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.

🕂 Network	>	Authentication	
System	(1) >	Method	Pre-shared Key
Policy & Objects	>	Pre-shared Key	•••••
Security Profiles	>	IKE	
	~	Version	1 2
Overlay Controller VPN		Mode	Aggressive Main (ID protection)
IPsec Tunnels	☆		Aggressive Main (15 protection)
IPsec Wizard		Phase 1 Proposal O Add	
IPsec Tunnel Template		Encryption AES256	Authentication SHA256
SSL-VPN Portals			
SSL-VPN Settings		Diffie-Hellman Groups	
VPN Location Map		Key Lifetime (seconds)	86400
User & Authentication	>	LocaLID	
WiFi & Switch Controller	>	Locario	L
Log & Report	>	XAUTH	
		Туре	Disabled

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**) <u>doivent être</u> <u>identiques sur les deux routeurs.</u>

Security Fabric	>	Phase 2 Selectors								
+ Network	>	Name Local		l Address		Remote Address				
🌣 System 🧉	>	toZyXEL 192.168.30.0		0/255.255	255.255.255.0 19		92.168.20.0/255.255.255.		55.0	
Policy & Objects	>									
Security Profiles	>	New Phase 2						_	0 0	
	~	Name		toZyXE	L					
Overlay Controller VPN		Comments		Comme	ents				SOUS-RE	SERUX
IPsec Tunnels	IPsec Tunnels 📅		Local Address		Subnet 👻 192.168.3		68.30.0/255	3.30.0/255.255.2 À R		ER
IPsec Wizard		Remote Address		Subnet	Subnet		5.255.2			
IPsec Tunnel Template		Advanced						-		
SSL-VPN Portals		Phase 2 Proposal	O Add							
SSL-VPN Settings		Encryption	AES256	•	Authenticat	tion	SHA256	•		
VPN Location Map		Enable Replay Det	ection 🔽							
User & Authentication	>	Enable Perfect For	ecy (PFS) 🔽							
♥WiFi & Switch Controller	>									
Log & Report	>	Diffie-Hellman Gr	oup	21 (15 (20 19 14 🗹 5		18 🗌 17 2 🔲 1	16		

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.

User & Authentication	>	XAUTH			🖋 Edi		
• WIFI& Switch Controller	í.	Type : D	isabled				
Log & Report	,	Dhara 2 Salastara					
		Phase 2 Se	electors		•		
		Name	Local Address	Remote Address	Add		
		toZyXEL	192.168.30.0/255.255.255.0	192.168.20.0/255.255.255.0			
		TOZYXEL	172.108.30.0/255.255.255.0	192.108.20.0/255.255.255.0	8		
ttps://192.168.1.99/ng/vpn/map					OK		

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 <u>entrant</u> et <u>sortant</u> du Tunnel VPN vers le réseau local dans lequel il effectue des transferts avec le sous-réseau distant.

2 Dashboard	> New Policy	New Policy				
🔆 Security Fabric	>					
+ Network	> Name 🕚	ToZyXE	Loutgoing			
System 👩	> Incoming I	nterface 😅 inte	rnal	•		
Policy & Objects	 Outgoing I 	nterface 🙆 toZ	yXEL	•		
Firewall Policy	Source		+			
Addresses	Destinatio	n	+			
Internet Service Database	Schedule	Co alwa	iys	•		
Services	Service		+			
Schedules	Action	V ACC	CEPT Ø DENY			
Virtual IPs	Inspection	Mode Flow-base	d Proxy-based			
IP Pools						

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.

	New Address	
XELot nterna	Name Color Type	ReseauSourceVPN Change Subnet
oZyXE	IP/Netmask Interface	192.168.30.0 255.255.255.0 ✓ internal ✓
lways	Comments	Write a comment Ø/255
ased	New Address	OK Cancel
XELou nterna oZyXI Iways	Name Color Type IP/Netmask Interface Static route configuration (Comments	ReseauDestinationVPN Change Subnet 192.168.20.0 255.255.255.0 192.toZyXEL Write a comment
ased		OK Cancel

On laisse les options suivantes par défaut :

7.	
+ Network >	Firewall / Network Options
System (1) >	NAT O
💄 Policy & Objects 🛛 🗸 🗸	IP Pool Configuration Use Outgoing Interface Address Use Dynamic IP Pool
Firewall Policy	Preserve Source Port 🔿
Addresses	Protocol Options default
Internet Service Database	Security Profiles
Schedules Virtual IPs IP Pools Protocol Options	AntiVirus Web Filter DNS Filter Application Control
Traffic Shapers Traffic Shaping Policy Traffic Shaping Profile	File Filter SSL Inspection
▲ Security Profiles >	Logging Options
□ VPN > ▲ User & Authentication > ♥ WiFi & Switch Controller > WiFi & Seport >	Log Allowed Traffic Security Events All Sessions Comments Write a comment Ø/1023
LOB & Report	Enable this policy 🔘

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.

2 Dashboard	>	Edit Static Route				
X Security Fabric	>	Automatic gateway retrieval 🚯 🕥				
Network		Destination	Subnet Named Address In	ternet Serv	ice	
Interfaces			ToZyxel_remote	•		
DNS		Interface	toZyXEL	•		
Packet Capture		Administrative Distance ()	10	1		
SD-WAN Zones		Comments	VPN: ToZyxel (Created by VPN wizard)	N 36/255		
Performance SLA		Status	Enabled ODisabled			
Static Routes	습	Advanced Options				
FortiExtender						
System	• •				OK	Cancel
Ballas C Objects	2					