**Documentation technique**

**Contexte et Objectifs**

Le projet VPN a pour but de mettre en place un environnement réseau sécurisé, permettant à des utilisateurs d’accéder à distance à un intranet privé via Internet, tout en garantissant la confidentialité, l’intégrité et l’authentification des connexions. L’objectif global est de concevoir, configurer et déployer une infrastructure VPN fiable. Cela inclut l’installation du serveur VPN, la configuration réseau, la mise en œuvre de mécanismes de sécurité, ainsi que la réalisation d’une démonstration fonctionnelle illustrant l’accès distant sécurisé au réseau interne.

**Objectifs principaux**

**Administration d’un serveur**

L’un des objectifs principaux de ce projet est de mettre en place un serveur fonctionnel, stable et sécurisé, reposant sur un système Linux (Raspberry Pi OS basé sur Debian) installé sur un Raspberry Pi. Il s’agit d'assurer l'installation et la configuration du système.

**Infrastructure Système & Réseaux**

Le projet vise également à concevoir une infrastructure réseau cohérente et sécurisée. Cela comprend la mise en place du routage, du NAT, la configuration du pare-feu ainsi que l’ouverture et la redirection des ports nécessaires pour le bon fonctionnement du VPN. Un accent particulier est mis sur la fiabilité de la connexion.

**Environnement virtuel**

Ensuite, l’environnement repose principalement sur un Raspberry Pi, utilisé comme plateforme matérielle pour déployer et tester l’infrastructure réseau. Ce choix permet de simuler un environnement de production à petite échelle, tout en offrant une configuration flexible, économe en ressources et facilement transportable. Le Raspberry Pi permet ainsi de valider les différentes étapes du projet dans un cadre réel, tout en restant proche des contraintes et exigences d’un déploiement professionnel.

**Sécurité**

Enfin, la sécurité constitue un pilier central de ce projet. L’objectif est de garantir une authentification forte des utilisateurs, par l’usage de certificats et potentiellement d’une authentification multifacteur. Le projet intègre également une réflexion sur la politique de sécurité, la gestion des accès au réseau interne via VPN.

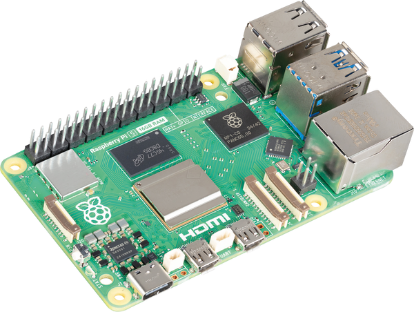
**Présentation des outils et justification du choix**

Pour ce projet de mise en place d’un accès VPN sécurisé à un réseau intranet, plusieurs outils et technologies ont été utilisés, chacun choisi pour sa pertinence et son efficacité dans le contexte.

**OpenVPN**

OpenVPN est un logiciel libre pour la création de VPN. Il permet de chiffrer le trafic réseau entre un client distant et le serveur local, garantissant sécurité et confidentialité. Nous l’avons choisi pour sa stabilité, sa compatibilité multiplateforme car il est disponible sur Windows, Linux, macOS, Android, iOS, ChromeOS. De plus, il est simple à installer et configurer grâce à des scripts automatisés comme celui d’Angristan.

**Raspberry Pi sous Raspberry Pi Os Lite**

Nous avons choisi d’hébergé le server VPN sur un **Raspberry Pi**, un mini-ordinateur (peu coûteux, économe en énergie et suffisamment puissant pour ce type de service). Nous avons choisi comme système d’exploitation Raspberry Pi Os Lite, pour sa légèreté, sa sécurité et sa compatibilité avec OpenVPN. C’est la meilleure solution pour héberger un service 24h/24 depuis chez soi comme pour ce projet.

**Etape de réalisation**

**Mise en place du Raspberry Pi 3B+**

D’abord nous avons commencé par installer Raspberry Pi Imager afin de mettre en place une image système sur la carte SD.

Pour cela nous avons connecté la carte SD à l'ordinateur et exécuté Raspberry Pi Imager puis avons choisi le système d’exploitation Raspberry Pi Os Lite. Aussi, lors de l’initialisation de l’os nous avons pu configurer différents paramètres du Raspberry comme le compte admin et son mot de passe et les configurations wifi.

Une image contenant texte, capture d’écran, Police, logo

Le contenu généré par l’IA peut être incorrect.

Capture d’écran pour la mise en place du Raspberry Pi.

Enfin, nous avons branché le Raspberry électriquement.

**Paramètres routeur (Livebox 6)**

**1. Configuration DynDNS**

Afin de pouvoir accéder à tout moment à notre réseau, nous avions besoin d’avoir un nom de domaine qui pointe en permanence vers l’IP changeante de notre box.  
Pour cela nous avons choisi d’utiliser l’outil No-IP et avons créé un compte et un nom de domaine : **myhomeraspberrypi.zapto.org**.

Ensuite, depuis le, panel de configuration de la box nous avons connecté l’outil No-IP à notre box.

Une image contenant texte, capture d’écran, Police, nombre

Le contenu généré par l’IA peut être incorrect.

**Installation & Configuration OpenVPN**

**1. Mise à jour système**

Une image contenant texte, carte de visite, capture d’écran, Rectangle

Le contenu généré par l’IA peut être incorrect.

Commande permettant de mettre à jour le système.

Tout d’abord on s’assure de mettre à jour le système et ses paquets pour s'assurer qu'on procède aux l’installation d’OpenVPN sur une base à jour.

**2. Téléchargement du script OpenVPN via Angristan**

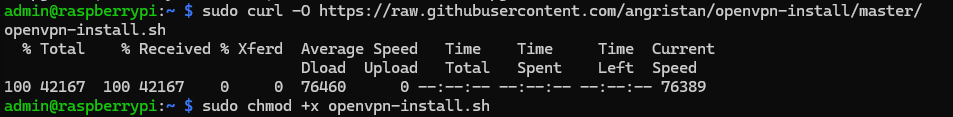
**Une image contenant texte, capture d’écran, carte de visite, Police

Le contenu généré par l’IA peut être incorrect.**

Commande permettant l’installation d’OpenVPN et la gestion de ses droits et accès.

On procède au téléchargement du script d'installation automatique d'OpenVPN depuis GitHub. Ensuite on rend le script exécutable, pour pouvoir le lancer. Enfin on lance le script avec les droits administrateurs. Il posera plusieurs questions pour configurer le serveur VPN (IP, port, DNS …).

**3. Configuration lors de l’installation**

****Nous avons ensuite exécuté le scripte d’installation de OpenVPN, avons mis l’IP local du Raspberry (192.168.1.42) et avons mis le nom de domaine associé à notre IP publique ([myhomeraspberrypi.zapto.org](http://myhomeraspberrypi.zapto.org)) et choisi le port 1194.

**Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.**

**Création des utilisateurs et utilisation d’OpenVPN Connect**

**1 - Création des utilisateurs**

On crée notre utilisateur Lucas a l’aide du script d’installation :

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

On transfert ensuite le fichier utilisateur « Lucas.ovpn » créé sur notre machine à l’aide de la commande scp :



**2 - Connection des utilisateurs**

Pour se connecter, il faut installer le logiciel client OpenVPN Connect et importer le fichier « .ovpn » transfert ci-dessus.

Une image contenant texte, capture d’écran, logiciel, Logiciel multimédia

Le contenu généré par l’IA peut être incorrect.

Il suffit ensuite d’appuyer sur le bouton de connexion pour se connecter au VPN !

Une image contenant texte, capture d’écran, conception

Le contenu généré par l’IA peut être incorrect.

**Mise en place de l’intranet : Partage de fichier samba**

**1 - Installation de Samba**

Sur le Raspberry nous avons installé samba à l'aide de la commande :

sudo apt install samba -y

Ensuite nous avons créé le dossier home/data qui sera notre dossier partagé et avons configuré ce partage dans /etc/samba/smb.conf puis nous avons redémarré Samba :

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

Une image contenant texte, Police, capture d’écran, conception

Le contenu généré par l’IA peut être incorrect.

Ensuite, nous avons créé un groupe d’utilisateur appelé « employe », où nous avons mis nos utilisateurs pour que toutes les personnes étant dans ce groupe aient accès à ce dossier data.

Une image contenant texte, capture d’écran, Police

Le contenu généré par l’IA peut être incorrect.

**2 - Accès utilisateur au dossier partagé**

Accès au dossier partagé depuis un Client Windows :

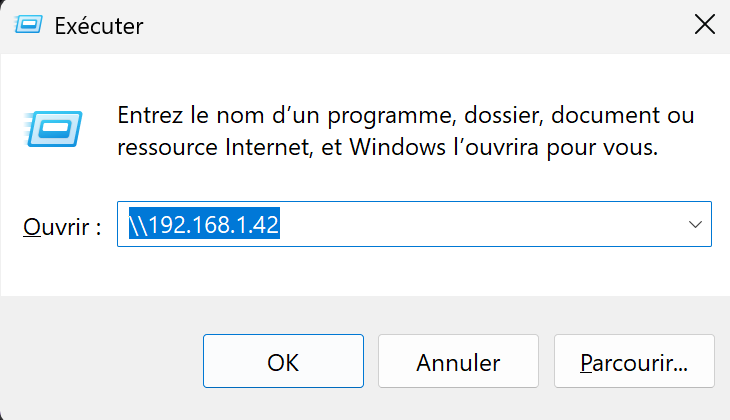
1. Ouvrir l'Explorateur de Fichiers :

* Cliquez sur l'icône de l'Explorateur de fichiers dans la barre des tâches (utilisez le raccourci clavier Win + E.)
* Accéder au dossier partagé : Dans la barre d'adresse de l'explorateur de fichiers, tapez \\<IP\_du\_Serveur\_Linux> et appuyez sur Entrée. Dans notre cas [\\168.192.1.42](file:///\\168.192.1.42).

Une image contenant capture d’écran, logiciel, Logiciel multimédia, texte

Le contenu généré par l’IA peut être incorrect.

* Utilisez le raccourci clavier Win + E et tapez \\<IP\_du\_Serveur\_Linux> (dans notre cas \\168.192.1.42.) et appuyez sur Entrée ou OK.



* Une fenêtre de connexion s’ouvrira, entrez les informations demandées

Une image contenant texte, capture d’écran, logiciel, Police

Le contenu généré par l’IA peut être incorrect.

* Vous avez accès aux fichiers partagés

Une image contenant capture d’écran, logiciel, Logiciel multimédia, Logiciel de graphisme

Le contenu généré par l’IA peut être incorrect.

**Supprimer les informations d'identification enregistrées**

**1. Ouvrir le Gestionnaire des identifiants :**

* Cliquez sur le menu **Démarrer** et tapez "**Gestionnaire des identifiants**".
* Sélectionnez **Gestionnaire des identifiants**.

**2. Supprimer les informations d'identification enregistrées :**

* Dans le **Gestionnaire des identifiants**, cliquez sur "**Identifiants Windows**".
* Recherchez l'entrée correspondant à l'adresse IP(ici, \\192.168.1.42).
* Cliquez sur la flèche à droite de l'entrée pour l'agrandir.
* Cliquez sur **Supprimer**.

**3. Confirmer la suppression :**

* Confirmez que vous souhaitez supprimer les informations d'identification.

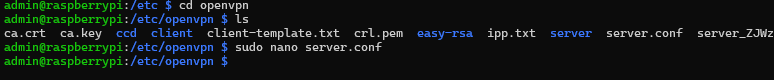
**Ou via l’Invite de commandes :**

* Cliquez sur le menu **Démarrer**, tapez "**cmd**", faites un clic droit sur "**Invite de commandes**" et sélectionnez "**Exécuter en tant qu'administrateur**".
* Supprimer les informations d'identification :
  + Dans l'invite de commande, tapez la commande suivante et appuyez sur **Entrée** :  
    net use \* /delete

Cette commande supprimera toutes les connexions réseau actives et les informations d'identification enregistrées.

**Log des activités de connection sur OpenVPN**

Nous avons configuré dans le fichier de configuration d’OpenVPN pour qu’un fichier server.conf :

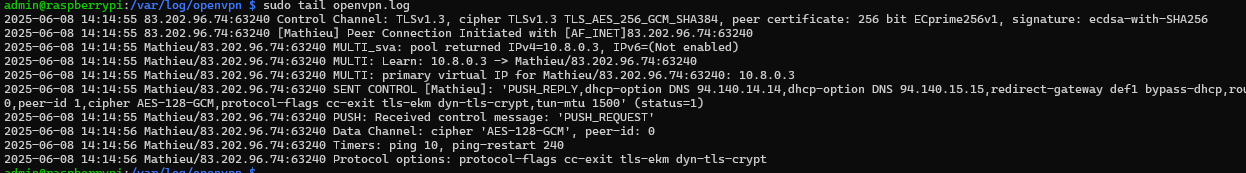




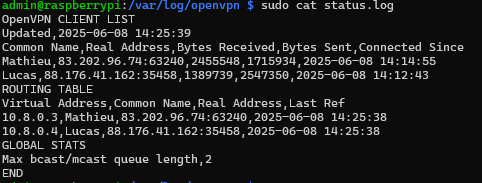
Le verb permet de choisir la quantité d’informations des logs.

Et nous avons donc maintenant de fichiers de log :

openvpn.log : Fichier dans lequel seront contenues toutes les activités de connexion sur le serveur VPN.



status.log : Fichier dans lequel seront contenues les informations concernant l’état du serveur VPN et dernières connexions.



**Glossaire :**

* **VPN (Virtual Private Network)** : Réseau privé virtuel permettant de créer une connexion sécurisée entre un utilisateur et un réseau distant via Internet.
* **SSH (Secure Shell)** : Protocole sécurisé permettant de se connecter à distance à un serveur pour le gérer en ligne de commande.
* **IP (Internet Protocol)** : Adresse unique permettant d’identifier chaque appareil sur un réseau.
* **Firewall (pare-feu)** : Outil de sécurité qui contrôle le trafic réseau entrant et sortant, selon des règles définies.
* **Raspberry Pi** : Mini-ordinateur peu coûteux, utilisé ici comme serveur pour héberger des services réseau.
* **Certificat SSL/TLS** : Fichier permettant d’assurer l’authenticité d’un serveur et de chiffrer les échanges de données.
* **IAM (Identity and Access Management)** : Système de gestion des identités et des droits d’accès aux ressources réseau.
* **Bash** : Langage de script utilisé sous Linux pour automatiser des tâches en ligne de commande.
* **TCP (Transmission Control Protocol)** : Protocole de transport fiable qui garantit la livraison des paquets dans le bon ordre, avec vérification des erreurs. Utilisé pour les connexions où la fiabilité est essentielle (ex : HTTP, SSH).
* **UDP (User Datagram Protocol)** : Protocole de transport plus rapide mais non fiable, sans vérification ni garantie de réception. Utilisé pour des applications en temps réel comme le streaming ou certains VPN.