

# Lab 10 – Nomade VPN IPsec avec PSK

## Table des Matières :

|                                                                            |    |
|----------------------------------------------------------------------------|----|
| 1. Création des profils de chiffrement (phase 1 IKE / phase 2 IPsec).....  | 3  |
| 2. Création du correspondant “nomade_entreprisea” (IKEv2).....             | 4  |
| 3. Création d’une politique Nomade.....                                    | 10 |
| 4. Client Windows 11 (installation du client VPN).....                     | 14 |
| 5. Installation du client TheGreenBow.....                                 | 18 |
| 6. Activation du mode Config (adresse IP attribuée par la passerelle)..... | 19 |
| 7. Affichage de la table de routage sur Windows 11.....                    | 25 |
| 8. Test FTP.....                                                           | 27 |

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

Résolution DNS

LISTE DES SERVEURS DNS UTILISÉS PAR LE FIREWALL

+ Ajouter    ✕ Supprimer

| Serveur DNS (machine) |
|-----------------------|
| srv_dns_priv          |
|                       |

# 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)

Interface de configuration EVA1 (VMSNSX09K0639A9) - MONITORING CONFIGURATION

VPN / VPN IPSEC

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

**PROFIL IKE : IKEPHASE1NOMADE**

Général

Commentaire:

Diffie-Hellman: DH14 MODP Group (2048-bits)

Durée de vie maximum (en secondes): 21600

**PROPOSITIONS**

| Chiffrement |       | Authentification |       |
|-------------|-------|------------------|-------|
| Algorithme  | Force | Algorithme       | Force |
| 1 aes       | 256   | sha2_256         | 256   |

Interface de configuration EVA1 (VMSNSX09K0639A9) - MONITORING CONFIGURATION

VPN / VPN IPSEC

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

**PROFIL IPSEC : IPSECPHASE2NOMADE**

Général

Commentaire:

Perfect Forward Secrecy (PFS): DH14 MODP Group (2048-bits)

Durée de vie maximum (en secondes): 3600

**PROPOSITIONS D'AUTHENTIFICATION**

| Algorithme    | Force |
|---------------|-------|
| 1 hmac_sha256 | 256   |

**PROPOSITIONS DE CHIFFREMENT**

+ Ajouter X Supprimer

VÉRIFICATION DE LA POLITIQUE

## 2. Création du correspondant “nomade\_entreprisea” (IKEv2)

- Création d'un correspondant ayant pour nom “nomade\_entreprisea” en nomade IKEv2

Interface de configuration Stormshield v4.3.11. Menu: MONITORING / CONFIGURATION. Page: EVA1 VMSNSX09K0639A9. Utilisateur: admin. Actions: ÉCRITURE, LOGS: ACCÈS COMPLET.

VPN / VPN IPSEC

POLITIQUE DE CHIFFREMENT - TUNNELS CORRESPONDANTS IDENTIFICATION PROFILS DE CHIFFREMENT

Entrer un filtre...

Passerelles distantes (1)

Ajouter Nouvelle passerelle distante

Actions Nouveau correspondant mobile

Commentaire:

Passerelle distante: Fw\_B

Adresse locale: Any

Profil IKE: IKE\_Phase1

Version IKE: IKEv2

CRÉER UN CORRESPONDANT MOBILE

### SÉLECTIONNER LA PASSERELLE - ASSISTANT DE CRÉATION DE CORRESPONDANT



Nom: nomade\_entreprisea

Version IKE: IKEv2

✗ ANNULER

« PRÉCÉDENT

» SUIVANT

## 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):

Clé pré-partagée (ASCII):  

Confirmer:

Saisir la clé en caractères ASCII: ☒

## CRÉER UN CORRESPONDANT MOBILE

## PARAMÈTRES D'IDENTIFICATION

## TUNNELS MOBILES : CLÉS PRÉ-PARTAGÉES (PSK)

|                                             |  |                           |                             |                                       |                               |
|---------------------------------------------|--|---------------------------|-----------------------------|---------------------------------------|-------------------------------|
| <input type="text" value="Clé recherchée"/> |  | <a href="#">+ Ajouter</a> | <a href="#">✕ Supprimer</a> | <a href="#">✎ Éditer la sélection</a> | <a href="#">📤 Exporter la</a> |
| Identité                                    |  |                           | Clé                         |                                       |                               |
| jsmith@a.net                                |  |                           | 0x4d6150534b21              |                                       |                               |
|                                             |  |                           |                             |                                       |                               |

## 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

VPN / VPN IPSEC

POLITIQUE DE CHIFFREMENT - TUNNELS CORRESPONDANTS IDENTIFICATION PROFILS DE CHIFFREMENT

Q Entrer un filtre... + Ajouter

Passerelles distantes (1)  
Site\_Fw\_A

Correspondants mobiles (1)  
nomade\_entreprisea

USERS AND GROUPS

**NOMADE\_ENTREPRISEA**

Général

Commentaire:

Passerelle distante: Any

Adresse locale: Any

Profil IKE: StrongEncryption

Version IKE: IKEv2

Identification

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

Local ID: Saisir un identifiant (optionnel)

ID du correspondant: Saisir un identifiant (optionnel)

Clé pré-partagée (PSK):  Éditer

Configuration avancée

STORMSHIELD Network Security v4.3.11

MONITORING CONFIGURATION EVA1 VMSNSX09K0639A9

admin

ÉCRITURE

LOGS - ACCÈS RESTREINT ?

CONFIGURATION

Rechercher...

SYSTÈME

RÉSEAU

Interfaces

Interfaces virtuelles

Routing

Routing multicast

DNS dynamique

DHCP

VPN / VPN IPSEC

POLITIQUE DE CHIFFREMENT - TUNNELS CORRESPONDANTS IDENTIFICATION PROFILS DE CHIFFREMENT

Q 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

- Le compte jsmith est bien spécifié

STORMSHIELD  
Network Security  
v4.311

MONITORINGCONFIGURATIONEVA1  
VMSNSX09K0639A9

admin  
ÉCRITURE  
LOGS - ACCÈS RESTREINT

VPN / VPN IPSEC

POLITIQUE DE CHIFFREMENT - TUNNELSCORRESPONDANTSIDENTIFICATIONPROFILS DE CHIFFREMENT

AUTORITÉ DE CERTIFICATION ACCEPTÉES

+ Ajouter X Supprimer

CA

TUNNELS MOBILES : CLÉS PRÉ-PARTAGÉES (PSK)

Clé recherchée+ Ajouter X SupprimerÉditer la sélectionExporter la liste des PSK

USERS AND GROUPS

Clé

jsmith@a.net0x4d6150534b21

Configuration avancée

### 3. Création d'une politique Nomade

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

The screenshot shows the Stormshield Network Security v4.3.11 interface. The user is logged in as 'admin'. The 'CONFIGURATION' tab is active, and the 'VPN / VPN IPSEC' section is selected. The 'POLITIQUE DE CHIFFREMENT - TUNNELS' tab is highlighted. The 'MOBILE - UTILISATEURS NOMADES' section is selected. A table lists the policies, with 'Nouvelle politique mobile simple' highlighted. The table has columns: Etat, Réseau distant, Profil de chiffrement, Mode Config, Keepalive, and Commentaire.

#### ASSISTANT DE POLITIQUE VPN IPSEC NOMADE

Les ressources locales définies sont accessibles à tous les utilisateurs authentifiés au travers d'un tunnel IPsec  
En mode standard, les utilisateurs distants présentent une adresse IP appartenant à un réseau qui leur est propre



**RESSOURCES LOCALES**

+ Ajouter
 X Supprimer

Network\_dmz1

Choix du correspondant:  
 nomade\_entreprisea

Réseaux distants:  
 Any

X ANNULER

✓ TERMINER

The screenshot shows 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 icons for navigation. The main content area is titled 'VPN / VPN IPSEC' and shows the 'POLITIQUE DE CHIFFREMENT - TUNNELS' tab. A table lists VPN policies, with the first policy 'IPsec 01 (01)' selected. The table has columns for 'Etat', 'Réseau local', 'Correspondant', 'Réseau distant', 'Profil de chiffrement', 'Mode Config', 'Keepalive', and 'Commentaire'. The 'Réseau distant' column for the first policy is highlighted with a red box.

| Etat | Réseau local | Correspondant      | Réseau distant   | Profil de chiffrement | Mode Config | Keepalive | Commentaire                  |
|------|--------------|--------------------|------------------|-----------------------|-------------|-----------|------------------------------|
| off  | Network_dmz1 | nomade_entreprises | <span>Net</span> | StrongEncryption      | off         |           | Originally created on 202... |

- Nous créons un nouvel objet "réseau" qui sera le réseau distant

The screenshot shows the 'CRÉER UN OBJET' (Create Object) form in the Stormshield interface. The left sidebar lists various object types: Machine, Réseau (selected), Plage d'adresses, Routeur, Groupe, Protocole IP, Port, Groupe de ports, Groupe de régions, and Objet temps. The main form has fields for 'Nom de l'objet', 'Adresses IPv4', 'Adresse IP de réseau', and 'Commentaire'. The 'Adresse IP de réseau' field is highlighted with a red box.

Nom de l'objet: Net-IPSECVPN

Adresses IPv4

Adresse IP de réseau: 172.32.1.0/24

Exemple 192.168.0.0/16 ou 192.168.0.0/255.255.0.0

Commentaire:

▪ Modification du profil de chiffrement antérieurement créé

The screenshot shows the Stormshield Network Security v4.3.11 interface. The left sidebar contains navigation options: CONFIGURATION, SYSTÈME, and RÉSEAU. The main panel is titled 'VPN / VPN IPSEC' and shows the 'POLITIQUE DE CHIFFREMENT - TUNNELS' tab. A table lists the configuration for 'IPsec 01 (01)'. The 'Mode Config' dropdown is highlighted with a red box, showing 'IPSECPhase2Nomade'.

| Id | Etat | Réseau local | Correspondant     | Réseau distant | Profil de chiffrement | Mode Config | Keepalive | Commentaire                 |
|----|------|--------------|-------------------|----------------|-----------------------|-------------|-----------|-----------------------------|
| 1  | on   | Network_dmz1 | nomade_entreprise | Net-IPSECVPN   | IPSECPhase2Nomade     | on          | 30        | Originally created on 20... |

▪ Nous activons le mode config

The screenshot shows the Stormshield Network Security v4.3.11 interface. The left sidebar contains navigation options: CONFIGURATION, SYSTÈME, and RÉSEAU. The main panel is titled 'VPN / VPN IPSEC' and shows the 'POLITIQUE DE CHIFFREMENT - TUNNELS' tab. A table lists the configuration for 'IPsec 01 (01)'. The 'Mode Config' dropdown is highlighted with a red box, showing 'on'.

| Id | Etat | Réseau local | Correspondant     | Réseau distant | Profil de chiffrement | Mode Config | Keepalive | Commentaire                  |
|----|------|--------------|-------------------|----------------|-----------------------|-------------|-----------|------------------------------|
| 1  | off  | Network_dmz1 | nomade_entreprise | Net-IPSECVPN   | IKE_Phase2            | on          | 30        | Originally created on 202... |

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

VPN IPSEC LAB10 (contient 4 règles, de 31 à 34)

|    |    |        |                                                                           |              |                             |     |                                   |
|----|----|--------|---------------------------------------------------------------------------|--------------|-----------------------------|-----|-----------------------------------|
| 31 | on | passer | Any                                                                       | Firewall_out | isakmp<br>isakmp_natt       | IPS | Crée le 2025-10-15 22:09:45, p... |
| 32 | on | passer | Any                                                                       | Firewall_out | Any<br>vpn-esp              | IPS | Crée le 2025-10-15 22:10:26, p... |
| 33 | on | passer | jsmith@b.net Net-IPSECVPN<br>Auth. par :VPN IPsec<br>via Tunnel VPN IPsec | Network_dmz1 | http<br>ftp<br>dns          | IPS | Crée le 2025-10-15 22:11:07, p... |
| 34 | on | passer | jsmith@b.net Net-IPSECVPN<br>Auth. par :VPN IPsec<br>via Tunnel VPN IPsec | Network_dmz1 | Any<br>icmp (requête Ech... | IPS | Crée le 2025-10-15 22:20:59, p... |

VPN (contient 2 règles, de 35 à 36)

<< < Page 1 sur 1 > >> ↺

Page courante 1 - 29 sur 29

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

STORMSHIELD v4.3.11  
Network Security

MONITORING CONFIGURATION EVA1 VMSNSX09K0639A9

UTILISATEURS / DROITS D'ACCÈS

ACCÈS PAR DÉFAUT ACCÈS DÉTAILLÉ SERVEUR PPTP

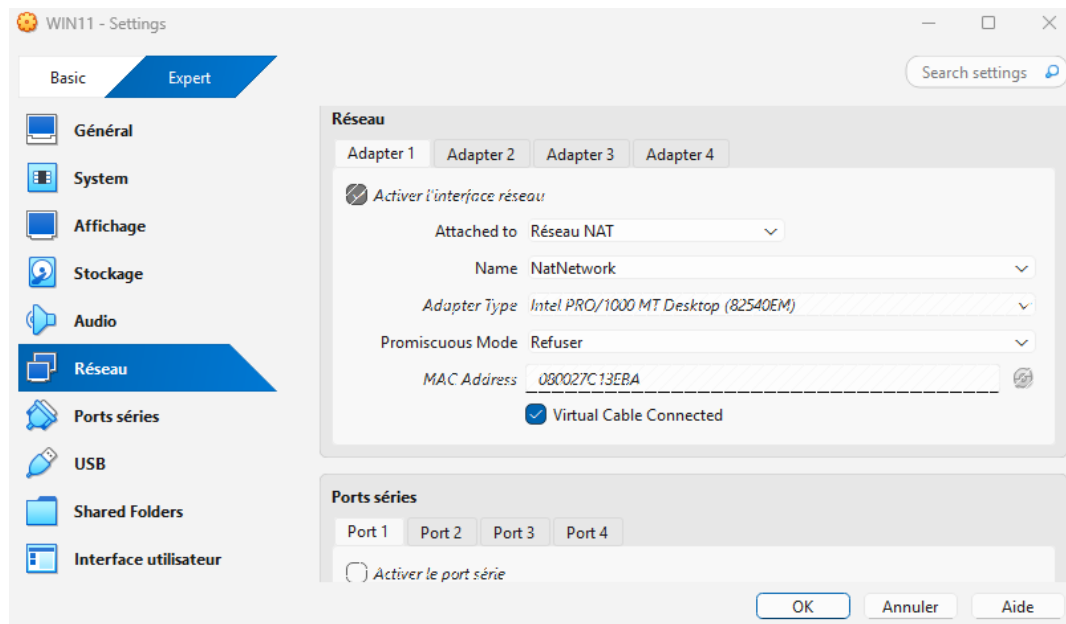
Rechercher...

+ Ajouter X Supprimer ↑ Monter ↓ Descendre

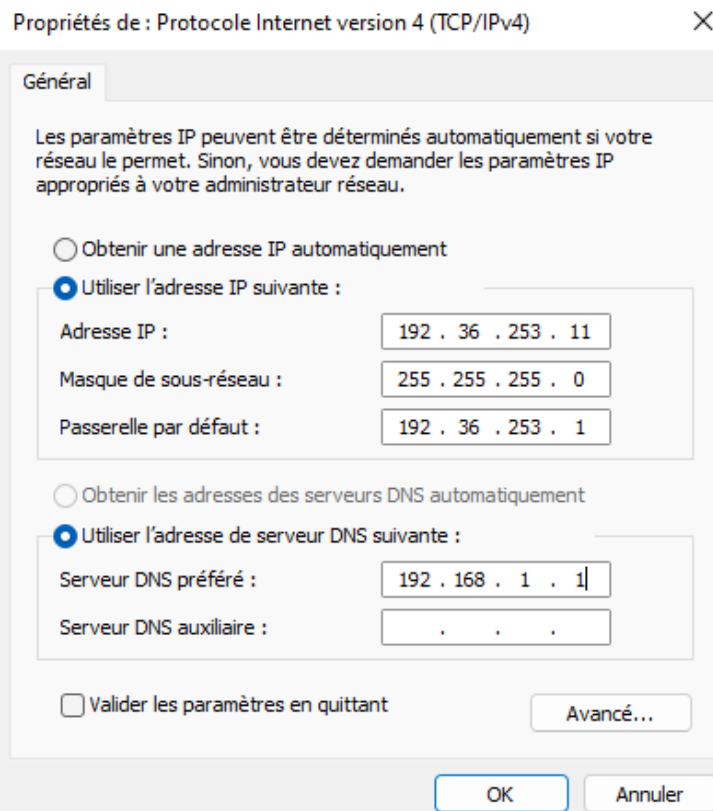
| Etat      | Utilisateur - groupe d'utilisateurs | VPN SSL Portail | IPSEC     | VPN SSL   | Parrainage | Description |
|-----------|-------------------------------------|-----------------|-----------|-----------|------------|-------------|
| 1  Activé | jsmith@b.net                        | Interdire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

## 4. Client Windows 11 (installation du client VPN)

- Nous avons créé le réseau Nat Network (192.36.253.0/24)



- Nous attribuons une ip à la machine



## ▪ Création de l'objet machine "WIN11"

**CRÉER UN OBJET**

**Machine**

Nom DNS (FQDN)

Réseau

Plage d'adresses

Routeur

Groupe

Protocole IP

Port

Groupe de ports

Groupe de régions

Objet temps

Nom de l'objet:

Adresse IPv4:

Adresse MAC:

**Résolution**

☒ Aucune (IP statique) ☐ Automatique

Commentaire:

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

**STORMSHIELD Network Security v4.3.11** **MONITORING CONFIGURATION EVA1** VMSNSX09K0639A9 **admin** **ÉCRITERE** **LOGS - ACCÈS RESTREINT ?**

**SYSTÈME / CONFIGURATION**

CONFIGURATION GÉNÉRALE **ADMINISTRATION DU FIREWALL** PARAMÈTRES RÉSEAUX

Accès à l'interface d'administration du Firewall

☒ Autoriser le compte 'admin' à se connecter

Port d'écoute:  [Configurer le certificat SSL du service](#)

Délai maximal d'inactivité (tous administrateurs):

☒ Activer la protection contre les attaques par force brute

Tentatives d'authentification autorisées:

Durée du blocage (minutes):

**ACCÈS AUX PAGES D'ADMINISTRATION DU FIREWALL**

[+ Ajouter](#) [X Supprimer](#)

Poste d'administration autorisé (machine ou groupe - réseau - plage d'adresses)

network\_internals

**WIN11**

Avertissement pour l'accès à l'interface d'administration

Fichier d'avertissement:  [Supprimer le fichier d'avertissement](#)

Accès distant par SSH

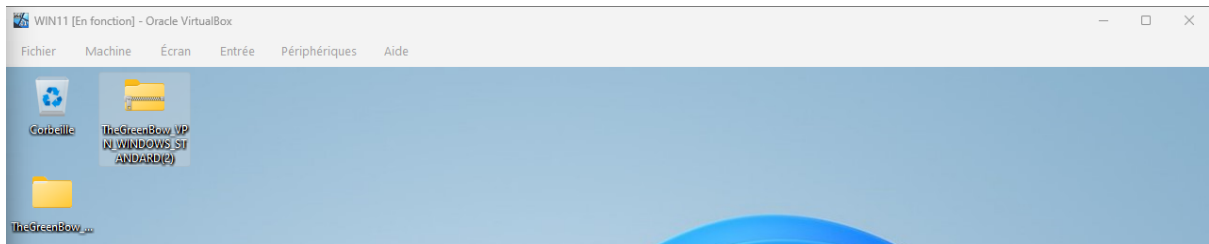
☒ Activer l'accès par SSH **!**

☒ Autoriser l'utilisation de mot de passe

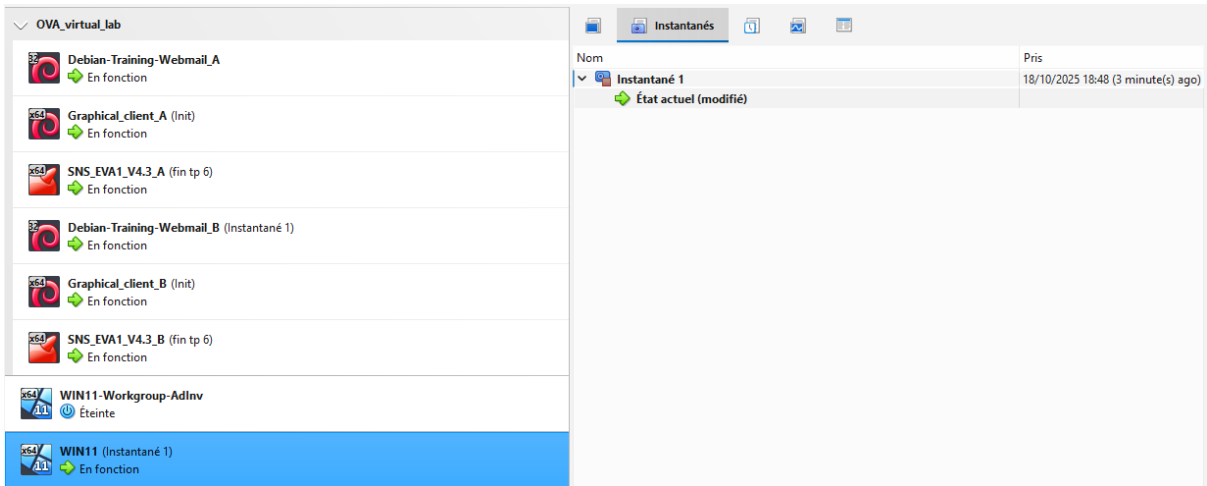
☐ Utiliser le shell nsrpc pour les administrateurs autres que le compte admin

Port d'écoute:

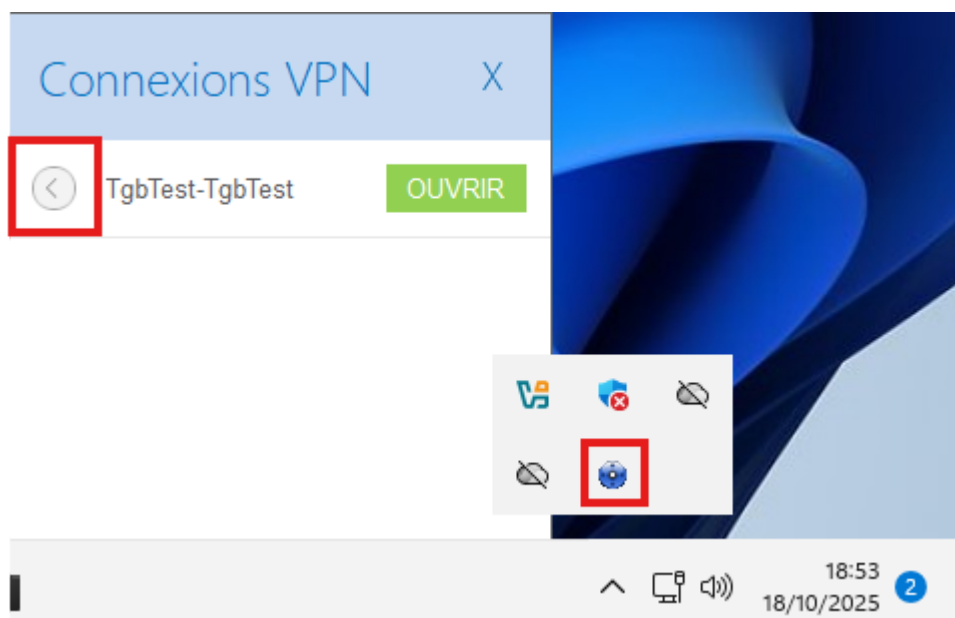
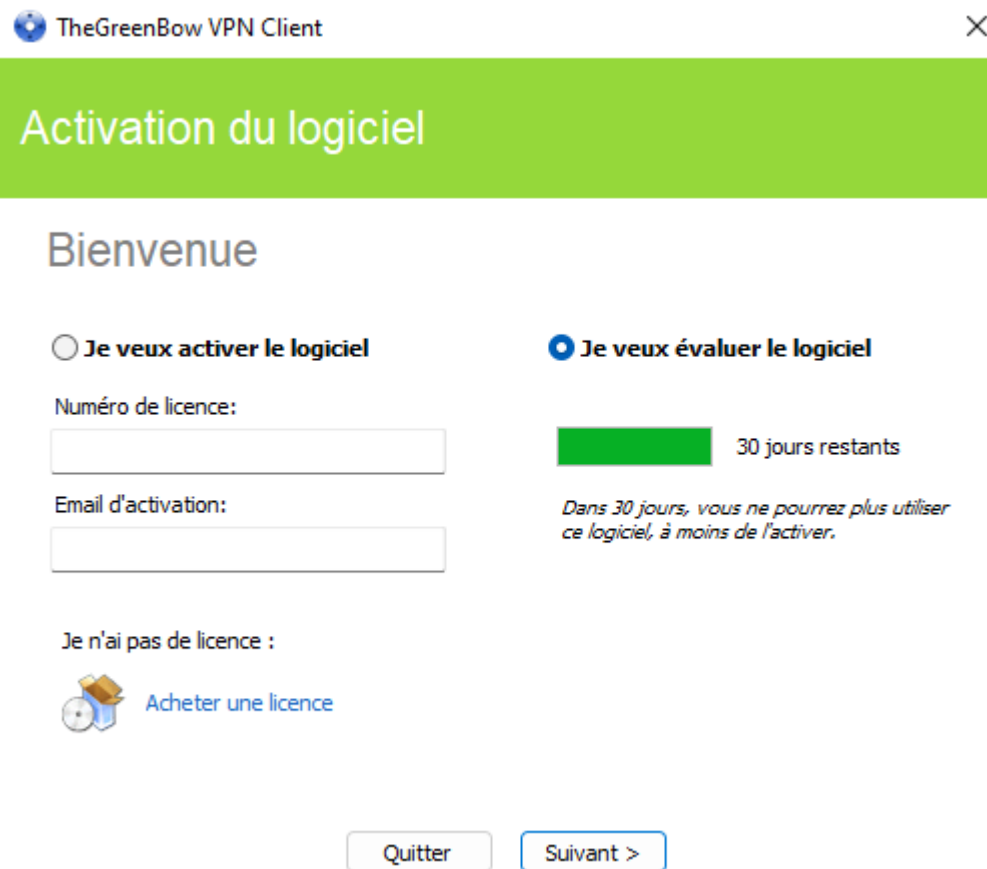
- Nous avons déplacé le fichier .zip sur notre machine physique puis sur la machine win11 puis nous l'avons dézip pour en extraire l'exécutable TheGreenBow



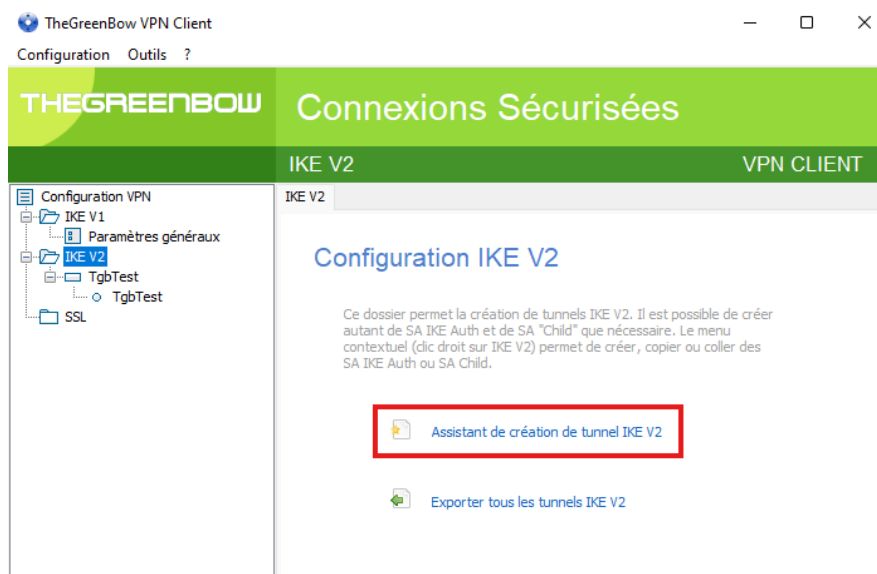
- Avant son exécution, nous réalisons une snapshot de la machine



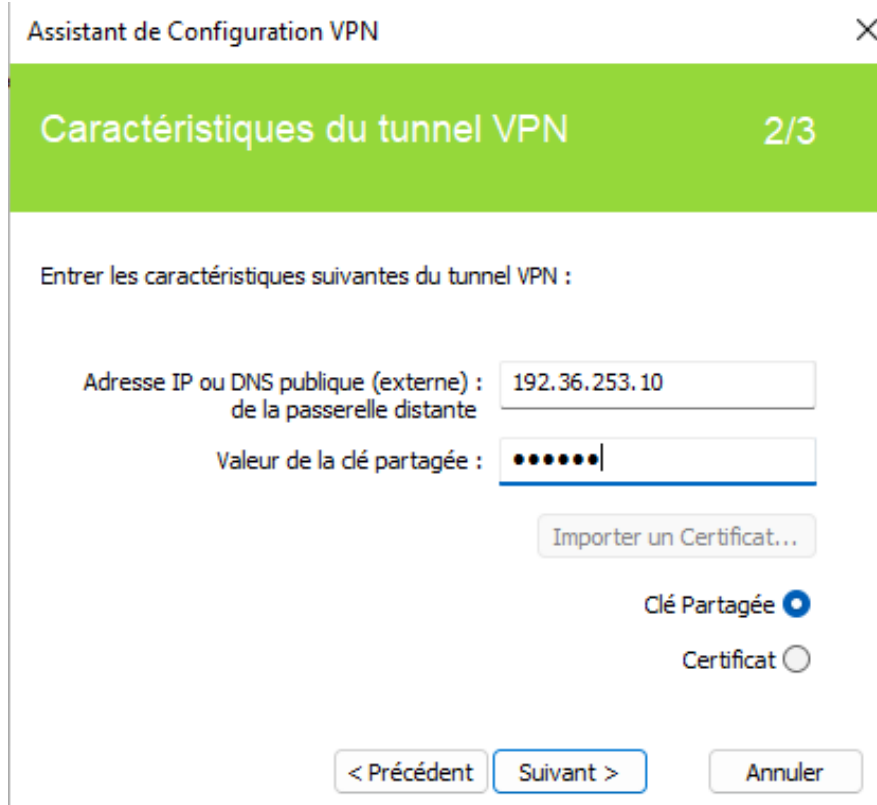
## 5. Installation du client TheGreenBow

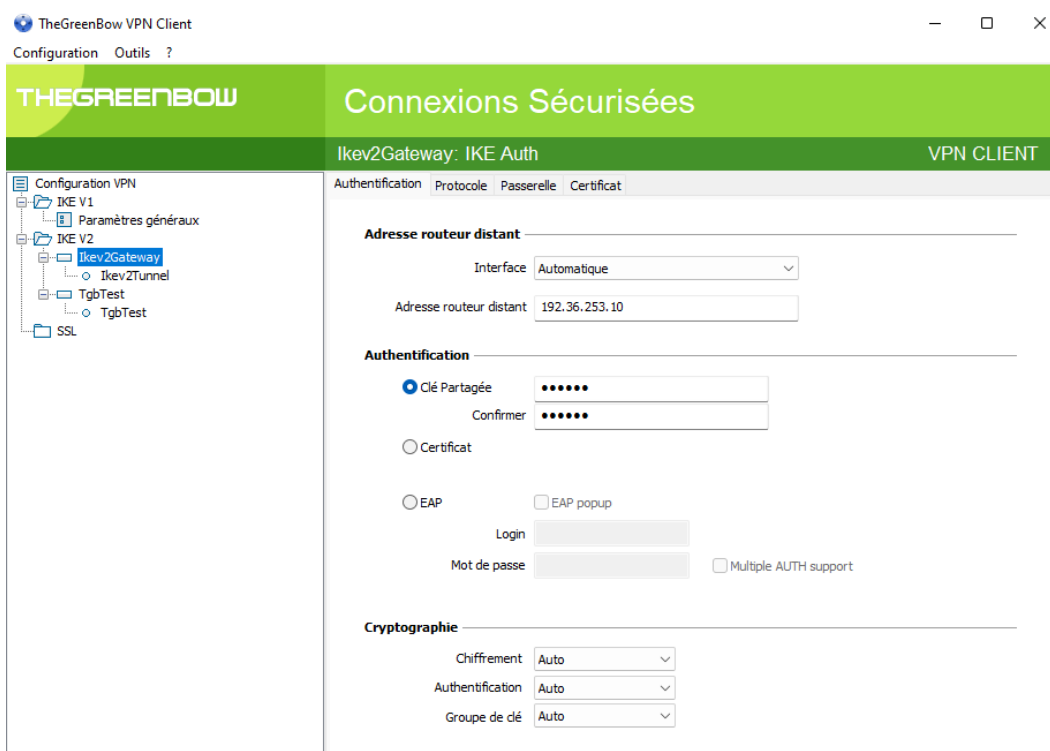
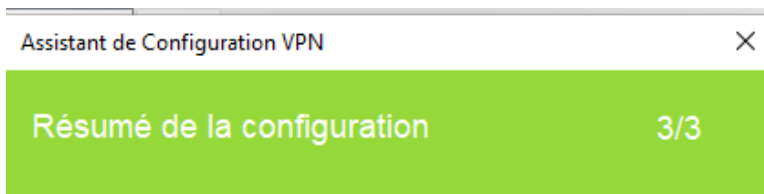


## 6. Activation du mode Config (adresse IP attribuée par la passerelle)



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





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

TheGreenBow VPN Client

Configuration Outils ?

## THEGREENBOW Connexions Sécurisées VPN CLIENT

Ikev2Gateway: IKE Auth

**Authentification** Protocole Passerelle Certificat

**Configuration VPN**

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

**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: AES CBC 256

Authentification: SHA2 256

Groupe de clé: DH14 (MODP 2048)

TheGreenBow VPN Client

Configuration Outils ?

## THEGREENBOW Connexions Sécurisées VPN CLIENT

Ikev2Gateway: IKE Auth

Authentification **Protocole** Passerelle Certificat

**Configuration VPN**

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

**Identité**

Local ID: Email jsmith@a.net

Remote ID: .....

**Fonctions avancées**

Fragmentation ☒ Taille des fragments: 1280

Port IKE: 500 ☐ Activer l'offset NAT

Port NAT: 4500

Initiation Childless ☐



- 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::9f00:36e4:1039: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

STORMSHIELD  
Network Security

MONITORING

CONFIGURATION

EVA1

VMSNSX09K0639A9

admin

ÉCRITURE

LOGS : ACCÈS COMPLET

LOG / VPN

Dernière heure

Actualiser

Rechercher...

Recherche avancée

Actions

RECHERCHE DU - 18/10/2025 20:24:18 - AU - 18/10/2025 21:24:18

| Enregistré à        | Message                           | Utilisateur | Nom de la source | Réseau local     | Nom de destination | Réseau distant   |
|---------------------|-----------------------------------|-------------|------------------|------------------|--------------------|------------------|
| 18/10/2025 21:19:56 | User authenticated in ASQ         | jsmith      | Firewall_out     | 172.16.1.0/24    | WIN11              | 172.32.1.1/32    |
| 18/10/2025 21:19:56 | IPSEC SA established              | jsmith      | Firewall_out     | 172.16.1.0/24    | WIN11              | 172.32.1.1/32    |
| 18/10/2025 21:19:56 | IKE SA established                | jsmith      | Firewall_out     |                  | WIN11              |                  |
| 18/10/2025 21:19:56 | No IDr configured, fall back o... | jsmith      | Firewall_out     |                  | WIN11              |                  |
| 18/10/2025 21:19:56 | User allowed                      | jsmith      | Firewall_out     |                  | WIN11              |                  |
| 18/10/2025 21:19:56 | INITIAL-CONTACT received          |             | Firewall_out     |                  | WIN11              |                  |
| 18/10/2025 21:19:56 | Received unknown vendor ID...     |             | Firewall_out     |                  | WIN11              |                  |
| 18/10/2025 21:19:41 | Charon configuration reloaded     |             |                  |                  |                    |                  |
| 18/10/2025 21:19:41 | Reloading charon configurati...   |             |                  |                  |                    |                  |
| 18/10/2025 21:10:17 | IPSEC SA deleted                  |             | Firewall_out     | 192.168.120.0... | Fw_B               | 192.168.120.1... |

DÉTAILS DE LA LIGNE DE LOG

Configuration

Nom de la règle199f8508d16\_1

Type de règlemobile

Dates

Enregistré à18/10/2025 21:19:56

Date et heure18/10/2025 21:19:56

Décalage GMT+0200

Destination

Nom de destinationWIN11

Destination192.36.253.11

STORMSHIELD  
Network Security

MONITORING

CONFIGURATION

EVA1

VMSNSX09K0639A9

admin

ÉCRITURE

LOGS : ACCÈS COMPLET

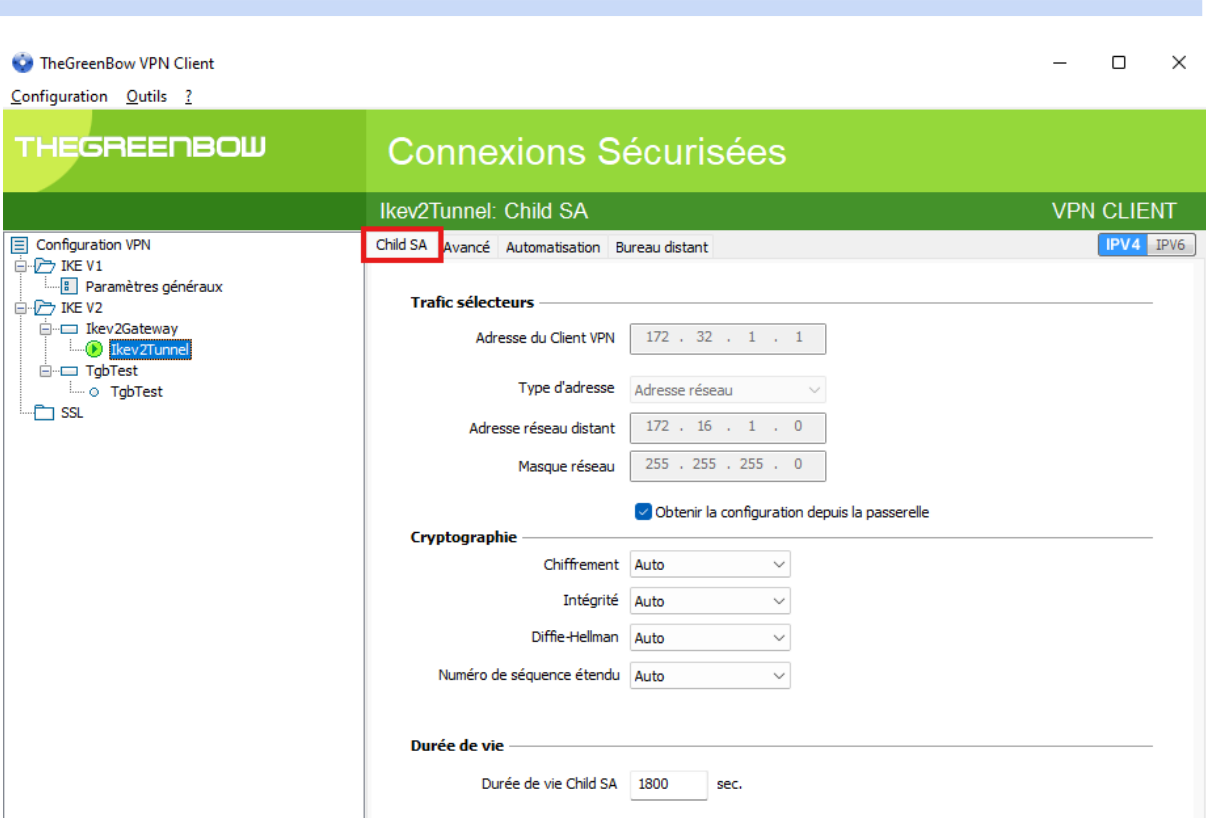
MONITOR / TUNNELS VPN IPSEC

Actualiser

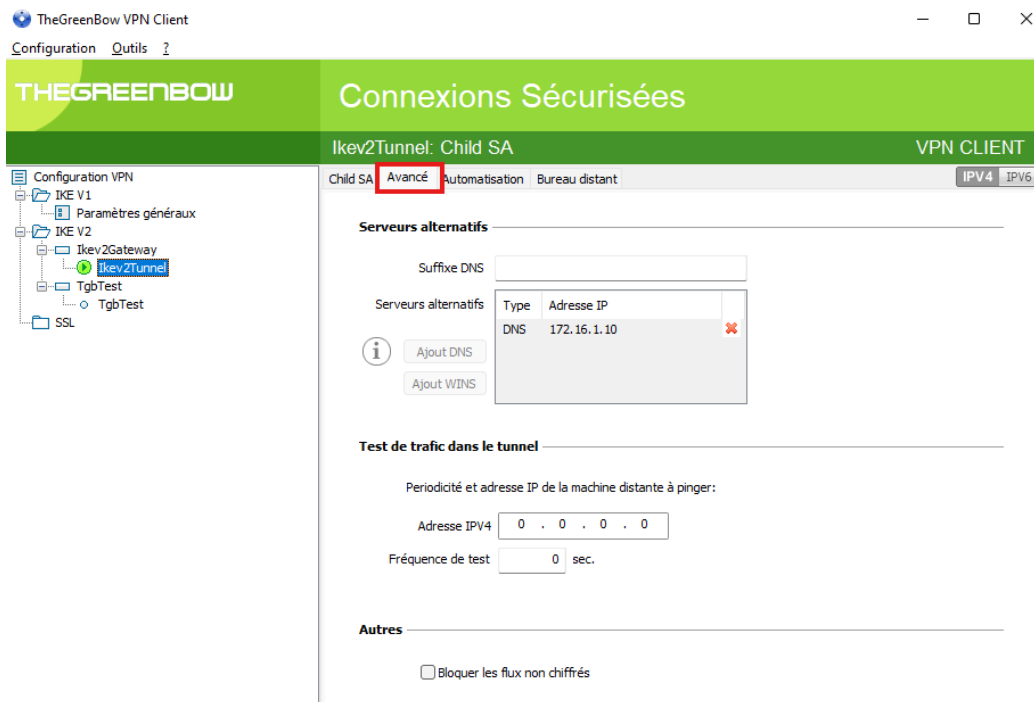
Configurer le service VPN IPsec

POLITIQUES

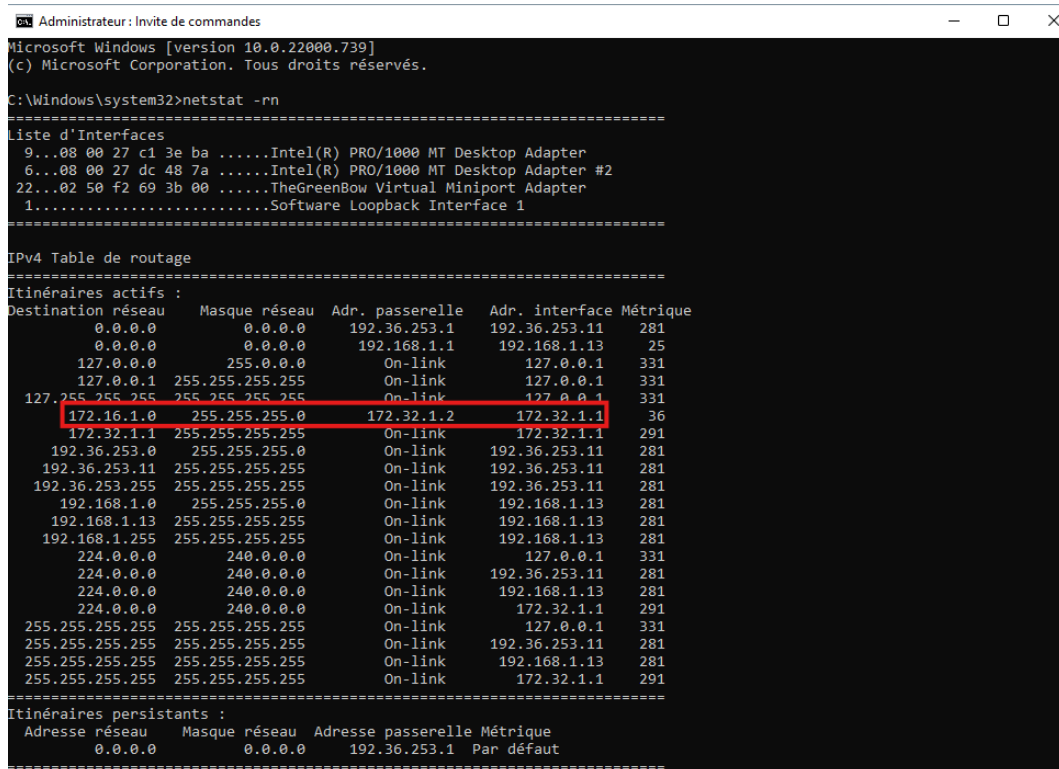
| Type                                       | État | Extrémité de trafic locale | Passerelle locale | Local ID | Passerelle distante | ID du correspon... | Extrémité de trafic distante |
|--------------------------------------------|------|----------------------------|-------------------|----------|---------------------|--------------------|------------------------------|
| Type : Tunnels site à site (1)             |      |                            |                   |          |                     |                    |                              |
| Firewall_VTL_vers_A                        | OK   | Firewall_out               | 192.36.253.10     | Fw_B     | 192.36.253.20       | IP_VTL_B           |                              |
| Type : Tunnels mobiles (1)                 |      |                            |                   |          |                     |                    |                              |
| Network_dmz1                               | OK   |                            | %any              |          | %any                |                    |                              |
| Type : Politiques d'exception (bypass) (1) |      |                            |                   |          |                     |                    |                              |
| Bypass                                     |      | rfc5735_loopback           | localhost         |          | localhost           |                    | any                          |



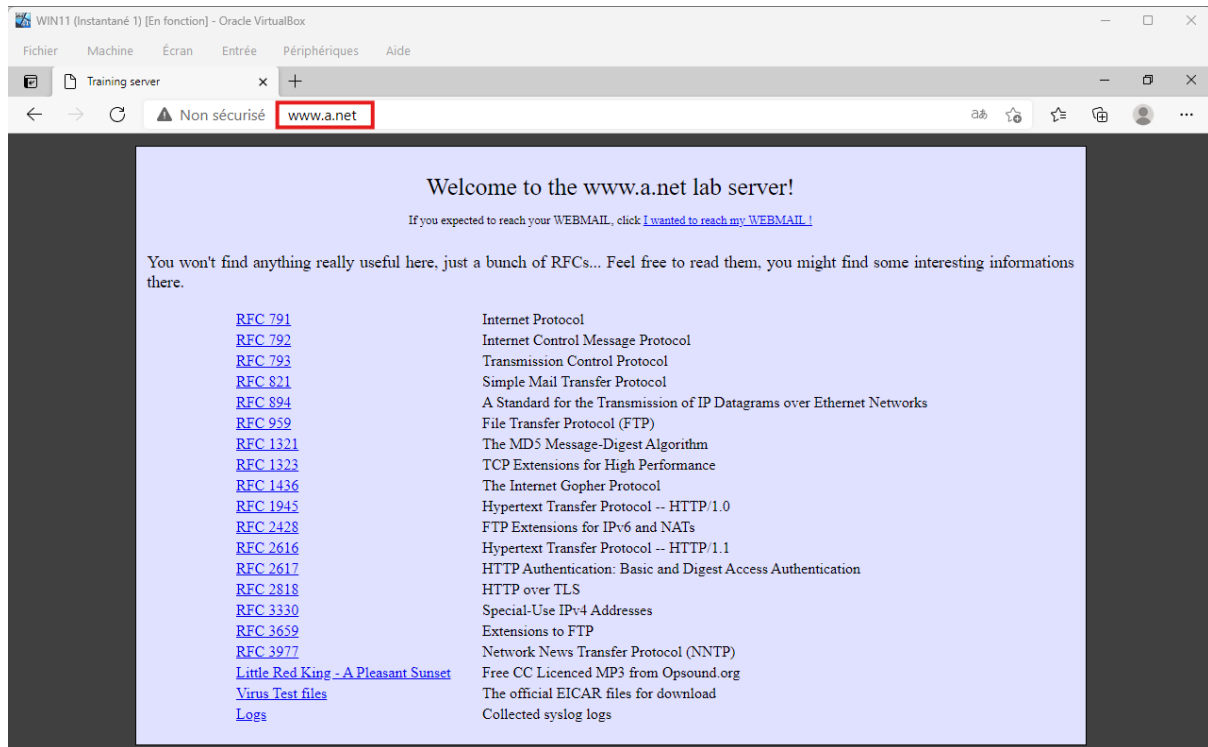
## 7. Affichage de la table de routage sur Windows 11



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



- Nous avons essayé de joindre le serveur web [www.a.net](http://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.

```
C:\Windows\system32 ftp ftp.a.net
Connecté à ftp.a.net.
220 (vsFTPd 2.0.7)
200 Always in UTF8 mode.
Utilisateur (ftp.a.net:(none)) : _
```

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

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

C:\Windows\system32 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=1 ms TTL=64
Réponse de 172.16.1.12 : octets=32 temps=3 ms TTL=64
Réponse de 172.16.1.12 : octets=32 temps=11 ms TTL=64
Réponse de 172.16.1.12 : octets=32 temps=4 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 = 11ms, Moyenne = 4ms

C:\Windows\system32>
```