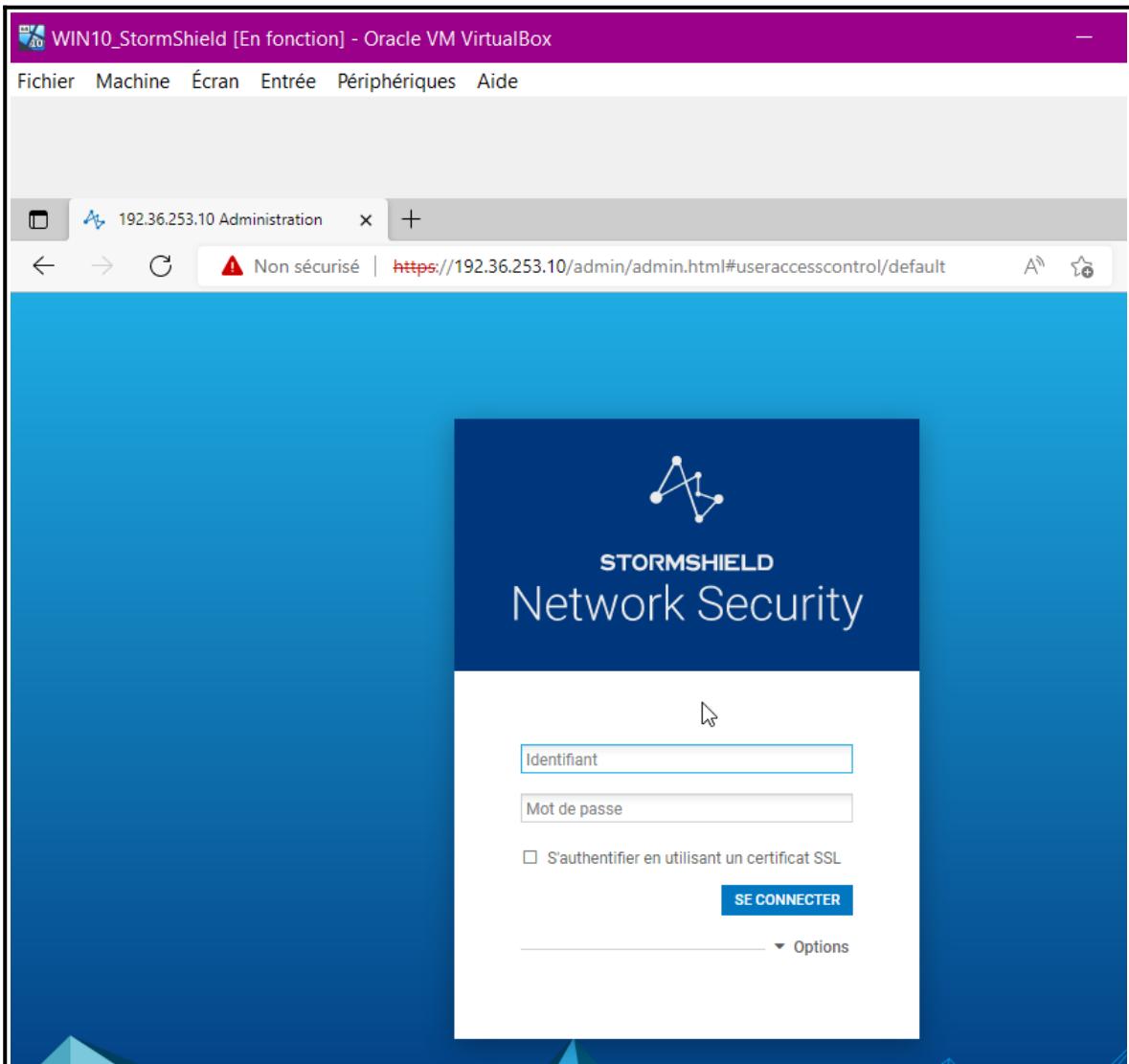




STORMSHIELD

LAB 12 :
IPSEC CERTIFICAT



1ère étape : Connexion au Stormshield de A de puis WIN10 avec l'adresse 192.36.253.10

The screenshot shows the EVA1 IPSEC configuration interface. The top navigation bar includes tabs for MONITORING, CONFIGURATION, and the current active tab, CORRESPONDANTS. The main content area displays a table for tunnel configurations. A specific row is selected for 'nomade_entreprisea'. The 'Identification' section is highlighted, showing the 'Méthode d'authentification' dropdown set to 'Certificat' and the certificate field containing 'entreprisea:sns.a.n'. Other fields visible include 'Passerelle distante' (Any), 'Configuration de secours' (None), 'Profil IKE' (StrongEncryption), and 'Version IKE' (IKEv2).

2ème étape : Nous basculons la méthode d'authentification de notre correspondant en Certificat.

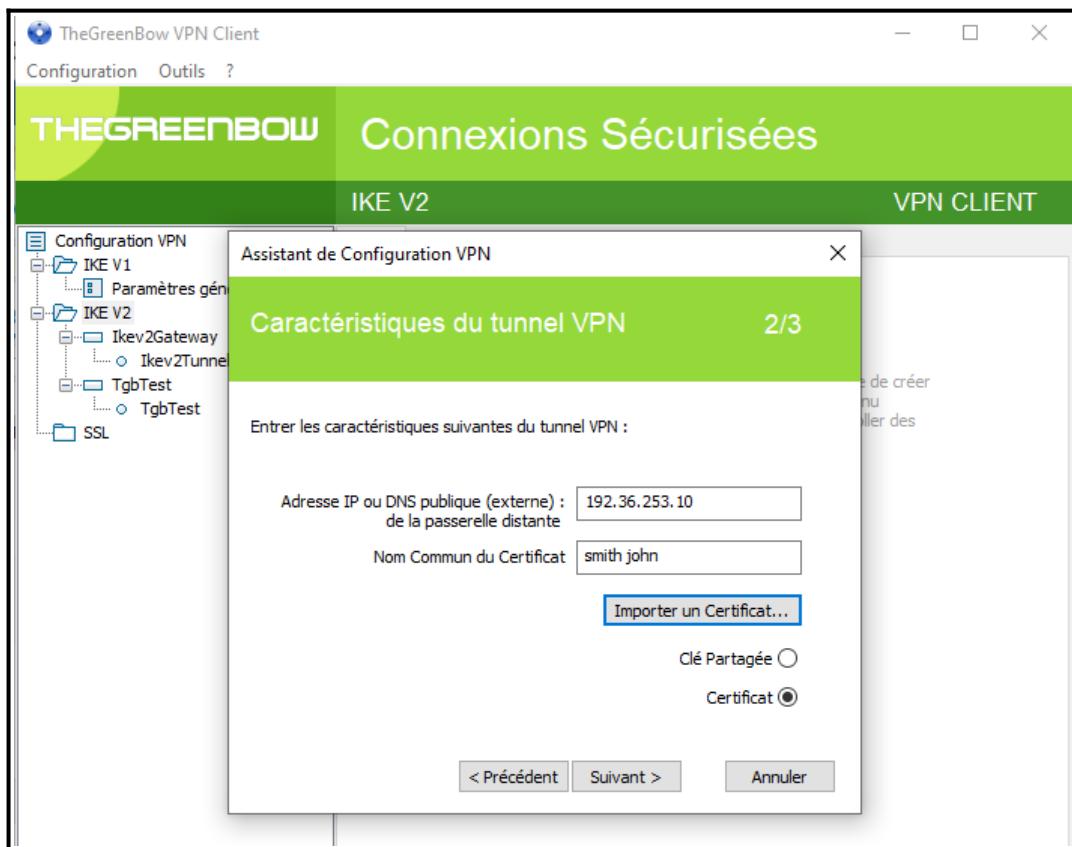
The screenshot shows a user profile for 'jsmith (john smith)'. The 'CERTIFICAT' tab is selected. The 'Expiration' field shows 'Nov 5 16:39:58 2023 GMT'. The 'Émis pour' section displays the following X.500 attributes:

Attribut	Valeur
Émetteur:	/C=FR/ST=France/L=Saint-Raphael/O=entreprisea/OU=enterprisea/CN=smith
Nom (CN):	smith john
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

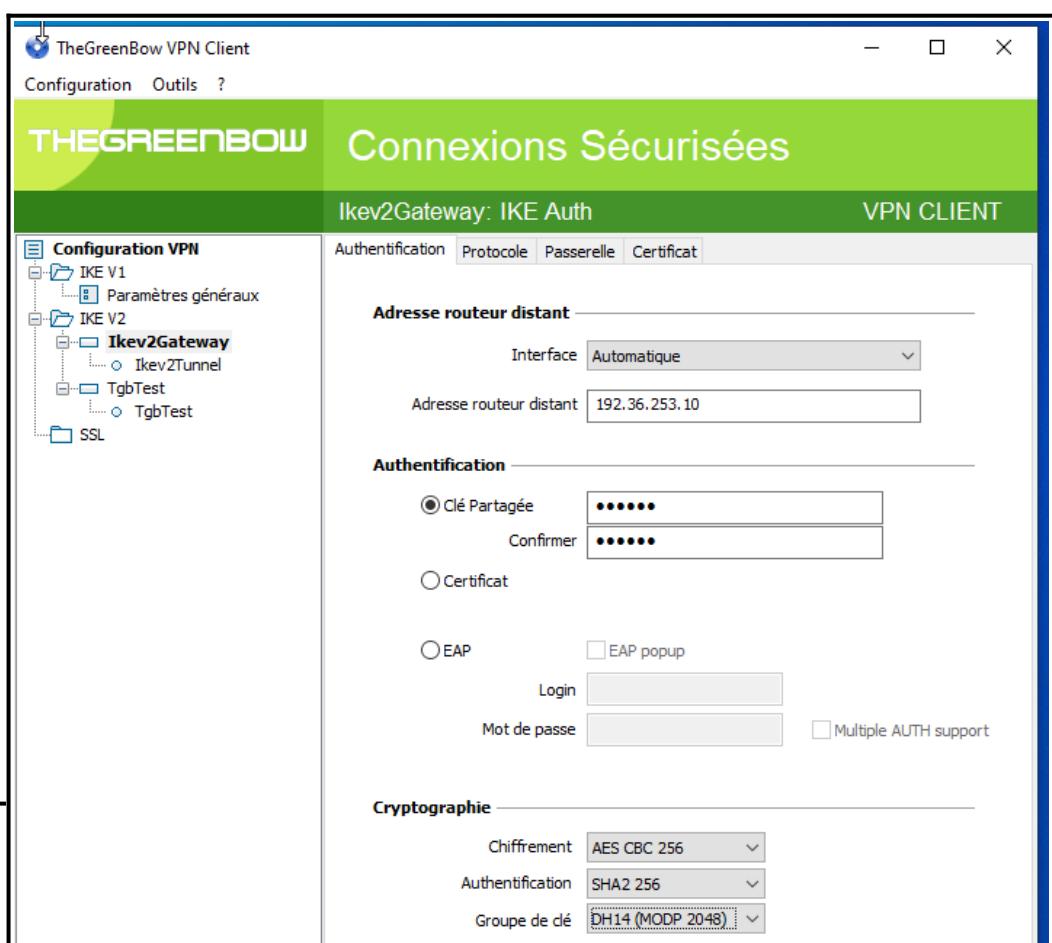
3ème étape : Résumé suite à la création du certificat utilisateur pour john smith .

4ème étape : Le certificat de l'utilisateur john smith se situe donc bien dans la catégorie certificats et pki de entreprisea.

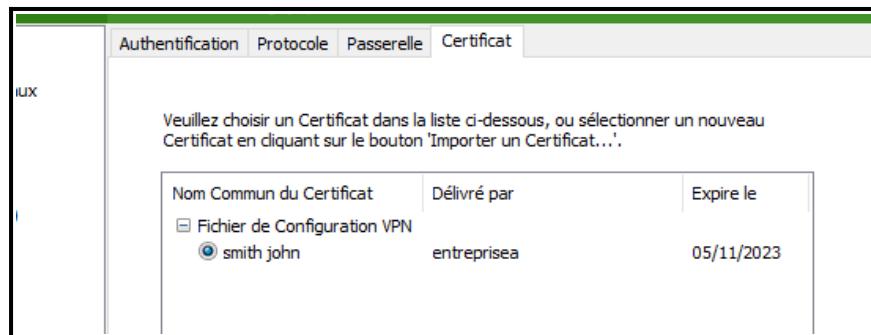
5ème étape : Nous téléchargeons le certificat en identité p12.



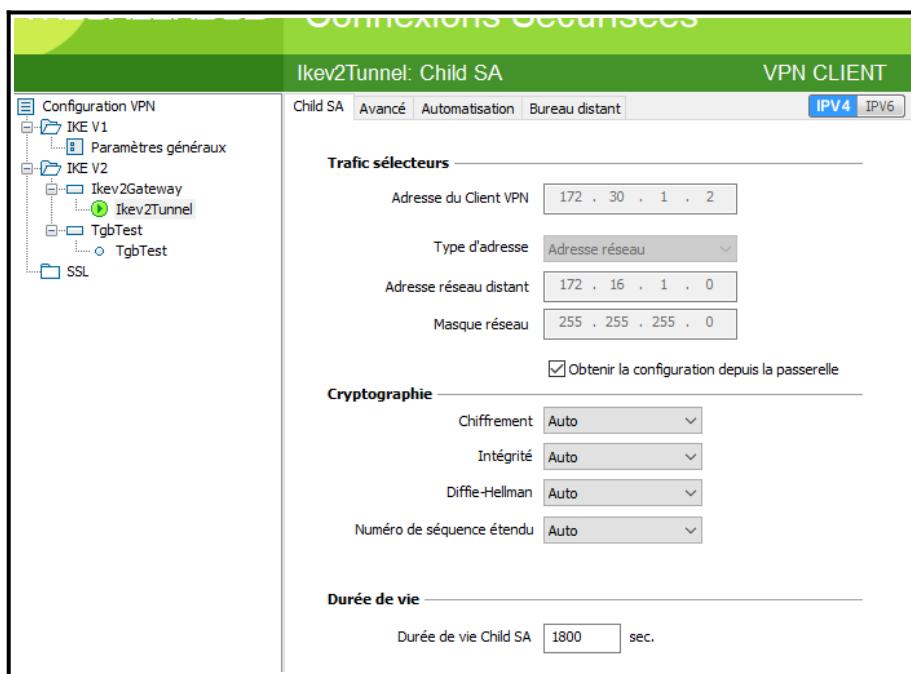
6ème étape : Via l'assistant de création de tunnel IKE V2 nous renseignons les caractéristiques du tunnel VPN.



7ème étape : Nous observons les informations du tunnel.



8ème étape : Le certificat que nous avons téléchargé précédemment à bien été importé.



9ème étape : Les adresses IP ont bien été renseignés.

Connexions sécurisées

Ikev2Tunnel: Child SA

VPN CLIENT

Configuration VPN

- IKE V1
 - Paramètres généraux
- IKE V2
 - Ikev2Gateway
 - Ikev2Tunnel
 - TgbTest
 - TgbTest
- SSL

Child SA Avancé Automatisation Bureau distant IPV4 IP

Serveurs alternatifs

Suffixe DNS:

Type	Adresse IP	
DNS	172.16.1.10	X

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.

10ème étape : Même chose dans l'onglet avancé.

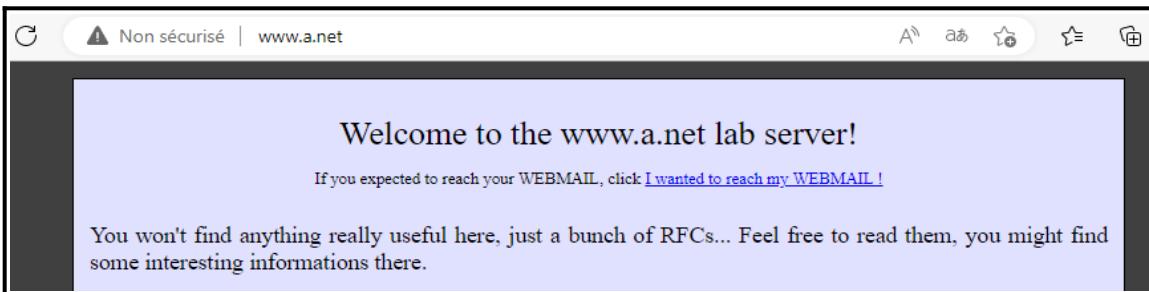
État	Nom du réseau l...	Nom de la passer...	Sens ↑	Nom de la passer...	Nom du réseau d...	Durée de ...	ID
Politique: none	rfc5735_loopback		← in		any		0
Politique: none	rfc5735_loopback		→ out		any		0
⚠ Pas de tu...	ip_VTI_B	Firewall_out	← 🔒 in	Fw_B	ip_VTI_B	8h 41m	1
⚠ Pas de tu...	ip_VTI_B	Firewall_out	→ 🔒 out	Fw_B	ip_VTI_B	8h 41m	1
✓ 1 Tunnel(s)	Network_dmz1	Firewall_out	← 🔒 in	WIN10		3m	2
✓ 1 Tunnel(s)	Network_dmz1	Firewall_out	→ 🔒 out	WIN10		3m	2

11ème étape : Les connexions VPN apparaissent bien.

```
C:\Users\ ADMIN>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<1ms 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 = 0ms, Maximum = 1ms, Moyenne = 0ms
```



12ème étape : Nous effectuons nos tests concernant le serveur web de A depuis WIN10 ainsi que le ping.