CONFIGURATION D'UN SERVEUR ET D'UN CLIENT OPENVPN SOUS LINUX

(KALI LINUX COMME SERVEUR ET UBUNTU COMME CLIENT)

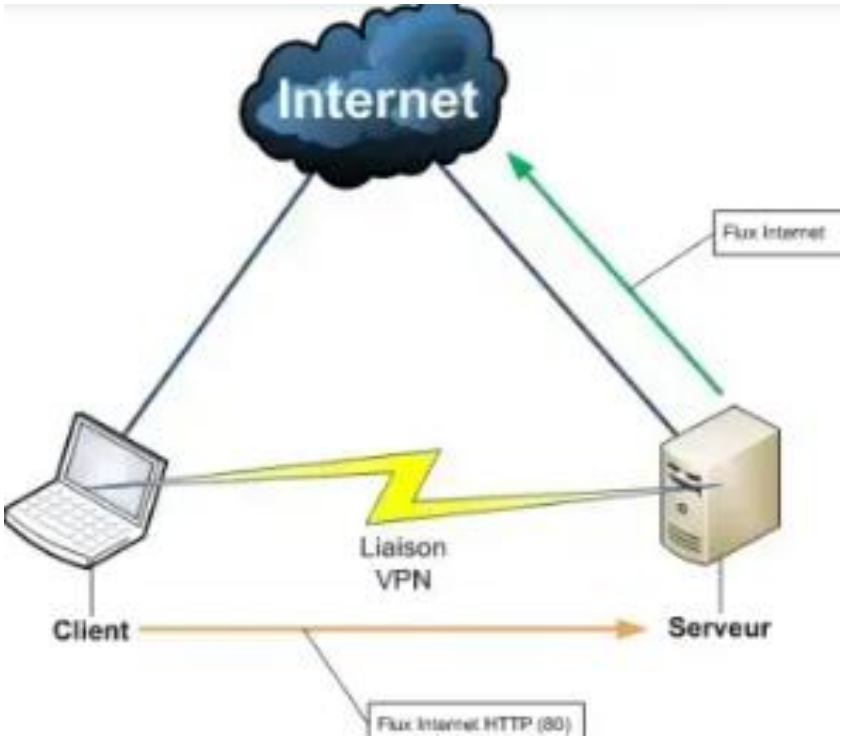
VPN 1

Projet VPN : Client / Serveur sur Linux :

ENET'COM
المدرسة الوطنية للإلكترونيك و الإتصالات بصفاقس
ECOLE NATIONALE D'ELECTRONIQUE ET DES TÉLÉCOMMUNICATIONS DE SFAX

Crée Par :

- Seifeddine EL Abed
- Aymen Gharbi
- Oussema Ben Ahmed



Plan

Introduction sur les VPN

Installation et configuration du serveur

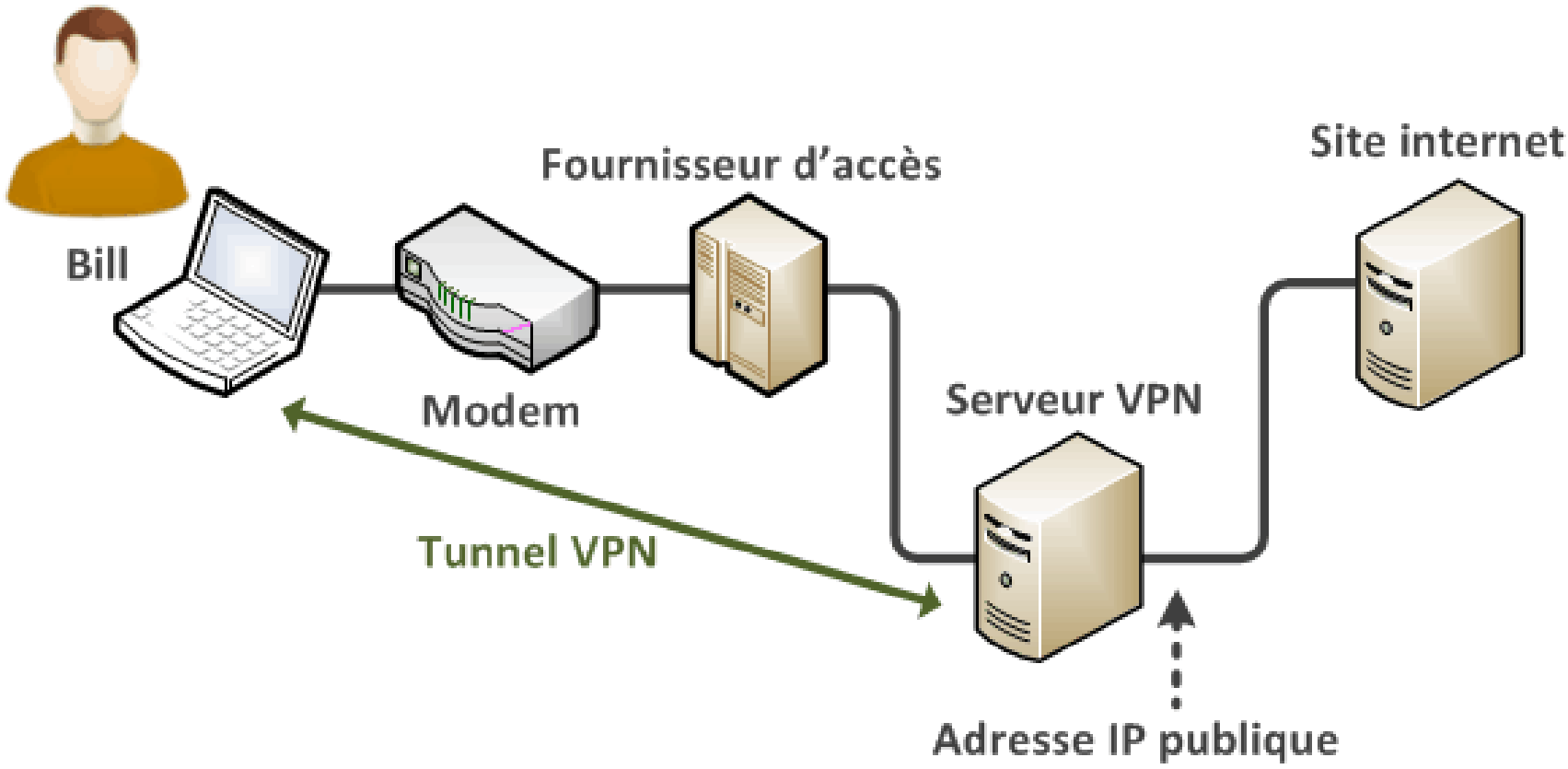
Envoi des certificats du serveur au client

Test du réseau

Conclusion

C'est quoi un VPN:

- Un VPN (réseau privé virtuel) est un service qui crée une connexion sécurisée
- Il chiffre votre connexion internet et masque votre adresse IP.
- Il permet de naviguer anonymement et d'accéder à des contenus géo-bloqués.
- Il sécurise les données échangées, notamment sur des réseaux publics.


Bill
Modem
Fournisseur d'accès
Site internet
Serveur VPN
Tunnel VPN
Adresse IP publique

Installation Serveur

- **Installation des paquets OpenVPN et Easy-RSA**
- **Commandes : sudo apt install openvpn easy-rsa**

➢ **Exécutez sudo apt install openvpn easy-rsa pour installer OpenVPN et Easy-RSA.**

```
┌──(kali㉿kali)-[~]
└─$ sudo apt install openvpn easy-rsa
Installing:
  easy-rsa  openvpn
```

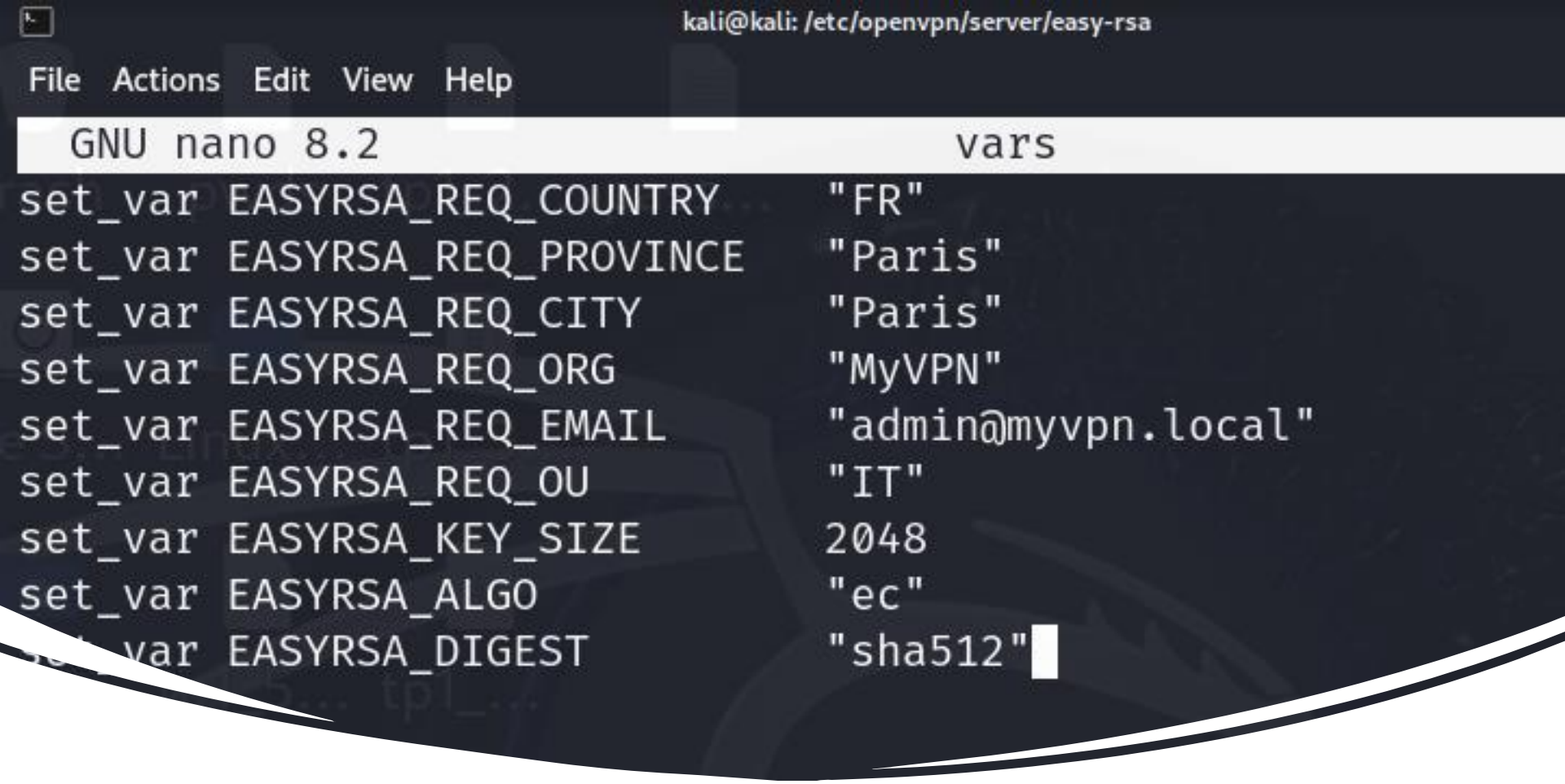
- **Vérification des interfaces réseau du serveur**
- **Commande : ifconfig**

➢ **Utilisez ifconfig pour identifier l'IP locale (ici 192.168.141.131) et assurer la connectivité réseau.**

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.141.131  netmask 255.255.255.0  broadcast
192.168.141.255
```

Création et configuration de l'environnement OpenVPN avec Easy-RSA

1. **Création du répertoire OpenVPN : sudo mkdir -p /etc/openvpn/server.**
2. **Copie des scripts Easy-RSA : sudo cp -r /usr/share/easy-rsa/ /etc/openvpn/server/.**
3. **Édition du fichier vars : sudo nano /etc/openvpn/server/easy-rsa/vars.**



Contenu du fichier vars

- Paramètres par défaut (pays: FR, ville: Paris, organisation: MyVPN).
- **Algorithmes :** ec (elliptic curve) et sha512 pour une sécurité renforcée.

Génération des Certificats

- **Init PKI:** Initialisez la PKI avec **sudo ./easyrsa init-pki** pour créer l'infrastructure clé.

```
┌──(kali㉿kali)-[/etc/openvpn/server/easy-rsa]
└─$ sudo ./easyrsa init-pki
Using Easy-RSA 'vars' configuration:
* /etc/openvpn/server/easy-rsa/vars
```

```
Notice
------

'init-pki' complete; you may now create a CA or requests.

Your newly created PKI dir is:
* /etc/openvpn/server/easy-rsa/pki

Using Easy-RSA configuration:
* /etc/openvpn/server/easy-rsa/vars
```

Génération des Certificats

- **Création de la CA :** Bâtissez l'Autorité de Certification (CA) via **./easyrsa build-ca nopass**, nommée "MyVPN-server".

```
┌──(kali㉿kali)-[/etc/openvpn/server/easy-rsa]
└─$ ./easyrsa build-ca nopass
```

```
Notice
------

CA creation complete. Your new CA certificate is at:
* /etc/openvpn/server/easy-rsa/pki/ca.crt

Create an OpenVPN TLS-AUTH|TLS-CRYPT-V1 key now: See 'help gen-tls'

Build-ca completed successfully.
```

Génération des Certificats

- Génèrer la requête de certificat du serveur VPN ainsi que sa clé privée, en utilisant 'MyVPN-CA' comme nom commun (CN) avec **sudo ./easyrsa gen-req server nopass.**

```
┌──(kali㉿kali)-[/etc/openvpn/server/easy-rsa]
└─$ sudo ./easyrsa gen-req server nopass
```

```
Notice
------

Private-Key and Public-Certificate-Request files created.
Your files are:
* req: /etc/openvpn/server/easy-rsa/pki/reqs/server.req
* key: /etc/openvpn/server/easy-rsa/pki/private/server.key
```

Génération des Certificats

- Signer le certificat du serveur avec l'autorité de certification (CA) en utilisant **`sudo ./easyrsa sign-req`** `server server`, générant un fichier `server.crt` valide pendant 825 jours.

```
┌──(kali㉿kali)-[/etc/openvpn/server/easy-rsa]
└─$ sudo ./easyrsa sign-req server server
```

```
Notice
------
Inline file created:
* /etc/openvpn/server/easy-rsa/pki/inline/private/server.inline


Notice
------
Certificate created at:
* /etc/openvpn/server/easy-rsa/pki/issued/server.crt
```

Génération des Certificats

- Générer la clé TLS-auth pour protéger le serveur VPN contre les attaques DDoS, en utilisant la commande sudo openvpn **--genkey secret ta.key.**

```
┌──(kali㉿kali)-[/etc/openvpn/server/easy-rsa]
└─$ sudo openvpn --genkey secret ta.key
```

Génération des Certificats

- Générer les paramètres Diffie-Hellman avec la commande **`./easyrsa gen-dh`** pour obtenir une clé de 2048 bits assurant une sécurité standard.

```
┌──(kali㉿kali)-[/etc/openvpn/server/easy-rsa]
└─$ ./easyrsa gen-dh
Using Easy-RSA 'vars' configuration:
* /etc/openvpn/server/easy-rsa/vars
Generating DH parameters, 2048 bit long safe prime
.....................................................................................
```

Configuration du Serveur OpenVPN

```
┌──(kali㉿kali)-[/etc/openvpn/server/easy-rsa]
└─$ sudo nano /etc/openvpn/server/server.conf
```

Paramètre	Valeur
Commande	sudo nano /etc/openvpn/server/server.conf
Port/Protocole	1194 / UDP
Certificats	ca.crt, server.crt, server.key, dh.pem
Réseau VPN	10.8.0.0/24
Routes	Push 192.168.141.0/24 et 10.8.0.0/24
DNS	8.8.8.8 (Google DNS)
Chiffrement	AES-256-GCM + SHA256

- **Édition du fichier de configuration `server.conf`.**

```
 GNU nano 8.2                    /etc/openvpn/server/server.conf *
port 1194
proto udp
dev tun
ca /etc/openvpn/server/easy-rsa/pki/ca.crt
cert /etc/openvpn/server/easy-rsa/pki/issued/server.crt
key /etc/openvpn/server/easy-rsa/pki/private/server.key
dh /etc/openvpn/server/easy-rsa/pki/dh.pem
server 10.8.0.0 255.255.255.0
push "route 192.168.141.0 255.255.255.0"  # addresse sous-réseau local
push "route 10.8.0.0 255.255.255.0" # sous reseau vpn
push "dhcp-option DNS 8.8.8.8"
keepalive 10 120
tls-auth /etc/openvpn/server/easy-rsa/ta.key 0
cipher AES-256-GCM
auth SHA256
persist-key
persist-tun
status /var/log/openvpn/openvpn-status.log
verb 3
```

Activation Routage & Démarrage Serveur

- **Activation du routage IP** :
- **Commande :** sudo sed -i 's/#net.ipv4.ip_forward=1/net.ipv4.ip_forward=1/' /etc/sysctl.conf
- **Application des changements :** `sudo sysctl -p`

- **Démarrage du service OpenVPN** :
- **Commande :** `sudo systemctl start openvpn-server@server`
- **Activation automatique au démarrage :** `sudo systemctl enable openvpn-server@server`

Envoi des fichiers de certification et de configuration du serveur au client

Commande : scp [fichier] nom_client@IP_client:path

```
┌──(kali㉿kali)-[/etc/openvpn/server/easy-rsa]
└─$ scp /etc/openvpn/server/easy-rsa/pki/{ca.crt,issued/server.crt,private/server.key,
ta.key} ubuntu@192.168.141.130:~/vpn_files/
ubuntu@192.168.141.130's password:
ca.crt                                        100%  753   467.9KB/s   00:00
server.crt                                    100% 2838     3.0MB/s   00:00
server.key                                    100%  306   364.1KB/s   00:00
scp: stat local "/etc/openvpn/server/easy-rsa/pki/ta.key": No such file or directory
```

```
┌──(kali㉿kali)-[/etc/openvpn/server/easy-rsa]
└─$ sudo scp /etc/openvpn/server/easy-rsa/ta.key ubuntu@192.168.141.130:~/vpn_files/
The authenticity of host '192.168.141.130 (192.168.141.130)' can't be established.
ED25519 key fingerprint is SHA256:xILfXpD1JMe/3kGPgcsOvGbn2E8BOM8wCSxpFo7YaDU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.141.130' (ED25519) to the list of known hosts.
ubuntu@192.168.141.130's password:
ta.key                                        100%  636   603.0KB/s   00:00
```

Installation Serveur

- **Installation des paquets OpenVPN**
- **Commandes : sudo apt install openvpn**

➢ **Exécutez sudo apt install openvpn pour installer OpenVPN sur Ubuntu.**

```
ubuntu@ubuntu:~$ sudo apt install openvpn
Lecture des listes de paquets... Fait
Construction de l'arbre des dépendances
Lecture des informations d'état... Fait
openvpn est déjà la version la plus récente (2.4.12-0ubuntu0.20.04.2).
openvpn passé en « installé manuellement ».
0 mis à jour, 0 nouvellement installés, 0 à enlever et 154 non mis à jour.
```

- **Installation des paquets OpenSSH**
- **Commandes : sudo apt install openssh**

```
ubuntu@ubuntu:~$ sudo apt install openssh-server
Lecture des listes de paquets... Fait
```

- **Copie des fichiers envoyés par le serveur**

```
ubuntu@ubuntu:~$ sudo cp vpn_files/* /etc/openvpn/client/
```

Configuration du Client

- **Creation du fichier de configuration**
- **Commandes : sudo nano /etc/openvpn/client/client.conf**
- **Paramètres : protocol udp, IP serveur, certificats, chiffrement**

```
ubuntu@ubuntu:~$ sudo nano /etc/openvpn/client/client.conf
```

```
  GNU nano 4.8                /etc/openvpn/client/client.conf
client
dev tun
proto udp
remote 192.168.141.131 1194  # l'IP du serveur Kali
resolv-retry infinite
nobind
persist-key
persist-tun
remote-cert-tls server
c Aide crt
cert client1.crt
key client1.key
tls-auth ta.key 1
cipher AES-256-GCM
auth SHA256
verb 3
```

Paramètres du Pare-feu

- Permission du port et de l'addresse du réseau vpn
- Commandes : sudo ufw allow 1194/udp
  sudo ufw allow from 10.8.0.0/24

```
ubuntu@ubuntu:~$ sudo ufw allow 1194/udp
Les règles ont été mises à jour
Les règles ont été mises à jour (IPv6)
ubuntu@ubuntu:~$ sudo ufw allow from 10.8.0.0/24
Les règles ont été mises à jour
```

Démarrage OpenVPN Client

- Démarrage et activation du client pour l'établissement du réseau
- Commandes : sudo systemctl start openvpn-client@client
  sudo systemctl enable openvpn-client@client

```
ubuntu@ubuntu:~$ sudo systemctl start openvpn-client@client
ubuntu@ubuntu:~$ sudo systemctl enable openvpn-client@client
Created symlink /etc/systemd/system/multi-user.target.wants/openvpn-client@client.service → /lib/sy
stemd/system/openvpn-client@.service.
```

Vérification des Logs

- Consultation du fichier status.log pour vérifier l'établissement du réseau
- Commandes : sudo tail -f /var/log/openvpn/openvpn-status.log
- Observation : État des connexions VPN

```
┌──(kali㉿kali)-[/etc/openvpn/server/easy-rsa]
└─$ sudo tail -f /var/log/openvpn/openvpn-status.log
TITLE,OpenVPN 2.6.14 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11]
[MH/PKTINFO] [AEAD] [DCO]
TIME,2025-04-20 16:34:20,1745181260
HEADER,CLIENT_LIST,Common Name,Real Address,Virtual Address,Virtual IPv6 Address,Bytes
 Received,Bytes Sent,Connected Since,Connected Since (time_t),Username,Client ID,Peer
ID,Data Channel Cipher
HEADER,ROUTING_TABLE,Virtual Address,Common Name,Real Address,Last Ref,Last Ref (time_
t)
GLOBAL_STATS,Max bcast/mcast queue length,0
GLOBAL_STATS,dco_enabled,0
END
```

Démarrage du réseau VPN

- Commandes : - Serveur : sudo tcpdump -i eth0 udp port 1194 -vv
  - Client : sudo tcpdump -i ens33 udp port 1194 -vv

```
ubuntu@ubuntu:~$ sudo tcpdump -i ens33 udp port 1194 -vv
tcpdump: listening on ens33, link-type EN10MB (Ethernet), capture size 262144 b
ytes
15:08:14.393791 IP (tos 0x0, ttl 64, id 22164, offset 0, flags [DF], proto UDP
(17), length 70)
    ubuntu.39822 > 192.168.141.131.openvpn: [bad udp cksum 0x9c9a -> 0x3155!] U
DP, length 42
15:08:16.626205 IP (tos 0x0, ttl 64, id 22588, offset 0, flags [DF], proto UDP
(17), length 70)
    ubuntu.39822 > 192.168.141.131.openvpn: [bad udp cksum 0x9c9a -> 0x5cb5!] U
DP, length 42
15:08:21.088036 IP (tos 0x0, ttl 64, id 22625, offset 0, flags [DF], proto UDP
(17), length 70)
    ubuntu.39822 > 192.168.141.131.openvpn: [bad udp cksum 0x9c9a -> 0x14f7!] U
DP, length 42
15:08:29.272020 IP (tos 0x0, ttl 64, id 22944, offset 0, flags [DF], proto UDP
(17), length 70)
    ubuntu.39822 > 192.168.141.131.openvpn: [bad udp cksum 0x9c9a -> 0x2b46!] U
DP, length 42
^C
4 packets captured
4 packets received by filter
0 packets dropped by kernel
```

```
┌──(kali㉿kali)-[/etc/…/server/easy-rsa/pki/private]
└─$ sudo tcpdump -i eth0 udp port 1194 -vv
tcpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
18:08:14.255597 IP (tos 0×0, ttl 64, id 22164, offset 0, flags [DF], proto UDP (17),
ength 70)
    192.168.141.130.39822 > 192.168.141.131.openvpn: [udp sum ok] UDP, length 42
18:08:16.492229 IP (tos 0×0, ttl 64, id 22588, offset 0, flags [DF], proto UDP (17),
ength 70)
    192.168.141.130.39822 > 192.168.141.131.openvpn: [udp sum ok] UDP, length 42
18:08:20.963232 IP (tos 0×0, ttl 64, id 22625, offset 0, flags [DF], proto UDP (17),
ength 70)
    192.168.141.130.39822 > 192.168.141.131.openvpn: [udp sum ok] UDP, length 42
18:08:29.160405 IP (tos 0×0, ttl 64, id 22944, offset 0, flags [DF], proto UDP (17),
ength 70)
    192.168.141.130.39822 > 192.168.141.131.openvpn: [udp sum ok] UDP, length 42
18:08:45.171734 IP (tos 0×0, ttl 64, id 23102, offset 0, flags [DF], proto UDP (17),
ength 70)
    192.168.141.130.39822 > 192.168.141.131.openvpn: [udp sum ok] UDP, length 42
^C
5 packets captured
5 packets received by filter
0 packets dropped by kernel
```

Conclusion

- Un VPN comme OpenVPN est essentiel pour sécuriser vos communications, protéger vos données sensibles et garantir l'accès distant à vos ressources en toute confidentialité. Que ce soit pour un usage professionnel ou personnel, sa configuration rigoureuse (chiffrement fort, gestion des certificats et monitoring) en fait un outil incontournable contre les cybermenaces. Adoptez-le pour naviguer et travailler en toute sérénité !

Merci pour votre Attention