
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 X 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)

The screenshot shows the Stormshield configuration interface for VPN/IPSEC. The user is logged in as 'admin'. The main menu includes 'MONITORING' and 'CONFIGURATION'. The current page is 'VPN / VPN IPSEC' with sub-tabs for 'POLITIQUE DE CHIFFREMENT - TUNNELS', 'CORRESPONDANTS', 'IDENTIFICATION', and 'PROFILS DE CHIFFREMENT'. The 'PROFILS DE CHIFFREMENT' tab is active, showing a list of profiles on the left and the configuration for 'PROFIL IKE : IKEPHASE1NOMADE' on the right. The 'IKEPHASE1NOMADE' profile is highlighted in red in the list. The configuration details for this profile are as follows:

PROFIL IKE : IKEPHASE1NOMADE

Général

Commentaire:

Diffie-Hellman:

Durée de vie maximum (en secondes):

PROPOSITIONS

		Chiffrement		Authentification	
	Algorithme	Force	Algorithme	Force	
1	aes	256	sha2_256	256	

The screenshot shows the Stormshield configuration interface for VPN/IPSEC. The user is logged in as 'admin'. The main menu includes 'MONITORING' and 'CONFIGURATION'. The current page is 'VPN / VPN IPSEC' with sub-tabs for 'POLITIQUE DE CHIFFREMENT - TUNNELS', 'CORRESPONDANTS', 'IDENTIFICATION', and 'PROFILS DE CHIFFREMENT'. The 'PROFILS DE CHIFFREMENT' tab is active, showing a list of profiles on the left and the configuration for 'PROFIL IPSEC : IPSECPHASE2NOMADE' on the right. The 'IPSECPHASE2NOMADE' profile is highlighted in red in the list. The configuration details for this profile are as follows:

PROFIL IPSEC : IPSECPHASE2NOMADE

Général

Commentaire:

Perfect Forward Secrecy (PFS):

Durée de vie maximum (en secondes):

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



The screenshot shows the Stormshield configuration interface. The top navigation bar includes 'MONITORING', 'CONFIGURATION', and 'EVA1'. The main menu on the left shows 'VPN / VPN IPSEC' selected. The central panel is titled 'CORRESPONDANTS' and contains a table with one entry 'Passerelles distantes (1)'. A context menu is open over this entry, with the option 'Nouveau correspondant mobile' highlighted in red. Below the menu, a form for creating a mobile peer is visible, with fields for 'Commentaire', 'Passerelle distante' (set to 'Fw_B'), 'Adresse locale' (set to 'Any'), 'Profil IKE' (set to 'IKE_Phase1'), and 'Version IKE' (set to 'IKEv2').

CRÉER UN CORRESPONDANT MOBILE

SÉLECTIONNER LA PASSERELLE - ASSISTANT DE CRÉATION DE CORRESPONDANT



Nom:

Version IKE:

✗ 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)

Clé recherchée		+ Ajouter	× Supprimer	✎ Éditer la sélection	↑ Exporter la
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

Entrer un filtre... + Ajouter

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 ?

VPN / VPN IPSEC

POLITIQUE DE CHIFFREMENT - TUNNELS CORRESPONDANTS IDENTIFICATION PROFILS DE CHIFFREMENT

Entrer un filtre... + Ajouter

NOMADE_ENTREPRISEA

Général

Commentaire:

Passerelle distante: Any

Adresse locale: Any

Profil IKE: IKEPhase1Nomade

Version IKE: IKEv2

Le compte jsmith est bien spécifié

The screenshot shows the Stormshield Network Security configuration interface. The top navigation bar includes 'MONITORING' and 'CONFIGURATION' tabs, with 'EVA1' and 'VMSNSX09K0639A9' displayed. The 'IDENTIFICATION' sub-tab is highlighted in red. Below the navigation, there are sections for 'AUTORITÉ DE CERTIFICATION ACCEPTÉES' (containing a 'CA' entry) and 'TUNNELS MOBILES : CLÉS PRÉ-PARTAGÉES (PSK)'. The PSK section contains a table with the following data:

Clé recherchée	Clé
jsmith@a.net	0x4d6150534b21

Additional interface elements include a search bar, '+ Ajouter', 'X Supprimer', and 'Éditer la sélection' buttons, and an 'Exporter la liste des PSK' link. A 'Configuration avancée' dropdown is visible at the bottom left.

3. Création d'une politique Nomade

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

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



The screenshot shows the Stormshield Network Security interface. The top navigation bar includes 'MONITORING' and 'CONFIGURATION' tabs, with 'EVA1' and 'VMSNSX09K0639A9' displayed. The left sidebar shows a navigation menu with 'VPN / VPN IPSEC' selected. The main content area is titled 'POLITIQUE DE CHIFFREMENT - TUNNELS' and shows a table of IPsec policies. The table has columns for 'Etat', 'Réseau local', 'Correspondant', 'Réseau distant', 'Profil de chiffrement', 'Mode Config', 'Keepalive', and 'Commentaire'. A red box highlights the 'Réseau distant' dropdown menu in the first row, which is currently set to 'Any'.

	Etat	Réseau local	Correspondant	Réseau distant	Profil de chiffrement	Mode Config	Keepalive	Commentaire
1	off	Network_dmz1	nomade_entreprises	Any	StrongEncryption	off		Originally created on 202...

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

The screenshot shows the 'CRÉER UN OBJET' form in the Stormshield interface. The left sidebar lists various object types: 'Machine', 'Réseau', 'Plage d'adresses', 'Routeur', 'Groupe', 'Protocole IP', 'Port', 'Groupe de ports', 'Groupe de régions', and 'Objet temps'. The 'Réseau' option is selected. The form fields are: 'Nom de l'objet:' with the value 'Net-IPSECVPN'; 'Adresses IPv4' section with 'Adresse IP de réseau:' containing '172.32.1.0/24' and an example 'Exemple 192.168.0.0/16 ou 192.168.0.0/255.255.0.0'; and 'Commentaire:' which is empty. A red box highlights the 'Nom de l'objet' and 'Adresse IP de réseau' fields.

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: 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 configuration page for VPN / VPN IPSEC. The 'POLITIQUE DE CHIFFREMENT - TUNNELS' tab is active, showing a table of VPN policies. The policy 'IPsec 01 (01)' is selected. The table has columns for 'Etat', 'Réseau local', 'Correspondant', 'Réseau distant', 'Profil de chiffrement', 'Mode Config', 'Keepalive', and 'Commentaire'. The 'Mode Config' dropdown for the 'IPSECPhase2Nomade' profile is highlighted with a red box.

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

- Nous activons le mode config

The screenshot shows the Stormshield Network Security configuration page for VPN / VPN IPSEC. The 'POLITIQUE DE CHIFFREMENT - TUNNELS' tab is active, showing a table of VPN policies. The policy 'IPsec 01 (01)' is selected. The table has columns for 'Etat', 'Réseau local', 'Correspondant', 'Réseau distant', 'Profil de chiffrement', 'Mode Config', 'Keepalive', and 'Commentaire'. The 'Mode Config' dropdown for the 'IKE_Phase2' profile is highlighted with a red box.

Etat	Réseau local	Correspondant	Réseau distant	Profil de chiffrement	Mode Config	Keepalive	Commentaire
off	Network_dmz1	nomade_entreprisea	Net-IPSECVPN	IKE_Phase2	on		Originally created on 202...

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

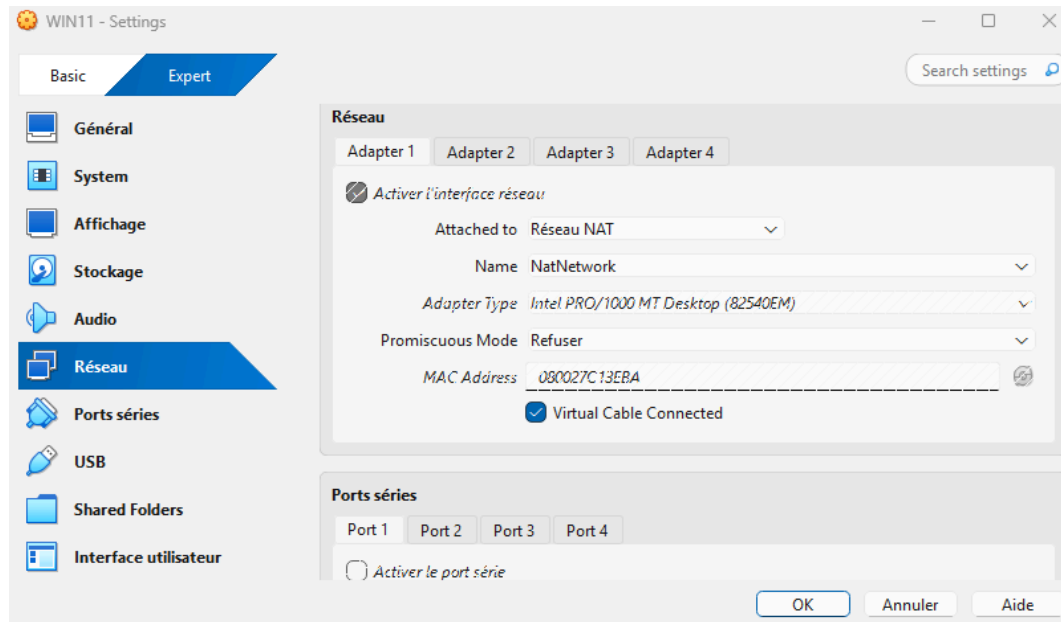
Id	Statut	Action	Source	Destination	Protocoles	Services	IPS	Créé le
31	on	passer	Any	Firewall_Out	isakmp, isakmp_natt		IPS	2025-10-15 22:09:45, p...
32	on	passer	Any	Firewall_Out	vpn-esp		IPS	2025-10-15 22:10:26, p...
33	on	passer	jsmith@b.net-IPsecVPN Auth. par :VPN IPsec via Tunnel VPN IPsec	Network_dmz1	http, ftp, dns		IPS	2025-10-15 22:11:07, p...
34	on	passer	jsmith@b.net-IPsecVPN Auth. par :VPN IPsec via Tunnel VPN IPsec	Network_dmz1	Any	icmp (requête Echv)	IPS	2025-10-15 22:20:59, p...

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

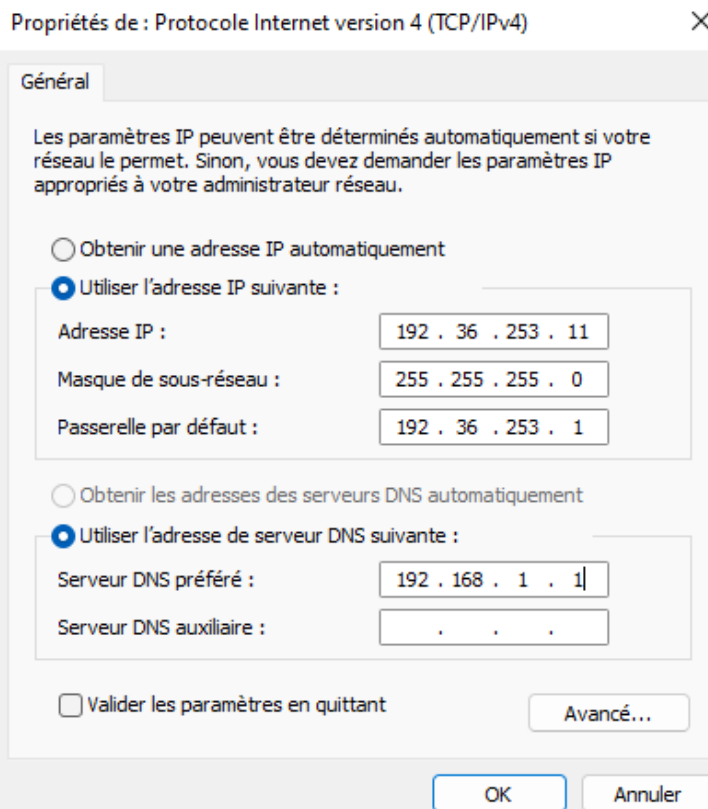
Etat	Utilisateur - groupe d'utilisateurs	VPN SSL Portail	IPSEC	VPN SSL	Parrainage	Description
1 Activé	jsmith@b.net	Interdire	Autoriser	Autoriser	Interdire	

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 ECRITURE 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: ...

Accès distant par SSH

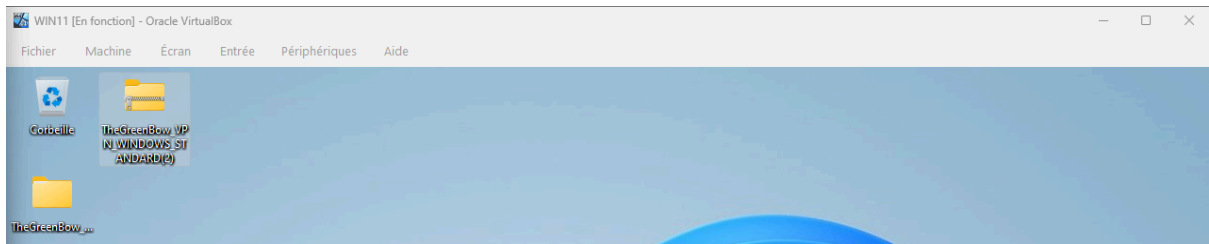
Activer l'accès par SSH

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

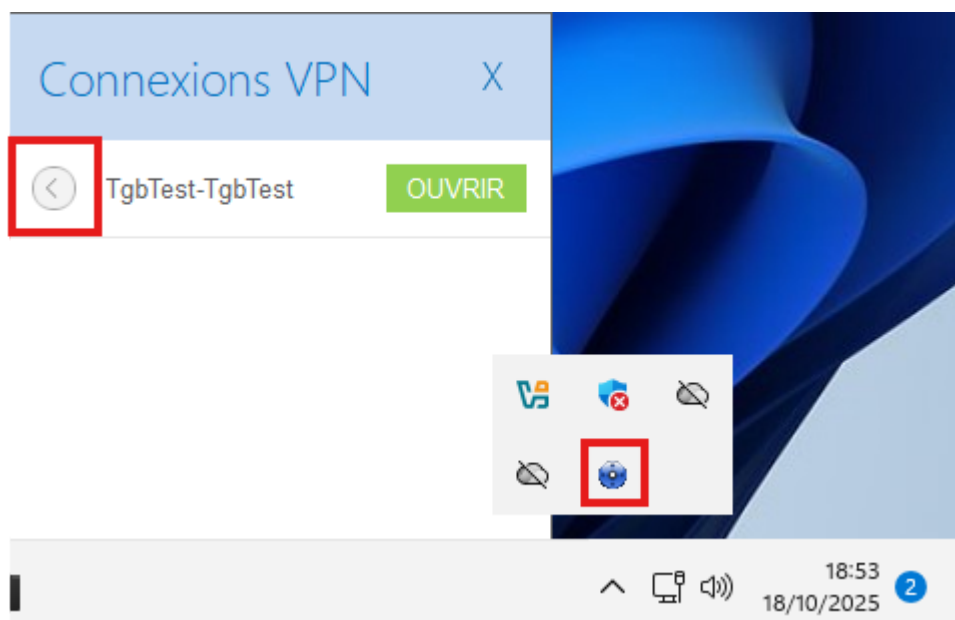
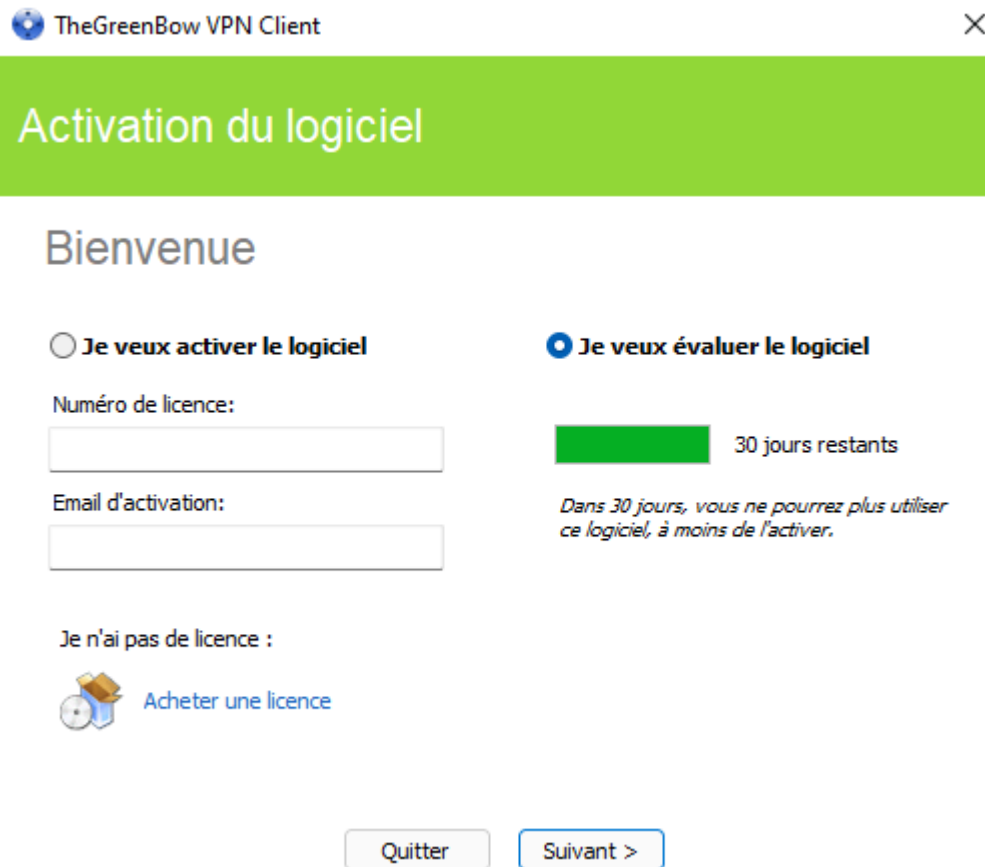
The screenshot shows a virtual machine management interface. On the left, a list of VMs is displayed under the folder 'OVA_virtual_lab'. The VMs are:

- Debian-Training-Webmail_A (En fonction)
- Graphical_client_A (Init) (En fonction)
- SNS_EVA1_V4.3_A (fin tp 6) (En fonction)
- Debian-Training-Webmail_B (Instantané 1) (En fonction)
- Graphical_client_B (Init) (En fonction)
- SNS_EVA1_V4.3_B (fin tp 6) (En fonction)
- WIN11-Workgroup-AdInv (Éteinte)
- WIN11 (Instantané 1) (En fonction)

On the right, a 'Snapshots' (Instantanés) table is shown for the selected VM. The table has two columns: 'Nom' and 'Pris'.

Nom	Pris
Instantané 1	18/10/2025 18:48 (3 minute(s) ago)
État actuel (modifié)	

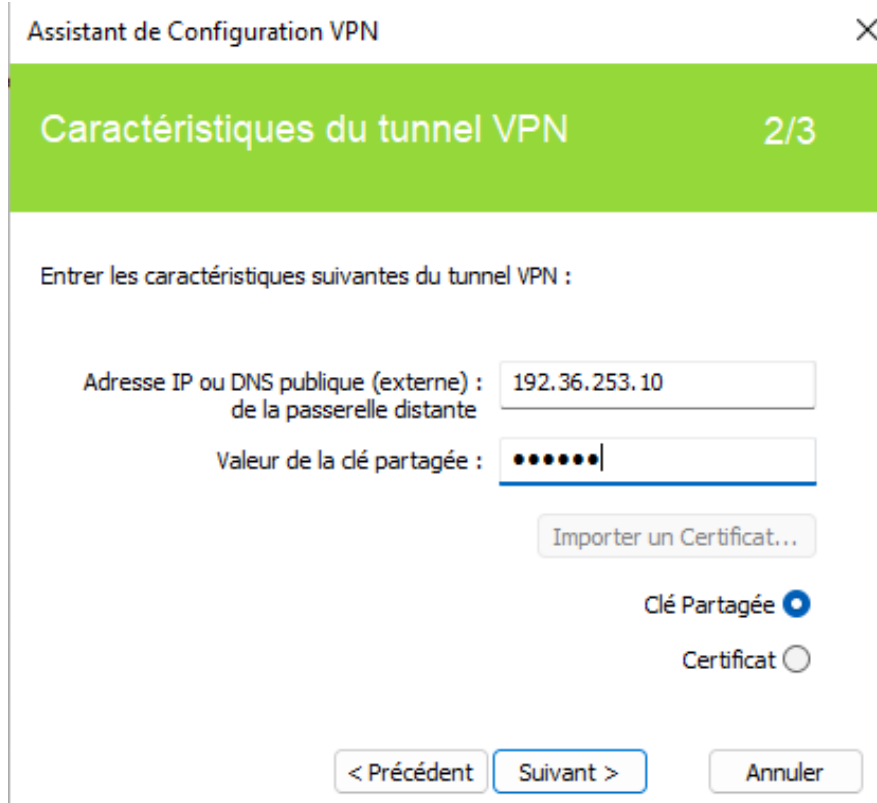
5. Installation du client TheGreenBow



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

The screenshot shows the 'TheGreenBow VPN Client' window. The title bar includes 'TheGreenBow VPN Client' and standard window controls. Below the title bar is a navigation menu with 'Configuration' and 'Outils ?'. The main interface has a green header with 'THEGREENBOW' on the left and 'Connexions Sécurisées' on the right. Below this is a sub-header 'Ikev2Gateway: IKE Auth' and 'VPN CLIENT'. On the left side, there is a tree view showing the VPN configuration structure: 'Configuration VPN' -> 'IKE V1' -> 'Paramètres généraux'; 'IKE V2' -> 'Ikev2Gateway' (selected) -> 'Ikev2Tunnel'; 'TgbTest'; 'TgbTest'; 'SSL'. The main area on the right is a configuration form for 'Ikev2Gateway: IKE Auth' with tabs for 'Authentification', 'Protocole', 'Passerelle', and 'Certificat'. The 'Authentification' tab is active. It contains sections for 'Adresse routeur distant', 'Authentification', and 'Cryptographie'. Under 'Adresse routeur distant', 'Interface' is set to 'Automatique' and 'Adresse routeur distant' is '192.36.253.10'. Under 'Authentification', 'Clé Partagée' is selected with a confirmation field. Under 'Cryptographie', 'Chiffrement', 'Authentification', and 'Groupe de clé' are all set to 'Auto'.

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

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 AES CBC 256

Authentification SHA2 256

Groupe de clé DH14 (MODP 2048)

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

Identité

Local ID Email jsmith@a.net

Remote ID

Fonctions avancées

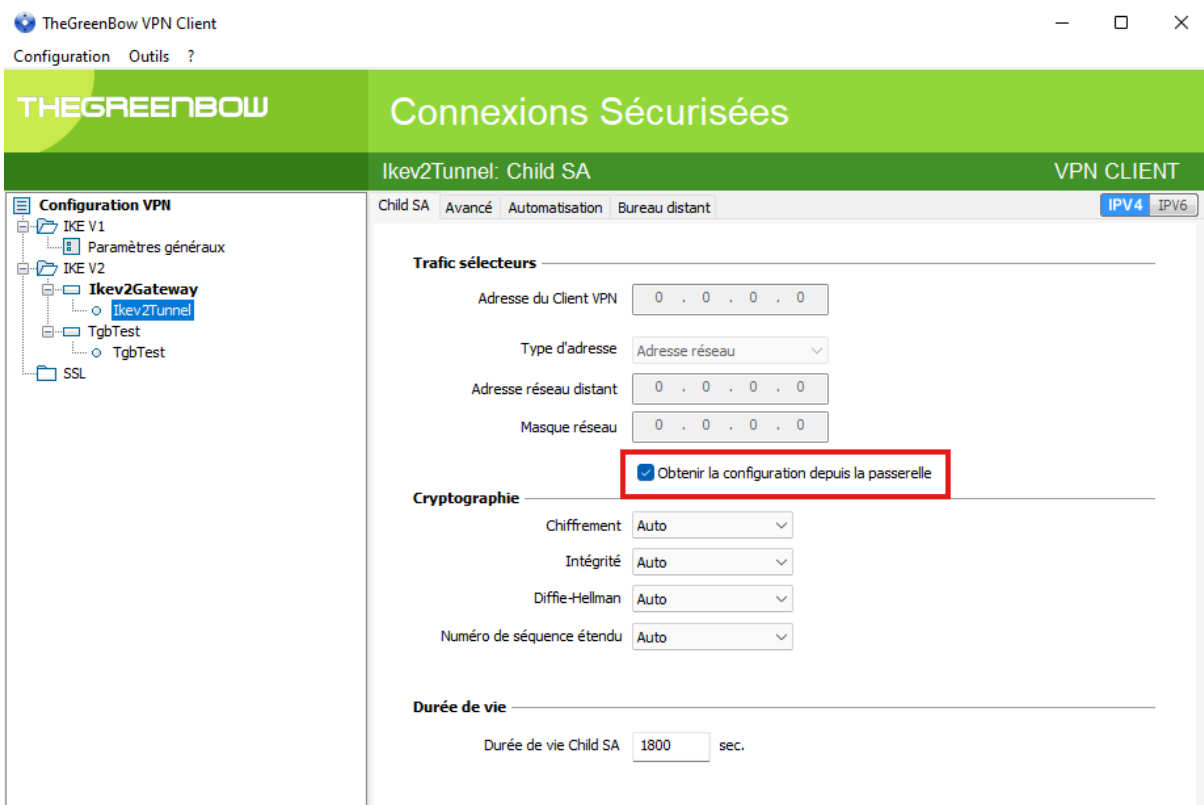
Fragmentation Taille des fragments 1280

Port IKE 500 Activer l'offset NATT

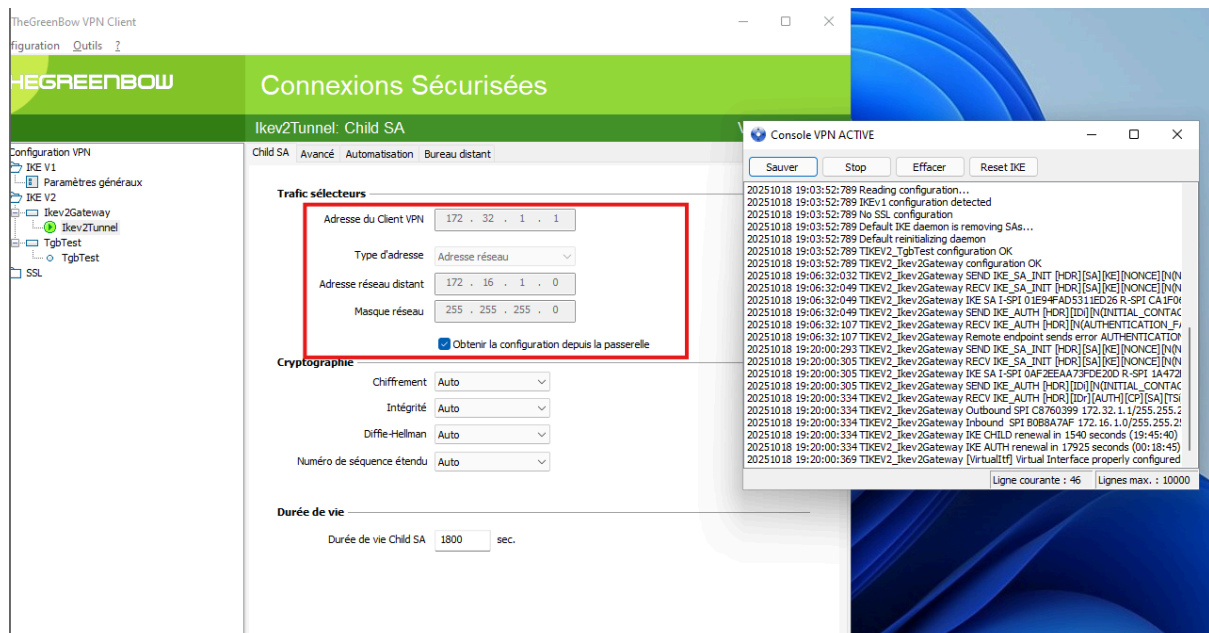
Port NAT 4500

Initiation Childless

- 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'obtention 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::95ca:36e4:1c39: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 v4.3.11 MONITORING CONFIGURATION EVA1 VMSNSX09K0639A9 admin ECRITURE 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 règle	199f8508d16_1
Type de règle	mobile
Dates	
Enregistré à	18/10/2025 21:19:56
Date et heure	18/10/2025 21:19:56
Décalage GMT	+0200
Destination	
Nom de destination	WIN11
Destination	192.36.253.11

STORMSHIELD Network Security v4.3.11 MONITORING CONFIGURATION EVA1 VMSNSX09K0639A9 admin ECRITURE 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)							
	OK	Firewall_VTL_vers_A	Firewall_out	192.36.253.10	Fw_B	192.36.253.20	IP_VTL_B
Type : Tunnels mobiles (1)							
	OK	Network_dmz1		%any		%any	
Type : Politiques d'exception (bypass) (1)							
		Bypass	rfc5735_loopback	localhost	localhost		any

TheGreenBow VPN Client

Configuration Outils ?

THEGREENBOW Connexions Sécurisées VPN CLIENT

Ikev2Tunnel: 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

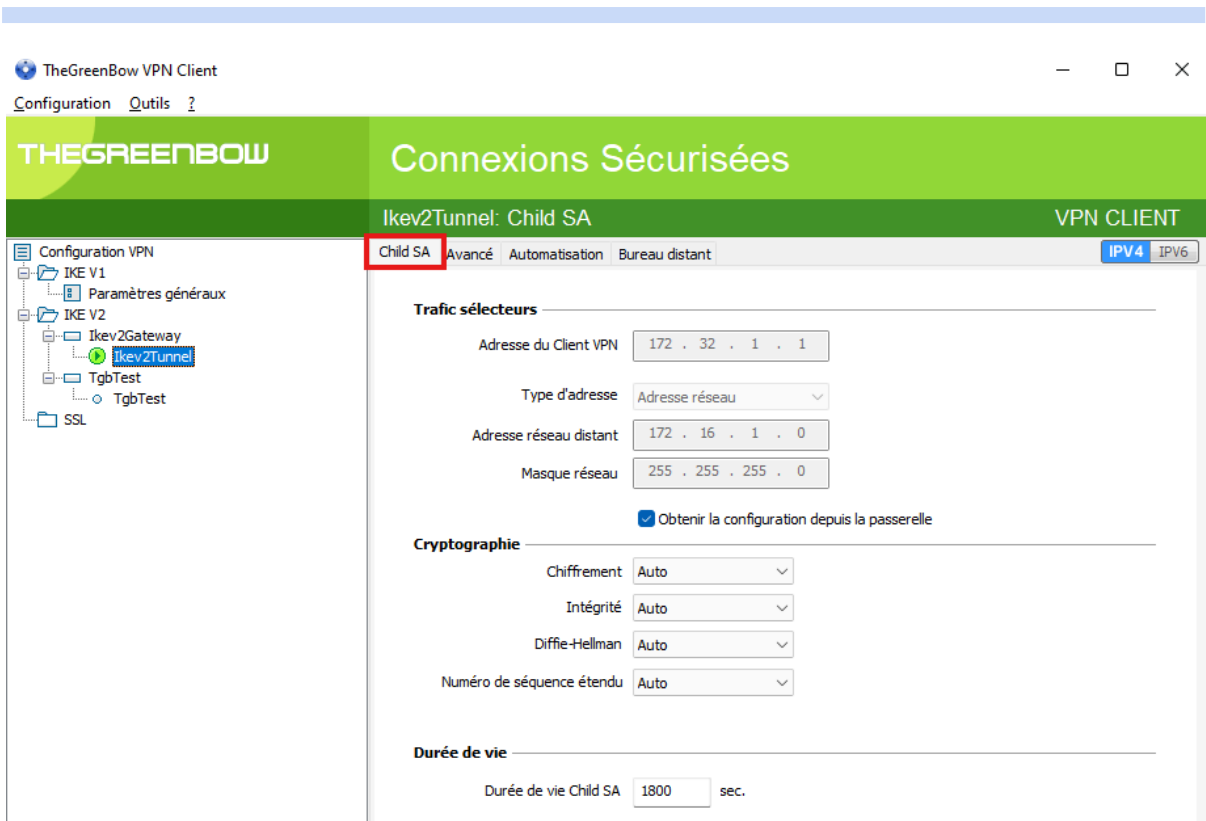
Intégrité Auto

Diffie-Hellman Auto

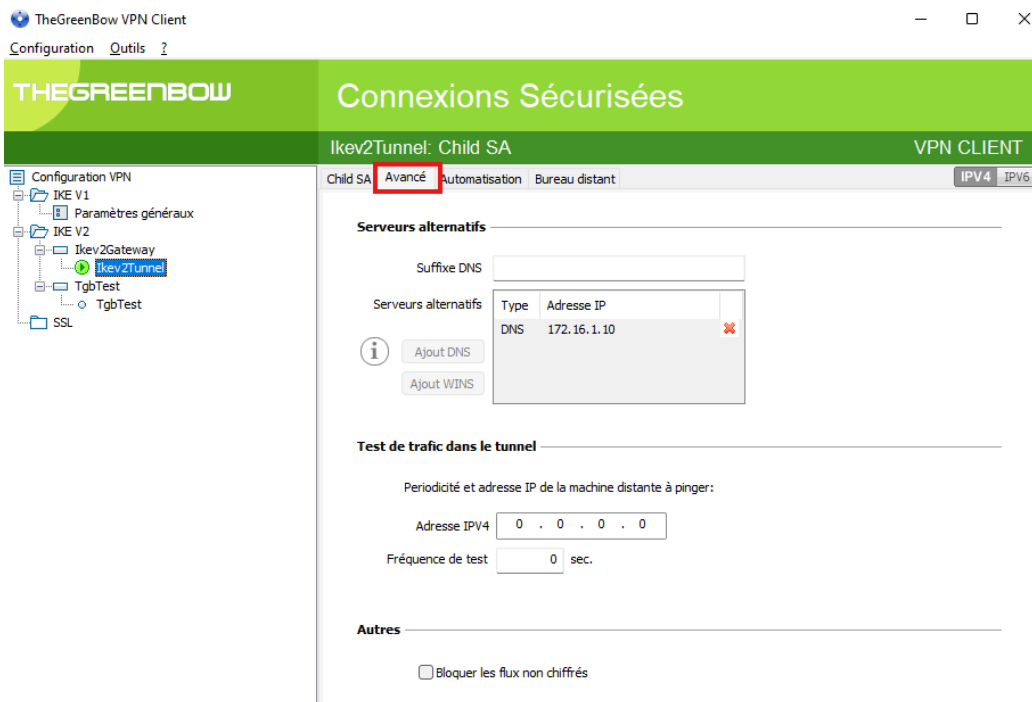
Numéro de séquence étendu Auto

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.

```

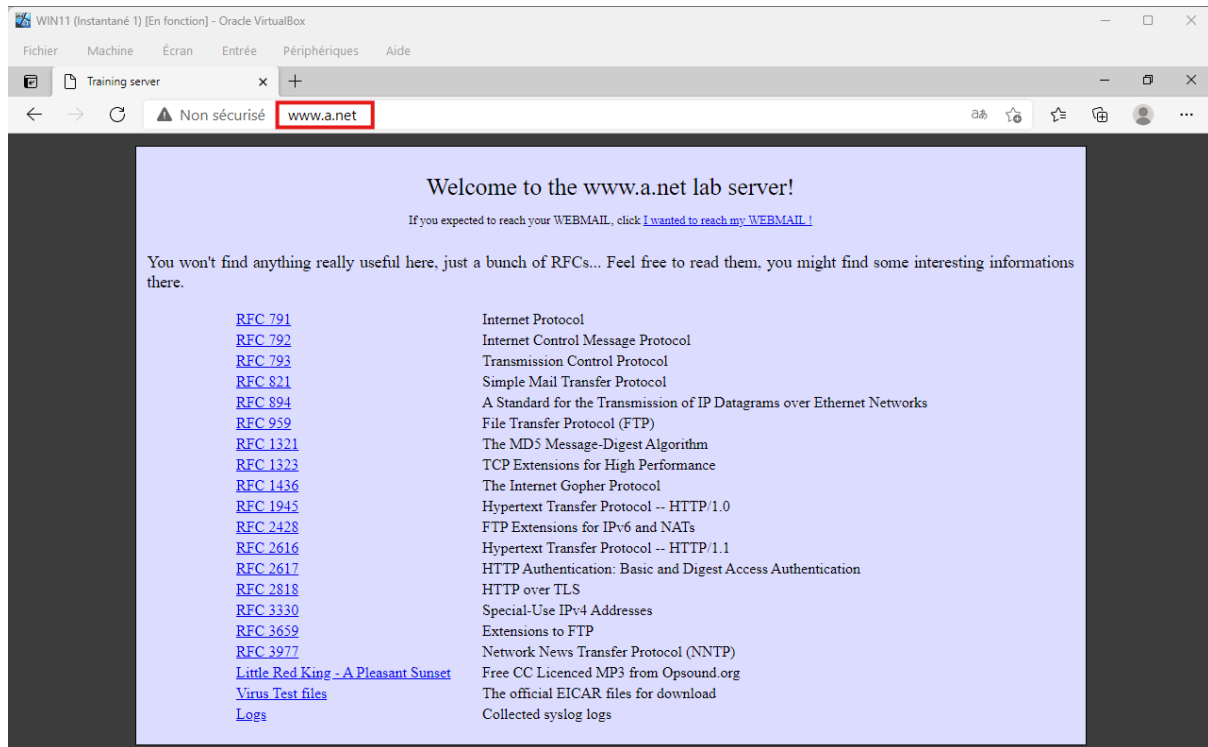
Administrateur: Invite de commandes
Microsoft Windows [version 10.0.22000.739]
(c) Microsoft Corporation. Tous droits réservés.

C:\Windows\system32>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
22...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
=====

```

- Nous avons 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.

```
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>
```