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.

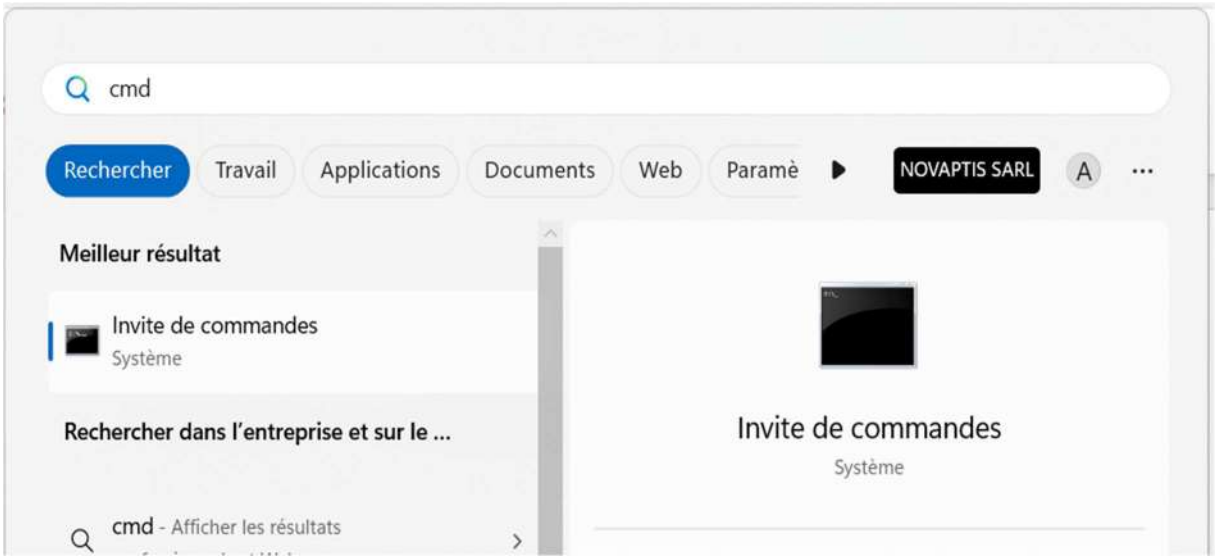
Le VPN SSL est basé sur le protocole SSL/TLS, principalement utilisé par accéder à des ressources web à distance de manière sécurisé.

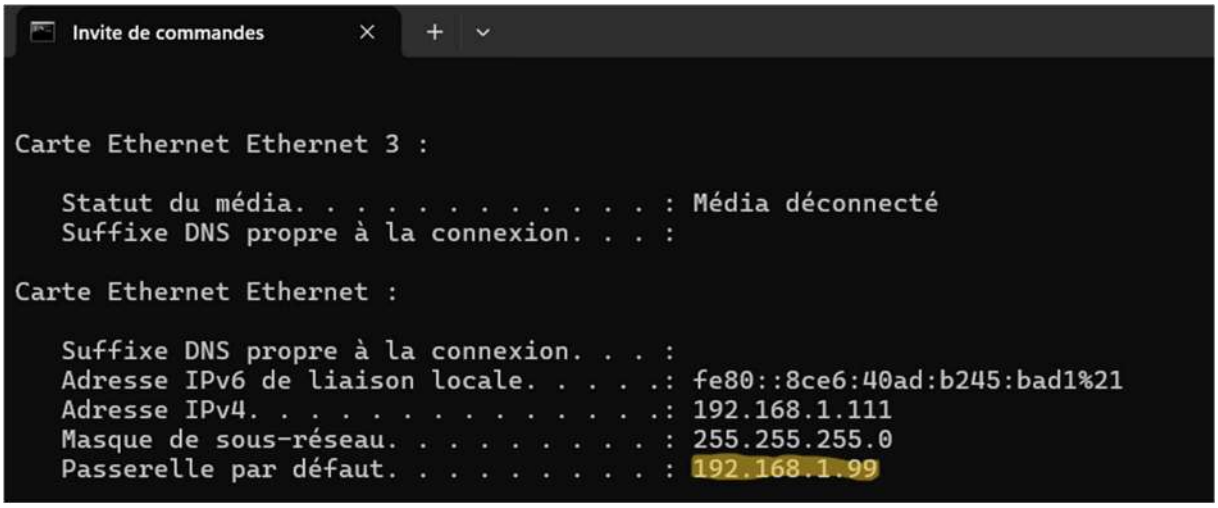
Comparé à IPsec le protocole SSL/TLS de crypte pas la couche réseau, il a donc une couche de sécurité en moins mais reste sécurisé pour acheminer les paquets entre le client et le serveur VPN.

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 :

Ouvrir une console et taper « ipconfig »

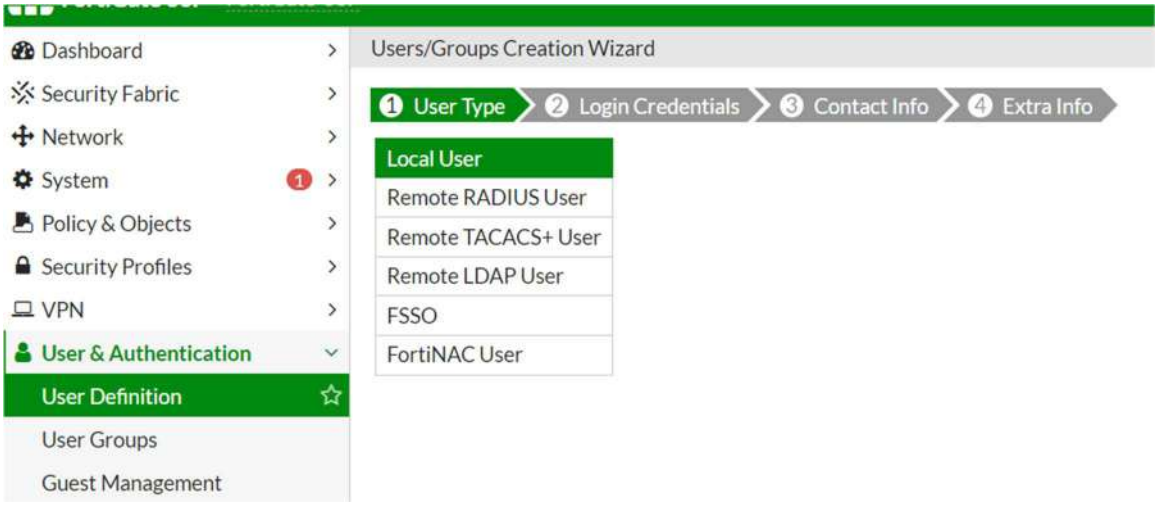




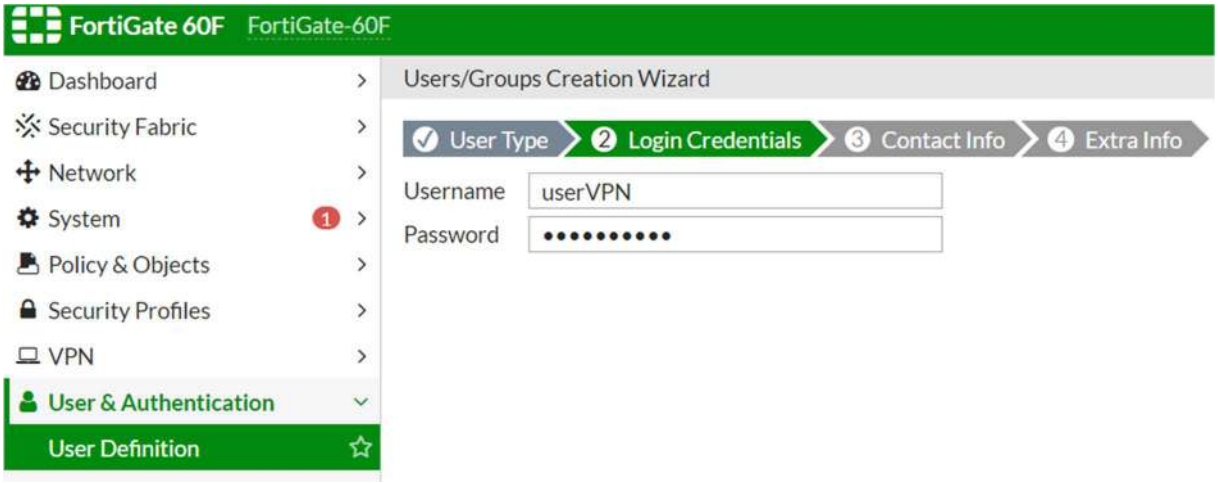
L'IP du routeur apparait, on peut la copier dans un navigateur, et se connecter avec ses identifiants d'administrateur.

1/ Définir un compte utilisateur local

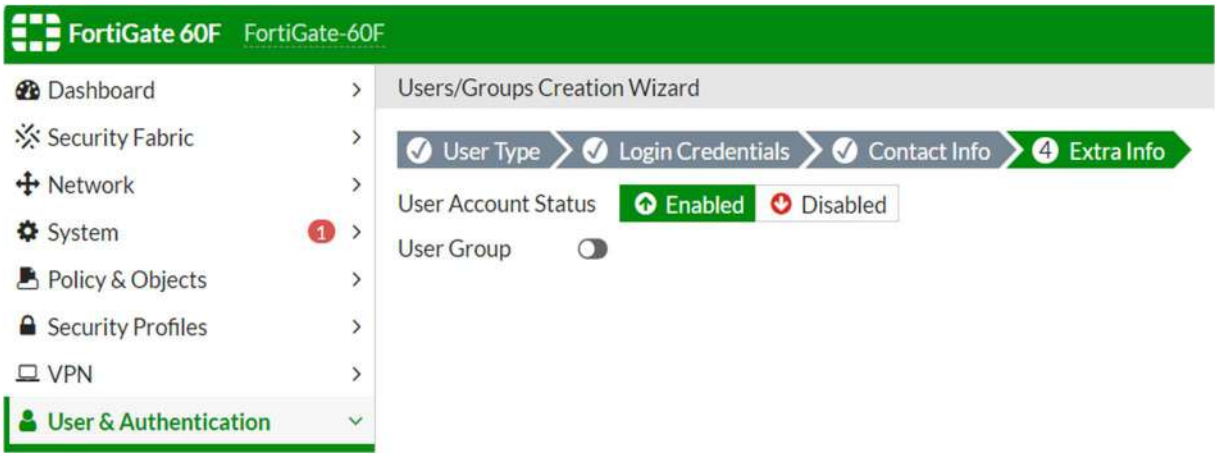
Le VPN-SSL en tant que VPN nomade demande une connexion de l'utilisateur distant. De ce fait la première chose à faire et de définir un compte local dans le routeur que l'on configurera plus tard lors de la configuration VPN pour l'autoriser à effectuer une connexion distante au VPN.



On crée un nouvel utilisateur local et ses identifiants.



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

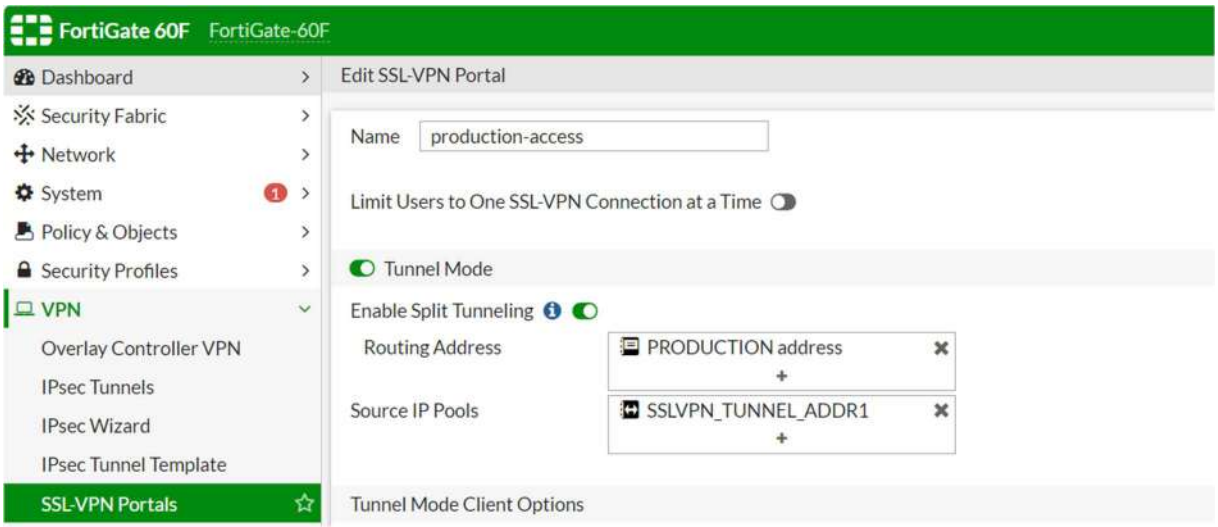


2/ Configuration Portail VPN-SSL et paramètres

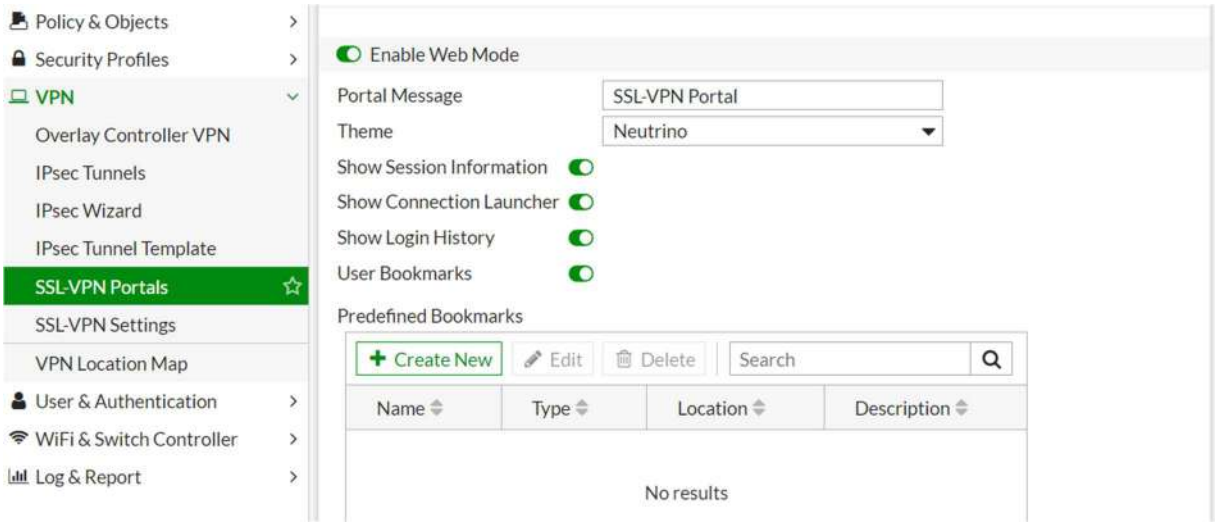
Dans VPN : SSL-VPN Portals :

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.

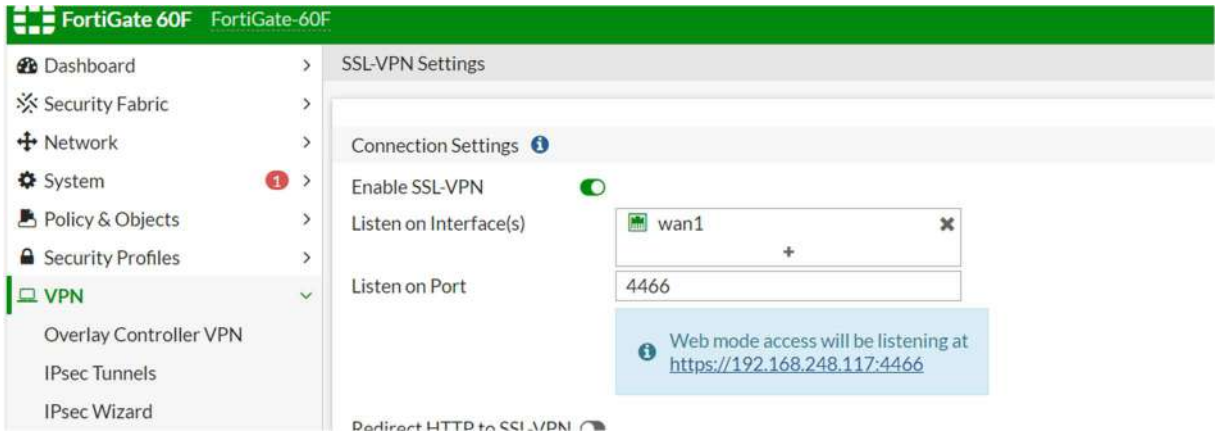
On active le split tunneling si on souhaite rediriger uniquement le trafic nécessaire vers le VPN, et utiliser notre connexion par défaut pour naviguer sur internet par exemple.



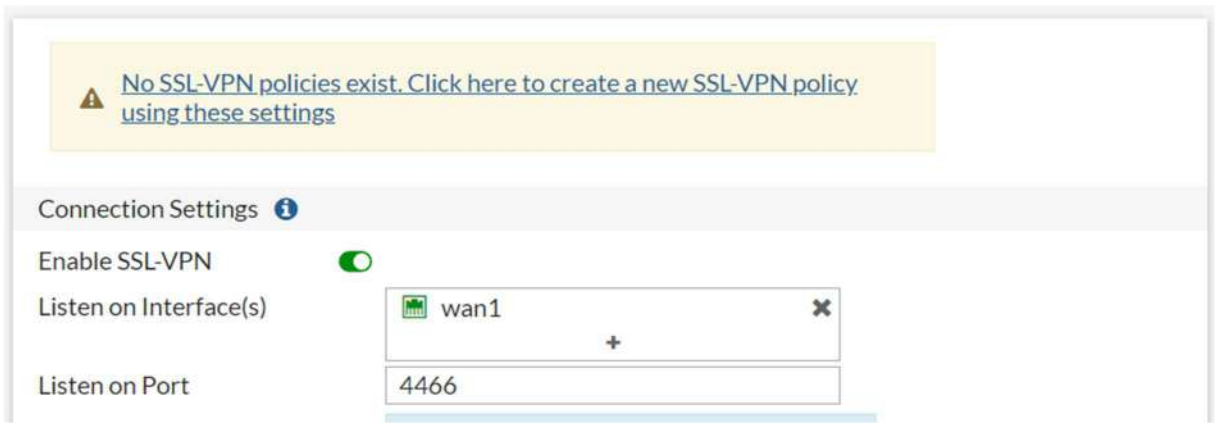
On peut activer le mode Web afin de pouvoir accéder facilement à une interface web pour se connecter au VPN en entrant dans un navigateur l'adresse IP publique du routeur distant. Cette étape n'est pas obligatoire puisque l'on peut s'y connecter directement depuis l'application FortiClient.



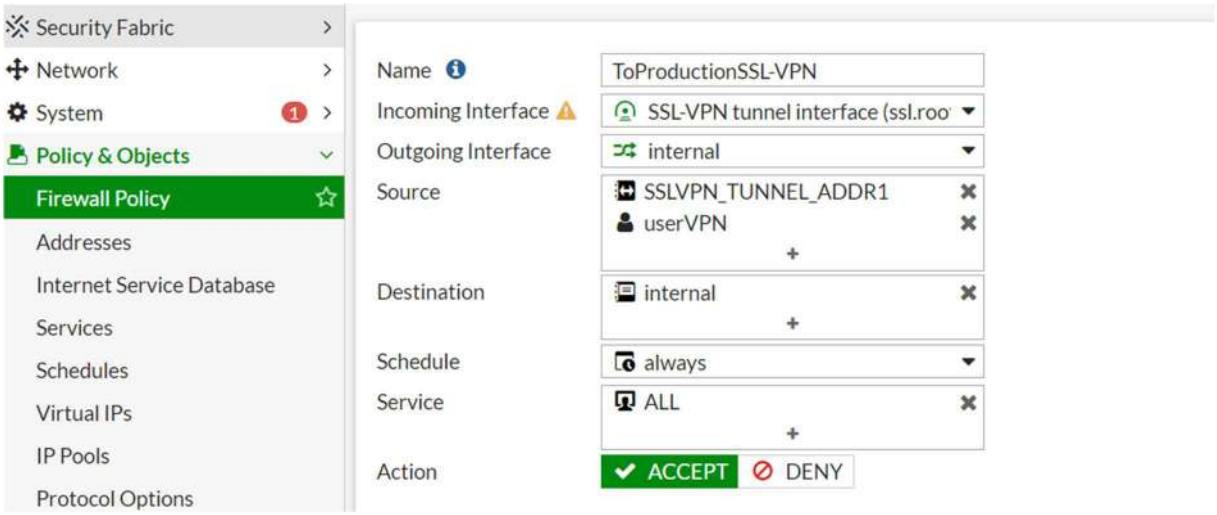
Ensuite, on configure les paramètres du VPN-SSL dans « SSL-VPN Settings », en sélectionnant l'interface WAN (s'il y a plusieurs port WAN, utiliser celui raccordé vers Internet) comme interface d'écoute avec le port souhaité, pour permettre à l'utilisateur distant de se connecter au VPN depuis ce port.



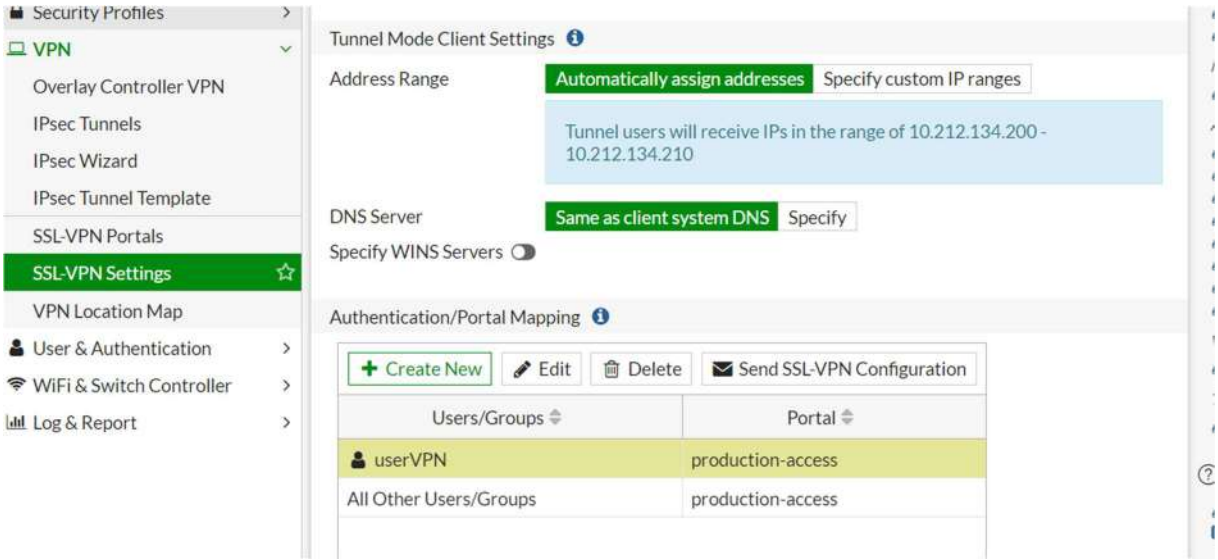
Un avertissement devrait apparaitre pour signaler une règle de pare-feu manquante pour autoriser un utilisateur extérieur à accéder au tunnel VPN :



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.

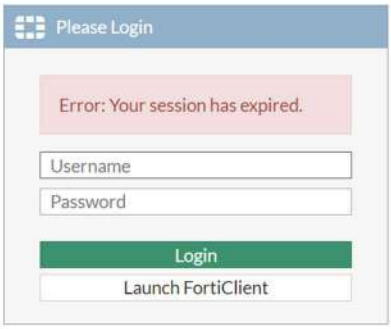


Enfin on autorise l'utilisateur à se connecter à distance si les identifiants de userVPN sont corrects.



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

port :



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 :

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