PROJET PERSONNEL – INTREGRATION D'UN FORTIGATE DANS MON HOMELAB

BRETON Théo

Projet N°4 : INTEGRATION D'UN PARE FEU FORTINET DANS MON HOMELAB

PARTIE 1 – LA REMISE A NIVEAU DU FORTIGATE

1. Identifiant par défaut

```
Utilisateur : maintainer
Mot de passe : bcpb suivi du numéro de série de votre appareil (en MAJUSCULES).
```

2. Gestion des administrateurs

Pour afficher la configuration d'un utilisateur spécifique (ici user1) :

```
show system admin bretont
```

Pour modifier ou attribuer un mot de passe à l'administrateur :

```
config system admin
    edit "user1"
        set password "MOTDEPASSE"
        set accprofile "super_admin"
        set vdom "root"
    next
end
```

3. Diagnostics et vérifications des interfaces

Pour afficher l'état physique des ports, leur mode (Statique/DHCP) et les adresses IP actuellement assignées :

```
get system interface physical
```

Pour voir la liste des baux DHCP (les adresses IP distribuées par le FortiWiFi aux machines connectées) :

```
get system dhcp lease
```

4. Configuration réseau de l'interface (Initialisation)

Lorsque l'interface n'avait pas encore de mode de fonctionnement défini, nous avons tenté de forcer l'IP statique. Pour rappel, la syntaxe exacte pour entrer dans le menu et ouvrir les accès d'administration (HTTPS, HTTP, SSH, PING) est :

```
config system interface
    edit "internal"
        set mode static
        set ip 192.168.1.99 255.255.255.0
        set allowaccess https http ssh ping
    next
end
```

(Note : C'est après cette étape que tu as basculé sur l'interface graphique pour fusionner internal et wifi dans le commutateur logiciel lan, puis fixer l'IP finale en 192.168.2.2).

5. Réinitialisation du pare-feu :

Le Reset d'usine complet (Factory Reset)

Cette commande efface toute la configuration (IP, utilisateurs, règles de firewall) et remet le FortiWiFi exactement comme s'il sortait d'usine.

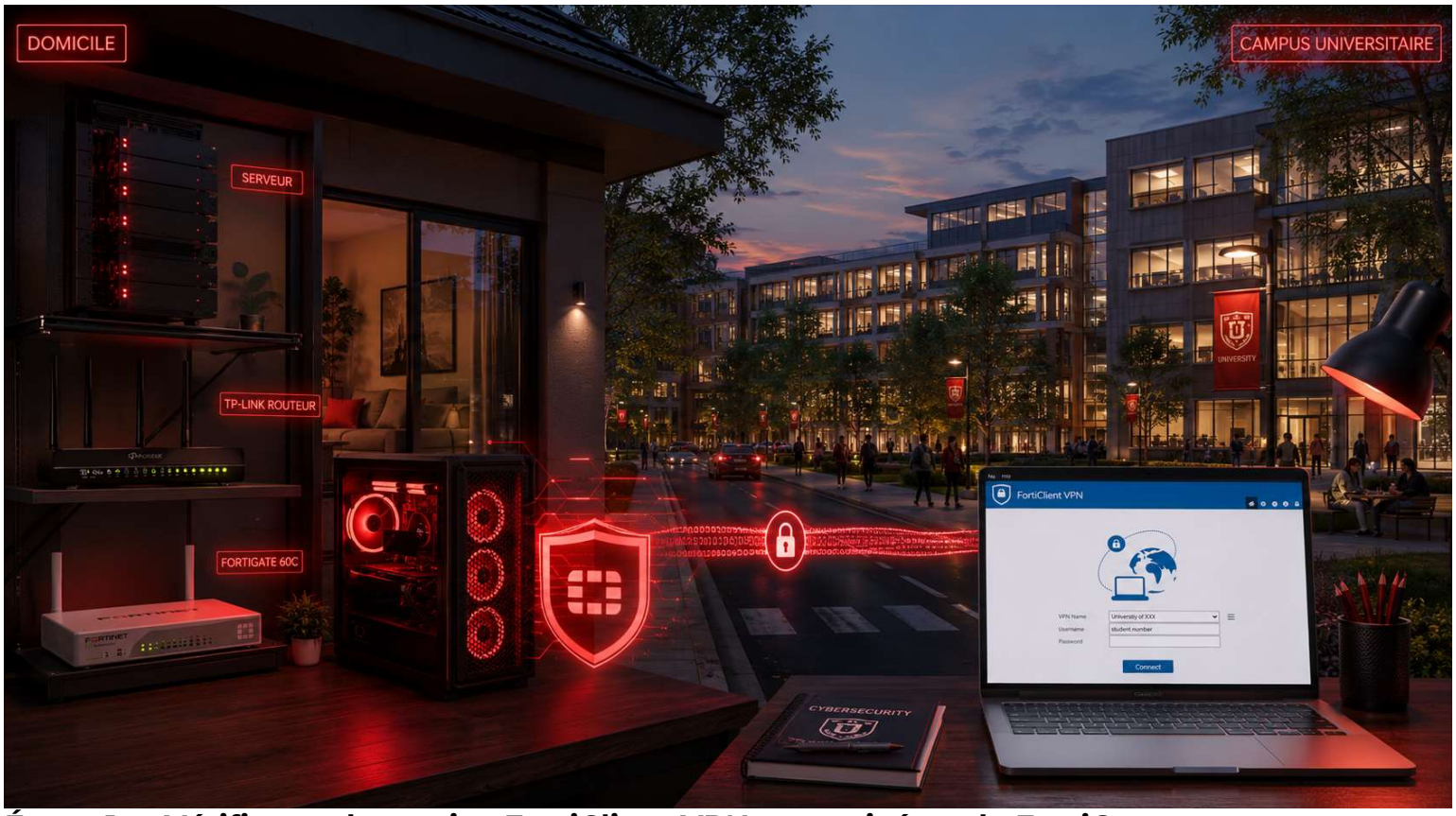
```
execute factoryreset
```

Le Reboot simple (Redémarrage)

```
execute reboot
```

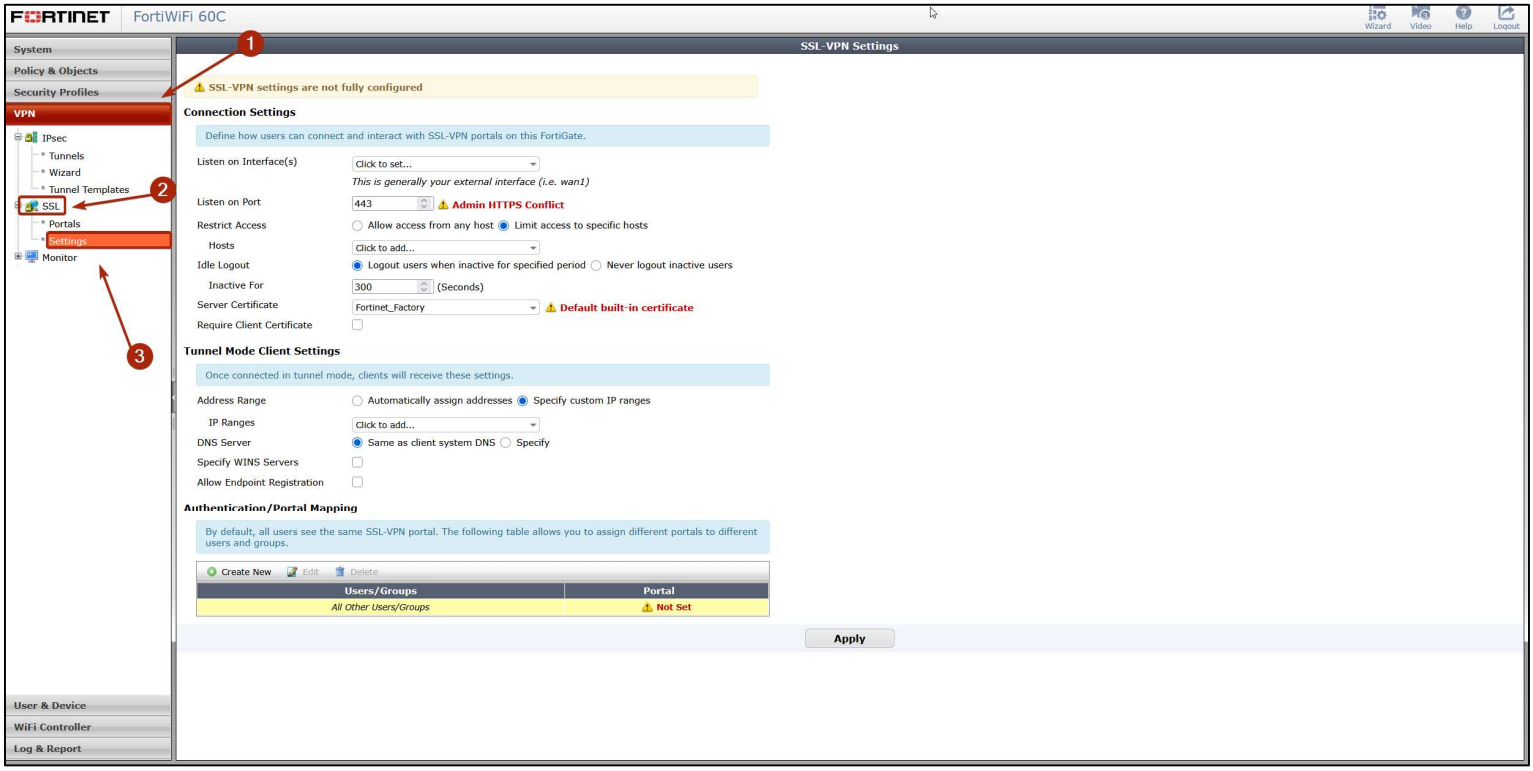
Valide avec y pour confirmer le redémarrage.

PARTIE 2 – CONFIGURATION DU SERVICE VPN DU FORTINET



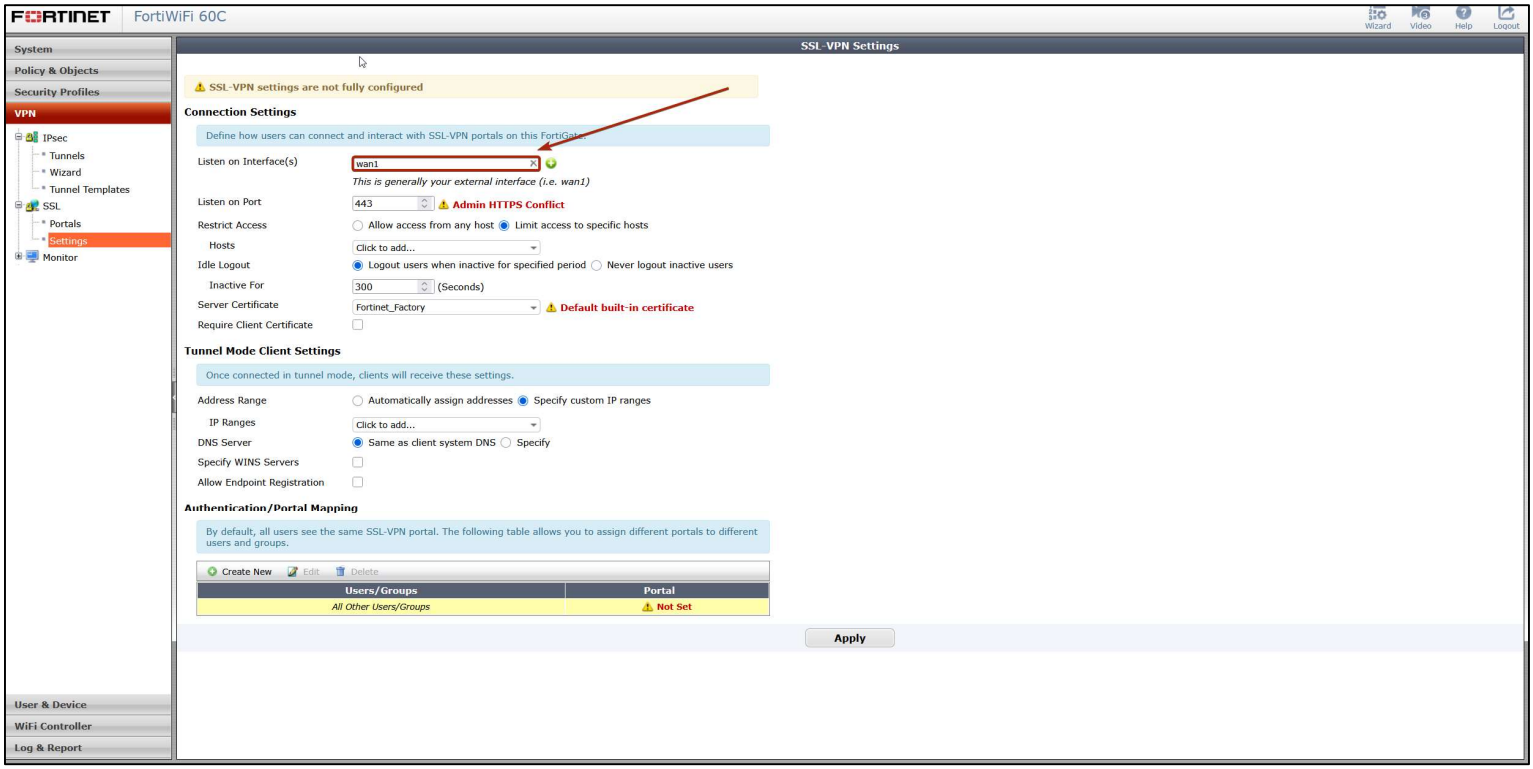
Étape 1 — Vérifie que le service FortiClient VPN est activé sur le FortiGate.
Dans **VPN → SSL-VPN Settings**
ou en CLI :

```
show vpn ssl settings
```



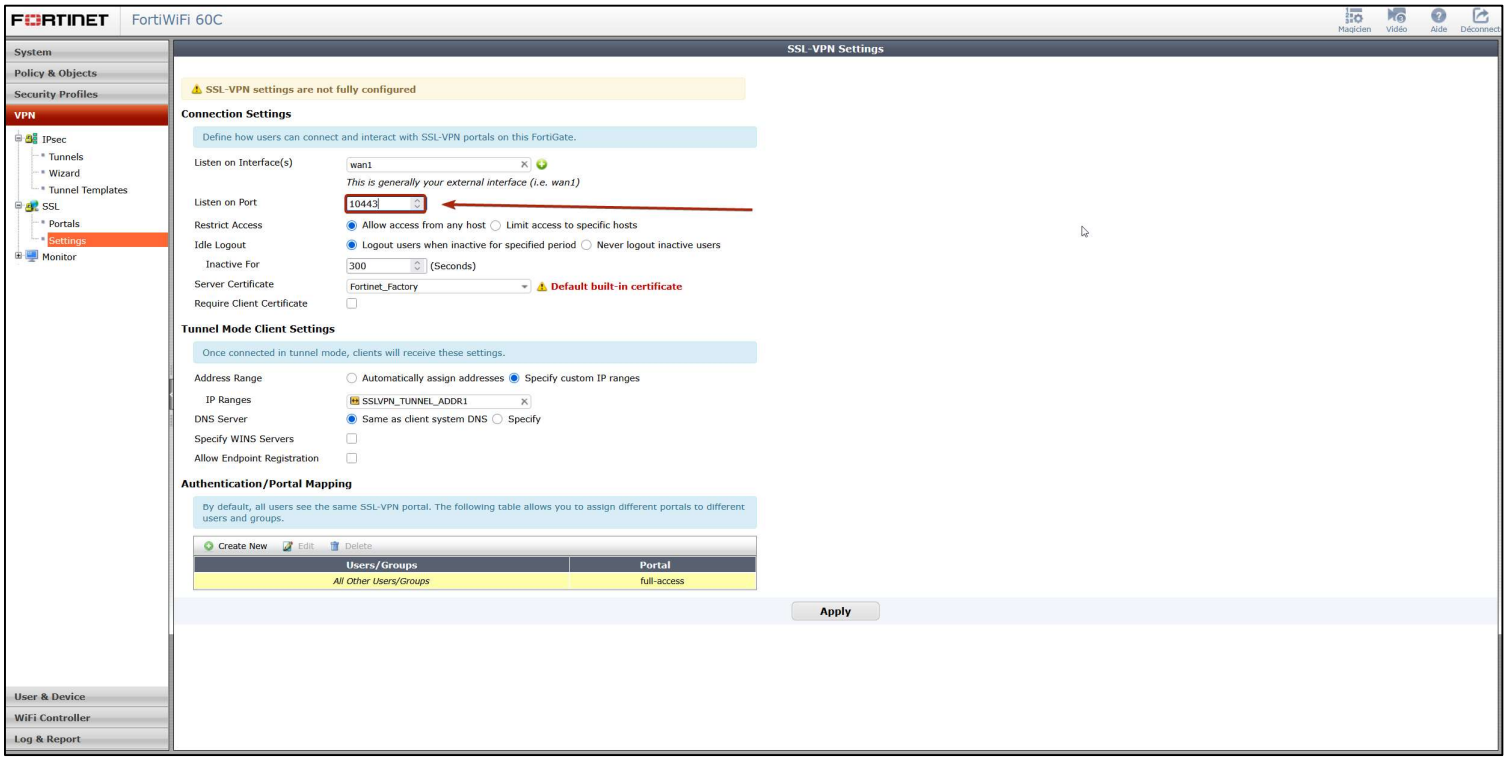
Étape 2 — Listen on Interface

Cliquer sur **"Click to set..."** à côté de **Listen on Interface(s)** et sélectionne ton interface WAN (probablement wan1).



Étape 3 — Changer le port d'écoute

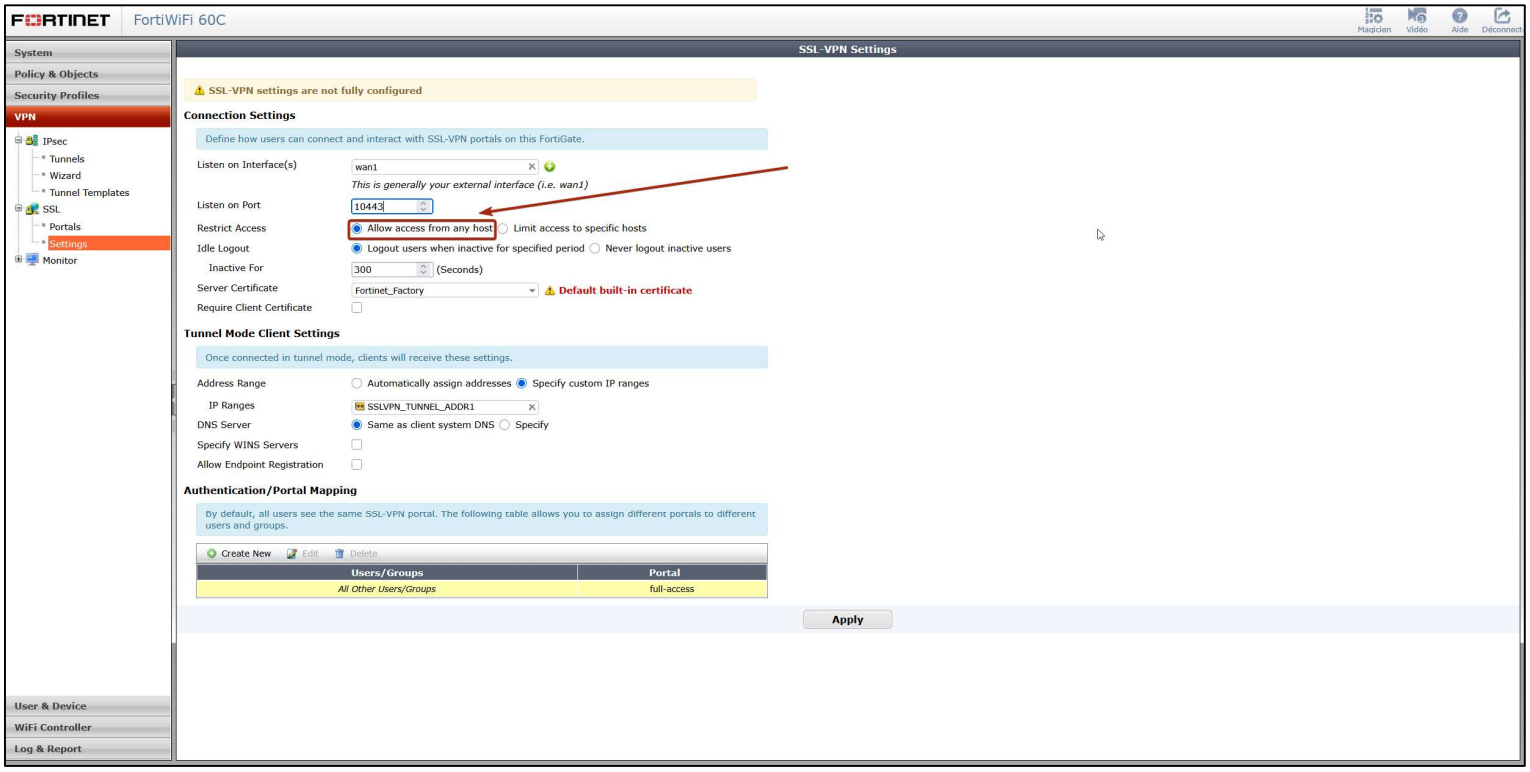
Le port **443 est en conflit** avec l'interface d'administration HTTPS. Il faut le changer. Dans le champ **Listen on Port**, remplace 443 par **10443** (port standard FortiClient, ou un autre port libre de ton choix).



Étape 4 — Restrict Access

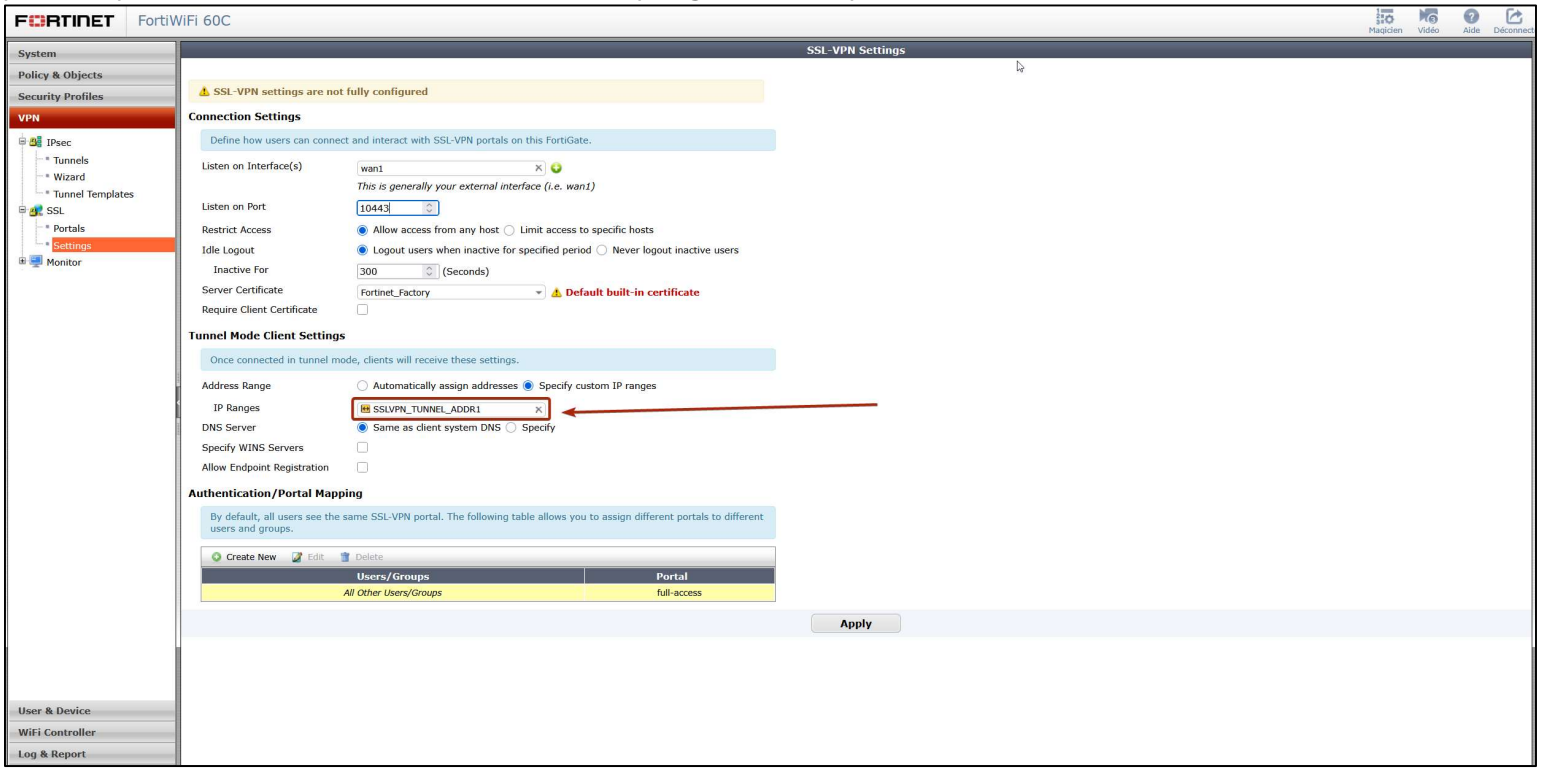
On peut voir **"Limit access to specific hosts"** est coché mais le champ **Hosts** est vide. Il faut soit :

- Sélectionner **"Allow access from any host"** ← plus simple pour commencer
- Ou ajouter une IP spécifique dans Hosts si tu veux restreindre l'accès



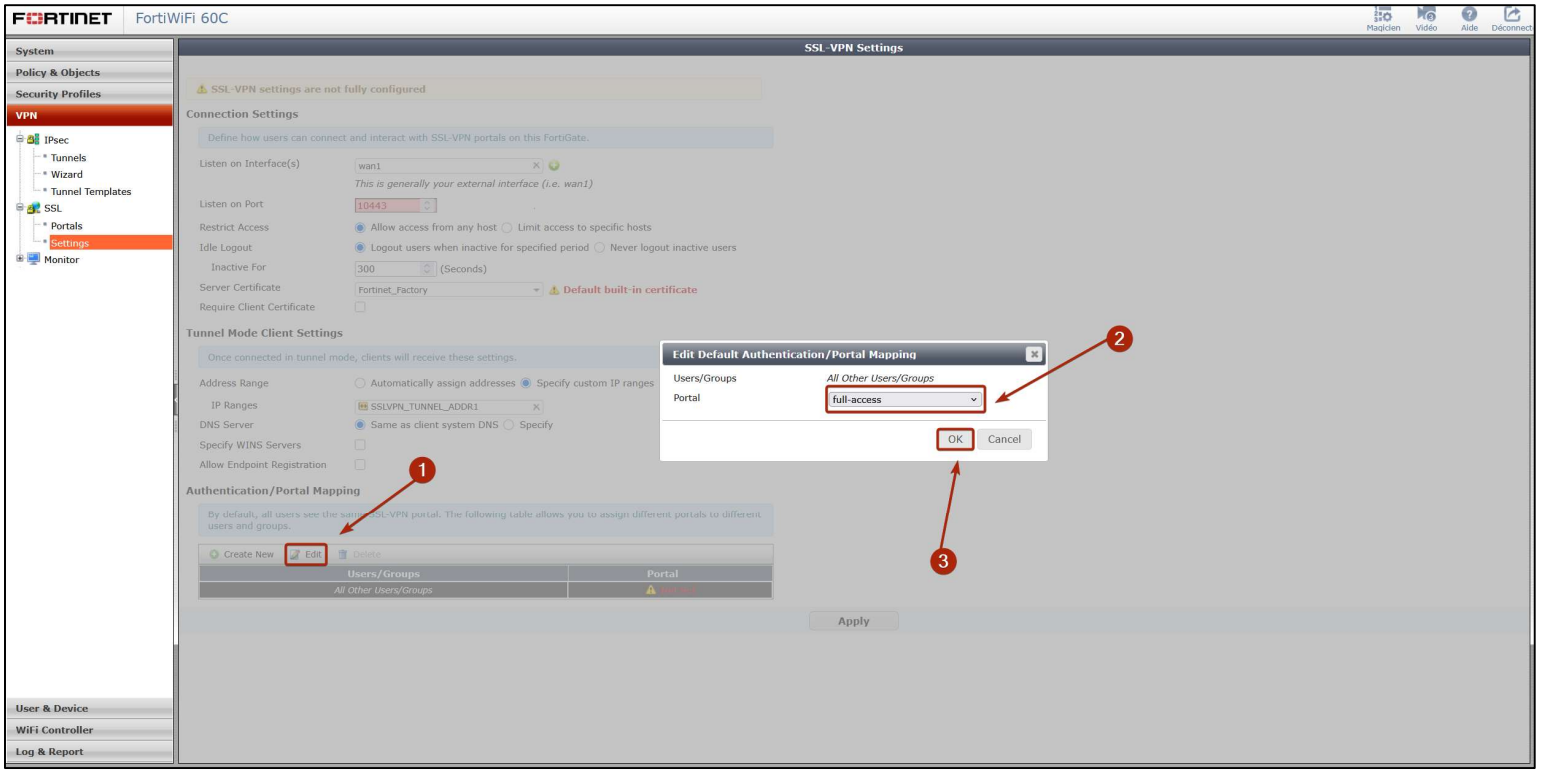
Étape 5 — IP Ranges (tunnel client)

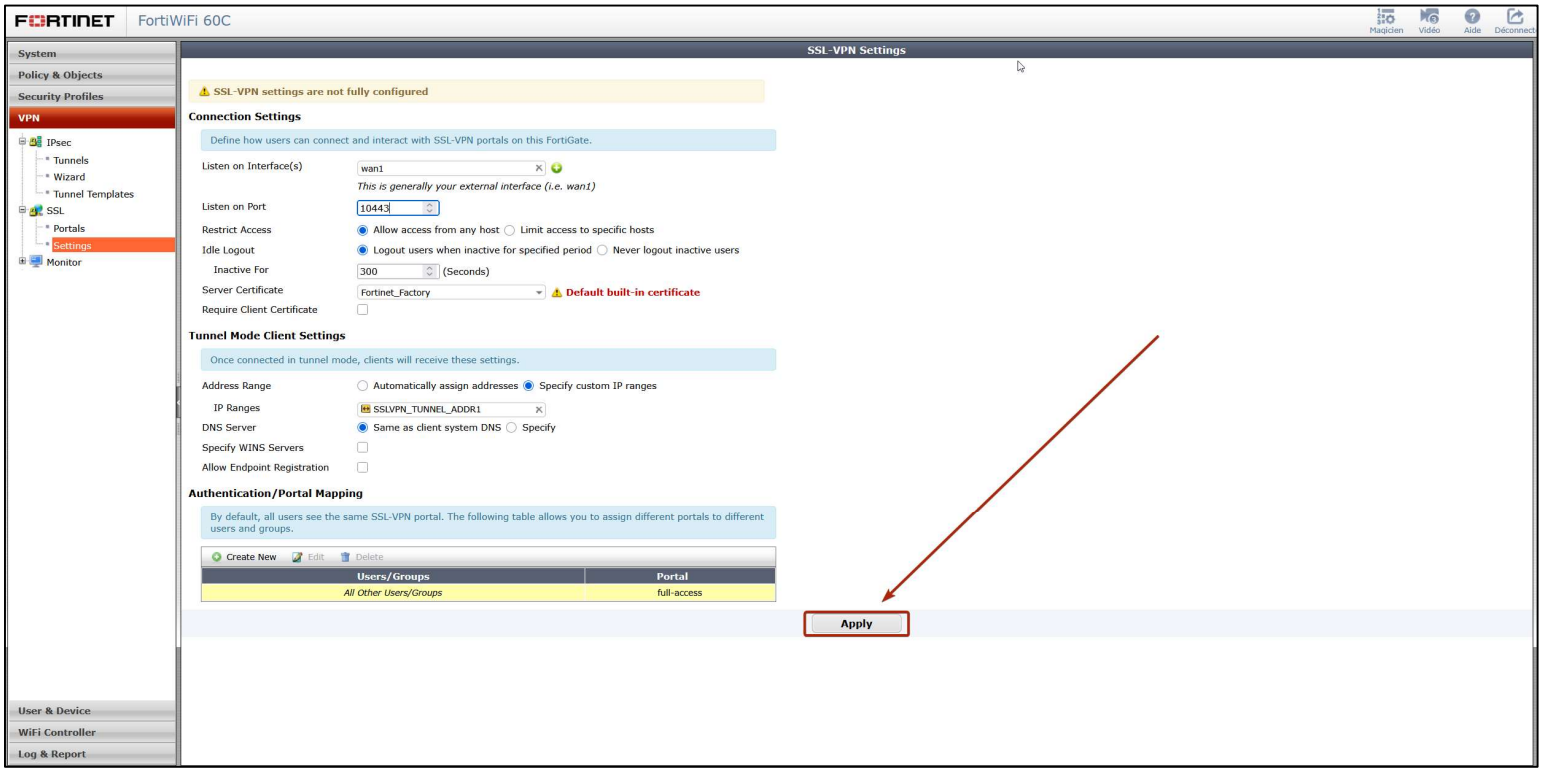
Dans **Tunnel Mode Client Settings**, cliquer sur **SSLVPN_TUNNEL_ADDR1** directement, c'est parfait pour commencer. On définira la plage exacte plus tard si besoin.



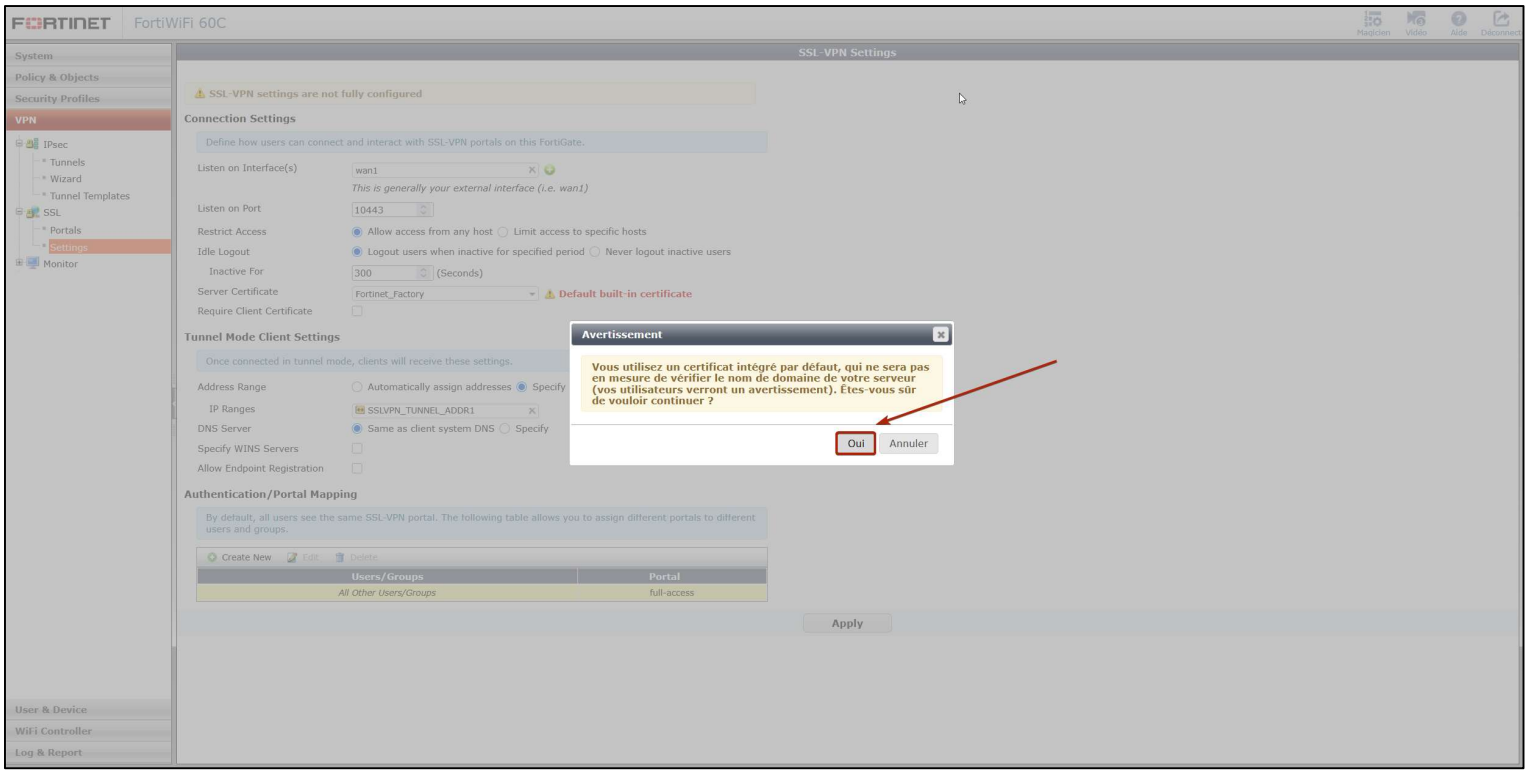
Étape 6 — Portal Mapping

Il reste le **"Not Set"** sur le portal. Clique sur la ligne **"All Other Users/Groups"** pour la sélectionner, puis clique sur **Edit**.
Dans la fenêtre qui s'ouvre, sélectionne le portal **full-access** dans le menu déroulant.



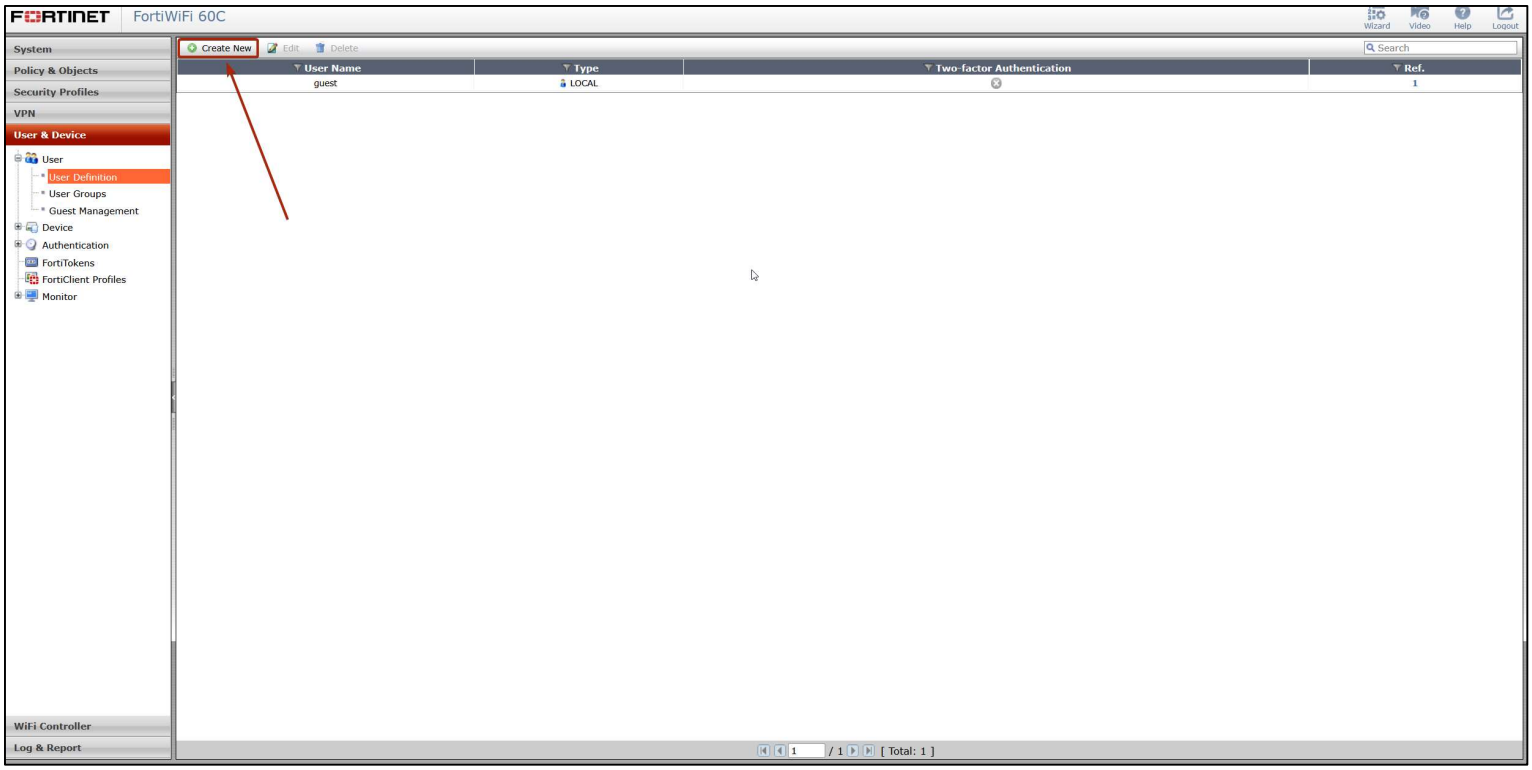


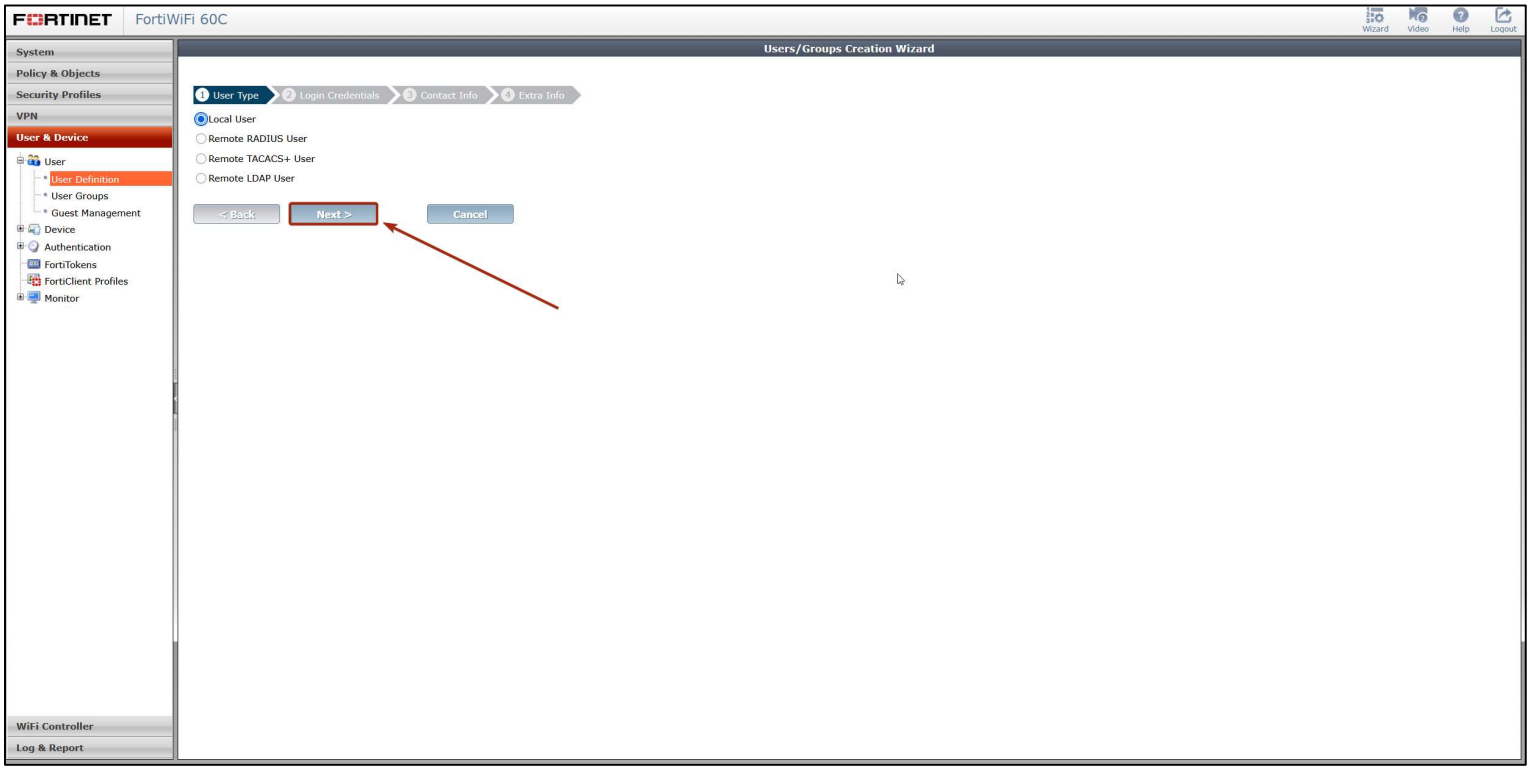
L'avertissement indique juste que le certificat par défaut **Fortinet_Factory** ne peut pas vérifier le nom de domaine — les utilisateurs verront un avertissement SSL dans FortiClient, c'est normal pour l'instant.
Cliquer sur **Oui** pour continuer.

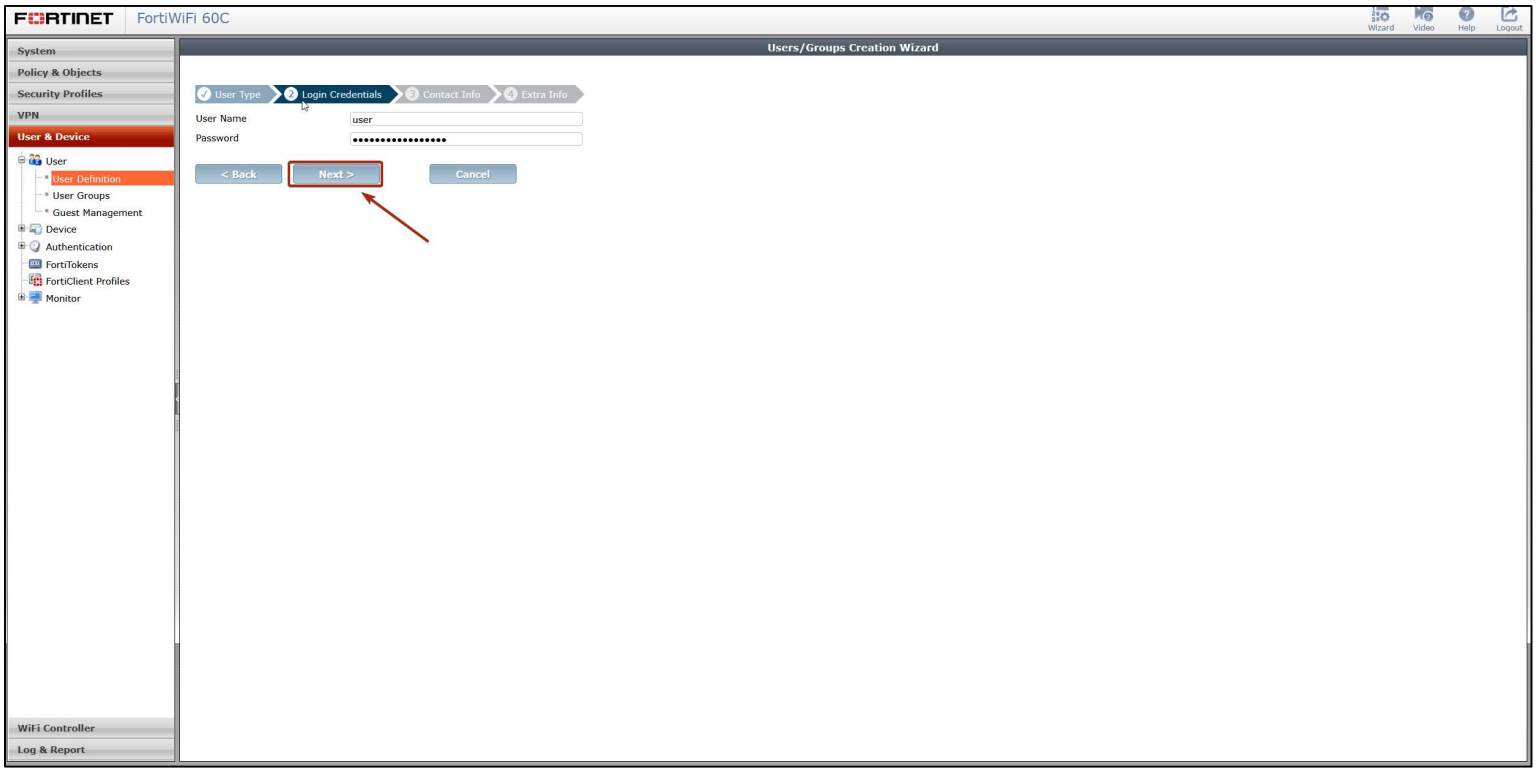


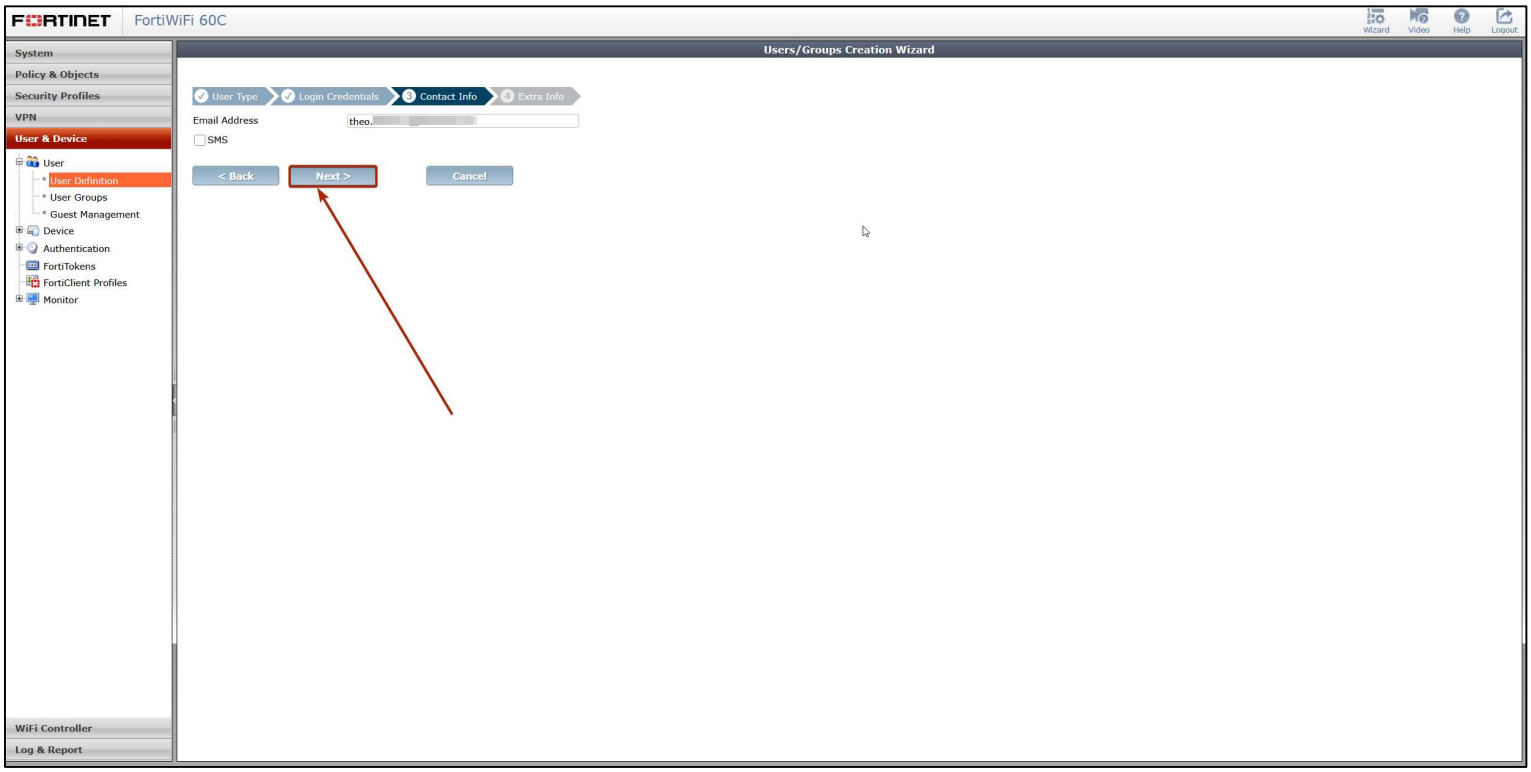
Étape 7 — Créer un utilisateur VPN

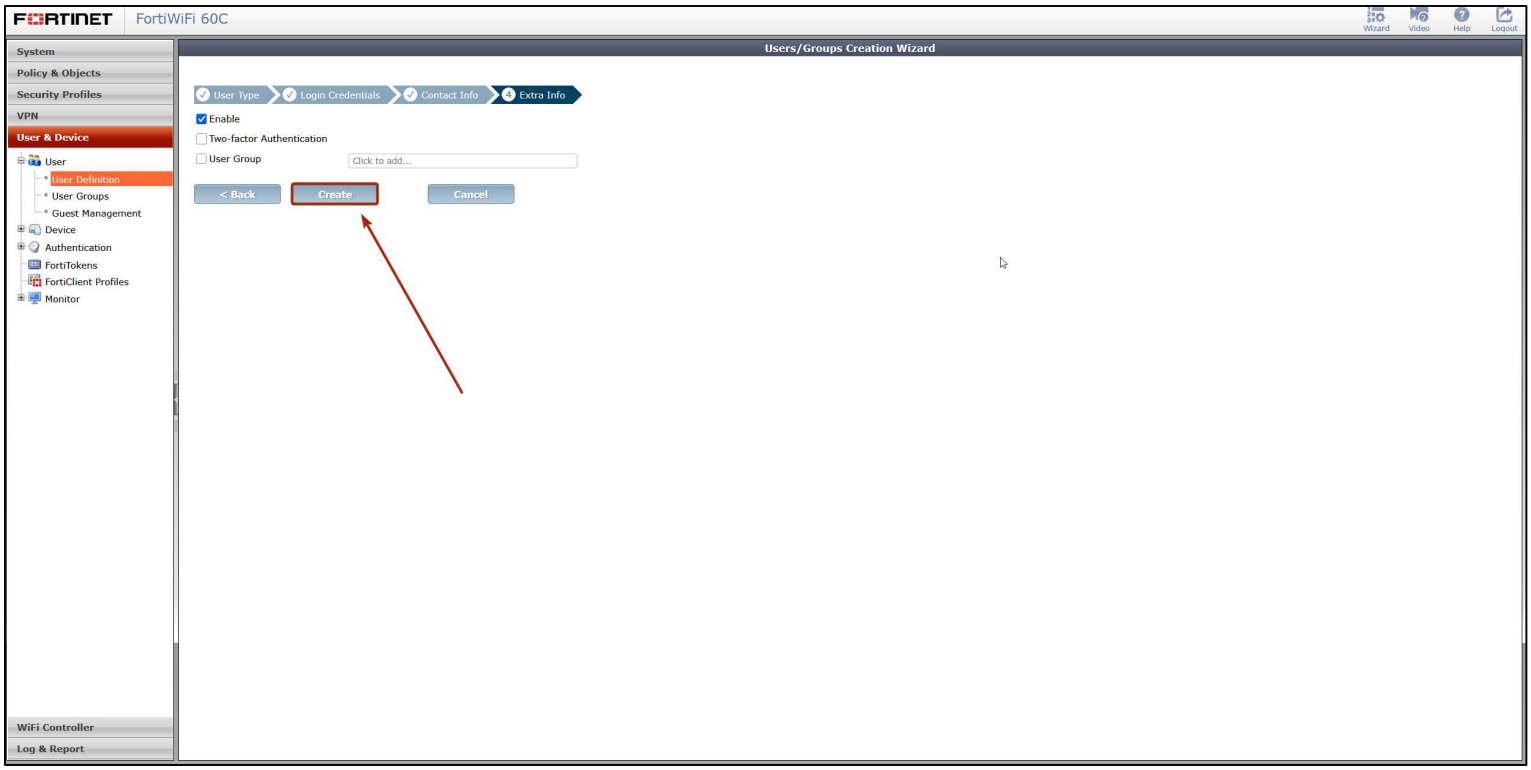
- Aller dans **User & Device → User Definition**
- Cliquer sur **Create New**
- Choisissez **Local User**
- Remplis :
- **Username** : le nom que tu veux (ex: vpnuser)
- **Password** : un mot de passe solide
- Clique **Next** jusqu'à la fin et **Submit**

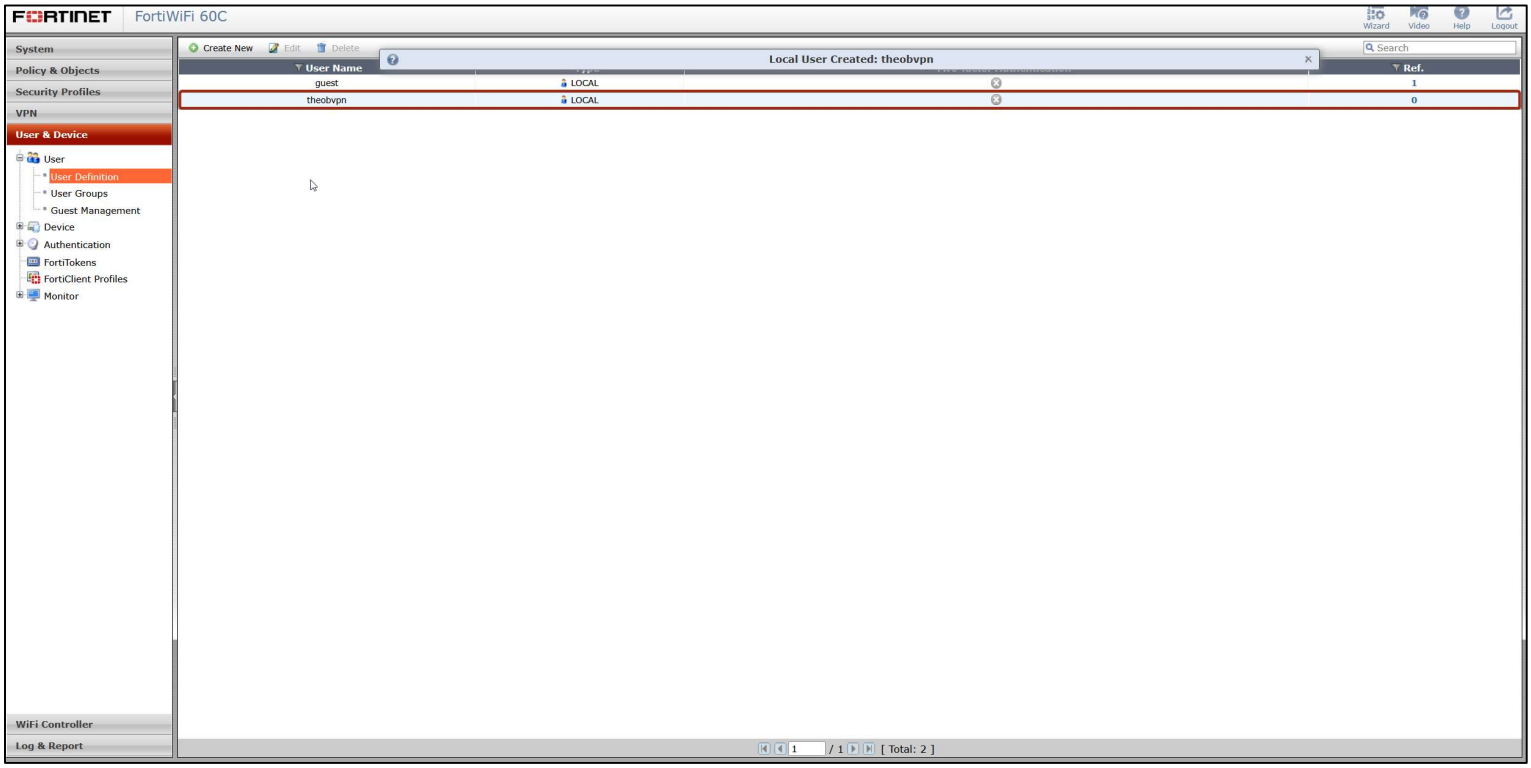

FORTINET
FortiWiFi 60C
Wizard
Video
Help
Logout
System
Policy & Objects
Security Profiles
VPN
User & Device
User
User Definition
User Groups
Guest Management
Device
Authentication
FortiTokens
FortiClient Profiles
Monitor
WiFi Controller
Log & Report
Create New
Edit
Delete
Search
User Name
Type
Two-factor Authentication
Ref.
guest
LOCAL
1
1
/ 1
[Total: 1]


FORTINET
FortiWiFi 60C
Wizard
Video
Help
Logout
System
Policy & Objects
Security Profiles
VPN
User & Device
User
User Definition
User Groups
Guest Management
Device
Authentication
FortiTokens
FortiClient Profiles
Monitor
WiFi Controller
Log & Report
Users/Groups Creation Wizard
1 User Type
2 Login Credentials
3 Contact Info
4 Extra Info
Local User
Remote RADIUS User
Remote TACACS+ User
Remote LDAP User
< Back
Next >
Cancel


FORTINET
FortiWiFi 60C
Wizard
Video
Help
Logout
System
Policy & Objects
Security Profiles
VPN
User & Device
User
User Definition
User Groups
Guest Management
Device
Authentication
FortiTokens
FortiClient Profiles
Monitor
WiFi Controller
Log & Report
Users/Groups Creation Wizard
User Type
Login Credentials
Contact Info
Extra Info
User Name
user
Password
< Back
Next >
Cancel

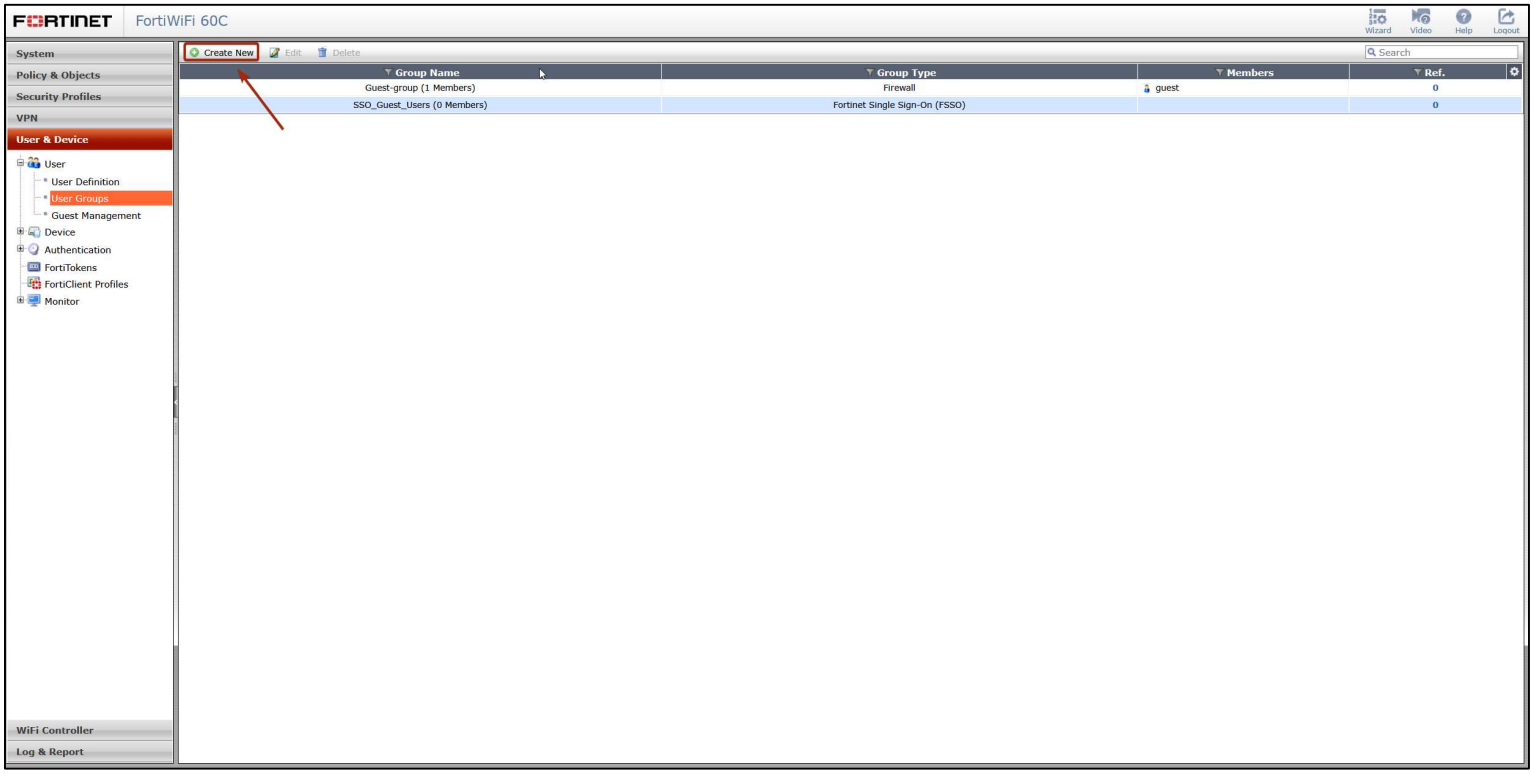

FORTINET
FortiWiFi 60C
Wizard
Video
Help
Logout
System
Policy & Objects
Security Profiles
VPN
User & Device
User
User Definition
User Groups
Guest Management
Device
Authentication
FortiTokens
FortiClient Profiles
Monitor
WiFi Controller
Log & Report
Users/Groups Creation Wizard
User Type
Login Credentials
Contact Info
Extra Info
Email Address
theo.
SMS
< Back
Next >
Cancel

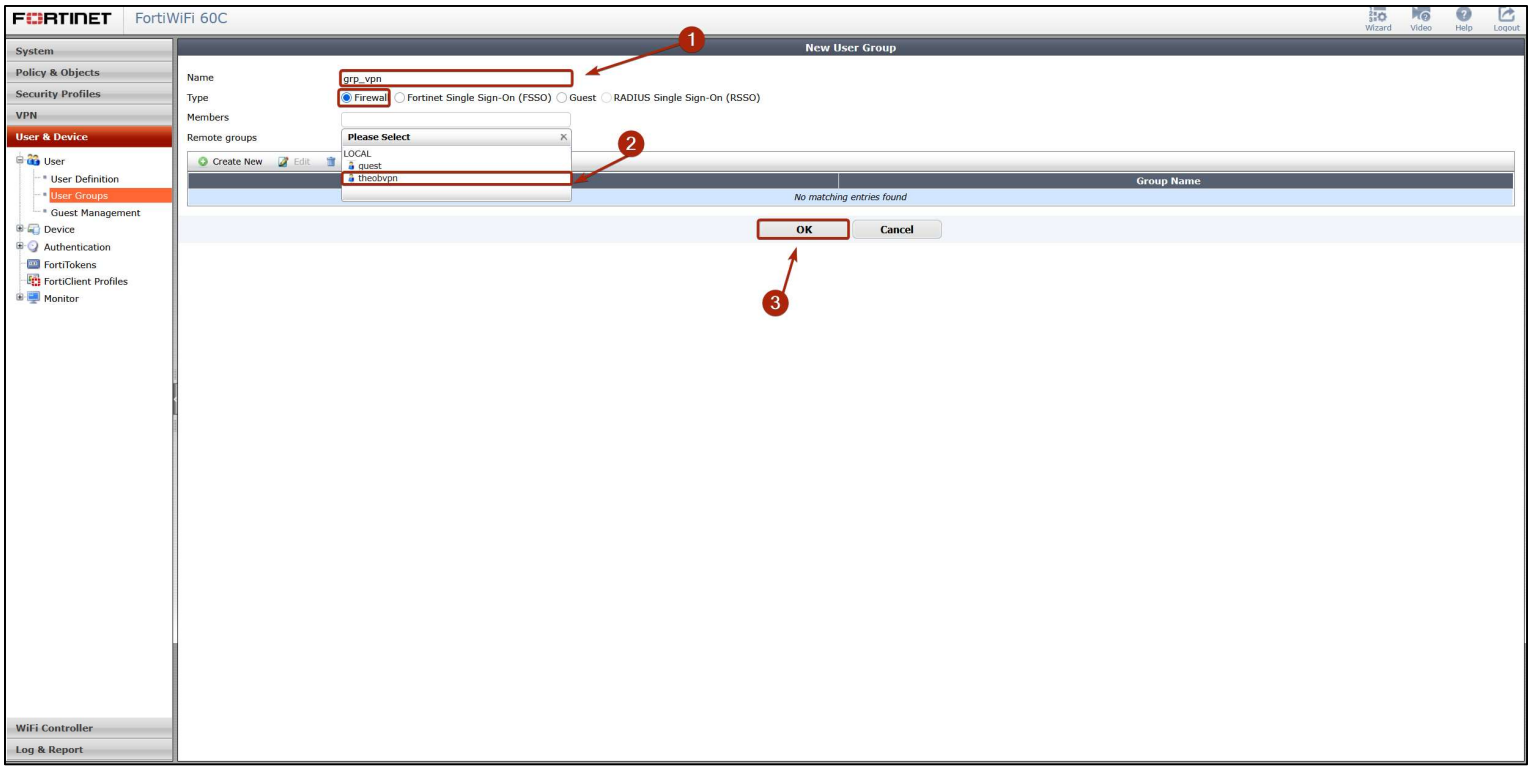

FORTINET
FortiWiFi 60C
Wizard
Video
Help
Logout
System
Policy & Objects
Security Profiles
VPN
User & Device
User
User Definition
User Groups
Guest Management
Device
Authentication
FortiTokens
FortiClient Profiles
Monitor
WiFi Controller
Log & Report
Users/Groups Creation Wizard
User Type
Login Credentials
Contact Info
4 Extra Info
Enable
Two-factor Authentication
User Group
Click to add...
< Back
Create
Cancel

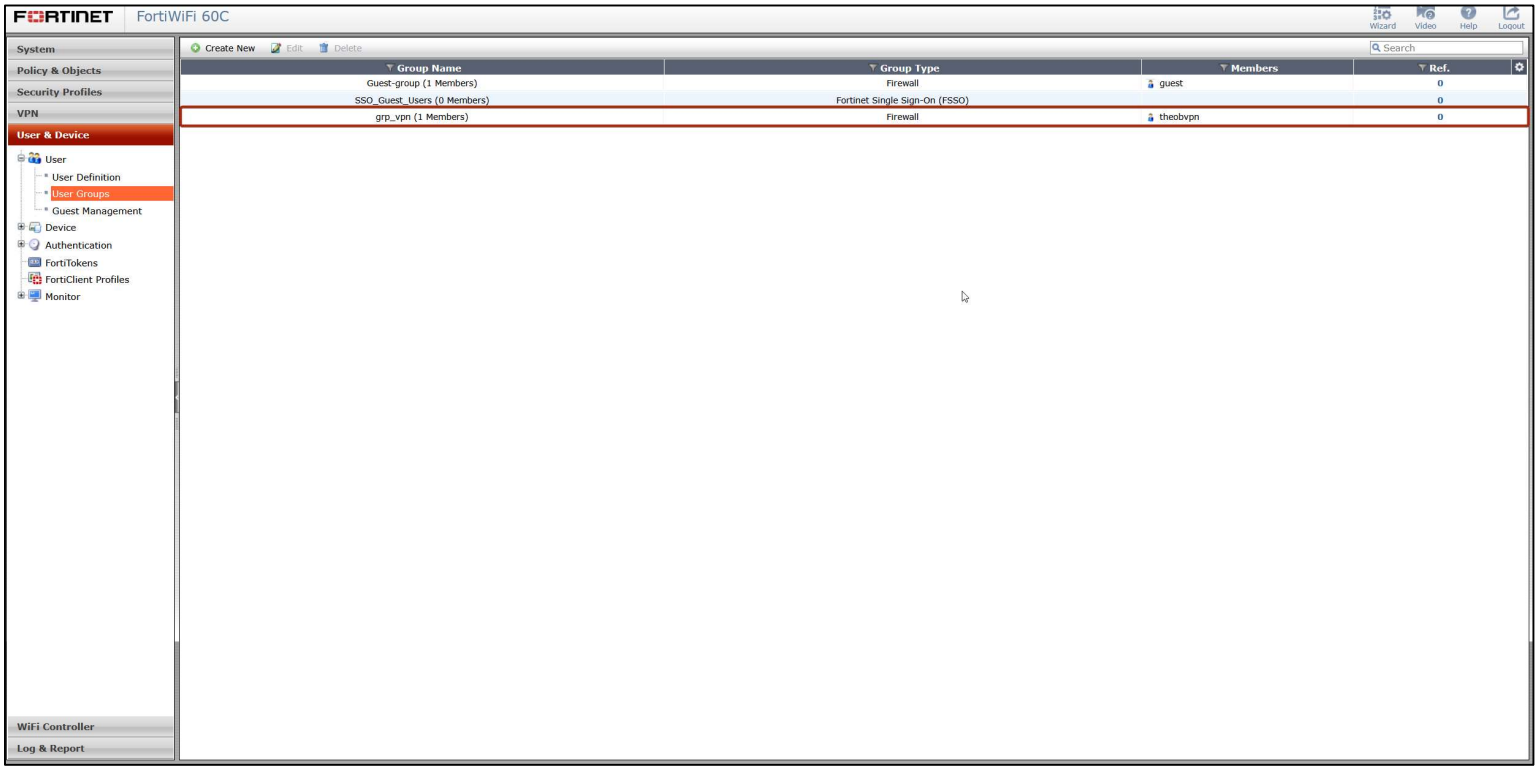

FORTINET
FortiWiFi 60C
Wizard
Video
Help
Logout
System
Policy & Objects
Security Profiles
VPN
User & Device
User
User Definition
User Groups
Guest Management
Device
Authentication
FortiTokens
FortiClient Profiles
Monitor
WiFi Controller
Log & Report
Create New
Edit
Delete
Search
Local User Created: theobvpn
User Name
Ref.
guest
LOCAL
1
theobvpn
LOCAL
0
1
/ 1
[Total: 2]

Étape 8 — Créer un groupe d'utilisateurs VPN
Avant la politique de pare-feu, il faut mettre l'utilisateur dans un groupe. Va dans **User & Device → User Groups** :

- Cliquer sur **Create New**
- **Name** : grp_vpn
- **Type** : Firewall
- Dans **Members**, clique sur **+** et ajoute theobvpn
- Clique **OK**



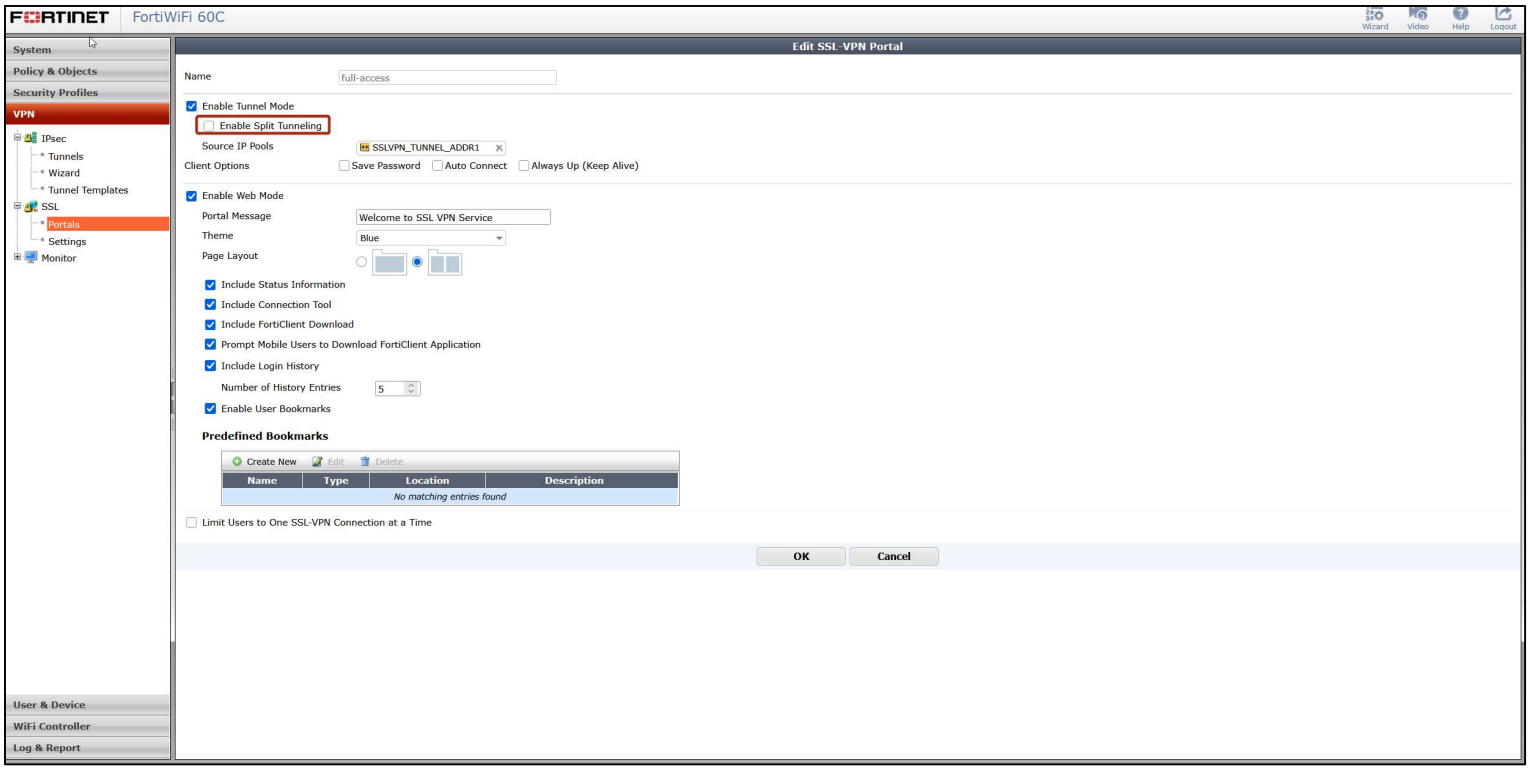




Étape 9 — Créer la politique de pare-feu SSL-VPN

Avant, aller **dans VPN → SSL-VPN Portals → full-access :**

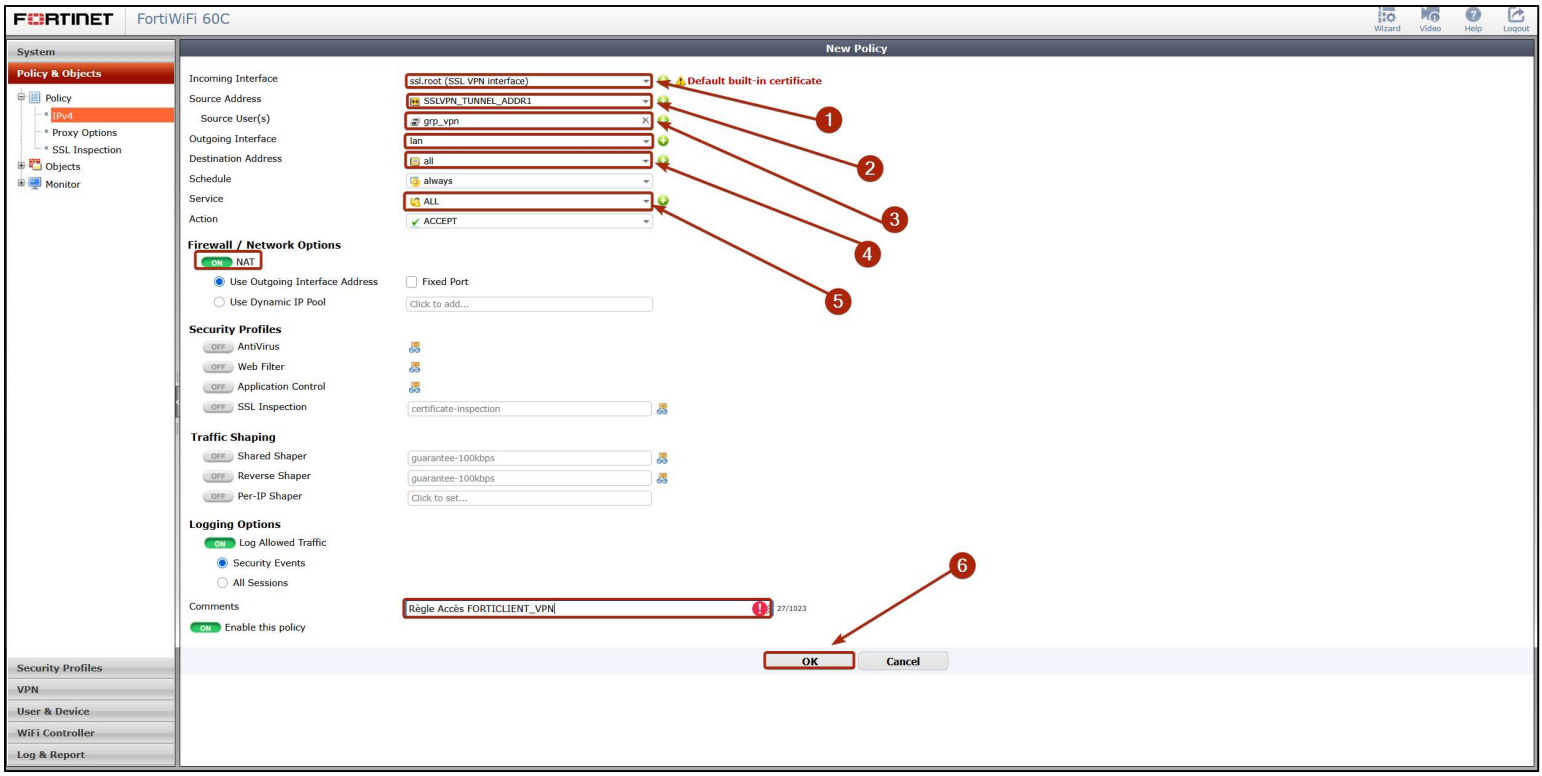
- Double-clique sur **full-access**
- Trouve l'option **Split Tunneling**
- Mets-la sur **Disabled**
- Clique **OK**

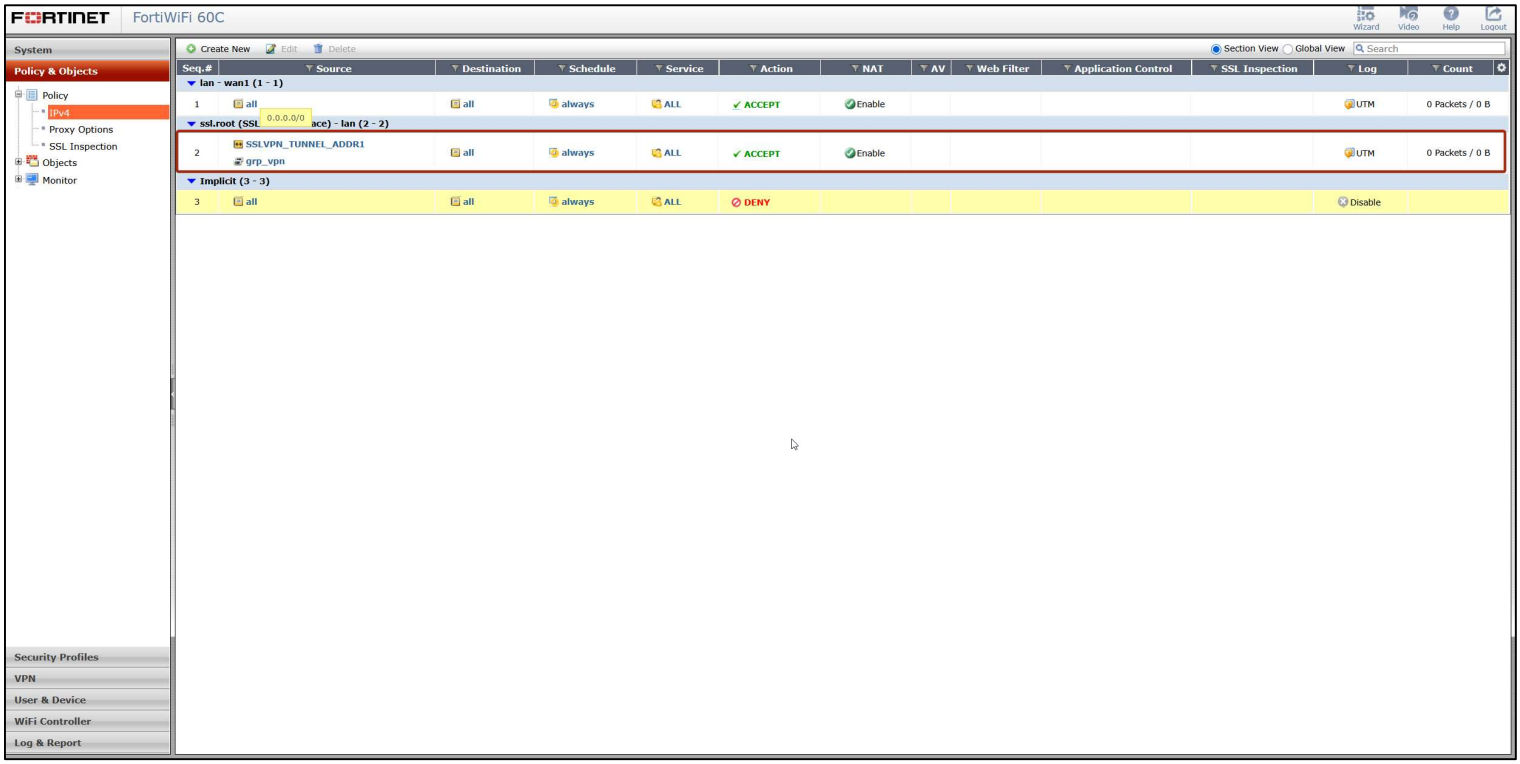


Va dans **Policy & Objects → Firewall Policy** puis **Create New** et remplis ainsi :

Champ	Valeur
Name	VPN_to_LAN
Incoming Interface	ssl.root
Outgoing Interface	lan (ou ton interface interne)
Source	SSLVPN_TUNNEL_ADDR1 + grp_vpn
Destination	all
Service	ALL
Action	ACCEPT

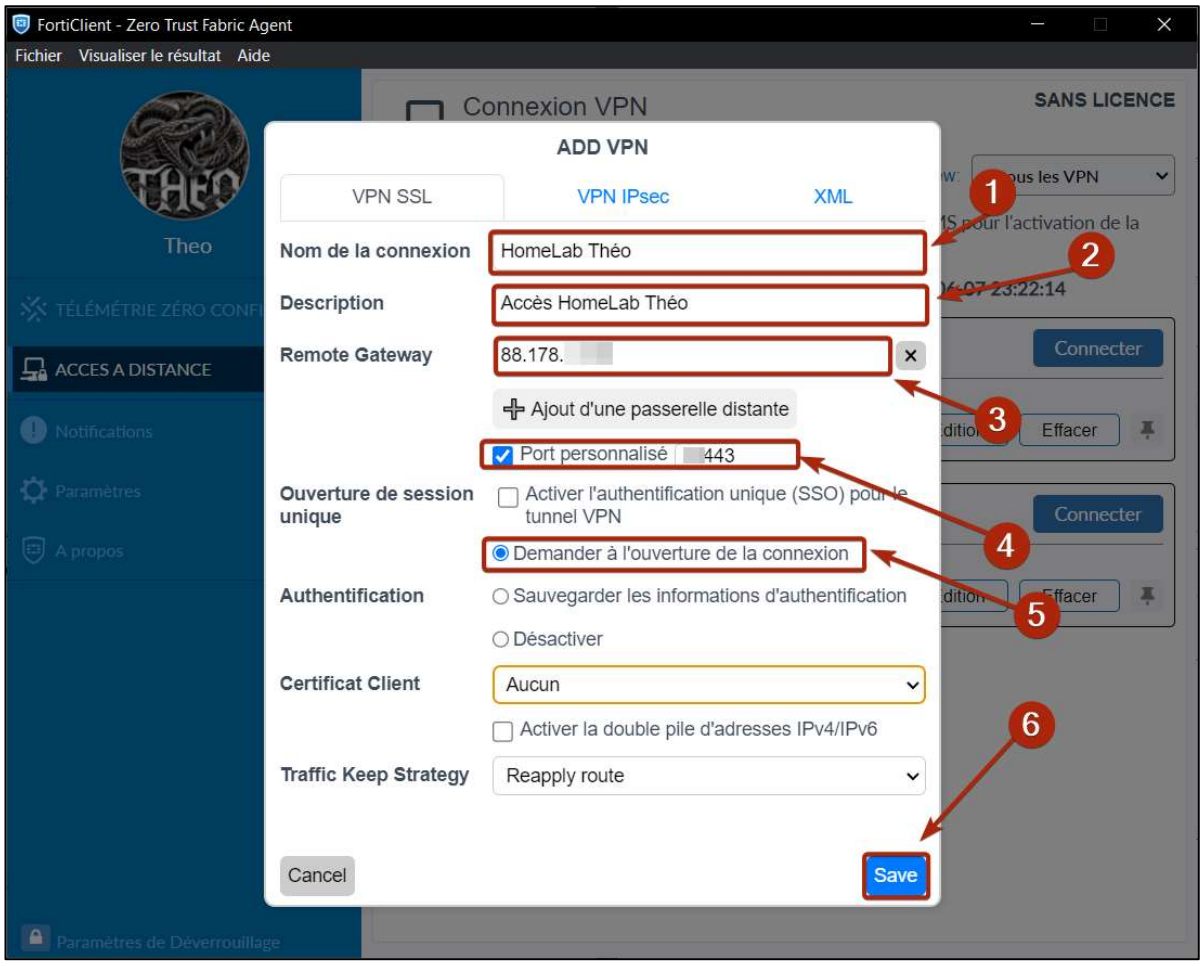
Pour ajouter **deux sources** (l'adresse ET le groupe), clique sur le **+** dans le champ Source et ajoute les deux.
Cliquer **OK** quand c'est fait et envoie une capture !

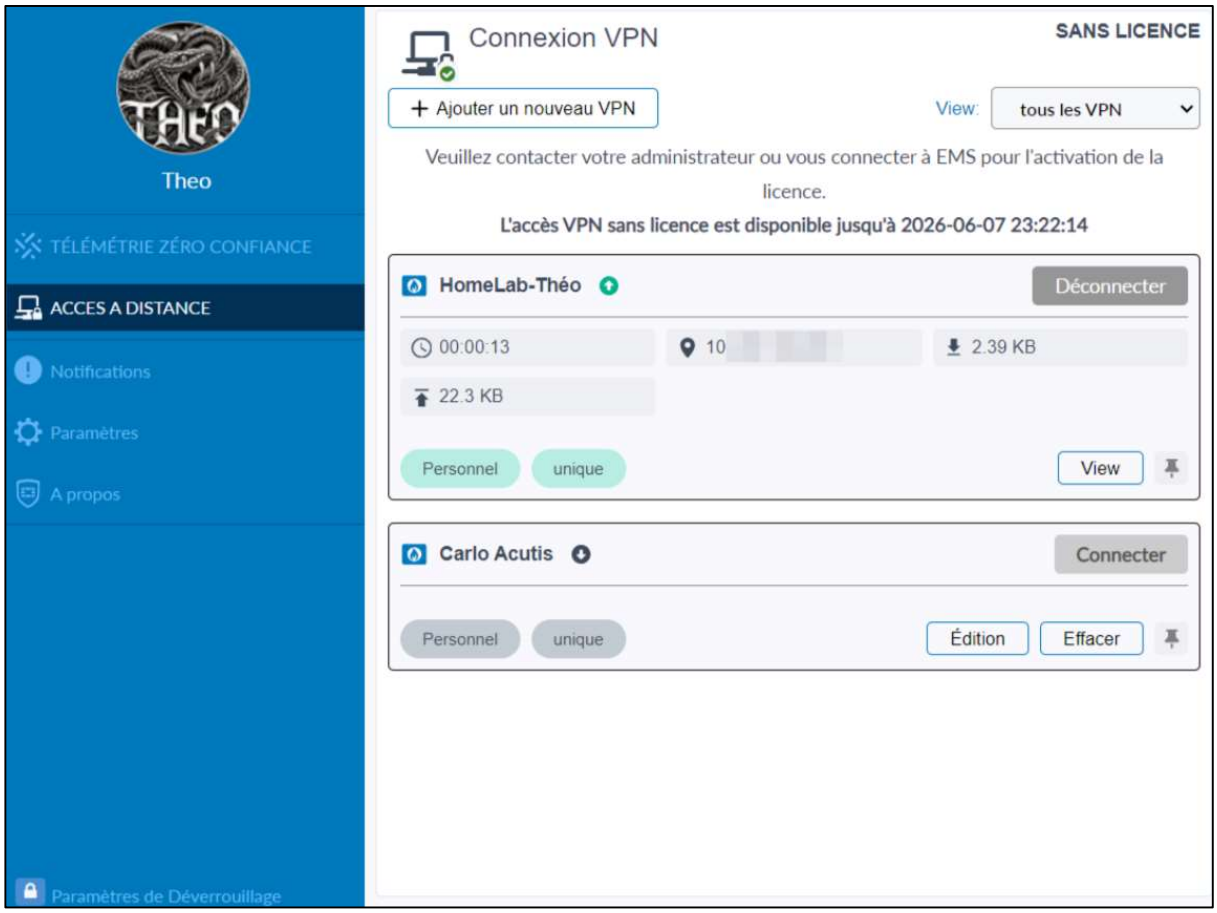

FORTINET
FortiWiFi 60C
Wizard
Video
Help
Logout
System
Policy & Objects
Policy
IPv4
Proxy Options
SSL Inspection
Objects
Monitor
Security Profiles
VPN
User & Device
WiFi Controller
Log & Report
New Policy
Incoming Interface
ssl.root (SSL VPN interface)
Default built-in certificate
Source Address
SSLVPN_TUNNEL_ADDR1
Source User(s)
grp_vpn
Outgoing Interface
lan
Destination Address
all
Schedule
always
Service
ALL
Action
ACCEPT
Firewall / Network Options
NAT
Use Outgoing Interface Address
Fixed Port
Use Dynamic IP Pool
Click to add...
Security Profiles
AntiVirus
Web Filter
Application Control
SSL Inspection
certificate-inspection
Traffic Shaping
Shared Shaper
guarantee-100kbps
Reverse Shaper
guarantee-100kbps
Per-IP Shaper
Click to set...
Logging Options
Log Allowed Traffic
Security Events
All Sessions
Comments
Règle Accès FORTICLIENT_VPN
27/1023
Enable this policy
OK
Cancel
1
2
3
4
5
6


FORTINET
FortiWiFi 60C
Wizard
Video
Help
Logout
System
Policy & Objects
Policy
IPv4
Proxy Options
SSL Inspection
Objects
Monitor
Security Profiles
VPN
User & Device
WiFi Controller
Log & Report
Create New
Edit
Delete
Section View
Global View
Search
Seq.#
Source
Destination
Schedule
Service
Action
NAT
AV
Web Filter
Application Control
SSL Inspection
Log
Count
lan - wan1 (1 - 1)
1
all
all
always
ALL
ACCEPT
Enable
UTM
0 Packets / 0 B
ssl.root (SSL
0.0.0.0/0
ace) - lan (2 - 2)
2
SSLVPN_TUNNEL_ADDR1
grp_vpn
all
always
ALL
ACCEPT
Enable
UTM
0 Packets / 0 B
Implicit (3 - 3)
3
all
all
always
ALL
DENY
Disable

Étape 10 — Configurer FortiClient VPN sur le PC client

- Ouvre **FortiClient VPN**
- Clique sur **Configure VPN**
- Remplis :
- **Connection Name** : VPN-Théo (ce que tu veux)
- **Remote Gateway** : l'**IP WAN** du réseau (l'IP publique de ta box/routeur)
- **Port** : 10443
- **Client Certificate** : None
- Clique **Save**
- Entre le **Username** : theobvpn et ton mot de passe
- Clique **Connect**




Theo
TÉLÉMÉTRIE ZÉRO CONFIANCE
ACCES A DISTANCE
Notifications
Paramètres
A propos
Paramètres de Déverrouillage
Connexion VPN
SANS LICENCE
+ Ajouter un nouveau VPN
View:
tous les VPN
Veuillez contacter votre administrateur ou vous connecter à EMS pour l'activation de la licence.
L'accès VPN sans licence est disponible jusqu'à 2026-06-07 23:22:14
HomeLab-Théo
Déconnecter
00:00:13
10
2.39 KB
22.3 KB
Personnel
unique
View
Carlo Acutis
Connecter
Personnel
unique
Édition
Effacer