



STORMSHIELD

LAB 11 : IPSEC PSK

WIN10_StormShield [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

VMSNSX09K0639A9@sns.a.net x +

Non sécurisé | <https://sns.a.net/admin/admin.html#ipsec>

MONITORING CONFIGURATION EVA1 VMSNSX09K0639A9 admin ÉCRITURE / ACCÈS RESTREINT

VPN / VPN IPSEC

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

Profil de chiffrement par défaut

Profil de chiffrement IKE (phase 1) : StrongEncryption

Profil de chiffrement IPsec (phase 2) : StrongEncryption

+ Ajouter x Supprimer

Type	Nom
IKE	StrongEncryption
IKE	GoodEncryption
IKE	Mobile
IKE	IKE Phase 1 (Diffie-hellman)
IPSEC	StrongEncryption
IPSEC	GoodEncryption
IPSEC	Mobile
IPSEC	PFS
IKE	IKEphase1Nomade

Général

Commentaire :

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

Durée de vie maximum (en secondes) : 21600

PROPOSITIONS

+ Ajouter x Supprimer ↑ Monter ↓ Descendre

	Chiffrement		Authentification	
	Algorithme	Force	Algorithme	Force
1	aes	256	sha2_256	256

X Annuler Enregistrer

1ère étape : Création du profil de chiffrement IKEphase1Nomade.

WIN10_StormShield [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

VMSNSX09K0639A9@sns.a.net x +

Non sécurisé | <https://sns.a.net/admin/admin.html#ipsec>

MONITORING CONFIGURATION EVA1 VMSNSX09K0639A9 admin ÉCRITURE / ACCÈS RESTREINT ?

VPN / VPN IPSEC

POLITIQUE DE CHIFFREMENT - TUNNELS CORRESPONDANTS IDENTIFICATION PROFILS DE CHIFFREMENT

Profils de chiffrement par défaut

Profil de chiffrement IKE (phase 1) : StrongEncryption

Profil de chiffrement IPsec (phase 2) : StrongEncryption

+ Ajouter x Supprimer

Type	Nom
IKE	StrongEncryption
IKE	GoodEncryption
IKE	Mobile
IKE	IKE Phase 1 (Diffie-hellman)
IPSEC	StrongEncryption
IPSEC	GoodEncryption
IPSEC	Mobile
IPSEC	PFS
IKE	IKEphase1Nomade
IPSEC	IPSECphase2Nomade

Général

Commentaire :

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

Durée de vie (en secondes) : 3600

PROPOSITIONS D'AUTHENTIFICATION

+ Ajouter x Supprimer

	Algorithme	Force
1	hmac_sha256	256

PROPOSITIONS DE CHIFFREMENT

PROPOSITIONS DE CHIFFREMENT

+ Ajouter x Supprimer

	Algorithme	Force
1	aes	256

2ème étape : Création de la politique de chiffrement IPSECphase2Nomade.

EDITION DE LA CLÉ

Identifiant (adresse IP, FQDN ou e-mail) :

Clé prépartagée (ASCII) :

Confirmer :

☒ Saisir la clé en caractères ASCII

Pas de clé trouvée

Texte recherché + Ajouter X Supprimer

Identité ▲	Clé
jsmith@a.net	0x4d6150534b21

Page 1 sur 1 Pas de clé trouvée

3ème étape : Création d'un nouveau correspondant IKEv2 en ajoutant une nouvelle identité.

VPN / VPN IPSEC

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

Chercher dans les corres Filtre ▼

+ Ajouter X Supprimer Renommer

Nom ▲
nomade_entreprisea
Site_Fw_B

Correspondant : nomade_entreprisea

Commentaire :

Passerelle distante :

Configuration de secours :

Profil IKE :

Version IKE :

Identification

Méthode d'authentification :

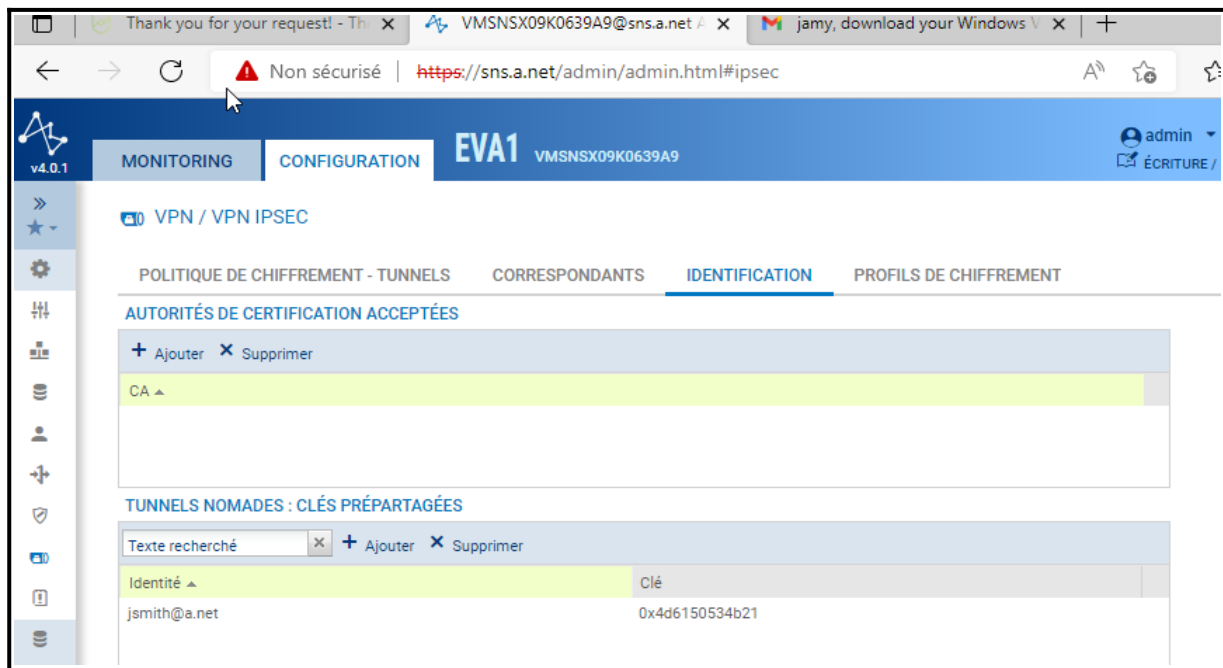
Certificat :

Local ID (Optionnel) :

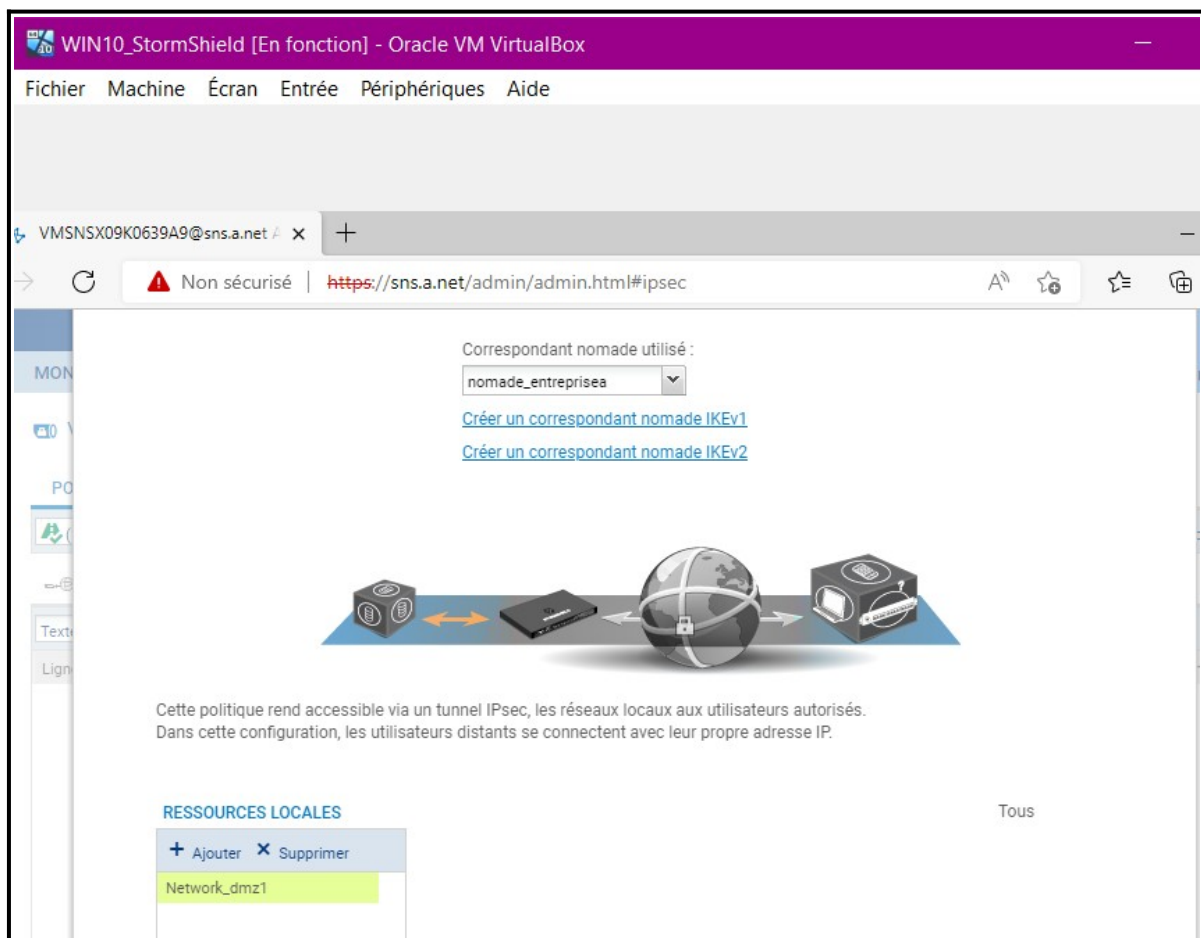
[Cliquer ici pour éditer la liste des PSK](#)

Configuration avancée

4ème étape : Sur notre nouveau correspondant nous modifions le profil IKE en indiquant IKEphase1Nomade.



5ème étape : Nous observons dans l'onglet identification l'apparition de la nouvelle clés prépartagées.



6ème étape : Ajout d'une nouvelle politique de chiffrement dans l'onglet utilisateurs nomades.

CREER UN OBJET

Machine Réseau Plage d'adresses IP Port Protocole IP Groupe Groupe de ports >>

Nom de l'objet : Net-IPSECVPN

Adresse IPv4

Adresse IP de réseau : 172.30.1.0/24

Exemple 192.168.0.0/16 ou 192.168.0.0/255.255.0.0

Commentaire :

7ème étape : Création de l'objet Net-IPSECVPN.

WIN10_StormShield [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

VMSNSX09K0639A9@sns.a.net / x

Non sécurisé | https://sns.a.net/admin/admin.html#ipsec

MONITORING CONFIGURATION EVA1 VMSNSX09K0639A9 admin ÉCRITURE / ACCÈS RESTREINT ?

VPN / VPN IPSEC

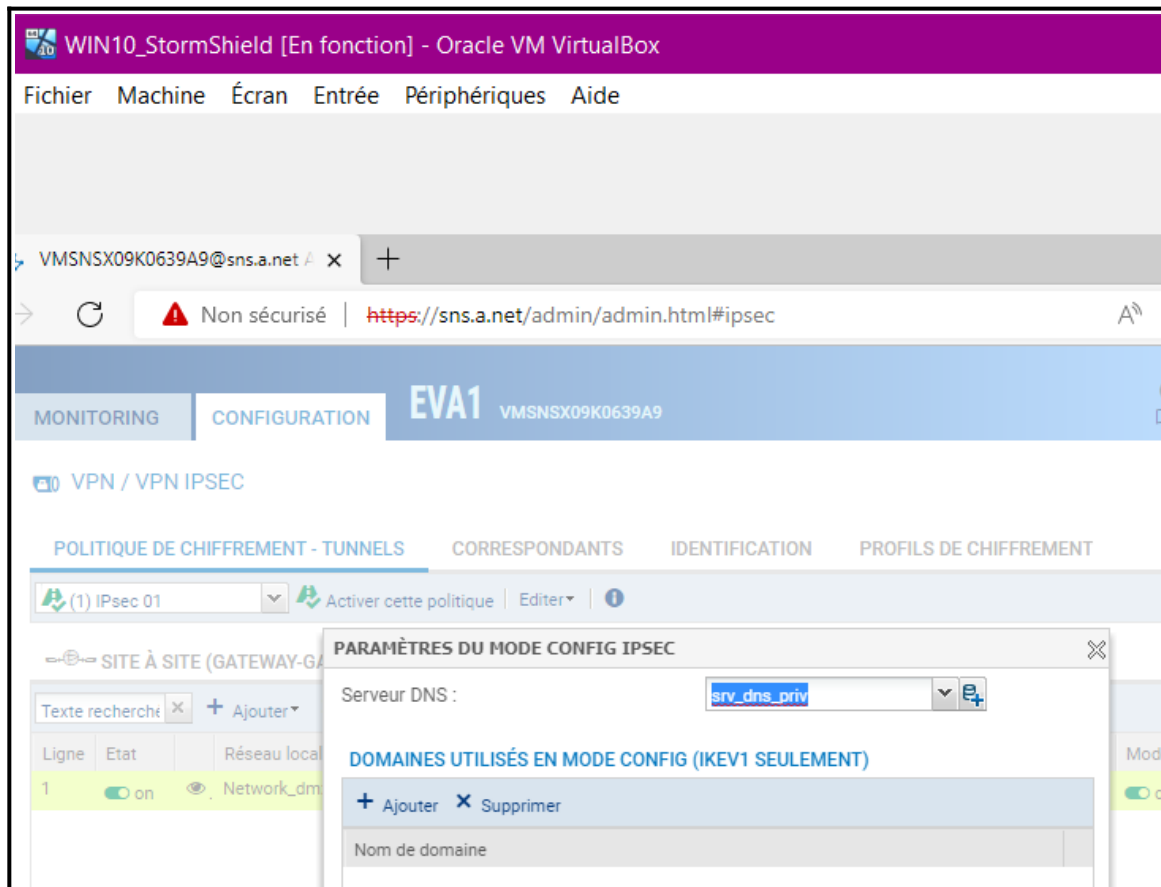
POLITIQUE DE CHIFFREMENT - TUNNELS CORRESPONDANTS IDENTIFICATION PROFILS DE CHIFFREMENT

(1) IPsec 01 Activer cette politique | Éditer | Désactiver la politique

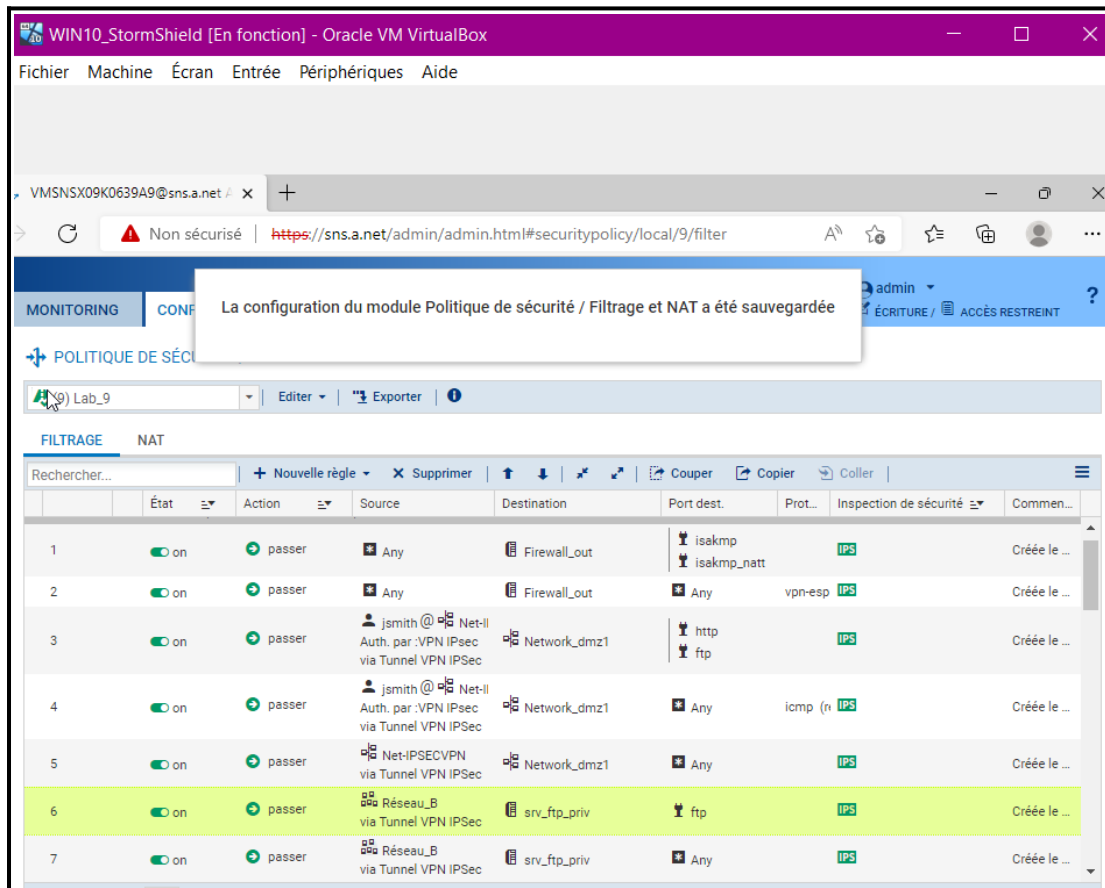
SITE À SITE (GATEWAY-GATEWAY) ANONYME - UTILISATEURS NOMADES

Ligne	Etat	Réseau local	Correspondant	Réseau nomade	Profil de chiffrement	Mode config	Commentaire
1	on	Network_dmz1	nomade_entreprisea	Net-IPSECVPN	IPSECphase2Nomz	off	

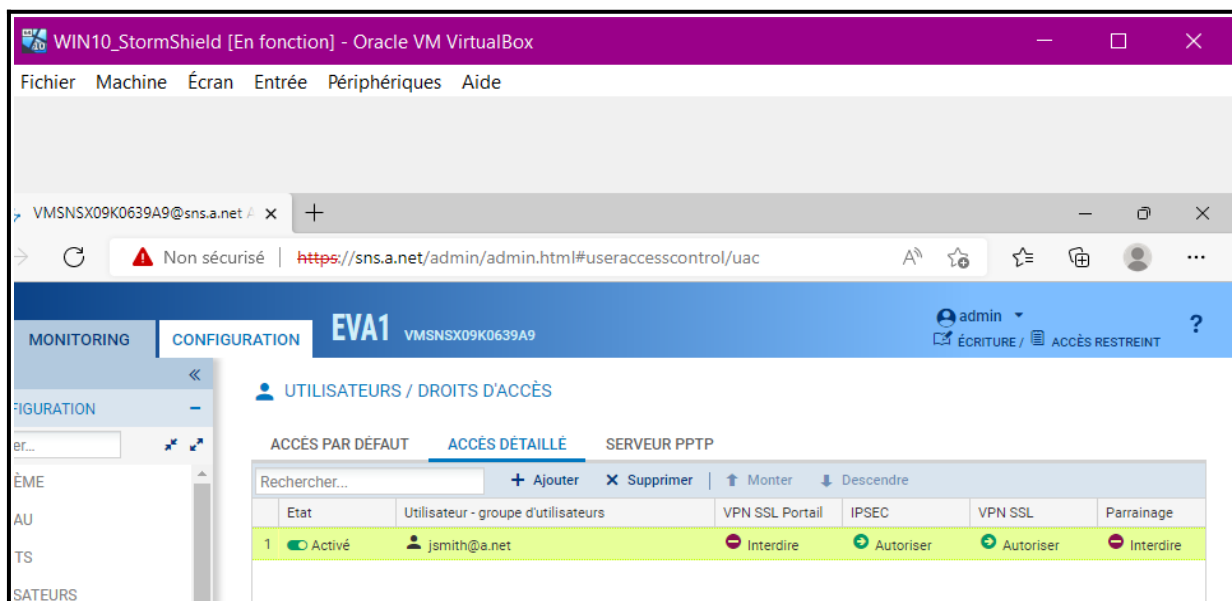
8ème étape : Ajout du profil de chiffrement avec l'objet créer précédemment dans la politique de filtrage.



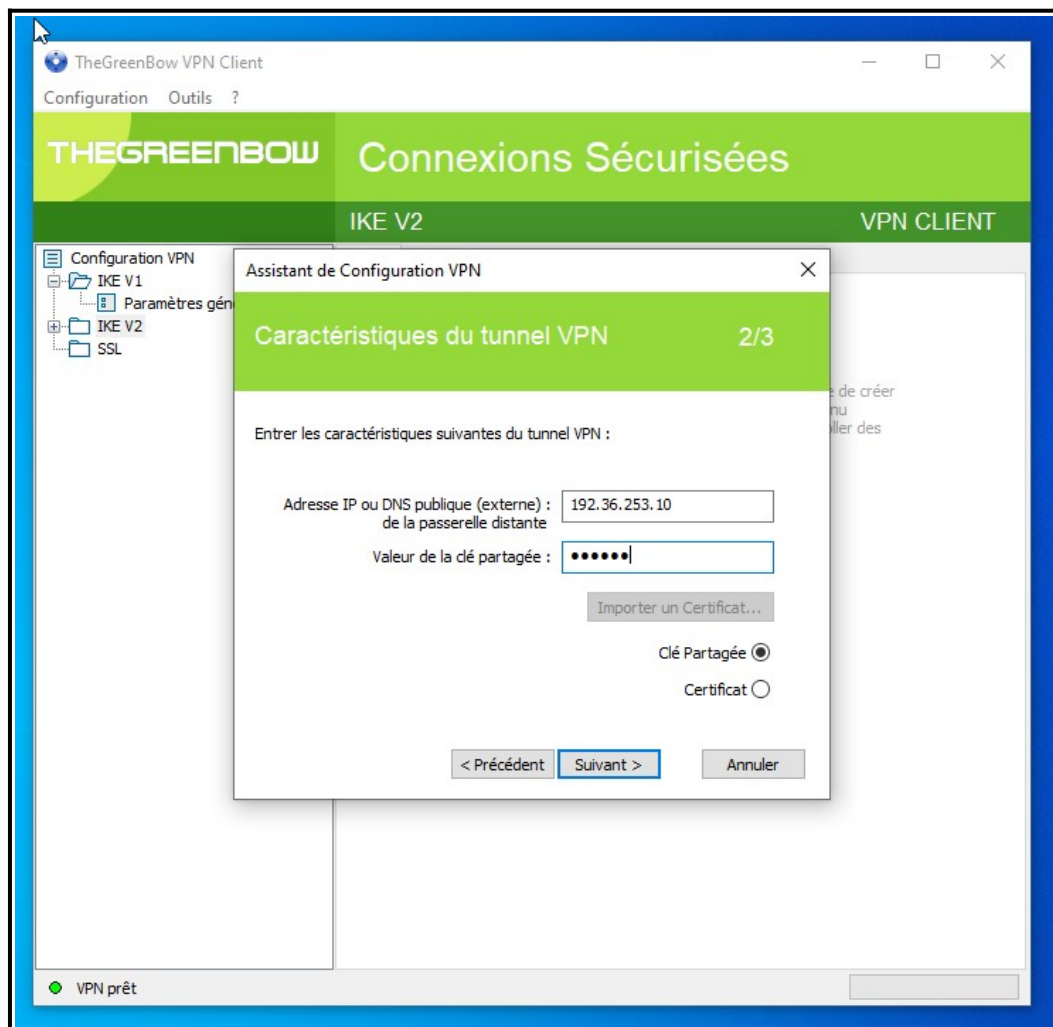
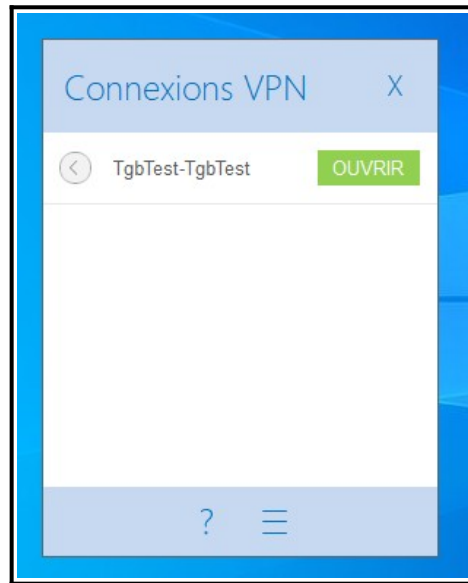
9ème étape : Dans le mode config ajout du serveur dns privé.

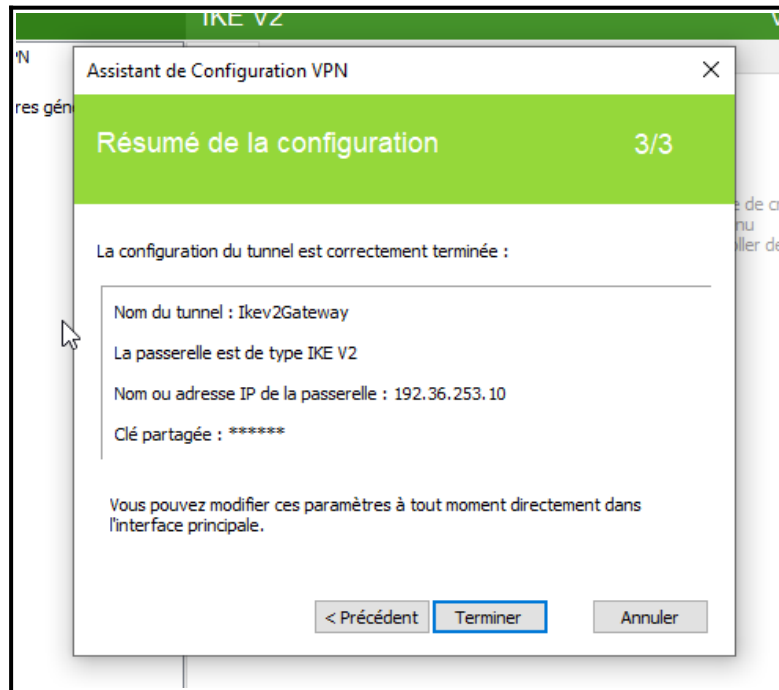


10ème étape : Ajout des règles de filtrages/nat concernant le VPN IPSEC Noamde et site à site.

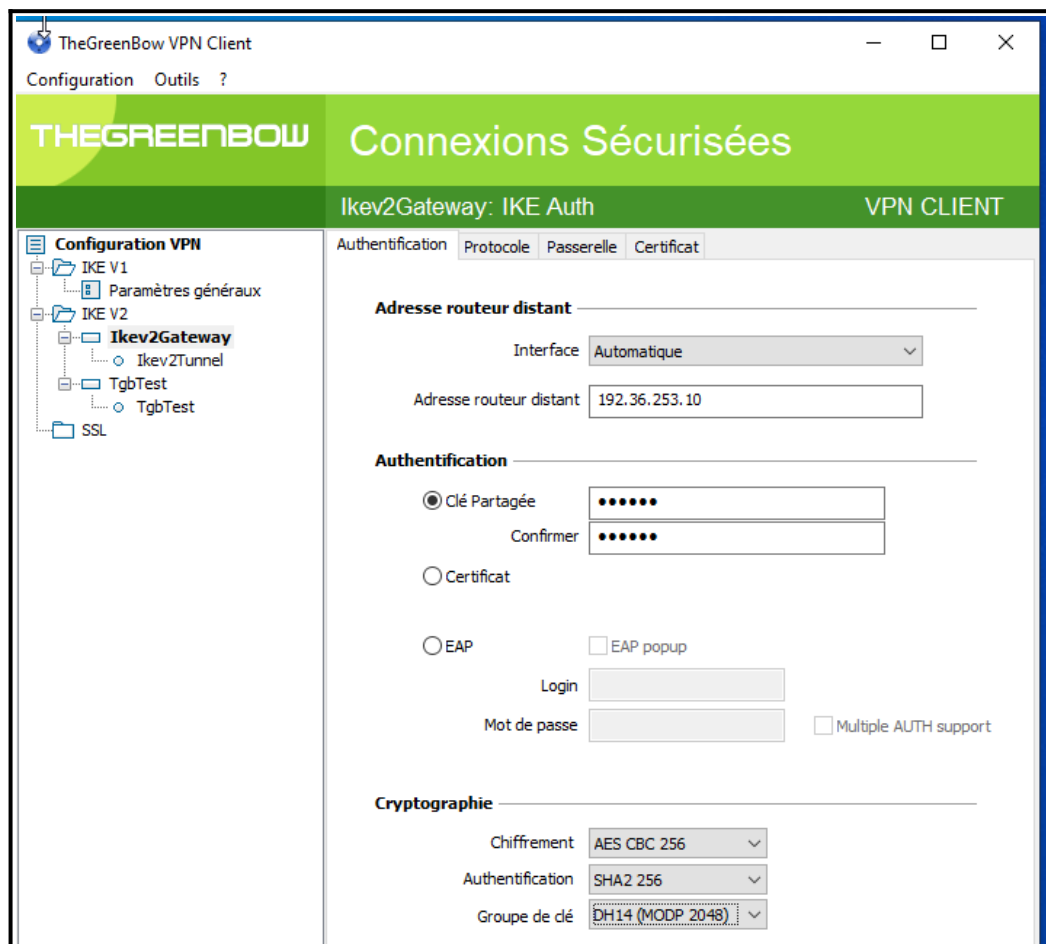


11ème étape : Modification des droits d'accès de l'utilisateur afin d'autoriser l'accès IPSEC.

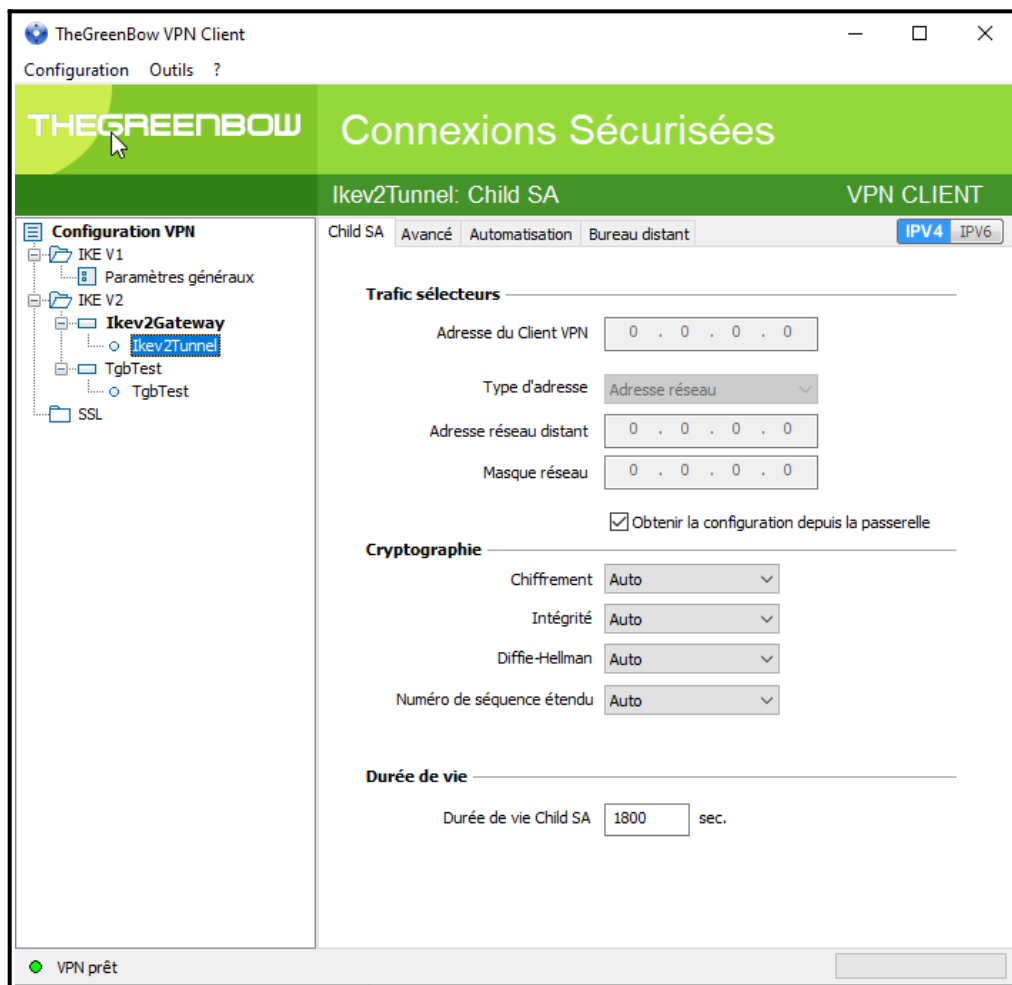
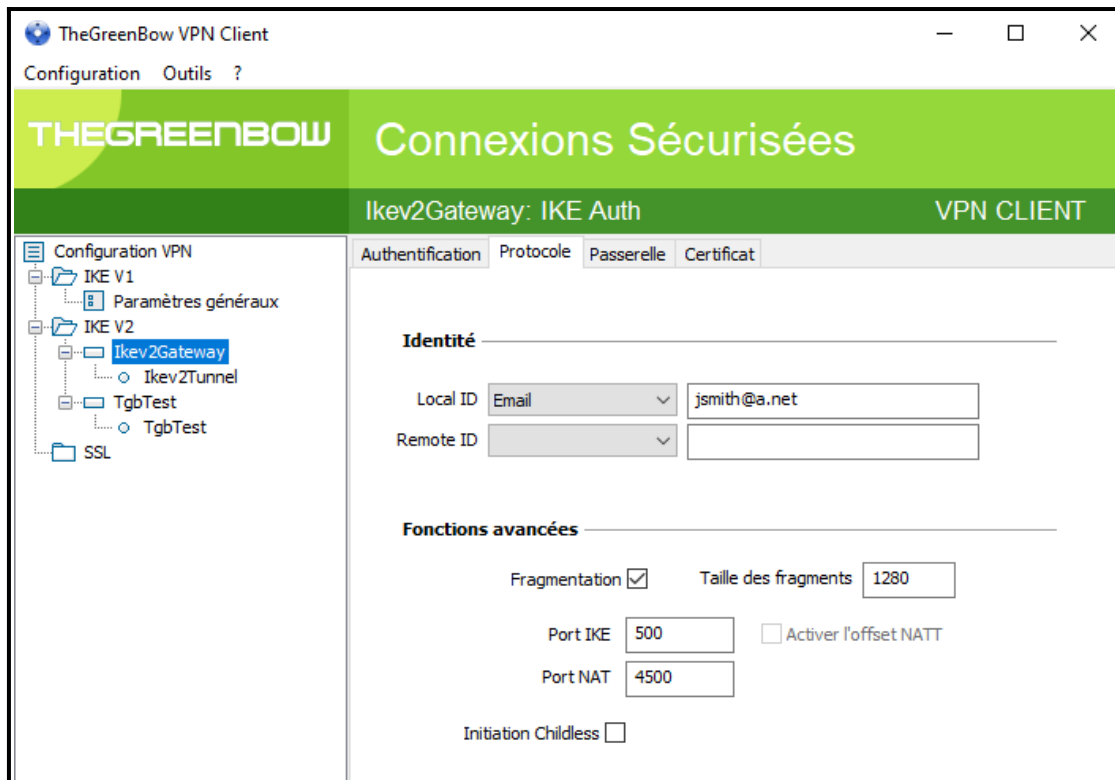




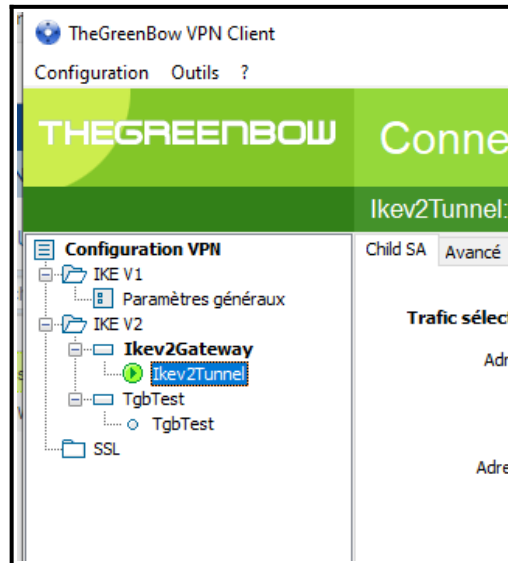
12ème étape : Installation du client TheGreenBow VPN en utilisant l'assistant de création de tunnel IKEv2, nous complétons les informations des caractéristiques du tunnel VPN la clé partagée.



13ème étape : Réglage de la cryptographie dans l'onglet authentification.



14ème étape : Modification dans l'onglet protocole.



15ème étape : Mise en route de la connexion sécurisée établie.

```

Carte Ethernet TGB Ikev2Gateway-Ikev2Tunnel :

Suffixe DNS propre à la connexion. . . :
Description. . . . . : TheGreenBow Virtual Miniport Adapter
Adresse physique . . . . . : 02-50-F2-42-E4-00
DHCP activé. . . . . : Non
Configuration automatique activée. . . : Oui
Adresse IPv6 de liaison locale. . . . : fe80::3400:d390:8e62:db27%24(préfééré)
Adresse IPv4. . . . . : 172.30.1.2(préfééré)
Masque de sous-réseau. . . . . : 255.255.255.0
Passerelle par défaut. . . . . :
Serveurs DNS. . . . . : 172.16.1.10
NetBIOS sur Tcpip. . . . . : Activé

C:\Users\ADMIN>

```

16ème étape : Un ipconfig /all nous permet de vérifier que nous obtenons bien les adresses ip souhaitées.

WIN10_StormShield [En fonction] - Oracle VM VirtualBox

Fichier Machine Écran Entrée Périphériques Aide

Thank you for your request! - Th x VMSNSX09K0639A9@sns.a.net x jamy, download your Windows V x +

Non sécurisé | https://sns.a.net/admin/admin.html#log_stream_vpn

MONITORING **CONFIGURATION** **EVA1** VMSNSX09K0639A9 admin ÉCRITURE / ACCÈS RES

LOG / VPN

Dernière heure Actualiser Rechercher... Recherche avancée

RECHERCHE DU - 04/11/2022 20:00:16 - AU - 04/11/2022 21:00:16

Enregistré à	Message	Utilisateur	Nom de la source	Réseau local	Nom de destin
04/11/2022 21:00:13	Negotiation failed		Anonymized		Fw_B
04/11/2022 21:00:13	The received traffic selectors did not match		Anonymized		Fw_B
04/11/2022 21:00:10	Negotiation failed		Anonymized		Fw_B
04/11/2022 21:00:10	IPSEC SA establishment failed: received TS_UNACCEP...		Anonymized		Fw_B
04/11/2022 20:59:46	User authenticated in ASQ	Anonymized	Anonymized	172.16.1.0/24	WIN10
04/11/2022 20:59:46	IPSEC SA established	Anonymized	Anonymized	172.16.1.0/24	WIN10
04/11/2022 20:59:46	IKE SA established	Anonymized	Anonymized		WIN10
04/11/2022 20:59:46	No IDr configured, fall back on IP address	Anonymized	Anonymized		WIN10
04/11/2022 20:59:46	User allowed	Anonymized	Anonymized		WIN10

DÉTAILS DE LA LIGNE DE LOG

Destination

Nom de destination WIN10

Destination 192.36.253.11

Réseau distant 172.30.1.2/32

Identifiant distant jsmith@a.net

Divers

Journaux vpn

Phase 2

Priorité Notice

Rôle responder

SPI entrant 0xcecc1bdc

SPI sortant 0xfbf334a4

Cookie initiateur 0x62bbdb902fae868b

Cookie réception 0x354bdd88e9369e82

Version IKE 2

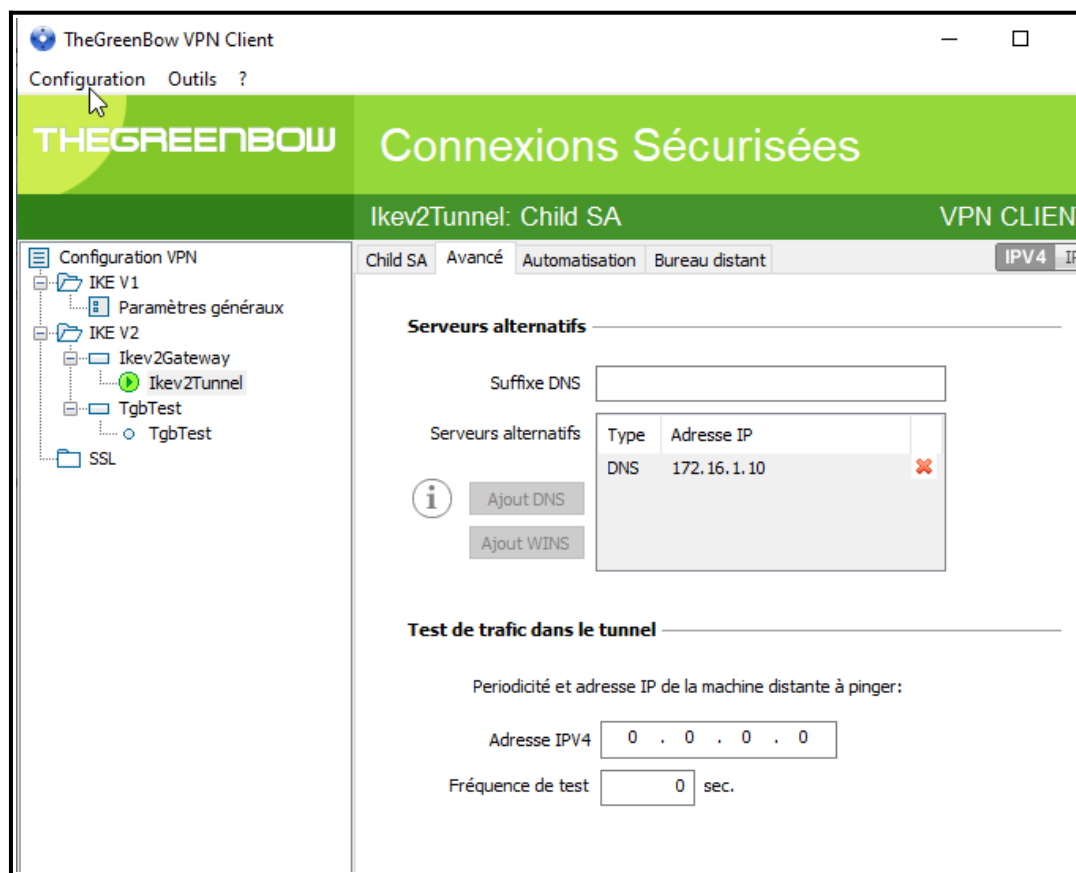
Message

Message User authenticated in ASQ

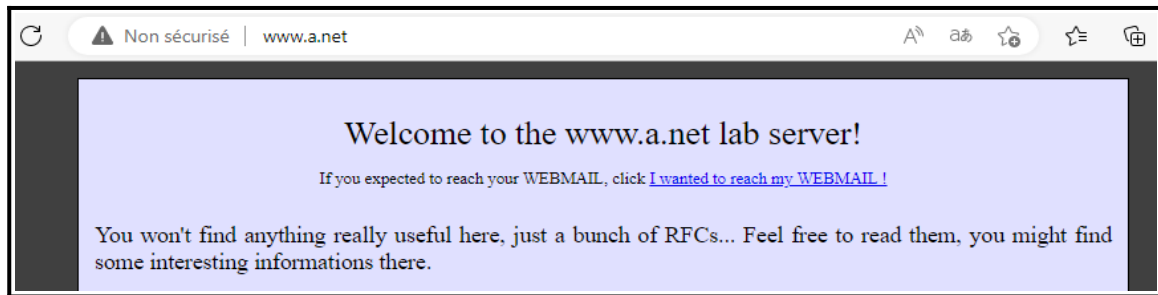
Source

Utilisateur Anonymized

17ème étape : Nous observons dans les logs VPN les activités que nous avons effectuées.



19ème étape : On constate que les changements suite au tunnel établie.



```
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
```

20ème étape : Nous effectuons différents tests tels qu'un ping ou encore un accès au serveur web de a depuis la WIN10.