UPEC
Connaissance - Action

UNIVERSITÉ
PARIS-EST CRÉTEIL
VAL DE MARNE

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

Allan ETTINGER

Groupe 7

PSTB-LP ASSR

Luka VALENCELLE
Jean-Christophe CANDELARIA SURETA
Donatien COTTENCEAU

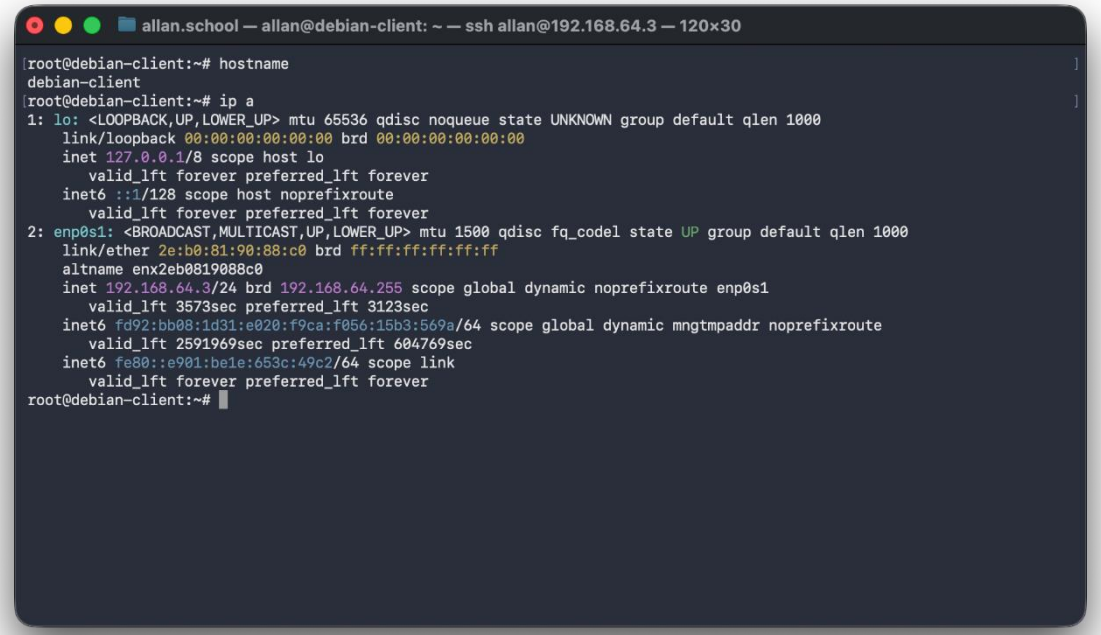
Rendu le 10 janvier 2026

Table des matières

Etape 1 : Préparation du laboratoire

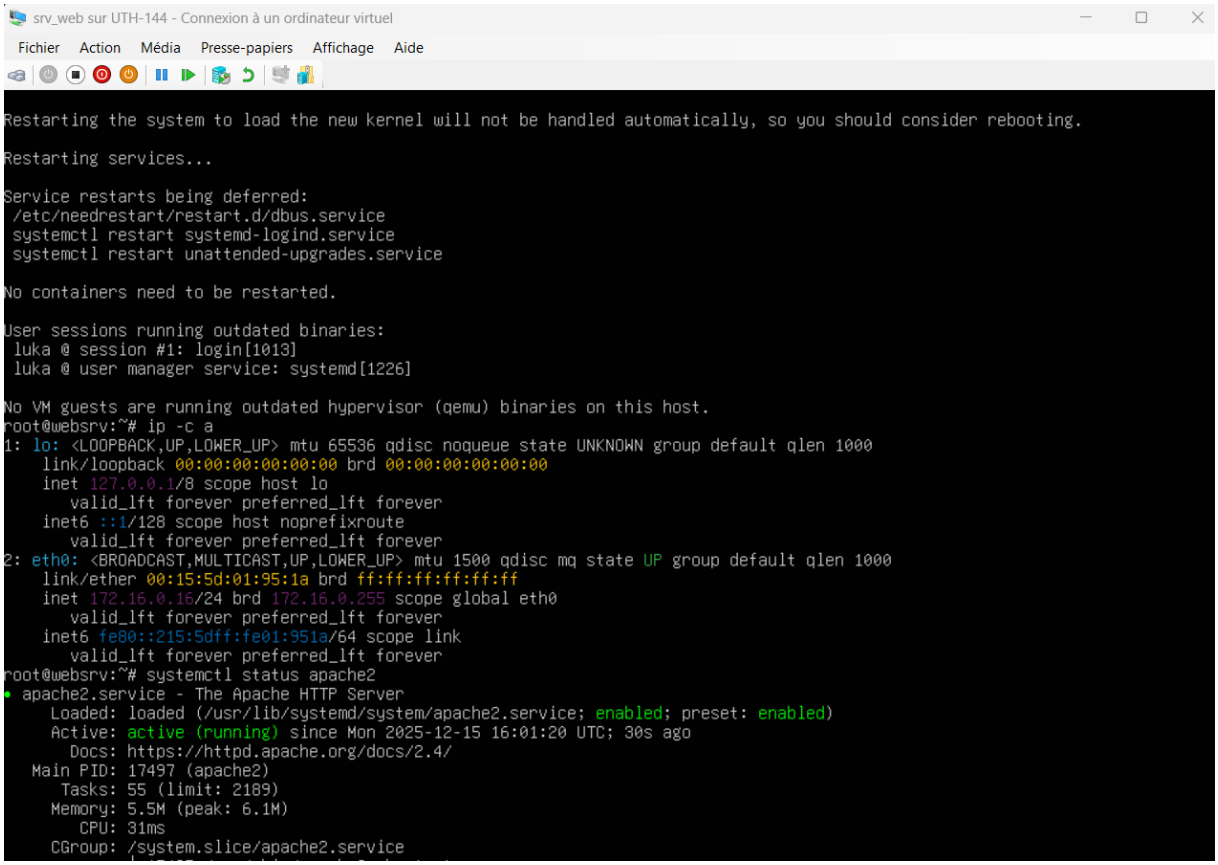
1. Configuration des machines clientes TEST VPN

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



2. Configuration du SRV WEB

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



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.

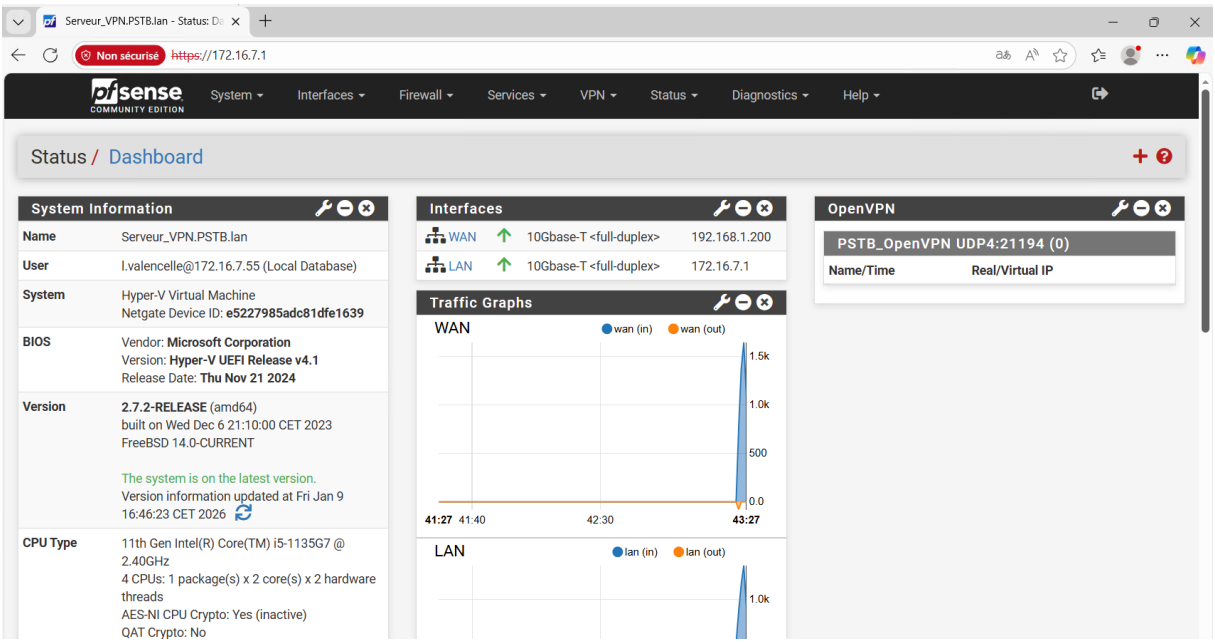
La capture ci-dessus illustre :

- 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.

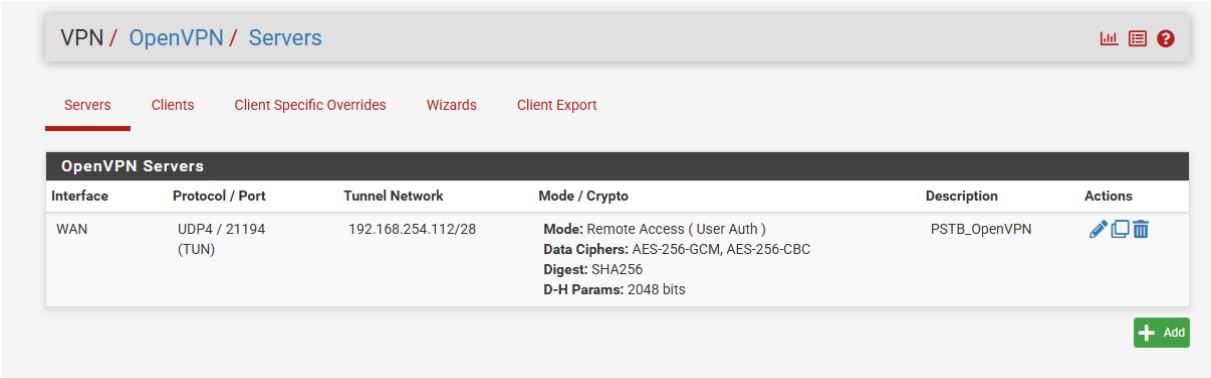
On y retrouve notamment :

- 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



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

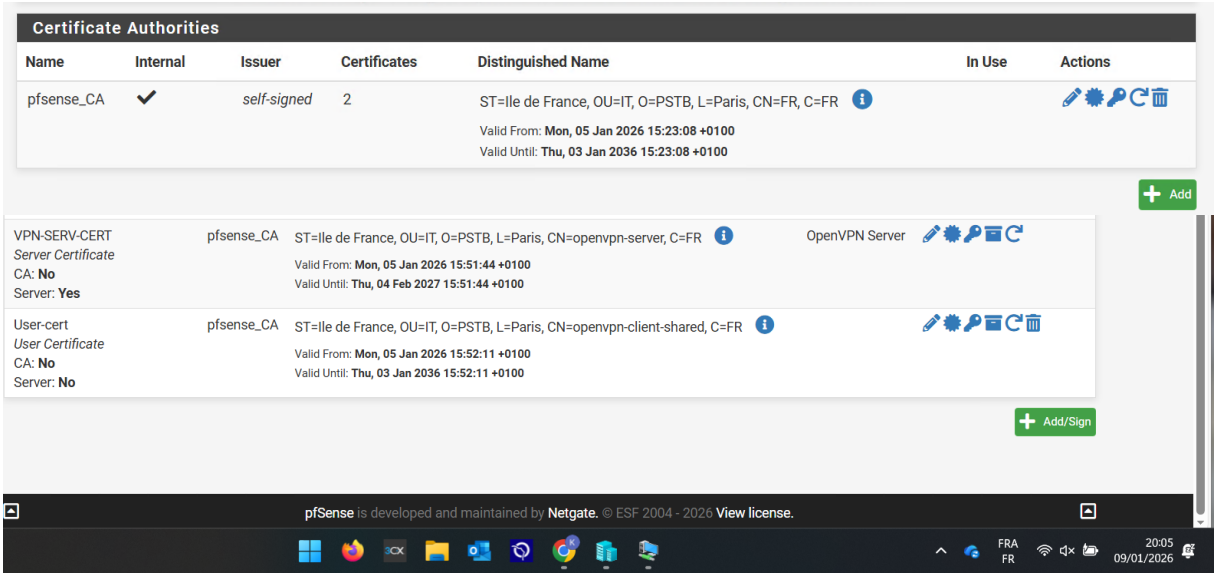
- Le serveur VPN est attaché à l'interface **WAN** et utilise le protocole **UDP sur le port 21194**, ce qui permet aux clients distants de se connecter depuis Internet. Nous avons utilisé ce port car le 1194 est réservé par défaut sur la box internet du labo, nous avons donc mis en place une règle de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

- 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 connaitre une combinaison login/password autorisé à se connecter.

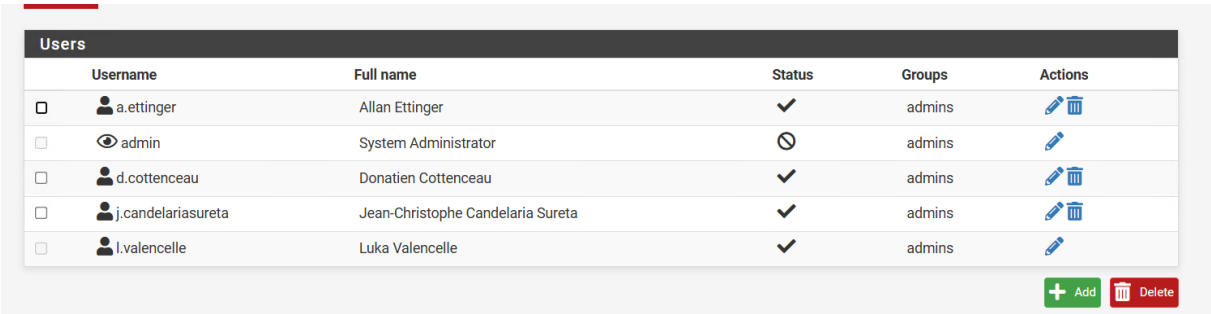
- Les paramètres de sécurité incluent l'utilisation des chiffrements **AES-256-GCM / AES-256-CBC**, un algorithme de hachage **SHA256**, ainsi que des paramètres Diffie-Hellman de 2048 bits, assurant la confidentialité et l'intégrité des communications VPN.

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).



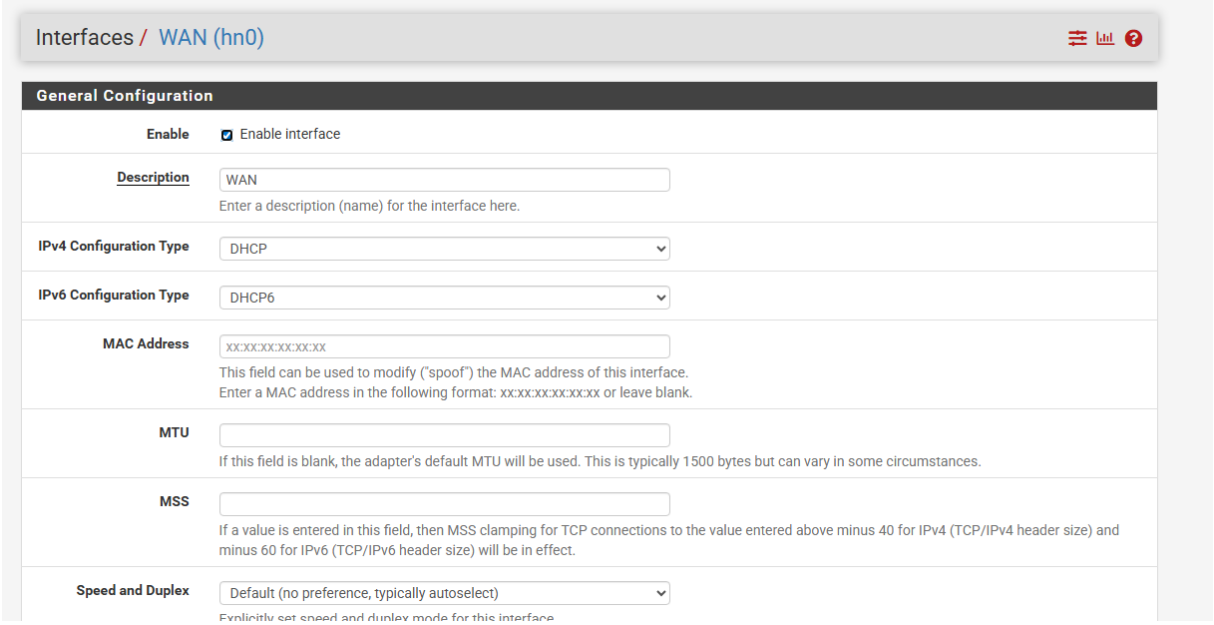
Cette configuration définit les paramètres essentiels du VPN et permet aux clients distants de se connecter de manière sécurisée.

2. Configuration des utilisateurs



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

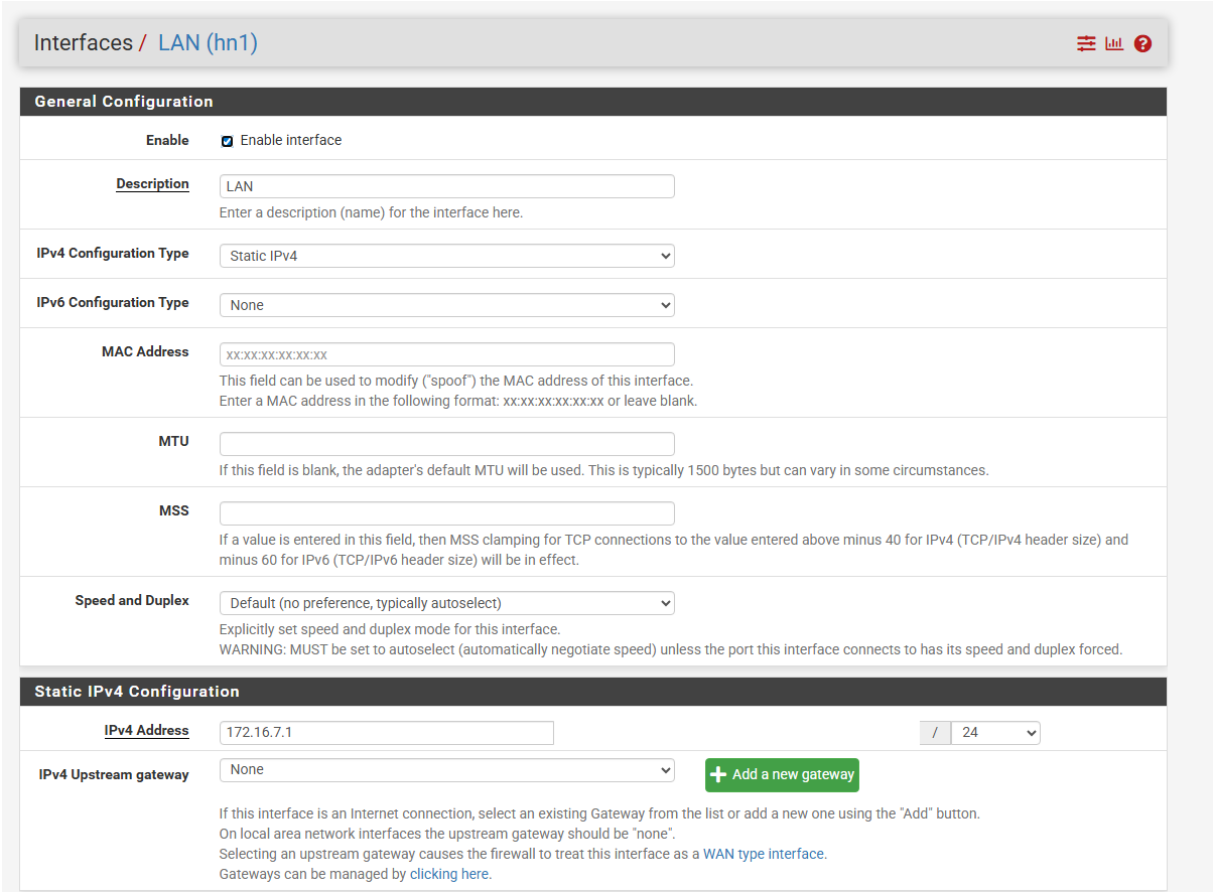


Cette capture d'écran présente la configuration de l'interface WAN, qui correspond à l'interface connectée au réseau externe (Internet).

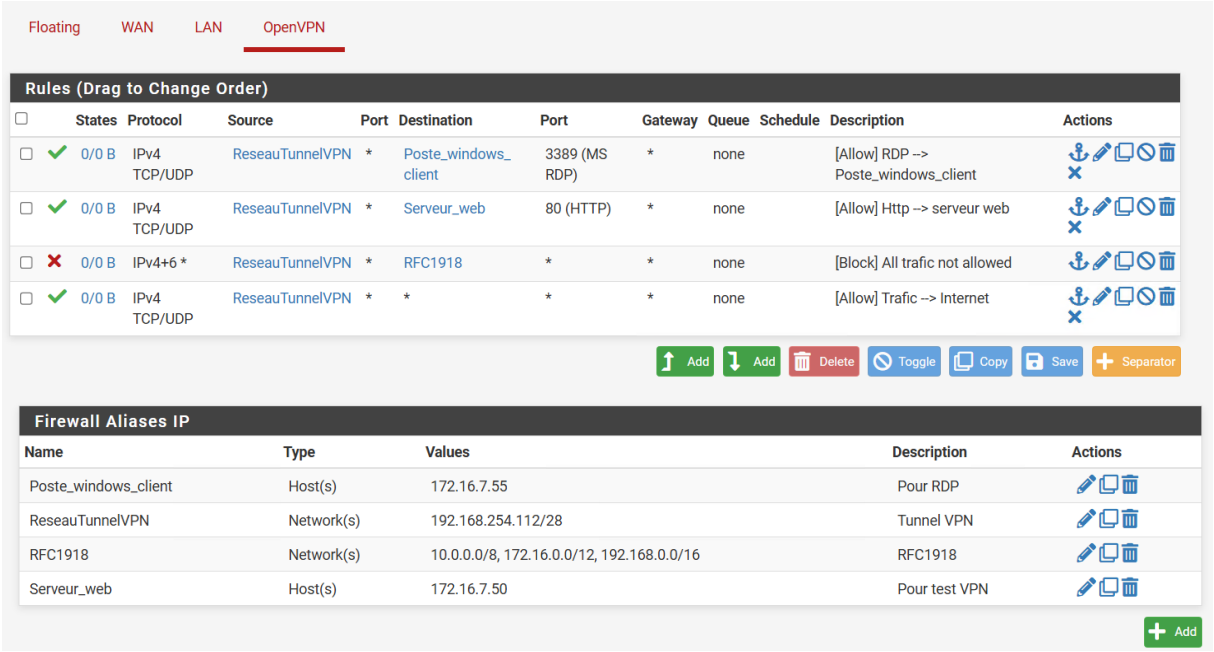
L'adressage IP est obtenu automatiquement via DHCP (IPv4 et IPv6), ce qui permet au pare-feu pfSense de communiquer avec l'extérieur (Nous avons choisis d'activer le DHCP IPv6 car le box internet du labo le propose par défaut).

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



5. Règles de pare-feu :



Floating | WAN | LAN | OpenVPN

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	

Add | Add | Delete | Toggle | Copy | Save | Separator

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	

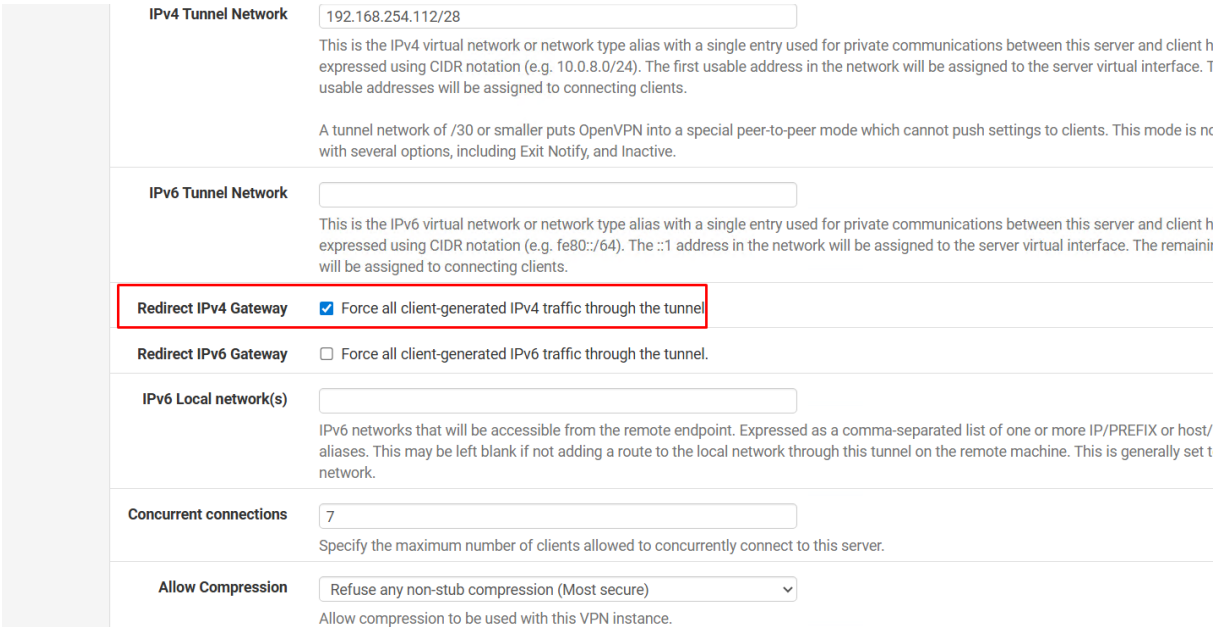
Add

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.

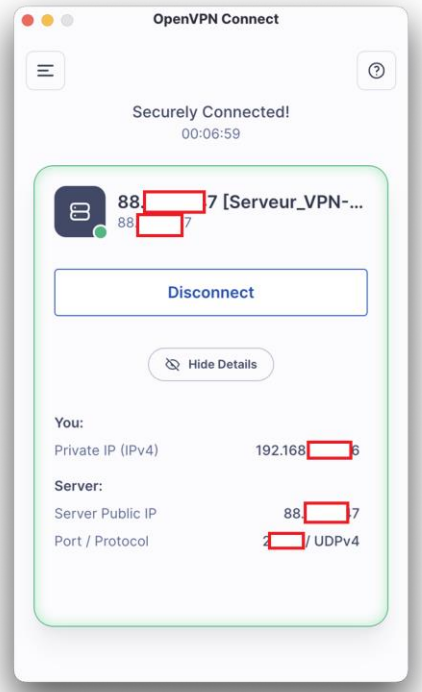
Une règle de blocage par défaut, placée en fin de liste, refuse tout autre trafic non explicitement autorisé, conformément au principe de sécurité de moindre privilège. Le pare-feu exécutant par défaut cette fonction, la règle sert surtout à pouvoir vérifier les states en cas de besoins.

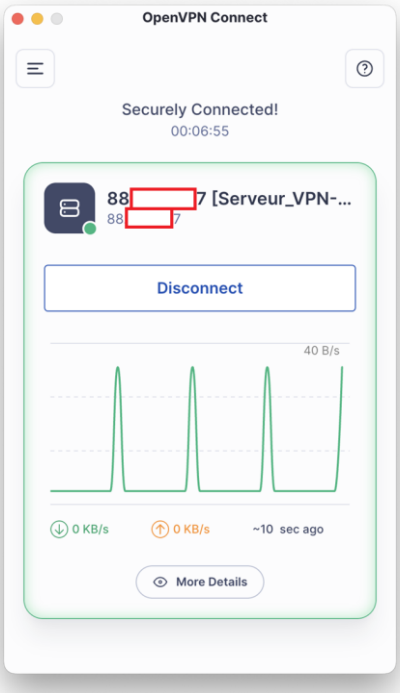
Et nous avons également dû forcer le trafic des utilisateurs à passer dans le tunnel VPN :

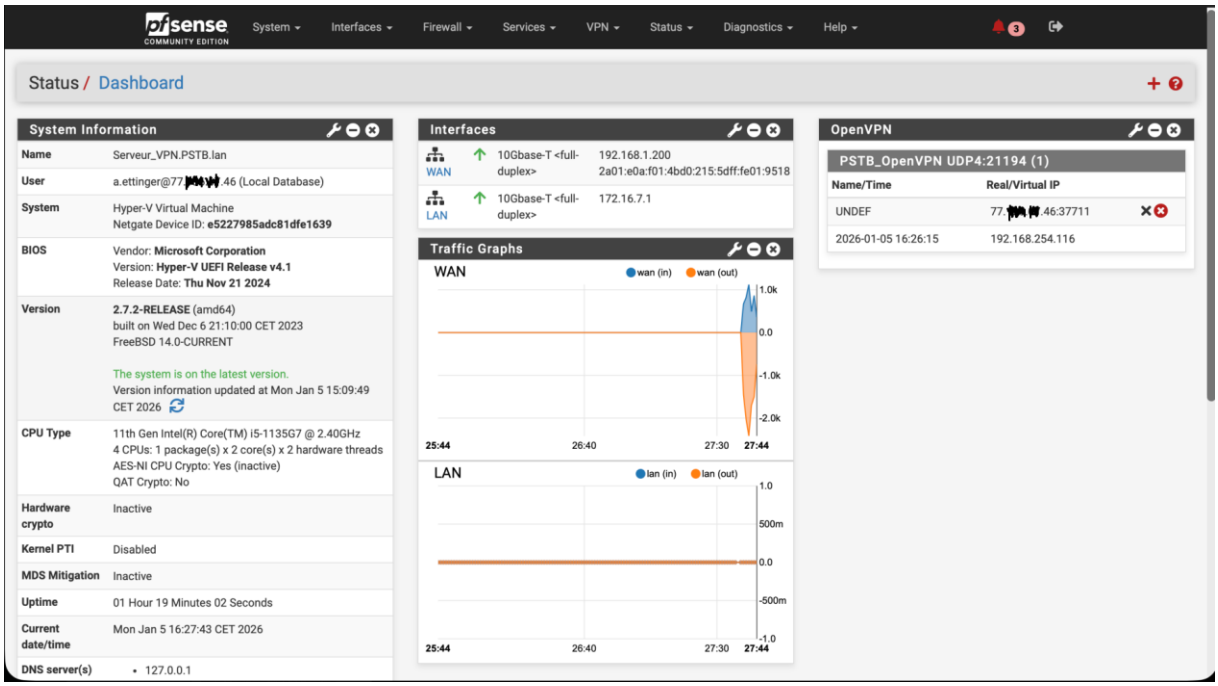

IPv4 Tunnel Network
192.168.254.112/28
This is the IPv4 virtual network or network type alias with a single entry used for private communications between this server and client h
expressed using CIDR notation (e.g. 10.0.8.0/24). The first usable address in the network will be assigned to the server virtual interface. T
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 nc
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 h
expressed using CIDR notation (e.g. fe80::/64). The ::1 address in the network will be assigned to the server virtual interface. The remainir
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/
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 t
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)
Allow compression to be used with this VPN instance.

Étape 3 : Tests

1. Client connecté au VPN depuis un poste Mac





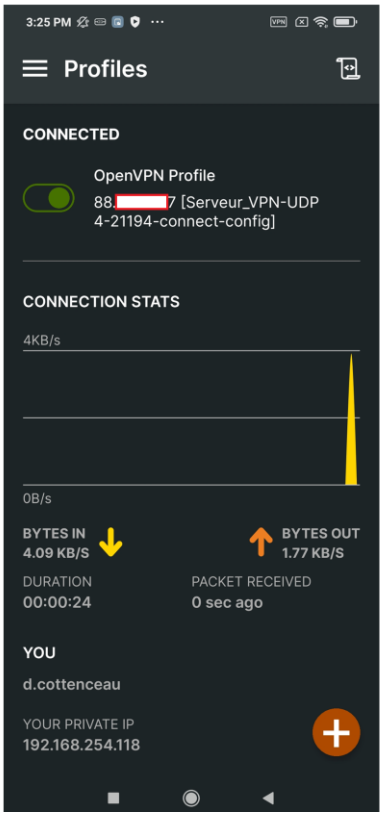


La capture d’écran montre l’application OpenVPN Connect sur un système macOS, confirmant une connexion VPN réussie.

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



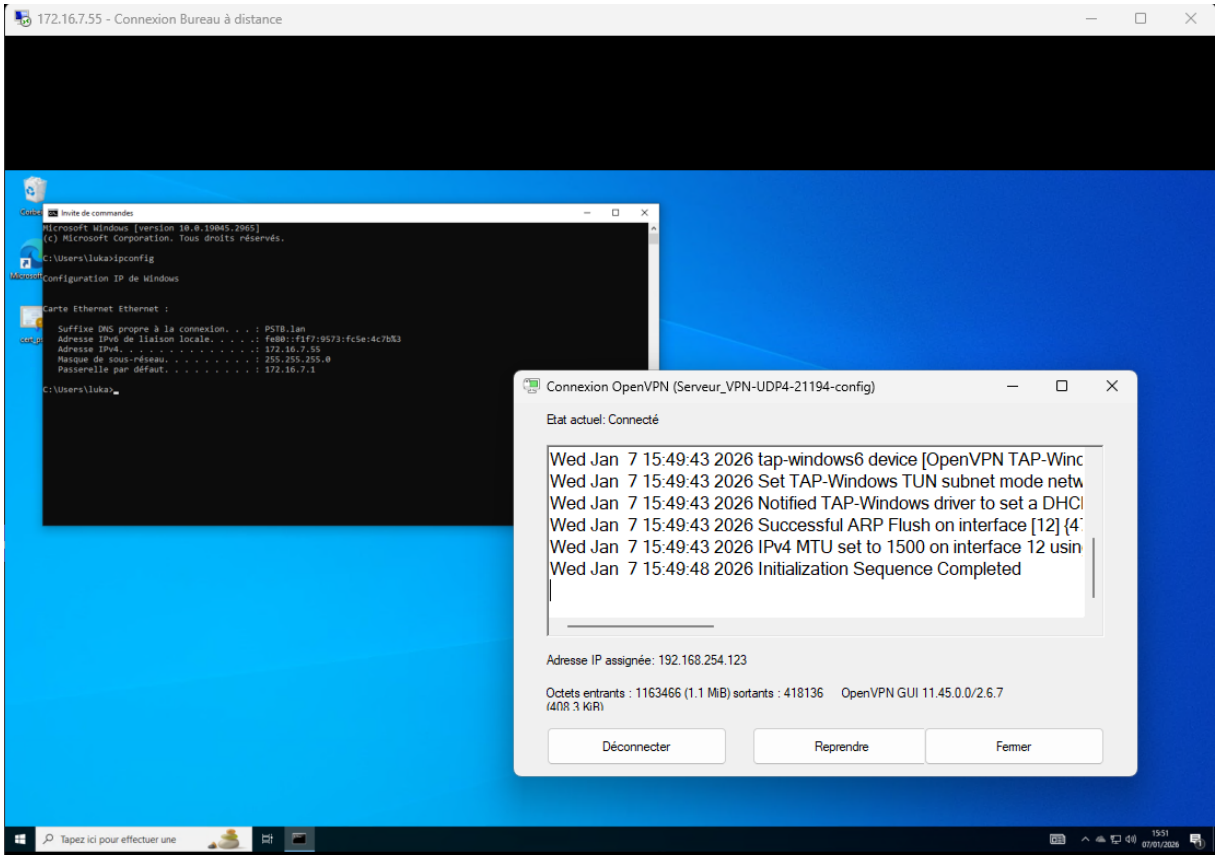
La capture d’écran montre la connexion VPN depuis un Android, où nous pouvons voir que le tunnel a bien été établi, avec le compte “d.cottenceau” et que l'IP de la machine dans le tunnel est : 192.168.254.118/28.

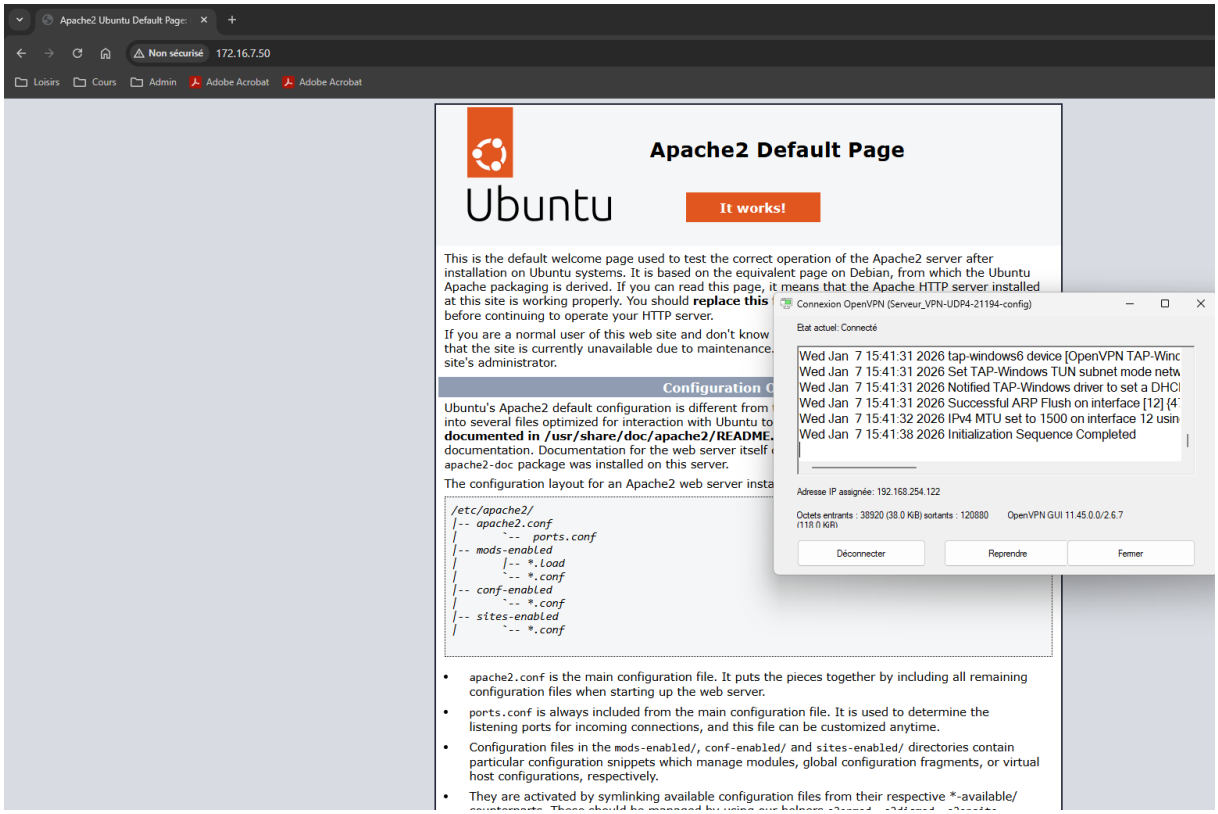
Le graphique nous montre également que le VPN est bien fonctionnel.

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

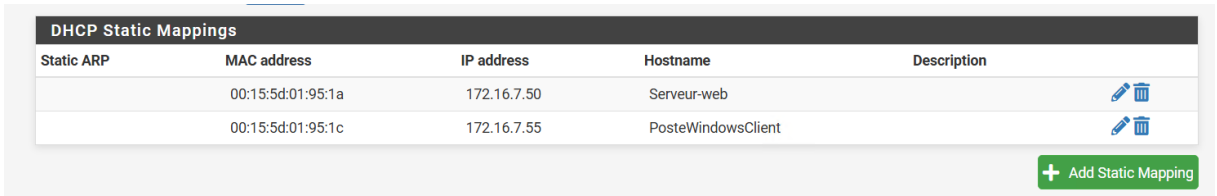




Sur les deux captures d'écran ci-dessus, nous pouvons voir que le poste Windows est bien disponible en RDP via le VPN.

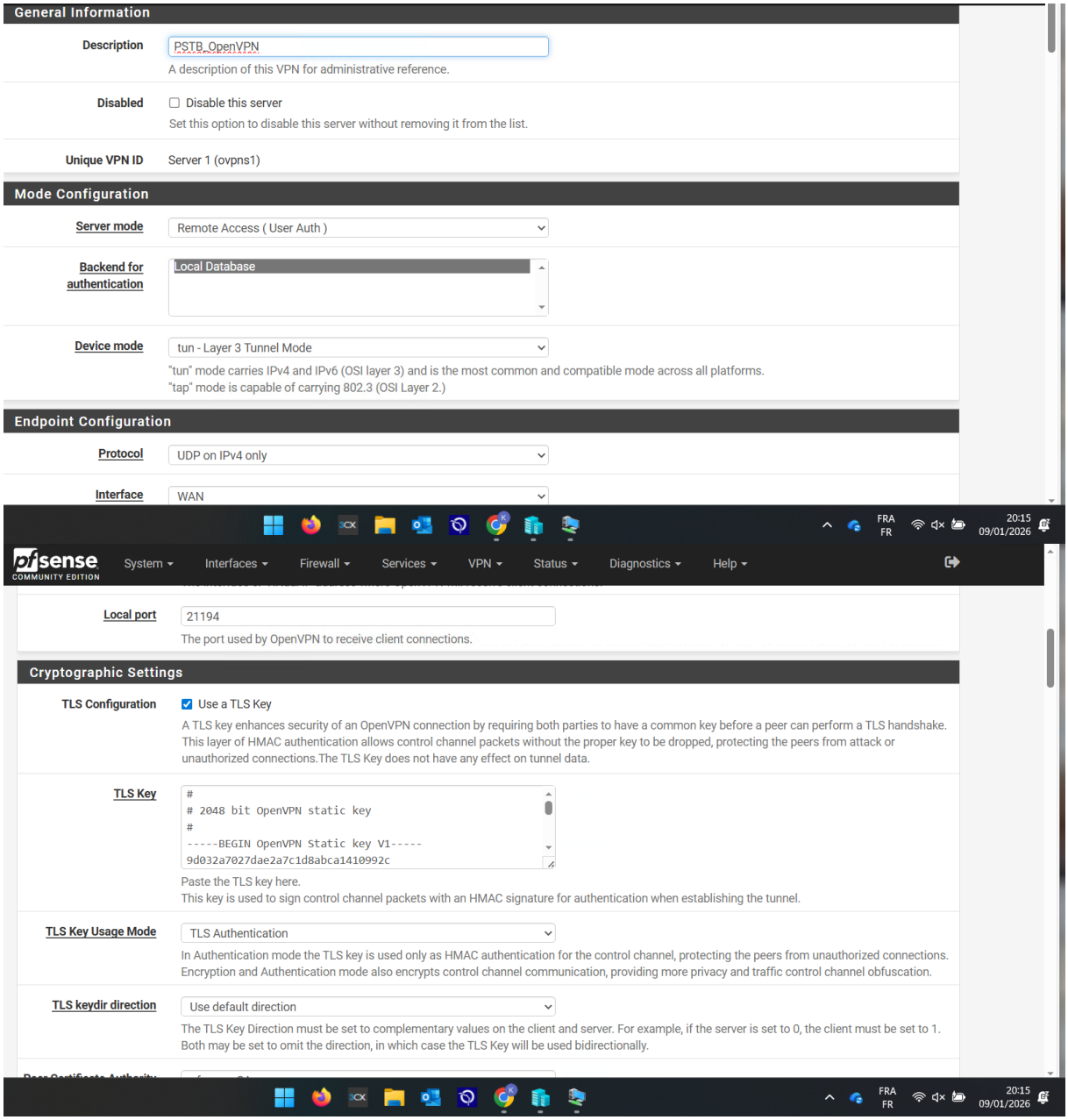
Nous pouvons voir l'IP de la machine en 172.16.7.55 ainsi que le serveur web (non personnalisé) qui est accessible grâce au VPN.

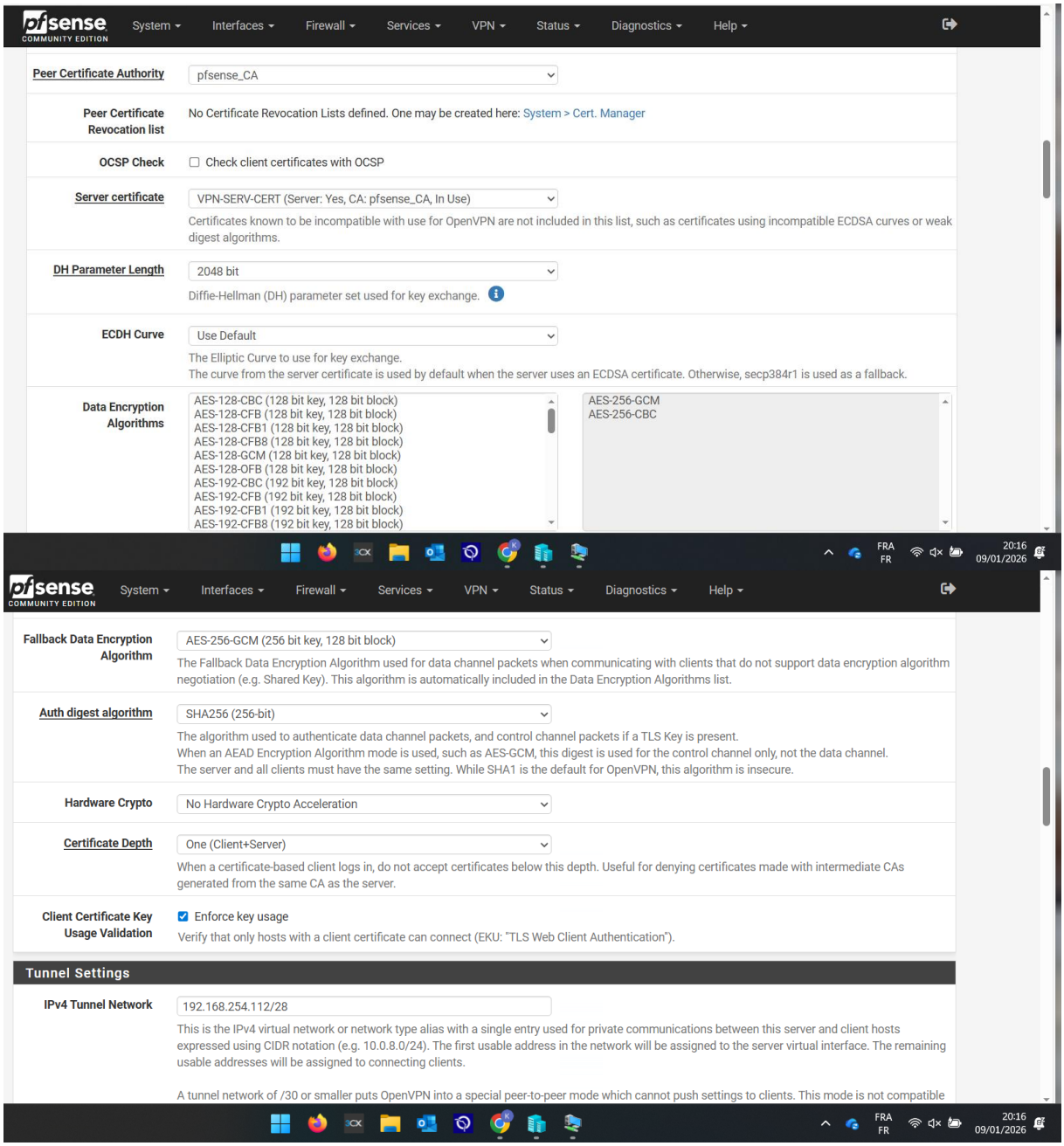
Nous voyons également son IP : 172.16.7.50, conformément à la réservation DHCP faite pour ces derniers.



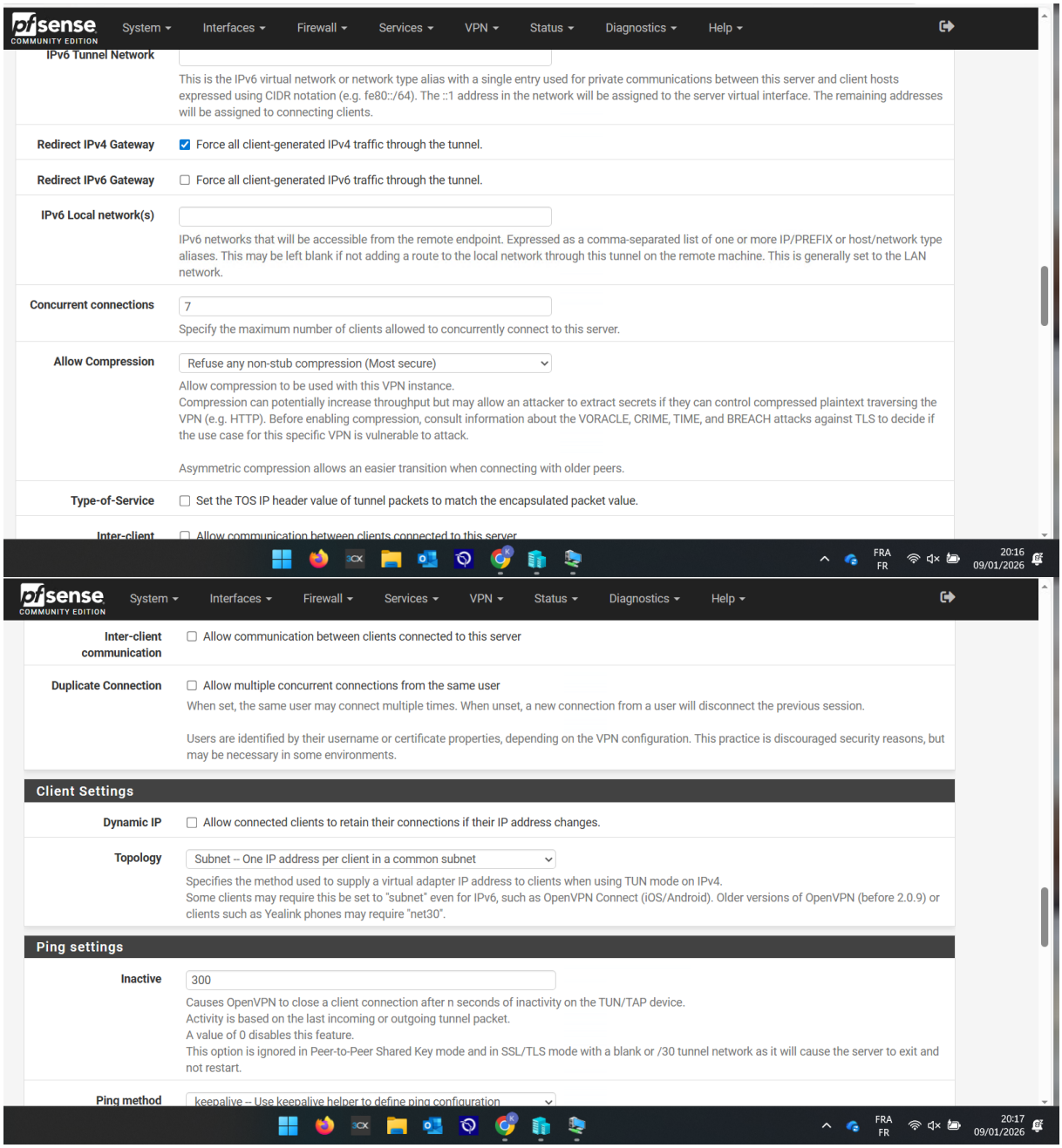
Annexes

1. Configuration serveur VPN entière

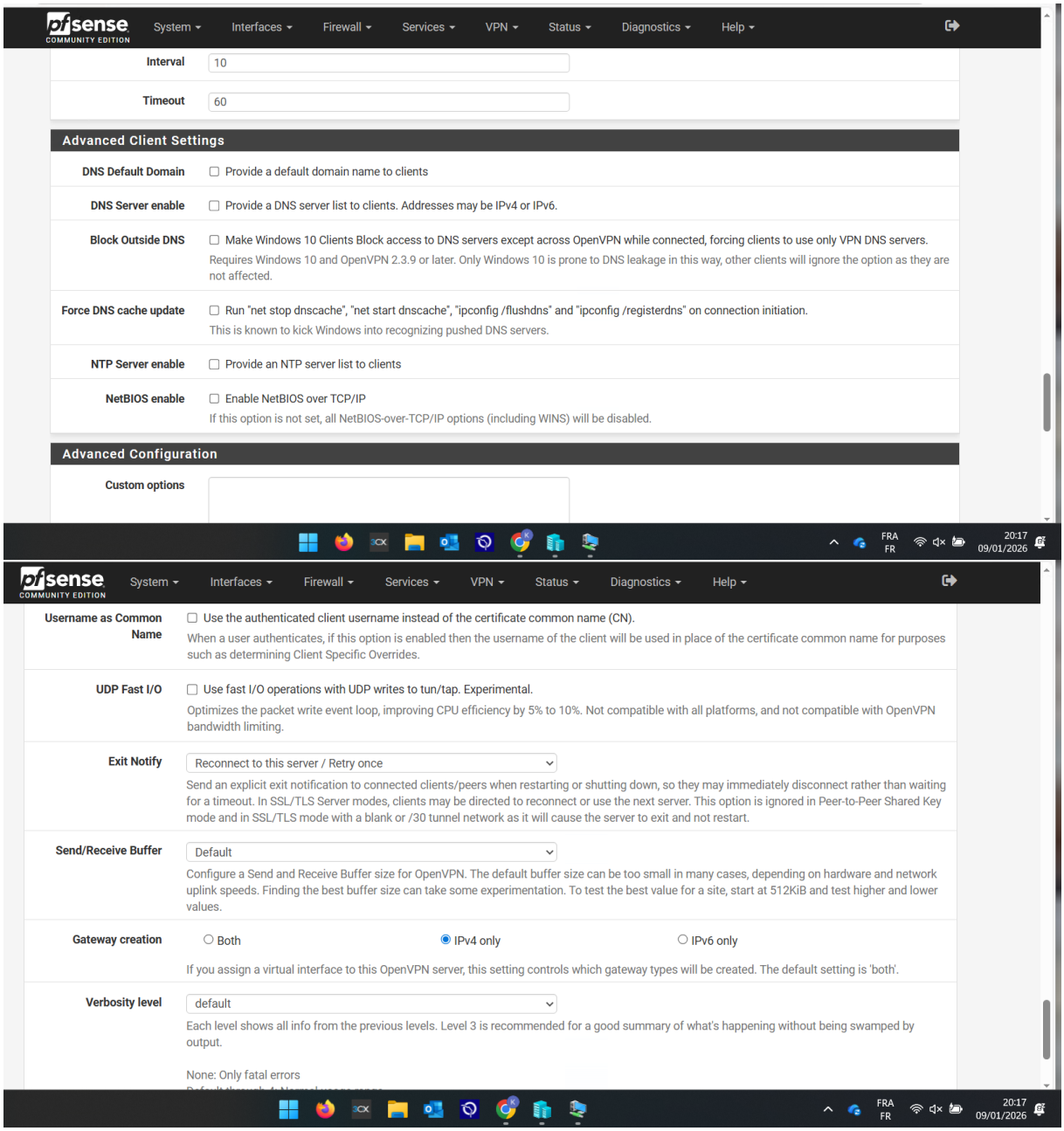



pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Peer Certificate Authority
pfsense_CA
Peer Certificate Revocation list
No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager
OCSP Check
Check client certificates with OCSP
Server 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
FRA
FR
20:16
09/01/2026

pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
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
FRA
FR
20:16
09/01/2026


pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
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
7
Specify the maximum number of clients allowed to concurrently connect to this server.
Allow Compression
Refuse any non-stub compression (Most secure)
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
FRA
FR
20:16
09/01/2026

pfsense COMMUNITY EDITION
System
Interfaces
Firewall
Services
VPN
Status
Diagnostics
Help
Inter-client communication
Allow communication between clients connected to this server
Duplicate Connection
Allow multiple concurrent connections from the same user
When set, the same user may connect multiple times. When unset, a new connection from a user will disconnect the previous session.
Users are identified by their username or certificate properties, depending on the VPN configuration. This practice is discouraged security reasons, but may be necessary in some environments.
Client Settings
Dynamic IP
Allow connected clients to retain their connections if their IP address changes.
Topology
Subnet -- One IP address per client in a common subnet
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
300
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
keepalive -- Use keepalive helper to define ping configuration
FRA
FR
20:17
09/01/2026



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.