MANOLIOS Benjamin *EPSI Montpellier*

N° candidat : 02443855566

Épreuve E6

Situation N°2

Mise en place d'un serveur OpenVPN pour sécuriser l'accès au réseau d'entreprise

Sommaires :

Table des matières

Contexte

Je suis actuellement employé à la Maison des Ligues de Lorraine (M2L), un établissement dépendant du Conseil Régional de Lorraine. Elle a pour mission de soutenir les ligues sportives régionales en leur fournissant des services logistiques, administratifs et techniques. La M2L héberge plusieurs structures dans différents bâtiments, proposant des bureaux équipés, des salles mutualisées (réunion, formation, amphithéâtre) et un accès à un réseau informatique commun.

Avec le développement du télétravail et les besoins de mobilité croissants, la M2L est confrontée à un nouveau défi : permettre un accès distant sécurisé à son réseau informatique pour certains profils, comme les techniciens, les responsables de ligue ou les administrateurs réseau. L'objectif est de leur offrir une solution fiable pour se connecter depuis l'extérieur, tout en garantissant la confidentialité des échanges et la sécurité des accès.

Pour répondre à ce besoin, la M2L a choisi de mettre en place un serveur VPN basé sur OpenVPN, un logiciel libre qui permet de créer une connexion sécurisée et chiffrée entre un utilisateur à distance et le réseau interne de l'organisation (comme s'il était physiquement sur place).

Ce serveur est capable de gérer :
• L'établissement d'un tunnel VPN sécurisé, assurant une connexion chiffrée entre l'utilisateur et le réseau M2L,
• La confidentialité des données échangées, grâce à un chiffrement fort,
• Le contrôle des accès, via des certificats ou des identifiants d'authentification,
• Une intégration au réseau interne pour permettre aux utilisateurs d'accéder aux services habituels (partages de fichiers, outils internes, etc.).

La solution est déployée sur une infrastructure virtualisée avec Proxmox VE, un outil qui permet de créer et gérer plusieurs machines virtuelles (VM) sur un seul serveur physique. OpenVPN y est hébergé aux côtés de plusieurs machines clientes (Windows/Linux).

Ce projet permet à la M2L de sécuriser l'accès distant à ses services informatiques et me permet de mettre en œuvre des compétences clés du BTS SIO SISR, notamment en administration réseau, virtualisation, et sécurité des accès distants.

CLIENT :

Maison des Ligues de Lorraine (M2L)

Description :

La Maison des Ligues de Lorraine (M2L) est un établissement public placé sous la responsabilité du Conseil Régional de Lorraine. Elle a pour mission de soutenir les différentes ligues sportives régionales en leur fournissant des locaux, des services logistiques, des équipements informatiques, ainsi qu'un accès à une infrastructure réseau partagée.

Avec l'évolution des usages numériques, la généralisation du télétravail et l'augmentation des déplacements professionnels, la M2L a exprimé le besoin de permettre un accès distant sécurisé à son réseau interne. C'est dans ce cadre qu'a été initié le projet de mise en place d'un serveur VPN basé sur OpenVPN.

L'objectif est d'autoriser les connexions à distance tout en assurant la confidentialité des données échangées et un contrôle strict des accès externes. La solution repose sur OpenVPN, un logiciel libre qui permet d'établir une connexion chiffrée entre l'utilisateur distant et le réseau interne, comme s'il était physiquement présent sur le site.

Ce projet renforce la mobilité des utilisateurs de la M2L tout en garantissant la sécurité du système d'information, grâce à une authentification par certificats et à l'intégration dans une infrastructure virtualisée existante.

Problème :

Jusqu'à présent, l'accès au réseau de la M2L ne pouvait se faire qu'en local, ce qui limitait fortement les possibilités de **travail à distance** et d'**intervention à distance** sur les équipements. De plus, aucune solution sécurisée n'était en place pour **protéger les connexions externes** aux ressources internes. Cela exposait l'infrastructure à des risques de piratage ou d'accès non autorisé.

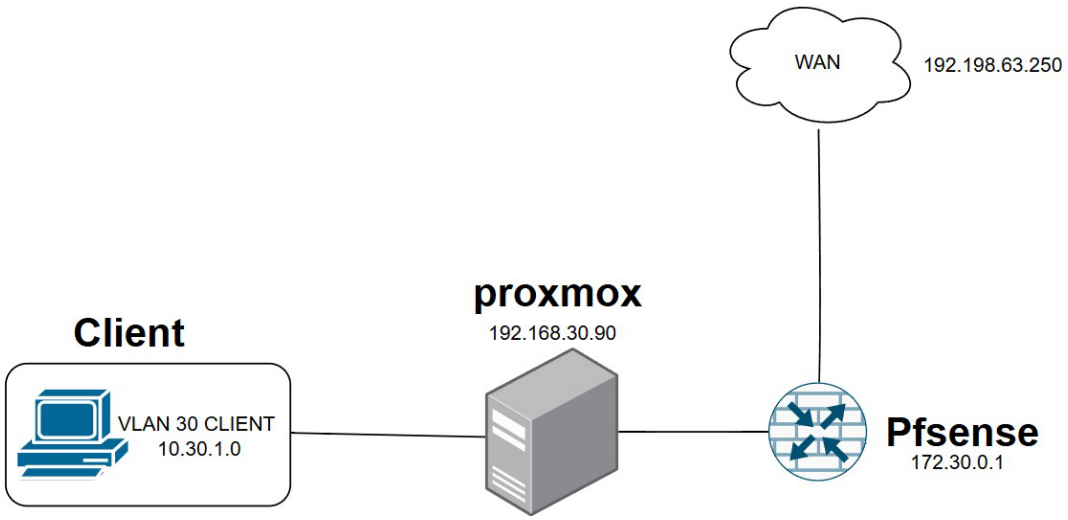
Solution :

Déployer un **serveur OpenVPN** dans l'infrastructure **virtualisée Proxmox VE**, et l'intégrer au réseau géré par pfSense pour permettre un **accès distant sécurisé** aux ressources internes de la M2L.

Les fonctionnalités mises en place incluent :

- **La création d'un tunnel VPN chiffré basé sur TLS/SSL** : cela permet de sécuriser les connexions à distance en chiffrant les données échangées entre l'utilisateur et le réseau interne,
- **L'authentification des utilisateurs via fichiers .ovpn personnalisés** : chaque utilisateur possède un fichier de configuration personnel contenant ses certificats de sécurité pour accéder au VPN,
- **La restriction des connexions aux équipements autorisés** : seules les machines disposant des bons fichiers de configuration peuvent se connecter, ce qui renforce la sécurité,
- **Le journal des connexions VPN** : toutes les connexions sont enregistrées pour assurer une traçabilité complète (utilisateur, date, durée, IP),
- **L'accès sécurisé aux services internes** : une fois connecté, l'utilisateur peut accéder aux serveurs, à l'intranet et aux ressources réseau comme s'il était physiquement sur le site.

Réseaux avant modification :



On y retrouve :

Un pare-feu pfSense

→ Connecté à Internet (WAN, IP publique : 192.198.63.250)

→ IP interne : 172.30.0.1

→ Il assure le routage, le DHCP et la sécurité du réseau

Un serveur Proxmox VE

→ IP : 192.168.30.90

→ Il héberge plusieurs machines virtuelles, réparties en VLAN

Deux VLANs configurés :

• VLAN 10 : pour les serveurs principaux

• VLAN 30 : pour les postes clients (ex : 10.30.1.0/24)

Problème identifié

Avec le développement du télétravail et les déplacements professionnels, certains utilisateurs de la M2L (techniciens, responsables de ligue, administrateurs) avaient besoin d'accéder au réseau interne à distance.
Cependant, aucun système sécurisé d'accès distant n'était en place. Cela représentait un risque important :

Les utilisateurs devaient parfois contourner la sécurité,

Aucun chiffrement des échanges n'était garanti,

Aucune traçabilité des connexions externes n'était possible.

Solution mise en œuvre

Pour répondre à ces besoins, j'ai déployé un serveur OpenVPN dans l'infrastructure virtualisée sous Proxmox VE, en complément de pfSense.

OpenVPN a été configuré pour :

Créer un tunnel VPN sécurisé basé sur TLS/SSL,

Authentifier les utilisateurs via des fichiers de configuration .ovpn personnalisés,

Restreindre les accès uniquement aux machines autorisées,

Consigner les connexions VPN dans un journal,

Permettre un accès sécurisé aux ressources internes (intranet, serveurs, services réseau).

Grâce à cette solution, les utilisateurs peuvent se connecter à distance comme s'ils étaient physiquement sur le site, tout en respectant les règles de sécurité du système d'information.

Avantages

Sécurité renforcée : les connexions sont chiffrées et protégées contre les interceptions,

Contrôle des accès : seuls les utilisateurs autorisés avec leur certificat peuvent se connecter,

Souplesse d'utilisation : compatible avec Windows, Linux, macOS, Android...,

Traçabilité complète : les connexions sont enregistrées et analysables,

Solution gratuite et fiable : OpenVPN est open source, reconnu pour sa stabilité et sa sécurité.

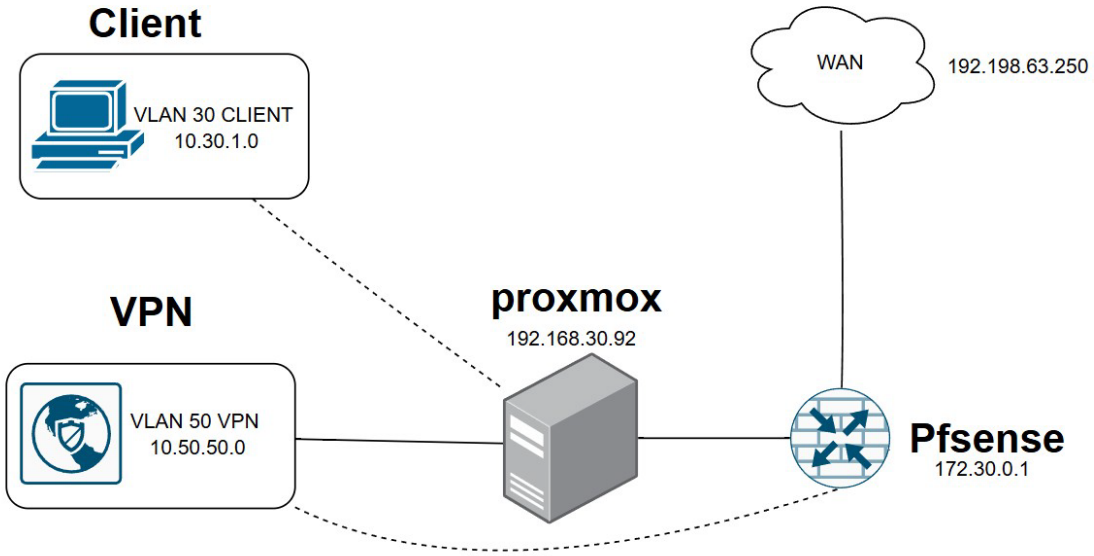
Inconvénients

Configuration technique : la mise en place demande une bonne connaissance réseau et sécurité (certificats, pare-feu, routage...),

Maintenance : il faut gérer les certificats et surveiller les journaux,

En cas de mauvaise configuration, l'accès distant peut ne pas fonctionner, voire exposer le réseau.
Toutefois, une fois en place, OpenVPN offre une solution performante, stable et professionnelle.

Réseaux après modification



Mise en place :

1. Prérequis et installation

Mettre à jour et installer OpenVPN et Easy-RSA :

sudo apt update
sudo apt install openvpn easy-rsa -y **2.**

Préparation de l'environnement PKI

Créer et initialiser le dossier PKI :

make-cadir ~/openvpn-ca cd
~/openvpn-ca Initialiser le
CA :

source ./vars ./clean-all
./build-ca

3. Génération des certificats et clés

Certificat serveur : ./build-key-server
server

Diffie-Hellman :
./build-dh

Clé TLS :
openvpn --genkey --secret ta.key

Clé client :
./build-key client1

4. Configuration du serveur OpenVPN Copier les fichiers dans

/etc/openvpn/server/ : ***sudo cp***

keys/{server.crt,server.key,ca.crt,dh.pem,ta.key} /etc/openvpn/server/

Créer et éditer le fichier : sudo nano /etc/openvpn/server/server.conf

Exemple de configuration :
port 1194
proto udp dev tun

ca ca.crt cert server.crt key server.key dh dh.pem tls-crypt ta.key

server 10.8.0.0 255.255.255.0 ifconfig-pool-persist ipp.txt push "redirect-gateway def1 bypass-dhcp" push "dhcp-option DNS 1.1.1.1" push "dhcp-option DNS 1.0.0.1"

keepalive 10 120
cipher AES-256-CBC
auth SHA256 user nobody group nogroup persist-key persist-tun

status openvpn-status.log log-append /var/log/openvpn.log verb 3 explicit-exit-notify 1

5. Activation du routage IP et NAT

Activer le routage dans /etc/sysctl.conf : net.ipv4.ip_forward=1

Appliquer : sudo
sysctl -p

Configurer le NAT :
sudo iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -o ens18 -j MASQUERADE

6. Démarrage et vérification du service Démarrer et activer le service :

sudo systemctl start openvpn@server sudo
systemctl enable openvpn@server

Vérification :
sudo systemctl status openvpn@server

7. Test de la connexion OpenVPN

Créer un fichier .ovpn pour le client puis tester la connexion avec un client OpenVPN.

8. Résumé des fichiers importants

Chemin	Rôle
/etc/openvpn/server/server.conf	Configuration du serveur
/etc/openvpn/server/	Certificats et clés
/etc/openvpn/server/server.log	Log du serveur OpenVPN	
/etc/sysctl.conf | Activation du routage IP |

Conclusion

La mise en place d'un **serveur OpenVPN** au sein de la **Maison des Ligues de Lorraine** a permis de répondre à un besoin crucial : **offrir un accès distant sécurisé** aux utilisateurs autorisés, dans un contexte de **mobilité croissante** et de **télétravail**.

Grâce à cette solution, les collaborateurs peuvent désormais **se connecter au réseau interne** de la M2L de manière **chiffrée**, depuis n'importe quel lieu, tout en **garantissant la confidentialité des données** et un **contrôle précis des accès**.

Ce projet s'intègre dans une **infrastructure virtualisée moderne** basée sur **Proxmox VE**, avec une supervision centralisée via **pfSense**, offrant une **architecture évolutive, sécurisée et performante**.

Sur le plan personnel, ce projet m'a permis de :

- **Mettre en pratique mes compétences** en administration réseau et sécurité,
- Me familiariser avec le **déploiement d'un VPN professionnel**,
- Travailler dans un **environnement virtualisé complexe**,
- Renforcer ma rigueur dans la configuration, le test et le suivi d'un service réseau.

Pour l'avenir, des évolutions sont envisageables, telles que :

- L'**intégration de l'authentification à deux facteurs (2FA)** pour renforcer la sécurité,
- La **mise en place de politiques d'accès plus fines**, par groupes d'utilisateurs ou plages horaires,
- L'automatisation de la **gestion des certificats** pour simplifier la maintenance.

ANNEXE BTS :

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2025**

ANNEXE 9-1-A : Fiche descriptive de réalisation professionnelle (recto)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	**N° réalisation** : 02
Nom, prénom : MANOLIOS Benjamin	**N° candidat** : 02443855566
☑ **Épreuve ponctuelle** ☐ **Contrôle en cours de formation**	**Date** :

Organisation support de la réalisation professionnelle

La Maison des Ligues de la Lorraine, établissement du Conseil Régional de Lorraine, est responsable de la gestion du service des sports et en particulier des ligues sportives ainsi que d'autres structures hébergées. La M2L doit fournir les infrastructures matérielles, logistiques et des services à l'ensemble des ligues sportives installées. Elle assure l'offre de services et de support technique aux différentes ligues déjà implantées (ou à venir) dans la région.
M2L souhaite mettre en place un serveur permettant une connexion sécurisée à distance.

Intitulé de la réalisation professionnelle

Installation et configuration d'un serveur VPN

Période de réalisation : 25/11/2024 - 26/03/25 **Lieu :** EPSI MONTPELLIER

Modalité : ☐ Seul ☑ En équipe

Compétences travaillées

- ☑ Concevoir une solution d'infrastructure réseau
- ☑ Installer, tester et déployer une solution d'infrastructure réseau
- ☑ Exploiter, dépanner et superviser une solution d'infrastructure réseau

Conditions de réalisation [1] (ressources fournies, résultats attendus)

Ressources fournies :

- Cahier des charges M2L
- Serveur Asus PRO Q570M
- Proxmox VE 8.2
- OpenVPN
- VM client Linux/Windows

Résultats attendus :

- Connexion sécurisée à distance
- Authentification sur le réseaux
- Création des certifica client/serveur

Description des ressources documentaires, matérielles et logicielles utilisées [2]

- Schéma réseau M2L
- Documentation d'installation et configuration de OpenVPN
- Documentation d'installation et configuration de VM client Linux/Windows
- Documentation d'installation et configuration de Proxmox

Modalités d'accès aux productions [3] et à leur documentation

Lien de production : lnsh.xyz/ed11ef

Lien de documentations :

- **OpenVPN** : lnsh.xyz/631992
- **Proxmox** : lnsh.xyz/ddf77c
- **Client** : lnsh.xyz/48f056

1 En référence aux *conditions de réalisation et ressources nécessaires* du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO.
2 Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.
3 Conformément au référentiel du BTS SIO « *Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve.* ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.
4 Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemples schéma complet de réseau mis en place et configurations des services.