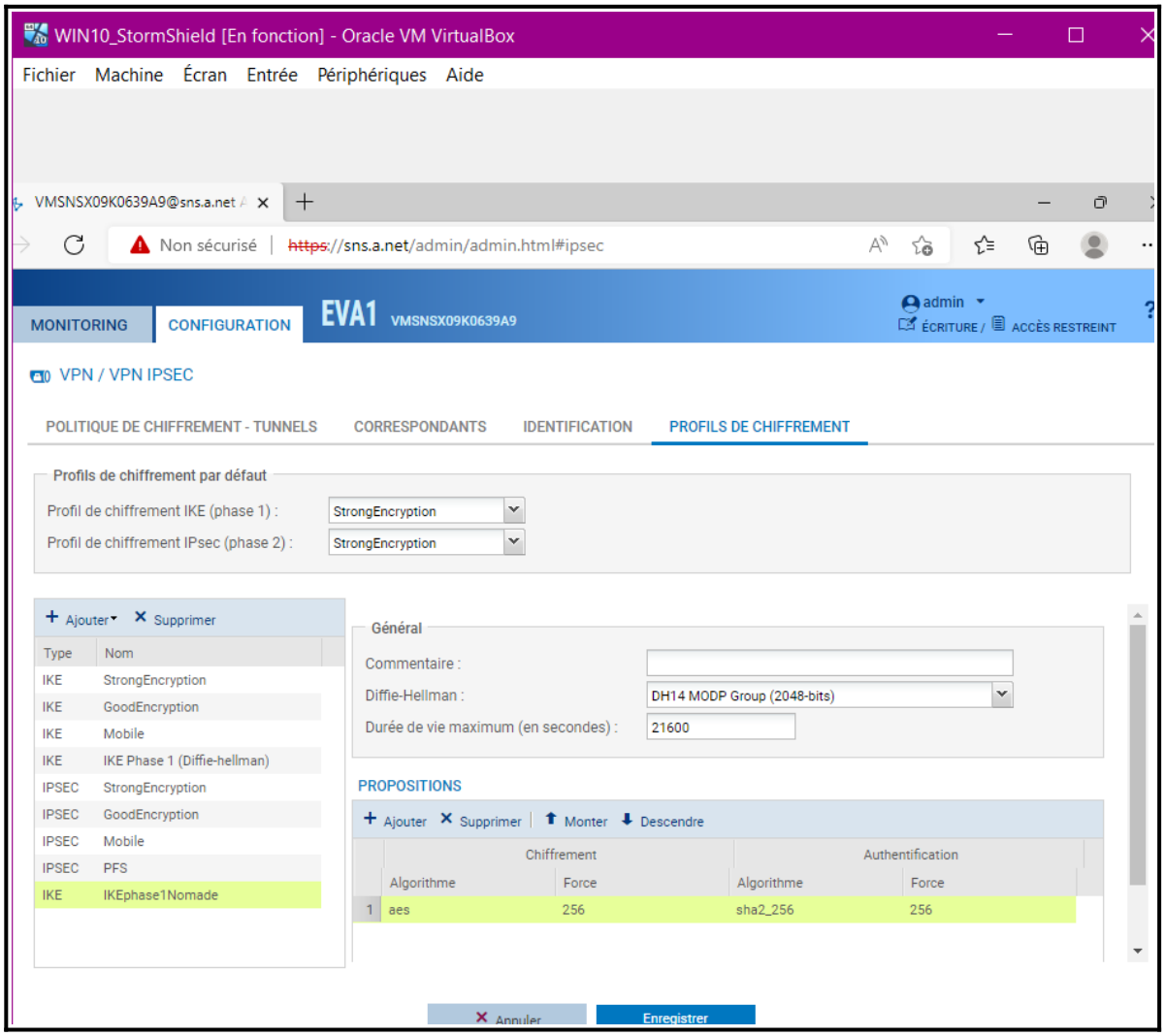
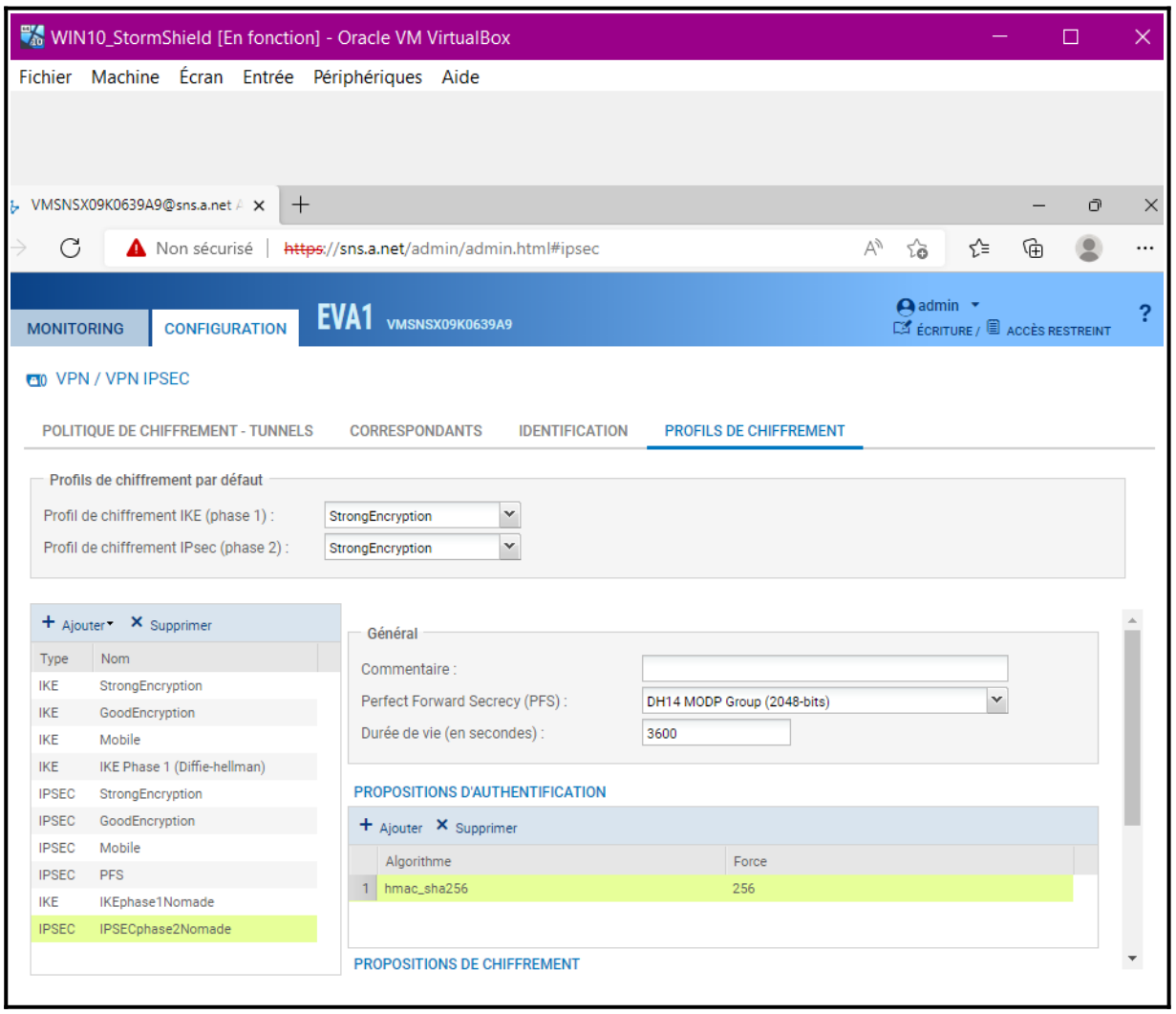
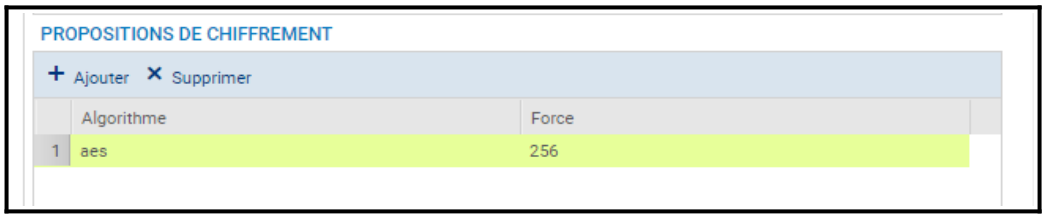
LAB 11 :
IPSEC PSK

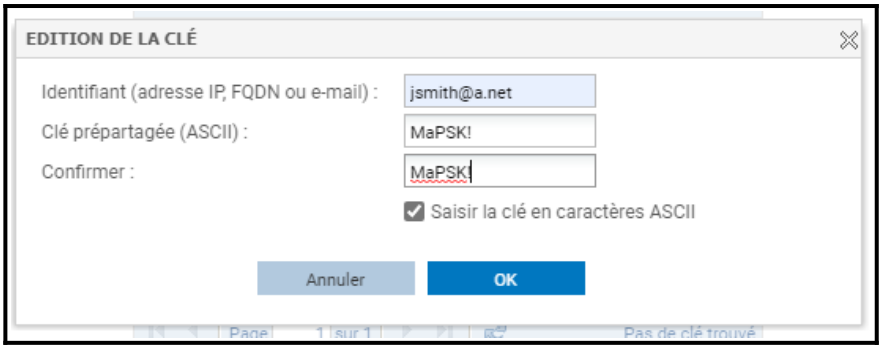


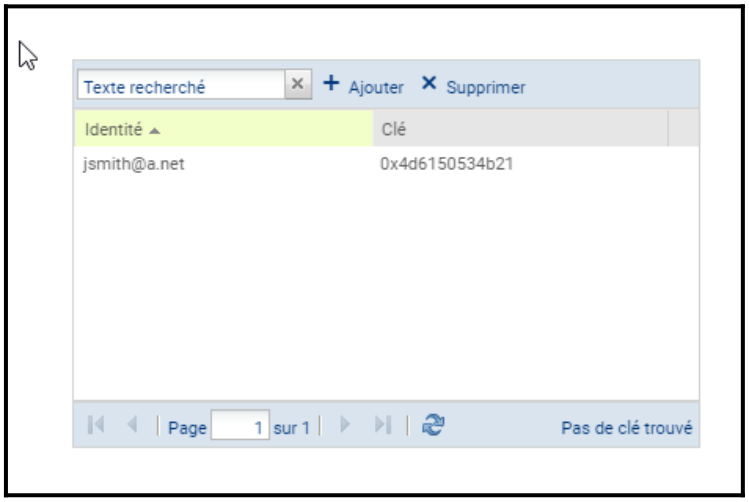
1ère étape : Création du profil de chiffrement IKEphase1Nomade.



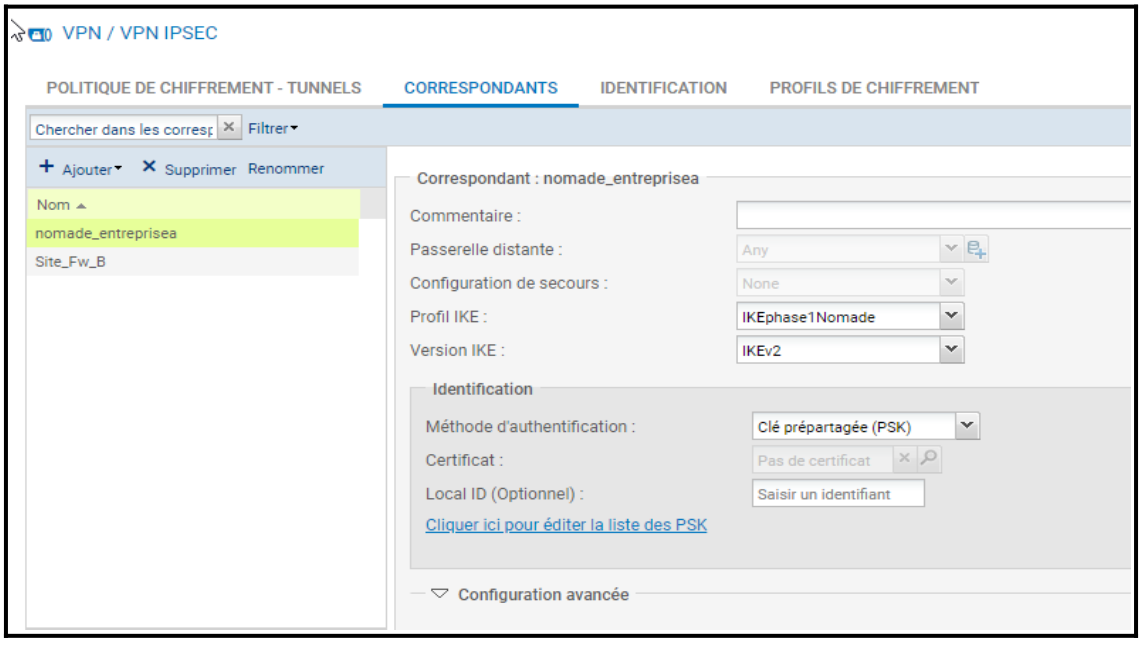


2ème étape : Création de la politique de chiffrement IPSECphase2Nomade.

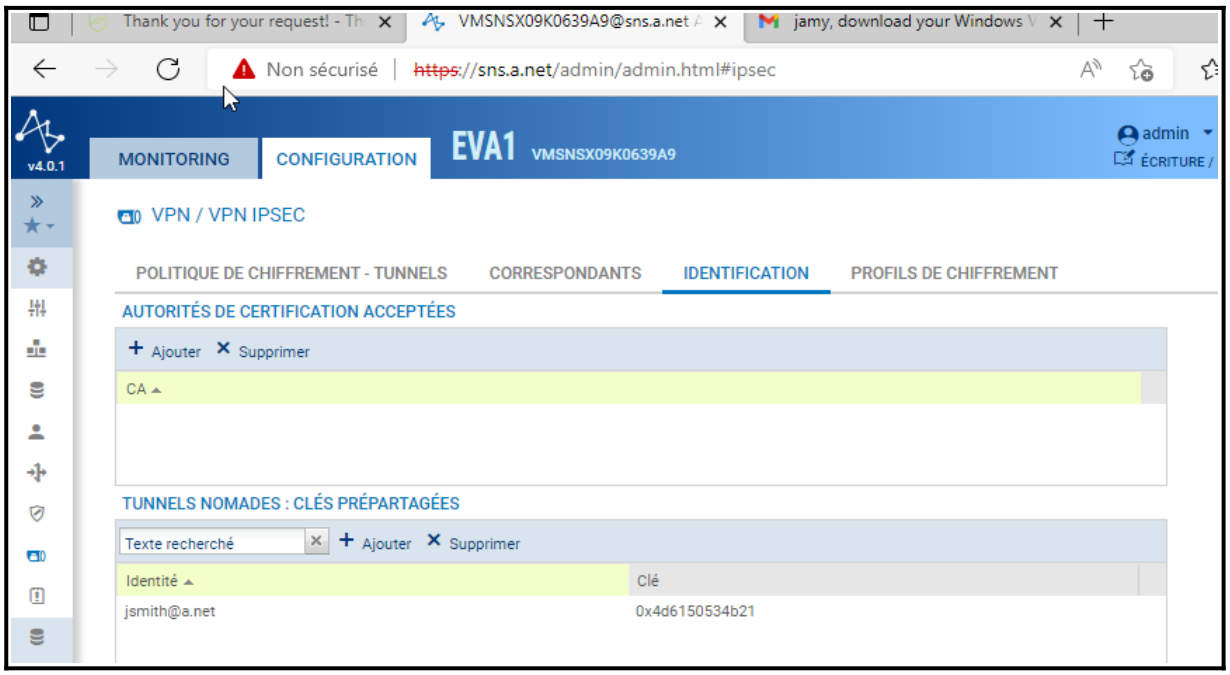




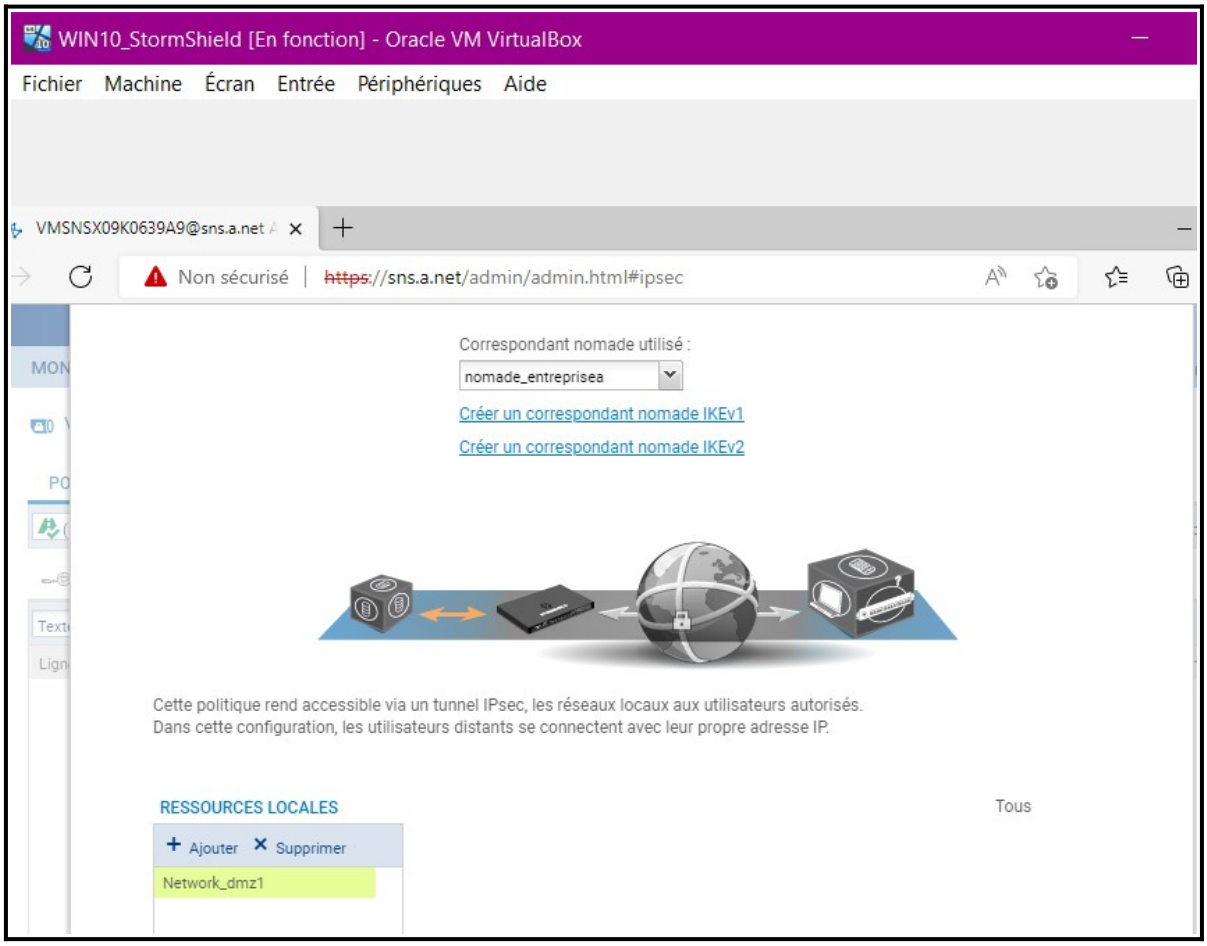
3ème étape : Création d'un nouveau correspondant IKEv2 en ajoutant une nouvelle identité.



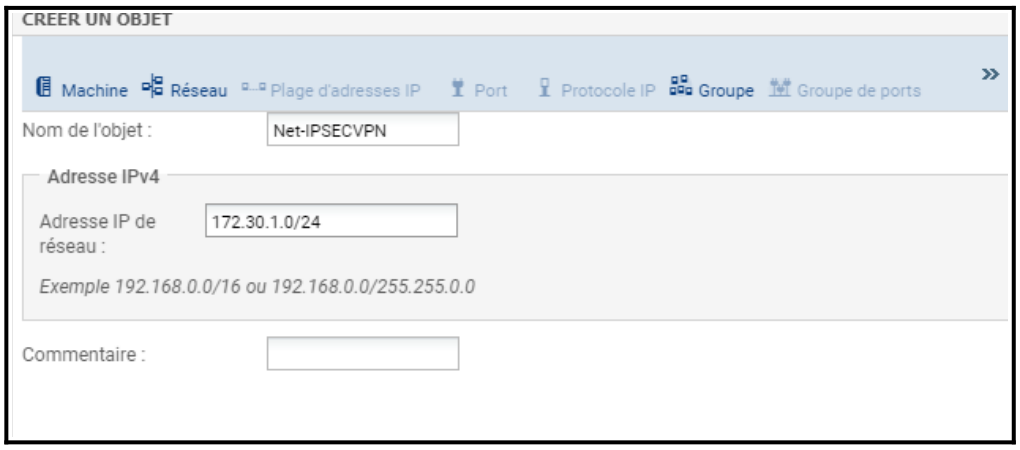
4ème étape : Sur notre nouveau correspondant nous modifions le profil IKE en indiquant IKEphase1Nomade.



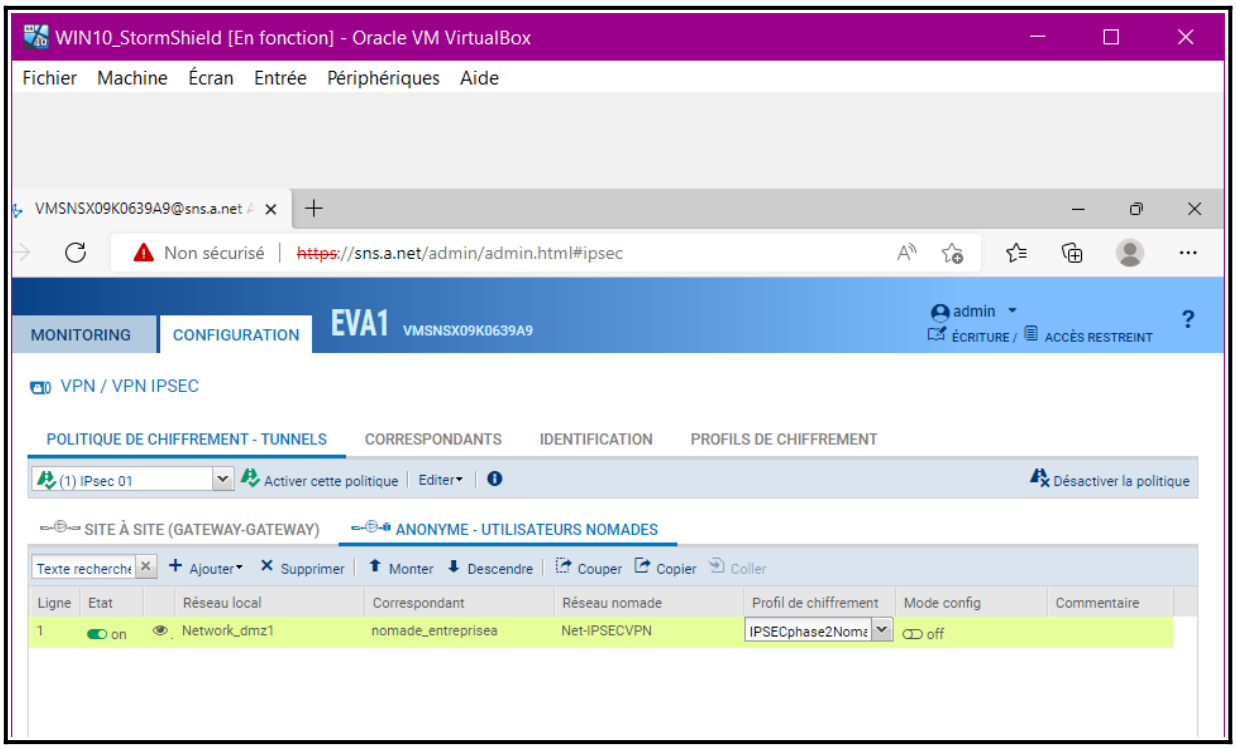
5ème étape : Nous observons dans l'onglet identification l'apparition de la nouvelle clés prépartagées.



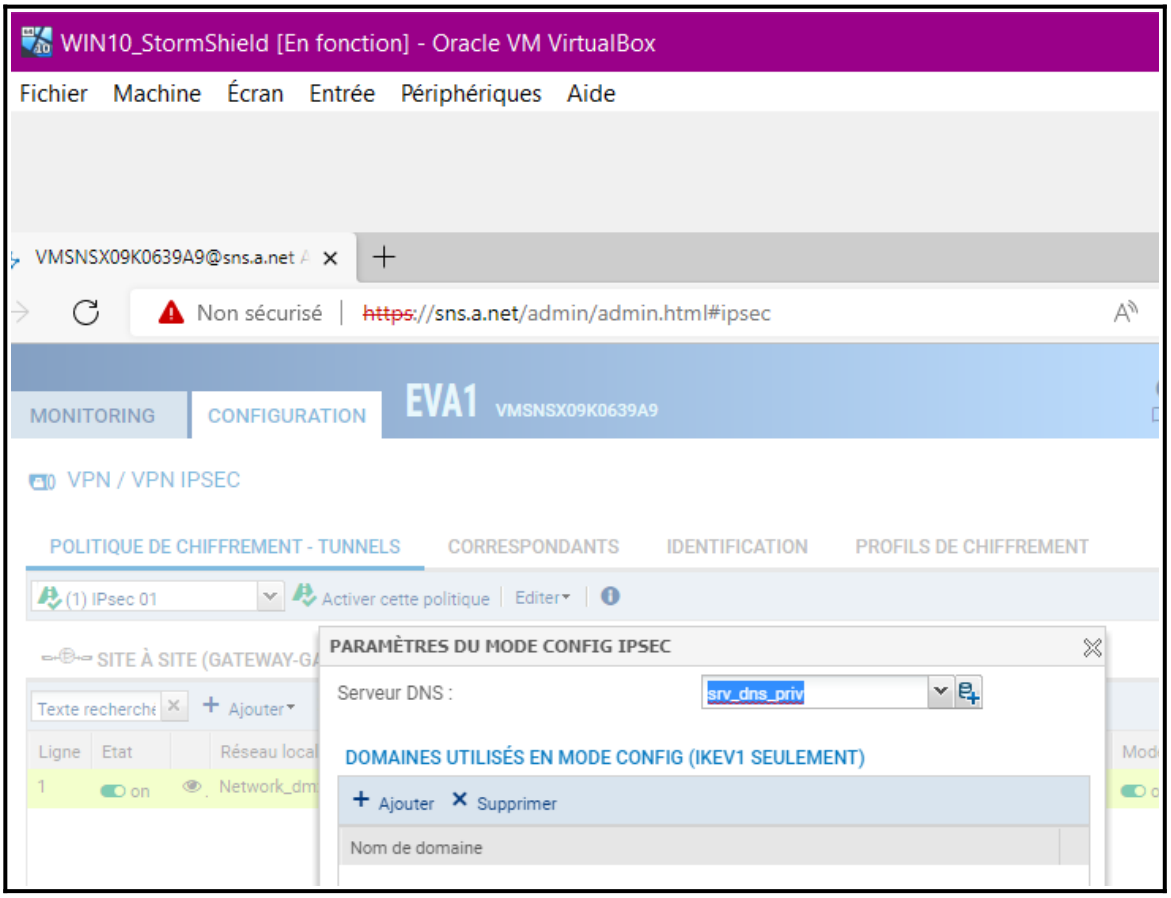
6ème étape : Ajout d'une nouvelle politique de chiffrement dans l'onglet utilisateurs nomades.



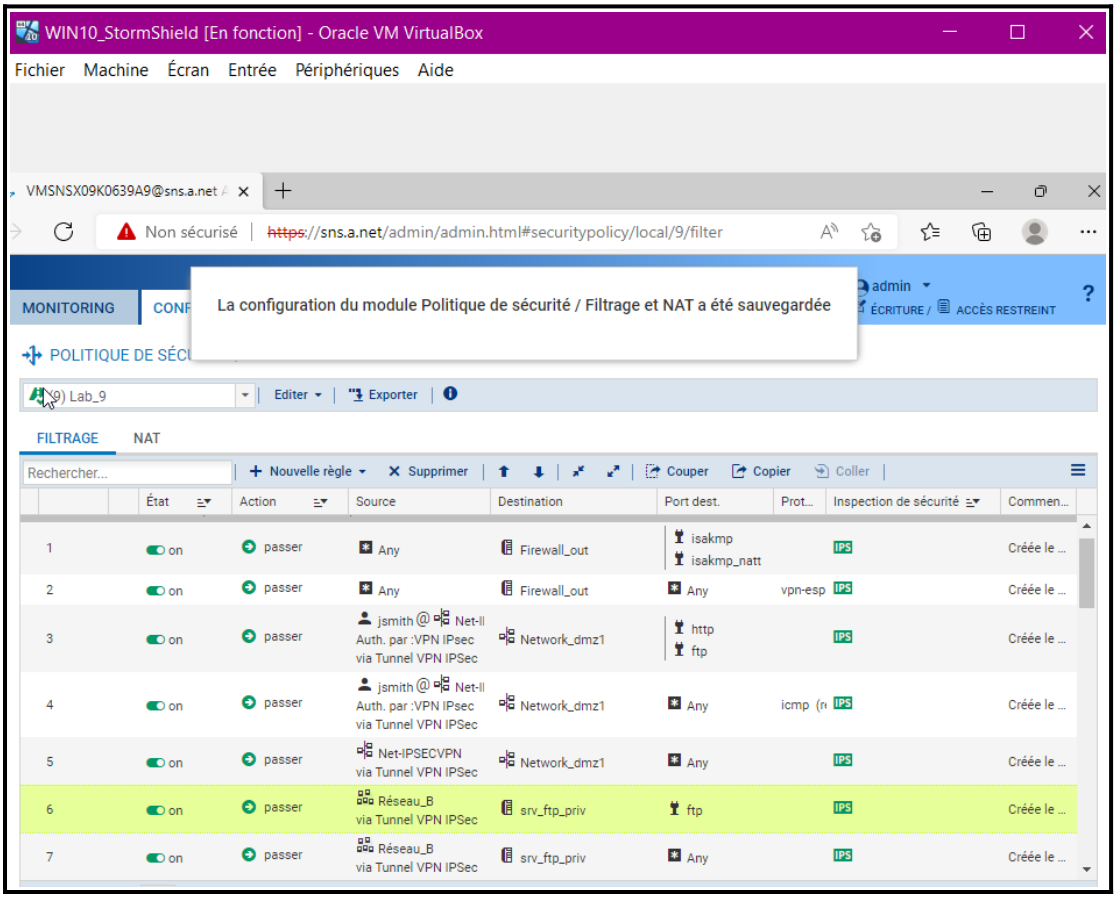
7ème étape : Création de l'objet Net-IPSECVPN.



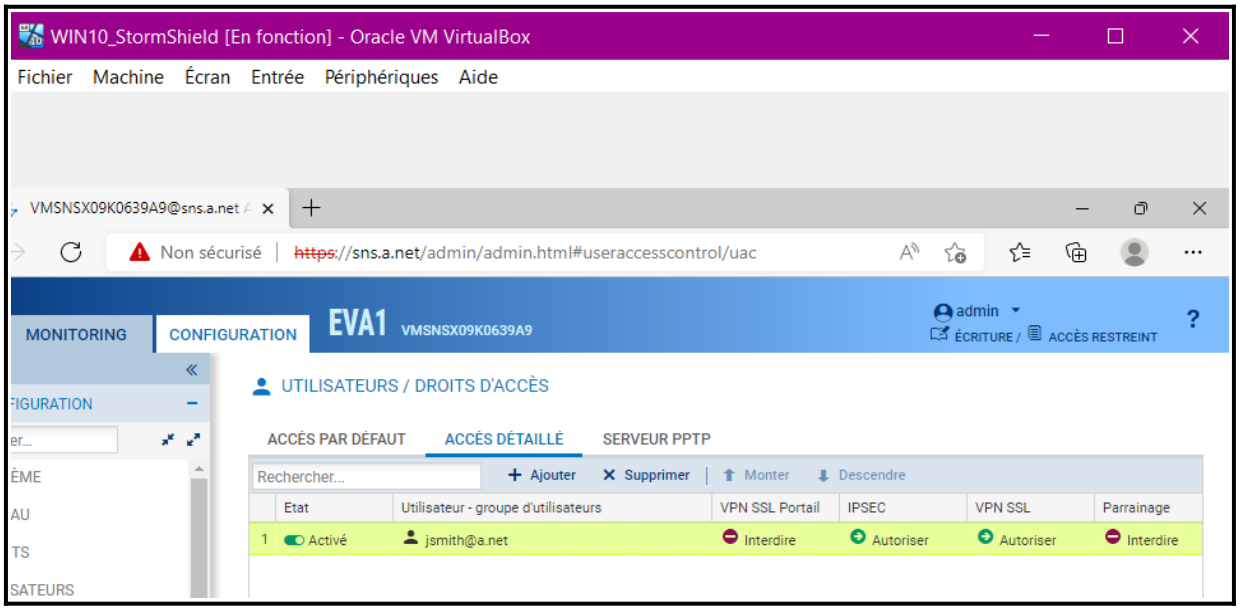
8ème étape : Ajout du profil de chiffrement avec l'objet créer précédemment dans la politique de filtrage.



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

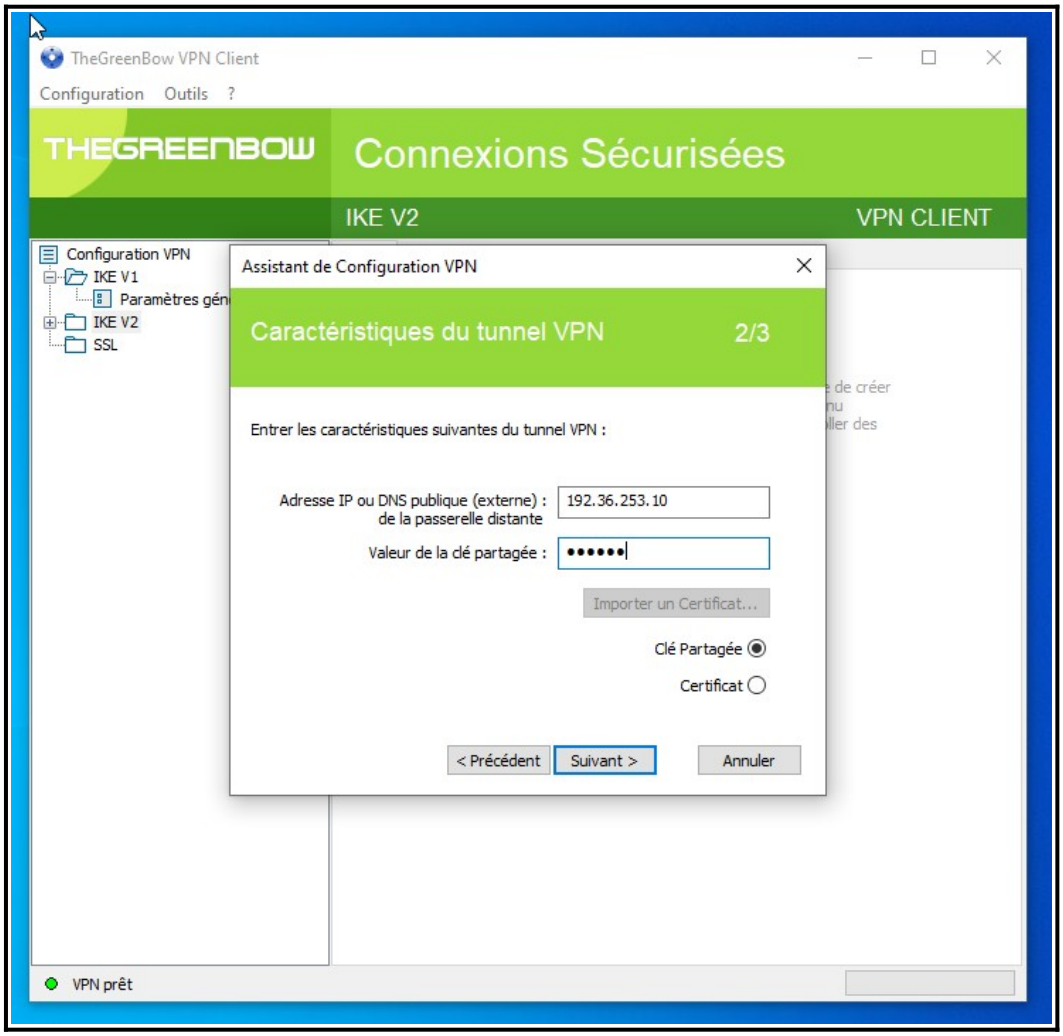


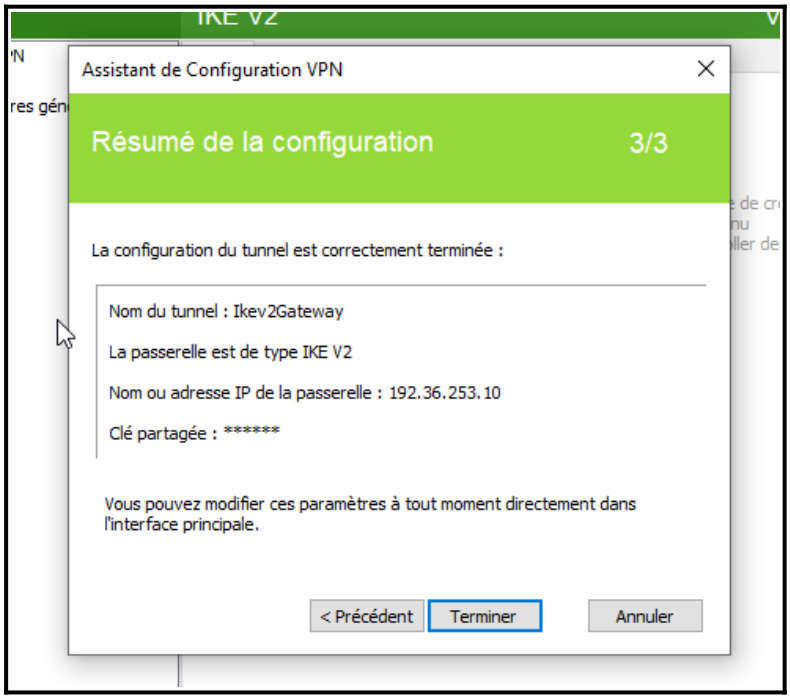
10ème étape : Ajout des règles de filtrages/nat concernant le VPN IPSEC Noamde et site à site.



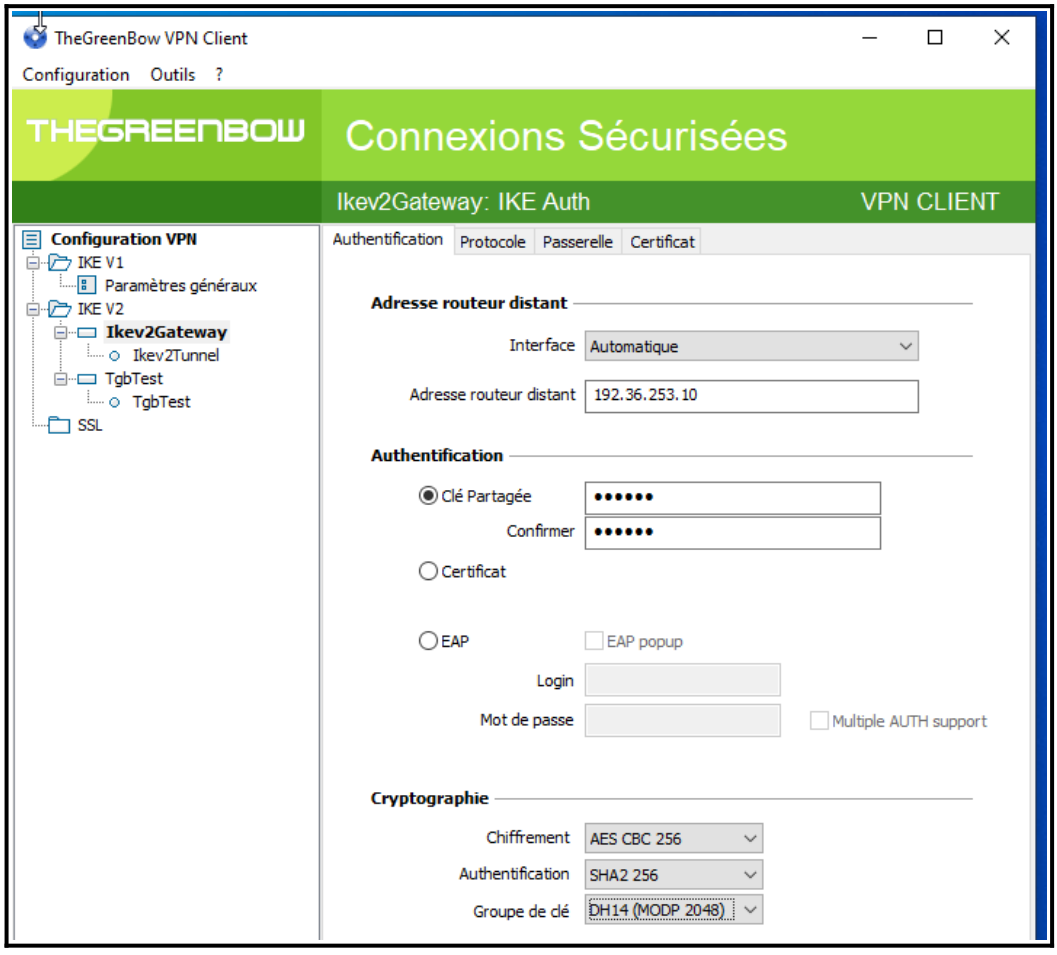
11ème étape : Modification des droits d'accès de l'utilisateur afin d'autoriser l'accès IPSEC.


Connexions VPN
X
TgbTest-TgbTest
OUVRIR
?

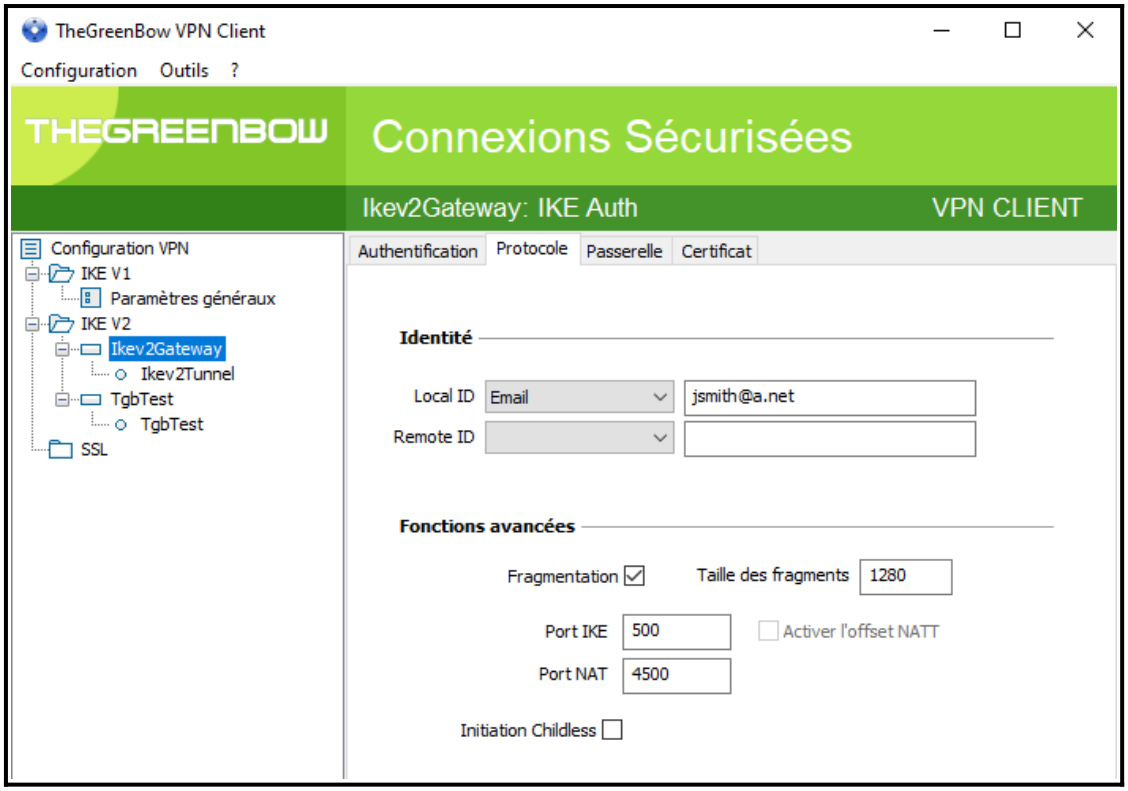

TheGreenBow VPN Client
Configuration
Outils
?
THEGREENBOW
Connexions Sécurisées
IKE V2
VPN CLIENT
Configuration VPN
IKE V1
Paramètres gén
IKE V2
SSL
Assistant de Configuration VPN
Caractéristiques du tunnel VPN
2/3
Entrer les caractéristiques suivantes du tunnel VPN :
Adresse IP ou DNS publique (externe) : de la passerelle distante
192.36.253.10
Valeur de la clé partagée :
Importer un Certificat...
Clé Partagée
Certificat
< Précédent
Suivant >
Annuler
VPN prêt

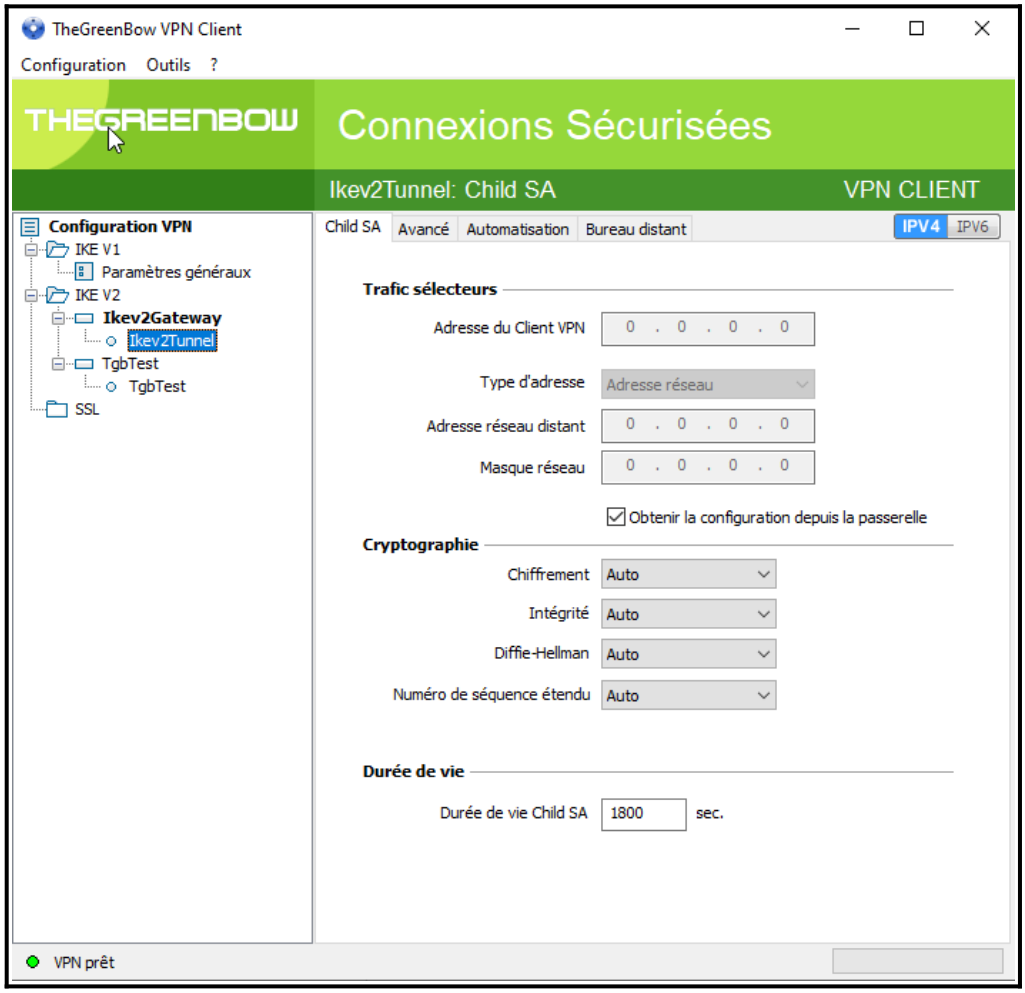


12ème étape : Installation du client TheGreenBow VPN en utilisant l'assistant de création de tunnel IKEv2, nous complétons les informations des caractéristiques du tunnel VPN la clé partagée.

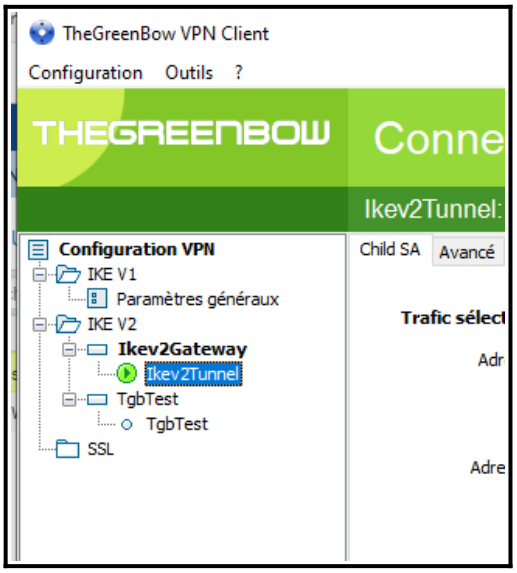


13ème étape : Réglage de la cryptographie dans l'onglet authentification.





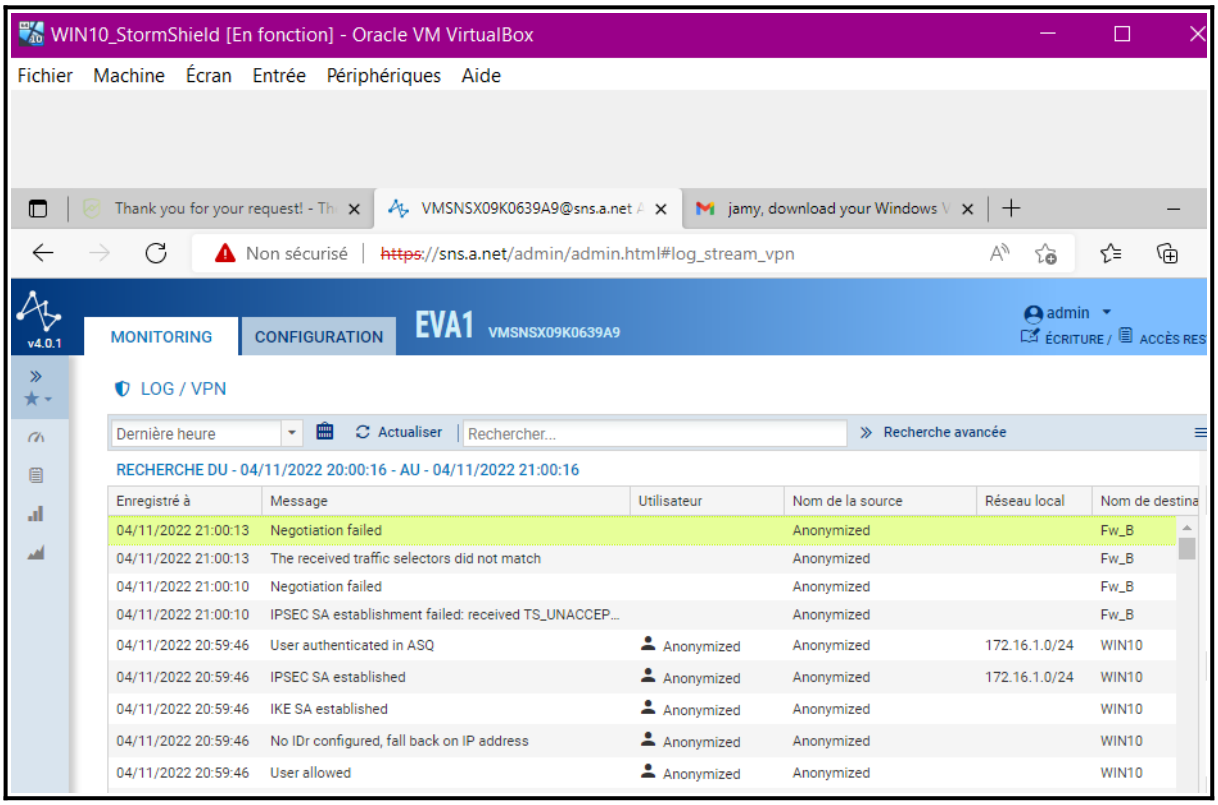
14ème étape : Modification dans l'onglet protocole.

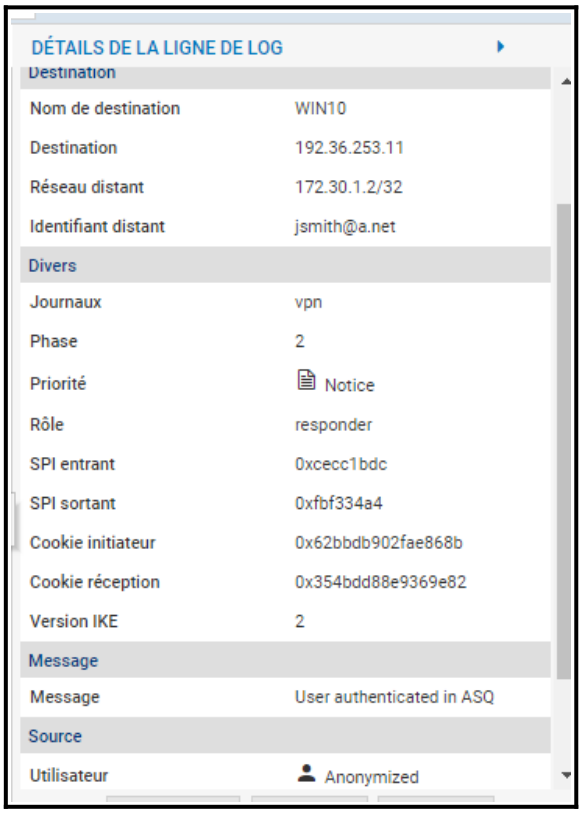


15ème étape : Mise en route de la connexion sécurisée établie.

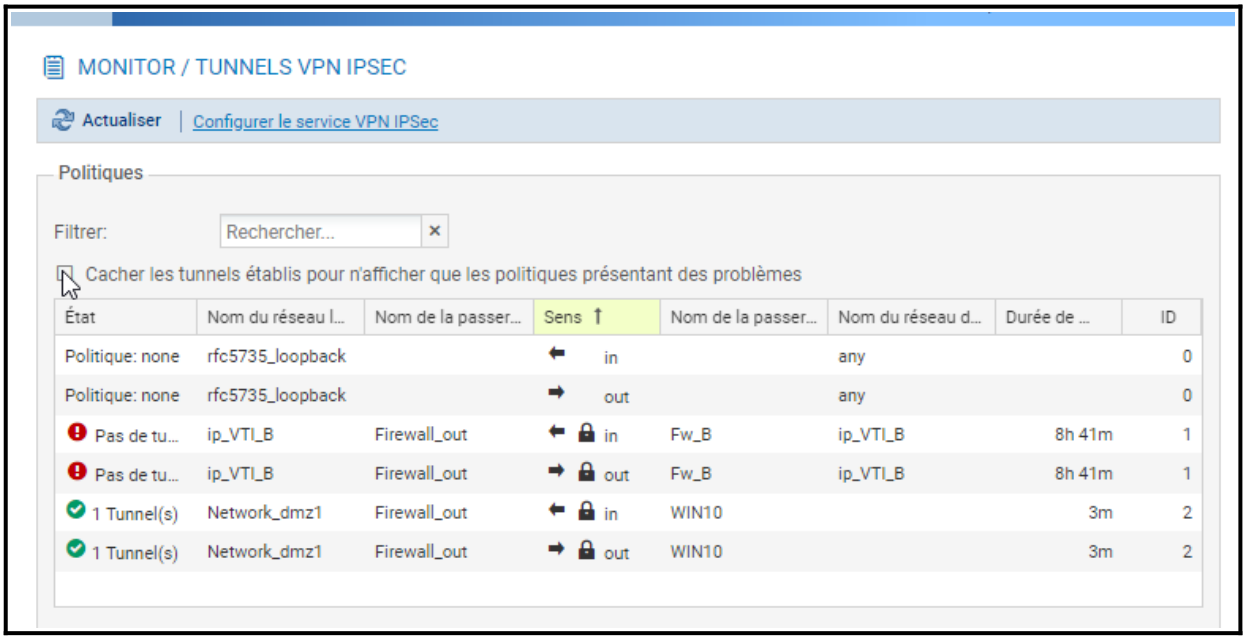
```
Carte Ethernet TGB Ikev2Gateway-Ikev2Tunnel :

   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(préféré)
   Adresse IPv4. . . . . . . . . . . . . .: 172.30.1.2(préféré)
   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.

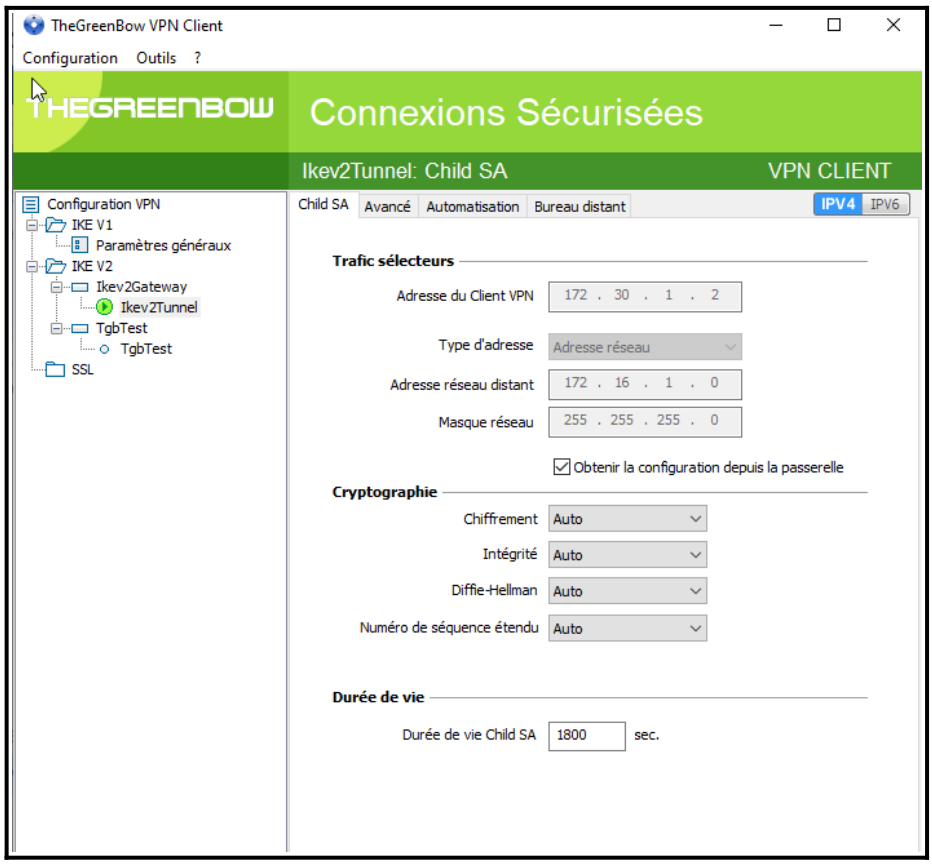


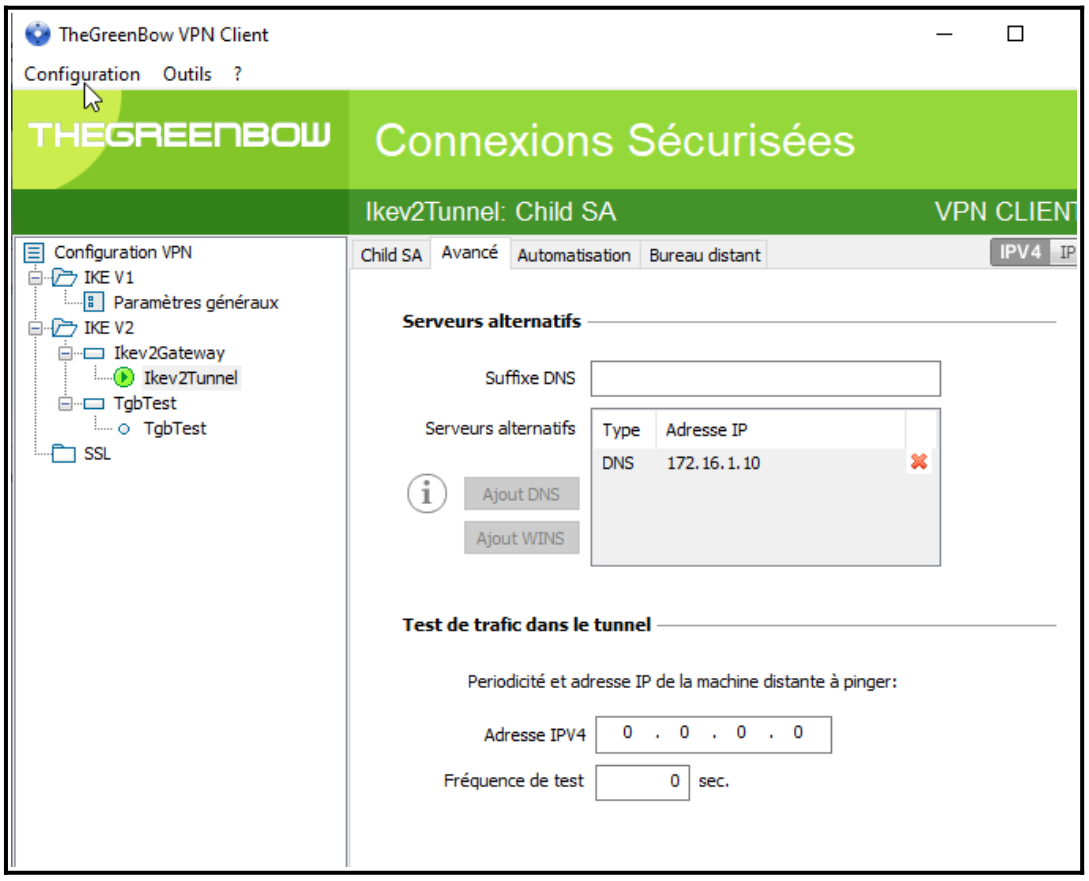


17ème étape : Nous observons dans les logs VPN les activités que nous avons effectuées.

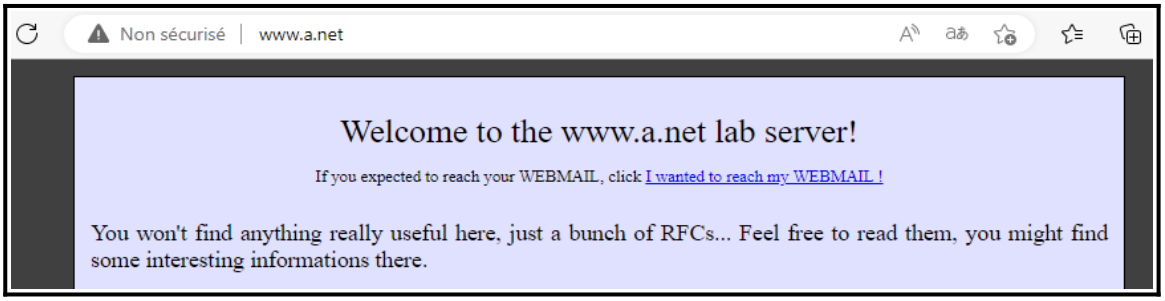


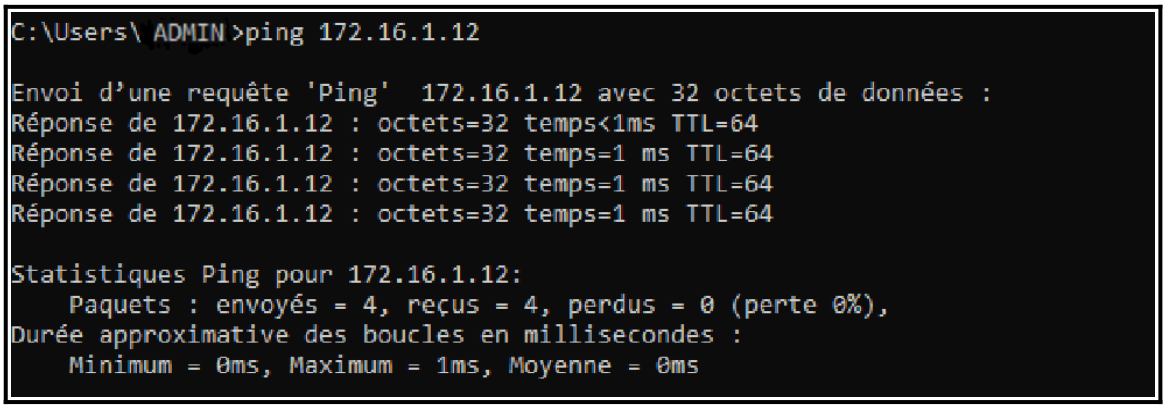
18ème étape : On observe les connexions VPN IPSEC effectuées sur les deux dernières lignes.





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





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