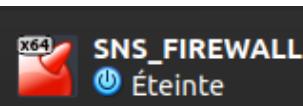


Dans ce tp, on va utiliser le firewall stormshield :



On va la cloner :



On va faire la config dans virtualbox (faire juste les réseaux interne, pas les ip):

INTERFACE	RÉSEAU VIRTUALBOX	NOM DU RÉSEAU	ADRESSAGE IP
1ère interface	Réseau interne	NUAGE-OUT	82.10.20.1/30
2ème interface	Réseau interne	LAN-TOULOUSE	192.168.50.254/24
3ème interface	Réseau interne	DMZ-TOULOUSE	172.16.10.254/24

FIREWALL-MARSEILLE

INTERFACE	RÉSEAU VIRTUALBOX	NOM DU RÉSEAU	ADRESSAGE IP
1ère interface	Réseau interne	NUAGE-OUT	82.10.20.2/30
2ème interface	Réseau interne	LAN-MARSEILLE	192.168.80.254
3ème interface	Réseau interne	DMZ-MARSEILLE	172.16.20.254/24

CLIENT-TOULOUSE

INTERFACE	RÉSEAU VIRTUALBOX	NOM DU RÉSEAU	ADRESSAGE IP
1ère interface	Réseau interne	LAN-TOULOUSE	192.168.50.1/24

CLIENT-MARSEILLE

INTERFACE	RÉSEAU VIRTUALBOX	NOM DU RÉSEAU	ADRESSAGE IP
1ère interface	Réseau interne	LAN-MARSEILLE	192.168.80.1/24

Mettre les 4 machines dans le bon réseau interne sans changer l'adresse ip

Dans un premier temps, le firewall est livré en configuration d'usine dans un bridge d'adresse IP 10.0.0.254.

Confiurer le client de toulouse avec la configuration IP suivante :

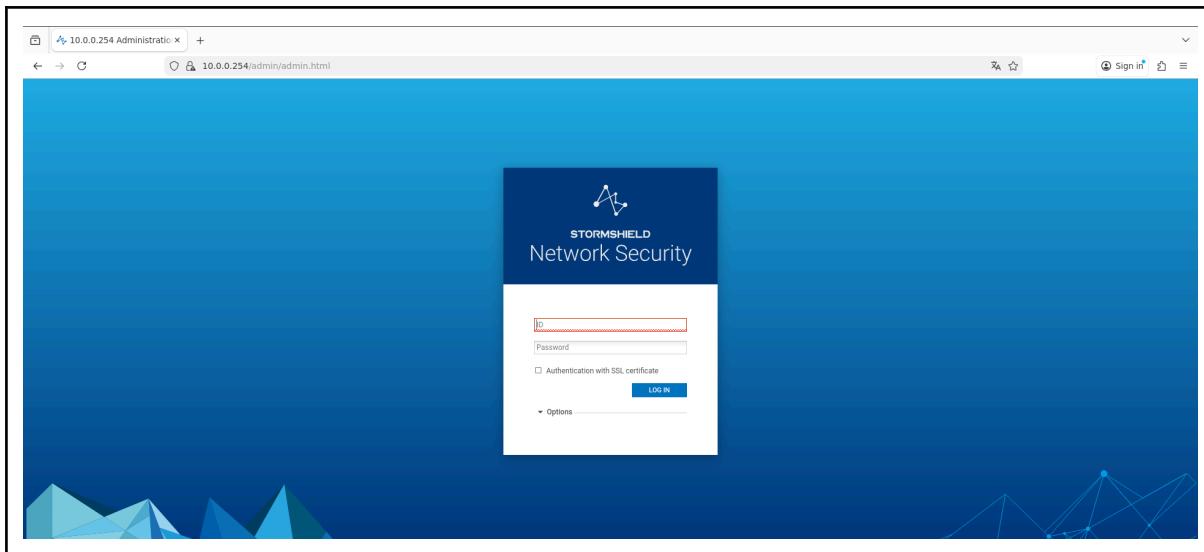
- adresse IP : 10.0.0.1/24 ;
- passerelle : 10.0.0.254.

Puis, se connecter au firewall de toulouse avec le navigateur en saisisant :

<https://10.0.0.254>. (bien mettre https sinon ça marchera pas)

Accepter le certificat proposé et poursuivre la connexion avec le login admin et le mot de passe par défaut admin.

L'étape suivante consiste à effectuer la configuration générale du firewall



Il faut mettre la langue du firewall en français, modifier le mot de passe par défaut et renommer le firewall.

Pour cela, vous aurez besoin d'obtenir le droit d'écriture sur le firewall (voir en haut à droite en cliquant sur admin).

Si la page de stormshield est en bleu, c'est qu'on a les droits

Pour la langue, il faut aller dans le menu système puis configuration.

Mettre aussi le bon fuseau horaire.

The screenshot shows the STORMSHIELD Network Security v4.3.11 configuration interface. The top navigation bar includes 'MONITORING' (selected), 'CONFIGURATION', and 'EVA1 VMSNSX09K0639A9'. The left sidebar has sections for Configuration (Administrators, License, Maintenance, Active Update, High Availability, Management Center, CLI), NETWORK, OBJECTS, USERS, SECURITY POLICY, APPLICATION PROTECTION, VPN, and NOTIFICATIONS. The main content area is titled 'SYSTEM / CONFIGURATION' under 'GENERAL CONFIGURATION'. It shows 'Keyboard (console): French'. Under 'Cryptographic settings', there are two checkboxes: 'Enable regular retrieval of certificate revocation lists (CRL)' and 'Enable "ANSSI Diffusion Restreinte (DR)" mode'. Under 'Password policy', it lists minimum password length, mandatory character types, and minimum entropy. A dropdown menu for 'Time zone' shows options like Europe/Monaco, Europe/Moscow, Europe/Nicosia, Europe/Oslo, Europe/Paris, Europe/Podgorica, Europe/Prague, Europe/Riga, Europe/Rome, Europe/Samara, Europe/San_Marino, Europe/Sarajevo, and Europe/Saratov, with 'Europe/Paris' selected. A note indicates the current date and time: 'Date/Time settings - 11/21/2025 04:54:08 PM'. Below this, another section for 'Date/Time settings' shows '11/21/2025 04:54:19 PM' and three checkboxes for 'Manual mode', 'Synchronize with your machine - 11/21/2025 04:54:20 PM', and 'Synchronize firewall time (NTP)'. The 'Time zone' dropdown here also shows 'Europe/Paris'.

Pour changer le mot de passe, il faut aller dans le menu système puis administrateur.

The screenshot shows the 'SYSTEM / ADMINISTRATORS' screen. The top navigation bar includes 'ADMINISTRATORS' (selected), 'ADMINISTRATOR ACCOUNT' (selected), and 'TICKET MANAGEMENT'. The left sidebar has sections for Configuration (Administrators, License, Maintenance, Active Update, High Availability, Management Center, CLI), NETWORK, OBJECTS, USERS, and SECURITY POLICY. The main content area shows an 'Authentication' section with a note: 'The default password of the admin account has not been changed'. It includes fields for 'Old password', 'Password', 'Confirm password', and a 'Password strength' indicator. Below this is an 'Exports' section with buttons for 'Administrator's private key' and 'Firewall's public key' labeled with 'Export private key' and 'Export public key' respectively.

Enfin, il faut changer le nom du firewall en fw-toulouse, il faut aller dans le menu système puis configuration.

The screenshot shows the 'SYSTEM / CONFIGURATION' interface with the 'GENERAL CONFIGURATION' tab selected. On the left, a sidebar lists 'Configuration', 'Administrators', 'License', 'Maintenance', 'Active Update', 'High Availability', 'Management Center', and 'CLI'. Under 'NETWORK', it lists 'OBJECTS', 'USERS', and 'SECURITY POLICY'. The main panel displays 'General configuration' settings: Firewall name (fw-toulouse), Firewall language (logs) (French), and Keyboard (console) (French). It also includes 'Cryptographic settings' and 'Password policy' sections.

Cliquer sur réseau puis sur interfaces. Les trois interfaces out, in et dmz seront sorties du bridge.

The screenshot shows the 'NETWORK / INTERFACES' interface with the 'Interfaces' tab selected. On the left, a sidebar lists 'Configuration', 'Administrators', 'License', 'Maintenance', 'Active Update', 'High Availability', 'Management Center', and 'CLI'. Under 'NETWORK', it lists 'Virtual interfaces' and 'Routing'. The main panel displays a table of network interfaces:

Interface	Port	Type	Status
bridge		Bridge	
out	1	Ethernet, 1 Gb/s	
in	2	Ethernet, 1 Gb/s	
dmz1	3	Ethernet, 1 Gb/s	

Double cliquer sur interface in. Cocher les deux options suivantes :

- Dynamique/statique ;
- Ip fixe (statique).

The screenshot shows the 'IN CONFIGURATION' tab for the 'in' interface. In the 'GENERAL' section, the 'Comments' field is empty. The 'This interface is:' dropdown is set to 'Internal (protected)' (selected). Below this, the 'Address range' and 'IPv4 address' sections are visible, both with their respective radio button options. A table for adding addresses is present, with one entry: 'Address/ Mask' is '192.168.50.254/24' and 'Comments' is 'lan'. The 'in' interface is highlighted in yellow.

Mettre la bonne adresse IP conformément au plan d'adressage figurant en page 2 puis valider. Vous allez perdre l'accès au boîtier ce qui est normal puisqu'il faut aussi modifier l'adressage IP de votre machine cliente.

The screenshot shows the 'IN CONFIGURATION' tab for the 'in' interface. In the 'GENERAL' section, the 'Comments' field is empty. The 'This interface is:' dropdown is set to 'Internal (protected)' (selected). Below this, the 'Address range' and 'IPv4 address' sections are visible, both with their respective radio button options. A table for adding addresses is present, with one entry: 'Address/ Mask' is '192.168.50.254/24' and 'Comments' is 'lan'. The 'in' interface is highlighted in yellow.

Modifier ensuite l'adressage IP du client de toulouse conformément au plan d'adressage puis se connecter à nouveau au firewall.

Editing Wired connection 1

Connection name **Wired connection 1**

General Ethernet 802.1X Security DCB Proxy **IPv4 Settings** IPv6 Settings

Method **Manual**

Addresses

Address	Netmask	Gateway	
192.168.50.1	24	192.168.50.254	Add
			Delete

DNS servers **192.168.100.10**

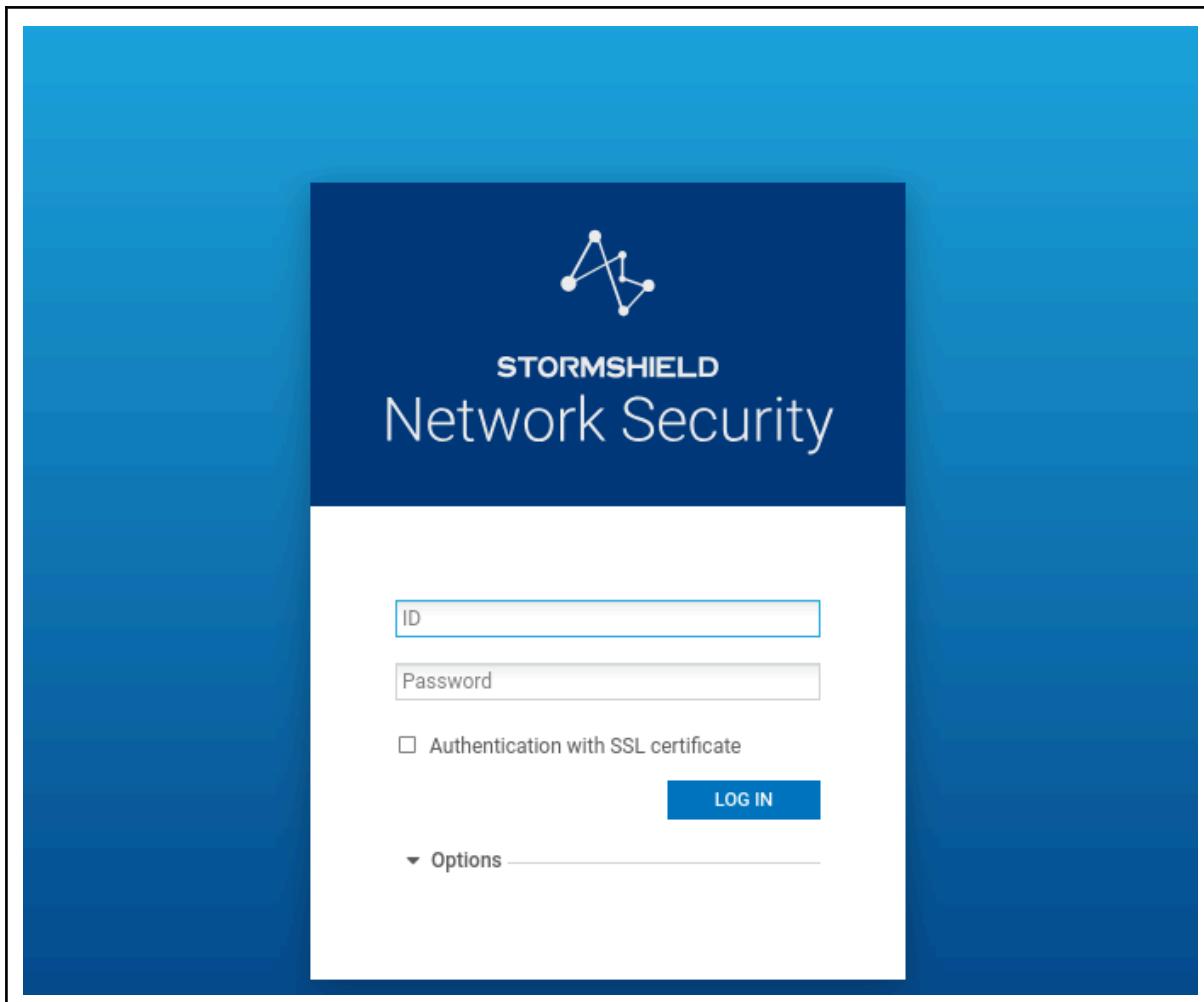
Search domains **mlif.local**

DHCP client ID

Require IPv4 addressing for this connection to complete

Routes...

Cancel **Save**



Une fois l'accès au firewall retrouvé, modifier les configurations IP des deux autres interfaces dmz (dmz-toulouse) et out (nuage-internet conformément au plan d'adressage puis valider)

out	1 Ethernet, 1 Gb/s	82.10.20.1/30
in	2 Ethernet, 1 Gb/s	192.168.50.254/24
dmz1	3 Ethernet, 1 Gb/s	172.16.10.254/24
bridge	Bridge	10.0.0.254/8

DEPUIS LA MACHINE CLIENT-MARSEILLE:

Reproduire les étapes précédentes 1 et 2 afin de modifier la configuration générale et IP du firewall de Marseille conformément au plan d'adressage fourni dans le tableau en travaillant depuis la machine CLIENT-MARSEILLE.

out	1 Ethernet, 1 Gb/s	82.10.20.2/30
in	2 Ethernet, 1 Gb/s	192.168.80.254/24
dmz1	3 Ethernet, 1 Gb/s	172.16.20.254/24
bridge	Bridge	10.0.0.254/8

DEPUIS LA MACHINE CLIENT-TOULOUSE :

Depuis le menu réseau, routage, routage statique IPv4, configurer la passerelle par défaut du firewall de toulouse. Cette passerelle est associée à l'interface out du firewall de Marseille soit 82.10.20.2/30. Pour cela, créer l'objet machine correspondant en le nommant GW-MARSEILLE.

Status	Destination network (host, network or group object)	Interface	Address range	Gateway	Comments
on	GW-MARSEILLE	out	82.10.20.2	GW-MARSEILLE	

General

Default gateway (router): **GW-MARSEILLE**

DEPUIS LA MACHINE CLIENT-MARSEILLE:

Faire de même sur le boîtier de Marseille en configurant la passerelle par défaut via un objet nommé GW-TOULOUSE d'adresse IP 82.10.20.1/30

Status	Destination network (host, network or group object)	Interface	Address range	Gateway	Comments
on	GW-TOULOUSE	out	82.10.20.1	GW-TOULOUSE	

General

Default gateway (router): **GW-TOULOUSE**

STOP 1

DEPUIS LA MACHINE CLIENT-TOULOUSE :

1- Configuration du tunnel :

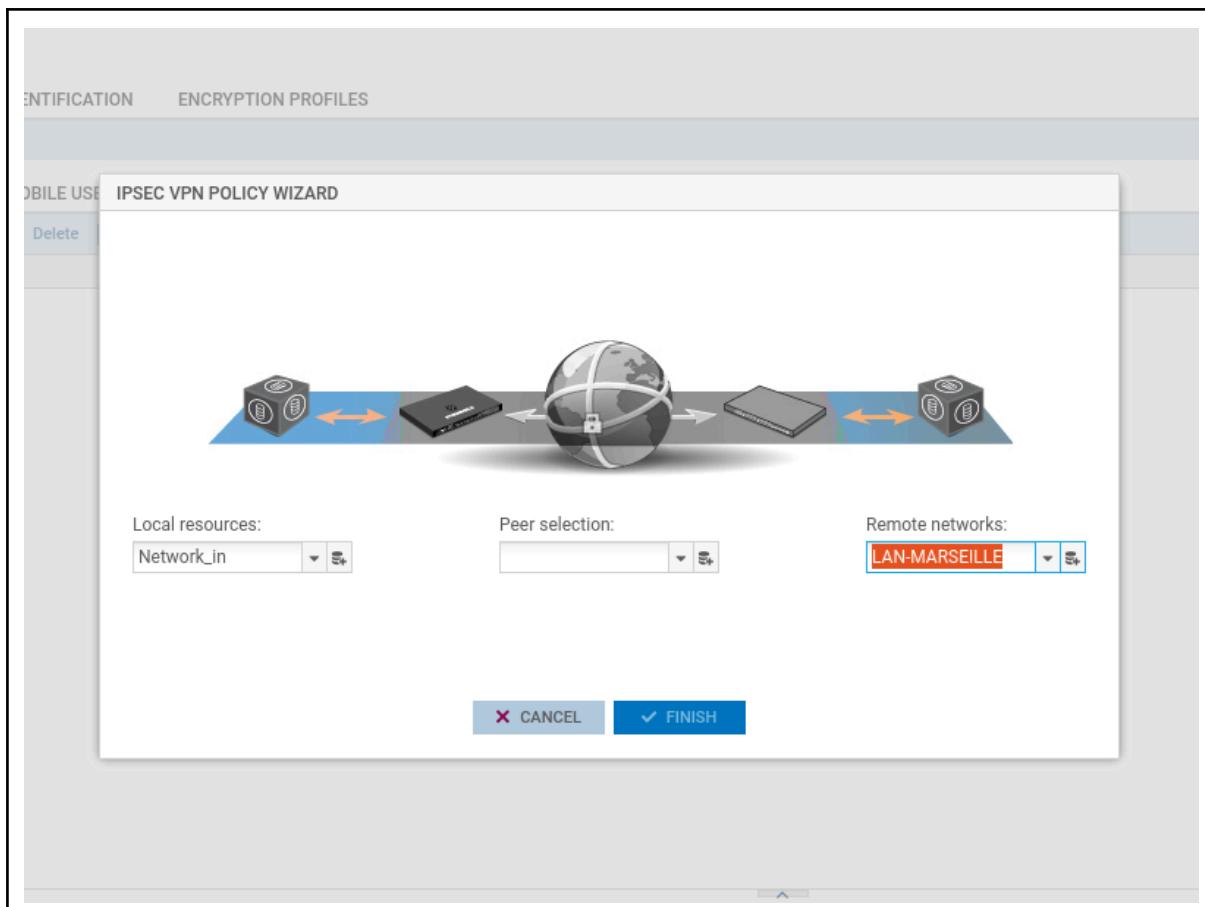
Cliquer sur VPN puis sur VPN Ipsec. Dans l'onglet Site à site, cliquer sur Ajouter puis sur tunnel site à site.

IPsec 01 (01) | Actions | **SITE TO SITE (GATEWAY-GATEWAY)** MOBILE - MOBILE USERS

Enter a filter | + Add | X Delete | Up | Down | Cut | Copy

	Status	Peer
	Standard site-to-site tunnel	

Dans réseau local, à gauche, saisir Network_in. Cela correspond au réseau local de Toulouse.



Dans Réseau Distant, créer un objet correspond au LAN de Marseille soit 192.168.80.0/24 et nommez le LAN-MARSEILLE.

CREATE AN OBJECT

Host

DNS name (FQDN)

Network

Address range

Router

Group

IP Protocol

Port

Port group

Region group

Time object

Object name:

IPv4 addresses

Network IP address:

Example 192.168.0.0/16 or 192.168.0.0/255.255.0.0

Comments:

✖ CLOSE + CREATE

Dans Choix du correspondant, créer un objet de type IKEv2 en indiquant l'adresse de l'interface out du firewall de Marseille soit 82.10.20.2. Nommer cet objet FW-MARSEILLE. Le wizard préfixe alors automatiquement le nom du correspondant avec Site_. Cliquer ensuite sur suivant puis sélectionner clé partagée PSK. Saisir deux fois le mot de passe, puis cliquer encore sur suivant et sur terminer.

IDENTIFICATION ENCRYPTION PROFILES

MOBILE USE IPSEC CREATE A REMOTE GATEWAY

SELECT THE GATEWAY - PEER CREATION WIZARD



Remote gateway:

Name:

IKE version:

IDENTIFICATION ENCRYPTION PROFILES

MOBILE USE IPSEC CREATE A REMOTE GATEWAY

PEER IDENTIFICATION - PEER CREATION WIZARD

Authentication type:

Certificate
 Pre-shared key (PSK)

Certificate:

Trusted CA:

Pre-shared key (PSK):

Confirm:

Enter the key in ASCII characters:

L'étape suivante consiste à configurer la politique de filtrage suivante.

FILTRAGE NAT								
Rechercher...	+ Nouvelle règle	X Supprimer	Etat	Action	Source	Destination	Port dest.	Protocole
Remote Management: Go to System - Configuration to setup the web administration application access (contient 2 règles, de 1 à 2)								
1	on	passer	Any		firewall_all	firewall_srv	https	IP
2	on	passer	Any		firewall_all	Any	icmp (requête Ech)	IP
Politique VPN (contient 2 règles, de 3 à 4)								
3	on	passer	Network_in		LAN-MARSEILLE	Any	IP	
4	on	passer	LAN-MARSEILLE via Tunnel VPN IPsec		Network_in	Any	IP	
Séparateur - regroupement de règles (contient 1 règles, de 5 à 5)								
5	on	bloquer	Any		Any	Any	IP	

Il faut donc ajouter les règles 3 et 4 de la capture d'écran ci-dessus. Pour créer ces règles de filtrage, utiliser l'omnibox et n'oubliez pas l'option **via Tunnel Ipsec** dans le champ sour ce de la règle numéro 4. Remarquez que cette configuration est très permissive car le port de destination est à any.

On a donc ajouté ces 2 règles :

EDITING RULE NO 5

General	Source	Destination	Port - Protocol	Inspection
	SOURCE			
	GENERAL	GEOLOCATION / REPUTATION		ADVANCED PROPERTIES
	Advanced properties <div style="border: 1px solid #ccc; padding: 5px;"> <p>Source port:</p> <div style="border: 1px solid #ccc; padding: 2px; margin-bottom: 5px;">+ Add X Delete</div> <div style="border: 1px solid #ccc; padding: 2px; height: 100px; overflow: auto;">Any</div> </div> <p>Via: IPsec VPN tunnel</p> <p>source DSCP: All</p>			
	Authentication <div style="border: 1px solid #ccc; padding: 5px;"> <p>Authentication method: None</p> </div>			
	X CANCEL ✓ OK			

Oublie pas de mettre ça pour la règle 4
Mettre les règles au dessus de la rule pour bloquer

DEPUIS LA MACHINE CLIENT-MARSEILLE:

Reproduire les mêmes étapes que précédemment en les adaptant sur le firewall du site de Marseille

CREATE AN OBJECT

Host
DNS name (FQDN)

Network

Address range

Router

Group

IP Protocol

Port

Port group

Region group

Time object

Object name:

IPv4 addresses

Network IP address:

Example 192.168.0.0/16 or 192.168.0.0/255.255.0.0

Comments:

X CLOSE + CREATE

ENTIFICATION ENCRYPTION PROFILES

MOBILE USE IPSEC CREATE A REMOTE GATEWAY

Delete

SELECT THE GATEWAY - PEER CREATION WIZARD

Remote gateway:

Name:

IKE version:

VPN (contains 2 rules, from 3 to 4)

	3	4	on	pass	Network_in	Any	Created on 2025-11-28 17:32:26 by admin (192.168.80.1)
	3	4	on	pass	Network_in	Any	Created on 2025-11-28 17:33:07 by admin (192.168.80.1)
	4	4	on	pass	LAN-TOULOUSE via IPsec VPN tunnel	Any	

DEPUIS LA MACHINE CLIENT-TOULOUSE:

Ouvrir un terminal et faire un ping vers 192.168.80.1. Ce ping doit aboutir.

Validé dans les 2 sens

Ensuite, vérifier l'état du tunnel en consultant les logs. Pour cela, cliquer sur l'onglet monitoring puis sur logs-journaux d'audit puis sur VPN

Type : Site-to-site tunnels (1)	OK	Network_in	Firewall_out	82.10.20.1	GW-MARSEILLE	82.10.20.2	LAN-MARSEILLE
Tunnels : Exception policies (bvoase) (1)							

DEPUIS LA MACHINE CLIENT-MARSEILLE:

Ouvrir un terminal et faire ping vers 192.168.50.1. Ce ping doit aboutir.

Vérifiez aussi les logs sur le firewall de Marseille.

EPUIS LA MACHINE CLIENT-TOULOUSE:

1- Création de l'autorité de certification :

Il s'agit de créer la CA (autorité de certification) qui servira pour les deux sites. C'est donc la CA de toulouse qui fera autorité.

Cliquer sur objets puis sur certificats et PKI. Ensuite cliquer sur ajouter puis sur autorité racine. Puis, remplir le wizard avec les informations suivantes :

CREATE ROOT AUTHORITY

CERTIFICATION AUTHORITY PROPERTIES



CN: fw-toulouse

Identifier: fw-toulouse

Authority attributes

Organization:	mlif
Organizational unit:	mlif
City (L):	toulouse
State (ST):	occitanie
Country:	France ▾

CANCEL

« PREVIOUS

» NEXT

CREATE ROOT AUTHORITY

CERTIFICATION AUTHORITY PROPERTIES



Certification authority password

Passphrase (8 chars min.): 

Confirm password:

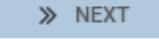
Strength meter: Fair

Mail:

Validity (days):

Type de clé:

Key size (bits):

 CANCEL  PREVIOUS  NEXT

mariokart8 le mdp

Dans l'écran suivant, saisir le mot de passe de la CA (ne surtout pas l'oublier). Puis cliquer deux fois sur suivant puis sur terminer.

2-Création du certificat du firewall de Toulouse :

Toujours depuis le menu certificat et PKI, cliquer sur ajouter puis sur identité serveur. Saisir le FQDN suivant fw-toulouse.mlif.local.

CREATE A SERVER IDENTITY

IDENTITY OPTIONS - CREATION WIZARD



Fully Qualified Domain Name (FQDN):

fw-toulouse.mlif.local

ID:

fw-toulouse.mlif.local

CANCEL

« PREVIOUS

» NEXT

CREATE A SERVER IDENTITY

IDENTITY OPTIONS - CREATION WIZARD



Select the parent Authority

Parent CA:

fw-toulouse

CA passphrase:

[REDACTED]



Authority attributes

Organization:

mlif

Organizational unit:

mlif

City (L):

toulouse

State (ST):

occitanie

Country:

France

CANCEL

PREVIOUS

NEXT

Cliquer ensuite sur suivant puis sélectionner la CA précédemment créée puis saisir son mot de passe. Les autres champs sont pré-remplis. Ensuite, cliquer sur suivant et laisser les valeurs de longueur de clé par défaut. Enfin, cliquez deux fois sur suivant puis sur terminer.
3- Création du certificat du firewall de Marseille :

Reproduire l'étape précédent n°2 afin de créer le certificat du firewall de Marseille en adaptant les valeurs (fw-marseille.mlif.local, ville de marseille dan ville et PACA dans état).

CREATE A SERVER IDENTITY

IDENTITY OPTIONS - CREATION WIZARD



Fully Qualified Domain Name (FQDN):

fw-marseille.mlif.local

ID:

fw-marseille.mlif.local

CANCEL

« PREVIOUS

» NEXT

CREATE A SERVER IDENTITY

IDENTITY OPTIONS - CREATION WIZARD



Select the parent Authority

Parent CA:

fw-toulouse

CA passphrase:

••••••••••••



Authority attributes

Organization:

mlif

Organizational unit:

mlif

City (L):

marseille

State (ST):

PACA

Country:

France

CANCEL

PREVIOUS

NEXT

Vous devez obtenir l'arborescence suivante :

fw-toulouse



fw-toulouse.mlif.local



fw-marseille.mlif.local



4- Transfert du certificat au site de Marseille :

Il faut maintenant envoyer au site de marseille son certificat accompagné du certificat de la CA. Toujours depuis le menu certificat et PKI, sélectionner le certificat du boitier de marseille en cliquant dessus puis cliquer ensuite sur le menu télécharger puis sur certificat au format P12.

Sauvegardez le certificat sur votre machine cliente en saisissant un mot de passe et envoyez ce fichier P12 sur la machine cliente de toulouse via la commande scp :

```
test@client-mlif:~/Téléchargements$ scp fw-marseille.mlif.local.p12 test@192.168.80.1:/home/
test
test@192.168.80.1's password:
fw-marseille.mlif.local.p12                                         100% 4448      1.4MB/s   00:00
```

DEPUIS LA MACHINE CLIENT-MARSEILLE:

Cliquez sur objets puis sur certificats et PKI. Ensuite, cliquez sur ajouter puis sur importer un fichier et sélectionnez le certificat envoyé par scp. Dans la boîte de dialogue, sélectionnez le format P12 et choisissez d'importer tous les éléments.

Vous devriez obtenir ceci :

DEPUIS LA MACHINE CLIENT-TOULOUSE:

Cliquez sur VPN puis sur VPN Ipsec et cliquez sur l'onglet identification. Dans la partie autorités de certifications acceptées, cliquez sur ajouter puis sélectionnez la CA créée précédemment soit fw-toulouse

DEPUIS LA MACHINE CLIENT-MARSEILLE:

Faites de même sur le firewall de marseille afin d'ajouter la CA de Toulouse en autorité de certification acceptée

ENCRYPTION POLICY - TUNNELS PEERS **IDENTIFICATION** ENCRYPTION PROFILES

APPROVED CERTIFICATION AUTHORITY

+ Add X Delete

CA

C=FR ST=occitanie L=toulouse O=mlif OU=mlif CN=fw-toulouse

Certificate

DEPUIS LA MACHINE CLIENT-TOULOUSE:

Cliquer sur VPN puis sur VPN Ipsec et dans l'onglet correspondant, dans la partie identification,sélectionner certificat au lieu de PSK et choisir le certificat du boitier de toulouse (fw-toulouse.mlif.local), puis valider.

ENCRYPTION POLICY - TUNNELS PEERS IDENTIFICATION ENCRYPTION PROFILES

Enter a filter

Remote gateways (1)

FW-MARSEILLE

General

Comment:

Remote gateway: GW-MARSEILLE

Local address: Any

IKE profile: StrongEncryption

IKE version: IKEv2

Identification

Authentication method: Certificate

Certificate: fw-toulouse:fw-toulouse.mlif.local

Local ID: Enter an ID (optional)

Peer ID: Enter an ID (optional)

Pre-shared key (PSK): Edit

Advanced properties

CHECKING THE POLICY

X CANCEL ✓ APPLY

DEPUIS LA MACHINE CLIENT-MARSEILLE:

Reproduire l'étape précédente sur le firewall de Marseille en sélectionnant le certificat correspondant (fw-marseille.mlif.local).

ENCRYPTION POLICY - TUNNELS PEERS IDENTIFICATION ENCRYPTION PROFILES

Enter a filter

Remote gateways (1)

FW-MARSEILLE

FW-MARSEILLE

General

Comment:

Remote gateway: GW-TOULOUSE

Local address: Any

IKE profile: StrongEncryption

IKE version: IKEv2

Identification

Authentication method: Certificate

Certificate: f=PACA L=marseille O=mlif OU=mlif CN=fw-marseille.mlif.local

Local ID: Enter an ID (optional)

Peer ID: Enter an ID (optional)

Pre-shared key (PSK): Edit

Advanced properties

CHECKING THE POLICY

CANCEL APPLY

7- Test du tunnel :

Faire un ping des deux cotés (ping l'autre machine) et vérifier dans les logs la bonne ouverture du tunnel.

Tunnel 2 validé

DEPUIS LA MACHINE CLIENT-MARSEILLE:

1- Crédation de la CA de Marseille :

En prenant appui sur le travail précédemment réalisé , créer une CA propre au site de Marseille. Cette CA servira à signer le futur certificat du firewall de Marseille.

Aller dans objects, certificates and pki et add root authority :

CREATE ROOT AUTHORITY

CERTIFICATION AUTHORITY PROPERTIES



CN:

fw-marseille

Identifier:

fw-marseille

Authority attributes

Organization:

mlif

Organizational unit:

mlif

City (L):

marseille

State (ST):

occitanie

Country:

France

CANCEL

PREVIOUS

NEXT

Mdp : mariokart8

Il faut ajouter le server identity :

CREATE A SERVER IDENTITY

IDENTITY OPTIONS - CREATION WIZARD



Fully Qualified Domain Name (FQDN):

fw-marseille.mlif.local

ID:

fw-marseille.mlif.local

CANCEL

PREVIOUS

NEXT

On met suivant on rentre le mdp et suivant suivant

On va telecharger le certificat de marseille en format pem :

On rentre la commande scp pour transférer le certificat

```
test@client-mlif:~/Téléchargements$ scp fw-marseille.mlif.local.pem test@192.168.50.1:/home/
test
test@192.168.50.1's password:
fw-marseille.mlif.local.pem                                              100% 3938    939.7KB/s   00:00
test@client-mlif:~/Téléchargements$
```

DEPUIS LA MACHINE CLIENT-TOULOUSE:

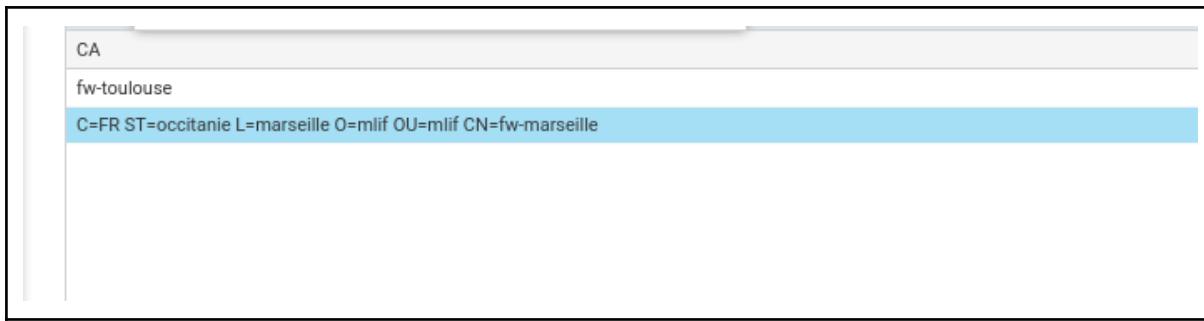
1- Import de la CA de Marseille :

Dans le menu objet, certificats et PKI, cliquer sur ajouter puis sur importer un fichier.
Sélectionner la CA de Marseille au format PEM et l'importer.

File to import:	C:\fakepath\fw-marseille.mlif.local.pem	...
File format:	<input type="radio"/> P12 <input type="radio"/> DER <input checked="" type="radio"/> PEM	
File password:	(redacted)	
What to import:	<input checked="" type="radio"/> All <input type="radio"/> Certificate(s) <input type="radio"/> Private key(s) <input type="radio"/> CRL <input type="radio"/> CA	
<input type="checkbox"/> Overwrite existing content		
<input type="button" value="CANCEL"/>		<input type="button" value="IMPORT"/>

2- Acceptation de la CA de Marseille :

Cliquer sur VPN puis sur VPN Ipsec, dans l'onglet identification, ajouter la CA de Marseille précédemment importée dans les autorités de certification acceptées puis valider.



DEPUIS LA MACHINE CLIENT-MARSEILLE:

1- Modification de la configuration du tunnel :

Modifier le tunnel afin de faire référence au nouveau certificat de Marseille et non à celui émis par la CA de Toulouse. Pour cela, cliquer sur le menu VPN puis sur VPN Ipsec et dans l'onglet correspondant, dans la partie certificat, mettre le certificat du firewall de Marseille signé par la nouvelle CA de Marseille. Enfin, activier la politique.

The screenshot shows the 'VPN / IPSEC VPN' configuration screen. The 'PEERS' tab is selected. On the left, under 'Remote gateways (1)', 'FW-MARS...' is listed. In the main panel, the 'FW-MARSEILLE' peer is configured with the following settings:

- General**:
 - Comment: (empty)
 - Remote gateway: GW-TOULOUSE
 - Local address: Any
 - IKE profile: StrongEncryption
 - IKE version: IKEv2
- Identification**:
 - Authentication method: Certificate
 - Certificate: fw-marseille:fw-marseille.mlif.local
 - Local ID: SSL proxy default authority
 - Peer ID:
 - sslvpn-full-default-authority
 - fw-toulouse
 - fw-marseille
 - fw-marseille.mlif.local (highlighted in yellow)
 - Pre-shared key (PSK): (empty)

At the bottom, there is a link labeled 'CHECKING THE POLICY'.

The screenshot shows a search results page for an LDAP directory. The search term used was 'C=FR ST=occitanie L=toulouse O=mlif OU=mlif CN=fw-toulouse'. The results table has one row, with the entry 'fw-marseille' displayed.

Stop 2

Avant de passer à la partie suivante, éteindre toutes vos machines.

4°) VPN SSL avec Pfsense

4.1°) Travaux préparatoires

Maquette mise en place :

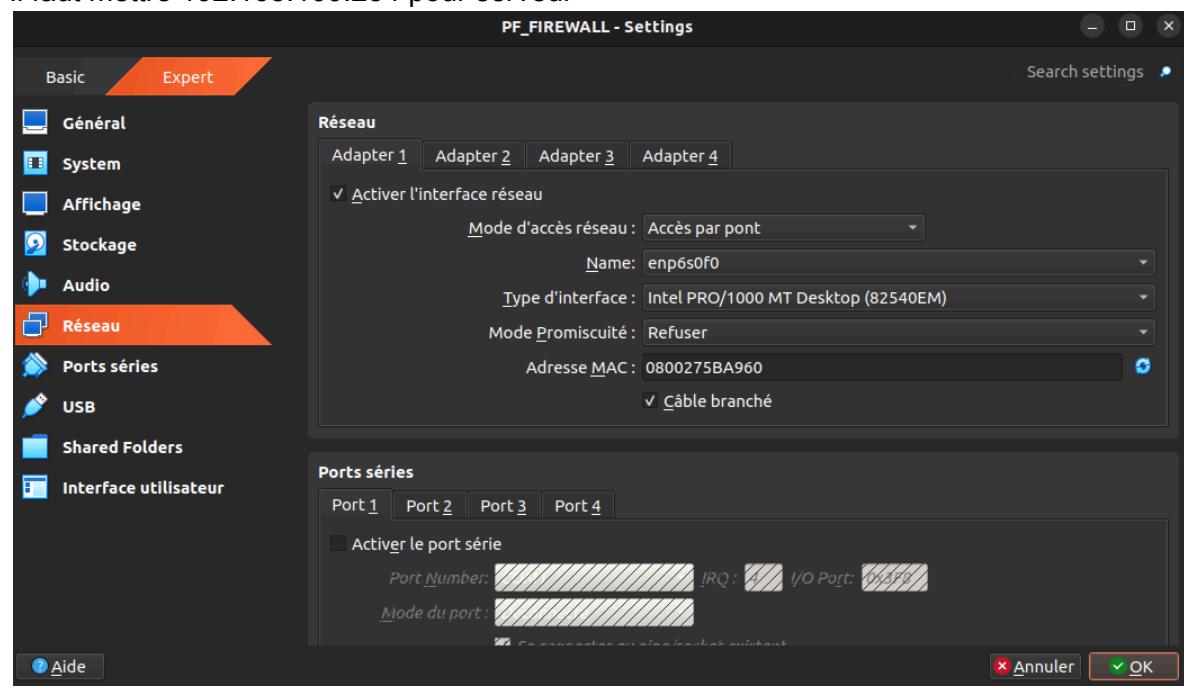
Reprendre le firewall du labo 1 sur le filtrage et le démarrer. N'oubliez pas de faire un snapshot afin de ne pas perdre la configuration existante.

Plan d'adressage :

FIREWALL MLIF PFSENSE

INTERFACE	RESEAU VIRTUALBOX	NOM DU RESEAU	ADRESSAGE IP
1ère interface	Accès par pont sur carte filaire	Bridge wan	172.17.124 123.X
2ème interface	Réseau interne	sw-dmz	192.168.200.254/24
3ème interface	Réseau interne	sw-serveur	172.16.100.254/24
4ème interface	Réseau interne	Sw-client	192.168.50.0/24

Il faut mettre 192.168.100.254 pour serveur



PF_FIREWALL - Settings

Basic Expert Search settings

Réseau

Adapter 1 Adapter 2 Adapter 3 Adapter 4

Activer l'interface réseau

Mode d'accès réseau : Réseau interne

Name: sw-serveur

Type d'interface : Intel PRO/1000 MT Desktop (82540EM)

Mode Promiscuité : Refuser

Adresse MAC : 0800271DC8D7

Câble branché

Ports séries

Port 1 Port 2 Port 3 Port 4

Activer le port série

Port Number: [] IRQ: [] I/O Port: []

Mode du port: []

PF_FIREWALL - Settings

Basic Expert Search settings

Réseau

Adapter 1 Adapter 2 Adapter 3 Adapter 4

Activer l'interface réseau

Mode d'accès réseau : Réseau interne

Name: sw-dmz

Type d'interface : Intel PRO/1000 MT Desktop (82540EM)

Mode Promiscuité : Refuser

Adresse MAC : 080027663C02

Câble branché

Ports séries

Port 1 Port 2 Port 3 Port 4

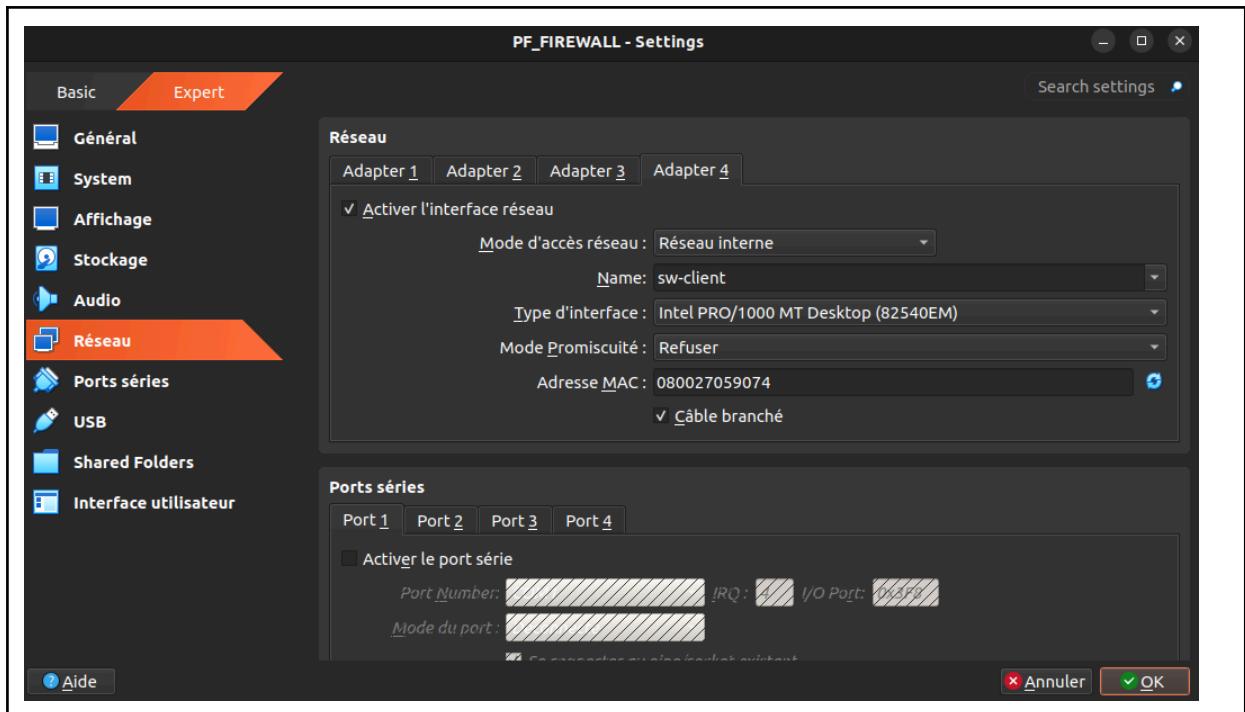
Activer le port série

Port Number: [] IRQ: [] I/O Port: []

Mode du port: []

Aide Annuler OK

Aide Annuler OK



Changer l'adresse des client (lan)

```
You can now access the webConfigurator by opening the following URL in your web browser:
http://192.168.50.20/

Press <ENTER> to continue.
VirtualBox Virtual Machine - Netgate Device ID: 7a5969dfa5e5b5c94391

*** Welcome to pfSense 2.7.0-RELEASE (amd64) on pf-firewall ***

WAN (wan)      -> em0      -> v4/DHCP4: 172.17.123.79/24
LAN (lan)      -> em3      -> v4: 192.168.50.20/24
SRV (opt1)     -> em1      -> v4: 192.168.100.254/24
DMZ (opt2)     -> em2      -> v4: 192.168.200.254/24

0) Logout (SSH only)          9) pfTop
1) Assign Interfaces           10) Filter Logs
2) Set interface(s) IP address 11) Restart webConfigurator
3) Reset webConfigurator password 12) PHP shell + pfSense tools
4) Reset to factory defaults   13) Update from console
5) Reboot system               14) Enable Secure Shell (sshd)
6) Halt system                 15) Restore recent configuration
7) Ping host                   16) Restart PHP-FPM
8) Shell

Enter an option: [
```

Pour le client nomade j'ai pris la kali :

MACHINE CLIENT NOMADE

Cette machine est un client externe et simule un accès extérieur depuis internet (réseau du lycée). C'est donc cette machine qui va accéder au réseau de la MLIF via son client VPN.

INTERFACE	RESEAU VIRTUALBOX	NOM DU RESEAU	ADRESSAGE IP
1ère interface	Accès par pont sur carte filaire	Bridge wan	172.17.124 123.X via le DHCP du lycée.

```
└─(test㉿kali2025)-[~]
└─$ 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: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:94:b3 brd ff:ff:ff:ff:ff:ff
    inet 172.17.123.12/24 brd 172.17.123.255 scope global dynamic noprefixroute eth0
        valid_lft 279sec preferred_lft 279sec
    inet6 fe80::a00:27ff:fe94:bab3/64 scope link noprefixroute
        valid_lft forever preferred_lft forever

└─(test㉿kali2025)-[~]
└─$ █
```

DEPUIS LA MACHINE CLIENT-MLIF:

Se connecter au firewall depuis une machine cliente appartenant au réseau client de la MLIF (192.168.50.30/24). Nommer votre machine client-mlif.

DEPUIS LA MACHINE CLIENT-NOMADE:

Cette machine cliente est en DHCP et reçoit une adresse du type 172.17.123|124.X.

Nommez cette machine kali puis installer l'outil de client VPN OpenVPN :

```
#apt-get install openvpn network-manager-openvpn
```

Suite à cette installation, il devient possible de configurer votre client VPN.

```
[sudo] password for test:
[root@kali2025] ~
# apt-get install openvpn network-manager-openvpn
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
openvpn is already the newest version (2.6.14-1).
openvpn set to manually installed.
network-manager-openvpn is already the newest version (1.12.0-2).
network-manager-openvpn set to manually installed.
0 upgraded, 0 newly installed, 0 to remove and 0 not upgraded.
```

4.2°) Configuration du VPN SSL

Il faudra configurer le serveur et le client VPN.

DEPUIS LA MACHINE CLIENT-MLIF:

1- Création de l'autorité de certification :

Se connecter au firewall pfSense puis cliquer sur système puis sur gestionnaire de certificats. Ensuite, dans l'onglet ACs, cliquer sur ajouter afin de créer une nouvelle autorité de certification.

Renseigner votre CA avec les valeurs suivantes :

The screenshot shows the 'Create / Edit CA' dialog box. At the top, there are three tabs: 'Authorities' (selected), 'Certificates', and 'Revocation'. Below the tabs, the title 'Create / Edit CA' is displayed. The form fields are as follows:

Descriptive name	CA-VPNSSL The name of this entry as displayed in the GUI for reference. This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", '
Method	Create an internal Certificate Authority
Trust Store	<input type="checkbox"/> Add this Certificate Authority to the Operating System Trust Store When enabled, the contents of the CA will be added to the trust store so that they will be trusted by the operating system.
Randomize Serial	<input type="checkbox"/> Use random serial numbers when signing certificates When enabled, if this CA is capable of signing certificates then serial numbers for certificates signed by this CA will be automatically randomized and checked for uniqueness instead of using the sequential value from Next Certificate Serial.

Internal Certificate Authority

Key type

RSA

2048

The length to use when generating a new RSA key, in bits.

The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

Digest Algorithm

sha256

The digest method used when the CA is signed.

The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid

Lifetime (days)

3650

Common Name

CA-VPNSSL

The following certificate authority subject components are optional and may be left blank.

Country Code

FR

State or Province

IDF

City

Paris

Organization

MLIF

Organizational Unit

Commerciaux

2- Création du certificat de l'utilisateur nomade :

Toujours depuis le gestionnaire de certificats, cliquer ensuite sur l'onglet certificats puis sur ajouter. Ensuite, renseigner les valeurs suivantes :

Add/Sign a New Certificate

Method Create an internal Certificate

Descriptive name CERT-JOHN-DOE

The name of this entry as displayed in the GUI for reference.
This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", '

Internal Certificate

Certificate authority CA-VPNSSL

Key type RSA

2048

The length to use when generating a new RSA key, in bits.
The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.

Digest Algorithm sha256

The digest method used when the certificate is signed.
The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid

Lifetime (days) 3650

The length of time the signed certificate will be valid, in days.
Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.

Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.

<u>Common Name</u>	b2b.mlif.local
The following certificate subject components are optional and may be left blank.	
<u>Country Code</u>	FR
<u>State or Province</u>	IDF
<u>City</u>	Paris
<u>Organization</u>	MLIF
<u>Organizational Unit</u>	Commerciaux

Certificate Attributes

<u>Attribute Notes</u>	The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode.
For Internal Certificates, these attributes are added directly to the certificate as shown.	
<u>Certificate Type</u>	User Certificate
Add type-specific usage attributes to the signed certificate. Used for placing usage restrictions on, or granting abilities to, the signed certificate.	
<u>Alternative Names</u>	FQDN or Hostname
Type	Value
Enter additional identifiers for the certificate in this list. The Common Name field is	

3- Transfert des certificats et de la clé de l'utilisateur :

Cliquer sur le bouton permettant d'exporter le certificat de l'autorité de certification.



Cliquer sur les boutons permettant d'exporter le certificat de l'utilisateur nomade ainsi que sa clé privée.



Ensuite, envoyer ces trois fichiers sur la machine cliente nomade via la commande scp.

Attention, votre firewall pfSense n'autorise peut-être pas ce flux. A vous de l'ouvrir afin que la commande scp soit un succès (UDP 1194).

Il faut aussi penser à ouvrir un flux sur l'interface wan du firewall pour autoriser les connexions VPN (SSH22).

Comme on a modifié l'ip de la firewall, on va faire :
sudo ip route add default via 192.168.50.20 (c'est l'ip de la lan)

Ensuite, on va faire les règles sur pfsense :

The screenshot shows the pfSense Firewall Rules configuration interface. At the top, there is a table with a single row containing the following fields: Action (0/0 B), Protocol (IPv4 UDP), Ports (* * WAN address 1194 * none), and a set of icons for edit, delete, and other actions.

The main area is titled "Edit Firewall Rule". It contains several sections:

- Action**: Set to "Pass". A note explains the difference between "block" and "reject": "Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded."
- Disabled**: An unchecked checkbox labeled "Disable this rule". A note says: "Set this option to disable this rule without removing it from the list."
- Interface**: Set to "WAN". A note says: "Choose the interface from which packets must come to match this rule."
- Address Family**: Set to "IPv4". A note says: "Select the Internet Protocol version this rule applies to."
- Protocol**: Set to "UDP". A note says: "Choose which IP protocol this rule should match."
- Source**: A section with a "Source" dropdown, an "Invert match" checkbox, and a "any" dropdown. To the right are "Source Address" and a separator field.
- Display Advanced**: A button with a gear icon.
- Note**: A message states: "The Source Port Range for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, any."

Destination

Destination	<input type="checkbox"/> Invert match	WAN address	▼	Destination Address	/	▼
Destination Port Range	OpenVPN (▼)	<input type="button" value=""/>	OpenVPN (▼)	<input type="button" value=""/>		
From	Custom	To	Custom			

Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.

Extra Options

Log	<input type="checkbox"/> Log packets that are handled by this rule
Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).	
Description	<input type="text"/>
A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.	
Advanced Options	<input type="button" value="Display Advanced"/>

Rule Information

Tracking ID	1764767115
Created	12/3/25 14:05:15 by admin@192.168.50.30 (Local Database)
Updated	12/3/25 14:05:15 by admin@192.168.50.30 (Local Database)

SSH :

<input type="checkbox"/>	<input checked="" type="checkbox"/>	0/500	IPv4	LAN	*	*	22	*	none	
		B	TCP	net			(SSH)			

Edit Firewall Rule

Action

Pass

Choose what to do with packets that match the criteria specified below.

Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded.

Disabled Disable this rule

Set this option to disable this rule without removing it from the list.

Interface

LAN

Choose the interface from which packets must come to match this rule.

Address

IPv4

Family

Select the Internet Protocol version this rule applies to.

Protocol

TCP

Choose which IP protocol this rule should match.

Source

Source Invert
match

LAN net

Source Address

/

Display Advanced

The **Source Port Range** for a connection is typically random and almost never equal to the destination port. In most cases this setting must remain at its default value, **any**.

THE SOURCE PORT RANGE FOR A CONNECTION IS TYPICALLY UNKNOWN AND ALMOST NEVER EQUAL TO THE DESTINATION PORT. IN MOST CASES THIS SETTING MUST REMAIN AT ITS DEFAULT VALUE, ANY.

Destination

Destination	<input type="checkbox"/> Invert match	any	Destination Address /
Destination Port Range	SSH (22)	From Custom	To Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.			

Extra Options

Log	<input type="checkbox"/> Log packets that are handled by this rule Hint: the firewall has limited local log space. Don't turn on logging for everything. If doing a lot of logging, consider using a remote syslog server (see the Status: System Logs: Settings page).
Description	A description may be entered here for administrative reference. A maximum of 52 characters will be used in the ruleset and displayed in the firewall log.
Advanced Options	Display Advanced

Rule Information

Tracking ID	1764767144
Created	12/3/25 14:05:44 by admin@192.168.50.30 (Local Database)
Updated	12/3/25 14:05:44 by admin@192.168.50.30 (Local Database)

Ensuite sur le client nomade :

```
sudo apt update
sudo apt install openssh-server
sudo systemctl enable --now ssh
sudo systemctl status ssh
```

Depuis le client de la mlif :

```
test@client-mlif:~/Téléchargements$ scp CERT-JOHN-DOE.key test@172.17.123.12:/home/test
test@172.17.123.12's password:
CERT-JOHN-DOE.key                                              100% 1704      554.8KB/s   00:00
test@client-mlif:~/Téléchargements$ scp CERT-JOHN-DOE.crt test@172.17.123.12:/home/test
test@172.17.123.12's password:
CERT-JOHN-DOE.crt                                              100% 1623      2.1MB/s   00:00
test@client-mlif:~/Téléchargements$ scp CA-VPNSSL.crt test@172.17.123.12:/home/test
test@172.17.123.12's password:
CA-VPNSSL.crt                                                 100% 1493     440.0KB/s   00:00
```

4- Création du certificat du serveur VPN :

Toujours depuis le gestionnaire de certificat, dans l'onglet certificats, cliquer sur ajouter et renseigner les champs avec les valeurs suivantes :

Add/Sign a New Certificate

Method	Create an internal Certificate
Descriptive name	CERT-SRV-VPN The name of this entry as displayed in the GUI for reference. This name can contain spaces but it cannot contain any of the following characters: ?, >, <, &, /, \, ", '
Internal Certificate	
Certificate authority	CA-VPNSSL
Key type	RSA
2048	The length to use when generating a new RSA key, in bits. The Key Length should not be lower than 2048 or some platforms may consider the certificate invalid.
Digest Algorithm	sha256 The digest method used when the certificate is signed. The best practice is to use an algorithm stronger than SHA1. Some platforms may consider weaker digest algorithms invalid
Lifetime (days)	3650 The length of time the signed certificate will be valid, in days. Server certificates should not have a lifetime over 398 days or some platforms may consider the certificate invalid.

Common Name	srv-vpn.mlif.local						
The following certificate subject components are optional and may be left blank.							
Country Code	FR						
State or Province	IDF						
City	Paris						
Organization	MLIF						
Organizational Unit	Commerciaux						
Certificate Attributes							
Attribute Notes	The following attributes are added to certificates and requests when they are created or signed. These attributes behave differently depending on the selected mode. For Internal Certificates, these attributes are added directly to the certificate as shown.						
Certificate Type	Server Certificate						
Alternative Names	<table border="1"> <tr> <td>FQDN or Hostname</td> <td>srv-vpn.mlif.local</td> </tr> <tr> <td>Type</td> <td>Value</td> </tr> <tr> <td colspan="2">Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.</td> </tr> </table>	FQDN or Hostname	srv-vpn.mlif.local	Type	Value	Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.	
FQDN or Hostname	srv-vpn.mlif.local						
Type	Value						
Enter additional identifiers for the certificate in this list. The Common Name field is automatically added to the certificate as an Alternative Name. The signing CA may ignore or change these values.							

5- Configuration du serveur VPN :

Cliquer sur VPN puis sur OpenVPN. Dans l'onglet serveurs, cliquer sur le bouton ajouter.

Puis configurer votre serveur avec les valeurs suivantes :

Dans un premier temps, saisir les informations suivantes sur le port d'écoute, l'interface et la description du VPN.

Serveurs Clients Ré-écritures spécifiques au client Assistants

Informations Générales

Description A description of this VPN for administrative reference.

Désactivé Désactiver ce serveur
Définissez cette option pour désactiver ce serveur sans le retirer de la liste.

Mode Configuration

Mode serveur

Mode dispositif
Le mode "tun" porte IPv4 et IPv6 (couche OSI 3) et est le mode le plus courant et compatible sur toutes les plates-formes.
Le mode "tap" est capable de transporter 802.3 (couche OSI 2.)

Endpoint Configuration

Protocole

Interface
L'interface ou l'adresse IP virtuelle où OpenVPN recevra les connexions des clients

Port local
Le port utilisé par OpenVPN pour recevoir des connexions client.

Configuration TLS	<input type="checkbox"/> Utiliser une clé TLS Une clé TLS améliore la sécurité d'une connexion OpenVPN en demandant aux deux parties d'avoir une clé commune avant qu'un pair puisse effectuer une négociation TLS. Cette couche d'authentification HMAC permet de transférer les paquets de canal de contrôle sans que la clé appropriée soit supprimée, protégeant les pairs contre les attaques ou les connexions non autorisées. La clé TLS n'a aucun effet sur les données du tunnel.												
Authorité de certification du pair	CA-VPNSSL												
Liste des Certificats de Révocation de pairs.	No Certificate Revocation Lists defined. One may be created here: System > Cert. Manager												
OCSP Check	<input type="checkbox"/> Check client certificates with OCSP												
Certificat du serveur	CERT-SRV-VPN (Serveur : Oui, CA : CA-VPNSSL)												
Longueur du paramètre *DH	2048 bit Ensemble de paramètres Diffie-Hellman (DH) utilisé pour l'échange de clés. i												
Courbe ECDH	Utiliser les valeurs par défaut La courbe elliptique à utiliser pour l'échange de clés. La courbe du certificat du serveur est utilisée par défaut lorsque le serveur utilise un certificat ECDSA. Sinon, secp384r1 est utilisé comme un repli.												
Data Encryption Algorithms	<table border="1"> <tr><td>AES-128-CBC (128 bit key, 128 bit block)</td><td>AES-256-GCM</td></tr> <tr><td>AES-128-CFB (128 bit key, 128 bit block)</td><td>AES-128-GCM</td></tr> <tr><td>AES-128-CFB1 (128 bit key, 128 bit block)</td><td>CHACHA20-POLY1305</td></tr> <tr><td>AES-128-CFB8 (128 bit key, 128 bit block)</td><td></td></tr> <tr><td>AES-128-GCM (128 bit key, 128 bit block)</td><td></td></tr> <tr><td>AES-128-OFB (128 bit key, 128 bit block)</td><td></td></tr> </table>	AES-128-CBC (128 bit key, 128 bit block)	AES-256-GCM	AES-128-CFB (128 bit key, 128 bit block)	AES-128-GCM	AES-128-CFB1 (128 bit key, 128 bit block)	CHACHA20-POLY1305	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-128-CBC (128 bit key, 128 bit block)	AES-256-GCM												
AES-128-CFB (128 bit key, 128 bit block)	AES-128-GCM												
AES-128-CFB1 (128 bit key, 128 bit block)	CHACHA20-POLY1305												
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)													

<p>AES-192-CFB8 (192 bit key, 128 bit block)</p> <p>Available Data Encryption Algorithms Click to add or remove an algorithm from the list</p> <p>The order of the selected Data Encryption Algorithms is respected by OpenVPN. This list is ignored in Shared Key mode. i</p>	<p>Allowed Data Encryption Algorithms. Click an algorithm name to remove it from the list</p>
<p>Fallback Data Encryption Algorithm</p> <p>AES-256-CBC (256 bit key, 128 bit block)</p> <p>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.</p>	
<p>Algorithm de hachage d'authentification</p> <p>SHA256 (256-bit)</p> <p>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.</p>	
<p>Chiffrement matériel</p> <p>Pas d'accélération cryptographique matérielle</p>	
<p>Profondeur du certificat</p> <p>Un (Client + Serveur)</p> <p>Lorsqu'un client basé sur un certificat se connecte, n'accepte pas les certificats au-dessous de cette profondeur. Utile pour refuser les certificats effectués avec des CA intermédiaires générées à partir de la même autorité de certification que le serveur.</p>	
<p>Client Certificate Key Usage Validation</p> <p><input checked="" type="checkbox"/> Enforce key usage</p> <p>Verify that only hosts with a client certificate can connect (EKU: "TLS Web Client Authentication").</p>	
<p>Paramètres du tunnel</p>	

Tunnel Settings	
IPv4 Tunnel Network	<input type="text" value="10.0.8.0/24"/> 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.
IPv6 Tunnel Network	<input type="text"/> 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	<input 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.
IPv4 Local network(s)	<input type="text" value="192.168.100.0/24,127.0.0.1/32,172.17.123.0/24,192.168.50.0/24,172.17.124.0/24,192.168.200.0/24"/> IPv4 networks that will be accessible from the remote endpoint. Expressed as a comma-separated list of one or more CIDR ranges 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.
IPv6 Local network(s)	<input type="text"/> 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.
Pour les ipv4 local network j'ai mis : 192.168.100.0/24,127.0.0.1/32,172.17.123.0/24,192.168.50.0/24,172.17.124.0/24,192.168.200.0/24	

<p>generally set to the LAN network.</p>	
Connexions simultanées	<input type="text" value="5"/> ▼ Spécifier le nombre maximum de clients autorisés à se connecter en même temps à ce serveur.
Allow Compression	<input checked="" type="checkbox"/> 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.
<p>Asymmetric compression allows an easier transition when connecting with older peers.</p>	
Type de service	<input type="checkbox"/> Définissez la valeur d'en-tête IP TOS des paquets de tunnel pour correspondre à la valeur du paquet encapsulé.
Communication inter-clients	<input type="checkbox"/> Autoriser la communication entre les clients connectés à ce serveur
Duplicer la connexion	<input type="checkbox"/> 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.
<h3>Paramètres du client</h3>	
IP dynamique	<input type="checkbox"/> Autoriser les clients connectés à conserver leurs connexions si leur adresse IP change.
Topologie	<input checked="" type="checkbox"/> Sous-réseau -- Une adresse IP par client dans ce sous-réseau ▼ Spécifie la méthode utilisée pour fournir une adresse IP d'adaptateur virtuel aux clients lors de l'utilisation du mode TUN sur IPv4.

environments.

Paramètres du client

IP dynamique Autoriser les clients connectés à conserver leurs connexions si leur adresse IP change.

Topologie

Sous-réseau -- Une adresse IP par client dans ce sous-réseau

Spécifie la méthode utilisée pour fournir une adresse IP d'adaptateur virtuel aux clients lors de l'utilisation du mode TUN sur IPv4.

Certains clients peuvent exiger que cela soit mis en «sous-réseau» même pour IPv6, par exemple OpenVPN Connect (iOS / Android). Les anciennes versions d'OpenVPN (avant 2.0.9) ou les clients tels que les téléphones Yealink peuvent nécessiter "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

keepalive helper uses interval and timeout parameters to define ping and ping-restart values as follows:

ping = interval

ping-restart = timeout*2

push ping = interval

push ping-restart = timeout

Intervalle

10

Délai d'attente

60

Dépannage client avancé

ping-restart = timeout*2 push ping = interval push ping-restart = timeout	
Intervalle	10
Délai d'attente	60
Paramètres clients avancés	
Domaine DNS par défaut	<input checked="" type="checkbox"/> Renseigner un nom de domaine par défaut aux clients.
Domaine DNS par défaut	mlif.local
Activer le Serveur DNS	<input checked="" type="checkbox"/> Fournir une liste de serveur DNS pour les clients. Les adresses peuvent être en IPv4 ou IPv6.
Serveur DNS 1	8.8.8.8
Serveur DNS 2	
Serveur DNS 3	
Serveur DNS 4	
Bloquer DNS Extérieur	<input type="checkbox"/> Bloquer aux clients Windows 10 l'accès aux serveurs DNS sauf à travers OpenVPN pendant qu'ils sont connectés, forçant les clients à n'utiliser que les serveurs DNS du VPN. Requiert Windows 10 et OpenVPN 2.3.9 ou ultérieur. Seul Windows 10 est sujet à une telle fuite DNS, les autres clients vont ignorer cette option puisqu'ils ne sont pas concernés
Forcer une mise à jour du cache DNS	<input type="checkbox"/> Exécuter "net stop dnscache", "net start dnscache", "ipconfig /flushdns" et "ipconfig /registerdns" après avoir initialisé la connexion.

Forcer une mise à jour du cache DNS Exécuter "net stop dnscache", "net start dnscache", "ipconfig /flushdns" et "ipconfig /registerdns" après avoir initialisé la connexion.
Ceci est connu pour permettre à Windows de reconnaître les serveurs DNS poussés.

Activer Serveur NTP Fournir une liste de serveurs NTP aux clients

Activer NetBIOS Activer NetBIOS sur TCP/IP
Si cette option n'est pas définie, toutes les options NetBIOS-over-TCP/IP (incluant WINS) seront désactivées.

Configuration avancée

Options personnalisés

Entrez toutes les options supplémentaires à ajouter à la configuration du serveur OpenVPN ici, séparées par un point-virgule.
EXEMPLE: appuyez sur "route 10.0.0.0 255.255.255.0"

UDP Fast E/S Utilisez des opérations d'E/S rapides avec des écritures UDP sur tun / tap. Expérimental.
Optimise la boucle d'événements d'écriture de paquets, améliorant l'efficacité du processeur de 5% à 10%. Non compatible avec toutes les plates-formes, et non compatible avec la limitation de bande passante OpenVPN.

Exit Notify Send an explicit exit notification to connected clients/peers when restarting or shutting down, so they may immediately disconnect rather than waiting for a timeout. In SSL/TLS Server modes, clients may be directed to reconnect or use the next server. 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.

Tampon

Exit notify ▼

Send an explicit exit notification to connected clients/peers when restarting or shutting down, so they may immediately disconnect rather than waiting for a timeout. In SSL/TLS Server modes, clients may be directed to reconnect or use the next server. 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.

Tampon d'envoi/reception ▼

Configurez une taille de mémoire tampon d'envoi et de réception pour OpenVPN. La taille de la mémoire tampon par défaut peut être trop faible dans de nombreux cas, selon les vitesses de liaison montante du matériel et du réseau. Trouver la meilleure taille de mémoire tampon peut faire quelques expériences. Pour tester la meilleure valeur pour un site, commencez à 512KiB et testez des valeurs plus élevées et plus faibles.

Création d'une passerelle

If you assign a virtual interface to this OpenVPN server, this setting controls which gateway types will be created. The default setting is 'both'.

Niveau de verbosité ▼

Chaque niveau affiche toutes les informations des niveaux précédents. Le niveau 3 est recommandé pour un bon résumé de ce qui se passe sans être submergé par la sortie.

Aucun: Seules les erreurs fatales
 Défaut à 4: Plage d'utilisation normale
 5: Caractères R et W sur la console pour chaque paquet lu et écrit. Les majuscules sont utilisées pour les paquets TCP/UDP et les minuscules sont utilisées pour les paquets TUN/TAP.
 6-11: plage d'informations de débogage

◀ pfSense is developed and maintained by Netgate. © ESF 2004 - 2025 [View license](#). ▶

Avant de configurer la configuration du client vpn, on va mettre une règle dans firewall , rules et openvpn:

Rules (Drag to Change Order)

<input type="checkbox"/>	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	✓ 0/2.65	IPv4 *	10.0.8.0/24	*	*	*	*	*		none	

6- Configuration du client VPN :

Configurer le client VPN avec les paramètres suivants :

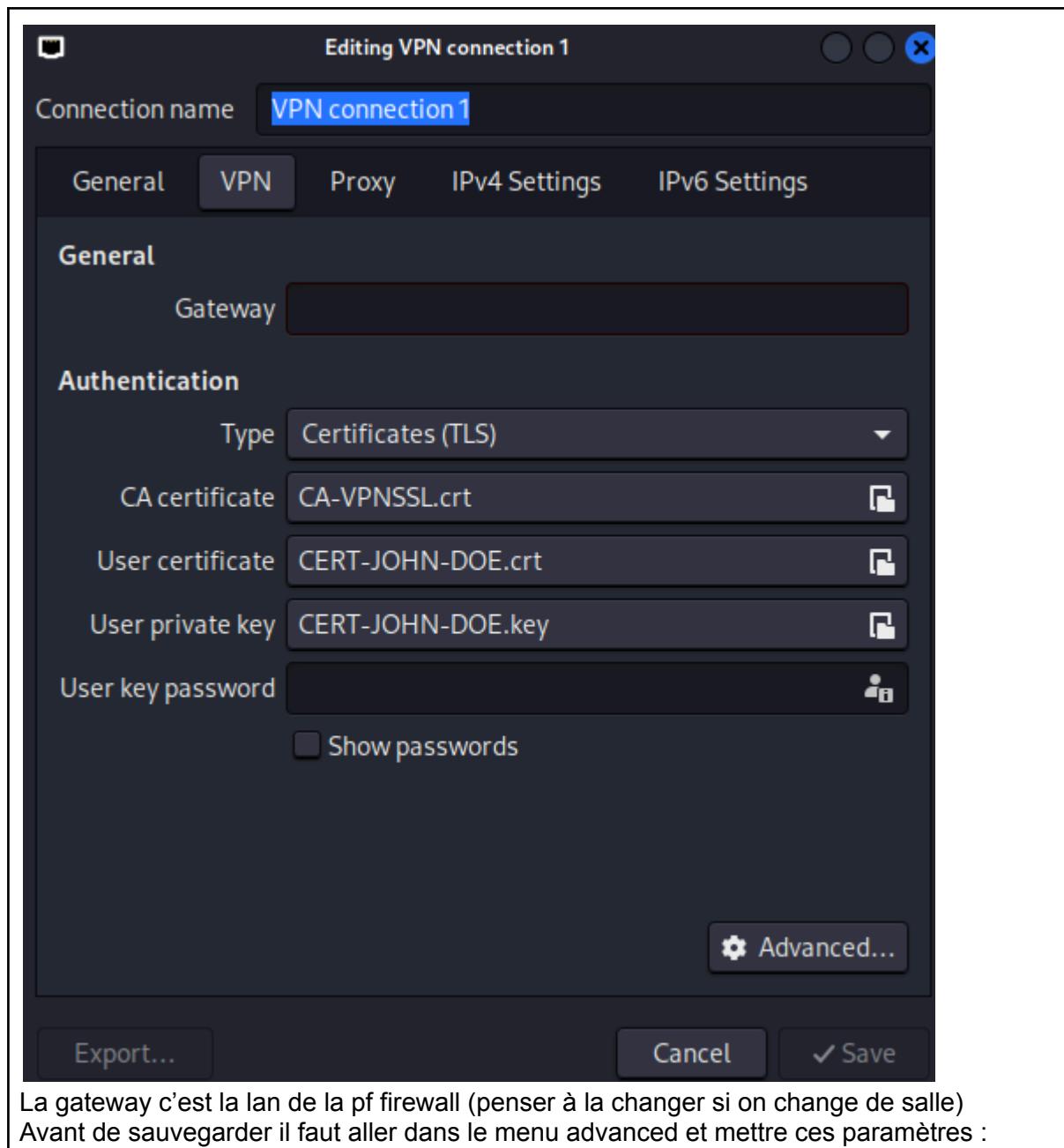
+

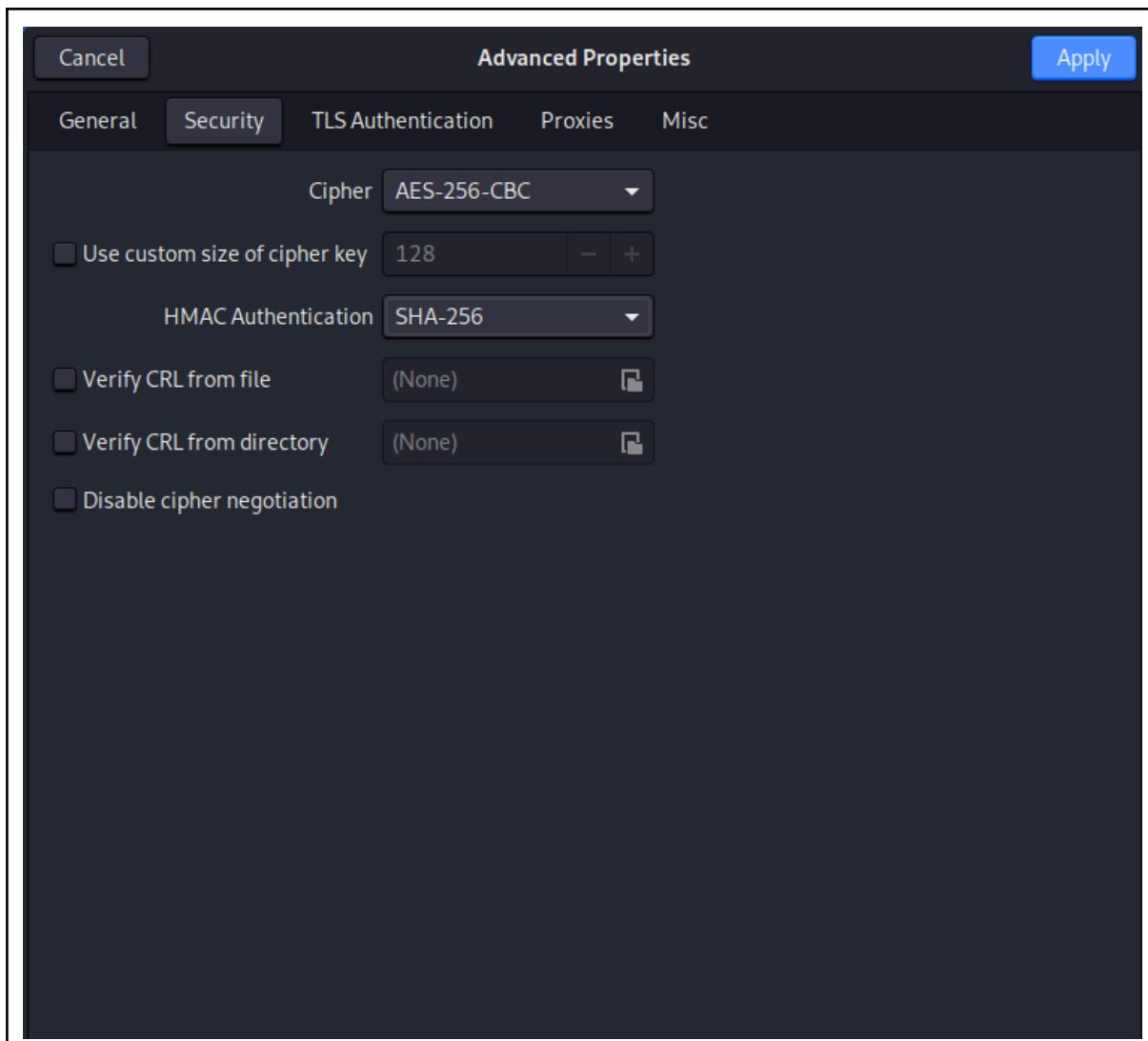
VPN

- Layer 2 Tunneling Protocol (L2TP)
- Cisco AnyConnect or OpenConnect (OpenConnect)
- Juniper Network Connect (OpenConnect)
- Palo Alto Networks GlobalProtect (OpenConnect)
- Pulse Connect Secure (OpenConnect)
- F5 BIG-IP SSL VPN (OpenConnect)
- Fortinet SSL VPN (OpenConnect)
- Array SSL VPN (OpenConnect)
- OpenVPN
- Point-to-Point Tunneling Protocol (PPTP)
- Cisco Compatible VPN (vpnc)
- Import a saved VPN configuration...

On prend openvpn (il faut scroller)

On a donc ces paramètres :

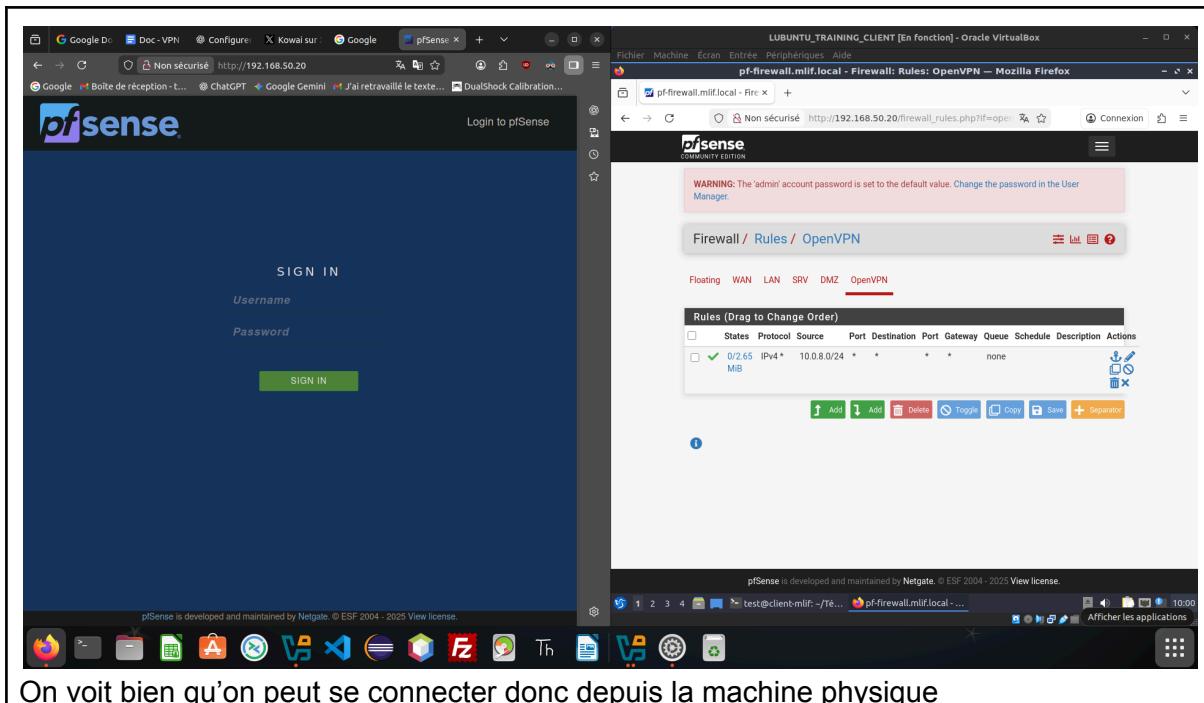




On ping donc l'adresse de la pfsense (la lan) :

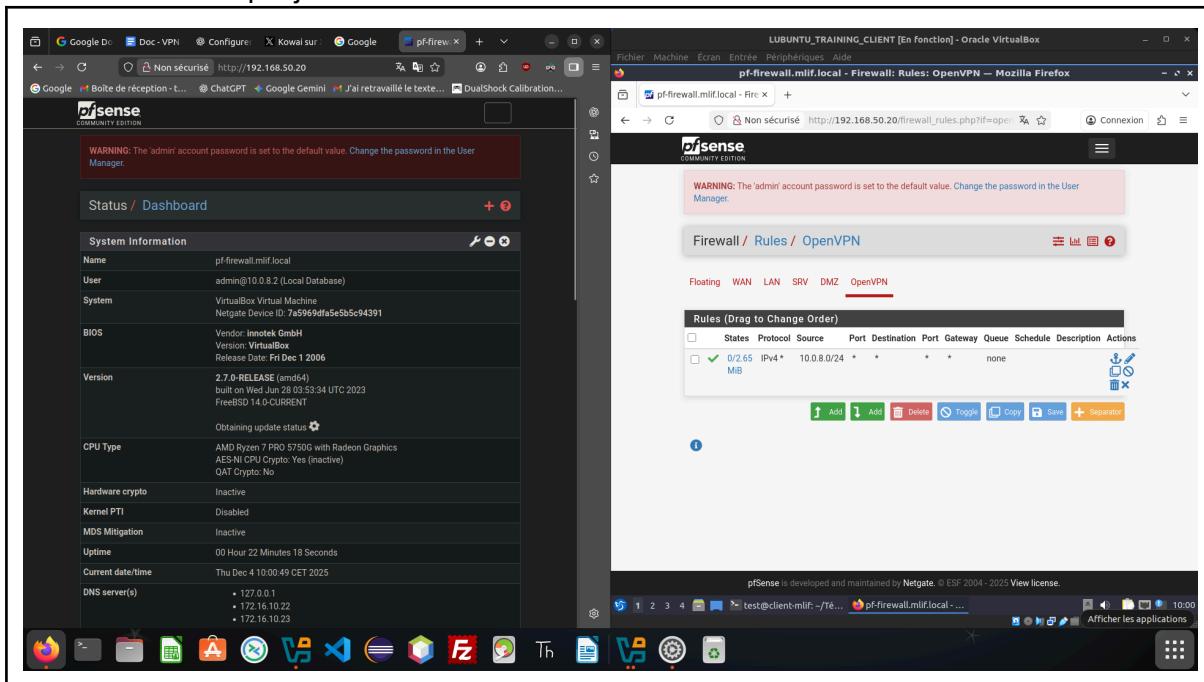
```
root@archa:/home/test# ping 192.168.50.20
PING 192.168.50.20 (192.168.50.20) 56(84) bytes of data.
64 bytes from 192.168.50.20: icmp_seq=8 ttl=64 time=0.510 ms
64 bytes from 192.168.50.20: icmp_seq=9 ttl=64 time=0.248 ms
64 bytes from 192.168.50.20: icmp_seq=10 ttl=64 time=0.366 ms
```

On se connecte donc au firewall :



On voit bien qu'on peut se connecter donc depuis la machine physique

Et là on voit donc que je suis connecté :



STOP 3

Les règles doivent ressembler à ça :

Firewall / Rules / WAN

Floating WAN LAN SRV DMZ OpenVPN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/> 1/36.96 MiB	IPv4 UDP	*	*	WAN address	1194 (OpenVPN)	*	none			
<input checked="" type="checkbox"/> 12/110 KiB	IPv4	*	*	*	*	*	none			

Add Add Delete Toggle Copy Save Separator

Firewall / Rules / LAN

Floating WAN LAN SRV DMZ OpenVPN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/> 0/0 B	*	*	*	LAN Address	80	*	*		Anti-Lockout Rule	
<input checked="" type="checkbox"/> 0/0 B	IPv4 TCP	LAN net	*	*	22 (SSH)	*	none			
<input checked="" type="checkbox"/> 0/62 KiB	IPv4	*	*	*	*	*	none			

Add Add Delete Toggle Copy Save Separator

Firewall / Rules / SRV

Floating WAN LAN SRV DMZ OpenVPN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/> 0/0 B	IPv4	*	*	*	*	*	none			

Add Add Delete Toggle Copy Save Separator

Firewall / Rules / DMZ

Floating WAN LAN SRV DMZ OpenVPN

Rules (Drag to Change Order)

States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input checked="" type="checkbox"/> 0/0 B	IPv4	*	*	*	*	*	none			

Add Add Delete Toggle Copy Save Separator

Firewall / Rules / OpenVPN

Floating WAN LAN SRV DMZ **OpenVPN**

Rules (Drag to Change Order)

	States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
<input type="checkbox"/>	57/37.83 MiB	IPv4 *	10.0.8.0/24	*	*	*	*	none			

Add Add Delete Toggle Copy Save Separator