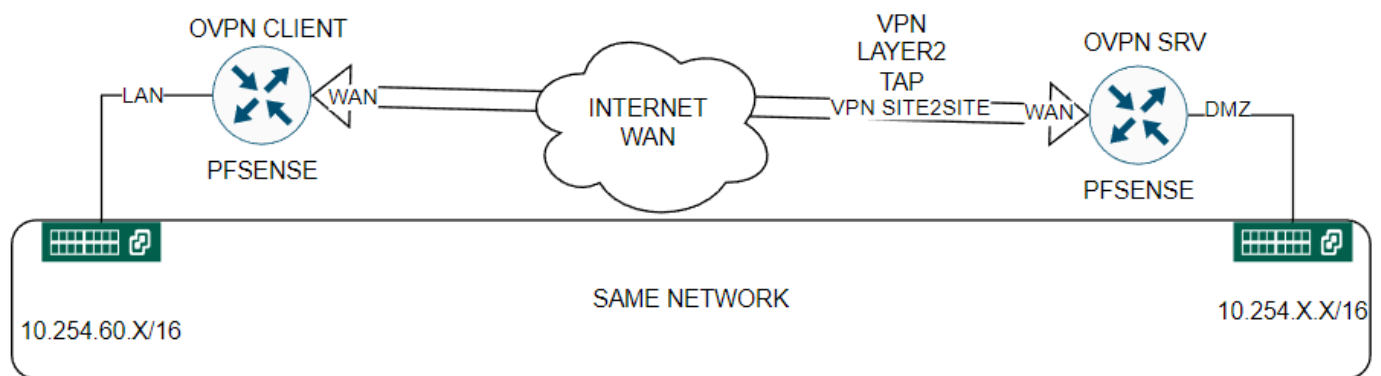
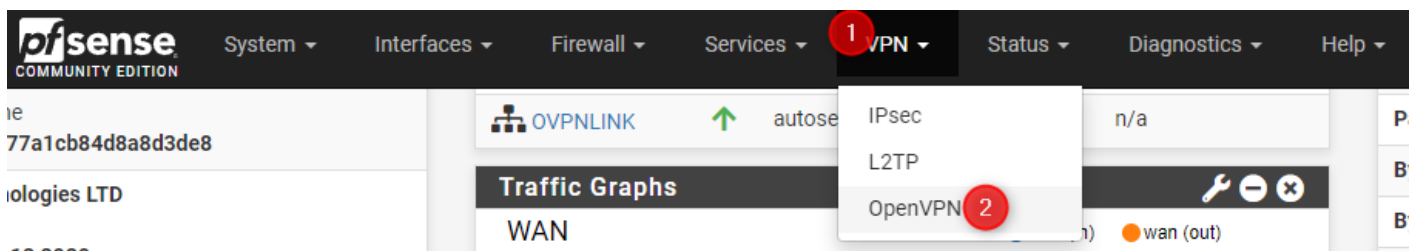


pfSense VPN site to site avec OPENVPN en L2 TAP en Shared KEY



PARTIE SERVEUR

Mise en place du serveur VPN sur pfSense



Configuration du openVPN "Server":

VPN / OpenVPN / Servers

Servers Clients Client Specific Overrides Wizards

OpenVPN Servers

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
+ Add					

Sélectionnez "tap - Layer 2 Tap Mode" dans le "Mode Configuration"

Modifier le "Server mode" en "Peer to Peer (Shared Key)"

(attention cette configuration ne sera plus supportée sur les futures versions il est recommandé un certificat)

Mode Configuration

Server mode Peer to Peer (Shared Key)

WARNING: OpenVPN has deprecated shared key mode as it does not meet current security standards. Shared key mode will be removed from future versions. Convert any existing shared key VPNs to TLS and do not configure any new shared key OpenVPN instances.

Device mode tap - Layer 2 Tap 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.)

Configuration du port utilisé pour le VPN dans "Endpoint Configuration"

(Il est recommandé de modifier le port par défaut)

Endpoint Configuration

Protocol UDP on IPv4 only

Interface WAN
 The interface or Virtual IP address where OpenVPN will receive client connections.

Local port 61194
 The port used by OpenVPN to receive client connections.

Configuration "IPv4 Tunnel Network" du "Tunnel Settings"

(ce réseau va être utilisé uniquement pour openVPN et n'aura pas d'impact sur le réseau)

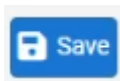
Tunnel Settings

IPv4 Tunnel Network 10.0.9.0/29

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 with several options, including Exit Notify, and Inactive.

Pouvez sauvegarder la configuration



Une fois sauvegardée ça nous donne :

VPN / OpenVPN / Servers

Servers Clients Client Specific Overrides Wizards

OpenVPN Servers

Interface	Protocol / Port	Tunnel Network	Mode / Crypto	Description	Actions
WAN	UDP4 / 61194 (TAP)	10.0.9.0/29	Mode: Peer to Peer (Shared Key) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256	OVPN-HETLINK	

+ Add

WARNING: OpenVPN has deprecated shared key mode as it does not meet current security standards. Shared key mode will be removed from future versions. Convert any existing shared key VPNs to TLS and do not configure any new shared key OpenVPN instances.

Configuration du openVPN "Client Specific Overrides":

VPN / OpenVPN / Client Specific Overrides

Servers Clients Client Specific Overrides Wizards

CSC Overrides

Disabled	Common Name	Description	Actions
----------	-------------	-------------	---------

+ Add

Donner un nom "VPN" dans "Commun Name" dans "Override Configuration"

Override Configuration

Common Name

VPN

Enter the X.509 common name for the client certificate, or the username for VPNs utilizing password authentication. This match is case sensitive. Enter "DEFAULT" to override default client behavior.

Connection blocking

☐ Block this client connection based on its common name.

Prevents the client from connecting to this server. Do not use this option to permanently disable a client due to a compromised key or password. Use a CRL (certificate revocation list) instead.

Server List

Select the servers that will utilize this override. When no servers are selected, the override will apply to all servers.

Configuration "IPv4 Tunnel Network" du "Tunnel Settings"

Pour "IPv4 Tunnel Network" mettez l'adresse IP de votre réseau local qui sera lié à votre VPN

(pour le reste vous pouvez le laisser comme dans le tutoriel ça n'aura pas d'impact sur le réseau)

Tunnel Settings

IPv4 Tunnel Network

10.254.0.0/16 **VOTRE RESEAU LOCAL**

The virtual IPv4 network or network type alias with a single entry used for private communications between this client and the server expressed using CIDR (e.g. 10.0.8.5/24).

With subnet topology, enter the client IP address and the subnet mask must match the IPv4 Tunnel Network on the server.

With net30 topology, the first network address of the /30 is assumed to be the server address and the second network address will be assigned to the client.

IPv6 Tunnel Network

The virtual IPv6 network or network type alias with a single entry used for private communications between this client and the server expressed using prefix (e.g. 2001:db9:1:1::100/64).

Enter the client IPv6 address and prefix. The prefix must match the IPv6 Tunnel Network prefix on the server.

IPv4 Local Network/s

10.2.2.0/24

These are the IPv4 server-side networks that will be accessible from this particular client. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases.

NOTE: Networks do not need to be specified here if they have already been defined on the main server configuration.

IPv6 Local Network/s

These are the IPv6 server-side networks that will be accessible from this particular client. Expressed as a comma-separated list of one or more IP/PREFIX networks.

NOTE: Networks do not need to be specified here if they have already been defined on the main server configuration.

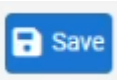
IPv4 Remote Network/s

10.3.3.0/24

These are the IPv4 client-side networks that will be routed to this client specifically using iroute, so that a site-to-site VPN can be established. Expressed as a comma-separated list of one or more CIDR ranges. May be left blank if there are no client-side networks to be routed.

NOTE: Remember to add these subnets to the IPv4 Remote Networks list on the corresponding OpenVPN server settings.

Pouvez sauvegarder la configuration



Une fois sauvegardée ça nous donne :

VPN / OpenVPN / Client Specific Overrides

Servers

Clients

Client Specific Overrides

Wizards

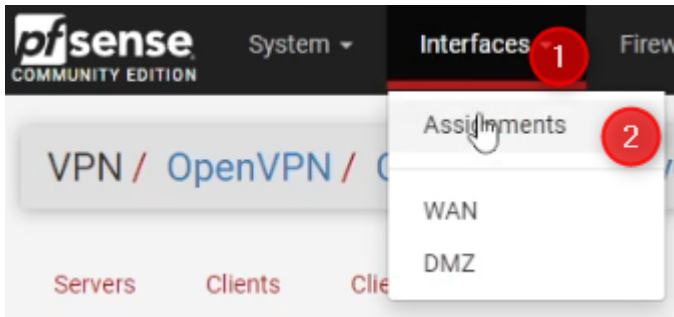
CSC Overrides

Disabled	Common Name	Description	Actions
No	VPN		

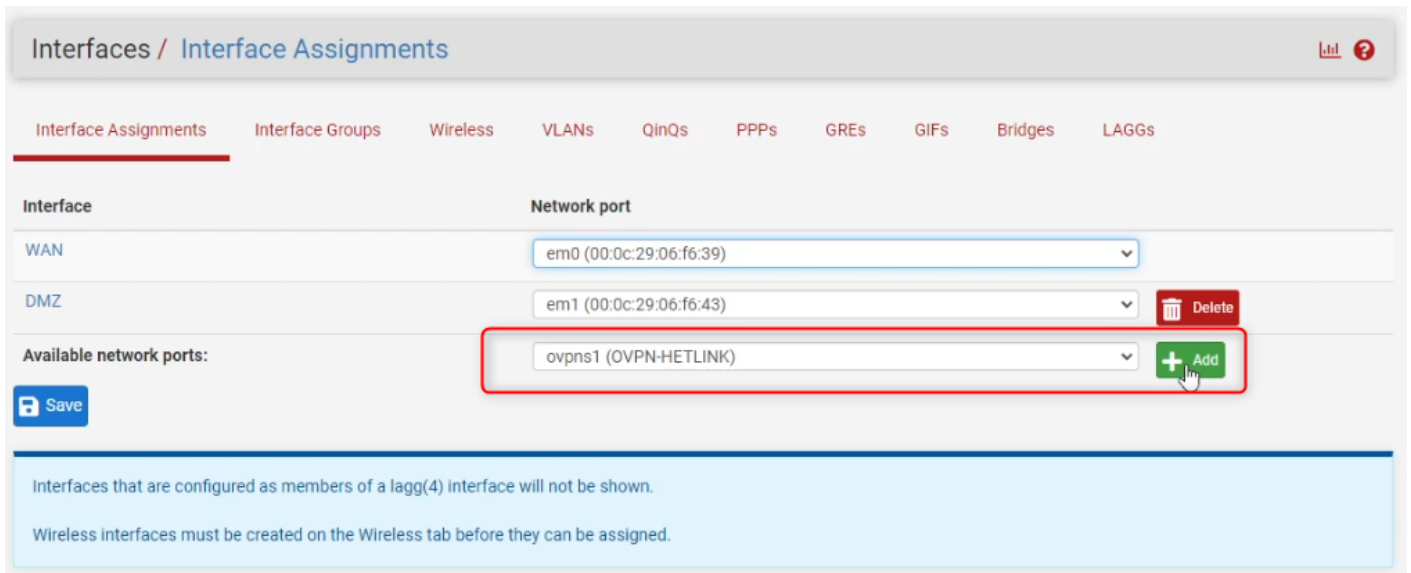
+ Add

Configurations des interfaces réseau

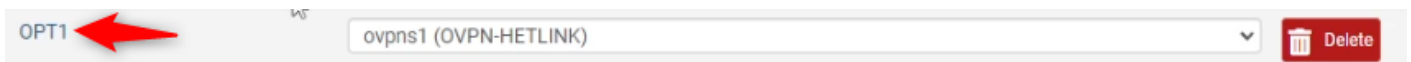
Allez dans "Interfaces" et ensuite dans "Assignments"



Ajouter la nouvelle interface disponible liée au VPN "ovpns1"



Aller sur la nouvelle interface "OPT1"



Activer l'interface via "Enable interface" et ajouter une description (le nom)

Interfaces / OPT1 (ovpn1)

General Configuration

Enable ☒ Enable interface

Description
Enter a description (name) for the interface here.

IPv4/IPv6 Configuration This interface type does not support manual address configuration on this page.

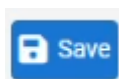
MAC Address
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

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/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex
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.

Pouvez sauvegarder la configuration



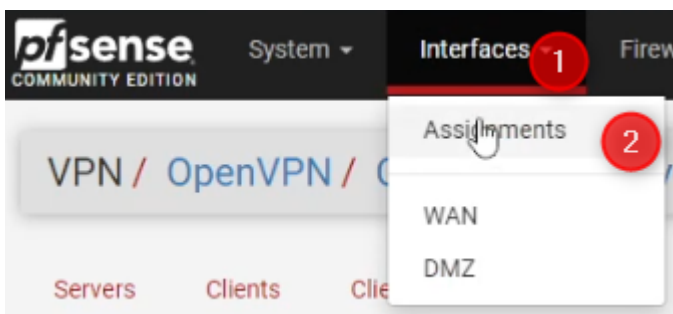
Appliquer les changements

The OVPNLINK configuration has been changed.
The changes must be applied to take effect.
Don't forget to adjust the DHCP Server range if needed after applying.

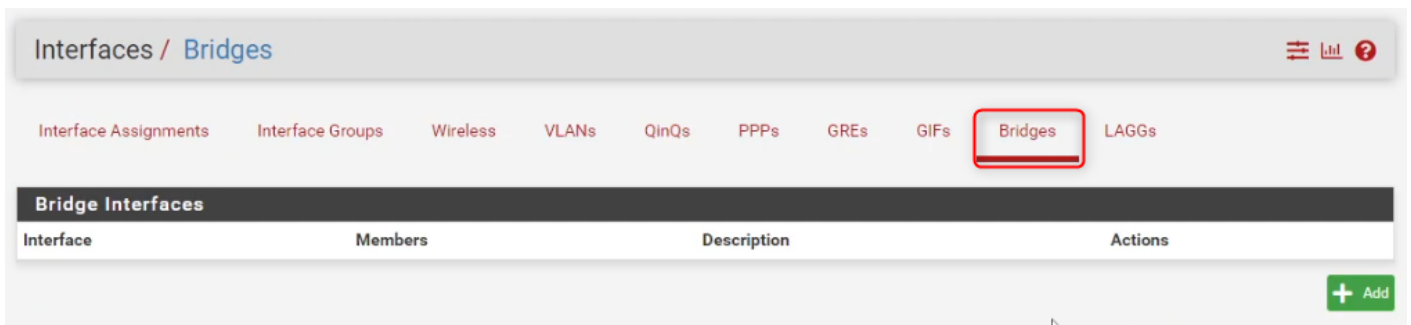
☒ Apply Changes

The changes have been applied successfully.

Retourner dans "Interfaces" et ensuite dans "Assignments"

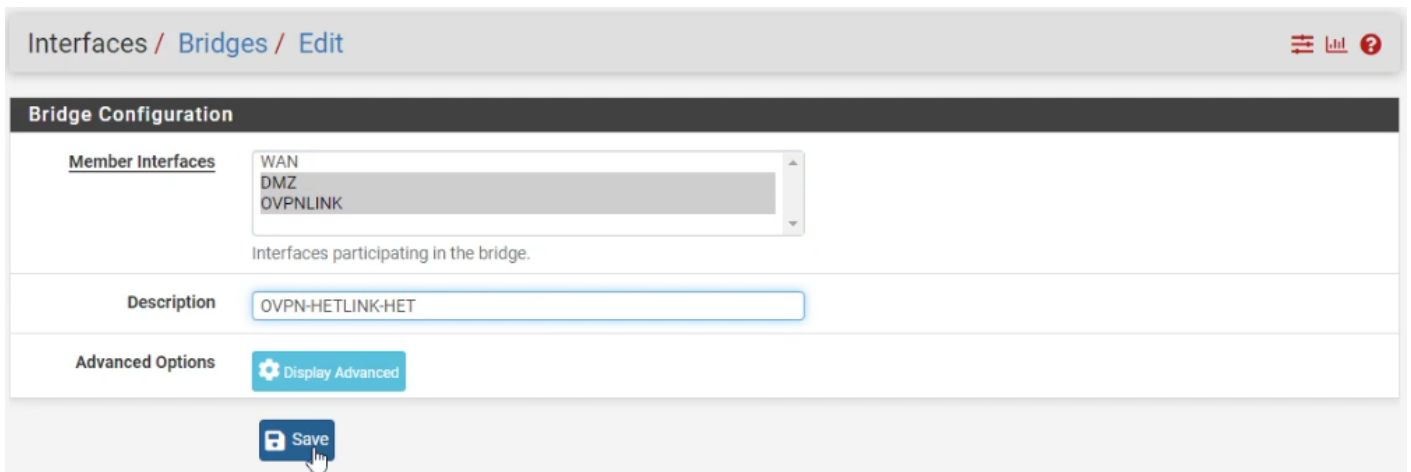


Allez dans la partie "Bridges"

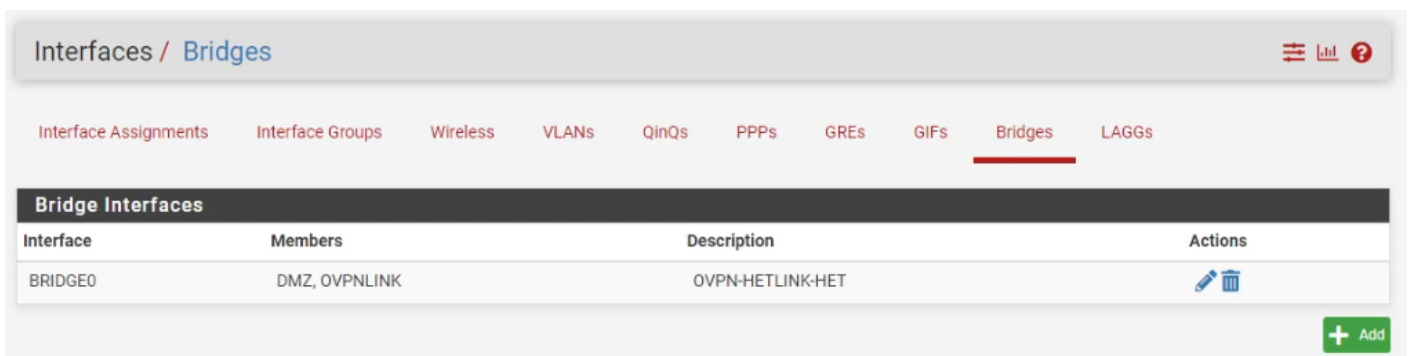


Créer un "Bridges" entre l'interface du réseau local et l'interface du VPN

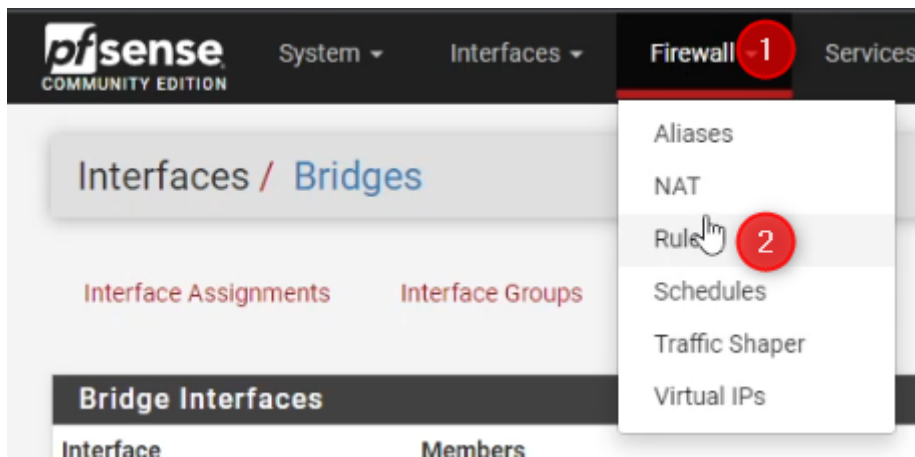
(pour cela vous avez juste à sélectionner les deux interfaces réseaux)



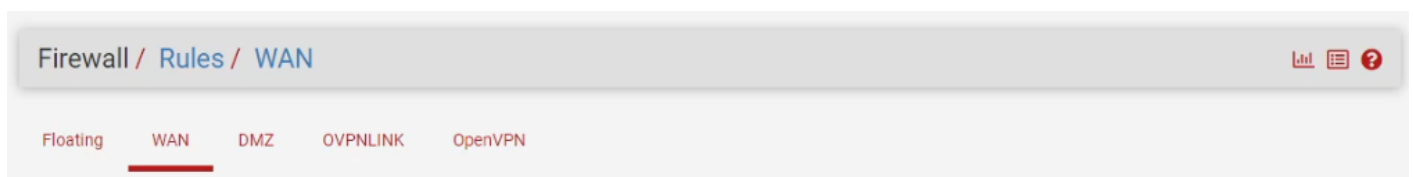
Ce qui nous donne cela:



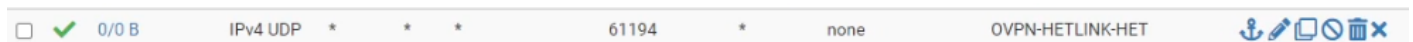
Configuration des règles de "Firewall" dans "Firewall" et ensuite dans "Rules"



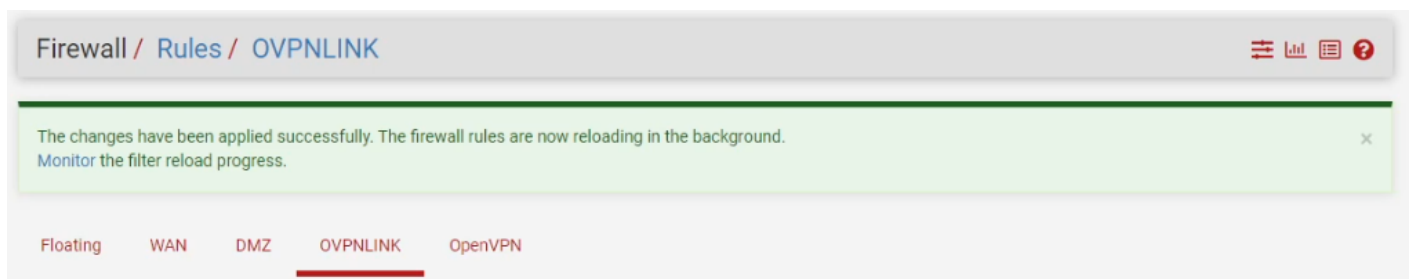
WAN:



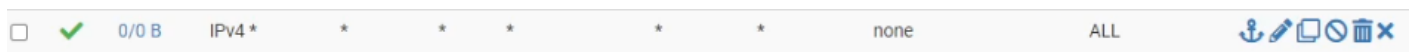
Ajout de la règle pour faire passer le trafic du VPN sur Internet (WAN)



OVPNLINK:



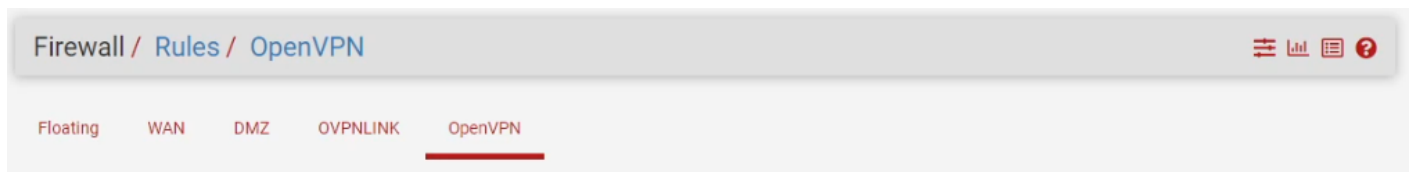
Ajout de la règle pour faire passer le trafic entre le VPN et le réseau



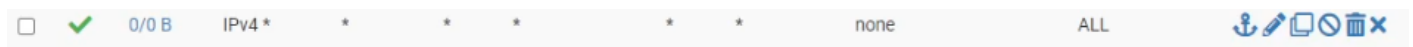
Ajout de la règle pour bloquer le trafic du DHCP sur le réseau via le VPN



OpenVPN:

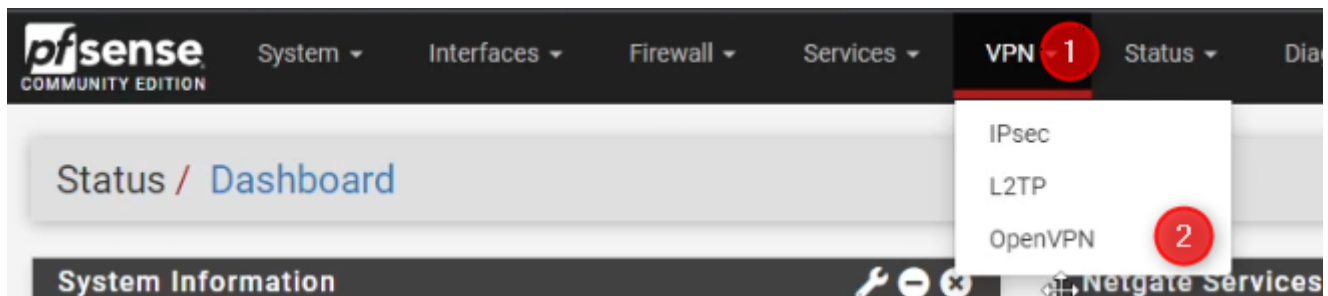


Ajout de la règle pour faire passer le trafic entre le VPN et le réseau

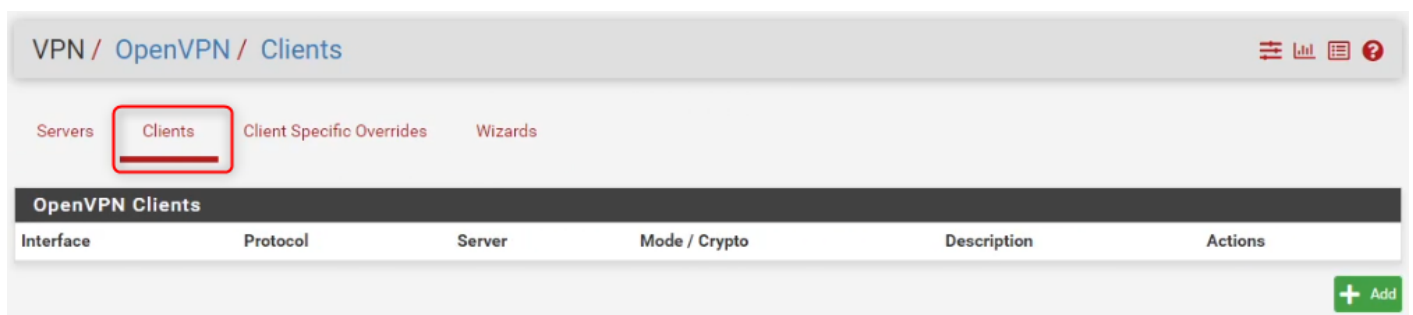


PARTIE CLIENT

Mise en place du client VPN sur pfSense



Configuration du openVPN "Clients":



Sélectionnez "tap - Layer 2 Tap Mode" dans le "Mode Configuration"

Modifier le "Server mode" en "Peer to Peer (Shared Key)"

(attention cette configuration ne sera plus supportée sur les futures versions il est recommandé un certificat)

Mode Configuration	
Server mode	Peer to Peer (Shared Key)
WARNING:	OpenVPN has deprecated shared key mode as it does not meet current security standards. Shared key mode will be removed from future versions. Convert any existing shared key VPNs to TLS and do not configure any new shared key OpenVPN instances.
Device mode	tap - Layer 2 Tap 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.)

Configuration du port utilisé pour le VPN dans "Endpoint Configuration" et dans "Server host or address" mettait l'adresse IP de votre serveur openVPN.

(l'adresse IP public de votre routeur pfSense configurait auparavant)

Endpoint Configuration	
Protocol	UDP on IPv4 only
Interface	WAN The interface used by the firewall to originate this OpenVPN client connection
Local port	61194 Set this option to bind to a specific port. Leave this blank or enter 0 for a random dynamic port.
Server host or address	IP PUBLIC DE VOTRE SRV OPENVPN The IP address or hostname of the OpenVPN server.
Server port	61194 The port used by the server to receive client connections.
Proxy host or address	 The address for an HTTP Proxy this client can use to connect to a remote server. TCP must be used for the client and server protocol.
Proxy port	
Proxy Authentication	none The type of authentication used by the proxy server.

Ajouter la clé pré partagée qui a été générée sur le serveur openVPN

Mettez la dans "Cryptographic Settings" en suite "Shared Key"

Cryptographic Settings

Auto generate

☐ Automatically generate a shared key

Shared Key

2048 bit OpenVPN static key

-----BEGIN OpenVPN Static key V1-----
a0b765782cf9e2e8820c77458eb66664

Paste the shared key here

Data Encryption Algorithms

ARIA-128-CBC (128 bit key, 128 bit block)
ARIA-128-CFB (128 bit key, 128 bit block)
ARIA-128-CFB1 (128 bit key, 128 bit block)
ARIA-128-CFB8 (128 bit key, 128 bit block)
ARIA-128-GCM (128 bit key, 128 bit block)
ARIA-128-OFB (128 bit key, 128 bit block)
ARIA-192-CBC (192 bit key, 128 bit block)
ARIA-192-CFB (192 bit key, 128 bit block)
ARIA-192-CFB1 (192 bit key, 128 bit block)
ARIA-192-CFB8 (192 bit key, 128 bit block)
ARIA-192-CFR8 (192 bit key, 128 bit block)

Available Data Encryption Algorithms
Click to add or remove an algorithm from the list

AES-256-GCM
AES-128-GCM
CHACHA20-POLY1305

Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list

The order of the selected Data Encryption Algorithms is respected by OpenVPN. This list is ignored in Shared Key mode.

Fallback Data Encryption Algorithm

AES-256-CBC (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. Set this to the same value as the server. While SHA1 is the default for OpenVPN, this algorithm is insecure.

Hardware Crypto

No Hardware Crypto Acceleration

Configuration "IPv4 Tunnel Network" du "Tunnel Settings"

Pour "IPv4 Tunnel Network" mettez l'adresse IP de votre réseau local qui sera lié à votre VPN

(pour le reste vous pouvez le laisser comme dans le tutoriel ça n'aura pas d'impact sur le réseau)

Tunnel Settings

IPv4 Tunnel Network

10.0.9.0/29

This is the IPv4 virtual network or network type alias with a single entry used for private communications between this client and the server expressed using CIDR notation (e.g. 10.0.8.0/24).

This should be left blank in most cases as servers typically provide addresses to clients dynamically.

The second usable address in this network will be assigned to the client virtual interface. Ensure the Topology setting matches the server when using SSL/TLS and TUN modes or the interface address may not be configured properly. A tunnel network of /30 or smaller puts OpenVPN into a special peer-to-peer mode which cannot receive settings from the server dynamically. This mode is not compatible with several options, including Exit Notify, and Inactive.

IPv6 Tunnel Network

This is the IPv6 virtual network or network alias with a single entry used for private communications between this client and the server expressed using CIDR notation (e.g. fe80::/64). When set static using this field, the ::2 address in the network will be assigned to the client virtual interface. Leave blank if the server is capable of providing addresses to clients.

IPv4 Remote network(s)

IPv4 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more CIDR ranges or host/network type aliases. If this is a site-to-site VPN, enter the remote LAN/s here. May be left blank for non site-to-site VPN.

IPv6 Remote network(s)

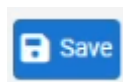
These are the IPv6 networks that will be routed through the tunnel, so that a site-to-site VPN can be established without manually changing the routing tables. Expressed as a comma-separated list of one or more IP/PREFIX or host/network type aliases. If this is a site-to-site VPN, enter the remote LAN/s here. May be left blank for non site-to-site VPN.

Limit outgoing bandwidth

Between 100 and 100,000,000 bytes/sec

Maximum outgoing bandwidth for this tunnel. Leave empty for no limit. The input value has to be something between 100 bytes/sec and 100 Mbytes/sec (entered as bytes per second). Not compatible with UDP Fast I/O.

Pouvez sauvegarder la configuration



Une fois sauvegardée ça nous donne :

VPN / OpenVPN / Clients

Servers

Clients

Client Specific Overrides

Wizards

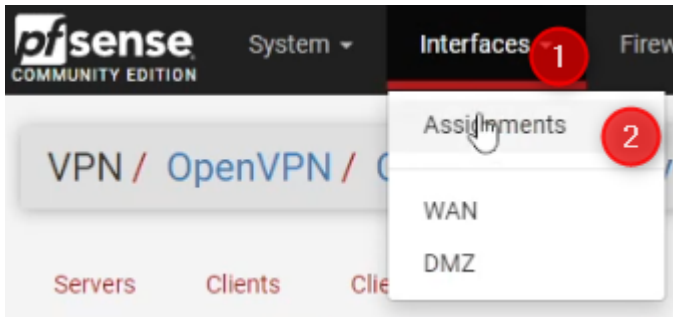
OpenVPN Clients					
Interface	Protocol	Server	Mode / Crypto	Description	Actions
WAN	UDP4 (TAP)	IP PUBLIC SRV OPENVPN :61194	Mode: Peer to Peer (Shared Key) Data Ciphers: AES-256-GCM, AES-128-GCM, CHACHA20-POLY1305, AES-256-CBC Digest: SHA256	OVPN-HETLINK	

+ Add

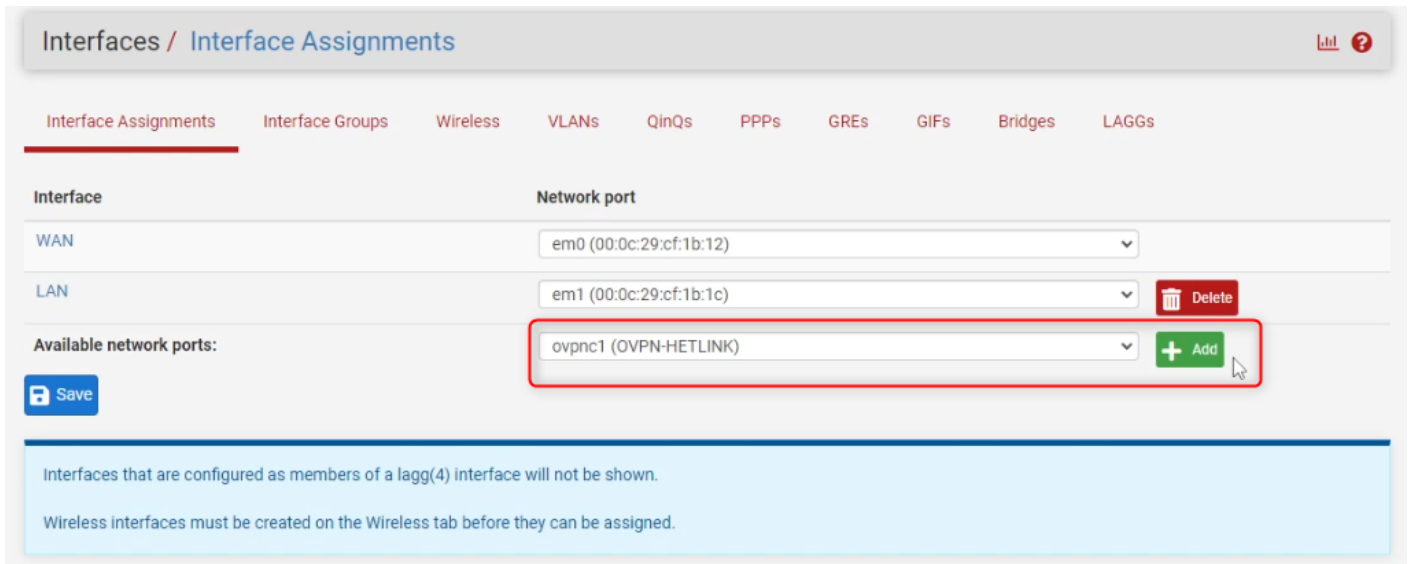
WARNING: OpenVPN has deprecated shared key mode as it does not meet current security standards. Shared key mode will be removed from future versions. Convert any existing shared key VPNs to TLS and do not configure any new shared key OpenVPN instances.

Configurations des interfaces réseau

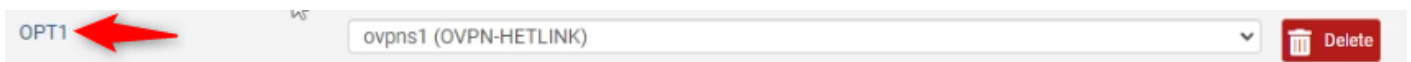
Allez dans "Interfaces" et ensuite dans "Assignments"



Ajouter la nouvelle interface disponible liée au VPN "ovpns1"



Aller sur la nouvelle interface "OPT1"



Activer l'interface via "Enable interface" et ajouter une description (le nom)

Interfaces / OPT1 (ovpn1)

General Configuration

Enable ☒ Enable interface

Description
Enter a description (name) for the interface here.

IPv4/IPv6 Configuration This interface type does not support manual address configuration on this page.

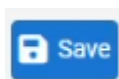
MAC Address
This field can be used to modify ("spoof") the MAC address of this interface.
Enter a MAC address in the following format: xx:xx:xx:xx:xx:xx or leave blank.

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/IPv4 header size) and minus 60 for IPv6 (TCP/IPv6 header size) will be in effect.

Speed and Duplex
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.

Pouvez sauvegarder la configuration



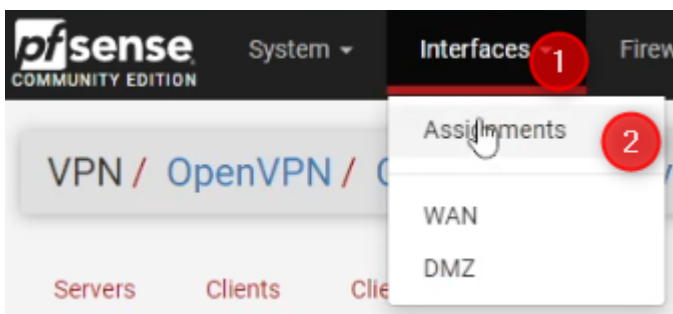
Appliquer les changements

The OVPNLINK configuration has been changed.
The changes must be applied to take effect.
Don't forget to adjust the DHCP Server range if needed after applying.

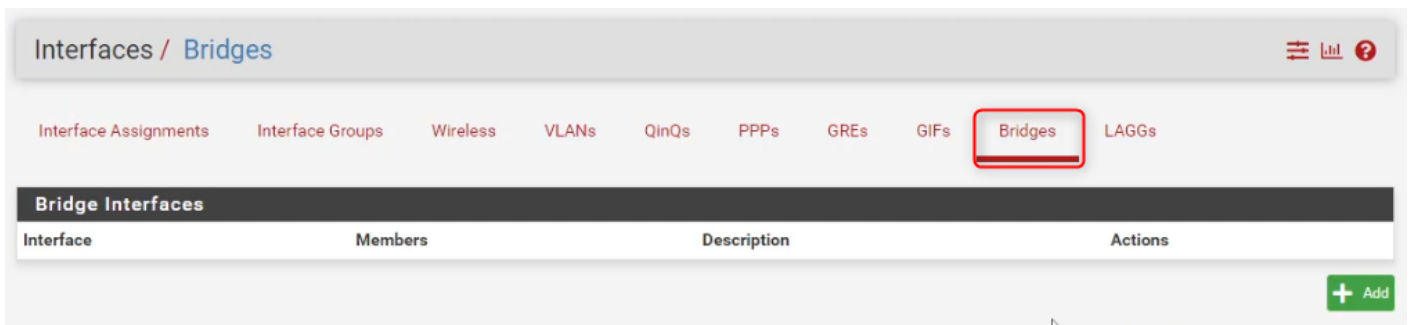
☒ Apply Changes

The changes have been applied successfully.

Retourner dans "Interfaces" et ensuite dans "Assignments"

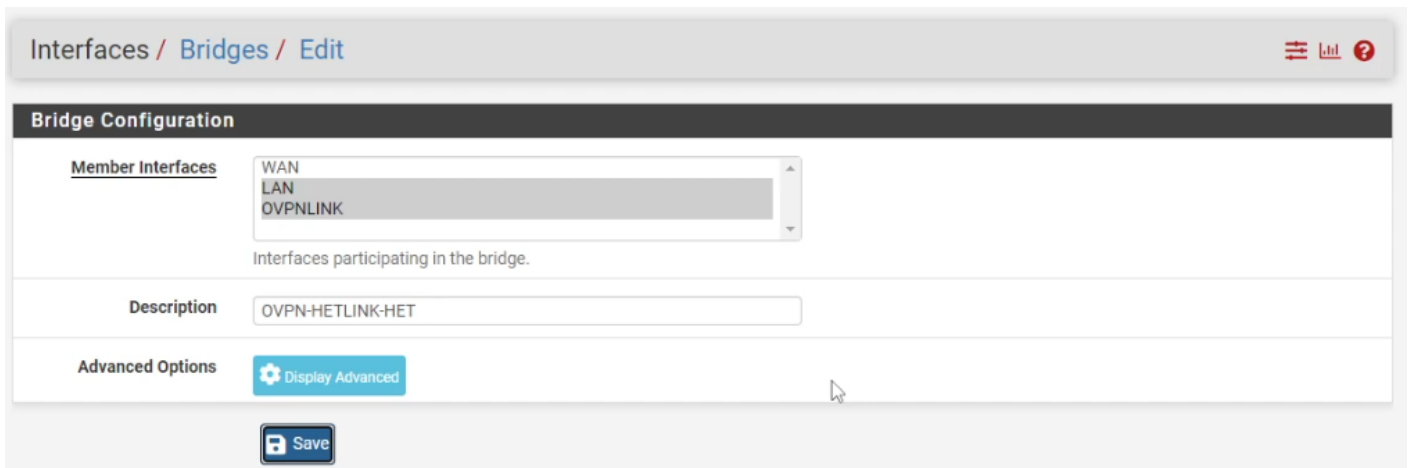


Allez dans la partie "Bridges"

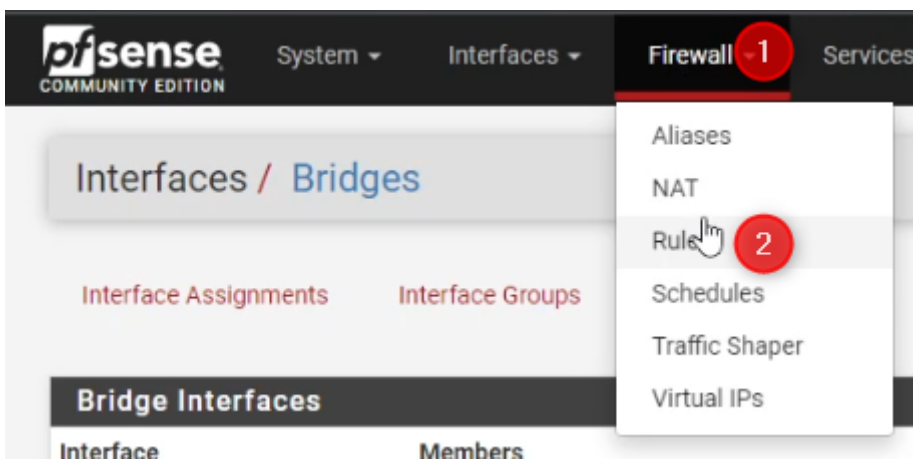


Créer un "Bridges" entre l'interface du réseau local et l'interface du VPN

(pour cela vous avez juste à sélectionner les deux interfaces réseaux)



Configuration des règles de "Firewall" dans "Firewall" et ensuite dans "Rules"



WAN:

Firewall / Rules / WAN

Floating

WAN

DMZ

OVPNLINK

OpenVPN

Ajout de la règle pour faire passer le trafic du VPN sur Internet (WAN)

☐
✓
0/0 B
IPv4 UDP
*
*
*
61194
*
none
OVPN-HETLINK

OVPNLINK:

Firewall / Rules / OVPNLINK

Floating

WAN

DMZ

OVPNLINK

OpenVPN

The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

Ajout de la règle pour faire passer le trafic entre le VPN et le réseau

☐
✓
0/0 B
IPv4 *
*
*
*
*
*
none
ALL

Ajout de la règle pour bloquer le trafic du DHCP sur le réseau via le VPN

☐
✗
0/0 B
IPv4 UDP
*
*
*
67 - 68
*
none
DHCP

OpenVPN:

Firewall / Rules / OpenVPN

Floating

WAN

DMZ

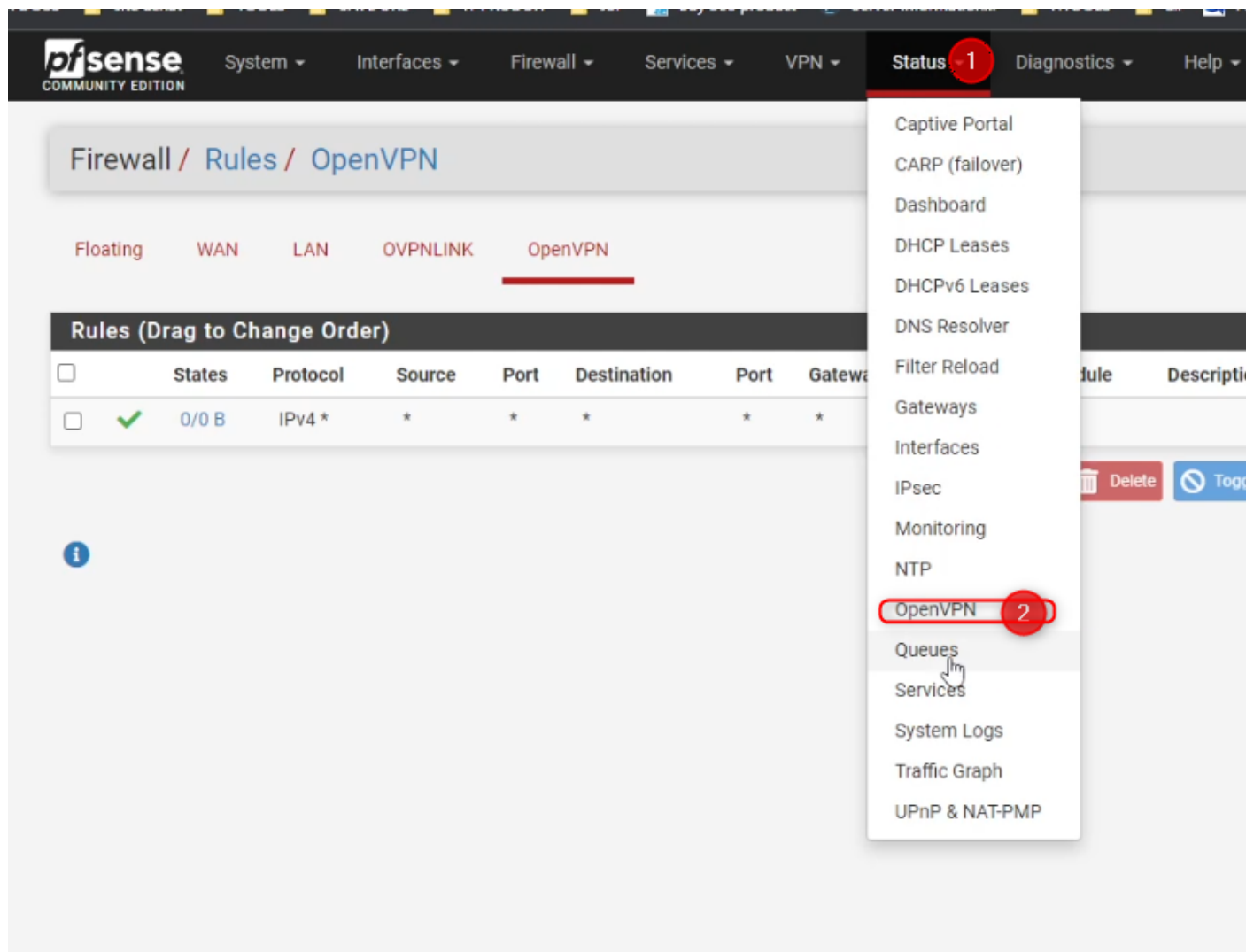
OVPNLINK

OpenVPN

Ajout de la règle pour faire passer le trafic entre le VPN et le réseau

☐
✓
0/0 B
IPv4 *
*
*
*
*
*
none
ALL

Contrôle de la connexion du VPN entre les deux routeurs



DEPUIS LE SERVEUR

Peer to Peer Server Instance Statistics							
Name	Status	Last Change	Virtual Address	Remote Host	Bytes Sent	Bytes Received	Service
ovpns1 OVPN-HETLINK UDP4:61194	Connected (Success)	Sun Oct 1 0:58:57 2023	10.0.9.1		37 KiB	3 KiB	✓ ↺ ↻

DEPUIS LE CLIENT

Client Instance Statistics								
Name	Status	Last Change	Local Address	Virtual Address	Remote Host	Bytes Sent	Bytes Received	Service
ovpnc1 OVPN-HETLINK UDP4:61194	Connected (Success)	Sun Oct 1 0:58:58 2023	10.0.6.254:61194	10.0.9.2	:61194	3 KiB	36 KiB	✓ ↺ ↻

Pour continuer le test nous pouvons effectuer un "ping" entre les deux sites

The screenshot shows the pfSense web interface. The top navigation bar includes links for System, Interfaces, Firewall, Services, VPN, Status, and Diagnostics. The Diagnostics menu is open, showing a list of diagnostic tools. The 'Ping' option is highlighted with a red box and a red circle containing the number 2. The background shows the 'Peer to Peer Server Instance Statistics' table with one entry for 'ovpns1'.

Peer to Peer Server Instance Statistics

Name	Status	Last Change	Virtual Address	Real Address
ovpns1 OVPN-HETLINK UDP4:61194	Connected (Success)	Sun Oct 1 0:58:57 2023	10.0.9.1	

Diagnostics Menu:

- ARP Table
- Authentication
- Backup & Restore
- Command Prompt
- DNS Lookup
- Edit File
- Factory Defaults
- Halt System
- iperf
- Limiter Info
- NDP Table
- Packet Capture
- pfinfo
- pfTop
- Ping**
- Reboot
- Routes
- S.M.A.R.T. Status
- Sockets
- States
- States Summary
- System Activity
- Tables
- Test Port
- Traceroute

Ping

Hostname 10.254.60.254**IP Protocol** IPv4**Source address** Automatically selected (default)

Select source address for the ping.

Maximum number of pings 3

Select the maximum number of pings.

Seconds between pings 1

Select the number of seconds to wait between pings.



Results

```
PING 10.254.60.254 (10.254.60.254): 56 data bytes
64 bytes from 10.254.60.254: icmp_seq=0 ttl=64 time=130.150 ms
64 bytes from 10.254.60.254: icmp_seq=1 ttl=64 time=44.381 ms
64 bytes from 10.254.60.254: icmp_seq=2 ttl=64 time=41.817 ms

--- 10.254.60.254 ping statistics ---
3 packets transmitted, 3 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 41.817/72.116/130.150/41.049 ms
```

Revision #3

Created 8 October 2023 15:49:32 by Admin

Updated 8 October 2023 17:58:00 by Admin