

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

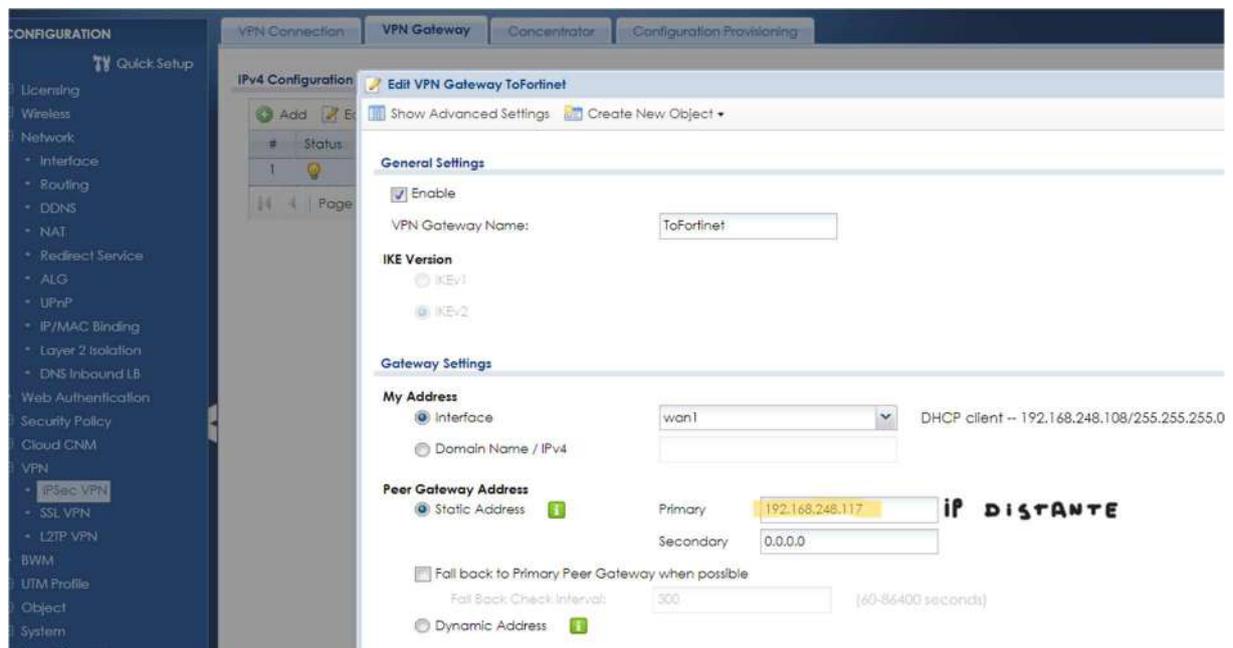
Réseau local routeur FORTINET à connecter en VPN : 192.168.30.0/24

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.

Authentication

Pre-Shared Key unmasked

Certificate default (See [My Certificates](#))

Advance

Local ID Type: IPv4

Content: 0.0.0.0

Peer ID Type: Any

Content:

Phase 1 Settings

SA Life Time: 86400 (180 - 3000000 Seconds)

Advance

Proposal

#	Encryption	Authentication
1	AES256	SHA256

Key Group: DH5

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 :

Add VPN Connection

Show Advanced Settings Create New Object

General Settings

Enable

Connection Name: ToFORTINET

Advance

VPN Gateway

Application Scenario

Site-to-site

Site-to-site with Dynamic Peer

Remote Access (Server Role)

Remote Access (Client Role)

VPN Tunnel interface

VPN Gateway: ToFortinet wan1 192.168.248.117, 0.0.0.0

Policy

Local Policy: comptabilite INTERFACE SUBNET, 192.168.20.0/24

Remote Policy: production SUBNET, 192.168.30.0/24

Advance

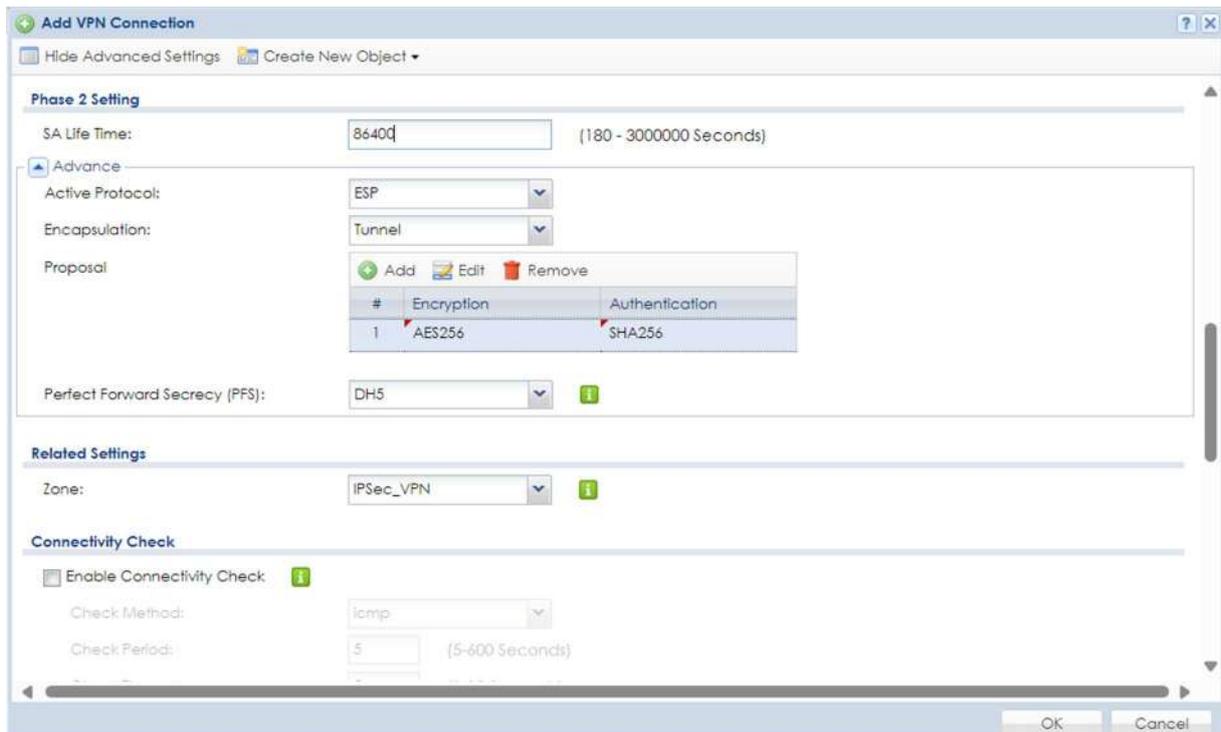
Phase 2 Setting

OK Cancel

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.

Id	Name	Source	Destination	Service	Action	Log
4	DMZ_to_WAN	DMZ	WAN	any	any	
5	IPSec_VPN_Outgoing	IPSec_VPN	any (Excludin...	any	any	
6	SSL_VPN_Outgoing	SSL_VPN	any (Excludin...	any	any	
7	TUNNEL_Outgoing	TUNNEL	any (Excludin...	any	any	
8	LAN1_to_Device	LAN1	ZyWALL	any	any	
9	LAN2_to_Device	LAN2	ZyWALL	any	any	
10	DMZ_to_Device	DMZ	ZyWALL	any	any	
11	WAN_to_Device	WAN	ZyWALL	any	any	
12	IPSec_VPN_to_Device	IPSec_VPN	ZyWALL	any	any	
13	SSL_VPN_to_Device	SSL_VPN	ZyWALL	any	any	

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.