Documentation de Configuration du Pare-feu pfSense

# Contexte

Le pare-feu pfSense est utilisé pour assurer la sécurité et la segmentation du réseau interne en gérant les interfaces WAN, LAN et DMZ. Il filtre le trafic réseau, autorise uniquement les connexions légitimes, et utilise la traduction d'adresses réseau (NAT) pour rediriger le trafic entrant vers les serveurs internes, notamment HAProxy.

# 1. Interface WAN

Sur l'interface WAN, les règles suivantes ont été mises en place pour autoriser l'accès aux services web hébergés en DMZ via HAProxy, tout en bloquant les connexions non autorisées.

Une image contenant texte, nombre, Police, logiciel

Le contenu généré par l’IA peut être incorrect.

## Règles :

• Autoriser le trafic TCP sur les ports 80 (HTTP) et 443 (HTTPS) vers l'adresse IP virtuelle 10.0.0.6 (HAProxy).  
• Rediriger le trafic HTTP/HTTPS provenant de WAN vers HAProxy (NAT).  
• Bloquer tout autre trafic entrant vers la DMZ.

## Utilité :

Garantir que seuls les services web (HTTP/HTTPS) sont exposés publiquement, assurant une surface d'attaque minimale.

# 2. Interface DMZ

La DMZ héberge les serveurs web et les proxys. Elle est configurée pour permettre un accès minimal et contrôlé au WAN, LAN et vice versa.

## Règles :

• Autoriser les connexions sortantes HTTP/HTTPS/FTP vers WAN.  
• Autoriser le trafic SQL (port 3306) entre les serveurs web et GaleraDB dans le LAN.  
• Autoriser les connexions de monitoring (Zabbix, Grafana).  
• Bloquer les connexions internes inutiles (ex. LANist).

## Utilité :

Protéger les ressources critiques tout en assurant le fonctionnement des services (web, monitoring, SQL).

# 3. Interface LAN

Le LAN correspond au réseau interne où se trouvent les utilisateurs et certains outils de supervision comme Zabbix.

## Règles :

• Autoriser Zabbix à interroger les serveurs web et HAProxy dans la DMZ.  
• Autoriser le trafic web sortant vers Internet.  
• Autoriser les connexions Anydesk et le trafic DNS.

## Utilité :

Permettre le fonctionnement du réseau interne tout en conservant un contrôle strict sur les flux sortants.

# 4. Règles NAT

Le NAT est utilisé pour rediriger le trafic provenant d'Internet vers les services web internes hébergés par HAProxy.

Une image contenant texte, logiciel, Page web, Site web

Le contenu généré par l’IA peut être incorrect.

## Configuration :

• NAT destination sur les ports 80 et 443 de l'adresse IP publique vers 10.0.0.5 (HAProxy).

## Utilité :

Permet aux utilisateurs externes d'accéder au site web hébergé en DMZ de manière transparente.