OpenVPN

Un réseau privé virtuel (Virtual Private Network : VPN) est une extension des réseaux locaux LAN.
VPN préserve la sécurité logique que l'on peut avoir à l'intérieur d'un réseau local. Un VPN est une interconnexion de réseaux locaux via la technique de «Tunnel» :
Virtual : Il relie deux réseaux «physiques» (réseaux locaux) par une liaison non fiable (Internet),
Privé : Seuls les ordinateurs des réseaux locaux de part et d'autre du VPN peuvent accéder aux données en clair.

Le VPN vise à apporter 3 éléments essentiels dans la transmission de données :

L'authentification des interlocuteurs
L'intégrité des données
La confidentialité

Principe général

Un réseau VPN repose sur un protocole appelé "**protocole de tunneling**". Ce protocole permet de faire circuler les informations de l'entreprise de façon cryptée d'un bout à l'autre du tunnel. Ainsi, les utilisateurs ont l'impression de se connecter directement sur le réseau de leur entreprise.

Le principe de Tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel. Afin d'assurer un accès aisé et peu coûteux aux intranets ou aux extranets d'entreprise, les réseaux privés virtuels d'accès simulent un réseau privé, alors qu'ils utilisent en réalité une infrastructure d'accès partagée, comme Internet.
Les données à transmettre peuvent être prises en charge par un protocole différent d'Ip. Dans Ce cas, le protocole de tunneling encapsule les données en ajoutant une en-tête.

→ Le tunneling est l'ensemble des processus d'encapsulation, de transmission et de désencapsulation.

Fonctionnalités des VPN

Il existe 3 types standard d'utilisation des VPN :
VPN d'accès : utilisé pour permettre à des utilisateurs **itinérants** d'accéder au réseau privé.
L'utilisateur se sert d'une connexion Internet pour établir la connexion VPN.
VPN intranet : utilisé pour relier au moins deux intranets entre eux. Ce type de réseau est particulièrement utile au sein d'une entreprise possédant plusieurs sites distants
VPN extranet : Une entreprise peut utiliser le VPN pour communiquer avec ses clients et ses partenaires. Elle ouvre alors son réseau local à ces derniers.

Caractéristiques fondamentales d'un VPN

- **Authentification d'utilisateur.** Seuls les utilisateurs autorisés doivent pouvoir s'identifier sur le réseau virtuel. De plus, un historique des connexions et des actions effectuées sur le réseau doit être conservé.
- **Gestion d'adresses**. Chaque client sur le réseau doit avoir une adresse privée. Cette adresse privée doit rester confidentielle. Un nouveau client doit pourvoir se connecter facilement au réseau et recevoir une adresse.
- **Cryptage des données**. Lors de leurs transports sur le réseau public les données doivent être protégées par un cryptage efficace.
- **Gestion de clés**. Les clés de cryptage pour le client et le serveur doivent pouvoir être générées et régénérées.
- **Prise en charge multiprotocole**. La solution VPN doit supporter les protocoles les plus utilisés sur les réseaux publics en particulier IP.

Protocoles utilisés pour réaliser une connexion VPN

Nous pouvons classer les protocoles que nous allons étudier en deux catégories :

- Les protocoles de niveau 2 : PPTP (Point to Point Protocol) , L2F (Layer 2 Forwarding Protocol) et enfin L2TP (Layer 2 Tunneling Protocol).

- Les protocoles de niveau 3 comme IPSec ou MPLS.

→ **Openvpn** est une solution de **tunnelisation OpenSource**, il utilise la bibliothèque d'**OpenSSL**.

Il existe 2 configurations possibles d'OpenVPN suivant le type de réseau que l'on souhaite mettre en place et suivant le contexte réseau :

- VPN ponté (interface tap) (couche 2)
- VPN routé (interface tun). (au dessus de la couche 2)

→ La configuration VPN routé est plus performant et plus fiable que le ponté. Le VPN ponté est utilisé dans une architecture réseau local, alors que le VPN routé peut aussi bien être utilisé dans cette architecture que pour relier 2 réseaux à travers l'internet.

Installation Configuration d'OpenVPN

```
# apt -y install openvpn easy-rsa iptables
# cd /usr/share/easy-rsa
# ./easyrsa init-pki
# ./easyrsa build-ca   ( choisir un mot de passe. Puis un nom à votre serveur )
# ./easyrsa build-server-full server1 nopass (donner le mot de passe de l'atape précedente)
# ./easyrsa build-client-full client1 nopass
# ./easyrsa gen-dh  ( protocole de cryptographie utilisé dans les échanges de clés)
# openvpn --genkey secret ./pki/ta.key  (creation de la clé TLS-AUTH)
# cp -pR /usr/share/easy-rsa/pki/{issued,private,ca.crt,dh.pem,ta.key} /etc/openvpn/server/
# cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf /etc/openvpn/server/
```

Les fichiers clés

Nom de fichier	**Utile à**	**Utilité**	**Secret**
ca.crt	Serveur et tous les clients	Certificat racine CA	NON
ca.key	Clé signant la machine seulement	Clé racine CA	OUI
dh.pem	Serveur seulement	Paramètres Diffie Hellman	NON
server.crt	Serveur seulement	Certificat serveur	NON
server.key	Serveur seulement	Clé serveur	OUI
client1.crt	Client1 seulement	Certificat Client1	NON
client1.key	Client1 seulement	Clé Client1	OUI

```
# nano /etc/openvpn/server/server.conf  (modifier les lignes suivante si besoin) :
        port 1194
        proto udp
        dev tun
        ca ca.crt
        cert issued/server1.crt
        key private/server1.key
        dh dh.pem
        server 192.168.100.0 255.255.255.0
        push "route 192.168.1.0 255.255.255.0"
        keepalive 10 120
        tls-auth ta.key 0
        comp-lzo
        persist-key
        persist-tun
        verb 3
# nano /etc/openvpn/server/add-bridge.sh
        #!/bin/bash
        IF=enp1s0 (interface réseau local)
        VPNIF=tun0
```

```
        echo 1 > /proc/sys/net/ipv4/ip_forward
        iptables -A FORWARD -i ${VPNIF} -j ACCEPT
        iptables -t nat -A POSTROUTING -o ${IF} -j MASQUERADE
# nano /etc/openvpn/server/remove-bridge.sh
        #!/bin/bash
        IF=enp1s0
        VPNIF=tun0
        echo 0 > /proc/sys/net/ipv4/ip_forward
        iptables -D FORWARD -i  ${VPNIF} -j ACCEPT
        iptables -t nat -D POSTROUTING -o ${IF} -j MASQUERADE

# chmod 700 /etc/openvpn/server/{add-bridge.sh,remove-bridge.sh}
# nano /lib/systemd/system/openvpn-server@.service ( ajouter à la fin de la section [Service]) :
        ExecStartPost=/etc/openvpn/server/add-bridge.sh
        ExecStopPost=/etc/openvpn/server/remove-bridge.sh

# systemctl daemon-reload
# systemctl enable --now openvpn-server@server
# systemctl status openvpn-server@server ( doit afficher « Initialization Sequence Completed »)
```

Pour un client windows :

Mettre les fichiers generés dans le réportoire config qui se trouve à C:\Program Files\OpenVPN\sample-config] ou C:\Program Files\OpenVPN\config :

```
        ca.crt
        client1.crt
        client1.key
        ta.key
        client.ovpn
```

le contenu du fichier client.ovpn :

```
        client
        proto udp
        remote 172.16.2.1 1194
        resolv-retry infinite
        nobind
        persist-key
        persist-tun
        ca ca.crt
        cert client1.crt
        key client1.key
        tls-auth ta.key 1
        comp-lzo
        verb 3
```

Télécharger et installer OpenVPN GUI