PAQUELET Etienne Groupe 11

KUT Suha

Jalon 35 : Filtrage Actif sur HQFWSRV

Bien que la **NAT** permette la translation d'adresse pour accéder au serveur dans la DMZ, nous avons veillé à restreindre les accès via des **règles de filtrage**. Seuls les protocoles nécessaires sont autorisés, et l'accès à l'interface d'administration de **pfSense** reste totalement bloqué depuis Internet pour des raisons évidentes de sécurité. Le but d'une DMZ est de séparer un serveur critique qui doit avoir accès à l'intérieur du réseau et à l'extérieur d'un réseau du réseau interne et d'internet. A cette fin, des règles de filtrages doivent être mise en place.

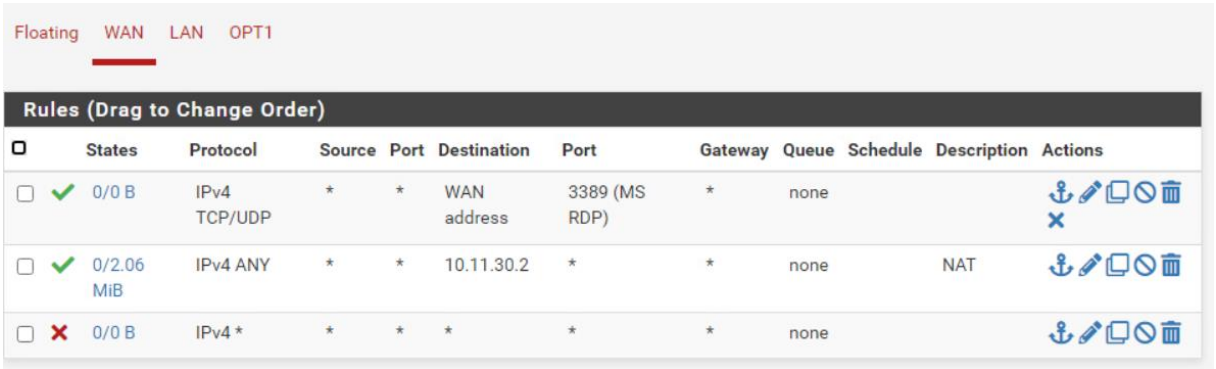
Par défaut, **tous les ports sont bloqués**, à l'exception de ceux nécessaires au bon fonctionnement du serveur web :

- **Port 80 (HTTP)** : pour permettre l'accès au site web en clair.
- **Port 3389 (RDP)** : permettre aux applications du bureau à distance d'être transmise aux clients.

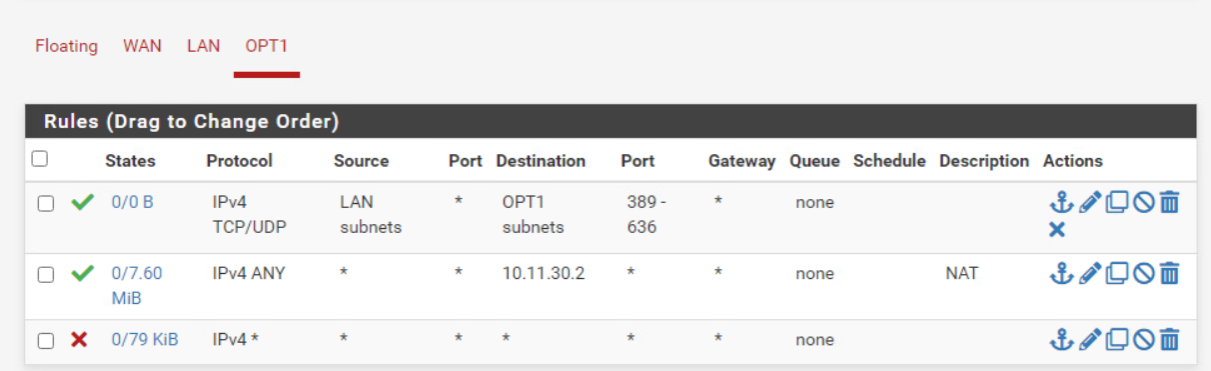
Remarque : Bien que nous n'ayons pas eu le temps de configurer **HTTPS** (port 443), une règle spécifique pour ce port aurait logiquement dû être mise en place pour assurer la sécurisation des échanges via SSL/TLS.

Cette approche minimaliste en termes d'ouverture de ports garantit que le serveur est uniquement accessible pour les services requis, limitant ainsi les risques d'attaques potentielles.

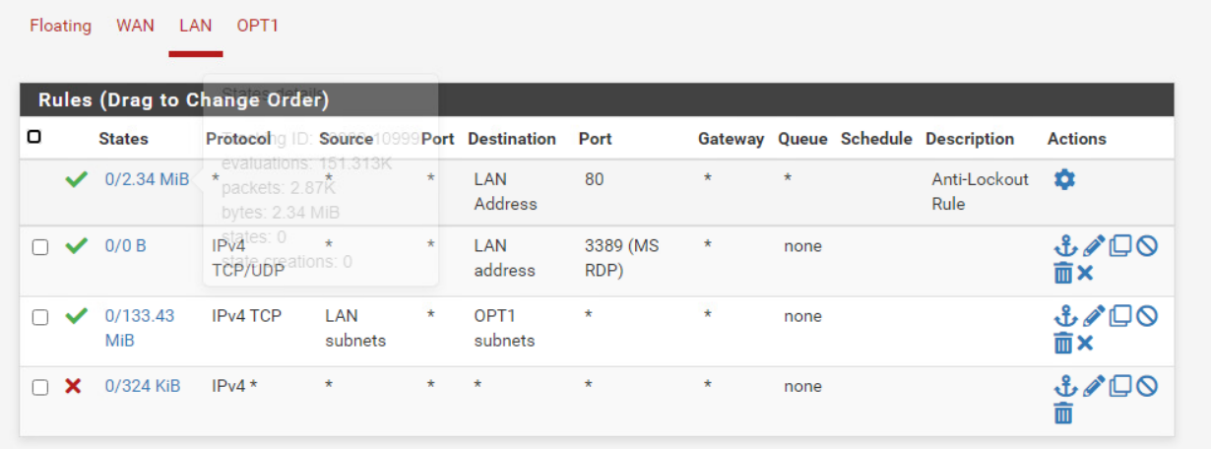
Règle de filtrage sur interface WAN (OUT)



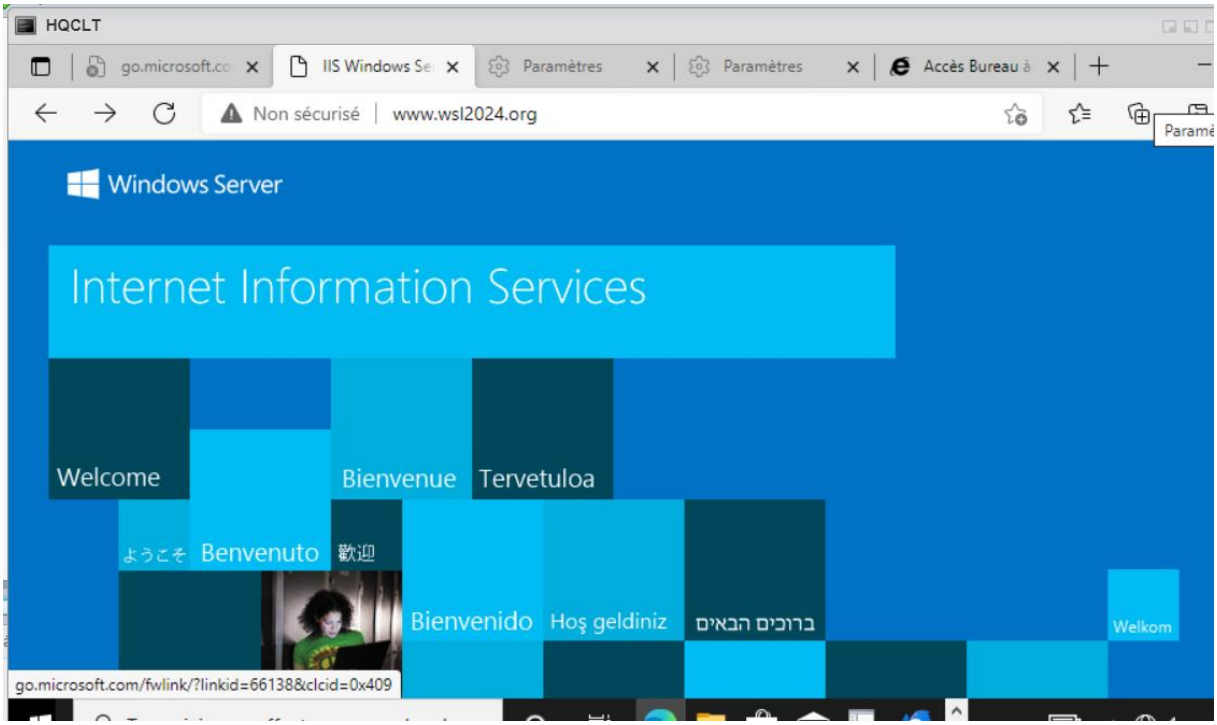
Règle de filtrage sur l'interface OPT1 (IN : réseaux internes) :



Règles de filtrages sur l'interface LAN (DMZ) :



Une fois ces règles mise en place, nous pouvions accéder, grâce au DNS interne, sur la page web du serveur grâce à la NAT depuis le réseau interne :



Depuis le réseau externe :