OPENVPN

Installation (Ruddy) :

L'installation d'OpenVPN est assez simple, mais la procédure dépend du système d'exploitation sur lequel vous souhaitez l'installer.

Sur Ubuntu, OpenVPN peut être installé via la commande Advanced Package Tool (APT).

sudo apt install openvpn

Les fichiers de configuration se trouvent dans le répertoire /etc/openvpn/. Vous y trouverez deux répertoires, ainsi qu'un script.

Le répertoire nommé client contiendra les fichiers relatifs à la configuration côté client, tandis que le répertoire server contiendra les fichiers de configuration côté serveur.

Le script update-resolv-conf est appelé une fois lorsque le VPN est activé et lorsqu'il est désactivé. Ce script est utilisé pour mettre à jour le fichier /etc/resolv.conf, qui est responsable du résolveur DNS du système.

Il ajoutera deux types d'informations dans le /etc/resolv.conf :

- Search-domain - Si un utilisateur essaie de pinguer host, le système tentera également de pinguer host.example.com
- Name Server - Le ... par le serveur OpenVPN

Du côté serveur, la configuration contient les éléments suivants :

- local a.b.c.d - Adresse locale sur laquelle le serveur doit écouter
- port 1194 - Port sur lequel le serveur doit écouter
- proto udp - Protocole utilisé pour communiquer avec les clients
- dev tun - Choix de créer un tunnel TUN ou TAP
- ca ca.crt - Certificat de l'Autorité de Certification (CA)
- cert server.crt - Certificat signé (par la CA) du serveur
- key server.key - Clé privée du serveur

Fonctionnement (Thomas) :

slides sur mise en place connexion :

- TLS Handshake pour établir une session
- Requêtes au serveur chiffrées par tunnel pour accès internet
- Désencapsulation puis renvoi au client des données

Fonctionnement (Anton) : Gestion des connexions et résilience

Gestion des connexions multiples :

OpenVPN permet à plusieurs clients de se connecter simultanément au même serveur.
Chaque client reçoit une adresse IP virtuelle, ce qui lui permet d'accéder aux ressources du réseau distant.
Le serveur peut gérer ces connexions via des règles de pare-feu et de routage, en contrôlant quels clients peuvent communiquer entre eux ou avec des sous-réseaux spécifiques.

Résilience et reprise après incident :

OpenVPN inclut des mécanismes de détection de déconnexion (par ex. via des pings ou des timeouts) pour rétablir la connexion automatiquement en cas d'interruption.
Si un serveur principal devient indisponible, un client peut basculer sur un serveur secondaire grâce à une configuration en failover.
Des fonctionnalités comme tls-auth ou tls-crypt peuvent être utilisées pour protéger le serveur contre des attaques de type DDoS ou des tentatives de connexion non autorisées.
Cette partie met en avant la robustesse d'OpenVPN et sa capacité à maintenir une connexion sécurisée et fiable, même en cas de perturbations.

Encapsulation (Farouk) :

OpenVPN est un VPN SSL il utilise par conséquent la très connue librairie OpenSSL offrant des implémentations des algorithmes de chiffrement les plus connus ainsi que du protocole SSL/TLS dont il fait usage pour assurer une transmission sécurisée sur Internet via un mécanisme d'encapsulation assez simple en réalité.

L'idée est que le client OpenVPN local à la machine le paquet original envoyé par l'utilisateur lors d'une requête réseau forgé conformément à la stack TCP/IP classique par exemple lors de l'accès à un site web, . Ce paquet va en fait être encapsulé et chiffré dans un nouveau paquet "OpenVPN" et va agir comme payload.

Ce paquet “OpenVPN” va être porteur d’informations classiques pour assurer sa transmission à la seule unique différence qu’il y a l’ajout d’un header OpenVPN permettant la gestion du tunnel.

Modes (Paul) :

OpenVPN peut fonctionner selon deux modes principaux : **TUN (routé)** et **TAP (ponté)**. Ces modes déterminent la façon dont les paquets sont transmis à travers le tunnel VPN.
TUN : Transmet seulement des paquets IP. Le paquet est directement envoyé avec l'adresse IP de destination définie. Les paquets IP sont encapsulés dans le tunnel avant transmission.
TAP : Fonctionne au niveau Ethernet. Transmet des trames Ethernet complètes, y compris les paquets ARP et les broadcasts. Permet aux clients VPN d’être dans le même réseau local (LAN) que le serveur. Peut transporter d’autres protocoles que l’IP (NetBIOS, etc.).

TUN :

+ Plus rapide que TAP (moins de surcharge car pas d'encapsulation Ethernet complète).
+ Évite la diffusion (broadcast) et donc réduit la consommation de bande passante.
+ Fonctionne bien sur les connexions mobiles et les réseaux avec NAT.
- Ne prend en charge que le trafic IP (pas d'autres protocoles réseau comme NetBIOS).
- Nécessite du routage pour permettre la communication entre le client et le réseau distant.

TAP :

+ Idéal pour créer un réseau LAN virtuel entre plusieurs sites distants.
+ Supporte IPv6 et d’autres protocoles non-IP.
- Moins performant que TUN car plus de surcharge (encapsulation complète Ethernet).
- Plus sensible aux problèmes de broadcast storm (trafic inutile sur le réseau).
- Peut être bloqué par certains pare-feu et routeurs.

TUN utilisé pour :

- Connexion distante à un réseau d’entreprise (accès aux serveurs via IP sans rejoindre le réseau local).
- VPN site-à-site entre deux sites distants qui utilisent des sous-réseaux distincts.

A privilégier si vous voulez un accès sécurisé et performant au réseau distant sans besoin d’être "virtuellement" dans le même LAN.

TAP utilisé pour :

- Accès distant à un réseau d’entreprise comme si l’utilisateur était physiquement connecté.
- Réseaux LAN étendus entre plusieurs sites avec des ressources partagées.

A privilégier si vous avez besoin d’un réseau totalement transparent, avec support des protocoles non-IP et des fonctionnalités comme le partage de fichiers Windows.

IPSEC

C’est quoi ? Ensemble de protocoles qui permettent la création des tunnels cryptés et authentifiés afin de “protéger” le protocole IP

Utilisations :

- **VPN (Virtual Private Network)** : Il permet de créer des tunnels sécurisés entre des sites distants ou des utilisateurs et un réseau privé.
- **Protection des communications réseau** : Il garantit que les données envoyées ne peuvent pas être interceptées ou modifiées par des attaquants.
- **Authentification des échanges** : Il s'assure que l'expéditeur et le destinataire sont bien ceux qu'ils prétendent être.

Le fonctionnement - mode transport

Chiffrement uniquement de la charge utile

- IP non chiffrées
- Messages plus légers
- Deux protocoles de sécurisation :
    - AH (Authentication Header) ⇒ Authentification et intégrité
    - ESP (Encapsulating Security Payload) ⇒ Confidentialité, intégrité et authentification

IPsec sécurise les échanges réseau en assurant :

- Confidentialité
- Intégrité
- Authentification

Deux modes :

- Transport : Chiffrement de la charge utile
- Tunnel : Protection complète du paquet IP

TOR (The Onion Router)

TOR (The Onion Router) est un réseau décentralisé qui permet aux utilisateurs de naviguer sur Internet de manière **anonyme** et sécurisée. Il fonctionne en **chiffrant** les données et en les faisant passer à travers plusieurs **nœuds** (serveurs) avant d'atteindre leur destination.

Comment ça marche ?

1. Lorsqu'un utilisateur envoie une requête via le navigateur TOR, ses données sont **chiffrées en plusieurs couches**, comme un oignon.
2. Ces données transitent par **au moins trois nœuds** :
    - **Nœud d'entrée** : reçoit la requête et la chiffre.
    - **Nœud relais** : fait passer la requête sans connaître l'origine ni la destination.
    - **Nœud de sortie** : déchiffre les données et les envoie au site final.
3. Chaque nœud ne connaît que l’adresse du nœud précédent et du suivant, garantissant ainsi **l’anonymat**.

Pourquoi utiliser TOR ?

- **Anonymat** : Empêche le suivi des adresses IP.
- **Accès aux contenus censurés** : Permet de contourner la surveillance et la censure d’Internet.
- **Navigation sécurisée** : Protège contre la surveillance et l’espionnage en ligne.

Limitations

- **Vitesse réduite** : À cause du passage par plusieurs nœuds.
- **Utilisation par des cybercriminels** : Le Dark Web repose en partie sur TOR.
- **Nœuds de sortie non sécurisés** : Les données non chiffrées peuvent être interceptées.

WireGuard

WireGuard est un protocole VPN (Virtual Private Network) **léger, rapide et sécurisé**. Il permet d'établir des connexions chiffrées entre des appareils à travers Internet, comme un tunnel sécurisé.

Comment ça marche ?

1. **Clés cryptographiques** : WireGuard utilise un système de **clés publiques et privées** (comme SSH) pour l'authentification et l'échange de données.
2. **Simplicité** : Contrairement à d'autres VPN (OpenVPN, IPsec), WireGuard est plus simple à configurer et à maintenir.
3. **Performance** : Il est optimisé pour être **rapide et léger**, avec un **temps de latence réduit** et une **bande passante élevée**.
4. **Sécurité** : Il utilise des algorithmes modernes comme **ChaCha20** pour le chiffrement, garantissant une forte protection contre les attaques.

Pourquoi utiliser WireGuard ?

- **Facilité d'installation** : Moins complexe que d'autres VPN.
- **Vitesse élevée** : Meilleure performance que OpenVPN et IPsec.
- **Sécurité moderne** : Utilise des protocoles de cryptographie récents.
- **Cross-platform** : Fonctionne sur Linux, Windows, macOS, iOS et Android.

Limitations

- **Pas d'IP dynamique native** : Il ne gère pas nativement les adresses IP dynamiques des clients.
- **Encore jeune** : Moins de fonctionnalités avancées que certains VPN plus anciens.

MullVad

Mullvad est un **service VPN** axé sur la **confidentialité et l'anonymat**. Il permet aux utilisateurs de masquer leur adresse IP et de sécuriser leur connexion Internet en chiffrant leurs données.

Pourquoi Mullvad se distingue ?

1. **Anonymat total**
    - Aucune information personnelle requise (pas d'email, pas de nom).
    - Paiement possible en **cryptomonnaies** ou en **espèces** pour plus d'anonymat.
2. **Politique stricte de "No-Logs"**
    - Mullvad **ne conserve aucune donnée utilisateur** (aucun historique de connexion, aucune activité).
3. **Sécurité robuste**
    - Utilise les protocoles **WireGuard** et **OpenVPN** pour un chiffrement de haute qualité.
    - Protection contre les **fuites DNS, IPv6 et WebRTC**.
4. **Facilité d'utilisation**
    - Application simple et efficace pour Windows, macOS, Linux, iOS et Android.
    - Aucun abonnement : un tarif unique de **5€ par mois**, sans engagement.
5. **Serveurs fiables**
    - Présent dans **plus de 40 pays** avec des **serveurs sécurisés** et rapides.

Limitations

- **Pas de support en temps réel** (uniquement email).
- **Moins de serveurs que certains concurrents (ex : NordVPN, ExpressVPN)**.
- **Pas d'options avancées comme le split tunneling** sur toutes les plateformes.