Guastamacchia
Livio
SIO2

04/03/2025

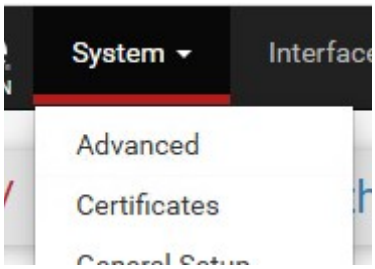
Configuration d'un VPN-SSL client-to-site avec OpenVPN :

Introduction :

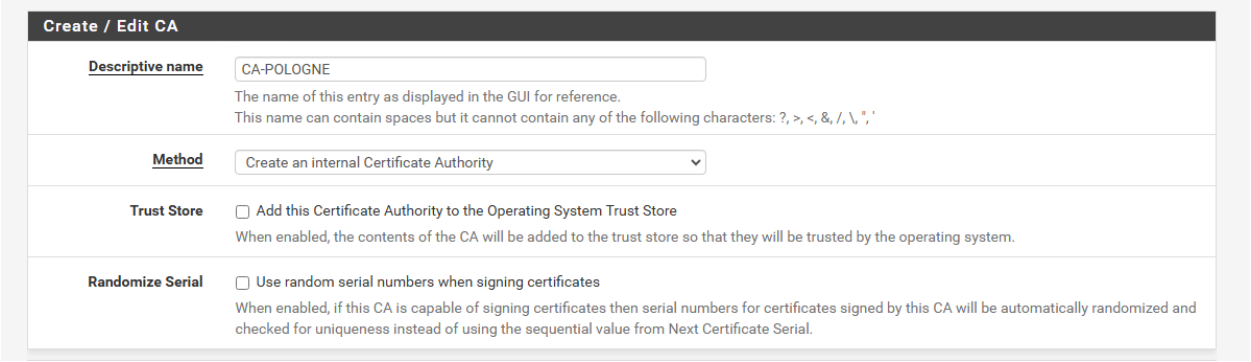
Dans ce TP, nous allons effectué,

TP :

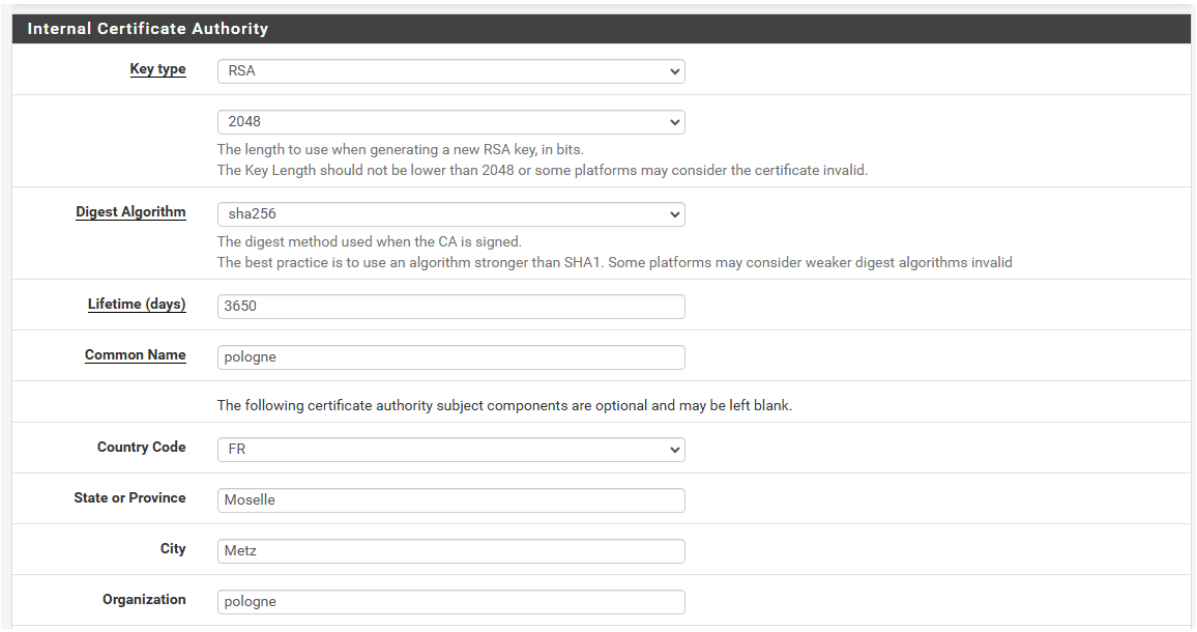
Pour débuter ce TP, Nous allons créé une autorité de certification sur notre pare-feu Pfsense.
Pour cela nous nous rendons dans « systeme » puis « certificate »



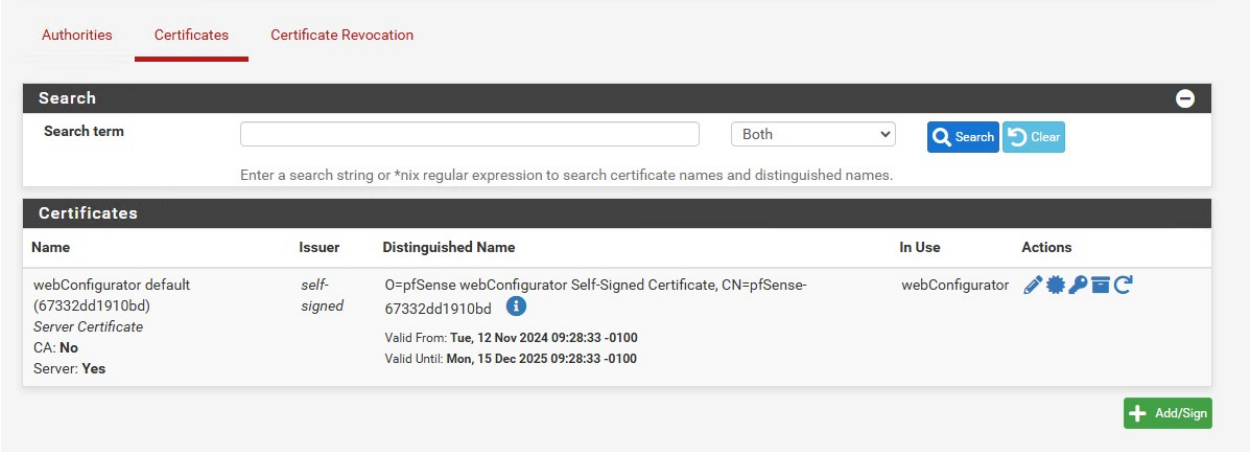
En premier lieu nous lui donnons un nom et prenons une autorité de certification interne



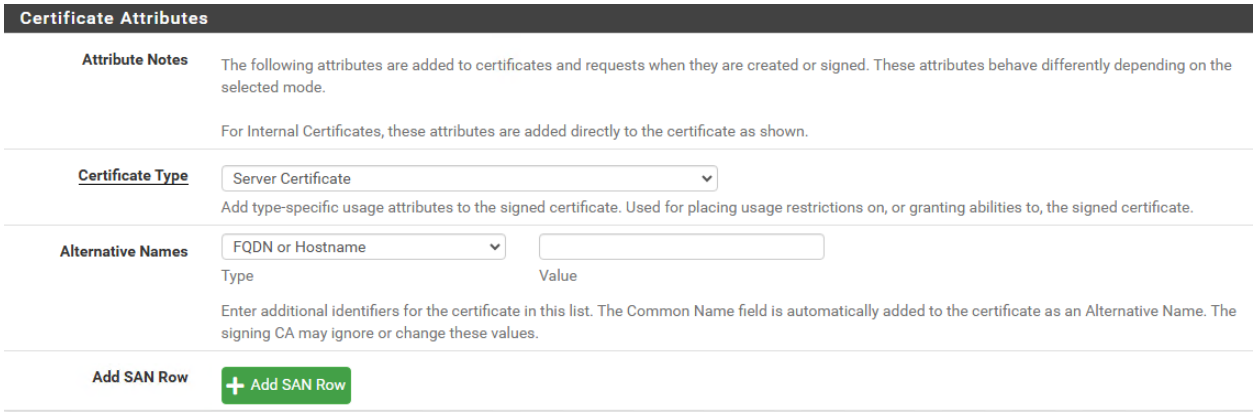
Ensuite, il nous reste plus qu'a rentrer les informations du certificat et notre autorité sera créer



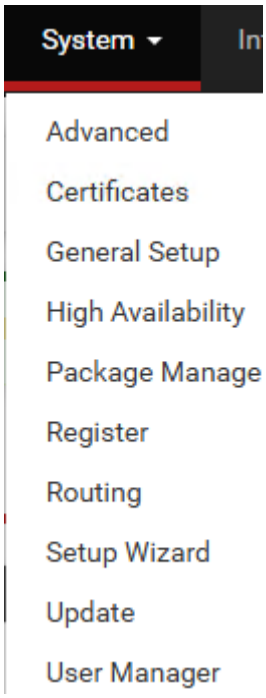
Passons maintenant a la créations du certificat, dans l'onglet « certificat »



Nous refaisons les même manipulation que précédemment, le petit changement sera a la fin. Nous devons choisir le type de certificat, nous choisissons un certificat de serveur

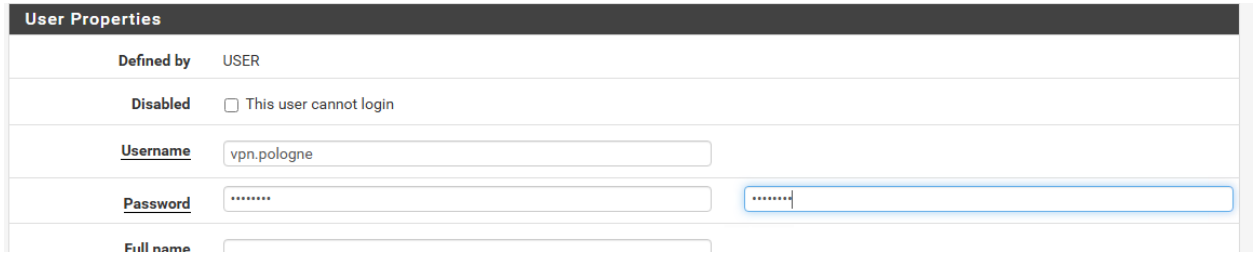


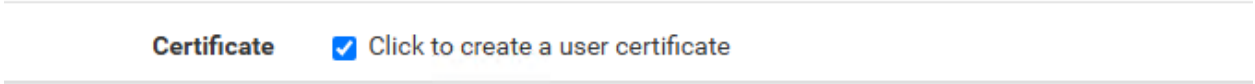
A présent, nous allons créé un utilisateur dans l'onglet « systeme » puis « user manager »

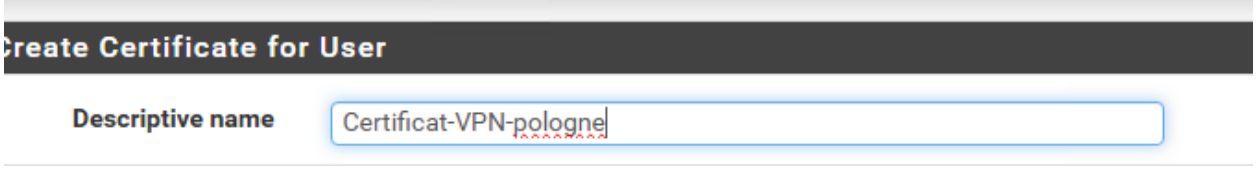


Pour créé un utilisateur il faudra lui donner un nom ainsi qu'un mot de passe. Nous pouvons aussi cocher la case certifi-

cat afin de lui créer un certificat utilisateur directement depuis l'interface de création de l'utilisateur. Il nous suffira juste de rentrer le nom du certificat.

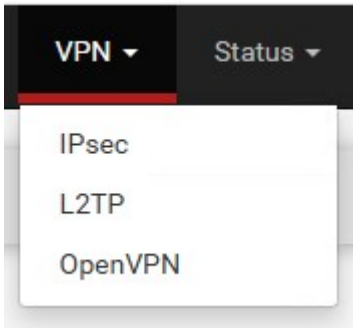




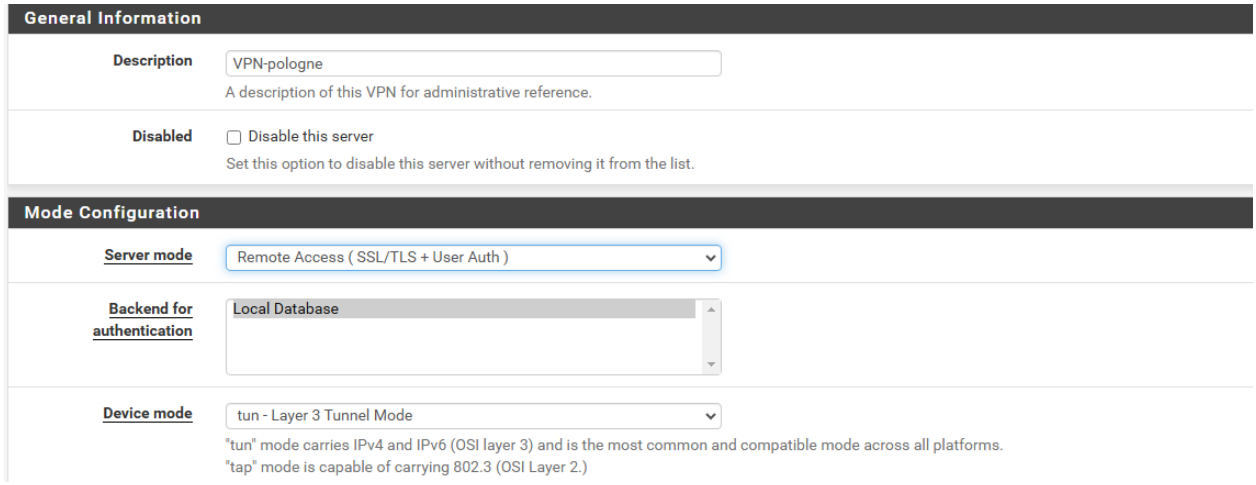


Création de la configuration de OpenVPN :

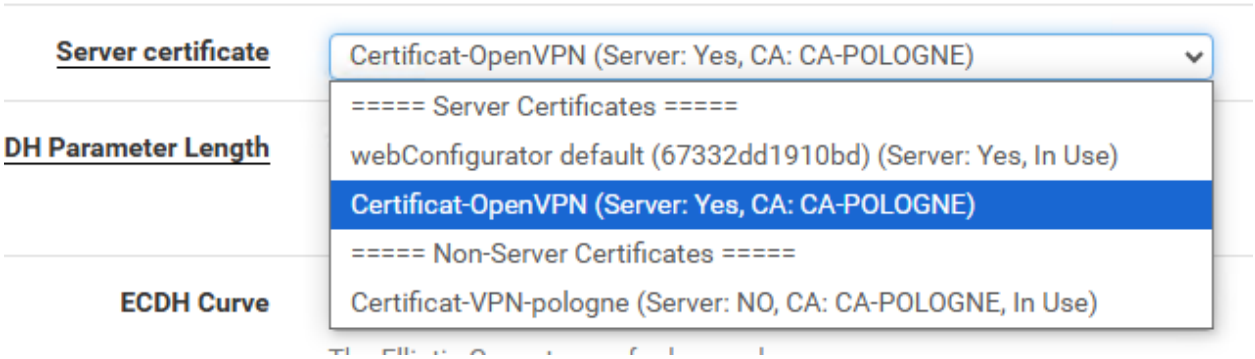
Pour créer la configuration il faudra allé dans l'onglet « VPN » puis « OpenVPN »



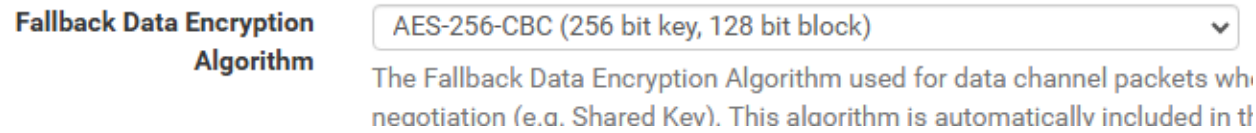
En mode de serveur nous prendrons « remote access (SSL/TLS + User auth) » qui est un accès a distance basée sur certificat et compte utilisateur. Nous prendrons la base de donnée local, si nous avons un annuaire LDAP nous le retrouvons aussi a cette endroit.



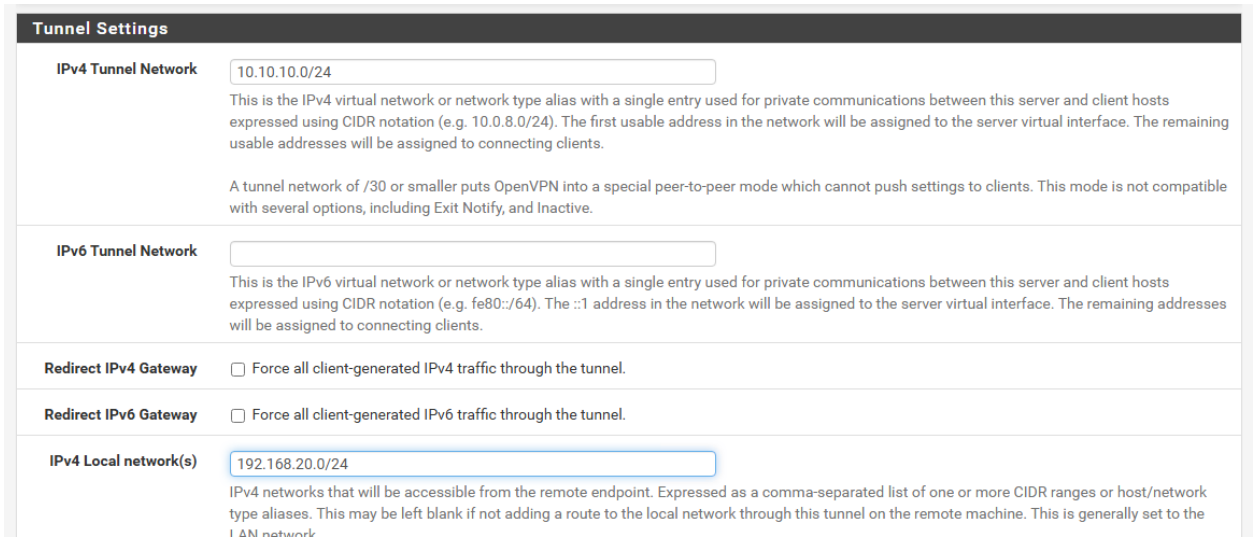
Au niveau de « server certificat » nous sélectionnons le certificat de serveur que nous avons créé précédemment



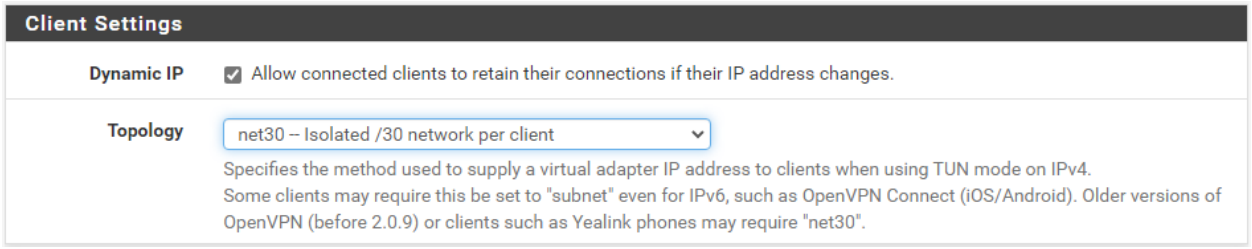
Nous prendrons la méthode de chiffrement ci-dessous, elle est plus lourde mais plus sécuriser



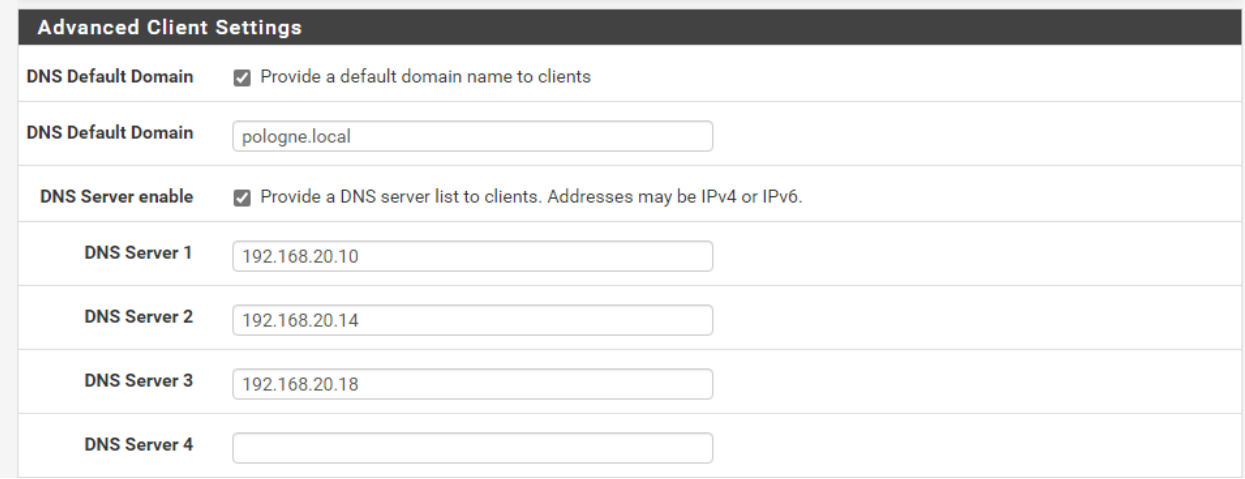
Passons aux paramètre IP, le tunnel network sera l'ip de notre VPN et l'ip local network sera la plage d'ip de destination de notre.



Nous cochons, la case IP dynamic afin que les clients puisse garder leur connexion au VPN.
Pour la topology nous prendrons en /30 afin que tous les clients soit sur un sous réseaux différent.



Ici, nous rentrons le domaine ainsi que les DNS

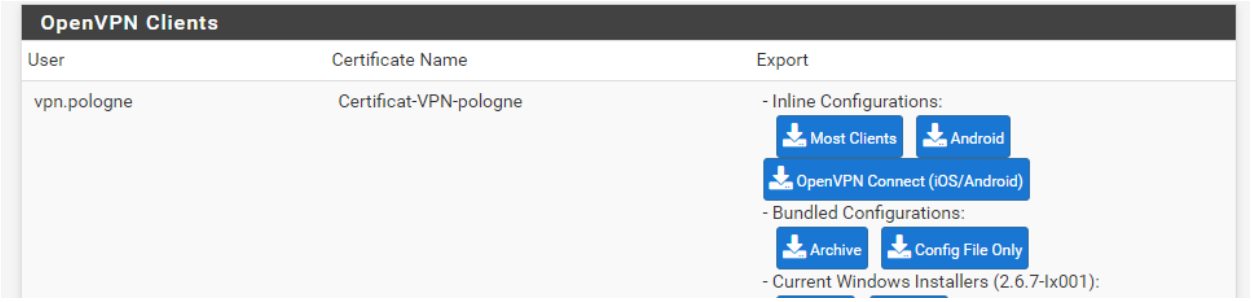


Dans les custom option, nous indiquons l'option « auth-nocache » qui évite la mise en cache des identifiant, ce qui offre plus de sécuriter

La configuration de OpenVPN coté serveur est fini, Nous allons voir comment exporter cette configuration car de base Pfsense ne le prend pas en charge. Pour cela nous allons allé dans le « package manager », dans la barre de recherche nous écrivons OpenVPN et nous trouverons « openvpn-client-export » et nous l'installons.

Dans l'onglet OpenVPN nous retrouvons un nouvelle onglet « client export », dans celui-ci nous pouvons laisser les paramètres par defaut, il faudra juste a nouveau écrire « auth-nocache » dans les configuration additionnelle

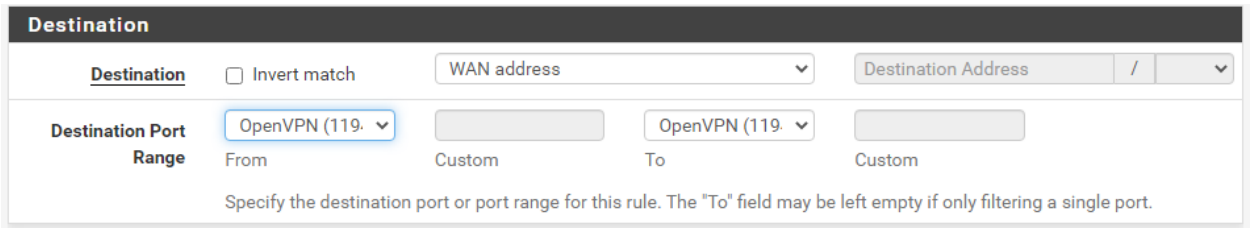
Pour obtenir la configuration, nous descendons en bas de page et prenons l'archive du bundled configurations



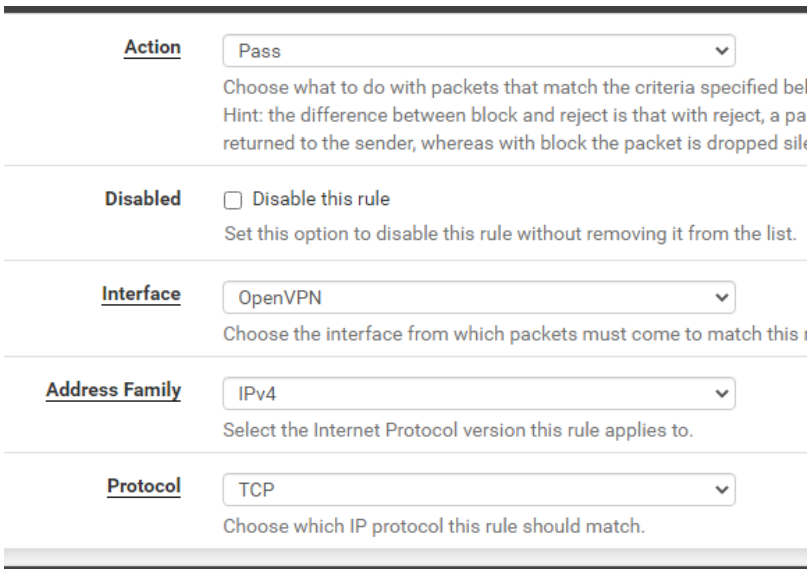
Passons a la création des règles de pare-feu.

Nous allons créé une nouvelle règle UDP sur l'interface WAN

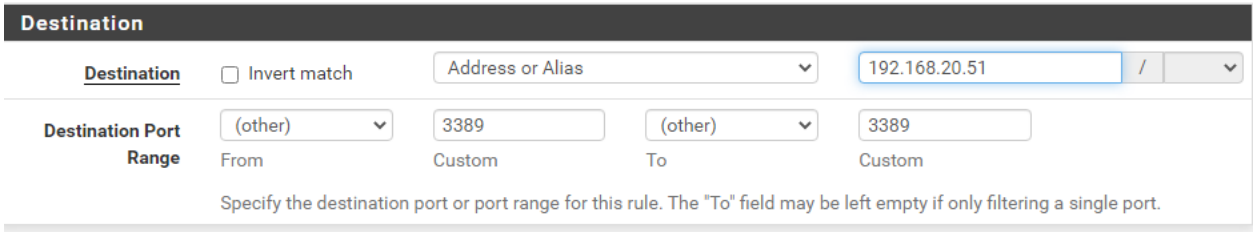
En destination nous prenons la WAN adress et pour le port, le port OpenVPN



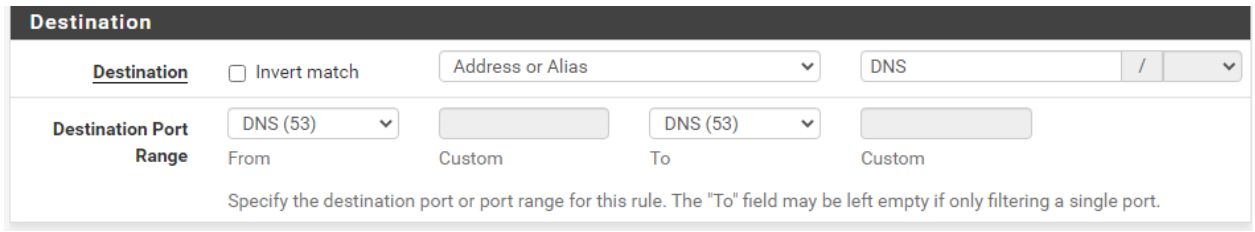
La prochaine règle sert a autoriser les ressources, Nous prendrons l'interface OpenVPN



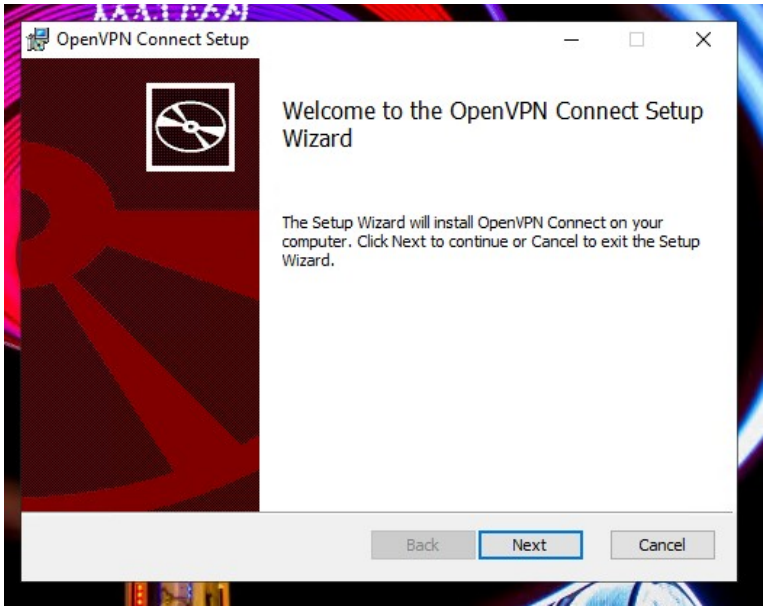
Dans la destination nous autoriserons le protocole rdp (port 3389) sur notre poste client



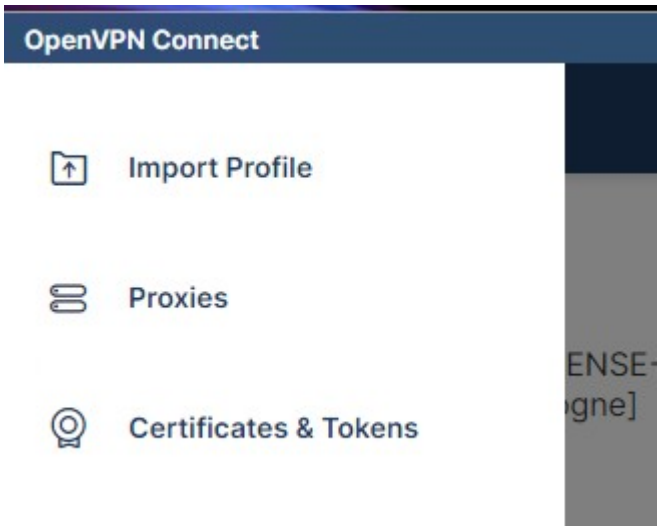
Ensuite, nous créons une règle sur l'interface OpenVPN pour le DNS, en destination j'ai pris un groupe créer au préalable nommer « DNS » qui regroupe mes trois serveur DNS. En port, nous prenons le port DNS (53)

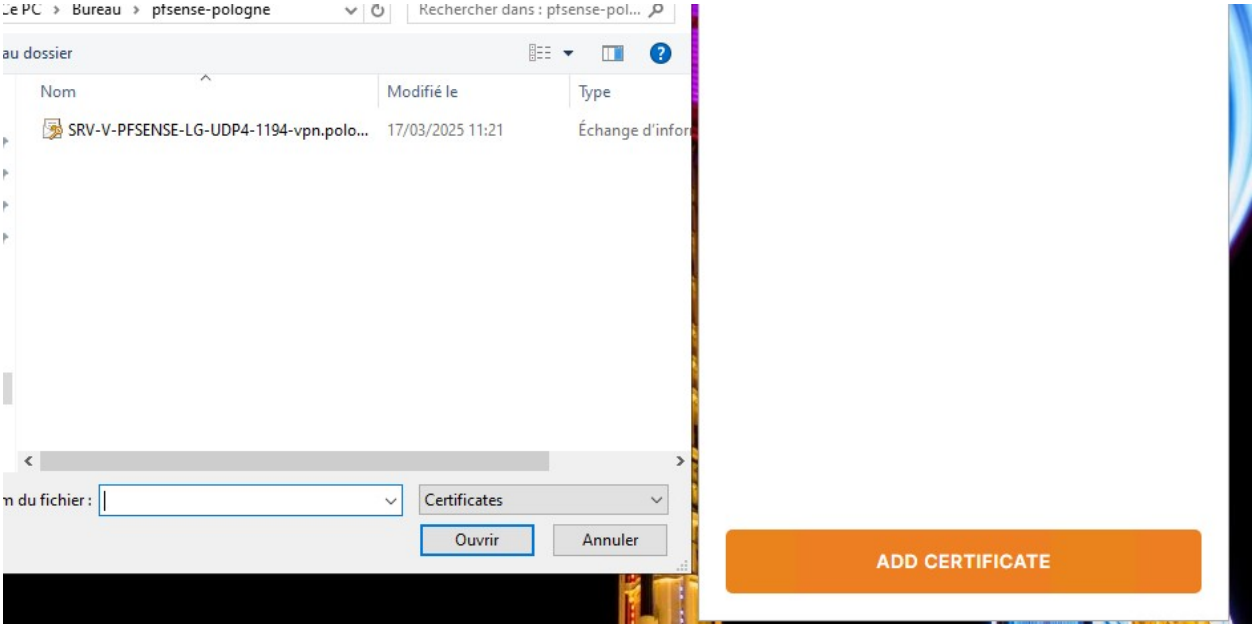


Passons sur le poste client a présent afin d'installer OpenVPN



Sur l'application, nous allons ajouter le certificat pour cela nous allons dans l'onglet « certificates & tokens » –> « add certificate » puis nous prenons le certificat qui se trouve dans le fichier export télécharger au préalable.





Après il ne suffit plus que se connecter au poste.