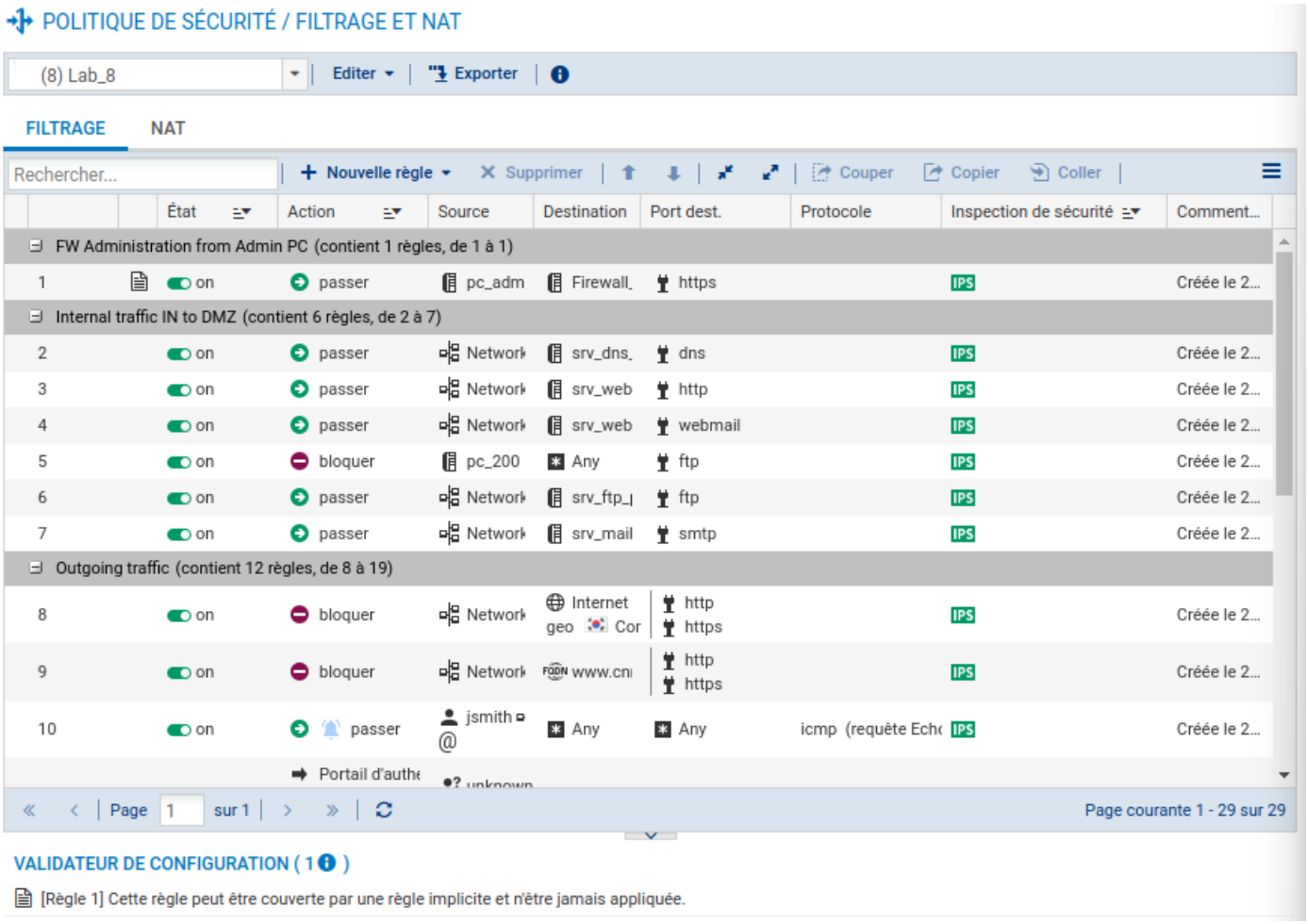
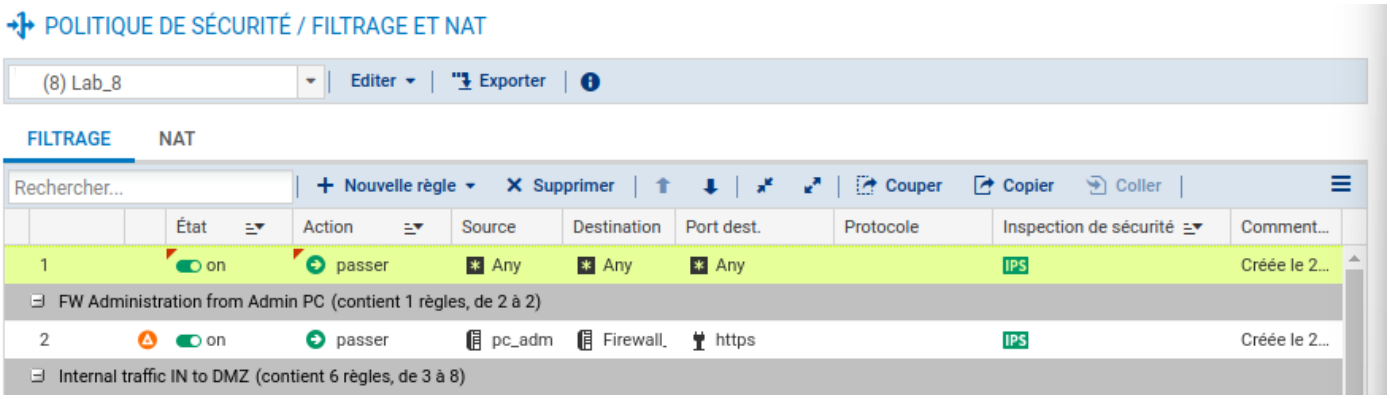
- Je copie la politique de filtrage/NAT (7) Lab_7 vers la politique numéro 8. Je renomme la politique numéro 8 « Lab_8 », puis j'active cette politique :



- J'ajoute une règle de filtrage Pass any any any en tête de cette politique :



- Je configure un tunnel IPsec avec une authentification par PSK pour relier mon réseau interne « 192.168.x.0/24 » à celui de l'autre entreprise en utilisant les profils de chiffrement par défaut (StrongEncryption) :

CRÉER UNE PASSERELLE DISTANTE

SÉLECTIONNER LA PASSERELLE - ASSISTANT DE CRÉATION DE CORRESPONDANT

Passerelle distante: Fw_A

Nom: Site_Fw_A

Version IKE: IKEv2

ANNULER PRÉCÉDENT SUIVANT

CRÉER UNE PASSERELLE DISTANTE

SÉLECTIONNER LA PASSERELLE - ASSISTANT DE CRÉATION DE CORRESPONDANT

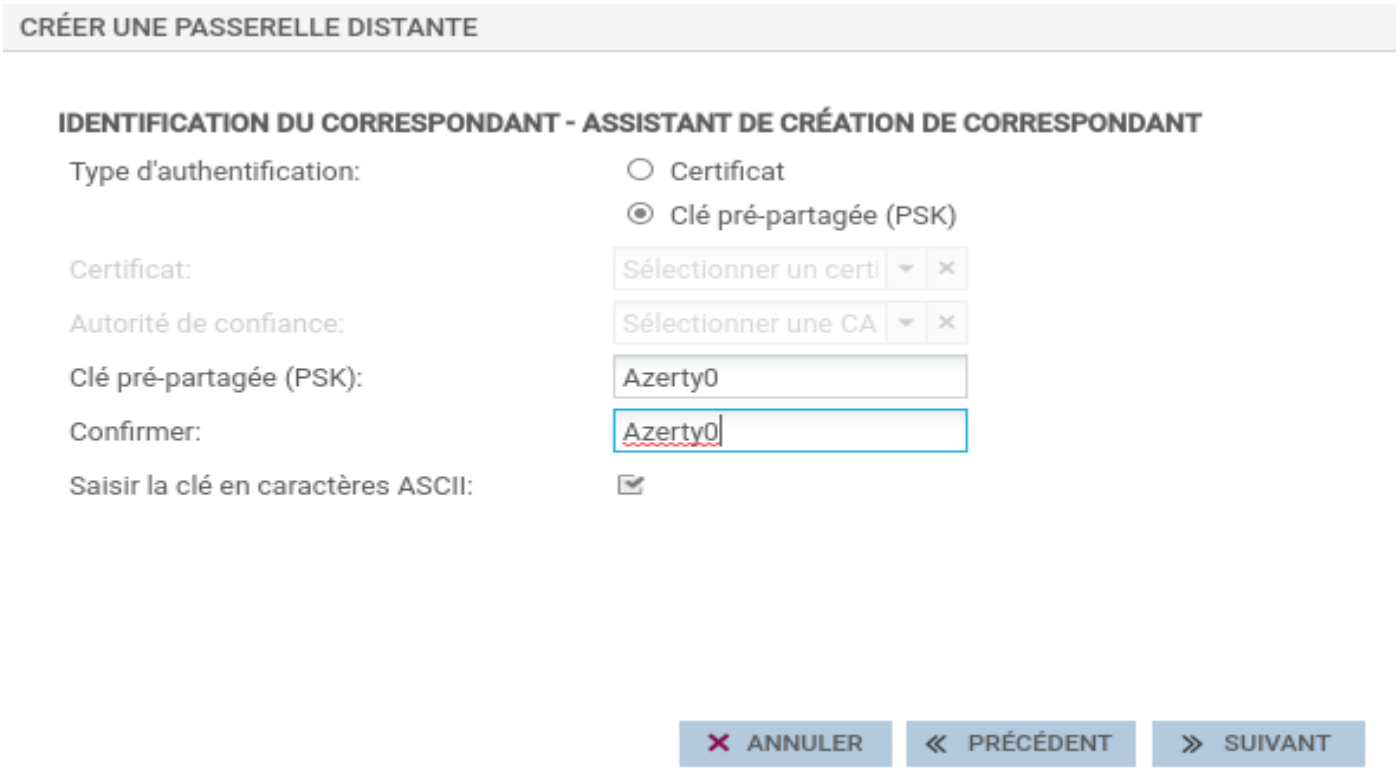
Passerelle distante: Fw_B

Nom: Site_Fw_B

Version IKE: IKEv2

ANNULER PRÉCÉDENT SUIVANT


CRÉER UNE PASSERELLE DISTANTE
IDENTIFICATION DU CORRESPONDANT - ASSISTANT DE CRÉATION DE CORRESPONDANT
Type d'authentification:
Certificat
Clé pré-partagée (PSK)
Certificat:
Sélectionner un certi
Autorité de confiance:
Sélectionner une CA
Clé pré-partagée (PSK):
Azerty0
Confirmer:
Azerty0
Saisir la clé en caractères ASCII:
ANNULER
PRÉCÉDENT
SUIVANT


CRÉER UNE PASSERELLE DISTANTE
IDENTIFICATION DU CORRESPONDANT - ASSISTANT DE CRÉATION DE CORRESPONDANT
Type d'authentification:
Certificat
Clé pré-partagée (PSK)
Certificat:
Sélectionner un certi
Autorité de confiance:
Sélectionner une CA
Clé pré-partagée (PSK):
Azerty0
Confirmer:
Azerty0
Saisir la clé en caractères ASCII:
ANNULER
PRÉCÉDENT
SUIVANT

ASSISTANT DE POLITIQUE VPN IPSEC

Ressources locales: Network_in

Choix du correspondant: Site_Fw_B

Réseaux distants: Lan_in_B

ANNULER TERMINER

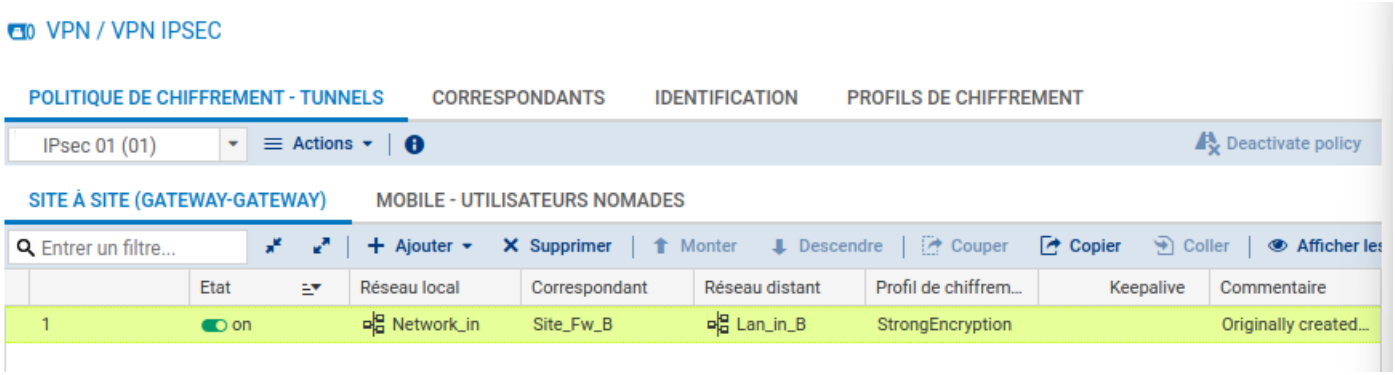
ASSISTANT DE POLITIQUE VPN IPSEC

Ressources locales: Network_in

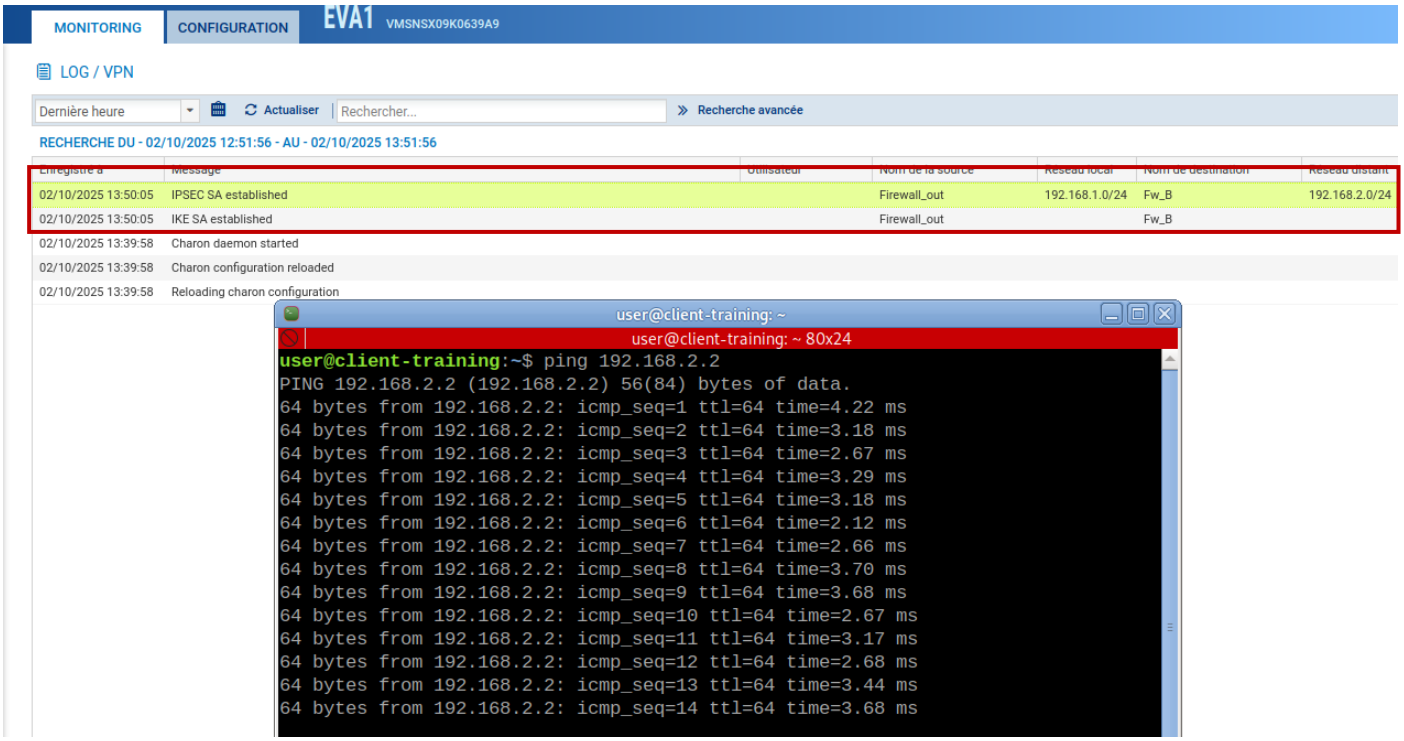
Choix du correspondant: Site_Fw_A

Réseaux distants: Lan_in_A

ANNULER TERMINER



- Je généré du trafic correspondant aux extrémités de trafic et je suis les étapes de négociation des tunnels et l'activité dans les tunnels depuis les journaux et le menu de supervision correspondants :



- Je modifie mes politiques IPSec pour relier cette fois mes deux réseaux Internes (IN + DM)) aux réseaux internes N + DM)) de l'autre entreprise. J'active la fonction keep-alive sur mon tunnel. Et je regarde le nombre de tunnels négociés dans la supervision :

CRÉER UN OBJET

- Machine
- Nom DNS (FQDN)
- Réseau
- Plage d'adresses
- Routeur
- Groupe
- Protocole IP
- Port
- Groupe de ports

Nom de l'objet: DMZ_In_B

Adresses IPv4

Adresse IP de réseau: 172.16.2.0/24

Exemple 192.168.0.0/16 ou 192.168.0.0/255.255.0.0

Commentaire:

CRÉER UN OBJET

- Machine
- Nom DNS (FQDN)
- Réseau
- Plage d'adresses
- Routeur
- Groupe
- Protocole IP
- Port

Nom de l'objet: DMZ_In_A

Adresses IPv4

Adresse IP de réseau: 172.168.1.0/24

Exemple 192.168.0.0/16 ou 192.168.0.0/255.255.0.0

Commentaire:

VPN / VPN IPSEC

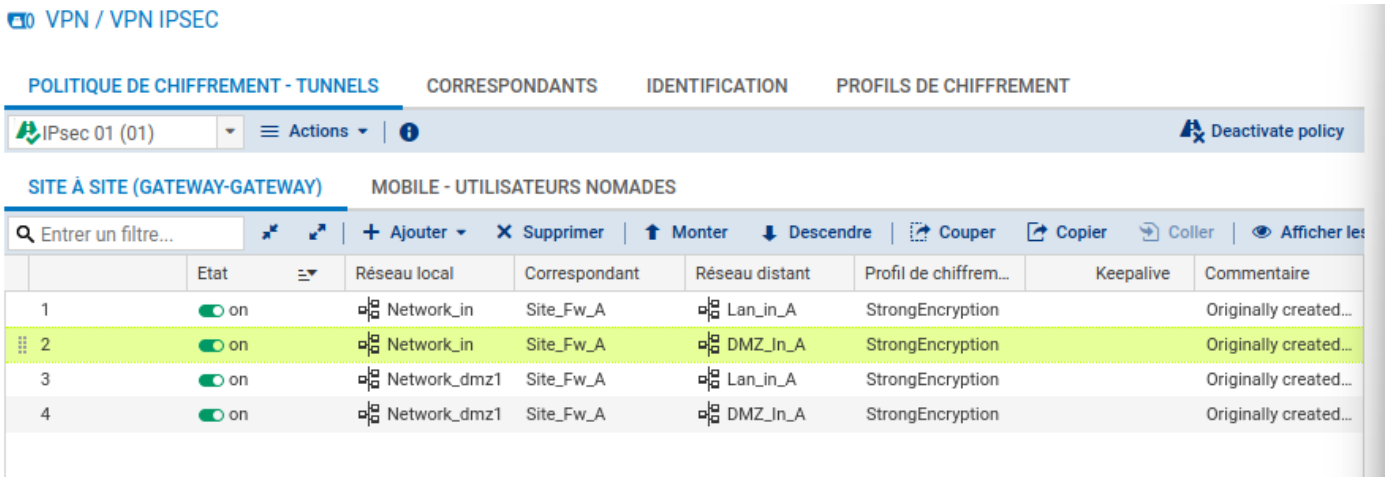
POLITIQUE DE CHIFFREMENT - TUNNELS | CORRESPONDANTS | IDENTIFICATION | PROFILS DE CHIFFREMENT

IPsec 01 (01) | Actions | Deactivate policy

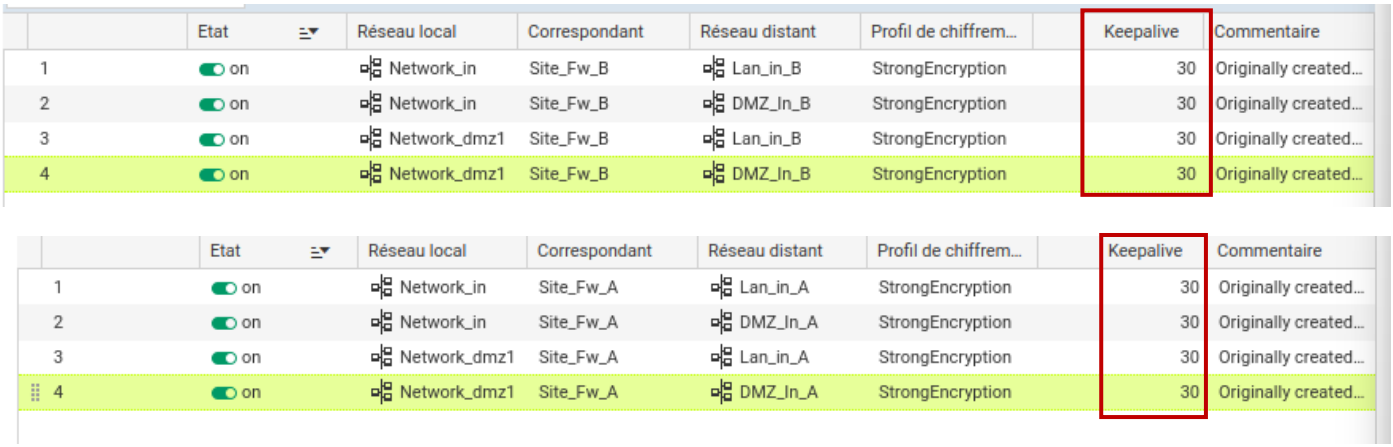
SITE À SITE (GATEWAY-GATEWAY) | MOBILE - UTILISATEURS NOMADES

Entrer un filtre... | Ajouter | Supprimer | Monter | Descendre | Couper | Copier | Coller | Afficher les

	Etat	Réseau local	Correspondant	Réseau distant	Profil de chiffrem...	Keepalive	Commentaire
1	on	Network_in	Site_Fw_B	Lan_in_B	StrongEncryption		Originally created...
2	on	Network_in	Site_Fw_B	DMZ_In_B	StrongEncryption		Originally created...
3	on	Network_dmz1	Site_Fw_B	Lan_in_B	StrongEncryption		Originally created...
4	on	Network_dmz1	Site_Fw_B	DMZ_In_B	StrongEncryption		Originally created...

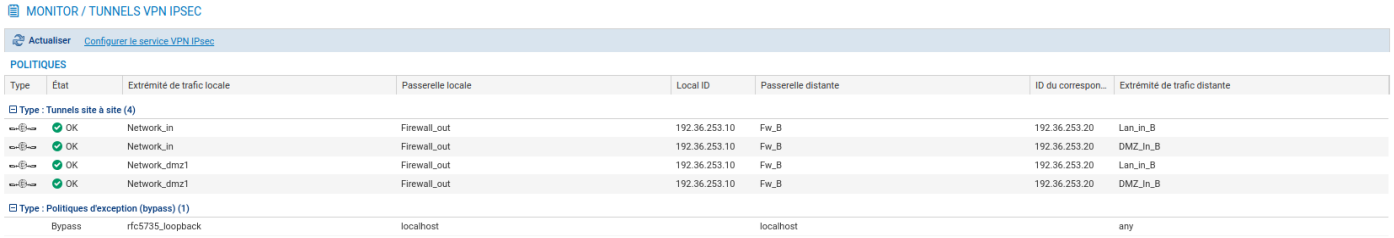


- J'active le keep-alive :

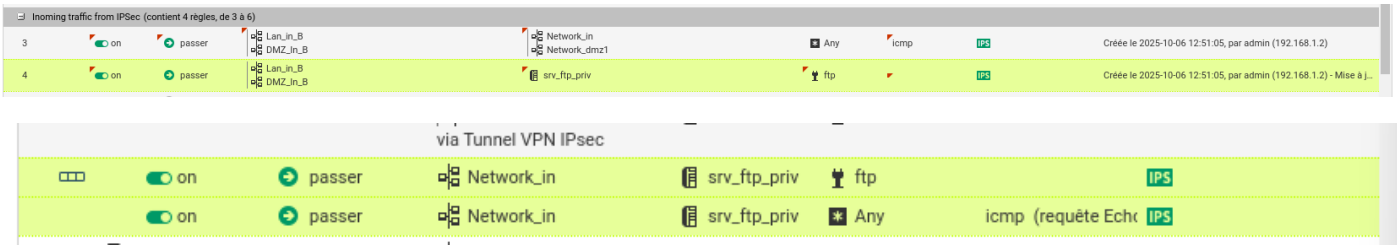


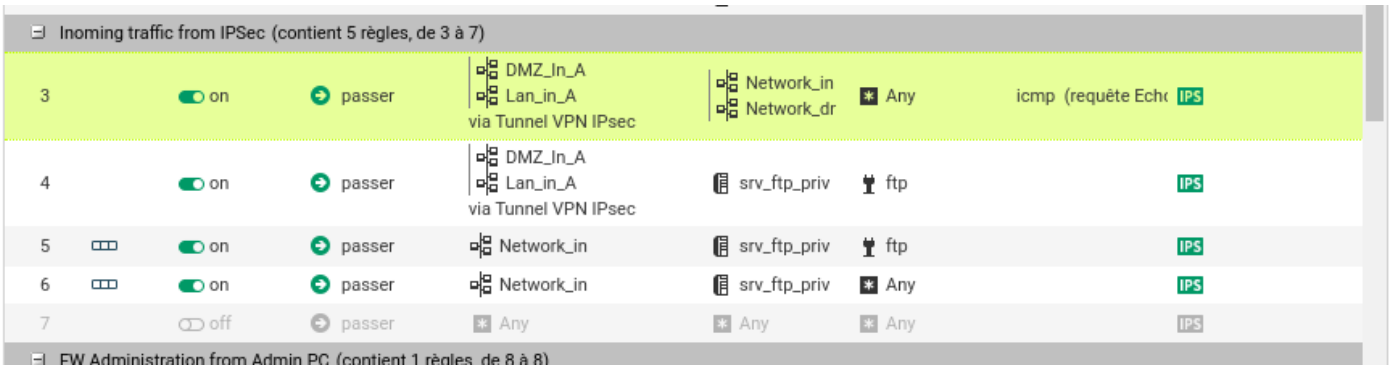
- N'ayant pas fonction j'ai tout fusionné en une seule politique (ne pas faire attention au profil de chiffrement c'est le screen de la question 7, car je n'ai pas le screen original de la politique) :

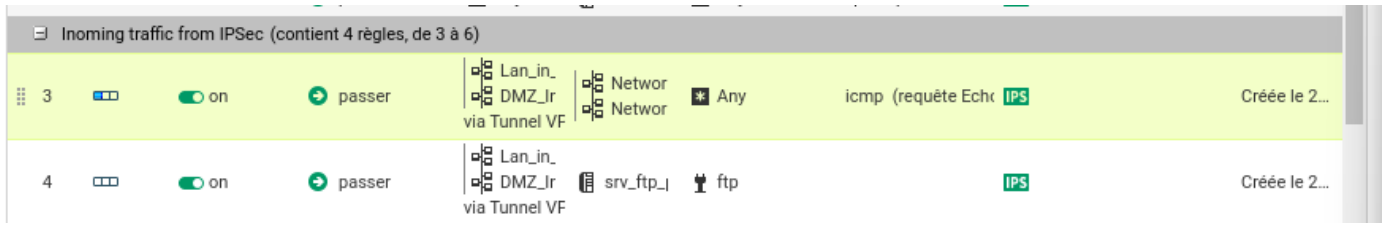
- Je regarde les tunels négociés :



- Je désactive la règle de filtrage Pass any any any et j'ajoute les règles autorisant les réseaux du site distant à joindre à pinger vos réseaux locaux et à joindre vos serveurs FTP et WEB (je le fais sur les deux firewalls) :



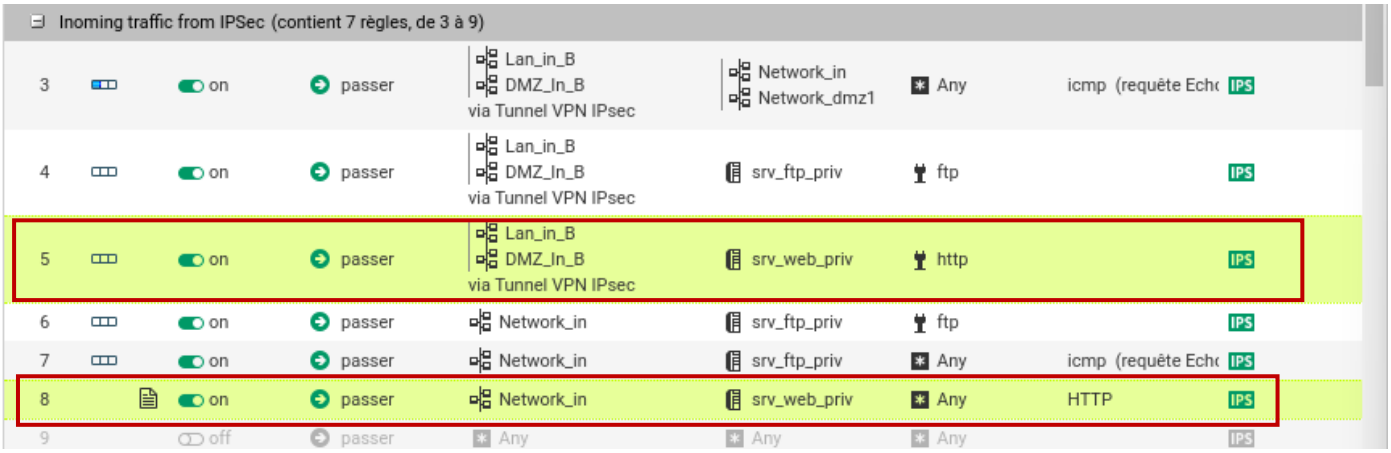


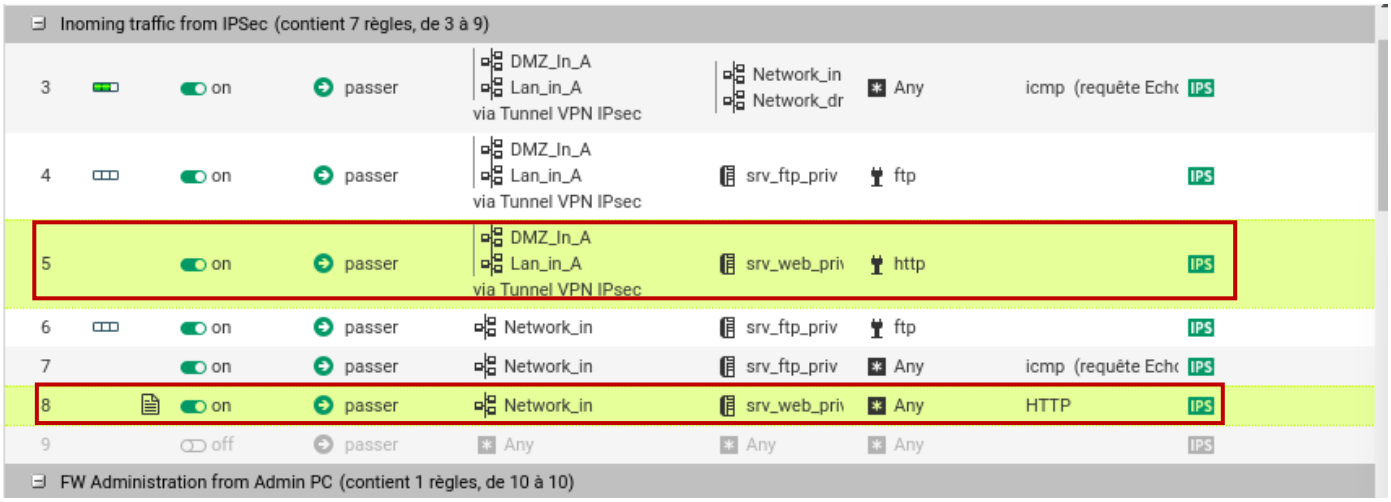


- Pour tester tous ca je ping l'entreprise A de B :

```
user@client-training:~$ ping 192.168.1.2
PING 192.168.1.2 (192.168.1.2) 56(84) bytes of data.
64 bytes from 192.168.1.2: icmp_seq=1 ttl=64 time=3.12 ms
64 bytes from 192.168.1.2: icmp_seq=2 ttl=64 time=3.66 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=64 time=3.69 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=64 time=3.68 ms
^C
--- 192.168.1.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 11ms
rtt min/avg/max/mdev = 3.119/3.539/3.692/0.253 ms
user@client-training:~$
```

➢ Je rajoute sur les deux firewals les règles de pour le web :



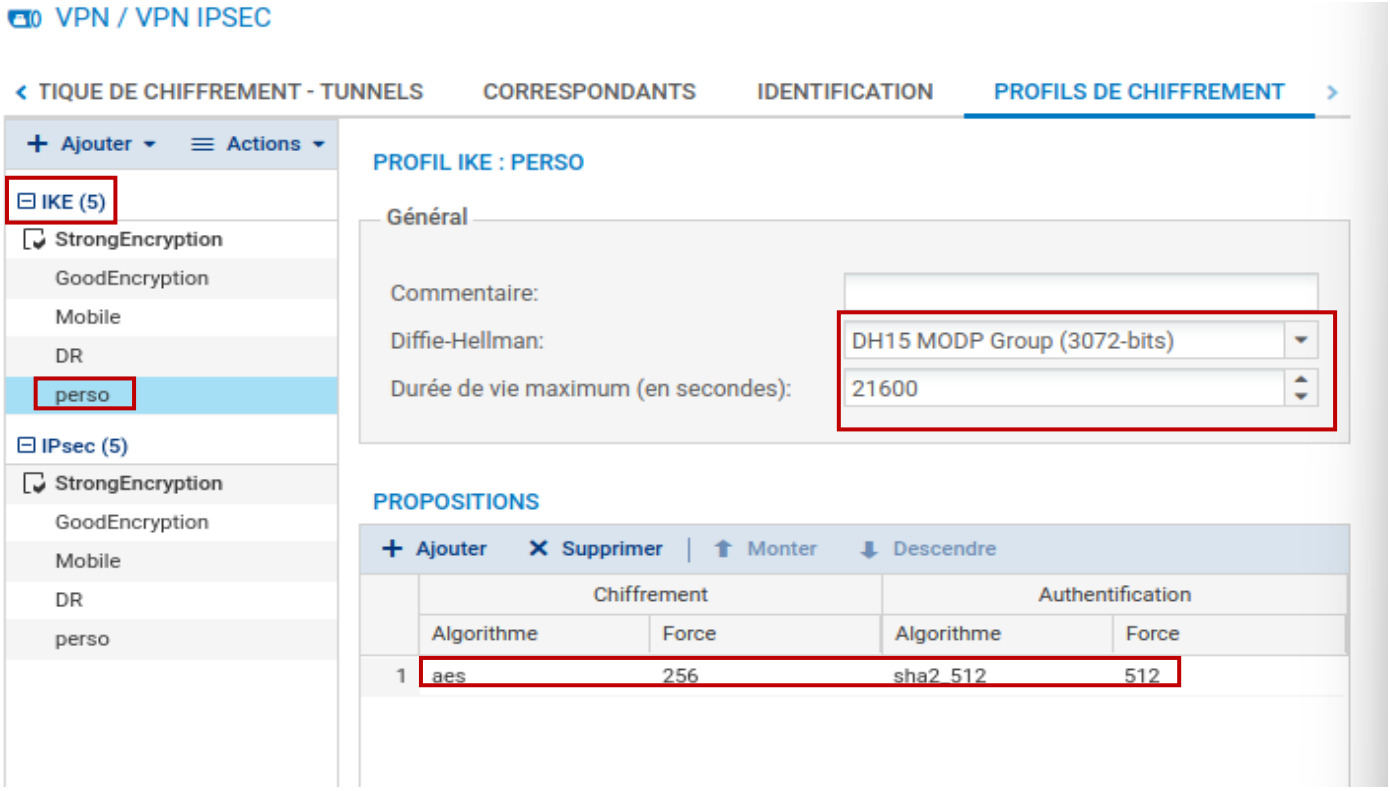


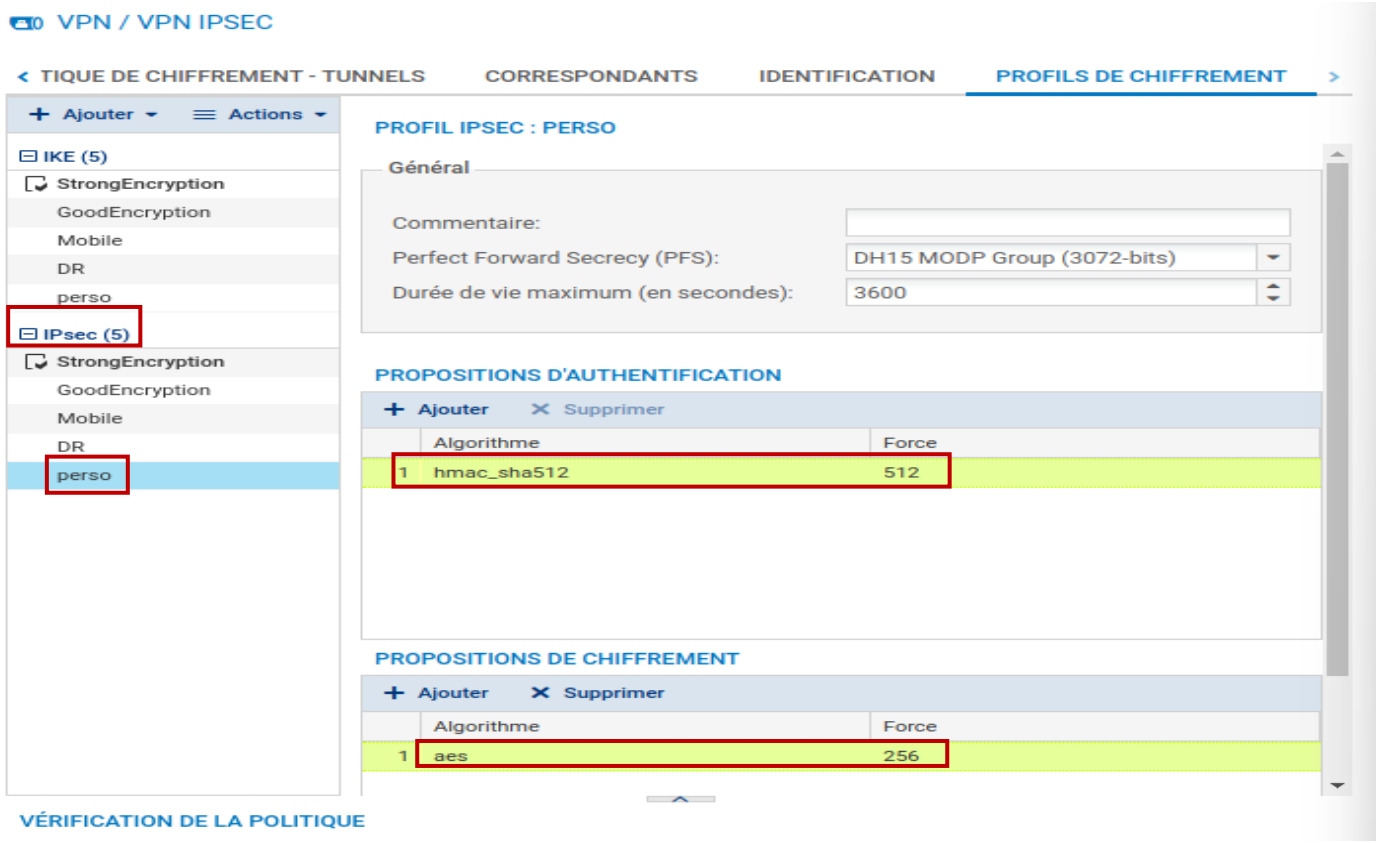
➢ Puis de A je ping B et vice-versa :

```
user@client-training:~$ ping 172.16.2.12
PING 172.16.2.12 (172.16.2.12) 56(84) bytes of data.
64 bytes from 172.16.2.12: icmp_seq=1 ttl=64 time=3.40 ms
64 bytes from 172.16.2.12: icmp_seq=2 ttl=64 time=4.06 ms
64 bytes from 172.16.2.12: icmp_seq=3 ttl=64 time=2.15 ms
64 bytes from 172.16.2.12: icmp_seq=4 ttl=64 time=3.27 ms
^C
--- 172.16.2.12 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 9ms
rtt min/avg/max/mdev = 2.146/3.219/4.060/0.688 ms
user@client-training:~$
```

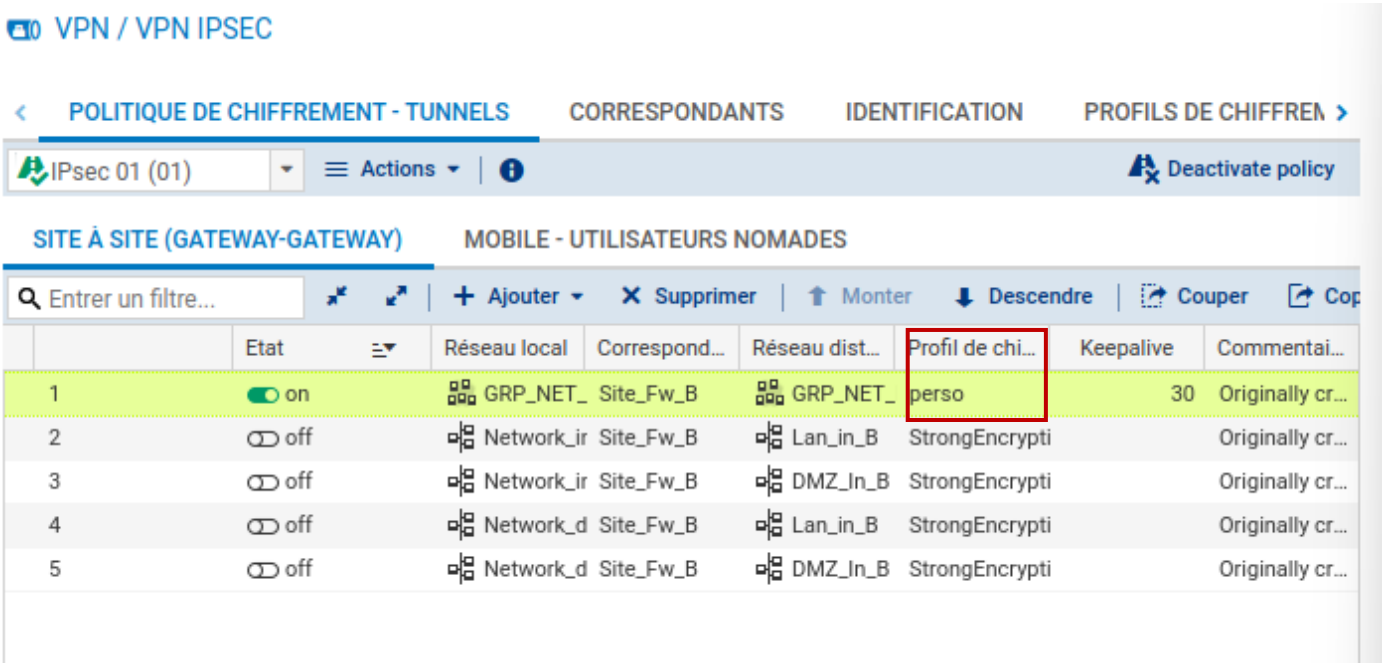
```
user@client-training:~$ ping 172.16.1.12
PING 172.16.1.12 (172.16.1.12) 56(84) bytes of data.
64 bytes from 172.16.1.12: icmp_seq=1 ttl=64 time=2.84 ms
64 bytes from 172.16.1.12: icmp_seq=2 ttl=64 time=13.5 ms
^C
--- 172.16.1.12 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 7ms
rtt min/avg/max/mdev = 2.836/8.171/13.507/5.336 ms
user@client-training:~$
```

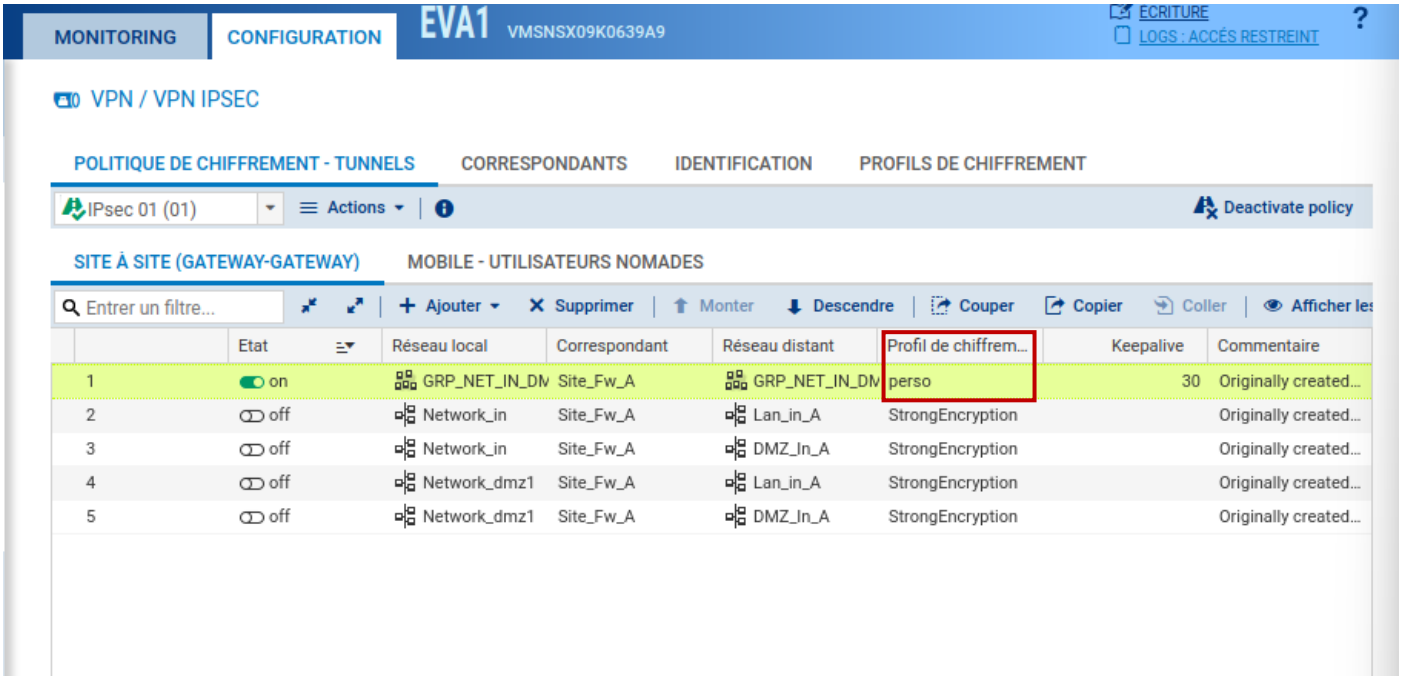
- Je crée 2 profiles de chiffrements IKE phase 1 et 2 :



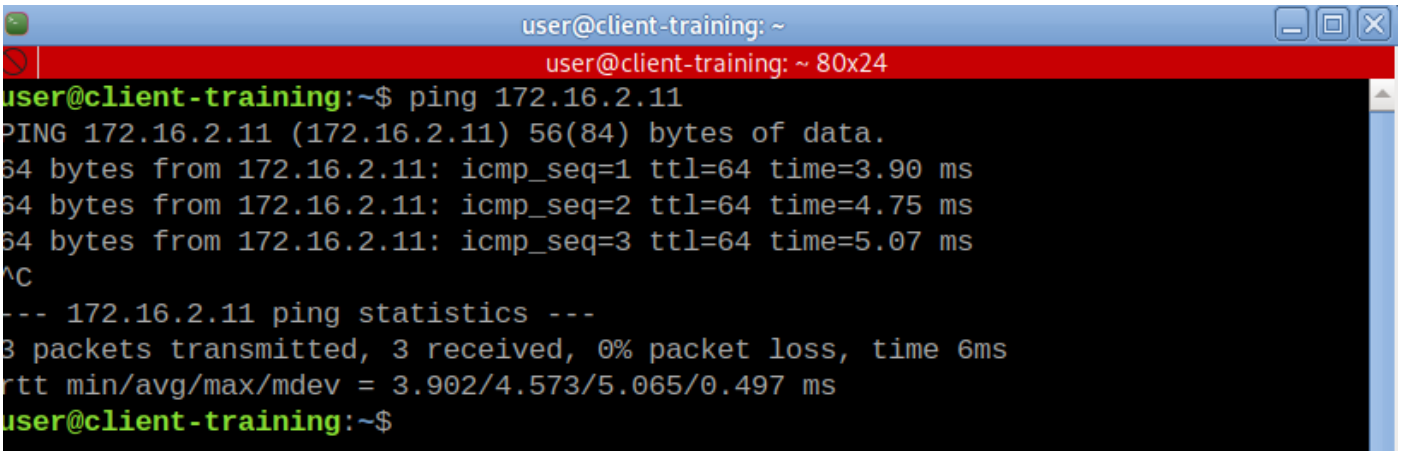


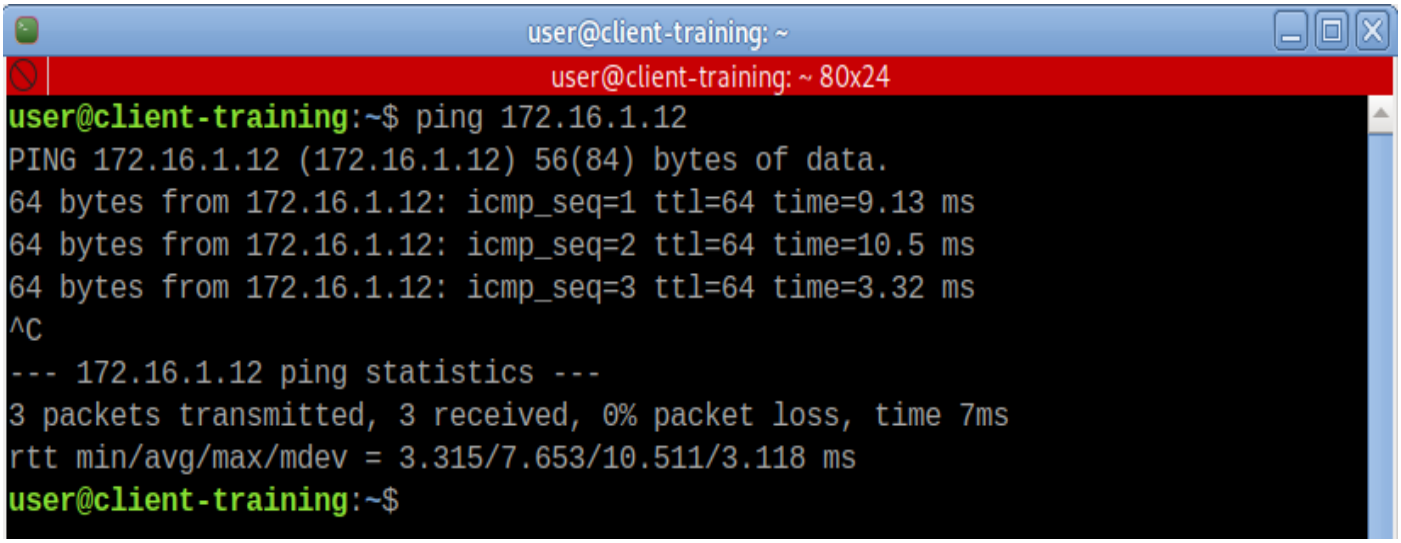
➢ J'applique mes profils de chiffrement sur mon VPN, puis je vérifie que tout fonctionne :



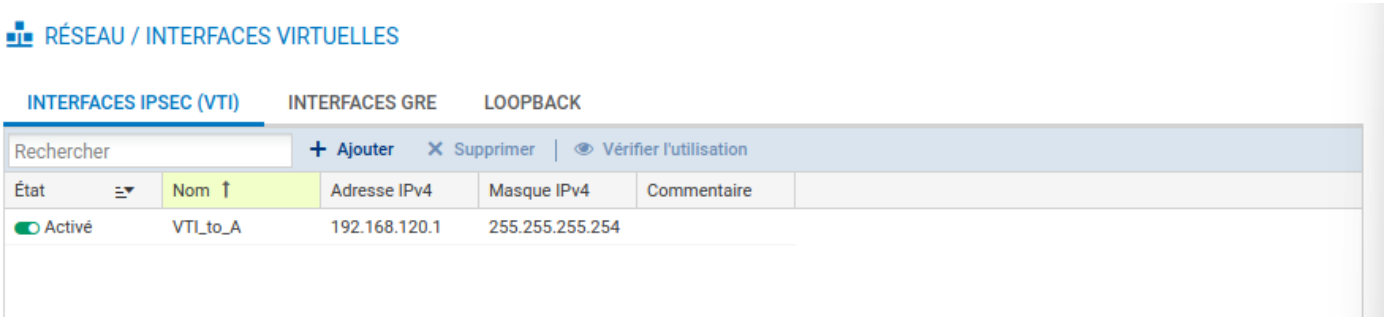


➢ Je ping de A vers B et vice-versa pour verifier que tout fonctionne :

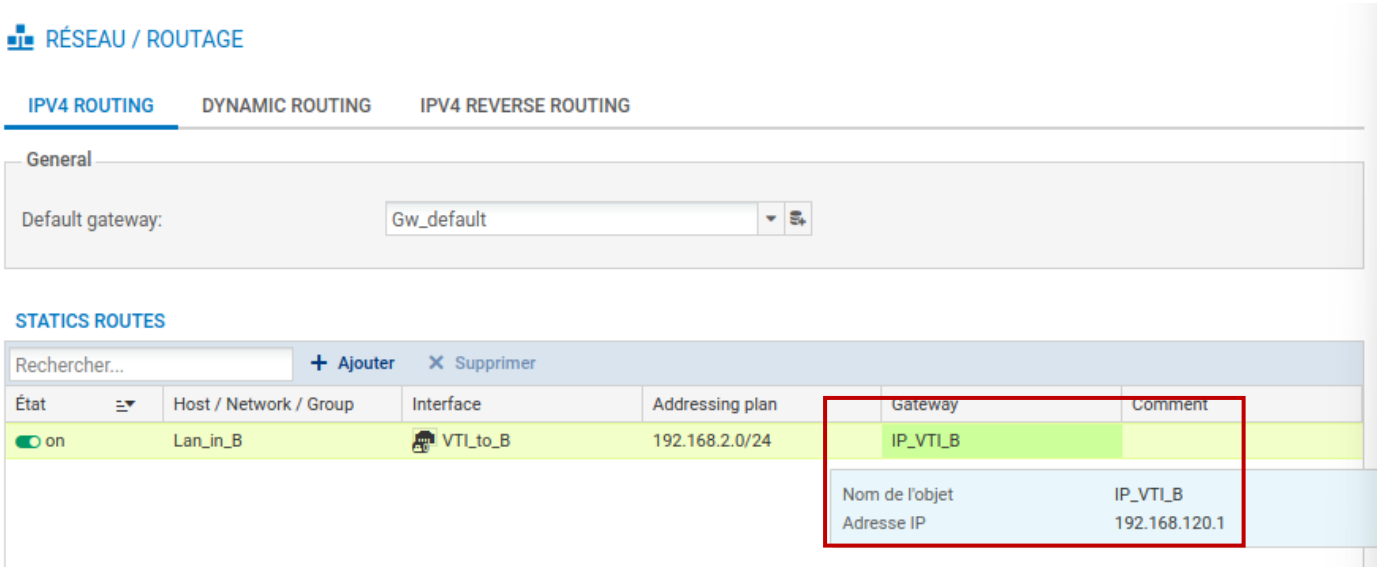


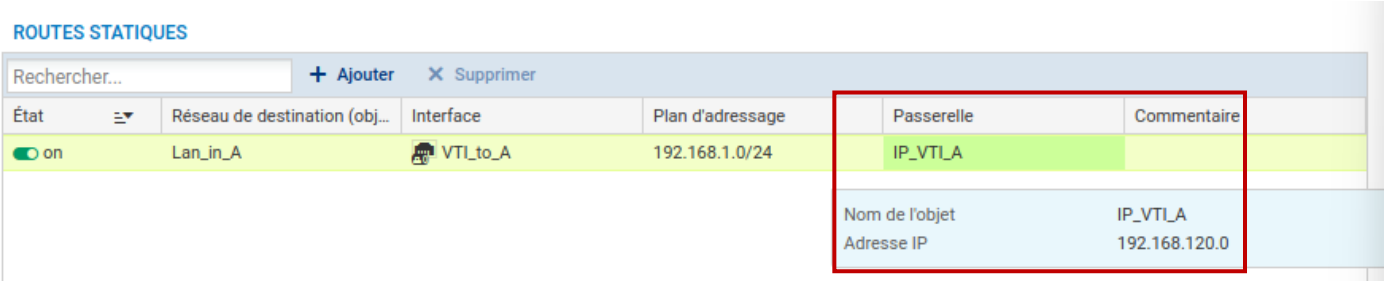


- Je réalise l'interconnexion de ces mêmes réseaux, mais en configurant des tunnels basés sur des VTI, avec du routage statique :
- Je crée les VTI de A et B :



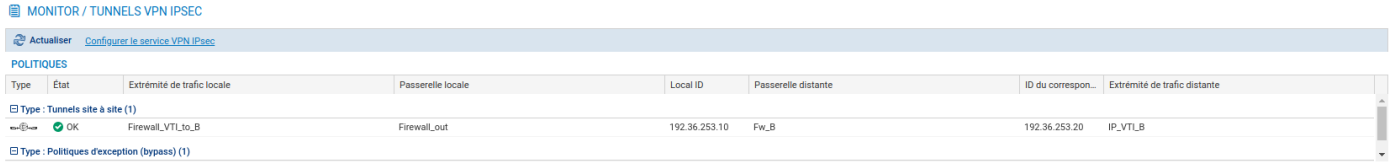
- Je créer les routes statiques (en créant au préalable l'objet IP_VTI_*) :

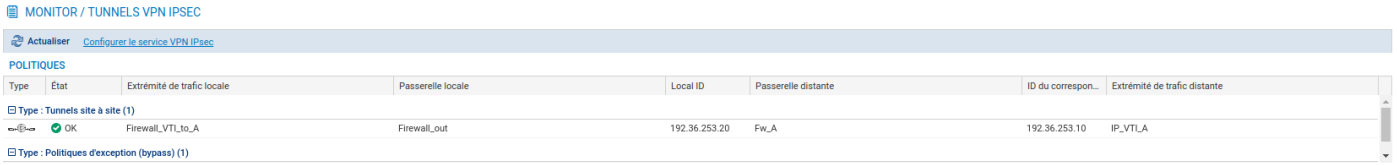




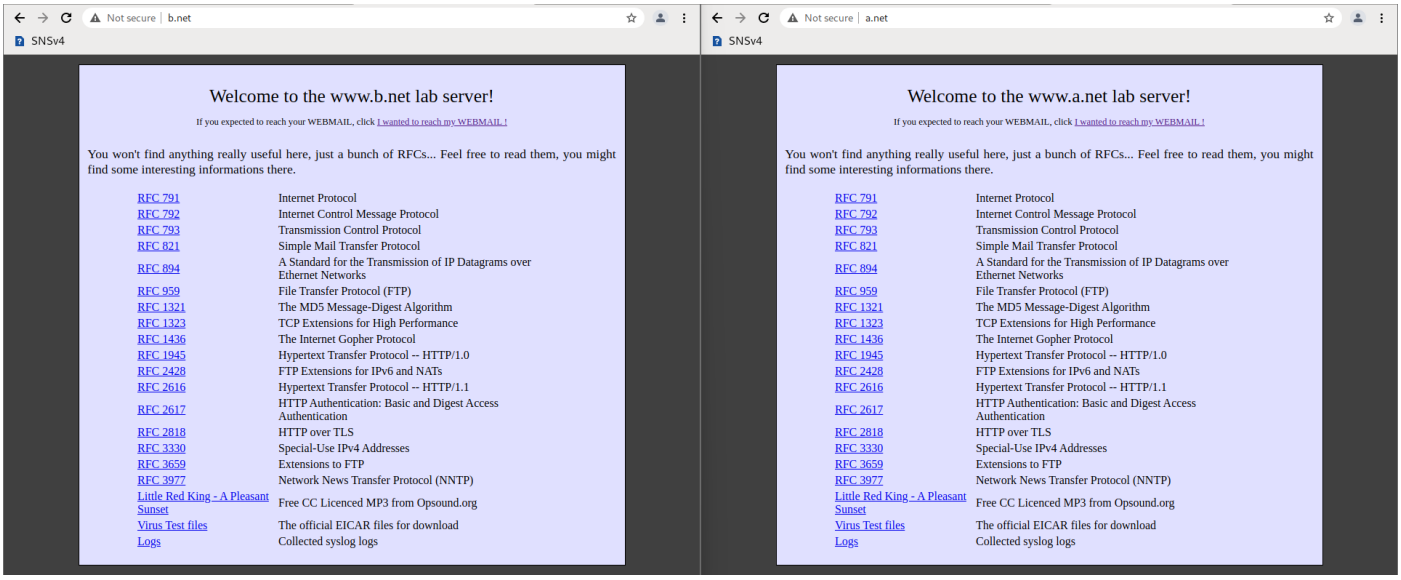
➢ J’ajoute les règles de filtrages adaptées :

➢ Je regarde que mes tunels sont bien fonctionels :





➢ Et enfin je test de me connecter de A sur b.net et de B vers a.net :



Quiz :

Q1– IPsec utilise TCP pour négocier la connexion, puisse envoie les données chiffrées grâce à UDP :

B. Faux

Q2–SHA1est un algorithme de hachage sûr pour les tunnels VPN :

B. Faux

Q3–Les VTI font partie du standardIKEv2 est ne sont pas disponibles sur IKEv1 :

B. Faux

Q4–Un tunnel IPsec garantit :

A. L'authentification

C. L'intégrité

D. La confidentialité

E. L'anti-rejeu

Q5–L'option keepalive permet au pare-feu de détecter des coupures de connexion :

B. Faux

Q6– La négociation d'un tunnel IPsec est initiée seulement s'il y a des données à envoyer dans le tunnel :

A. Vrai

Q7– Sans VTI, il est impossible de faire fonctionner deux tunnels entre les mêmes réseaux simultanément (pour un besoin de redondance par exemple) :

A. Vrai

Q8– Une route statique est nécessaire pour que le firewall puisse envoyer les paquets dans un tunnel IPsec :

B. Vrai seulement avec des VTI