

Documentation : Mise en oeuvre – FortiGate F60

Contexte

Dans le cadre du projet Vénus, le pare-feu FortiGate F60 a été utilisé pour assurer la segmentation logique du réseau, l’adressage des différents sous-réseaux et la centralisation de certains services d’infrastructure. L’objectif était d’isoler les différents usages du réseau tout en conservant une administration cohérente et sécurisée de l’ensemble de l’infrastructure.

Configuration des interfaces réseau

La configuration du FortiGate repose sur la création d’interfaces de type VLAN 802.1Q, chacune rattachée à une interface physique dédiée du pare-feu. Chaque réseau dispose ainsi de sa propre passerelle sur le FortiGate, ce qui permet de séparer clairement les flux entre les différents segments de l’infrastructure.

Les interfaces configurées sont les suivantes :

- VLAN 10 – Administration : interface rattachée à internal1, adresse 192.168.10.254/24.
- VLAN 20 – Direction : interface rattachée à internal2, adresse 192.168.20.254/24.
- VLAN 30 – Wi-Fi : interface rattachée à internal3, adresse 192.168.30.254/24.
- VLAN 99 – Management : interface rattachée à internal4, adresse 192.168.99.254/24.

Cette organisation permet d’identifier clairement le rôle de chaque réseau et d’attribuer une passerelle dédiée à chaque VLAN. Les accès d’administration ont également été activés de manière contrôlée sur ces interfaces, notamment pour les tests réseau et l’administration sécurisée de l’équipement.

	Name ↕	Type ↕	Members ↕	IP/Netmask ↕	Administrative Access ↕	DHCP Clients ↕	DHCP Ranges ↕	Ref. ↕
					HTTPS Security Fabric Connection			
	 internal1	 Physical Interface		0.0.0.0/0.0.0.0				1
	 Administration	 VLAN		192.168.10.254/255.255.255.0	PING HTTPS SNMP HTTP		Relay: 192.168.99.201	4
	 internal2	 Physical Interface		0.0.0.0/0.0.0.0				1
	 DIRECTION	 VLAN		192.168.20.254/255.255.255.0	PING HTTPS SNMP HTTP		Relay: 192.168.99.201	3
	 internal3	 Physical Interface		0.0.0.0/0.0.0.0				1
	 Wi-Fi	 VLAN		192.168.30.254/255.255.255.0	PING HTTPS SNMP HTTP		Relay: 192.168.99.201	3
	 internal4	 Physical Interface		0.0.0.0/0.0.0.0				1
	 Management	 VLAN		192.168.99.254/255.255.255.0	PING HTTPS SSH SNMP HTTP		Relay: 192.168.99.201	6

Figure 1 : Vue d'ensemble des interfaces configurées sur le FortiGate.

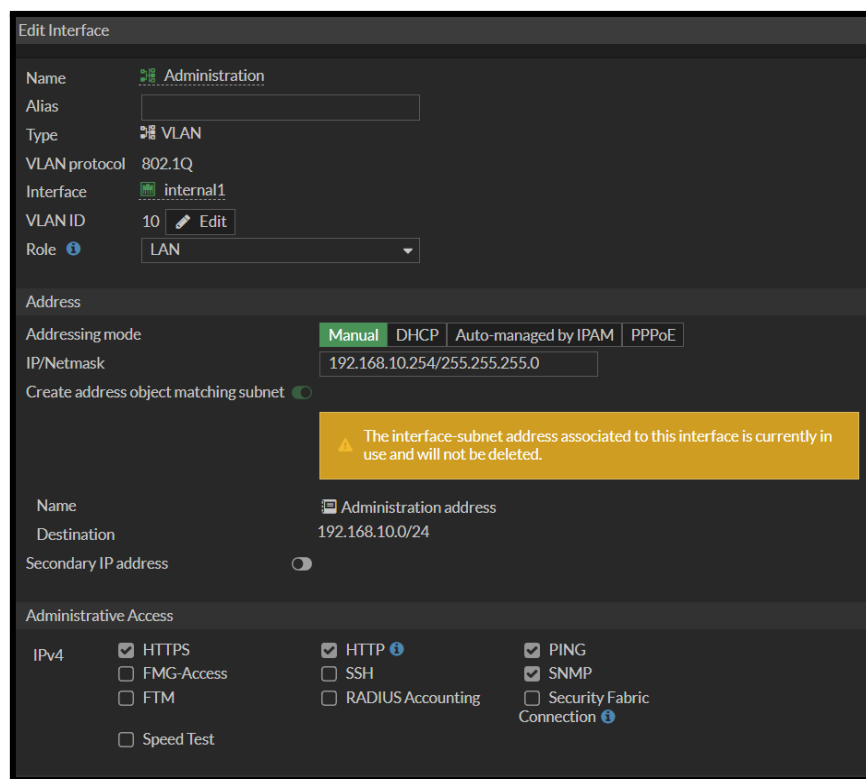


Figure 2 : Configuration de l'interface VLAN 10 – Administration (configuration similaire sur chaque interface avec leur IP respective)

Mise en place du DHCP Relay

L'adressage IP dynamique de l'infrastructure est assuré par un serveur Windows situé dans le VLAN 99, à l'adresse 192.168.99.201. Les postes présents dans les VLAN 10, 20 et 30 ne pouvant pas recevoir directement les diffusions DHCP depuis un autre réseau, il a été nécessaire d'activer la fonction DHCP Relay sur les interfaces concernées. Le DHCP Relay permet au FortiGate d'intercepter les requêtes DHCP émises par les clients des différents VLAN et de les transmettre au serveur DHCP centralisé. Cette configuration rend possible l'attribution automatique d'adresses IP aux machines des VLAN Administration, Direction et Wi-Fi tout en conservant une architecture réseau segmentée.

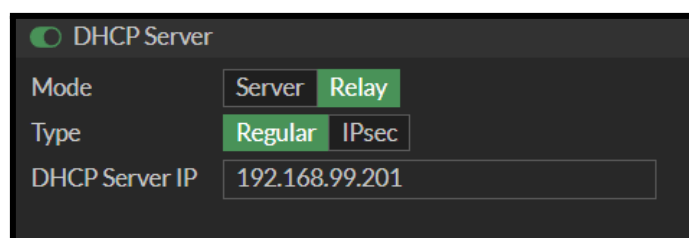


Figure 3 : Activation du mode DHCP Relay sur chaque interface

Politique de filtrage et routage (Firewall Policies)

Le FortiGate agissant selon le principe du "Deny All" par défaut, aucune communication n'est possible entre les VLANs ni vers l'extérieur sans la création explicite d'une politique de pare-feu (Firewall Policy).

L'objectif de sécurité était double :

1. Permettre aux clients de chaque VLAN d'accéder aux services d'annuaire et d'authentification centralisés sur l'Active Directory.
2. Autoriser l'accès à Internet de manière contrôlée pour chaque sous-réseau.

1. Interconnexion avec les services d'infrastructure (Active Directory)

Afin que les machines des VLANs clients (ex : Administration, Direction, Wi-Fi) puissent se connecter au domaine, une règle de filtrage spécifique a été mise en place pour chaque interface entrante vers le VLAN 99 (Management).

Le service "Windows AD", qui regroupe les ports indispensables à l'authentification (LDAP, Kerberos, DNS, SMB), a été défini comme le seul trafic autorisé pour ces liaisons inter-VLAN.

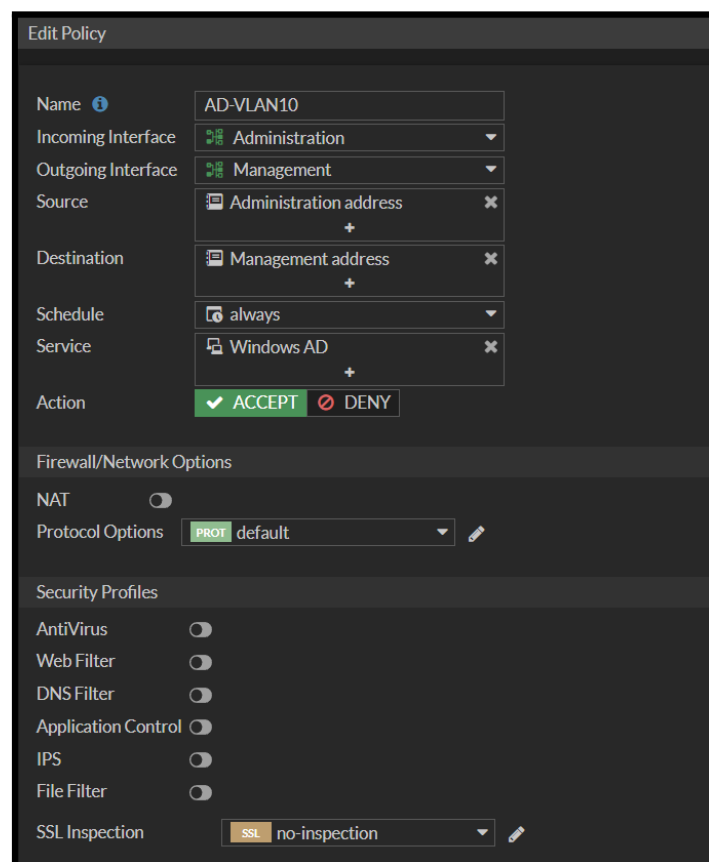


Figure 4 : Détail de la règle "AD-VLAN10"

2. Accès à Internet et Translation d'Adresse (NAT)

Pour que le trafic local puisse être routé sur Internet, des règles autorisant tous les services ("ALL") depuis chaque VLAN client vers l'interface WAN1 ont été créées. Contrairement aux flux inter-VLAN, la fonction de translation d'adresse réseau (NAT) a été obligatoirement activée sur ces règles. Le FortiGate masque ainsi les adresses IP privées des clients en utilisant l'adresse IP publique/externe de son interface de sortie (Use Outgoing Interface Address).

Edit Policy

Name ⓘ

Internet-VLAN10

Incoming Interface

Administration

Outgoing Interface

wan1

Source

Administration address

+

Destination

all

+

Schedule

always

Service

ALL

+

Action

✓ ACCEPT

✗ DENY

Firewall/Network Options

NAT

●

IP Pool Configuration

Use Outgoing Interface Address

Use Dynamic IP Pool

Preserve Source Port

○

Protocol Options

PROT

 default

✎

Security Profiles

AntiVirus

○

Web Filter

○

DNS Filter

○

Application Control

○

IPS

○

File Filter

○

SSL Inspection

SSL

 no-inspection

✎

OK

Cancel

Figure 5 : Détail de la règle "Internet-VLAN10"

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes	Type
Administration → Management 1										
AD-VLAN10	Administration address	Management address	always	Windows AD	ACCEPT	Disabled	SSL no-inspection	UTM	399.29 kB	Standard
Administration → wan1 1										
Internet-VLAN10	Administration address	all	always	ALL	ACCEPT	Enabled	SSL no-inspection	UTM	0 B	Standard
DIRECTION → Management 1										
AD-VLAN20	DIRECTION address	Management address	always	Windows AD	ACCEPT	Disabled	SSL no-inspection	UTM	0 B	Standard
DIRECTION → wan1 1										
Internet-VLAN20	DIRECTION address	all	always	ALL	ACCEPT	Enabled	SSL no-inspection	UTM	0 B	Standard
Management → wan1 1										
Internet-VLAN99	Management address	all	always	ALL	ACCEPT	Enabled	SSL no-inspection	UTM	36.42 MB	Standard
Venus-VPN → Management 1										
vpn_Venus-VPN_remote_0	Venus-VPN_range	Management address	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	194.06 MB	Standard
VPN-VLAN10 → Administration 1										
vpn_VPN-VLAN10_remote_0	VPN-VLAN10_range	Administration address	always	ALL	ACCEPT	Enabled	SSL no-inspection	UTM	0 B	Standard
Wi-Fi → Management 1										
AD-VLAN30	Wi-Fi address	Management address	always	Windows AD	ACCEPT	Disabled	SSL no-inspection	UTM	0 B	Standard
Wi-Fi → wan1 1										
Internet-VLAN30	Wi-Fi address	all	always	ALL	ACCEPT	Enabled	SSL no-inspection	UTM	0 B	Standard
Implicit 1										

Figure 6 : Vue de la table de filtrage complète synthétisant l'ensemble des flux autorisés sur l'infrastructure Vénus.

Pour que ce trafic puisse effectivement quitter l'infrastructure, une route statique par défaut (0.0.0.0/0) a été configurée sur le FortiGate, pointant vers la passerelle du Fournisseur d'Accès Internet via l'interface WAN1.

Accès distant sécurisé (VPN IPsec – VLAN 10)

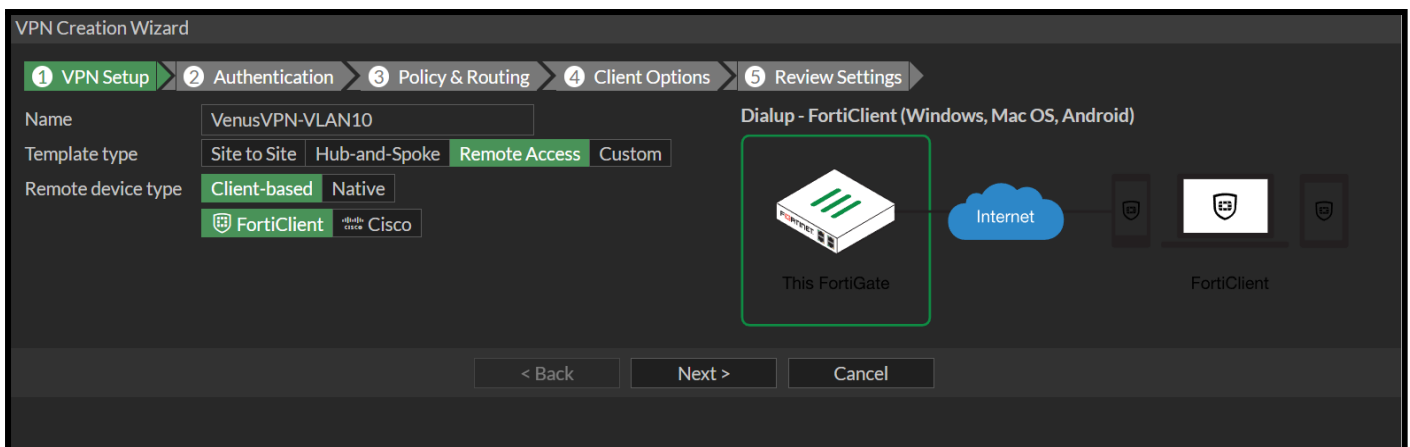
Afin de permettre aux employés du service d'accéder au réseau de l'entreprise depuis l'extérieur en situation de télétravail, un tunnel VPN IPsec de type Dial-up a été mis en place sur le FortiGate. Ce service permet de rejoindre le réseau du VLAN 10 de manière chiffrée, tout en contrôlant les utilisateurs autorisés à se connecter.

1. Création du groupe d'utilisateurs

Un groupe d'utilisateurs dédié au VPN a d'abord été créé afin de restreindre l'accès aux seuls employés autorisés. Ce groupe sert de filtre d'authentification lors de l'ouverture du tunnel.

2. Configuration du tunnel IPsec

Le tunnel a ensuite été configuré en mode Dial-up avec les paramètres suivants : interface entrante wan1, méthode d'authentification par Pre-Shared Key, et attribution du groupe d'utilisateurs autorisé.



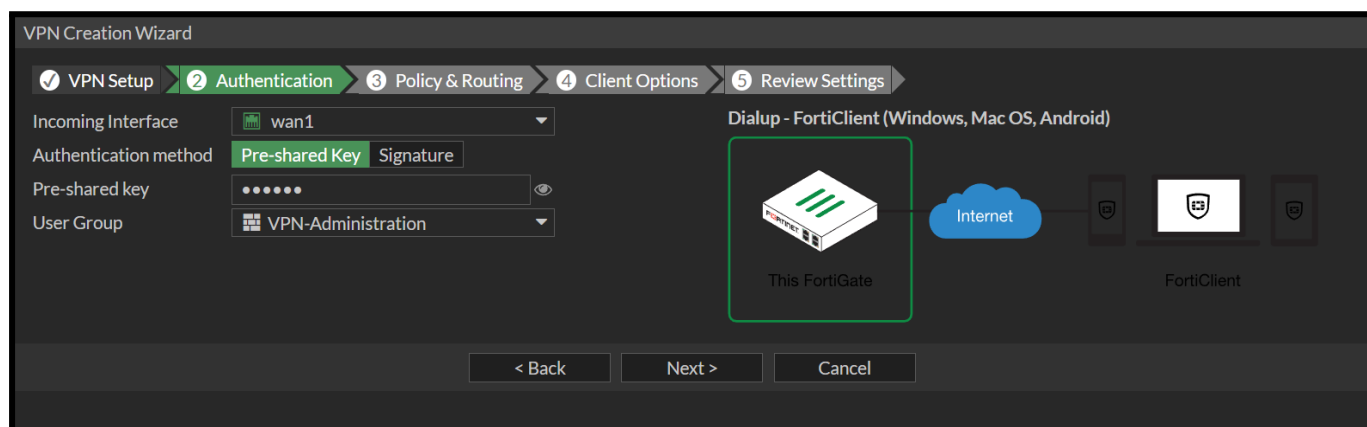


Figure 7 : Configuration du Tunnel IpSec et paramètres d'authentification

3. Paramètres d'attribution réseau

Le tunnel a été associé à l'interface locale du réseau Administration / VLAN 10, avec une plage d'adresses IP dédiée aux clients VPN 192.168.110.1 à 192.168.110.10. Le serveur DNS utilisé par les clients VPN a été défini sur 192.168.99.201 (*adresse Windows Server*) afin de permettre la résolution des noms internes.

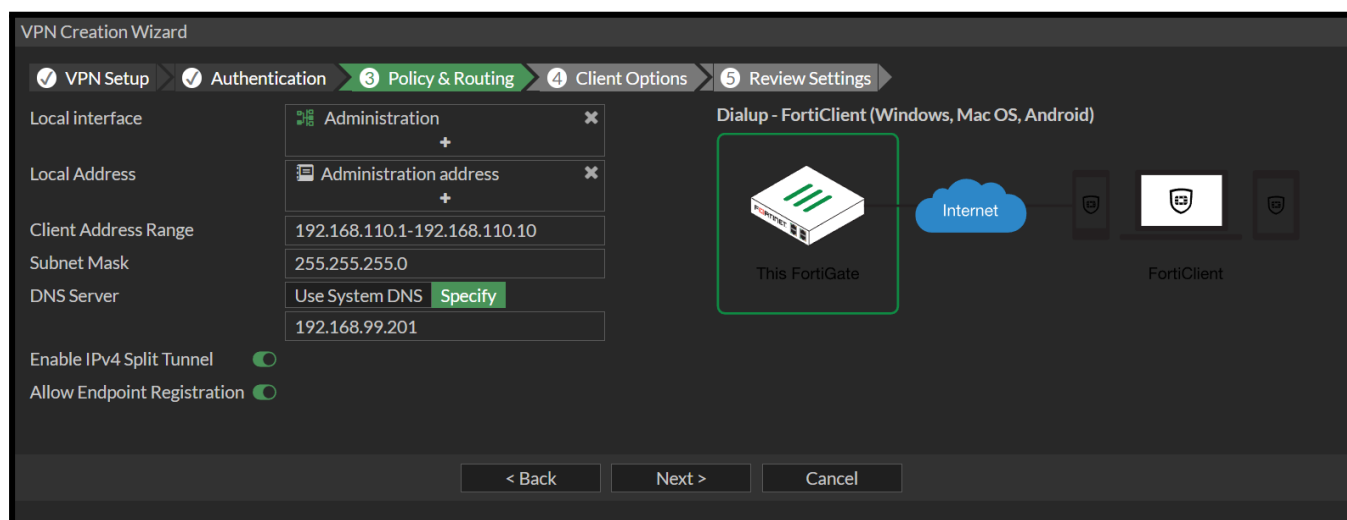


Figure 8 : Configuration du routage et des politiques du VPN

4. Passage en mode Custom

Une fois le tunnel créé, il a été modifié en mode Custom pour ajouter des paramètres avancés. Un Peer ID *vpn-vlan10* a été configuré afin d'éviter les conflits entre plusieurs VPN sur la même interface wan1. Le groupe Diffie-Hellman a également été réglé sur 20 pour renforcer la sécurité des échanges de clés en phase 1 et phase 2.

Authentication

Method

Pre-shared Key

Pre-shared Key

.....

IKE

Version

12

Mode

AggressiveMain (ID protection)

Peer Options

Accept Types

Specific peer ID

Peer ID

vpn-vlan10

Figure 9 : Attribution du “PeerID” (ID du VPN)

Phase 1 Proposal

+

Add

✓

↺

Encryption

AES128

Authentication

SHA256

✕

Encryption

AES256

Authentication

SHA256

✕

Encryption

AES128

Authentication

SHA1

✕

Encryption

AES256

Authentication

SHA1

✕

Diffie-Hellman Group

32

31

30

29

28

27

21

20

19

18

17

16

15

14

5

2

1

Key Lifetime (seconds)

86400

Local ID

Edit Phase 2

Name: VPN-VLAN10

Comments: VPN: VPN-VLAN10 (Created by VPN wizard)

Local Address: Subnet 0.0.0.0/0.0.0.0

Remote Address: Subnet 0.0.0.0/0.0.0.0

☐ Advanced...

Phase 2 Proposal + Add

Encryption	AES128	Authentication	SHA1	☒
Encryption	AES256	Authentication	SHA1	☒
Encryption	AES128	Authentication	SHA256	☒
Encryption	AES256	Authentication	SHA256	☒
Encryption	AES128GCM			☒
Encryption	AES256GCM			☒
Encryption	CHACHA20POLY1305			☒

Enable Replay Detection ☒

Enable Perfect Forward Secrecy (PFS) ☒

Diffie-Hellman Group

☐ 32	☐ 31	☐ 30	☐ 29	☐ 28	☐ 27
☐ 21	☒ 20	☐ 19	☐ 18	☐ 17	☐ 16
☐ 15	☐ 14	☐ 5	☐ 2	☐ 1	

Local Port: All ☒

Remote Port: All ☒

Protocol: All ☒

Autokey Keep Alive: ☐

Key Lifetime: Seconds

Figure 10 : Configuration du DH Group sur la phase 1 et 2

Afin que le service DNS fonctionne via VPN la configuration suivante est nécessaire:

Depuis le CLI du Fortigate:

```
Venus-FortiGate-60F#config vpn ipsec phase1-interface
Venus-FortiGate-60F (phase1-interface)# edit "VENUS-VPN"
Venus-FortiGate-60F (VENUS-VPN)# set domain "venus.local"
Venus-FortiGate-60F (VENUS-VPN)# next
```

Sur la configuration du VPN IpSec renseigner l'IP du serveur DNS

Network

IP Version: IPv4

Incoming Interface: wan1

Use system DNS in mode config: ☐

Assign IP From: ☒ Range

IPv4 mode config

Client Address Range: 192.168.150.1-192.168.150.10

Subnet Mask: 255.255.255.0

DNS Server: 192.168.99.201

Enable IPv4 Split Tunnel: ☒

Accessible Networks: Management address

Dead Peer Detection: Disable On Idle **On Demand**

DPD retry count: 3

DPD retry interval: 20 s

Forward Error Correction: Egress ☐ Ingress ☐

Advanced...

5. Déploiement et Configuration du Poste Client (FortiClient)

La validation finale du service d'accès distant s'effectue sur le poste de l'utilisateur (employé en télétravail). L'agent FortiClient (préalablement installé) doit être configuré pour correspondre exactement aux paramètres cryptographiques (Phases 1 et 2) définis sur le pare-feu.

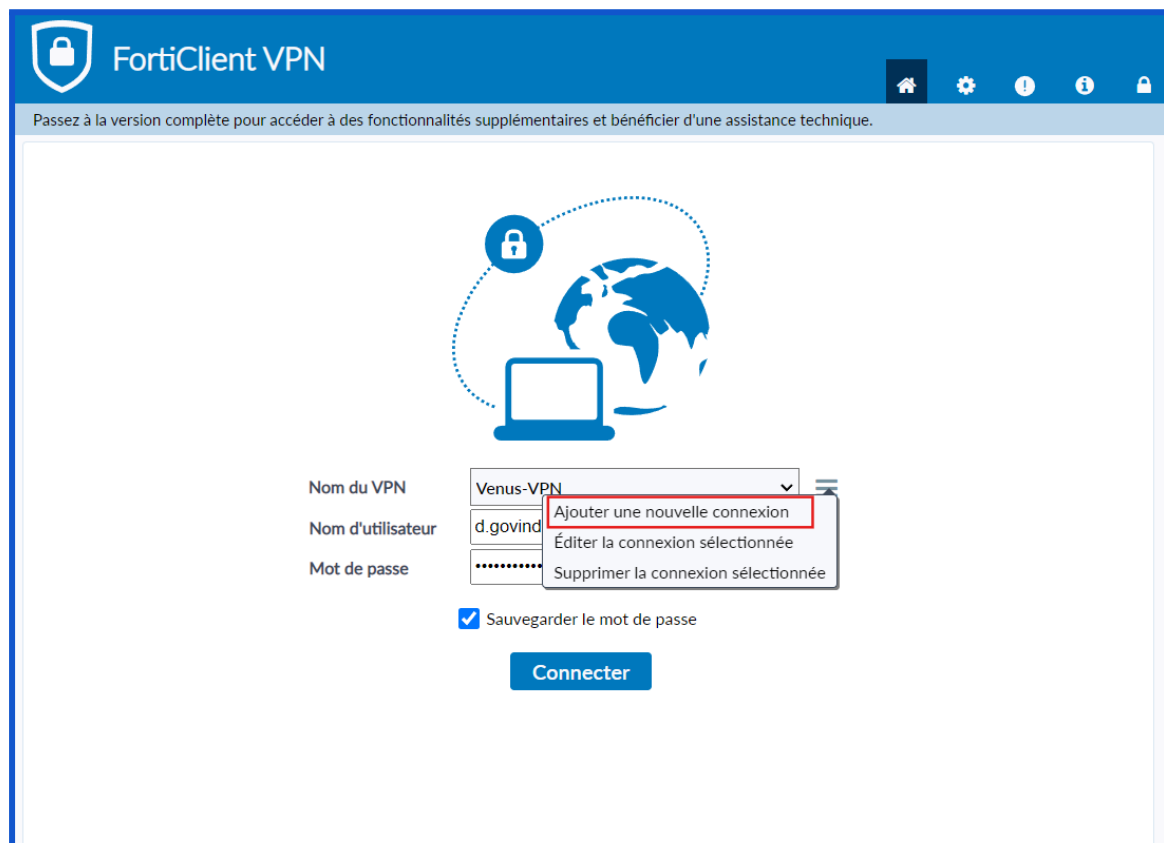


Figure 11 : Ajout d'une nouvelle connexion

Méthodologie de configuration de la nouvelle connexion :

- Type de connexion : Sélection du protocole VPN IPsec.
- Nom et Description : "VPN-VLAN10" / "VPN-Administration Vénus".
- Passerelle distante : Renseignement de l'adresse IP publique de l'interface WAN1 du FortiGate (172.16.63.80).
- Méthodologie d'authentification : Sélection de "Clé partagée" (Pre-Shared Key) et saisie de la clé.

FortiClient VPN

Passez à la version complète pour accéder à des fonctionnalités supplémentaires et bénéficier d'une assistance technique.

Editer la connexion VPN

VPN: VPN SSL | VPN IPsec | XML

Nom de la connexion: VPN-VLAN10

Description: VPN-Administration Vénus

Passerelle distante: 172.16.63.80 [X]

+ Ajout d'une passerelle distante

Méthode d'authentification: Clé partagée

Authentification (XAuth): ☒ Demander à l'ouverture de la connexion ☐ Sauvegarder les informations d'authentification ☐ Désactiver

VPN SSL de basculement: [Aucun]

Single Sign On Settings: ☐ Activer l'authentification unique (SSO) pour le tunnel VPN

+ Paramètres avancés

Annuler Sauvegarder

Figure 11 : Configuration d'une nouvelle connexion VPN

Paramètres cryptographiques avancés :

Pour que la négociation IKE réussisse, les paramètres avancés du client doivent refléter le mode "Custom" du FortiGate :

- Phase 1 : Forçage du Groupe DH sur 20 (au lieu de la valeur par défaut) et renseignement de l'ID Local (vpn-vlan10). Cet ID Local correspond au "Peer ID" attendu par le pare-feu pour aiguiller la connexion vers le bon tunnel.
- Phase 2 : Forçage du Groupe DH sur 20 pour la Perfect Forward Secrecy (PFS).

The image shows the FortiClient VPN configuration window. The top bar is blue with the FortiClient VPN logo and a navigation bar. Below the bar, a message says: "Passez à la version complète pour accéder à des fonctionnalités supplémentaires et bénéficier d'une assistance technique." The main area is divided into sections: "Paramètres avancés", "Paramètres VPN", and "Phase 1".

Paramètres VPN

- IKE: ☒ Version 1 ☐ Version 2
- Mode: ☐ Principal ☒ Aggressif
- Address Assignment: ☒ Config Mode ☐ Configuré manuellement ☐ DHCP dans IPsec

Phase 1

Proposition IKE

Chiffrement	AES128	Authentification	SHA1
Chiffrement	AES256	Authentification	SHA256

Groupe DH

☐ 1	☐ 2	☐ 5	☐ 14	☐ 15
☐ 16	☐ 17	☐ 18	☐ 19	☒ 20
☐ 21				

Durée de vie de la clé: sec

ID Local:

☒ Détection de la perte du pair
☒ NAT Traversal
☐ Activer le LAN local

Phase 2

☐ Activer le LAN local

Proposition IKE

Chiffrement	AES128	Authentification	SHA1
Chiffrement	AES256	Authentification	SHA256

Durée de vie de la clé: ☒ 43200 Secondes
☐ 5120 KOctets

☒ Activer la protection contre le rejeu
☒ Activer la fonction Perfect Forward Secrecy (PFS)

Groupe DH:

Buttons: Annuler, Sauvegarder

Figure 11 : Configuration des Phase 1 et 2

Validation de l'accès :

Une fois la configuration sauvegardée, l'employé lance la connexion en saisissant ses identifiants personnels (ID + Mot de passe) rattachés au groupe d'utilisateurs autorisé sur le FortiGate. Le tunnel s'établit, et le client reçoit son adresse IP dans la plage 192.168.110.1-192.168.110.10

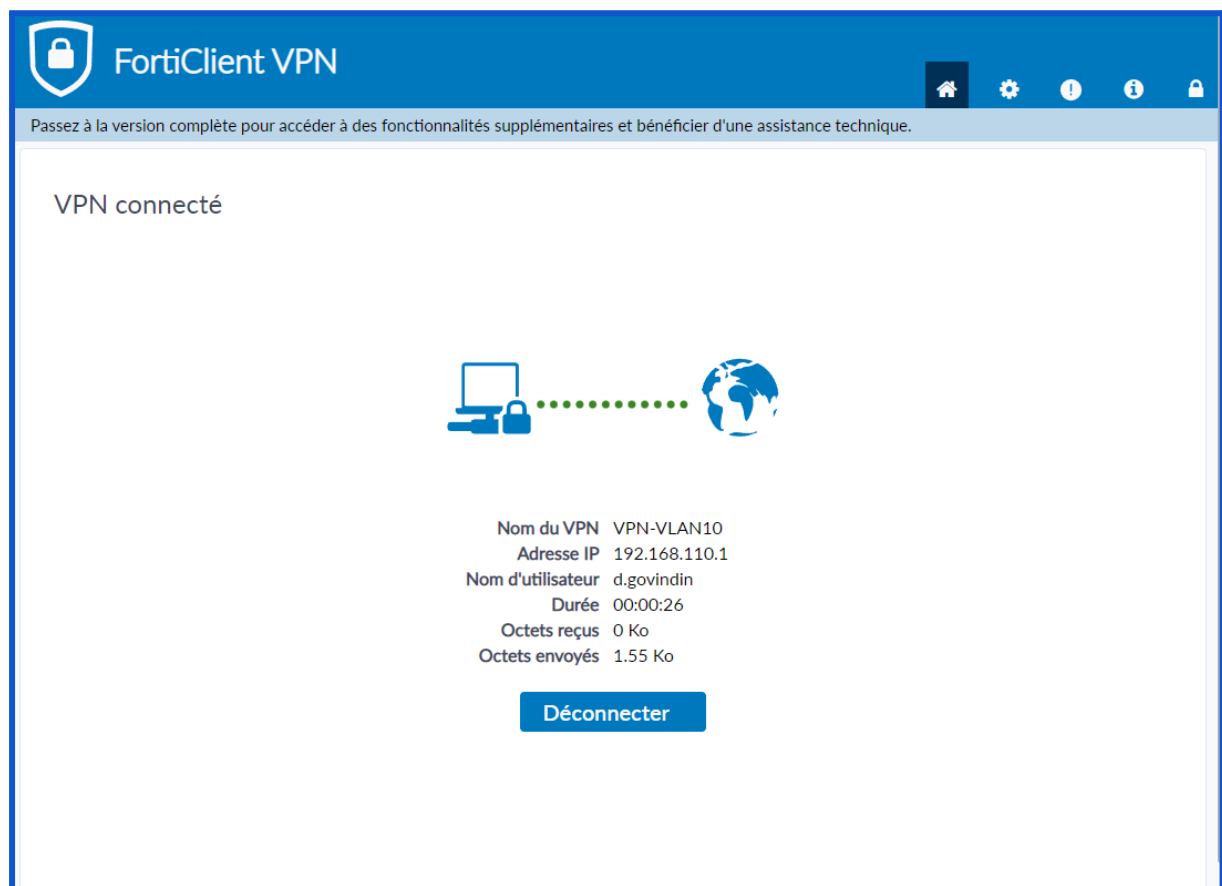


Figure 11 : Connexion au VLAN 10 réussie via VPN