Situation professionnelle
Mise en place d'un tunnel IPsec sous PfSense

Théo DELETTRE

Session 2025

N° candidat : 02345602698

Table des matières

1 Cahier des charges – Expression des besoins

1.1 Descriptif de l'existant

L'établissement dispose de deux sites géographiquement distants. Chaque site est protégé par un pare-feu PfSense configuré indépendamment. Actuellement, aucune interconnexion sécurisée n'existe entre les deux sites, ce qui empêche les utilisateurs d'un site d'accéder aux ressources (serveurs, partages de fichiers, services applicatifs) de l'autre site.

1.2 Besoin(s)

- Mettre en place une interconnexion réseau sécurisée entre les deux sites via un tunnel VPN IPSec.
- Garantir la confidentialité, l'intégrité et la disponibilité des communications entre les deux sites.
- Permettre aux utilisateurs des deux sites d'accéder aux ressources partagées de façon transparente.
- Assurer la compatibilité avec l'infrastructure réseau existante.

1.3 Contrainte(s)

- Temps : Mise en place à réaliser dans un délai court (1 à 2 semaines).
- Technique : Maintenir la compatibilité avec les versions actuelles de PfSense déjà en production.
- Organisationnel : Interventions à effectuer sans interruption des services critiques en production.
- Budget : Aucune dépense supplémentaire ; utilisation exclusive des fonctionnalités intégrées à PfSense (solutions open source).

2 Ressources

2.1 Ressources mises à disposition

- Accès administrateur aux deux pare-feux PfSense (interface Web et console).
- Schémas réseau des deux sites (adresses IP internes, sous-réseaux, passerelles).
- Disponibilité de plages IP non utilisées pour configurer le VPN si nécessaire.

2.2 Ressources nécessaires pour la réalisation

- Documentation officielle PfSense sur la mise en place d'un VPN IPSec site-à-site.
- Accès à des outils de test réseau (ping, traceroute, nmap) pour vérifier la connectivité.
- Possibilité de créer des règles de pare-feu personnalisées pour autoriser le trafic VPN.

3 Analyse

3.1 Descriptifs des solutions

Solution	Description
VPN IPSec site-à-site (PfSense)	Configuration d'un tunnel VPN IPSec directement entre les deux pare-feux PfSense. Connexion permanente et sécurisée entre les deux réseaux LAN. Solution native, sans logiciel tiers.
VPN OpenVPN site-à-site (PfSense)	Utilisation d'OpenVPN en mode site-à-site avec certificats. Moins standard qu'IPSec pour les interconnexions inter-entreprises, mais plus souple à configurer.
VPN avec appliance dédiée (matériel)	Installation de routeurs VPN matériels sur chaque site. Coût supplémentaire et peu pertinent ici, car PfSense intègre déjà ces fonctions.
Accès distant par VPN individuel	Connexion VPN par utilisateur (client OpenVPN ou IPSec) vers un site, avec redirection vers l'autre site manuellement. Moins adapté à un usage permanent ou transparent.

3.2 Comparaison des solutions

Critère	VPN IPSec site-à-site	OpenVPN site-à-site	VPN matériel dédié	VPN individuel (accès distant)
Coût	Gratuit (intégré à PfSense)	Gratuit (intégré à PfSense)	Élevé (matériel à acheter)	Gratuit (si infra existante)
Performance	Élevée	Bonne	Très bonne (dépend du matériel)	Moyenne à faible
Simplicité d'administration	Moyenne	Moyenne	Faible (matériel spécifique)	Moyenne
Sécurité	Élevée (norme entreprise)	Élevée	Très élevée	Moyenne (gestion utilisateurs)
Transparence pour les utilisateurs	Oui	Oui	Oui	Non (connexion manuelle)
Interopérabilité	Standard	Moins répandu	Dépend du matériel	Faible

3.3 Choix d'une solution

La solution retenue est la mise en place d'un tunnel VPN IPSec site-à-site entre les deux pare-feux PfSense.

Cette solution présente les avantages suivants :

- Elle est native à PfSense, ne nécessite aucun coût supplémentaire, et respecte les standards de sécurité professionnelle.
- Elle assure une connexion permanente, transparente pour les utilisateurs, permettant l'accès direct aux ressources du site distant.
- Elle est adaptée au contexte technique et organisationnel existant, notamment à l'infrastructure déjà en place (PfSense sur les deux sites).

3.4 Plan d'adressage – Schéma – Tables de routage

LANs :

LAN	LAN Vswitch	Plage d'adresses (CIDR)	Capacité d'hôtes	Plage DHCP
LAN2 - Critique (inclut Backups)	GRETA-LAN-2080	192.168.2.0/24	254	X
LAN3 - Serveurs	GRETA-LAN-2081	192.168.3.0/24	254	X
LAN4 - Supervision	GRETA-LAN-2082	192.168.4.0/24	254	X
LAN5 - Utilisateurs	GRETA-LAN-2083	192.168.5.0/24	254	192.168.5.10 - 192.168.5.240
LAN6 - Guest (Réseau invité avec vouchers)	GRETA-LAN-2084	192.168.6.0/24	254	192.168.6.10 - 192.168.6.240
LAN99 - HA/PfSync	GRETA-LAN-2085	192.168.99.0/24	254	X
LAN100 - DMZ	GRETA-DMZ-2089	192.168.100.0/24	254	X
WAN (routeur)	WAN_GRETA	192.168.20.0/24	254	X
LAN Distant	X	172.16.10.0/24	254	172.16.10.10 - 172.16.10.240

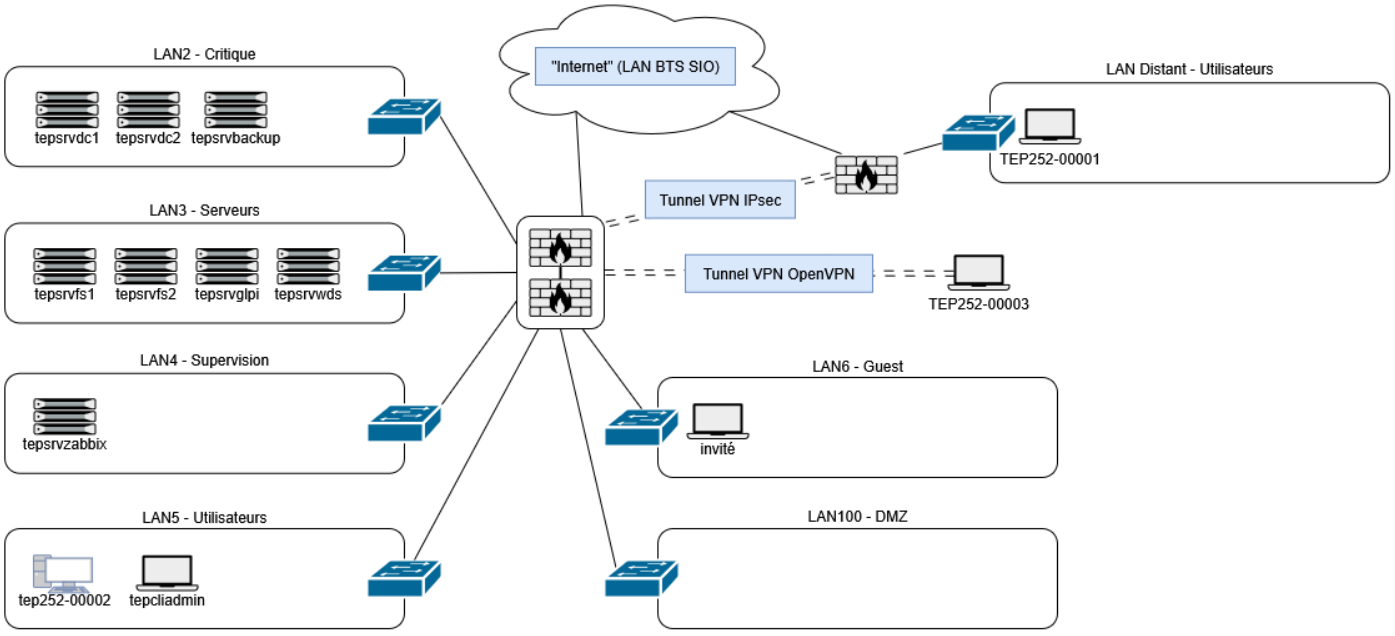
Site principal :

Nom machine	Nom DNS	LAN2	LAN3	LAN4	LAN5	LAN6	LAN99 (PFSYNC)	LAN100 (DMZ)	WAN
UFA208-PfSense-Primary	pfSense-Primary	192.168.2.252	192.168.3.252	192.168.4.252	192.168.5.252	192.168.6.252	192.168.99.1	192.168.100.252	192.168.20.108
UFA208-PfSense-Secondary	pfSense-Secondary	192.168.2.253	192.168.3.253	192.168.4.253	192.168.5.253	192.168.6.253	192.168.99.2	192.168.100.253	192.168.20.109
(IP virt PfSense)	x	192.168.2.254	192.168.3.254	192.168.4.254	192.168.5.254	192.168.6.254	x	192.168.100.254	192.168.20.208
UFA208-tepcliadmin	tepcliadmin.teppe.local	x	x	x	DHCP	x	x	x	x
UFA208-tepsrvdc1	tepsrvdc1.teppe.local	192.168.2.1	x	x	x	x	x	x	x
UFA208-tepsrvdc2	tepsrvdc1.teppe.local	192.168.2.2	x	x	x	x	x	x	x
UFA208-tepsrvbackup	tepsrvbackup.teppe.local	192.168.2.3	x	x	x	x	x	x	x
UFA208-tepsrvfs1	tepsrvdc1.teppe.local	x	192.168.3.1	x	x	x	x	x	x
UFA208-tepsrvfs2	tepsrvdc1.teppe.local	x	192.168.3.2	x	x	x	x	x	x
UFA208-tepsrvwds	tepsrvdc1.teppe.local	x	192.168.3.3	x	x	x	x	x	x
UFA208-tepsrvglpi	glpi.teppe.local	x	192.168.3.4	x	x	x	x	x	x
UFA208-tepsrvzabbix	zabbix.teppe.local	x	x	192.168.4.1	x	x	x	x	x
UFA208-tep252-00002	tep252-00002.teppe.local	x	x	x	DHCP	x	x	x	x
UFA208-invité		x	x	x	x	DHCP	x	x	x

Site distant – postes nomades :

Nom machine	Nom DNS	LAN	WAN (LAN BTS SIO)
PfSense-SiteDistant	PfSense-Site-Distant	172.16.10.254	DHCP
TEP252-00001	TEP252-00001.teppe.local	DHCP	x
TEP252-00003	TEP252-00003.teppe.local	x	DHCP

Topologie :



3.5 Etude de l'impact sur le SI existant

La mise en place du tunnel VPN IPSec aura un impact limité et maîtrisé sur le système d'information existant.

Aucun changement majeur n'est apporté aux configurations internes des deux sites, les modifications se concentrent uniquement au niveau des pare-feux PfSense.

Le trafic inter-site passera par le tunnel chiffré, mais les communications locales (intra-site) resteront inchangées.

Points d'attention :

- Nécessité de créer des règles de pare-feu adaptées pour autoriser les flux inter-sites.
- Risque temporaire d'indisponibilité en cas de mauvaise configuration du tunnel.
- Surveillance initiale renforcée post-déploiement pour garantir la stabilité.

3.6 Phasage de l'intervention

Phase	Description
Configuration du tunnel	Création du tunnel IPSec sur les deux pare-feux PfSense avec les paramètres IKE.
Mise en place des règles	Création des règles de pare-feu autorisant les flux inter-sites nécessaires.
Tests de connectivité	Vérification du bon fonctionnement du tunnel et accès aux ressources distantes.

3.7 Prévision des tests de validation

Des tests de remonté des données (SNMP/agent Zabbix) seront effectués à mesure de l'ajout d'hôtes au serveur Zabbix.

Test	Objectif
Ping inter-sites	Vérifier la connectivité réseau entre les deux LAN via VPN.
Accès aux services distants	Tester les connexions aux partages, serveurs ou services applicatifs.

3.8 Déploiement

Une procédure de configuration des tunnels VPN IPsec est disponible à l'adresse : https://theodelettre.fr/wp-content/uploads/2025/05/Creation-dun-tunnel-IPsec-sous-PfSense.pdf

4 Mise en place

4.1 Réalisation

4.1.1 Détails des configurations

Élément	Configuration
Type de VPN	IPSec site-à-site
Authentification	Clé partagée (PSK)
IKE version	IKEv2
Phase 1	AES-256 / SHA256 / DH Group 14
Phase 2	ESP / AES-256 / SHA256
Réseaux autorisés	LAN du site A ↔ LAN du site B
Ports ouverts	UDP 500 et UDP 4500
Configuration pare-feu	Règles autorisant les flux inter-sites sur chaque PfSense

4.2 Rapport de tests

Test	Résultat	Commentaire
Ping inter-sites	Réussi	Latence conforme, aucune perte de paquet.
Accès aux ressources distantes	Réussi	Partages et services accessibles.
Persistance après redémarrage	Confirmée	La configuration VPN est automatiquement relancée.

4.3 Rapport de déploiement

Le tunnel VPN IPSec entre les deux sites a été déployé sans incident majeur. Les configurations ont été réalisées en heures creuses pour éviter toute perturbation. Les tests de validation ont confirmé la bonne connectivité entre les réseaux distants.

Le tunnel est stable, persistant et répond aux besoins fonctionnels exprimés. Aucune dégradation du service existant n'a été observée.

5 Bilan

5.1 Conclusion

L'interconnexion VPN entre les deux sites a été mise en place avec succès. Cette solution open source respecte les contraintes de sécurité, de budget et de délais.

Elle permet désormais un accès fluide et sécurisé aux ressources entre les deux sites sans modifier les infrastructures locales existantes.

5.2 Auto critique/Auto évaluation sur la qualité du travail réalisé

Globalement, le travail accompli est fonctionnel, stable, sécurisé, et conforme aux objectifs initiaux.