Configuration tunnel VPN site-to-site : routeur FORTINET

IP publique routeur ZyXEL : 192.168.248.108

IP publique routeur FORTINET : 192.168.248.117

Réseau local routeur ZyXEL à connecter en VPN : 192.168.20.0/24

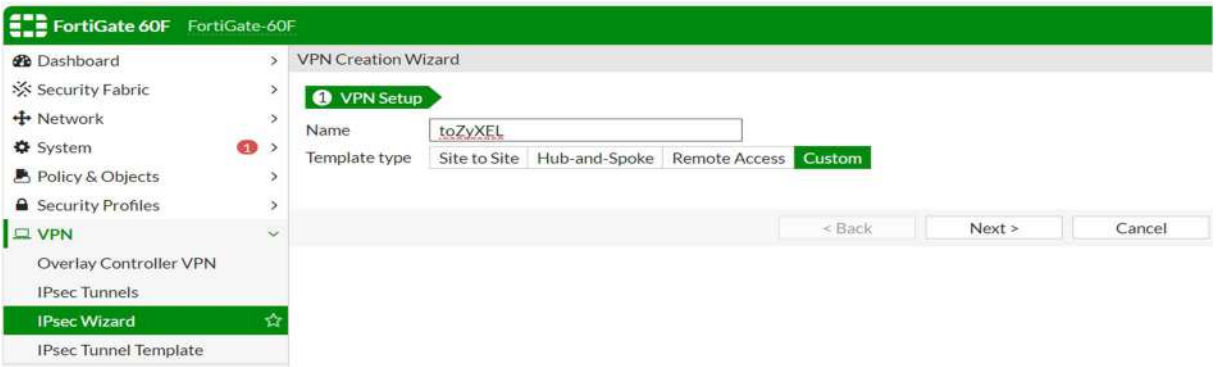
Réseau local routeur FORTINET à connecter en VPN : 192.168.30.0/24

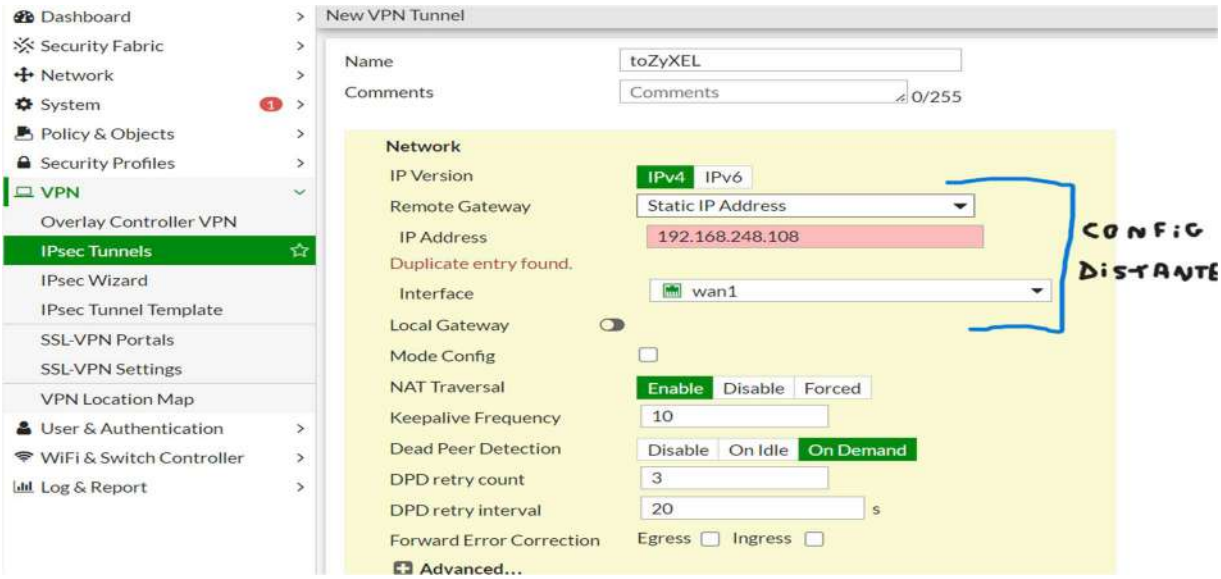
1/ Création & configuration d'un tunnel IPsec site-to-site

Sur FORTINET :

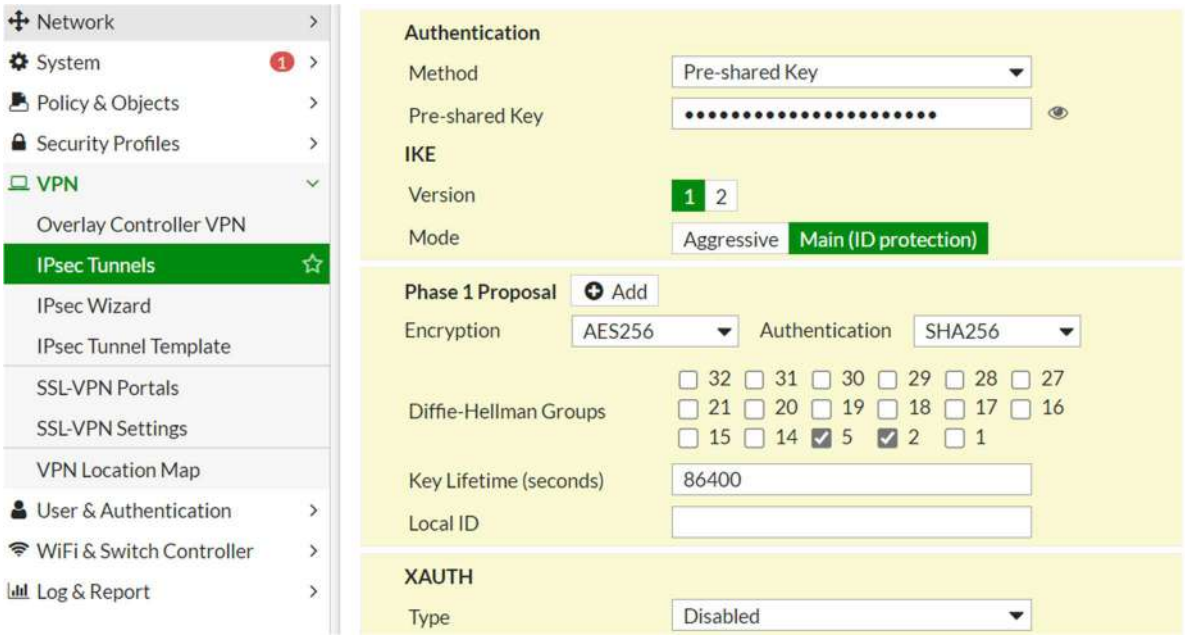
Phase 1 :

On crée un nouveau tunnel VPN IPsec customisé vers le routeur ZyXEL.



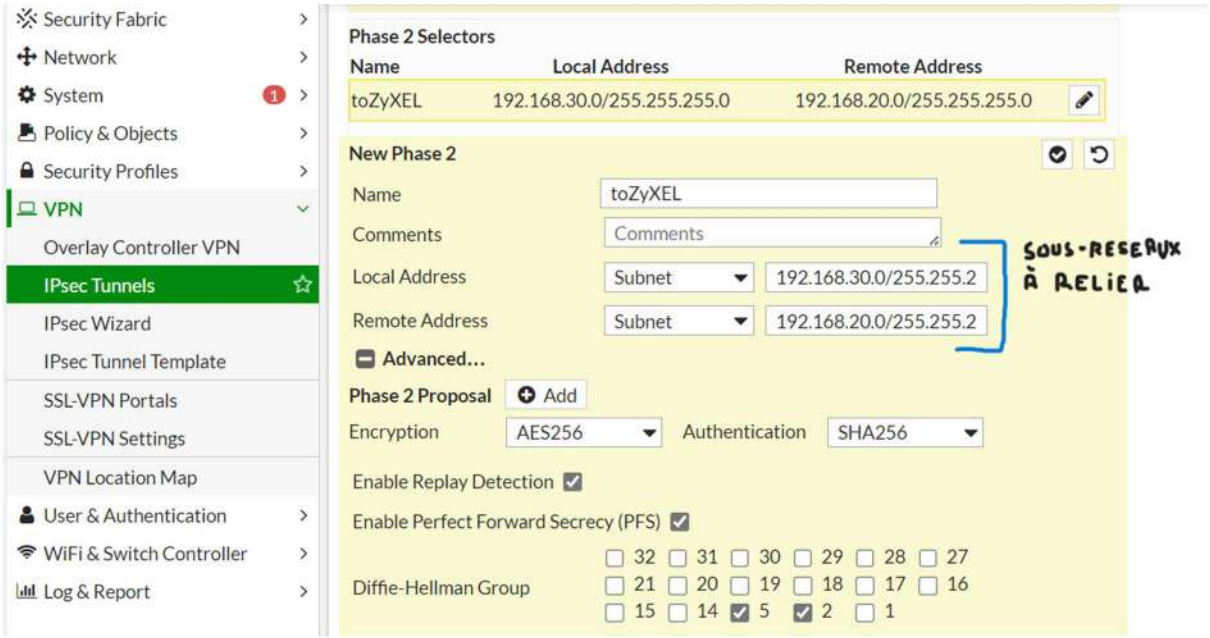


On signale la machine distante avec laquelle il devra communiquer en spécifiant son adresse IP publique.

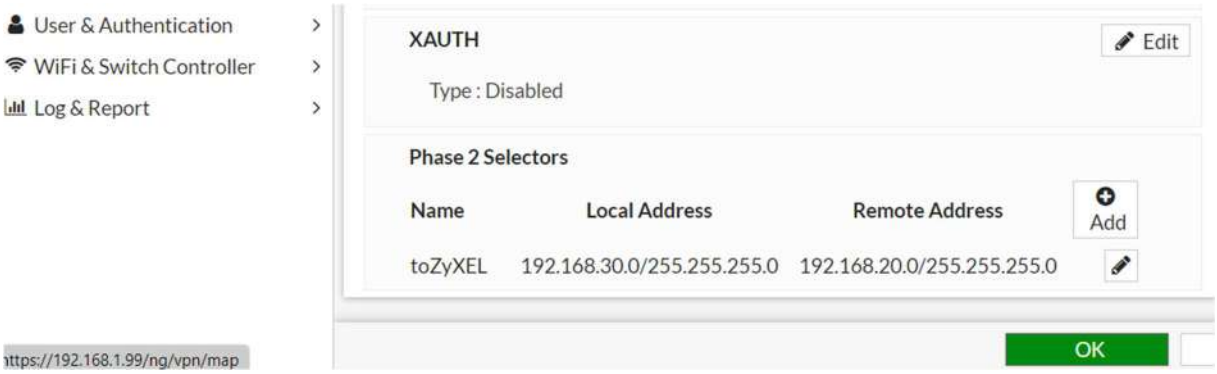


Toujours dans la phase 1, pour établir une connexion VPN les paramètres d'authentification (**Pre-Shared Key**), de protocole utilisé (**IKE Version**), et cryptage (**Encryption, Authentification, Diffie-Hellman Group(s), Key Lifetime**) **doivent être identiques sur les deux routeurs.**

Phase 2 :



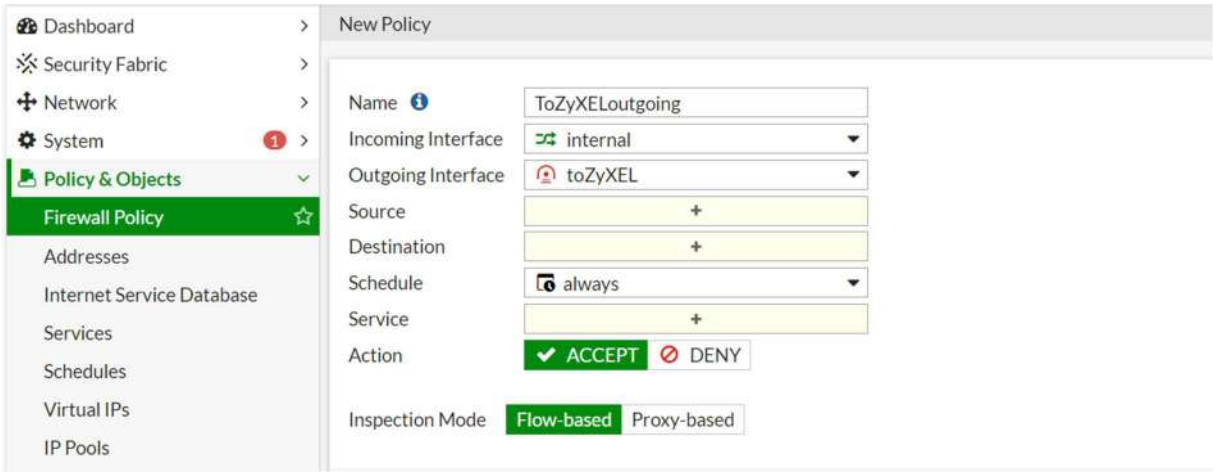
Les méthodes de chiffrement ainsi que le(s) Diffie-Hellman Group peuvent être différents de la phase 1 MAIS doivent être identiques à la phase 2 du routeur distant.



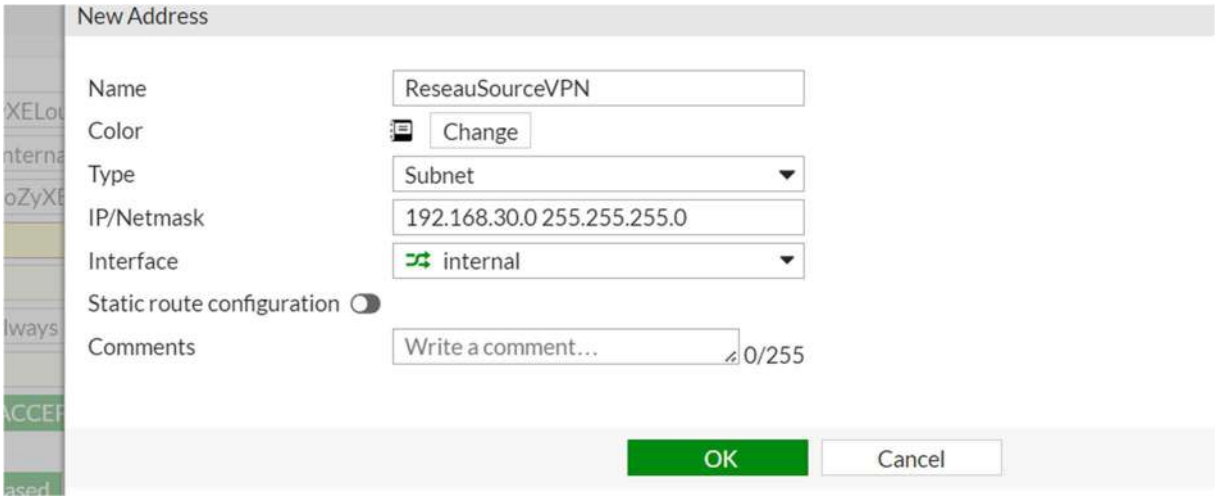
Il est possible d'ajouter directement d'autres réseaux à relier via tunnel VPN avec les mêmes paramètres sans devoir recréer un autre tunnel VPN.

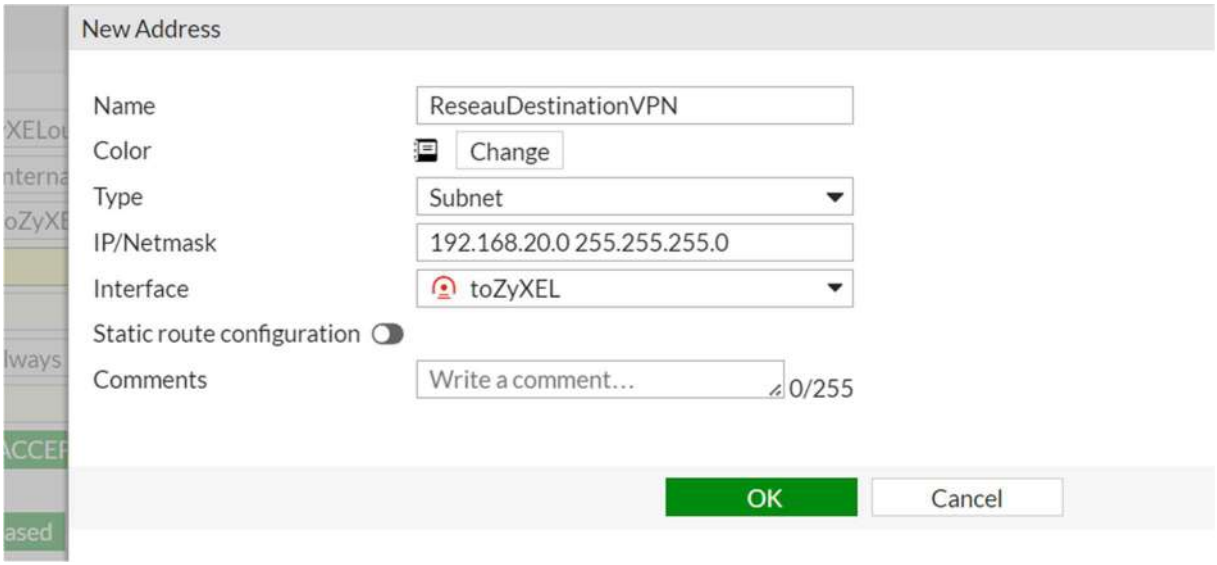
Règles de pare-feu :

Dans Firewall Policy, on vient créer deux règles de pare-feu pour autoriser le trafic **entrant** et **sortant** du Tunnel VPN vers le réseau local dans lequel il effectue des transferts avec le sous-réseau distant.

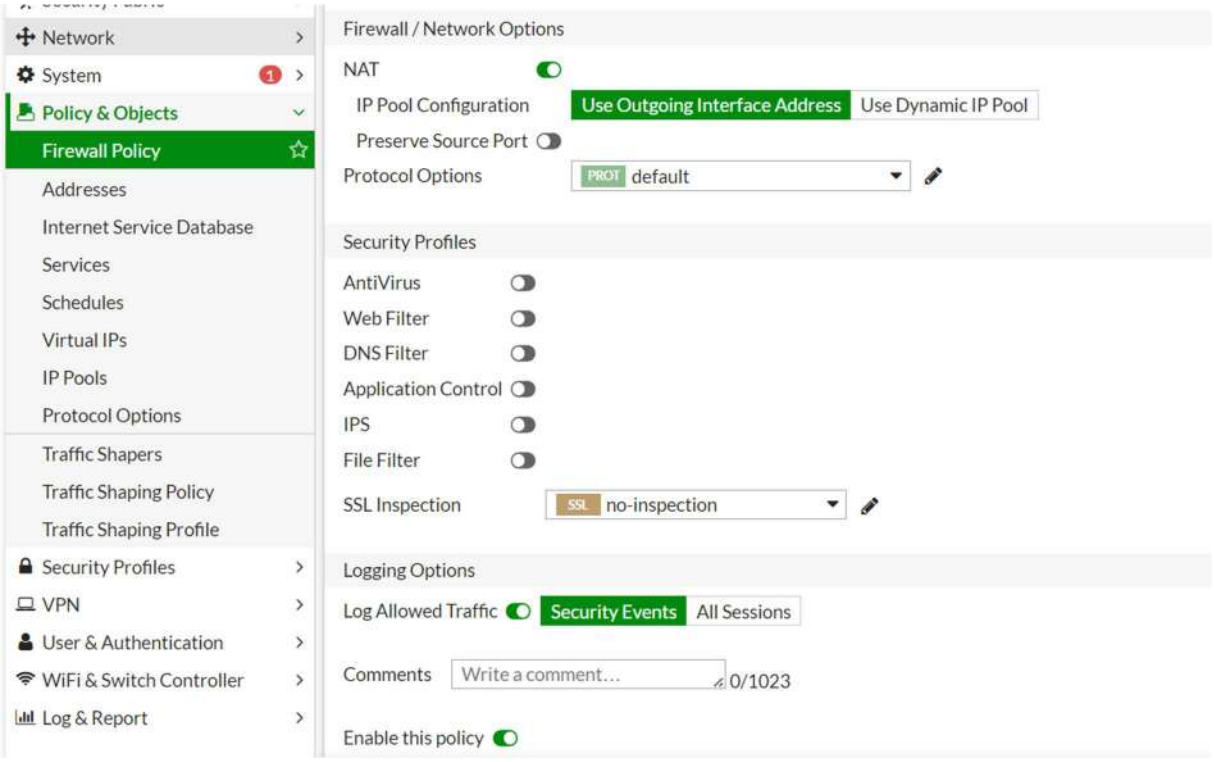


Pour la **source** et la **destination,** on crée une nouvelle adresse avec l'adresse du réseau correspondant au sous réseau local pour la source, et au sous réseau distant pour la destination.





On laisse les options suivantes par défaut :



Il ne reste plus qu'à créer la règle inverse pour autoriser le trafic provenant du Tunnel VPN ToZyXEL pour que la configuration du VPN du routeur FORTINET soit terminée.

Route Statique :

Enfin, une route statique doit s'être créer automatiquement afin de rediriger les données ayant pour destination le sous-réseau 192.168.20.0/24 vers le Tunnel VPN.