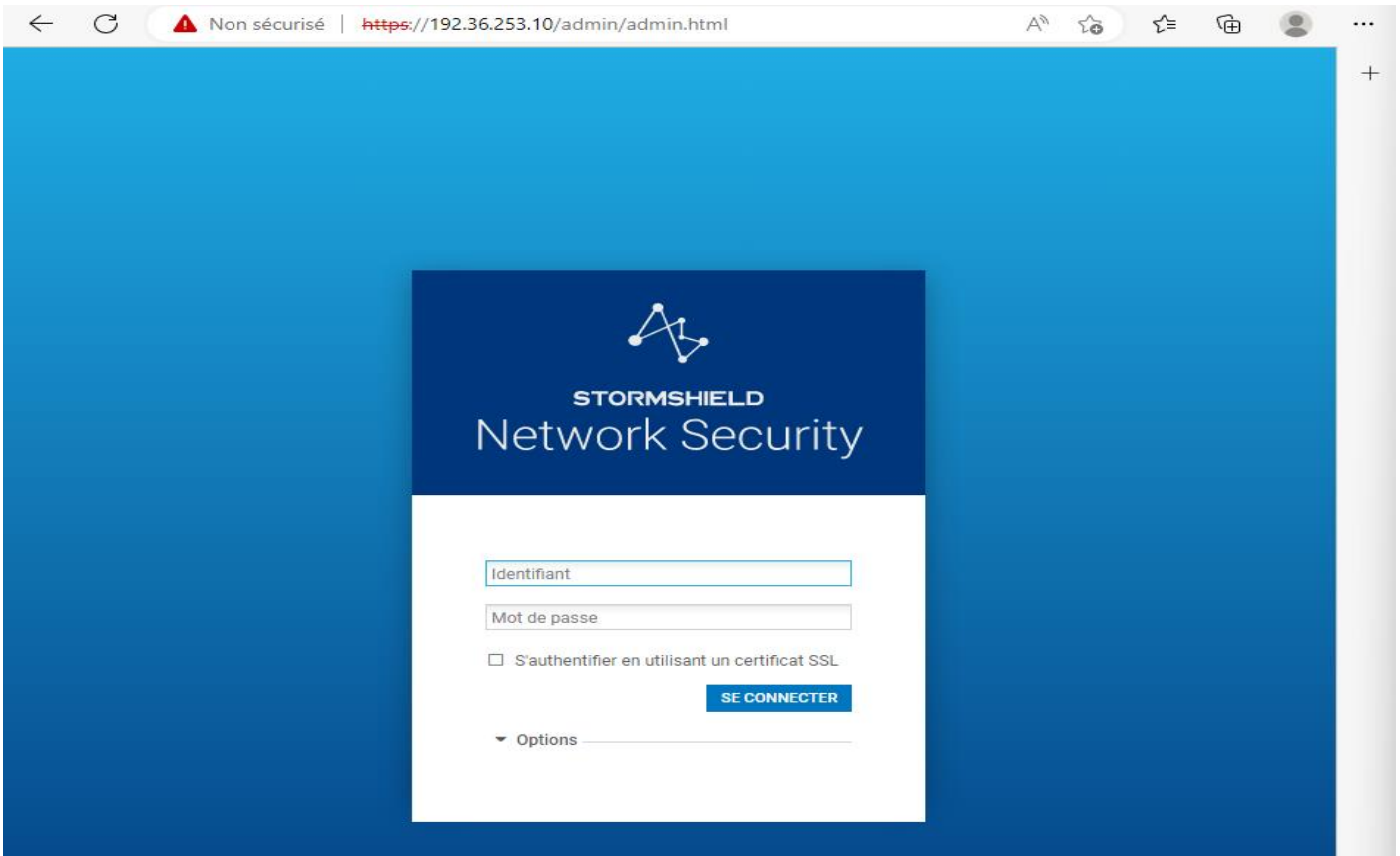
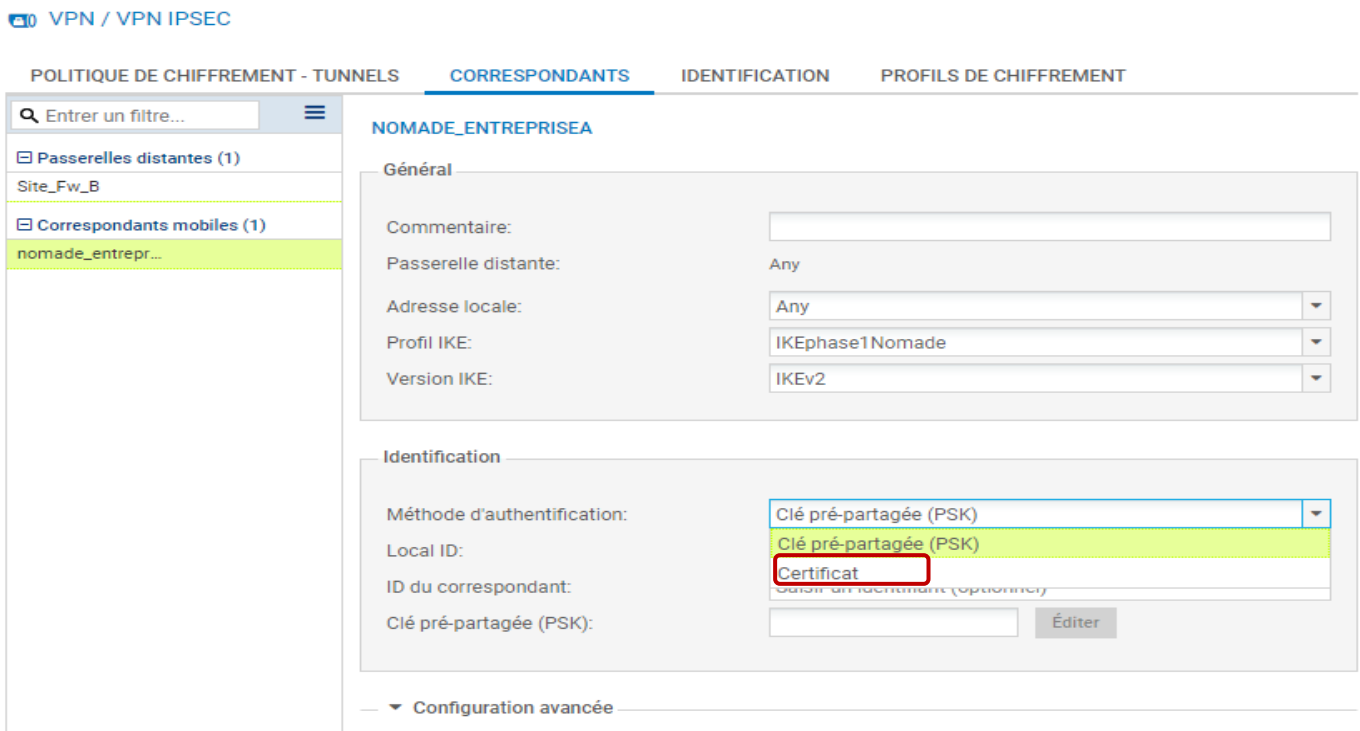


Lab 12 – Nomade VPN IPsec avec certificat

➤ Je me connecte sur le StormShield de A sur la Windows 11 :



➤ Puis je sélectionne Certificat dans les correspondants :



➤ De base il n'y a pas de certificat j'en sélectionne celui du sns.a.net :

VPN / VPN IPSEC

POLITIQUE DE CHIFFREMENT - TUNNELS **CORRESPONDANTS** IDENTIFICATION PROFILS DE CHIFFREMENT

🔍 Entrer un filtre... ☰

- Passerelles distantes (1)
Site_Fw_B
- Correspondants mobiles (1)
nomade_entrepr...

NOMADE_ENTREPRISEA

Général

Commentaire:

Passerelle distante: Any

Adresse locale: Any ▾

Profil IKE: IKEphase1Nomade ▾

Version IKE: IKEv2 ▾

Identification

Méthode d'authentification: Certificat ▾

Certificat: ✕

- SSL proxy default authority 🔑
- sslvpn-full-default-authority 🔑
- entreprisea 🔑
- sns.a.net** 🔑

Local ID:

ID du correspondant:

Clé pré-partagée (PSK):

▾ Configuration avancée

VPN / VPN IPSEC

POLITIQUE DE CHIFFREMENT - TUNNELS **CORRESPONDANTS** IDENTIFICATION PROFILS DE CHIFFREMENT

🔍 Entrer un filtre... ☰

- Passerelles distantes (1)
Site_Fw_B
- Correspondants mobiles (1)
nomade_entrepr...

NOMADE_ENTREPRISEA

Général

Commentaire:

Passerelle distante: Any

Adresse locale: Any ▾

Profil IKE: IKEphase1Nomade ▾

Version IKE: IKEv2 ▾

Identification

Méthode d'authentification: Certificat ▾

Certificat: **entreprisea:sns.a.net** ▾ ✕

Local ID: Saisir un identifiant (optionnel)

ID du correspondant: Saisir un identifiant (optionnel)

Clé pré-partagée (PSK): Éditer

➤ Puis je le définis par défaut :

OBJETS / CERTIFICATS ET PKI

The screenshot shows a web interface for managing PKI objects. The top navigation bar includes a search field, a filter dropdown set to 'Tous', and buttons for '+ Ajouter', 'Révoquer', and 'Actions'. The main content area has tabs for 'DÉTAILS', 'RÉVOCATION (CRL)', and 'PROFILS DE CERTIFICATS'. The 'DÉTAILS' tab is active, showing a table with columns for 'Validité', 'Émis le:', and 'Sujet:'. A context menu is open over a row, listing actions: 'Ajouter', 'Vérifier l'utilisation', 'Télécharger', 'Actions', 'Révoquer', 'Créer la CRL', 'Supprimer la CRL', 'Supprimer la clé privée', 'Définir comme défaut' (highlighted in red), and 'Publication LDAP'.

➤ Je renseigne les informations nécessaires (123AZEqsdl!) :

CRÉATION DE L'IDENTITÉ UTILISATEUR ✕

Le mot de passe de l'autorité de certification (CA) est nécessaire à la création d'un certificat utilisateur.

Protection du certificat pour sa publication (export)

Mot de passe (8 car. min.):

Confirmez le mot de passe:

Excellent

Mot de passe de l'autorité de certification

Mot de passe: 👁️ 🔑

✕ ANNULER ✓ CRÉER L'IDENTITÉ

➤ J'observe toutes les informations sur le certificat crée précédemment :

UTILISATEURS / UTILISATEURS

Rechercher... | Utilisateurs | + Ajouter un utilisateur | + Ajouter un groupe | X Supprimer | Vérifier l'utilisation

Cn
 John Smith@sns.net
 Peter WOOD@a.net

jsmith (Smith John)

COMPTE | **CERTIFICAT** | MEMBRE DES GROUPES

Créer l'identité | X Supprimer

Validité

Émis le: Oct 12 15:50:38 2025 GMT
 Expiration: Oct 13 15:50:38 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:

➤ Je constate la présence de jsmith dans les objets/certificats et PKI :

CONFIGURATION

Rechercher...

SYSTÈME
 RÉSEAU
OBJETS
 Réseau
 URL
 Certificats et PKI
 UTILISATEURS

OBJETS / CERTIFICATS ET PKI

Entrer un filtre... | Filtre : Tous | + Ajouter | X Révoquer | Actions

sslvpn-full-default-authority
 entreprisea
 sns.a.net
John Smith
 SSL proxy default authority

DÉTAILS | RÉVOCATION (CRL) | PROFILS DE CERTIFICATS

Validité

Émis le: Oct 6 15:16:41 2025 GMT
 Expiration: Oct 11 15:16:41 2035 GMT

Émis pour

➤ J'autorise jsmith à avoir les droits sur le VPNIPsec :

UTILISATEURS / DROITS D'ACCÈS

ACCÈS PAR DÉFAUT | **ACCÈS DÉTAILLÉ** | SERVEUR PPTP

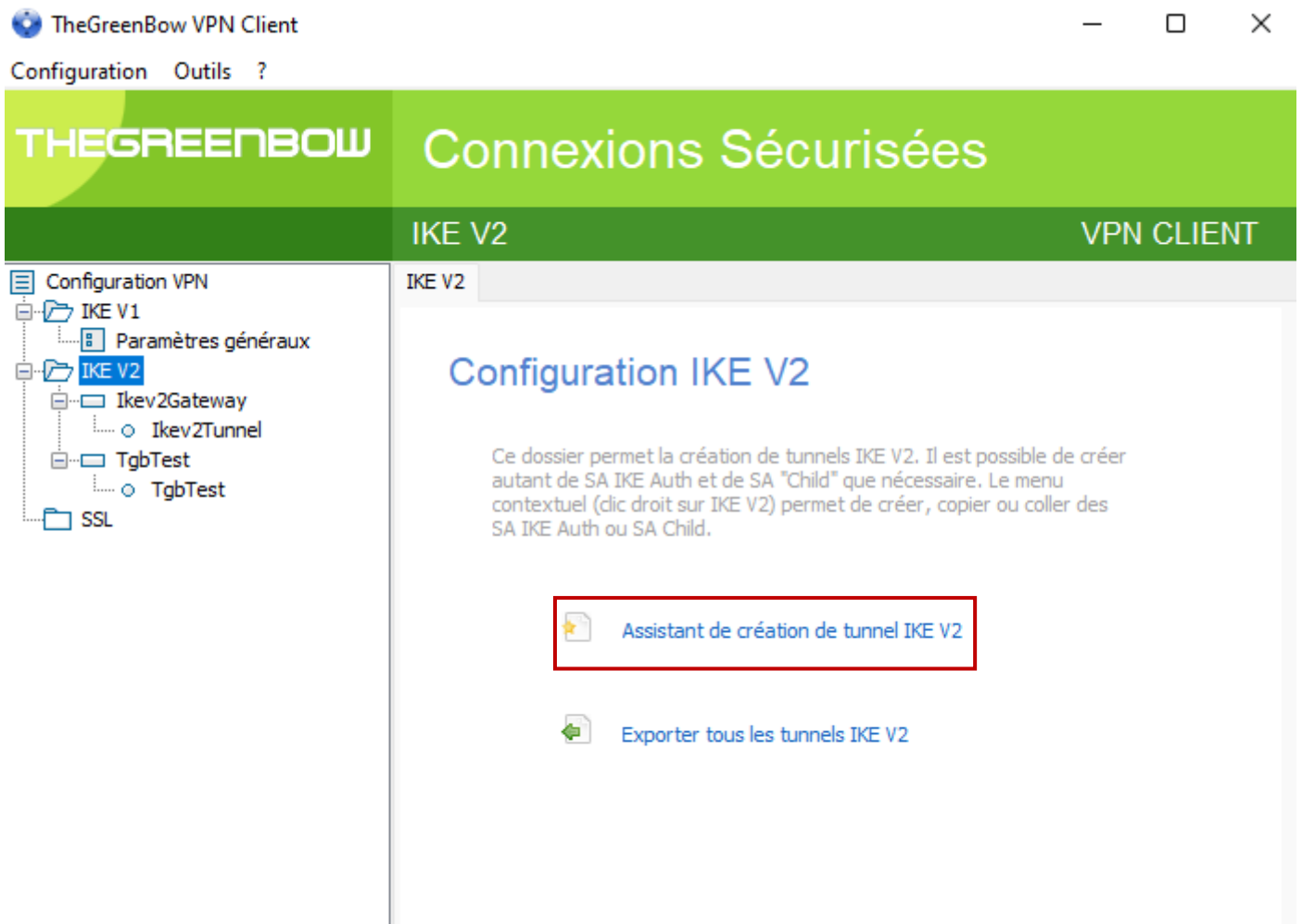
Rechercher... | + Ajouter | X Supprimer | Monter | Descendre

Etat	Utilisateur - groupe d'utilisateurs	VPN SSL Portail	IPSEC	VPN SSL	Parrainage	Description
1	Activé jsmith@a.net	Interdire	Autoriser	Autoriser	Interdire	

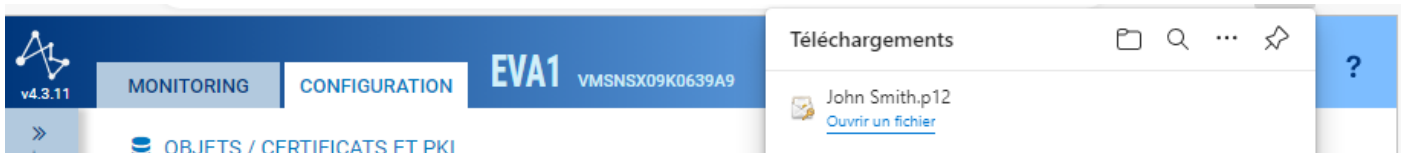
➤ Je créer les règles de filtrages qui vont avec :

Id	Etat	Actif	Passer	Source	Destination	Services	Actions	Description
5	on	passer	Any	Firewall_out	isakmp, isakmp_natt	IPS	Créée le 2025-10-06 11:34:06, par admin (192.168.1.2)	
6	on	passer	Any	Firewall_out	vpn-esp	IPS	Créée le 2025-10-06 11:34:35, par admin (192.168.1.2)	
7	on	passer	jsmith @ Net-IPSECVPN Auth. par: VPN IPsec via Tunnel VPN IPsec	Network_dmz1	http, ftp, dns	IPS	Créée le 2025-10-13 13:11:58, par admin (192.168.1.2)	
8	on	passer	jsmith @ Net-IPSECVPN Auth. par: VPN IPsec via Tunnel VPN IPsec	Network_dmz1	Any	icmp (requête Ech)	IPS	Créée le 2025-10-13 13:11:58, par admin (192.168.1.2) - Mis...

- Je vais sur TheGreenBow VPN, je choisis l'assistant de création de tunnel :



- J'installe le certificat de John Smith en .p12 :



- Sur le VPN je renseigne l'ip et j'importe le certificat :

Caractéristiques du tunnel VPN

2/3

Entrer les caractéristiques suivantes du tunnel VPN :

Adresse IP ou DNS publique (externe) : 192.36.253.10
de la passerelle distante

Nom Commun du Certificat John Smith

Importer un Certificat...

Clé Partagée Certificat

< Précédent

Suivant >

Annuler

- Je choisis l'extension .p12 :

Importer un nouveau Certificat.

Choisir ci-dessous le format du Certificat :

 Format PEM Format P12

Suivant >

Annuler

- Et le chemin d'installation du certificat :

Importer un nouveau Certificat.

Importer un Certificat P12 dans le fichier de Configuration VPN.

Certificat P12

- Je regarde dans l'onglet Authentification et je regarde que l'ip soit la bonne et que l'authentification se fasse en certificat :

Authentification Protocole Passerelle Certificat

Adresse routeur distant

Interface

Adresse routeur distant

Authentification

Clé Partagée

Confirmer

Certificat

EAP EAP popup

Login

Mot de passe Multiple AUTH support

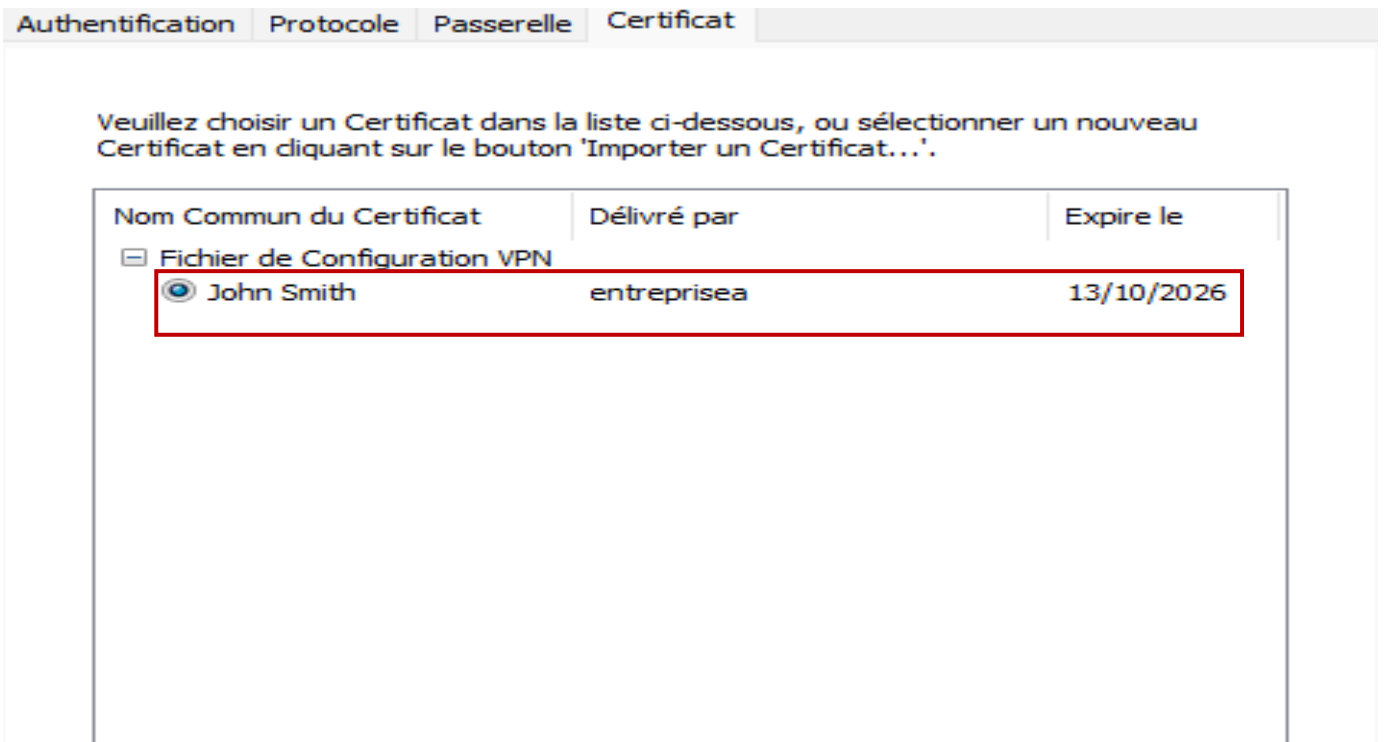
Cryptographie

Chiffrement

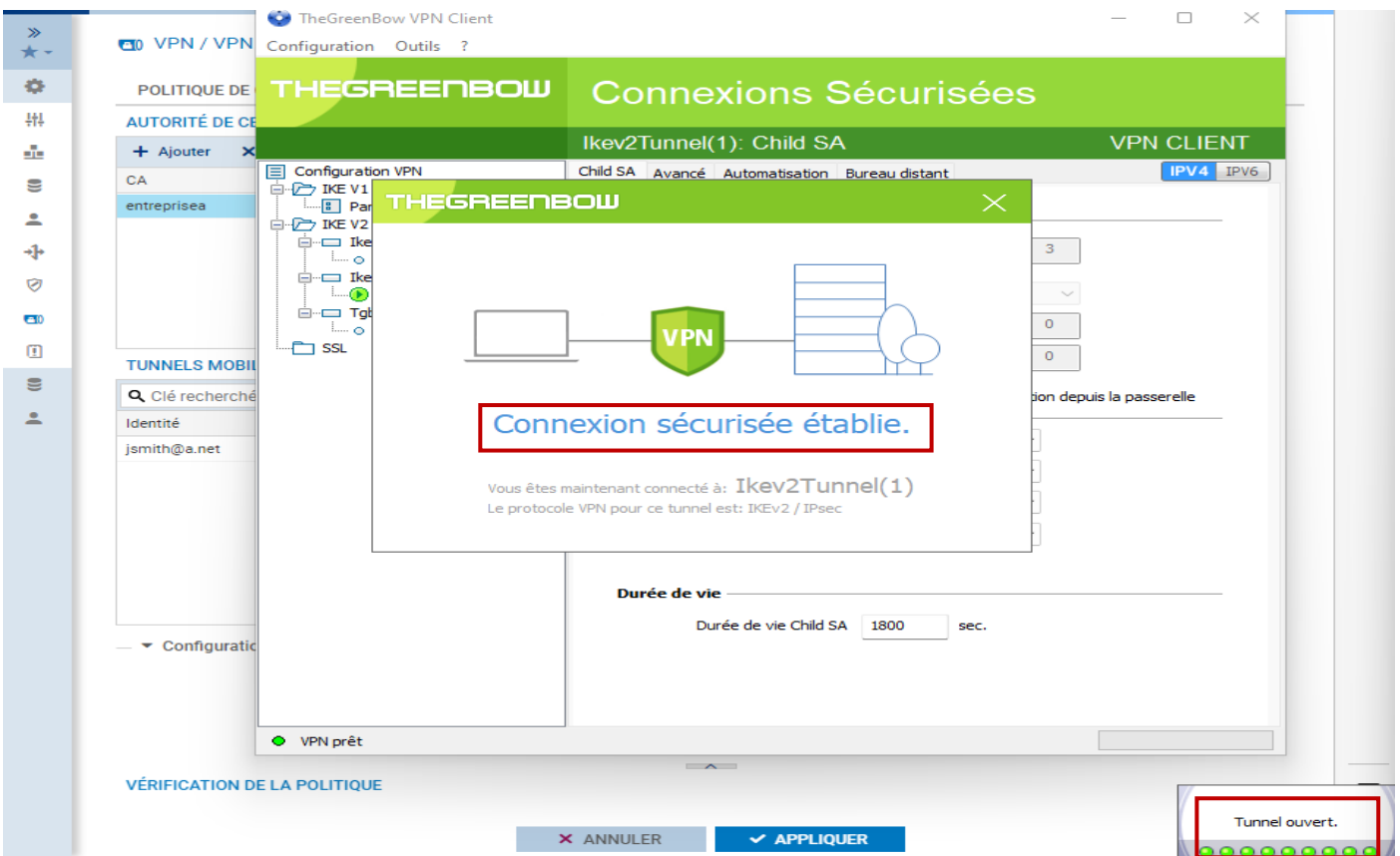
Authentification

Groupe de clé

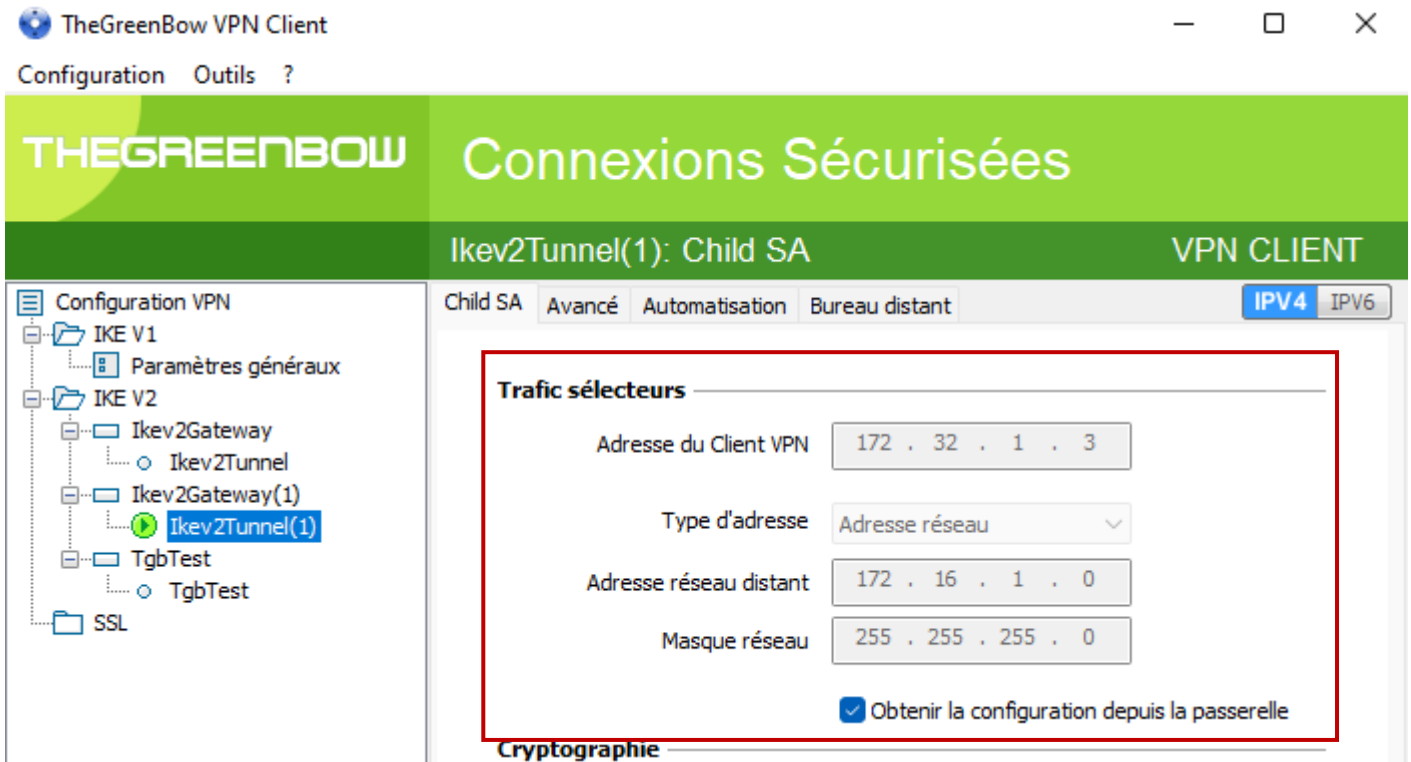
➤ Je vérifie que le certificat utiliser soit bien celui de John Smith :



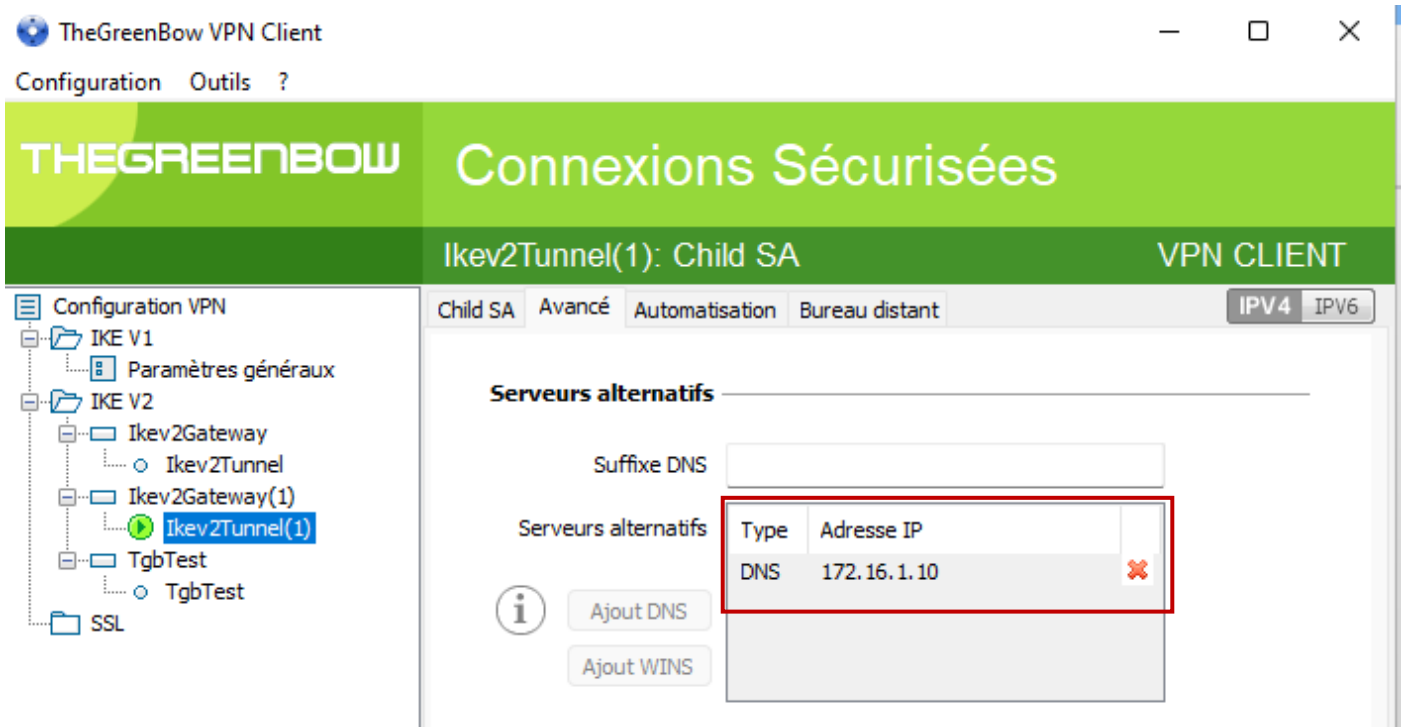
➤ Je lance la connexion sécurisée :



- Je vérifie la configuration de l'adresse du client VPN :



- Mais aussi les serveurs alternatifs :



➤ Je regarde les tunnels les tunnels sur Stormshield :

MONITOR / TUNNELS VPN IPSEC

Actualiser Configurer le service VPN IPsec

POLITIQUES

Type	État	Extrémité de trafic locale	Passerelle locale	Local ID	Passerelle distante	ID du correspon...	Extrémité de trafic distante
E Type : Tunnels mobiles (1)							
OK		Network_dmz1		C=FR, ST=Franc...			%any

➤ J'affiche la table de routage sur la machine Windows 11 :

```
C:\Users\X>netstat -rn
=====
Liste d'Interfaces
 7...08 00 27 b2 05 24 .....Intel(R) PRO/1000 MT Desktop Adapter
12...02 50 f2 da 28 00 .....TheGreenBow Virtual Miniport Adapter
1.....Software Loopback Interface 1
=====

IPv4 Table de routage
=====
Itinéraires actifs :
Destination réseau    Masque réseau    Adr. passerelle    Adr. interface    Métrique
 0.0.0.0              0.0.0.0          192.36.253.1      192.36.253.11     281
 127.0.0.0            255.0.0.0        On-link           127.0.0.1         331
 127.0.0.1            255.255.255.255  On-link           127.0.0.1         331
 127.255.255.255      255.255.255.255  On-link           127.0.0.1         331
 172.16.1.0           255.255.255.0    172.32.1.1        172.32.1.3        36
 172.32.1.3           255.255.255.255  On-link           172.32.1.3        291
 192.36.253.0         255.255.255.0    On-link           192.36.253.11     281
 192.36.253.11        255.255.255.255  On-link           192.36.253.11     281
 192.36.253.255       255.255.255.255  On-link           192.36.253.11     281
 224.0.0.0            240.0.0.0        On-link           127.0.0.1         331
 224.0.0.0            240.0.0.0        On-link           192.36.253.11     281
 224.0.0.0            240.0.0.0        On-link           172.32.1.3        291
 255.255.255.255      255.255.255.255  On-link           127.0.0.1         331
 255.255.255.255      255.255.255.255  On-link           192.36.253.11     281
 255.255.255.255      255.255.255.255  On-link           172.32.1.3        291
=====
Itinéraires persistants :
Adresse réseau    Masque réseau    Adresse passerelle    Métrique
 0.0.0.0          0.0.0.0          192.36.253.1          Par défaut
=====

IPv6 Table de routage
=====
Itinéraires actifs :
If Metric Network Destination    Gateway
 1 331 ::1/128 On-link
 7 281 fe80::/64 On-link
12 291 fe80::/64 On-link
12 291 fe80::96e:1a73:20d6:73de/128
    On-link
 7 281 fe80::33bc:6f0d:f538:7ed6/128
    On-link
 1 331 ff00::/8 On-link
 7 281 ff00::/8 On-link
12 291 ff00::/8 On-link
=====
Itinéraires persistants :
Aucun
```

➤ Je me rends sur www.a.net :



➤ Je fais le test ftp avec ftp [ftp.a.net](ftp://ftp.a.net):

```
C:\Users\X>ftp ftp.a.net
Connecté à ftp.a.net.
```

➤ Et enfin test avec un ping :

```
Microsoft Windows [version 10.0.22000.1641]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\X>ping 172.16.1.12

Envoi d'une requête 'Ping' 172.16.1.12 avec 32 octets de données :
Réponse de 172.16.1.12 : octets=32 temps=1 ms TTL=64
Réponse de 172.16.1.12 : octets=32 temps=8 ms TTL=64
Réponse de 172.16.1.12 : octets=32 temps=2 ms TTL=64
Réponse de 172.16.1.12 : octets=32 temps=2 ms TTL=64

Statistiques Ping pour 172.16.1.12:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
    Durée approximative des boucles en millisecondes :
        Minimum = 1ms, Maximum = 8ms, Moyenne = 3ms

C:\Users\X>*
```