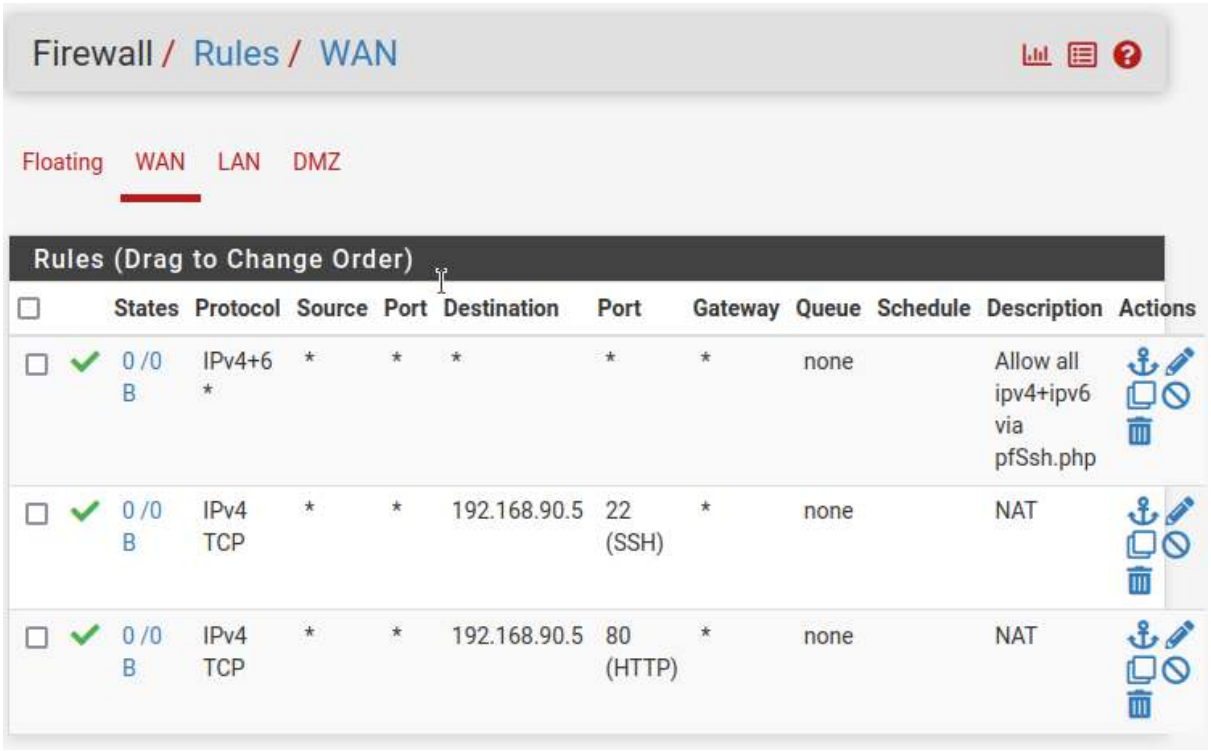
1. LAN :

Les PC clients sur le LAN ont accès à tous les autres segments du réseau, offrant une flexibilité maximale aux utilisateurs internes.



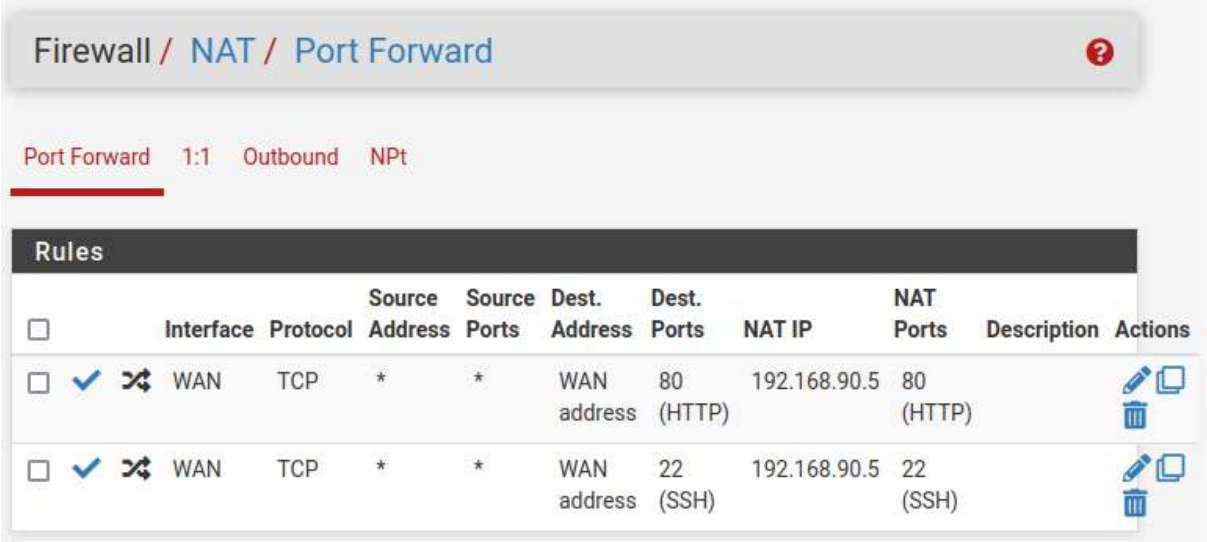
2. WAN :

L'accès du WAN est limité à la DMZ. Cela permet au PC-WAN d'accéder au serveur Ubuntu via le service SSH en utilisant Putty, grâce à une règle spécifique ajoutée dans le menu de configuration de pfSense sous Firewall/NAT/Port Forward. Cela empêche toute communication directe avec le LAN, minimisant ainsi les risques de sécurité.

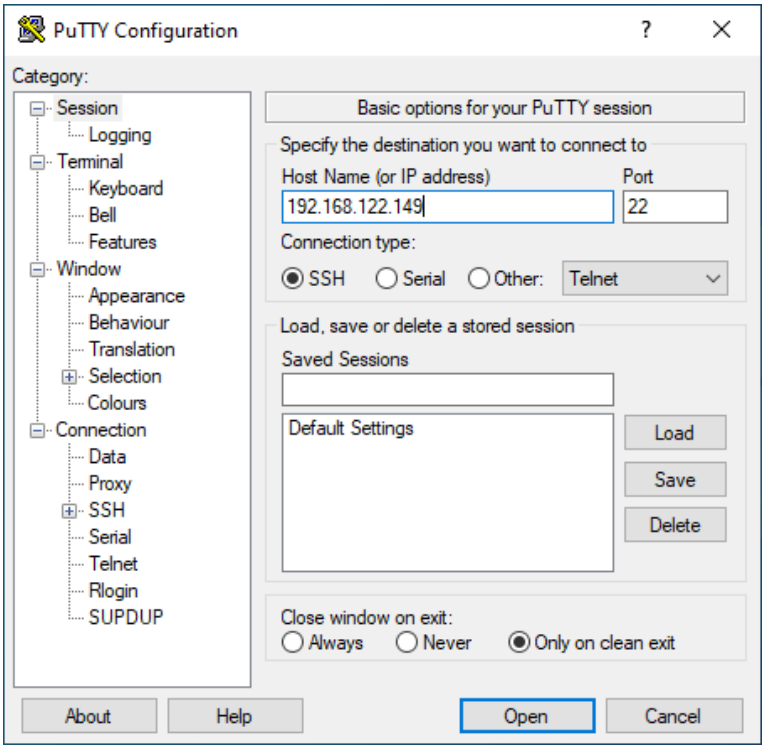


3. DMZ :

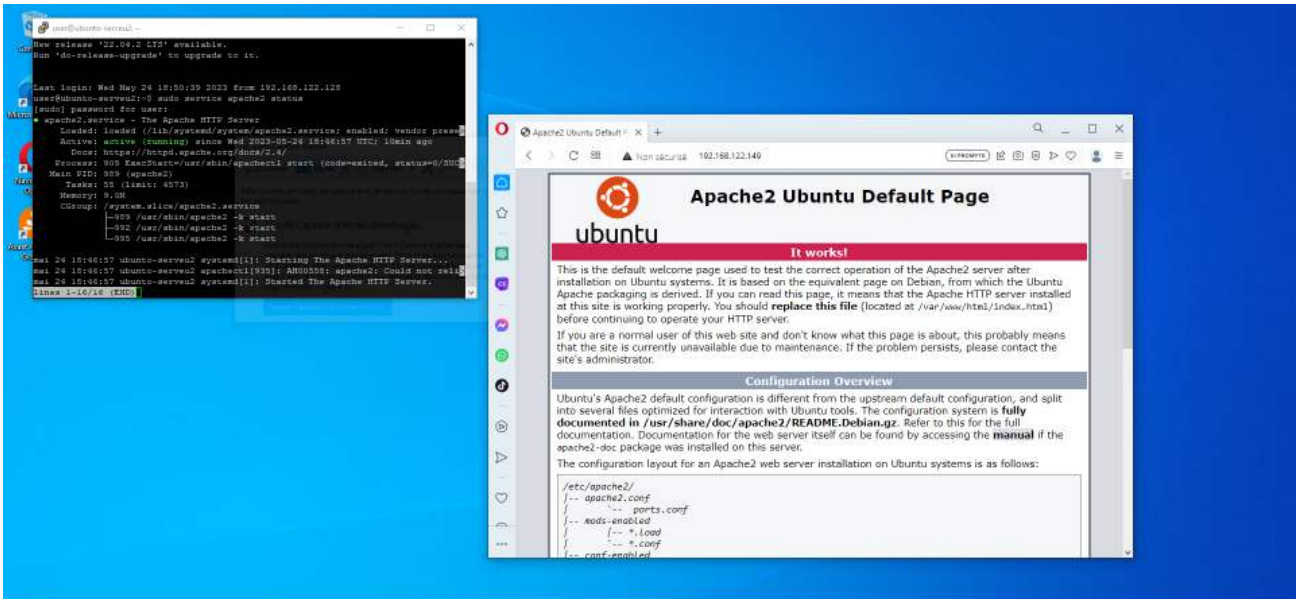
La DMZ est strictement isolée, sans accès ni au LAN ni au WAN, limitant ainsi l'exposition du serveur Ubuntu aux autres segments du réseau, à l'exception de l'accès autorisé au PC-WAN via SSH ou HTTP.



En complément de ces politiques d'accès, nous avons mis en œuvre une règle de Port Forwarding, redirigeant certains ports et protocoles du WAN vers la DMZ. Cette règle renforce la sécurité en minimisant les ports directement exposés à Internet tout en permettant l'accès nécessaire au serveur.



Ce niveau d'accès a été mis en place en ajoutant une règle spécifique dans le menu de configuration de pfSense sous Firewall/NAT/Port Forward. Cette règle autorise le PC-WAN à accéder au serveur Ubuntu via le service SSH en utilisant Putty. Cela assure que le PC-WAN peut atteindre le serveur quand nécessaire, tout en maintenant la séparation stricte du LAN pour minimiser les risques de sécurité.



Conclusion

En somme, ce dossier technique offre un aperçu de la complexité liée à la conception, à la configuration et à la gestion d'une infrastructure réseau performante et sécurisée. Les différentes stratégies de sécurité mises en œuvre démontrent un équilibre entre flexibilité et sécurité, permettant à chaque segment du réseau de fonctionner efficacement tout en minimisant les risques.

Le déploiement de GNS3 et de pfSense dans ce projet illustre leurs puissantes capacités à créer des environnements de réseau sécurisés et opérationnels. Cela souligne le potentiel des outils modernes dans la construction et la gestion des infrastructures réseau.

En guise de conclusion, ce projet étudiant met en exergue la sophistication de la construction d'une infrastructure réseau. Il met en lumière les compétences essentielles et les connaissances requises pour répondre aux défis de sécurité et aux besoins variés dans l'environnement dynamique du réseau moderne. Ce projet est un témoignage du travail rigoureux et de l'expertise nécessaire pour naviguer dans le paysage toujours en évolution de la technologie réseau.