Ressources Documentaires – Réalisation Professionnelle n°1

Examen / Épreuve	BTS Services Informatiques aux Organisations (SIO) - Option SISR - Épreuve E6
Intitulé du projet	Sécurisation périmétrique et haute disponibilité d'une passerelle pare-feu
Candidat	MALAUSSENA Maxence
Établissement	Lycée Saint-Exupéry - Saint-Raphaël
Période de réalisation	Novembre - Décembre 2025

1. Contexte et besoins

1.1 Présentation de l'organisation

L'infrastructure s'inscrit dans le cadre de la modernisation des accès du réseau interne. L'organisation requiert un accès Internet sécurisé, stable et résilient pour l'ensemble de ses collaborateurs, tout en garantissant la disponibilité continue de ses services web publiés en interne.

1.2 Problèmes identifiés

L'analyse fonctionnelle de l'ancienne architecture a révélé des faiblesses structurelles majeures :

- L'absence de redondance de la passerelle pare-feu d'accès constituait un point de défaillance unique (SPOF).
- Toute maintenance corrective, mise à jour de règles de filtrage ou panne matérielle sur le pare-feu entraînait une déconnexion immédiate du réseau interne vis-à-vis d'Internet et rendait le serveur web injoignable.

1.3 Objectifs fixés

Pour pallier ces dysfonctionnements, le cahier des charges impose de :

- Mettre en place un mécanisme de haute disponibilité (HA) transparent pour les pare-feux périmétriques.
- Assurer la continuité de service pour le trafic à destination et en provenance du réseau interne.
- Garantir la disponibilité permanente d'accès au serveur web hébergé en interne.

2. Solutions envisagées et solution retenue

2.1 Comparatif des architectures

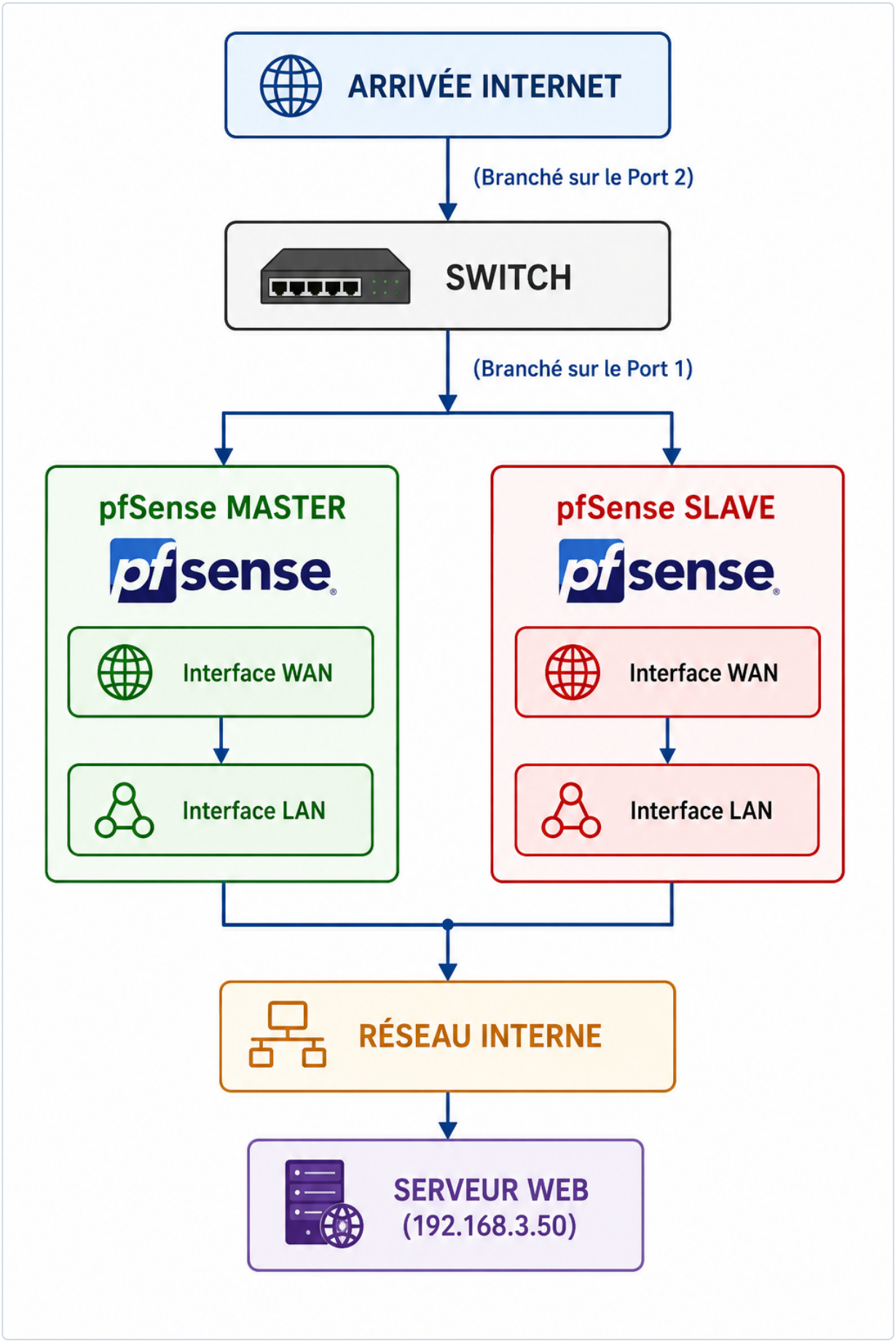
Solution envisagée	Avantages	Inconvénients
Cluster pfSense en Haute Disponibilité (CARP)	Bascule matérielle automatique et instantanée, synchronisation complète des règles et des états de sessions (pfSync).	Nécessite trois adresses IP par segment réseau (une par nœud physique + une IP virtuelle).
Pare-feu unique avec contrat de support matériel J+1	Simplicité de configuration et coût d'acquisition initial réduit.	Temps d'interruption important en cas de panne matérielle lourde (non tolérant aux pannes).

2.2 Solution retenue

La solution retenue est le déploiement de **deux machines pfSense configurées en mode Master / Slave (Haut Disponibilité)**. Cette architecture s'appuie sur le protocole CARP pour le partage d'IP virtuelles et pfSync pour la réplication d'état des connexions en temps réel.

3. Architecture réseau et interconnexion physique

3.1 Schéma de l'infrastructure déployée


ARRIVÉE INTERNET
(Branché sur le Port 2)
SWITCH
(Branché sur le Port 1)
pfSense MASTER
pfsense
Interface WAN
Interface LAN
pfSense SLAVE
pfsense
Interface WAN
Interface LAN
RÉSEAU INTERNE
SERVEUR WEB
(192.168.3.50)

3.2 Topologie physique et raccordement

L'interconnexion des différents composants s'effectue via un commutateur central selon une organisation physique stricte :

- **Arrivée Internet (WAN) :** Le flux provenant du fournisseur d'accès est raccordé directement sur le **Port 2** du Switch.
- **Passerelles pfSense :** Les interfaces supérieures (WAN) des deux pare-feux pfSense (Master et Slave) sont raccordées sur le **Port 1** du Switch.
- **Réseau Interne (LAN) :** Les interfaces inférieures (LAN) des pare-feux distribuent le trafic vers le segment réseau interne où est localisé le serveur web de production.

3.3 Adressage IP

Équipement / Interface	Rôle / Description	Adresse IP	Raccordement physique / Switch
Arrivée Internet	Source du trafic WAN extérieur	-	Branché sur le **Port 2**
pfSense MASTER	Pare-feu principal actif (gère le trafic nominal)	IP Configuration HA	Interface supérieure sur le **Port 1**
pfSense SLAVE	Pare-feu secondaire passif (reprend le trafic en cas de panne)	IP Configuration HA	Interface supérieure sur le **Port 1**
Réseau Interne	Segment LAN de production sécurisé	192.168.3.X /24	Délivré par les interfaces LAN des pfSense
Serveur WEB	Serveur applicatif interne publié	**192.168.3.50**	Connecté au segment réseau interne

> **Spécificité de l'interconnexion :** Le switch central sert de nœud d'interconnexion matériel clé. Le couplage de l'arrivée Internet sur le Port 2 et des deux instances pfSense sur le Port 1 permet une distribution redondante et étanche des flux WAN avant leur traitement et filtrage à destination du réseau interne.

4. Mise en œuvre technique

Le déploiement a été structuré selon les étapes opérationnelles suivantes :

1. **Installation des instances pfSense :** Déploiement du système d'exploitation pfSense sur deux machines physiques ou virtuelles distinctes (Master et Slave).
2. **Câblage physique :** Brassage des liens conformément au plan d'architecture (Internet sur le Port 2, pare-feux sur le Port 1 du switch).
3. **Configuration du protocole CARP :** Création des adresses IP virtuelles partagées pour le WAN et le LAN permettant la bascule d'adresse MAC virtuelle transparente pour les clients.
4. **Configuration de XMLRPC sync (pfSync) :** Activation de la synchronisation automatique des règles de filtrage depuis le nœud Master vers le nœud Slave pour éliminer la double administration.

5. Validation et Tests de recette

Scénario de Test	Action réalisée	Résultat attendu	Résultat obtenu
Disponibilité nominale du serveur Web	Accès à l'adresse du serveur web depuis l'extérieur.	Le serveur web à l'adresse 192.168.3.50 répond correctement via le pfSense Master.	**OK**
Coupure du pare-feu pfSense MASTER	Arrêt ou déconnexion du nœud Master.	Le pfSense SLAVE détecte l'absence du Master et bascule instantanément en mode actif. Le flux réseau n'est pas coupé.	**OK** (Bascule transparente)
Rétablissement du nœud MASTER	Redémarrage du pfSense MASTER.	Le Master reprend son rôle prioritaire automatiquement sans provoquer de perturbation de trafic.	**OK**

6. Bilan et perspectives

La mise en œuvre de ce cluster pfSense en haute disponibilité répond parfaitement au besoin de résilience périmétrique. L'élimination du SPOF garantit que le serveur web interne (192.168.3.50) reste disponible et que les utilisateurs conservent leur connectivité Internet même lors d'une défaillance matérielle complète d'un des deux pare-feux. Cette architecture offre une base stable pour l'intégration future de politiques de filtrage plus avancées (système de détection d'intrusion IDS/IPS).