



Virtual Private Network VPN

Encadré par:

- Prof Moukhafi Mehdi

Réalisé par:

- Ajidad Nouhayla
- El abbioui Khadija
- Ramli Manare

**Introduction au
réseau informatique 01**

04 Petites Notions

Les Modèles réseaux 02

05 Installation

Cryptage 03

06 Wireshark

01

INTRODUCTION AU RESEAU INFORMATIQUE

• Definition:

Un réseau informatique est un système de communication qui permet aux appareils de se connecter, de partager des ressources et de communiquer entre eux. Cela facilite le partage de données et la collaboration entre les utilisateurs.

Histoire :

- **1960** : Création d'Arpanet,
- **1970** : Arpanet s'étend et relie de plus en plus d'institutions académiques et de centres de recherche.
- **1980** : Développement et adoption des protocoles TCP/IP
- **1990** : L'Internet devient accessible au grand public avec l'arrivée des fournisseurs d'accès Internet à domicile
- **2000** : L'expansion d'Internet se poursuit avec l'émergence des réseaux sociaux et des services en ligne.
- **2010** : Les réseaux sans fil et la connectivité mobile se développent, permettant un accès Internet plus pratique et nomade.
- **2020** : Les réseaux informatiques continuent de se développer et d'évoluer, avec une utilisation croissante de l'Internet des objets.

02

Les Modèles Réseaux

● Histoire :

Modèle OSI :

- 1970 : L'ISO (Organisation internationale de normalisation) développe le modèle OSI (Open Systems Interconnection)
- 1984 : Publication du modèle OSI. Ce modèle comprend 7 couches.

Modèle TCP/IP :

- 1970 : Le modèle TCP/IP (Transmission Control Protocol/Internet Protocol) est développé par le Département de la Défense des États-Unis Arpanet.
- 1980 : Le modèle TCP/IP devient la norme de facto pour les communications sur Internet. Il comprend 4 couches.

Modèle OSI

vs

Modèle TCP/IP

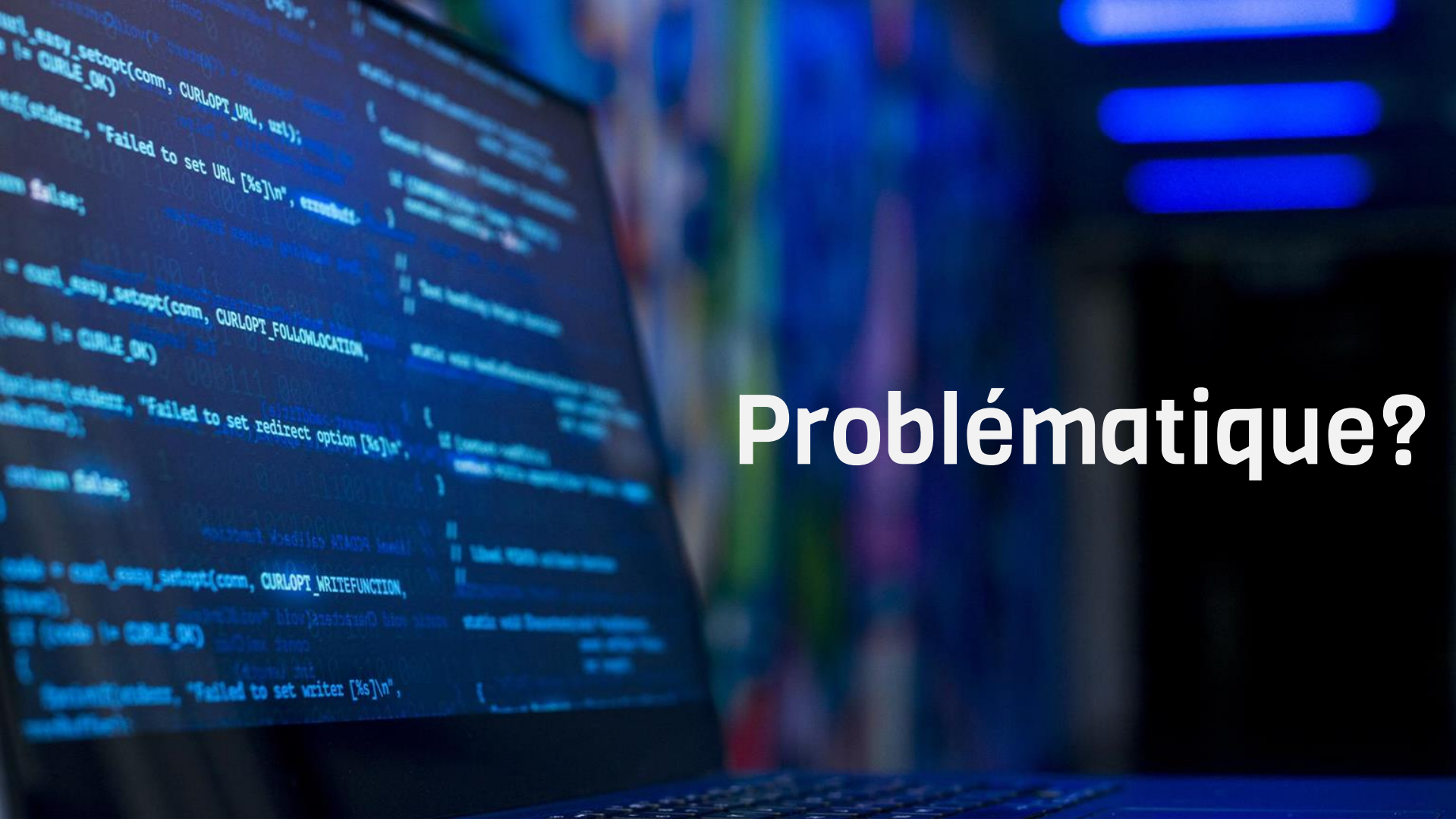
Application	HTTP, SMTP,DNS, FTP	Application
Présentation	SSL	
Session	Control sessions between applications	
Transport	TCP , UDP	Transport
Réseau	ICMP,IP,IPsec,IPv4,IPv6	Internet
Liaison de données	Adress MAC,Ethernet	Accès réseau
Physique	Rj45, Fibre,Hubs	

TCP

VS

UDP

TCP	UDP
Protocole orienté connexion .	Protocole sans connexion.
Garantit la livraison des données dans l'ordre correct.	Aucune garantie de livraison des données.
Utilisé pour les applications qui nécessitent une transmission fiable des données.	Utilisé pour les applications où la vitesse est primordiale.
Mécanismes de retransmission	Aucun mécanisme de retransmission



Problématique?

VPN

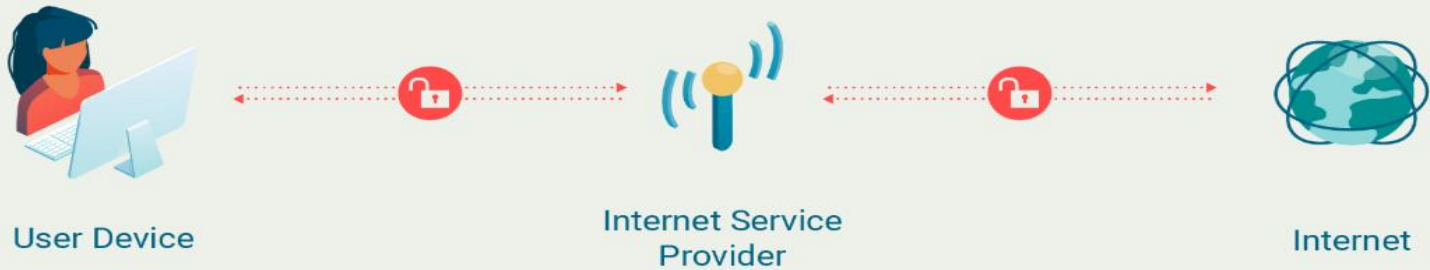
Les **VPN**, ou réseaux privés virtuels, sont des outils qui permettent de *sécuriser* et de *protéger* votre connexion Internet, renforcent votre confidentialité et vous permettent de contourner les restrictions géographiques.

Lorsque vous utilisez un VPN, tout votre trafic Internet est acheminé à travers un serveur distant, ce qui *masque* votre adresse IP réelle et *chiffre* vos données.

VPN



No VPN



Où ?

Au niveau de la couche :

Application

Présentation

Session

Transport

Réseau

**Liaison
/Physique**

Types :

Host to LAN

- **Accès distant** d'un hôte au LAN distant via internet (Host to LAN)



Types :

LAN to LAN

- Connexion entre plusieurs LANs distant via Internet (LAN to LAN)



Avantages

- Ils renforcent votre confidentialité en masquant votre adresse IP et en rendant vos activités en ligne plus difficiles à tracer.
- Ils sécurisent vos données en les chiffrant, ce qui les rend illisibles pour les personnes malveillantes qui pourraient tenter de les intercepter.
- Ils sont également utilisés pour contourner les restrictions géographiques.

Inconvénients:

Ralentissement de la
vitesse de connexion

Coût supplémentaire

Compatibilité limitée

Risques potentiels pour la
sécurité

03

Cryptage

Types:

Chiffrement Asymétrique	Chiffrement Symétrique
Paire de clés(Publique et privée)	Cle unique partagée
Clé publique pour chiffrer	Cle unique pour chiffrer
Clé publique pour déchiffrer	Cle unique pour déchiffrer
Communication sécurisée sans partage de clé	Partage de la meme clé secrete
Plus lent	Plus rapide
Utilisé pour sécuriser les échanges de données sensibles	Utilisé pour des communication rapides et securisées
<ul style="list-style-type: none">• RSA• DSA• ...	<ul style="list-style-type: none">• RC4• AES•

• Algorithme RSA :

RSA (*Rivest-Shamir-Adleman*) RSA est utilisé dans divers protocoles de sécurité, y compris dans la sécurisation des communications Internet (par exemple, dans SSL/TLS pour sécuriser les connexions HTTPS), la signature numérique, et l'échange sécurisé de clés.

• Protocole SSL :

Le protocole **SSL** (*Secure Sockets Layer*) est généralement considéré comme faisant partie de la couche de présentation du modèle OSI. Cet protocole est utilisé pour sécuriser les communications sur Internet en fournissant un chiffrement des données et une authentification des parties impliquées dans la communication.

04

Petites notions

Encapsulation / Désencapsulation:

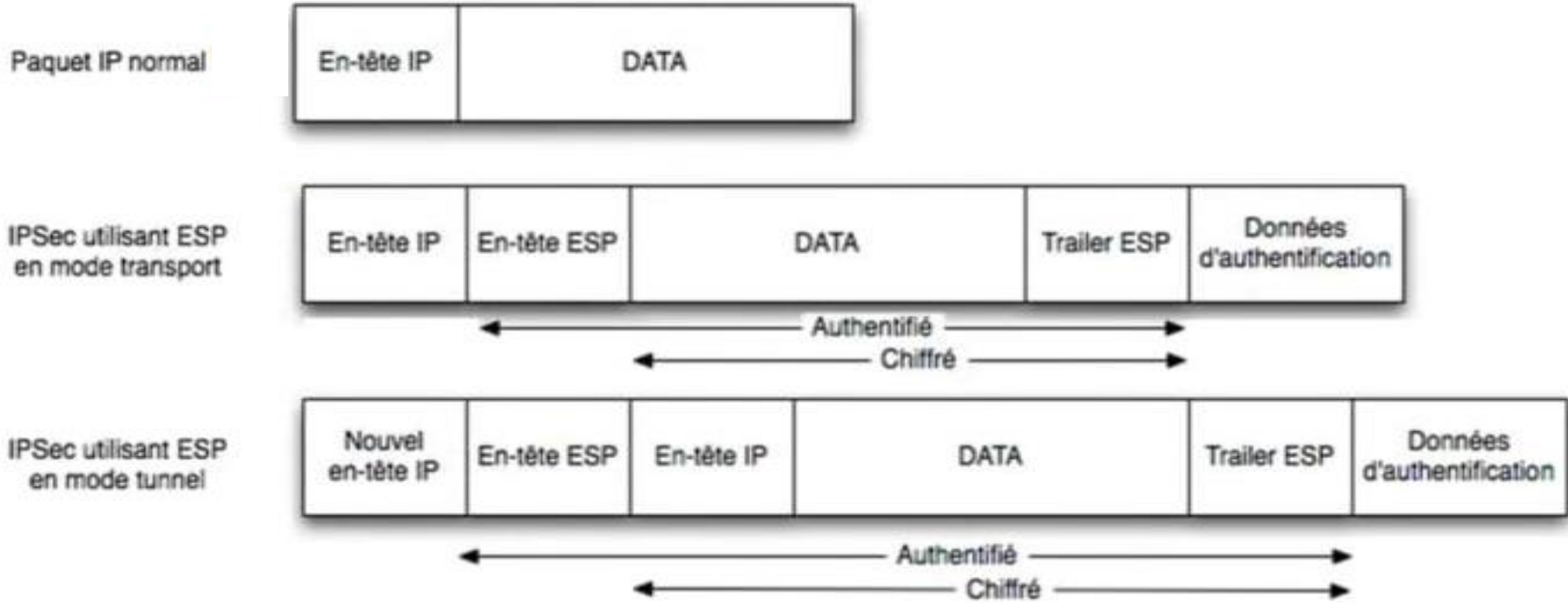


IP security:

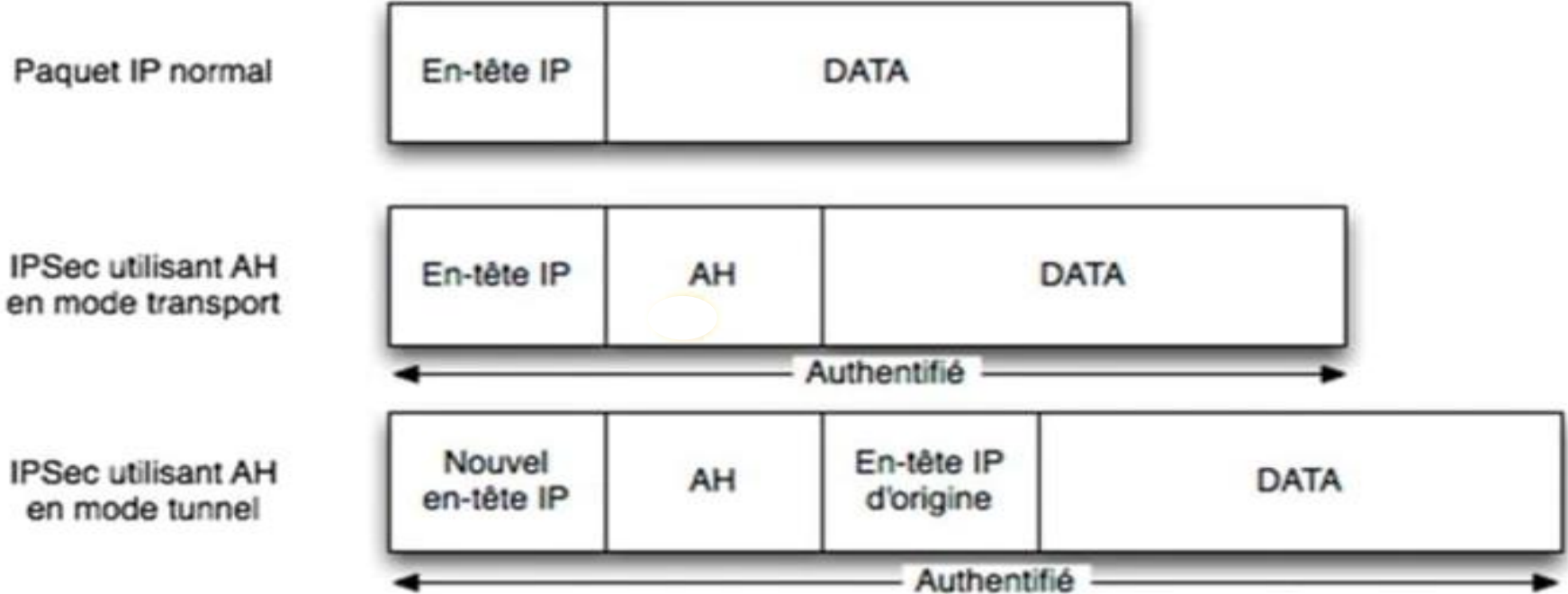
IPsec (Internet Protocol Security) est un ensemble de protocoles utilisés pour sécuriser les communications sur les réseaux IP, offrant des fonctionnalités de confidentialité, d'intégrité et d'authentification des données.

Il est utilisé dans le VPN pour encapsuler et protéger les données qui sont transmises à travers le tunnel VPN.

Le protocole ESP



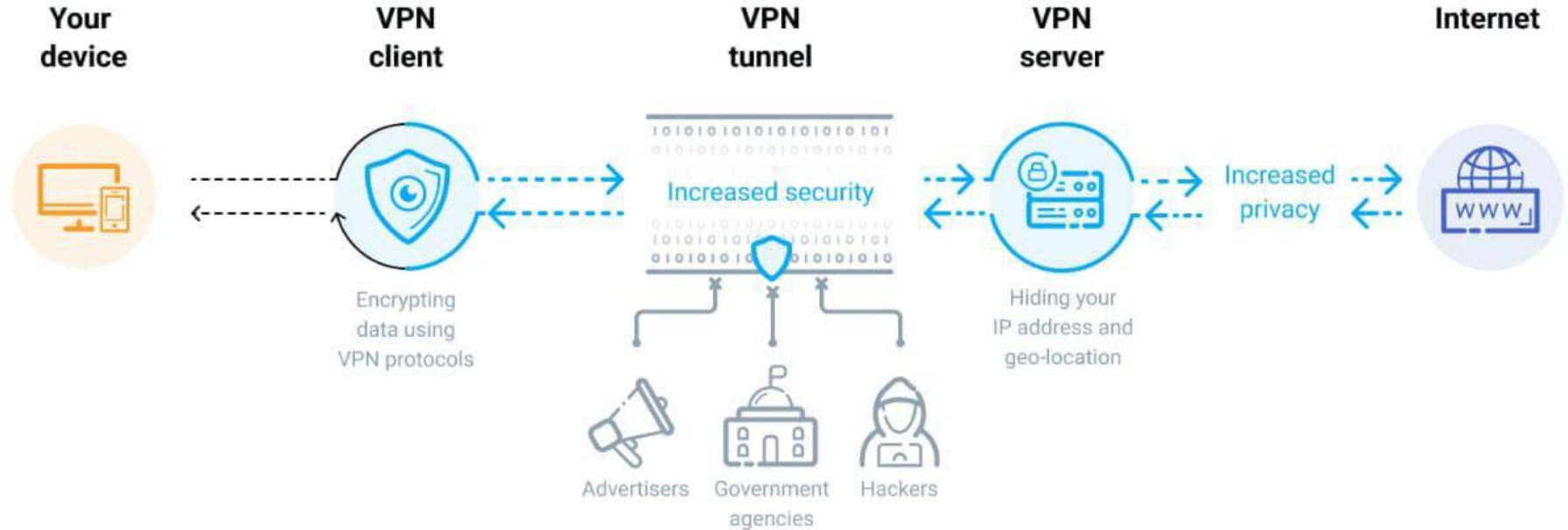
Le protocole AH



Adresse MAC:

L'adresse MAC, ou Media Access Control, est un identifiant unique attribué à chaque périphérique réseau. Il s'agit d'une combinaison de chiffres et de lettres qui permet d'identifier de manière unique un appareil sur un réseau local.

Principe du tunnelisation :



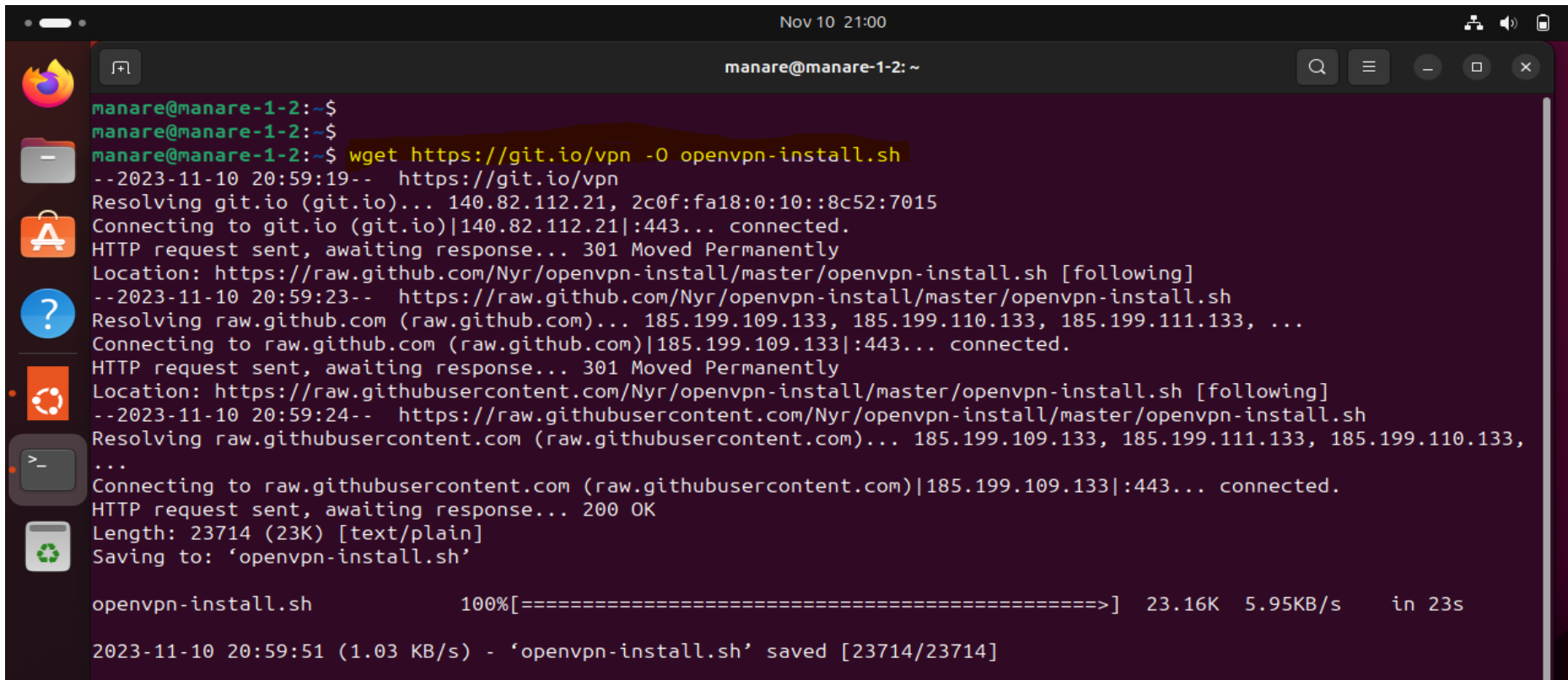
05

Installation

OpenVPN:

Un OpenVPN est un logiciel open source qui permet de créer un réseau privé virtuel (VPN) sécurisé.

Installation:



```
manare@manare-1-2: ~  
manare@manare-1-2:~$  
manare@manare-1-2:~$ wget https://git.io/vpn -O openvpn-install.sh  
--2023-11-10 20:59:19-- https://git.io/vpn  
Resolving git.io (git.io)... 140.82.112.21, 2c0f:fa18:0:10::8c52:7015  
Connecting to git.io (git.io)|140.82.112.21|:443... connected.  
HTTP request sent, awaiting response... 301 Moved Permanently  
Location: https://raw.githubusercontent.com/Nyr/openvpn-install/master/openvpn-install.sh [following]  
--2023-11-10 20:59:23-- https://raw.githubusercontent.com/Nyr/openvpn-install/master/openvpn-install.sh  
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.109.133, 185.199.110.133, 185.199.111.133, ...  
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.109.133|:443... connected.  
HTTP request sent, awaiting response... 301 Moved Permanently  
Location: https://raw.githubusercontent.com/Nyr/openvpn-install/master/openvpn-install.sh [following]  
--2023-11-10 20:59:24-- https://raw.githubusercontent.com/Nyr/openvpn-install/master/openvpn-install.sh  
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.109.133, 185.199.111.133, 185.199.110.133, ...  
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.109.133|:443... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 23714 (23K) [text/plain]  
Saving to: 'openvpn-install.sh'  
  
openvpn-install.sh      100%[=====>]  23.16K  5.95KB/s  in 23s  
  
2023-11-10 20:59:51 (1.03 KB/s) - 'openvpn-install.sh' saved [23714/23714]
```

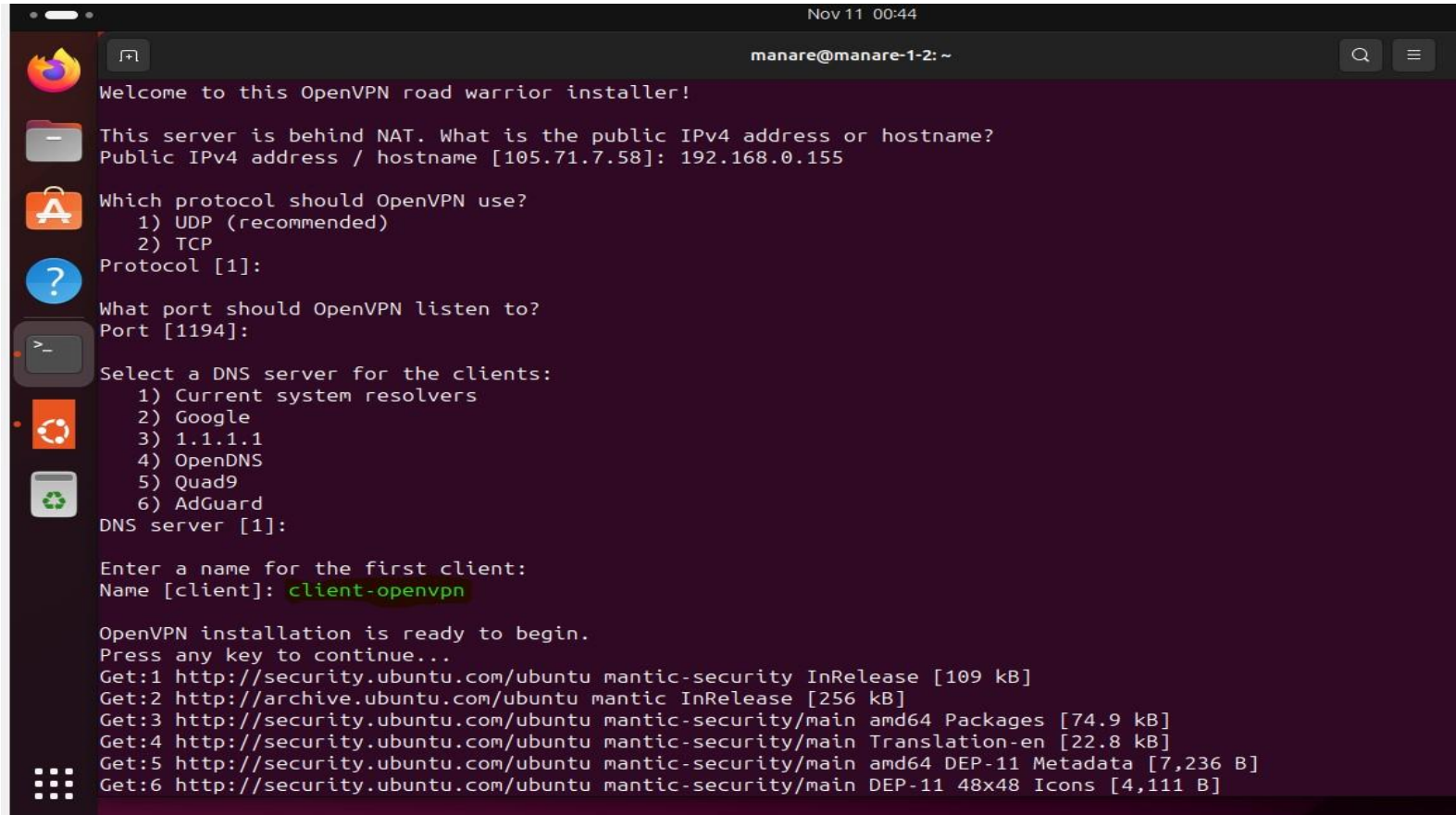
Donner la permission d'exécution:

```
manare@manare-1-2:~$  
manare@manare-1-2:~$  
manare@manare-1-2:~$  
manare@manare-1-2:~$ sudo chmod +x openvpn-install.sh  
[sudo] password for manare:  
manare@manare-1-2:~$  
manare@manare-1-2:~$  
manare@manare-1-2:~$
```

Executer openvpn:

```
manare@manare-1-2: ~  
manare@manare-1-2:~$  
manare@manare-1-2:~$  
manare@manare-1-2:~$  
manare@manare-1-2:~$  
manare@manare-1-2:~$ sudo ./openvpn-install.sh  
[sudo] password for manare:
```


Configuration :



The screenshot shows a terminal window titled "manare@manare-1-2: ~" with a timestamp of "Nov 11 00:44". The terminal displays the output of the "OpenVPN road warrior installer". The installation process is interactive, asking for various configuration options. The user has provided the following inputs:

- Public IPv4 address / hostname: 192.168.0.155
- Protocol: 1) UDP (recommended)
- Port: 1194
- DNS server: 1) Current system resolvers
- Client name: client-openvpn

The installer then proceeds to download necessary components from the Ubuntu security repository. The output shows the following progress:

```
OpenVPN installation is ready to begin.
Press any key to continue...
Get:1 http://security.ubuntu.com/ubuntu mantic-security InRelease [109 kB]
Get:2 http://archive.ubuntu.com/ubuntu mantic InRelease [256 kB]
Get:3 http://security.ubuntu.com/ubuntu mantic-security/main amd64 Packages [74.9 kB]
Get:4 http://security.ubuntu.com/ubuntu mantic-security/main Translation-en [22.8 kB]
Get:5 http://security.ubuntu.com/ubuntu mantic-security/main amd64 DEP-11 Metadata [7,236 B]
Get:6 http://security.ubuntu.com/ubuntu mantic-security/main DEP-11 48x48 Icons [4,111 B]
```

```
Get:4 http://security.ubuntu.com/ubuntu mantic-security/main Translation-en [22.8 kB]
Get:5 http://security.ubuntu.com/ubuntu mantic-security/main amd64 DEP-11 Metadata [7,236 B]
Get:6 http://security.ubuntu.com/ubuntu mantic-security/main DEP-11 48x48 Icons [4,111 B]
Get:7 http://security.ubuntu.com/ubuntu mantic-security/main DEP-11 64x64 Icons [8,578 B]
Get:8 http://security.ubuntu.com/ubuntu mantic-security/main DEP-11 64x64@2 Icons [29 B]
Get:9 http://security.ubuntu.com/ubuntu mantic-security/main amd64 c-n-f Metadata [1,560 B]
Get:10 http://security.ubuntu.com/ubuntu mantic-security/restricted amd64 Packages [116 kB]
Get:11 http://security.ubuntu.com/ubuntu mantic-security/restricted Translation-en [18.1 kB]
Get:12 http://security.ubuntu.com/ubuntu mantic-security/restricted amd64 c-n-f Metadata [420 B]
Get:13 http://security.ubuntu.com/ubuntu mantic-security/universe amd64 Packages [19.2 kB]
Get:14 http://security.ubuntu.com/ubuntu mantic-security/universe Translation-en [8,536 B]
Get:15 http://security.ubuntu.com/ubuntu mantic-security/universe amd64 DEP-11 Metadata [3,860 B]
Get:16 http://security.ubuntu.com/ubuntu mantic-security/universe DEP-11 48x48 Icons [4,111 B]
Get:17 http://security.ubuntu.com/ubuntu mantic-security/universe DEP-11 64x64 Icons [8,636 B]
Get:18 http://security.ubuntu.com/ubuntu mantic-security/universe DEP-11 64x64@2 Icons [29 B]
Get:19 http://security.ubuntu.com/ubuntu mantic-security/universe amd64 c-n-f Metadata [788 B]
Get:20 http://security.ubuntu.com/ubuntu mantic-security/multiverse amd64 Packages [2,896 B]
Get:21 http://security.ubuntu.com/ubuntu mantic-security/multiverse Translation-en [800 B]
Get:22 http://security.ubuntu.com/ubuntu mantic-security/multiverse amd64 c-n-f Metadata [232 B]
Get:23 http://archive.ubuntu.com/ubuntu mantic-updates InRelease [109 kB]
Get:24 http://archive.ubuntu.com/ubuntu mantic/main amd64 DEP-11 Metadata [465 kB]
Get:25 http://archive.ubuntu.com/ubuntu mantic/universe amd64 Packages [15.2 MB]
Ign:25 http://archive.ubuntu.com/ubuntu mantic/universe amd64 Packages
Get:26 http://archive.ubuntu.com/ubuntu mantic/universe Translation-en [5,951 kB]
Ign:26 http://archive.ubuntu.com/ubuntu mantic/universe Translation-en
Get:27 http://archive.ubuntu.com/ubuntu mantic/universe amd64 DEP-11 Metadata [3,793 kB]
Ign:27 http://archive.ubuntu.com/ubuntu mantic/universe amd64 DEP-11 Metadata
Get:28 http://archive.ubuntu.com/ubuntu mantic/universe DEP-11 48x48 Icons [3,702 kB]
Get:29 http://archive.ubuntu.com/ubuntu mantic/universe DEP-11 64x64 Icons [7,723 kB]
Get:30 http://archive.ubuntu.com/ubuntu mantic/universe DEP-11 64x64@2 Icons [75.0 kB]
```




manare@manare-1-2: ~



```
Get:25 http://archive.ubuntu.com/ubuntu mantic/universe amd64 Packages [15.2 MB]
Get:26 http://archive.ubuntu.com/ubuntu mantic/universe Translation-en [5,951 kB]
Get:27 http://archive.ubuntu.com/ubuntu mantic/universe amd64 DEP-11 Metadata [3,793 kB]
Fetched 34.2 MB in 36min 1s (15.8 kB/s)
Reading package lists... Done
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
openvpn is already the newest version (2.6.5-0ubuntu1).
openvpn set to manually installed.
ca-certificates is already the newest version (20230311ubuntu1).
ca-certificates set to manually installed.
The following additional packages will be installed:
  libssl3
The following packages will be upgraded:
  libssl3 openssl
2 upgraded, 0 newly installed, 0 to remove and 35 not upgraded.
Need to get 3,118 kB of archives.
After this operation, 0 B of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu mantic-updates/main amd64 libssl3 amd64 3.0.10-1ubuntu2.1 [1,930 kB]
Get:2 http://archive.ubuntu.com/ubuntu mantic-updates/main amd64 openssl amd64 3.0.10-1ubuntu2.1 [1,188 kB]
Fetched 3,118 kB in 33s (94.7 kB/s)
Preconfiguring packages ...
(Reading database ... 141605 files and directories currently installed.)
Preparing to unpack .../libssl3_3.0.10-1ubuntu2.1_amd64.deb ...
Unpacking libssl3:amd64 (3.0.10-1ubuntu2.1) over (3.0.10-1ubuntu2) ...
Preparing to unpack .../openssl_3.0.10-1ubuntu2.1_amd64.deb ...
Unpacking openssl (3.0.10-1ubuntu2.1) over (3.0.10-1ubuntu2) ...
Setting up libssl3:amd64 (3.0.10-1ubuntu2.1) ...
Setting up openssl (3.0.10-1ubuntu2.1) ...
Processing triggers for man-db (2.11.2-3) ...
Processing triggers for libc-bin (2.38-1ubuntu6) ...
```



×

Notice

```
* /etc/openvpn/server/easy-rsa/pki/ca.crt
```

```
No Easy-RSA 'vars' configuration file exists!
```

```
* openssl OpenSSL 3.0.10 1 Aug 2023 (Library: OpenSSL 3.0.10 1 Aug 2023)
```

— — — — —

Your files are:

```
* key: /etc/openvpn/server/easy-rsa/pki/private/server.key
```

Check that the request matches the signature

Signature nk

manare@manare-1-2: ~

Notice

Certificate created at:

* /etc/openvpn/server/easy-rsa/pki/issued/client-openvpn.crt

Notice

Inline file created:

* /etc/openvpn/server/easy-rsa/pki/inline/client-openvpn.inline

No Easy-RSA 'vars' configuration file exists!

Using SSL:

* openssl OpenSSL 3.0.10 1 Aug 2023 (Library: OpenSSL 3.0.10 1 Aug 2023)

Using configuration from /etc/openvpn/server/easy-rsa/pki/openssl-easyrsa.cnf

Notice

An updated CRL has been created:

* /etc/openvpn/server/easy-rsa/pki/crl.pem

2023-11-10 21:52:01 DEPRECATED OPTION: The option --secret is deprecated.

2023-11-10 21:52:01 WARNING: Using --genkey --secret filename is DEPRECATED. Use --genkey secret filename instead.

Created symlink /etc/systemd/system/multi-user.target.wants/openvpn-iptables.service → /etc/systemd/system/openvpn-iptables.service.

Created symlink /etc/systemd/system/multi-user.target.wants/openvpn-server@server.service → /lib/systemd/system/openvpn-server@.service.

Finished!

The client configuration is available in: /root/client-openvpn.ovpn

New clients can be added by running this script again.

manare@manare-1-2:~\$

Activation du Firewall:

```
manare@manare-1-2:~$  
manare@manare-1-2:~$  
manare@manare-1-2:~$ sudo ufw enable  
Firewall is active and enabled on system startup  
manare@manare-1-2:~$ sudo ufw status  
Status: active  
manare@manare-1-2:~$  
manare@manare-1-2:~$
```

manare@manare-1-2:~\$

manare@manare-1-2:~\$

manare@manare-1-2:~\$ sudo ufw allow 1194/udp

Rule added

Rule added (v6)

manare@manare-1-2:~\$ sudo ufw status

Status: active

To	Action	From
--	-----	----
1194/udp	ALLOW	Anywhere
1194/udp (v6)	ALLOW	Anywhere (v6)

manare@manare-1-2:~\$

Installation du net tools:

```
manare@manare-1-2:~$  
manare@manare-1-2:~$ sudo apt install net-tools  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following NEW packages will be installed:  
  net-tools  
0 upgraded, 1 newly installed, 0 to remove and 35 not upgraded.  
Need to get 204 kB of archives.  
After this operation, 815 kB of additional disk space will be used.  
Ign:1 http://archive.ubuntu.com/ubuntu mantic/main amd64 net-tools amd64 2.10-0.1ubuntu3  
Get:1 http://archive.ubuntu.com/ubuntu mantic/main amd64 net-tools amd64 2.10-0.1ubuntu3 [204 kB]  
Fetched 204 kB in 40s (5,147 B/s)  
Selecting previously unselected package net-tools.  
(Reading database ... 141605 files and directories currently installed.)  
Preparing to unpack .../net-tools_2.10-0.1ubuntu3_amd64.deb ...  
Unpacking net-tools (2.10-0.1ubuntu3) ...  
Setting up net-tools (2.10-0.1ubuntu3) ...  
Processing triggers for man-db (2.11.2-3) ...  
manare@manare-1-2:~$
```

manare@manare-1-2:~\$

manare@manare-1-2:~\$

manare@manare-1-2:~\$ sudo netstat -anp | grep openvpn

udp 0 0 10.0.2.15:1194 0.0.0.0:*

3305/openvpn

unix 3 [] STREAM CONNECTED 32272 3305/openvpn

manare@manare-1-2:~\$

• Déplacement du fichier client:

```
root@manare-1-2:~# ls -l
total 12
-rw-r--r-- 1 root root 4984 Nov 11 01:38 client-openvpn.ovpn
drwx----- 6 root root 4096 Nov 10 20:07 snap
root@manare-1-2:~# cp client-openvpn.ovpn /home/manare/
root@manare-1-2:~# exit
exit
manare@manare-1-2:~$
```

Installation du network manager :

```
manare@manare-1-2:~$  
manare@manare-1-2:~$  
manare@manare-1-2:~$ sudo apt install -y network-manager-openvpn  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following NEW packages will be installed:  
  network-manager-openvpn  
0 upgraded, 1 newly installed, 0 to remove and 35 not upgraded.  
Need to get 58.5 kB of archives.  
After this operation, 283 kB of additional disk space will be used.  
Get:1 http://archive.ubuntu.com/ubuntu mantic/main amd64 network-manager-openvpn amd64 1.10.2-3  
  [58.5 kB]  
Fetched 58.5 kB in 1s (43.7 kB/s)  
Selecting previously unselected package network-manager-openvpn.  
(Reading database ... 141635 files and directories currently installed.)  
Preparing to unpack .../network-manager-openvpn_1.10.2-3_amd64.deb ...  
Unpacking network-manager-openvpn (1.10.2-3) ...  
Setting up network-manager-openvpn (1.10.2-3) ...  
Processing triggers for dbus (1.14.10-1ubuntu1) ...  
manare@manare-1-2:~$  
manare@manare-1-2:~$  
manare@manare-1-2:~$
```

La plage VPN:

```
manare@manare-1-2:~$  
manare@manare-1-2:~$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default q  
len 1000  
    link/ether 08:00:27:f6:88:24 brd ff:ff:ff:ff:ff:ff  
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute enp0s3  
        valid_lft 84716sec preferred_lft 84716sec  
3: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN grou  
p default qlen 500  
    link/none  
    inet 10.8.0.1/24 scope global tun0  
        valid_lft forever preferred_lft forever  
    inet6 fe80::2f4d:bdbe:7ef3:c730/64 scope link stable-privacy  
        valid_lft forever preferred_lft forever  
manare@manare-1-2:~$  
manare@manare-1-2:~$
```

06

Wireshark

Définition:

Wireshark est un logiciel open source d'analyse des protocoles réseau créé par Gerald Combs en 1998, largement utilisé pour la capture et l'analyse des paquets de données transitant à travers un réseau.

Comment fonctionne ?

Wireshark est un outil de capture et d'analyse de paquets. Il capture le trafic du réseau local et stocke les données ainsi obtenues pour permettre leur analyse hors ligne. Wireshark est capable de capturer le trafic Ethernet, Bluetooth, sans fil (IEEE.802.11), Frame Relay et plus encore.

**Voyons ensemble
le test**

MERCI POUR
VOTRE
ATTENTION
AVEZ-VOUS
DE
QUESTION?

RESOURCES

- Lien du script : <https://raw.githubusercontent.com/Nyr/openvpn-install/master/openvpn-install.sh>
- <https://fr.scribd.com/document/430938747/CM3-VPN>
- <https://www.kaspersky.fr/resource-center/definitions/tunneling-protocol>
- <https://www.cloudflare.com/fr-fr/learning/network-layer/what-is-tunneling/#:~:text=Qu'est%2Dce%20que%20le,un%20r%C3%A9seau%20%C3%A0%20un%20autre.>
- <https://www.varonis.com/fr/blog/comment-utiliser-wireshark#:~:text=Wireshark%20est%20un%20outil%20de,Frame%20Relay%20et%20plus%20encore.>