## Mise en place d'un VPN Nomade Client-Serveur FORTINET

## 1/ Configuration sur le routeur FORTINET

Pour accéder à l'interface web du routeur une fois connecté au routeur :

Ouvrir une console et taper « ipconfig »

Q cmd						
Rechercher Travail Applications	Documents	Web	Paramè	•	NOVAPTIS SARL	A
Meilleur résultat						
Invite de commandes Système				TAC:		
Rechercher dans l'entreprise et sur le			Invite	de co	ommandes <sup>ème</sup>	
Q cmd - Afficher les résultats	, –					

Invite de commandes	
Carte Ethernet Ethernet 3 :	
Statut du média	Média déconnecté
Carte Ethernet Ethernet :	
Suffixe DNS propre à la connexion : Adresse IPv6 de liaison locale Adresse IPv4 Masque de sous-réseau Passerelle par défaut	fe80::8ce6:40ad:b245:bad1%21 192.168.1.111 255.255.255.0 192.168.1.99

L'IP du routeur apparait, on peut la copier dans un navigateur, et se connecter avec ses identifiants d'adminstrateur.

Non sécurisé | https://192.168.1.99/login?redir=%2Fng

Username	
Deenuard	

Nous devons tout d'abord créer un utilisateur par défaut qui aura un identifiant et un mot de passe pour pouvoir se connecter à distance au VPN. Cette connexion permet de l'autoriser au niveau du pare-feu à accéder au réseau local, dans notre cas nous voudrons rendre accessible le sous-réseau QUALITE depuis le Tunnel VPN QualiteVPN.

2 Dashboard	>	Users/Groups Creation Wizard		
🔆 Security Fabric	>	1 User Type 2 Login Credentials 3 3 Contact Info 4 Extra Info		
🕂 Network	>			
🌣 System 🧉	) >	Local User Remote RADIUS User		
Policy & Objects	>	Remote TACACS+ Licer		
Security Profiles	>	Remote LDAP User		
U VPN	>	FSSO		
User & Authentication	~	FortiNAC User		
User Definition	☆			
User Groups				
Guest Management				

On crée un nouvel utilisateur local et ses identifiants.

FortiGate 60F	FortiGate-60F		
🔁 Dashboard	>	Users/Grou	ps Creation Wizard
🔆 Security Fabric	>	🕢 User Tv	npe 2 Login Credentials 3 3 Contact Info 2 4 Extra Info
+ Network	>	Username	user//PN
System	1 >	Password	
Policy & Objects	>	1 dosword	
Security Profiles	>		
L VPN	>		
🔒 User & Authenticati	on 🗸		
User Definition	☆		

On active le compte, puis on viendra créer un groupe associé au VPN plus tard pour ajouter cet utilisateur à ce groupe.

FortiGate 60F	FortiGate-60F	
🔁 Dashboard	>	Users/Groups Creation Wizard
🔆 Security Fabric	>	User Type 🔪 🖉 Login Credentials 🔪 🖉 Contact Info 🔪 🐴 Extra Info
+ Network	>	
System	1 >	User Group
Policy & Objects	>	
Security Profiles	>	
□ VPN	>	
🛔 User & Authenticati	on 🗸	

Dans User Groups on crée le nouveau group pour les utilisateurs ayant des accès VPN.

2 Dashboard	>	New User G	roup		
🔆 Security Fabric	>	Name	groupVPN		Select Entries
+ Network	>	Type	Firewall		Q Search
System	0 >	type	Fortinet Single Sign-On (FSSO)		LISER (2)
Policy & Objects	>		RADIUS Single Sign-On (RSSO)	ngle Sign-On (RSSO)	Local (2)
Security Profiles	>		Guest		🛔 guest
	>	Members	🛔 userVPN		🛔 userVPN
. Licer E. Authentication			+		C PKIUSER
User Definition					🍰 tun0_peer
User Groups	合				
Guest Management					
LDAP Servers					
RADIUS Servers					
Authentication Settings					

Ensuite, nous pouvons créer un nouveau Tunnel VPN en IPsec, en spécifiant bien « remote Access » pour activer le mode VPN Client-Serveur.



Dans un deuxième temps, on définit une Pre-Shared Key, et on rend le VPN accessible aux utilisateurs du « groupVPN » précédemment créé.

FortiGate 60F	ortiGate-60	F				
Dashboard	>	VPN Creation Wizard				
℅ Security Fabric	>	VPN Setup	uthentication 3 3 Polic	cy & Routing > @ Client C		view Settings
+ Network	>	Incoming Interface	🔳 wan1	•	,	
System	<b>()</b> >	Authentication method	Pre-shared Key Signat	ure		Dialup - Forticilent (Wi
Policy & Objects	>	Pre-shared key	·····	() ()		$\sim$
Security Profiles	>	User Group	groupVPN	•		
P VPN	~	· · · · · · · · · · · · · · · · · · ·				10:33
Overlay Controller VI	PN					This FortiGate
IPsec Tunnels					l	
IPsec Wizard	☆					10
IPsec Tunnel Template	e			< Back	Next >	Cancel
SSL-VPN Portals						
CCL V/DNI Cottings						

On spécifie quelle sous-réseau (ou quelle machines...) sera accessible par la connexion VPN, et on configure la plage d'adressage IP de l'utilisateur distant. Pour limiter le nombre de connexion distante, on met comme plage 192.168.40.250 à 192.168.40.254.

🔁 Dashboard	>	VPN Creation Wizard				
Security Fabric	>	🔮 VPN Setup 🔪 🖉 Auth	entication > 3 Policy & Routi	ng 🔪 👍 Client Optie	ons 🔰 🗿 Review	v Settings
System	0 >	Local interface	<ul> <li>QUALITE</li> <li>+</li> </ul>	×	Dial	lup - FortiClient (W
Policy & Objects Security Profiles	>	Local Address	QUALITE address	×		11.
	~	Client Address Range Subnet Mask	192.168.40.250-192.168. 255.255.255.255	40.254		A REAL PROPERTY OF
Overlay Controller VPN IPsec Tunnels		DNS Server Enable IPv4 Split Tuppel	Use System DNS Specify	e		This FortiGate
IPsec Wizard	습	Allow Endpoint Registration	0			
IPsec Tunnel Template			1			
SSL-VPN Portals SSL-VPN Settings				< Back	Next >	Cancel

🚯 Dashboard	>	VPN Creation Wizar	d				
<ul> <li>Security Fabric</li> <li>Network</li> <li>System</li> <li>Policy &amp; Objects</li> <li>Security Profiles</li> <li>VPN</li> <li>Overlay Controller VPN IPsec Tunnels</li> </ul>	> 3 > > >	VPN Setup Save Password Auto Connect Always Up (Keep Al	Authenticat	ion 🔪 🗹 Policy & Ro	uting 🔪 🕢 Client Optio	ons <b>&gt; 6</b> Re	view Settings Dialup - FortiClient
IPsec Wizard	습				< Back	Next >	Cancel
IPsec Tunnel Template							

Une fois le VPN configuré, on vérifie que la règle de pare-feu associée permettant les entrée et sortie de données dans le tunnel VPN a bien été créé automatiquement :

~		LYXET 1					
	B	n1 1					
	🔁 💩 QUALITE → 💁 ToZyxel 🚯						
	🗄 🙆 QUALITE → 🔚 wan1 📵	).					
	☐ QualiteVPN →  QUALI	ITE 1					
	vpn_QualiteVPN_remote_0	QualiteVPN_range	QUALITE address	lo always	D ALL	✓ ACCEPT	
	🗈 🍙 ToZyxel →🚳 PRODUCT	ION 1					
	🖸 🙆 ToZyxel → 🚳 QUALITE	1					
	> ☆	Image: a problem of the production of the production of the production of the production of the product of t	Image: Constraint of the second	Image: Constraint of the constrai	Image: Constraint of the system of the	<ul> <li>PRODUCTION → I wan1  wan1 wanne wan1  wan1 wanne wan1 wanne wanne wanne wan1  wan1 wanne wan1 wan1 wanne wan1 wanne wan1  wan1 wanne w</li></ul>	

## 2/ Installation et utilisation du logiciel FortiClient

Installation de FortClient : <u>https://www.fortinet.com/support/product-downloads#vpn</u>

Désormais pour se connecter à distance en tant que client à notre sous-réseau derrière notre routeur FORTINET, celui-ci propose une application FortiClient permettant d'entrer l'adresse et les informations nécessaire à la connexion au VPN.



On met l'IP publique de notre routeur distant, ainsi que la même Pre-Shared Key configurée lors de la création du Tunnel VPN, et on demande les identifiants de connexion avant l'ouverture.

On peut trouver l'IP publique dans Network>Interface>WAN sur l'interface Web du routeur FORTINET :



## Dans le logiciel FortiClient :

VPN	VPN SSL VPN IPsec XML	
Nom de la connexion	QualiteVPN	
Description		
Passerelle distante	192.168.248.117	×
	+Ajout d'une passerelle distante	
Méthode d'authentification	Clé partagée	~
Authentification (XAuth)	O Demander à l'ouverture de la O Sauvegarder I connexion d'authentifica	les informations O ation Désactives
VPN SSL de basculemen	[Aucun]	~
Single Sign On Settings	Activer l'authentification unique (SSO) pour le tunn	nel VPN





La connexion au Tunnel VPN depuis un poste client distant est réussie !