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

BTS SIO SISR 2024/2025

Sommaires :

Table des matières

Contexte

Contexte et besoins de la Maison des Ligues de Lorraine (M2L)

La Maison des Ligues de Lorraine (M2L) est un établissement sous l'égide du Conseil Régional de Lorraine, ayant pour mission principale d’assurer la gestion et le support des ligues sportives régionales ainsi que d'autres structures hébergées. Afin de garantir un fonctionnement optimal et sécurisé, la M2L met à disposition des infrastructures adaptées, incluant des ressources matérielles et logistiques, permettant aux ligues de bénéficier d’un environnement stable et performant.

Dans cette optique, la M2L souhaite moderniser et centraliser la gestion de son infrastructure informatique. Cette modernisation vise à simplifier l’administration des utilisateurs, la gestion des adresses IP et le déploiement d’applications au sein de son réseau. En adoptant une solution intégrée et automatisée, la M2L aspire à renforcer la sécurité, optimiser la gestion des accès et faciliter l’organisation des ressources informatiques pour les ligues sportives qu’elle héberge.

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 **ressources informatiques**, des **services techniques** et un **accès à un réseau mutualisé**.

Avec l'évolution des usages et l'augmentation du nombre de structures hébergées, la M2L est confrontée à un nouveau besoin : permettre à certains utilisateurs (techniciens, responsables de ligues, administrateurs réseau) de **se connecter à distance** au réseau de l'organisation **en toute sécurité**, notamment dans un contexte de télétravail ou de déplacement professionnel.

C'est dans ce cadre que le projet de **mise en place d'un serveur VPN** basé sur **OpenVPN** a été initié. L'objectif est d'établir un **accès distant chiffré** au réseau interne tout en assurant la **confidentialité des données échangées** et le **contrôle des connexions externes**.

Accès sécurisé au réseau avec OpenVPN

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 :

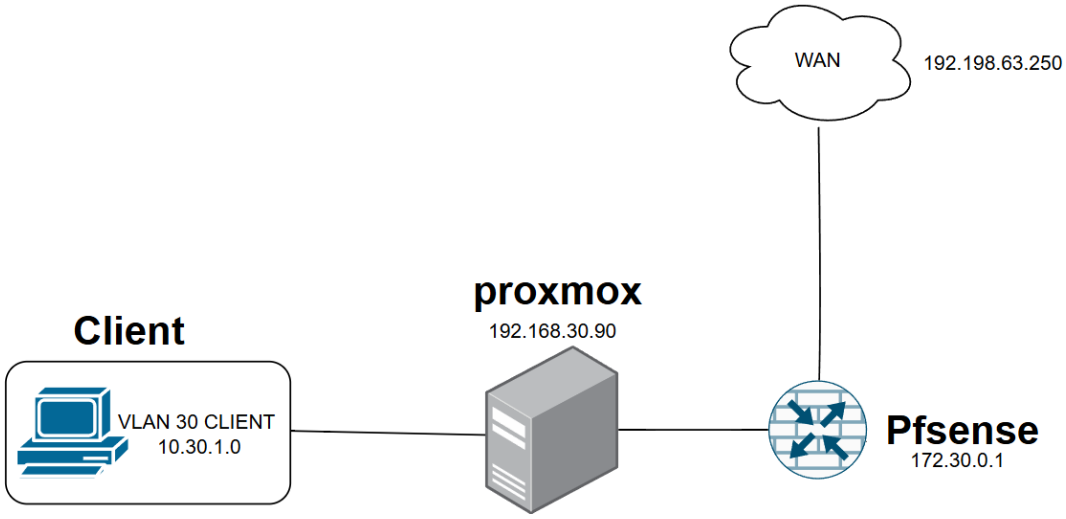
Déployer un **serveur OpenVPN** dans l'infrastructure virtualisée Proxmox, en intégration avec pfSense pour la gestion réseau.
Les fonctionnalités mises en place incluent :

- La **création d'un tunnel VPN chiffré** basé sur TLS/SSL
- L'**authentification des utilisateurs** via fichiers de configuration .ovpn personnalisés

- La **restriction des connexions** aux seuls équipements autorisés
- Le **journal des connexions VPN** pour assurer un suivi des accès
- L'accès sécurisé aux services internes (intranet, serveurs, gestion réseau)

Cette solution permet à la M2L de **gagner en flexibilité** tout en maintenant un haut niveau de **sécurité informatique**. L'accès à distance est désormais **sécurisé, contrôlé et chiffré**, ce qui constitue un **progrès important dans la gestion moderne de l'infrastructure réseau**.

Réseaux avant modification :



On y retrouve :

Solution :

Déploiement d'OpenVPN pour un accès distant sécurisé

Problème :

La M2L ne disposait pas de solution pour permettre aux utilisateurs de se connecter à distance au réseau. Cela limitait le télétravail et exposait le système à des risques si des connexions non sécurisées étaient utilisées.

Solution :

J'ai mis en place un serveur OpenVPN sur une machine virtuelle hébergée via Proxmox VE. Le serveur établit un tunnel sécurisé entre les utilisateurs distants et le réseau interne de la M2L. Chaque utilisateur utilise un fichier .ovpn personnalisé pour se connecter.
Le trafic est chiffré, l'accès est restreint, et le tout est géré via l'interface pfSense.

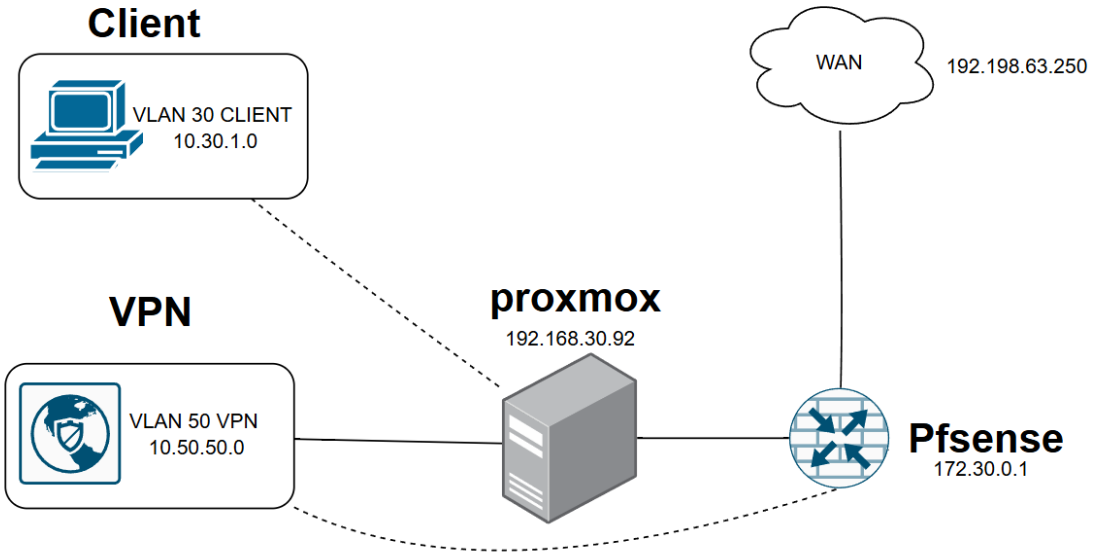
Avantages :

- **Connexion sécurisée à distance**
- **Compatible sur tous les systèmes**
- **Facile à administrer et à déployer**

Inconvénients :

- **Nécessite une bonne configuration réseau**
- **Les utilisateurs doivent être accompagnés pour l'installation initiale du client VPN**

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 répond à un besoin essentiel de connexion sécurisée à distance. Grâce à cette solution, les utilisateurs autorisés peuvent désormais accéder au réseau interne de manière chiffrée, depuis n'importe quel lieu, tout en maintenant la confidentialité des données et un bon niveau de contrôle administratif.

Ce projet a permis d'améliorer la sécurité globale de l'infrastructure, tout en rendant l'environnement de travail plus flexible, notamment dans le cadre du télétravail ou des déplacements. La solution choisie, basée sur OpenVPN, est compatible avec la plupart des systèmes d'exploitation et reste facile à administrer. Intégrée dans un environnement virtualisé Proxmox et supervisée via pfSense, elle offre une architecture moderne et scalable.

Ce travail m'a permis de renforcer mes compétences en administration réseau, en sécurisation des accès, et en déploiement de services dans un contexte professionnel. Pour l'avenir, des améliorations comme l'intégration d'une authentification à deux facteurs pourraient encore renforcer la sécurité des connexions distantes.

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.