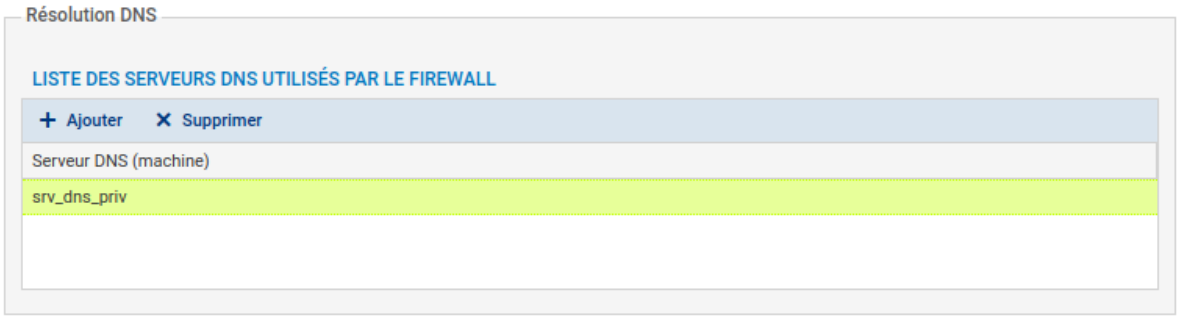
Lab 10 – Nomade VPN IPsec avec PSK

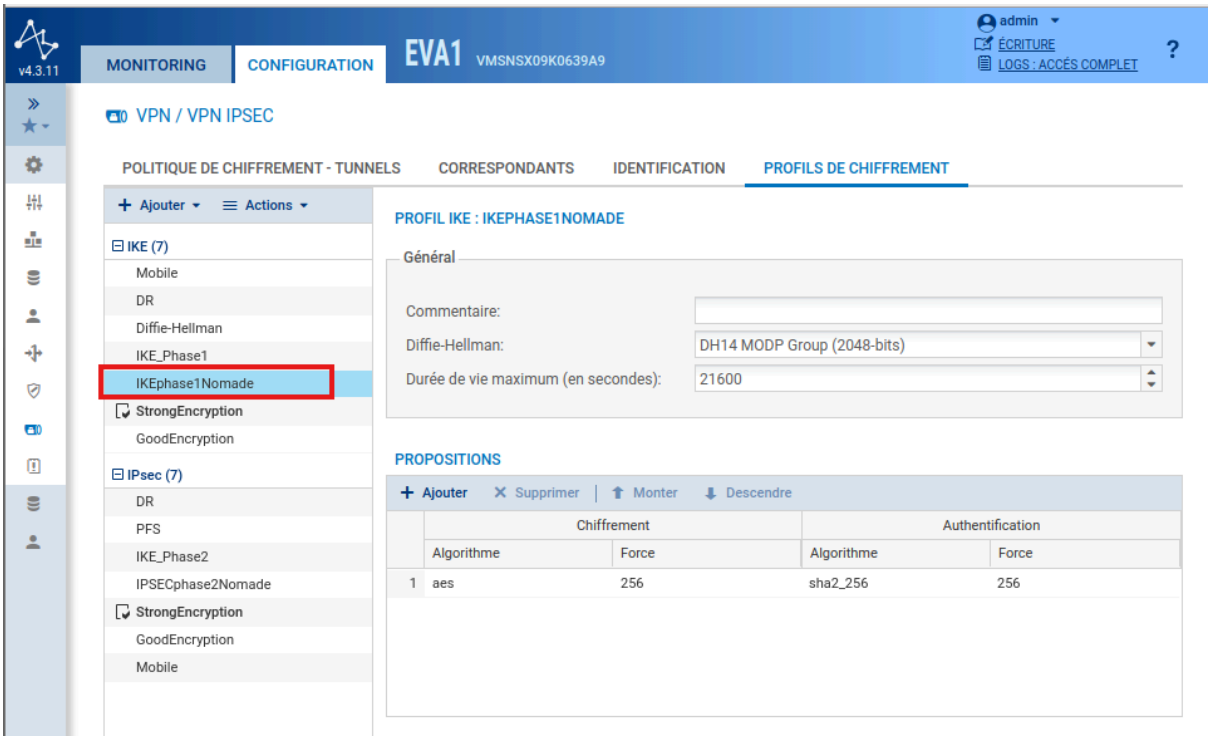
Table des Matières :

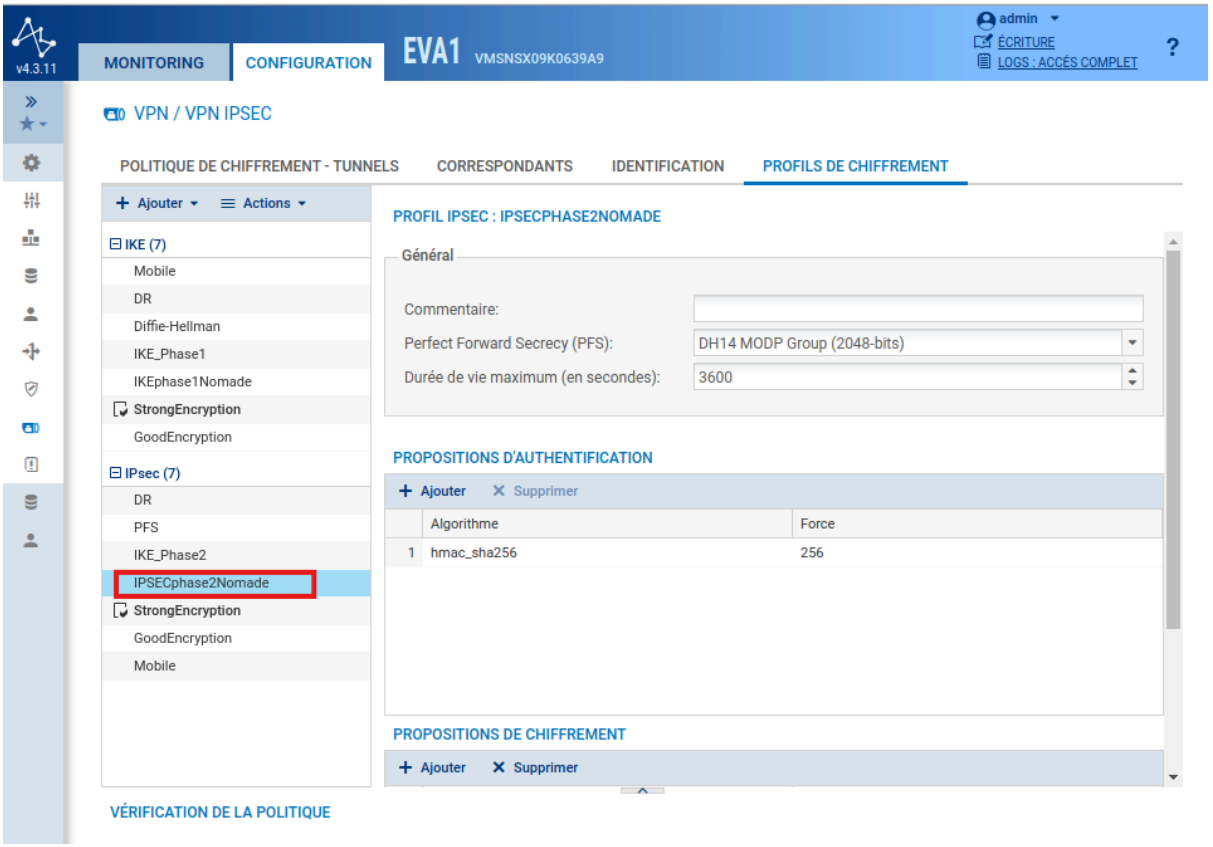
▪ Tout d’abord nous avons supprimé les deux serveurs dns déjà présents pour éviter qu’il y ait un conflit



1. Création des profils de chiffrement (phase 1 IKE / phase 2 IPsec)

- Création de nouveaux profils de chiffrement phase 1(ike) et de phase 2(ipsec)

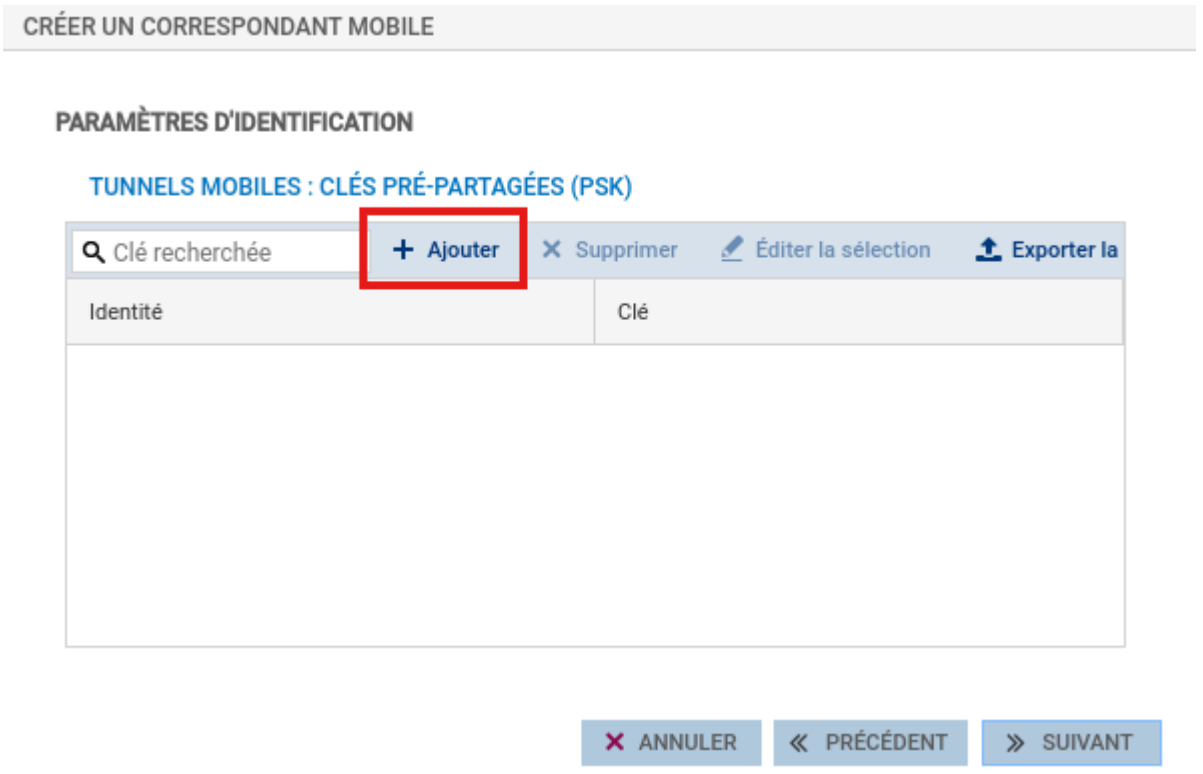


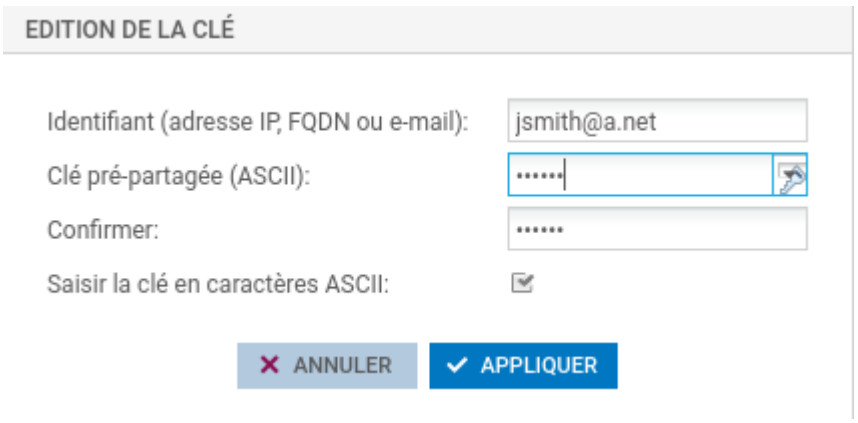


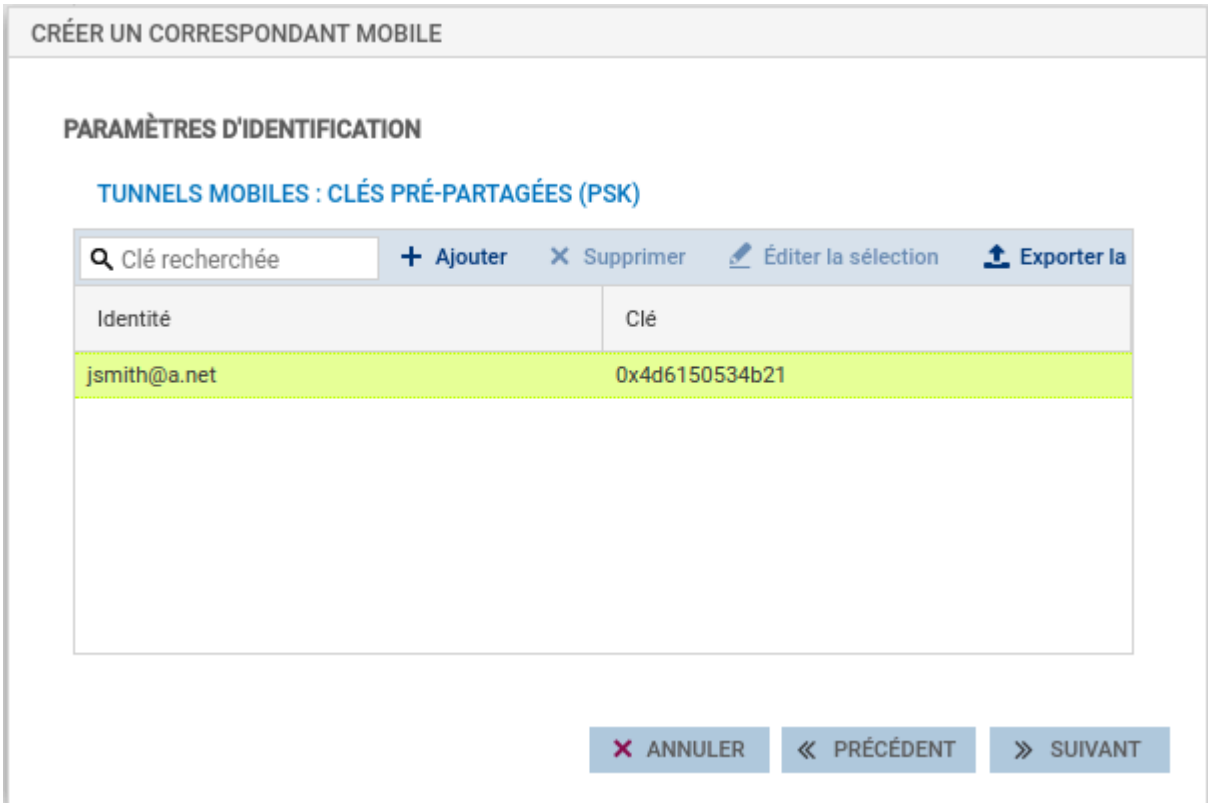
2. Création du correspondant “nomade_entreprisea” (IKEv2)

▪ Création d’un correspondant ayant pour nom “nomade_entreprisea” en nomade IKEv2


CRÉER UN CORRESPONDANT MOBILE
IDENTIFICATION DU CORRESPONDANT - ASSISTANT DE CRÉATION DE CORRESPONDANT
Type d'authentification:
Certificat
Certificat et Xauth (iPhone)
Clé pré-partagée (PSK)
ANNULER
PRÉCÉDENT
SUIVANT

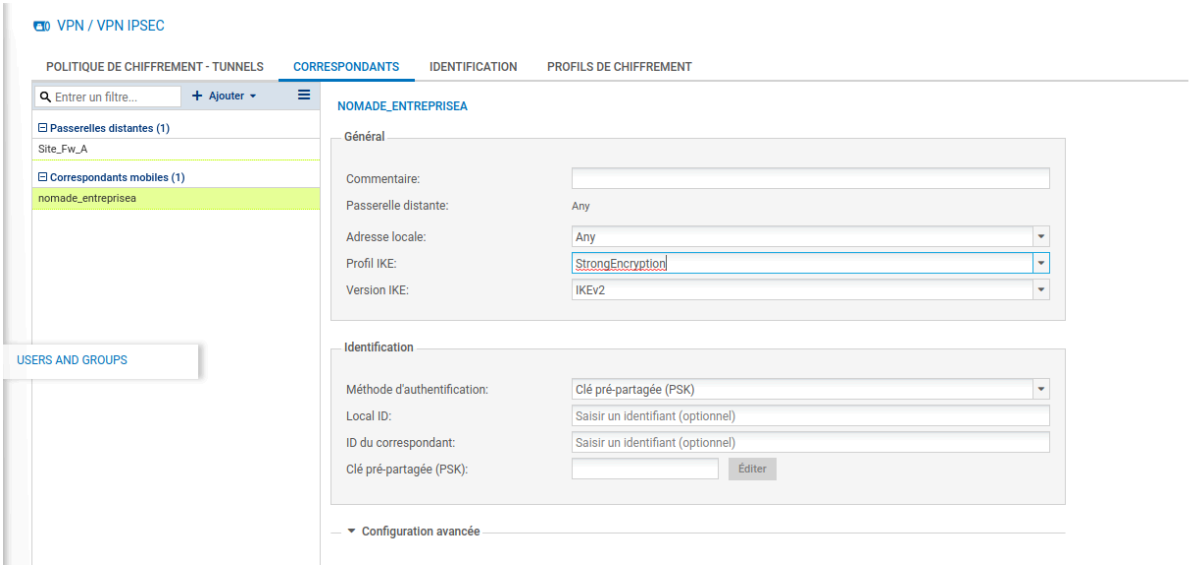

CRÉER UN CORRESPONDANT MOBILE
PARAMÈTRES D'IDENTIFICATION
TUNNELS MOBILES : CLÉS PRÉ-PARTAGÉES (PSK)
Clé recherchée
Ajouter
Supprimer
Éditer la sélection
Exporter la
Identité
Clé
ANNULER
PRÉCÉDENT
SUIVANT

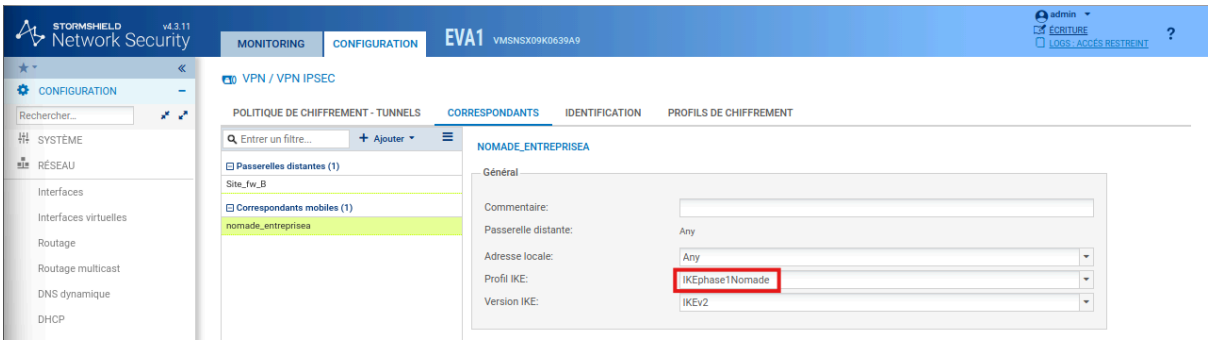

EDITION DE LA CLÉ
Identifiant (adresse IP, FQDN ou e-mail):
jsmith@a.net
Clé pré-partagée (ASCII):
Confirmer:
Saisir la clé en caractères ASCII:
ANNULER
APPLIQUER


CRÉER UN CORRESPONDANT MOBILE
PARAMÈTRES D'IDENTIFICATION
TUNNELS MOBILES : CLÉS PRÉ-PARTAGÉES (PSK)
Clé recherchée
Ajouter
Supprimer
Éditer la sélection
Exporter la
Identité
Clé
jsmith@a.net
0x4d6150534b21
ANNULER
PRÉCÉDENT
SUIVANT

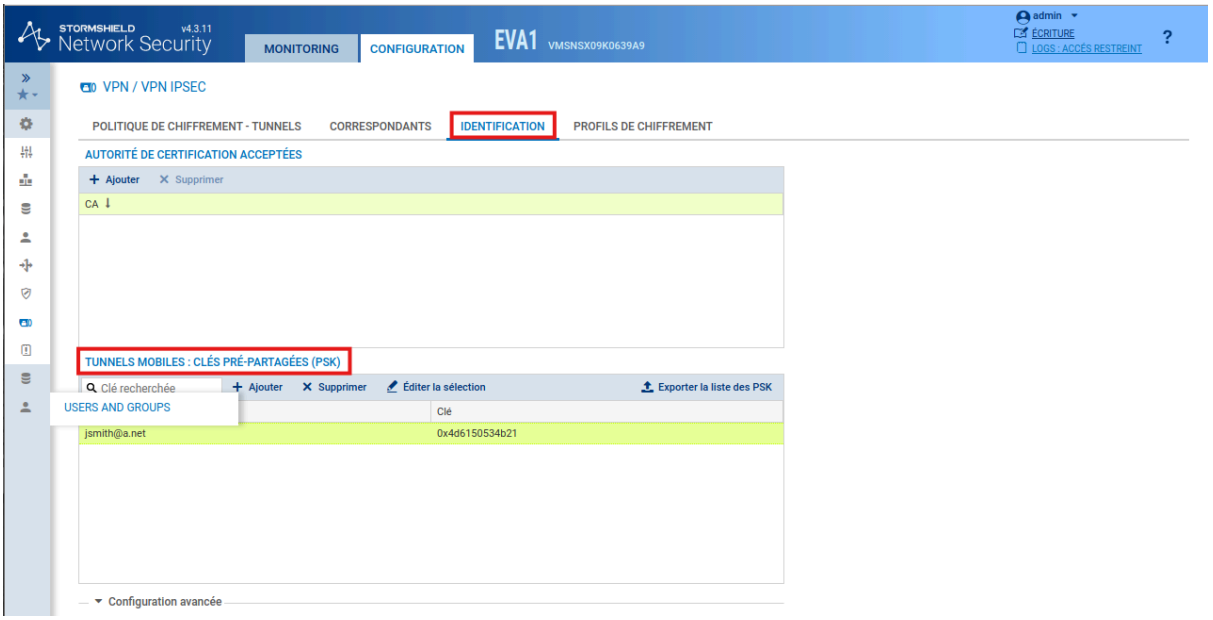

CRÉER UN CORRESPONDANT MOBILE
RÉSUMÉ - ASSISTANT DE CRÉATION DE CORRESPONDANT
Correspondant mobile
Nom:
nomade_entreprisea
Identification du correspondant : clé pré-partagée
Les clés pré-partagées sont listées dans l'onglet Identification du module VPN IPsec
ANNULER
PRÉCÉDENT
TERMINER

- Suite à cela, nous changeons son profil IKE par un profil antérieurement créé



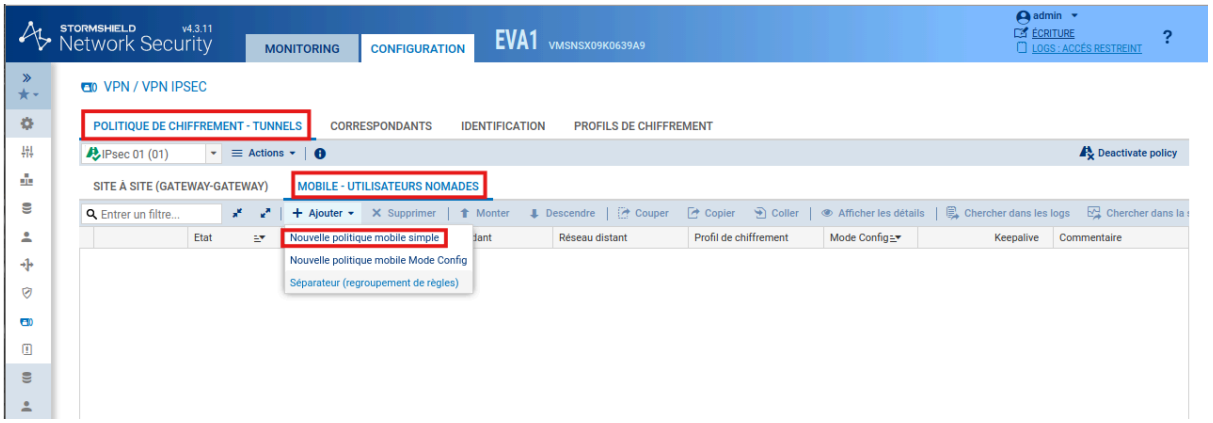


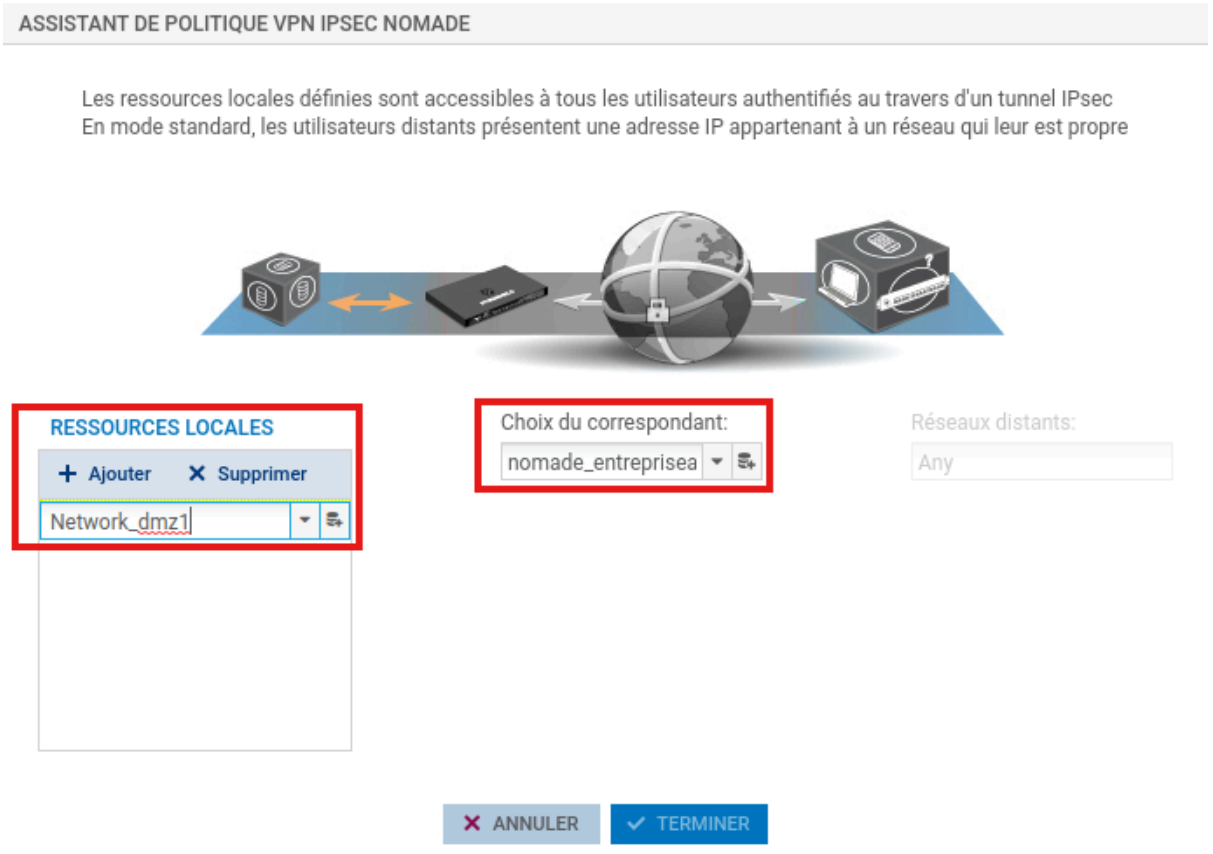
- Le compte jsmith est bien spécifié

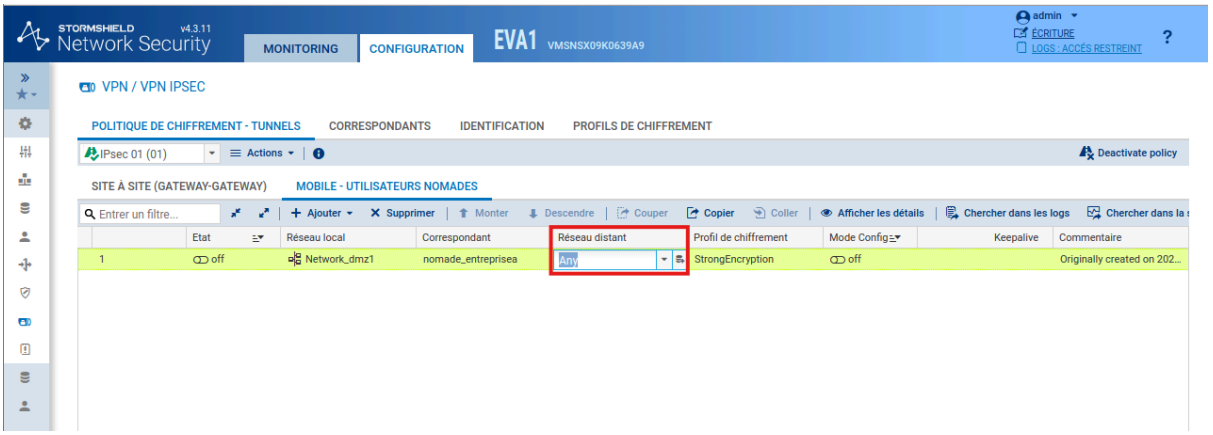


3. Création d'une politique Nomade

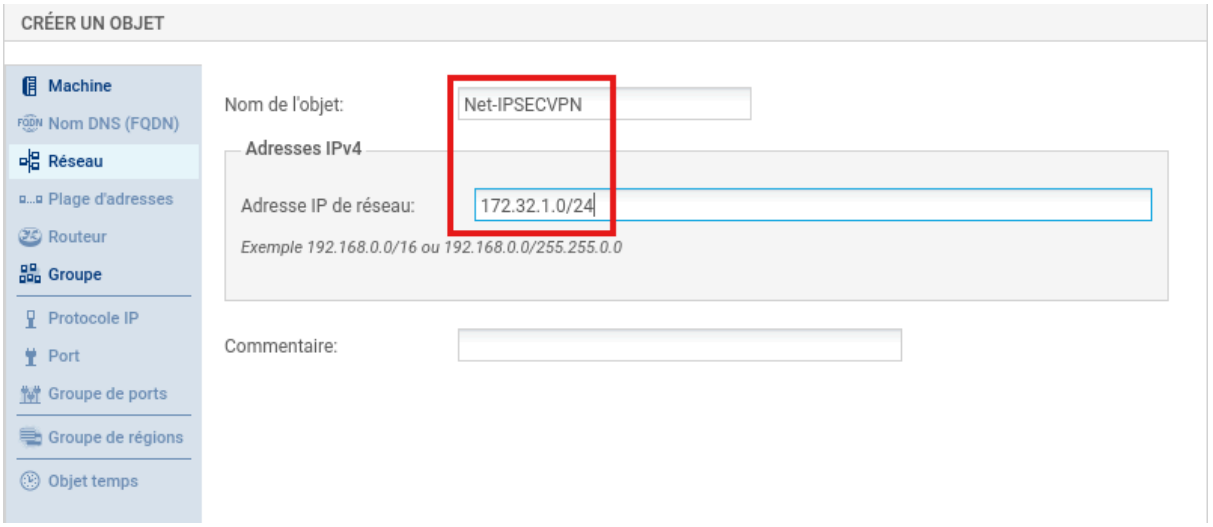
- Création d'une nouvelle politique nomade (simple).



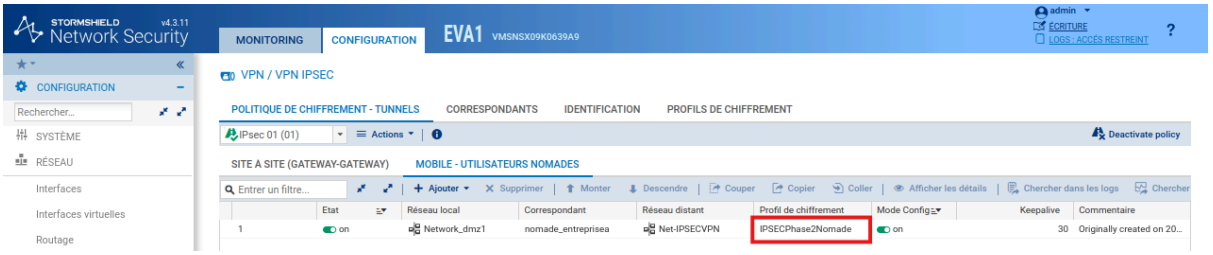




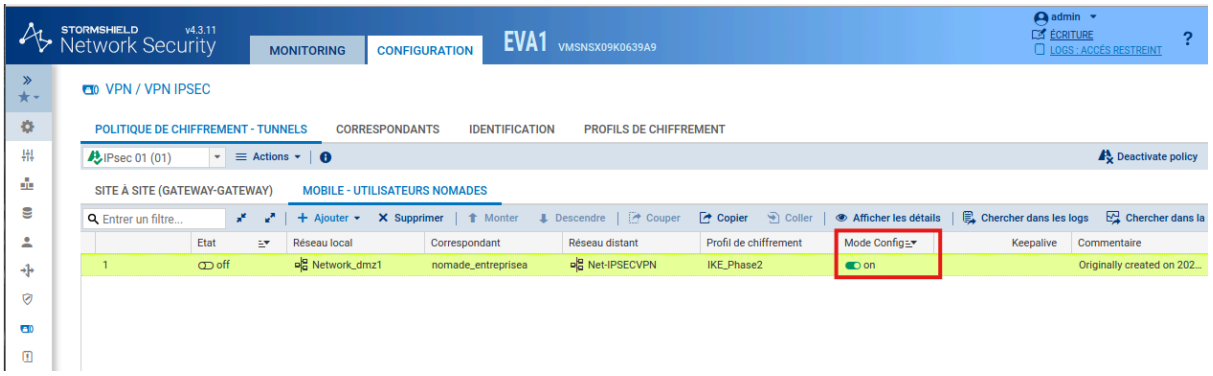
- Nous créons un nouvel objet “réseau” qui sera le réseau distant



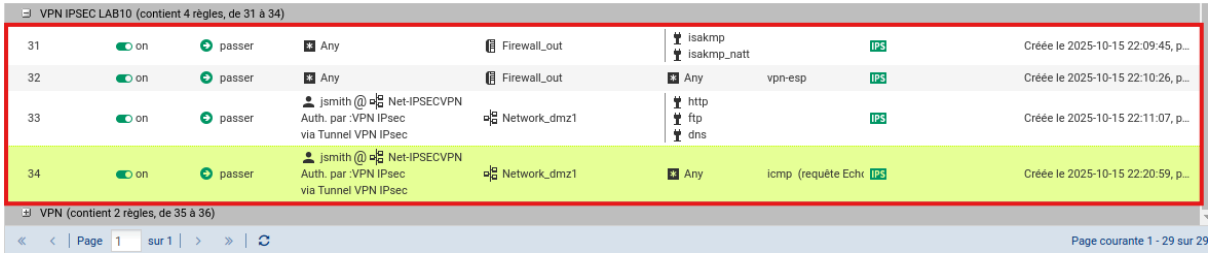
- Modification du profil de chiffrement antérieurement créé



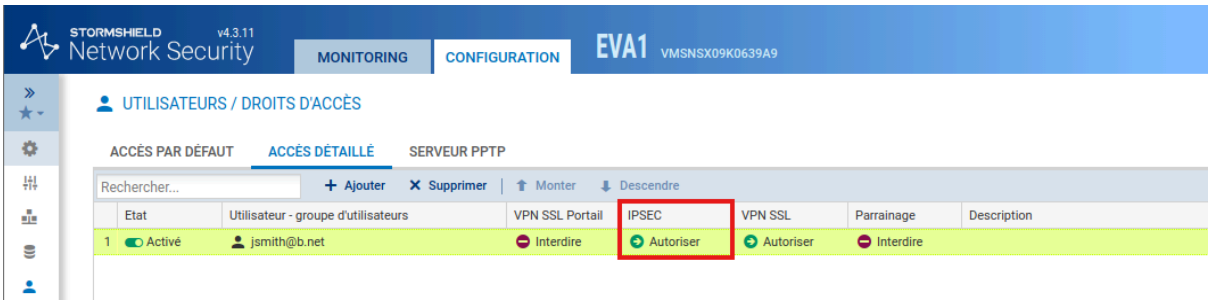
- Nous activons le mode config



▪ Nous avons mis en place quatre règles de filtrage afin de sécuriser chaque étape de la connexion VPN

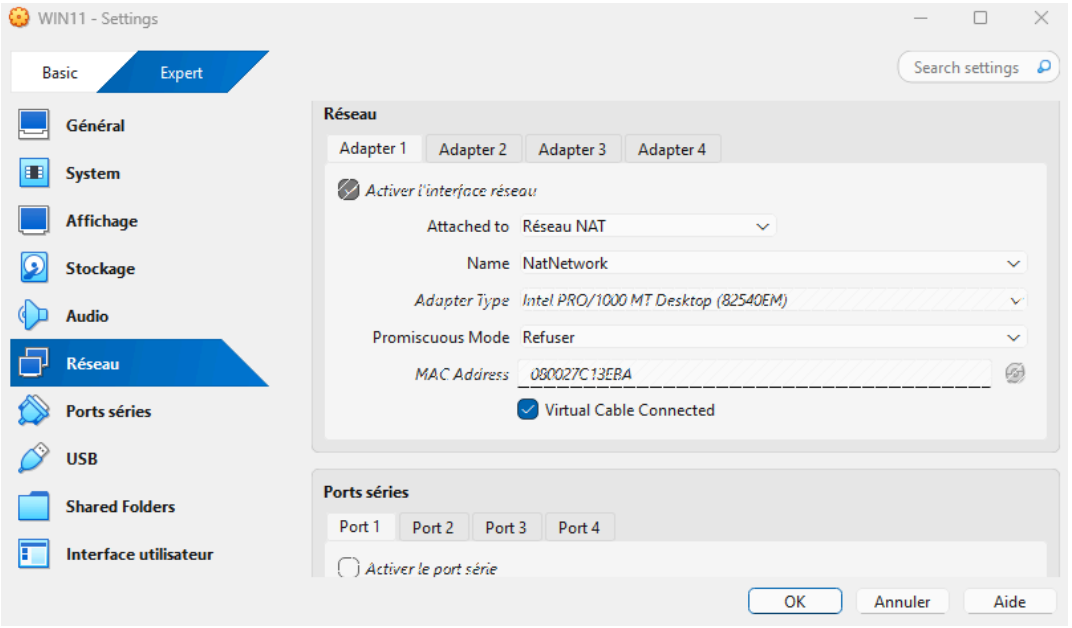


▪ Nous autorisons l'accès IPSEC pour l'utilisateur jsmith

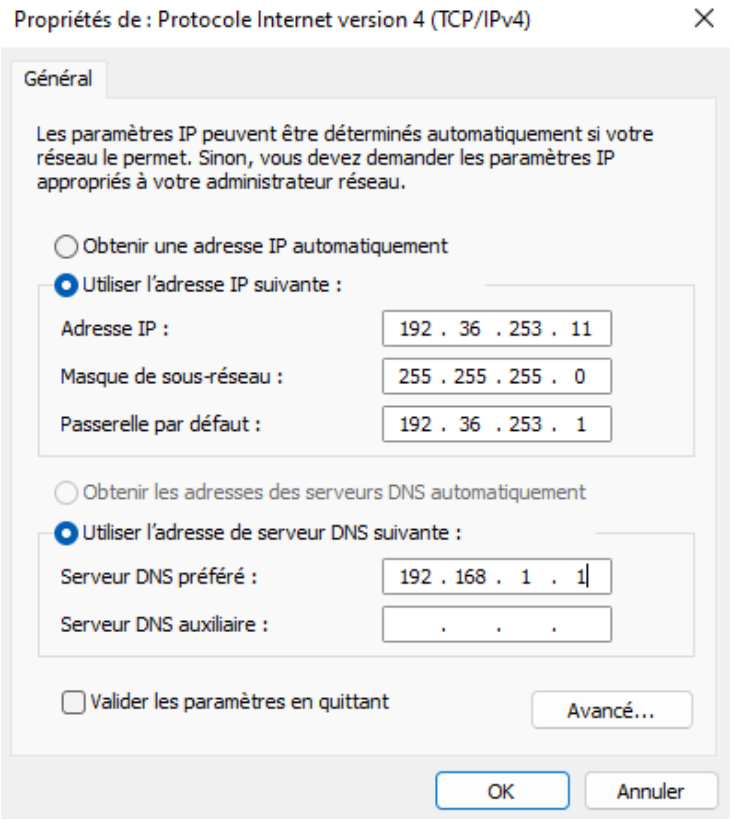


4. Client Windows 11 (installation du client VPN)

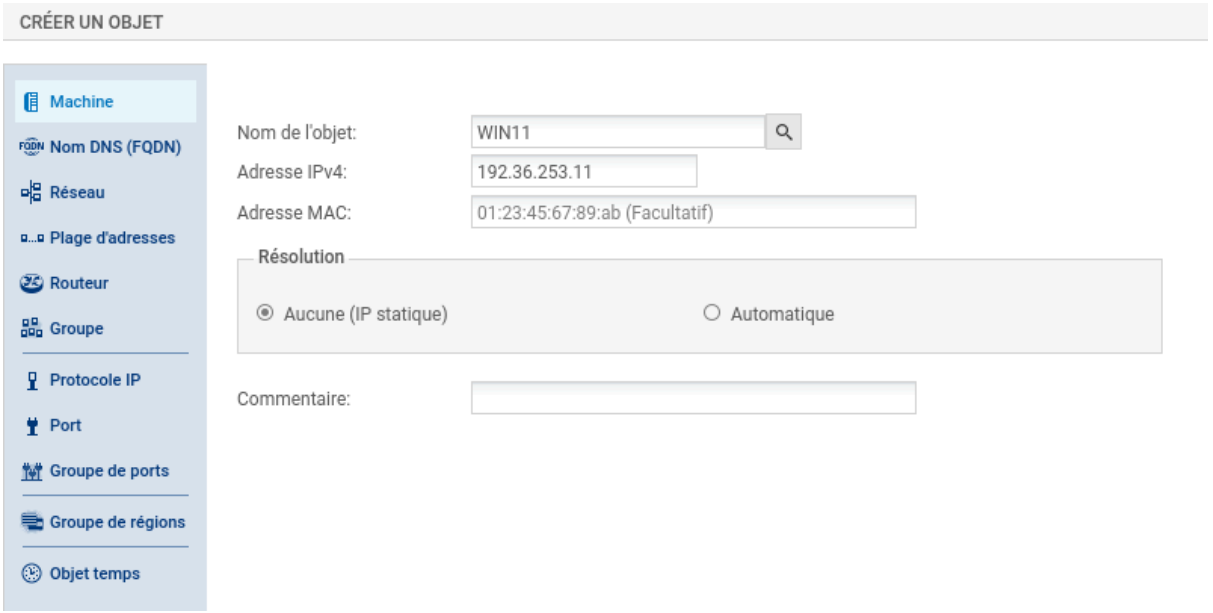
▪ Nous avions créé le réseau Nat Network (192.36.253.0/24)



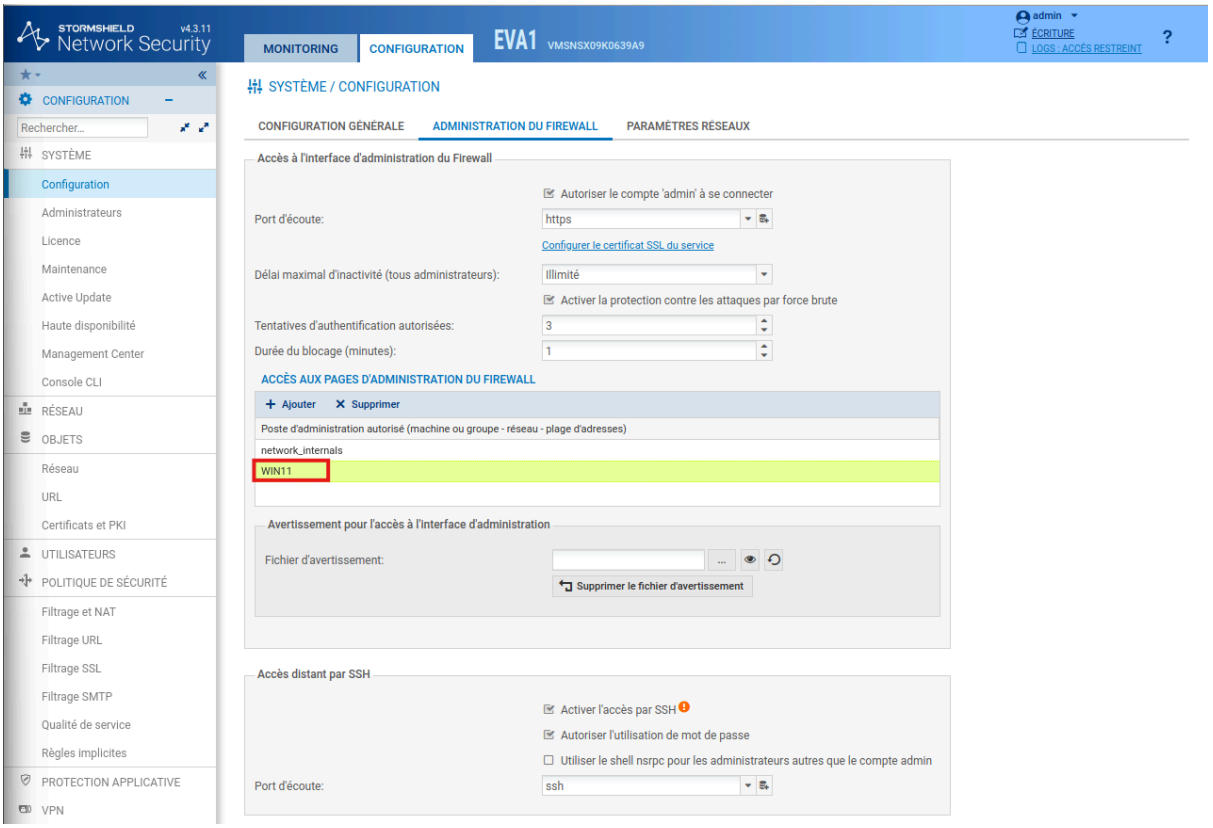
▪ Nous attribuons une ip à la machine



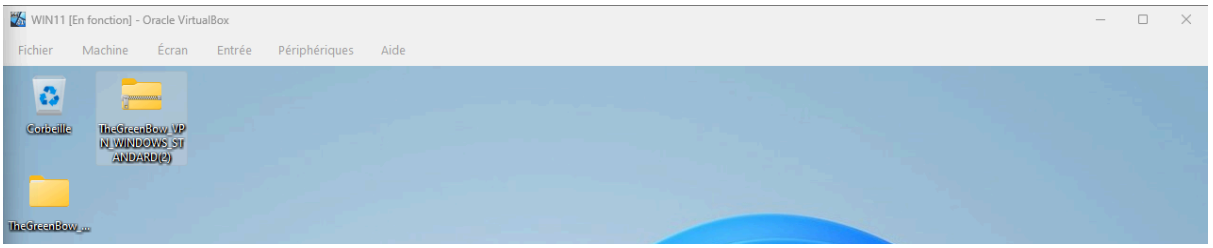
- Création de l'objet machine "WIN11"



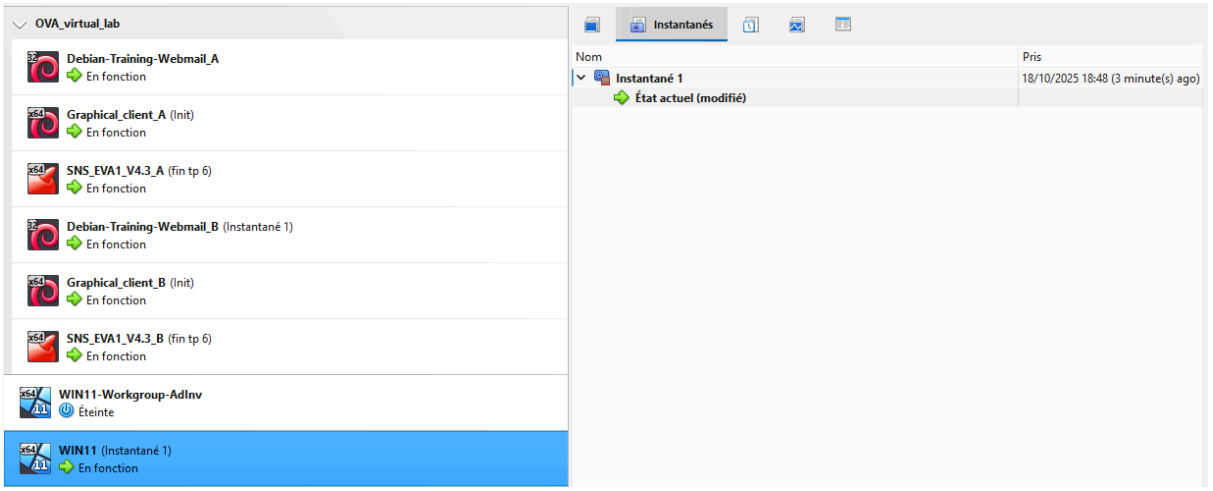
- Nous autorisons la machine WIN11 à joindre aux pages d'administrations du firewall



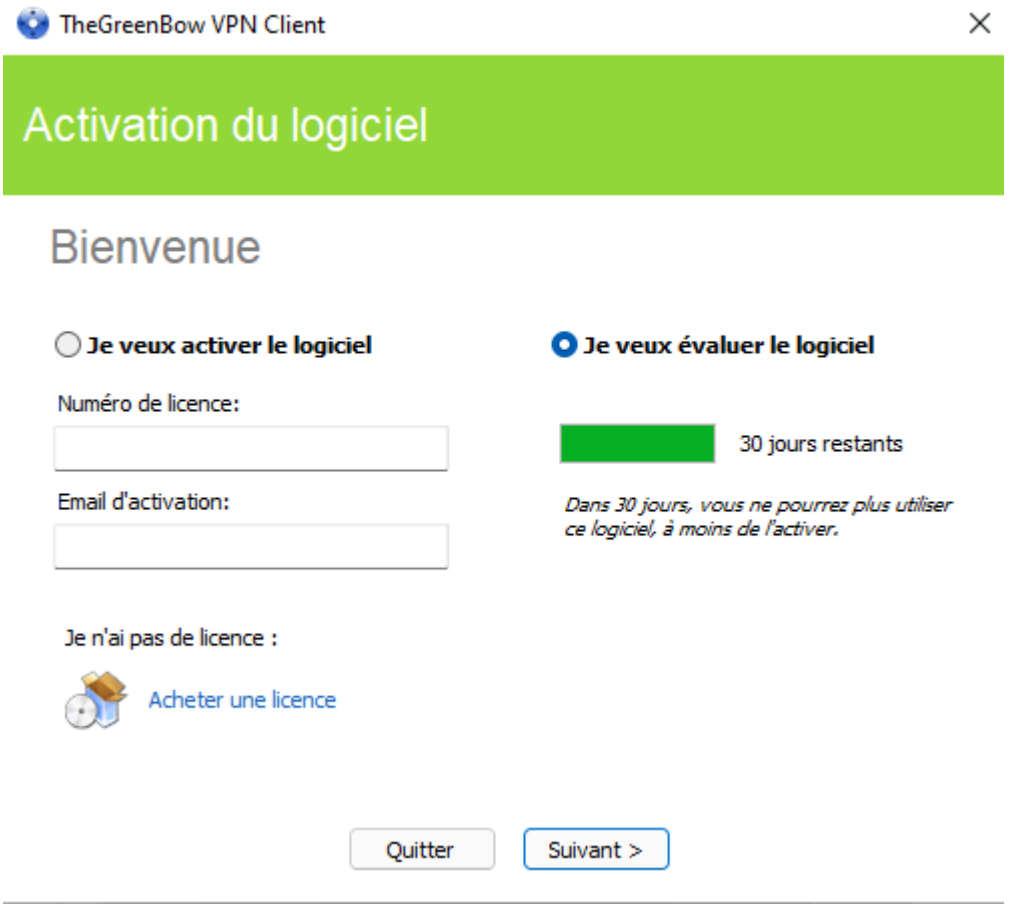
▪ Nous avons déplacé le fichier .zip sur notre machine physique puis sur la machine win11 puis nous l’avons dézip pour en extraire l'exécutable TheGreenBow

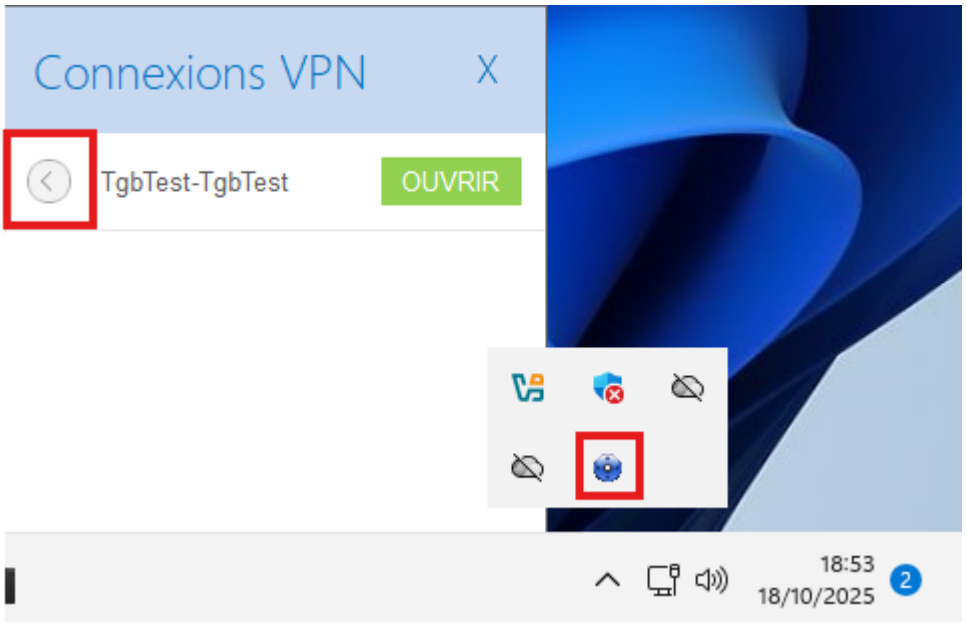


- Avant son exécution, nous réalisons une snapshot de la machine

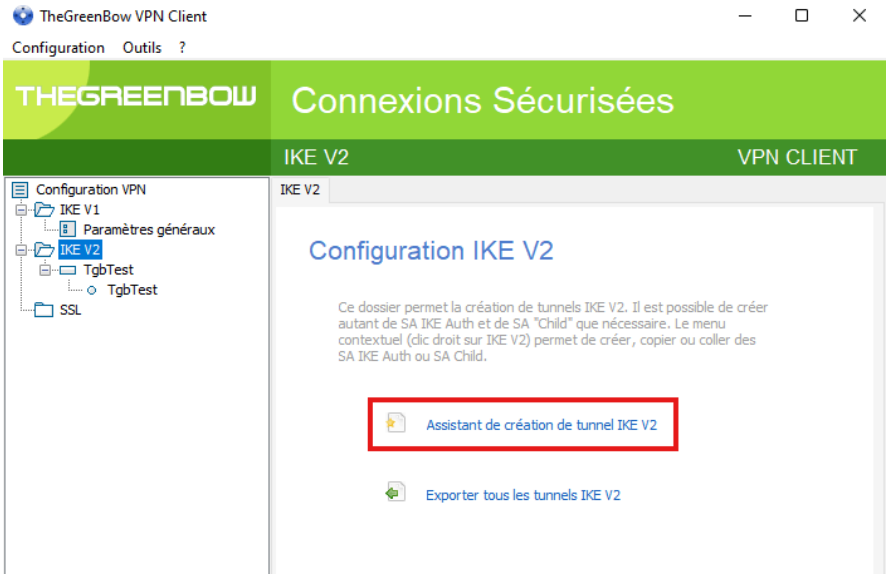


5. Installation du client TheGreenBow

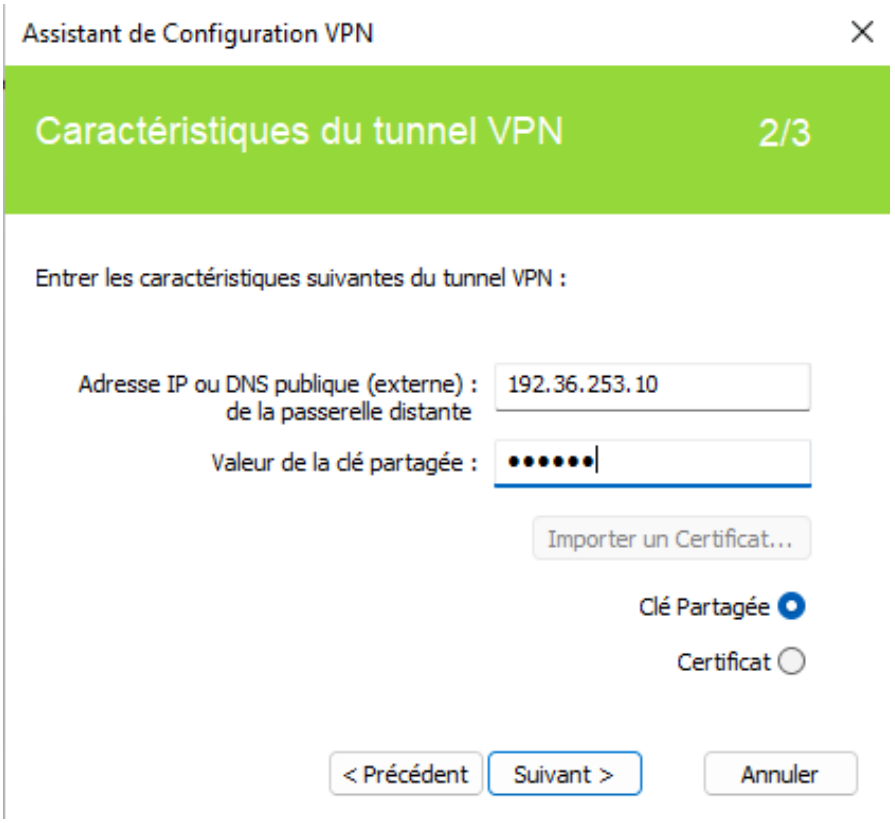


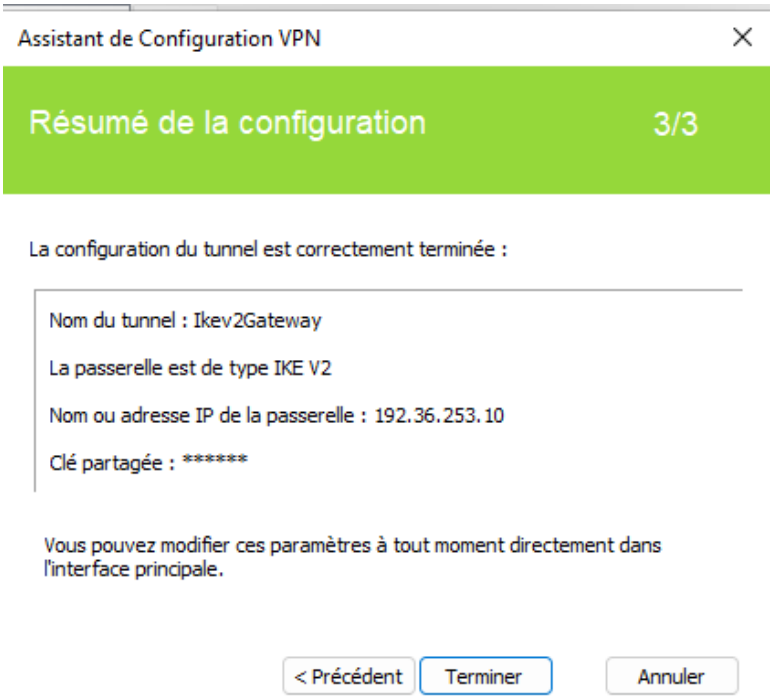


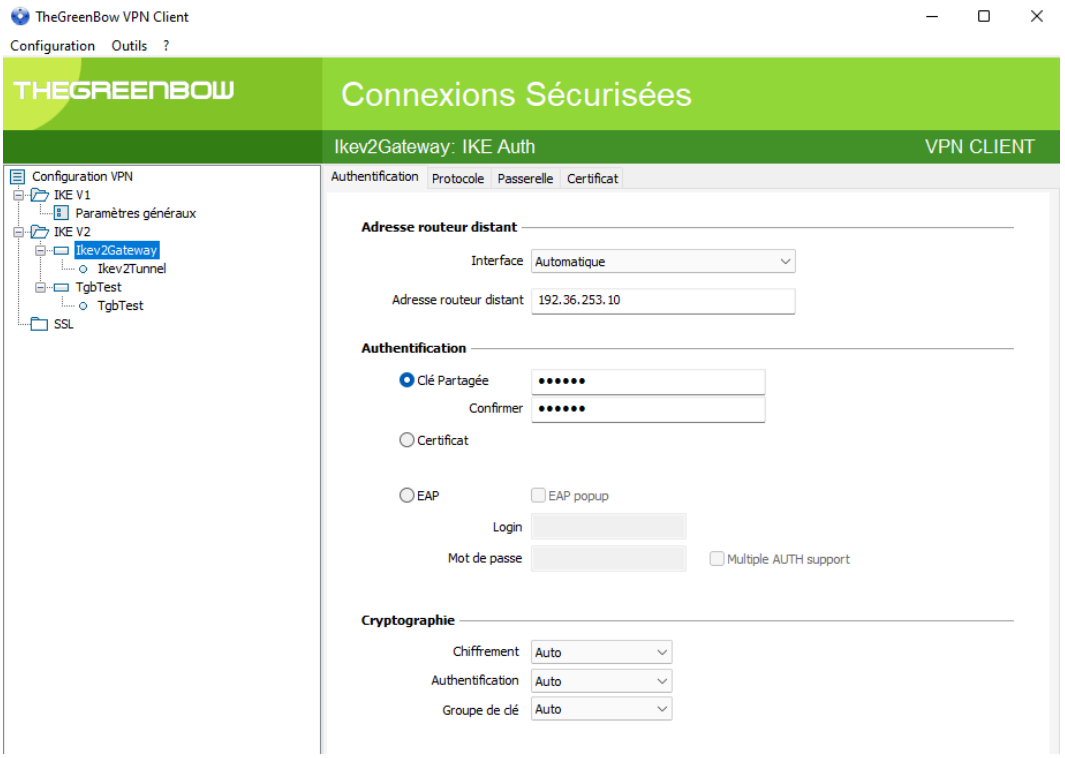
6. Activation du mode Config (adresse IP attribuée par la passerelle)



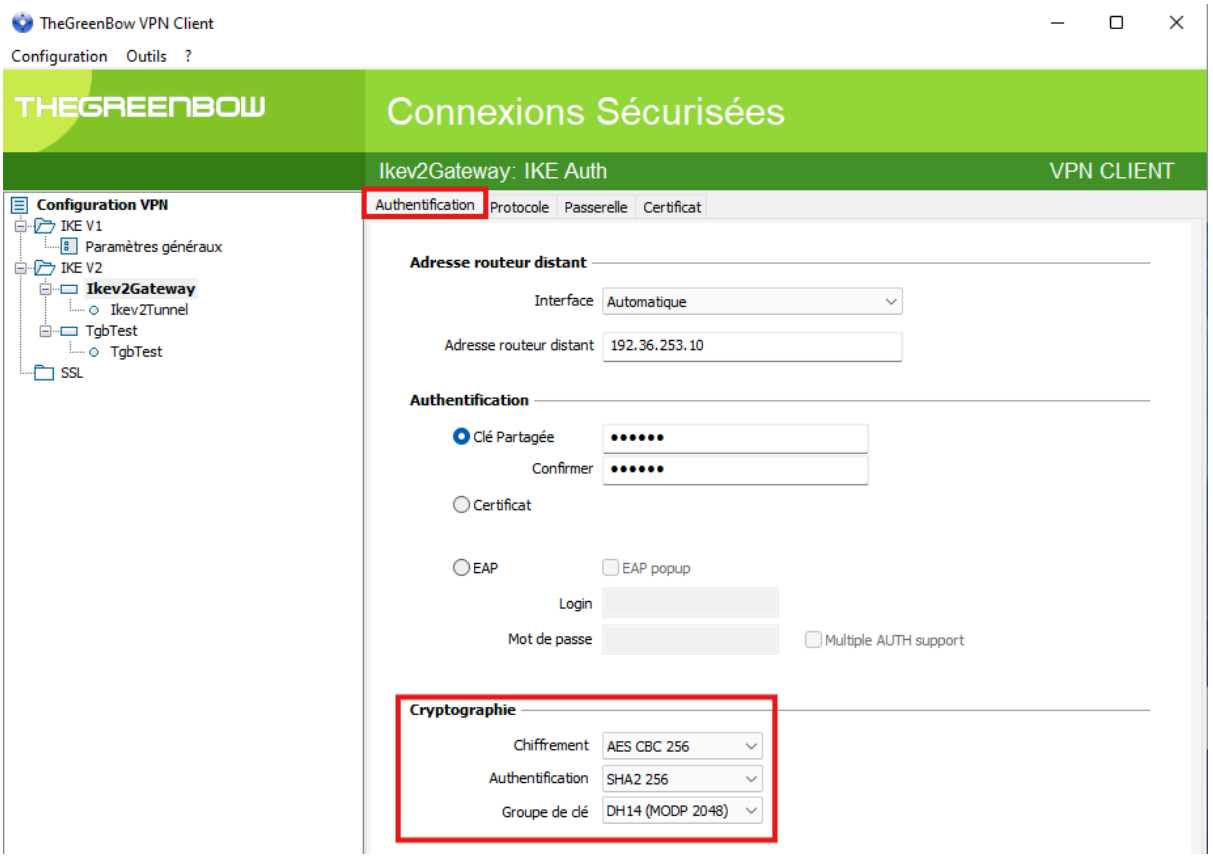
▪ Nous renseignons l'ip du routeur virtuel ou DNS publique en tant que passerelle distante

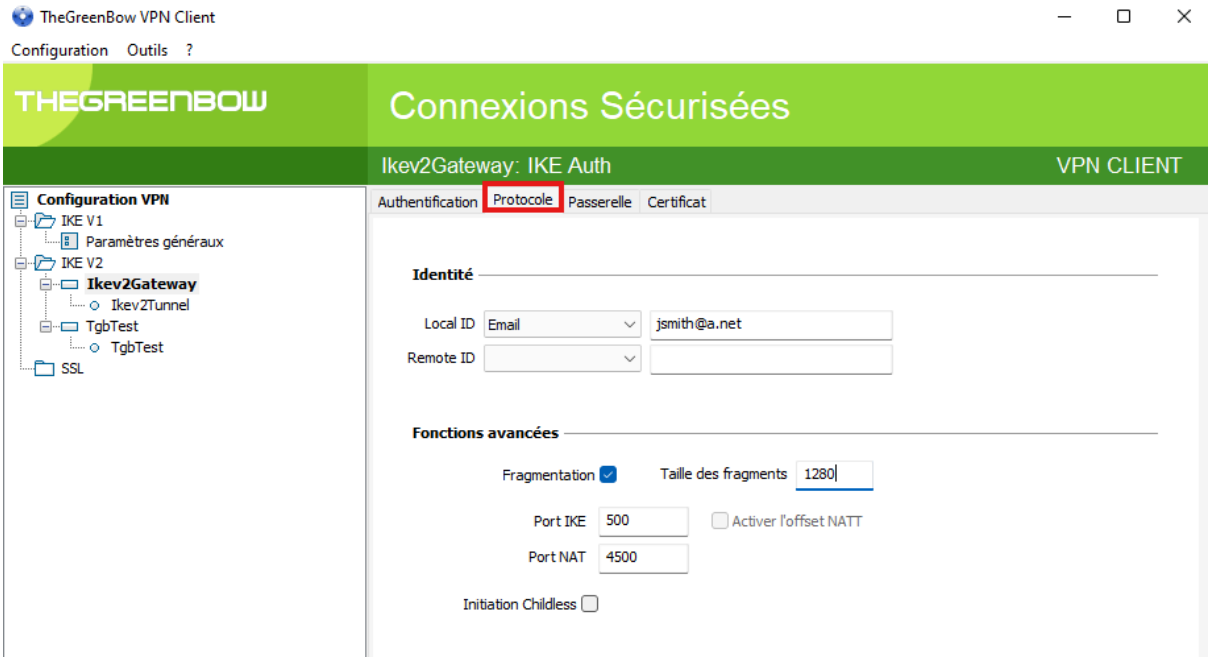



Assistant de Configuration VPN
Résumé de la configuration
3/3
La configuration du tunnel est correctement terminée :
Nom du tunnel : Ikev2Gateway
La passerelle est de type IKE V2
Nom ou adresse IP de la passerelle : 192.36.253.10
Clé partagée : ******
Vous pouvez modifier ces paramètres à tout moment directement dans l'interface principale.
< Précédent
Terminer
Annuler

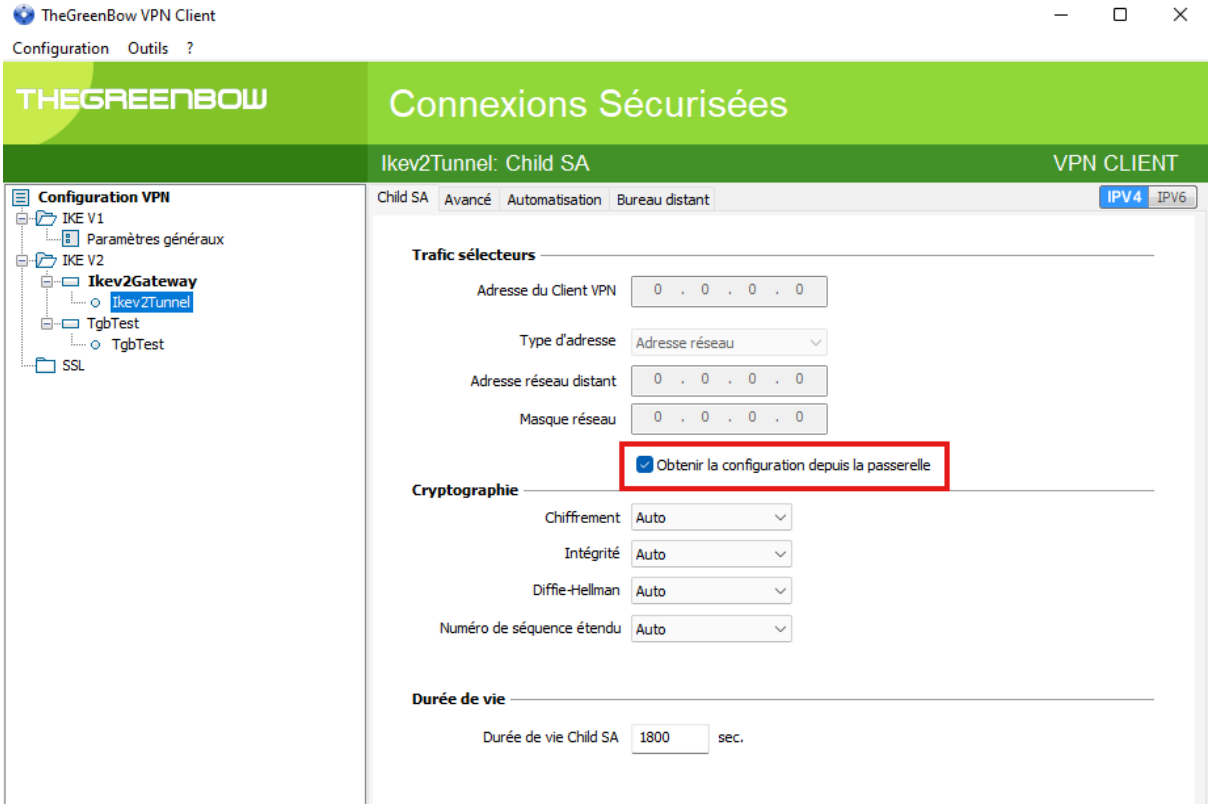

TheGreenBow VPN Client
Configuration Outils ?
THEGREENBOW
Connexions Sécurisées
Ikev2Gateway: IKE Auth
VPN CLIENT
Configuration VPN
IKE V1
Paramètres généraux
IKE V2
Ikev2Gateway
Ikev2Tunnel
TgbTest
TgbTest
SSL
Authentification
Protocole
Passerelle
Certificat
Adresse routeur distant
Interface
Automatique
Adresse routeur distant
192.36.253.10
Authentification
Clé Partagée
Confirmer
Certificat
EAP
EAP popup
Login
Mot de passe
Multiple AUTH support
Cryptographie
Chiffrement
Auto
Authentification
Auto
Groupe de clé
Auto

- Dans l'onglet authentification nous renseignons les valeurs dans le champ Cryptographie

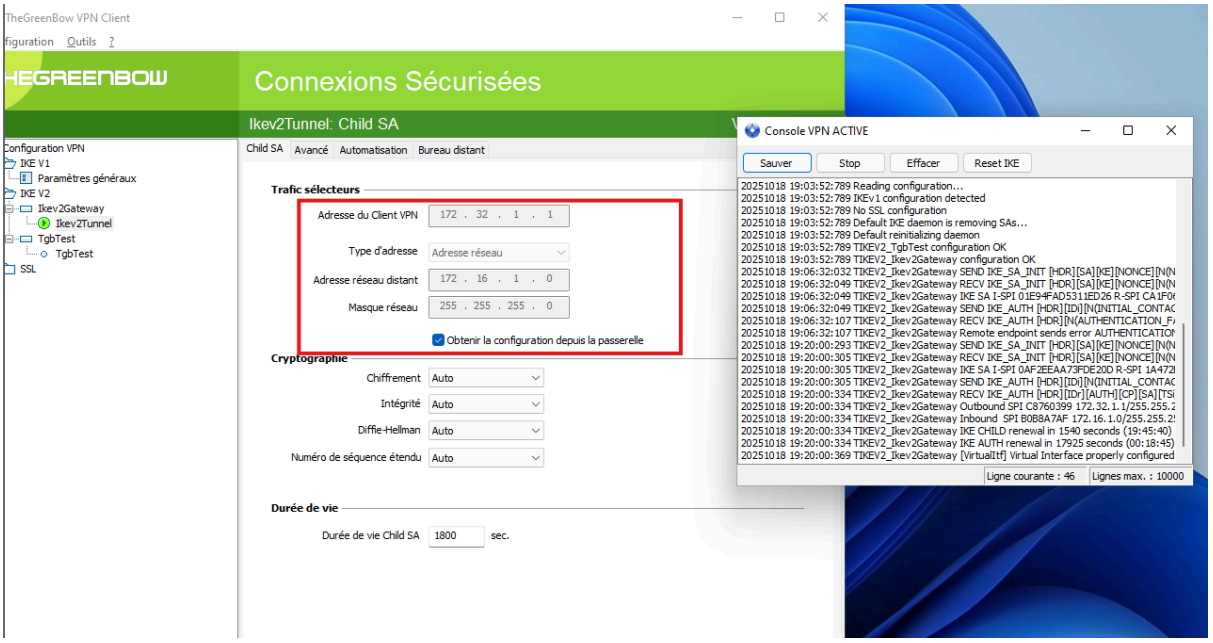




▪ Nous cochons “Obtenir la configuration depuis la passerelle”



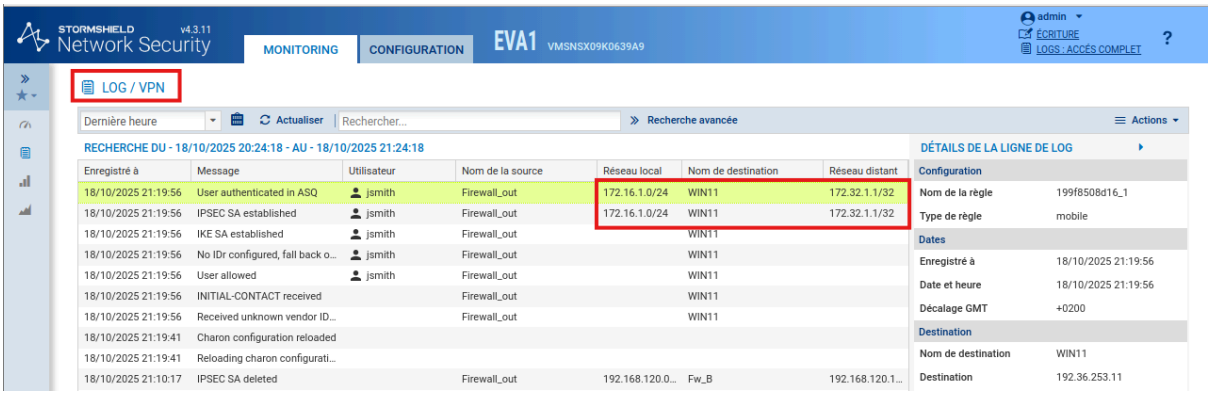
▪ Nous constatons que le tunnel s’est bien créé ainsi que dans la console VPN

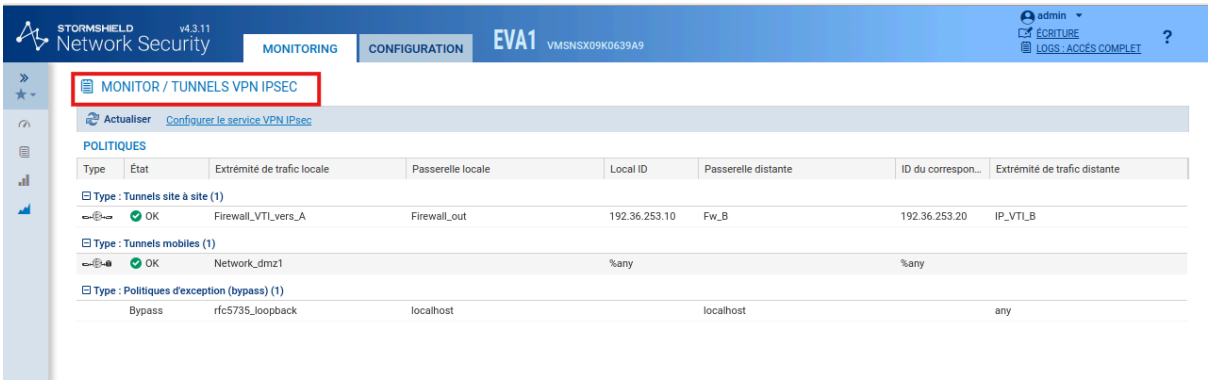


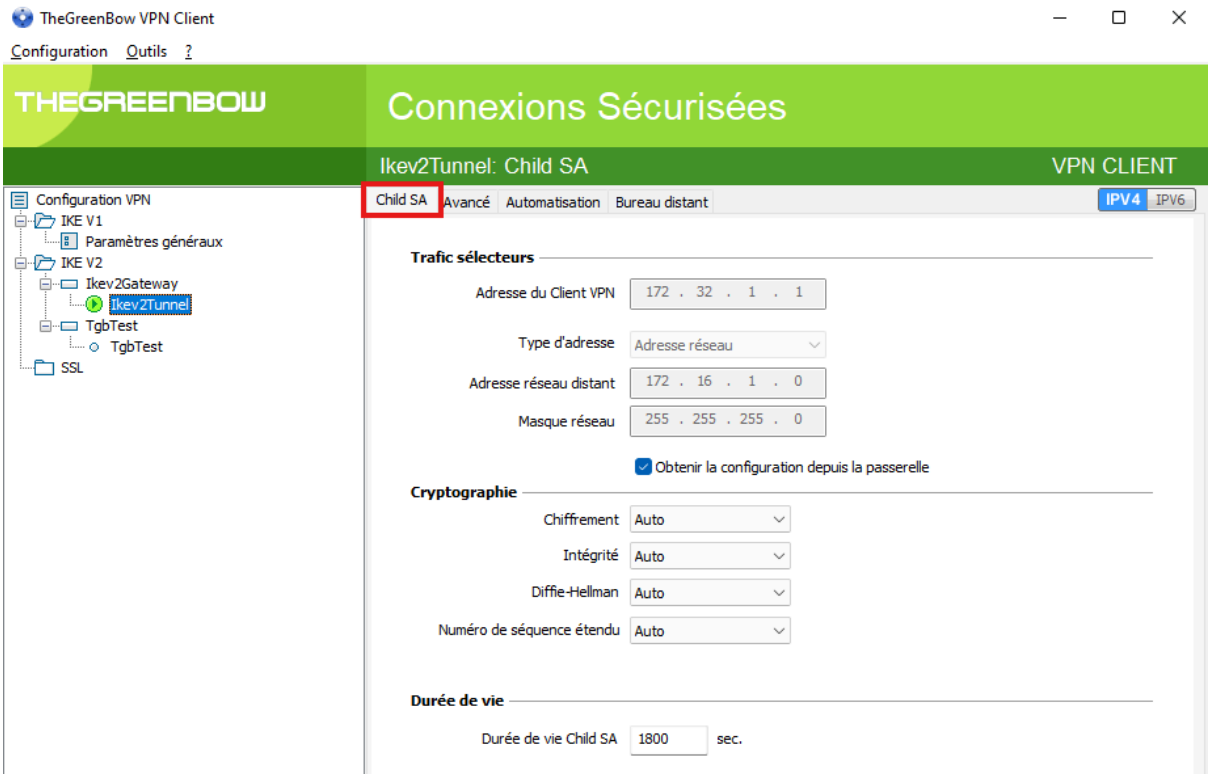
- Nous constatons l'obtentions de l'adresse IP cliente

```
Carte Ethernet TGB Ikev2Gateway-Ikev2Tunnel :

   Suffixe DNS propre à la connexion. . . :
   Description. . . . . . . . . . . . . . : TheGreenBow Virtual Miniport Adapter
   Adresse physique . . . . . . . . . . . : 02-50-F2-69-3B-00
   DHCP activé. . . . . . . . . . . . . . : Non
   Configuration automatique activée. . . : Oui
   Adresse IPv6 de liaison locale. . . . .: fe80::[illegible]:af48%22(préféré)
   Adresse IPv4. . . . . . . . . . . . . .: 172.32.1.1(préféré)
   Masque de sous-réseau. . . . . . . . . : 255.255.255.255
   Passerelle par défaut. . . . . . . . . :
   Serveurs DNS. . . . . . . . . . . . . : 172.16.1.10
   NetBIOS sur Tcpip. . . . . . . . . . . : Activé

C:\Windows\system32>
```

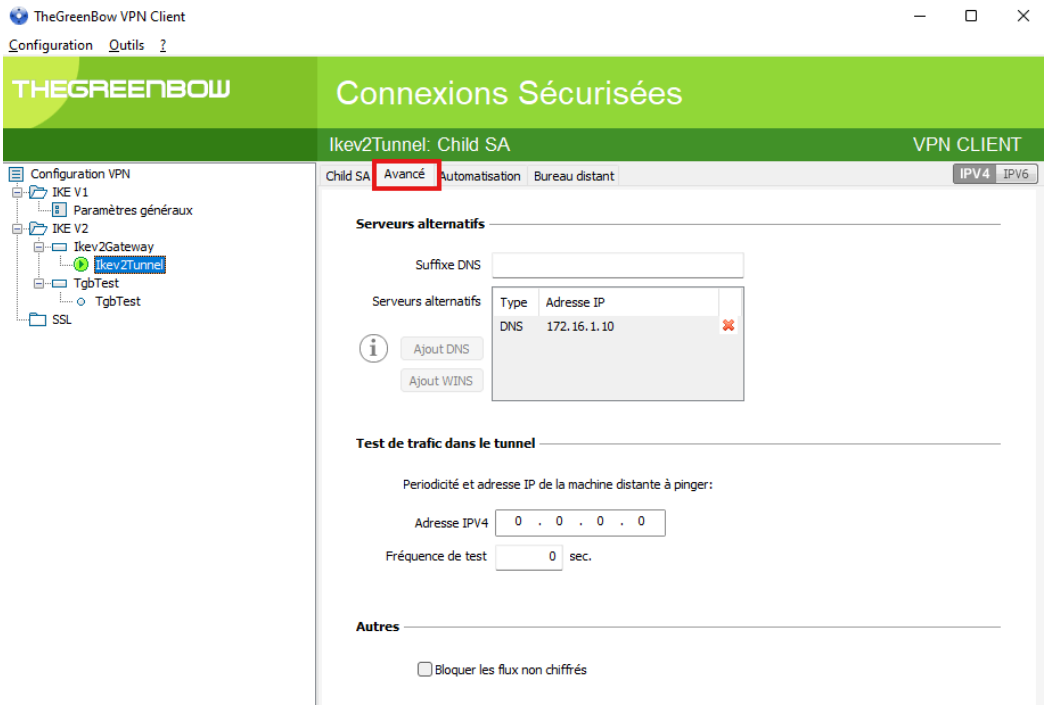
- Nous constatons que le tunnel a bien été créé dans les logs



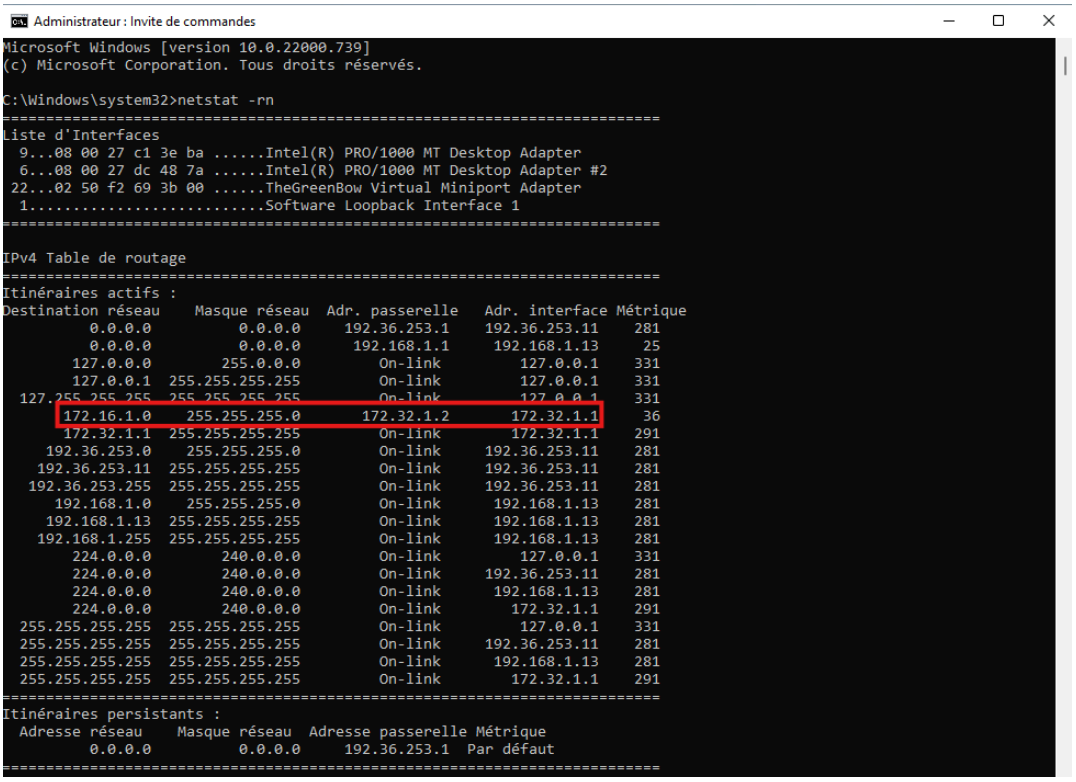



TheGreenBow VPN Client
Configuration Outils ?
THEGREENBOW
Connexions Sécurisées
Ikev2Tunnel: Child SA
VPN CLIENT
Configuration VPN
IKE V1
Paramètres généraux
IKE V2
Ikev2Gateway
Ikev2Tunnel
TgbTest
TgbTest
SSL
Child SA
Avancé
Automatisation
Bureau distant
IPV4
IPV6
Trafic sélecteurs
Adresse du Client 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
Durée de vie
Durée de vie Child SA
1800
sec.

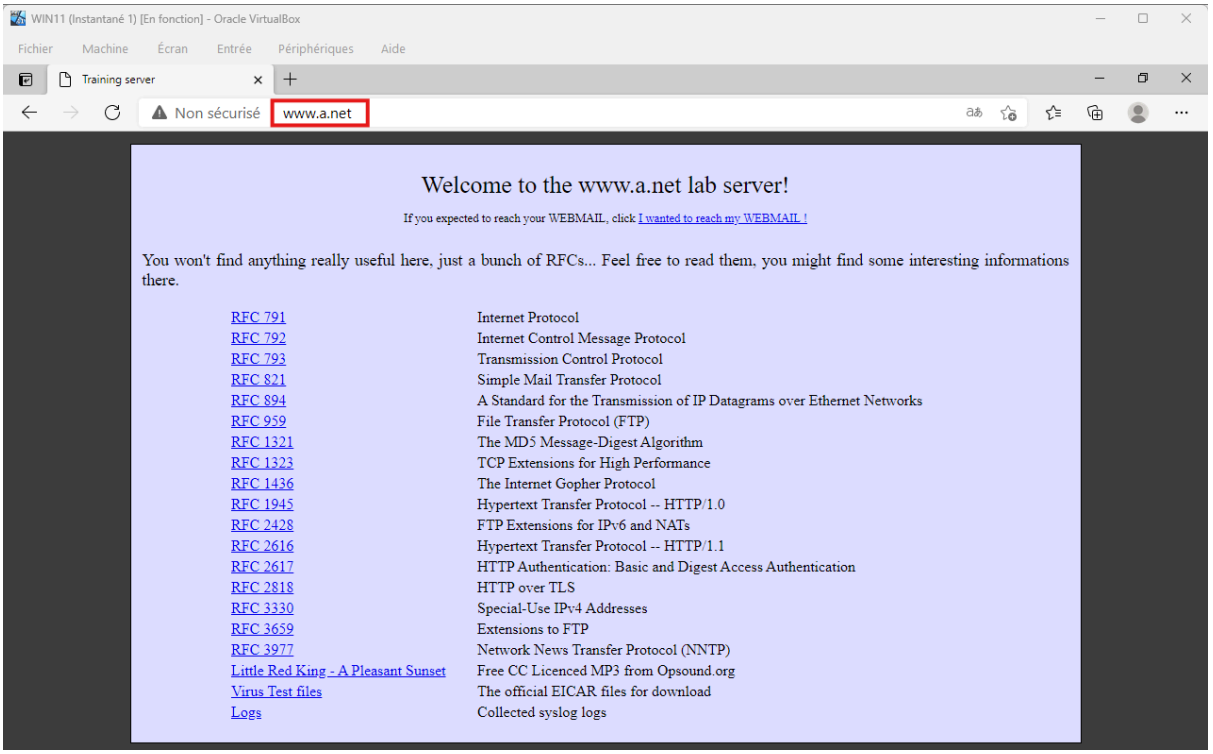
7. Affichage de la table de routage sur Windows 11



▪ Nous avons activé le mode Config afin que la passerelle distribue automatiquement l'adresse IP au client. Cela simplifie la gestion du réseau.

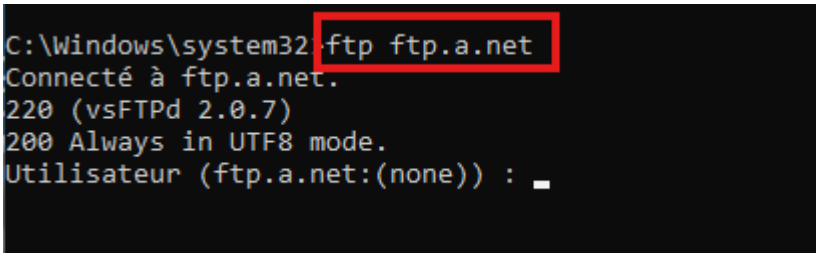


- Nous avions essayé de joindre le serveur web www.a.net



8. Test FTP

▪ Enfin, nous avons testé la connexion en lançant une commande FTP. Le test a confirmé que le VPN fonctionne comme prévu.



▪ Pour finir, nous avons effectué un ping vers l'un des serveurs de la DMZ.