

Rapport - VPN IPsec Client-to-Site avec FortiGate & FortiClient

Informations Générales

Nom de l'étudiant : Imen Ouled Belgacem/Syrine Ben Ali

Classe / Groupe : 4infoCS

Date du TP : 15/05/2025

Sujet du TP : VPN Remote Access (Client-to-Site) - FortiGate & FortiClient

Objectifs

- Configurer un VPN IPsec Client-to-Site avec authentification locale.
 - Permettre l'accès sécurisé à un réseau LAN via FortiClient.
 - Assurer la supervision et le logging de la connexion VPN.
-

Architecture Réseau

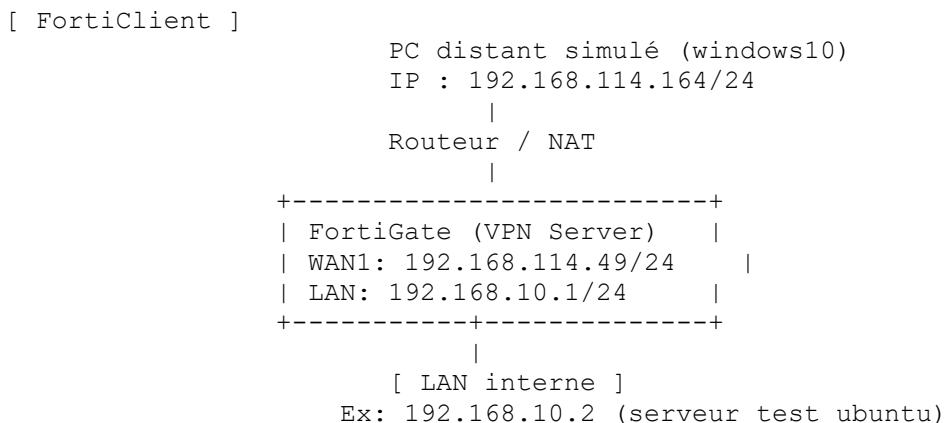


Schéma de l'architecture :

- **FortiClient (poste distant simulé)** : 192.168.114.164/24
- **FortiGate WAN1** : 192.168.114.49/24
- **FortiGate LAN** : 192.168.10.1/24
- **Serveur interne (LAN)** : 192.168.10.2
- **Pool VPN IP** : 10.100.100.0/32

Non sécurisé https://192.168.114.49/ng/interface

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges
LAN (port9)	Physical Interface		192.168.10.1/255.255.255.0	PING HTTPS SSH SNMP HTTP	1	192.168.10.2-192.168.10.254
mgmt	Physical Interface		192.168.114.39/255.255.255.0	PING HTTPS SSH HTTP Security Fabric Connection		
port2	Physical Interface		0.0.0.0/0.0.0			
port3	Physical Interface		0.0.0.0/0.0.0			
port4	Physical Interface		0.0.0.0/0.0.0			
port5	Physical Interface		0.0.0.0/0.0.0			
port6	Physical Interface		0.0.0.0/0.0.0			
port7	Physical Interface		0.0.0.0/0.0.0			
port8	Physical Interface		0.0.0.0/0.0.0			
WAN1 (port1)	Physical Interface		192.168.114.49/255.255.255.0	PING HTTPS SSH SNMP		

Non sécurisé https://192.168.114.49/ng/interface

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients
port2	Physical Interface		0.0.0.0/0.0.0	Security Fabric Connection	
port3	Physical Interface		0.0.0.0/0.0.0		
port4	Physical Interface		0.0.0.0/0.0.0		
port5	Physical Interface		0.0.0.0/0.0.0		
port6	Physical Interface		0.0.0.0/0.0.0		
port7	Physical Interface		0.0.0.0/0.0.0		
port8	Physical Interface		0.0.0.0/0.0.0		
WAN1 (port1)	Physical Interface		192.168.114.49/255.255.255.0	PING HTTPS SSH SNMP	

Non sécurisé https://192.168.114.49/ng/objects

Name	Details	Interface	Type	Ref.
FABRIC_DEVICE	0.0.0.0/0		Address	0
FIREWALL_AUTH_PORTAL_ADDRESS	0.0.0.0/0		Address	0
IPsec_VPN_range	10.100.100.1 - 10.100.100.50		Address	1
LOCAL	192.168.10.0/24	LAN (port9)	Address	3
SSLVPN_TUNNEL_ADDR1	10.212.134.200 - 10.212.134.210		Address	2
all	0.0.0.0/0		Address	2
none	0.0.0.0/32		Address	0
gmail.com	gmail.com		Address	1
login.microsoft.com	login.microsoft.com		Address	1
login.microsoftonline.com	login.microsoftonline.com		Address	1
login.windows.net	login.windows.net		Address	1
wildcard.dropbox.com	*.dropbox.com		Address	0
wildcard.google.com	*.google.com		Address	1

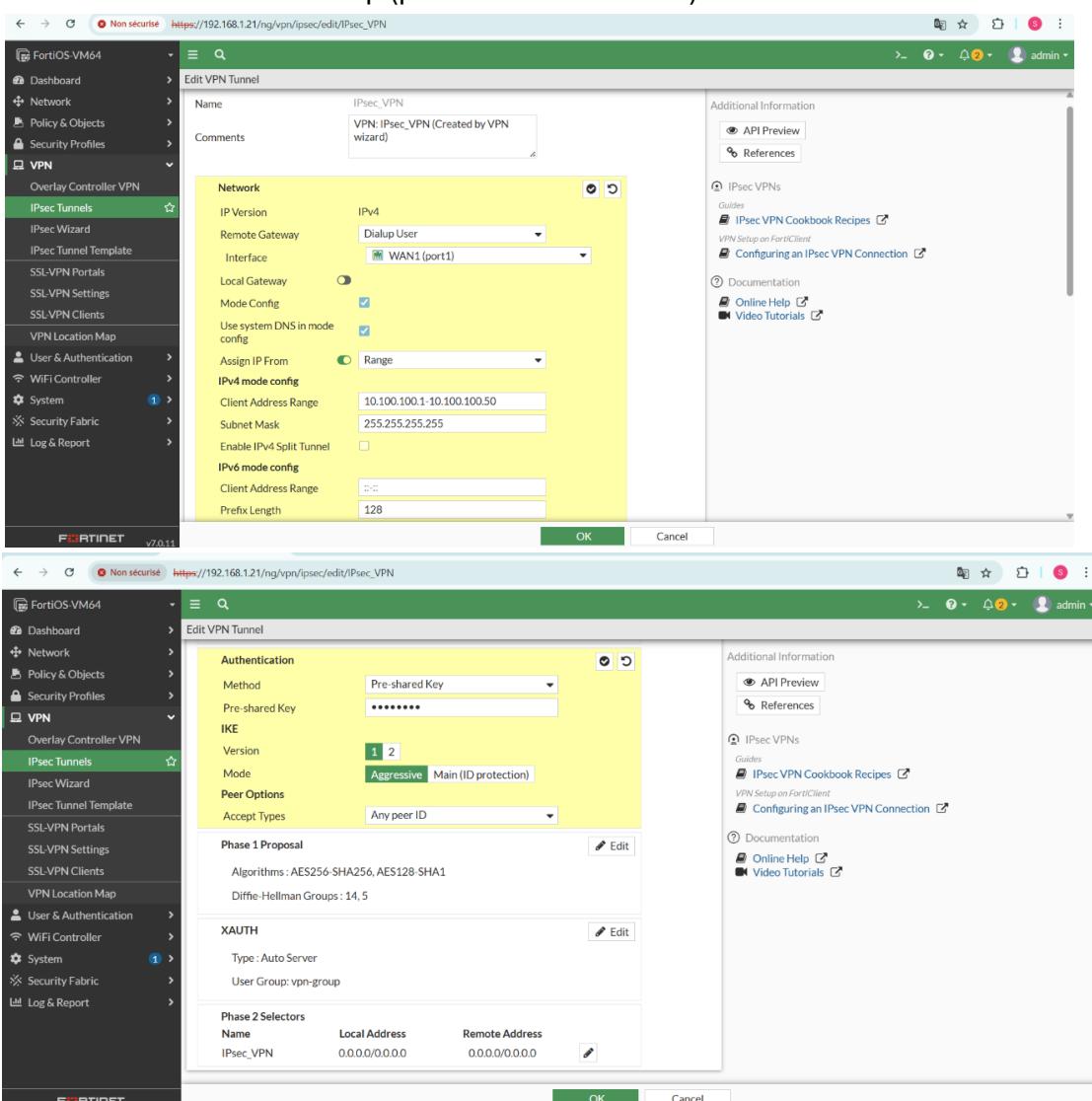
Paramètres VPN IPsec

Phase 1 :

- Mode : Aggressive
- PSK : VPN2025!
- Encryption : AES256
- Hash : SHA256
- DH Group : 14
- PFS : Activé

Phase 2 :

- Encryption : AES256
- Hash : SHA256
- PFS : Oui
- Local LAN : 192.168.10.0/24
- Remote Client : Dial-Up (pool 10.100.100.0/32)



The screenshot displays two stacked configuration windows from the FortiManager interface, version v7.0.11, for setting up an IPsec VPN tunnel named "IPsec_VPN".

Top Window (Phase 1):

- Name:** IPsec_VPN
- Comments:** VPN-IPsec_VPN (Created by VPN wizard)
- Network:**
 - IP Version:** IPv4
 - Remote Gateway:** Dialup User
 - Interface:** WAN1 (port1)
 - Local Gateway:** (checkbox)
 - Mode Config:** (checkbox) checked
 - Use system DNS in mode config:** (checkbox) checked
 - Assign IP From:** Range (radio button selected)
 - IPv4 mode config:**
 - Client Address Range:** 10.100.100.1-10.100.100.50
 - Subnet Mask:** 255.255.255.255
 - Enable IPv4 Split Tunnel:** (checkbox)
 - IPv6 mode config:**
 - Client Address Range:** :: (radio button selected)
 - Prefix Length:** 128
- Additional Information:**
 - API Preview
 - References

Bottom Window (Phase 2):

- Authentication:**
 - Method:** Pre-shared Key
 - Pre-shared Key:** *****
- IKE:**
 - Version:** 1 2
 - Mode:** Aggressive | Main (ID protection)
- Peer Options:**
 - Accept Types:** Any peer ID
- Phase 1 Proposal:**
 - Algorithms: AES256-SHA256, AES128-SHA1
 - Diffie-Hellman Groups: 14, 5
- XAUTH:**
 - Type: Auto Server
 - User Group: vpn-group
- Phase 2 Selectors:**

Name	Local Address	Remote Address
IPsec_VPN	0.0.0/0.0.0.0	0.0.0/0.0.0.0

Edit VPN Tunnel

Authentication

Authentication Method : Pre-shared Key
IKE Version : 1, Mode : Aggressive

Phase 1 Proposal

- Add
- Encryption AES256 Authentication SHA256
- Encryption AES128 Authentication SHA1

Diffie-Hellman Group: 15, 14, 5, 2, 1

Key Lifetime (seconds): 86400

XAUTH

Type : Auto Server
User Group: vpn-group

Phase 2 Selectors

Name	Local Address	Remote Address
IPsec_VPN	0.0.0.0/0.0.0	0.0.0.0/0.0.0

OK Cancel

Edit VPN Tunnel

Comments: wizard

Local Address: Subnet 0.0.0.0/0.0.0

Remote Address: Subnet 0.0.0.0/0.0.0

Advanced...

Phase 2 Proposal

- Add
- Encryption AES256 Authentication SHA256
- Encryption AES128 Authentication SHA1

Enable Replay Detection

Enable Perfect Forward Secrecy (PFS)

Diffie-Hellman Group: 15, 14, 5, 2, 1

Local Port: All

Remote Port: All

Protocol: All

Autokey Keep Alive

Key Lifetime: Seconds 43200

OK Cancel

Authentification :

- Nom utilisateur : vpnuser
- Mot de passe : vpn1234

User Definition

Name	Type	Two-factor Authentication	Groups	Status
guest	LOCAL	<input type="checkbox"/>	Guest-group	Enabled
vpnuser	LOCAL	<input type="checkbox"/>	vpn-group	Enabled

Create New Edit Clone Delete Search

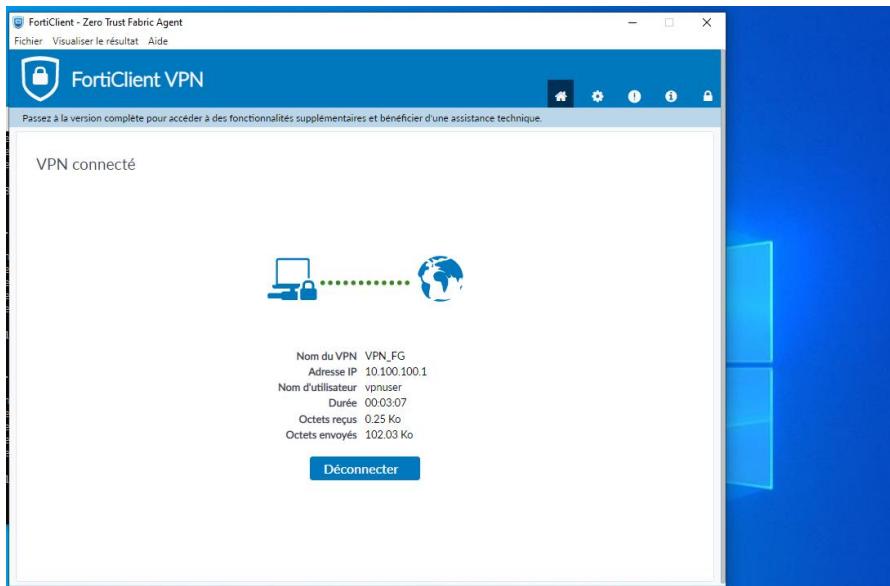
Group Name	Group Type	Members
Guest-group	Firewall	guest
SSO_Guest_Users	Fortinet Single Sign-On (FSSO)	
vpn-group	Firewall	vpnuser

Captures et Preuves de Fonctionnement

1. Connexion réussie avec FortiClient :

Tunnel	Interface Binding	Status	Ref.
IPSec_VPN	WAN1 (port1)	1 dialup connection(s)	3

2. Adresse IP attribuée :



```

Invité de commandes
Paquets : envoyés = 2, reçus = 0, perdus = 2 (perte 100%),
Ctrl+C
^C
C:\Users\sirin>ipconfig

Configuration IP de Windows

Carte Ethernet Ethernet :
  Suffrage DNS propre à la connexion. . . .
  Adresse IPv6 de liaison locale. . . . . : fe80::b228:bfcb:f303:968e%12
  Adresse IPv4. . . . . : 10.100.100.1
  Masque de sous-réseau. . . . . : 255.255.255.255
  Passerelle par défaut. . . . . : 10.100.100.2

Carte Ethernet Ethernet 2 :
  Statut du média. . . . . : Média déconnecté
  Suffrage DNS propre à la connexion. . . .

Carte Ethernet Ethernet0 :
  Suffrage DNS propre à la connexion. . . .
  Adresse IPv6 de liaison locale. . . . . : fe80::60f:aa74:cab4:808a%15
  Adresse IPv4. . . . . : 192.168.114.164
  Masque de sous-réseau. . . . . : 255.255.255.0
  Passerelle par défaut. . . . . : 192.168.114.222

C:\Users\sirin>

```

```

FortiOS-UM64 # execute ping 192.168.10.1
PING 192.168.10.1 (192.168.10.1): 56 data bytes
64 bytes from 192.168.10.1: icmp_seq=0 ttl=255 time=3.1 ms
64 bytes from 192.168.10.1: icmp_seq=1 ttl=255 time=0.1 ms
64 bytes from 192.168.10.1: icmp_seq=2 ttl=255 time=0.0 ms
64 bytes from 192.168.10.1: icmp_seq=3 ttl=255 time=0.1 ms
64 bytes from 192.168.10.1: icmp_seq=4 ttl=255 time=0.1 ms

--- 192.168.10.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.6/3.1 ms

FortiOS-UM64 # execute ping 192.168.114.164
PING 192.168.114.164 (192.168.114.164): 56 data bytes
64 bytes from 192.168.114.164: icmp_seq=0 ttl=128 time=1.6 ms
64 bytes from 192.168.114.164: icmp_seq=1 ttl=128 time=1.4 ms
64 bytes from 192.168.114.164: icmp_seq=2 ttl=128 time=1.3 ms
64 bytes from 192.168.114.164: icmp_seq=3 ttl=128 time=1.1 ms
64 bytes from 192.168.114.164: icmp_seq=4 ttl=128 time=1.1 ms

--- 192.168.114.164 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.1/1.3/1.6 ms

FortiOS-UM64 #

```

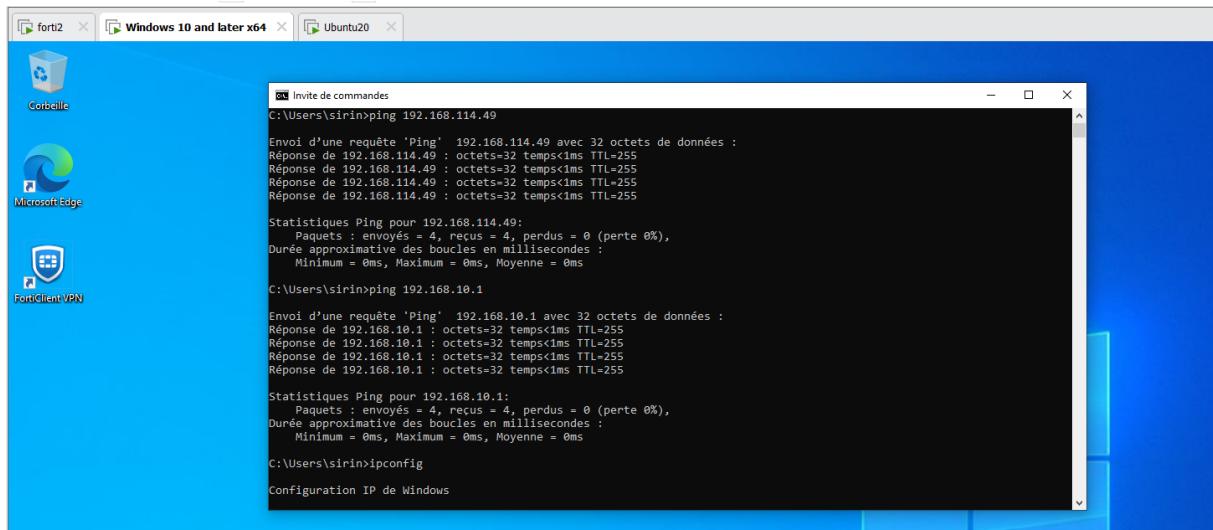
```

FortiOS-VM64 # execute ping 10.100.100.1
PING 10.100.100.1 (10.100.100.1): 56 data bytes
64 bytes from 10.100.100.1: icmp_seq=0 ttl=128 time=1.3 ms
64 bytes from 10.100.100.1: icmp_seq=1 ttl=128 time=0.7 ms
64 bytes from 10.100.100.1: icmp_seq=2 ttl=128 time=1.0 ms
64 bytes from 10.100.100.1: icmp_seq=3 ttl=128 time=1.1 ms
64 bytes from 10.100.100.1: icmp_seq=4 ttl=128 time=0.8 ms

--- 10.100.100.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.7/0.9/1.3 ms

FortiOS-VM64 #

```



```

forti2      Windows 10 and later x64      Ubuntu20

Invite de commandes
C:\Users\sirin>ping 192.168.114.49
Envoi d'une requête 'Ping' 192.168.114.49 avec 32 octets de données :
Réponse de 192.168.114.49 : octets=32 temps<1ms TTL=255

Statistiques Ping pour 192.168.114.49:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\sirin>ping 192.168.10.1
Envoi d'une requête 'Ping' 192.168.10.1 avec 32 octets de données :
Réponse de 192.168.10.1 : octets=32 temps<1ms TTL=255

Statistiques Ping pour 192.168.10.1:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms

C:\Users\sirin>ipconfig
Configuration IP de Windows

```

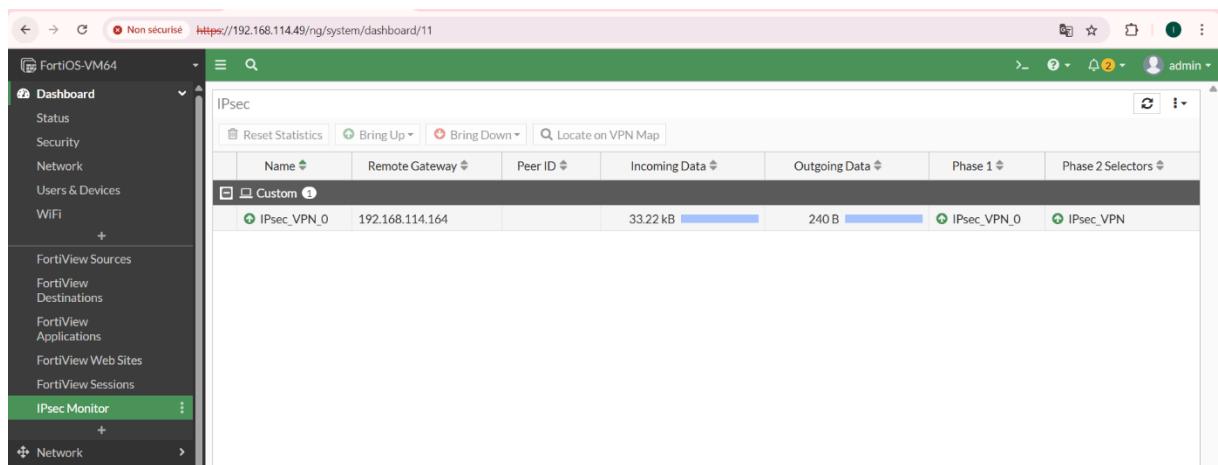
```

strine@ubuntu:~$ ping 192.168.114.49
PING 192.168.114.49 (192.168.114.49) 56(84) bytes of data.
64 bytes from 192.168.114.49: icmp_seq=1 ttl=255 time=0.976 ms
64 bytes from 192.168.114.49: icmp_seq=2 ttl=255 time=0.796 ms
64 bytes from 192.168.114.49: icmp_seq=3 ttl=255 time=0.666 ms
64 bytes from 192.168.114.49: icmp_seq=4 ttl=255 time=0.737 ms
64 bytes from 192.168.114.49: icmp_seq=5 ttl=255 time=1.33 ms
64 bytes from 192.168.114.49: icmp_seq=6 ttl=255 time=0.560 ms
64 bytes from 192.168.114.49: icmp_seq=7 ttl=255 time=0.772 ms
64 bytes from 192.168.114.49: icmp_seq=8 ttl=255 time=0.623 ms
64 bytes from 192.168.114.49: icmp_seq=9 ttl=255 time=0.811 ms
64 bytes from 192.168.114.49: icmp_seq=10 ttl=255 time=0.507 ms
64 bytes from 192.168.114.49: icmp_seq=11 ttl=255 time=0.442 ms
64 bytes from 192.168.114.49: icmp_seq=12 ttl=255 time=0.690 ms
64 bytes from 192.168.114.49: icmp_seq=13 ttl=255 time=0.725 ms
64 bytes from 192.168.114.49: icmp_seq=14 ttl=255 time=0.668 ms
64 bytes from 192.168.114.49: icmp_seq=15 ttl=255 time=0.581 ms
64 bytes from 192.168.114.49: icmp_seq=16 ttl=255 time=0.661 ms
64 bytes from 192.168.114.49: icmp_seq=17 ttl=255 time=0.559 ms
64 bytes from 192.168.114.49: icmp_seq=18 ttl=255 time=0.638 ms
64 bytes from 192.168.114.49: icmp_seq=19 ttl=255 time=0.669 ms
^C
--- 192.168.114.49 ping statistics ---
19 packets transmitted, 19 received, 0% packet loss, time 18273ms
rtt min/avg/max/mdev = 0.442/0.705/1.325/0.187 ms
strine@ubuntu:~$ ping 192.168.10.1
PING 192.168.10.1 (192.168.10.1) 56(84) bytes of data.
64 bytes from 192.168.10.1: icmp_seq=1 ttl=255 time=0.599 ms
64 bytes from 192.168.10.1: icmp_seq=2 ttl=255 time=0.601 ms
64 bytes from 192.168.10.1: icmp_seq=3 ttl=255 time=0.470 ms
64 bytes from 192.168.10.1: icmp_seq=4 ttl=255 time=0.739 ms
64 bytes from 192.168.10.1: icmp_seq=5 ttl=255 time=0.662 ms
64 bytes from 192.168.10.1: icmp_seq=6 ttl=255 time=1.00 ms
^C
--- 192.168.10.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5051ms
rtt min/avg/max/mdev = 0.470/0.679/1.003/0.165 ms
strine@ubuntu:~$ 

```

4. Supervision FortiGate :

- VPN Monitor :



Name	Remote Gateway	Incoming Data	Outgoing Data	Phase 1	Phase 2 Selectors
IPsec_VPN_0	192.168.114.164	33.22 kB	240 B	IPsec_VPN_0	IPsec_VPN

- Log & Report > VPN Events :

Date/Time	Level	Action	Status	Message	VPN Tunnel
Minute ago	[Progress Bar]	tunnel-stats		IPsec tunnel statistics	IPsec_VPN_0
9 minutes ago	[Progress Bar]	tunnel-up		IPsec connection status change	IPsec_VPN_0
9 minutes ago	[Progress Bar]	phase2-up		IPsec phase 2 status change	IPsec_VPN_0
41 minutes ago	[Progress Bar]	tunnel-down		IPsec connection status change	IPsec_VPN_0
41 minutes ago	[Progress Bar]	phase2-down		IPsec phase 2 status change	IPsec_VPN_0
41 minutes ago	[Progress Bar]	tunnel-stats		IPsec tunnel statistics	IPsec_VPN_0
51 minutes ago	[Progress Bar]	tunnel-stats		IPsec tunnel statistics	IPsec_VPN_0
Hour ago	[Progress Bar]	tunnel-stats		IPsec tunnel statistics	IPsec_VPN_0
Hour ago	[Progress Bar]	tunnel-stats		IPsec tunnel statistics	IPsec_VPN_0
Hour ago	[Progress Bar]	tunnel-up		IPsec connection status change	IPsec_VPN_0
Hour ago	[Progress Bar]	phase2-up		IPsec phase 2 status change	IPsec_VPN_0
Hour ago	[Progress Bar]	tunnel-down		IPsec connection status change	IPsec_VPN_0
Hour ago	[Progress Bar]	phase2-down		IPsec phase 2 status change	IPsec_VPN_0
Hour ago	[Progress Bar]	tunnel-stats		IPsec tunnel statistics	IPsec_VPN_0
Hour ago	[Progress Bar]	tunnel-up		IPsec connection status change	IPsec_VPN_0
Hour ago	[Progress Bar]	phase2-up		IPsec phase 2 status change	IPsec_VPN_0

Export / Configuration

Extrait config FortiGate : (partie VPN et policies pertinentes)

Three screenshots of the FortiGate configuration interface showing the VPN creation wizard steps:

- Step 1: VPN Setup**
 - Name: IPsec_VPN
 - Template type: Site to Site - Hub-and-Spoke
 - Remote device type: Client-based
 - Diagram: Shows a FortiGate connected to the Internet and multiple FortiClients.
- Step 2: Authentication**
 - Incoming Interface: WAN1 (port1)
 - Authentication method: Pre-shared key
 - Pre-shared key: VPN2025!
 - User Group: vpn-group
 - Diagram: Shows a FortiGate connected to the Internet and multiple FortiClients.
- Step 3: Policy & Routing**
 - Local interface: LAN (port9)
 - Local Address: LOCAL
 - Client Address Range: 10.100.100.1-10.100.100.50
 - Subnet Mask: 255.255.255.255
 - DNS Server: Use System DNS
 - Enable IPv4 Split Tunnel: Enabled
 - Allow Endpoint Registration: Enabled
 - Diagram: Shows a FortiGate connected to the Internet and multiple FortiClients.

The screenshot shows the FortiOS-VM64 interface with the 'IPsec Wizard' selected in the sidebar. The main window displays the 'VPN Creation Wizard' progress: 'VPN Setup' (checkmark), 'Authentication' (checkmark), 'Policy & Routing' (checkmark), 'Client Options' (checkmark), and 'Review Settings' (checkmark). A green message box at the top states: 'The VPN has been set up'. Below this, the 'Object Summary' section lists the configuration details:

- Split Tunnel Group: IPsec_VPN_split (Edit)
- Phase 1 interface: IPsec_VPN (Edit)
- Phase 2 interface: IPsec_VPN
- Address: IPsec_VPN_range (Edit)
- Remote to local policies: vpn_IPsec_VPN_remote_0 (1)
- Endpoint Registration: Enable

Buttons at the bottom include 'Add Another' and 'Show Tunnel List'.

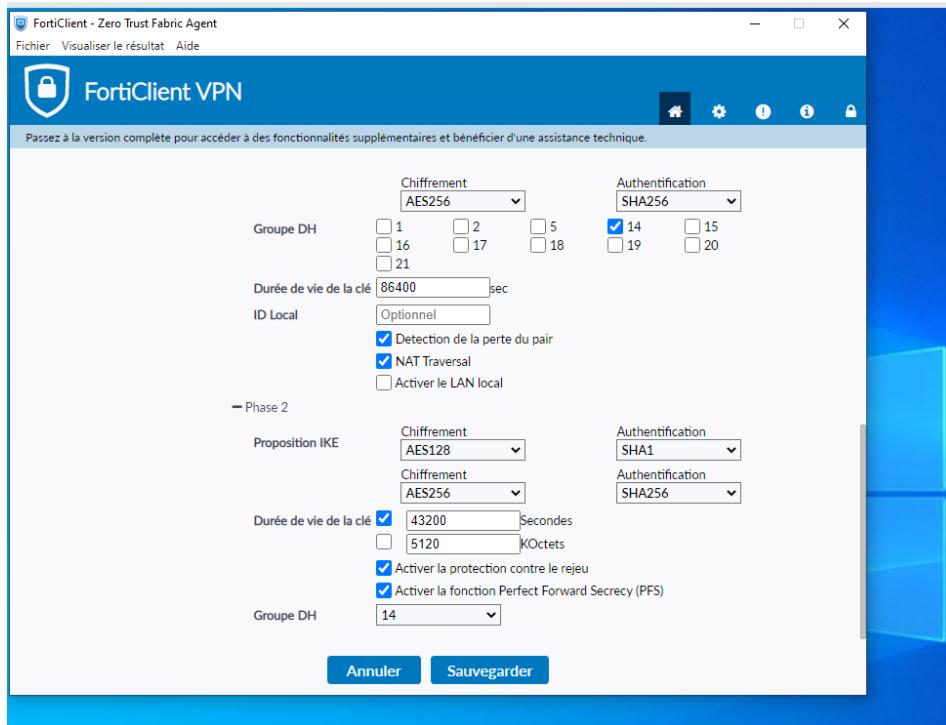
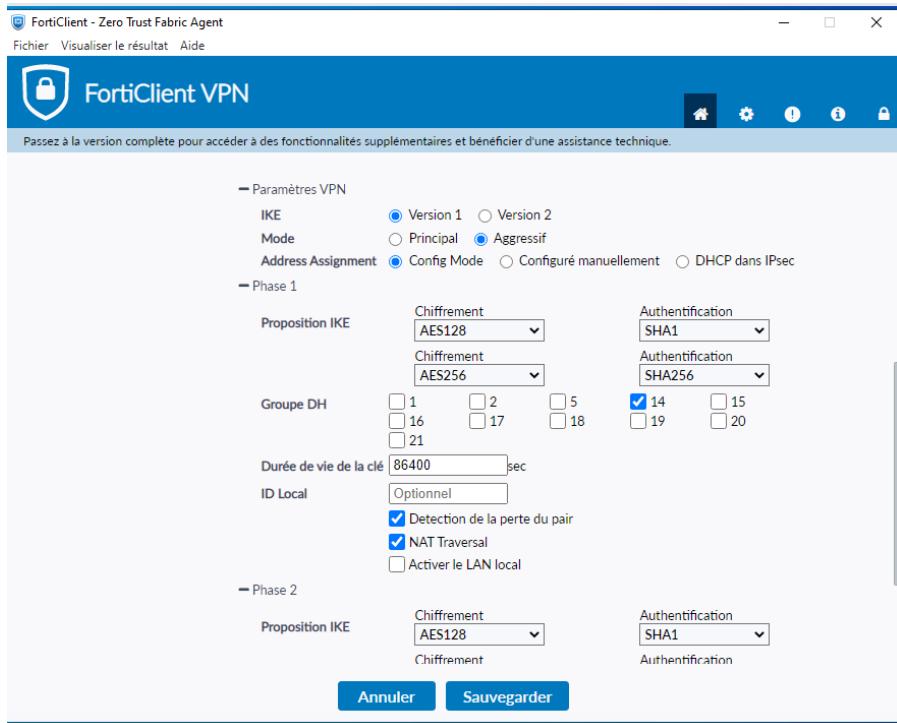
The screenshot shows the FortiOS-VM64 interface with the 'Firewall Policy' selected in the sidebar. The main window displays a list of firewall rules:

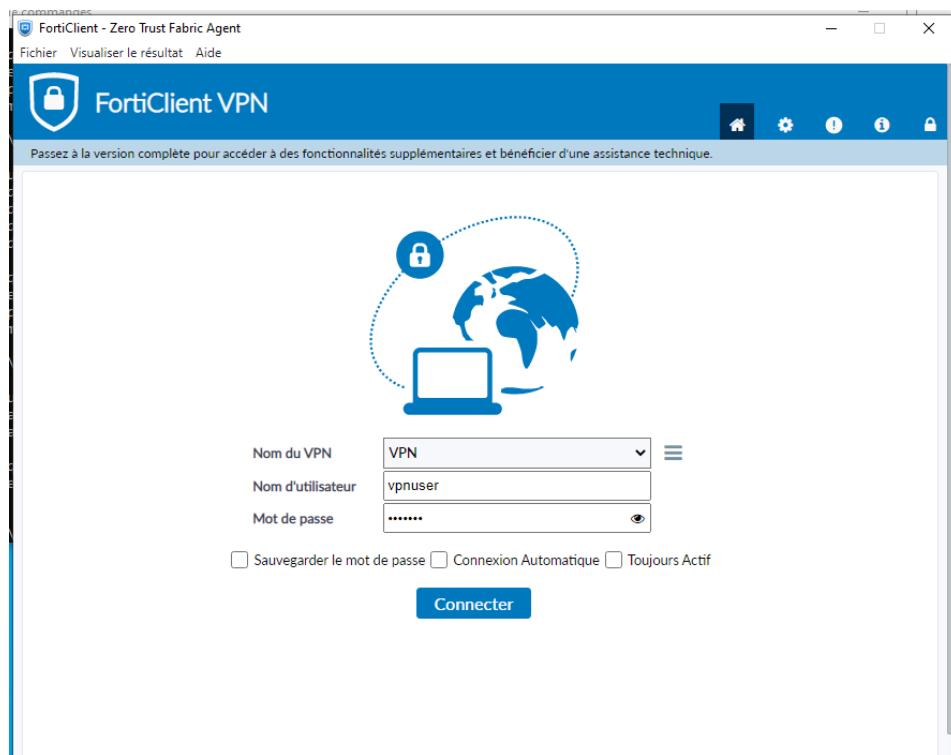
Name	Source	Destination	Schedule	Action	NAT	Security Profiles	Log	Bytes	
IPsec_VPN → LAN (port9)	vpn_IPsec_VPN_remote_0	IPsec_VPN_range	LOCAL	always	ALL	ACCEPT	Enabled	ssl no-inspection	All 3.36 kB
LAN (port9) → WAN1 (port1)	LAN_to_WAN	LOCAL	all	always	ALL	ACCEPT	Enabled	ssl no-inspection	UTM 7.73 kB
Implicit									

The screenshot shows the FortiClient - Zero Trust Fabric Agent interface with the 'Editor la connexion VPN' (Edit VPN Connection) dialog open. The 'VPN' tab is selected. The configuration fields are as follows:

- Nom de la connexion:** VPN
- Description:** (empty)
- Passerelle distante:** 192.168.114.49
+ Ajout d'une passerelle distante
- Méthode d'authentification:** Clé partagée
.....
- Authentification (XAuth):** Demander à l'ouverture de la connexion (radio button selected)
- VPN SSL de basculement:** [Aucun]
- Single Sign On Settings:** Activer l'authentification unique (SSO) pour le tunnel VPN (checkbox)
- Autres options:** Sauvegarder les informations d'authentification, Désactiver
- Paramètres avancés:** + Paramètres avancés

At the bottom are 'Annuler' (Cancel) and 'Sauvegarder' (Save) buttons.



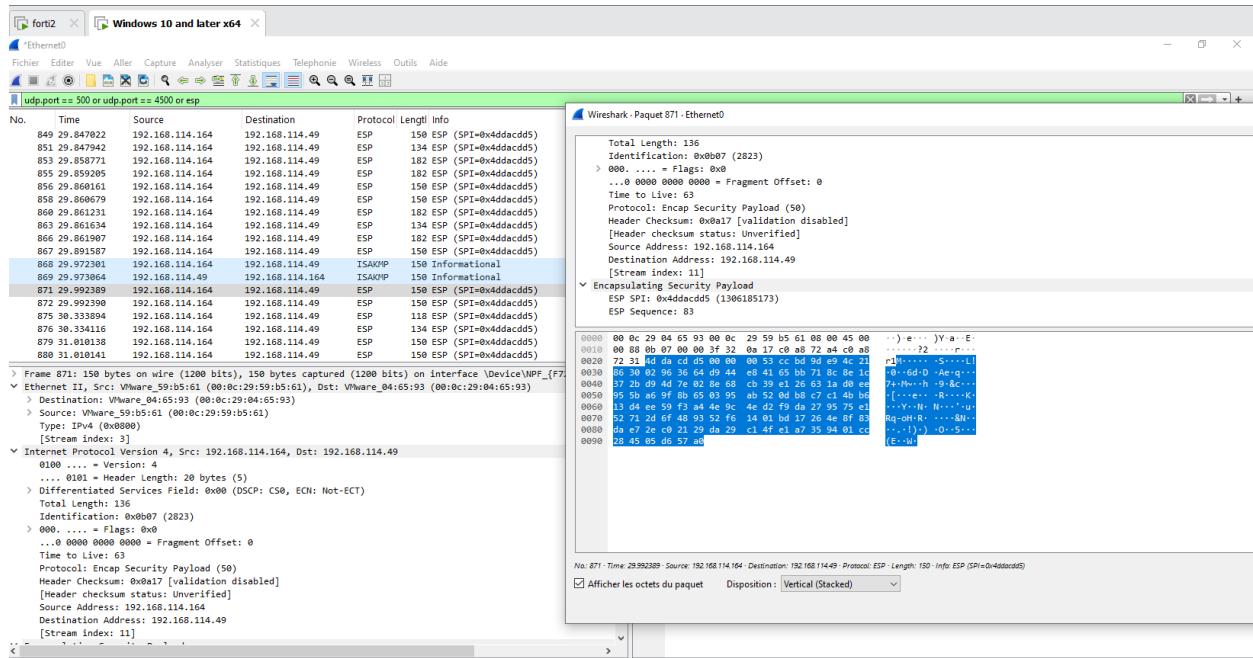


Filtre Wireshark :

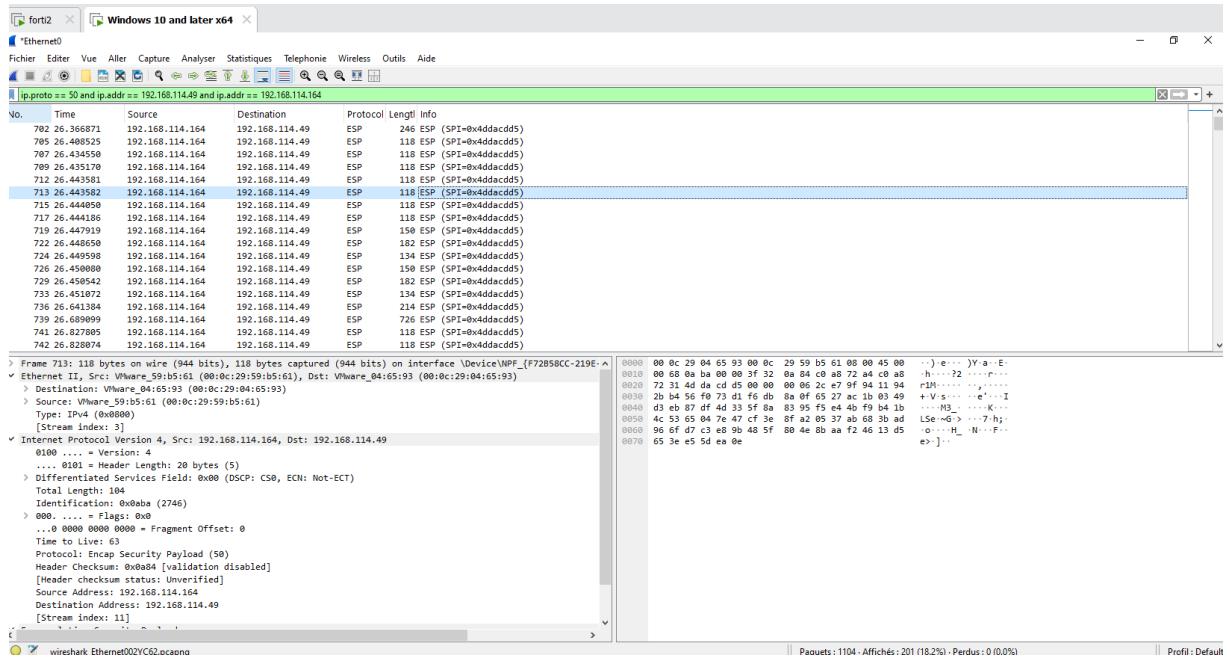
Sur l'interface WAN du FortiGate :

Objectif ici : Filtre Wireshark pour prouver l'établissement IPsec (IKE / ESP)

Présence des paquets ESP, le tunnel IPsec est bien établi et en cours d'utilisation.

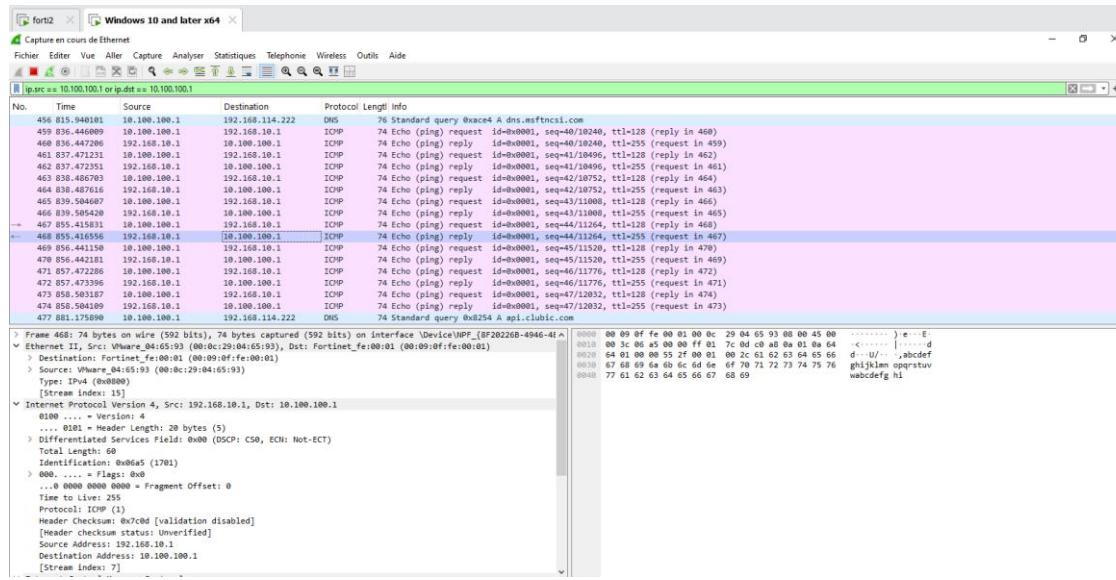
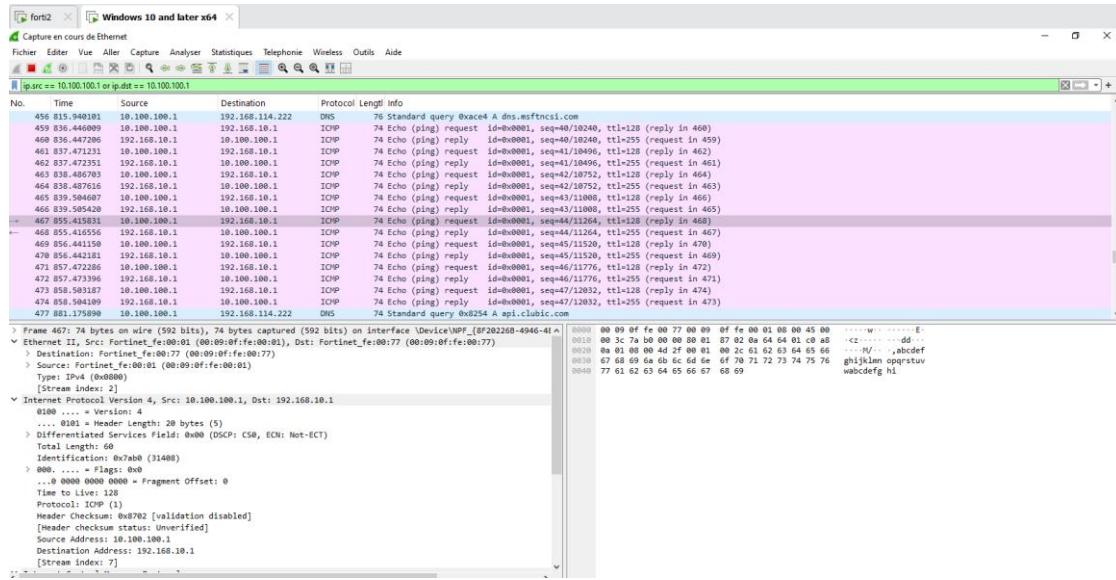


les paquets ESP entre deux adresses précises, par exemple entre ton client VPN (192.168.114.164) et le FortiGate (192.168.114.49)



Sur l'interface VPN :

Objectif ici : VPN attribuée au client (ex: 10.100.100.1) est utilisée pour communiquer avec le réseau interne (LAN).



Conclusion

Nous avons réussi à établir un tunnel VPN IPsec entre FortiClient et FortiGate en utilisant une configuration correcte des phases 1 et 2. Le tunnel a été testé et validé grâce à Wireshark, où nous avons observé des paquets ESP (protocole 50), ce qui prouve que les données sont bien chiffrées.

Ce projet nous a permis de mieux comprendre le fonctionnement d'un VPN IPsec, la configuration côté client et pare-feu, ainsi que l'importance du bon choix de mode réseau (bridged/NAT). Même si certaines limites techniques ont été rencontrées, le tunnel sécurisé fonctionne comme prévu.