

Lab 10 – Nomade VPN IPsec avec PSK

➤ Je crée les profils de chiffrement de phase 1 et 2 :

VPN / VPN IPSEC

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

PROFIL IKE : IKEPHASE1NOMADE

Général

Commentaire:

Diffie-Hellman:

Durée de vie maximum (en secondes):

PROPOSITIONS

+ Ajouter **X Supprimer** **↑ Monter** **↓ Descendre**

	Chiffrement		Authentification	
	Algorithme	Force	Algorithme	Force
1	aes	256	sha2_256	256

VPN / VPN IPSEC

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

PROFIL IPSEC : IPSECPHASE2NOMADE

Général

Commentaire:

Perfect Forward Secrecy (PFS):

Durée de vie maximum (en secondes):

PROPOSITIONS D'AUTHENTIFICATION

+ Ajouter **X Supprimer**

	Algorithme	Force
1	hmac_sha256	256

PROPOSITIONS DE CHIFFREMENT

+ Ajouter **X Supprimer**

	Algorithme	Force
1	aes	256

VÉRIFICATION DE LA POLITIQUE

➤ Puis je créer un nouveau correspondant mobile :

VPN / VPN IPSEC

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

Entrez un filtre...

Passerelles distantes (1)
Site_Fw_B

- + Ajouter
- + Dupliquer
- Renommer
- Supprimer
- Vérifier l'utilisation

SITE_FW_B

Général

Commentaire:

Passerelle distante: Fw_B

Any

StrongEncryption

Version IKE: IKEv2

Nouvelle passerelle distante

Nouveau correspondant mobile

➤ Je choisis son nom :

CRÉER UN CORRESPONDANT MOBILE

SÉLECTIONNER LA PASSERELLE - ASSISTANT DE CRÉATION DE CORRESPONDANT



Nom:

Version IKE:

✘ ANNULER << PRÉCÉDENT >> SUIVANT

➤ Je choisis une clé pré-partagée 123AZEqsdl :

IDENTIFICATION DU CORRESPONDANT - ASSISTANT DE CRÉATION DE CORRESPONDANT

Type d'authentification:

- Certificat
 Certificat et Xauth (iPhone)
 Clé pré-partagée (PSK)

[✖ ANNULER](#)[⏪ PRÉCÉDENT](#)[⏩ SUIVANT](#)

PARAMÈTRES D'IDENTIFICATION

TUNNELS MOBILES : CLÉS PRÉ-PARTAGÉES (PSK)

Q 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:

- Je recherche john smith et je l'ajoute :

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				

- Et je valide :

CRÉER UN CORRESPONDANT MOBILE

RÉSUMÉ - ASSISTANT DE CRÉATION DE CORRESPONDANT

Correspondant mobile

Nom:

Identification du correspondant : clé pré-partagée

Les clés pré-partagées sont listées dans l'onglet Identification du module VPN IPsec

➤ Je sélectionne le profil IKE créer précédemment :

VPN / VPN IPSEC

POLITIQUE DE CHIFFREMENT - TUNNELS CORRESPONDANTS IDENTIFICATION PROFILS DE CHIFFREMENT

Entrer un filtre...

Passerelles distantes (1)
Site_Fw_B

Correspondants mobiles (1)
nomade_entreprise

NOMADE_ENTREPRISE

Général

Commentaire:

Passerelle distante: Any

Adresse locale: Any

Profil IKE: IKEphase1Nomade

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

➤ J'ajoute jsmith au tunnel nomade et entreprise a en autorité de certification (sur le screen je ne l'ai pas fait je l'ai rectifier par la suite :

VPN / VPN IPSEC

POLITIQUE DE CHIFFREMENT - TUNNELS CORRESPONDANTS IDENTIFICATION PROFILS DE CHIFFREMENT

AUTORITÉ DE CERTIFICATION ACCEPTÉES

+ Ajouter X Supprimer

CA

TUNNELS MOBILES : CLÉS PRÉ-PARTAGÉES (PSK)

Clé recherchée + Ajouter X Supprimer Éditer la sélection Exporter la liste des PSK

Identité	Clé
jsmith@a.net	0x4d6150534b21

➤ Je créer une nouvelle politique de chiffrement en anonyme, et je choisis les bons paramètres :

< POLITIQUE DE CHIFFREMENT - TUNNELS CORRESPONDANTS IDENTIFICATION PROFILS DE CHIFFREMENT >

IPsec 01 (01) Actions Deactivate policy

SITE À SITE (GATEWAY-GATEWAY) MOBILE - UTILISATEURS NOMADES

Entrer un filtre... + Ajouter X Supprimer Monter Descendre Couper Copier

Etat	Réseau ...	Corresp...	Réseau ...	Profil de...	Mode Config	Keepa...	Comme...
<div style="border: 1px solid red; padding: 5px; display: inline-block;">+ Ajouter</div> Nouvelle politique mobile simple Nouvelle politique mobile Mode Config Séparateur (regroupement de règles)							

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_entreprise

Réseaux distants:

Any

- Je créer un nouveau réseau ip qui sera distribué aux utilisateurs VPN IPsec nomades :

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:

Adresses IPv4

Adresse IP de réseau:

Exemple 192.168.0.0/16 ou 192.168.0.0/255.255.0.0

Commentaire:

- Et j'ajoute le profil de chiffrement et le réseau nomade à la politique de chiffrement créer précédemment :

POLITIQUE DE CHIFFREMENT - TUNNELS CORRESPONDANTS IDENTIFICATION PROFILS DE CHIFFREMENT

IPsec 01 (01) Actions Deactivate policy

SITE À SITE (GATEWAY-GATEWAY) MOBILE - UTILISATEURS NOMADES

Id	Statut	Réseau local	Correspondant	Réseau distant	Profil de chiffrement	Mode Config	Keepalive	Commentaire
1	off	Network_dmz1	nomade_entreprise	Net-IPSECVPN	IPSECphase2Nomade	off		Originally created on 2025-10-13 13:07:2...

- J'active aussi le mode config et je mets le srv_dns_priv comme serveur DNS utilisé :

PARAMÈTRES DU MODE CONFIG POUR LA RÈGLE SÉLECTIONNÉE (01)

Paramètres DNS

Serveur DNS utilisé:

DOMAINES UTILISÉS EN MODE CONFIG

+ Ajouter X Supprimer

Nom de domaine

ANNULER

APPLIQUER

➤ Je rajoute les règles de filtrage suivantes :

➤ POLITIQUE DE SÉCURITÉ / FILTRAGE ET NAT

Rechercher...	État	Action	Source	Destination	Port dest.	Protocole	Inspection de sécurité	Commentaire
1	off	passer	Any	Any	Any		IPS	Créée le 2025-10-02 13:24:20, par admin (192.168.1.2)
2	off	passer	Net-SSLVPN_TCP Net-SSLVPN_UDP via Tunnel VPN SSL	Internet	http https		IPS	Créée le 2025-10-09 17:43:55, par admin (192.168.1.2)
3	on	passer	Net-SSLVPN_UDP Net-SSLVPN_TCP via Tunnel VPN SSL	Network_internals	Any		IPS	Créée le 2025-10-09 14:19:02, par admin (192.168.1.2)
4	on	passer	Network_in	Fw_B	https		IPS	Créée le 2025-10-09 14:19:07, par admin (192.168.1.2)
5	on	passer	Any	Firewall_out	isakmp isakmp_natt		IPS	Créée le 2025-10-06 11:34:06, par admin (192.168.1.2)
6	on	passer	Any	Firewall_out	Any	vpn-esp	IPS	Créée le 2025-10-06 11:34:35, par admin (192.168.1.2)
7	on	passer	jsmith@Net-IPSECVPN Auth. par VPN IPsec via Tunnel VPN IPsec	Network_dmz1	http ftp		IPS	Créée le 2025-10-13 13:11:58, par admin (192.168.1.2)
8	on	passer	jsmith@Net-IPSECVPN Auth. par VPN IPsec via Tunnel VPN IPsec	Network_dmz1	Any	icmp (requête Echv)	IPS	Créée le 2025-10-13 13:11:58, par admin (192.168.1.2) - Mise à j...

➤ Je mets à jsmith les droits d'accès au VPN IPsec :

➤ UTILISATEURS / DROITS D'ACCÈS

ACCÈS PAR DÉFAUT	ACCÈS DÉTAILLÉ	SERVEUR PPTP				
Rechercher...	+ Ajouter	x Supprimer				
État	Utilisateur - groupe d'utilisateurs	VPN SSL Portail	IPSEC	VPN SSL	Parrainage	Description
1	Activé	jsmith@ia.net	Interdire	Autoriser	Autoriser	Interdire

➤ Sur une machine Windows 11 je configure le réseau NAT NatNetwork :

Clone de WIN11-Workgroup-Adlnv - Settings

Basic Expert

Search settings

Réseau

Adapter 1 Adapter 2 Adapter 3 Adapter 4

Activer l'interface réseau

Attached to Réseau NAT

Name NatNetwork

Adapter Type Intel PRO/1000 MT Desktop (82540EM)

Promiscuous Mode Refuser

MAC Address 08002700CF9A

Virtual Cable Connected

➤ Puis je reconfigure les ip :

Général

Les paramètres IP peuvent être déterminés automatiquement si votre réseau le permet. Sinon, vous devez demander les paramètres IP appropriés à votre administrateur réseau.

Obtenir une adresse IP automatiquement

Utiliser l'adresse IP suivante :

Adresse IP : 192 . 36 . 253 . 11

Masque de sous-réseau : 255 . 255 . 255 . 0

Passerelle par défaut : 192 . 36 . 253 . 1

Obtenir les adresses des serveurs DNS automatiquement

Utiliser l'adresse de serveur DNS suivante :

Serveur DNS préféré : . . .

Serveur DNS auxiliaire : . . .

Valider les paramètres en quittant

Avancé...

➤ Je créer l'objet WIN11 pour l'implémenter dans l'accès du firewall :

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: WIN11

Adresse IPv4: 192.36.253.11

Adresse MAC: 01:23:45:67:89:ab (Facultatif)

Résolution

Aucune (IP statique)

Automatique

Commentaire:

✕ FERMER

+ CRÉER ET DUPLIQUER

+ CRÉER

- Je l'implémente sur l'accès du firewall :

🔧 SYSTÈME / CONFIGURATION

CONFIGURATION GÉNÉRALE **ADMINISTRATION DU FIREWALL** PARAMÈTRES RÉSEAUX

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

- Après avoir installé le VPN TheGreenBow choisis la durée gratuite de 30 jours :

 TheGreenBow VPN Client ✕

Activation du logiciel


Bienvenue

Je veux activer le logiciel


Numéro de licence:

Email d'activation:

Je n'ai pas de licence :

 [Acheter une licence](#)

Je veux évaluer le logiciel

 30 jours restants

Dans 30 jours, vous ne pourrez plus utiliser ce logiciel, à moins de l'activer.

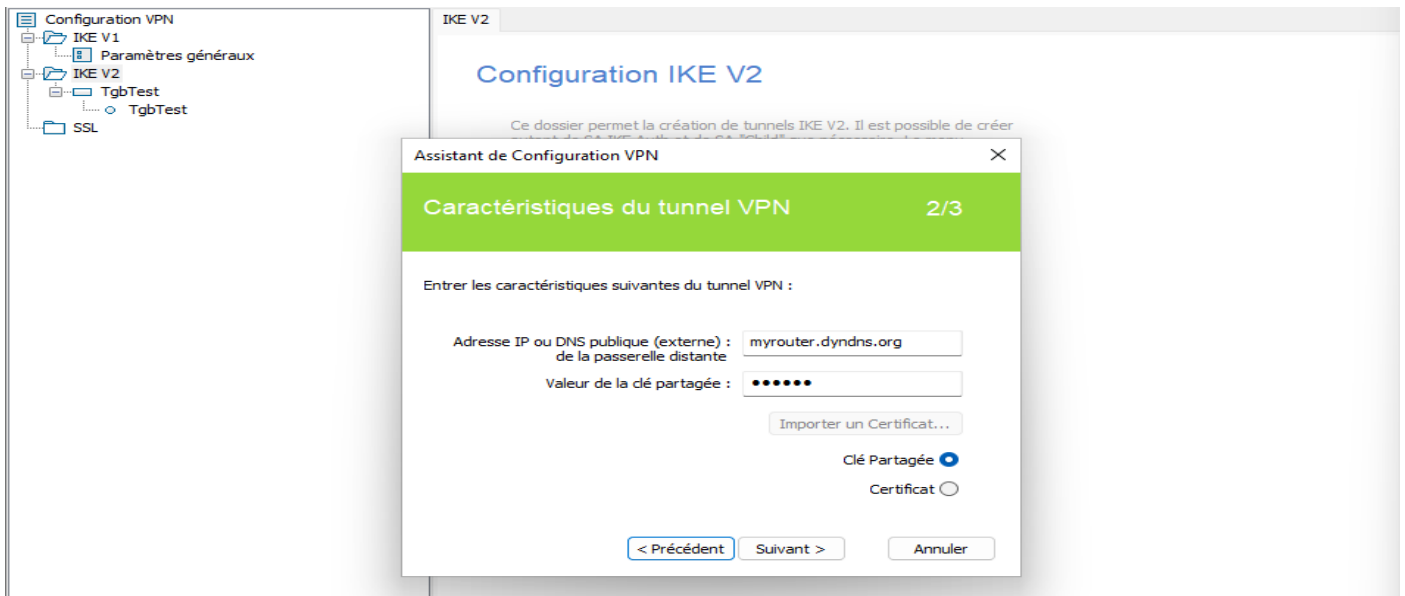
- Je vérifie qu'il à bien été installé :



- Je rentre dans le VPN et je choisis l'asistant création de tunnel :



- Je configure l'ip de la passerelle distante et je rajoute la valeur de la clé partagée :



- Je fais terminer :

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 : myrouter.dyndns.org
Clé partagée : *****

Vous pouvez modifier ces paramètres à tout moment directement dans l'interface principale.

< Précédent

Terminer

Annuler

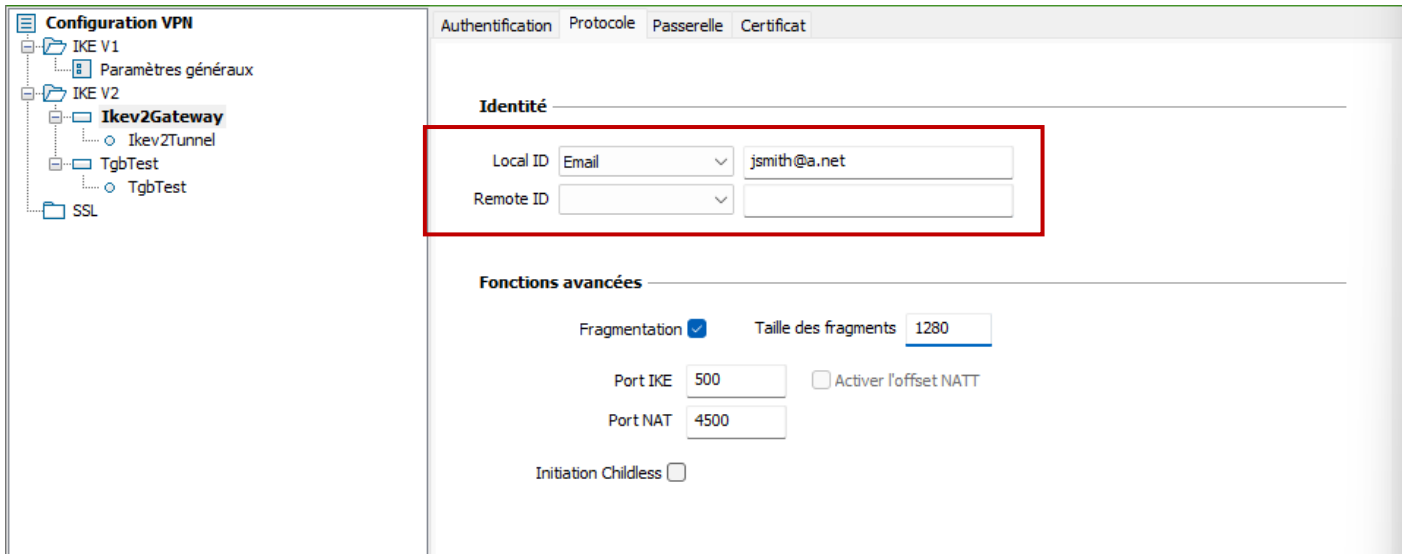
- Après avoir sauvegarder (Ctrl + S), je regarde les paramètres d'authentification et je configure la cryptographie (je ne l'ai pas screen quand je l'ai fait) :

The screenshot shows the 'Configuration VPN' interface with a tree view on the left and a main configuration area on the right. The tree view includes 'IKE V1', 'Paramètres généraux', 'IKE V2', 'Ikev2Gateway', 'Ikev2Tunnel', 'TgbTest', and 'SSL'. The main configuration area is titled 'Authentification' and has tabs for 'Authentification', 'Protocole', 'Passerelle', and 'Certificat'. The 'Authentification' tab is active. It shows the following settings:

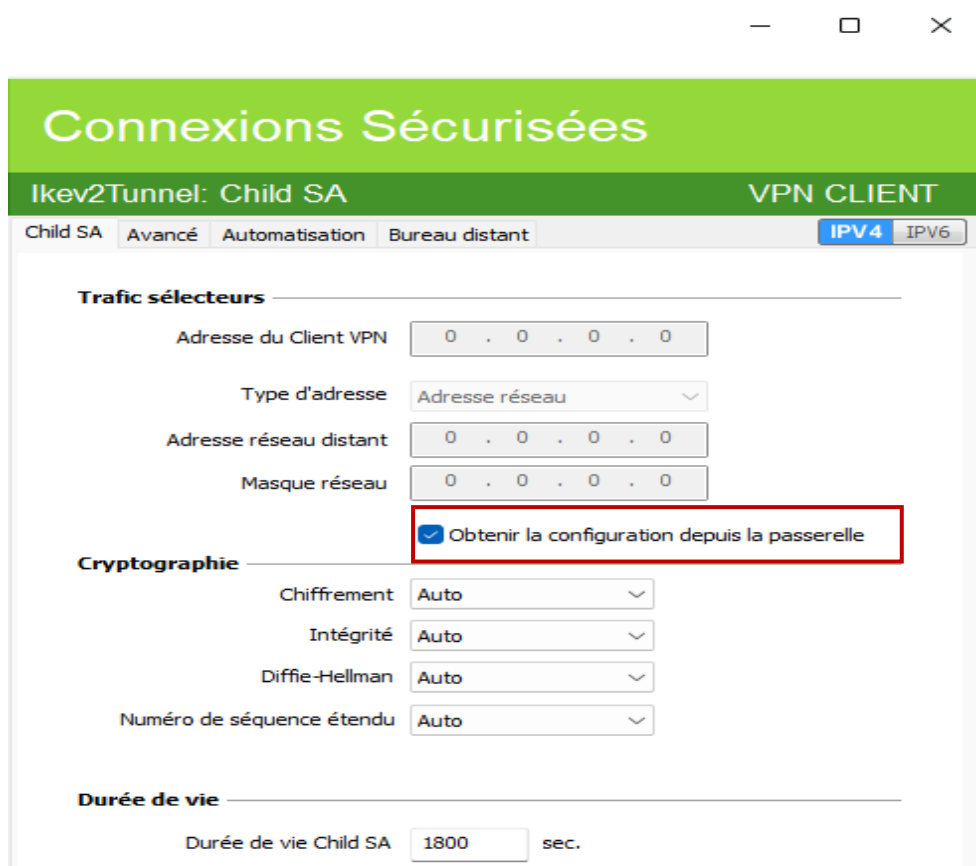
- Adresse routeur distant**: Interface: Automatique, Adresse routeur distant: 192.36.253.10
- Authentification**: Clé Partagée (with fields for Clé Partagée and Confirmer, both containing *****), Certificat
- EAP: EAP popup, Login: [field], Mot de passe: [field], Multiple AUTH support
- Cryptographie**: Chiffrement: Auto, Authentification: Auto, Groupe de clé: Auto

A red arrow points from the text above to the 'Cryptographie' section in the screenshot.

➤ Je vais dans l'onglet protocole et je saisis l'email de jsmith :



➤ Je coche la case obtenir la configuration depuis la passerelle :



➤ Je lance la connexion sécurisée :

The screenshot shows a Windows desktop with a blue background. In the top-left corner, there is a 'Corbelle' (Recycle Bin) icon. The main window is the 'GreenBow Connexions Sécurisées' application. The left sidebar shows a tree view with 'Ikev2Gateway' selected. The main area displays the configuration for 'Ikev2Gateway: IKE Auth'. The configuration includes:

- Adresse routeur distant:** Interface: Automatique, Adresse routeur distant: 192.36.253.10
- Authentification:** Clé Partagée (with masked fields for key and confirmation), Certificat, EAP (with EAP popup, Login field, and Mot de passe field), Multiple AUTH support
- Cryptographie:** Chiffrement: AES CBC 256, Authentification: SHA2 256, Groupe de clé: DH14 (MODP 2048)

Overlaid on the right is a 'Console VPN ACTIVE' window showing a log of system events. The log includes messages such as 'TIKEV2_Ikev2Gateway configuration OK', 'TIKEV2_Ikev2Gateway IKE SA I-SPI 8787C5C306B8547C R-SPI EC045:', and 'TIKEV2_Ikev2Gateway [VirtualItf] Virtual Interface properly configured'. At the bottom of the console window, it shows 'Ligne courante : 25' and 'Lignes max. : 10000'.

➤ Puis je vais dans le cmd pour faire un ipconfig /all :

```

Suffixe DNS propre à la connexion. . . :
Description. . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Adresse physique . . . . . : 08-00-27-B2-05-24
DHCP activé. . . . . : Non
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . . : fe80::33bc:6f0d:f538:7ed6%7(préfér )
Adresse IPv4. . . . . : 192.36.253.11(pr f r )
Masque de sous-r seau. . . . . : 255.255.255.0
Passerelle par d faut. . . . . : 192.36.253.1
IAID DHCPv6 . . . . . : 101187623
DUID de client DHCPv6. . . . . : 00-01-00-01-30-7E-82-F5-08-00-27-B2-05-24
NetBIOS sur Tcpi. . . . . : Activ 

Carte Ethernet TGB Ikev2Gateway-Ikev2Tunnel :

Suffixe DNS propre à la connexion. . . :
Description. . . . . : TheGreenBow Virtual Miniport Adapter
Adresse physique . . . . . : 02-50-F2-DA-28-00
DHCP activ . . . . . : Non
Configuration automatique activ e. . . : Oui
Adresse IPv6 de liaison locale. . . . . : fe80::96e:1a73:20d6:73de%12(pr f r )
Adresse IPv4. . . . . : 172.32.1.1(pr f r )
Masque de sous-r seau. . . . . : 255.255.255.255
Passerelle par d faut. . . . . :
Serveurs DNS. . . . . : 172.16.1.10
NetBIOS sur Tcpi. . . . . : Activ 

```

➤ Je retourne sur StormShield et je vais regarder les logs :

LOG / VPN

Derni re heure Actualiser Rechercher... Recherche avanc e Actions

RECHERCHE DU - 13/10/2025 15:58:15 - AU - 13/10/2025 16:58:15

Enregistr� �	Message	Utilisateur	Nom de la source	R�seau local	Nom de destination	R�seau distant
13/10/2025 16:55:00	User authenticated in ASQ	jsmith	Firewall_out	172.16.1.0/24	WIN11	172.32.1.1/32
13/10/2025 16:55:00	IPSEC SA established	jsmith	Firewall_out	172.16.1.0/24	WIN11	172.32.1.1/32
13/10/2025 16:55:00	IKE SA established	jsmith	Firewall_out			
13/10/2025 16:55:00	No IDr configured, fall back on IP address	jsmith	Firewall_out		WIN11	
13/10/2025 16:55:00	User allowed	jsmith	Firewall_out		WIN11	
13/10/2025 16:55:00	INITIAL-CONTACT received		Firewall_out		WIN11	
13/10/2025 16:55:00	Received unknown vendor ID: 0d.cb.b1:f0.bf.ff:80.b2:4b:e3:74:e8:36:5d:ad:93		Firewall_out		WIN11	
13/10/2025 16:53:03	Charon configuration reloaded					
13/10/2025 16:53:03	Reloading charon configuration					
13/10/2025 16:46:37	Negotiation failed		Firewall_out		WIN11	
13/10/2025 16:46:37	Peer PSK mismatched		Firewall_out		WIN11	
13/10/2025 16:46:37	INITIAL-CONTACT received		Firewall_out		WIN11	
13/10/2025 16:46:37	Received unknown vendor ID: 0d.cb.b1:f0.bf.ff:80.b2:4b:e3:74:e8:36:5d:ad:93		Firewall_out		WIN11	
13/10/2025 16:45:35	Charon daemon started					
13/10/2025 16:45:35	Charon configuration reloaded					
13/10/2025 16:45:35	Reloading charon configuration					

D TAILS DE LA LIGNE DE LOG

Configuration

Nom de la r gle 199dcd3122c_1

Type de r gle mobile

Dates

Enregistr    13/10/2025 16:55:00

Date et heure 13/10/2025 16:55:00

D calage GMT +0200

Destination

Nom de destination WIN11

Destination 192.36.253.11

R seau distant 172.32.1.1/32

Identifiant distant jsmith@a.net

Divers

Journaux vpn

Phase 2

Priorit  Notice

➤ Puis je regarde les tunnels :

MONITOR / TUNNELS VPN IPSEC

Actualiser Configurer le service VPN IPsec

POLITIQUES

Type	�tat	Extr�mit� de trafic locale	Passerelle locale	Local ID	Passerelle distante	ID du correspon...	Extr�mit� de trafic distante
EJ Type : Tunnelles mobiles (1)							
	OK	Network_dmz1		%any		%any	
EJ Type : Politiques d'exception (bypass) (1)							
Association de s�curit� (SA) IKE							
Aucune association de s�curit� n'a �t� trouv�e pour cette SPD (Security Policy Database)							

- Je retourne sur le VPN (toujours avec la connexion sécurisée de lancé) pour vérifier l'adresse du client VPN :

THEGREENBOW Connexions Sécurisées VPN CLIENT

Ikev2Tunnel: Child SA

Child SA Avancé Automatisation Bureau distant **IPV4** IPV6

Traffic 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.

- Puis je vais dans « avancé », pour voir les serveurs alternatifs :

THEGREENBOW Connexions Sécurisées VPN CLIENT

Ikev2Tunnel: Child SA

Child SA Avancé Automatisation Bureau distant **IPV4** IPV6

Serveurs alternatifs

Suffixe DNS

Type	Adresse IP
DNS	172.16.1.10

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.

Autres

Bloquer les flux non chiffrés

```

Microsoft Windows [version 10.0.22000.1641]
(c) Microsoft Corporation. Tous droits réservés.

C:\Users\X>netstat -rn
=====
Liste d'Interfaces
 7...08 00 27 b2 05 24 .....Intel(R) PRO/1000 MT Desktop Adapter
12...02 50 f2 da 28 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
=====

IPv6 Table de routage
=====
Itinéraires actifs :
If Metric Network Destination Gateway
1 331 ::1/128 On-link
7 281 fe80::/64 On-link
12 291 fe80::/64 On-link
12 291 fe80::96e:1a73:20d6:73de/128 On-link
7 281 fe80::33bc:6f0d:f538:7ed6/128 On-link
1 331 ff00::/8 On-link
7 281 ff00::/8 On-link
12 291 ff00::/8 On-link
=====
Itinéraires persistants :
Aucun

```

➤ Je fais le test sur www.a.net:



- Je fais un test FTP grâce a la commande ftp <ftp.a.net>:

```
C:\Users\X>ftp ftp.a.net
Connecté à ftp.a.net.
```

- Et enfin je teste avec un ping :

```
Microsoft Windows [version 10.0.22000.1641]
(c) Microsoft Corporation. Tous droits réservés.

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

Statistiques Ping pour 172.16.1.12:
    Paquets : envoyés = 3, reçus = 3, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 1ms, Maximum = 2ms, Moyenne = 1ms
Ctrl+C
^C
C:\Users\X>
```