Configuration tunnel VPN site-to-site : routeur ZyXEL

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

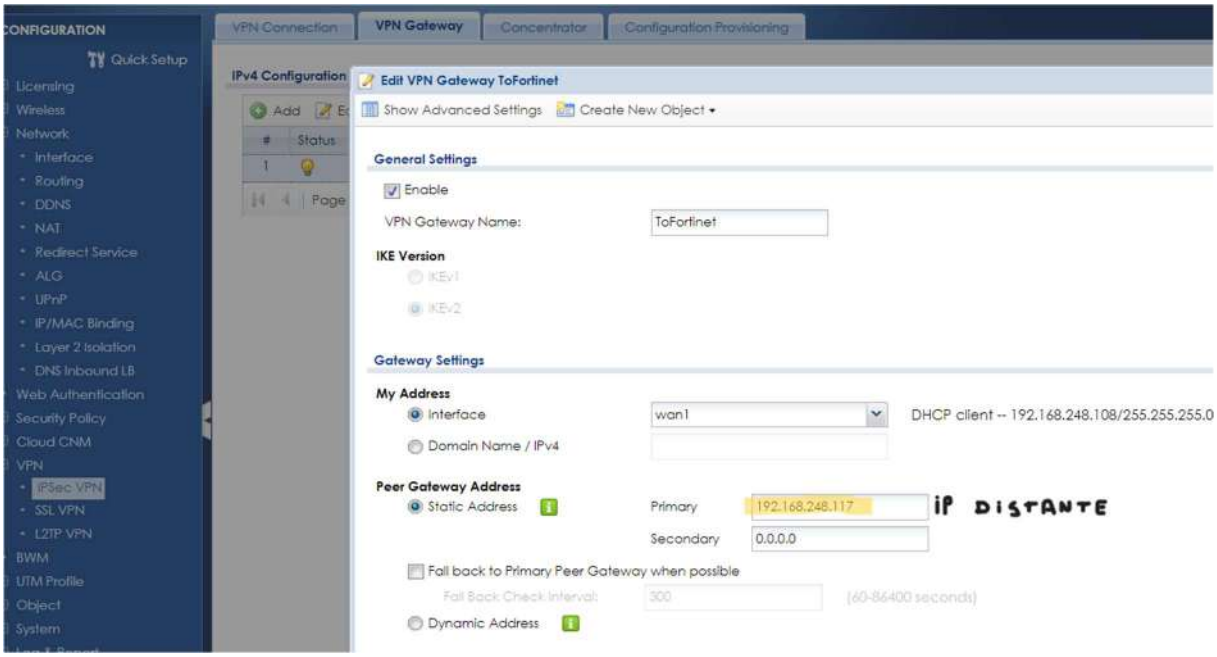
Réseau local routeur FORTINET à connecter en VPN : 192.168.30.0/24

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

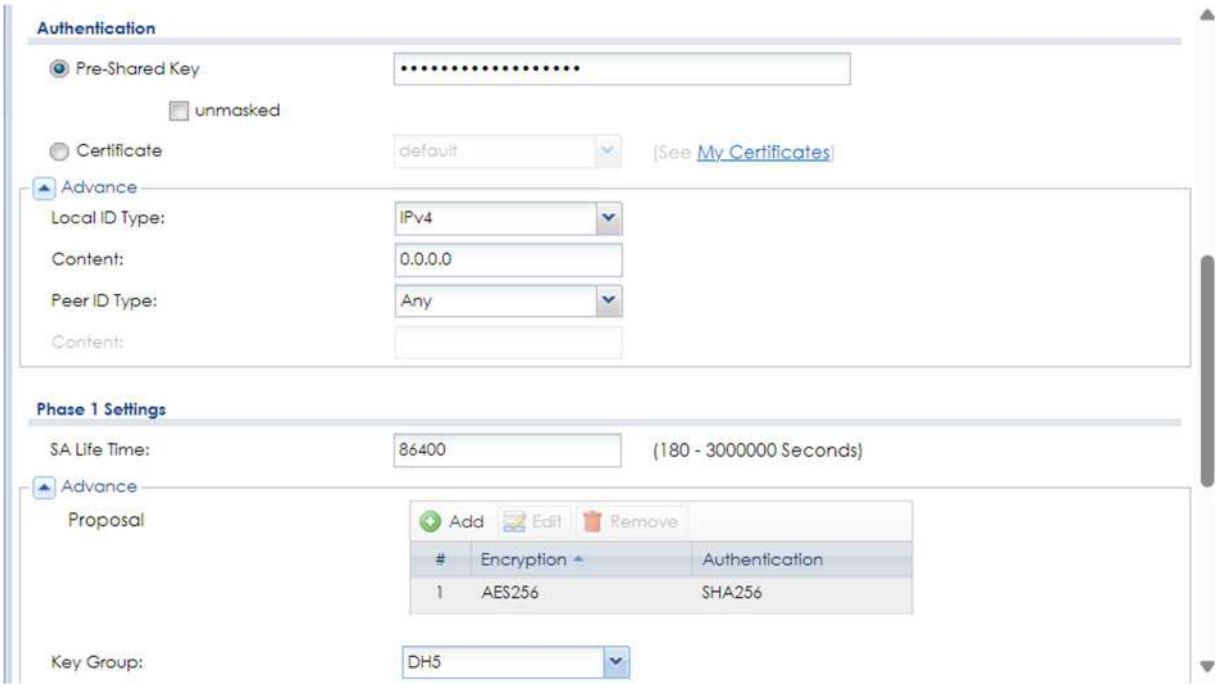
Sur ZyXEL :

Phase 1 :

On crée une nouvelle VPN Gateway pour spécifier avec qui communiquer ?

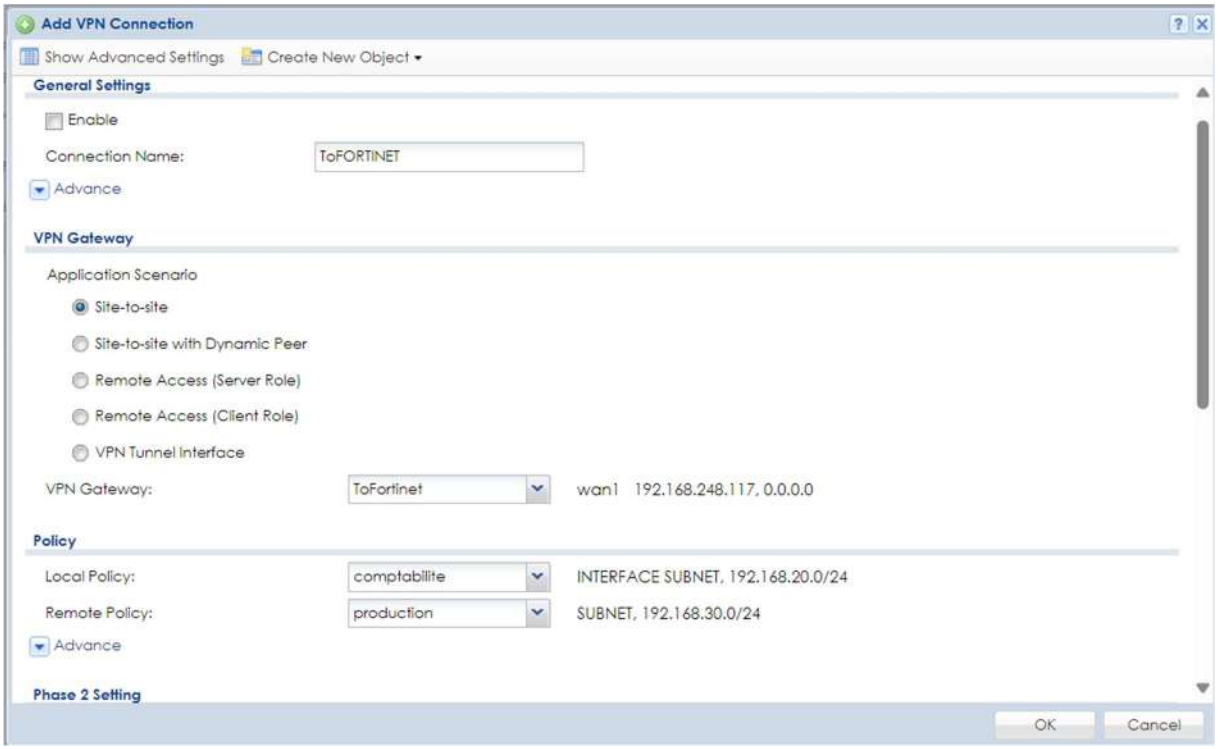


On signale la machine distante avec laquelle il devra communiquer en spécifiant son adresse IP publique.



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.**

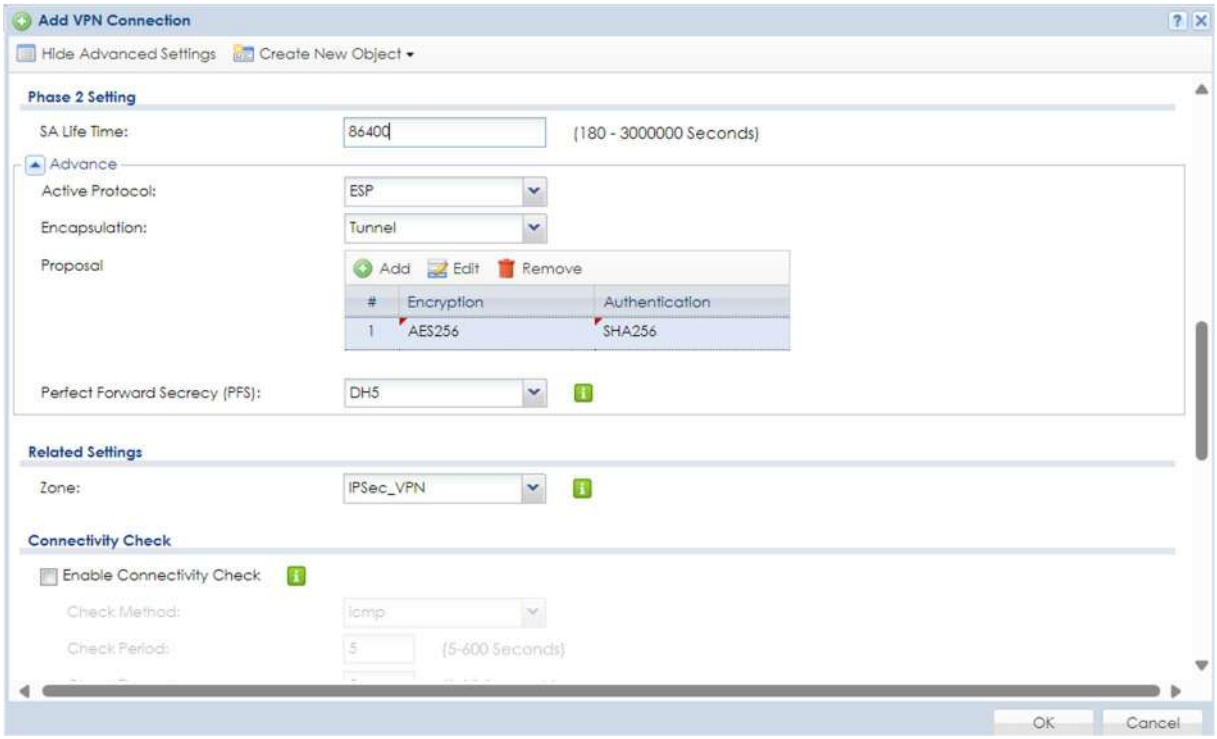
Phase 2 :



Dans « VPN connection » on ajoute un nouveau VPN.

On sélectionne « ToFortinet » le VPN Gateway crée à la phase 1. On crée deux objets adresses IPv4 que l'on nomme ici comptabilité et production mais qui correspondent au réseau local du ZyXEL et le réseau distant sur lequel on veut se connecter en VPN.

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.



On laisse les autres paramètres par défaut.

Règles de pare-feu :

Dans Firewall Policy, deux règles de pare-feu sont présentes par défaut pour autoriser le trafic **entrant** et **sortant** des Tunnel VPN avec le protocole IPsec vers le(s) réseaux internes.

La configuration du VPN sur le routeur ZyXEL est terminée.

Route Statique :

Les routeurs ZyXEL comprennent à la création du VPN qu'elle doivent router en interne les paquets qui voudraient rejoindre un réseau distant via le tunnel VPN créé, tant qu'il n'existe pas un réseau identique sur le réseau local. Il n'y a donc pas besoin de configurer des routes statiques.