Configuration VPN SSL sur un routeur FORTINET

Une autre technologie très utilisée par les VPN est la technologie SSL (Secure Socket Layer), qui, comme IPsec est utilisée pour sécuriser les communications sur internet, mais celle-ci fonctionne différemment.

Le VPN SSL est basé sur le protocole SSL/TLS, principalement utilisé par accéder à des ressources web à distance de manière sécurisé.

Comparé à IPsec le protocole SSL/TLS de crypte pas la couche réseau, il a donc une couche de sécurité en moins mais reste sécurisé pour acheminer les paquets entre le client et le serveur VPN.

Sous-réseau Production à rendre accessible en VPN : 192.168.30.0/24

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

Q cmd							
Rechercher Travail Applications	Documents	Web	Paramè	•	NOVAPTIS SARL	A	
Meilleur résultat							
Système				HC.			
Rechercher dans l'entreprise et sur le			Invite	de co _{Syst}	ommandes ^{ème}		
Q cmd - Afficher les résultats	>						

Ouvrir une console et taper « ipconfig »

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

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

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

Username	
Deserverd	

1/ Définir un compte utilisateur local

Le VPN-SSL en tant que VPN nomade demande une connexion de l'utilisateur distant. De ce fait la première chose à faire et de définir un compte local dans le routeur que l'on configurera plus tard lors de la configuration VPN pour l'autoriser à effectuer une connexion distante au VPN.



On crée un nouvel utilisateur local et ses identifiants.

FortiGate 60F	FortiGate-60F		
🚯 Dashboard	>	Users/Grou	ps Creation Wizard
🔆 Security Fabric	>	🗸 User Tv	ne 2 Login Credentials 3 3 Contact Info 2 4 Extra Info
+ Network	>	Username	userVPN
System	(1) >	Password	
Policy & Objects	>	1 doortor d	
Security Profiles	>		
□ VPN	>		
🔒 User & Authenticat	ion 🗸 🗸		
User Definition	☆		

On active le compte, puis on crée un groupe associé au VPN pour ajouter cet utilisateur à ce groupe.



2 Dashboard	>	New User G	roup		
🔆 Security Fabric	>	Name	group\/PN		Select Entries
+ Network	>	Tune	Groupell		O Search
System	•	Type	Fortinet Single Sign-On (ESSO)		
Policy & Objects	>		RADIUS Single Sign-On (RSSO)		Local (2)
Security Profiles	>		Guest		a guest
D VPN	>	Members	LuserVPN	×	🛔 userVPN
Liser & Authentication	~		+		PKIUSER
User Definition					tun0_peer
User Groups	☆				
Guest Management					
LDAP Servers					
RADIUS Servers					
Authentication Settings					

2/ Configuration Portail VPN-SSL et paramètres

Dans VPN : SSL-VPN Portals :

On crée une autorisation pour rendre accessible en VPN-SSL le sous-réseau souhaité (Production : 192.168.30.0/24) par le tunnel SSLVPN_TUNNEL proposé par défaut par le routeur FORTINET.

On active le split tunneling si on souhaite rediriger uniquement le trafic nécessaire vers le VPN, et utiliser notre connexion par défaut pour naviguer sur internet par exemple.

FortiGate 60F Forti	iGate-60F			
Dashboard	>	Edit SSL-VPN Portal		
 Security Fabric Network System Policy & Objects 	> > 1 >	Name production-access	onnection at a Time 🕥	
Security Profiles	>	C Tunnel Mode		
VPN Overlay Controller VPN IPsec Tunnels IPsec Wizard IPsec Tunnel Template	v	Enable Split Tunneling 🚯 🜑 Routing Address Source IP Pools	 PRODUCTION address SSLVPN_TUNNEL_ADDR1 + 	×
SSL-VPN Portals	☆	Tunnel Mode Client Options		

On peut activer le mode Web afin de pouvoir accéder facilement à une interface web pour se connecter au VPN en entrant dans un navigateur l'adresse IP publique du routeur distant. Cette étape n'est pas obligatoire puisque l'on peut s'y connecter directement depuis l'application FortiClient.

Policy & Objects	>						
Security Profiles	>	C Enable Web Mod	e				
	~	Portal Message		SSL-VPN Por	tal		
Overlay Controller VPN		Theme		Neutrino		•	
IPsec Tunnels		Show Session Inform	ation 🔘				
IPsec Wizard		Show Connection La	uncher 🔘				
IPsec Tunnel Template		Show Login History	•				
SSL-VPN Portals	☆	User Bookmarks	0				
SSL-VPN Settings		Predefined Bookman	ks				
VPN Location Map		+ Create New	🖋 Edit	🗊 Delete	Search		Q
User & Authentication	>	Name 🌻	Type 🌲	Locat	tion ≑	Description #	:
WiFi & Switch Controller	>						
Log & Report	>			No result	5		

Ensuite, on configure les paramètres du VPN-SSL dans « SSL-VPN Settings », en sélectionnant l'interface WAN (s'il y a plusieurs port WAN, utiliser celui raccordé vers Internet) comme interface d'écoute avec le port souhaité, pour permettre à l'utilisateur distant de se connecter au VPN depuis ce port.

FortiGate 60F FortiC	Gate-60F			
🖚 Dashboard	>	SSL-VPN Settings		
🔆 Security Fabric	>			
+ Network	>	Connection Settings ()		
System	1 >	Enable SSL-VPN	0	
Policy & Objects	>	Listen on Interface(s)	🔳 wan1	×
Security Profiles	>		+	
	~	Listen on Port	4466	
Overlay Controller VPN			Web mode access	s will be listening at
IPsec Tunnels			https://192.168.2	248.117:4466
IPsec Wizard		Padiract HTTP to SSL VPN		

Un avertissement devrait apparaitre pour signaler une règle de pare-feu manquante pour autoriser un utilisateur extérieur à accéder au tunnel VPN :

▲ No SSL-VPN policies using these settings	s exist. Click here to create a new s	SSL-VPN policy
Connection Settings ()		
Enable SSL-VPN		
Listen on Interface(s)	🖮 wan1 🔸	×
Listen on Port	4466	

Appliquez les paramètres modifiés puis cliquez sur le texte bleu comme indiqué, pour créer la règle pour autoriser le trafic du réseau (Production) à sortir par le tunnel VPN-SSL pour que l'utilisateur distant (userVPN) puisse y accéder.



Enfin on autorise l'utilisateur à se connecter à distance si les identifiants de userVPN sont corrects.

Security Profiles	>			
	~	Tunnel Mode Client Settings		
Overlay Controller VPN IPsec Tunnels		Address Range Automatically a	ssign addresses Specify custom IP ranges ill receive IPs in the range of 10.212.134.200 -	
IPsec Wizard IPsec Tunnel Template		DNS Server Same as client s	vstem DNS Specify	
SSL-VPN Portals		Specify WINS Servers	ysen bro speeny	
SSL-VPN Settings	습			
VPN Location Map		Authentication/Portal Mapping 0		
User & Authentication WiFi & Switch Controller	>	+ Create New 🖋 Edit 🗎 Delete	Send SSL-VPN Configuration	
Log & Report	>	Users/Groups 🖨	Portal ≑	
		🛔 userVPN	production-access	
		All Other Users/Groups	production-access	

Sur un réseau distant on peut accéder à l'interface de connexion au VPN-SSL soit par l'interface web depuis un navigateur, avec l'adresse IP publique du réseau, et le bon



Soit par l'application FortiClient, en créant une nouvelle connexion VPN-SSL et en indiquant l'IP publique distante, le port, et le certificat client pour identifier la machine physique responsable de la demande de connexion :

FortiClient VPN	* * 0 6
Passez à la version complète pour accéder à des fonctionnalités supplémentaires et bénéficier d'une assistance t	echnique.
Nom du VPN	_
Nom d'utilisateur	_
Mot de passe	
Certificat Client a6ebbf66-f21e-48fb-bbc3-228e86807a ¥	۲
Sauvegarder le mot de passe	

Il ne reste plus qu'à mettre les bons identifiants et la connexion en VPN est réussie !

VPN connecté



Nom du VPN	ProductionVPN		
Adresse IP	10.212.134.200		
Nom d'utilisateur	userVPN		
Durée	00:00:03		
Octets reçus	0 Ko		
Octets envoyés	3.02 Ko		

Déconnecter