

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)

Floating WAN LAN OPT1											
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP/UDP	*	*	WAN address	3389 (MS RDP)	*	none			
<input type="checkbox"/>	✓ 0/2.06 MiB	IPv4 ANY	*	*	10.11.30.2	*	*	none		NAT	
<input type="checkbox"/>	✗ 0/0 B	IPv4 *	*	*	*	*	*	none			

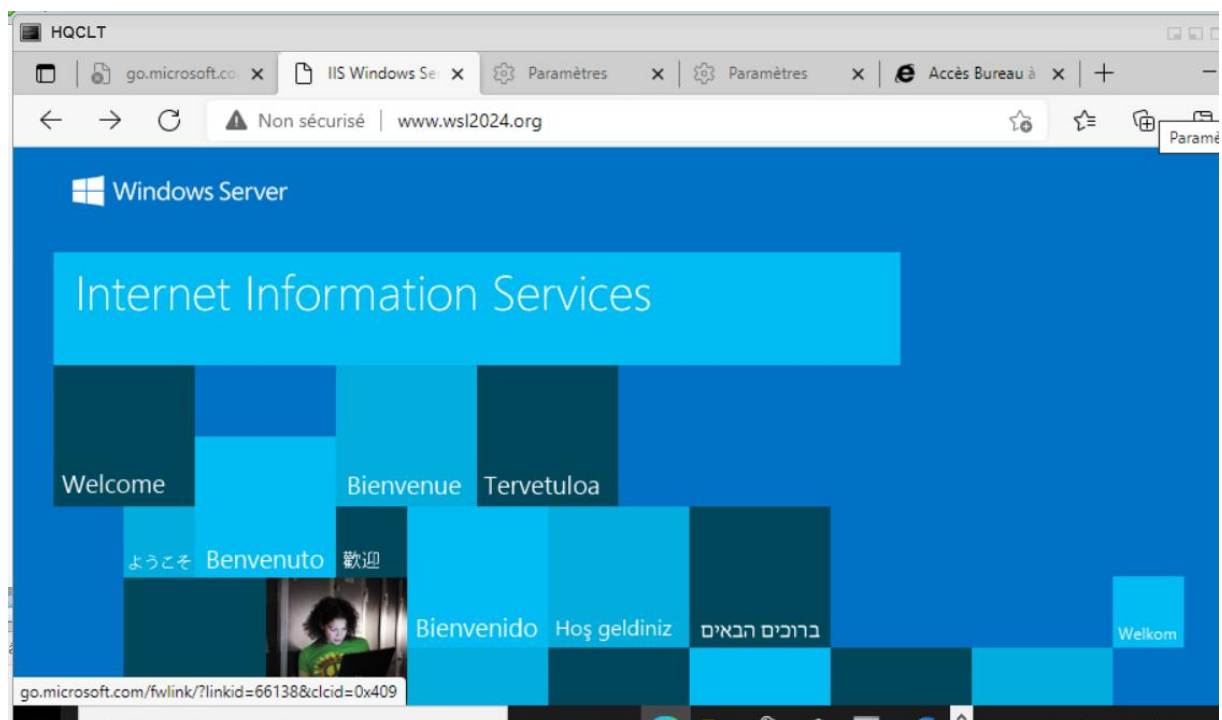
Règle de filtrage sur l'interface OPT1 (IN : réseaux internes) :

Floating WAN LAN OPT1											
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP/UDP	LAN subnets	*	OPT1 subnets	389 - 636	*	none			
<input type="checkbox"/>	✓ 0/7.60 MiB	IPv4 ANY	*	*	10.11.30.2	*	*	none		NAT	
<input type="checkbox"/>	✗ 0/79 KiB	IPv4 *	*	*	*	*	*	none			

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

Floating WAN LAN OPT1											
Rules (Drag to Change Order)											
<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/>	✓ 0/2.34 MiB	IPv4 TCP/UDP	LAN Address	80	LAN address	3389 (MS RDP)	*	*		Anti-Lockout Rule	
<input type="checkbox"/>	✓ 0/0 B	IPv4 TCP/UDP	LAN subnets	*	OPT1 subnets	*	*	none			
<input type="checkbox"/>	✓ 0/133.43 MiB	IPv4 TCP	LAN subnets	*	OPT1 subnets	*	*	none			
<input type="checkbox"/>	✗ 0/324 KiB	IPv4 *	*	*	*	*	*	none			

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



Depuis le réseau externe :

