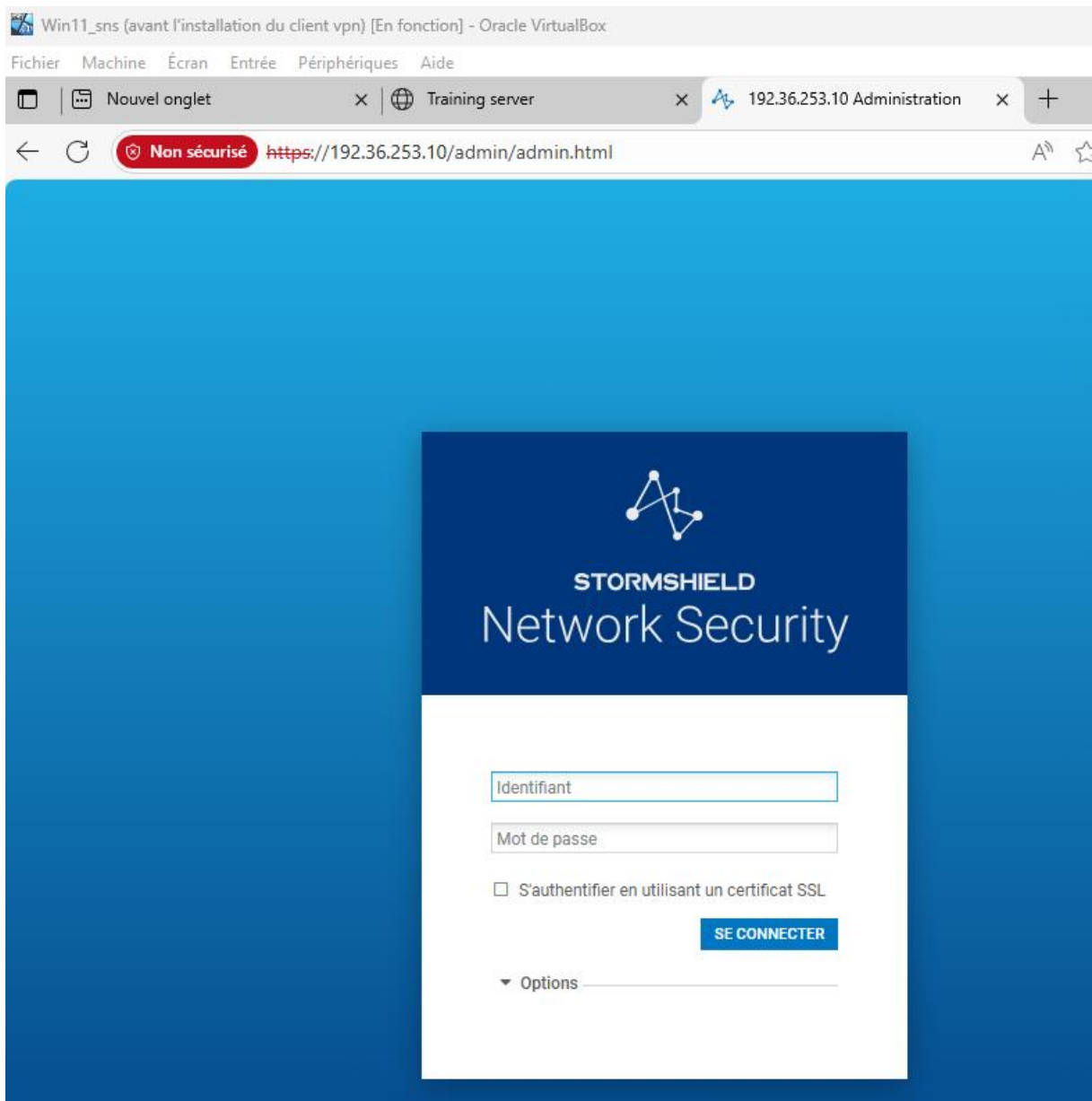


Lab 12 – Nomade VPN IPsec avec certificat

Table des matières

Lab 12 – Nomade VPN IPsec avec certificat 1

- Nous nous connectons au SNS via la machine Win 11.



- Nous mettons le certificat à la place de la clé pré-partagée.

VPN / VPN IPSEC

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

MOBILE_ENTREPRISEA

Général

Commentaire:

Passerelle distante: Any

Adresse locale: Any

Profil IKE: IKEphase1Nomade

Version IKE: IKEv2

Identification

Méthode d'authentification: Certificat

Certificat:

Local ID:

ID du correspondant: Saisir un identifiant (optionnel)

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**

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

🔍 Entrez un filtre...

📁 Passerelles distantes (1)

Site_fw_B

📁 Correspondants mobiles (1)

mobile_entreprisea

MOBILE_ENTREPRISEA

Général

Commentaire:

Passerelle distante: Any

Adresse locale:

Profil IKE:

Version IKE:

Identification

Méthode d'authentification:

Certificat:

Local ID:

ID du correspondant:

Clé pré-partagée (PSK): Éditer

◦ Nous mettons l'entreprise a dans Autorité de certification acceptées.

AUTORITÉ DE CERTIFICATION ACCEPTÉES

+ Ajouter × Supprimer

CA
entreprisea

TUNNELS MOBILES : CLÉS PRÉ-PARTAGÉES (PSK)

🔍 Clé recherchée + Ajouter × Supprimer ✎ Éditer la sélection 📄 Exporter la liste des PSK

Identité	Clé
jsmith@a.net	0x4d6150534b21

- Nous créons le certificat de l'utilisateur jsmith.

UTILISATEURS / UTILISATEURS

Rechercher... Utilisateurs + Ajouter un utilisateur + Ajouter un groupe X Supprimer

Cn

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

jsmith (Smith John)

COMPTE CERTIFICAT MEMBRE DES GROUPES

Créer l'identité X Supprimer

Pas de certificat pour cet utilisateur.

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:

Faible

Mot de passe de l'autorité de certification

Mot de passe:

X ANNULER

✓ CRÉER L'IDENTITÉ

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 12 15:00:31 2025 GMT
Expiration:	Oct 13 15:00:31 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:	

- Nous vérifions que l'utilisateur apparaît dans la PKI.

OBJETS / CERTIFICATS ET PKI

Entrer un filtre... Filtre : Tous

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

- Nous activons l'IPsec pour l'utilisateur jsmith.

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
1	Activé	jsmith@a.net	Interdire	Autoriser	Autoriser	Interdire

POLITIQUE DE SÉCURITÉ / FILTRAGE ET NAT

(9) Lab_9 Editer Exporter

FILTRAGE NAT

Rechercher... + Nouvelle règle X Supprimer ↑ ↓ Couper Copier Coller

	État	Action	Source	Destination	Port dest.	Protocole	Inspect
VPN IPsec nomade / site à site (contient 4 règles, de 1 à 4)							
1	on	passer	Any	Firewall_out	isakmp isakmp_natt		IPS
2	on	passer	Any	Firewall_out	Any	vpn-esp	IPS
3	on	passer	jsmith@ Net-IP-SecVP Auth. par :VPN IPsec via Tunnel VPN IPsec	Network_dmz1	http ftp dns_udp		IPS
4	on	passer	jsmith@ Net-IP-SecVP Auth. par :VPN IPsec via Tunnel VPN IPsec	Network_dmz1	Any	icmp (requête Ech	IPS

- Nous créons un nouveau tunnel VPN avec certificat.

TheGreenBow VPN Client

Configuration Outils ?

THEGREENBOW Connexions Sécurisées

IKE V2 VPN CLIENT

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

VPN prêt



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

Clé Partagée

Certificat



Importer un nouveau Certificat.

Choisir ci-dessous le format du Certificat :

Format PEM

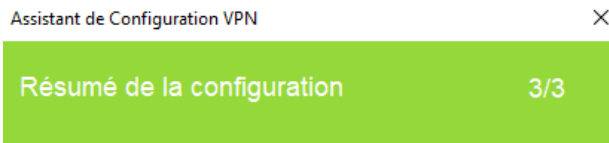
Format P12



Mot de passe du fichier PKCS12



Veuillez entrer le mot de passe du fichier ci-dessous :

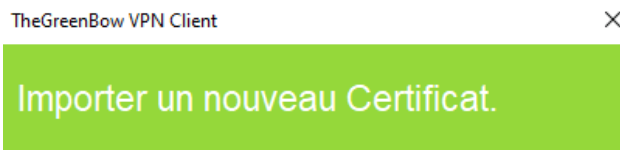


La configuration du tunnel est correctement terminée :

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.

< Précédent Terminer Annuler

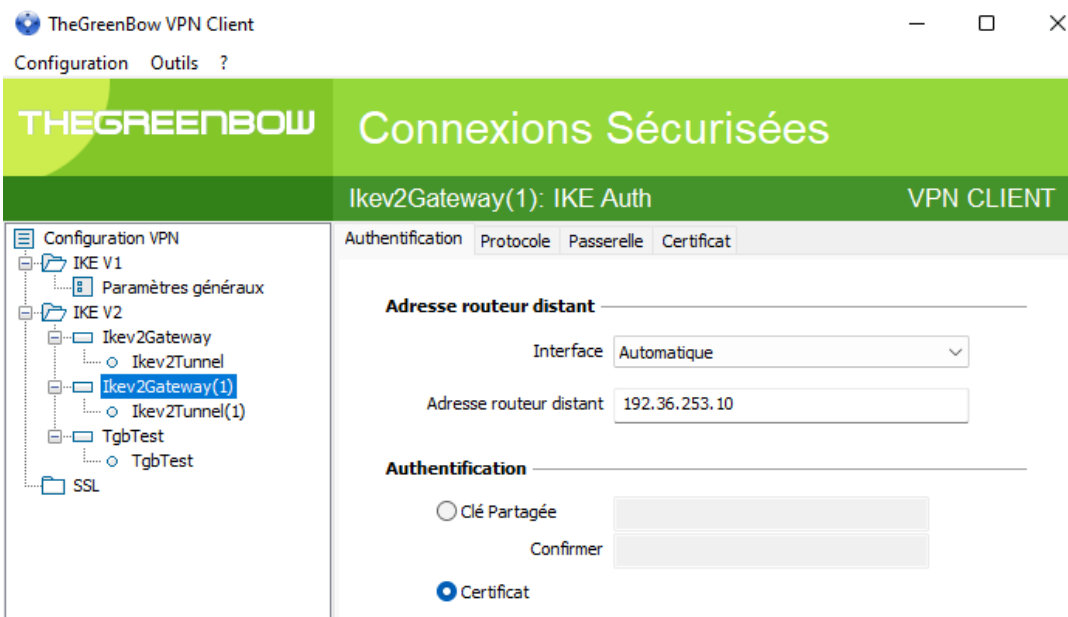


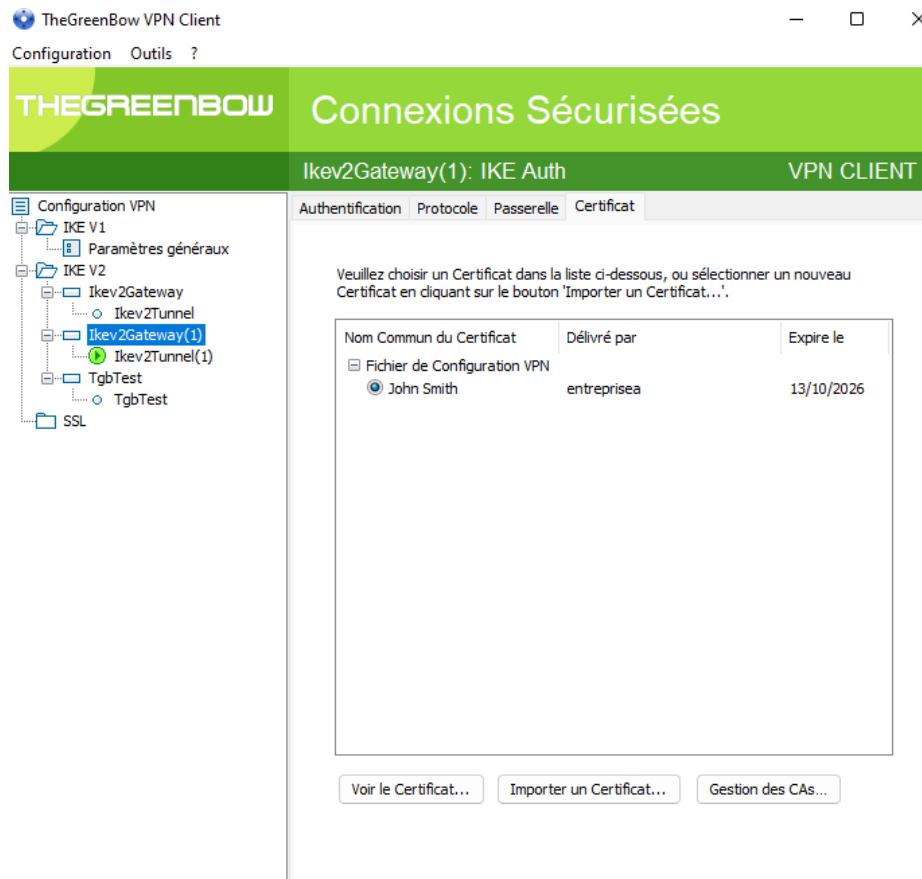
Importer un Certificat P12 dans le fichier de Configuration VPN.

Certificat P12 C:\Users\X\Desktop\John Smith.p Parcourir

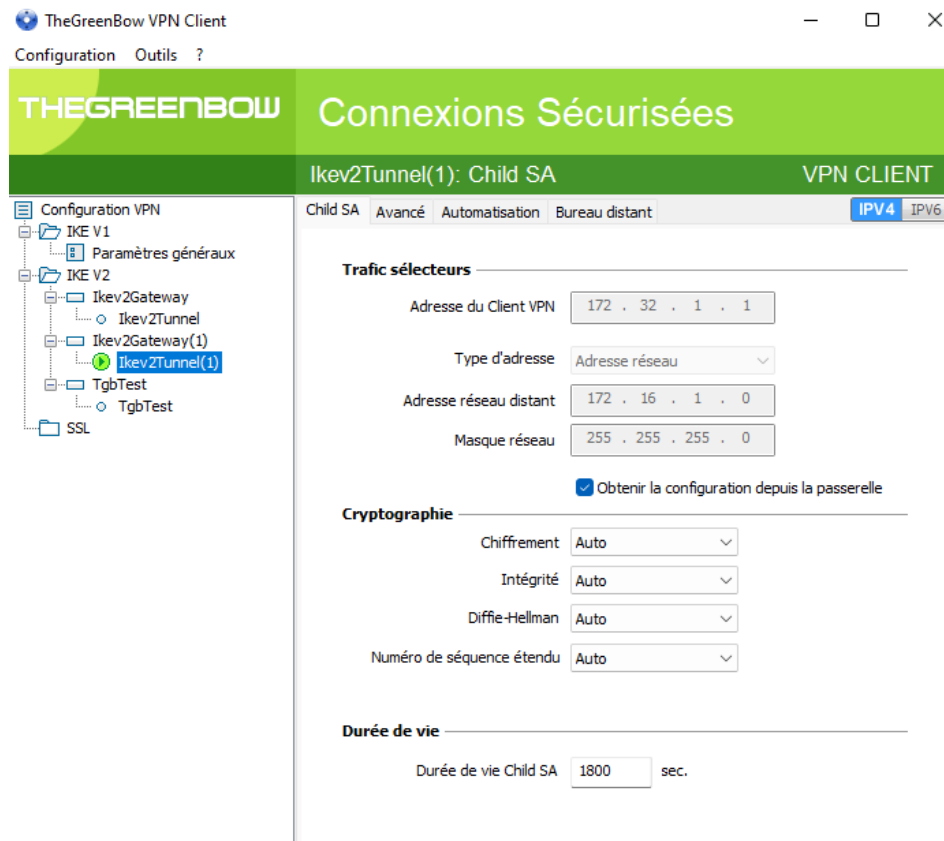
< Précédent OK Annuler

- Une fois le tunnel monté, nous vérifions que le certificat est bien celui de John Smith.





- Nous exécutons le VPN et constatons que nous retrouvons les mêmes informations qu'avec le tunnel par PSK.



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

	Type	Adresse IP
(i)	DNS	172.16.1.10 ✖

Test de trafic dans le tunnel

Periodicité et adresse IP de la machine distante à pinger:

Adresse IPV4

Fréquence de test sec.

- Nous voyons que le tunnel est bien configuré.

MONITOR / TUNNELS VPN IPSEC

Actualiser
[Configurer le service VPN IPsec](#)

POLITIQUES

Type	État	Extrémité de...	Passerelle l...	Local ID	Passerelle d...	ID du correspon...	Extrémité de...
Type : Tunnels site à site (1)							
Type : Tunnels mobiles (1)							
	OK	Network_dm...		C=FR, ST=Franc...		%any	

- Nous affichons la table de routage sur WIN11.

```
C:\Users\X>netstat -rn
=====
Liste d'Interfaces
 7...08 00 27 4c 9b 75 .....Intel(R) PRO/1000 MT Desktop Adapter
12...02 50 f2 e3 34 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  172.32.1.2     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
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         172.32.1.1     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         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
=====
```

- Nous testons l'accès au site WEB et FTP.



```
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=2 ms TTL=64
Réponse de 172.16.1.12 : octets=32 temps=1 ms TTL=64
Réponse de 172.16.1.12 : octets=32 temps=1 ms TTL=64
Réponse de 172.16.1.12 : octets=32 temps=1 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 = 2ms, Moyenne = 1ms

C:\Users\X>_
```