

TP – Le VPN : Un Outil de Connectivité Sécurisée ou d’Anonymisation ?

Allan ETTINGER

Groupe 7

PSTB-LP ASSR

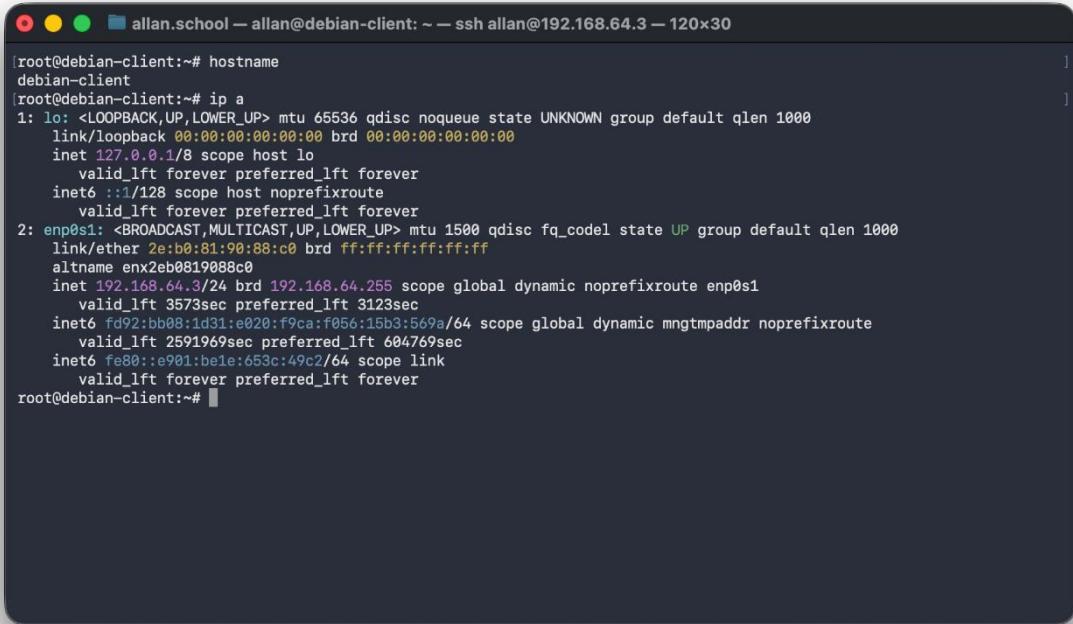
Table des matières

<i>Etape 1 : Préparation du laboratoire</i>	2
1. Configuration des machines clientes TEST VPN.....	3
2. Configuration du SRV WEB.....	3
3. Installation du FW pfSense et accès à l'interface web.....	4
<i>Etape 2 : Validation des tests</i>	5
1. Configuration Serveur VPN.....	5
2. Configuration des utilisateurs.....	5
3. Configuration WAN.....	5
4. Configuration LAN	5
5. Règles de pare-feu :	5
<i>Étape 3 : Tests</i>	5
1. Client connecté au VPN depuis un poste Mac	5
2. Client connecté au VPN depuis un Android	5
3. Client connecté depuis un poste Windows	5
4. Connexion RDP et HTTP	5
<i>Annexes</i>	5
1. Configuration serveur VPN entière.....	5

Etape 1 : Préparation du laboratoire

1. Configuration des machines clientes TEST VPN

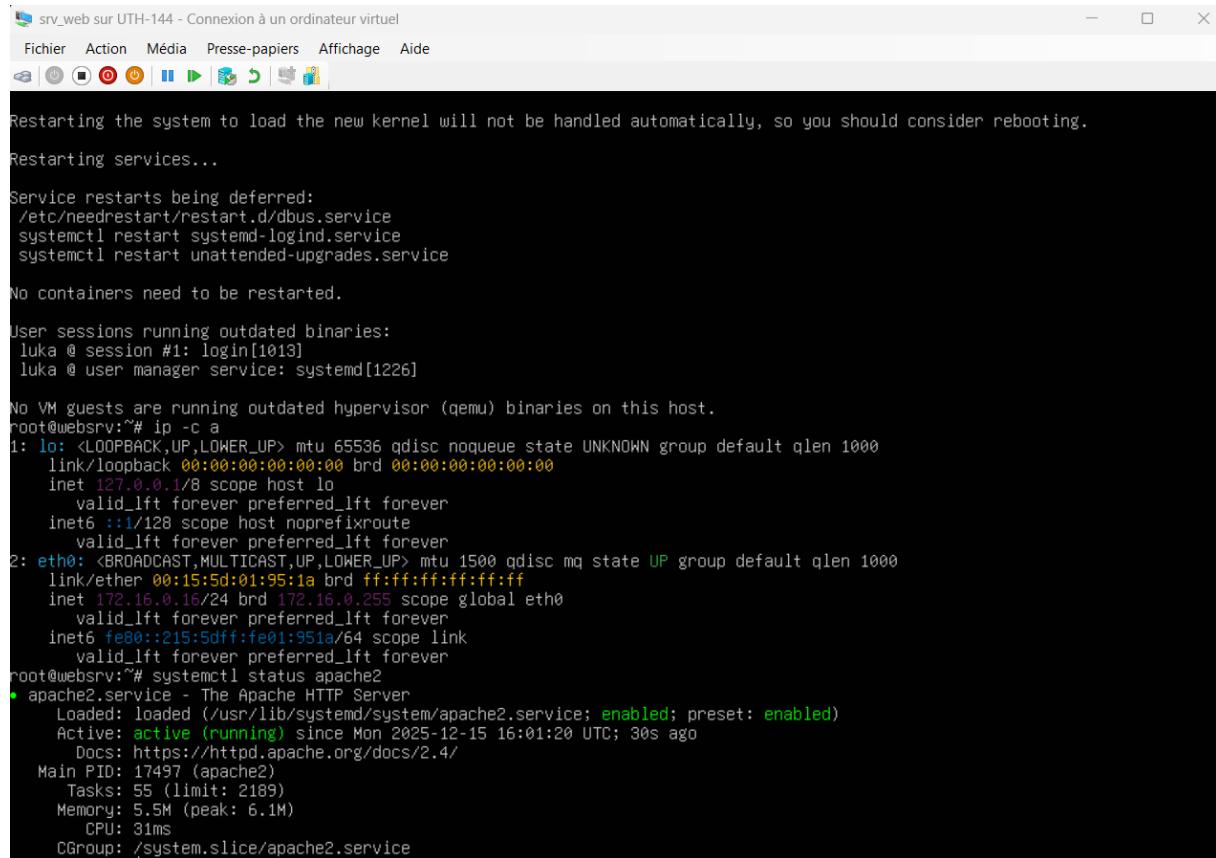
Installer les OS et Vérifier que l'IP est obtenue via DHCP (WAN)



```
allan.school — allan@debian-client: ~ — ssh allan@192.168.64.3 — 120x30
[root@debian-client:~# hostname
debian-client
[root@debian-client:~# 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 noprefixroute
                valid_lft forever preferred_lft forever
2: enp0s1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 2e:b0:81:90:88:c0 brd ff:ff:ff:ff:ff:ff
        altname enx2eb0819088c0
        inet 192.168.64.3/24 brd 192.168.64.255 scope global dynamic noprefixroute enp0s1
            valid_lft 3573sec preferred_lft 3123sec
            inet6 fd92:bb08:1d31:e020:f9ca:f056:15b3:569a/64 scope global dynamic mngtmpaddr noprefixroute
                valid_lft 2591969sec preferred_lft 604769sec
                inet6 fe80::e901:be1e:653c:49c2/64 scope link
                    valid_lft forever preferred_lft forever
root@debian-client:~# ]
```

2. Configuration du SRV WEB

Installer le serveur web de votre choix, IIS sous Windows recommandé, et définir une IP fixe.



```
srv_web sur UTH-144 - Connexion à un ordinateur virtuel
Fichier Action Média Presse-papiers Affichage Aide
Restarting the system to load the new kernel will not be handled automatically, so you should consider rebooting.
Restarting services...
Service restarts being deferred:
/etc/needrestart/restart.d/dbus.service
systemctl restart systemd-logind.service
systemctl restart unattended-upgrades.service

No containers need to be restarted.

User sessions running outdated binaries:
luka @ session #1: login[1013]
luka @ user manager service: systemd[1226]

No VM guests are running outdated hypervisor (qemu) binaries on this host.
root@websrv:~# ip -c 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
    inetc6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:15:5d:01:95:1a brd ff:ff:ff:ff:ff:ff
    inet 172.16.0.16/24 brd 172.16.0.255 scope global eth0
        valid_lft forever preferred_lft forever
    inetc6 fe80::215:5dff:fe01:951a/64 scope link
        valid_lft forever preferred_lft forever
root@websrv:~# systemctl status apache2
● apache2.service - The Apache HTTP Server
  Loaded: loaded (/usr/lib/systemd/system/apache2.service; enabled; preset: enabled)
  Active: active (running) since Mon 2025-12-15 16:01:20 UTC; 30s ago
    Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 17497 (apache2)
     Tasks: 55 (limit: 2189)
    Memory: 5.5M (peak: 6.1M)
      CPU: 31ms
     CGroup: /system.slice/apache2.service
```

Le serveur web Apache a été installé et activé sur la machine virtuelle. La commande « `systemctl status apache2` » confirme que le service Apache2 est en cours d'exécution et configuré pour démarrer automatiquement (statut : *active (running)*, preset : *enabled*).

La configuration réseau a également été vérifiée à l'aide de la commande `ip -c a`. L'interface `eth0` dispose d'une adresse IP fixe : `192.168.0.255`, ce qui permet d'assurer la stabilité des connexions au serveur.

La capture ci-dessus illustre :

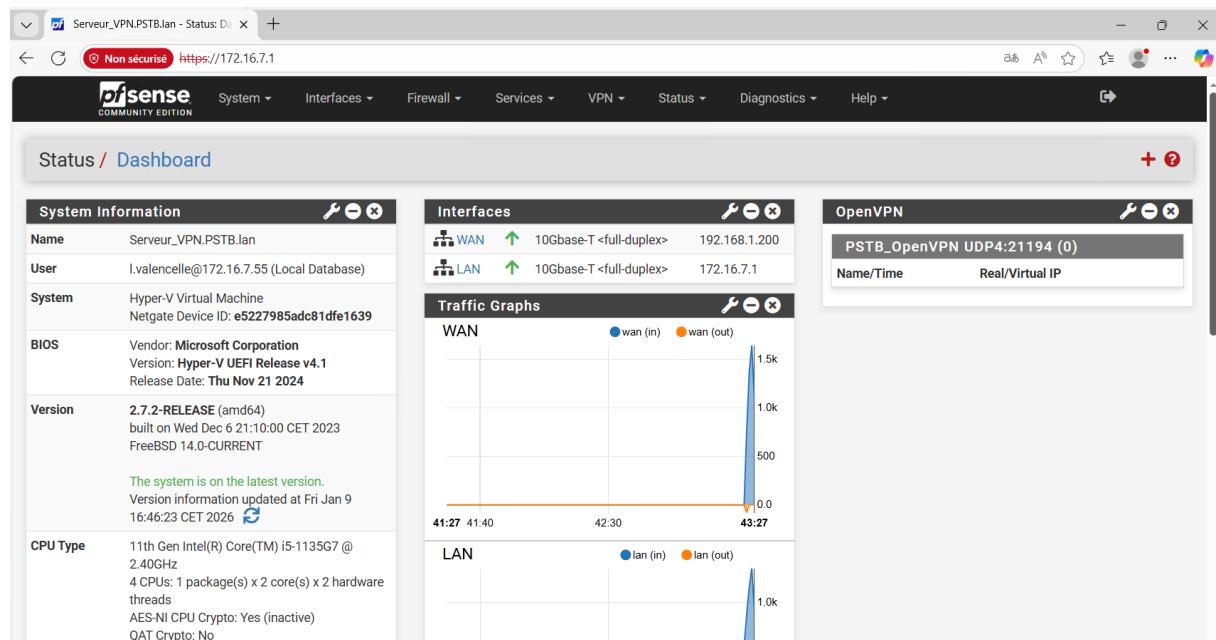
- L'état du service Apache2 (actif et fonctionnel).
- L'adresse IP fixe attribuée à l'interface réseau `eth0` (Par la suite l'ip fixé a été changé par `172.16.7.50` afin de respecter la demande.).
- La confirmation que le serveur est prêt à héberger des services web.

3. Installation du FW pfSense et accès à l'interface web

Depuis la machine du réseau LAN, accéder à l'interface web de pfSense en utilisant l'IP LAN du pare-feu pour finaliser la configuration.

Configuration des Interfaces Réseau du pfSense :

- I. WAN en DHCP (Le routeur étant une VM sur un poste portable l'ip WAN est amené à changer).
- II. LAN en IP fixe



Après l'installation du pare-feu pfSense, l'accès à l'interface d'administration web a été effectué depuis un navigateur en utilisant l'adresse IP de l'interface LAN du pare-feu.

La figure ci-dessus présente le tableau de bord (Dashboard) de pfSense, qui permet de visualiser l'état général du système.

On y retrouve notamment :

- Les informations système (nom de la machine, version de pfSense, type de matériel et processeur),
- L'état des interfaces réseau (WAN et LAN) avec leurs adresses IP respectives,
- Les connexion VPN en cours,
- Les graphiques de trafic réseau en temps réel pour chaque interface.

Cette interface web centralise l'administration du pare-feu et permet de configurer les règles de filtrage, le routage, les services réseau ainsi que les fonctionnalités VPN.

Etape 2 : Validation des tests

1. Configuration Serveur VPN

The screenshot shows the 'Servers' tab selected in the 'OpenVPN / OpenVPN / Servers' interface. A single server entry is listed:

OpenVPN Servers					
Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 21194 (TUN)	192.168.254.112/28	Mode: Remote Access (User Auth) Data Ciphers: AES-256-GCM, AES-256-CBC Digest: SHA256 D-H Params: 2048 bits	PSTB_OpenVPN	

A green 'Add' button is located at the bottom right.

Cette capture d'écran montre le serveur OpenVPN configuré dans pfSense :

- Le serveur VPN est attaché à l'interface **WAN** et utilise le protocole **UDP sur le port 21194**, ce qui permet aux clients distants de se connecter depuis Internet. Nous avons utilisé ce port car le 1194 est réservé par défaut sur la box internet du labo, nous avons donc mis en place une règle de redirection sur cette box :

The screenshot shows a 'Redirections' table with one active rule:

Liste des redirections				
Active	Redirection	IP source	Destination	
Active	Protocole: udp WAN : 21194 LAN: 21194 Commentaire:	Toutes	Serveur VPN	

- Le réseau de tunnel attribué aux clients VPN est **192.168.254.112/28**, qui correspond au réseau du tunnel (Si un client se connecte il se verra attribuer une ip dans ce réseau).
- Le mode d'authentification est configuré en **Remote Access (User Auth)**, indiquant que pour se connecter l'utilisateur doit connaître une combinaison login/password autorisé à se connecter.
- Les paramètres de sécurité incluent l'utilisation des chiffrements **AES-256-GCM / AES-256-CBC**, un algorithme de hachage **SHA256**, ainsi que des paramètres Diffie-Hellman de 2048 bits, assurant la confidentialité et l'intégrité des communications VPN.

De plus nous avons également mis en place une autorité de certification interne au serveur VPN avec un certificat serveur (pour le serveur VPN) et un certificat utilisateurs (pour les utilisateurs du VPN).

The screenshot shows the 'Certificate Authorities' section of the pfSense web interface. It lists three certificates:

- pfsense_CA**: Internal, self-signed, 2 certificates, Distinguished Name: ST=Île de France, OU=IT, O=PSTB, L=Paris, CN=FR, C=FR. Valid From: Mon, 05 Jan 2026 15:23:08 +0100, Valid Until: Thu, 03 Jan 2036 15:23:08 +0100. Actions: edit, delete, info.
- VPN-SERV-CERT**: Server Certificate, CA: No, Server: Yes. Issuer: pfsense_CA. Distinguished Name: ST=Île de France, OU=IT, O=PSTB, L=Paris, CN=openvpn-server, C=FR. Valid From: Mon, 05 Jan 2026 15:51:44 +0100, Valid Until: Thu, 04 Feb 2027 15:51:44 +0100. Actions: edit, delete, info, OpenVPN Server.
- User-cert**: User Certificate, CA: No, Server: No. Issuer: pfsense_CA. Distinguished Name: ST=Île de France, OU=IT, O=PSTB, L=Paris, CN=openvpn-client-shared, C=FR. Valid From: Mon, 05 Jan 2026 15:52:11 +0100, Valid Until: Thu, 03 Jan 2036 15:52:11 +0100. Actions: edit, delete, info.

At the bottom right, there are 'Add' and 'Add/Sign' buttons. The browser status bar at the bottom indicates: pfSense is developed and maintained by Netgate. © ESF 2004 - 2026 View license. FRA FR 20:05 09/01/2026.

Cette configuration définit les paramètres essentiels du VPN et permet aux clients distants de se connecter de manière sécurisée.

2. Configuration des utilisateurs

The screenshot shows the 'Users' section of the pfSense web interface. It lists five users:

Username	Full name	Status	Groups	Actions
a.ettinger	Allan Ettlinger	✓	admins	
admin	System Administrator	✗	admins	
d.cottenceau	Donatien Cottenceau	✓	admins	
j.candelariasureta	Jean-Christophe Candelaria Sureta	✓	admins	
l.valencelle	Luka Valencelle	✓	admins	

At the bottom right, there are 'Add' and 'Delete' buttons. The browser status bar at the bottom indicates: pfSense is developed and maintained by Netgate. © ESF 2004 - 2026 View license. FRA FR 20:05 09/01/2026.

Pour des raisons de sécurité et pour permettre de remonter jusqu'à la source de chaque modification sur le routeur, nous avons choisi de désactiver le compte admin, et de créer des accès personnels pour chaque membre du groupe.

3. Configuration WAN

Interfaces / WAN (hn0)

General Configuration

Enable	<input checked="" type="checkbox"/> Enable interface
Description	WAN Enter a description (name) for the interface here.
IPv4 Configuration Type	DHCP
IPv6 Configuration Type	DHCP6
MAC Address	XX:XX:XX:XX:XX:XX This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.
MTU	 If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	 If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IP header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex	Default (no preference, typically autoselect) <small>Explicitly set speed and duplex mode for this interface</small>

Cette capture d'écran présente la configuration de l'interface WAN, qui correspond à l'interface connectée au réseau externe (Internet).

L'adressage IP est obtenu automatiquement via DHCP (IPv4 et IPv6), ce qui permet au pare-feu pfSense de communiquer avec l'extérieur (Nous avons choisis d'activer le DHCP IPv6 car le box internet du labo le propose par défaut).

Cette interface est essentielle car elle sert de point d'entrée aux connexions VPN OpenVPN provenant des clients distants (La box internet redirigeant les requêtes vers le pare-feu grâce à la règle de NAT présenter précédemment dans le TP).

4. Configuration LAN

Interfaces / LAN (hn1)

General Configuration

Enable	<input checked="" type="checkbox"/> Enable interface
Description	LAN Enter a description (name) for the interface here.
IPv4 Configuration Type	Static IPv4
IPv6 Configuration Type	None
MAC Address	XX:XX:XX:XX:XX:XX This field can be used to modify ("spoof") the MAC address of this interface. Enter a MAC address in the following format: xx:xx:xx:xxxx or leave blank.
MTU	If this field is blank, the adapter's default MTU will be used. This is typically 1500 bytes but can vary in some circumstances.
MSS	If a value is entered in this field, then MSS clamping for TCP connections to the value entered above minus 40 for IPv4 (TCP/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.
Speed and Duplex	Default (no preference, typically autoselect) Explicitly set speed and duplex mode for this interface. WARNING: MUST be set to autoselect (automatically negotiate speed) unless the port this interface connects to has its speed and duplex forced.

Static IPv4 Configuration

IPv4 Address	172.16.7.1	/	24
IPv4 Upstream gateway	None	+ Add a new gateway	
If this interface is an Internet connection, select an existing Gateway from the list or add a new one using the "Add" button. On local area network interfaces the upstream gateway should be "none". Selecting an upstream gateway causes the firewall to treat this interface as a WAN type interface. Gateways can be managed by clicking here .			

5. Règles de pare-feu :

The screenshot shows a firewall configuration interface with two main sections: 'Rules (Drag to Change Order)' and 'Firewall Aliases IP'.

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
0/0 B	IPv4 TCP/UDP	ReseauTunnelVPN	*	Poste_windows_client	3389 (MS RDP)	*	none		[Allow] RDP --> Poste_windows_client	
0/0 B	IPv4 TCP/UDP	ReseauTunnelVPN	*	Serveur_web	80 (HTTP)	*	none		[Allow] Http --> serveur web	
0/0 B	IPv4+6 *	ReseauTunnelVPN	*	RFC1918	*	*	none		[Block] All trafic not allowed	
0/0 B	IPv4 TCP/UDP	ReseauTunnelVPN	*	*	*	*	none		[Allow] Trafic --> Internet	

Firewall Aliases IP

Name	Type	Values	Description	Actions
Poste_windows_client	Host(s)	172.16.7.55	Pour RDP	
ReseauTunnelVPN	Network(s)	192.168.254.112/28	Tunnel VPN	
RFC1918	Network(s)	10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16	RFC1918	
Serveur_web	Host(s)	172.16.7.50	Pour test VPN	

Cette table présente les règles de pare-feu configurées pour le tunnel OpenVPN. Elle autorise explicitement deux types de trafic :

- **L'accès RDP (port 3389)** vers la machine nommée Poste_windows_client, permettant un accès distant sécurisé.
- **L'accès HTTP (port 80)** vers le Serveur_web, permettant la consultation du site hébergé en interne.

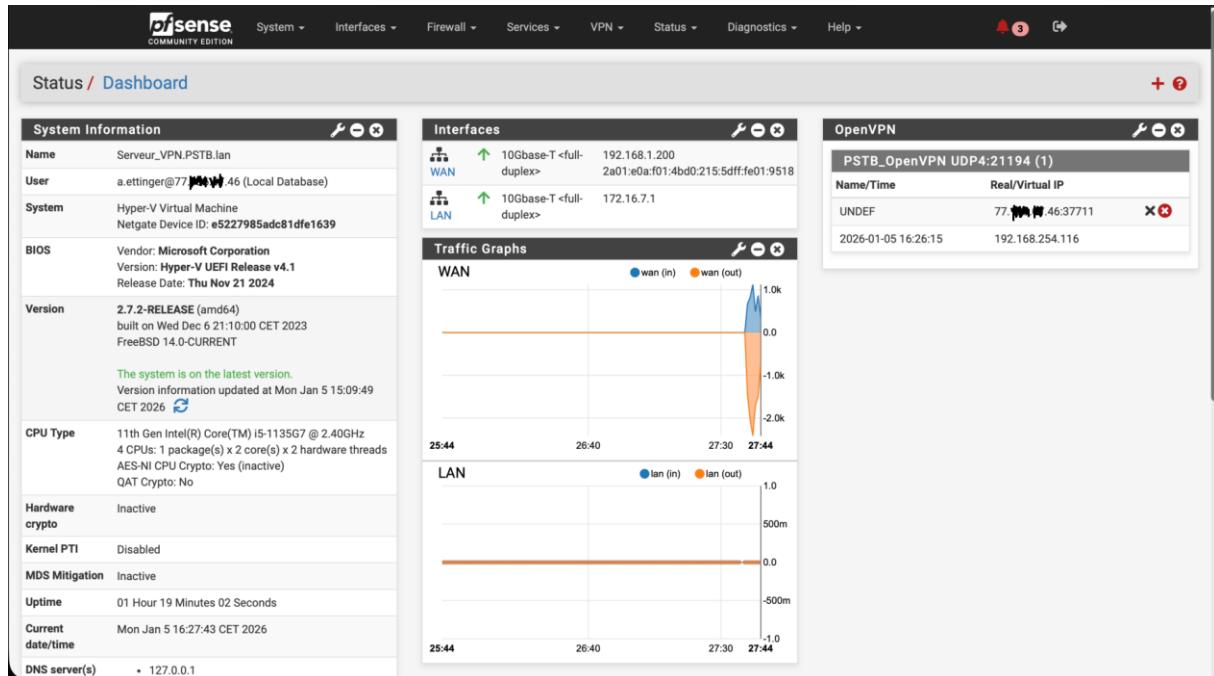
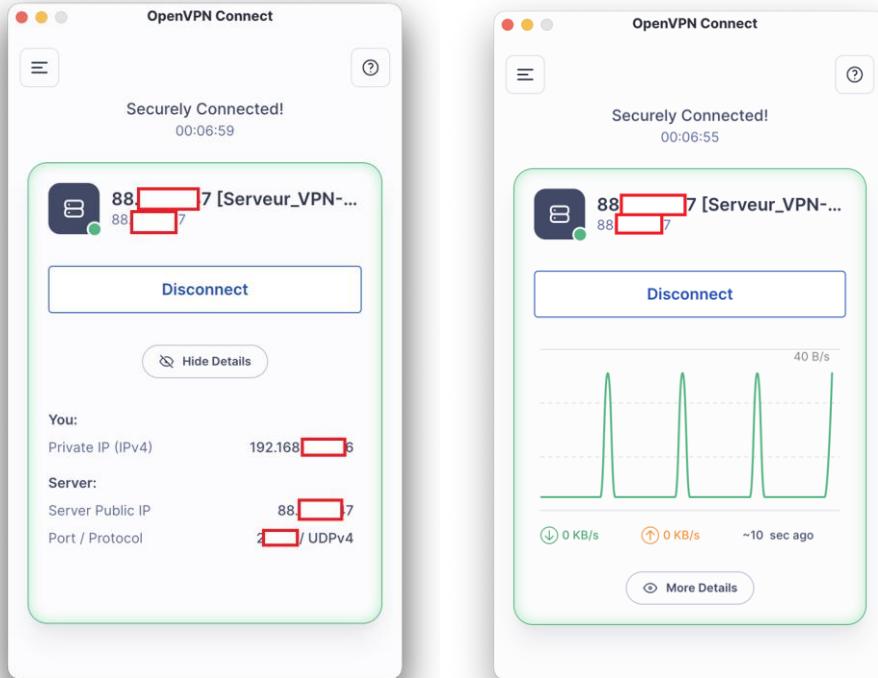
Une règle de blocage par défaut, placée en fin de liste, refuse tout autre trafic non explicitement autorisé, conformément au principe de sécurité de moindre privilège. Le pare-feu exécutant par défaut cette fonction, la règle sert surtout à pouvoir vérifier les states en cas de besoins.

Et nous avons également dû forcer le trafic des utilisateurs à passer dans le tunnel VPN :

IPv4 Tunnel Network	192.168.254.112/28
This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts. It is expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.	
A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which cannot push settings to clients. This mode is not supported with several options, including Exit Notify, and Inactive.	
IPv6 Tunnel Network	
This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts. It is expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.	
Redirect IPv4 Gateway	<input checked="" type="checkbox"/> Force all client-generated IPv4 traffic through the tunnel
Redirect IPv6 Gateway	<input type="checkbox"/> Force all client-generated IPv6 traffic through the tunnel.
IPv6 Local network(s)	
IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX or host aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set by the network.	
Concurrent connections	7
Specify the maximum number of clients allowed to concurrently connect to this server.	
Allow Compression	Refuse any non-stub compression (Most secure) <input type="button" value="▼"/>
Allow compression to be used with this VPN instance.	

Étape 3 : Tests

1. Client connecté au VPN depuis un poste Mac

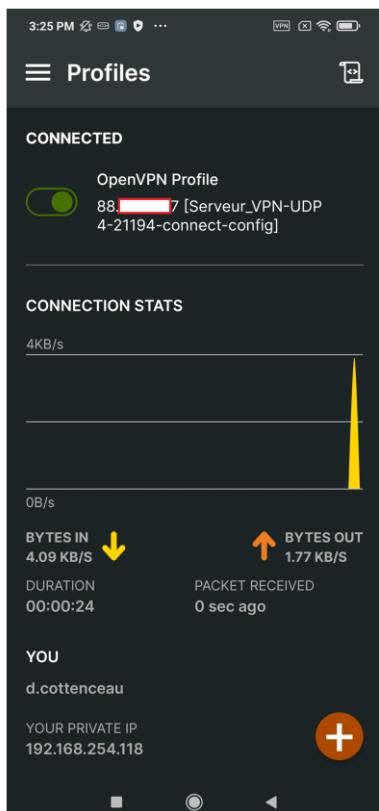


La capture d'écran montre l'application OpenVPN Connect sur un système macOS, confirmant une connexion VPN réussie.

Le message « Securely Connected! » est clairement affiché, accompagné de l'adresse IP publique attribuée et du nom du serveur (Serveur_VPN). Le temps de connexion (00:06:55) et le graphique de transfert de données (réception à 40 B/s) indiquent que le tunnel est actif et fonctionnel.

Ce résultat prouve que le client macOS est correctement configuré et qu'il communique avec le serveur VPN.

2. Client connecté au VPN depuis un Android



La capture d'écran montre la connexion VPN depuis un Android, où nous pouvons voir que le tunnel a bien été établi, avec le compte “d.cottenceau” et que l'IP de la machine dans le tunnel est : 192.168.254.118/28.

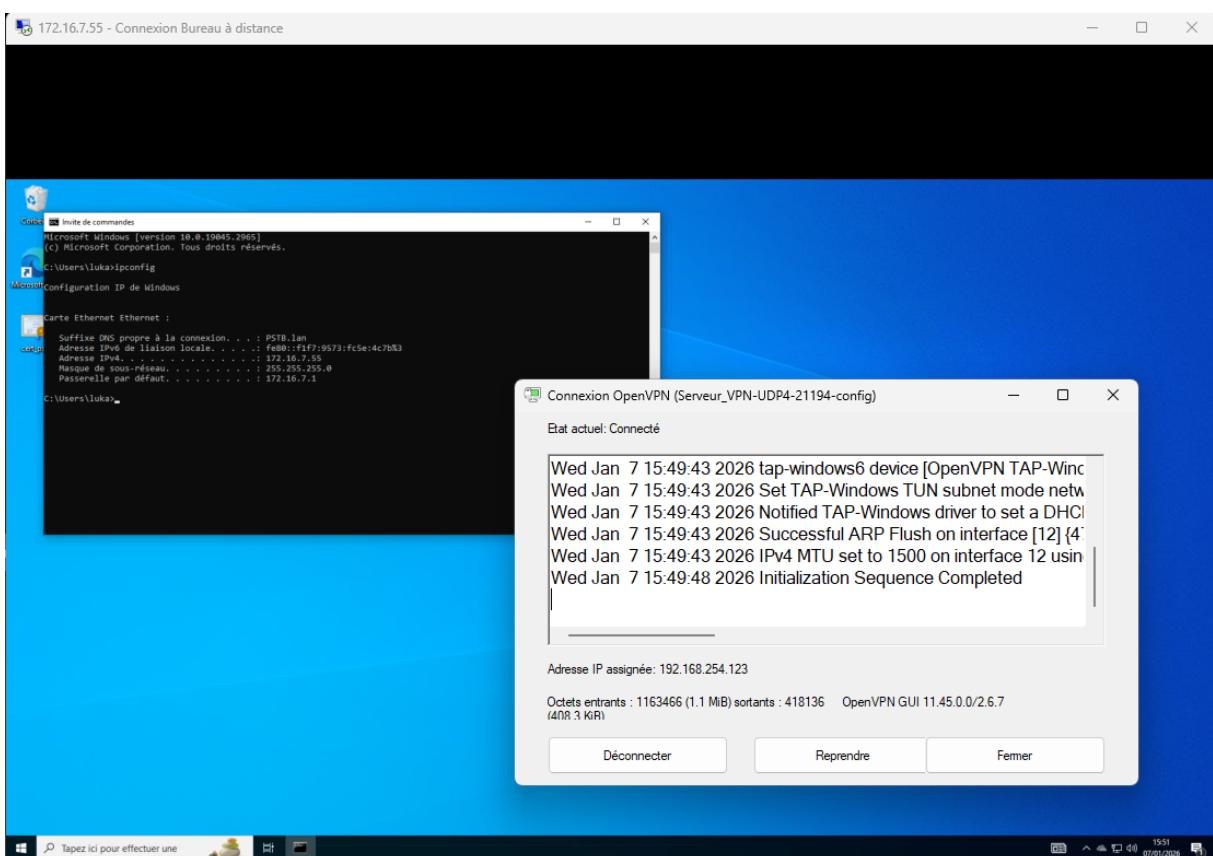
Le graphique nous montre également que le VPN est bien fonctionnel.

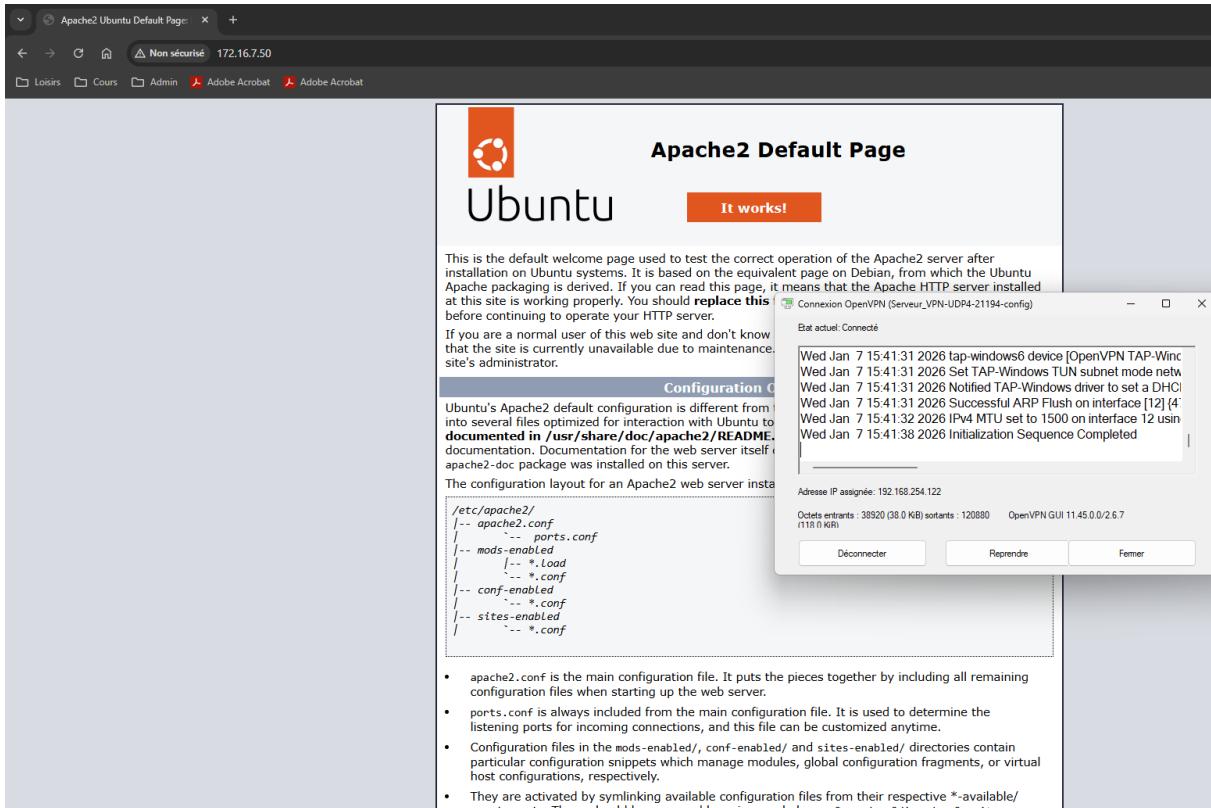
3. Client connecté depuis un poste Windows



Dans cette capture d'écran, nous pouvons voir que le poste Windows de Donatien est connecté au VPN et que son adresse IP dans le tunnel est 192.168.254.119/28.

4. Connexion RDP et HTTP





Sur les deux captures d'écran ci-dessus, nous pouvons voir que le poste Windows est bien disponible en RDP via le VPN.

Nous pouvons voir l'IP de la machine en 172.16.7.55 ainsi que le serveur web (non personnalisé) qui est accessible grâce au VPN.

Nous voyons également son IP : 172.16.7.50, conformément à la réservation DHCP faite pour ces derniers.

DHCP Static Mappings				
Static ARP	MAC address	IP address	Hostname	Description
00:15:5d:01:95:1a	172.16.7.50	Serveur-web		
00:15:5d:01:95:1c	172.16.7.55	PosteWindowsClient		
+ Add Static Mapping				

Annexes

1. Configuration serveur VPN entière

The screenshot shows the pfSense OpenVPN configuration interface. It includes sections for General Information, Mode Configuration, Endpoint Configuration, and Cryptographic Settings.

General Information:

- Description: PSTB_OpenVPN
- A description of this VPN for administrative reference.
- Disabled: Disable this server
- Set this option to disable this server without removing it from the list.
- Unique VPN ID: Server 1 (ovpn1)

Mode Configuration:

- Server mode: Remote Access (User Auth)
- Backend for authentication: Local Database
- Device mode: tun - Layer 3 Tunnel Mode
 - "tun" mode carries IPv4 and IPv6 (OSI layer 3) and is the most common and compatible mode across all platforms.
 - "tap" mode is capable of carrying 802.3 (OSI Layer 2).

Endpoint Configuration:

- Protocol: UDP on IPv4 only
- Interface: WAN

Cryptographic Settings:

- TLS Configuration:
 - Use a TLS Key
 - A TLS key enhances security of an OpenVPN connection by requiring both parties to have a common key before a peer can perform a TLS handshake. This layer of HMAC authentication allows control channel packets without the proper key to be dropped, protecting the peers from attack or unauthorized connections. The TLS Key does not have any effect on tunnel data.
- TLS Key:

```
#  
# 2048 bit OpenVPN static key  
#-----BEGIN OpenVPN Static key V1-----  
9d032a7027dae2a7c1d8abca1410992c
```

Paste the TLS key here.
This key is used to sign control channel packets with an HMAC signature for authentication when establishing the tunnel.
- TLS Key Usage Mode: TLS Authentication
 - In Authentication mode the TLS key is used only as HMAC authentication for the control channel, protecting the peers from unauthorized connections. Encryption and Authentication mode also encrypts control channel communication, providing more privacy and traffic control channel obfuscation.
- TLS keydir direction: Use default direction
 - The TLS Key Direction must be set to complementary values on the client and server. For example, if the server is set to 0, the client must be set to 1. Both may be set to omit the direction, in which case the TLS Key will be used bidirectionally.

pfSense COMMUNITY EDITION

Peer Certificate Authority: pfsense_CA

Peer Certificate Revocation list: No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager

OCSP Check: Check client certificates with OCSP

Server certificate: VPN-SERV-CERT (Server: Yes, CA: pfsense_CA, In Use)

Certificates known to be incompatible with use for OpenVPN are not included in this list, such as certificates using incompatible ECDSA curves or weak digest algorithms.

DH Parameter Length: 2048 bit

Diffie-Hellman (DH) parameter set used for key exchange. ⓘ

ECDH Curve: Use Default

The Elliptic Curve to use for key exchange. The curve from the server certificate is used by default when the server uses an ECDSA certificate. Otherwise, secp384r1 is used as a fallback.

Data Encryption Algorithms: AES-128-CBC (128 bit key, 128 bit block)
AES-128-CFB (128 bit key, 128 bit block)
AES-128-CFB1 (128 bit key, 128 bit block)
AES-128-CFB8 (128 bit key, 128 bit block)
AES-128-GCM (128 bit key, 128 bit block)
AES-128-OFB (128 bit key, 128 bit block)
AES-192-CBC (192 bit key, 128 bit block)
AES-192-CFB (192 bit key, 128 bit block)
AES-192-CFB1 (192 bit key, 128 bit block)
AES-192-CFB8 (192 bit key, 128 bit block)

AES-256-GCM
AES-256-CBC

Fallback Data Encryption Algorithm: AES-256-GCM (256 bit key, 128 bit block)

The Fallback Data Encryption Algorithm used for data channel packets when communicating with clients that do not support data encryption algorithm negotiation (e.g. Shared Key). This algorithm is automatically included in the Data Encryption Algorithms list.

Auth digest algorithm: SHA256 (256-bit)

The algorithm used to authenticate data channel packets, and control channel packets if a TLS Key is present.
When an AEAD Encryption Algorithm mode is used, such as AES-GCM, this digest is used for the control channel only, not the data channel.
The server and all clients must have the same setting. While SHA1 is the default for OpenVPN, this algorithm is insecure.

Hardware Crypto: No Hardware Crypto Acceleration

Certificate Depth: One (Client+Server)

When a certificate-based client logs in, do not accept certificates below this depth. Useful for denying certificates made with intermediate CAs generated from the same CA as the server.

Client Certificate Key Usage Validation: Enforce key usage
Verify that only hosts with a client certificate can connect (EKU: "TLS Web Client Authentication").

Tunnel Settings

IPv4 Tunnel Network: 192.168.254.112/28

This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. The remaining usable addresses will be assigned to connecting clients.

A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which cannot push settings to clients. This mode is not compatible

System, **Interfaces**, **Firewall**, **Services**, **VPN**, **Status**, **Diagnostics**, **Help**, **Logout**

20:16 FRA FR 09/01/2026

IPv6 Tunnel Network

This is the IPv6 virtual network or network type alias with a single entry used for private communications between this server and client hosts expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remaining addresses will be assigned to connecting clients.

Redirect IPv4 Gateway Force all client-generated IPv4 traffic through the tunnel.

Redirect IPv6 Gateway Force all client-generated IPv6 traffic through the tunnel.

IPv6 Local network(s)

IPv6 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more IP/PREFIX or host/network type aliases. This may be left blank if not adding a route to the local network through this tunnel on the remote machine. This is generally set to the LAN network.

Concurrent connections Specify the maximum number of clients allowed to concurrently connect to this server.

Allow Compression Allow compression to be used with this VPN instance. Compression can potentially increase throughput but may allow an attacker to extract secrets if they can control compressed plaintext traversing the VPN (e.g. HTTP). Before enabling compression, consult information about the VORACLE, CRIME, TIME, and BREACH attacks against TLS to decide if the use case for this specific VPN is vulnerable to attack.

Asymmetric compression allows an easier transition when connecting with older peers.

Type-of-Service Set the TOS IP header value of tunnel packets to match the encapsulated packet value.

Inter-client Allow communication between clients connected to this server.

Client Settings

Dynamic IP Allow connected clients to retain their connections if their IP address changes.

Topology Specifies the method used to supply a virtual adapter IP address to clients when using TUN mode on IPv4. Some clients may require this be set to "subnet" even for IPv6, such as OpenVPN Connect (iOS/Android). Older versions of OpenVPN (before 2.0.9) or clients such as Yealink phones may require "net30".

Ping settings

Inactive Causes OpenVPN to close a client connection after n seconds of inactivity on the TUN/TAP device. Activity is based on the last incoming or outgoing tunnel packet. A value of 0 disables this feature. This option is ignored in Peer-to-Peer Shared Key mode and in SSL/TLS mode with a blank or /30 tunnel network as it will cause the server to exit and not restart.

Ping method

The screenshot shows two pages of the pfSense web interface:

- Advanced Client Settings:**
 - Interval:** 10
 - Timeout:** 60
 - DNS Default Domain:** Provide a default domain name to clients
 - DNS Server enable:** Provide a DNS server list to clients. Addresses may be IPv4 or IPv6.
 - Block Outside DNS:** Make Windows 10 Clients Block access to DNS servers except across OpenVPN while connected, forcing clients to use only VPN DNS servers. Requires Windows 10 and OpenVPN 2.3.9 or later. Only Windows 10 is prone to DNS leakage in this way, other clients will ignore the option as they are not affected.
 - Force DNS cache update:** Run "net stop dnscache", "net start dnscache", "ipconfig /flushdns" and "ipconfig /registerdns" on connection initiation. This is known to kick Windows into recognizing pushed DNS servers.
 - NTP Server enable:** Provide an NTP server list to clients
 - NetBIOS enable:** Enable NetBIOS over TCP/IP
If this option is not set, all NetBIOS-over-TCP/IP options (including WINS) will be disabled.
- Advanced Configuration:**
 - Custom options:** [Text input field]

Les différentes IP publiques visibles sur les captures d'écran ont été censurées car ce sont celles du laboratoire et des membres du groupes. N'ayant pas d'importance capitale dans ce TP, nous avons choisi de les censurer.