Pare-feu pfSense

Filtrage WAN — Équipement physique

Version : 1.0

Rédacteur : Florian Besse

Date : Mai 2026

Formation : BTS SIO option SISR

Domaine : centresio.local

1. Présentation

Le pare-feu de l'infrastructure Centre SIO est un équipement physique opérant sous pfSense CE. Il constitue la frontière entre le réseau WAN (accès à Internet) et les segments internes. Il prend en charge le filtrage du trafic par règles LAN, le contrôle des flux sortants et la protection périmétrique contre les connexions non sollicitées depuis l'extérieur.

Le routage entre les VLANs internes est assuré par le routeur Cisco. pfSense intervient uniquement sur la frontière LAN/WAN.

Solution : **pfSense CE (Community Edition)**
Type d'équipement : **Firewall physique**
Interface WAN : **Connexion vers le réseau externe**
Interface LAN : **Connexion vers le réseau interne de l'infrastructure**
Console d'administration : **Interface web HTTPS — accessible depuis le réseau interne**

2. Règles LAN

Les règles LAN définissent ce que les machines internes sont autorisées à faire vers l'extérieur ou vers d'autres segments. pfSense applique un filtrage par alias pour les destinations autorisées.

2.1 — Flux bloqués

ICMP : **Bloqué en sortie — pas de ping vers l'extérieur**
FTP : **TCP 21 — bloqué**
SMB : **TCP 445 — bloqué en sortie WAN**
HTTP (partiel) : **TCP 80 — autorisé uniquement vers des destinations définies dans les alias**

2.2 — Flux autorisés

HTTPS : **TCP 443 — autorisé vers Internet — mises à jour Windows, Amazon, Google Drive**
DNS : **UDP/TCP 53 — autorisé vers les DC internes (10.0.90.11 et 10.0.90.6)**
Mises à jour Windows : **HTTPS vers les serveurs Microsoft Update — nécessaire pour WSUS et les postes**
NTP : **UDP 123 — synchronisation temporelle**

3. Règles WAN

Aucune connexion initiée depuis l'extérieur n'est autorisée à entrer dans l'infrastructure. L'ensemble du trafic WAN entrant non sollicité est rejeté par défaut.

Accès entrant : **Rejet total — aucune règle d'accès entrant configurée**

Sessions sortantes : **Autorisées par stateful filtering — le retour des connexions initiées en interne est accepté**

NAT : **Masquerading automatique — toutes les sources LAN vers WAN**

4. Paramètres généraux

Mode de filtrage : **Stateful — suivi de connexion actif**

Règle implicite finale : **Deny all — tout ce qui n'est pas explicitement autorisé est rejeté**

Journalisation : **Activée sur les règles de refus**

Sauvegarde config : **Export XML disponible depuis Diagnostics > Backup & Restore**