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

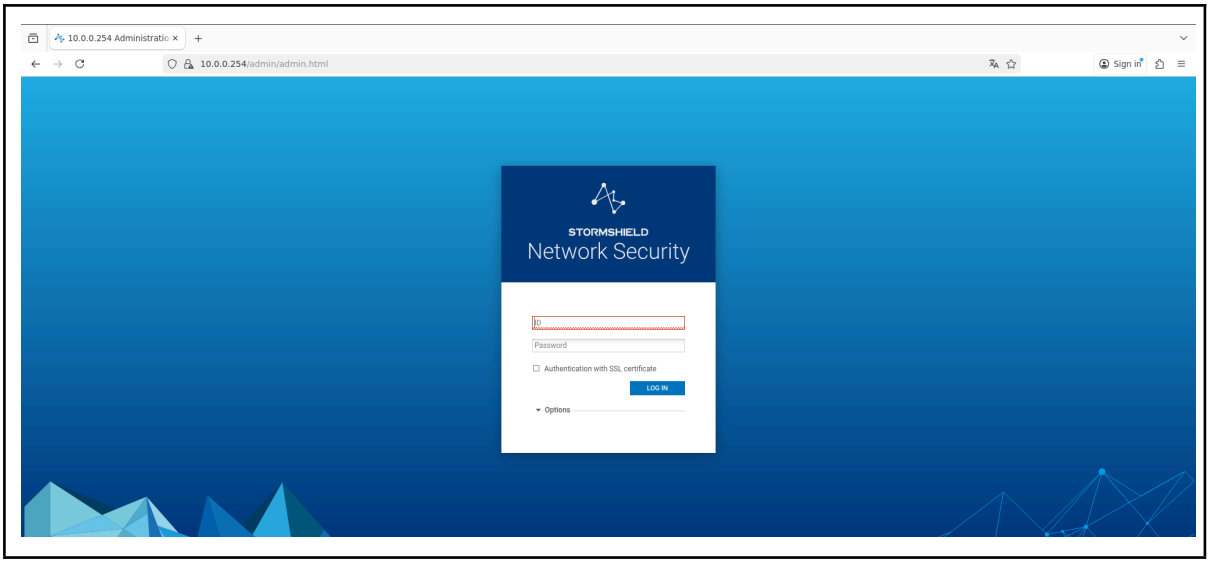
INTERFACE	RÉSEAU VIRTUALBOX	NOM DU RÉSEAU	ADRESSAGE IP
1ère interface	Réseau interne	LAN-TOULOUSE	192.168.50.1/24

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

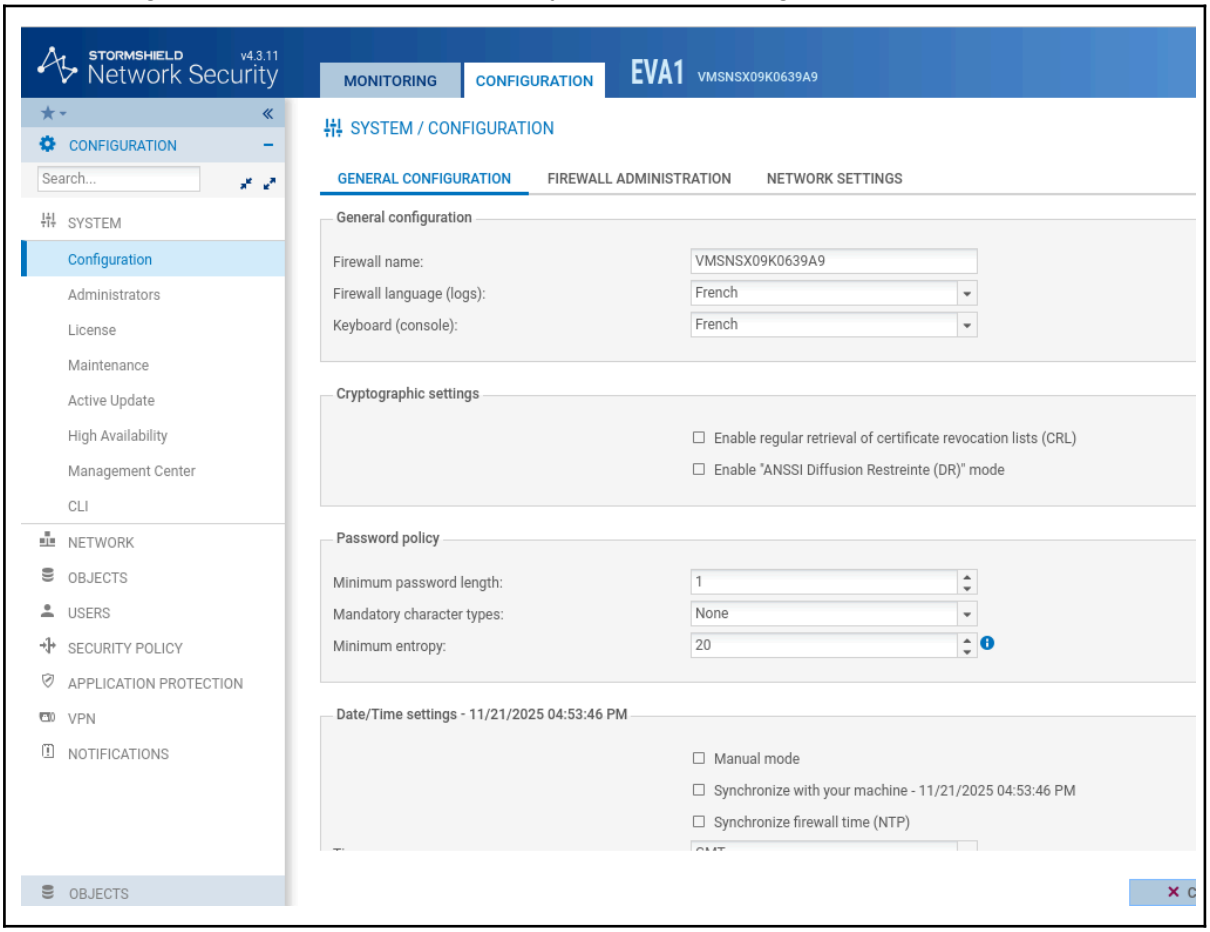
Dans un premier temps, le firewall est livré en configuration d'usine dans un bridge d'adresse IP 10.0.0.254.
Confiurer le client de toulouse avec la configuration IP suivante :
• adresse IP : 10.0.0.1/24 ;
• passerelle : 10.0.0.254.
Puis, se connecter au firewall de toulouse avec le navigateur en saisisant : 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



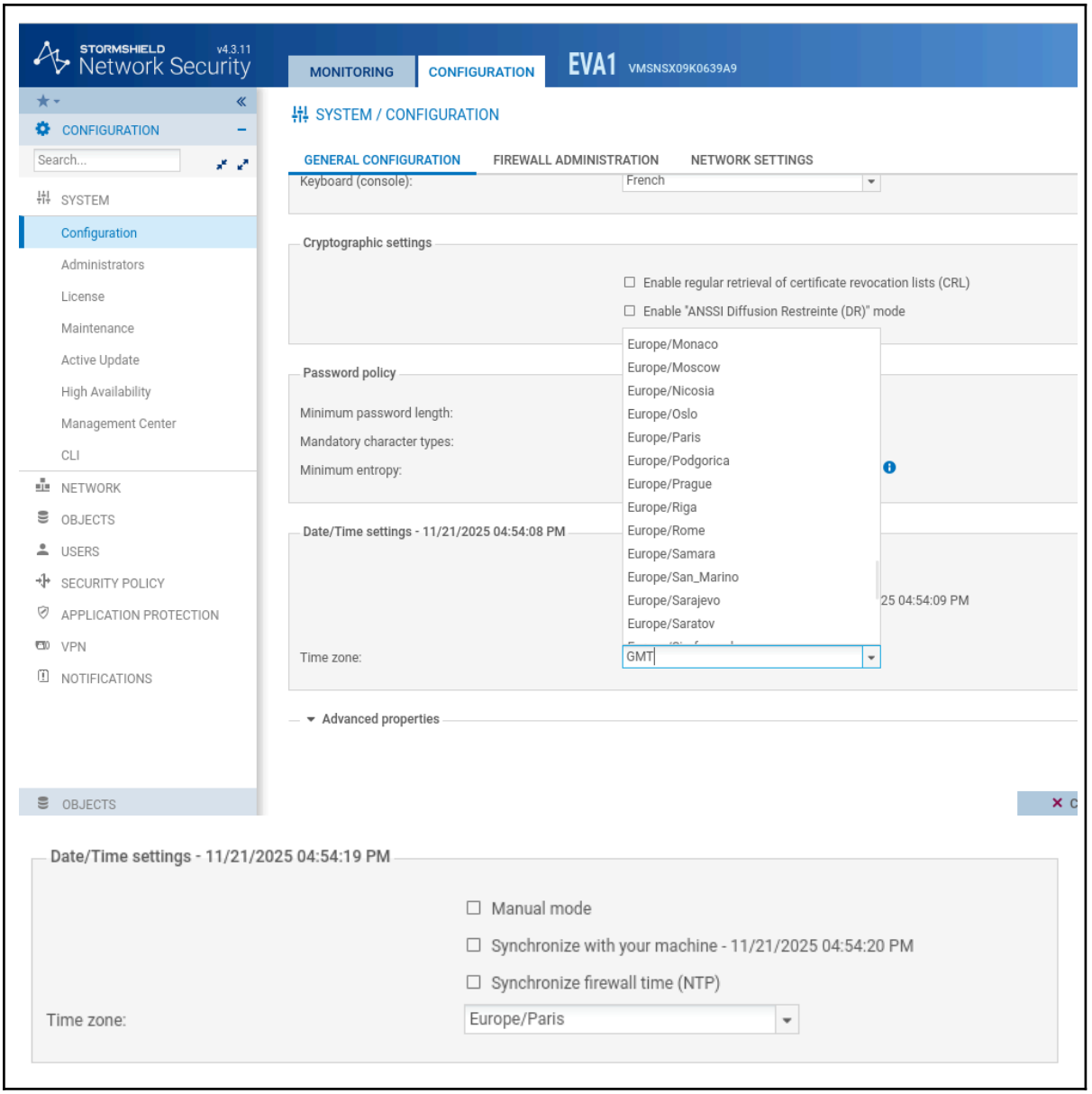
Il faut mettre la langue du firewall en français, modifier le mot de passe par défaut et renommer le firewall.
Pour cela, vous aurez besoin d'obtenir le droit d'écriture sur le firewall (voir en haut à droite en cliquant sur admin).

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

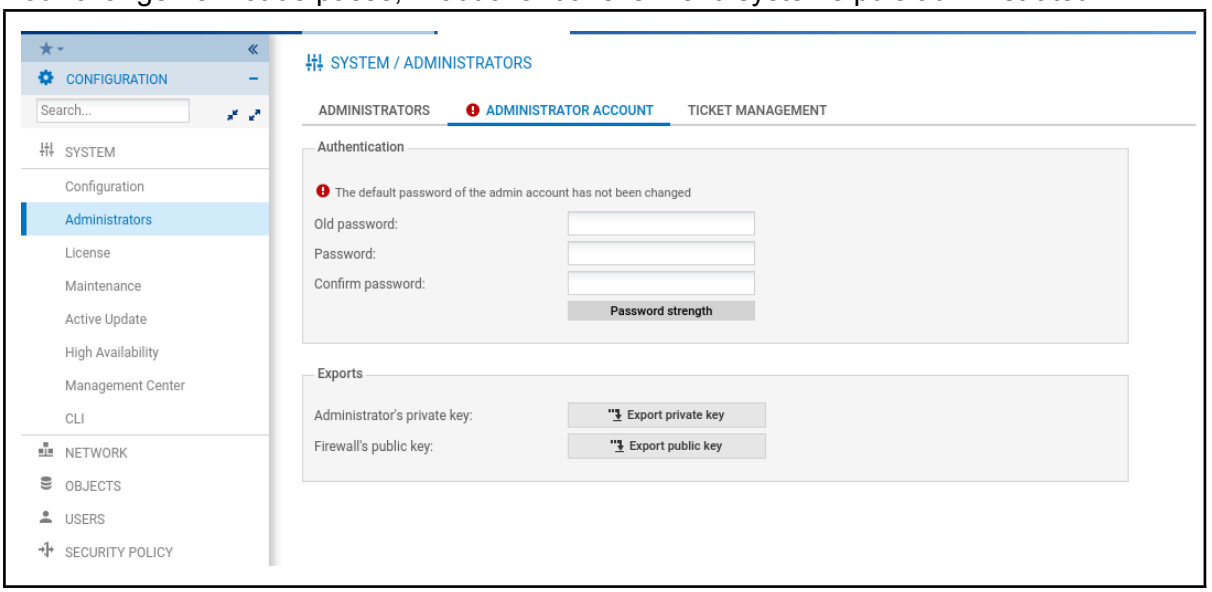
Pour la langue, il faut aller dans le menu système puis configuration.



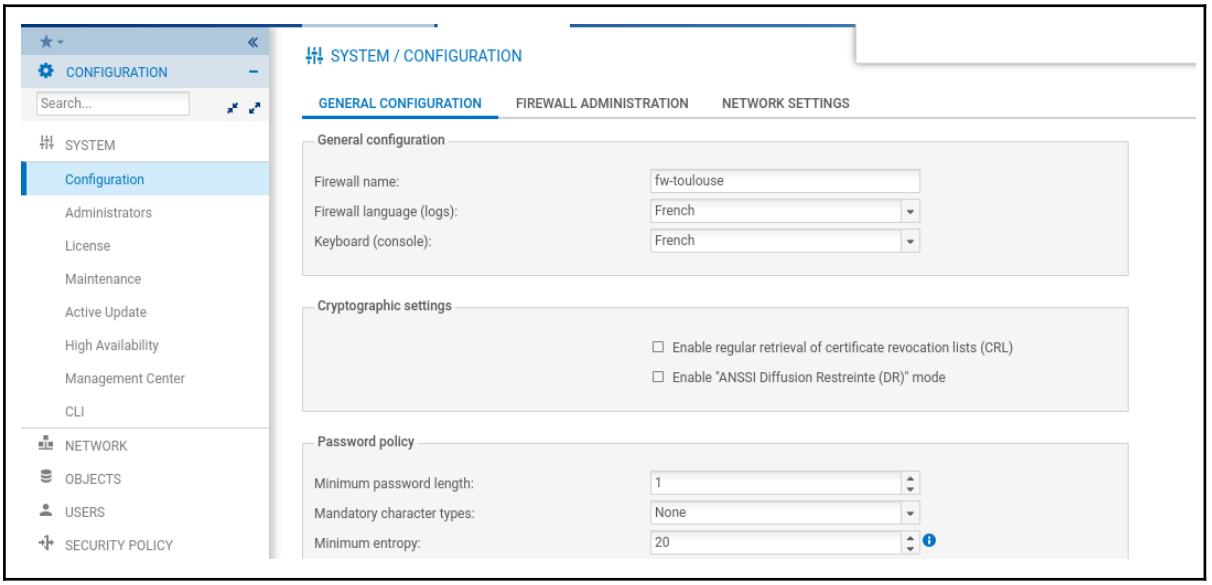
Mettre aussi le bon fuseau horaire.



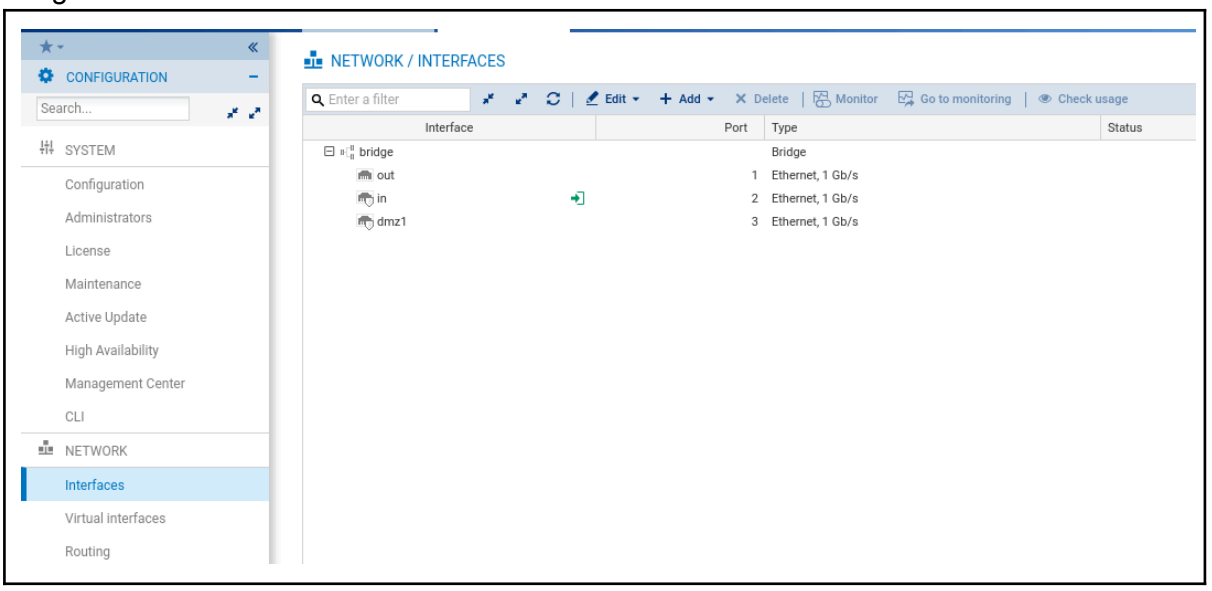
Pour changer le mot de passe, il faut aller dans le menu système puis administrateur.



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



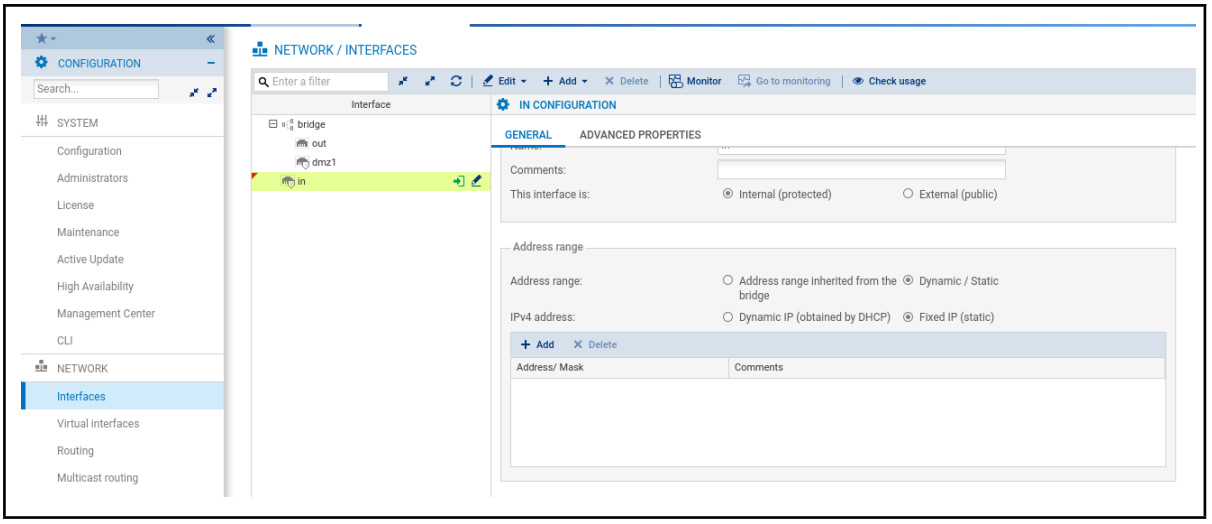
Cliquer sur réseau puis sur interfaces. Les trois interfaces out, in et dmz seront sorties du bridge.



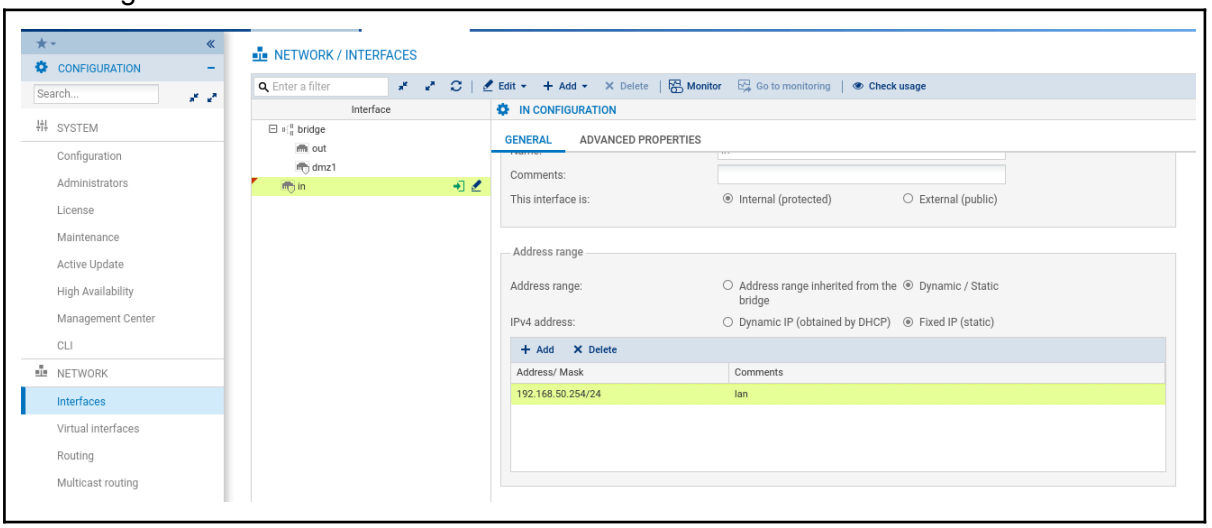
Double cliquer sur interface in. Cocher les deux options suivantes :

• Dynamique/statique ;

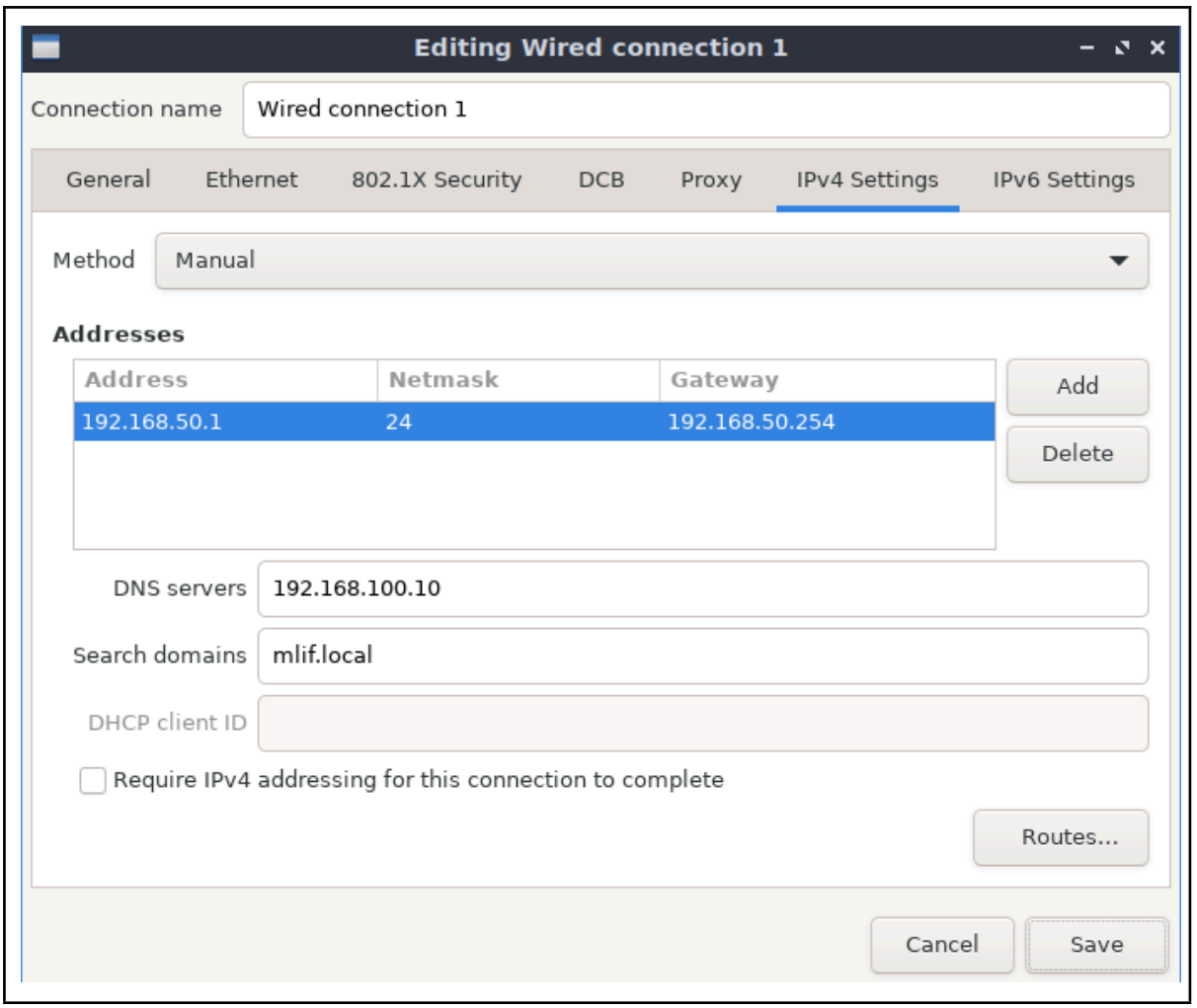
• Ip fixe (statique).



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.



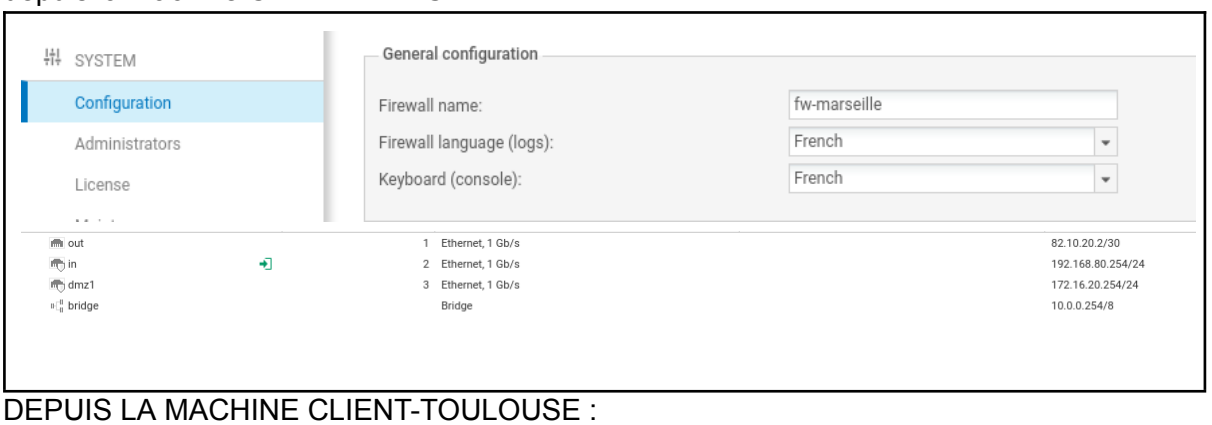
Modifier ensuite l'adressage IP du client de toulouse conformément au plan d'adressage puis se connecter à nouveau au firewall.


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, mofifier les configurations IP des deux autres interfaces dmz (dmz-toulouse) et out (nuage-internet conformément au plan d'adressage puis valider)

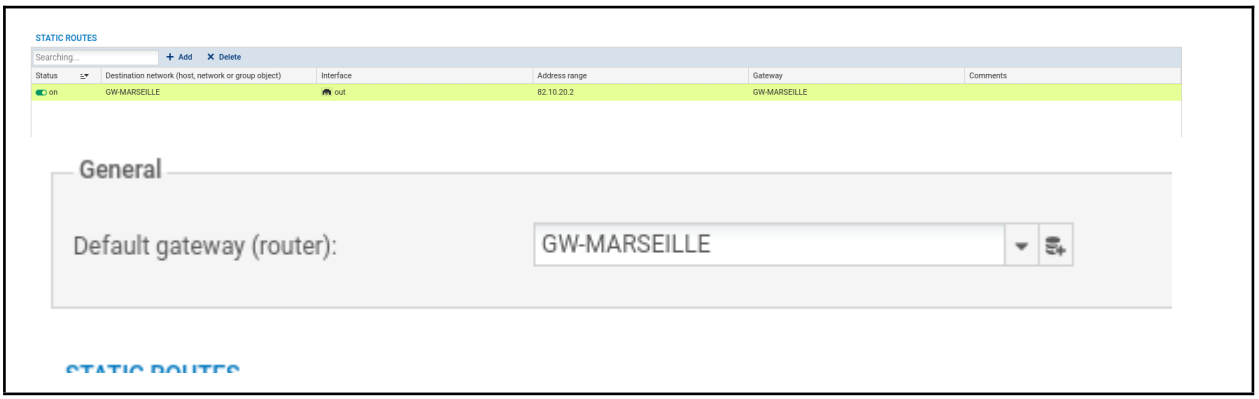
DEPUIS LA MACHINE CLIENT-MARSEILLE:

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.

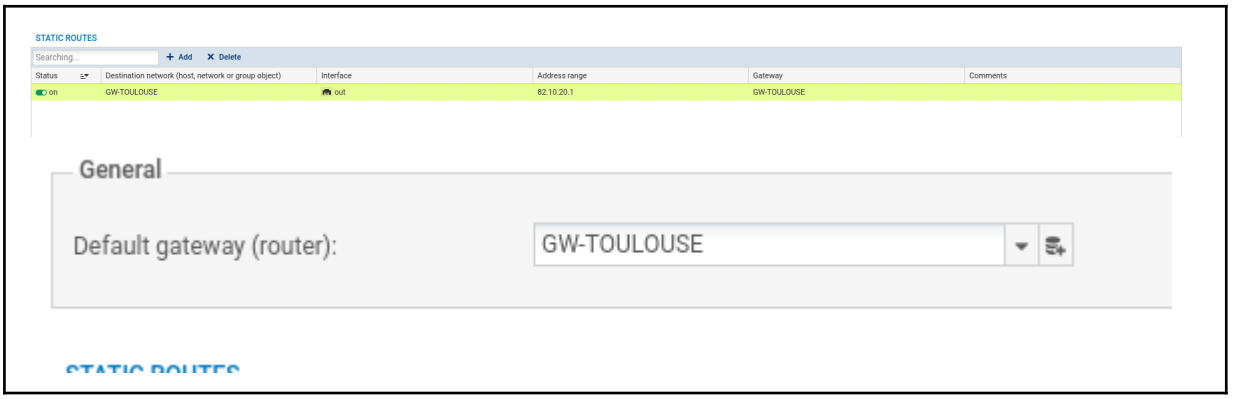


DEPUIS LA MACHINE CLIENT-TOULOUSE :

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.

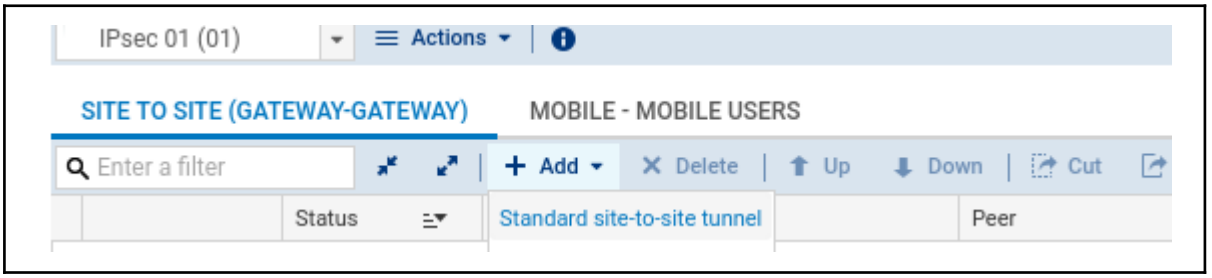


DEPUIS LA MACHINE CLIENT-MARSEILLE:
Faire de même sur le boitier de Marseille en configurant la passerelle par défaut via un objet nommé GW-TOULOUSE d'adresse IP 82.10.20.1/30

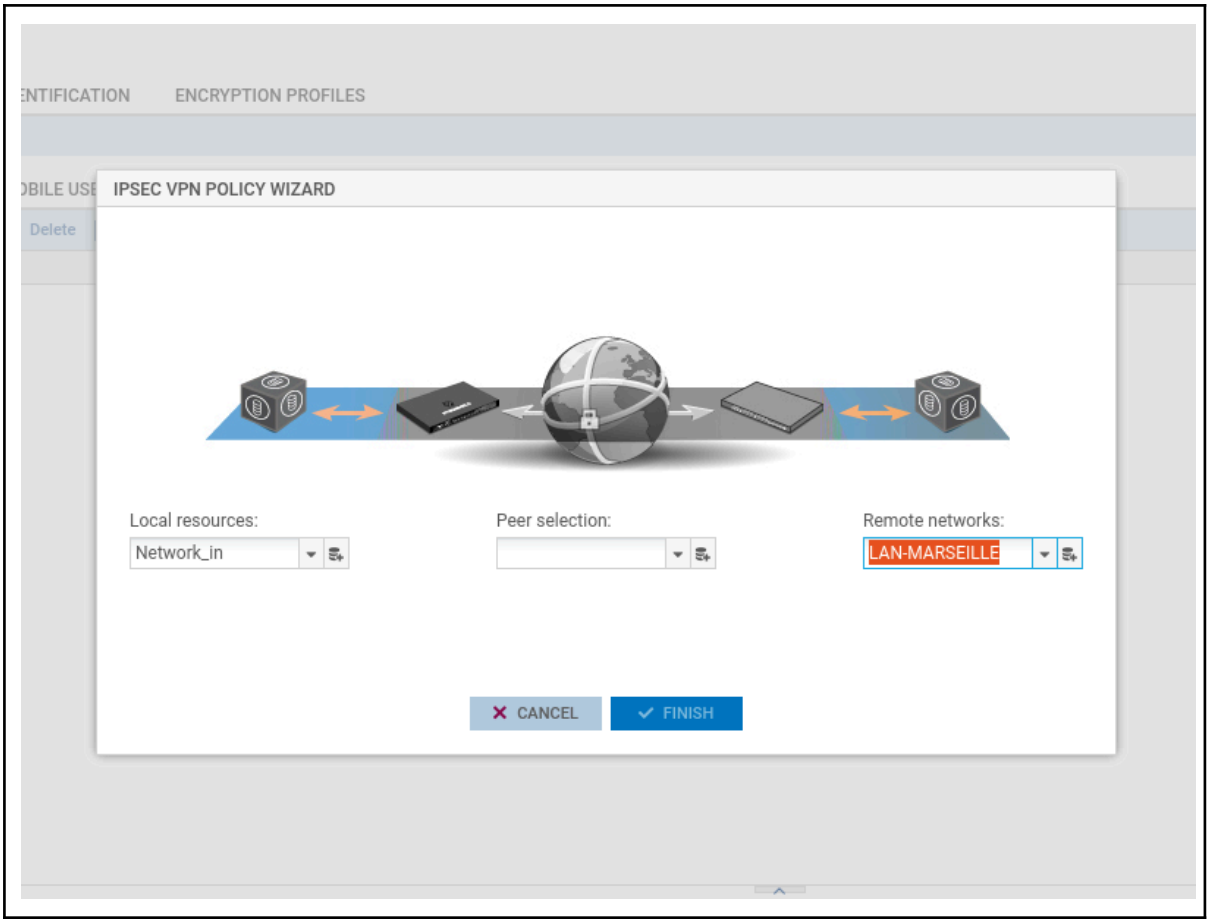


STOP 1

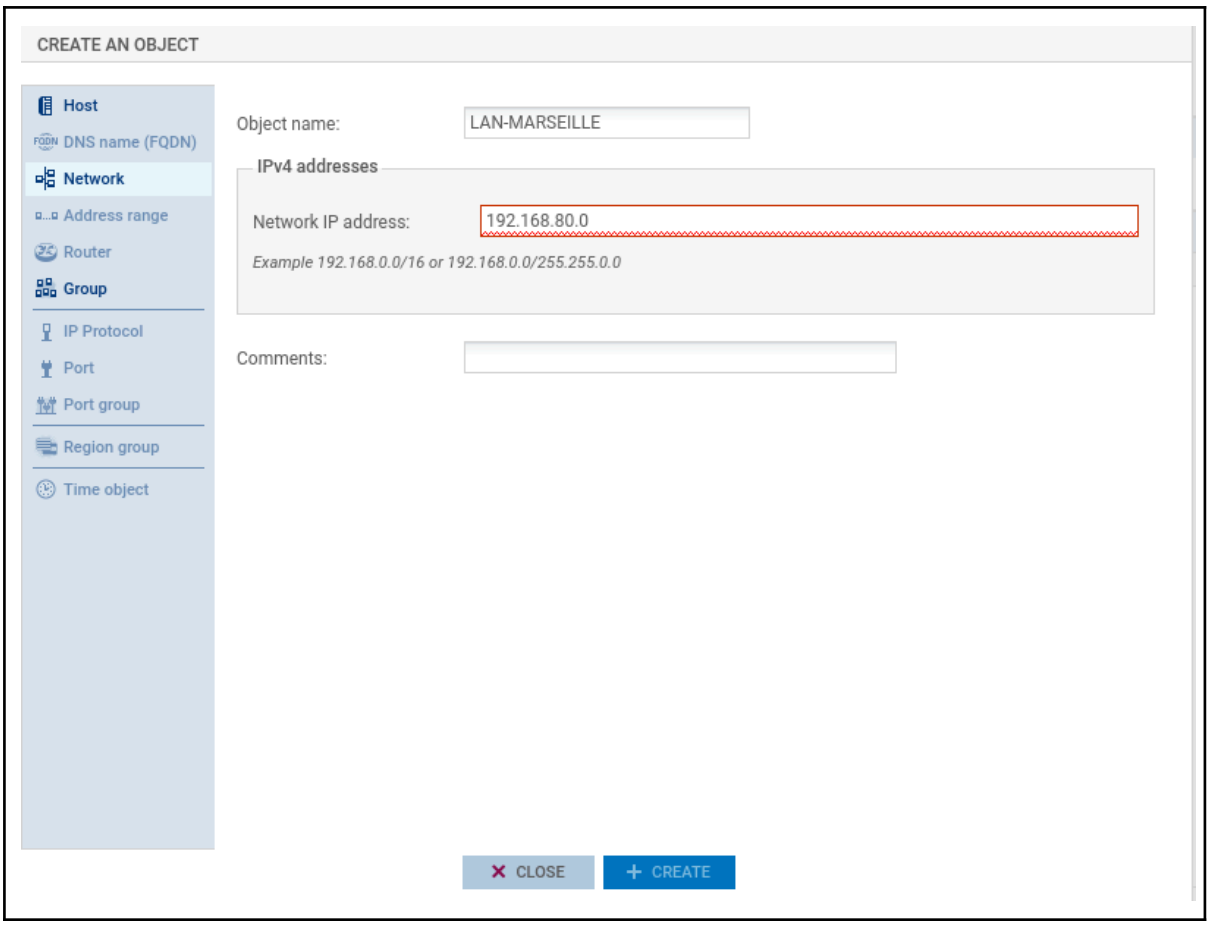
DEPUIS LA MACHINE CLIENT-TOULOUSE :
1- Configuration du tunnel :
Cliquer sur VPN puis sur VPN Ipsec. Dans l'onglet Site à site, cliquer sur Ajouter puis sur tunnel site à site.



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

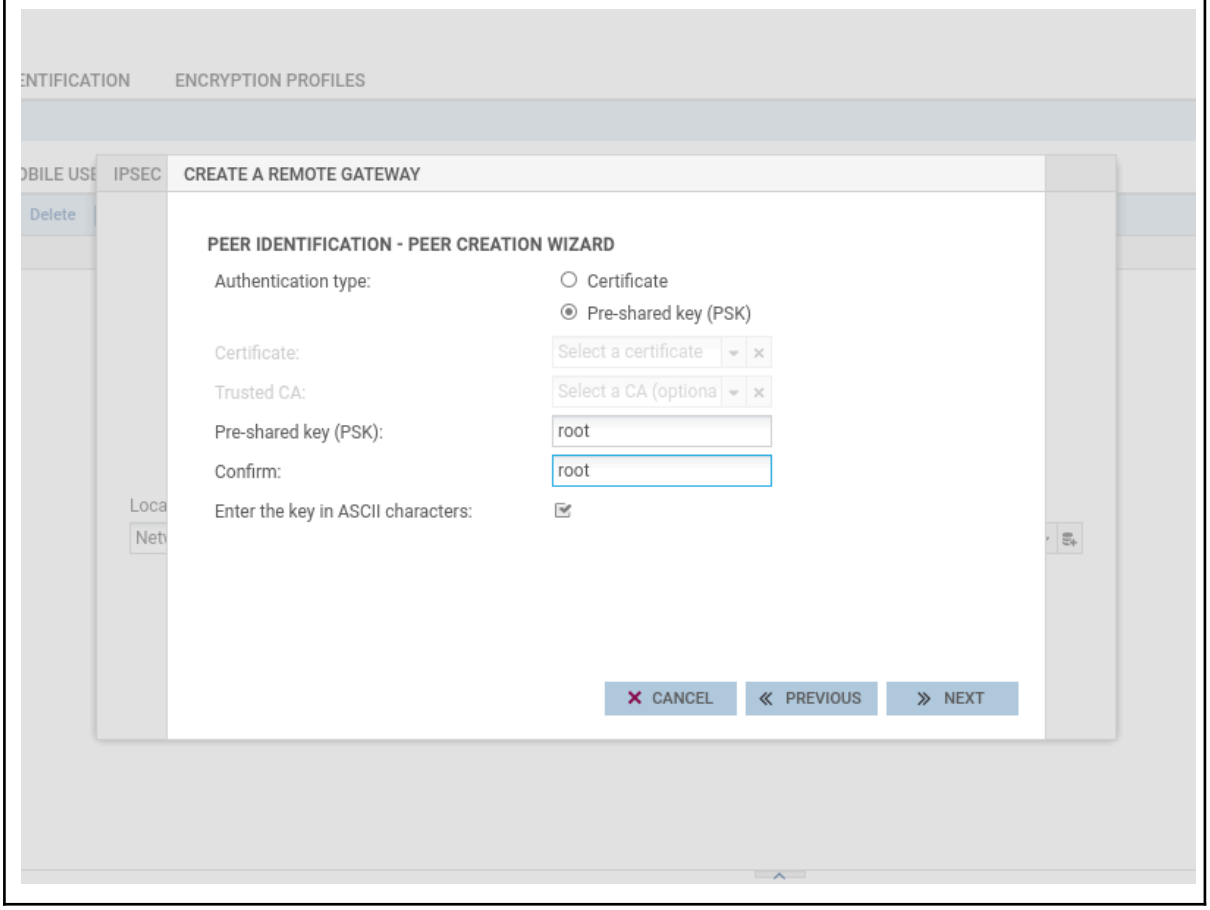


Dans Réseau Distant, créer un objet correspond au LAN de Marseille soit 192.168.80.0/24 et nommez le LAN-MARSEILLE.

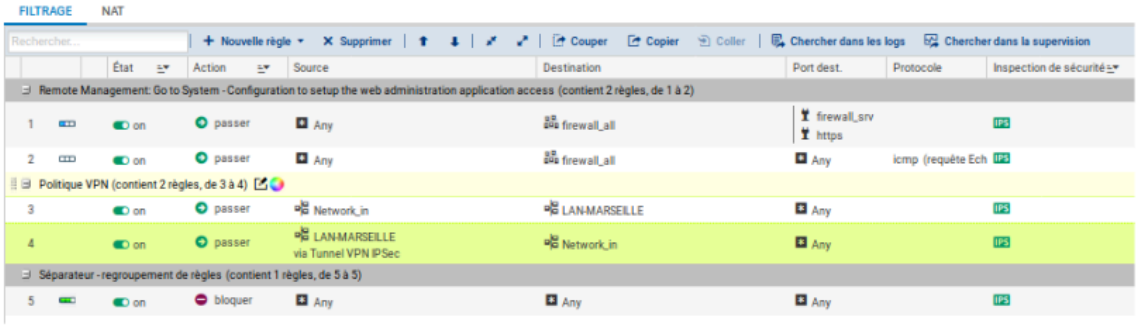


Dans Choix du correspondant, créer un objet de type IKEv2 en indiquant l'adresse de l'interface out du firewall de Marseille soit 82.10.20.2. Nommer cet objet FW-MARSEILLE.
Le wizard préfixe alors automatiquement le nom du correspondant avec Site_.
Cliquer ensuite sur suivant puis sélectionner clé partagée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


ENTIFICATION
ENCRYPTION PROFILES
OBILE USE
IPSEC
CREATE A REMOTE GATEWAY
Delete
SELECT THE GATEWAY - PEER CREATION WIZARD
Remote gateway:
GW-MARSEILLE
Name:
FW-MARSEILLE
IKE version:
IKEv2
CANCEL
PREVIOUS
NEXT

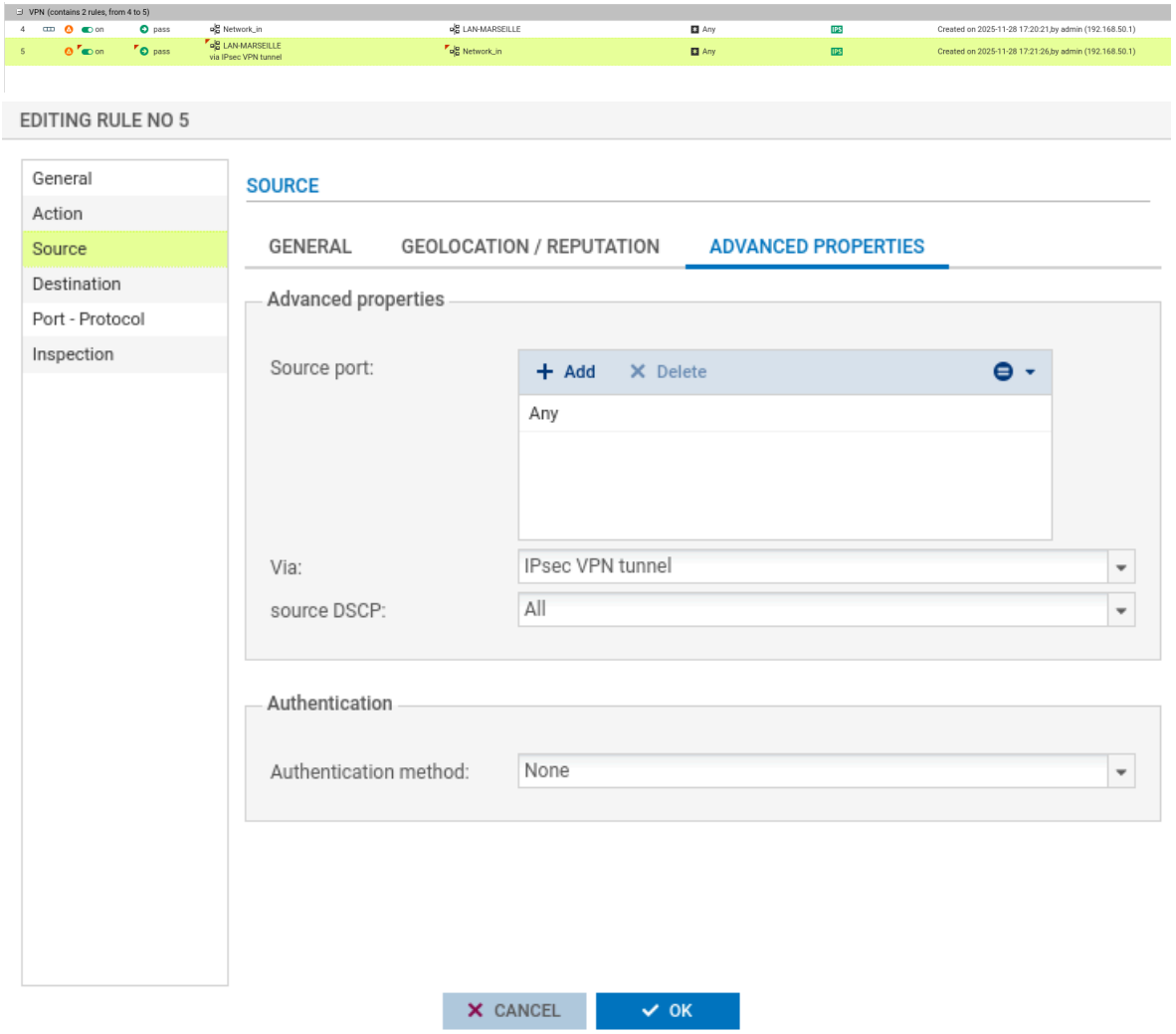

ENTIFICATION
ENCRYPTION PROFILES
OBILE USE
IPSEC
CREATE A REMOTE GATEWAY
Delete
PEER IDENTIFICATION - PEER CREATION WIZARD
Authentication type:
Certificate
Pre-shared key (PSK)
Certificate:
Select a certificate
Trusted CA:
Select a CA (optiona
Pre-shared key (PSK):
root
Confirm:
root
Enter the key in ASCII characters:
CANCEL
PREVIOUS
NEXT

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



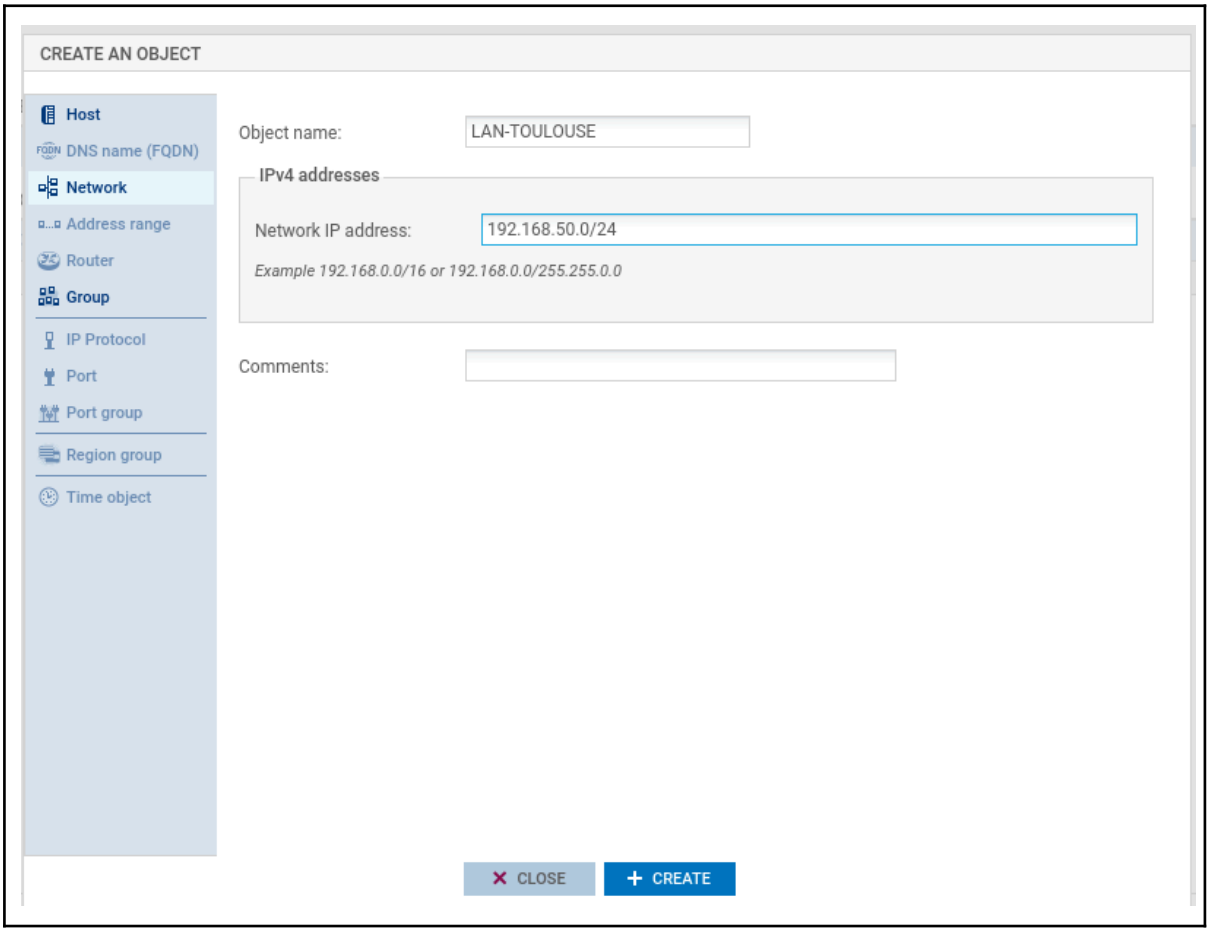
Il faut donc ajouter les règles 3 et 4 de la capture d'écran ci-dessus. Pour créer ces rèles de filtrage, utiliser l'omnibox et n'oubliez pas l'option **via Tunnel Ipsec** dans le champ sour ce de la règle numéro 4. Remarquez que cette configuration est très permissive car le port de destination est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

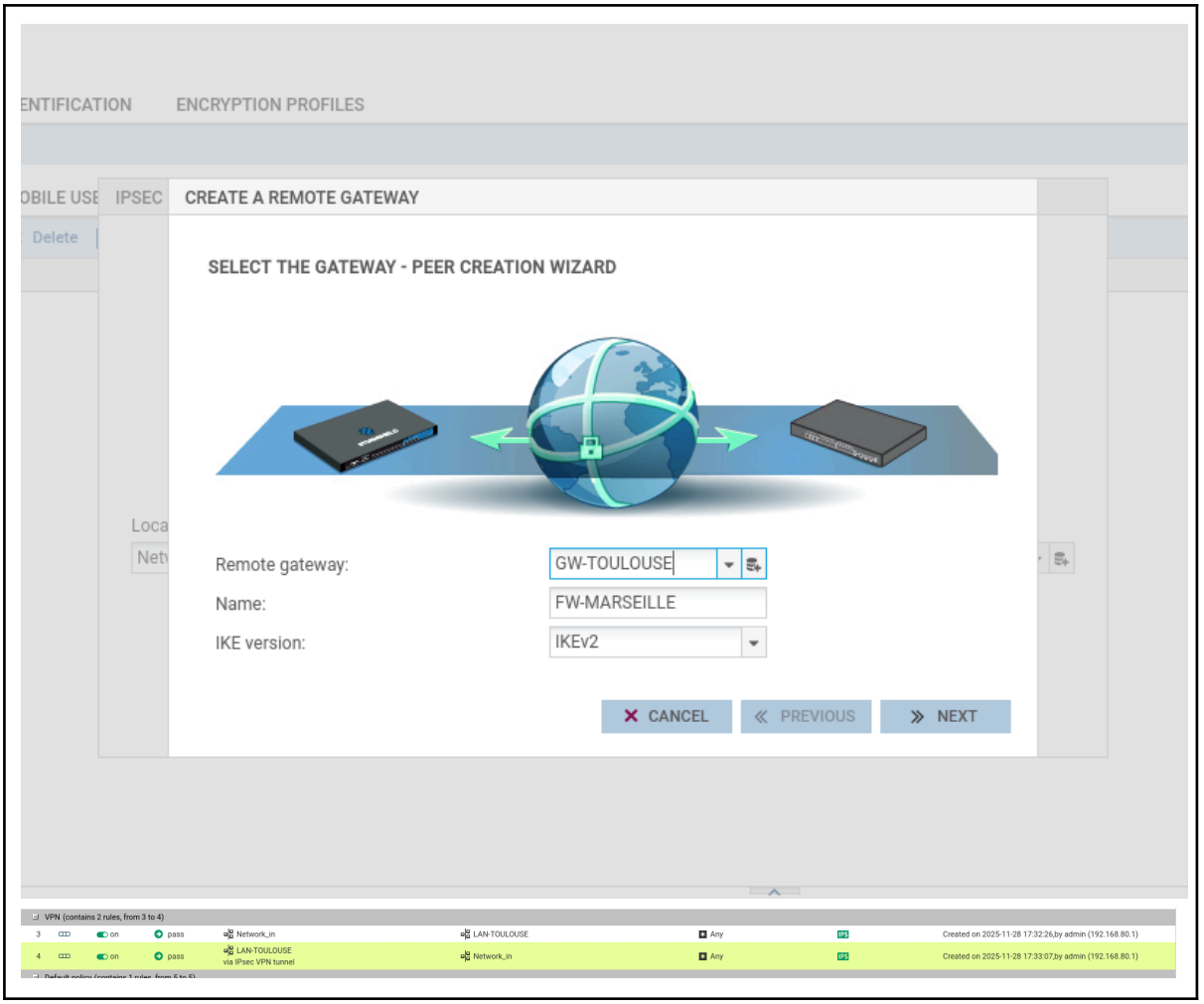
On a donc ajouté ces 2 règles :



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

DEPUIS LA MACHINE CLIENT-MARSEILLE:
Reproduire les mêmes étapes que précédement en les adaptant sur le firewall du site de Marseille

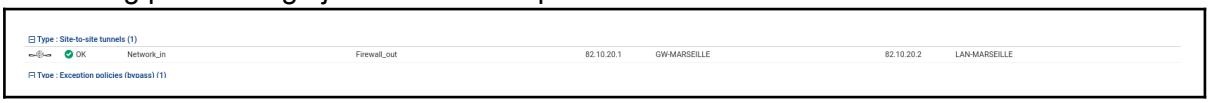




DEPUIS LA MACHINE CLIENT-TOULOUSE:
Ouvrir un terminal et faire un ping vers 192.168.80.1. Ce ping doit aboutir.

Validé dans les 2sens

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



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

Autority attributes

Organization: mlif

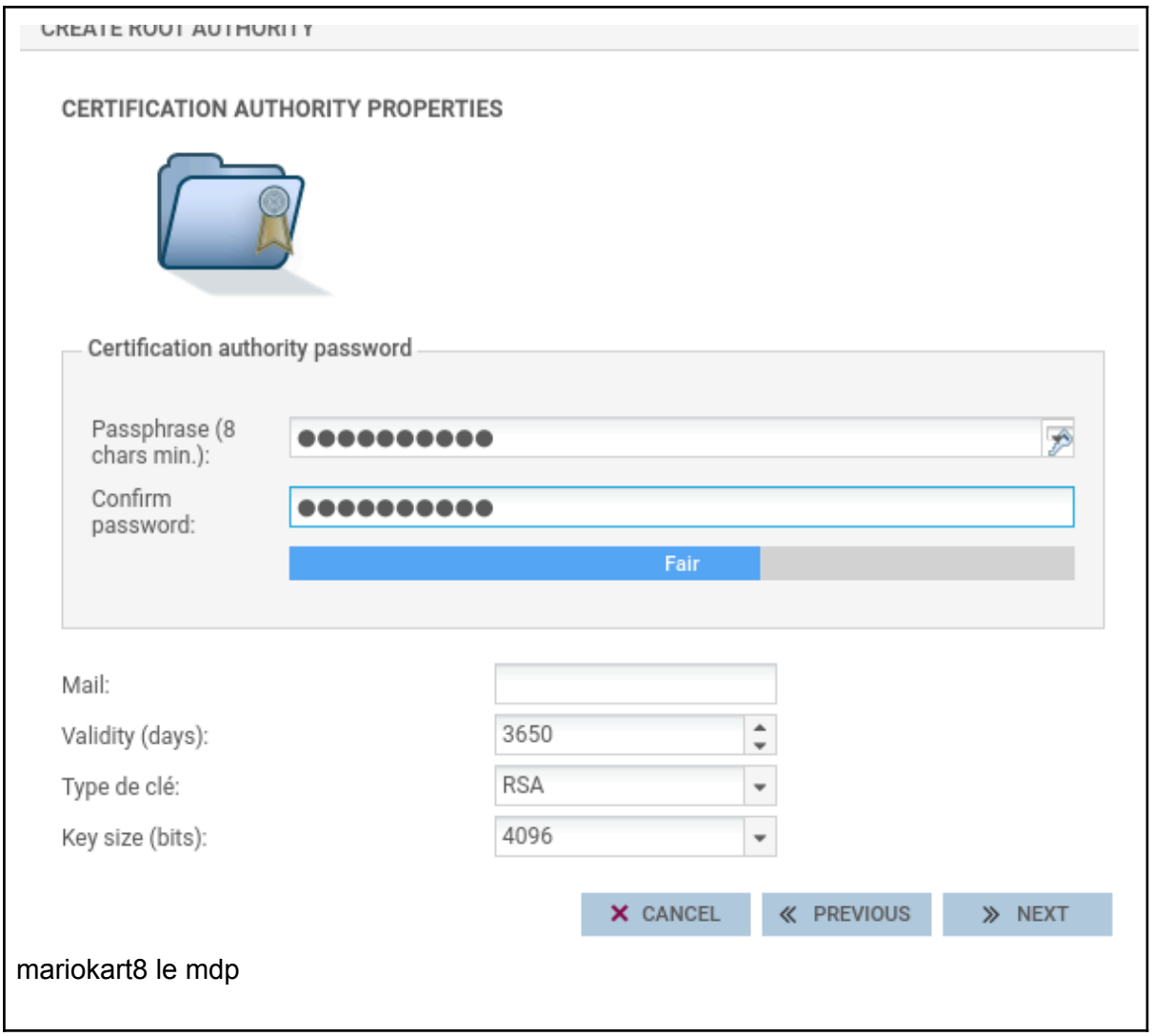
Organizational unit: mlif

City (L): toulouse

State (ST): occitanie

Country: France

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.

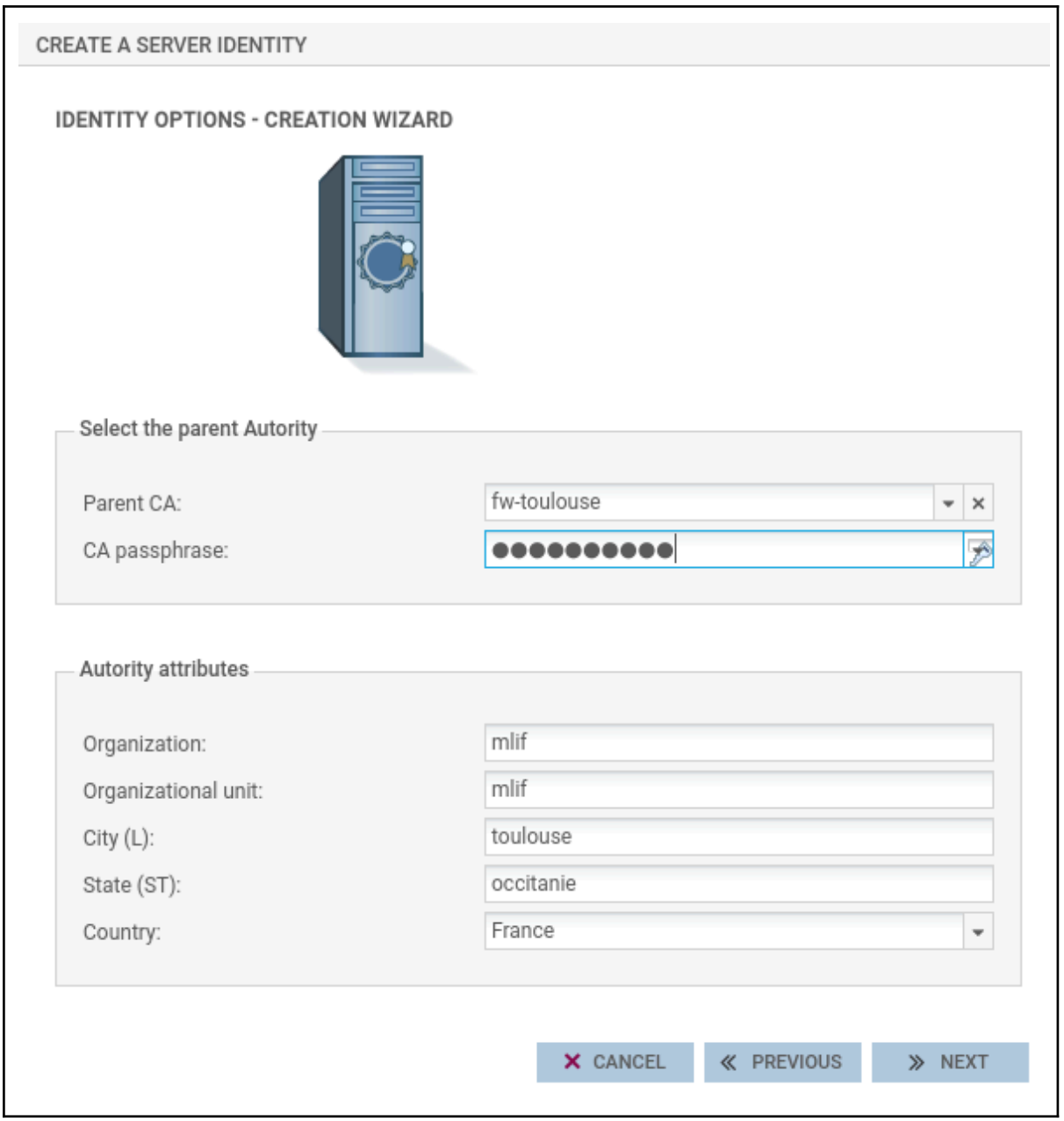
CREATE A SERVER IDENTITY

IDENTITY OPTIONS - CREATION WIZARD

Fully Qualified Domain Name (FQDN): fw-toulouse.mlif.local

ID: fw-toulouse.mlif.local

CANCEL PREVIOUS NEXT



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 defaut. 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).

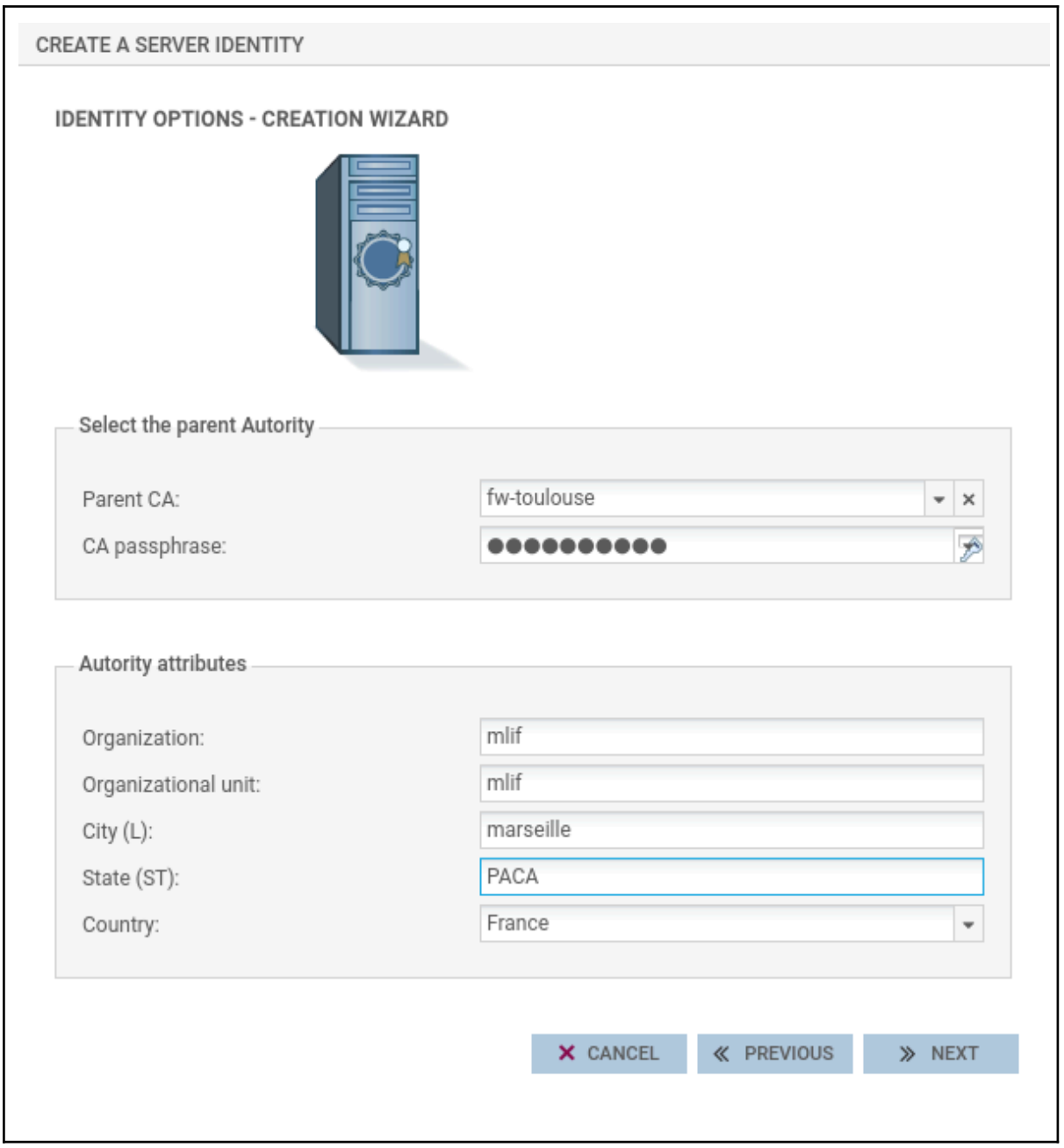
CREATE A SERVER IDENTITY

IDENTITY OPTIONS - CREATION WIZARD

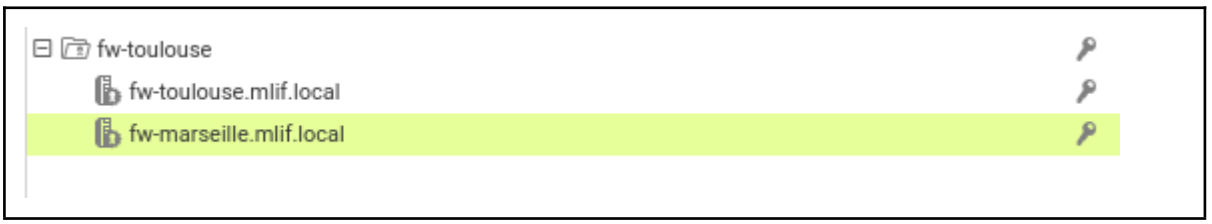
Fully Qualified Domain Name (FQDN): fw-marseille.mlif.local

ID: fw-marseille.mlif.local

CANCEL PREVIOUS NEXT

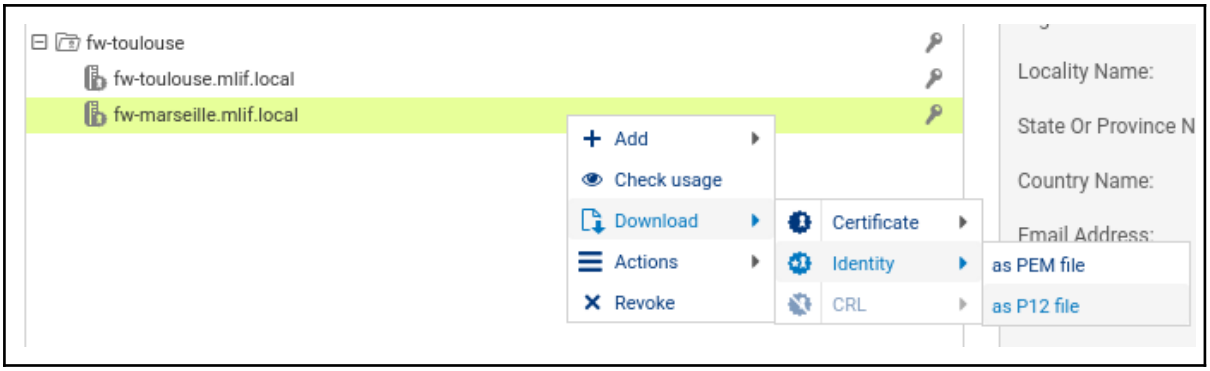


Vous devez obtenir l'arborescence suivante :



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 envoyer 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
```

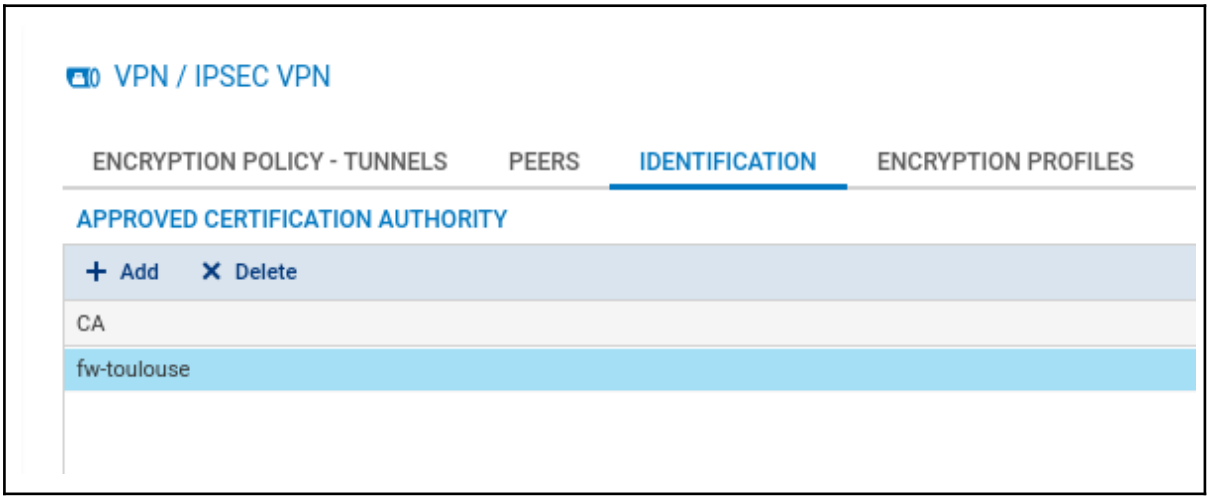
DEPUIS LA MACHINE CLIENT-MARSEILLE:

Cliquer sur objets puis sur certificats et PKI. Ensuite, cliquer sur ajouter puis sur importer un fichier et sélectionner le certificat envoyé par scp. Dans la boite de dialogue, sélectionner le format P12 et choisir d'importer tous les élements.

Vous devriez obtenir ceci :

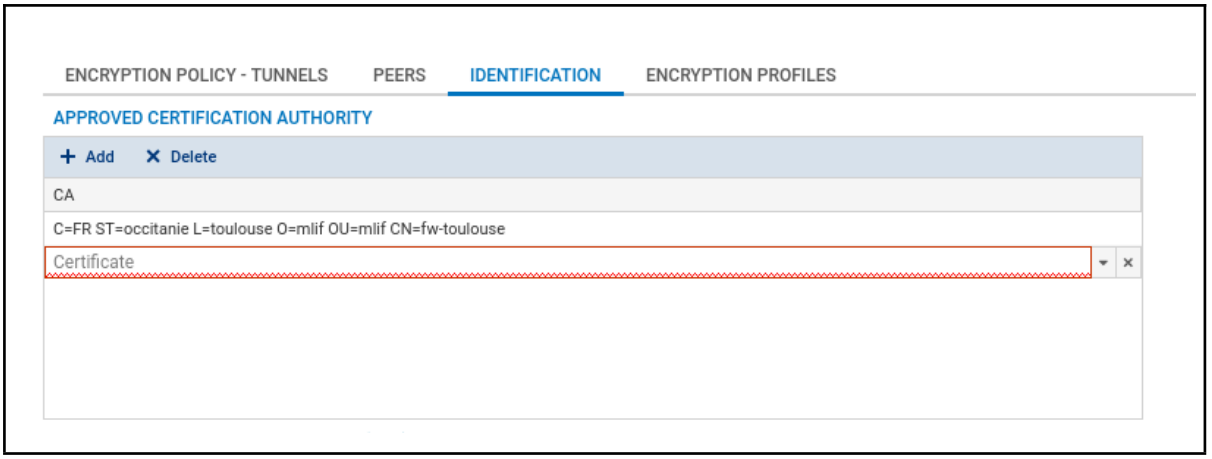
DEPUIS LA MACHINE CLIENT-TOULOUSE:

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



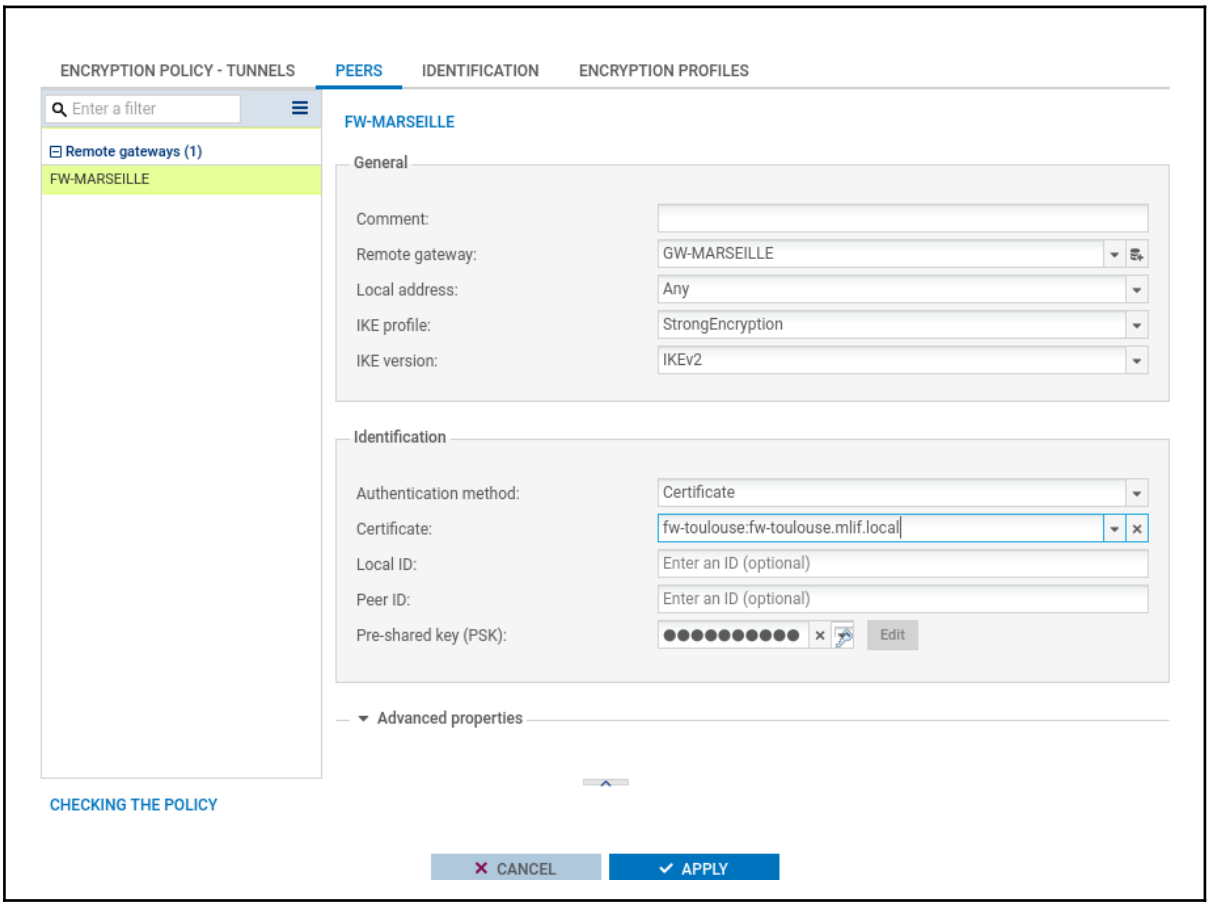
DEPUIS LA MACHINE CLIENT-MARSEILLE:

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



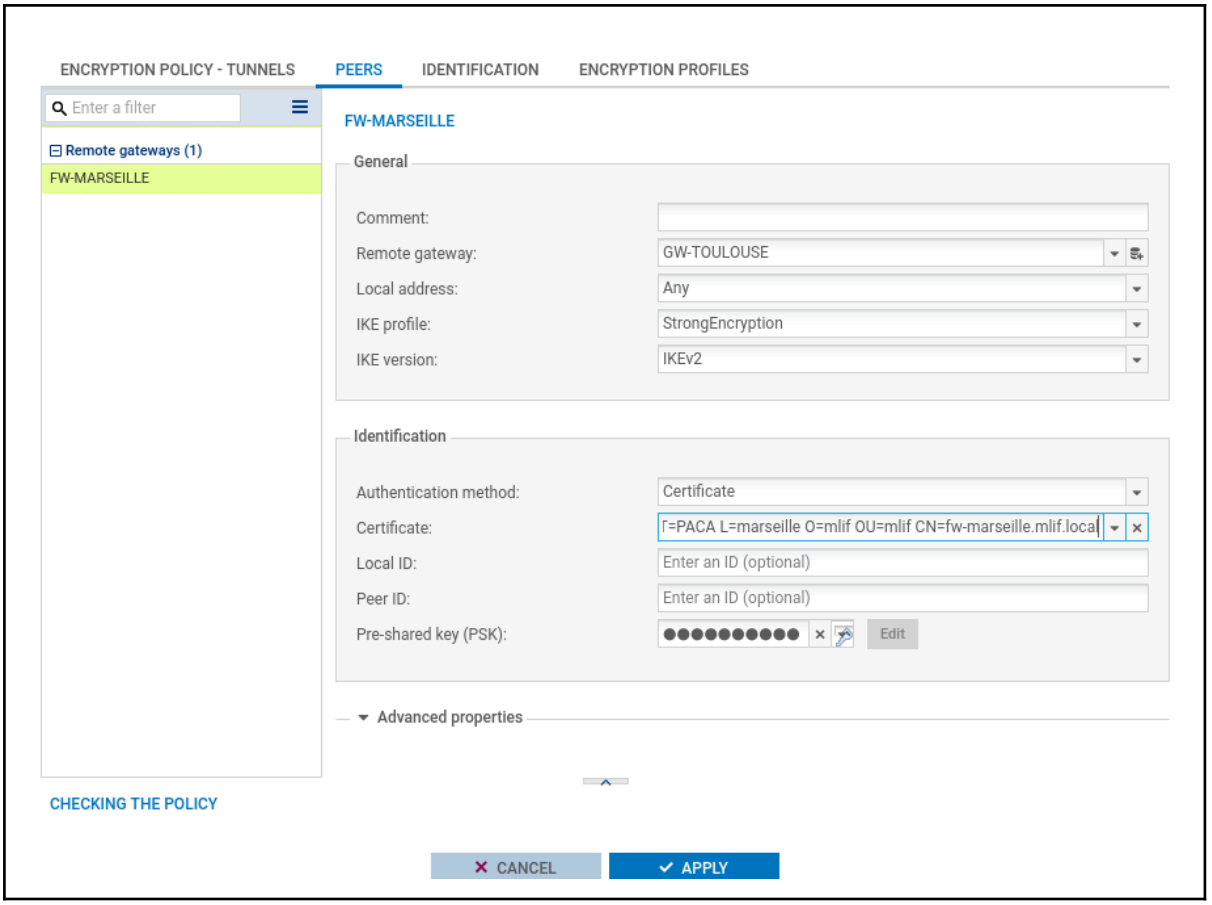
DEPUIS LA MACHINE CLIENT-TOULOUSE:

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.



DEPUIS LA MACHINE CLIENT-MARSEILLE:

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



7- Test du tunnel :

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

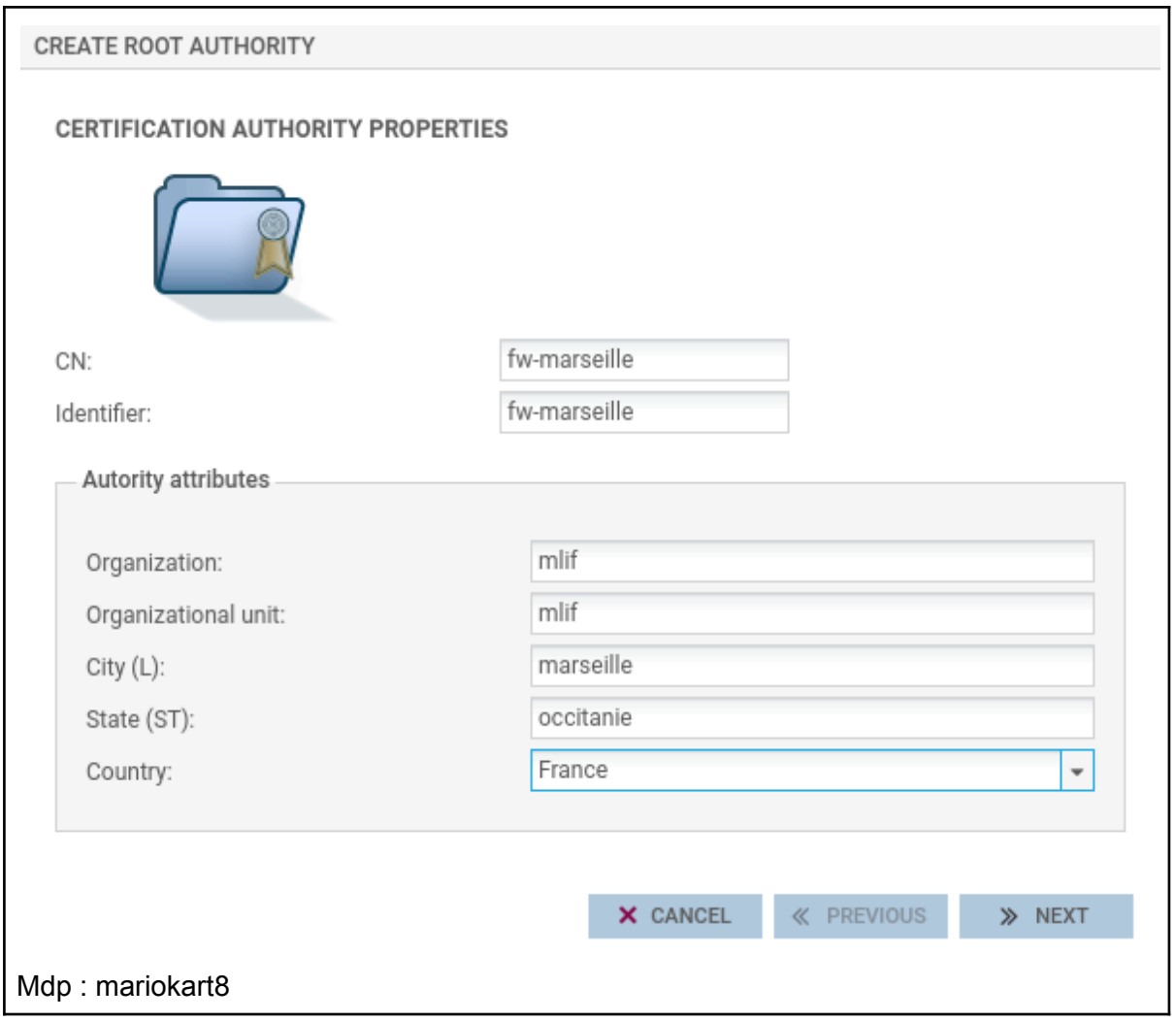
Tunnel 2 validé

DEPUIS LA MACHINE CLIENT-MARSEILLE:

1- Création de la CA de Marseille :

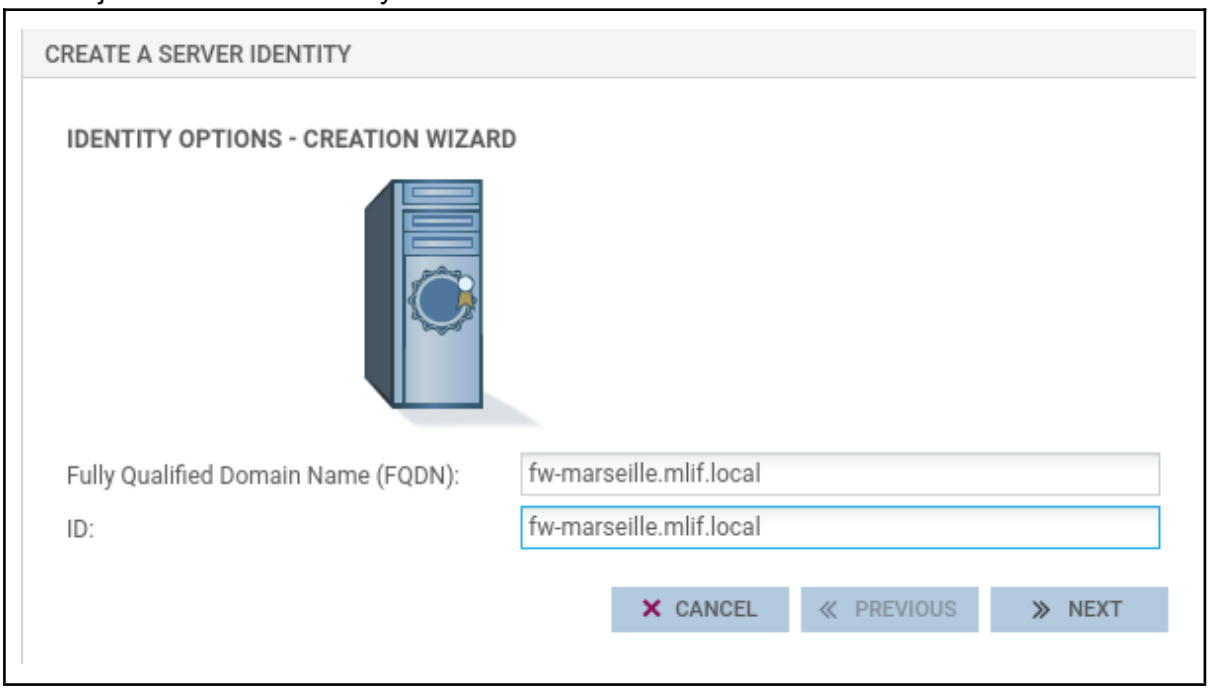
En prenant appui sur le travail précédemment réalisé , créer une CA propre au site de Marseille. Cette CA servira à signer le futur certificat du firewall de Marseille.

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



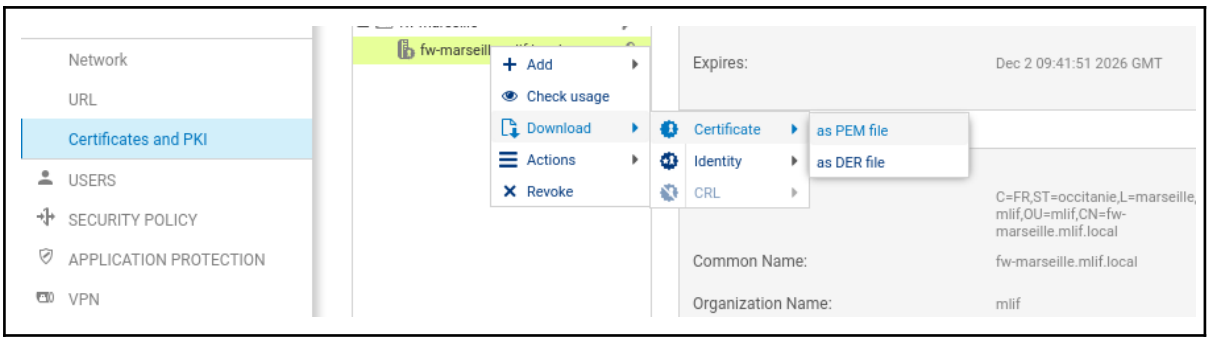
Mdp : mariokart8

Il faut ajouter le server identity :



On met suivant on rentre le mdp et suivant suivant

On va telecharger le certificat de marseille en format pem :



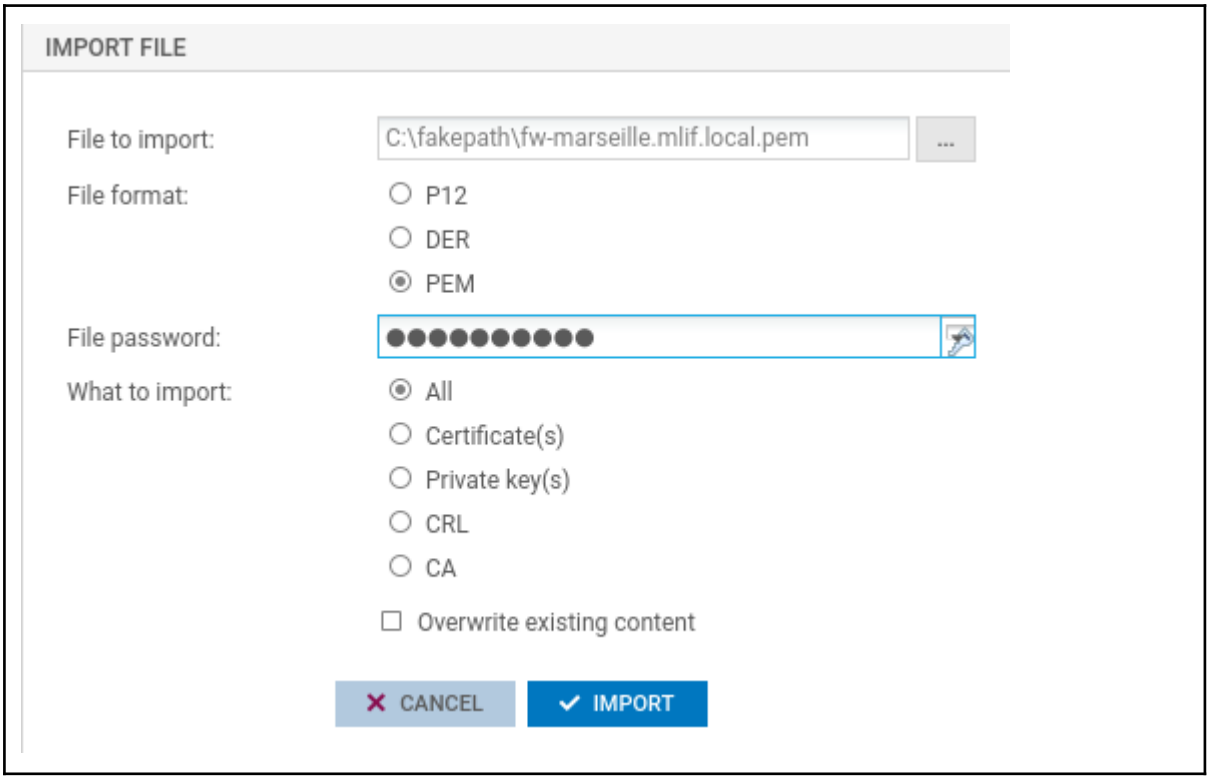
On rentre la commande scp pour transférer le certificat

```
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:

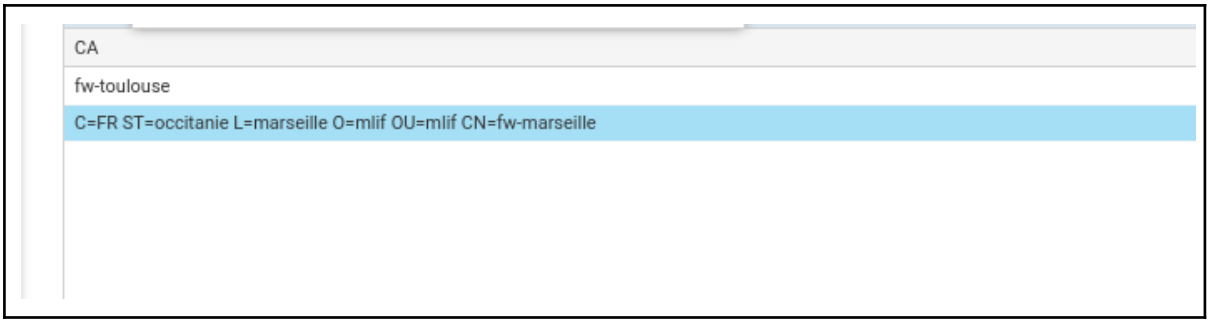
1- Import de la CA de Marseille :

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.



2- Acceptation de la CA de Marseille :

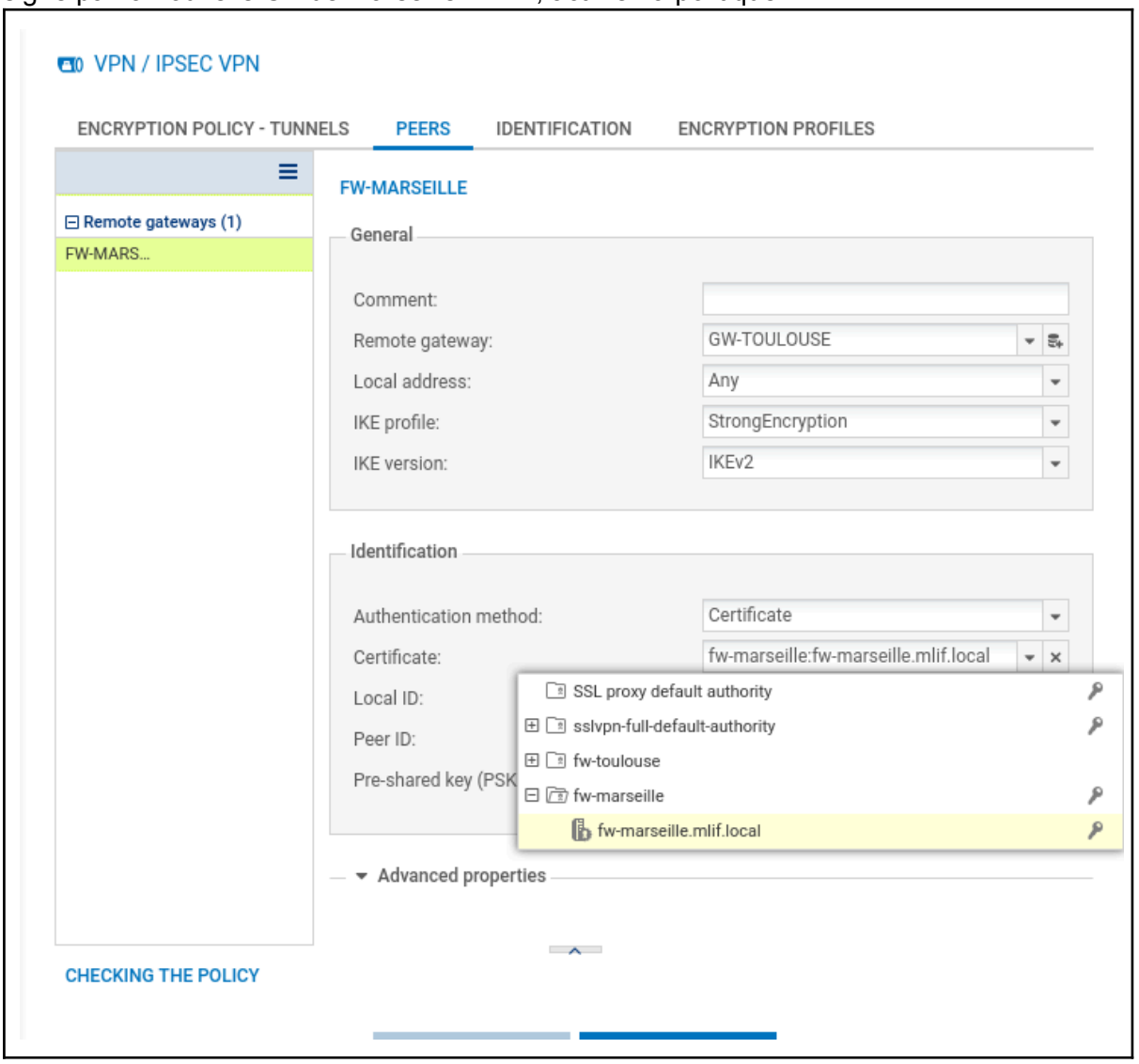
Cliquer sur VPN puis sur VPN Ipsec, dans l'onglet identification, ajouter la CA de Marseille précédemment importée dans les autorités de cettifcation acceptées puis valider.

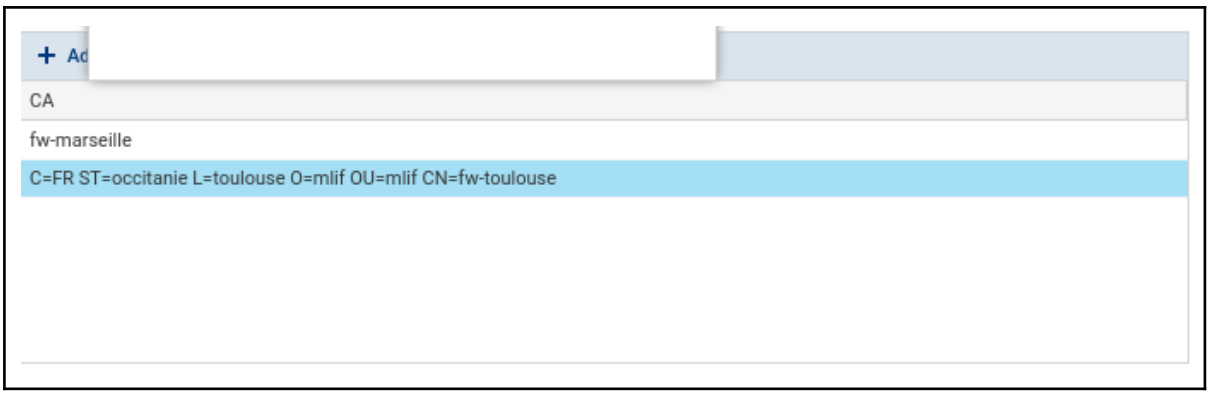


DEPUIS LA MACHINE CLIENT-MARSEILLE:

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.





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 :

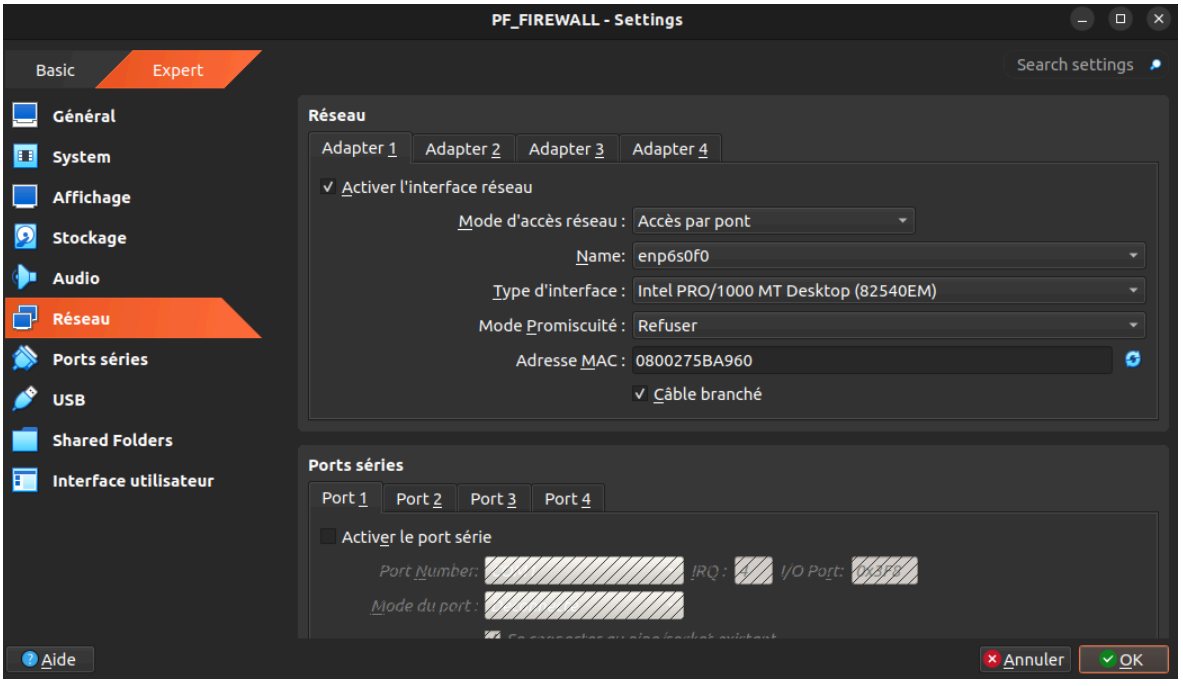
Reprendre le firewall du labo 1 sur le filtrage et le démarrer. N'oubliez pas de faire un snapshot afin de ne pas perdre la configuration existante.

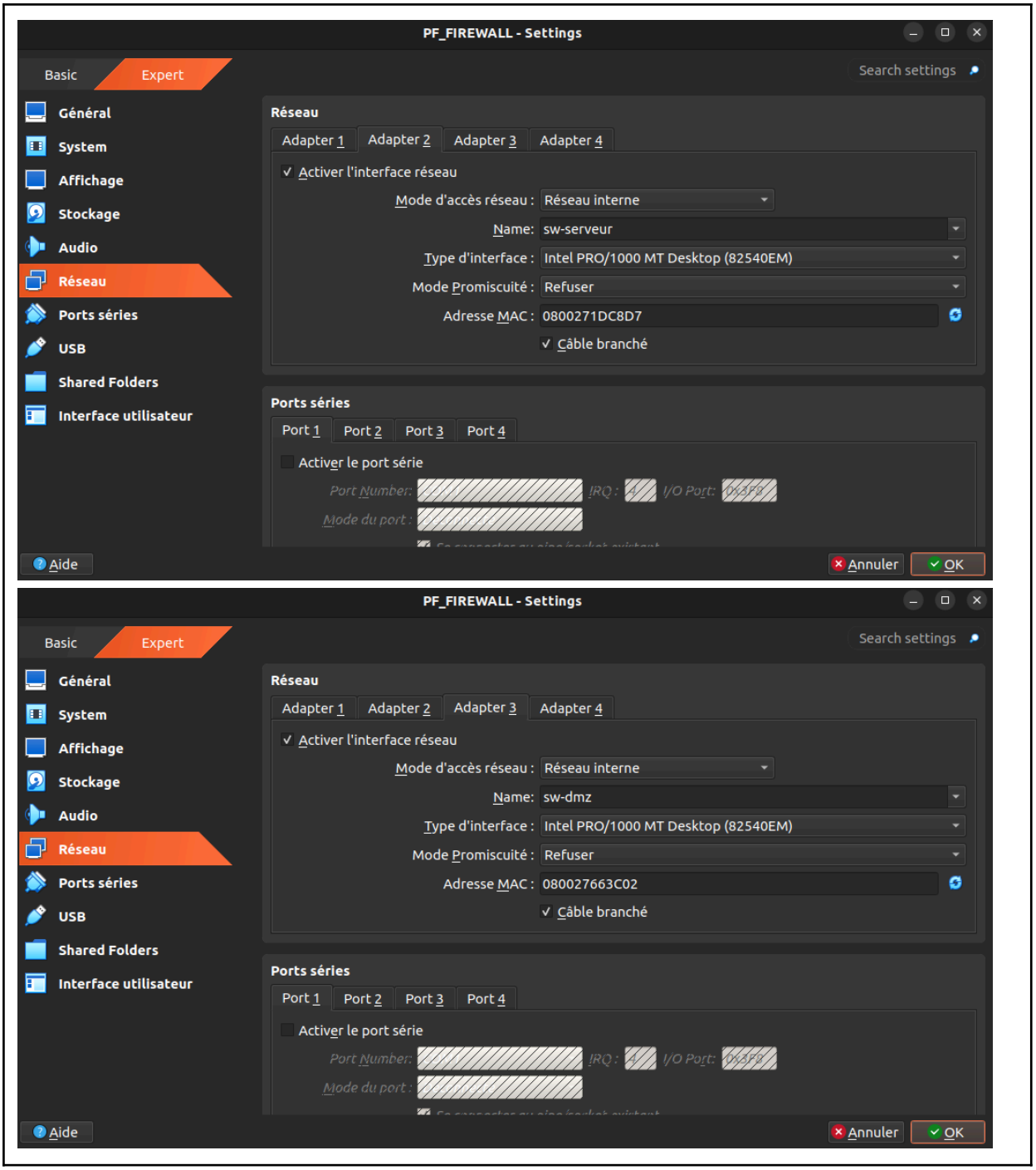
Plan d'adressage :

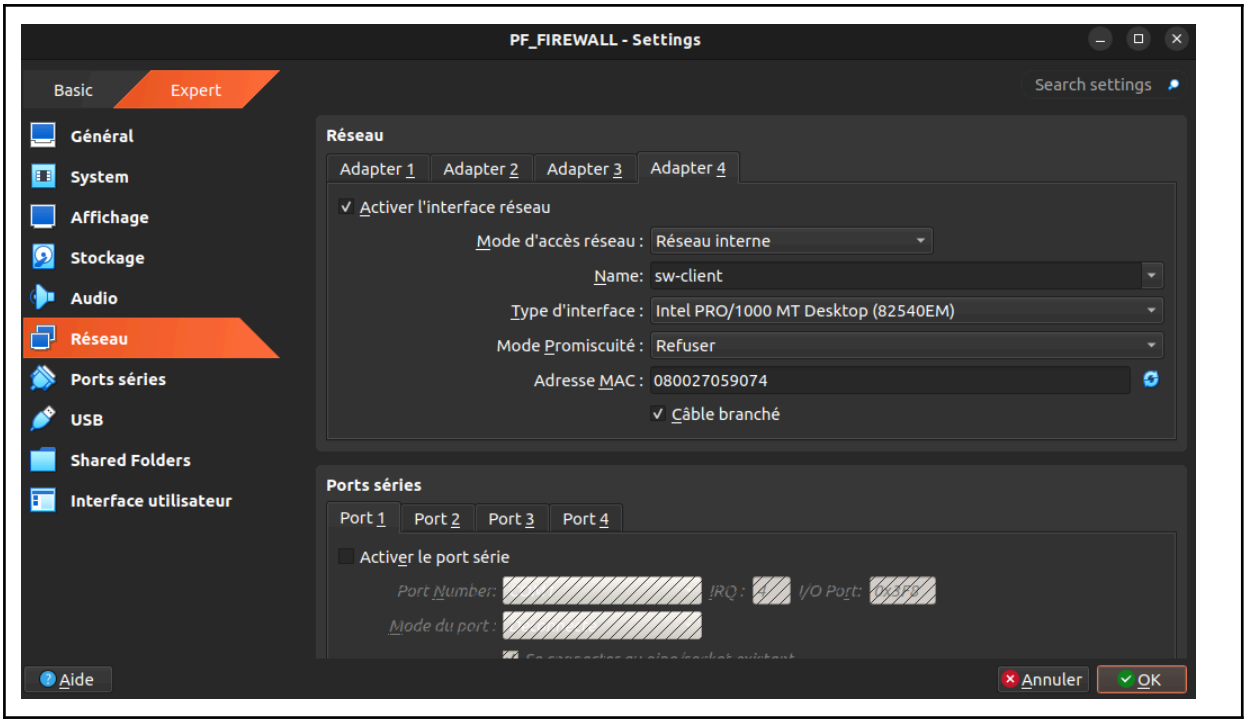
FIREWALL MLIF PFSENSE

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
Général
System
Affichage
Stockage
Audio
Réseau
Ports séries
USB
Shared Folders
Interface utilisateur
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 :
Aide
Annuler
OK
PF_FIREWALL - Settings
Basic
Expert
Search settings
Général
System
Affichage
Stockage
Audio
Réseau
Ports séries
USB
Shared Folders
Interface utilisateur
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



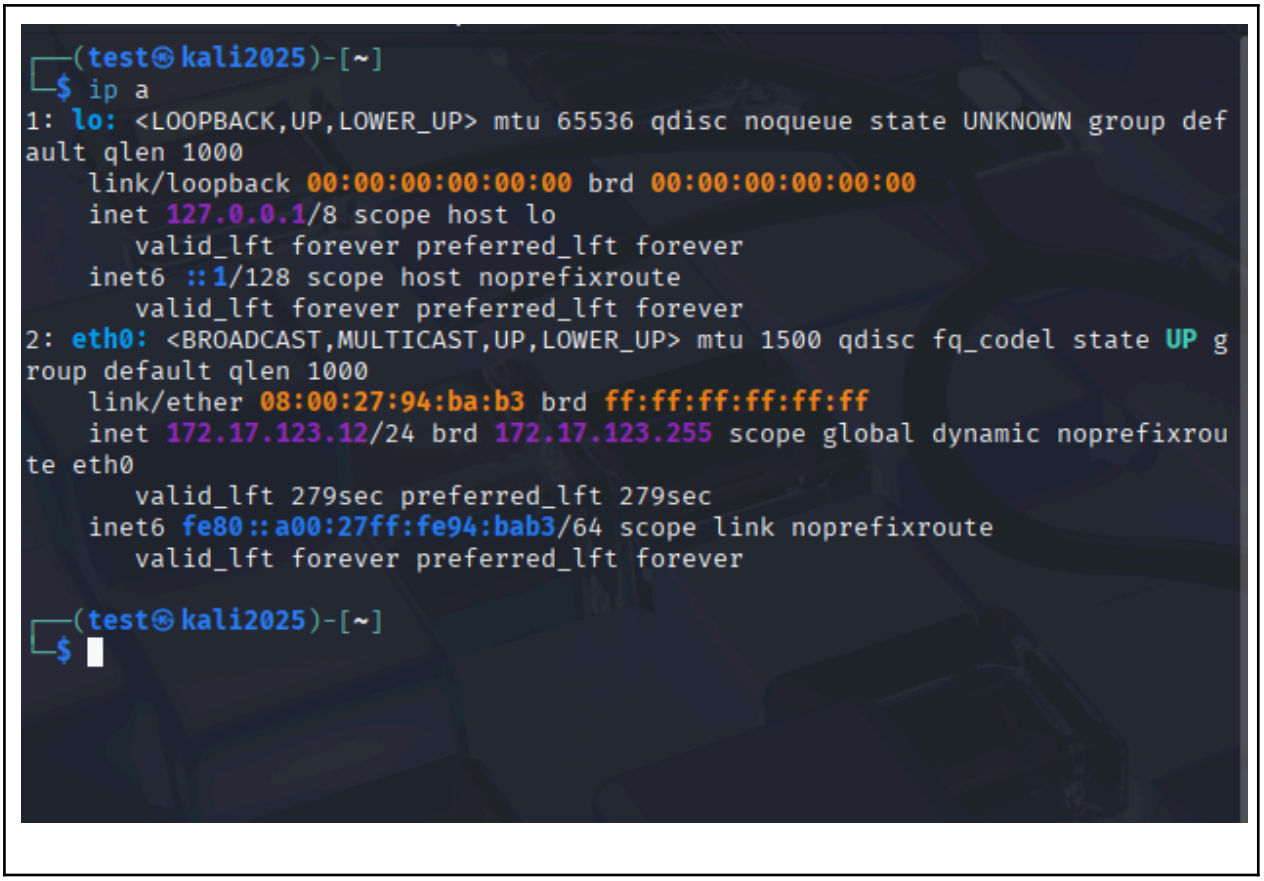
Changer l'adresse des client (lan)

Pour le client nomade j'ai pris la kali :

MACHINE CLIENT NOMADE

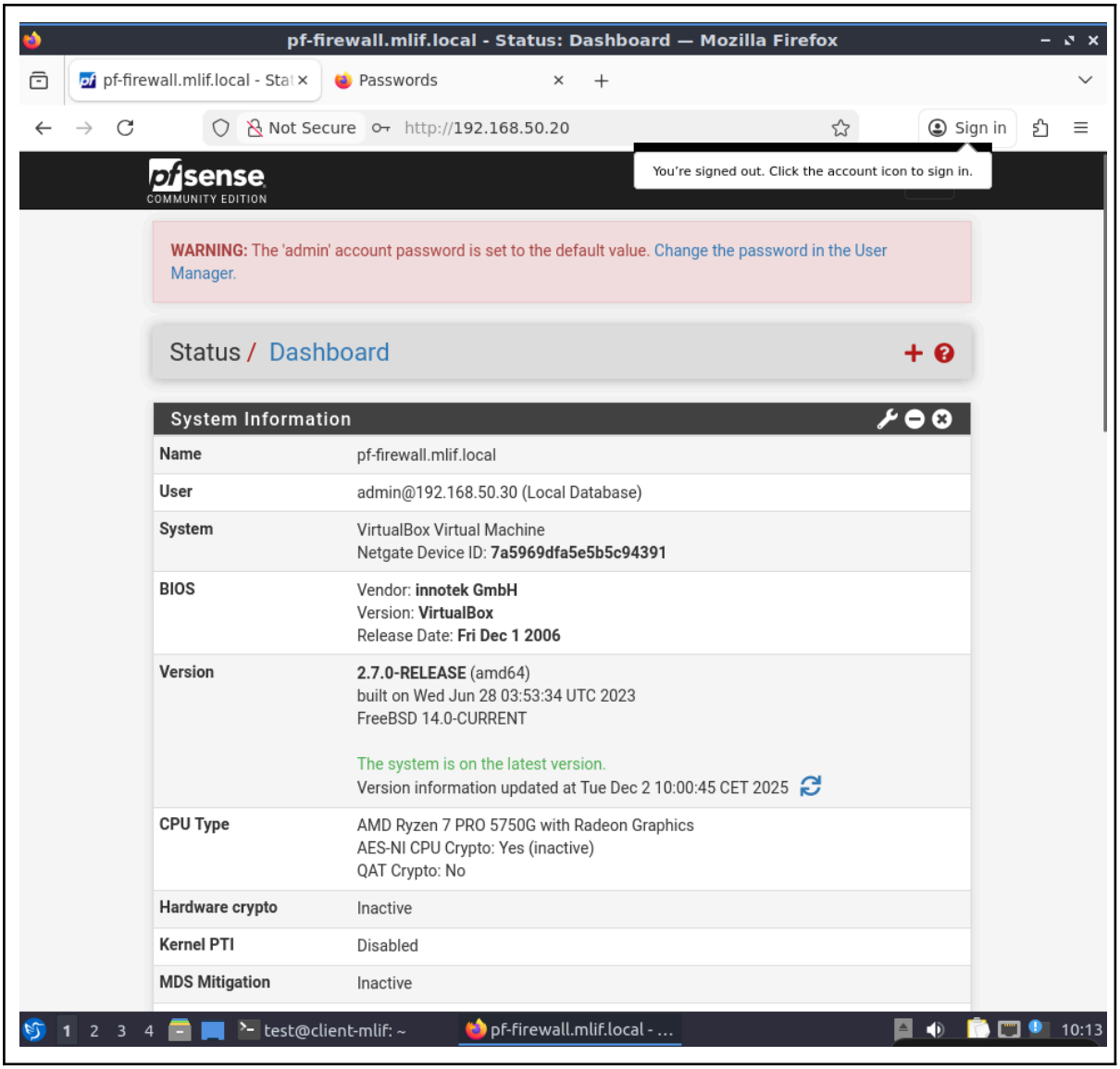
Cette machine est un client externe et simule un accès extérieur depuis internet (réseau du lycée). C'est donc cette machine qui va accéder au réseau de la MLIF via son client VPN.

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.



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.

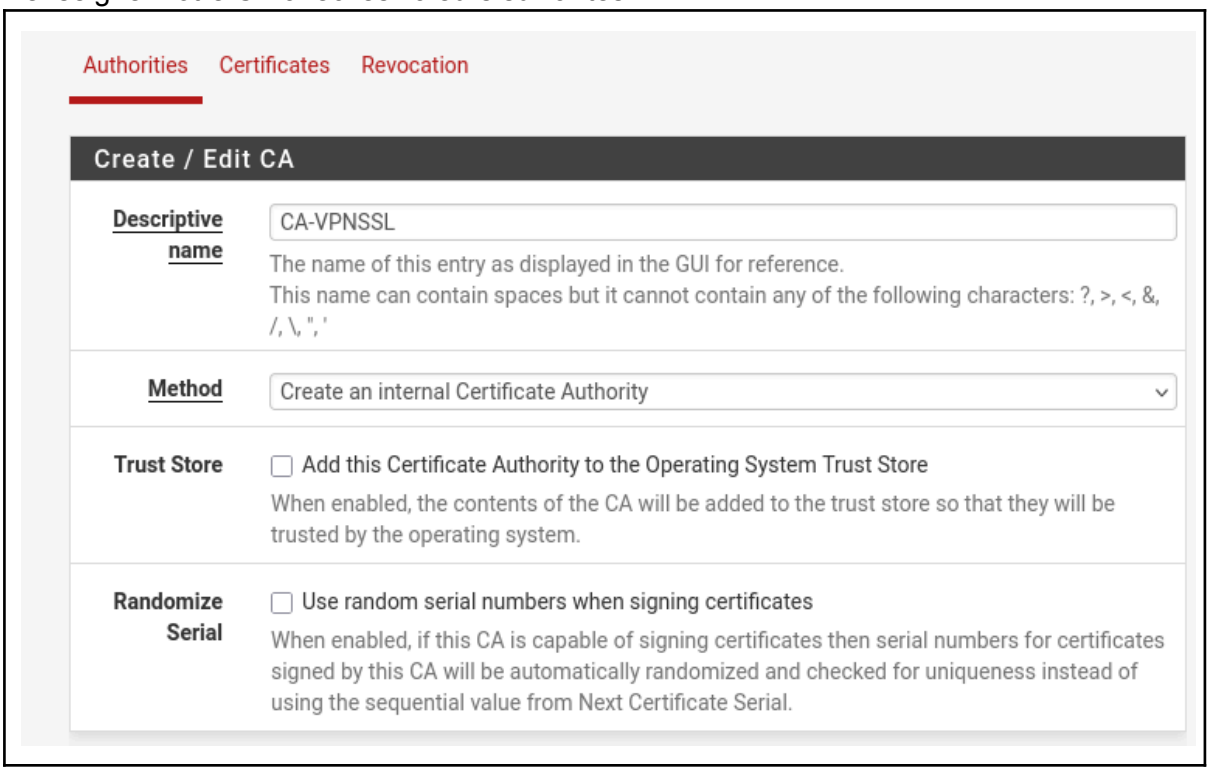
```
┌──(root㉿kali2025)-[/home/test]
└─# apt-get install openvpn network-manager-openvpn
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
openvpn is already the newest version (2.6.14-1).
openvpn set to manually installed.
network-manager-openvpn is already 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.
```

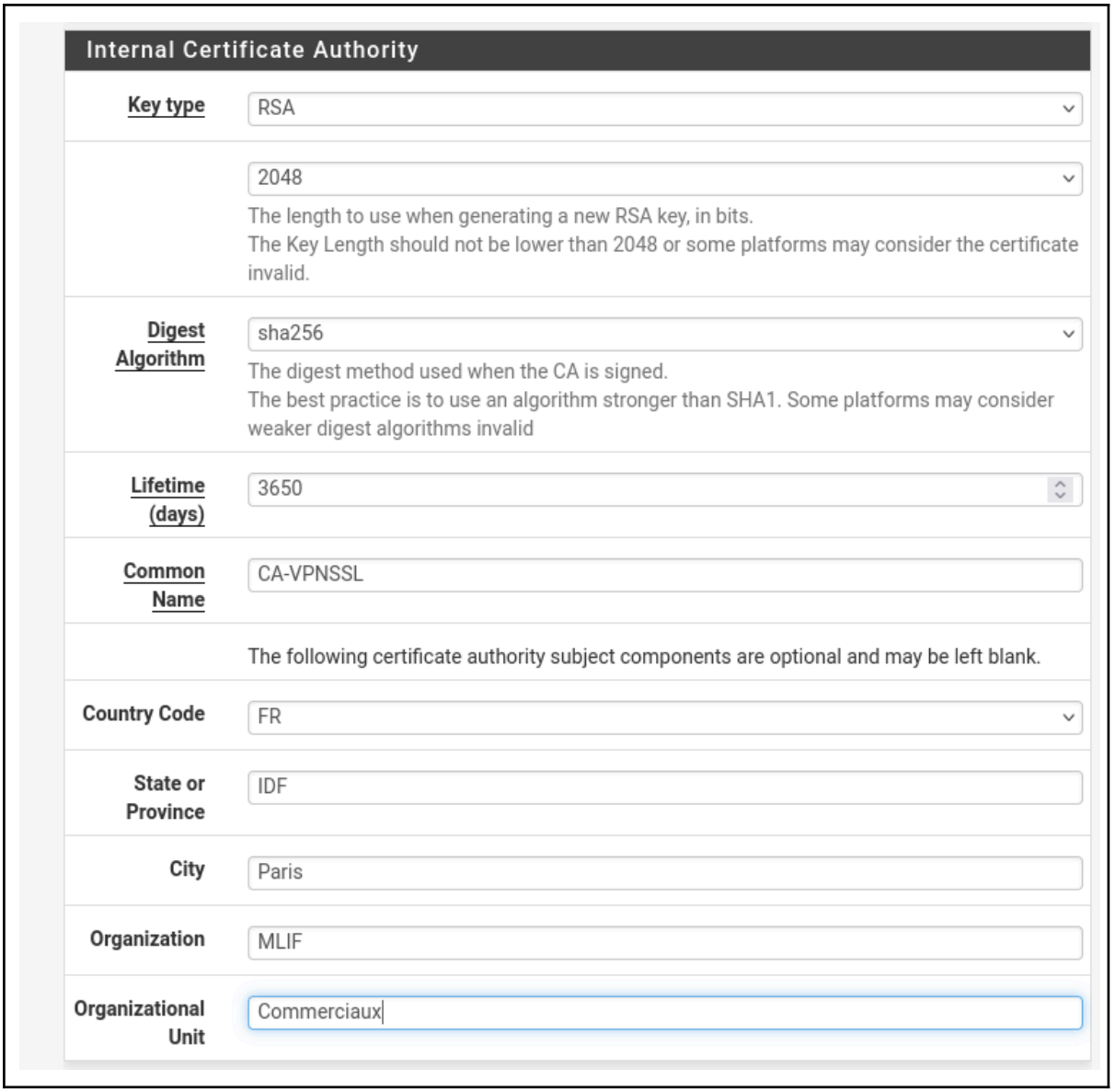
4.2°) Configuration du VPN SSL

Il faudra configurer le serveur et le client VPN.

DEPUIS LA MACHINE CLIENT-MLIF:

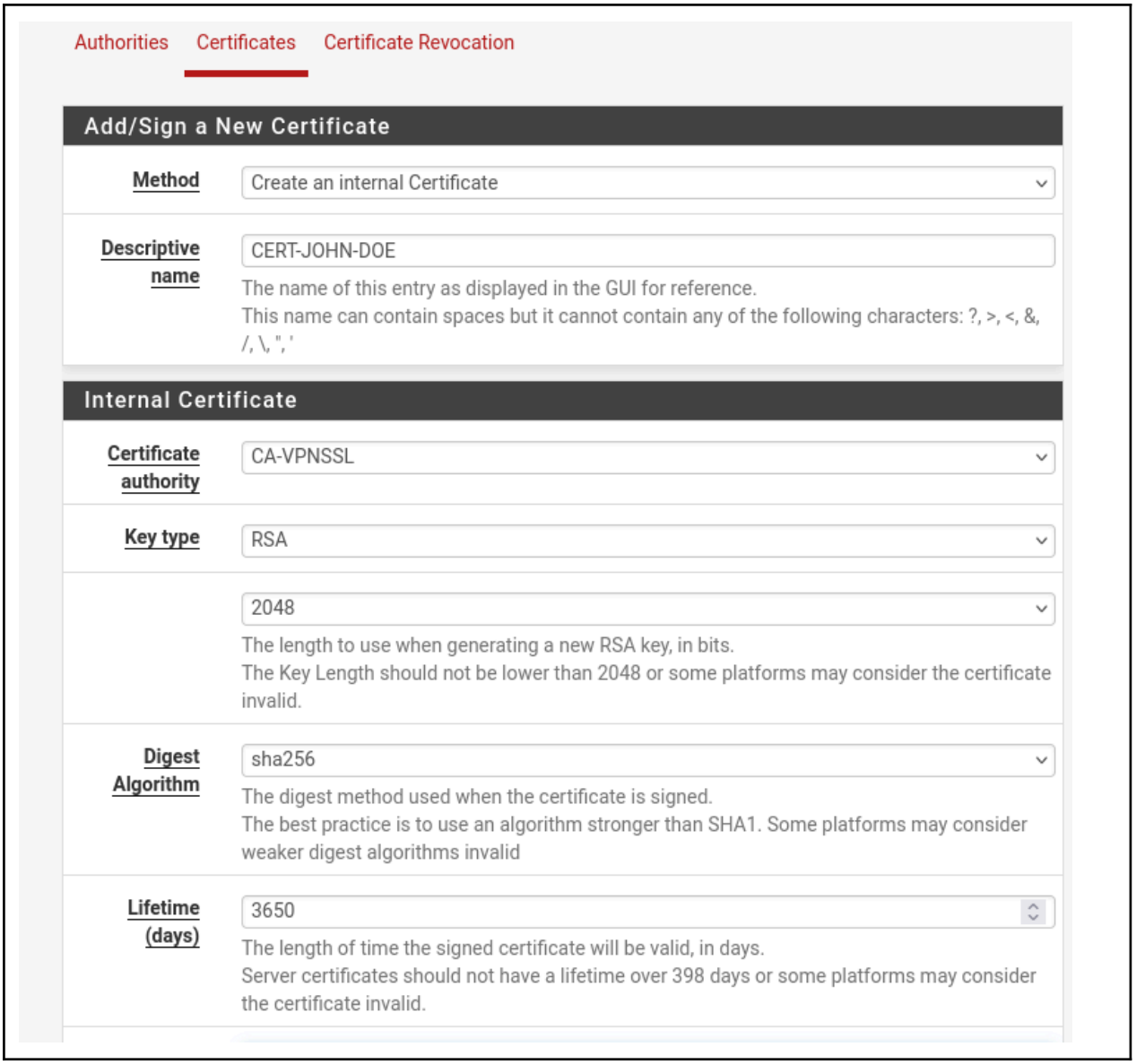
1- Création de l’autorité de certification :
Se connecter au firewall pfsense puis cliquer sur système puis sur gestionnaire de certificats. Ensuite, dans l’onglet ACs, vliquer sur ajouter afin de créer une nouvelle autorité de certification.
Renseigner votre CA avec les valeurs suivantes :

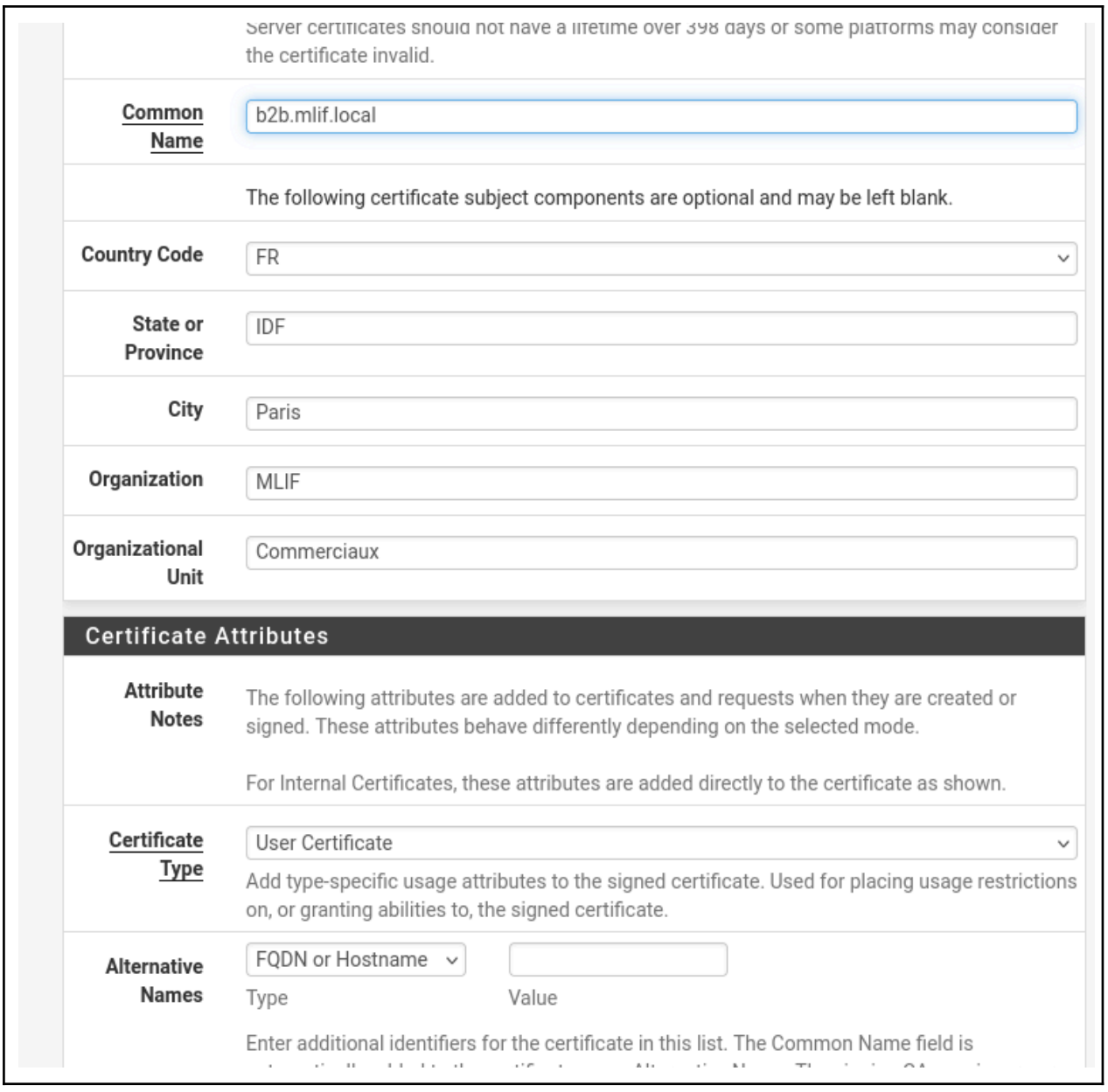




2- Création du certificat de l'utilisateur nomade :

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


Authorities
Certificates
Certificate Revocation
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.

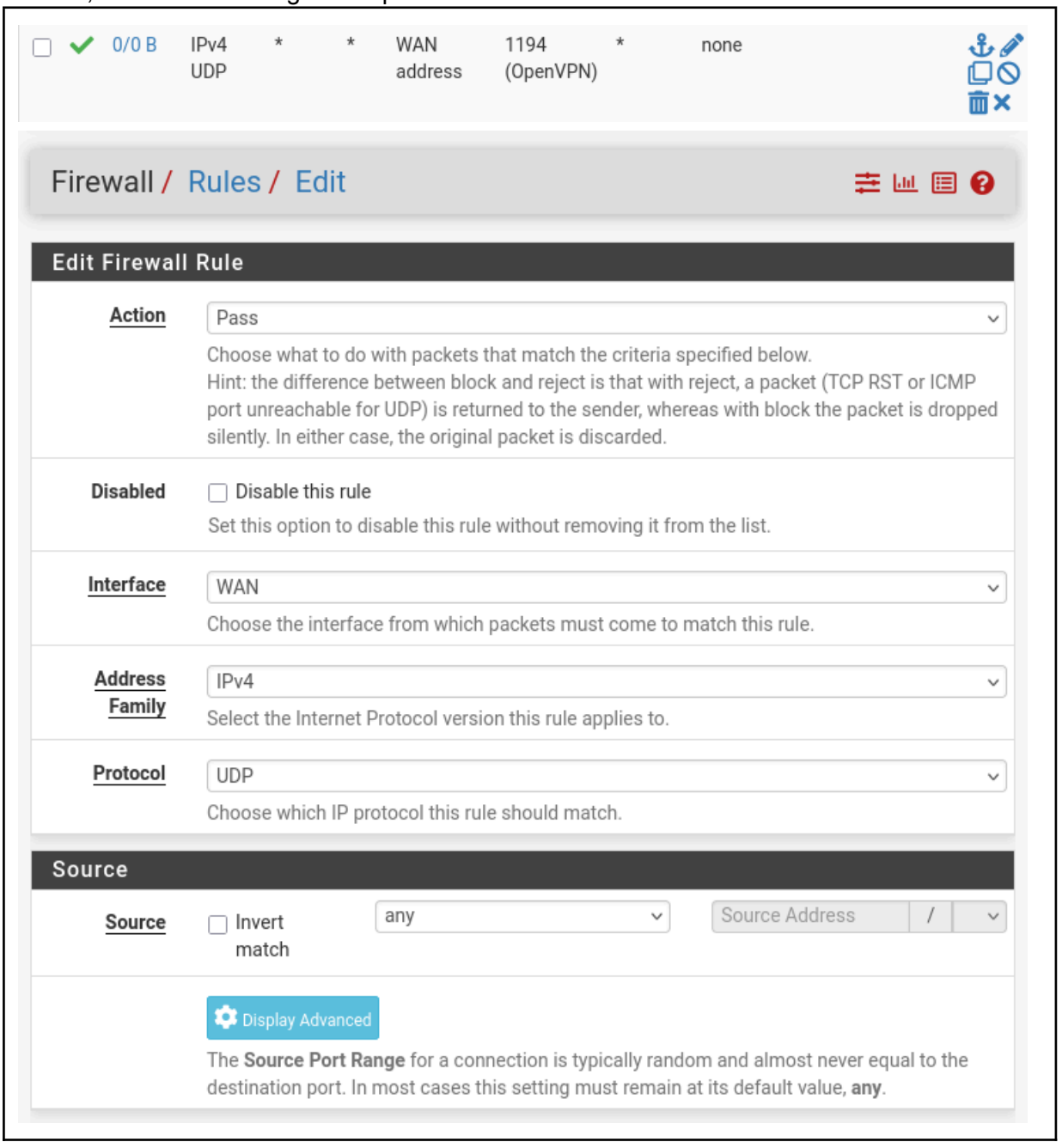


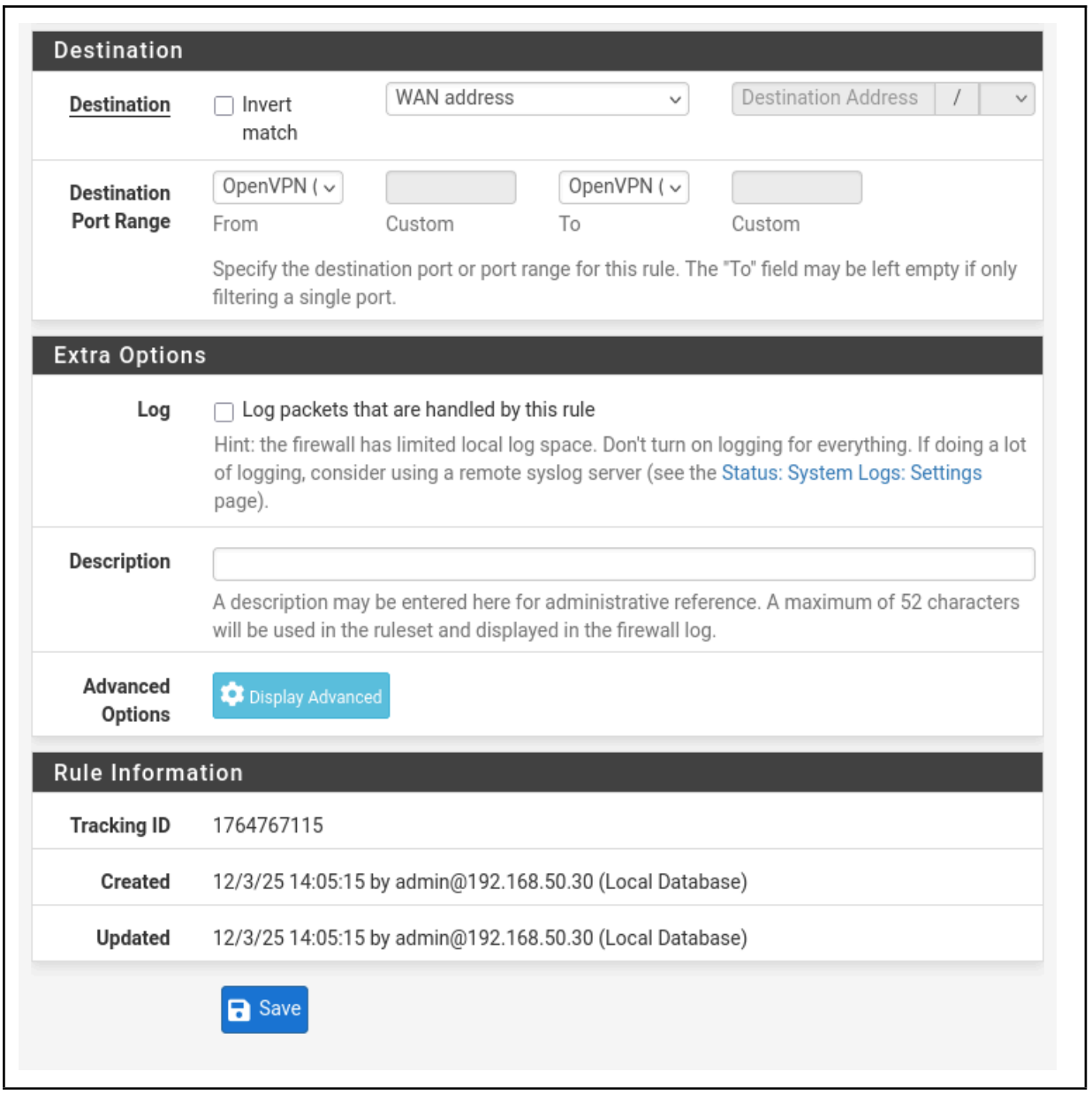
Ensuite, envoyer ces trois fichiers sur la machine cliente nomade via la commande scp. Attention, votre firewall pfsense n'autorise peut être pas ce flux. A vous de l'ouvrir afin que la commande scp soit un succès (UDP 1194).

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

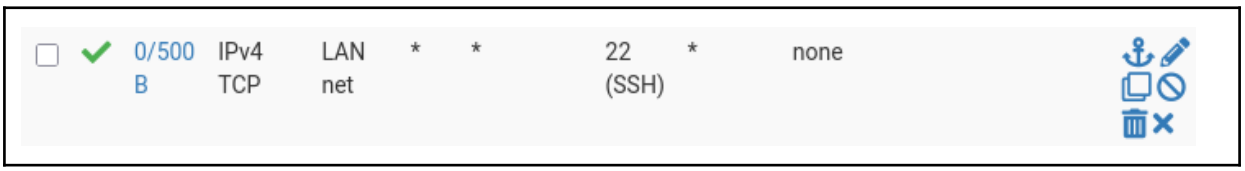
Comme on a modifié l'ip de la firewall, on va faire :
sudo ip route add default via 192.168.50.20 (c'est l'ip de la lan)

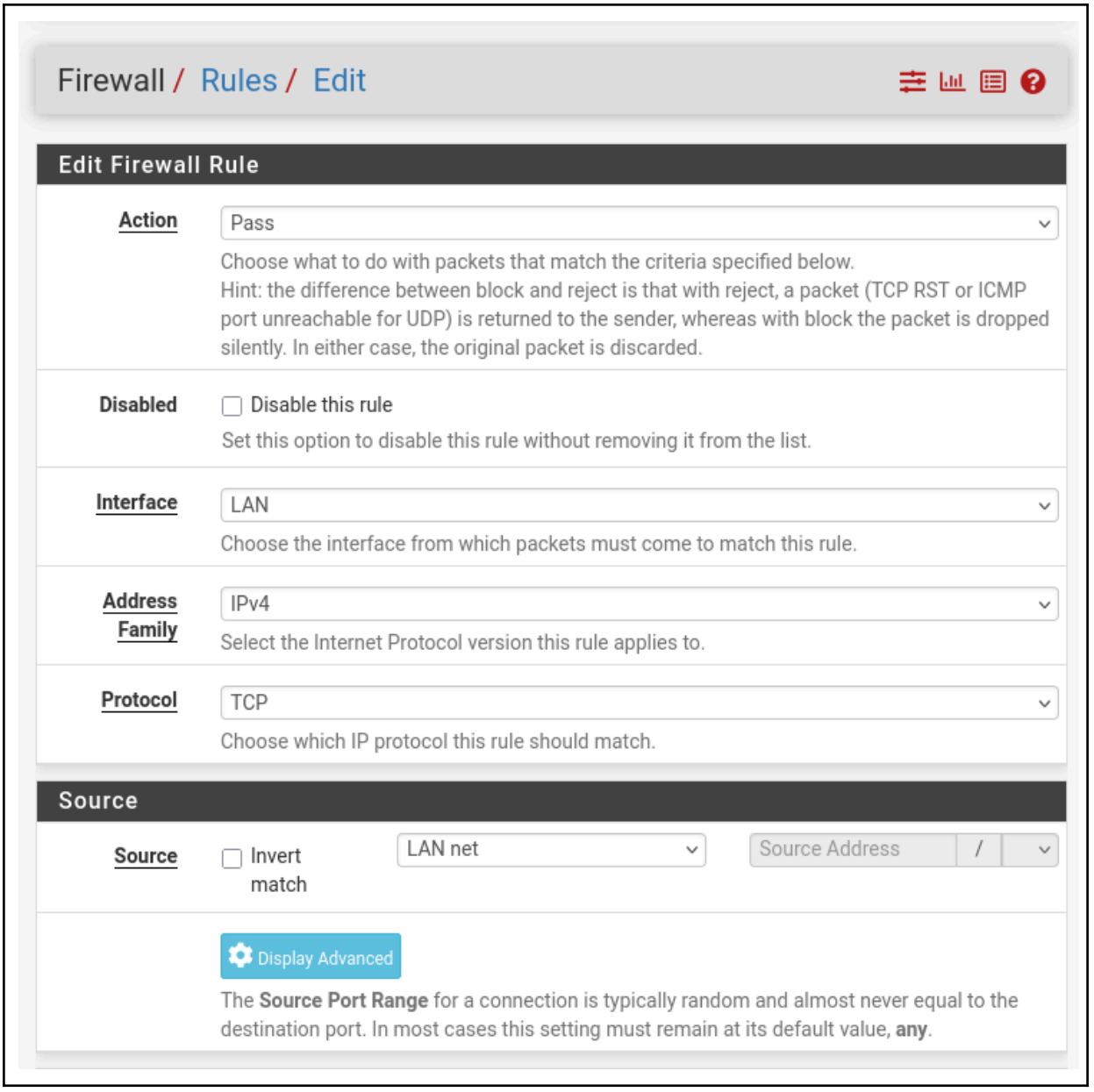
Ensuite, on va faire les règles sur pfsense :

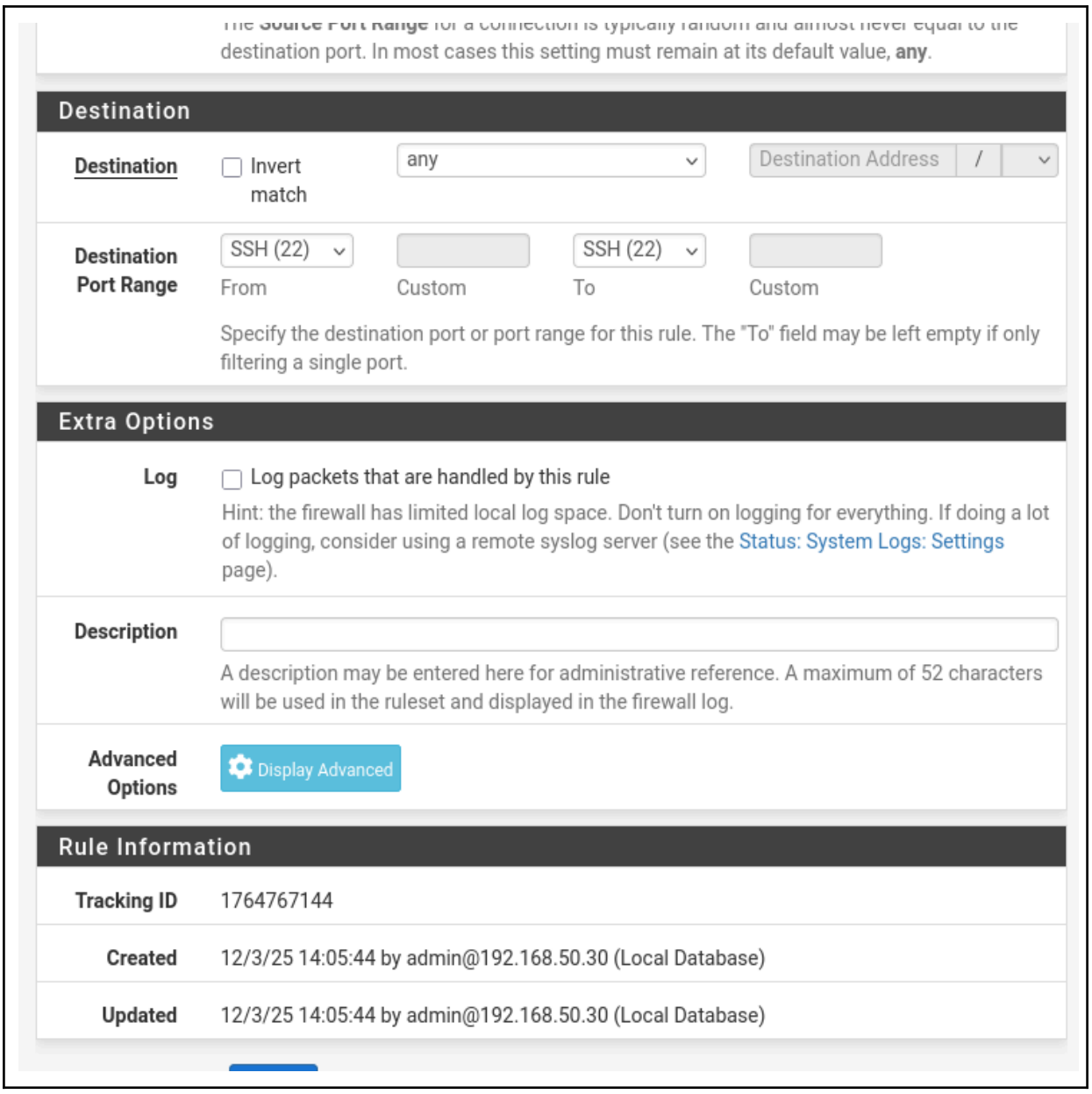



Destination
Destination
Invert match
WAN address
Destination Address
/
Destination Port Range
OpenVPN (
From
Custom
OpenVPN (
To
Custom
Specify the destination port or port range for this rule. The "To" field may be left empty if only filtering a single port.
Extra Options
Log
Log packets that are handled 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
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)
Save

SSH :


0/500 B
IPv4 TCP
LAN net
*
*
22 (SSH)
*
none


Firewall / Rules / Edit
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 Family
IPv4
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.



Ensuite sur le client nomade :

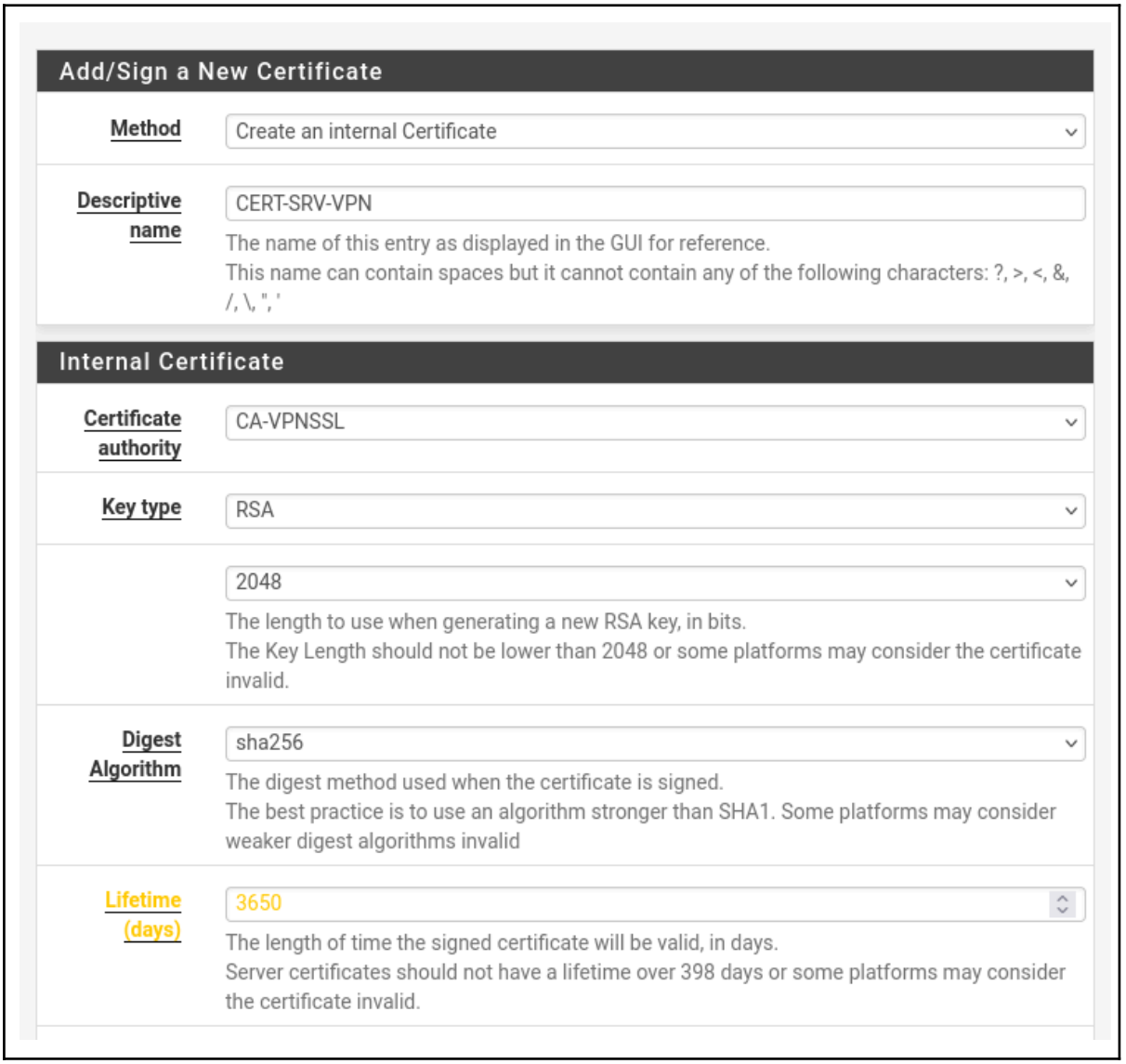
```
sudo apt update
sudo apt install openssh-server
sudo systemctl enable --now ssh
sudo systemctl status ssh
```

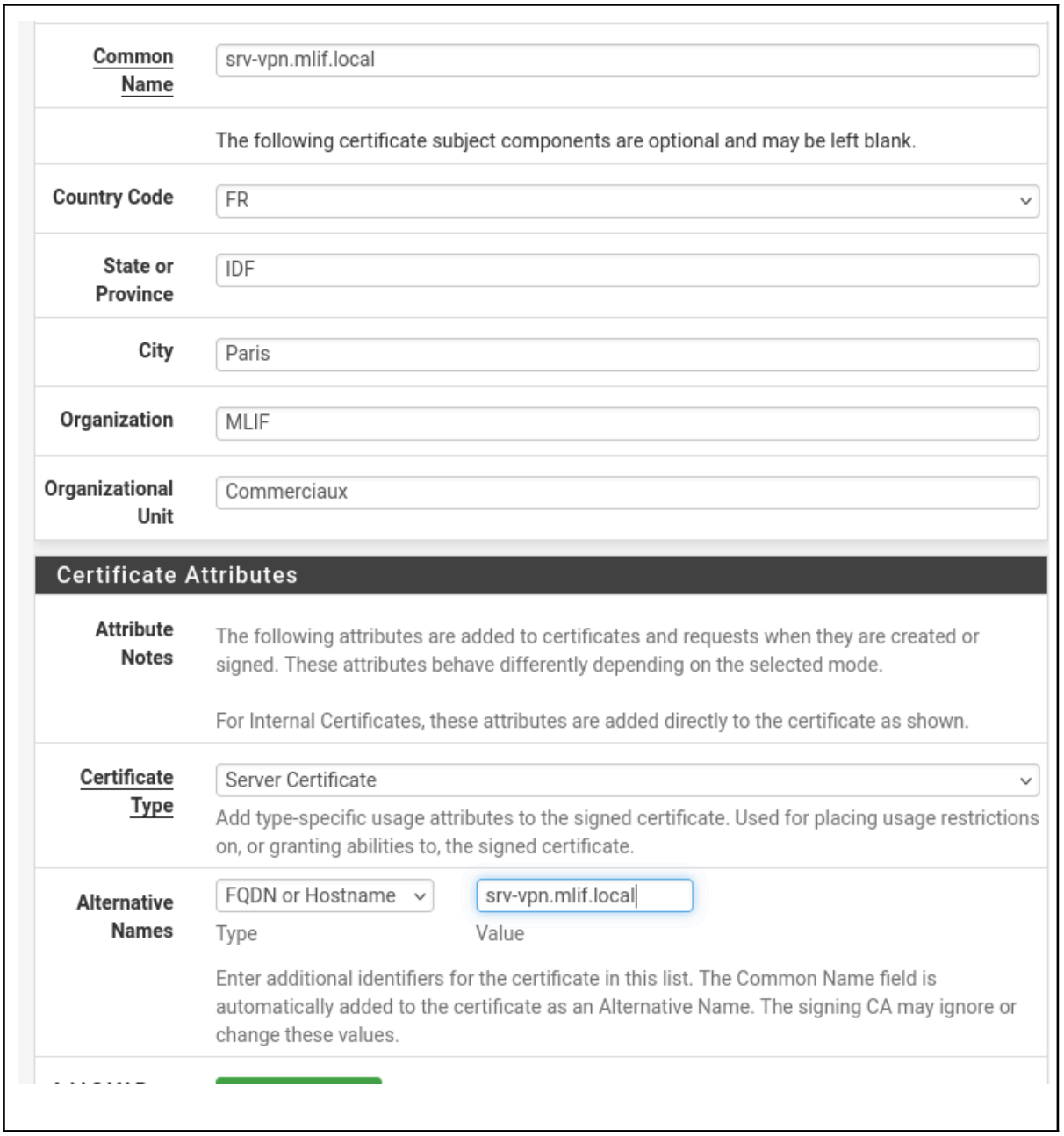
Depuis le client de la mlif :

```
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 :





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 VPN-NOMADE-MLIF

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 Accès à distance (SSL/TLS)

Mode dispositif tun - Layer 3 Tunnel Mode

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 UDP on IPv4 only

Interface WAN

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

Port local 1194

Le port utilisé par OpenVPN pour recevoir des connexions client.

Configuration TLS	☐ 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	☐ 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.
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	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-256-GCM AES-128-GCM CHACHA20-POLY1305

AES-192-CFB8 (192 bit key, 128 bit block)

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

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.

Algorithme de hachage d'authentification

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.

Chiffrement matériel

Pas d'accélération cryptographique matérielle

Profondeur du certificat

Un (Client + Serveur)

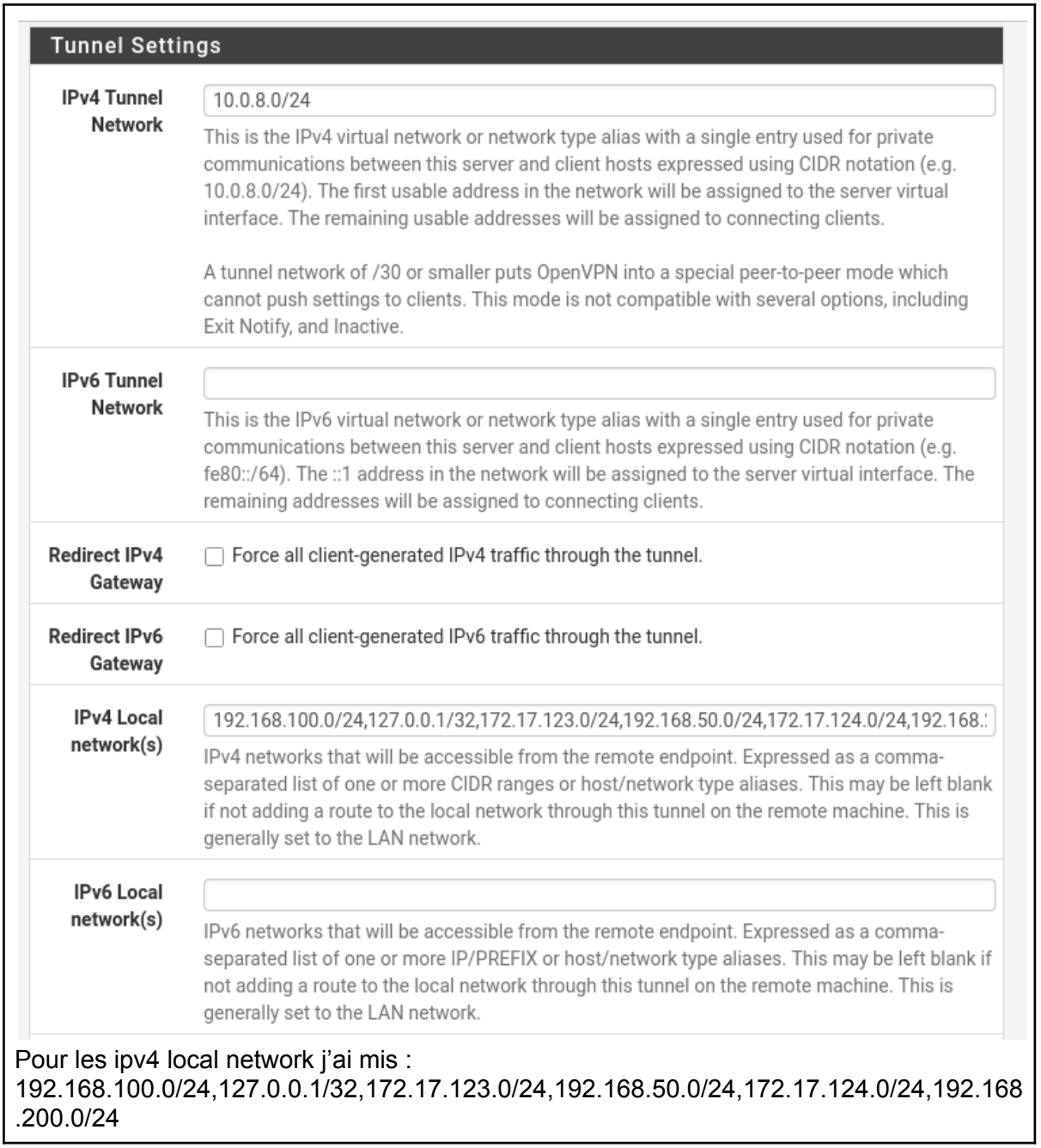
Lorsqu'un client basé sur un certificat se connecte, n'accepte pas les certificats au-dessous de cette profondeur. Utile pour refuser les certificats effectués avec des CA intermédiaires générées à partir de la même autorité de certification que le serveur.

Client Certificate Key Usage Validation

Enforce key usage

Verify that only hosts with a client certificate can connect (EKU: "TLS Web Client Authentication").

Paramètres du tunnel



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

generally set to the LAN network.

Connexions simultanées

5

Spécifier le nombre maximum de clients autorisés à se connecter en même temps à ce serveur.

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 de service

☐ Définissez la valeur d'en-tête IP TOS des paquets de tunnel pour correspondre à la valeur du paquet encapsulé.

Communication inter-clients

☐ Autoriser la communication entre les clients connectés à ce serveur

Dupliquer la connexion

☐ 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.

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.

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

Paramètres clients avancés

ping-restart = timeout*2
push ping = interval
push ping-restart = timeout

Intervalle 10

Délai d'attente 60

Paramètres clients avancés

Domaine DNS par défaut ☑ Renseigner un nom de domaine par défaut aux clients.

Domaine DNS par défaut mlif.local

Activer le Serveur DNS ☑ Fournisser 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 ☐ 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.

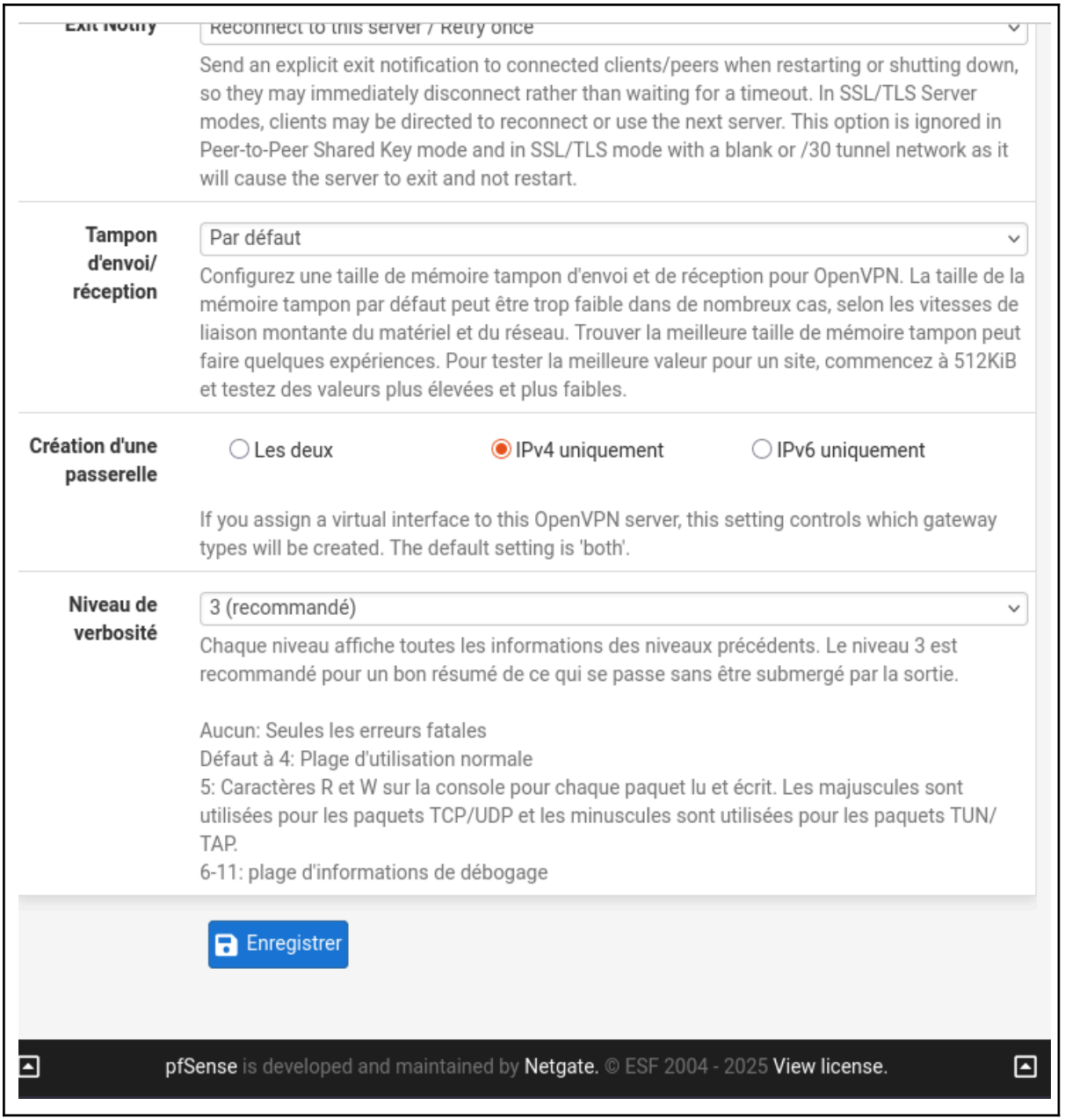
Requiert Windows 10 et OpenVPN 2.3.9 ou ultérieur. Seul Windows 10 est sujet à une telle fuite DNS, les autres clients vont ignorer cette option puisqu'ils ne sont pas concernés

Forcer une mise à jour du cache DNS ☐ Exécuter "net stop dnscache", "net start dnscache", "ipconfig /flushdns" et"ipconfig /registerdns" après avoir initialisé la connexion.

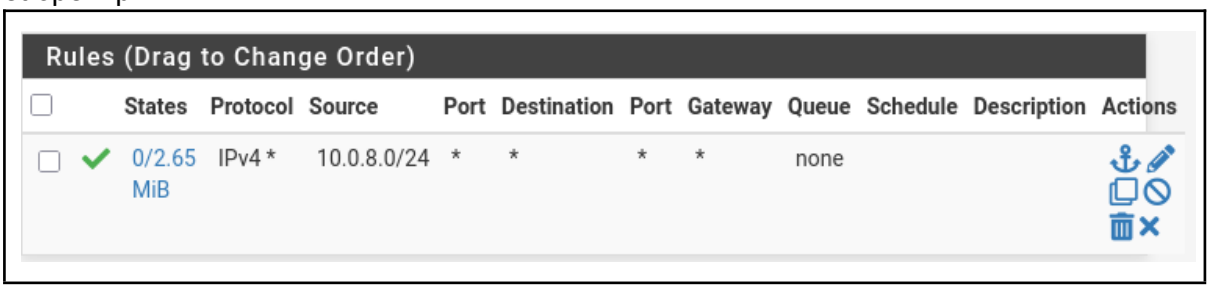
Forcer une mise à jour du cache DNS	☐ Exécuter "net stop dnscache", "net start dnscache", "ipconfig /flushdns" et"ipconfig / registerdns" après avoir initialisé la connexion. Ceci est connu pour permettre à Windows de reconnaître les serveurs DNS poussés.
Activer Serveur NTP	☐ Fournisser une liste de 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	Reconnect to this server / Retry once 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	Par défaut

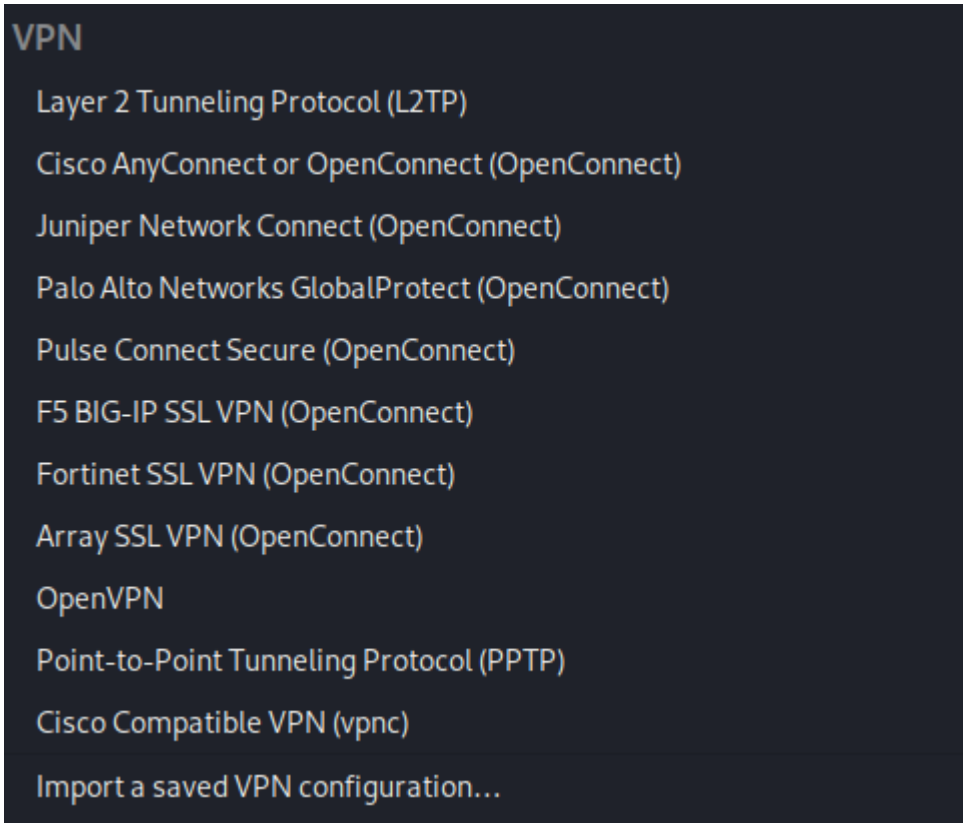


Avant de configurer la configuration du client vpn, on va mettre une règle dans firewall , rules et openvpn:



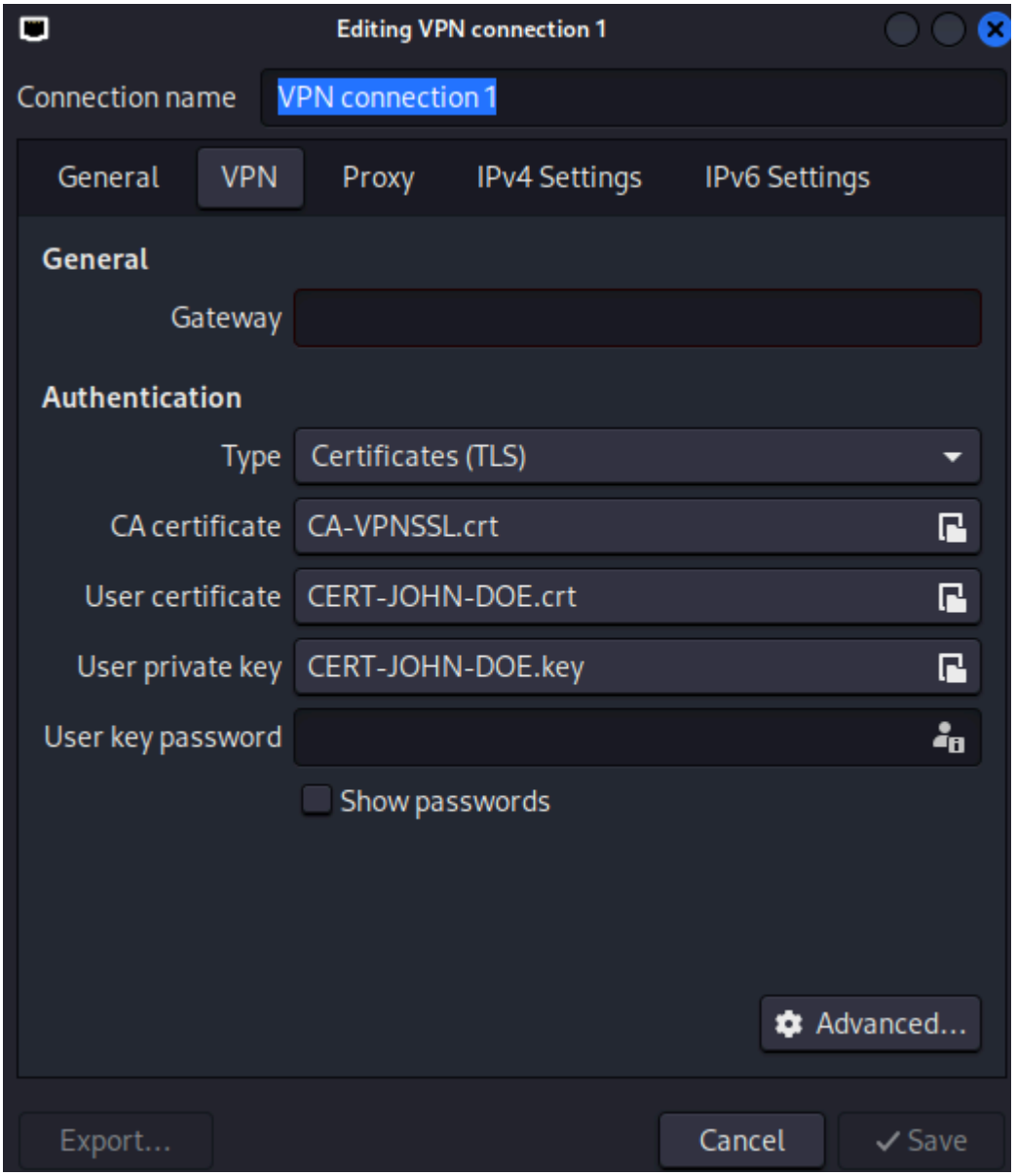
6- Configuration du client VPN :

Configurer le client VPN avec les paramètres suivants :

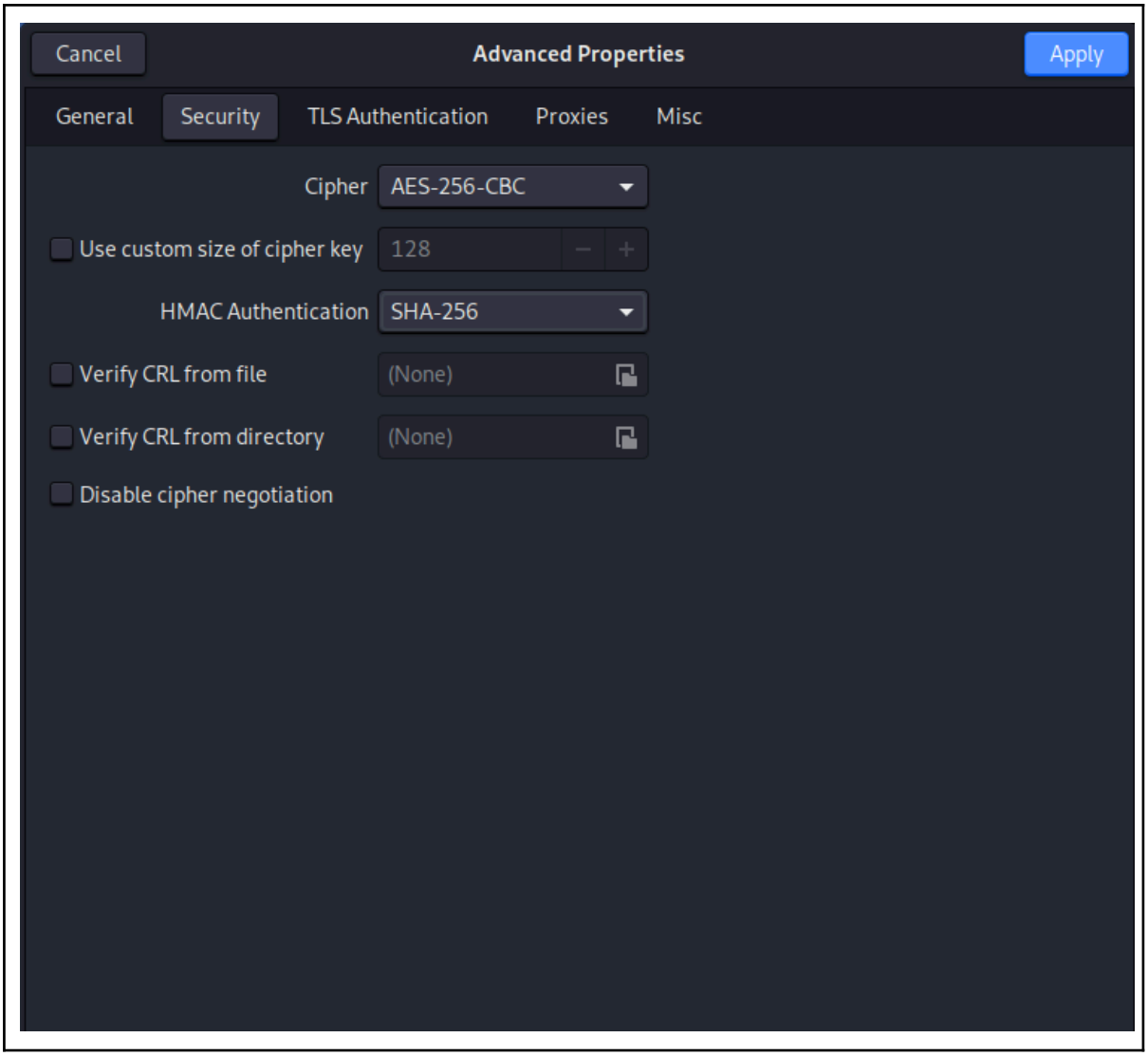


On prend openvpn (il faut scroller)

On a donc ces paramètres :



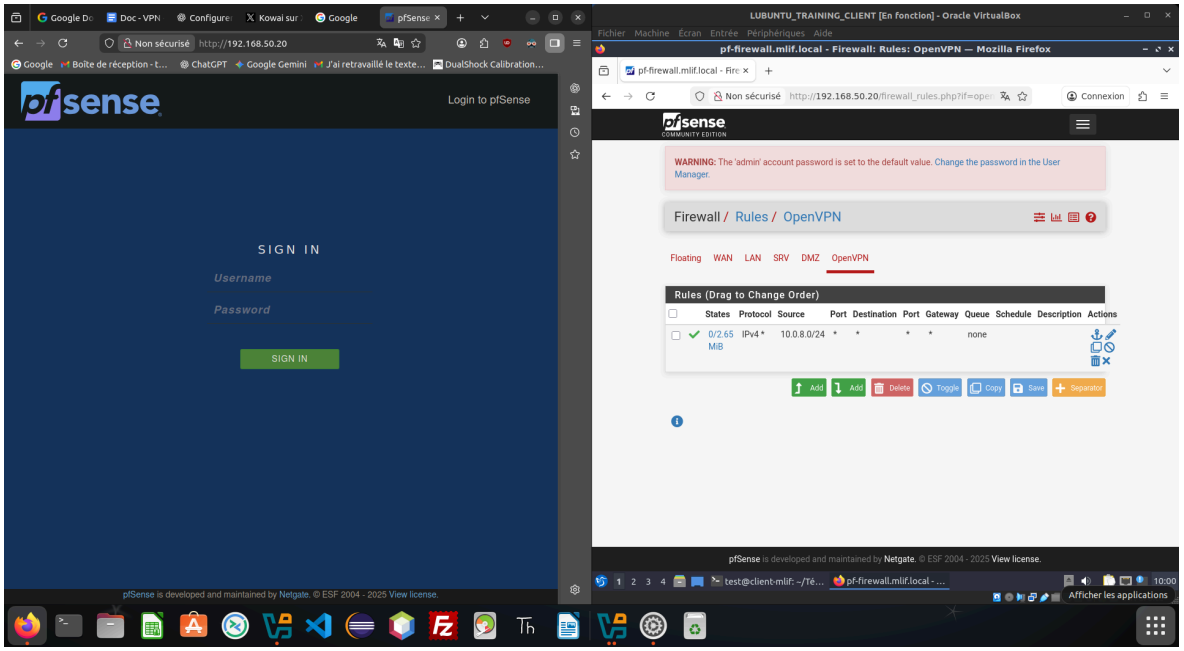
La gateway c'est la lan de la pf firewall (penser à la changer si on change de salle)
Avant de sauvegarder il faut aller dans le menu advanced et mettre ces paramètres :



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

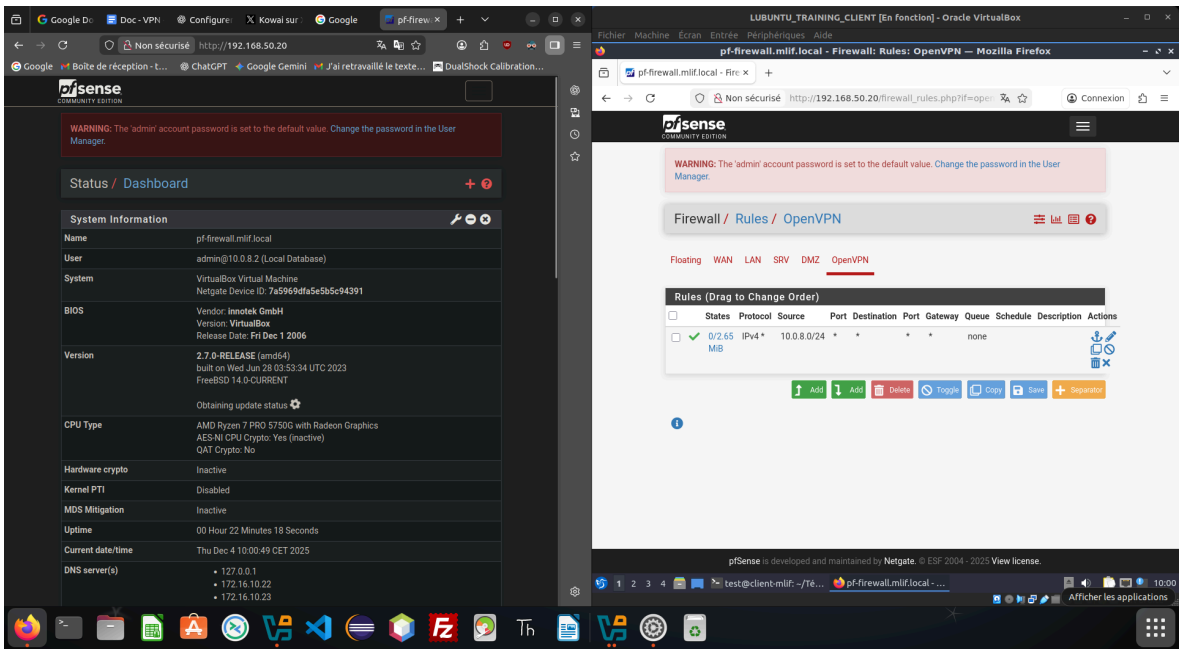
```
root@archa:/home/test# ping 192.168.50.20
PING 192.168.50.20 (192.168.50.20) 56(84) bytes of data.
64 bytes from 192.168.50.20: icmp_seq=8 ttl=64 time=0.510 ms
64 bytes from 192.168.50.20: icmp_seq=9 ttl=64 time=0.248 ms
64 bytes from 192.168.50.20: icmp_seq=10 ttl=64 time=0.366 ms
```

On se connecte donc au firewall :



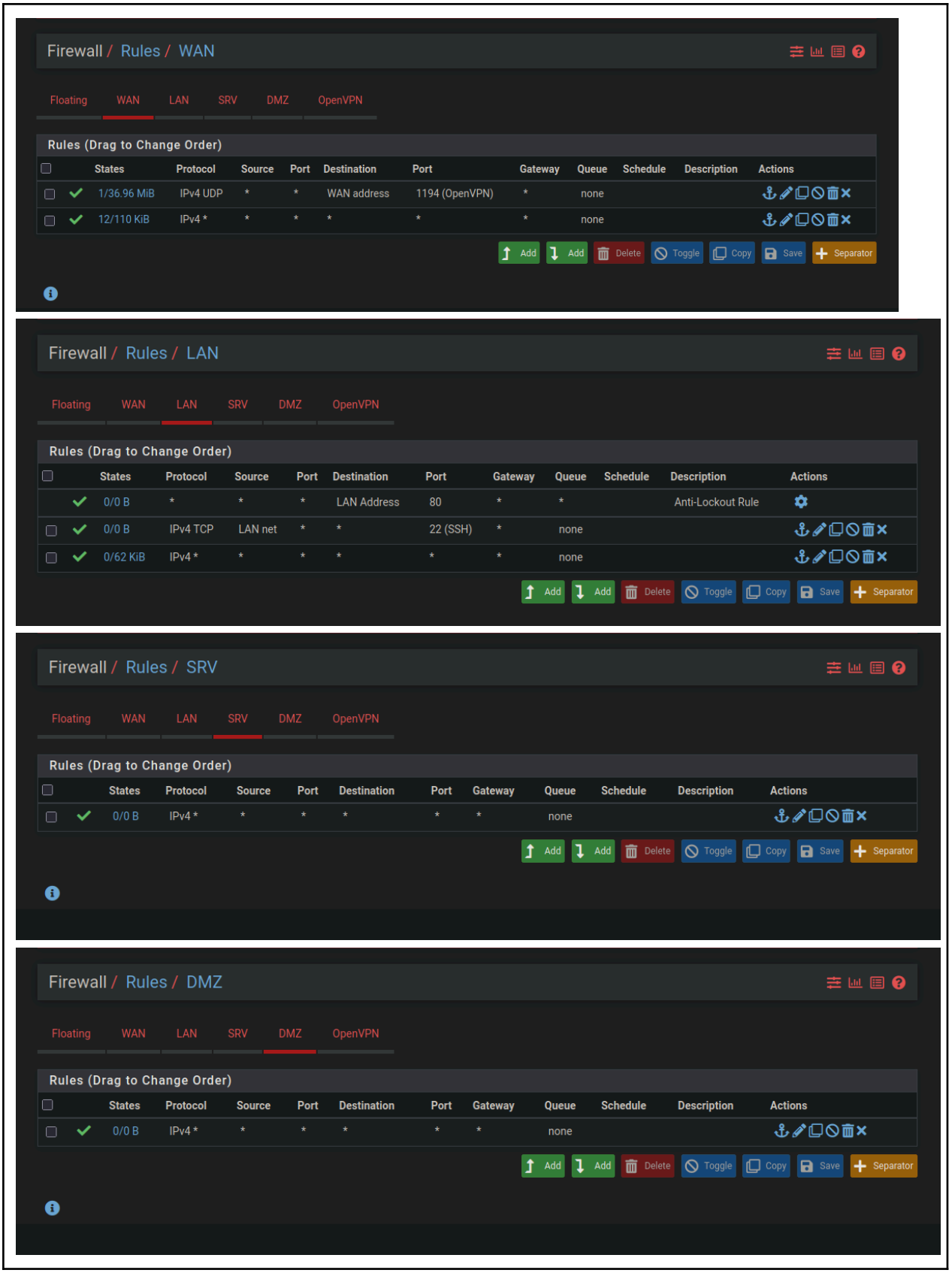
On voit bien qu'on peut se connecter donc depuis la machine physique

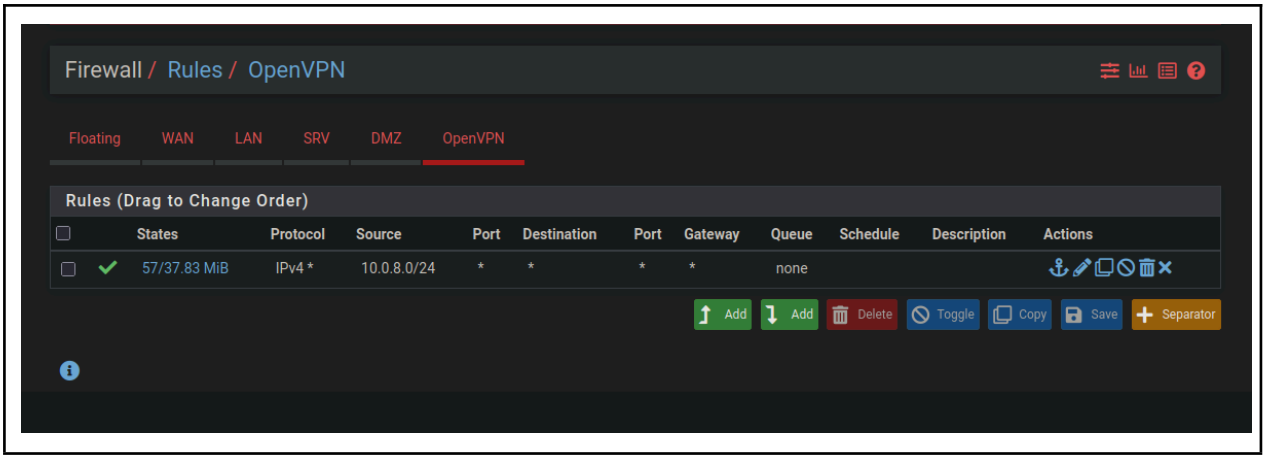
Et la on voit donc que je suis connecté :



STOP 3

Les règles doivent ressembler à ca :


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
1/36.96 MiB IPv4 UDP * * WAN address 1194 (OpenVPN) * none
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
0/0 B * * * LAN Address 80 * * Anti-Lockout Rule
0/0 B IPv4 TCP LAN net * * 22 (SSH) * none
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
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
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
57/37.83 MiB
IPv4 *
10.0.8.0/24
*
*
*
*
none
Add
Add
Delete
Toggle
Copy
Save
Separator