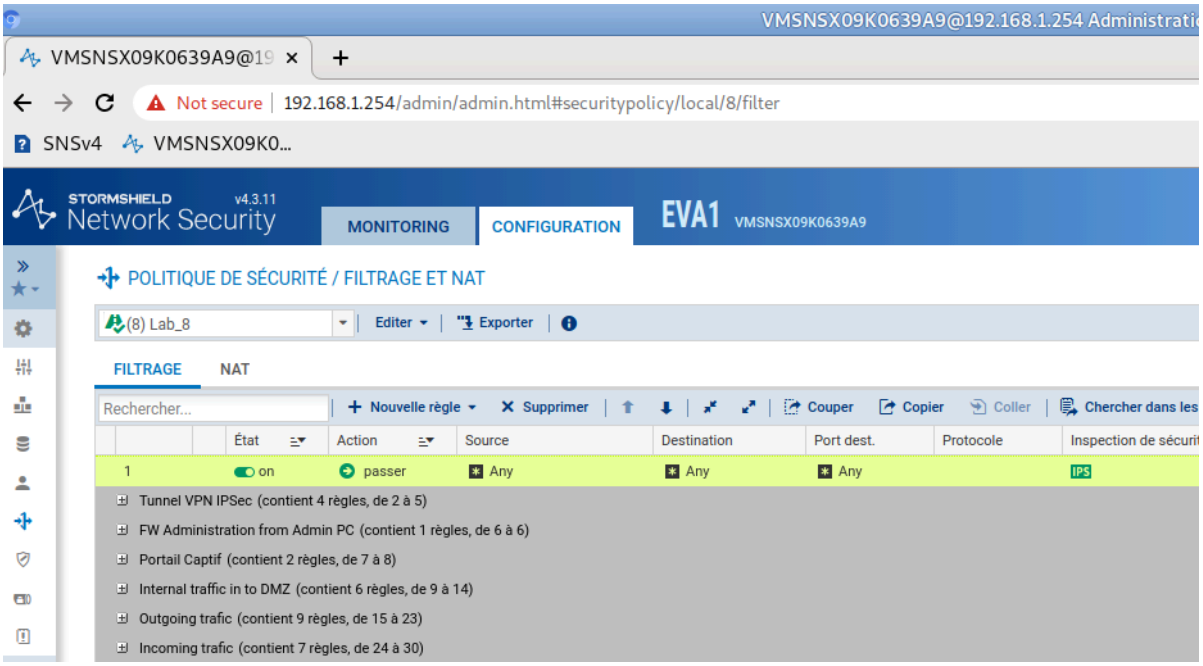
BTS 1 - Services Informatiques aux Organisations

BTS SIO SISR – Lab 8 StormShield

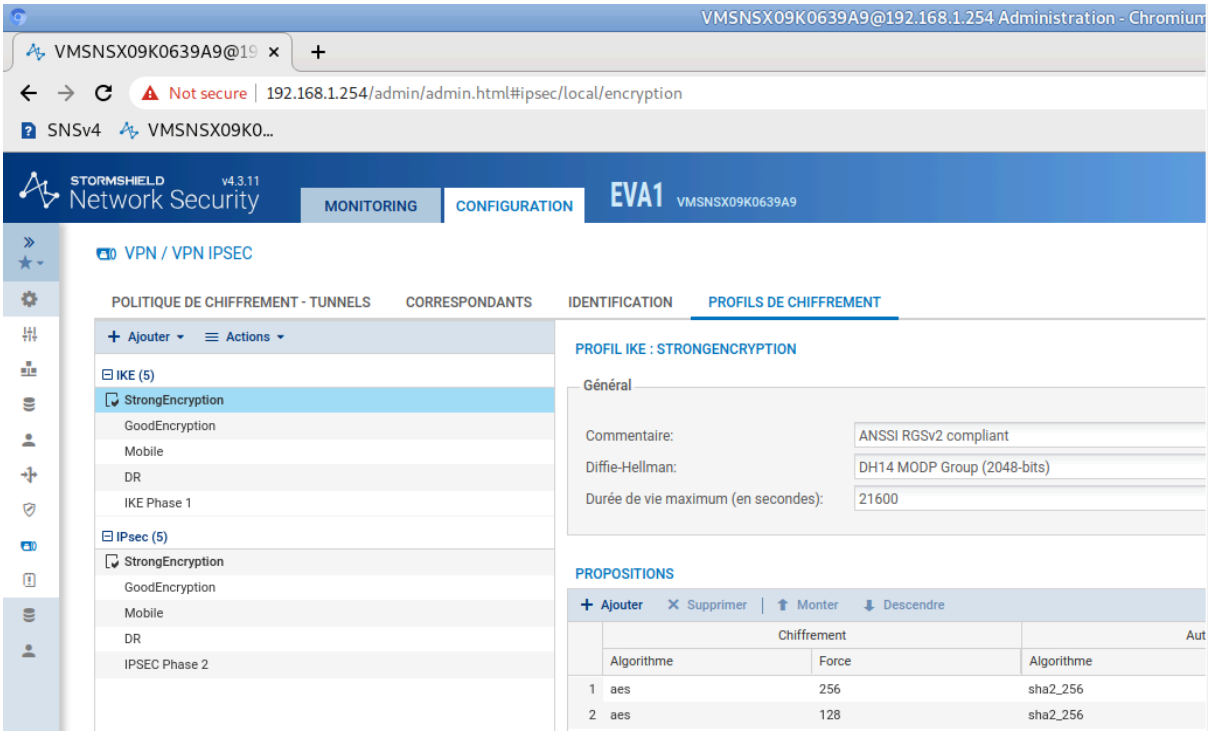
1. Les étapes effectuées sur le site A

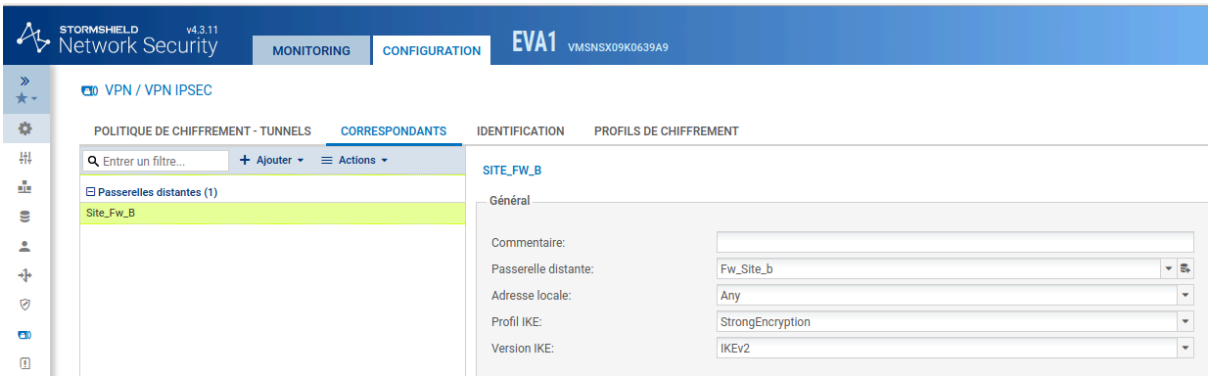
1.1 Ajout de la règle de filtrage Pass any any any en tête de la politique :



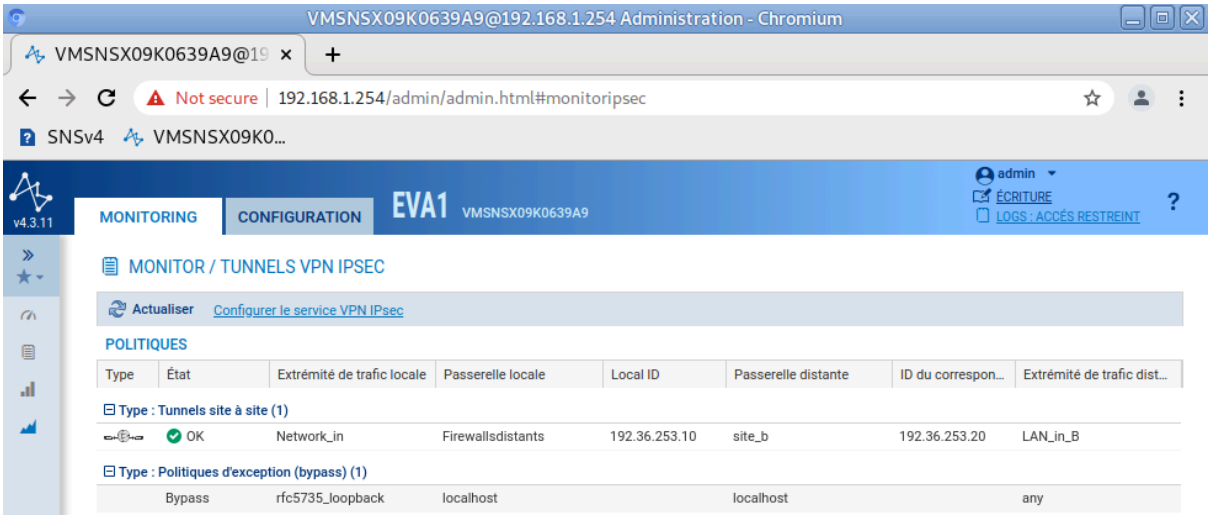
1.2 Configuration du tunnel IPSec pour le site distant

Visualisation de la IKE StrongEncryption :



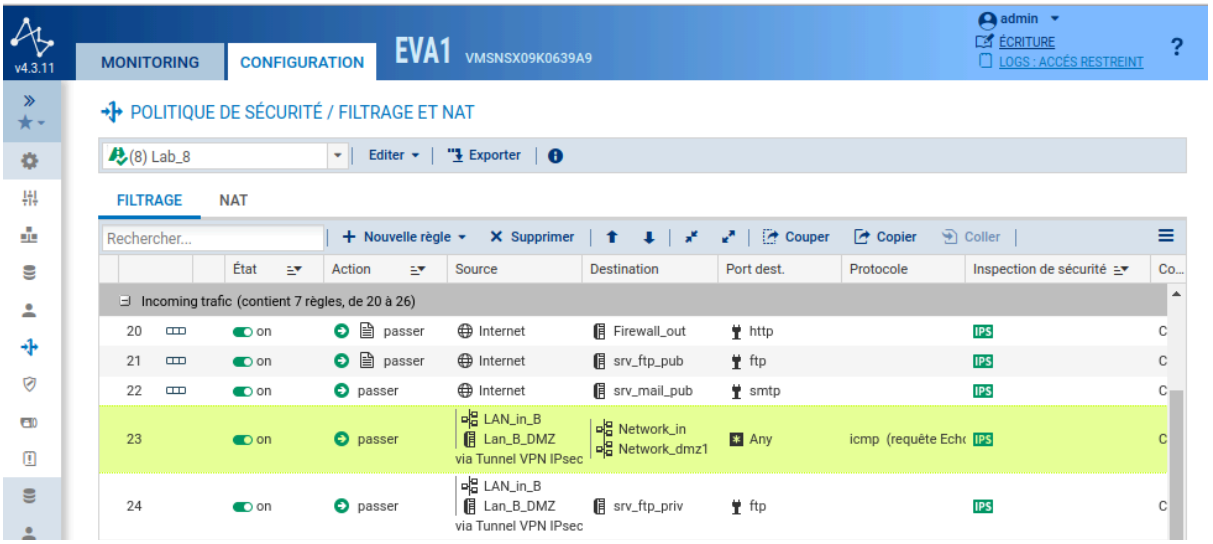


1.3 Visualisation du tunnel depuis le menu de supervision :



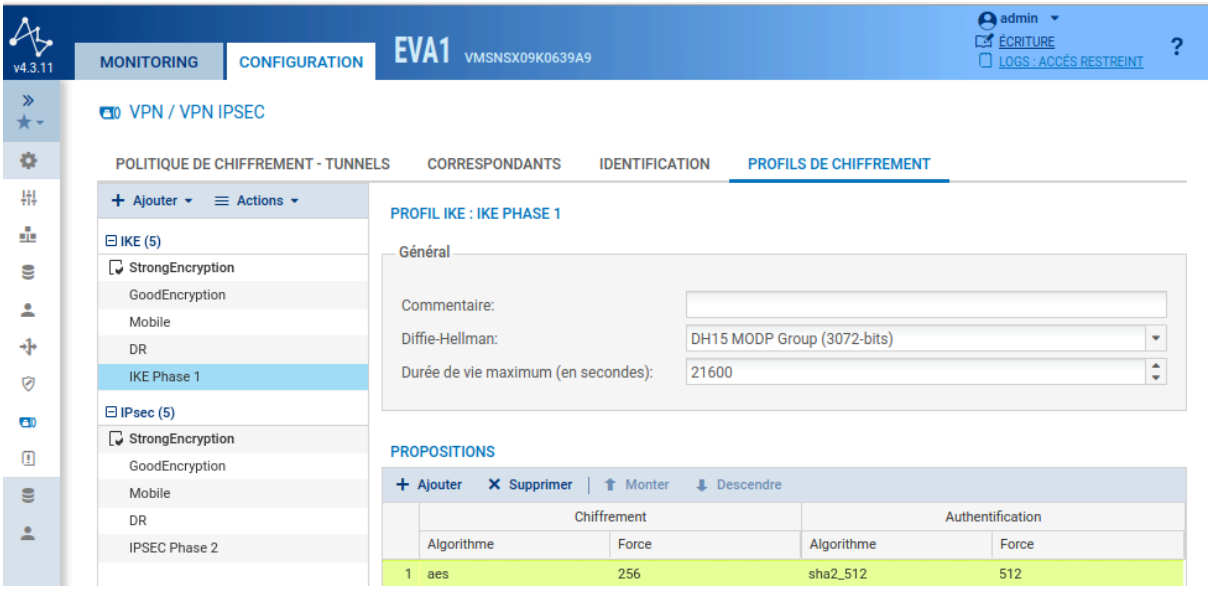
1.4 Réseaux DMZ vers le réseau IN et inversement :

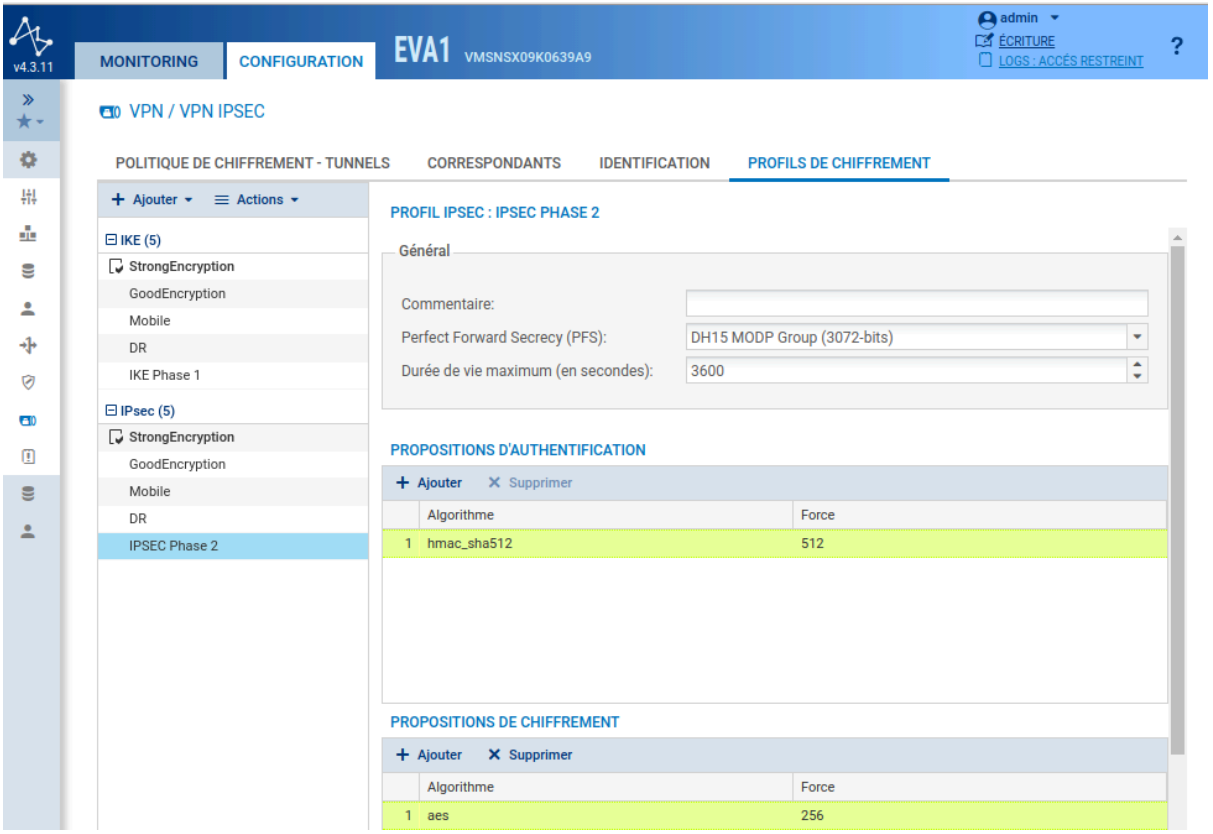
1.5 Ajout des règles de filtrages pour permettre l'accès et le ping au serveur FTP :



Sur le firewall du site B, ajout des règles de filtrage pour compléter l'accès :

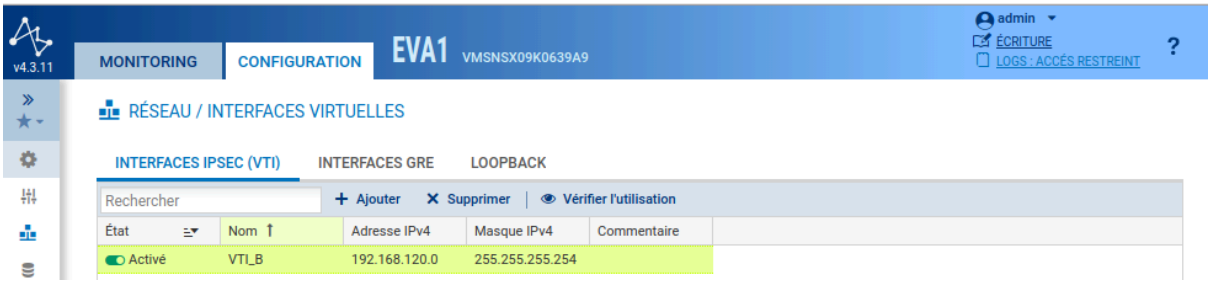
1.6 Création des profil IKE et IPSec :





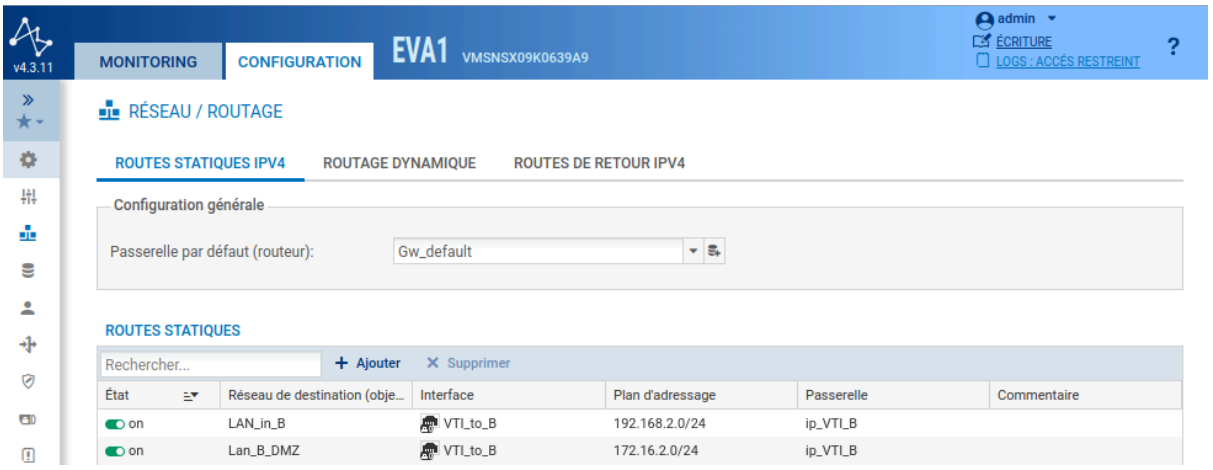
1.7 Changement du profil de chiffrement de StrongEncryption en IPSec Phase 2 et mise en place de l'IKE Phase 1 :

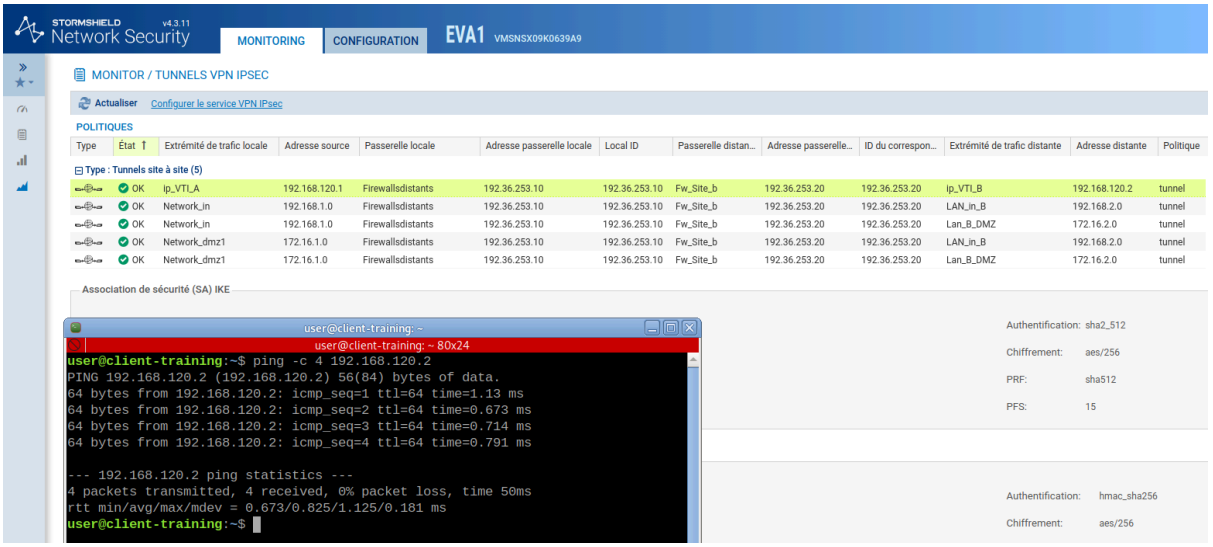
1.8 Création de la VTI pour le site distant :



Ajout des routes statiques pour accéder au réseau distants via la VTI locale et l'adresse IP de la VTI distante :

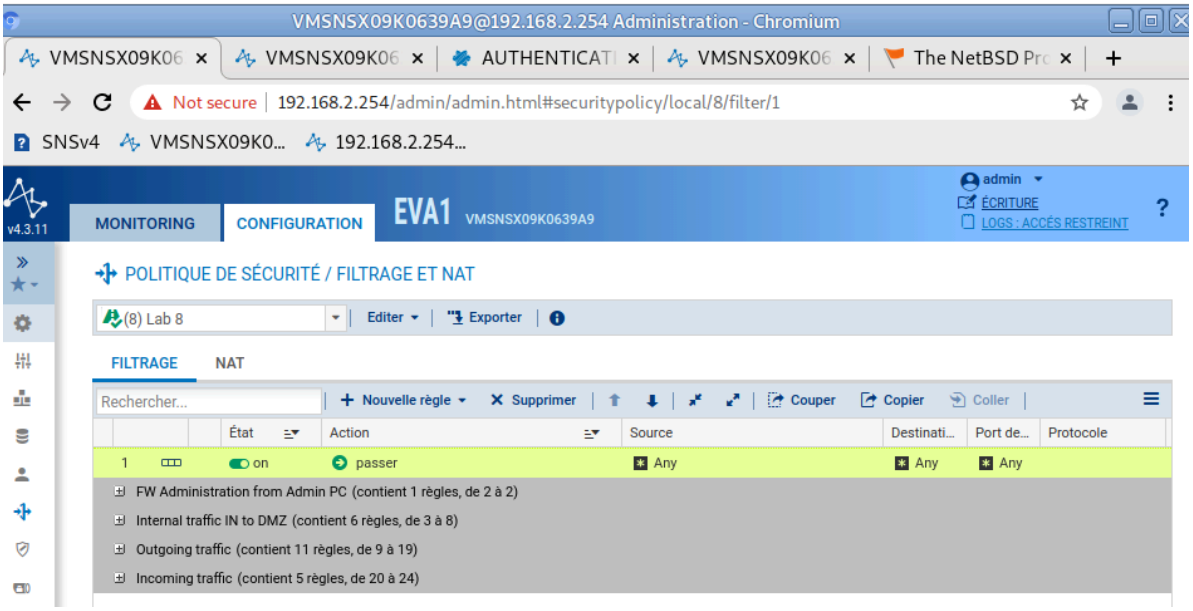
Modification des règles de filtrage pour indiquer la VTI comme interface source et destination pour le trafic transmis via le tunnel VPN IPSec :





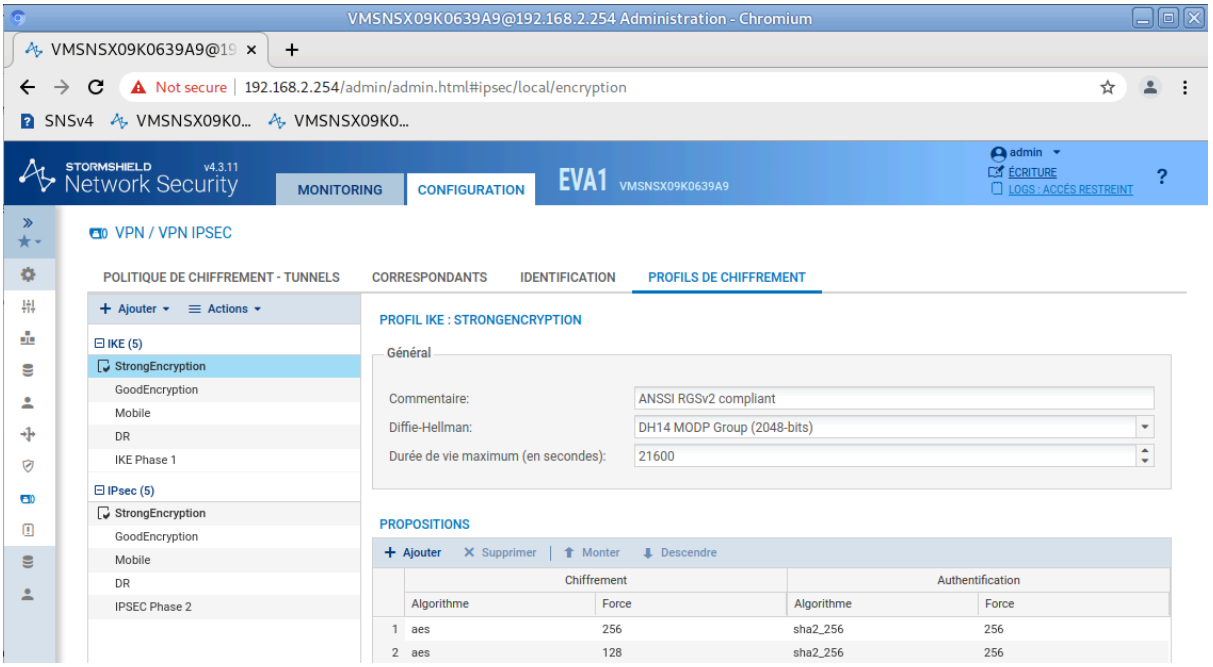
2. Les étapes effectuées sur le site B

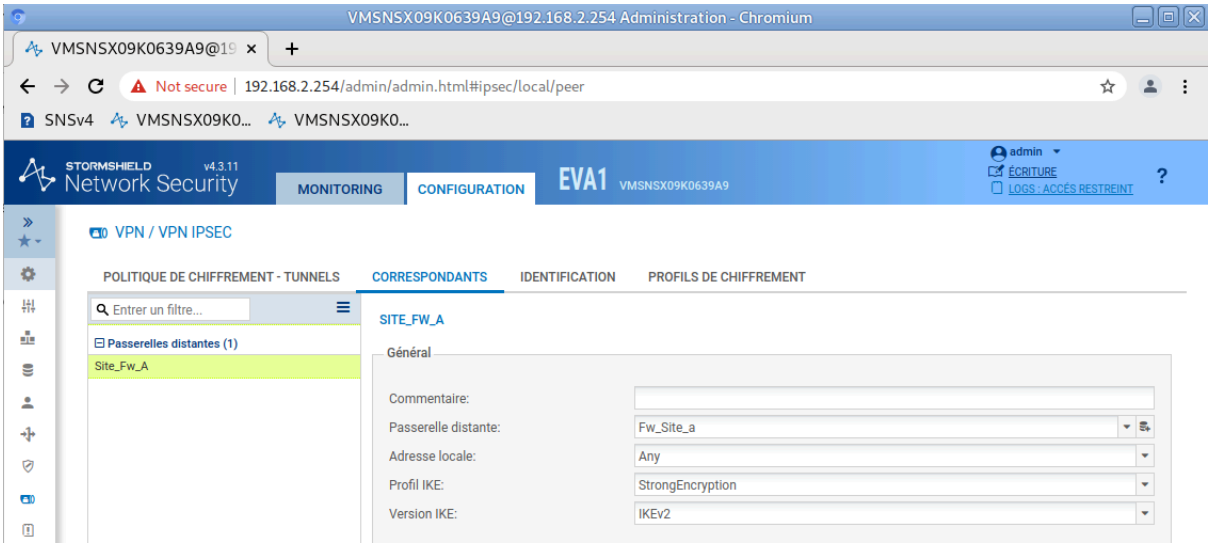
2.1 Ajout de la règle de filtrage Pass any any any en tête de la politique :



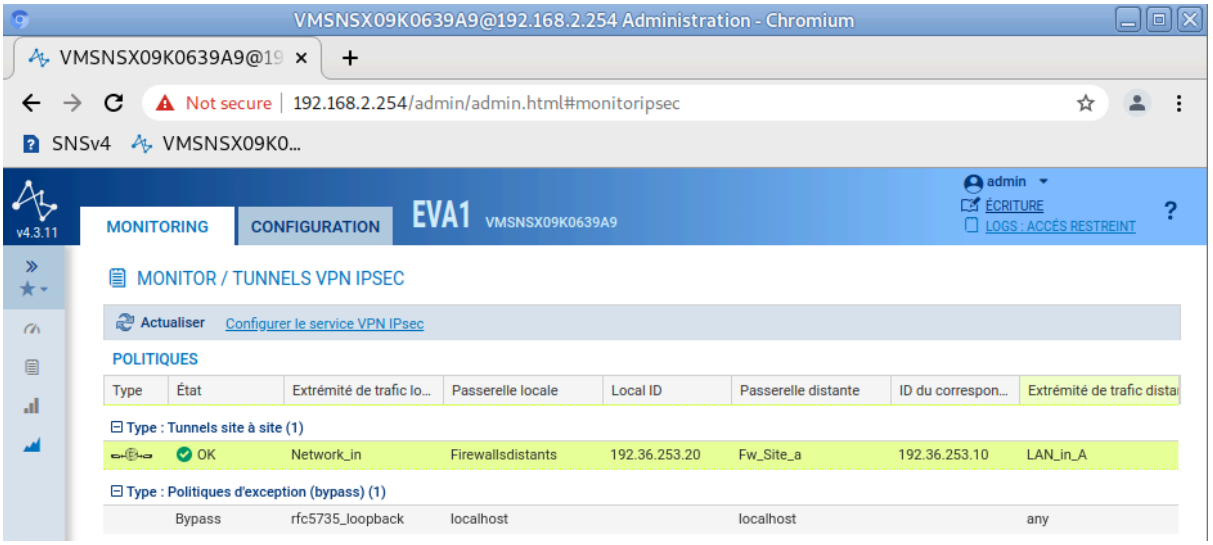
2.2 Configuration du tunnel IPSec pour le site distant :

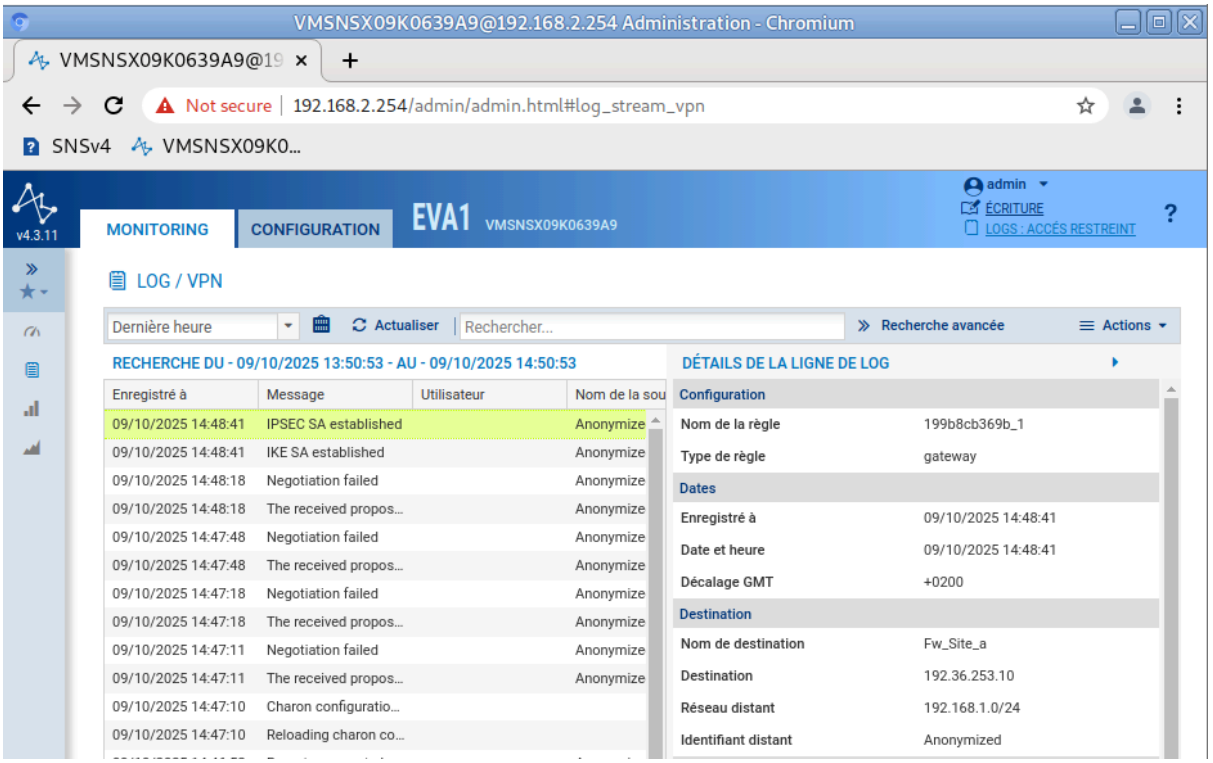
Visualisation de la IKE StrongEncryption :



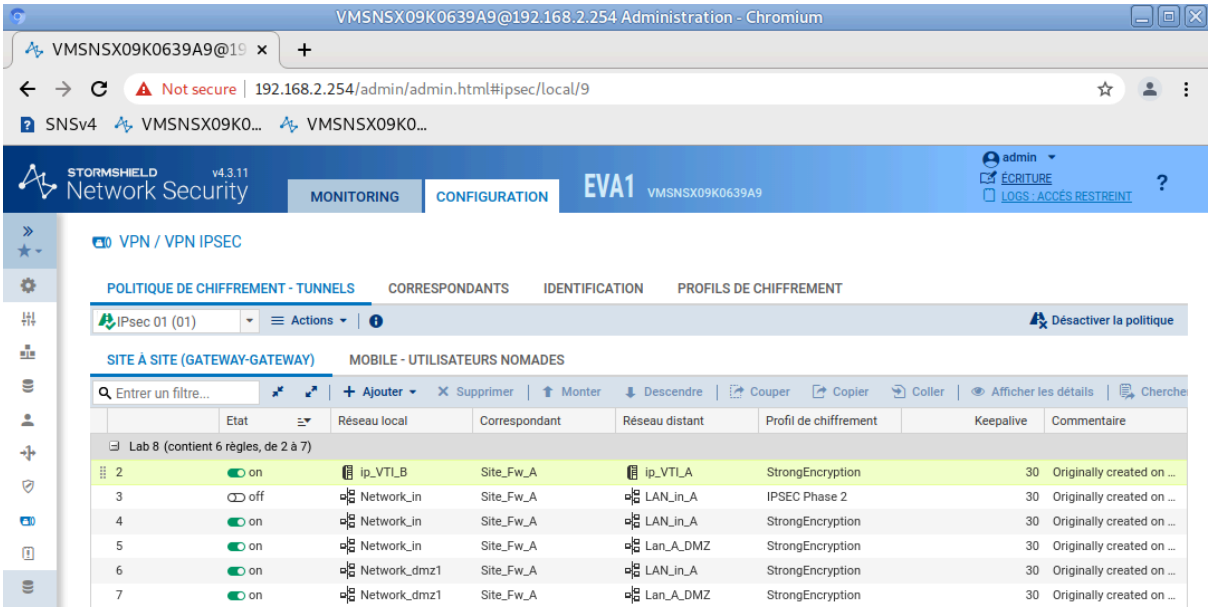


2.3 Visualisation du tunnel depuis le menu de supervision :

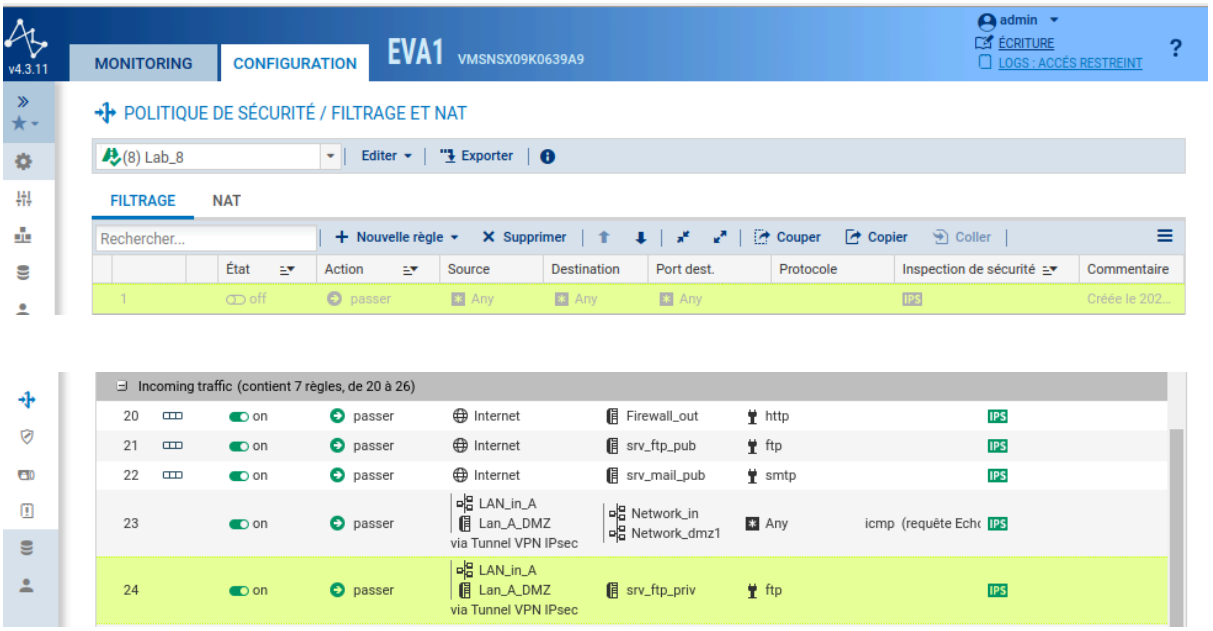




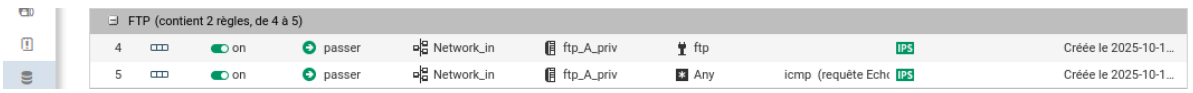
2.4 Réseaux DMZ vers le réseau IN et inversement :



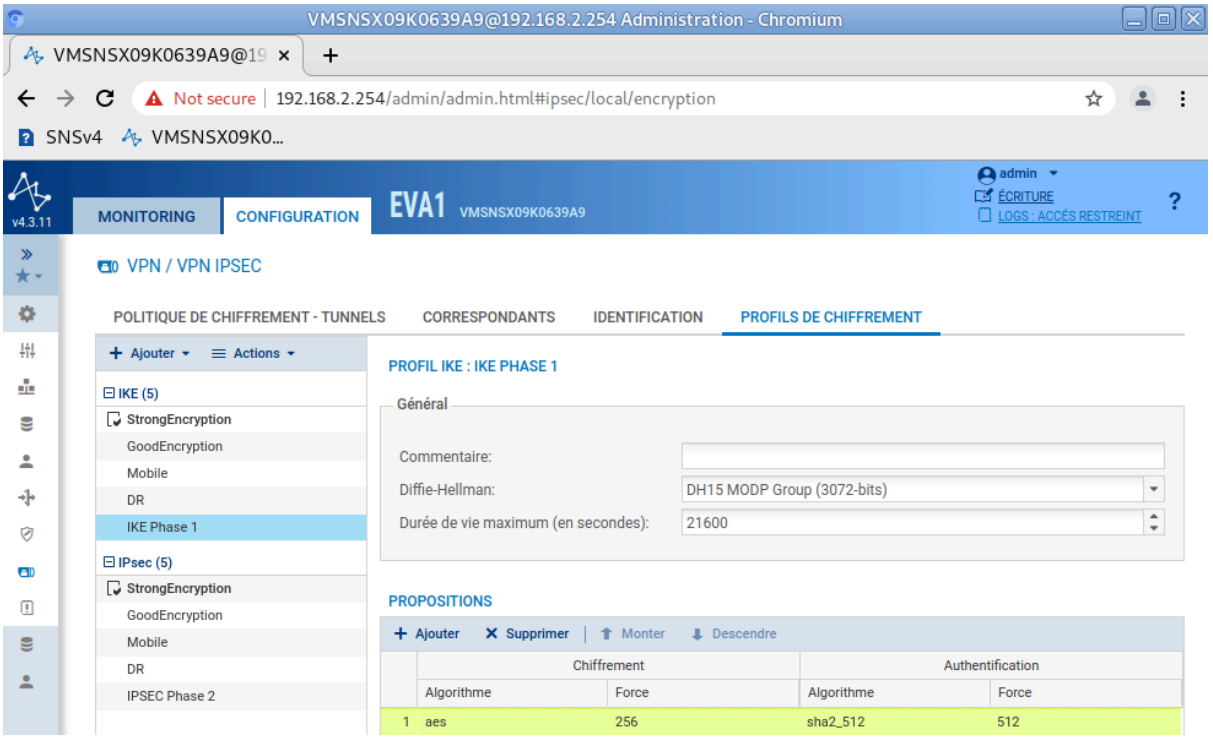
2.5 Ajout des règles de filtrages pour permettre l'accès et le ping au serveur FTP :

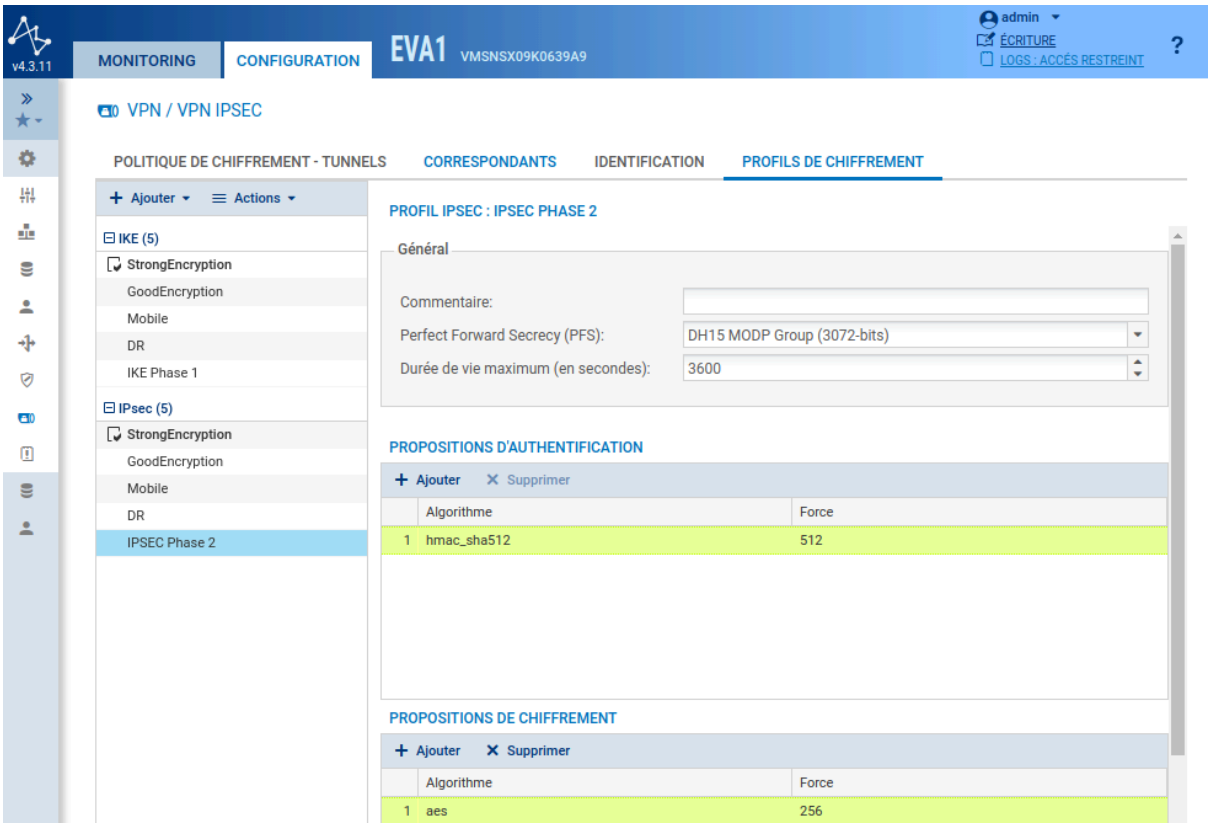


Sur le firewall du site A, ajout des règles de filtrage pour compléter l'accès :



2.6 Création des profil IKE et IPSec :



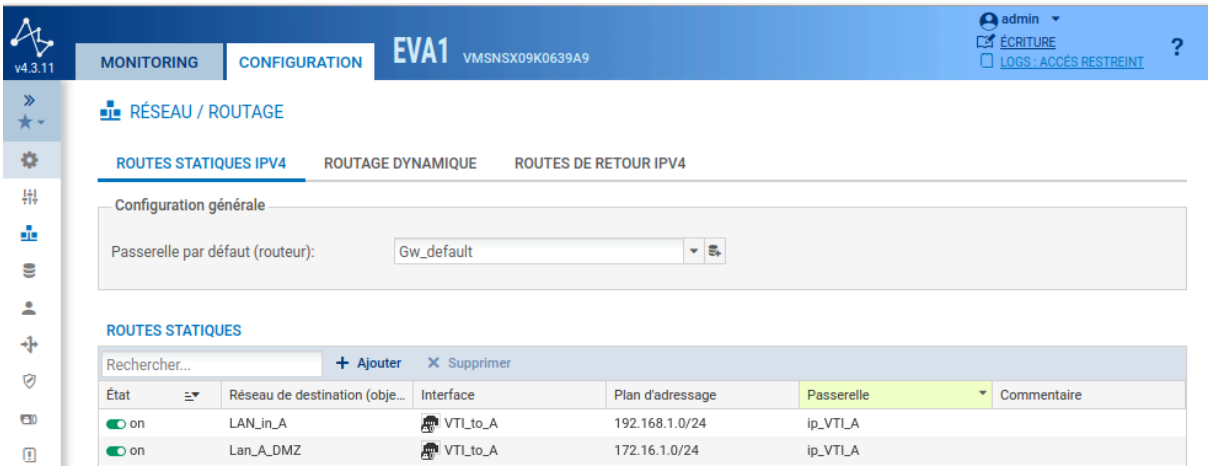


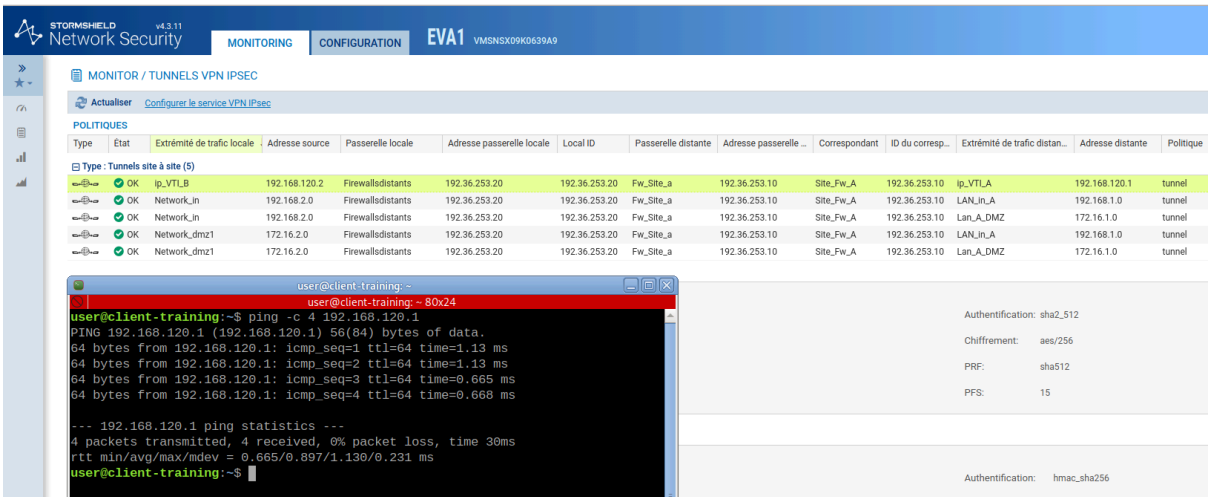
2.7 Changement du profil de chiffrement de StrongEncryption en IPSec Phase 2 et mise en place de l'IKE Phase 1 :

2.8 Création de la VTI pour le site distant :

Ajout des routes statiques pour accéder au réseau distants via la VTI locale et l'adresse IP de la VTI distante :

Modification des règles de filtrage pour indiquer la VTI comme interface source et destination pour le trafic transmis via le tunnel VPN IPSec :





3. Les questions

Q1 - IPsec utilise TCP pour négocier la connexion, puisse envoie les données chiffrées grâce à UDP :
A. Vrai
B. Faux

Q2 - SHA1 est un algorithme de hachage sûr pour les tunnel VPN :
A. Vrai
B. Faux

Q3 - Les VTI font partie du standard IKEv2 est ne sont pas disponibles sur IKEv1 :
A. Vrai
B. Faux

Q4 - Un tunnel IPsec garantit :
A. L'authentification
B. La qualité de service
C. L'intégrité
D. La confidentialité E. L'anti-rejeu F. La réception

Q5 - L'option keepalive permet au pare-feu de détecter des coupures de connexion :
A. Vrai
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
B. Faux

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
B. Faux

Q8 – Une route statique est nécessaire pour que le firewall puisse envoyer les paquets dans un tunnel IPsec :
A. Vrai dans tous les cas
B. Vrai seulement avec des VTI
C. Vrai seulement avec de la correspondance de politique (tunnel IPsec standard)
D. Faux dans tous les cas