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

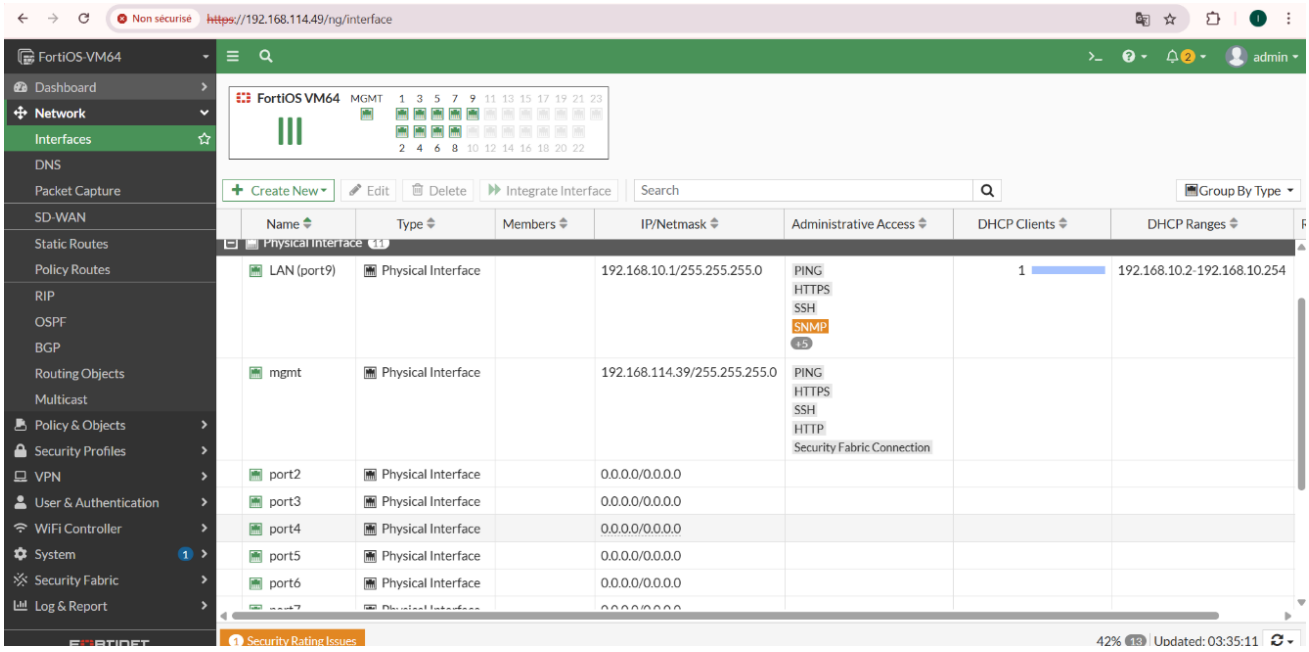
- Configurer un VPN IPsec Client-to-Site avec authentification locale.
- Permettre l'accès sécurisé à un réseau LAN via FortiClient.
- Assurer la supervision et le logging de la connexion VPN.

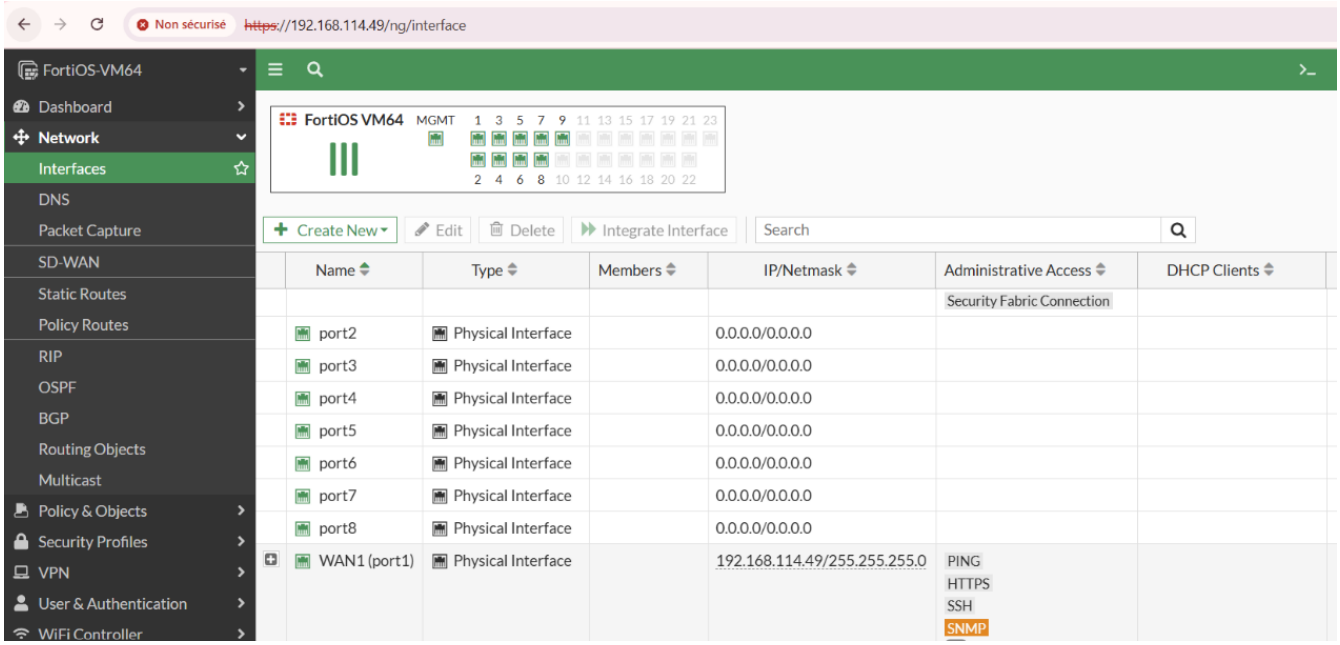
🛠️ Architecture Réseau

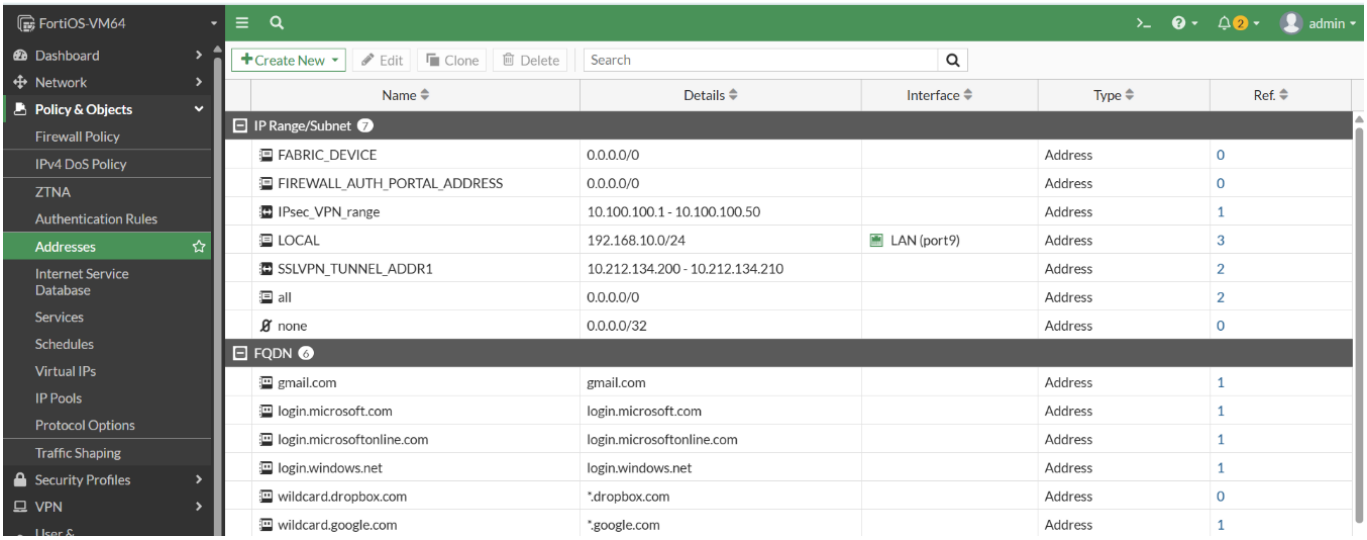
```
[ FortiClient ]
                        PC distant simulé (windows10)
                        IP : 192.168.114.164/24
                              |
                        Routeur / NAT
                              |
                  +--------------------------+
                  | FortiGate (VPN Server)   |
                  | WAN1: 192.168.114.49/24    |
                  | LAN: 192.168.10.1/24     |
                  +-----------+--------------+
                              |
                        [ LAN interne ]
                    Ex: 192.168.10.2 (serveur test ubuntu)
```

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
FortiOS-VM64
Dashboard
Network
Interfaces
DNS
Packet Capture
SD-WAN
Static Routes
Policy Routes
RIP
OSPF
BGP
Routing Objects
Multicast
Policy & Objects
Security Profiles
VPN
User & Authentication
WiFi Controller
System
Security Fabric
Log & Report
FortiOS VM64 MGMT
admin
Create New
Edit
Delete
Integrate Interface
Search
Group By Type
Name
Type
Members
IP/Netmask
Administrative Access
DHCP Clients
DHCP Ranges
Physical Interface
LAN (port9)
Physical Interface
192.168.10.1/255.255.255.0
PING
HTTPS
SSH
SNMP
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
0.0.0.0/0.0.0.0
port3
Physical Interface
0.0.0.0/0.0.0.0
port4
Physical Interface
0.0.0.0/0.0.0.0
port5
Physical Interface
0.0.0.0/0.0.0.0
port6
Physical Interface
0.0.0.0/0.0.0.0
Security Rating Issues
42%
Updated: 03:35:11


Non sécurisé https://192.168.114.49/ng/interface
FortiOS-VM64
Dashboard
Network
Interfaces
DNS
Packet Capture
SD-WAN
Static Routes
Policy Routes
RIP
OSPF
BGP
Routing Objects
Multicast
Policy & Objects
Security Profiles
VPN
User & Authentication
WiFi Controller
FortiOS VM64 MGMT
Create New
Edit
Delete
Integrate Interface
Search
Name
Type
Members
IP/Netmask
Administrative Access
DHCP Clients
Security Fabric Connection
port2
Physical Interface
0.0.0.0/0.0.0.0
port3
Physical Interface
0.0.0.0/0.0.0.0
port4
Physical Interface
0.0.0.0/0.0.0.0
port5
Physical Interface
0.0.0.0/0.0.0.0
port6
Physical Interface
0.0.0.0/0.0.0.0
port7
Physical Interface
0.0.0.0/0.0.0.0
port8
Physical Interface
0.0.0.0/0.0.0.0
WAN1 (port1)
Physical Interface
192.168.114.49/255.255.255.0
PING
HTTPS
SSH
SNMP


FortiOS-VM64
admin
Dashboard
Network
Policy & Objects
Firewall Policy
IPv4 DoS Policy
ZTNA
Authentication Rules
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Protocol Options
Traffic Shaping
Security Profiles
VPN
Create New
Edit
Clone
Delete
Search
Name
Details
Interface
Type
Ref.
IP Range/Subnet 7
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
FQDN 6
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

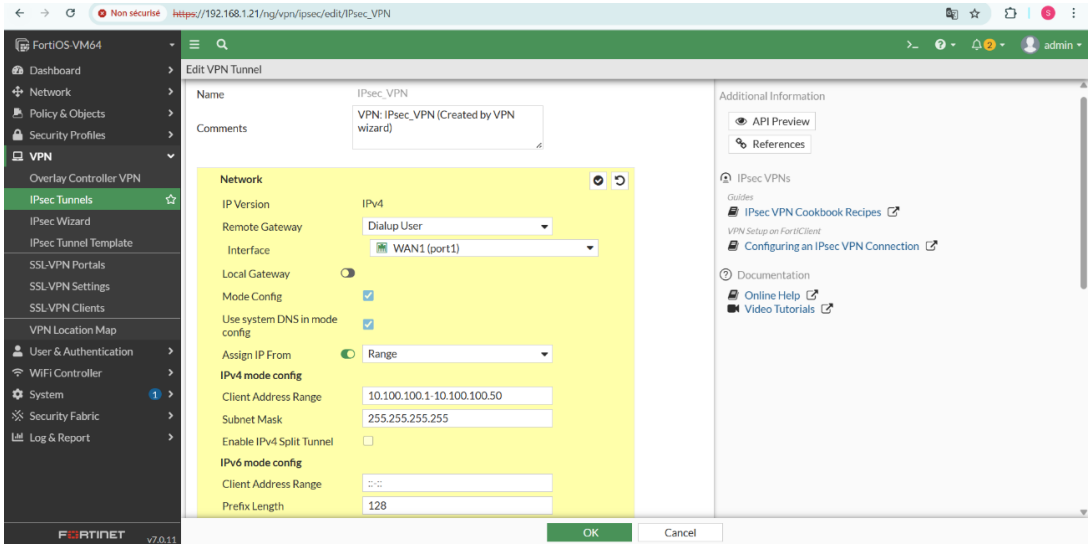
🔒 Paramètres VPN IPsec

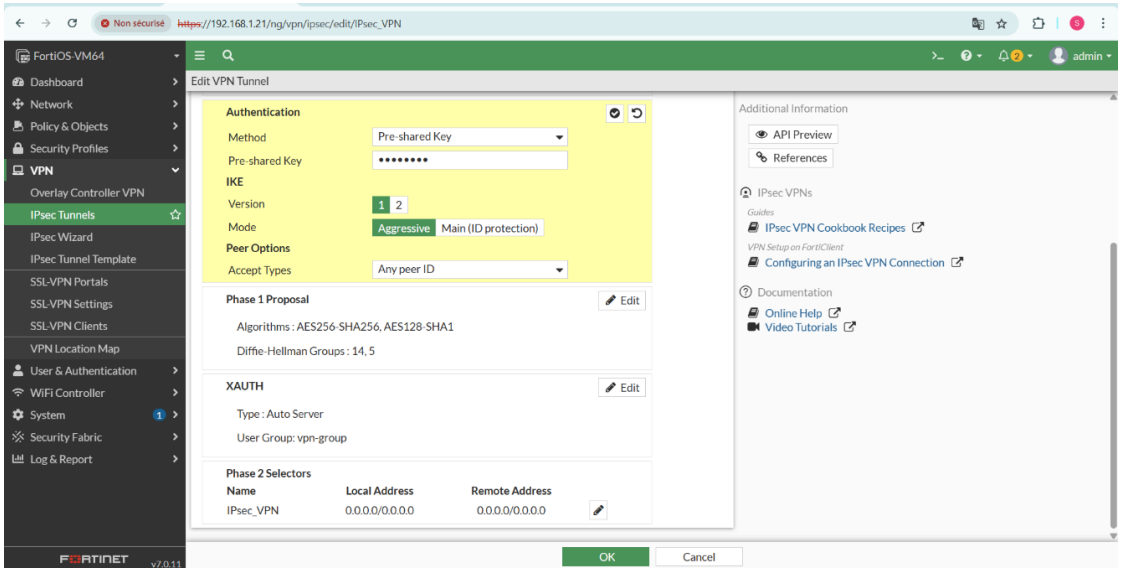
Phase 1 :

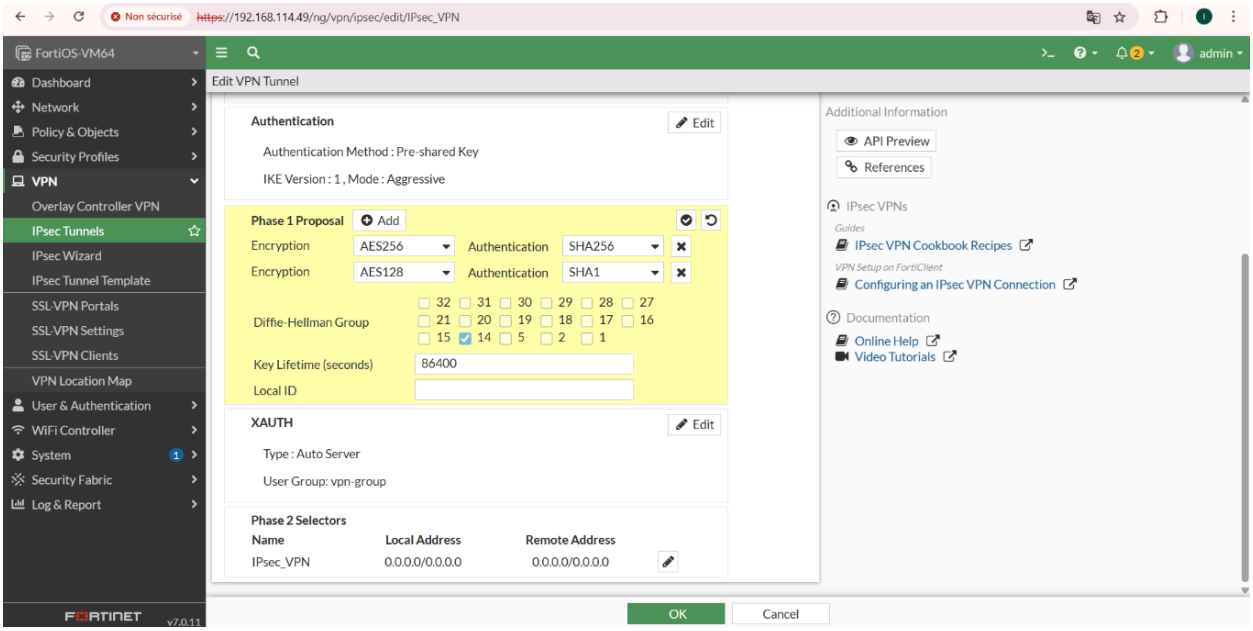
- Mode : Aggressive
- PSK : VPN2025!
- Encryption : AES256
- Hash : SHA256
- DH Group : 14
- PFS : Activé

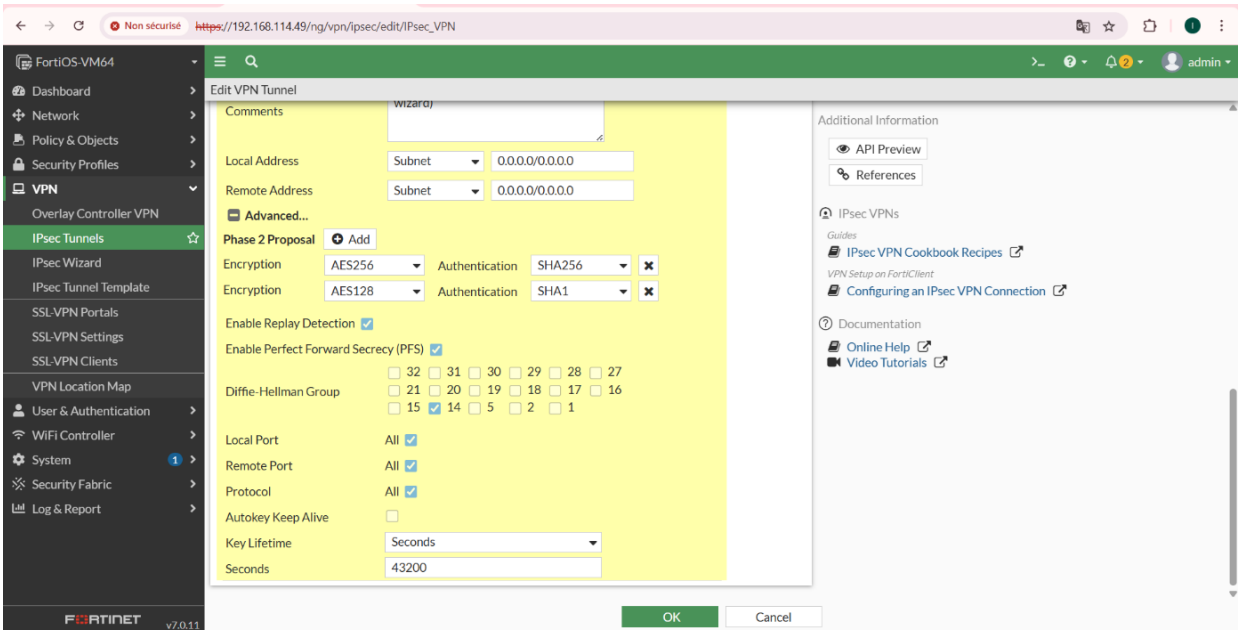
Phase 2 :

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



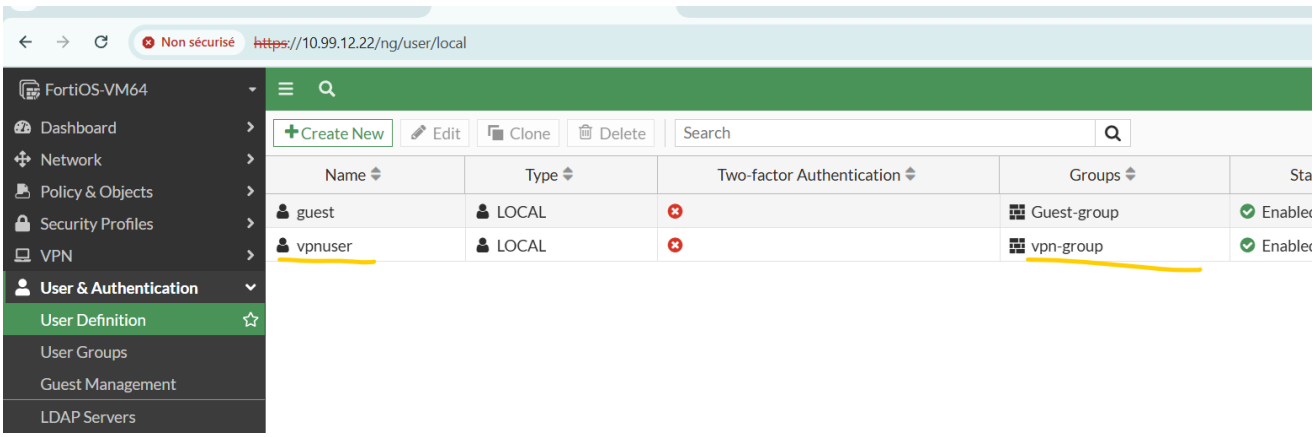


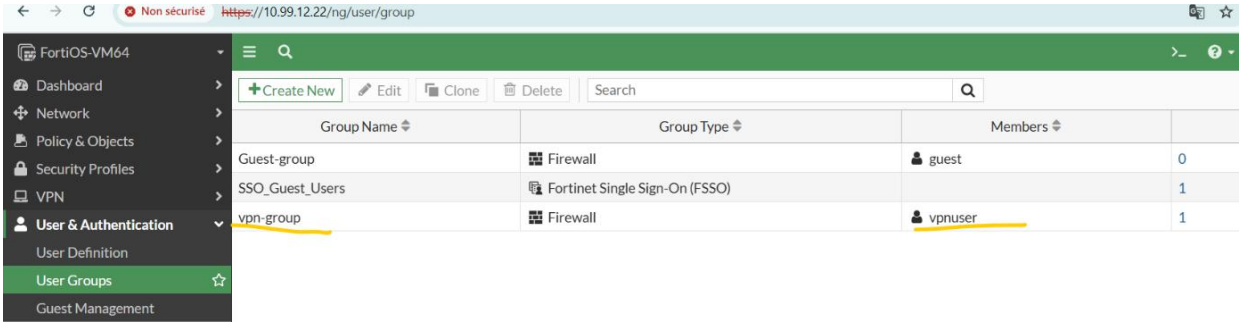




Authentification :

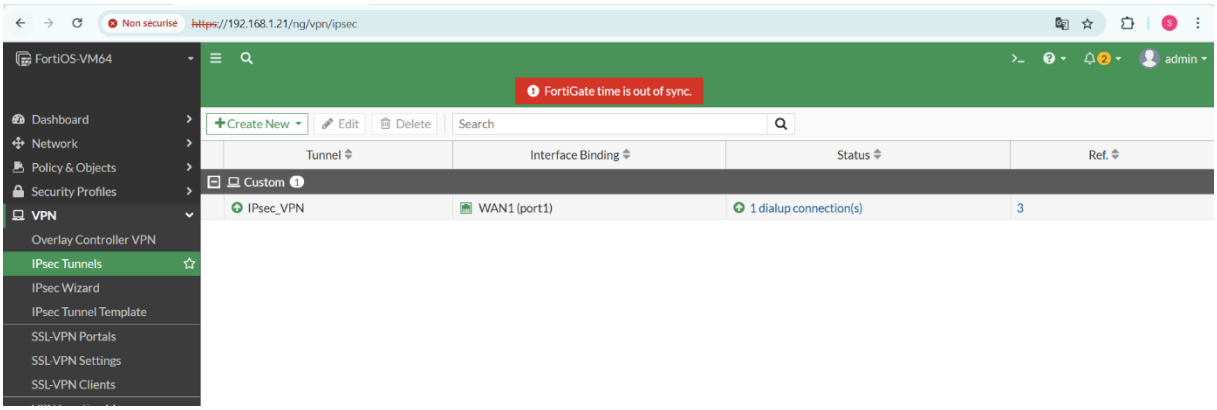
- Nom utilisateur : vpnuser
- Mot de passe : vpn1234



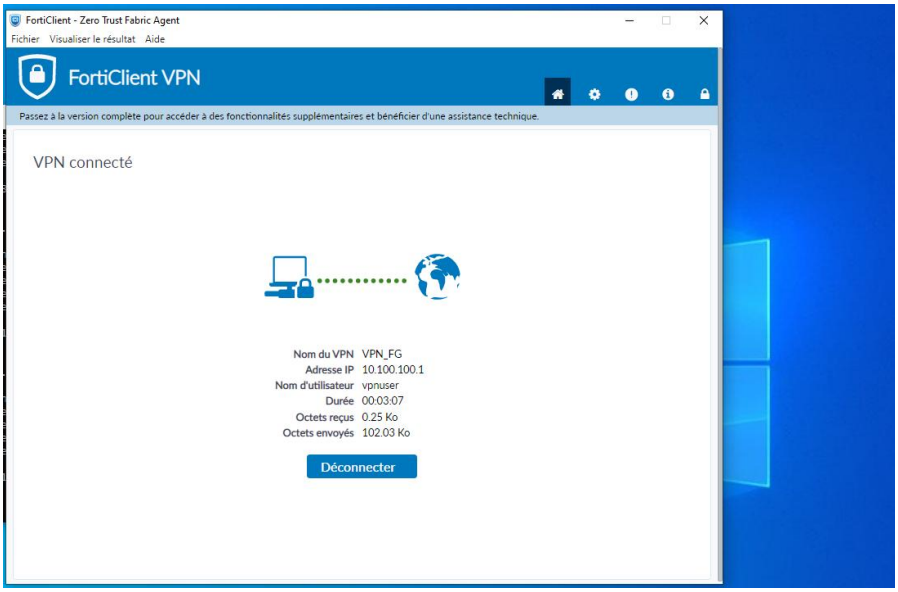


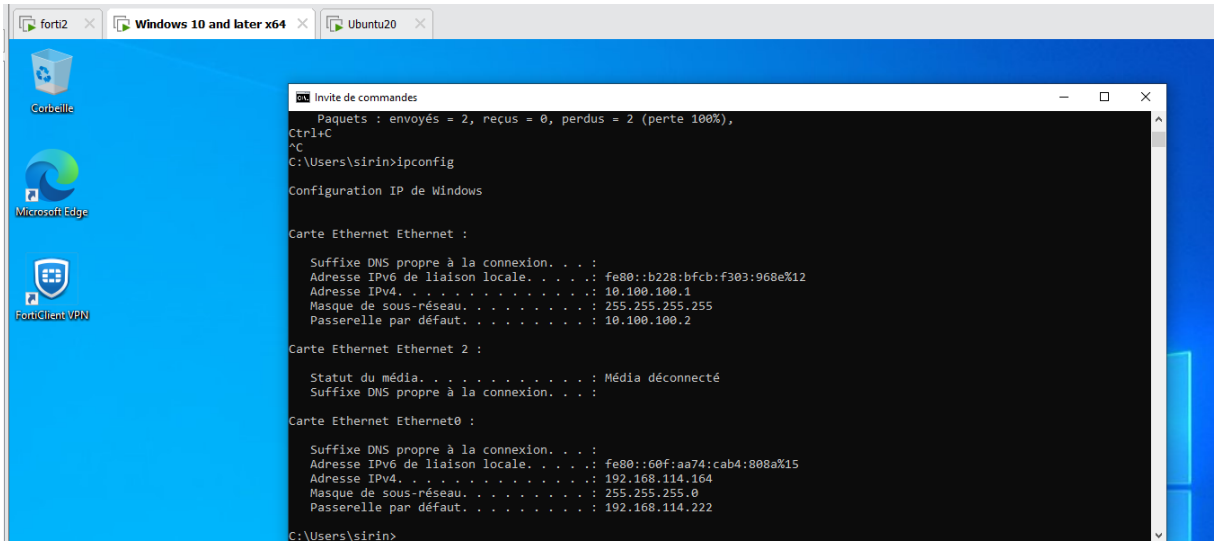
📊 Captures et Preuves de Fonctionnement

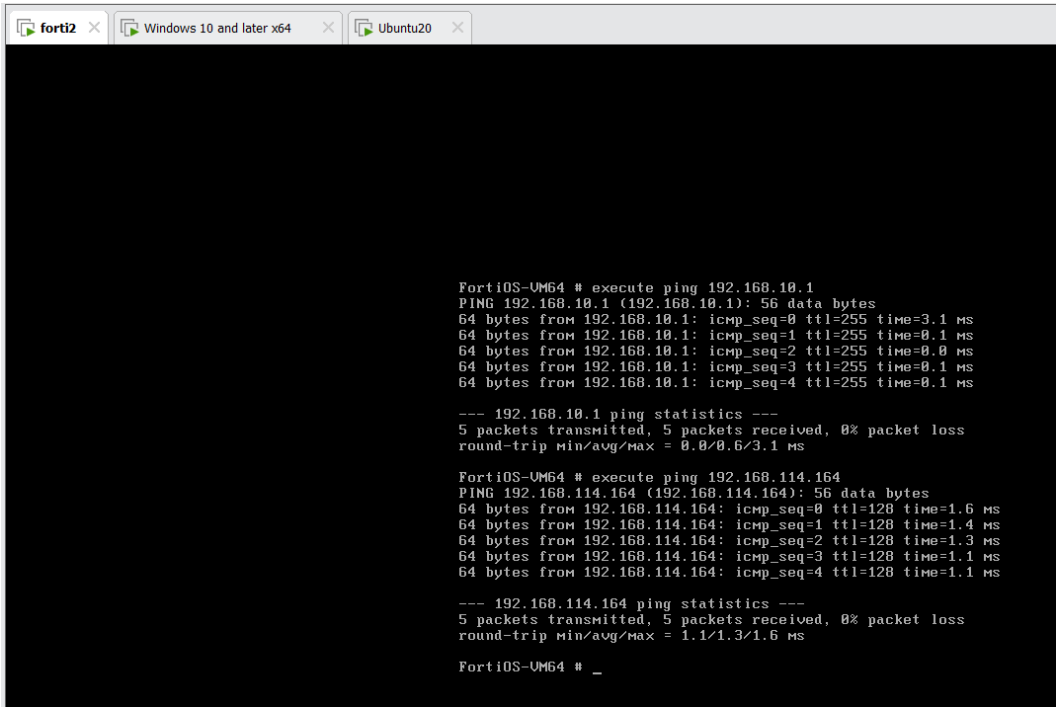
1. Connexion réussie avec FortiClient :

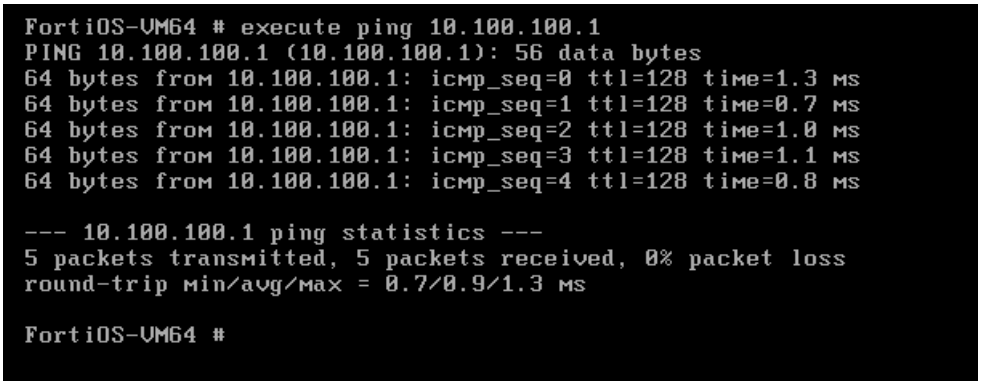


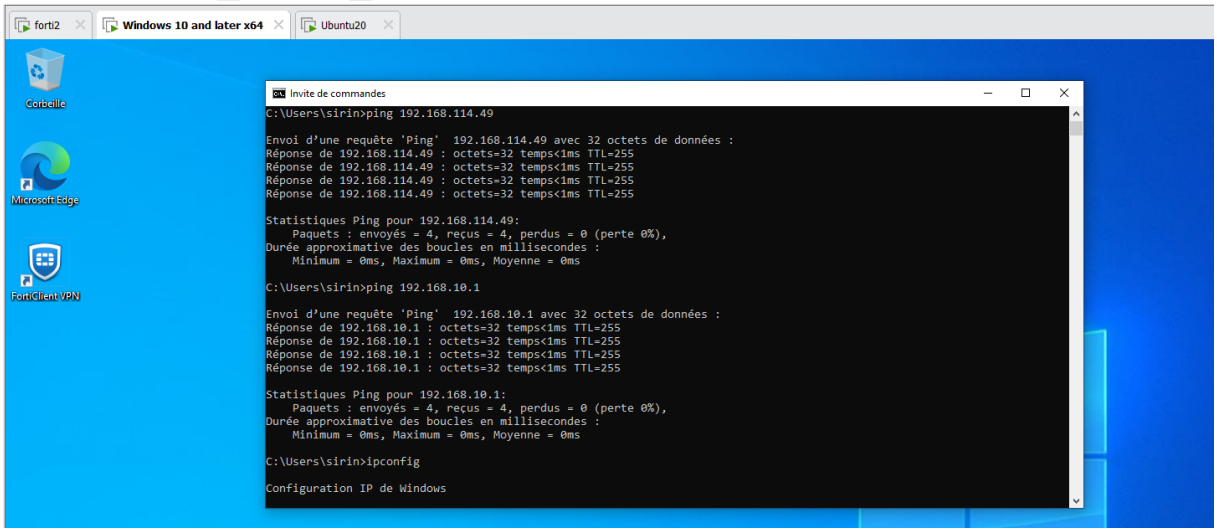
2. Adresse IP attribuée :

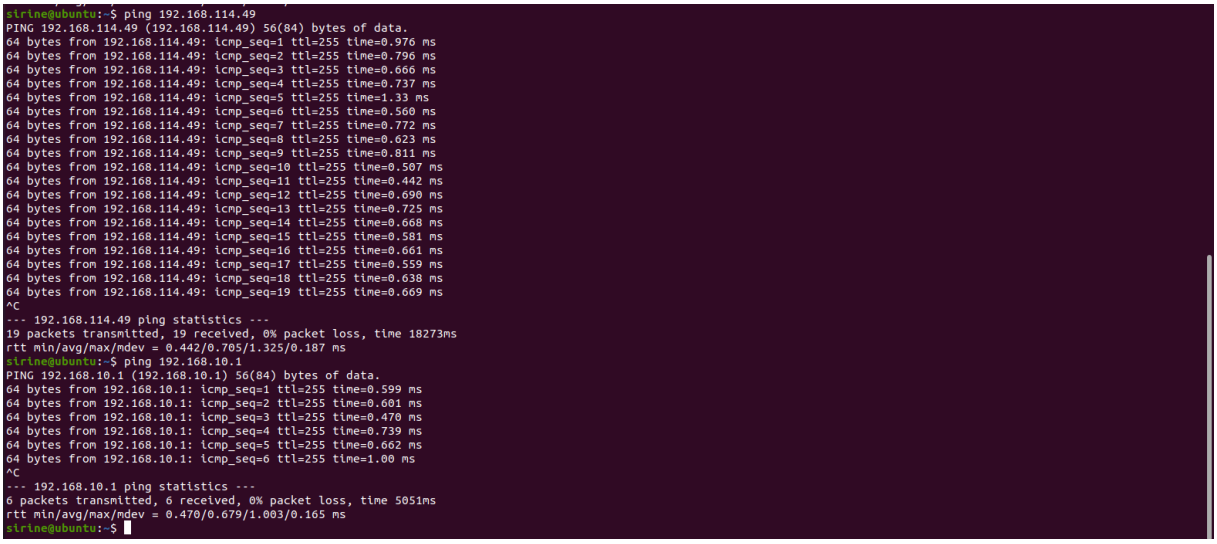



forti2
Windows 10 and later x64
Ubuntu20
Corbeille
Microsoft Edge
FortiClient VPN
Invite de commandes
Paquets : envoyés = 2, reçus = 0, perdus = 2 (perte 100%),
Ctrl+C
^C
C:\Users\sirin>ipconfig
Configuration IP de Windows
Carte Ethernet Ethernet :
Suffixe DNS propre à la connexion. . . :
Adresse IPv6 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
Suffixe DNS propre à la connexion. . . :
Carte Ethernet Ethernet0 :
Suffixe 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>


forti2
Windows 10 and later x64
Ubuntu20
FortiOS-VM64 # 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-VM64 # 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-VM64 # _

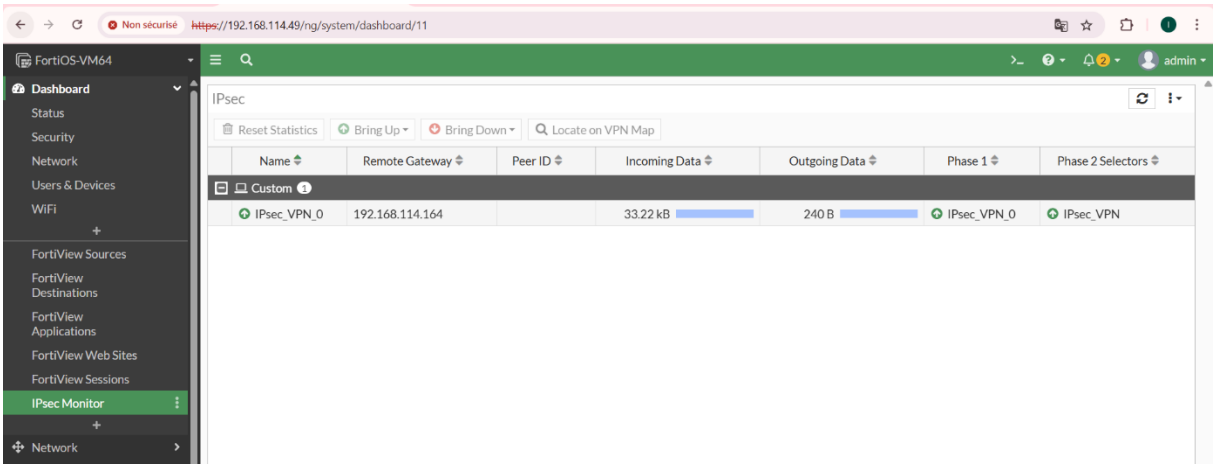

FortiOS-VM64 # execute ping 10.100.100.1
PING 10.100.100.1 (10.100.100.1): 56 data bytes
64 bytes from 10.100.100.1: icmp_seq=0 ttl=128 time=1.3 ms
64 bytes from 10.100.100.1: icmp_seq=1 ttl=128 time=0.7 ms
64 bytes from 10.100.100.1: icmp_seq=2 ttl=128 time=1.0 ms
64 bytes from 10.100.100.1: icmp_seq=3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



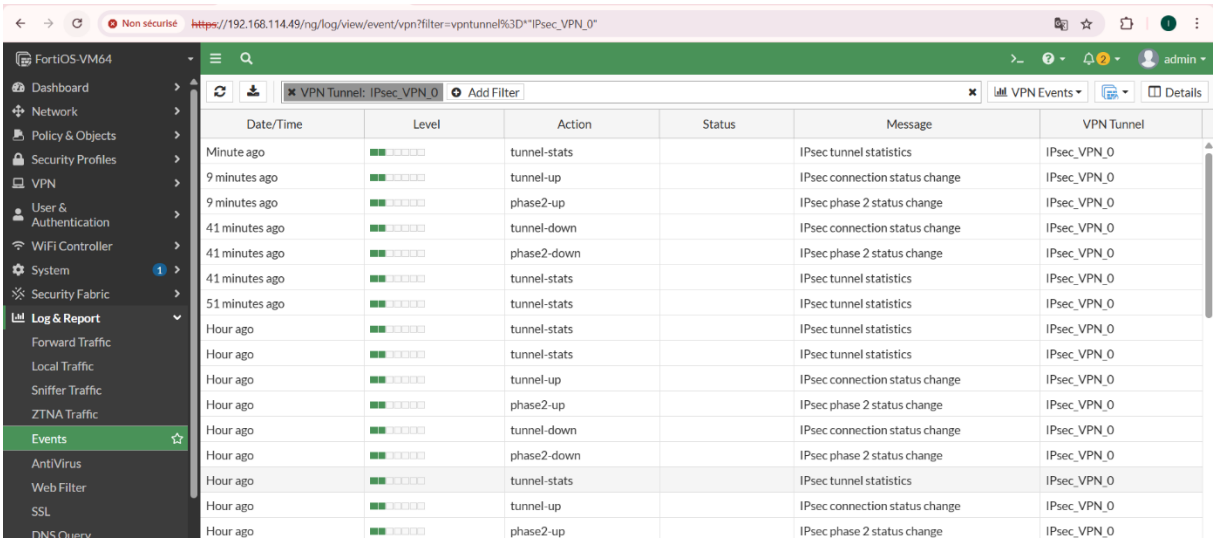


4. Supervision FortiGate :

- VPN Monitor :

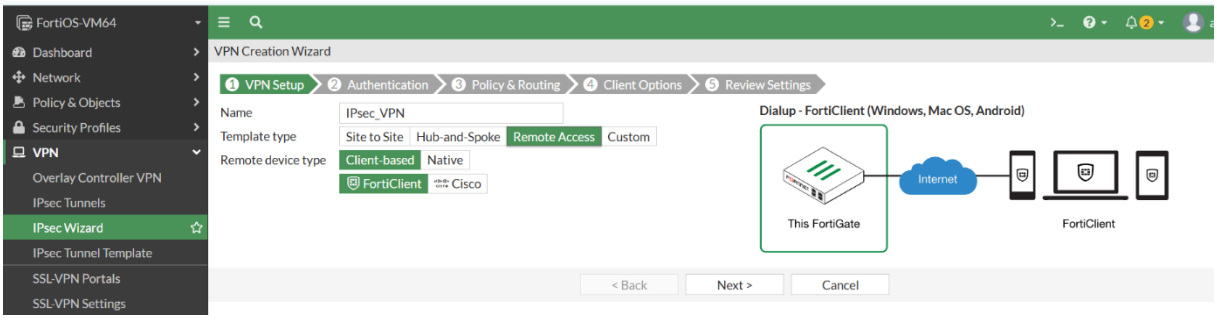


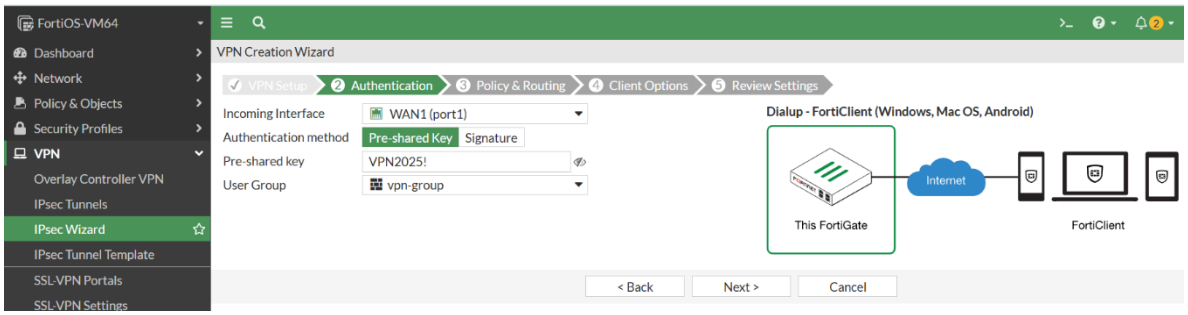
- Log & Report > VPN Events :

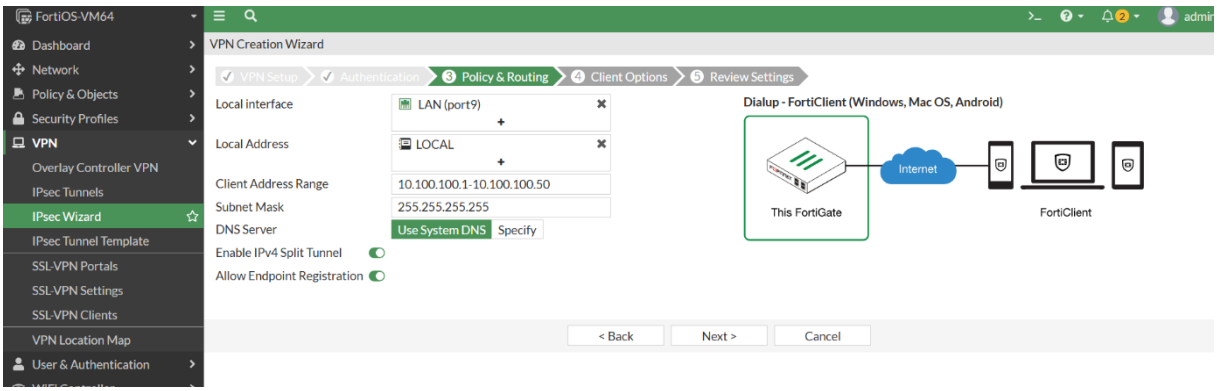


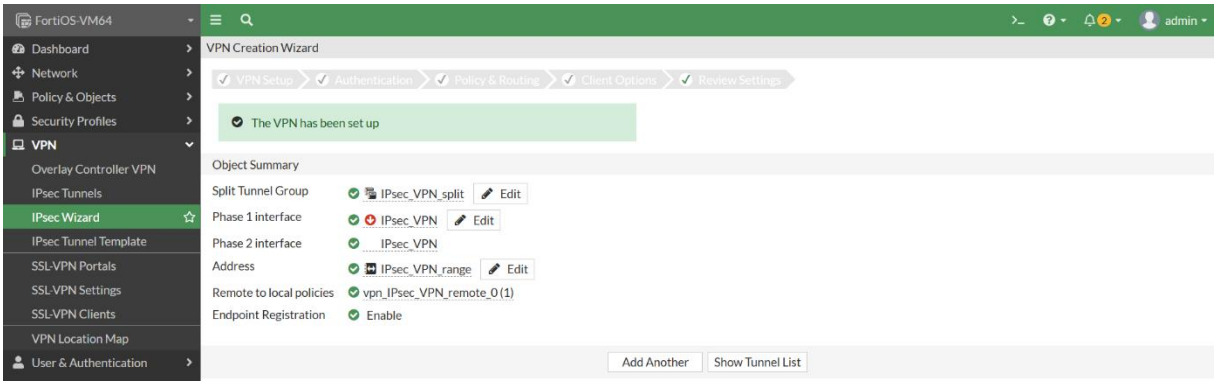
📁 Export / Configuration

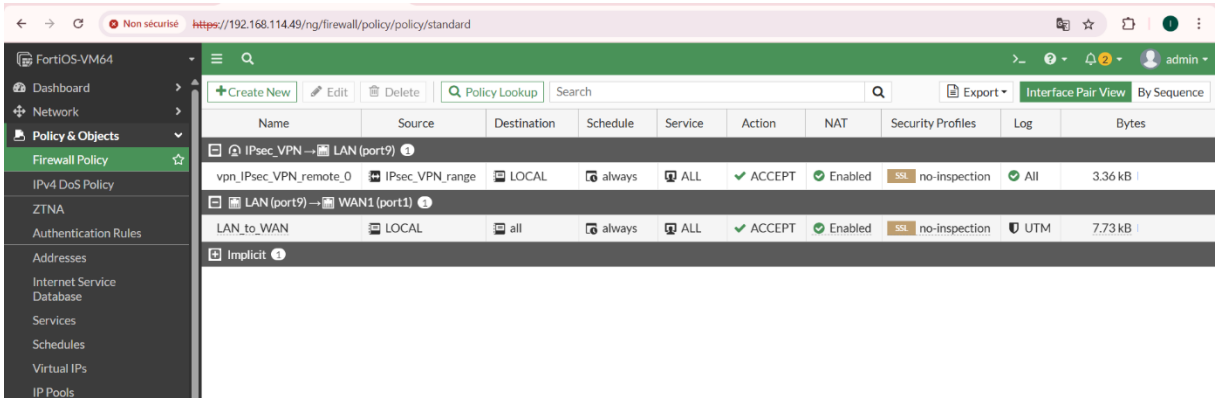
Extrait config FortiGate : *(partie VPN et policies pertinentes)*

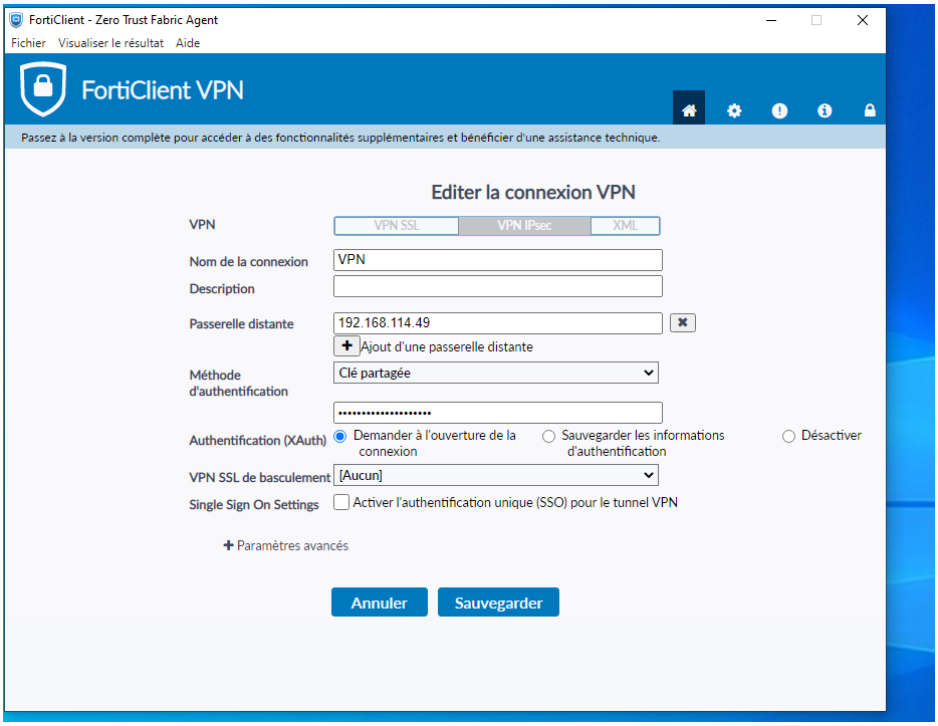


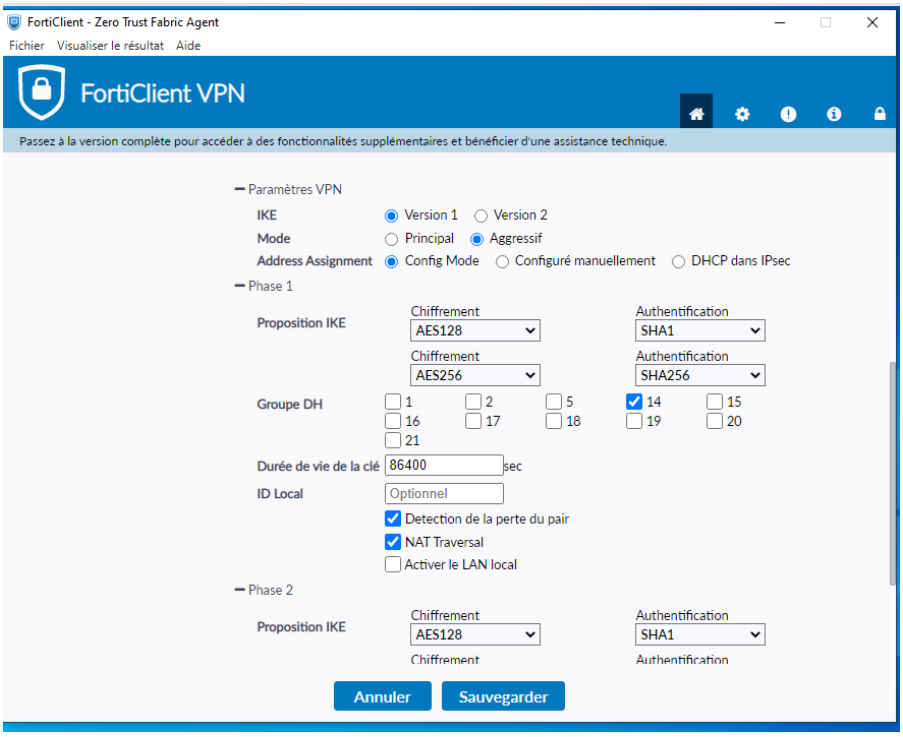


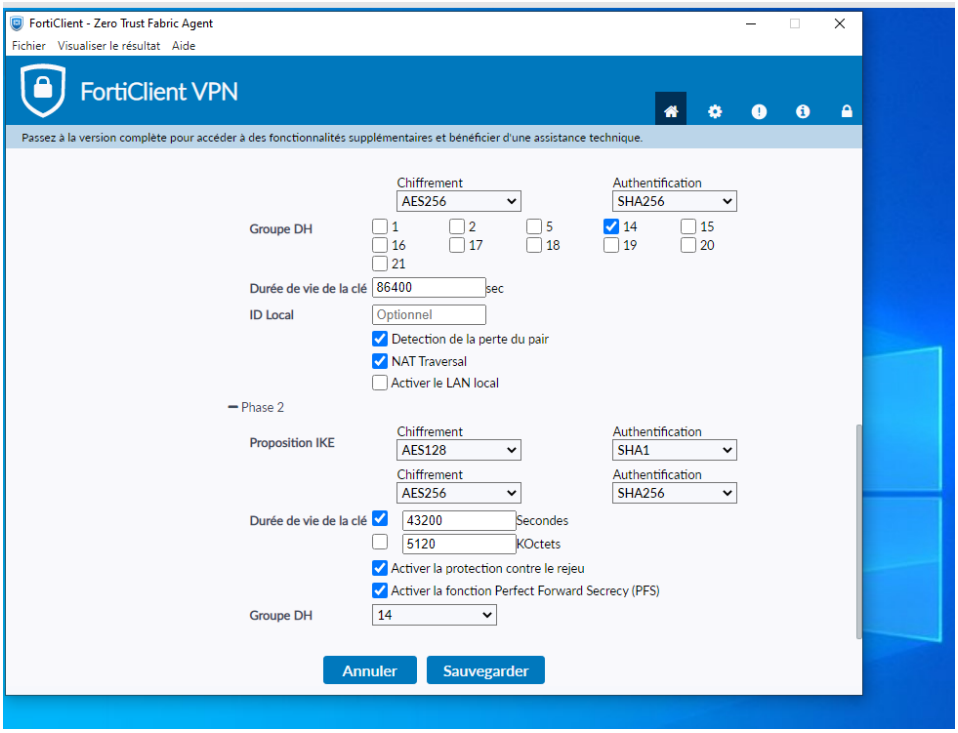


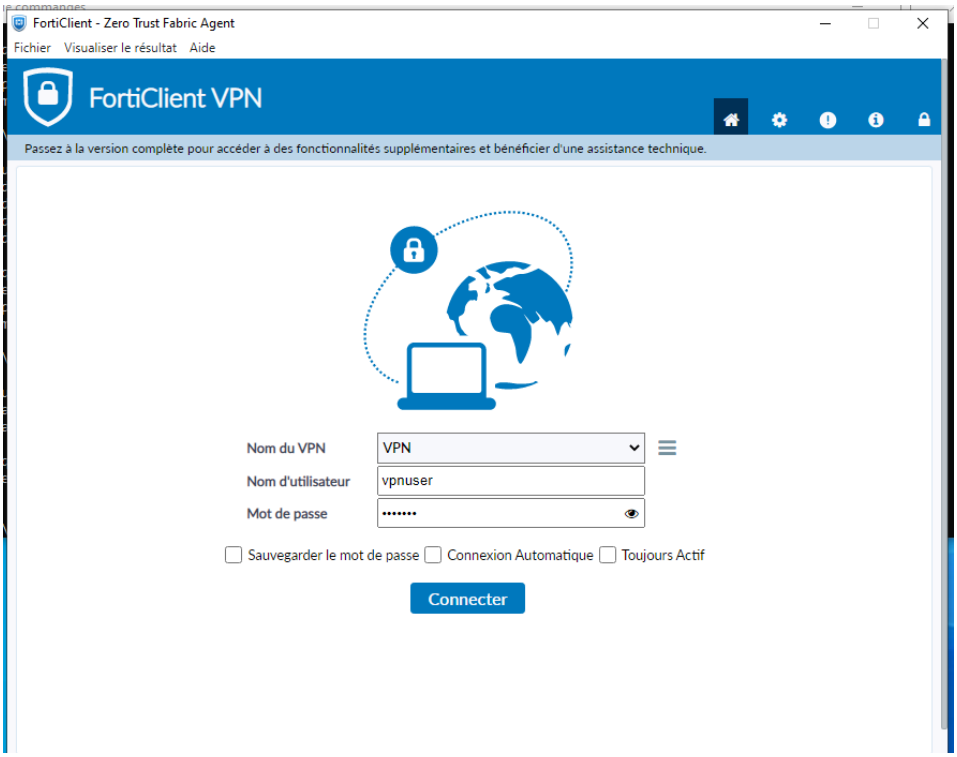

FortiOS-VM64
admin
Dashboard
Network
Policy & Objects
Security Profiles
VPN
Overlay Controller VPN
IPsec Tunnels
IPsec Wizard
IPsec Tunnel Template
SSL-VPN Portals
SSL-VPN Settings
SSL-VPN Clients
VPN Location Map
User & Authentication
VPN Creation Wizard
VPN Setup
Authentication
Policy & Routing
Client Options
Review Settings
The VPN has been set up
Object Summary
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
Add Another
Show Tunnel List


Non sécurisé
https://192.168.114.49/ng/firewall/policy/policy/standard
FortiOS-VM64
admin
Dashboard
Network
Policy & Objects
Firewall Policy
IPv4 DoS Policy
ZTNA
Authentication Rules
Addresses
Internet Service Database
Services
Schedules
Virtual IPs
IP Pools
Create New
Edit
Delete
Policy Lookup
Search
Export
Interface Pair View
By Sequence
Name
Source
Destination
Schedule
Service
Action
NAT
Security Profiles
Log
Bytes
IPsec_VPN → LAN (port9)
vpn_IPsec_VPN_remote_0
IPsec_VPN_range
LOCAL
always
ALL
ACCEPT
Enabled
no-inspection
All
3.36 kB
LAN (port9) → WAN1 (port1)
LAN_to_WAN
LOCAL
all
always
ALL
ACCEPT
Enabled
no-inspection
UTM
7.73 kB
Implicit


FortiClient - Zero Trust Fabric Agent
Fichier
Visualiser le résultat
Aide
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
Description
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
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


FortiClient - Zero Trust Fabric Agent
Fichier Visualiser le résultat Aide
FortiClient VPN
Passez à la version complète pour accéder à des fonctionnalités supplémentaires et bénéficier d'une assistance technique.
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
86400
sec
ID Local
Optionnel
Detection de la perte du pair
NAT Traversal
Activer le LAN local
Phase 2
Proposition IKE
Chiffrement
AES128
Authentification
SHA1
Annuler
Sauvegarder


FortiClient - Zero Trust Fabric Agent
Fichier Visualiser le résultat Aide
FortiClient VPN
Passez à la version complète pour accéder à des fonctionnalités supplémentaires et bénéficier d'une assistance technique.
Chiffrement
AES256
Authentification
SHA256
Groupe DH
1 2 5 14 15
16 17 18 19 20
21
Durée de vie de la clé
86400
sec
ID Local
Optionnel
Detection de la perte du pair
NAT Traversal
Activer le LAN local
Phase 2
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
14
Annuler
Sauvegarder

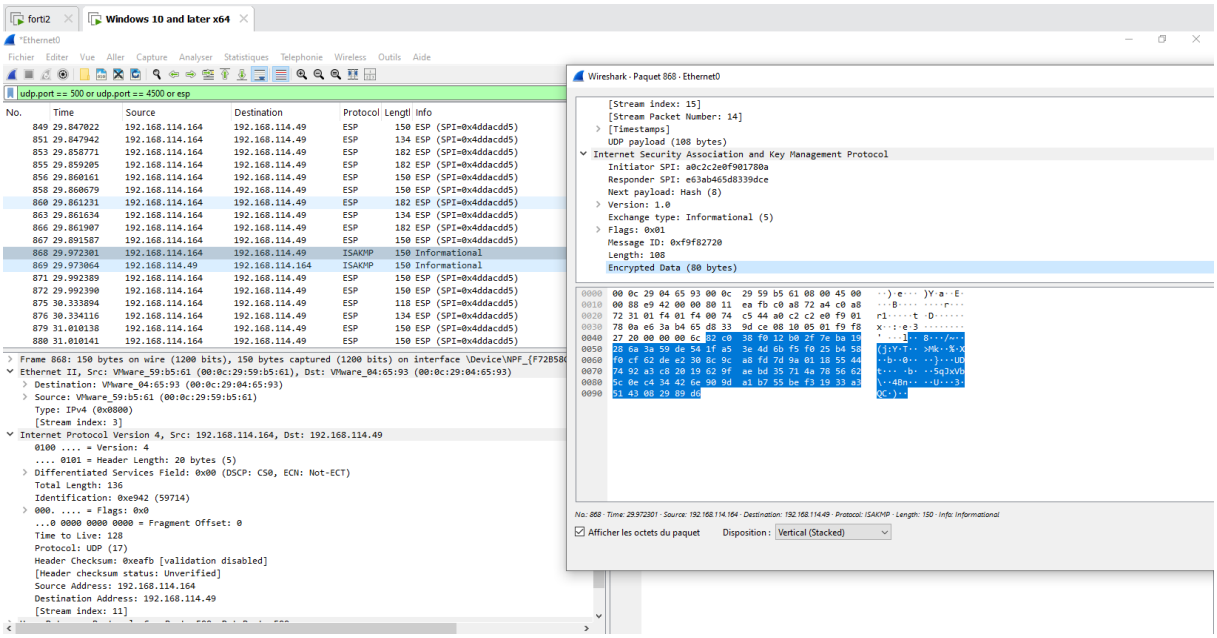


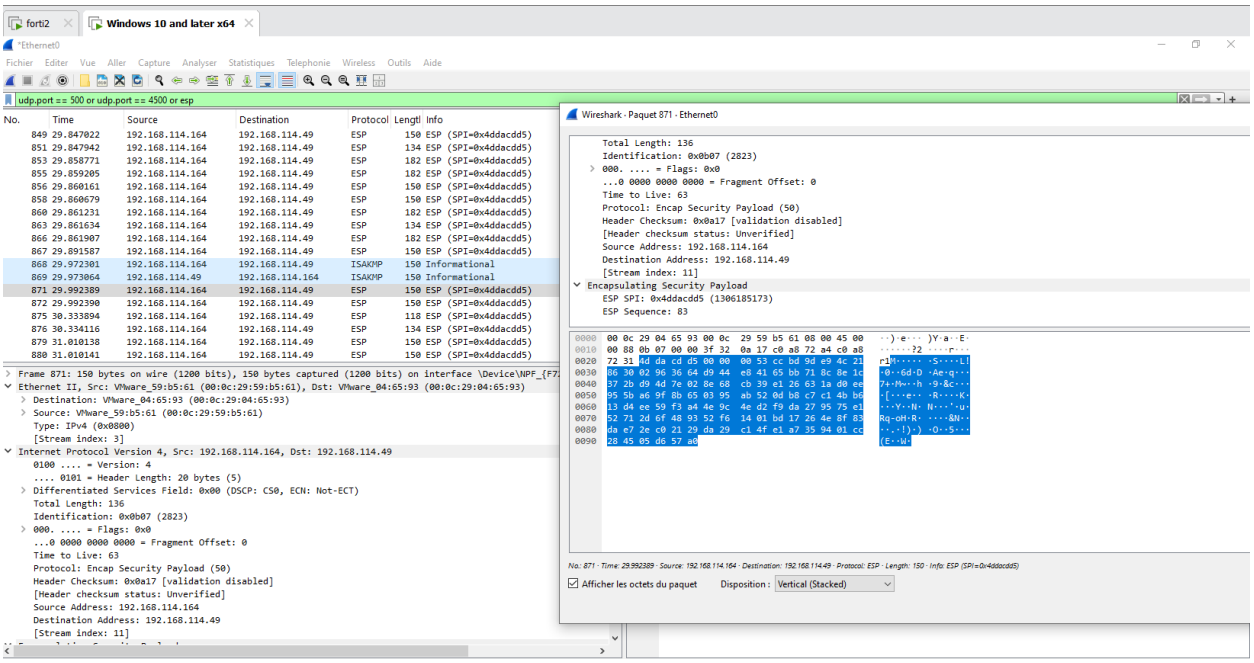
Filtre Wireshark :

Sur l'interface WAN du FortiGate :

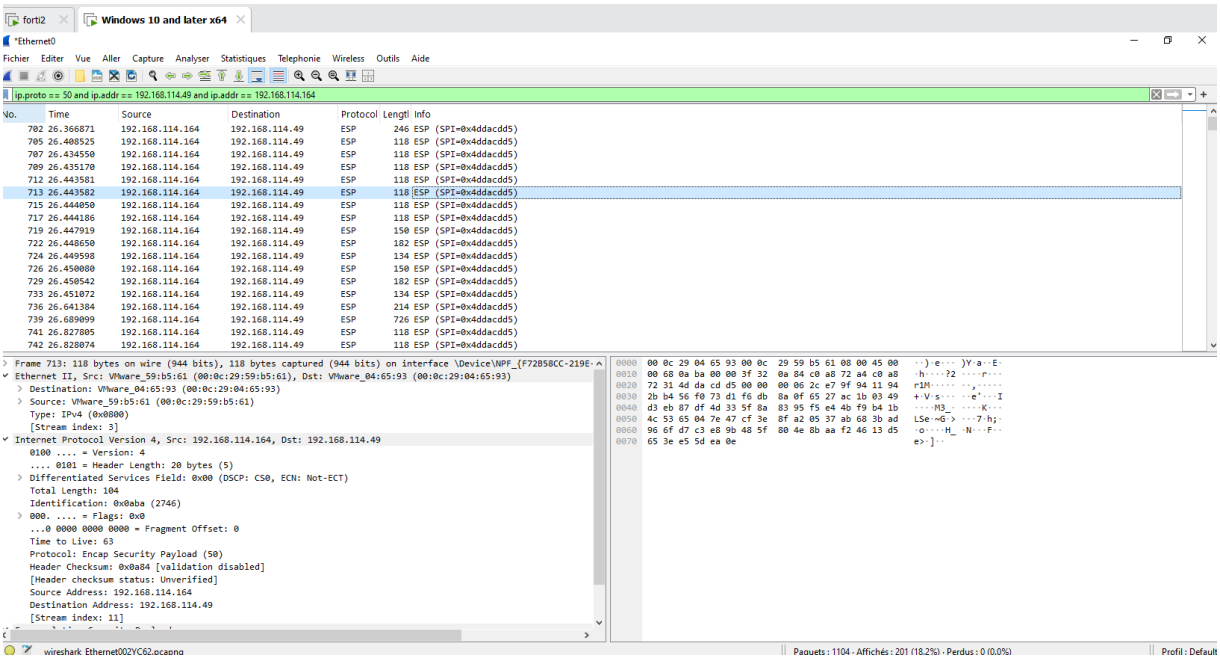
Objectif ici : Filtre Wireshark pour prouver l'établissement IPsec (IKE / ESP)

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



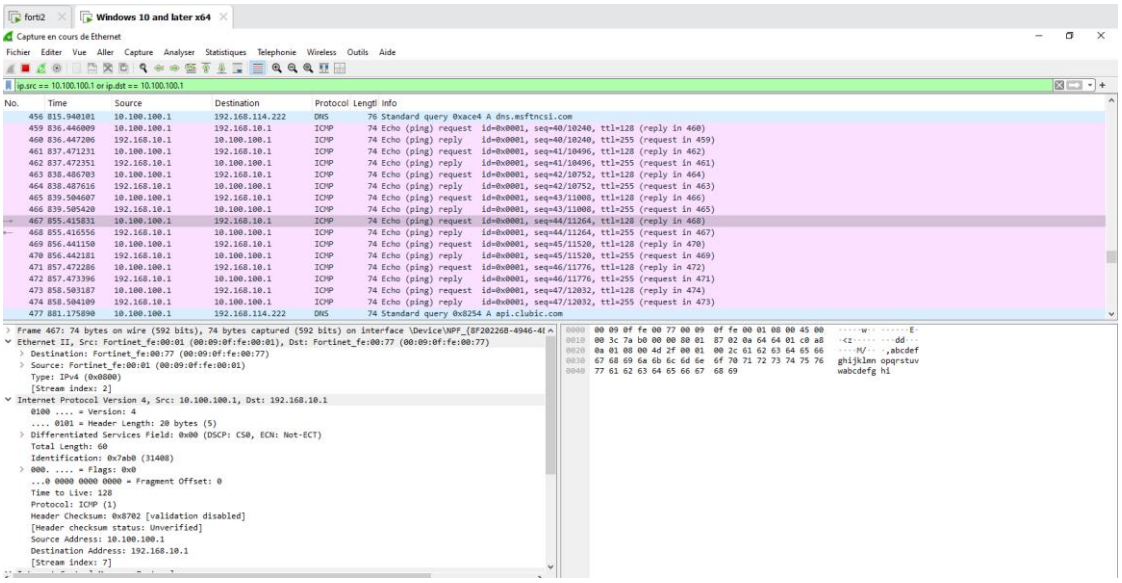


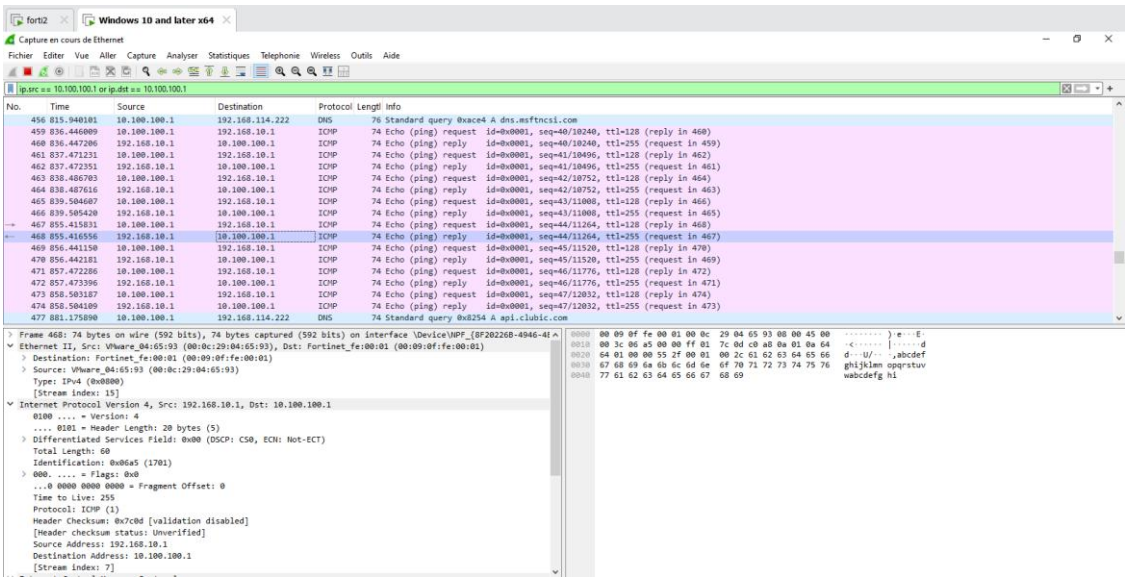
les paquets ESP entre deux adresses précises, par exemple entre ton client VPN (192.168.114.164) et le FortiGate (192.168.114.49)



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.