Configuration pare-feu pfSense — SNCF DSI

Période : 10/2025 – 12/2025	**Entreprise :** SNCF — DSI	**Candidat :** Soul Florian

Objectif de la mission

Installer et configurer pfSense comme pare-feu périmétrique de la SNCF DSI : règles de filtrage, NAT, VPN site-à-site IPSec et journalisation des événements.

Compétences BTS SIO mobilisées

Gérer le patrimoine informatique	Répondre aux incidents et demandes
Mettre à disposition des utilisateurs un service informatique	Vérifier la continuité d'un service informatique

1. Présentation de la mission

Configuration et sécurisation d'un pare-feu pfSense pour la SNCF DSI. pfSense est une distribution FreeBSD dédiée aux fonctions de routage/filtrage. La mission couvre l'installation, la configuration des règles de filtrage, le NAT, la mise en place d'un VPN site-à-site IPSec et la journalisation des événements.

2. Schéma réseau cible

Interface pfSense	Nom	Réseau	Rôle
em0	WAN	IP publique / DHCP FAI	Connexion Internet SNCF
em1	LAN	192.168.10.0/24	Réseau interne DSI
em2	DMZ	192.168.100.0/24	Serveurs exposés (web, mail)
em3	VPN	10.10.0.0/24	Tunnels VPN site-à-site

3. Installation de pfSense

- Télécharger pfSense CE 2.7.x depuis pfsense.org (image ISO)
- Installer sur un serveur dédié ou VM avec 3+ interfaces réseau
- Suivre l'assistant d'installation : partitionnement automatique recommandé
- Au premier démarrage : assigner les interfaces WAN/LAN via la console
- Accéder à l'interface web : https://192.168.10.1 (admin / pfsense)
- Changer le mot de passe admin immédiatement (System > User Manager)

4. Configuration des règles de filtrage

4.1 — Interface LAN (politique : défaut permissif, durcir progressivement)

Source	Destination	Port	Action	Commentaire
LAN net	WAN net	80, 443	AUTORISER	Navigation web
LAN net	WAN net	53	AUTORISER	DNS sortant
LAN net	DMZ net	80, 443, 22	AUTORISER	Accès serveurs DMZ
LAN net	LAN net	any	AUTORISER	Trafic interne
LAN net	WAN net	any	BLOQUER	Bloquer tout le reste sortant

4.2 — Interface DMZ (politique : restrictive)

- Bloquer tout trafic initié depuis la DMZ vers le LAN (anti-rebond)
- Autoriser uniquement les réponses aux connexions initiées depuis le LAN
- Autoriser DMZ vers WAN sur port 80/443 pour les mises à jour

5. Configuration du NAT

```
# NAT sortant (Outbound NAT) — masquerade Firewall > NAT > Outbound : Mode 'Automatic' # pfSense crée automatiquement les règles de masquerade pour LAN et DMZ # NAT entrant (Port Forward) — exposition d'un serveur web en DMZ Firewall > NAT > Port Forward : Interface : WAN Protocole : TCP Port destination : 443 IP destination : IP WAN IP redir : 192.168.100.10 (serveur web DMZ) Port redir : 443
```

6. VPN Site-à-Site IPSec

- VPN > IPSec > Tunnels > Add P1 (Phase 1 : authentification)
- Remote Gateway : IP publique du site distant (ex. 203.0.113.50)
- Méthode d'auth : Clé pré-partagée (PSK) — utiliser une clé de 32 caractères minimum
- Algorithme : AES-256, SHA-256, DH Group 14
- Ajouter une Phase 2 : réseau local 192.168.10.0/24 <-> réseau distant 10.20.0.0/24
- Appliquer les changements et vérifier : VPN > IPSec > Status (doit afficher ESTABLISHED)

7. Journalisation

```
# Status > System Logs > Firewall : logs des connexions bloquées # Configurer la remontée Syslog vers Zabbix ou SIEM Status > System Logs > Settings : Enable Remote Logging : OUI Remote Syslog Server : 192.168.10.20 (serveur Zabbix) Remote Facility : LOG_LOCAL0
```

8. Livrables attendus

- Capture des interfaces réseau pfSense configurées
- Capture du tableau de règles de filtrage LAN et DMZ
- Capture du statut du tunnel VPN IPSec (ESTABLISHED)

- Capture des logs de pare-feu avec des connexions bloquées
- Schéma réseau mis à jour avec pfSense positionné