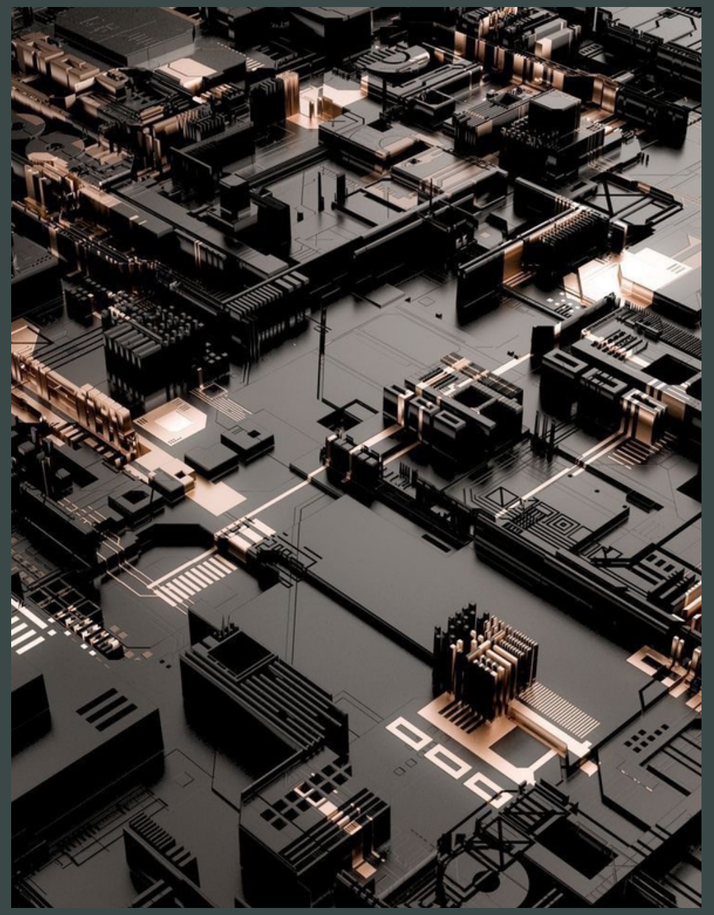
INFRASTRUCTURE & SYSTÈME D'INFORMATION

B2 INFORMATIQUE



CABEE PAULINE
VELAY YOHAN

26/05/2023

TOULOUSE YNOV CAMPUS

SOMMAIRE

TOULOUSE ynov CAMPUS

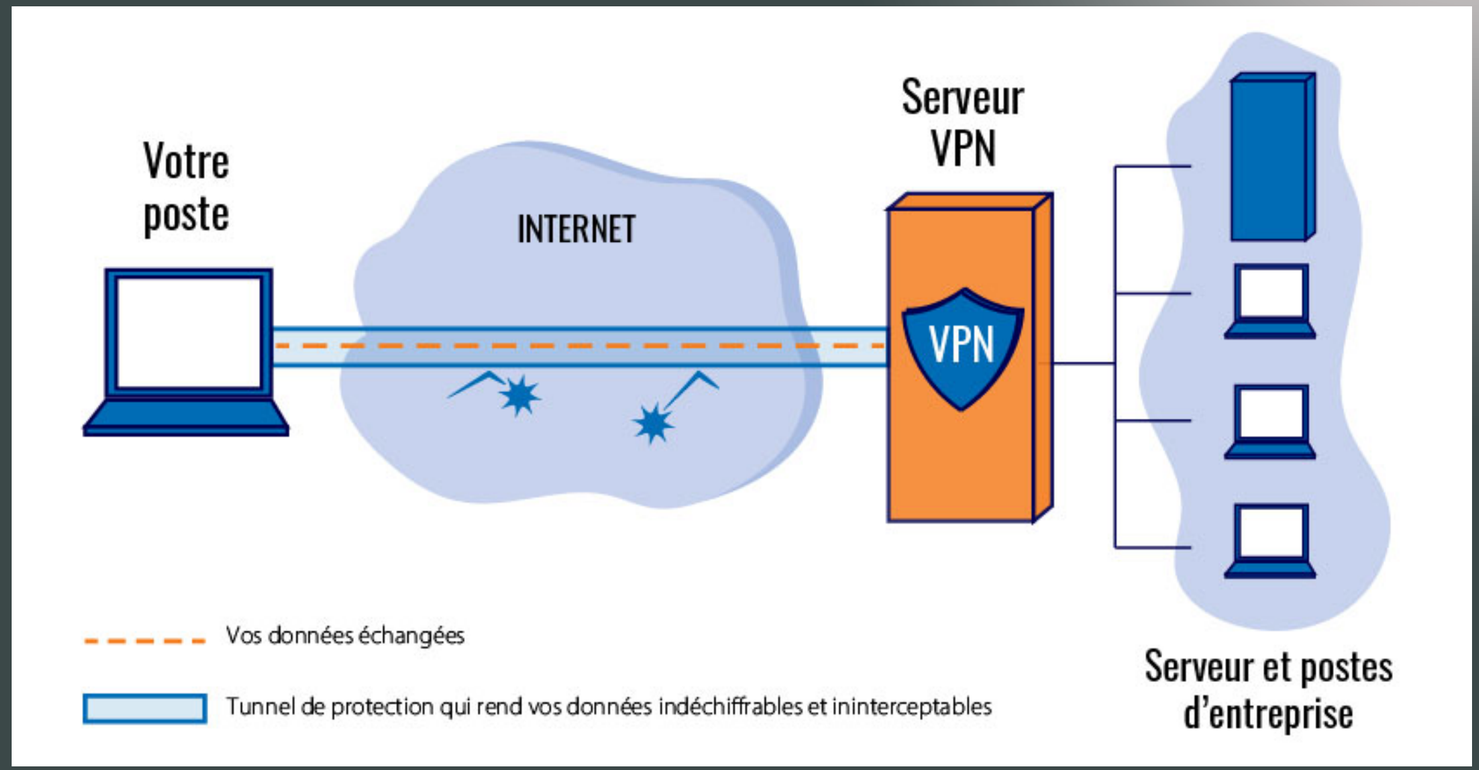
DÉFINITIONS GLOBALES

VPN

Serveur

IP Adress

Firewall

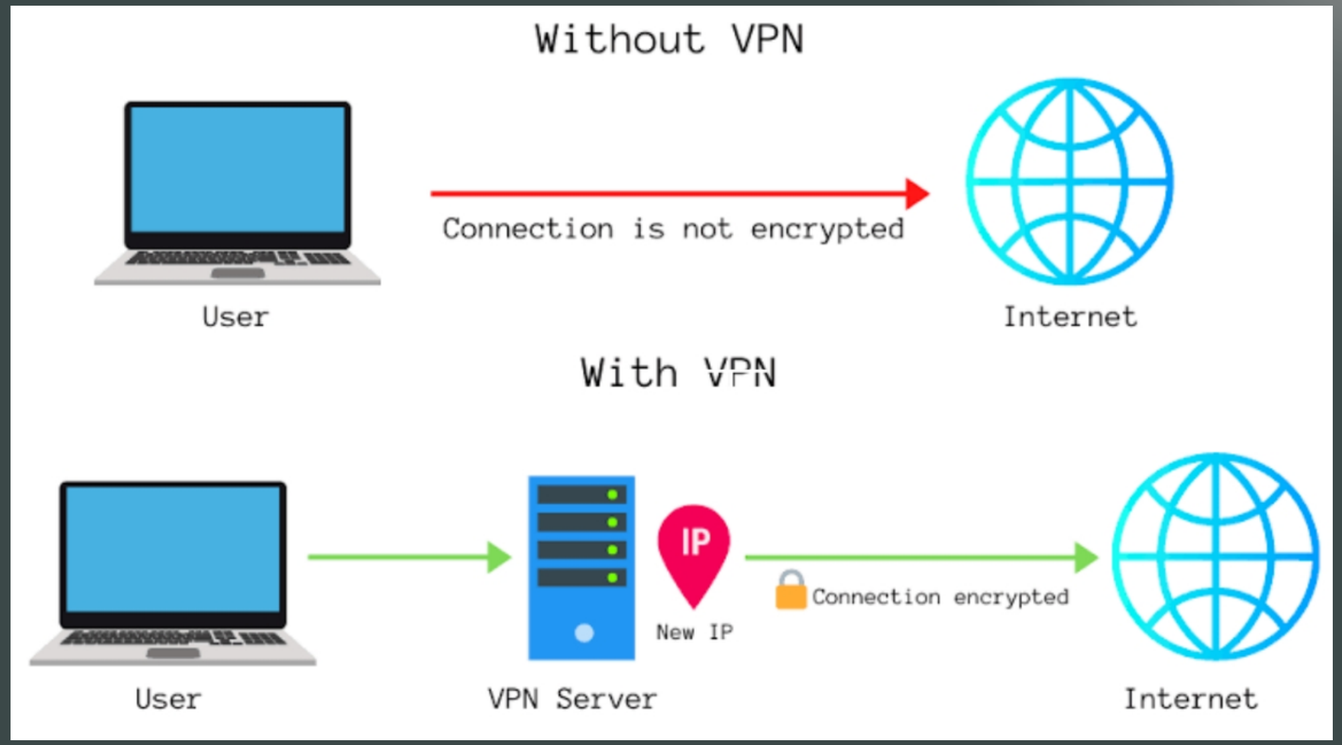


TOULOUSE ynov CAMPUS

OUTILS NÉCESSAIRE POUR LA MIS EN PLACE DES MODULES

OUTILS:

- SERVEUR
- POSTE CLIENT
- OPEN VPN



INTRODUCTION

PRÉREQUIS:

- SERVEUR CERTIFICAT
- SERVEUR OPENVPN
- (2E SERVEUR OPENVPN)
- MACHINE CLIENTE

SOLUTIONS À METTRE EN ŒUVRE :

- UN SERVEUR UBUNTU AVEC UN UTILISATEUR SUDO NON ROOT ET UN PARE-FEU ACTIVÉ.
- UN SERVEUR UBUNTU DISTINCT, ÉTABLI EN TANT QU'AUTORITÉ DE CERTIFICATION (AC) PRIVÉE, QUE NOUS APPELLERONS SERVEUR AC
- UN SERVEUR FACULTATIF UBUNTU POUR POUVOIR FAIRE LA REDONDANCE ET LOAD BALANCING
- UNE MACHINE CLIENTE QUE VOUS UTILISEREZ POUR VOUS CONNECTER À VOTRE SERVEUR OPENVPN.

TOULOUSE ynov CAMPUS

CADRE ET SCHÉMA

Tunnel VPN

Connexion chiffré

Redirection

Renvoie sur le port 1194

Client

Présent sur un réseau extérieur.

Pare-feu

Pare-feu du réseau auquel le VPN appartient.

Écoute sur les ports 65192 et 65193 (Permet de différencier les 2 serveurs VPN présent sur le réseau.)

Serveur VPN

Serveur dédié pour gérer les connexions VPNs et les redirections.

Écoute sur le ports 1194

Log toutes les connexions et les actions effectuer sur le réseau.

Protection des données

En passant par le VPN les données sont en premier lieux chiffré et le client utilise la paserelle du reseau du VPN.

Accès direct aux données

En passant par le VPN le client peut accéder au données présentes sur le réseau du VPN, comme des ressources, des applications ou autres.

TOULOUSE ynov CAMPUS

LES ETAPES

- **ETAPE 1:**
- INSTALLATION OPENVPN + EASY RSA
- CREATION D'UNE ICP POUR OPENVPN
- CREATION DEMANDE CERTIFICAT OPENVPN + CLÉ SECURITE
- FINALISATION DU CERTIFICAT

1

- **ETAPE 2:**
- CONFIGURATION MATERIEL OPENVPN
- GÉNÉRATION CERTIFICAT CLIENT+ PAIRE DE CLÉ
- CONFIGURER OPENVPN
  - REDIRECT GATEWAY
  - PORT ET PROTOCOLE
- CONFIGURATION RESEAU OPENVPN

2

- **ETAPE 3:**
- CONFIGURATION PARE FEU
- DEMARRER OPENVPN
- CRÉER INFRASTRUCTURE CLIENT
- GÉNÉRER CONFIGURATIONS CLIENT
- INSTALLATION

3

ETAPE 1 : DÉMONSTRATION

INSTALLATION OPENVPN + EASY RSA

1

```
$ sudo apt update
$ sudo apt install openvpn easy-rsa
$ mkdir ~/easy-rsa
$ ln -s /usr/share/easy-rsa/* ~/easy-rsa/
$ sudo chown serveur ~/easy-rsa
$ chmod 700 ~/easy-rsa
$ cd ~/easy-rsa
$ nano vars
```

CREATION D'UNE ICP POUR OPENVPN
CREATION DEMANDE CERTIFICAT OPENVPN + CLÉ SECURITE

2

```
(Modification de vars avec :

set_var EASYRSA_ALGO "ec"
set_var EASYRSA_DIGEST "sha512")

$ ./easyrsa init-pki
$ cd ~/easy-rsa
$ ./easyrsa gen-req server nopass
$ sudo cp /home/serveur/easy-rsa/pki/private/server.key /etc/openvpn/server/
```

FINALISATION DU CERTIFICAT

3

```
$ scp /home/serveur/easy-rsa/pki/reqs/server.req serveur@your_ca_server_ip:/tmp
(- On passe sur le serveur CA)
$ cd ~/easy-rsa
$ ./easyrsa import-req /tmp/server.req server
$ ./easyrsa sign-req server server
$ scp pki/issued/server.crt serveur@your_vpn_server_ip:/tmp
$ scp pki/ca.crt serveur@your_vpn_server_ip:/tmp
(- On passe sur le serveur openvpn)
$ sudo cp /tmp/{server.crt,ca.crt} /etc/openvpn/server
```

ETAPE 2: DÉMONSTRATION

CONFIGURATION MATERIEL OPENVPN 1

```
$ cd ~/easy-rsa
$ openvpn --genkey --secret ta.key
$ sudo cp ta.key /etc/openvpn/server
```

GÉNÉRATION CERTIFICAT CLIENT+ PAIRE DE CLÉ 2

```
$ mkdir -p ~/client-configs/keys
$ chmod -R 700 ~/client-configs
$ cd ~/easy-rsa
$ ./easyrsa gen-req client1 nopass
$ cp pki/private/client1.key ~/client-configs/keys/
$ scp pki/reqs/client1.req serveur@your_ca_server_ip:/tmp
(- On passe sur le serveur CA)
$ cd ~/easy-rsa
$ ./easyrsa import-req /tmp/client1.req client1
$./easyrsa sign-req client client1
$ scp pki/issued/client1.crt serveur@your_server_ip:/tmp
(- On passe sur le serveur openvpn)
$ cp /tmp/client1.crt ~/client-configs/keys/
$ cp ~/easy-rsa/ta.key ~/client-configs/keys/
$ sudo cp /etc/openvpn/server/ca.crt ~/client-configs/keys/
$ sudo chown serveur.serveur ~/client-configs/keys/*
```

CONFIGURER OPENVPN 3

```
$ sudo cp /usr/share/doc/openvpn/examples/sample-config-files/server.conf.gz/etc/openvpn/server/
$ sudo gunzip /etc/openvpn/server/server.conf.gz
$ sudo nano /etc/openvpn/server/server.conf
(Modification des clés de sécurté + auth SHA256 algo cryptage)
(Modification dns pour rediriger tout le trafic par le vpn)
(Ajuster le port et le protocole passage udp à tcp par exemple)
```

```
$ sudo nano /etc/sysctl.conf
$ sudo sysctl -p
```

TOULOUSE ynov CAMPUS

ETAPE 3: DÉMONSTRATION

CONFIGURATION PARE FEU 1

```
$ ip route list default
$ sudo nano /etc/ufw/before.rules
(modifier règles UFW)
$ sudo nano /etc/default/ufw
(modifier politique par défaut -drop à -accept)
$ sudo ufw allow 1194/udp
$ sudo ufw allow OpenSSH
$ sudo ufw disable
$ sudo ufw enable
```

DEMARRER OPENVPN
CRÉER INFRASTRUCTURE CLIENT 2

```
$ sudo systemctl -f enable openvpn-server@server.service
$ sudo systemctl start openvpn-server@server.service
$ sudo systemctl status openvpn-server@server.service
$ mkdir -p ~/client-configs/files
$ cp /usr/share/doc/openvpn/examples/sample-config-files/client.conf
$ nano ~/client-configs/base.conf
(modifier fichier base.conf)
$ nano ~/client-configs/make_config.sh
(ajouter un script à ce fichier)
$ chmod 700 ~/client-configs/make_config.sh
```

GÉNÉRER CONFIGURATIONS CLIENT
INSTALLATION

3

```
$ cd ~/client-configs
$ ./make_config.sh client1
$ ls ~/client-configs/files
(Installation poste client + connexion)
$ sudo openvpn --config client1.ovpn
```

TOULOUSE ynov CAMPUS

LA SÉCURITÉ

- Changement des ports exposés à internet (65192 et 65193)
- Connexion à l'aide d'un certificat client + mot de passe
- Logging des connexions/déconnexions de chaque client
- Loadbalancing & Failover à l'aide de 2 serveurs VPN
- Attribution d'IP fixe à chaque client

PROBLÈMES RENCONTRÉS

- Serveurs à distance
- Pas de DNS (IP public exposé)

DÉMONSTRATION DE NOTRE VPN

CONCLUSION

POUR CONCLURE, NOUS AVONS EXPLORÉ LES NOTIONS DE BASE DES RÉSEAUX PRIVÉS VIRTUELS (VPN) ET LEUR UTILITÉ DANS LE CONTEXTE ACTUEL, EN METTANT L'ACCENT SUR LES PRINCIPES DE CRYPTOGRAPHIE ET DE CHIFFREMENT QUI SOUS-TENDENT LE FONCTIONNEMENT D'OPENVPN.

LES PROBLEMES QUE VOUS POURRIEZ RENCONTRER SONT FACILEMENT EVITABLES GRACE AU SUIVI PRECIS DE NOTRE DOCUMENT.

TOULOUSE ynov CAMPUS

MERCI POUR VOTRE ÉCOUTE

DES QUESTIONS

TOULOUSE ynov CAMPUS