

## BTS 1 - Services Informatiques aux Organisations

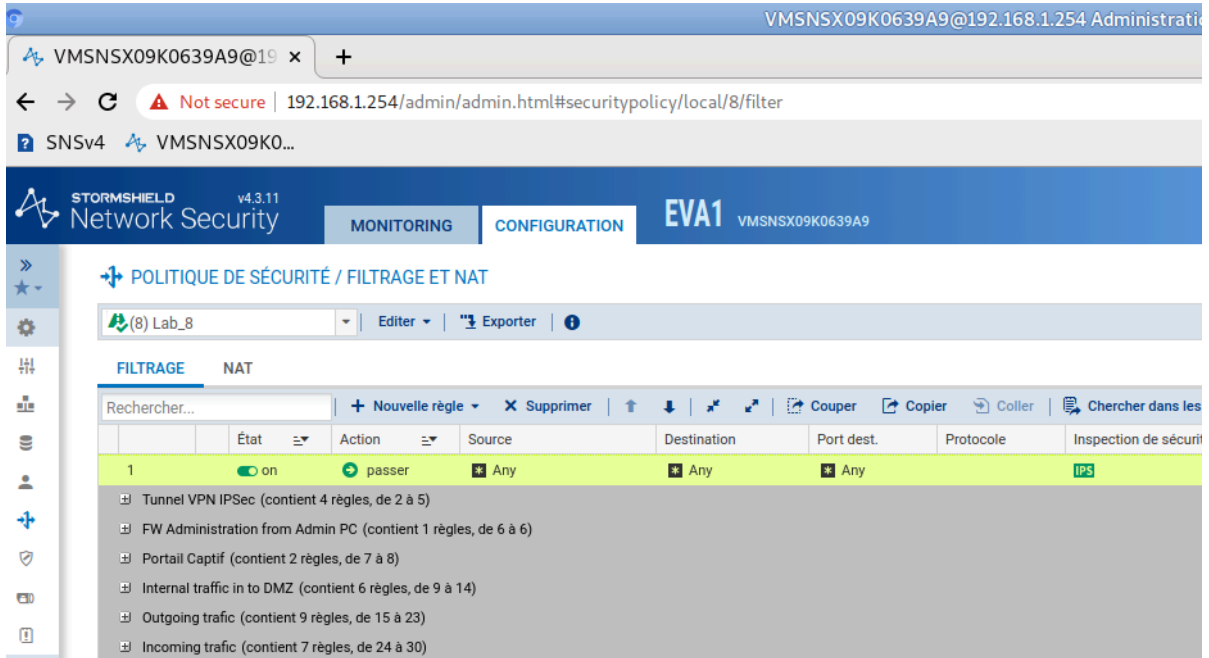


### BTS SIO SISR – Lab 8 StormShield

1. Les étapes effectuées sur le site A.....	1
2. Les étapes effectuées sur le site B.....	8
3. Les questions.....	15

# 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 :

The screenshot shows the Stormshield Network Security v4.3.11 administration interface. The browser address bar indicates the URL: 192.168.1.254/admin/admin.html#ipsec/local/encryption. The interface is in the 'CONFIGURATION' tab, specifically under 'VPN / VPN IPSEC' > 'PROFILS DE CHIFFREMENT'. The selected profile is 'PROFIL IKE : STRONGENCRYPTION'. The 'Général' section shows the following configuration:

- Commentaire: ANSSI RGSv2 compliant
- Diffie-Hellman: DH14 MODP Group (2048-bits)
- Durée de vie maximum (en secondes): 21600

The 'PROPOSITIONS' table below shows the encryption proposals:

+ Ajouter   X Supprimer   ↑ Monter   ↓ Descendre			
	Chiffrement		Aut
	Algorithme	Force	
1	aes	256	sha2_256
2	aes	128	sha2_256

The screenshot shows the Stormshield Network Security v4.3.11 administration interface. The browser address bar indicates the URL: 192.168.1.254/admin/admin.html#ipsec/local/encryption. The interface is in the 'CONFIGURATION' tab, specifically under 'VPN / VPN IPSEC' > 'CORRESPONDANTS'. The selected peer is 'SITE\_FW\_B'. The 'Général' section shows the following configuration:

- Commentaire: (empty)
- Passerelle distante: Fw\_Site\_b
- Adresse locale: Any
- Profil IKE: StrongEncryption
- Version IKE: IKEv2

1.3 Visualisation du tunnel depuis le menu de supervision :

The screenshot shows the 'MONITOR / TUNNELS VPN IPSEC' page. It features a table of active tunnels. The first tunnel is of type 'Tunnels site à site (1)' and is in an 'OK' state. It connects 'Network\_in' to 'Firewallsdistants' with local ID '192.36.253.10' and remote ID 'site\_b'. The remote gateway is '192.36.253.20' and the traffic interface is 'LAN\_in\_B'. A second tunnel of type 'Politiques d'exception (bypass) (1)' is also shown, with a 'Bypass' state and local ID 'rfc5735\_loopback'.

Type	État	Extrémité de trafic locale	Passerelle locale	Local ID	Passerelle distante	ID du correspon...	Extrémité de trafic dist...
Type : Tunnels site à site (1)							
↔	OK	Network_in	Firewallsdistants	192.36.253.10	site_b	192.36.253.20	LAN_in_B
Type : Politiques d'exception (bypass) (1)							
	Bypass	rfc5735_loopback	localhost		localhost		any

The screenshot shows the 'LOG / VPN' page with a search filter for '09/10/2025 13:49:30 - AU - 09/10/2025 14:49:30'. A log entry is highlighted: '09/10/2025 14:48:40 IPSEC SA established' by an 'Anonymized' user. To the right, the 'DÉTAILS DE LA LIGNE DE LOG' are shown, including configuration details like rule name '199b8c7bc54\_1', rule type 'gateway', and destination 'site\_b' at IP '192.36.253.20'.

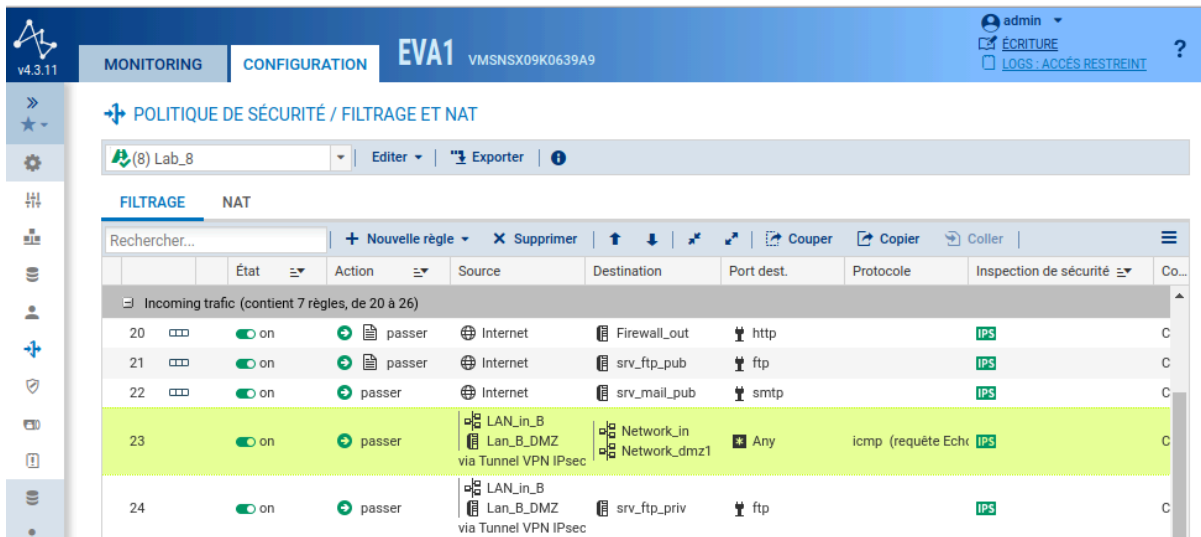
Enregistré à	Message	Utilisateur	Nom de la source
09/10/2025 14:48:40	IPSEC SA established	Anonymized	Anonymized
09/10/2025 14:48:40	IKE SA established	Anonymized	Anonymized
09/10/2025 14:48:39	Charon configuratio...		
09/10/2025 14:48:39	Unable to terminate ...		
09/10/2025 14:48:39	Received DELETE fo...	Anonymized	Anonymized
09/10/2025 14:48:39	Sending DELETE for ...	Anonymized	Anonymized
09/10/2025 14:48:39	Reloading charon co...		
09/10/2025 14:48:35	Negotiation failed	Anonymized	Anonymized
09/10/2025 14:48:35	IPSEC SA establish...	Anonymized	Anonymized
09/10/2025 14:48:35	Negotiation failed	Anonymized	Anonymized
09/10/2025 14:48:35	The received traffic ...	Anonymized	Anonymized
09/10/2025 14:48:18	No matching peer c...	Anonymized	Anonymized

1.4 Réseaux DMZ vers le réseau IN et inversement :

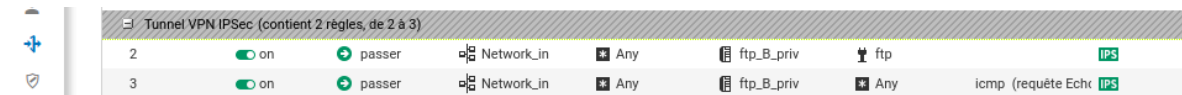
The screenshot shows the 'VPN / VPN IPSEC' configuration page. It displays a table of tunnels under the 'SITE À SITE (GATEWAY-GATEWAY)' section. Two tunnels are listed, both with a status of 'on'. Tunnel 2 connects 'Firewall\_VTL\_to\_B' to 'ip\_VTL\_B' using 'StrongEncryption'. Tunnel 3 connects 'Network\_in' to 'LAN\_in\_B' using 'IPSEC Phase 2'.

	Etat	Réseau local	Correspondant	Réseau distant	Profil de chiffreme...	Keepalive	Commentaire
Lab 8							
2	on	Firewall_VTL_to_B	Site_Fw_B	ip_VTL_B	StrongEncryption		Originally created ...
3	on	Network_in	Site_Fw_B	LAN_in_B	IPSEC Phase 2	30	Originally created ...

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 :

The screenshot shows the configuration page for 'PROFILS DE CHIFFREMENT' under 'VPN / VPN IPSEC'. The left sidebar lists various profiles, with 'IKE Phase 1' selected. The main content area shows the configuration for 'PROFIL IKE : IKE PHASE 1'.

**PROFILS DE CHIFFREMENT**

**PROFIL IKE : IKE PHASE 1**

Général

Commentaire:

Diffie-Hellman:

Durée de vie maximum (en secondes):

**PROPOSITIONS**

	Chiffrement		Authentification	
	Algorithme	Force	Algorithme	Force
1	aes	256	sha2_512	512

The screenshot shows the configuration page for 'PROFILS DE CHIFFREMENT' under 'VPN / VPN IPSEC'. The left sidebar lists various profiles, with 'IPSEC Phase 2' selected. The main content area shows the configuration for 'PROFIL IPSEC : IPSEC PHASE 2'.

**PROFILS DE CHIFFREMENT**

**PROFIL IPSEC : IPSEC PHASE 2**

Général

Commentaire:

Perfect Forward Secrecy (PFS):

Durée de vie maximum (en secondes):

**PROPOSITIONS D'AUTHENTIFICATION**

	Algorithme	Force
1	hmac_sha512	512

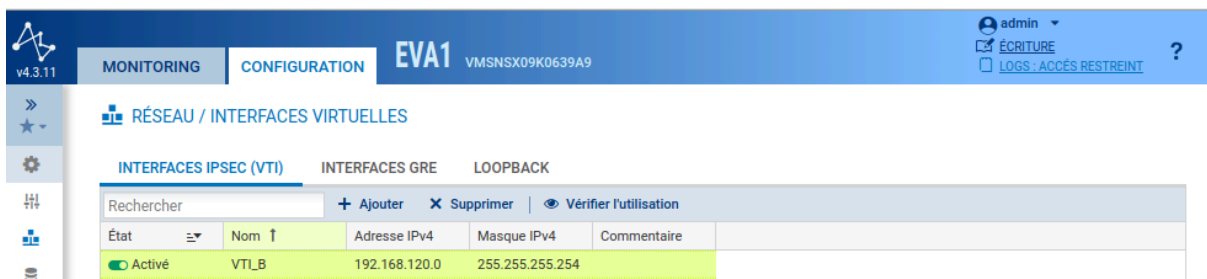
**PROPOSITIONS DE CHIFFREMENT**

	Algorithme	Force
1	aes	256

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 :

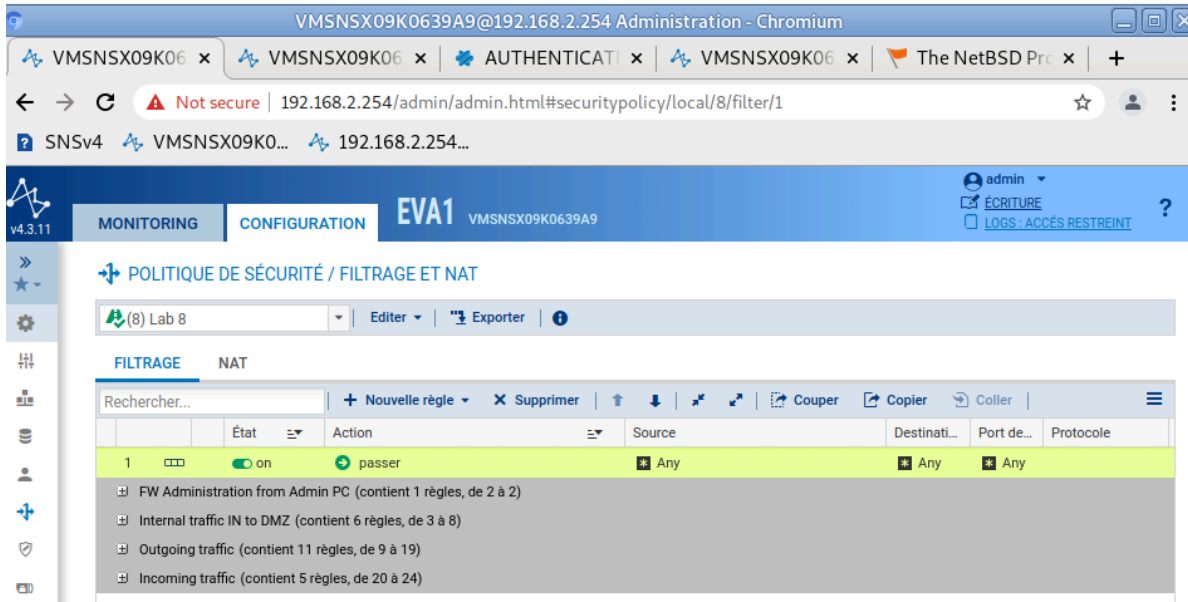


Ajout des routes statiques pour accéder au réseau distants via la VTI locale et l'adresse IP de la VTI distante :

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 :

The screenshot shows the Stormshield Network Security administration interface. The browser address bar indicates the URL: 192.168.2.254/admin/admin.html#ipsec/local/encryption. The interface is in French and shows the 'CONFIGURATION' tab. The left sidebar has 'VPN / VPN IPSEC' selected. The main content area is titled 'PROFILS DE CHIFFREMENT' and shows a list of profiles on the left, with 'StrongEncryption' selected. The right pane displays the configuration for 'PROFIL IKE : STRONGENCRIPTION'.

**PROFIL IKE : STRONGENCRIPTION**

Général

Commentaire: ANSSI RGSv2 compliant

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

Durée de vie maximum (en secondes): 21600

**PROPOSITIONS**

	Chiffrement		Authentification	
	Algorithme	Force	Algorithme	Force
1	aes	256	sha2_256	256
2	aes	128	sha2_256	256

The screenshot shows the Stormshield Network Security administration interface. The browser address bar indicates the URL: 192.168.2.254/admin/admin.html#ipsec/local/peer. The interface is in French and shows the 'CONFIGURATION' tab. The left sidebar has 'VPN / VPN IPSEC' selected. The main content area is titled 'CORRESPONDANTS' and shows a list of remote gateways on the left, with 'Site\_Fw\_A' selected. The right pane displays the configuration for 'SITE\_FW\_A'.

**SITE\_FW\_A**

Général

Commentaire:

Passerelle distante: Fw\_Site\_a

Adresse locale: Any

Profil IKE: StrongEncryption

Version IKE: IKEv2

2.3 Visualisation du tunnel depuis le menu de supervision :

The screenshot shows the 'MONITOR / TUNNELS VPN IPSEC' page in the administration interface. It features a table of active policies and a sidebar with navigation options.

Type	État	Extrémité de trafic lo...	Passerelle locale	Local ID	Passerelle distante	ID du correspon...	Extrémité de trafic dista
Type : Tunnels site à site (1)							
Network_in	OK	Firewallsdistant	192.36.253.20	Fw_Site_a	192.36.253.10	LAN_in_A	
Type : Politiques d'exception (bypass) (1)							
Bypass		rfc5735_loopback	localhost		localhost		any

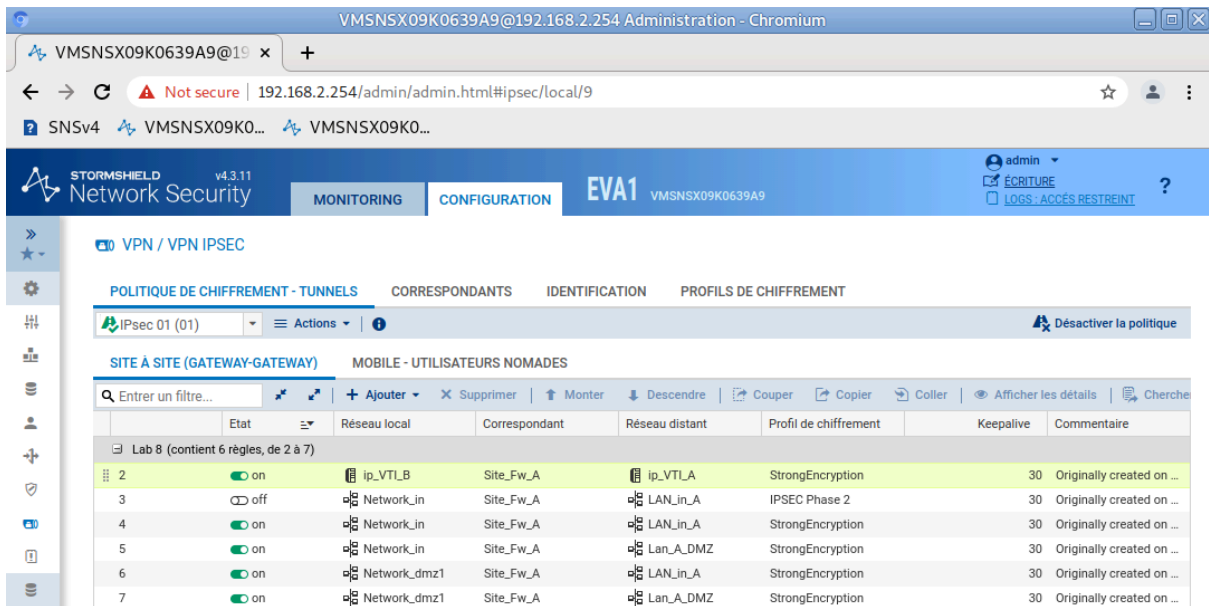
The screenshot shows the 'LOG / VPN' page with a search filter for the time range '09/10/2025 13:50:53 - AU - 09/10/2025 14:50:53'. A log entry is highlighted, and its details are shown on the right.

Enregistré à	Message	Utilisateur	Nom de la sou
09/10/2025 14:48:41	IPSEC SA established	Anonymize	
09/10/2025 14:48:41	IKE SA established	Anonymize	
09/10/2025 14:48:18	Negotiation failed	Anonymize	
09/10/2025 14:48:18	The received propos...	Anonymize	
09/10/2025 14:47:48	Negotiation failed	Anonymize	
09/10/2025 14:47:48	The received propos...	Anonymize	
09/10/2025 14:47:18	Negotiation failed	Anonymize	
09/10/2025 14:47:18	The received propos...	Anonymize	
09/10/2025 14:47:11	Negotiation failed	Anonymize	
09/10/2025 14:47:11	The received propos...	Anonymize	
09/10/2025 14:47:10	Charon configuratio...		
09/10/2025 14:47:10	Reloading charon co...		

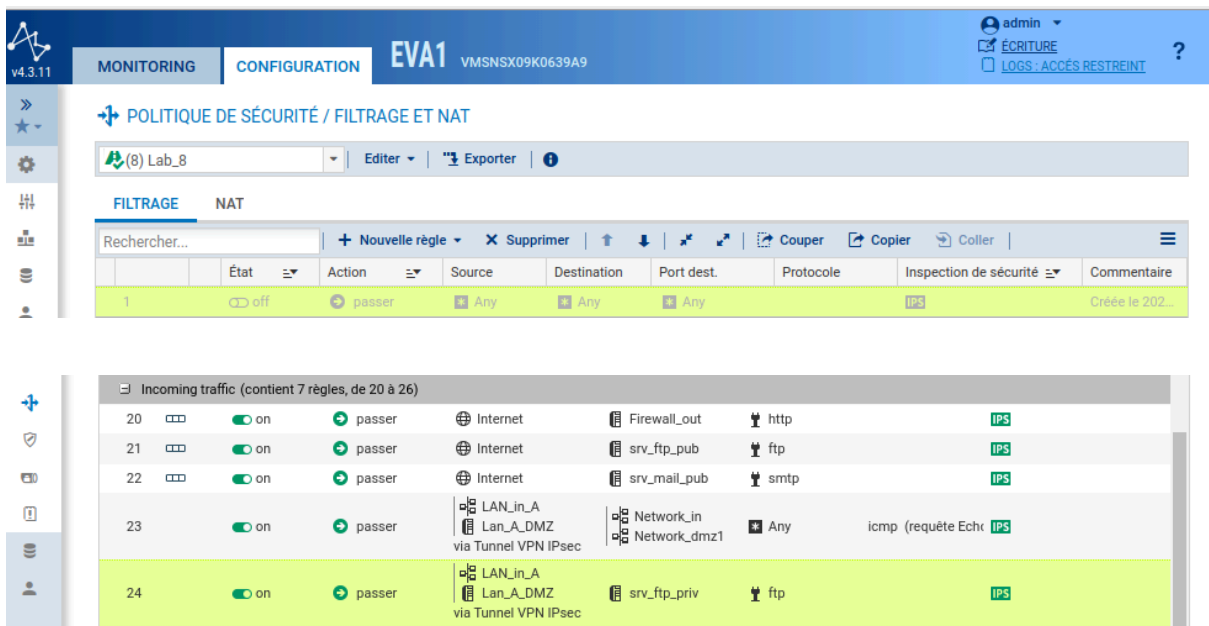
  

DÉTAILS DE LA LIGNE DE LOG	
<b>Configuration</b>	
Nom de la règle	199b8cb369b_1
Type de règle	gateway
<b>Dates</b>	
Enregistré à	09/10/2025 14:48:41
Date et heure	09/10/2025 14:48:41
Décalage GMT	+0200
<b>Destination</b>	
Nom de destination	Fw_Site_a
Destination	192.36.253.10
Réseau distant	192.168.1.0/24
Identifiant distant	Anonymized

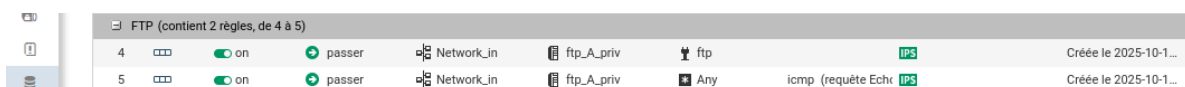
2.4 Réseaux DMZ vers le réseau IN et inversement :



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 :

The screenshot shows the configuration page for 'PROFILS DE CHIFFREMENT' under 'VPN / VPN IPSEC'. The left sidebar lists IKE and IPsec profiles. The main area is for 'PROFIL IKE : IKE PHASE 1'.

**PROFILS DE CHIFFREMENT**

**PROFIL IKE : IKE PHASE 1**

Général

Commentaire:

Diffie-Hellman:

Durée de vie maximum (en secondes):

**PROPOSITIONS**

		Chiffrement		Authentification	
	Algorithme	Force	Algorithme	Force	
1	aes	256	sha2_512	512	

The screenshot shows the configuration page for 'PROFILS DE CHIFFREMENT' under 'VPN / VPN IPSEC'. The left sidebar lists IKE and IPsec profiles. The main area is for 'PROFIL IPSEC : IPSEC PHASE 2'.

**PROFILS DE CHIFFREMENT**

**PROFIL IPSEC : IPSEC PHASE 2**

Général

Commentaire:

Perfect Forward Secrecy (PFS):

Durée de vie maximum (en secondes):

**PROPOSITIONS D'AUTHENTIFICATION**

	Algorithme	Force
1	hmac_sha512	512

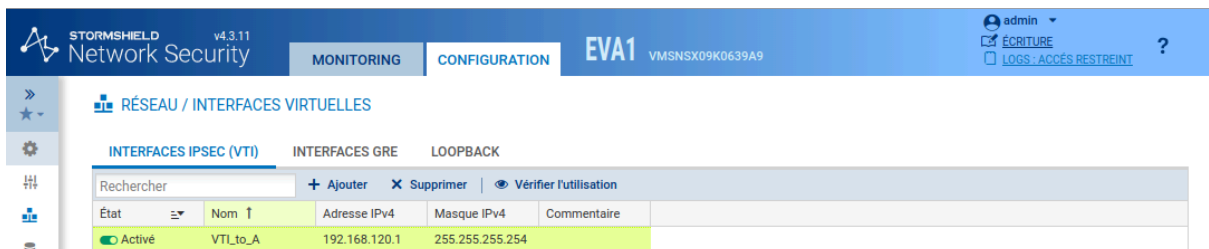
**PROPOSITIONS DE CHIFFREMENT**

	Algorithme	Force
1	aes	256

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



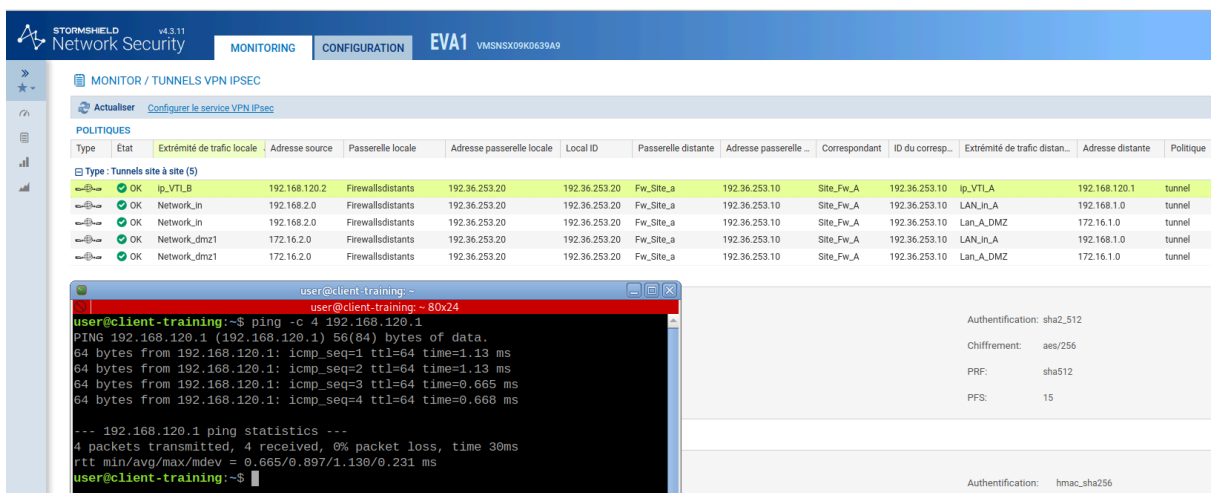
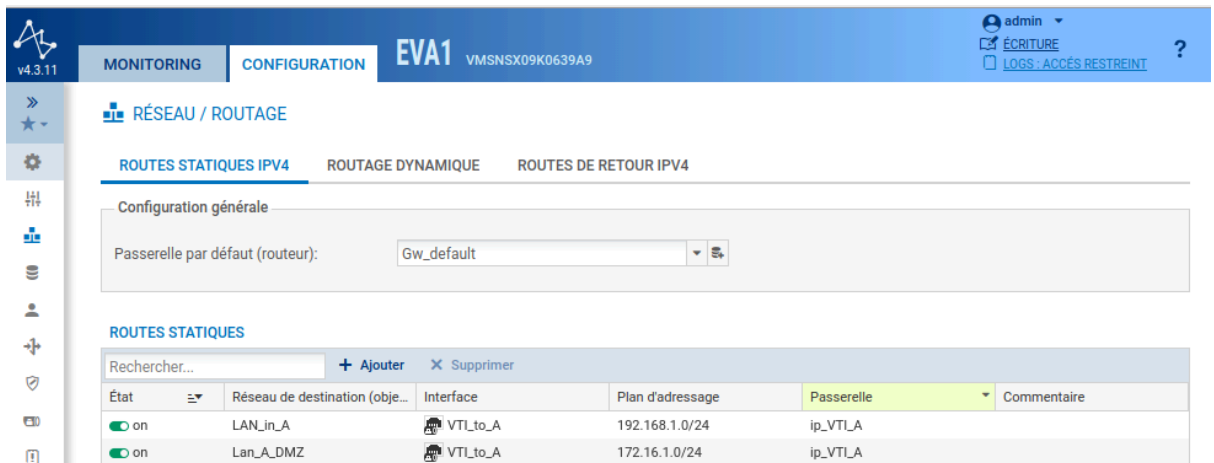
2.8 Création de la VTI pour le site distant :



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, puis envoie les données chiffrées grâce à UDP :

A. Vrai

**B. Faux**

Q2 - SHA1 est un algorithme de hachage sûr pour les tunnels VPN :

A. Vrai

**B. Faux**

Q3 - Les VTI font partie du standard IKEv2 et 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