BTS SIO 2023/2025

# CONTEXTE ENTREPRISE

Mise en place OpenVPN Site-to-Site





Amine Laouar

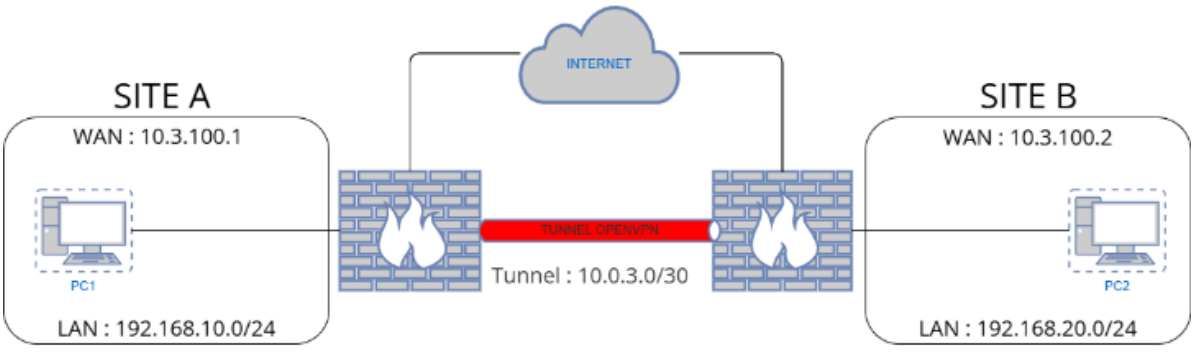
29/04/2025

# TABLE DES MATIERES

## PRÉSENTATION DE L'ENTREPRISE

L'entreprise **ALCORP**, située à Annecy, est une jeune société spécialisée dans la cybersécurité et les services d'infrastructure réseau pour les PME. Face à une croissance rapide et à l'ouverture d'un nouveau site distant, **ALCORP** a souhaité assurer une communication sécurisée entre ses deux sites.

L'objectif principal est d'assurer un accès sécurisé aux ressources internes depuis les deux localisations physiques de l'entreprise tout en garantissant la confidentialité, l'intégrité et la disponibilité des échanges.



Pour cela, une solution VPN site-à-site a été mise en œuvre à l'aide de **PfSense** et **OpenVPN**, technologies reconnues pour leur robustesse et leur flexibilité

Ce projet permet à l'entreprise :

- D'établir un **tunnel VPN sécurisé** entre le siège et la succursale ;

- D'assurer **un accès aux fichiers et services internes depuis les deux réseaux locaux** ;

- De **centraliser** les ressources tout en les maintenant protégées ;

- De **renforcer** son infrastructure réseau avec des outils open-source fiables.

Cette mise en place **renforce** la sécurité du système d'information de ALCORP et anticipe les futurs besoins d'interconnexion sécurisée à travers d'autres sites ou télétravailleurs.

## INSTALLATION ET CONFIGURATION DU VPN OPENVPN SUR PFSENSE

**Étapes réalisées :**

- Création de deux réseaux distincts : 192.168.10.0/24 (site principal) et 192.168.20.0/24 (site distant) ;

- Installation et configuration de deux routeurs pfSense 2.7.2 sur des machines virtuelles ;

- Paramétrage des interfaces WAN et LAN pour chaque site ;

- Configuration du routage statique entre les deux sous-réseaux.

## 2 – MISE EN PLACE DU TUNNEL VPN SÉCURISÉ

Technologie utilisée : **OpenVPN intégré à pfSense**.

**Tâches réalisées :**

- Création d'un serveur OpenVPN sur le site principal ;
- Génération des certificats SSL/TLS via le gestionnaire CA de pfSense ;
- Configuration du client VPN sur le site distant ;
- Ouverture du port UDP 1194 sur les pare-feu pour autoriser la connexion VPN ;
- Vérification de la connectivité (tests de ping et d'accès aux ressources partagées).

## 3 – TESTS ET VALIDATION

**Objectifs atteints :**

Connexion VPN établie automatiquement au démarrage des deux routeurs ;

Accès réseau croisé entre les deux LAN simulés (tests réussis entre clients Windows) ;

Les ressources internes sont disponibles et les communications sont chiffrées.

## 4 – OUTILS UTILISÉS

**pfSense** 2.7.2 (firewall open-source) ;

**OpenVPN** pour le chiffrement des flux réseau ;

**Hyper-V** pour la virtualisation de l'infrastructure ;

**Clients de test** : Windows Server 2022 et Windows 11.

## 5 – ÉVOLUTIONS POSSIBLES

Ajout d’un accès VPN pour télétravailleurs ;

Intégration avec un contrôle d’accès plus granulaire via Active Directory ;

Supervision du trafic VPN avec un outil comme Zabbix ou TrueCommand ;

Renforcement de la sécurité avec une authentification à double facteur (2FA).

## 6 – LIMITATIONS

La solution est actuellement limitée à un tunnel unique entre deux sites ;

L’administration du VPN nécessite des connaissances réseau avancées ;

Aucune interface de supervision centralisée n’a encore été intégrée ;

Pas de solution de haute disponibilité mise en place en cas de panne du pfSense principal.