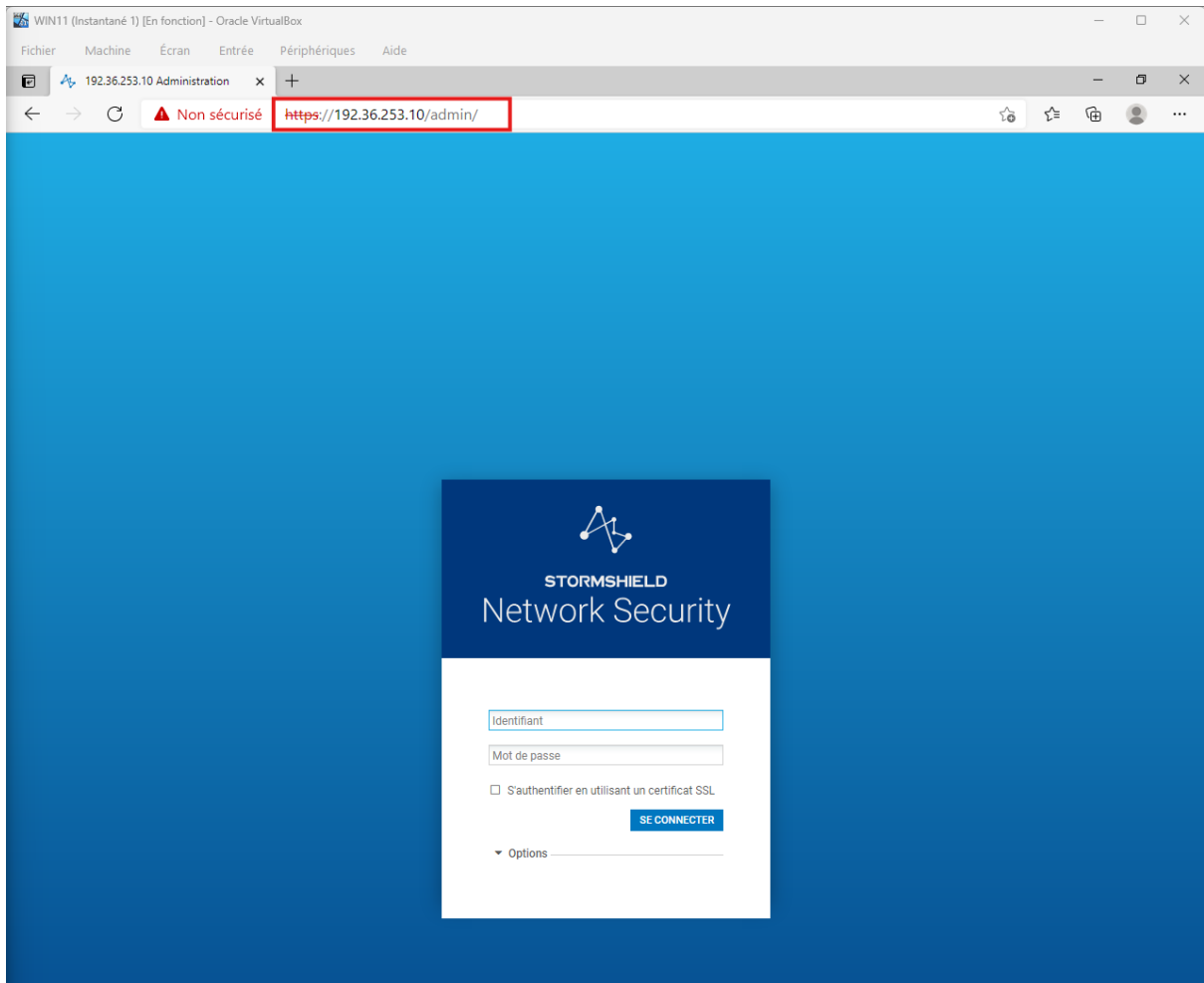


Lab 12 – Nomade VPN IPsec avec certificat

Table des matières :

Lab 12 – Nomade VPN IPsec avec certificat.....	1
1. Modification de la méthode d'identification.....	3
2. Définition de l'autorité de certification.....	4
3. Création du certificat utilisateur.....	7
4. Configuration des droits et pare-feu.....	9
6. Paramétrage du VPN.....	14
7. Tests de connectivité.....	18

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

STORMSHIELD Network Security v4.3.11
MONITORING CONFIGURATION EVA1 VMSNSX09K0639A9

VPN / VPN IPSEC

POLITIQUE DE CHIFFREMENT - TUNNELS CORRESPONDANTS IDENTIFICATION PROFILS DE CHIFFREMENT

Entrer un filtre... + Ajouter

Passerelles distantes (1)
Site_fw_B

Correspondants mobiles (1)
nomade_entreprisea

NOMADE_ENTREPRISEA

Général

Commentaire:

Passerelle distante: Any

Adresse locale: Any

Profil IKE: IKEphase1Nomade

Version IKE: IKEv2

Identification

Méthode d'authentification: Clé pré-partagée (PSK)

Local ID:

ID du correspondant:

Clé pré-partagée (PSK): Éditer

Identification

Méthode d'authentification: Certificat

Certificat:

Local ID:

ID du correspondant:

Clé pré-partagée (PSK):

SSL proxy default authority

sslvpn-full-default-authority

entreprisea

sns.a.net

VPN / VPN IPSEC

POLITIQUE DE CHIFFREMENT - TUNNELS CORRESPONDANTS IDENTIFICATION PROFILS DE CHIFFREMENT

Entrer un filtre... + Ajouter

Passerelles distantes (1)
Site_fw_B

Correspondants mobiles (1)
nomade_entreprisea

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

Configuration avancée

2. Définition de l'autorité de certification

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

The image displays two screenshots of the Stormshield Network Security v4.3.11 web interface, specifically the 'IDENTIFICATION' tab under 'VPN / VPN IPSEC' configuration.

Top Screenshot: Shows the 'AUTORITÉ DE CERTIFICATION ACCEPTÉES' section. It includes a table with one entry, 'CA'. Above the table are buttons for '+ Ajouter' and 'X Supprimer'. The interface also shows the 'MONITORING' and 'CONFIGURATION' tabs, and the user 'admin' is logged in.

Bottom Screenshot: Shows the same interface after adding new certification authorities. The table now contains three entries: 'CA', 'entreprisea', and 'entreprise'. The 'entreprisea' entry is highlighted with a red box. Below the table, there is a section for 'TUNNELS MOBILES : CI-ÉS PRÉ-PARTAGÉS (PSK)'.

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

The screenshot shows the STORMSHIELD Network Security v4.3.11 interface. The top navigation bar includes 'MONITORING' and 'CONFIGURATION'. The left sidebar contains various icons for navigation. The main content area is titled 'OBJETS / CERTIFICATS ET PKI' and displays a list of certificates and authorities. The 'entreprisea' entry is highlighted in green. A right-click context menu is open over the 'entreprisea' entry, showing options such as 'Ajouter', 'Vérifier l'utilisation', 'Télécharger', 'Actions', and 'Révoquer'. The 'Actions' option is selected, and a sub-menu is displayed with options like 'Créer la CRL', 'Supprimer la CRL', 'Supprimer la clé privée', 'Définir comme défaut', and 'Publication LDAP'. The 'Définir comme défaut' option is highlighted in red.

STORMSHIELD Network Security v4.3.11

MONITORING CONFIGURATION

OBJETS / CERTIFICATS ET PKI

Entrer un filtre... Filtre : Tous

sslvpn-full-default-authority

entreprisea

SSL proxy default authority

+ Ajouter

👁 Vérifier l'utilisation

📄 Télécharger

☰ Actions

✕ Révoquer

DÉTAILS RÉVOCA

Validité

Émis le:

Créer la CRL

Supprimer la CRL

Supprimer la clé privée

Définir comme défaut

Publication LDAP

Sujet:

Nom (CN):

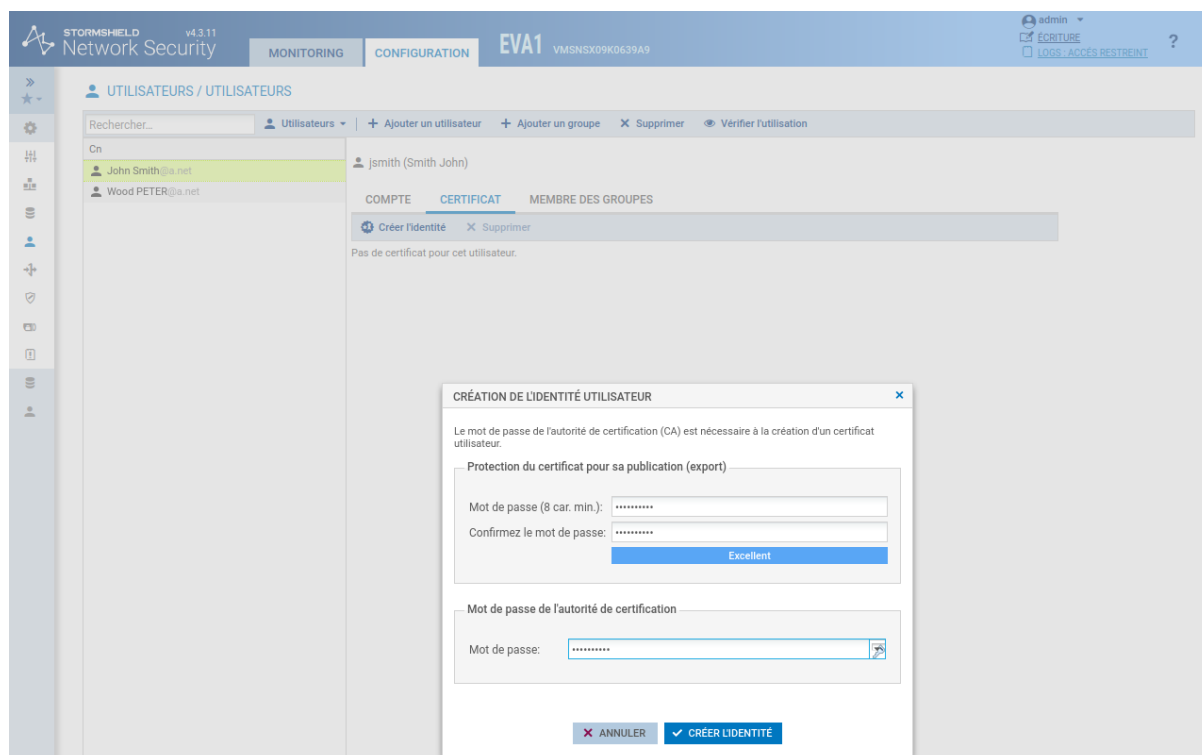
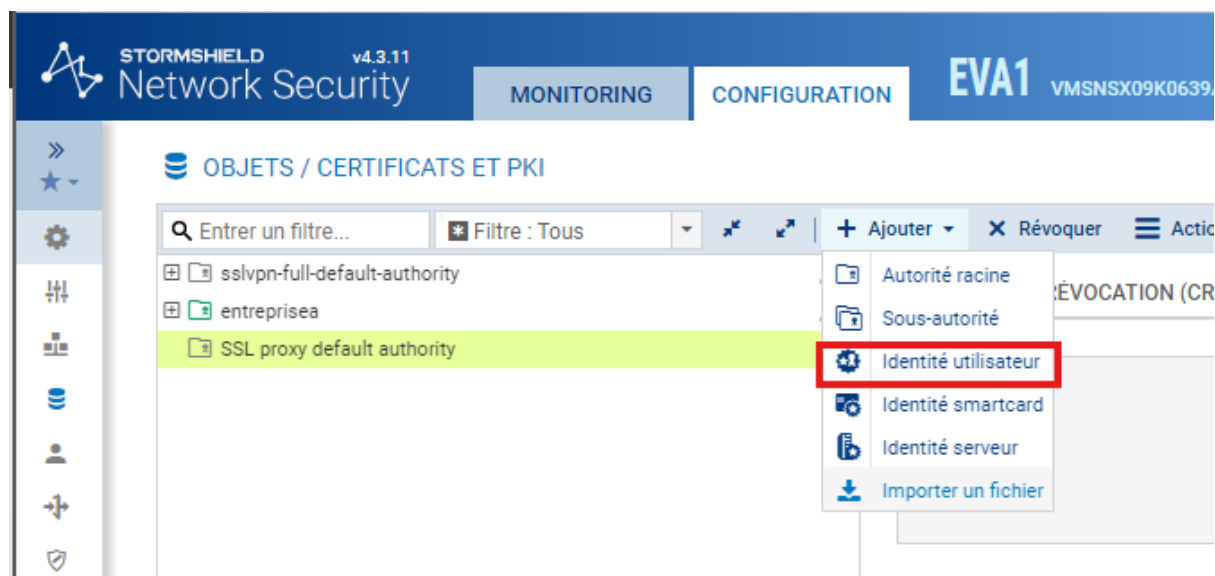
Nom de l'organisation

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



3. Création du certificat utilisateur

- Création du certificat de l'utilisateur John Smith



The screenshot displays the Stormshield web interface, divided into two main sections. The top section, titled "UTILISATEURS / UTILISATEURS", shows a list of users on the left and detailed information for "jsmith (Smith John)" on the right. The bottom section, titled "OBJETS / CERTIFICATS ET PKI", shows a list of certificates on the left and detailed information for a specific certificate on the right.

UTILISATEURS / UTILISATEURS

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

Cn

- John Smith@ia.net
- Wood PETER@ia.net

jsmith (Smith John)

COMPTE CERTIFICAT MEMBRE DES GROUPES

Créer l'identité X 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@ia.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@ia.net

Autres informations:

Somme de contrôle:

OBJETS / CERTIFICATS ET PKI

Entrez un filtre... Filtre: Tous + Ajouter X Révoquer Actions Télécharger V 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 Smith,emailAddress=jsmith@ia.net

4. Configuration des droits et pare-feu

- Configuration des règles de pare-feu

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	

32	on	passer	Any	Firewall_out	isakmp isakmp_natt	IPs	Crée le 2025-10-18 16:37:18, pa...
33	on	passer	Any	Firewall_out	Any vpn-esp	IPs	Crée le 2025-10-18 16:37:18, pa...
34	on	passer	jsmith @ Net-IPSECVPN Auth. par :VPN IPsec via Tunnel VPN IPsec	Network_dmz1	http ftp dns_udp	IPs	Crée le 2025-10-18 16:38:36, pa...
35	on	passer	jsmith @ Net-IPSECVPN Auth. par :VPN IPsec via Tunnel VPN IPsec	Network_dmz1	Any icmp (requête Ech...	IPs	Crée le 2025-10-18 16:38:36, pa...

Configuration du client VPN

5. Importation du certificat utilisateur

- Téléchargement de l'identité de jsmith au format p12

ENTREZ UN MOT DE PASSE POUR PROTÉGER LE CERTIFICAT JOHN SMI...

Entrez le mot de passe:

Confirmer:

Excellent

Télécharger le certificat (P12) Annuler

Téléchargements

John Smith (1).p12
[Ouvrir un fichier](#)

[Afficher plus](#)

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

THEGREENBOW Connexions Sécurisées

IKE V2 VPN CLIENT

Configuration VPN

- IKE V1
- Paramètres généraux
- IKE V2**
- SSL

Configuration IKE V2

Ce dossier permet la création de tunnels IKE V2. Il est possible de créer autant de SA IKE Auth et de SA "Child" que nécessaire. Le menu contextuel (clic droit sur IKE V2) permet de créer, copier ou coller des SA IKE Auth ou SA Child.

Assistant de création de tunnel IKE V2

Exporter tous les tunnels IKE V2

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) : 192.36.253.10
de la passerelle distante

Nom Commun du Certificat <Utilisez le bouton importer >

Importer un Certificat...

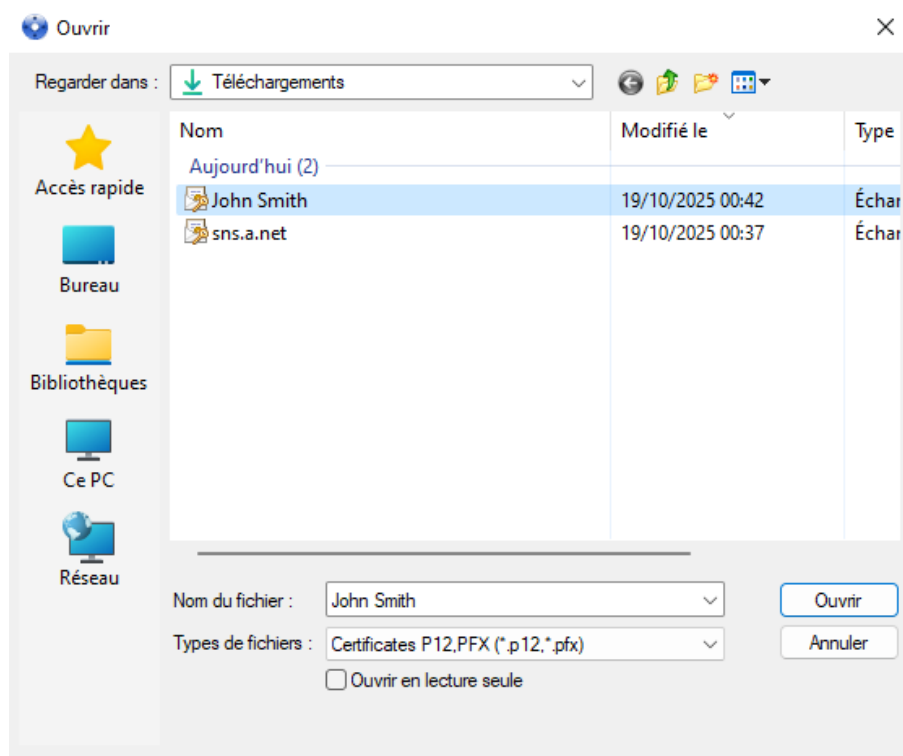
Clé Partagée ☐

Certificat ☒

< Précédent

Suivant >

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

Assistant de Configuration VPN

✕

Résumé de la configuration

3/3

La configuration du tunnel est correctement terminée :

Nom du tunnel : Ikev2Gateway(1)

Le tunnel est de type IKE V2

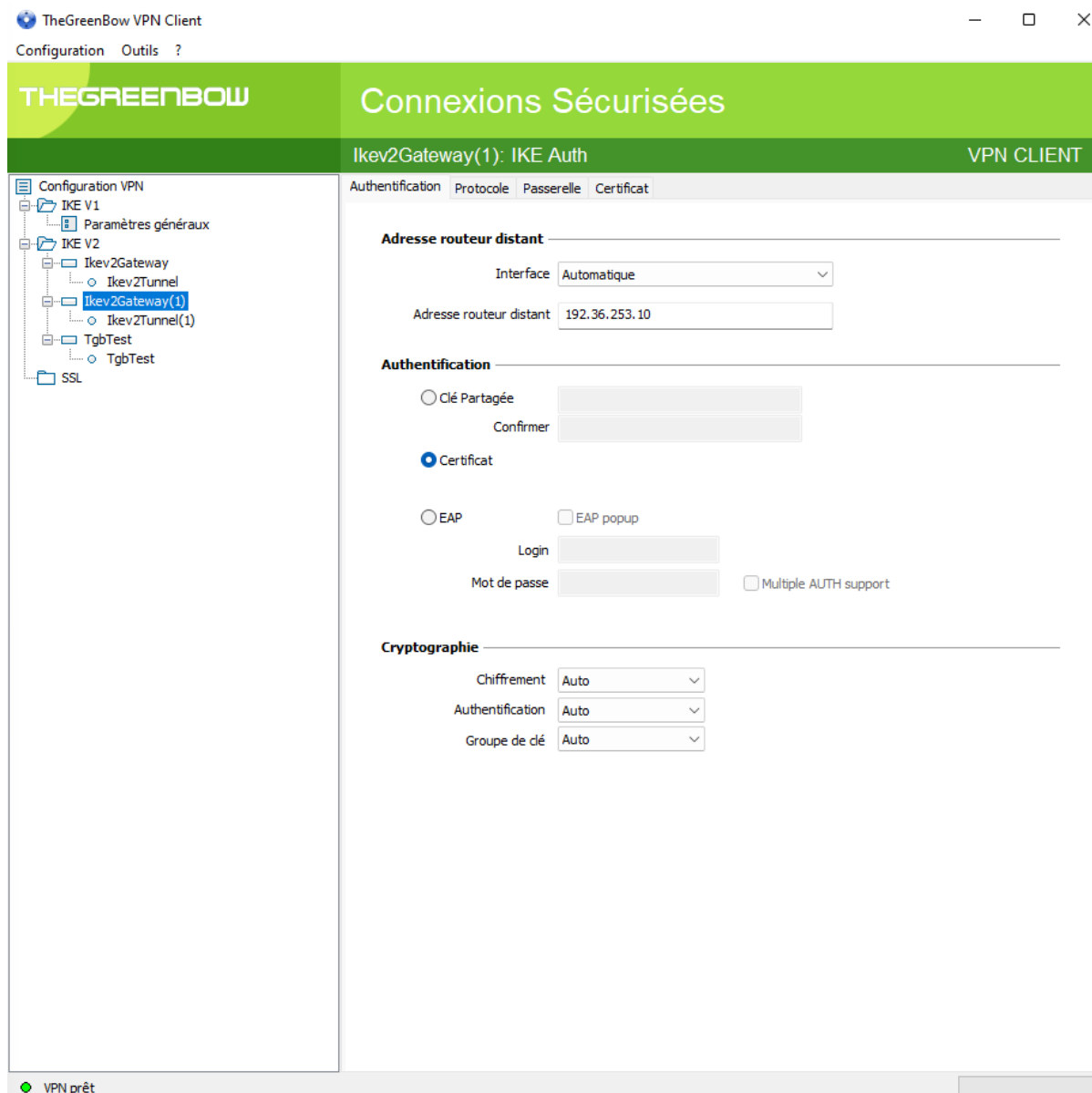
Nom ou adresse IP de la passerelle : 192.36.253.10

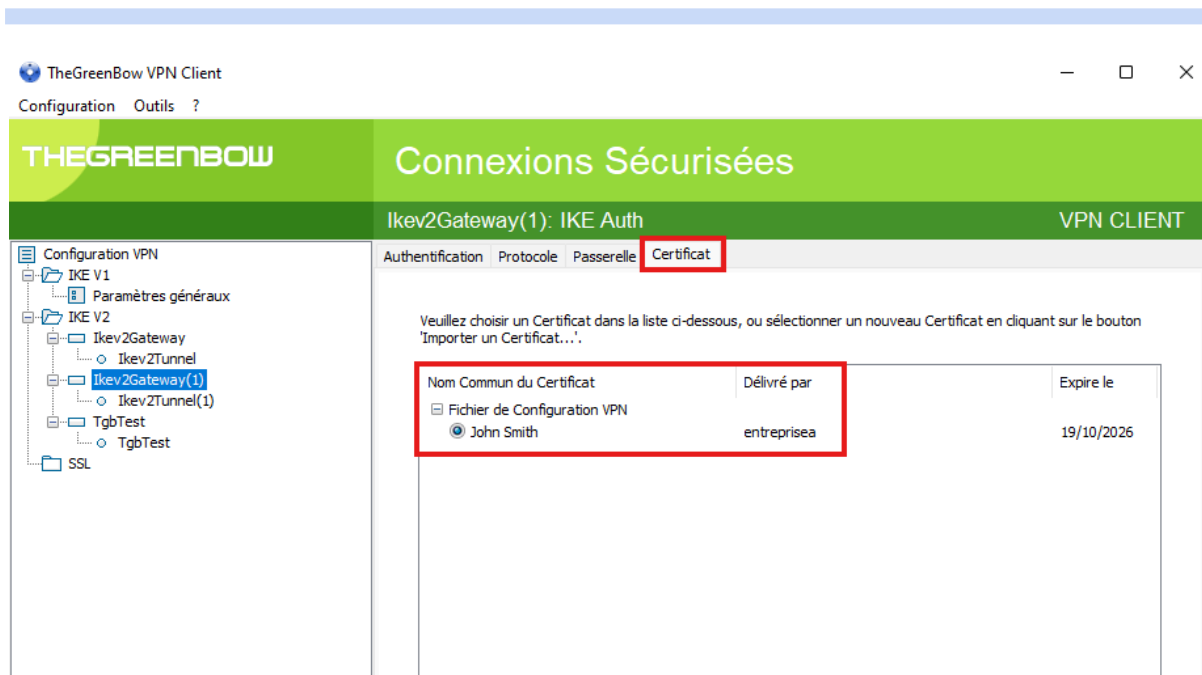
Nom commun du certificat : John Smith

Vous pouvez modifier ces paramètres à tout moment directement dans l'interface principale.

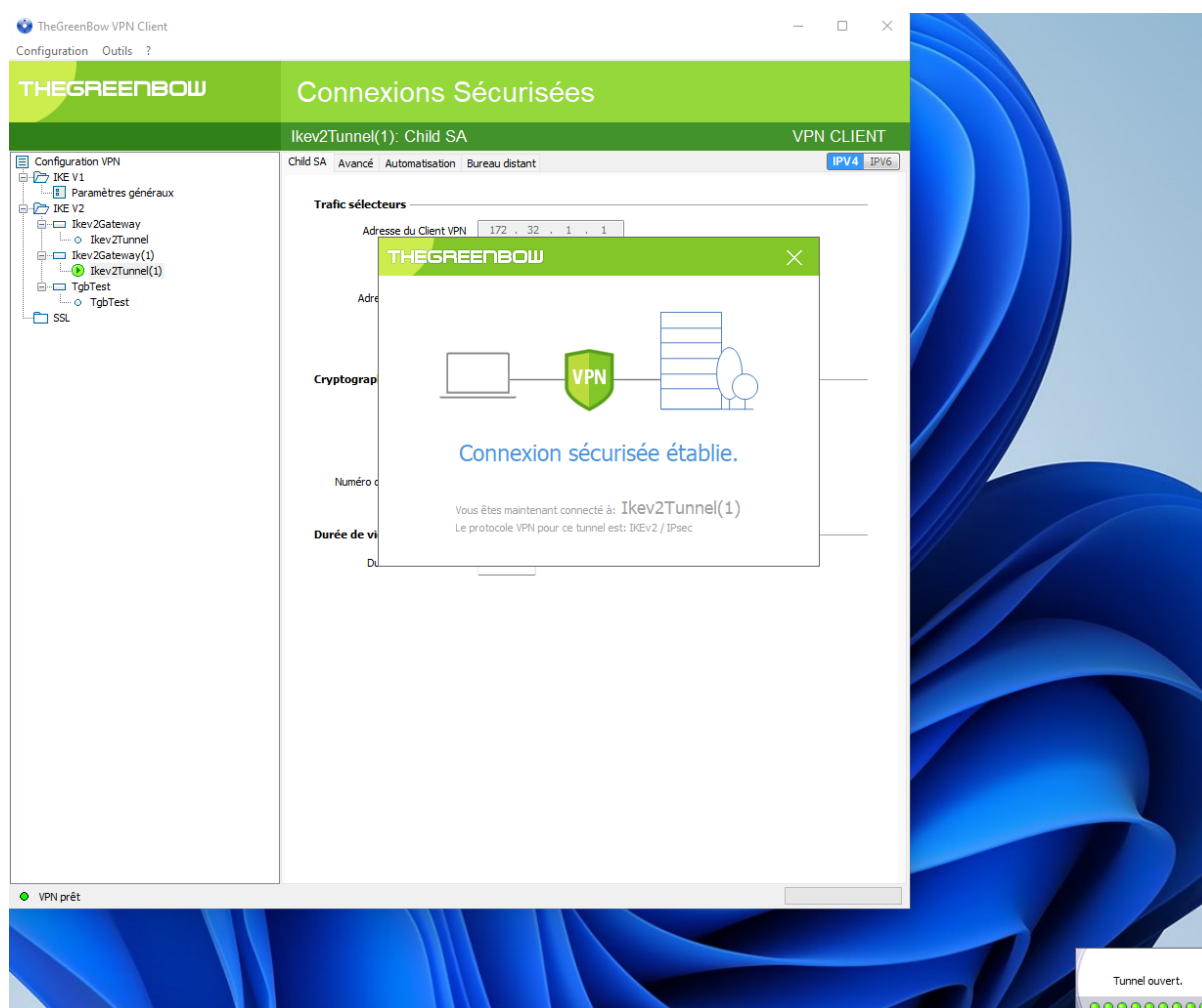
6. Paramétrage du VPN

- 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

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

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

MONITOR / TUNNELS VPN IPSEC

Actualiser Configurer le service VPN IPsec

POLITIQUES

Type	Etat	Extrémité de trafic locale	Passerelle locale	Local ID ↓	Passerelle distante	ID du correspon...	Extrémité de trafic distante
Type : Tunnels site à site (1)							
●	Aucun tun...	Firewall_VTL_yers_A	Firewall_out	192.36.253.10	Frw_B	192.36.253.20	IP_VTL_B
Type : Tunnels mobiles (1)							
●	OK	Network_dtmz1	C=FR, ST=France, L=Saint-Raphael, O=entreprise, OU=entreprise, CN=sns.a.net			%any	
Type : Politiques d'exception (bypass) (1)							
Bypass	rfc5735_loopback	localhost	localhost	any			

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

```

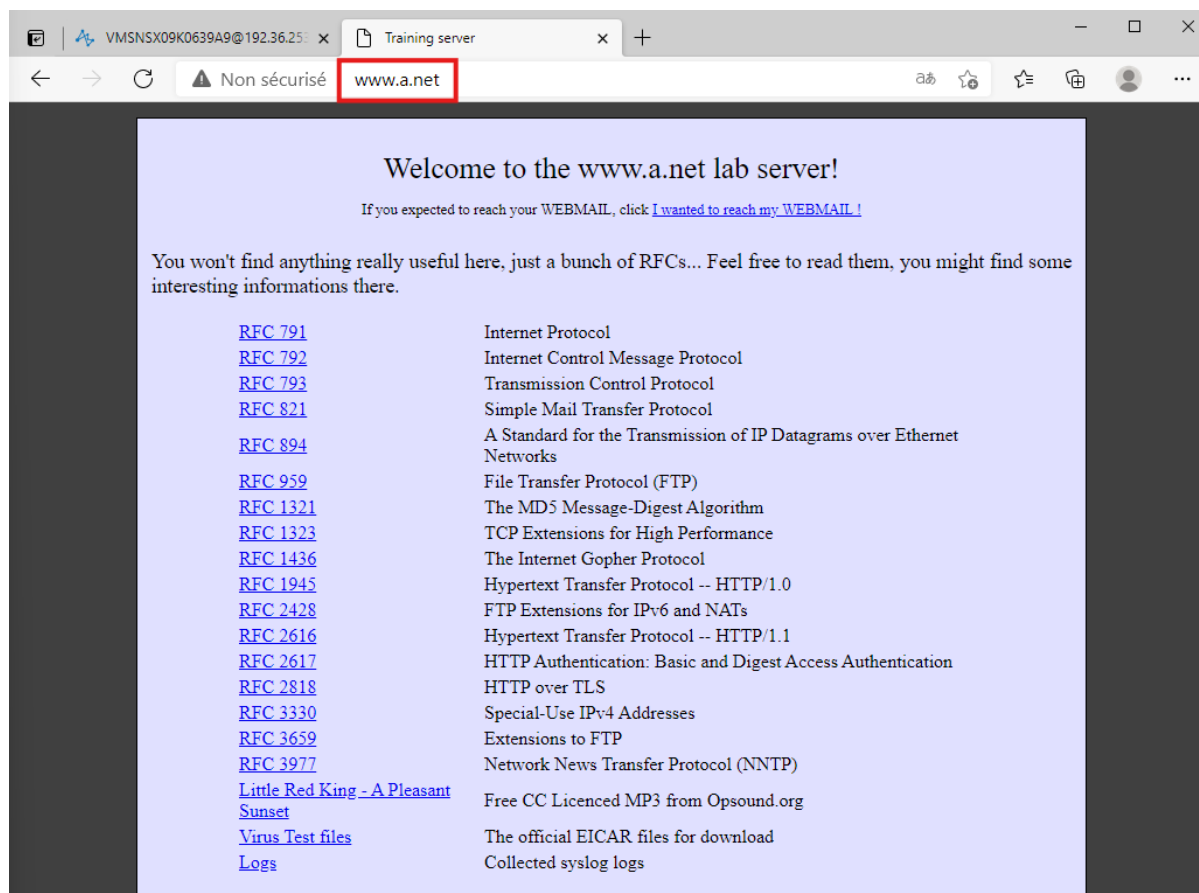
C:\Users\LocalAdmin>netstat -rn
=====
Liste d'Interfaces
  9...08 00 27 c1 3e ba .....Intel(R) PRO/1000 MT Desktop Adapter
  6...08 00 27 dc 48 7a .....Intel(R) PRO/1000 MT Desktop Adapter #2
 14...02 50 f2 69 3b 00 .....TheGreenBow Virtual Miniport Adapter
 1.....Software Loopback Interface 1
=====

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
  0.0.0.0              0.0.0.0          192.168.1.1        192.168.1.13      25
 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    172.32.1.2         172.32.1.1        36
172.32.1.1            255.255.255.255 On-link            172.32.1.1        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
192.168.1.0           255.255.255.0    On-link            192.168.1.13      281
192.168.1.13          255.255.255.255 On-link            192.168.1.13      281
192.168.1.255         255.255.255.255 On-link            192.168.1.13      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            192.168.1.13      281
224.0.0.0             240.0.0.0        On-link            172.32.1.1        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            192.168.1.13      281
255.255.255.255       255.255.255.255 On-link            172.32.1.1        291
=====
Itinéraires persistants :
Adresse réseau    Masque réseau    Adresse passerelle    Métrique
  0.0.0.0          0.0.0.0          192.36.253.1          Par défaut
=====

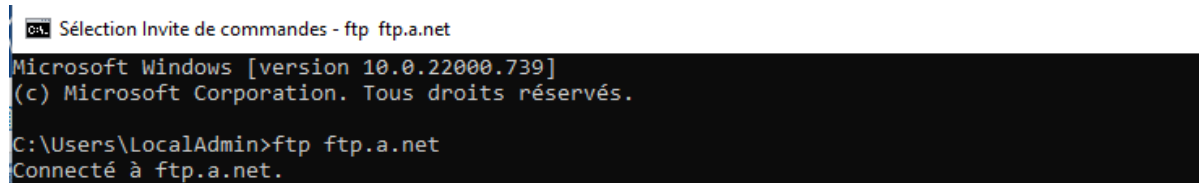
```

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.



```
Invite de commandes
Microsoft Windows [version 10.0.22000.739]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\LocalAdmin>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=7 ms TTL=64
Réponse de 172.16.1.12 : octets=32 temps=5 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=3 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 = 2ms, Maximum = 7ms, Moyenne = 4ms

C:\Users\LocalAdmin>
```