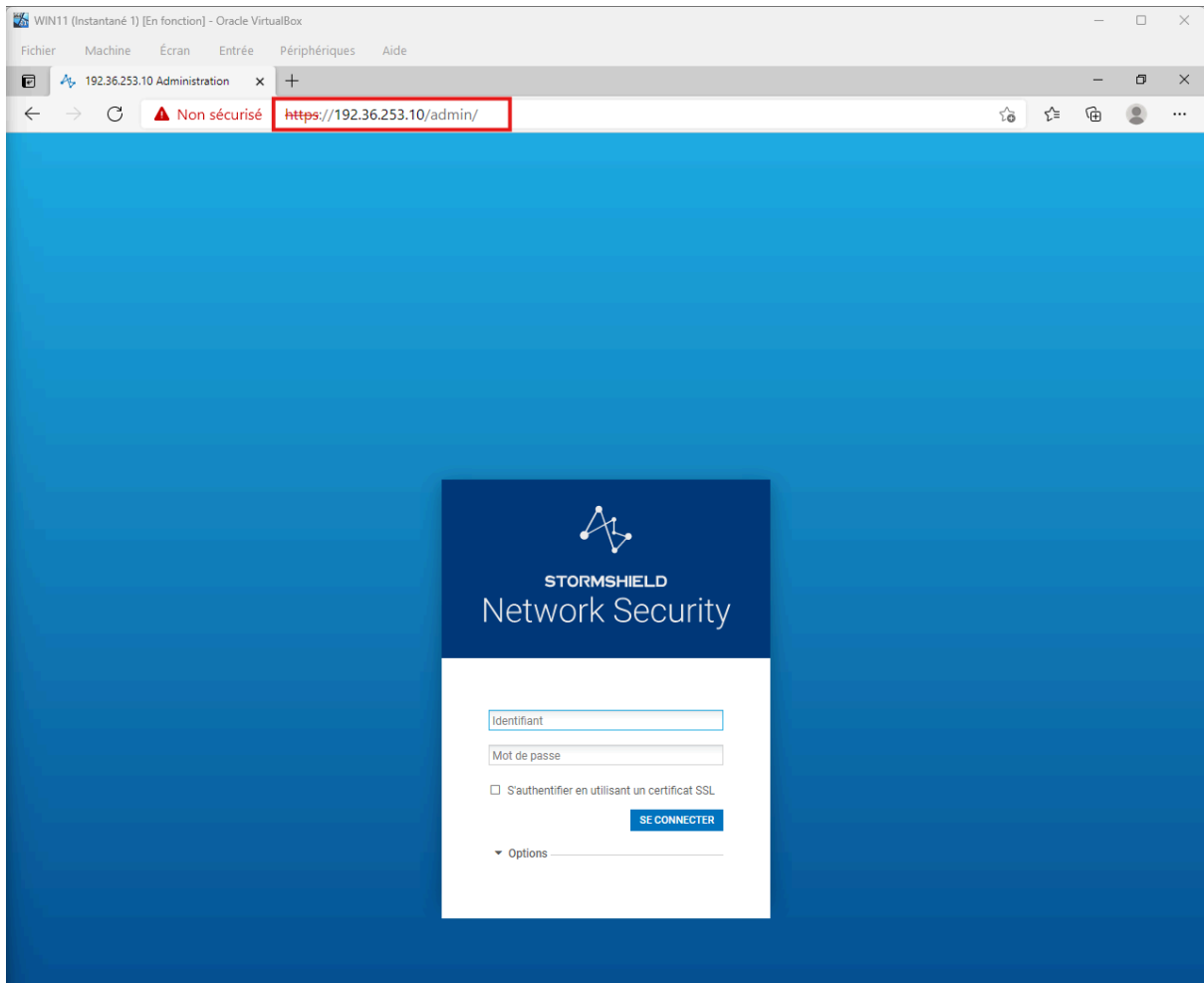

Lab 12 – Nomade VPN IPsec avec certificat

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
admin ÉCRITURE LOGS - ACCÈS R

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_entrisea

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: Clé pré-partagée (PSK)

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_entrisea

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 screenshot displays the Stormshield Network Security v4.3.11 interface. The top navigation bar includes 'MONITORING' and 'CONFIGURATION' tabs, with 'EVA1' and 'VMSNSX09K0639A9' displayed. The left sidebar contains various system icons. The main content area is titled 'VPN / VPN IPSEC' and has sub-tabs for 'POLITIQUE DE CHIFFREMENT - TUNNELS', 'CORRESPONDANTS', 'IDENTIFICATION', and 'PROFILS DE CHIFFREMENT'. The 'IDENTIFICATION' tab is active, showing 'AUTORITÉ DE CERTIFICATION ACCEPTÉES'. A table lists the accepted authorities, with 'entreprisea' highlighted in yellow. A red box highlights the '+ Ajouter' button and the 'entreprisea' entry. A dropdown menu is open, showing 'Certificat' and a list of certificates: 'SSL proxy default authority', 'sslvpn-full-default-authority', and 'entreprisea' (highlighted in yellow). The bottom status bar indicates 'TUNNELS MOBILES : CI ES PRÉ-PARTAGÉES (PSK)'.

STORMSHIELD v4.3.11 Network Security

MONITORING CONFIGURATION EVA1 VMSNSX09K0639A9

VPN / VPN IPSEC

POLITIQUE DE CHIFFREMENT - TUNNELS CORRESPONDANTS IDENTIFICATION PROFILS DE CHIFFREMENT

AUTORITÉ DE CERTIFICATION ACCEPTÉES

+ Ajouter x Supprimer

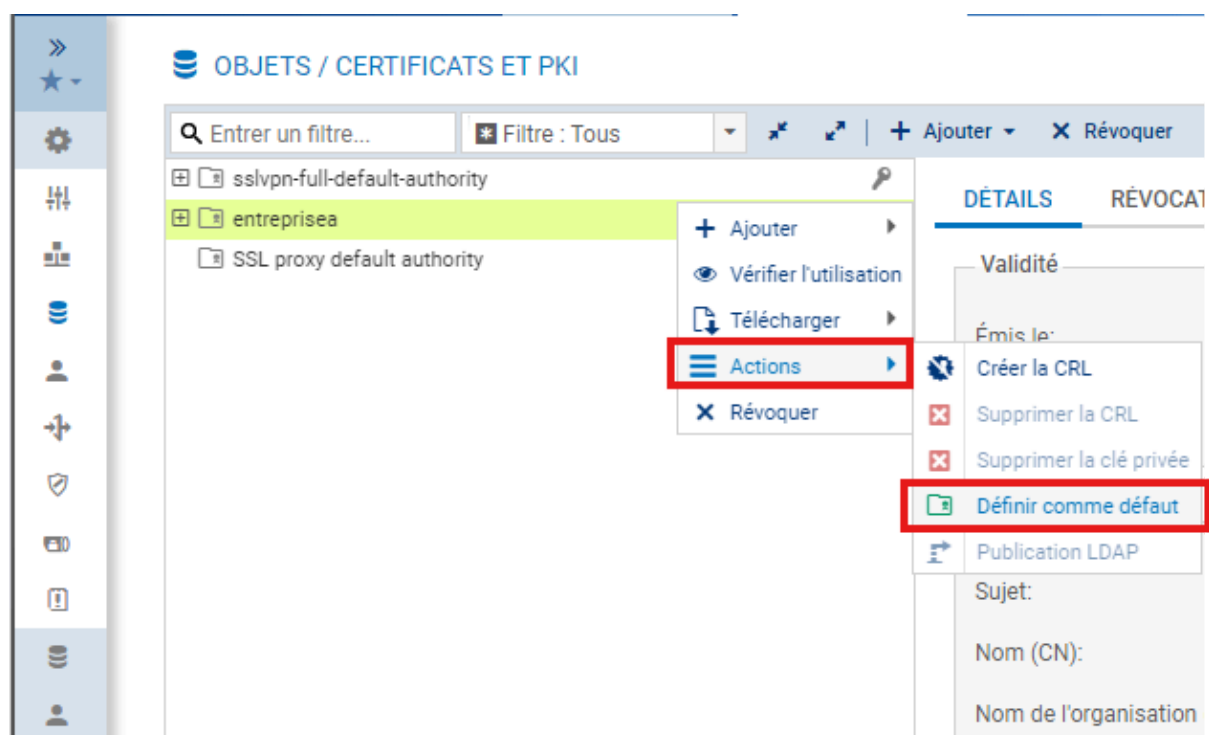
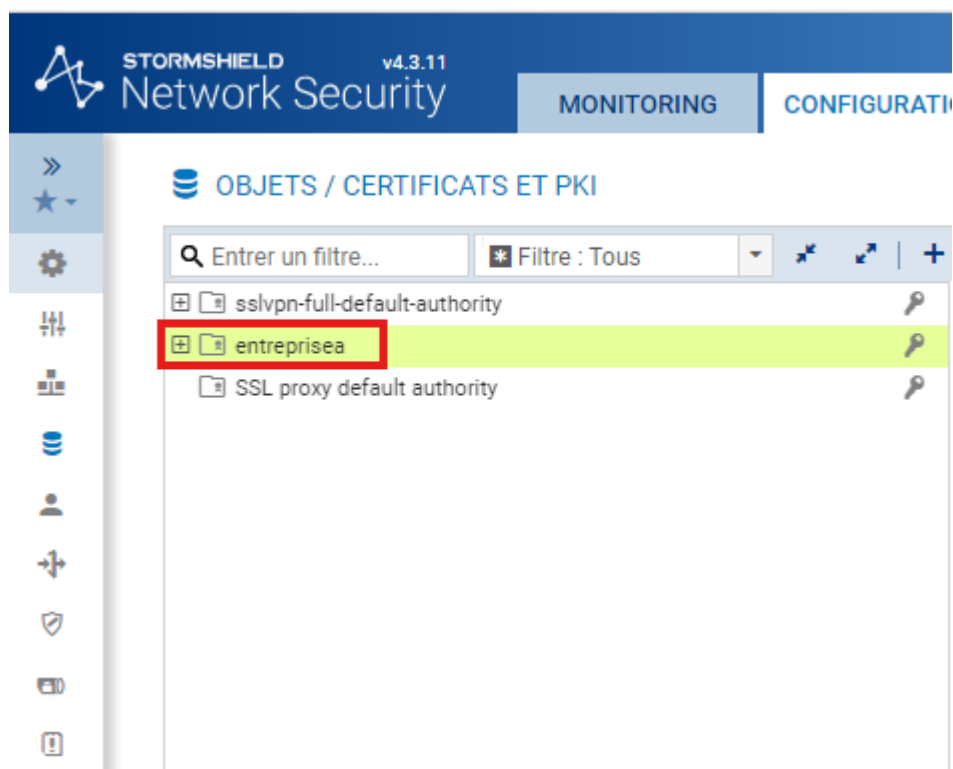
Autorité de Certification
CA
entreprisea

Certificat

- SSL proxy default authority
- sslvpn-full-default-authority
- entreprisea

TUNNELS MOBILES : CI ES PRÉ-PARTAGÉES (PSK)

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

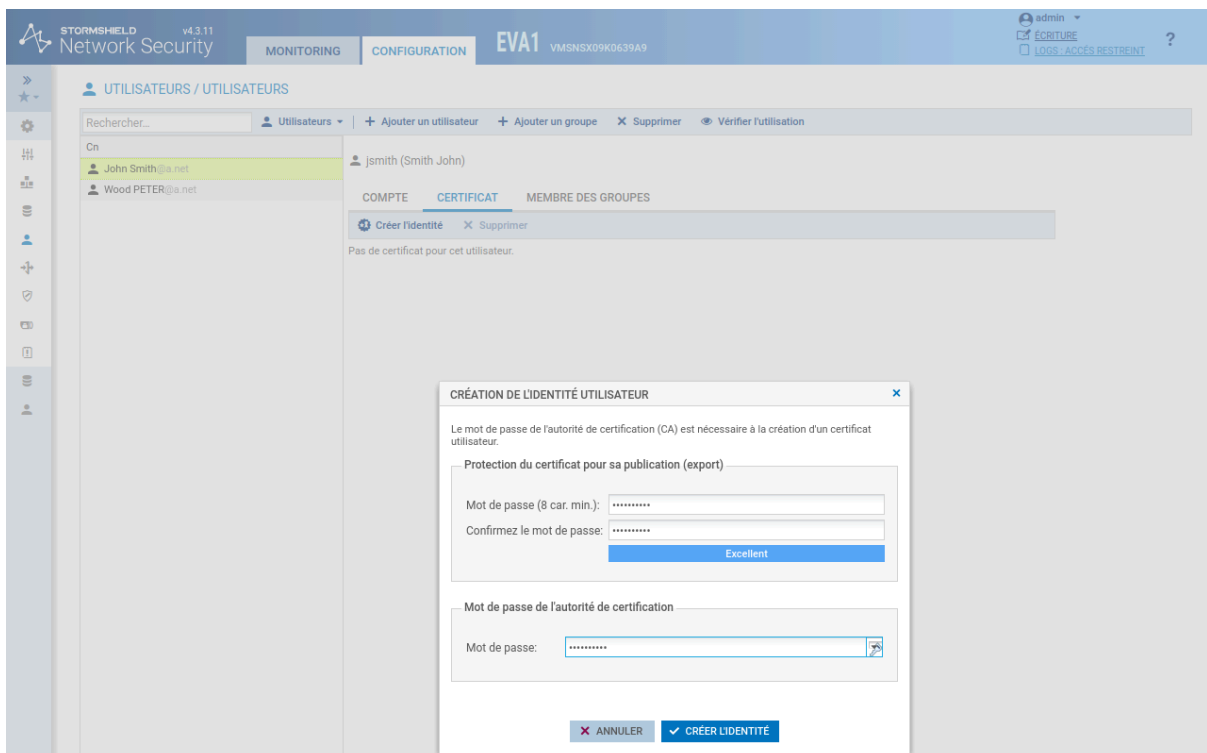
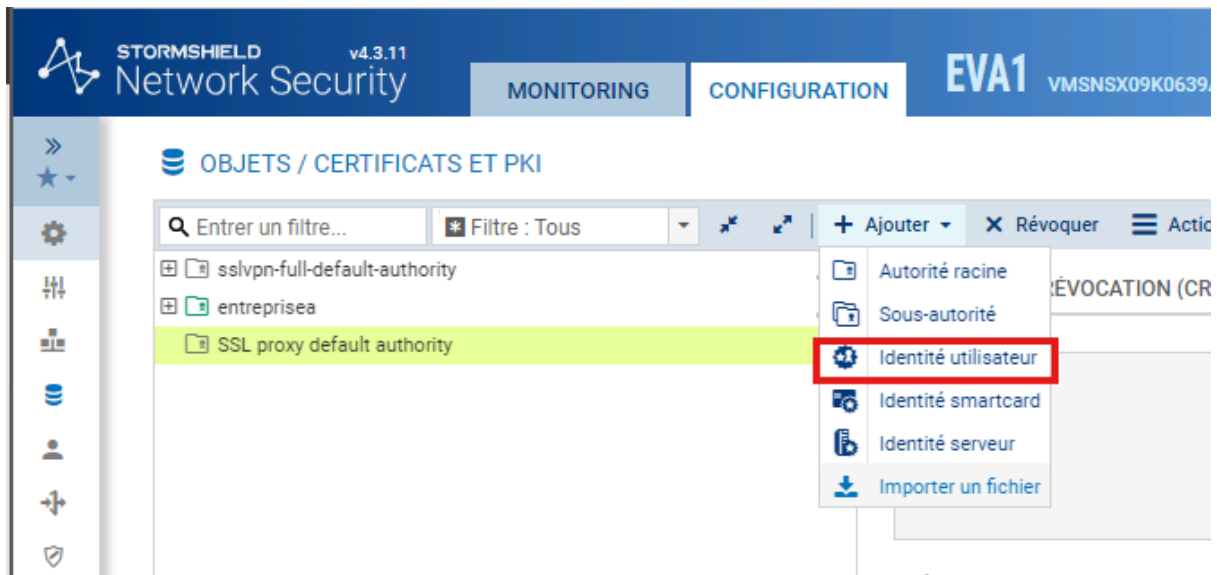


- Après l'avoir définie par défaut il apparaît en vert



3. Création du certificat utilisateur

- Création du certificat de l'utilisateur John Smith



UTILISATEURS / UTILISATEURS

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

Cn
 John Smith@a.net
 Wood PETER@a.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@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 ECRITURE LOGS - ACCES RESTREINT ?

OBJETS / CERTIFICATS ET PKI

Entrer 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@a.net

4. Configuration des droits et pare-feu

- Configuration des règles de pare-feu

The screenshot displays the Stormshield management interface. At the top, the navigation menu includes 'UTILISATEURS / DROITS D'ACCÈS'. Below this, there are tabs for 'ACCÈS PAR DÉFAUT', 'ACCÈS DÉTAILLÉ', and 'SERVEUR PPTP'. The 'ACCÈS DÉTAILLÉ' tab is active, showing a table of user access configurations. The table has columns for 'Etat', 'Utilisateur - groupe d'utilisateurs', 'VPN SSL Portail', 'IPSEC', 'VPN SSL', 'Parrainage', and 'Description'. The first row shows a user 'jsmith@a.net' with 'Activé' status, 'Interdire' for VPN SSL Portail, 'Autoriser' for IPSEC, 'Autoriser' for VPN SSL, and 'Interdire' for Parrainage.

Below the user access table, there is a list of firewall rules. The table has columns for rule number, status, action, user/group, destination, services, and creation date. Rule 34 is highlighted in green and is the focus of the configuration. It is named 'Net-IPSECVPN Auth. par VPN IPsec via Tunnel VPN IPsec', has a status of 'on', an action of 'passer', and is applied to the 'Network_dmz1' destination. The services listed are 'http', 'ftp', and 'dns_udp'. The rule was created on 2025-10-18 at 16:38:36.

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

Numéro	Statut	Action	Utilisateur / Groupe	Destination	Services	Date de création
32	on	passer	Any	Firewall_out	isakmp, isakmp_natt	Créée le 2025-10-18 16:37:18, pa...
33	on	passer	Any	Firewall_out	Any, vpn-esp	Créée 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	Créée 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...	Créée 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 VPN CLIENT

IKE V2

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) :
de la passerelle distante

Nom Commun du Certificat

Importer un Certificat...

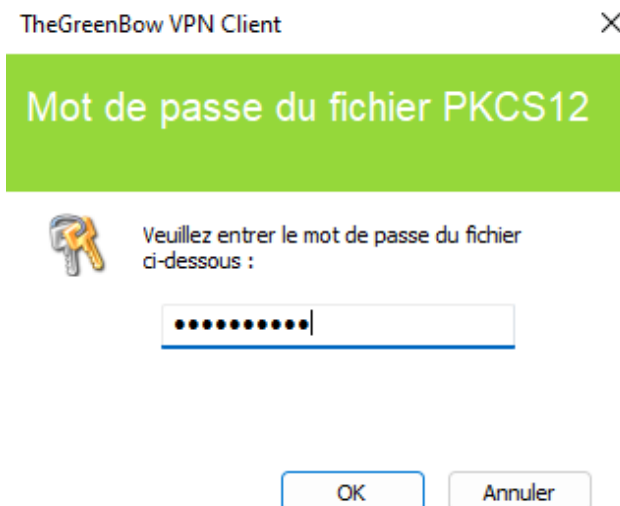
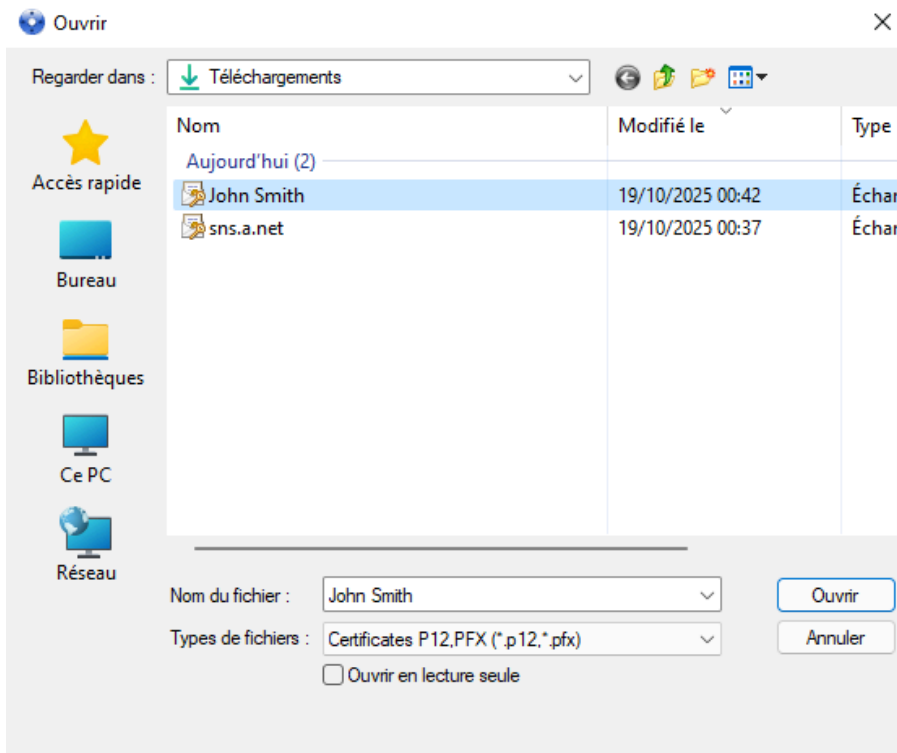
Clé Partagée

Certificat

< Précédent

Suivant >

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.

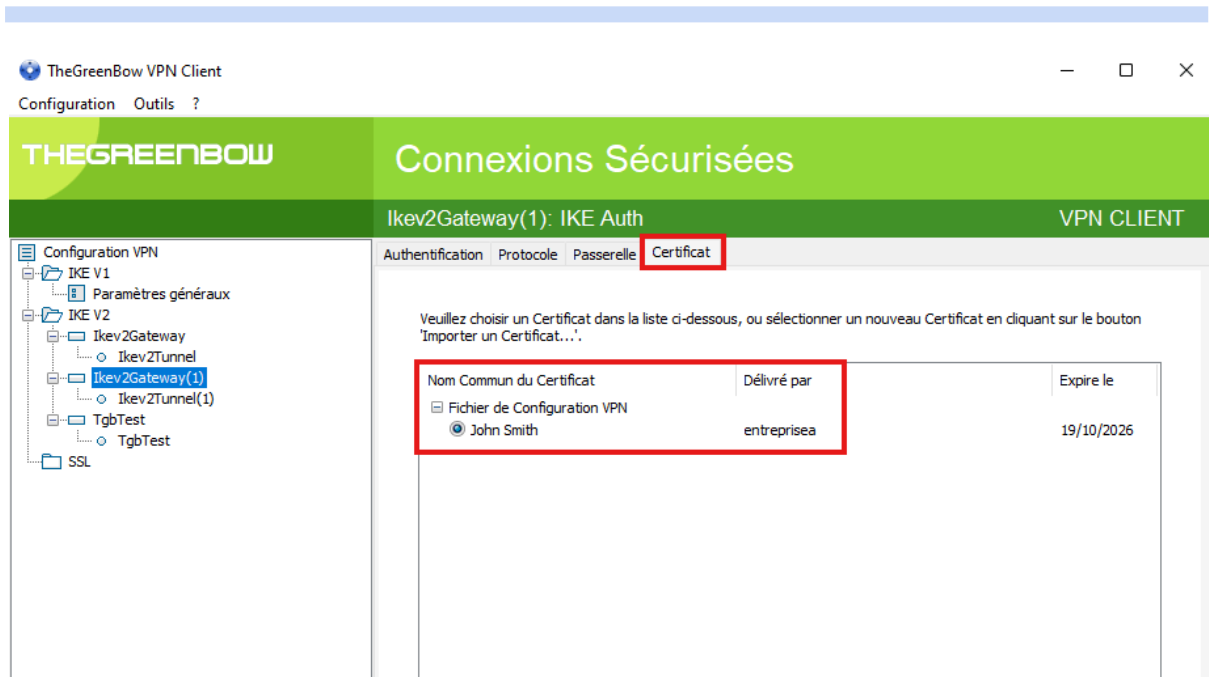
6. Paramétrage du VPN

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

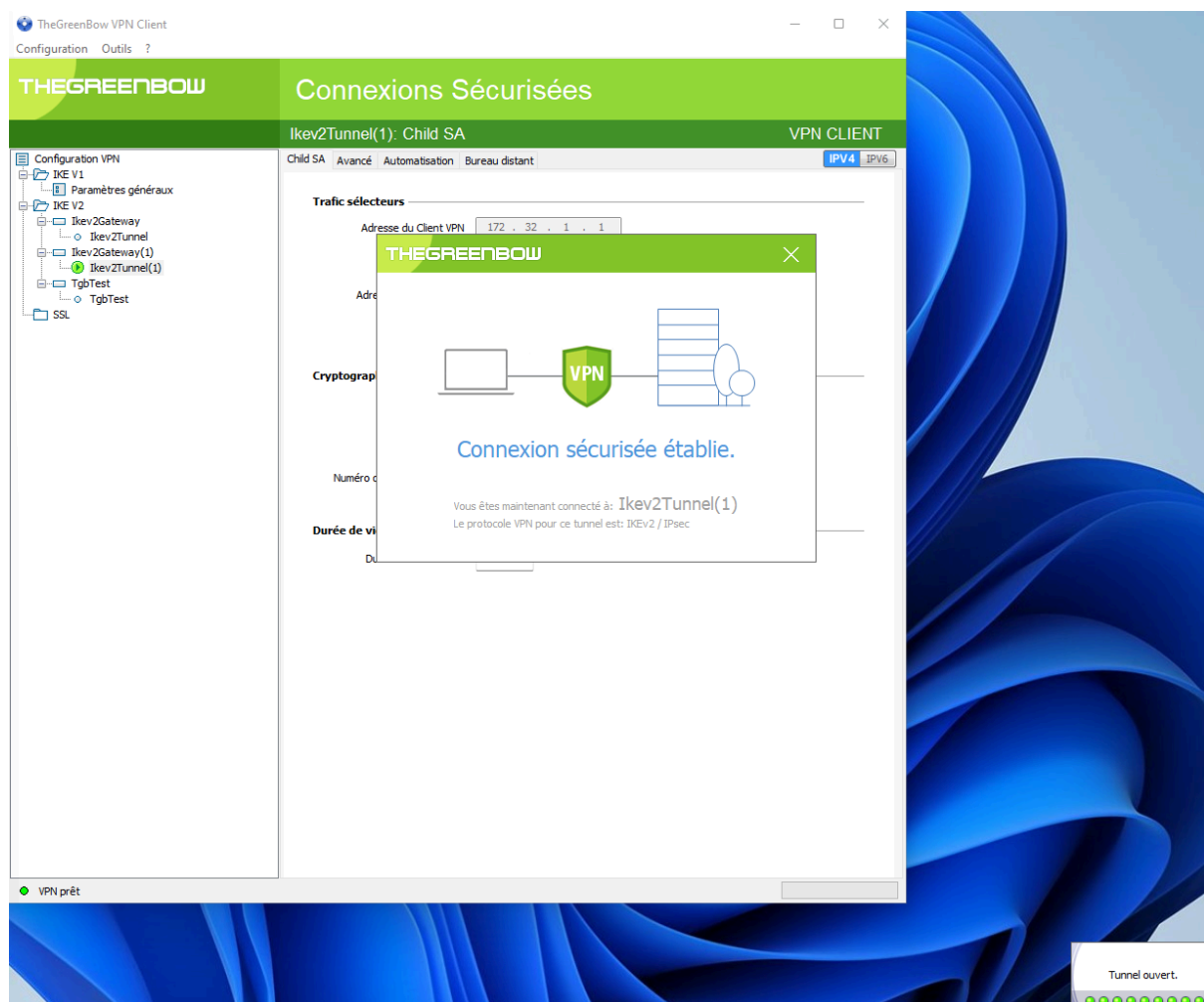
The screenshot shows the configuration window for 'Ikev2Gateway(1): IKE Auth' in TheGreenBow VPN Client. The window title is 'TheGreenBow VPN Client' and it has standard window controls. The main header is 'Connexions Sécurisées' and the sub-header is 'VPN CLIENT'. The left sidebar shows a tree view of the configuration, with 'Ikev2Gateway(1)' selected. The main area is divided into tabs: 'Authentification', 'Protocole', 'Passerelle', and 'Certificat'. The 'Authentification' tab is active, showing the following settings:

- Adresse routeur distant:** Interface: Automatique (dropdown), Adresse routeur distant: 192.36.253.10 (text input).
- Authentification:** Clé Partagée, Certificat, EAP. Under Clé Partagée, there are 'Confirmer' and 'Mot de passe' fields. Under EAP, there is an 'EAP popup' checkbox, a 'Login' field, and a 'Multiple AUTH support' checkbox.
- Cryptographie:** Chiffrement: Auto (dropdown), Authentification: Auto (dropdown), Groupe de clé: Auto (dropdown).

At the bottom left, there is a status indicator: a green dot followed by 'VPN prêt'.



▪ La connexion a été établie



TheGreenBow VPN Client
Configuration Outils ?

THEGREENBOW Connexions Sécurisées VPN CLIENT

Ikev2Tunnel(1): Child SA

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 VPN CLIENT

Ikev2Tunnel(1): Child SA

Child SA Avancé Automatisation Bureau distant **IPV4** IPV6

Serveurs alternatifs

Suffixe DNS

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_VTLyers_A	Firewall_out	192.36.253.10	Fw_B	192.36.253.20	IP_VTLB
Type : Tunnels mobiles (1)							
DK		Network_dmrz1	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.

```

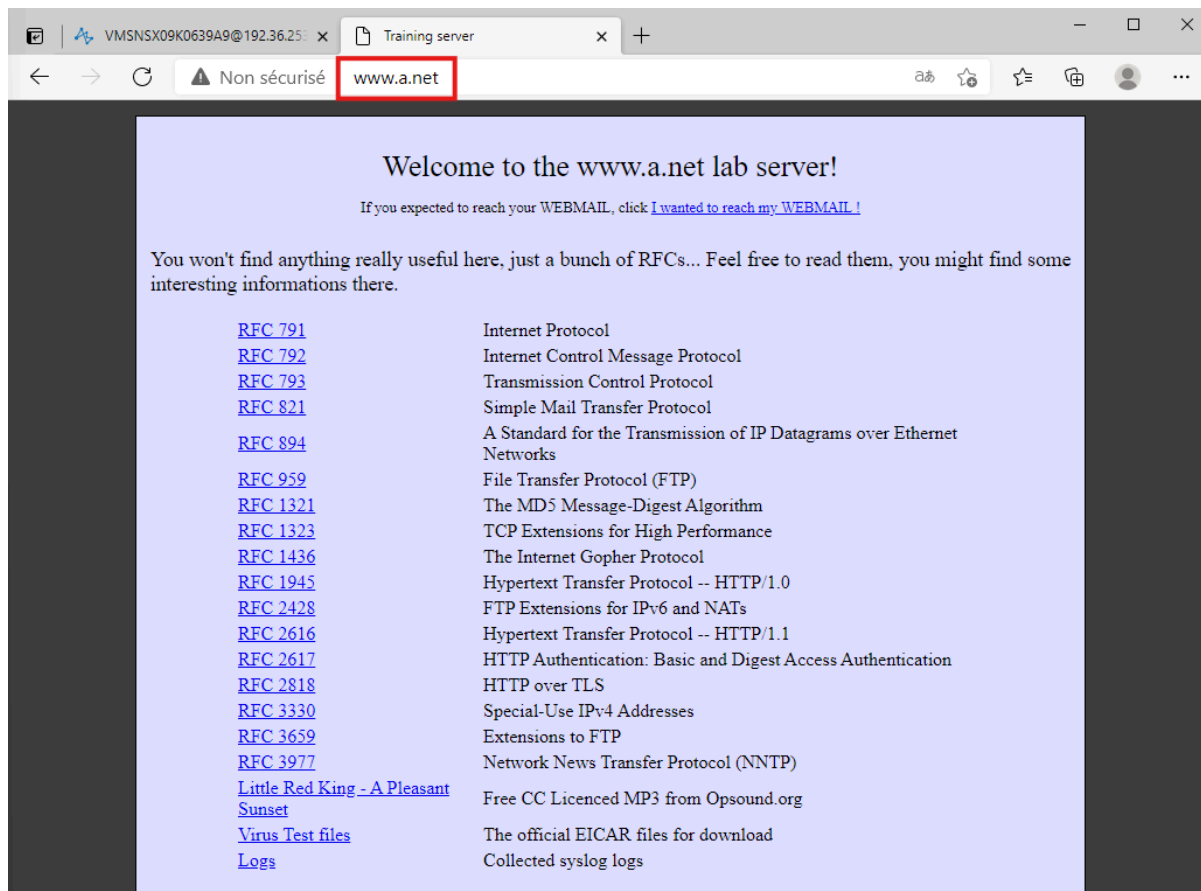
C:\Users\LocalAdmin>netstat -rn
=====
Liste d'Interfaces
 9...08 00 27 c1 3e ba .....Intel(R) PRO/1000 MT Desktop Adapter
 6...08 00 27 dc 48 7a .....Intel(R) PRO/1000 MT Desktop Adapter #2
14...02 50 f2 69 3b 00 .....TheGreenBow Virtual Miniport Adapter
 1.....Software Loopback Interface 1
=====

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)

```
cmd. Sélection Invite de commandes - ftp ftp.a.net
Microsoft Windows [version 10.0.22000.739]
(c) Microsoft Corporation. Tous droits réservés.

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