Configuration d’un pare-feu Fortigate M2L

Dans le cadre de l’évolution et sécurisation du parc informatique de la M2L, la solution FORTINET a été choisie, C’est un routeur faisant également office de pare-feu équipé de multiples options de sécurisation , de filtrages web , configuration VPN et autres.

Cahier des charges

- Remplacement du commutateur SWM2L(lvl3) et du routeur RTRM2L du contexte.
- Le pare-feu FORTINET FORTIGATE 30e assure la sécurisation des zones LAN,DMZ,WAN mais également la translation d’adresse NAT/PAT entre LAN et WAN, le filtrage des accès web et la configuration VPN.

Contraintes

- Aucun changement sur le plan d’adressage

Initialisation

Tout d'abord pour réinitialiser le Fortinet il faudrait:

1. se rendre dans le mode console -
2. écrire admin
3. appuyer sur entrer 2 fois (vue qu'il n'y a pas encore de mot de passe (dans notre cas))
4. écrire execute factory et puis entrer

Configuration Initiale

Admin

config system interface #entre directement dans l'intdaterface

edit port1 #pour edité l'interface n°1

set mode sattic #Port en statique donc pas de DHCP

set IP 172.1.2.254/24 (par exemple)

set allowaccess http ssh ping #accord des permission d'accès à distance avec l'adresse IP

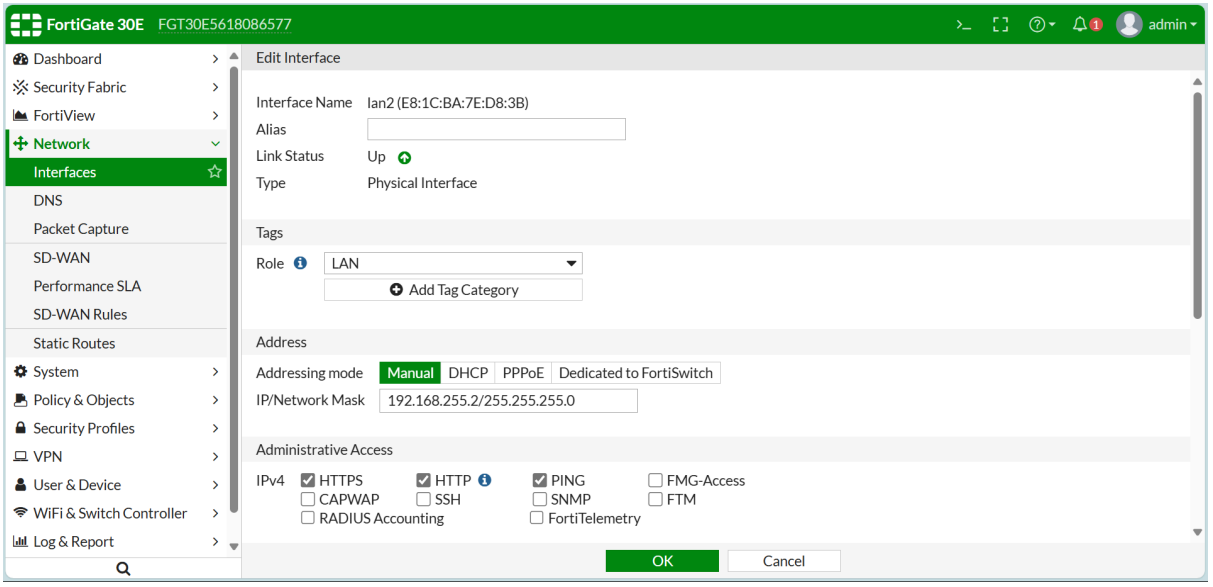
show #Vérification des paramètres

end #effectuer une sauvegarde

Configuration des interface LAN

Tout d'abord, après s'être log sur le routeur, on a créé une interface avec l'UI sur le LAN correspondant, içi le LAN 2 avec l'adresse 192.168.255.2 255.255.255.0 .

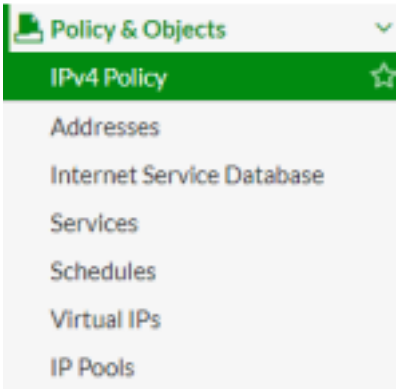
On'y active les accès HTTPS,HTTP pour les services web, PING pour les tests, SSH pour les connexions à distances CAPWAP et FMG-Access.



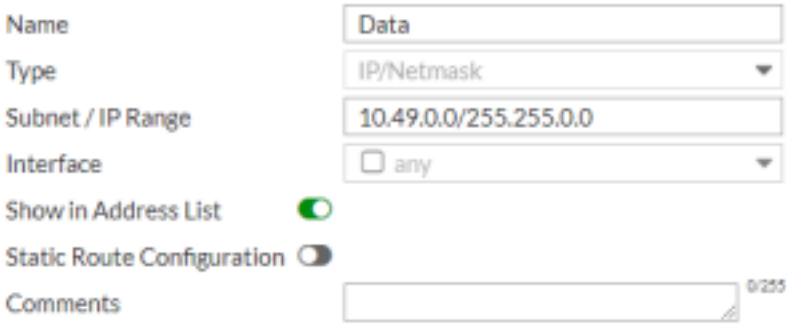
Filtrage firewall

Pour créer un filtrage firewall, il faut faire une **nouvelle Policy** mais avant de créer cette Policy il faudra créer des adresses (ce n'est pas obligatoire cela dépend de quel filtrage que tu veux faire), il y deux façons de le faire

La première méthode est d'aller directement dans adresse



Ensuite faire un create -> adresse, il faut lui donner un nom et une adresse range par exemple 10.49.0.0/16



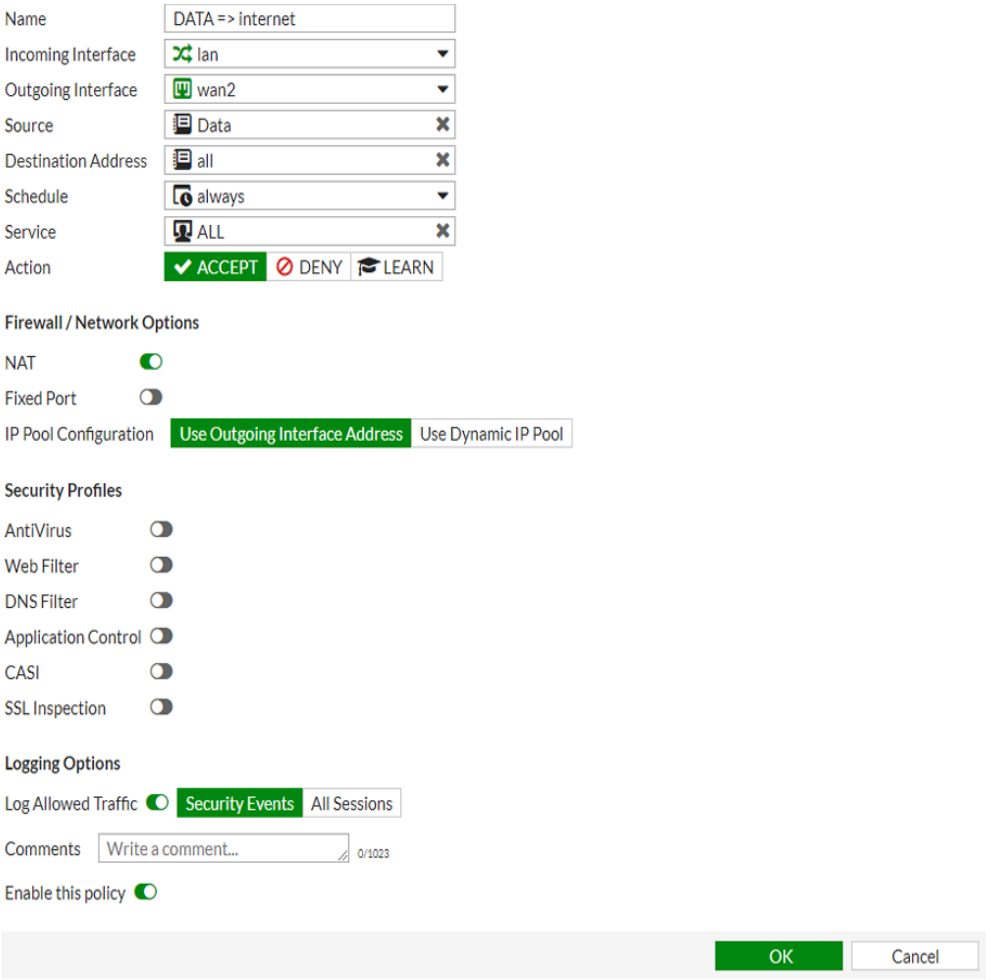
La deuxième méthode est de créer directement dans l'IPV4 Policy

On fait créer une nouvelle Policy -> cliquer sur source

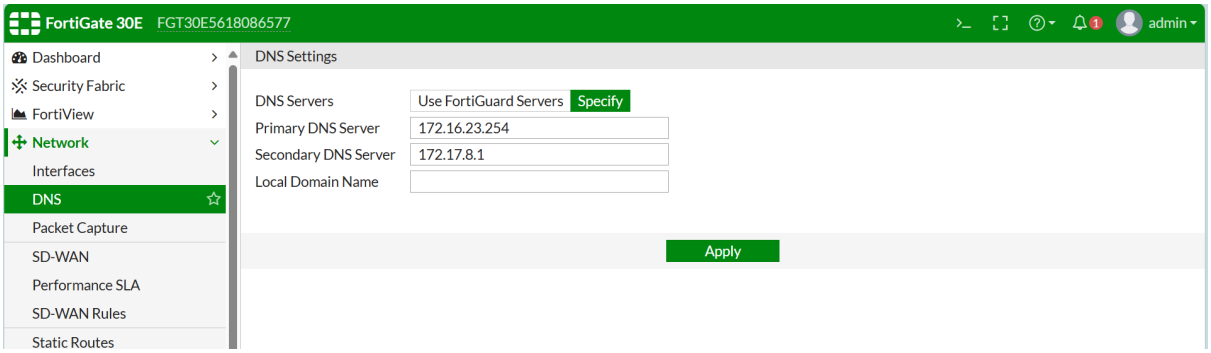
ensuite **+** puis **adresse .**

Par la suite nous allons dans IPv4 Policy, puis créer un filtre qui permet à la ranger de l'adresse 10.49.0.0 d'accéder à internet

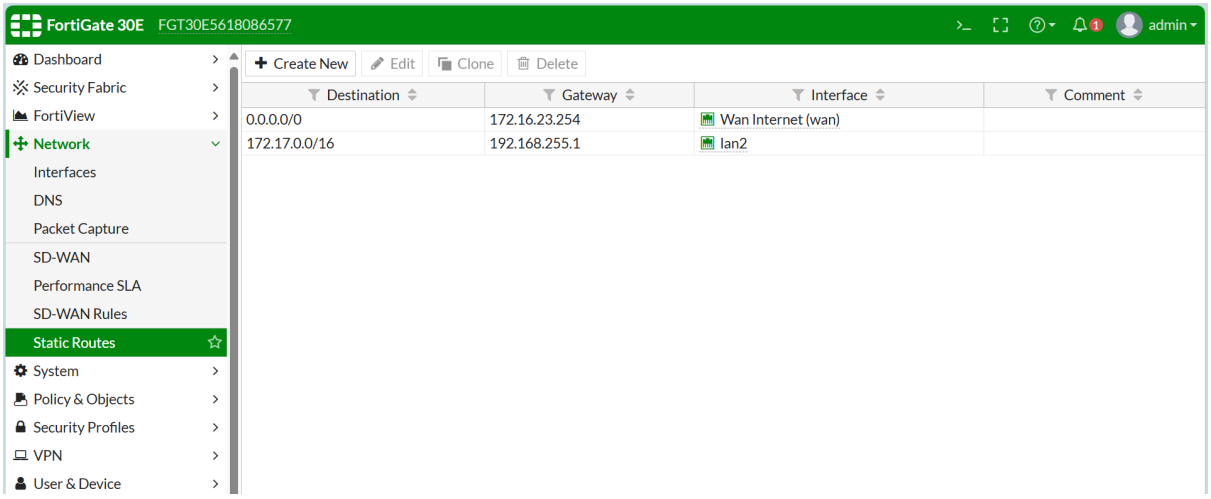
On fait créer une nouvelle Policy

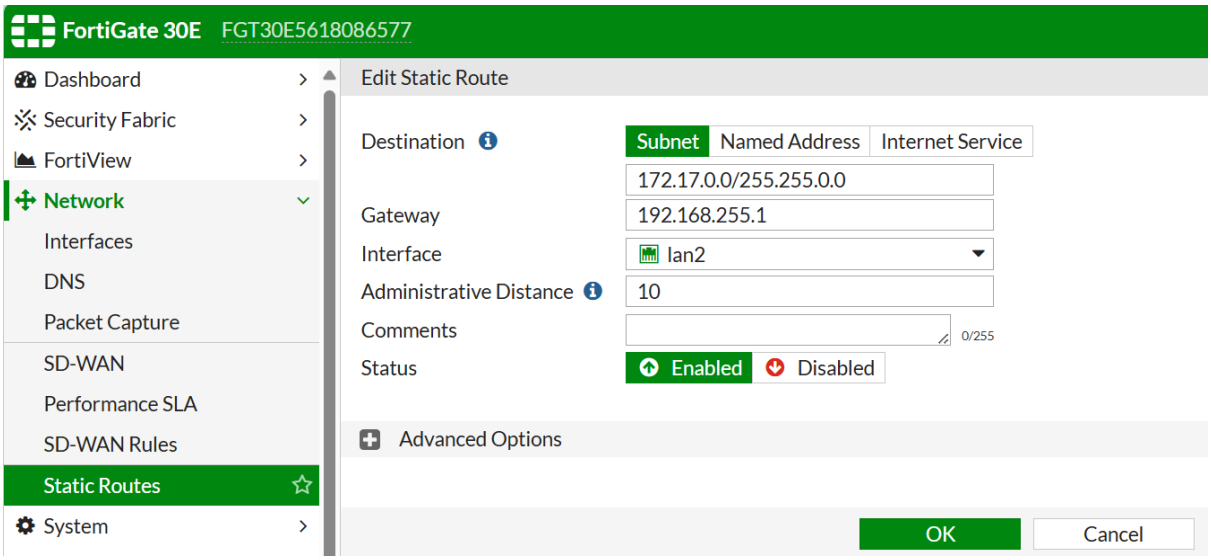


Configuration du DNS



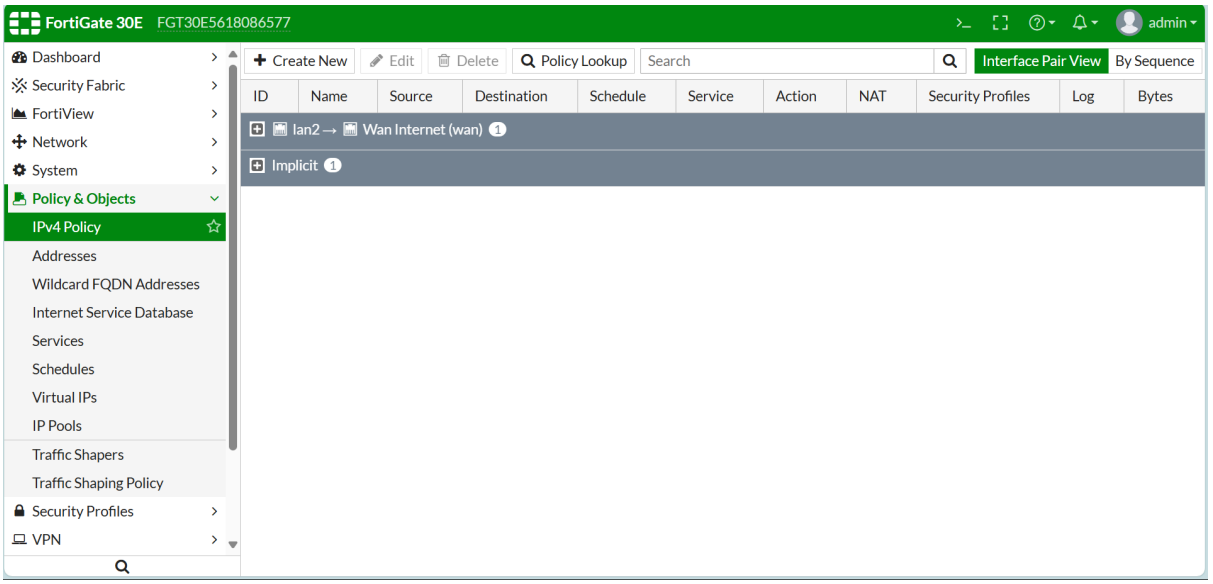
Configuration de la route statique

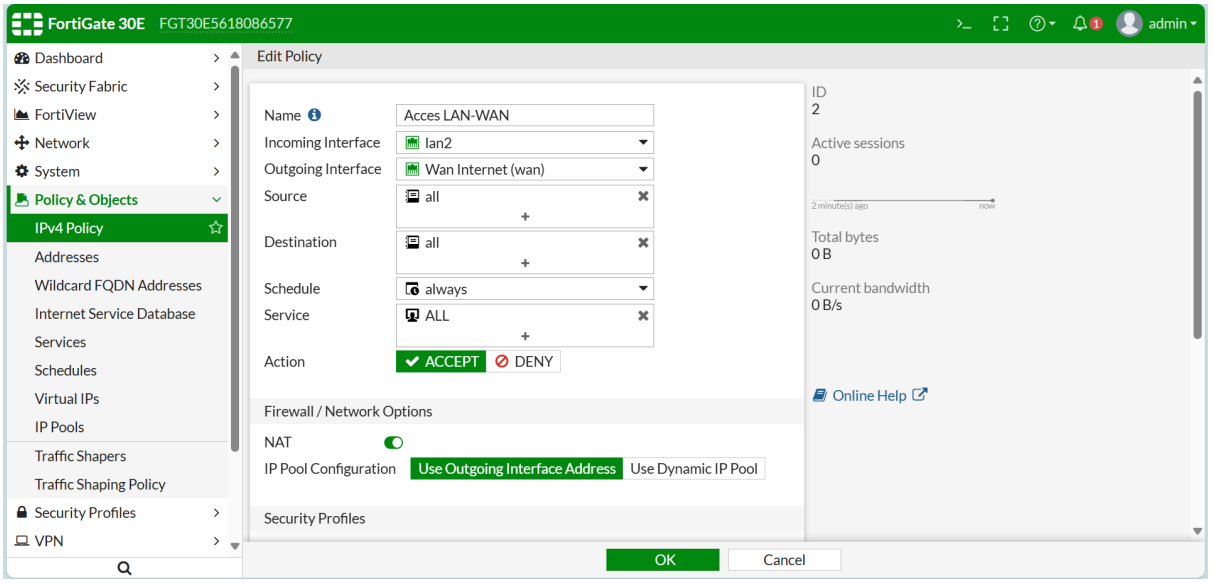




Liaison LAN-WAN

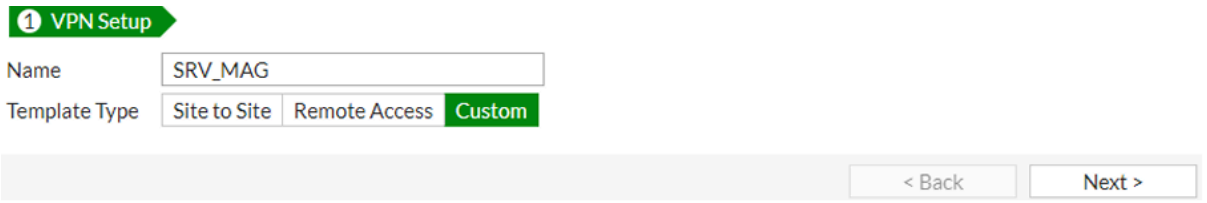
On va dans Policy & Objects > IPv4 Policy



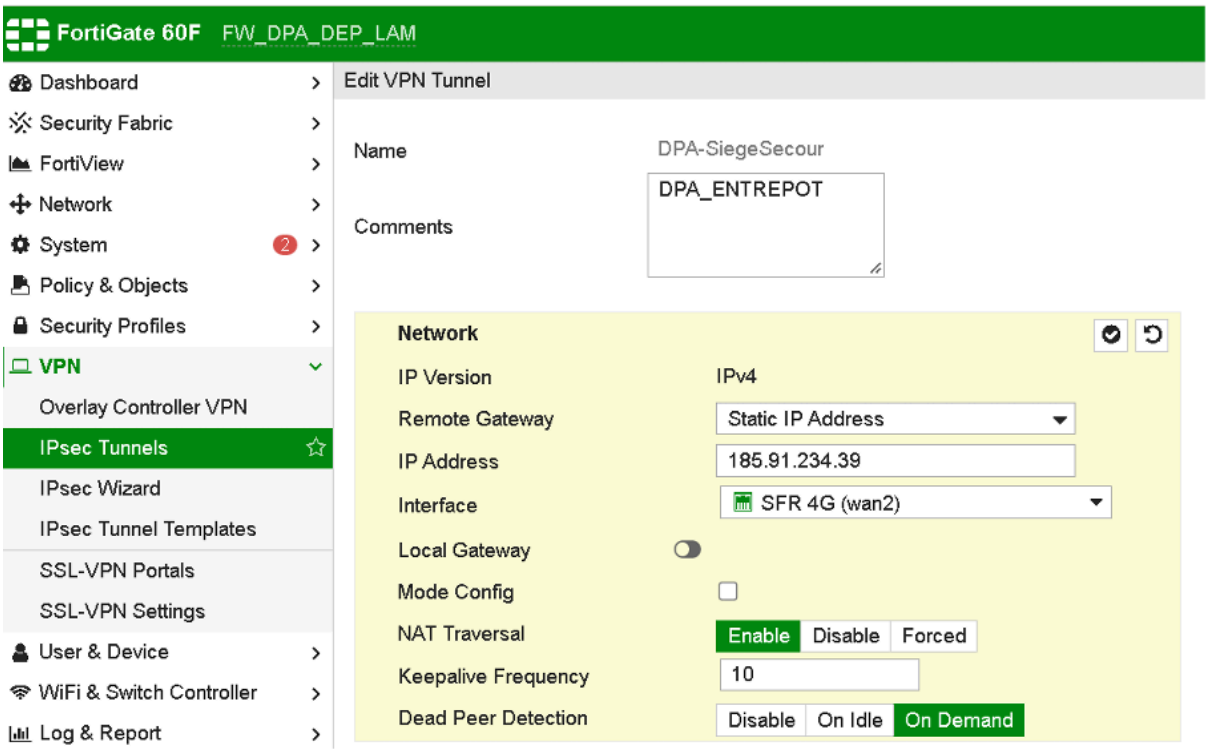


Configuration des Portail VPN SSL

Pour commencer, il faut cliquer sur VPN -> IPsec Wizard -> custom , vous appuyer sur Next

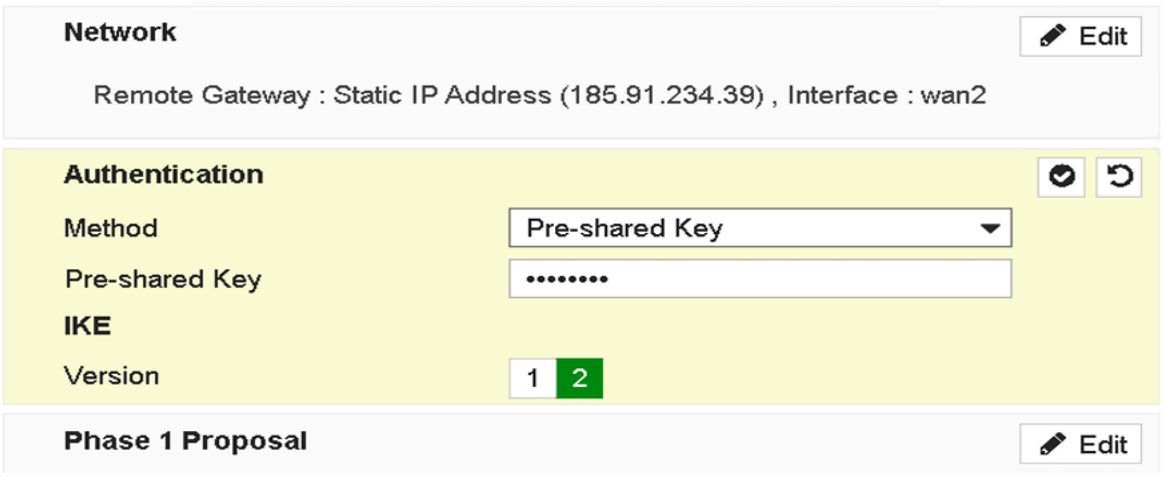


Après il faut configurer le tunnel du VPN



Ensuite la création du tunnel du VPN

D'abord créer une clé pré-partagée



Authentication Edit

Authentication Method : Pre-shared Key

IKE Version : 2

Phase 1 Proposal Add

Encryption AES128 Authentication SHA256

Diffie-Hellman Groups 31 30 29 28 27 21 20 19 18 17 16 15 14 5 2 1

Key Lifetime (seconds) 86400

Local ID 160

Phase 2 Selectors

Phase 1 Proposal Edit

Algorithms : AES128-SHA256

Diffie-Hellman Groups : 14, 5

Phase 2 Selectors

Name	Local Address	Remote Address
DPA-SiegeSecour	10.43.0.0/255.255.0.0	10.0.0.0/255.0.0.0

Edit Phase 2

Name DPA-SiegeSecour

Comments Comments

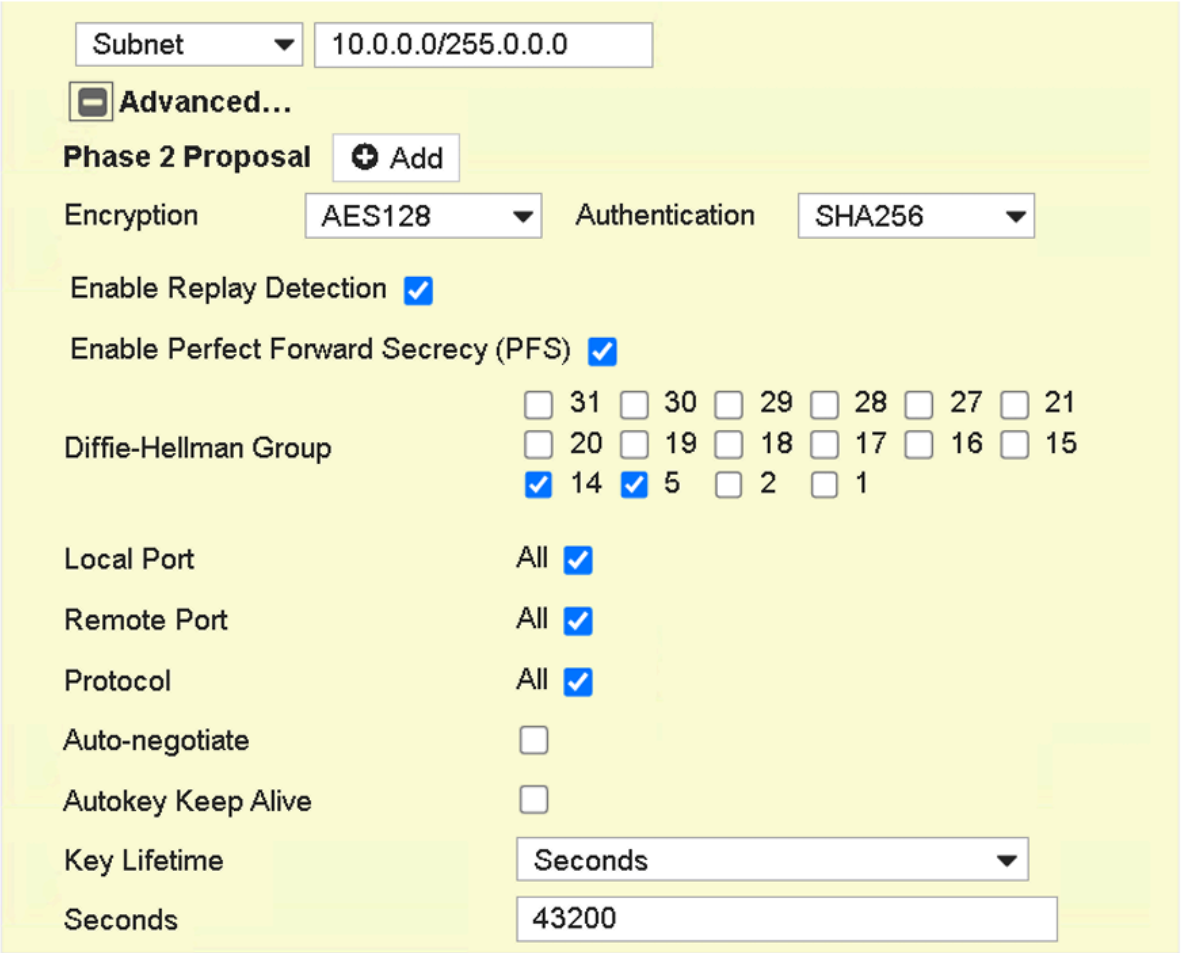
Local Address

Subnet 10.43.0.0/255.255.0.0

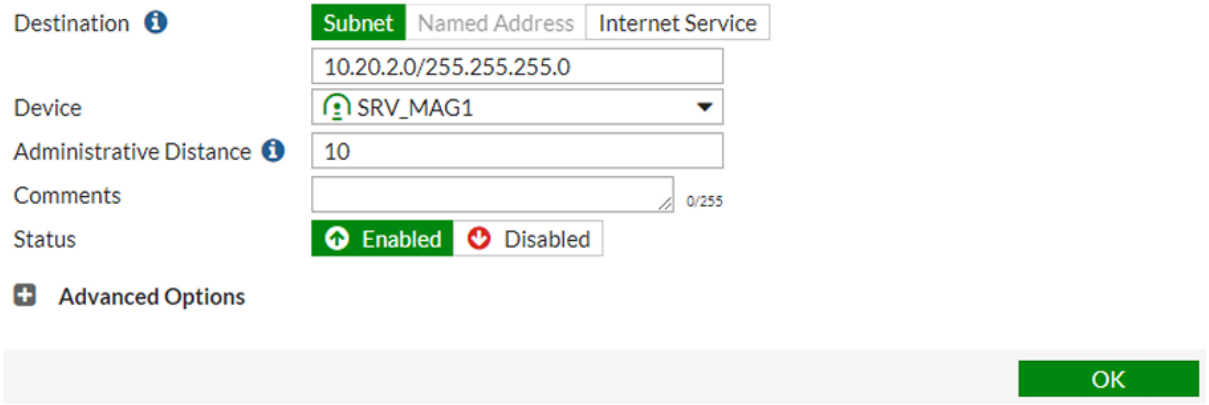
Remote Address

Subnet 10.0.0.0/255.0.0.0

Advanced...

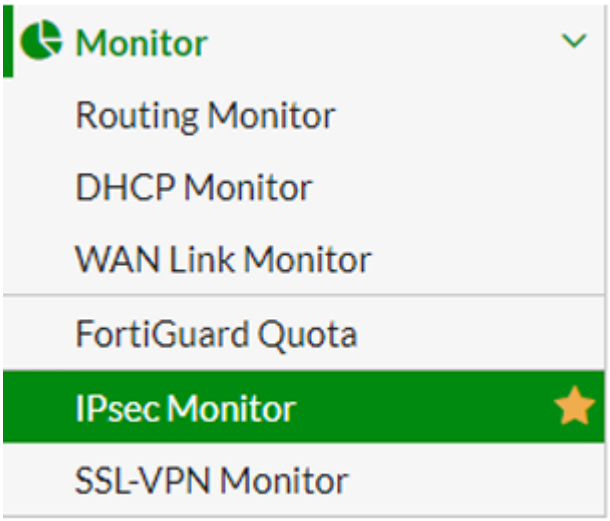


une fois que tout cela est fait , il faut créer une nouvelle route pour accéder au vpn

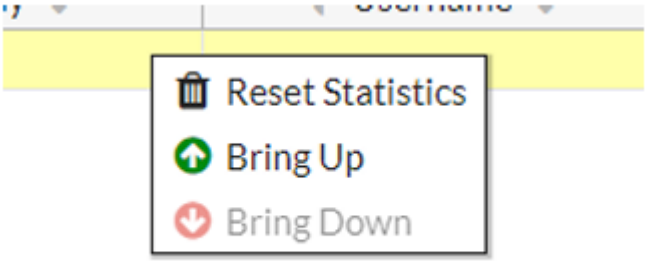


Lorsque vous choisissez le vpn dans device, il retire automatiquement le Gateway

Une fois la route créer, il est nécessaire de d'aller dans monitor -> IPsec monitor

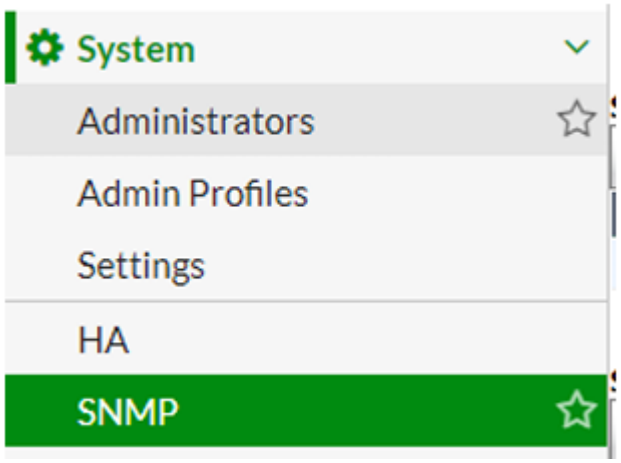


Puis vous faite une clique droite et vous cliquer sur Bring-up



Configuration SNMP

Donc dans l'onglet SNMP



On y ajoute le nom de la communauté et renseigner l'adresse du VPN, ensuite on active le SNMP Agent en haut de l’écran.