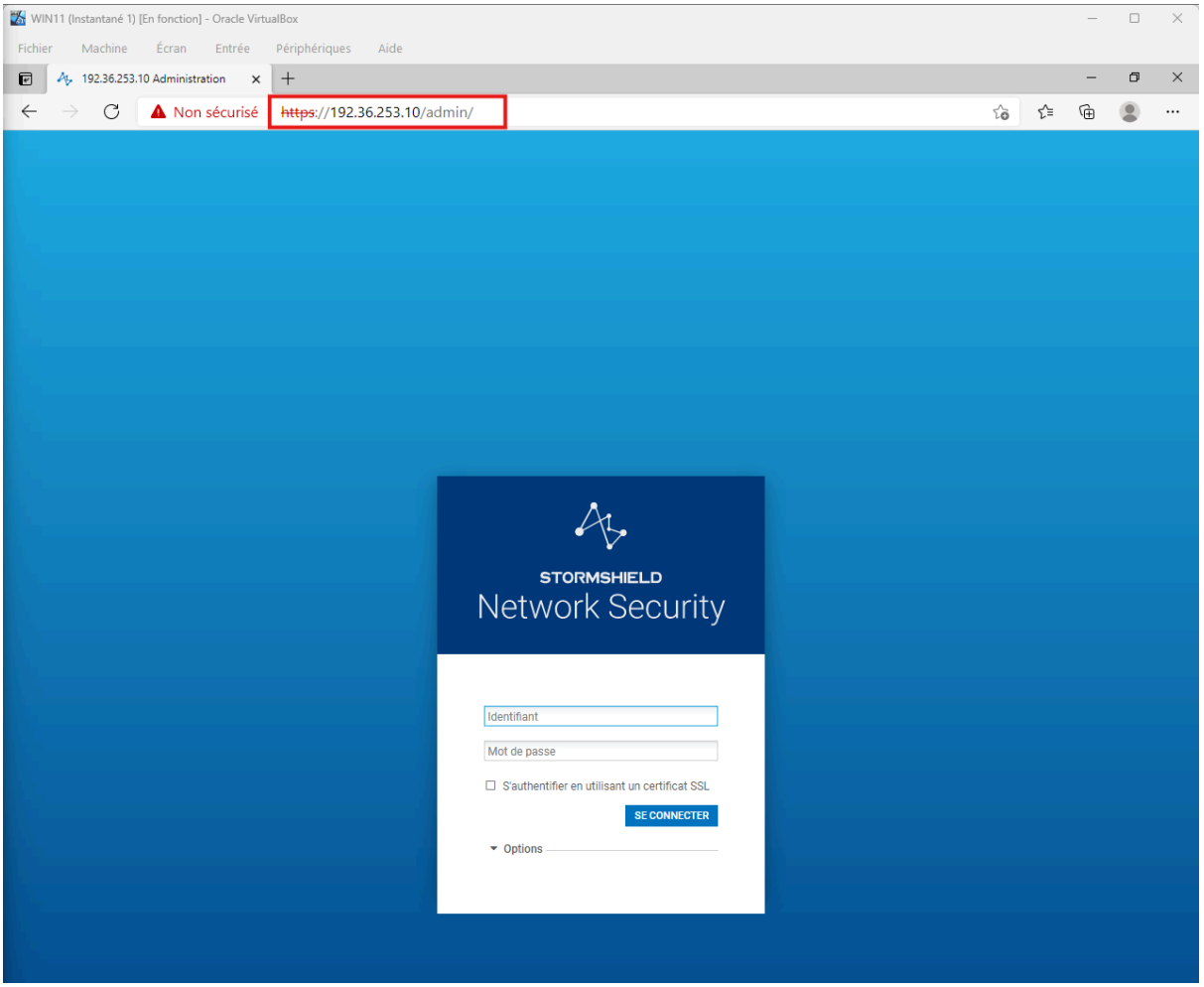
Lab 12 – Nomade VPN IPsec avec certificat

Table des matières :

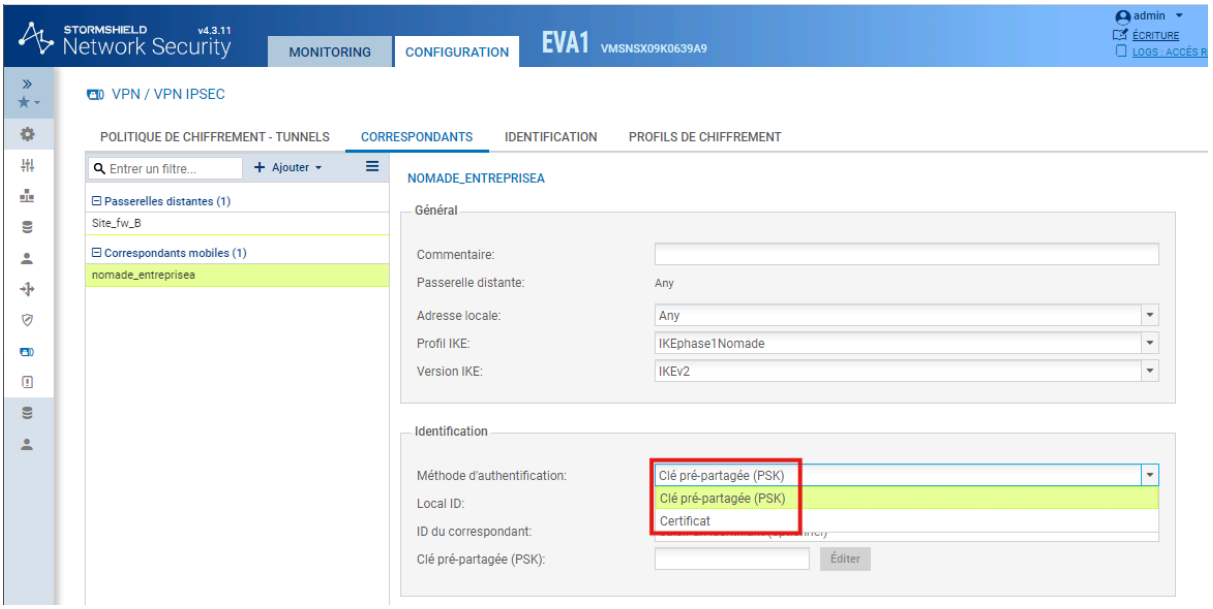
VM WIN11 réseau natnetwork (@IP 192.36.253.11)

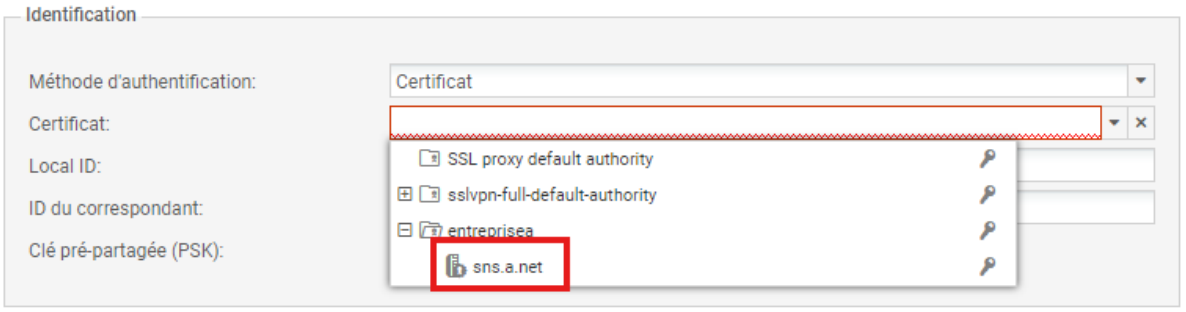


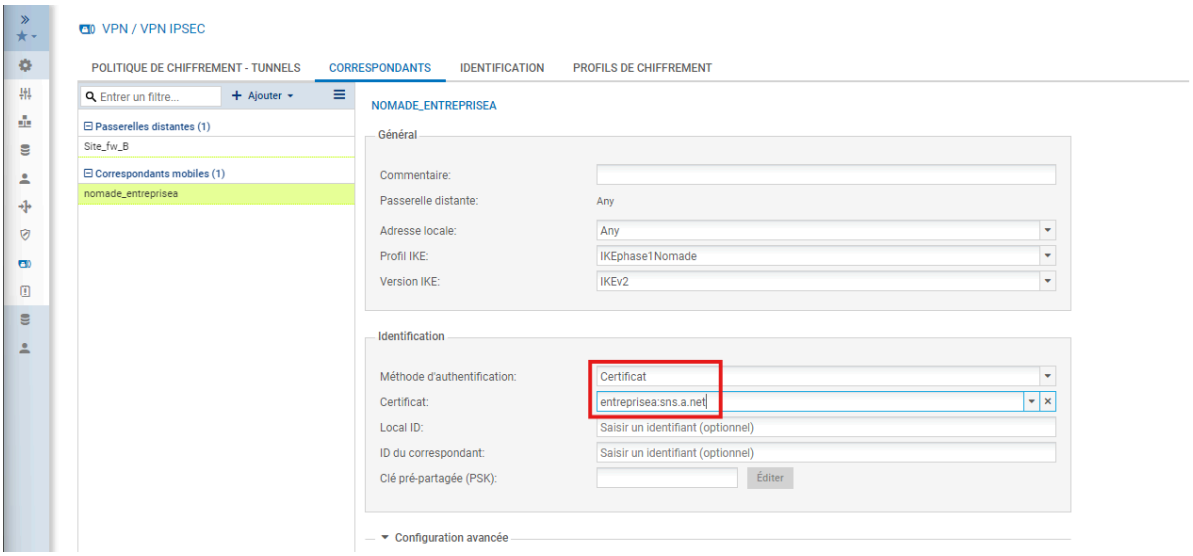
Configuration du serveur VPN

1. Modification de la méthode d'identification

- Nous changeons la méthode d'authentification en la remplaçant par certificat

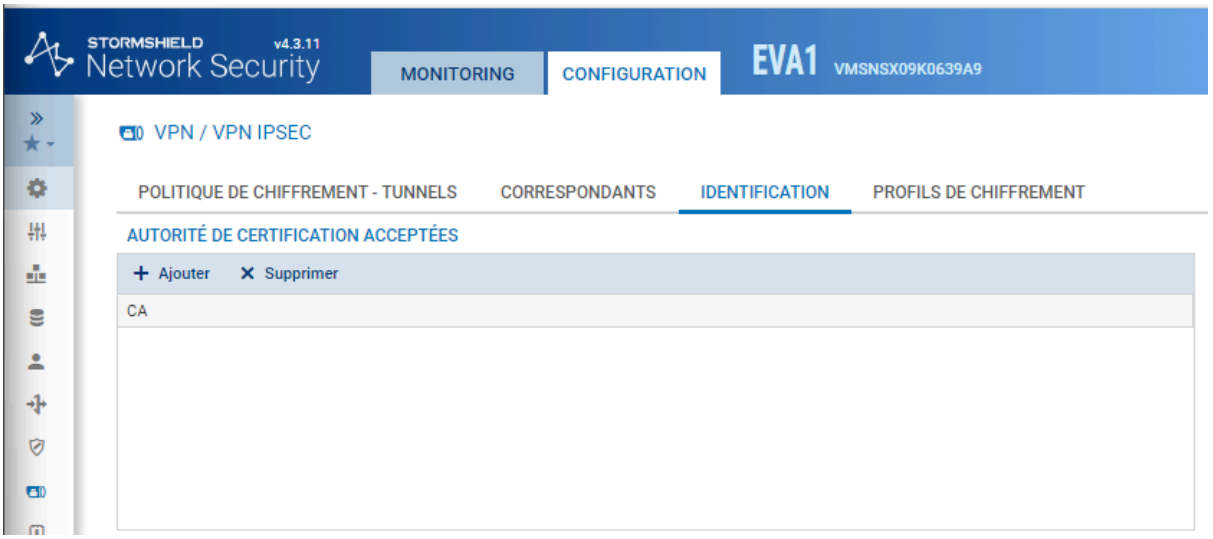


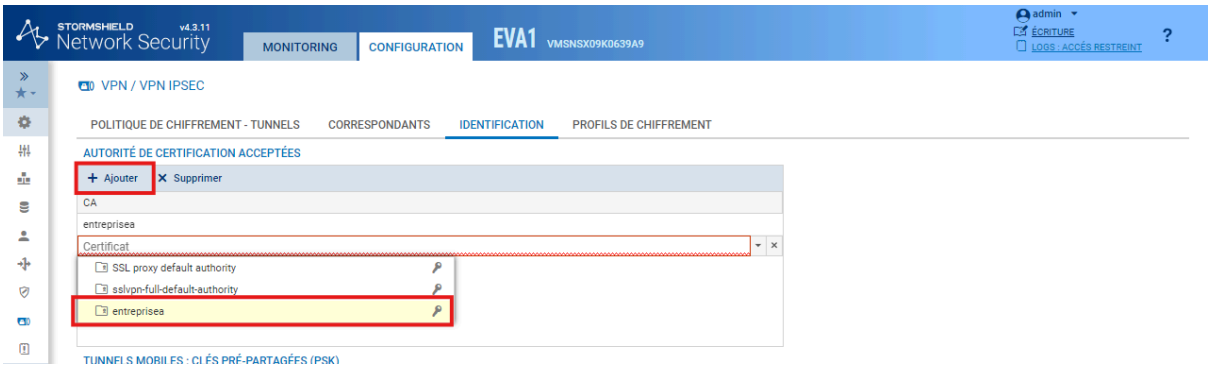




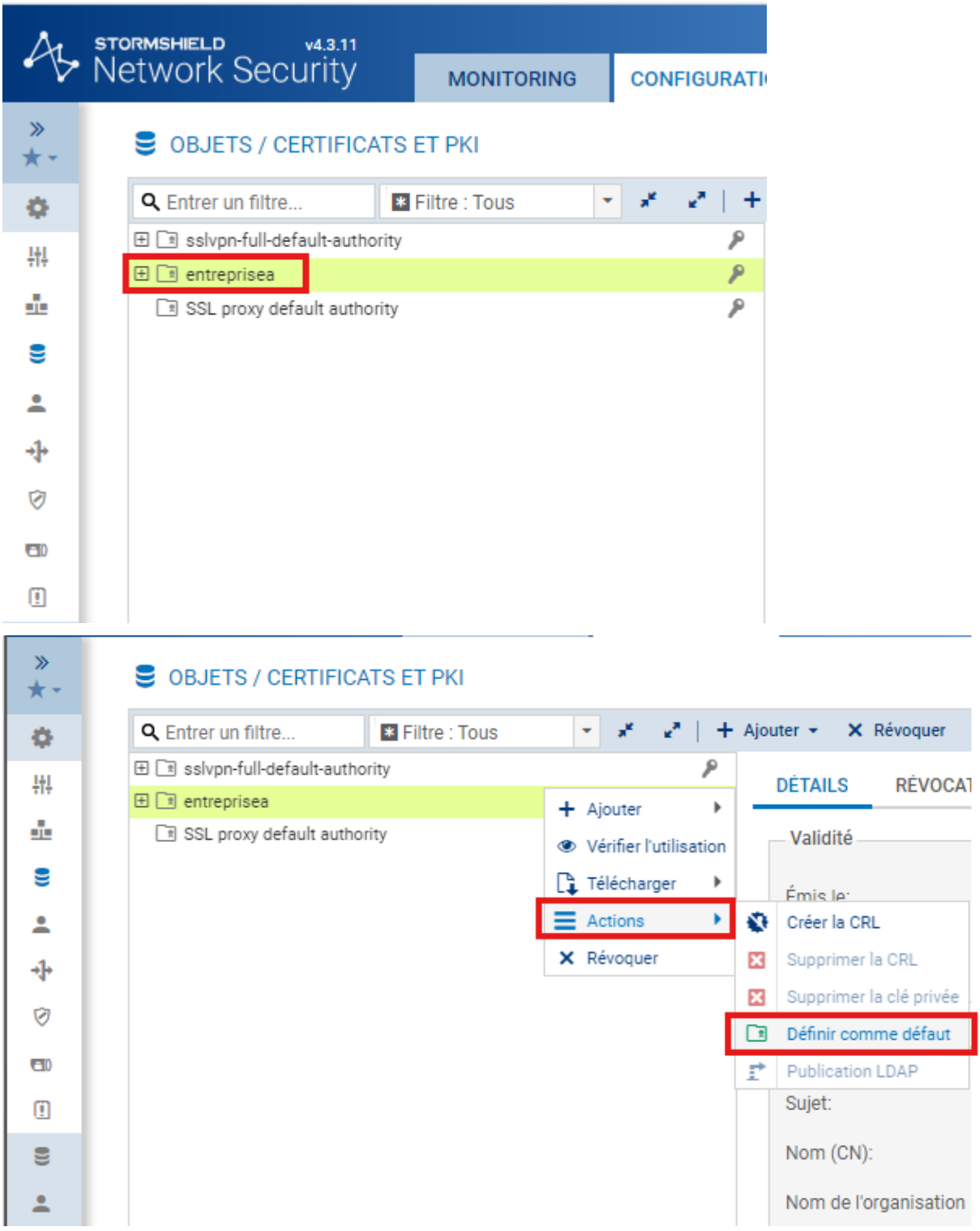
2. Définition de l'autorité de certification

▪ Définition de ll'autorité de certification dans Identification pour les certificats qui vont se présenter au SNS





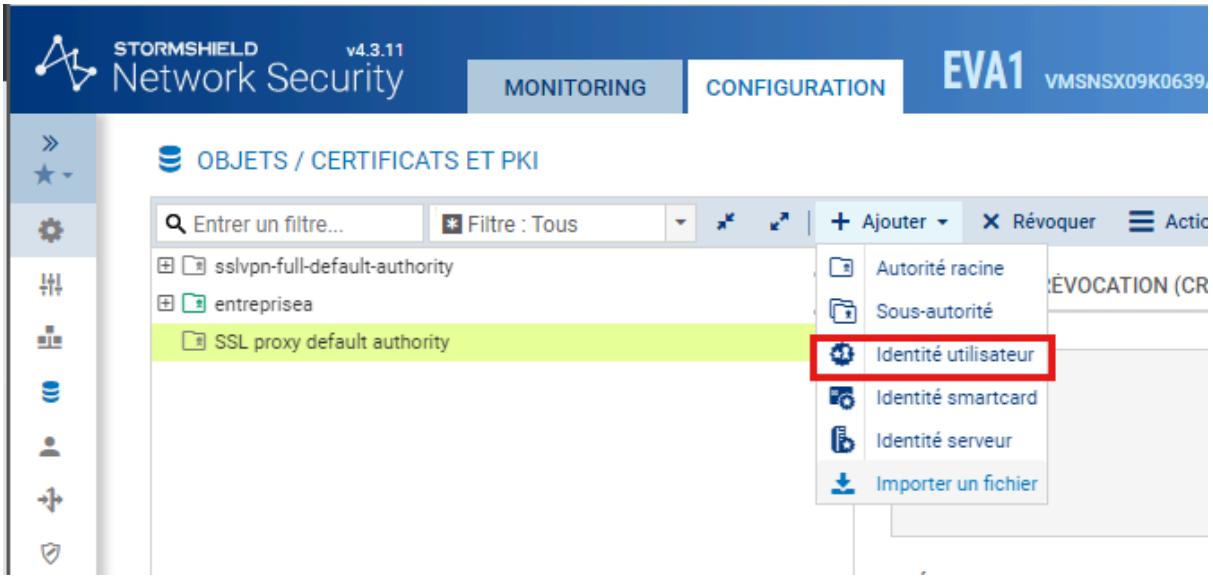
▪ Nous définissons l'autorité de certification comme autorité par défaut en cliquant droit sur l'autorité entreprisea dans Certificats et PKI

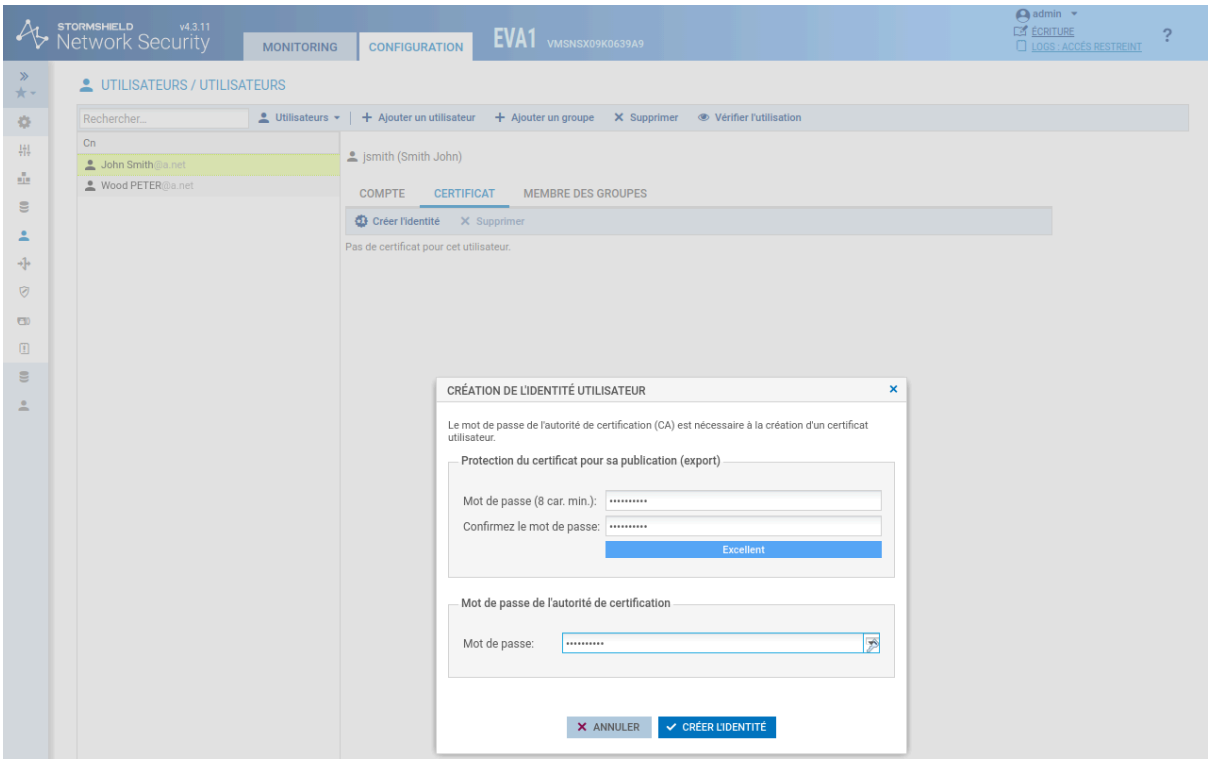


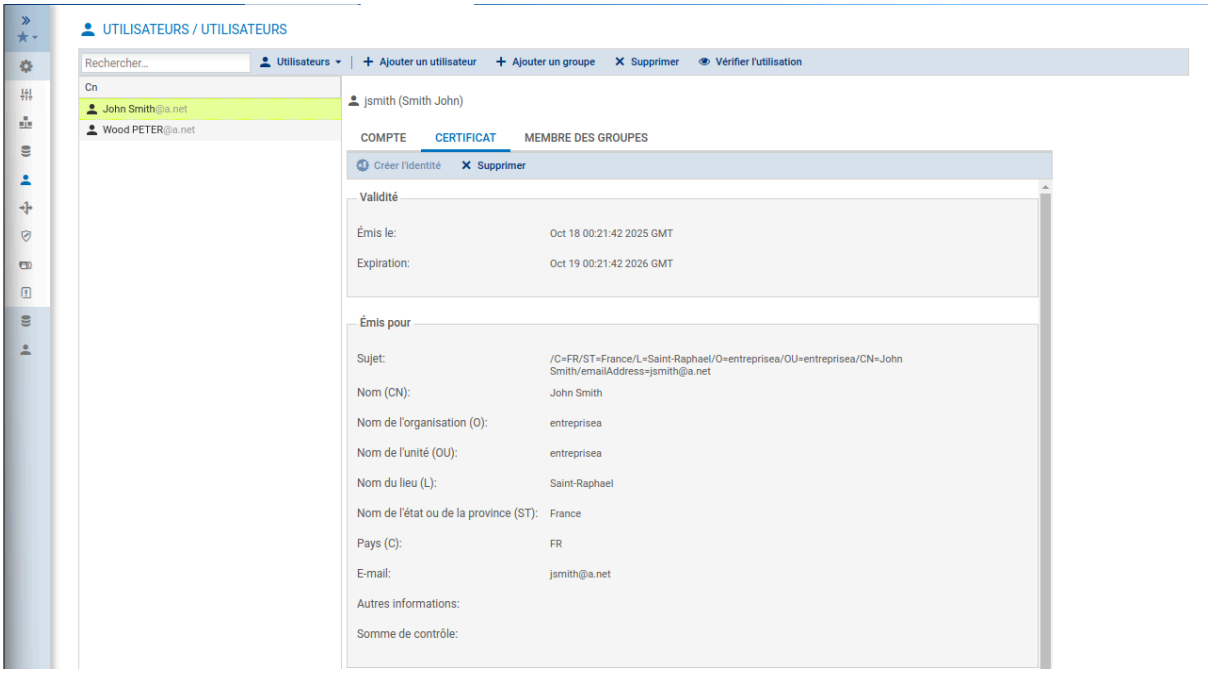
▪ Après l'avoir définie par défaut il apparaît en vert

3. Création du certificat utilisateur

▪ Création du certificat de l'utilisateur John Smith



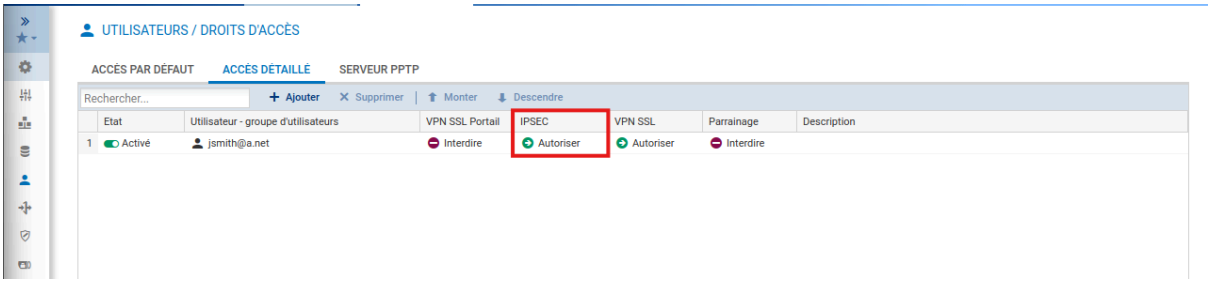


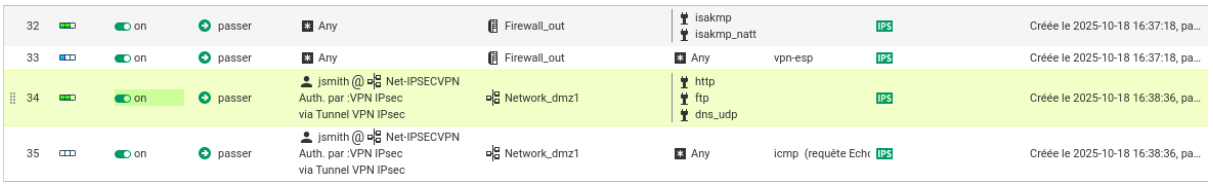

UTILISATEURS / UTILISATEURS
Rechercher...
Utilisateurs
Ajouter un utilisateur
Ajouter un groupe
Supprimer
Vérifier l'utilisation
Cn
John Smith@a.net
Wood PETER@a.net
jsmith (Smith John)
COMPTE
CERTIFICAT
MEMBRE DES GROUPES
Créer l'identité
Supprimer
Validité
Émis le: Oct 18 00:21:42 2025 GMT
Expiration: Oct 19 00:21:42 2026 GMT
Émis pour
Sujet: /C=FR/ST=France/L=Saint-Raphael/O=entreprisea/OU=entreprisea/CN=John Smith/emailAddress=jsmith@a.net
Nom (CN): John Smith
Nom de l'organisation (O): entreprisea
Nom de l'unité (OU): entreprisea
Nom du lieu (L): Saint-Raphael
Nom de l'état ou de la province (ST): France
Pays (C): FR
E-mail: jsmith@a.net
Autres informations:
Somme de contrôle:


STORMSHIELD v4.3.11
Network Security
MONITORING
CONFIGURATION
EVA1
VMSNSX09K0639A9
admin
ÉCRITURE
LOGS : ACCÈS RESTREINT
OBJETS / CERTIFICATS ET PKI
Entrer un filtre...
Filtre : Tous
Ajouter
Révoquer
Actions
Télécharger
Vérifier l'utilisation
Configuration check CRL automatic
sslvpn-full-default-authority
entreprisea
sns.a.net
John Smith
SSL proxy default authority
DÉTAILS
RÉVOCATION (CRL)
PROFILS DE CERTIFICATS
Validité
Émis le: Oct 18 00:21:42 2025 GMT
Expiration: Oct 19 00:21:42 2026 GMT
Émis pour
Sujet: C=FR,ST=France,L=Saint-Raphael,O=entreprisea,OU=entreprisea,CN=John

4. Configuration des droits et pare-feu

- Configuration des règles de pare-feu

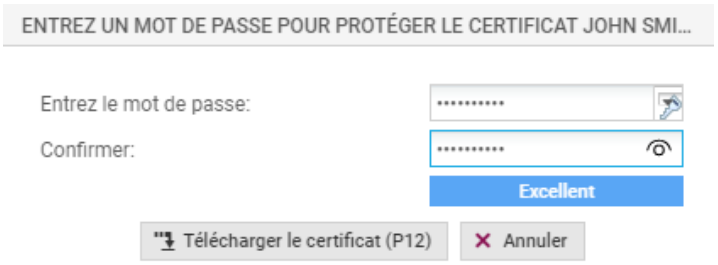


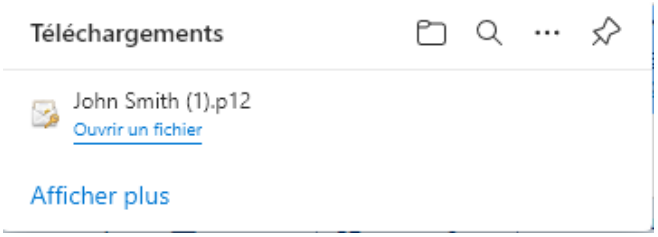


Configuration du client VPN

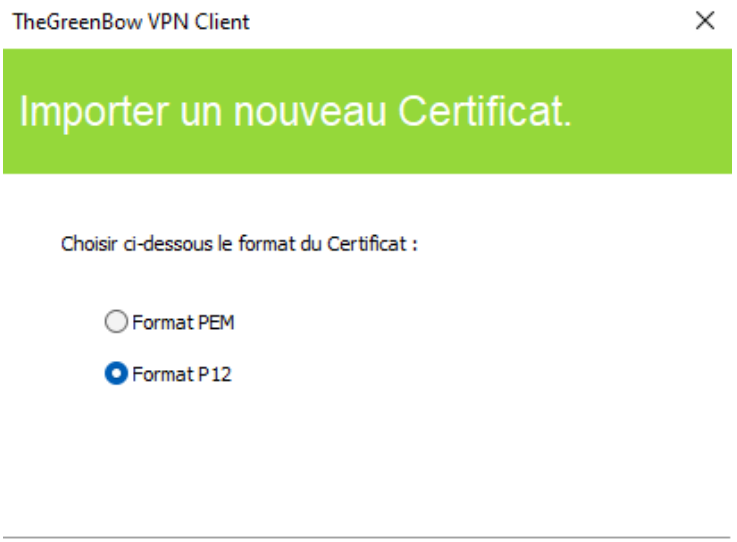
5. Importation du certificat utilisateur

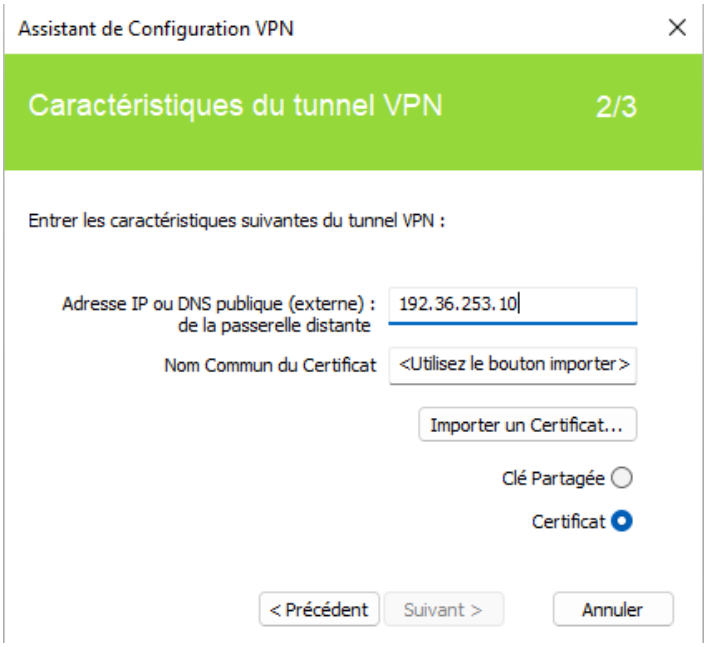
▪ Téléchargement de l'identité de jsmith au format p12

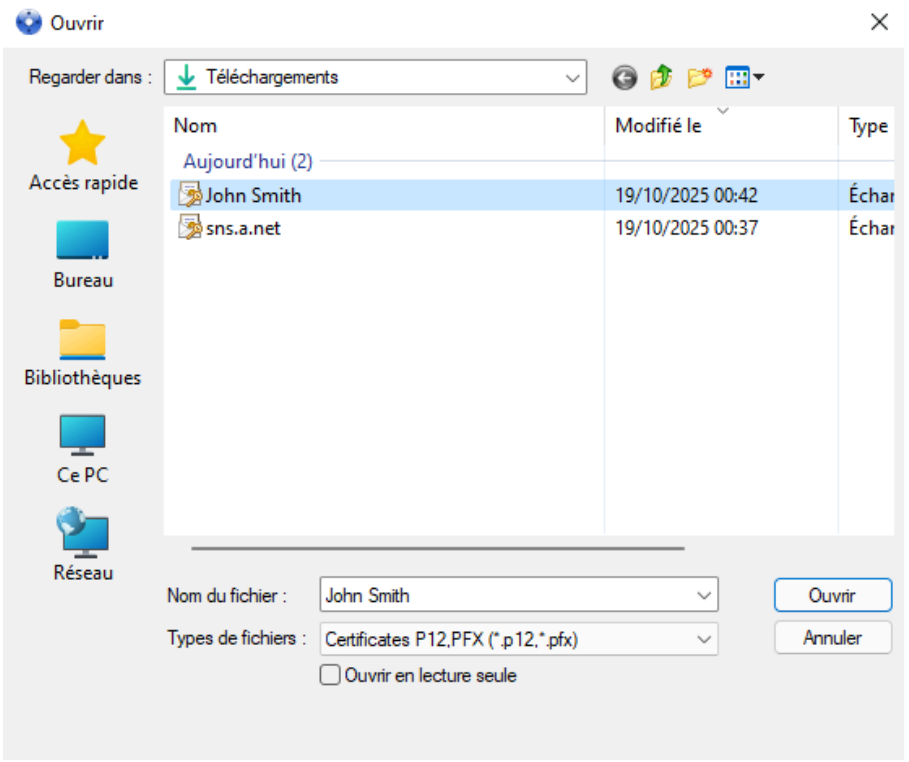


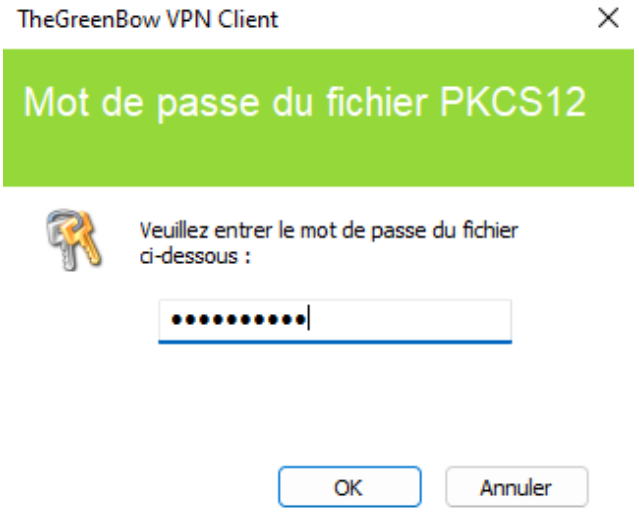


▪ Configuration d'un profil IKEv2 à l'aide de l'assistant de création de tunnel IKEv2


TheGreenBow VPN Client
Importer un nouveau Certificat.
Choisir ci-dessous le format du Certificat :
Format PEM
Format P12
Suivant >
Annuler


Assistant de Configuration VPN
Caractéristiques du tunnel VPN
2/3
Entrer les caractéristiques suivantes du tunnel VPN :
Adresse IP ou DNS publique (externe) : de la passerelle distante
192.36.253.10
Nom Commun du Certificat
<Utilisez le bouton importer>
Importer un Certificat...
Clé Partagée
Certificat
< Précédent
Suivant >
Annuler

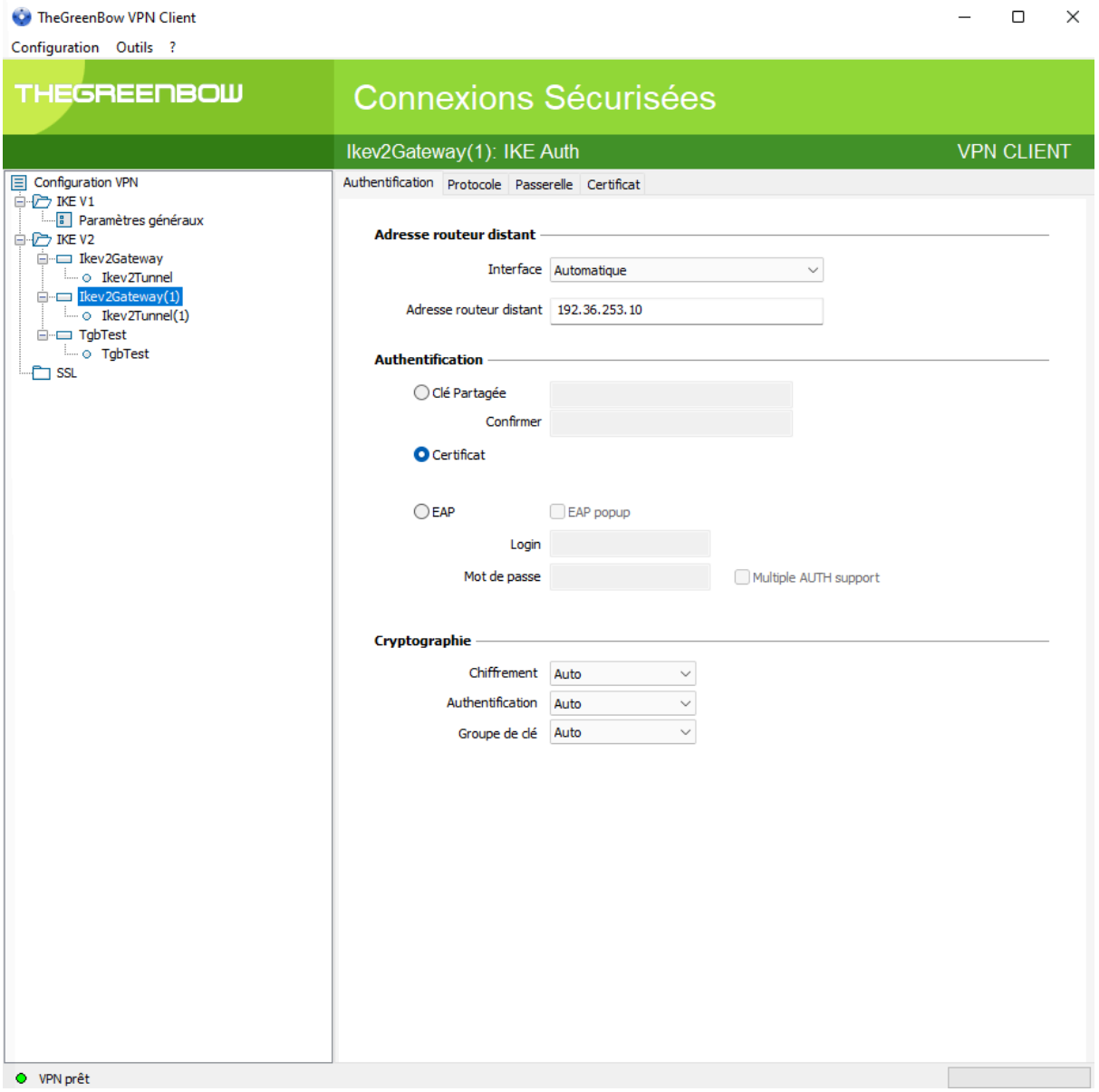

Ouvrir
Regarder dans :
Téléchargements
Accès rapide
Bureau
Bibliothèques
Ce PC
Réseau
Nom
Modifié le
Type
Aujourd'hui (2)
John Smith
19/10/2025 00:42
Échar
sns.a.net
19/10/2025 00:37
Échar
Nom du fichier :
John Smith
Types de fichiers :
Certificates P12,PFX (*.p12,*.pfx)
Ouvrir en lecture seule
Ouvrir
Annuler

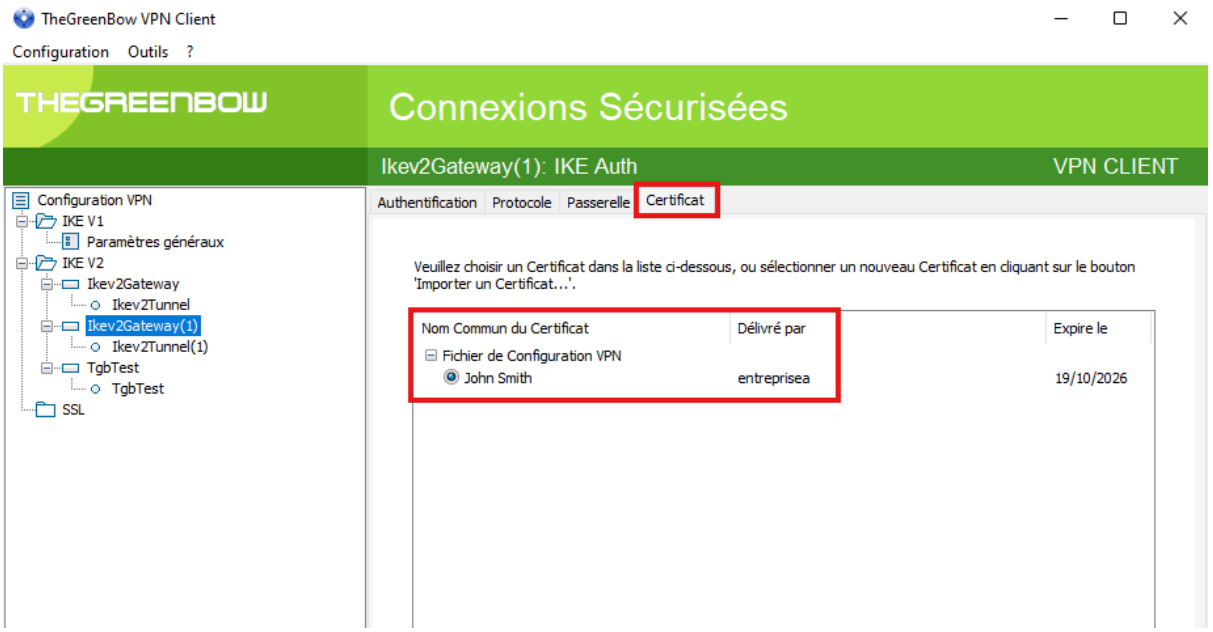

TheGreenBow VPN Client
Mot de passe du fichier PKCS12
Veuillez entrer le mot de passe du fichier ci-dessous :
OK
Annuler


TheGreenBow VPN Client
Importer un nouveau Certificat.
Importer un Certificat P12 dans le fichier de Configuration VPN.
Certificat P12
C:\Users\LocalAdmin\Downloads\
Parcourir
< Précédent
OK
Annuler
Assistant de Configuration VPN
Résumé de la configuration
3/3
La configuration du tunnel est correctement terminée :
Nom du tunnel : Ikev2Gateway(1)
Le tunnelest de type IKE V2
Nom ou adresse IP de la passerelle : 192.36.253.10
Nom commun du certificat : John Smith
Vous pouvez modifier ces paramètres à tout moment directement dans l'interface principale.
< Précédent
Terminer
Annuler

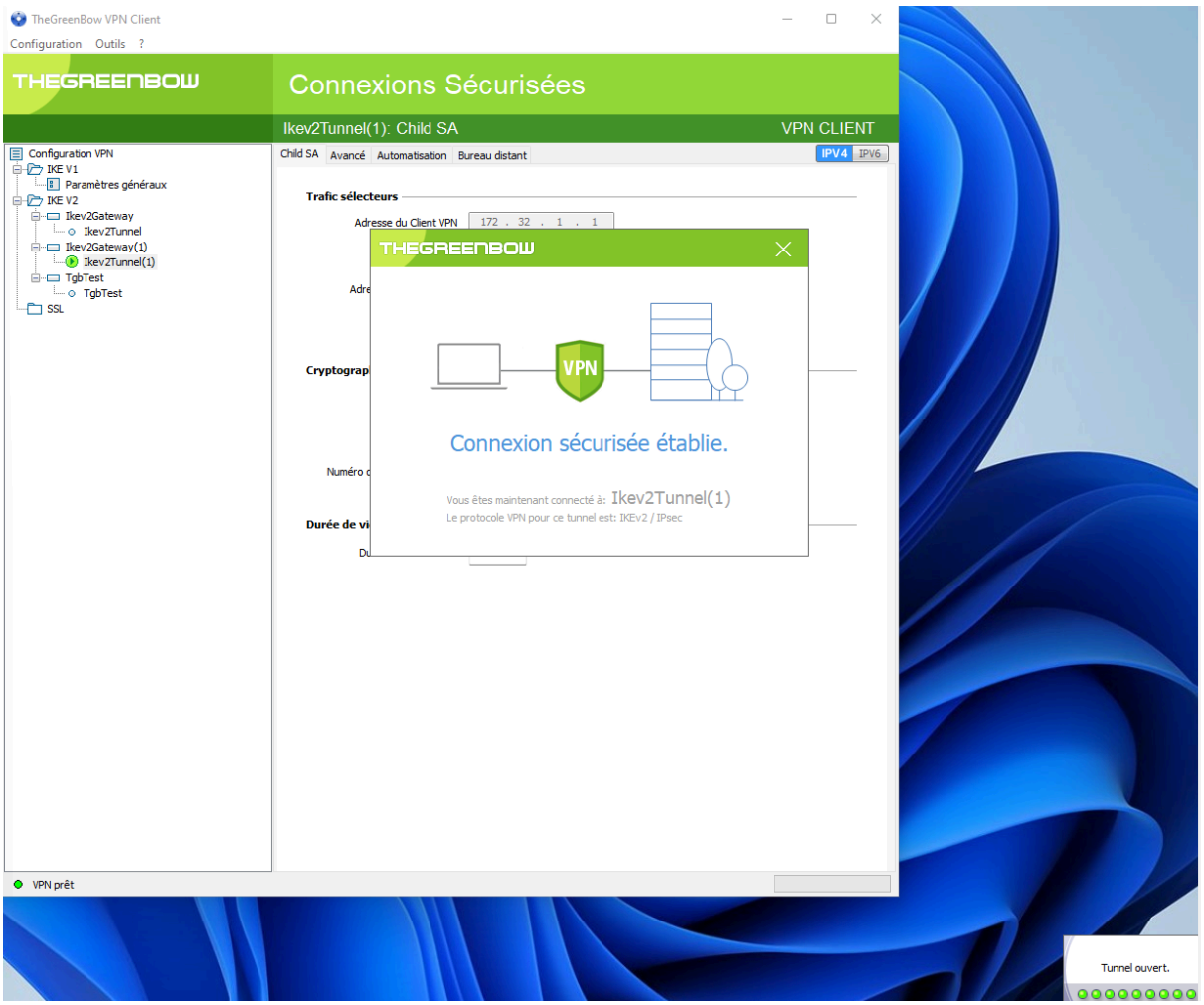
6. Paramétrage du VPN

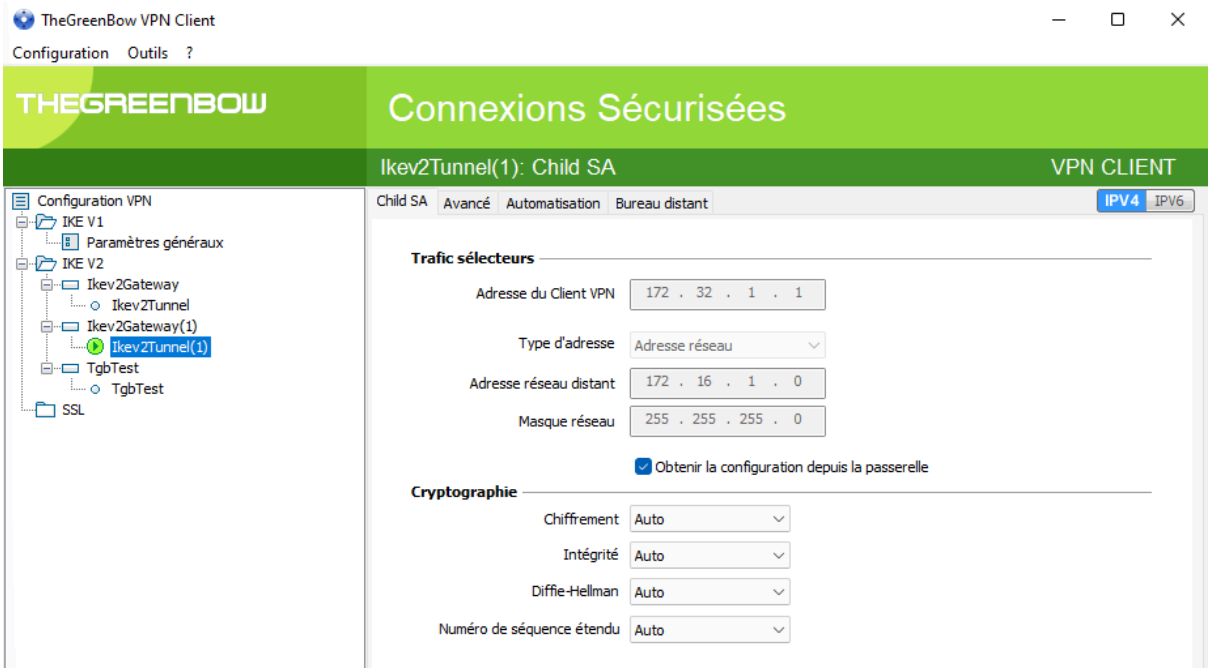
- Nous constatons que les paramètres définis antérieurement ont bien été pris en compte

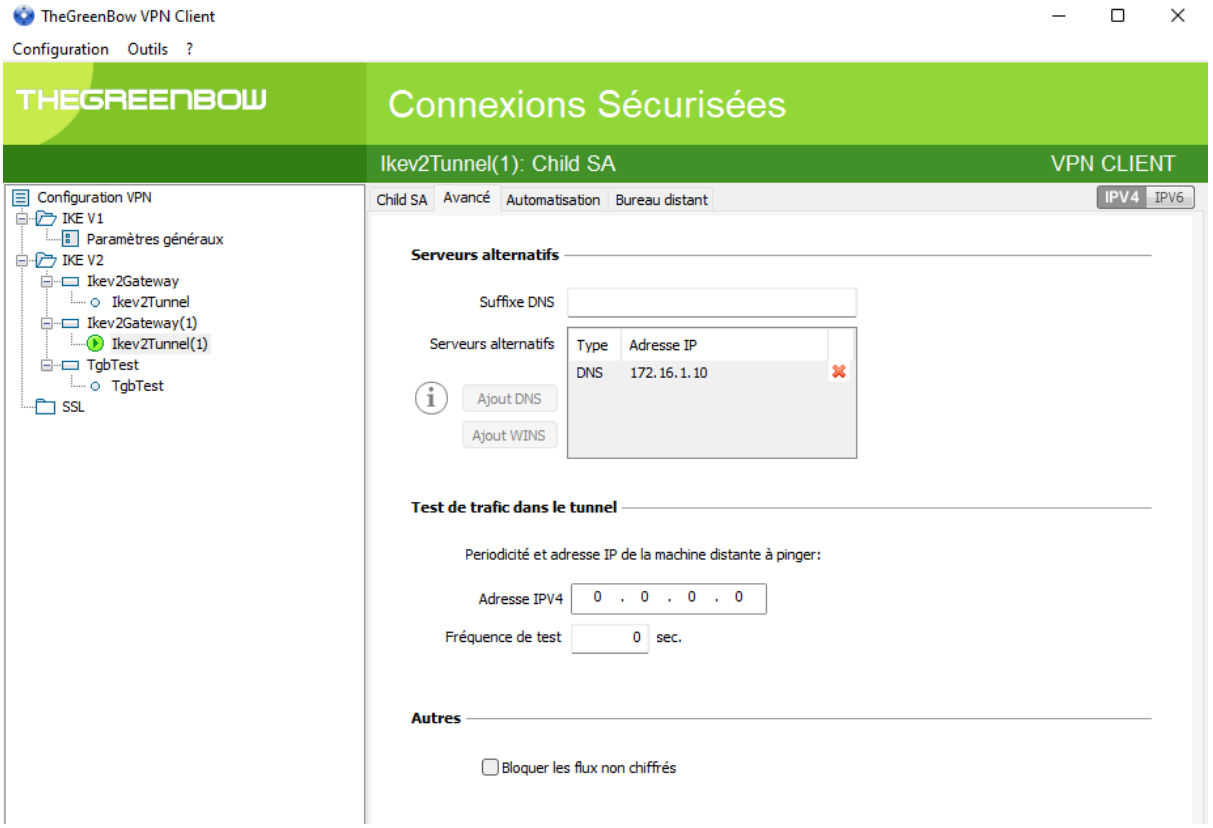




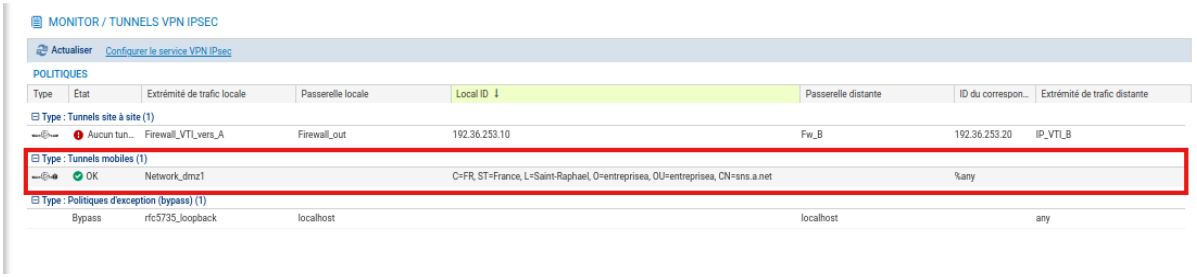
- La connexion a été établie



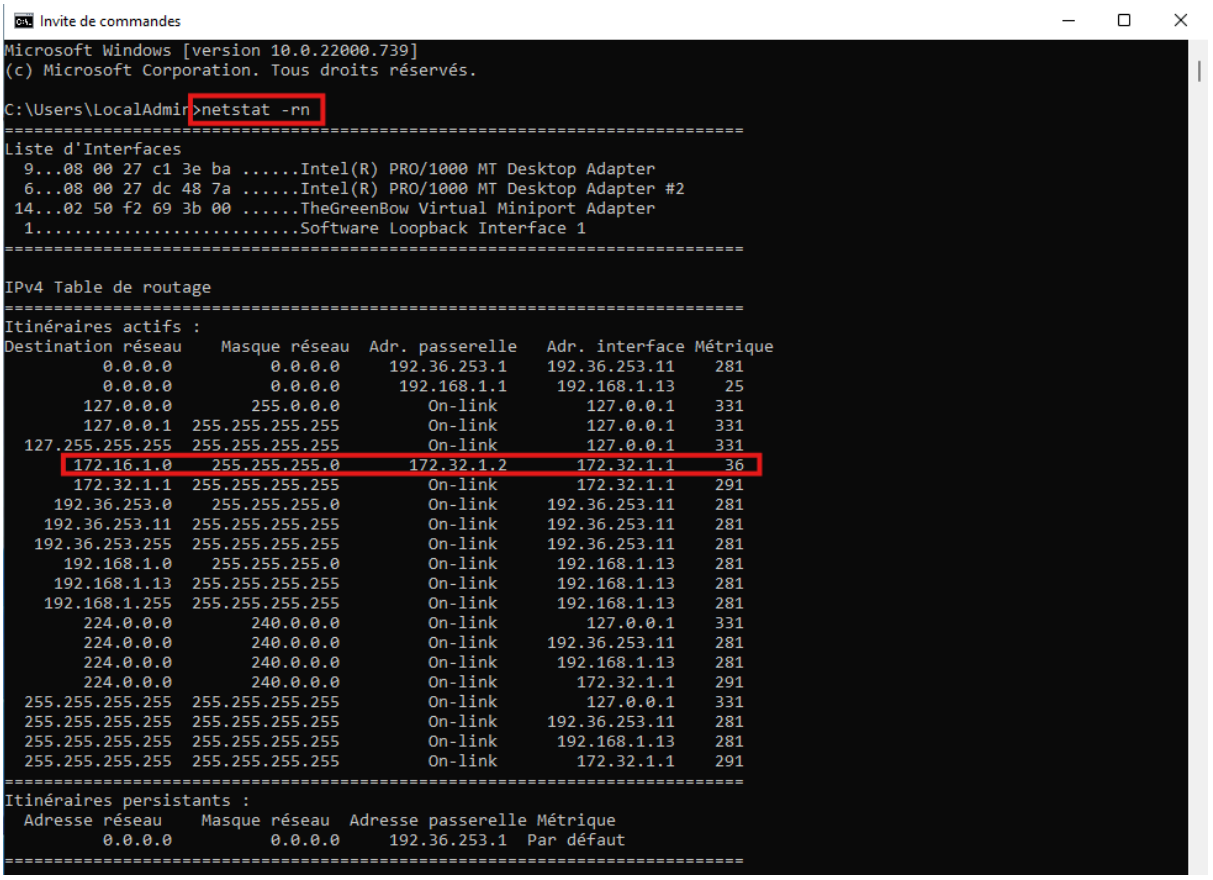

TheGreenBow VPN Client
Configuration Outils ?
THEGREENBOW
Connexions Sécurisées
Ikev2Tunnel(1): Child SA
VPN CLIENT
Configuration VPN
IKE V1
Paramètres généraux
IKE V2
Ikev2Gateway
Ikev2Tunnel
Ikev2Gateway(1)
Ikev2Tunnel(1)
TgbTest
TgbTest
SSL
Child SA
Avancé
Automatisation
Bureau distant
IPV4
IPV6
Trafic sélecteurs
Adresse du Client VPN
172 . 32 . 1 . 1
Type d'adresse
Adresse réseau
Adresse réseau distant
172 . 16 . 1 . 0
Masque réseau
255 . 255 . 255 . 0
Obtenir la configuration depuis la passerelle
Cryptographie
Chiffrement
Auto
Intégrité
Auto
Diffie-Hellman
Auto
Numéro de séquence étendu
Auto


TheGreenBow VPN Client
Configuration Outils ?
THEGREENBOW
Connexions Sécurisées
Ikev2Tunnel(1): Child SA
VPN CLIENT
Configuration VPN
IKE V1
Paramètres généraux
IKE V2
Ikev2Gateway
Ikev2Tunnel
Ikev2Gateway(1)
Ikev2Tunnel(1)
TgbTest
TgbTest
SSL
Child SA
Avancé
Automatisation
Bureau distant
IPV4
IPV6
Serveurs alternatifs
Suffixe DNS
Serveurs alternatifs
Type
Adresse IP
DNS
172.16.1.10
Ajout DNS
Ajout WINS
Test de trafic dans le tunnel
Periodicité et adresse IP de la machine distante à pinger:
Adresse IPV4
0 . 0 . 0 . 0
Fréquence de test
0
sec.
Autres
Bloquer les flux non chiffrés

▪ Nous constatons dans les logs VPN l'authentification par certificat

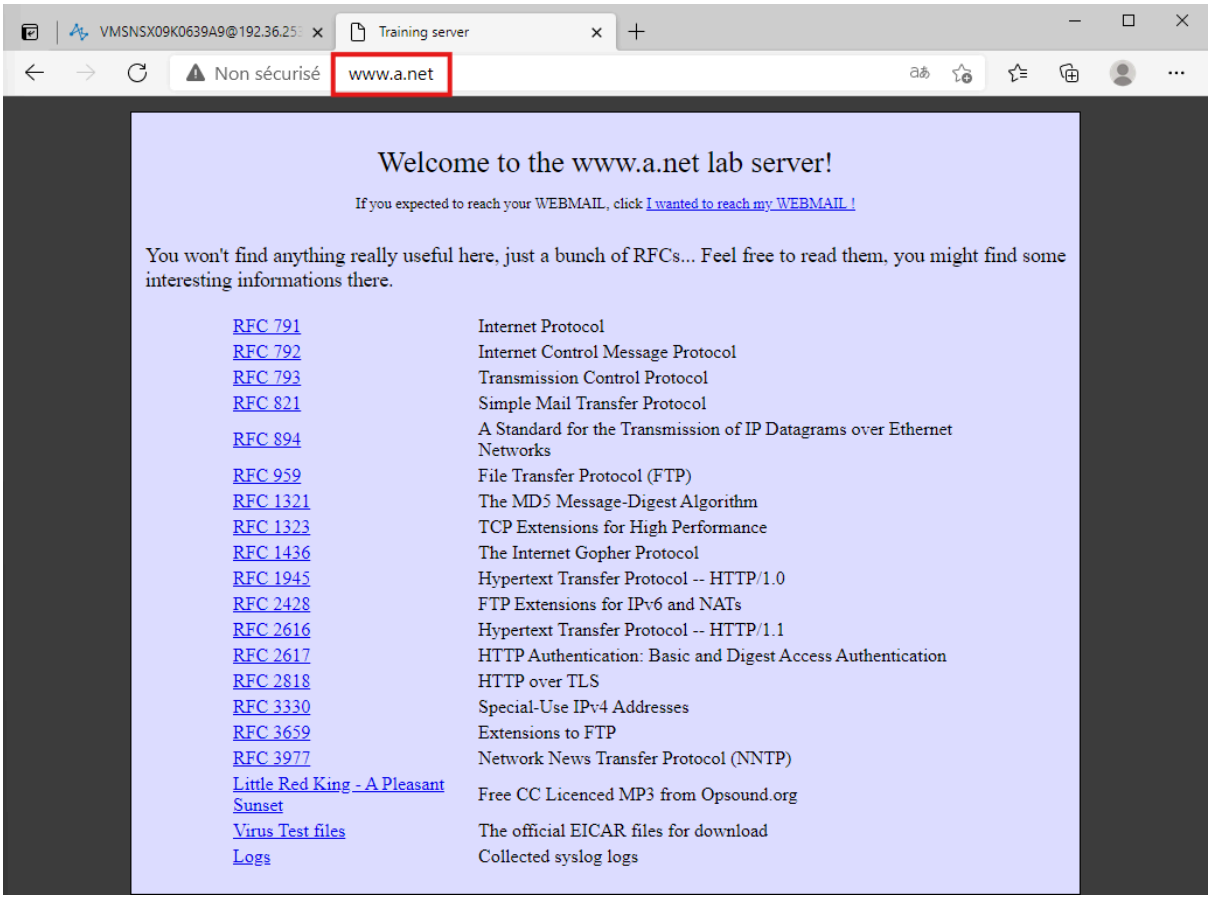


▪ En affichant la table de routage à l'aide de la commande netstat -rn, nous pouvons voir qu'une route s'est ajoutée.

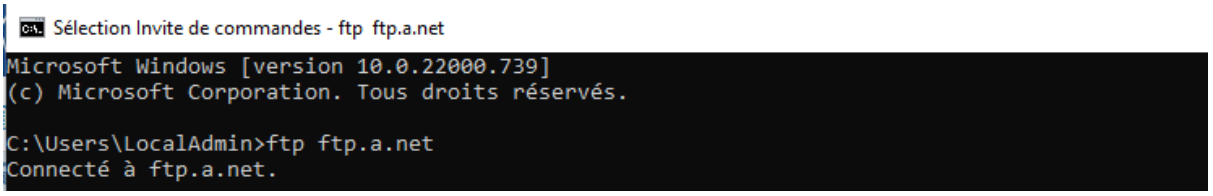


7. Tests de connectivité

- Nous testons l'accès au serveur web



- Test de la connexion transfert via FTP (commande ftp ftp.a.net)



- Test de connectivité par ping du serveur dans la DMZ.