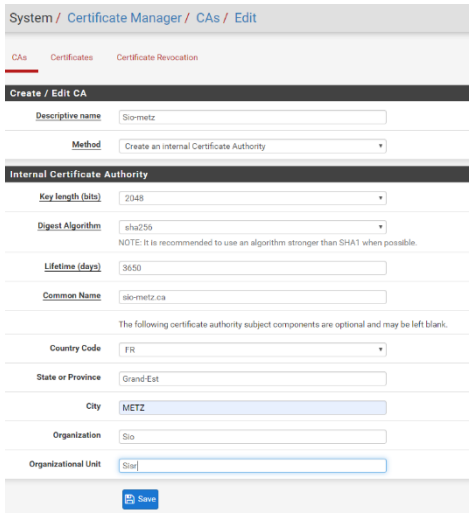
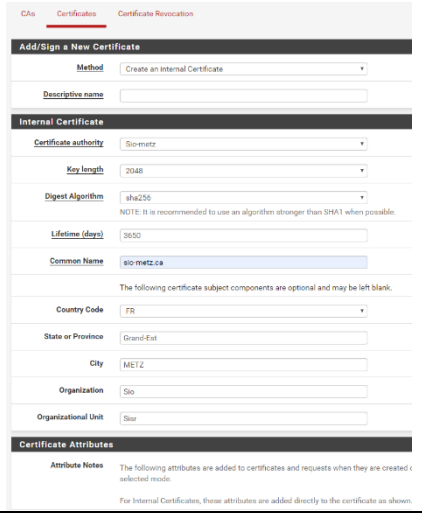
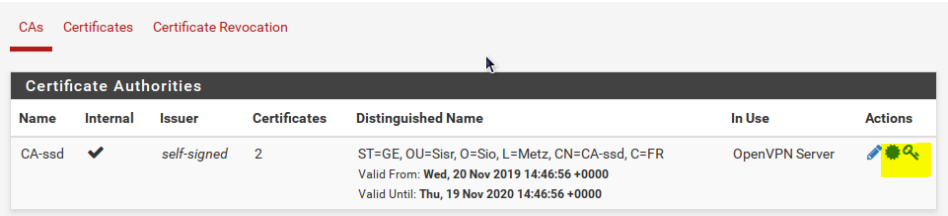
Serveurs Vpn Sous PfSense : TLS Inter-Sites

Schéma

Création des certificats	
Serveur 1	Serveur 2
1 créer l'autorité de certification et son certificat	1 ' importer le certificat de l'autorité
aller dans System Certificates Onglet CA	aller dans System Certificates Onglet CA
+ add et saisir les champs 	+ add puis importer le certificat de l'autorité 

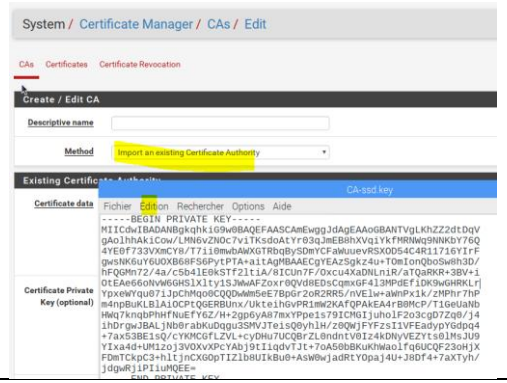
Exporter le certificat de l'autorité.



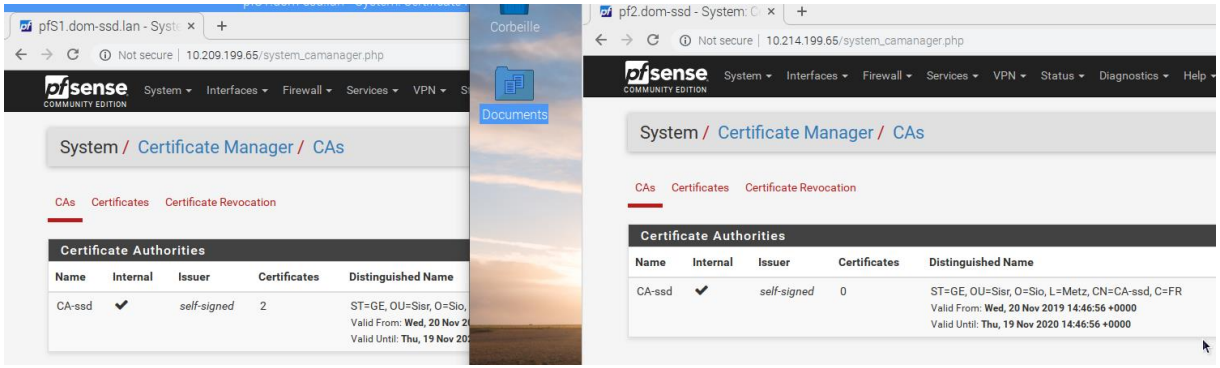
Utiliser WinSCP pour faire transiter les fichiers si vous avez des clients Linux.

Si votre client est en Windows préférer un éditeur de texte comme notepad++.

Pour importer, on colle l'ensemble de la clé ou des données

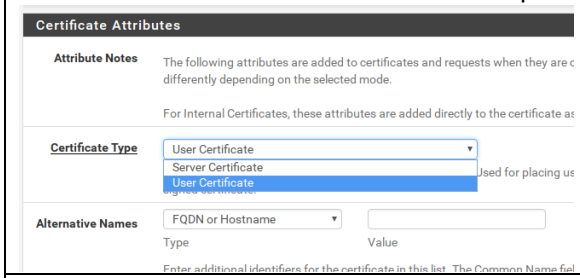


Vous devez obtenir quelque chose d'approchant



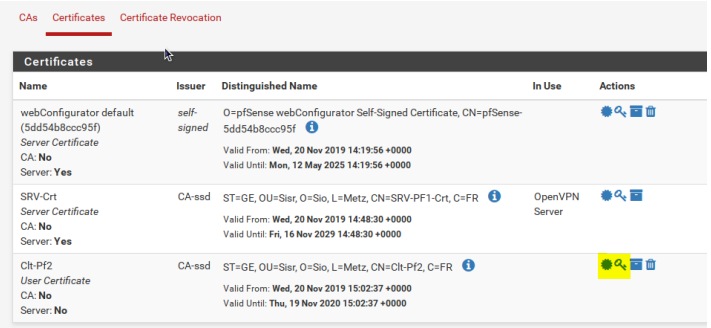
2 créer le certificat du serveur principal

dans Certificates - faire Add et créer le certificat serveur .
Attention : dans les attributs de certificat, choisir serveur et à faire le lien avec les informations de l'autorité de certification précédemment créée



3 créer le certificat du serveur 2

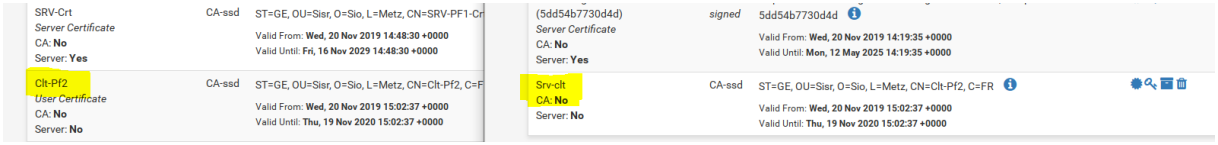
Exporter le certificat et la clé

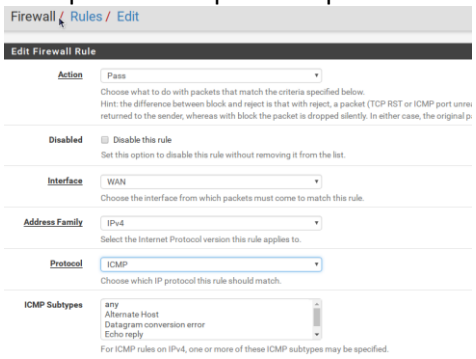
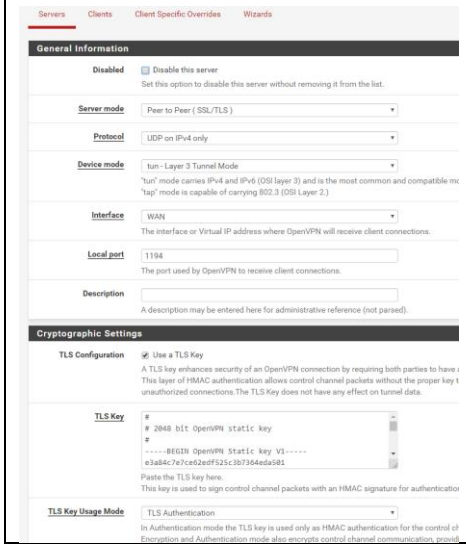


3' Importer le certificat client depuis le serveur principal

dans Certificates - faire Add et importer le certificat et la clé du client

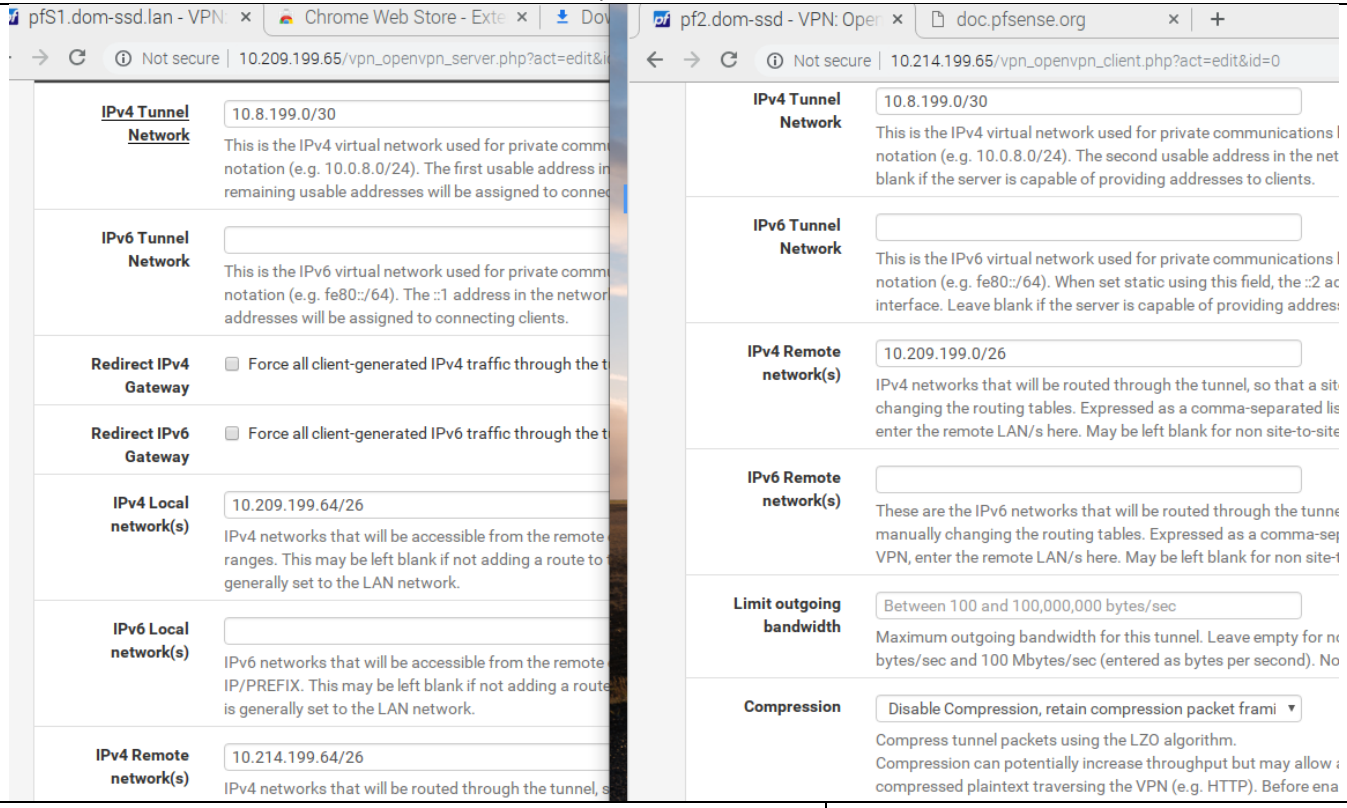
Le nom est différent à l'affichage mais les données et les clés sont identiques.

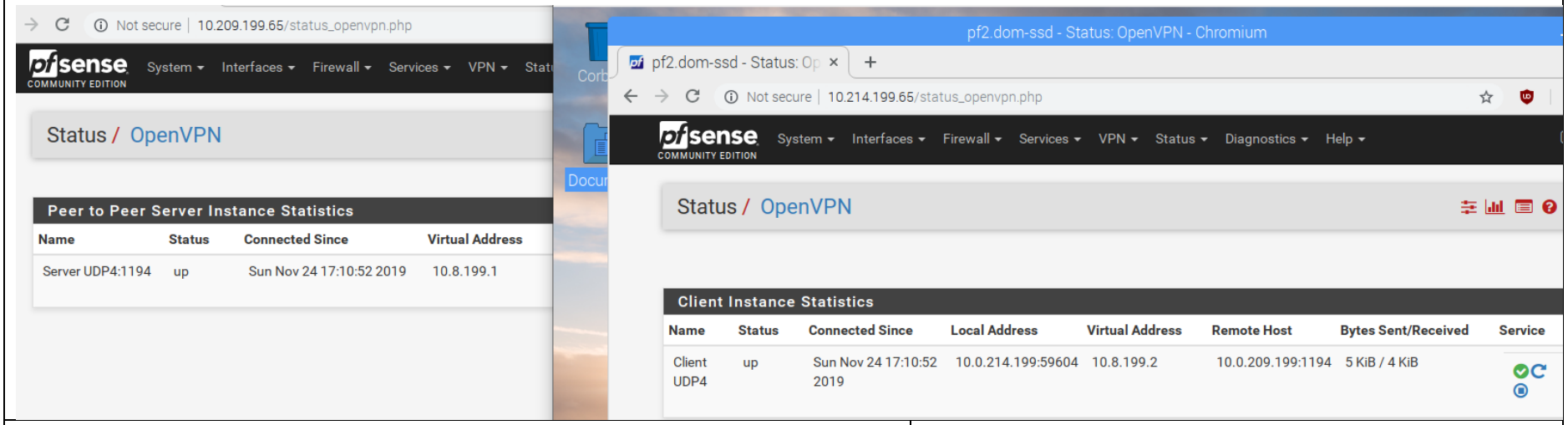


<table>
<tr><td colspan="2">Création du VPN</td></tr>
<tr><td colspan="2">Petite recommandation : créer une règle sur les deux serveurs pour laisser passer le protocole ICMP sur l’interface Wan, le temps du réglage.
 
</td></tr>
<tr><td>Ensuite aller dans le Menu VPN,</td><td></td></tr>
<tr><td>OpenVPN, aller dans l’onglet serveur et Add/
Saisir les infos toujours en cohérence avec les infos des certificats.
UDP est plus rapide pour les liaisons site à site.</td><td>OpenVPN, aller dans l’onglet client et Add/</td></tr>
<tr><td></td><td>Saisir les infos en cohérence avec le 1 serveur</td></tr>
<tr><td> 
</td><td>Importer la clé TLS</td></tr>
</table>

Pour TLS : choisir générer. Sauvegarder la configuration puis rouvrir la page et copier la clé TLS dans un fichier qui sera exporté sur le serveur 2.

Saisir les parametres de réseau



La création d'un service VPN client ou serveur génère une nouvelle carte réseau. Il faut aller dans le menu Interface de chaque serveur pour assigner les cartes Vpn. Il faudra ensuite les activer.

Création des règles	
Il faut autoriser le trafic entre les sites – A faire par étapes : quel interfaces quels réseaux Autorisé au plus large puis réduire.	
Le tunnel est établi