Direction des Systèmes d'Information

TechConnect

Interconnexion sécurisée des sites de Limoges et Bordeaux

via un VPN Site-à-Site OpenVPN SSL/TLS

1. PRESENTATION DE L'ENTREPRISE

TechConnect est une entreprise spécialisée dans la distribution de matériel informatique et la fourniture de services informatiques aux PME. Fondée en 2012, elle emploie aujourd'hui 85 collaborateurs répartis sur deux sites : le siège social de Limoges et l'agence commerciale de Bordeaux, ouverte en 2019.

La Direction des Systèmes d'Information (DSI) est rattachée au siège de Limoges. Elle est responsable de l'ensemble de l'infrastructure réseau, des serveurs internes et de la sécurité informatique des deux sites.

Répartition des effectifs

Site	Ville	Effectif	Rôle
Site A — Siège social	Limoges	60 collaborateurs	Direction, DSI, comptabilité, logistique
Site B — Agence	Bordeaux	25 collaborateurs	Équipe commerciale, support client

2. CONTEXTE ET EXPRESSION DU BESOIN

2.1 — SITUATION INITIALE

Depuis l'ouverture de l'agence de Bordeaux, les équipes commerciales accèdent aux ressources internes de l'entreprise (serveur de fichiers, outils de gestion) via des connexions non sécurisées ou en passant par des solutions de partage en ligne tierces. Cette situation présente plusieurs risques :

- Exposition des données confidentielles de l'entreprise sur des plateformes externes.
- Absence de traçabilité des accès aux ressources internes.
- Latence importante et instabilité des connexions pour les applications métier.
- Impossibilité pour la DSI de superviser et de sécuriser les flux de données inter-sites.

2.2 — OBJECTIFS DU PROJET

La DSI de TechConnect a décidé de mettre en place une solution d'interconnexion sécurisée entre les deux sites. Les objectifs sont les suivants :

- Créer un lien réseau privé et chiffré entre le site de Limoges et celui de Bordeaux.
- Permettre aux collaborateurs de Bordeaux d'accéder aux ressources internes du siège de manière transparente et sécurisée.
- Assurer la confidentialité et l'intégrité des données échangées entre les deux sites.
- Centraliser la gestion de la sécurité réseau au niveau de la DSI à Limoges.
- Mettre en place une infrastructure évolutive, capable d'accueillir de nouveaux sites ou des utilisateurs nomades à terme.

3. SOLUTION TECHNIQUE RETENUE

3.1 — CHOIX TECHNOLOGIQUES

Après étude des différentes solutions disponibles (IPsec, WireGuard, OpenVPN), la DSI a retenu OpenVPN en mode Site-à-Site avec authentification SSL/TLS. Ce choix repose sur les critères suivants :

Critère	Justification
Maturité	OpenVPN est une solution éprouvée, déployée dans des milliers d'entreprises depuis plus de 20 ans.
Sécurité	Chiffrement AES-256-GCM, Perfect Forward Secrecy, authentification par PKI (CA + certificats).
Open source	Aucun coût de licence. Communauté active et mises à jour régulières.
Intégration	pfSense CE intègre nativement OpenVPN avec une interface web complète.
Évolutivité	Ajout simple de nouveaux sites ou d'accès nomades sans refonte de l'architecture.

3.2 — ARCHITECTURE RETENUE

Chaque site est équipé d'un pare-feu pfSense CE qui assure à la fois le routage, le filtrage des flux et la gestion du tunnel VPN. Le site de Limoges (Siège) héberge le serveur OpenVPN. Le site de Bordeaux (Agence) héberge le client OpenVPN qui initie la connexion.

La PKI (Infrastructure à Clés Publiques) est gérée par la DSI depuis le pfSense du siège. Elle comprend une Autorité de Certification (CA) interne qui signe les certificats de chaque équipement participant au tunnel.

3.3 — PLAN D'ADRESSAGE RÉSEAU

Réseau	Plage d'adresses	Site	Rôle
LAN Siège	192.168.10.0/24	Limoges	Réseau interne Site A
LAN Agence	192.168.20.0/24	Bordeaux	Réseau interne Site B

WAN (lien inter-sites)	172.16.0.0/24	Les deux	Lien WAN entre les deux pare-feux
Tunnel VPN	10.0.0.0/30	Virtuel	Interfaces virtuelles du tunnel OpenVPN

4. INFRASTRUCTURE DÉPLOYÉE

4.1 — INVENTAIRE DES ÉQUIPEMENTS

Équipement	Rôle	Adresse IP	Localisation
pfSense A (Siège)	Pare-feu / Serveur OpenVPN	WAN: 172.16.0.10 | LAN: 192.168.10.1	Limoges
pfSense B (Agence)	Pare-feu / Client OpenVPN	WAN: 172.16.0.20 | LAN: 192.168.20.1	Bordeaux
Poste Client A	Poste utilisateur Site A	192.168.10.50	Limoges
Poste Client B	Poste utilisateur Site B	192.168.20.50	Bordeaux

4.2 — FLUX RÉSEAU AUTORISÉS

Source	Destination	Protocole	Objet
pfSense B WAN (172.16.0.20)	pfSense A WAN:1194	UDP	Établissement du tunnel OpenVPN
192.168.10.0/24	192.168.20.0/24	Tout	Trafic inter-sites via tunnel
192.168.20.0/24	192.168.10.0/24	Tout	Trafic inter-sites via tunnel
192.168.10.0/24	Internet	TCP/UDP	Navigation, mises à jour (via pfSense A)

192.168.20.0/24	Internet	TCP/UDP	Navigation, mises à jour (via pfSense B)

4.3 — COMPOSANTS PKI

Élément PKI	Nom	Hébergé sur	Rôle
Autorité de Certification	CA_VPN_TechConnect	pfSense A	Signe et valide tous les certificats du tunnel
Certificat Serveur	cert-serveur-pfsense-a	pfSense A	Authentifie pfSense A auprès des clients
Certificat Client	cert-client-pfsense-b	pfSense B	Authentifie pfSense B auprès du serveur

5. INDEX DES DOCUMENTATIONS TECHNIQUES

La mise en œuvre complète du projet est couverte par quatre documents techniques. Chaque document est autonome et peut être consulté indépendamment. Ils sont présentés dans l'ordre logique de déploiement.

Référence	Titre	Description
DOC-01	Préparation de l'environnement de virtualisation	Configuration de l'hyperviseur Proxmox VE : création des bridges réseau virtuels, téléversement des ISOs, création et paramétrage des machines virtuelles, configuration du NAT et vérification de l'environnement avant déploiement.
DOC-02	Installation et configuration des postes clients	Déploiement des postes clients Debian 13 : installation depuis ISO, configuration de l'adressage IP statique, installation des outils réseau (ping, traceroute, nmap), et validation de la connectivité LAN.
DOC-03	Installation et configuration des pare-feux pfSense CE	Installation de pfSense CE sur les deux sites : assignation des interfaces WAN et LAN, configuration console, premier accès à l'interface web, assistant de configuration initiale, activation du serveur DHCP sur chaque LAN.

DOC-04	Configuration du tunnel OpenVPN Site-à-Site (SSL/TLS)	Mise en place de la PKI (CA, certificats serveur et client), export et import des certificats entre les deux sites, configuration du serveur OpenVPN sur pfSense Limoges, configuration du client OpenVPN sur pfSense Bordeaux, règles de filtrage firewall, tests de connectivité.

6. BILAN DU PROJET

6.1 — RESULTATS OBTENUS

Le tunnel VPN Site-à-Site entre les sites de Limoges et Bordeaux est pleinement opérationnel. Les objectifs initiaux définis par la DSI ont été atteints :

- Tunnel OpenVPN SSL/TLS établi avec chiffrement AES-256-GCM et Perfect Forward Secrecy.
- Les postes des deux sites communiquent de manière transparente et sécurisée.
- L'accès aux ressources internes depuis Bordeaux ne transite plus par des services tiers.
- La PKI interne permet une gestion centralisée des certificats par la DSI.
- La surveillance du tunnel est assurée via les outils de diagnostic intégrés à pfSense.