

Lab 8 – VPN IPsec (Site à site)

Table des matières :

1. Ajout d'une règle de filtrage générale.....	2
2. Configuration d'un tunnel IPsec avec authentification PSK.....	3
3. Génération de trafic et observation des négociations de tunnel.....	5
4. Extension du tunnel aux réseaux internes et activation du keep-alive.....	7
5. Application de nouvelles règles de filtrage spécifiques.....	9
6. Création de nouveaux profils de chiffrement personnalisés.....	11
7. Application des nouveaux profils et tests de connectivité.....	14
8. Mise en place d'un tunnel basé sur des interfaces VTI.....	18

1. Ajout d'une règle de filtrage générale

- Nous avons commencé par créer une règle de filtrage « Pass any any any » placée en tête de la politique existante.

Cette règle permet de laisser transiter tous les flux le temps de la configuration du tunnel VPN IPsec, afin d'éviter tout blocage lors des phases de test et de négociation.

The screenshot displays the Stormshield Network Security v4.3.11 interface. The left sidebar shows the 'CONFIGURATION' menu with options like 'Rechercher...', 'SYSTÈME', 'Configuration', 'Administrateurs', 'Licence', 'Maintenance', 'Active Update', and 'Haute disponibilité'. The main area is titled 'POLITIQUE DE SÉCURITÉ / FILTRAGE ET NAT' and shows a configuration for 'Lab_8'. A table of filtering rules is visible, with the first rule highlighted in red. This rule is named '1', is 'on', has an action of 'passer', and source, destination, and port are all set to 'Any'. Below the table, there are links to view specific rule sets: 'FW Administration from Admin PC (contient 1 règles, de 2 à 2)', 'internal traffic IN to DMZ (contient 6 règles, de 3 à 8)', 'Outgoing traffic (contient 12 règles, de 9 à 20)', and 'incoming traffic (contient 6 règles, de 21 à 26)'.

	État	Action	Source	Destination	Port dest.	Protocole	Inspection de sécurité	Commentaire
1	on	passer	Any	Any	Any		IPsec	Créée le 2025-10-05 ...

2. Configuration d'un tunnel IPsec avec authentification PSK

▪ J'ai ensuite configuré un tunnel IPsec site à site entre notre réseau interne 192.168.x.0/24 et celui du site distant.

Pour cela, nous avons utilisé une clé pré-partagée (PSK) comme méthode d'authentification, avec les profils de chiffrement par défaut (StrongEncryption).

Cette étape établit la première liaison sécurisée entre les deux réseaux.

CRÉER UNE PASSERELLE DISTANTE

IDENTIFICATION DU CORRESPONDANT - ASSISTANT DE CRÉATION DE CORRESPONDANT

Type d'authentification: ☐ Certificat ☒ Clé pré-partagée (PSK)

Certificat: x

Autorité de confiance: x

Clé pré-partagée (PSK):

Confirmer:

Saisir la clé en caractères ASCII: ☒

[X ANNULER](#)[« PRÉCÉDENT](#)[» SUIVANT](#)

ASSISTANT DE POLITIQUE VPN IPSEC



Ressources locales:

x

Choix du correspondant:

x

Réseaux distants:

x

[X ANNULER](#)[✓ TERMINER](#)

Q Entrer un filtre...

Ajouter

Supprimer

Monter

Descendre

Couper

Copier

Coller

	Etat	Réseau local	Correspondant	Réseau distant	Profil de chiffre...	Keepalive	Commentaire
1	 on	 Network_in	Site_Fw_A	 Net_in_A	StrongEncryption		Originally creat...

3. Génération de trafic et observation des négociations de tunnel

▪ Afin de vérifier le bon fonctionnement du tunnel, nous avons généré du trafic entre les deux extrémités (par exemple via un ping entre deux machines internes).

J'ai ensuite observé les journaux IPsec et les menus de supervision pour suivre la négociation des phases IKE et l'établissement du tunnel IPsec.

```

user@client-training: ~
user@client-training: ~ 80x24
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=2 ttl=64 time=72.2 ms
64 bytes from 192.168.1.2: icmp_seq=3 ttl=64 time=74.5 ms
64 bytes from 192.168.1.2: icmp_seq=4 ttl=64 time=49.0 ms
64 bytes from 192.168.1.2: icmp_seq=5 ttl=64 time=74.1 ms
64 bytes from 192.168.1.2: icmp_seq=6 ttl=64 time=84.1 ms
64 bytes from 192.168.1.2: icmp_seq=7 ttl=64 time=66.3 ms
^C
--- 192.168.1.2 ping statistics ---
7 packets transmitted, 6 received, 14.2857% packet loss, time 97ms
rtt min/avg/max/mdev = 49.021/70.022/84.135/10.766 ms
user@client-training:~$

```

MONITORING CONFIGURATION EVA1 VMSNSX09K0639A9 admin ÉCRITURE LOGS : ACCÈS COMPLET

MONITOR / TUNNELS VPN IPSEC

Actualiser Configurer le service VPN IPsec

POLITIQUES

Type	État	Extrémité de trafic loc...	Passerelle locale	Local ID	Passerelle distante	ID du correspon...	Extrémité de trafic dis...
Type : Tunnels site à site (1)							
↔	OK	Network_in	Firewall_out	192.36.253.20	Fw_A	192.36.253.10	Lan_in_A
Type : Politiques d'exception (bypass) (1)							
Bypass		rfc5735_loopback	localhost		localhost		any

v4.3.11

»

★

MONITORING

CONFIGURATION

EVA1

VMSNSX09K0639A9

admin

ÉCRITURE

LOGS : ACCÈS COMPLET

?

LOG / VPN

Dernière heure

Actualiser

Rechercher...

Recherche avancée

Actions

RECHERCHE DU - 06/10/2025 11:40:46 - AU - 06/10/2025 12:40:46

Enregistré à	Message	Utilisateur	Nom de la source
06/10/2025 12:07:38	IPSEC SA established	Anonymized	
06/10/2025 12:07:38	IKE SA established	Anonymized	
06/10/2025 11:58:40	Charon daemon star...		
06/10/2025 11:58:40	Charon configuratio...		
06/10/2025 11:58:40	Reloading charon co...		

DÉTAILS DE LA LIGNE DE LOG

Configuration

Nom de la règle

199b8840347_1

Type de règle

gateway

Dates

Enregistré à

06/10/2025 12:07:38

Metreau Nicolas - Lab 8 - Page 6

4. Extension du tunnel aux réseaux internes et activation du keep-alive

- Nous avons modifié la configuration pour relier les réseaux internes IN et DMZ de notre site à ceux du site distant.

Cette étape étend la portée du tunnel afin de permettre la communication complète entre les deux infrastructures.

Ensuite, j'ai activé la fonction keep-alive pour maintenir le tunnel actif même en absence de trafic, garantissant ainsi une meilleure stabilité.

PROPRIÉTÉS

Nom de l'objet:

Net_DMZ_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:

PROPRIÉTÉS

Nom de l'objet:

Net_DMZ_A

Adresses IPv4

Adresse IP de réseau:

172.16.1.0/24

Exemple 192.168.0.0/16 ou 192.168.0.0/255.255.0.0

Commentaire:

Q Entrer un filtre...								
+ Ajouter X Supprimer ↑ Monter ↓ Descendre Couper Copier Coller Afficher les détails								
	Etat	Réseau local	Correspondant	Réseau distant	Profil de chiffrement	Keepalive	Commentaire	
1	on	Network_in	Site_Fw_A	Net_in_A	StrongEncryption	30	Originally created on ...	
2	on	Network_in	Site_Fw_A	Net_DMZ_A	StrongEncryption	30	Originally created on ...	
3	on	Network_dmz1	Site_Fw_A	Net_in_A	StrongEncryption	30	Originally created on ...	
4	on	Network_dmz1	Site_Fw_A	Net_DMZ_A	StrongEncryption	30	Originally created on ...	

SITE A SITE (GATEWAY-GATEWAY)

MOBILE - UTILISATEURS NOMADES

Q Entrer un filtre...

+ Ajouter

X Supprimer

↑ Monter

↓ Descendre

✂ Couper

📋 Copier

📄 Coller

	Etat	Réseau local	Correspondant	Réseau distant	Profil de chiffr...	Keepalive	Commentaire
1	on	Network_in	Site_fw_B	Net_in_B	StrongEncryption	30	Originally crea...
2	on	Network_in	Site_fw_B	Net_DMZ_B	StrongEncryption	30	Originally crea...
3	on	Network_dmz1	Site_fw_B	Net_in_B	StrongEncryption	30	Originally crea...
4	on	Network_dmz1	Site_fw_B	Net_DMZ_B	StrongEncryption	30	Originally crea...

```

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=89.5 ms
64 bytes from 172.16.2.12: icmp_seq=2 ttl=64 time=94.1 ms
64 bytes from 172.16.2.12: icmp_seq=3 ttl=64 time=84.3 ms
64 bytes from 172.16.2.12: icmp_seq=4 ttl=64 time=75.5 ms
^C
--- 172.16.2.12 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 7ms
rtt min/avg/max/mdev = 75.485/85.847/94.115/6.921 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=60.1 ms
64 bytes from 172.16.1.12: icmp_seq=2 ttl=64 time=93.4 ms
64 bytes from 172.16.1.12: icmp_seq=3 ttl=64 time=83.3 ms
64 bytes from 172.16.1.12: icmp_seq=4 ttl=64 time=83.1 ms
^C
--- 172.16.1.12 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 19ms
rtt min/avg/max/mdev = 60.089/79.989/93.433/12.223 ms
user@client-training:~$

```



STORMSHIELD

Network Security

v4.3.11

MONITORING

CONFIGURATION

EVA1

VMSNSX09K0639A9

admin

ÉCRITURE

LOGS - ACCÈS COMPLET

?

LOG / VPN

Dernière heure

Actualiser

Rechercher...

Recherche avancée

Actions

RECHERCHE DU - 06/10/2025 12:06:56 - AU - 06/10/2025 13:06:56

Enregistré à	Message	Utilisateur	Nom de la source	Réseau local	Nom de de
06/10/2025 13:02:10	IPSEC SA established	Anonymized	172.16.2.0/24	Fw_A	
06/10/2025 13:02:10	IPSEC SA established	Anonymized	192.168.2.0/24	Fw_A	
06/10/2025 13:02:10	IPSEC SA established	Anonymized	172.16.2.0/24	Fw_A	

DÉTAILS DE LA LIGNE DE LOG

Configuration

Nom de la règle

199b8bc3d24_4

Type de règle

gateway

Dates



STORMSHIELD
Network Security

v4.3.11

MONITORING

CONFIGURATION

EVA1

VMSNSX09K0639A9

admin

ÉCRITURE

LOGS - ACCÈS RESTREINT

?

LOG / VPN

Dernière heure

Actualiser

Rechercher...

Recherche avancée

Actions

RECHERCHE DU - 06/10/2025 12:07:46 - AU - 06/10/2025 13:07:46

Enregistré à	Message	Utilisateur	Nom de la source	Réseau local	Nom de destination	Réseau distant
06/10/2025 13:02:11	IPSEC SA established	Anonymized	172.16.1.0/24	Fw_B	172.16.2.0/24	
06/10/2025 13:02:11	IPSEC SA established	Anonymized	172.16.1.0/24	Fw_B	192.168.2.0/24	
06/10/2025 13:02:11	IPSEC SA established	Anonymized	192.168.1.0/24	Fw_B	172.16.2.0/24	

5. Application de nouvelles règles de filtrage spécifiques

- Une fois le tunnel validé et opérationnel, j'ai désactivé la règle temporaire "Pass any any any".

Nous avons ensuite ajouté des règles ciblées permettant au site distant de joindre nos réseaux internes, de ping nos machines locales et d'accéder à nos serveurs FTP et Web. Cela assure un filtrage plus précis et conforme aux bonnes pratiques de sécurité.

Regles IPSec (contient 2 règles, de 28 à 29)						
28		passer	Net_DMZ_A Lan_in_A via Tunnel VPN IPsec	Network_in Network_dmz1	Any	icmp (requête
29		passer	Net_DMZ_A Lan_in_A via Tunnel VPN IPsec	srv_ftp_priv_B	ftp	

FILTAGE NAT							
Rechercher...	+ Nouvelle règle	X Supprimer	↑ ↓ ↺ ↻	Couper	Copier	Coller	Chercher dans les logs
	État	Action	Source	Destination	Port dest.	Protocole	
1		passer	Network_in	srv_ftp_priv_B srv_web_priv_B	ftp http		
2		passer	Network_in	srv_ftp_priv_B srv_web_priv_B	Any	icmp (requête f	

FILTAGE NAT								
Rechercher...	+ Nouvelle règle	X Supprimer	↑ ↓ ↺ ↻	Couper	Copier	Coller		
	État	Action	Source	Destination	Port dest.	Protocole	Inspection	
1		passer	Network_in	srv_ftp_priv_A srv_web_priv_A	ftp http		IPS	
2		passer	Network_in	srv_ftp_priv_A srv_web_priv_A	Any	icmp (requête Echc	IPS	

Regles IPSec (contient 2 règles, de 28 à 29)						
28		passer	Net_DMZ_B Lan_in_B via Tunnel VPN IPsec	Network_in Network_dmz1	Any	icmp (requête Echc IPS
29		passer	Net_DMZ_B Lan_in_B via Tunnel VPN IPsec	srv_ftp_priv_A	ftp	IPS

```
user@client-training:~$ ping 172.16.2.11
PING 172.16.2.11 (172.16.2.11) 56(84) bytes of data.
64 bytes from 172.16.2.11: icmp_seq=1 ttl=64 time=103 ms
64 bytes from 172.16.2.11: icmp_seq=2 ttl=64 time=80.1 ms
64 bytes from 172.16.2.11: icmp_seq=3 ttl=64 time=104 ms
^C
--- 172.16.2.11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 14ms
rtt min/avg/max/mdev = 80.064/95.932/104.383/11.228 ms
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=50.9 ms
64 bytes from 172.16.2.12: icmp_seq=2 ttl=64 time=41.9 ms
64 bytes from 172.16.2.12: icmp_seq=3 ttl=64 time=43.5 ms
^C
```

```
user@client-training:~$ ping 172.16.1.11
PING 172.16.1.11 (172.16.1.11) 56(84) bytes of data.
64 bytes from 172.16.1.11: icmp_seq=1 ttl=64 time=80.0 ms
64 bytes from 172.16.1.11: icmp_seq=2 ttl=64 time=62.4 ms
^C
--- 172.16.1.11 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1ms
rtt min/avg/max/mdev = 62.426/71.200/79.975/8.778 ms
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=98.3 ms
64 bytes from 172.16.1.12: icmp_seq=2 ttl=64 time=55.4 ms
^C
--- 172.16.1.12 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 3ms
rtt min/avg/max/mdev = 55.380/76.815/98.250/21.435 ms
```

6. Création de nouveaux profils de chiffrement personnalisés

▪ Nous avons ensuite défini de nouveaux profils de chiffrement plus robustes :

Phase 1 (IKE) :

- DH Group : DH15 MODP
- Durée de vie : 21600 s
- Authentification : SHA2_512
- Chiffrement : AES 256 bits

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

+ Ajouter Actions

☐ IKE (5)

- ☒ StrongEncryption
- GoodEncryption
- Mobile
- DR
- IKE Phase1**

☐ IPsec (5)

- ☒ StrongEncryption
- GoodEncryption
- Mobile
- DR
- IPSEC Phase2**

PROFIL IKE : IKE PHASE1

Général

Commentaire:

Diffie-Hellman:

Durée de vie maximum (en secondes):

PROPOSITIONS

+ Ajouter X Supprimer Monter Descendre

Chiffrement		Authentification	
Algorithme	Force	Algorithme	Force
1 aes	256	sha2_512	512

- Phase 2 (IPsec) :
 - PFS : DH15 MODP
 - Durée de vie : 3600 s
 - Authentification : HMAC_SHA512
 - Chiffrement : AES 256 bits

+ Ajouter Actions

IKE (5)

StrongEncryption

GoodEncryption

Mobile

DR

IKE Phase1

IPsec (5)

StrongEncryption

GoodEncryption

Mobile

DR

IPSEC Phase2

PROFIL IPSEC : IPSEC PHASE2

Général

Commentaire:

Perfect Forward Secrecy (PFS):

DH15 MODP Group (3072-bits)

Durée de vie maximum (en secondes):

3600

PROPOSITIONS D'AUTHENTIFICATION

+ Ajouter X Supprimer

	Algorithme	Force
1	hmac_sha512	512

PROPOSITIONS DE CHIFFREMENT

+ Ajouter X Supprimer

	Algorithme	Force
1	aes	256

7. Application des nouveaux profils et tests de connectivité

- Une fois les profils créés, nous les avons appliqués au tunnel VPN existant. J'ai ensuite effectué des tests de connectivité (ping entre les machines des deux sites) pour vérifier la stabilité et la performance du nouveau chiffrement. Les journaux IPsec ont été analysés pour confirmer la bonne négociation avec les nouveaux paramètres.

POLITIQUE DE CHIFFREMENT - TUNNELS CORRESPONDANTS IDENTIFICATION PROFILS DE CHIFFREMENT

Q Entrer un filtre... + Ajouter ≡

Passerelles distantes (1)
Site_fw_B

SITE_FW_B

Général

Commentaire:

Passerelle distante: Fw_B

Adresse locale: Any

Profil IKE: **IKE Phase1**

Version IKE: IKEv2

Identification

Méthode d'authentification: Clé pré-partagée (PSK)

Local ID: Saisir un identifiant (optionnel)

ID du correspondant: Saisir un identifiant (optionnel)

Clé pré-partagée (PSK): x

— Configuration avancée —

- Test également du bon fonctionnement sur B :

VPN / VPN IPSEC

POLITIQUE DE CHIFFREMENT - TUNNELS CORRESPONDANTS IDENTIFICATION PROFILS DE CHIFFREMENT

Q Entrer un filtre... + Ajouter ≡

Passerelles distantes (1)
Site_fw_A

SITE_FW_A

Général

Commentaire:

Passerelle distante: Fw_A

Adresse locale: Any

Profil IKE: **IKE Phase1**

Version IKE: IKEv2

- Application du profil de phase 2 :
- Test également du bon fonctionnement sur A :

VPN / VPN IPSEC

POLITIQUE DE CHIFFREMENT - TUNNELS		CORRESPONDANTS		IDENTIFICATION		PROFILS DE CHIFFREMENT															
IPsec 01 (01)		Actions		Deactivate policy																	
SITE A SITE (GATEWAY-GATEWAY)				MOBILE - UTILISATEURS NOMADES																	
Entrez un filtre...		Ajouter		Supprimer		Monter		Descendre		Couper		Copier		Coller		Afficher les détails		Chercher dans les logs		Chercher	
	Etat	Réseau local		Correspondant		Réseau distant		Profil de chiffrement		Keepalive		Commentaire									
1	on	Network_in		Site_fw_B		Net_in_B		IPSEC Phase 2		30		Originally created on 2025...									
2	on	Network_in		Site_fw_B		Net_DMZ_B		IPSEC Phase 2		30		Originally created on 2025...									
3	on	Network_dmz1		Site_fw_B		Net_in_B		IPSEC Phase 2		30		Originally created on 2025...									
4	on	Network_dmz1		Site_fw_B		Net_DMZ_B		IPSEC Phase 2		30		Originally created on 2025...									

Test également du bon fonctionnement sur B :

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

Entrez un filtre...

+ Ajouter

X Supprimer

↑ Monter

↓ Descendre

Couper

Copier

Coller

Afficher les détails

Chercher dans les logs

Chercher dans la

	Etat	Réseau local	Correspondant	Réseau distant	Profil de chiffrement	Keepalive	Commentaire
1	on	Network_in	Site_Fw_A	Net_in_A	IPSEC Phase2	30	Originally created on 2025-1...
2	on	Network_in	Site_Fw_A	Net_DMZ_A	IPSEC Phase2	30	Originally created on 2025-1...
3	on	Network_dmz1	Site_Fw_A	Net_in_A	IPSEC Phase2	30	Originally created on 2025-1...
4	on	Network_dmz1	Site_Fw_A	Net_DMZ_A	IPSEC Phase2	30	Originally created on 2025-1...

- Nous effectuons plusieurs ping depuis la machine de B vers les machines de la DMZ de A :

```
user@client-training:~$ ping 172.16.1.11
PING 172.16.1.11 (172.16.1.11) 56(84) bytes of data.
64 bytes from 172.16.1.11: icmp_seq=1 ttl=64 time=112 ms
64 bytes from 172.16.1.11: icmp_seq=2 ttl=64 time=47.8 ms
^C
--- 172.16.1.11 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1ms
rtt min/avg/max/mdev = 47.828/79.894/111.960/32.066 ms
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=42.1 ms
64 bytes from 172.16.1.12: icmp_seq=2 ttl=64 time=37.7 ms
^C
--- 172.16.1.12 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 3ms
rtt min/avg/max/mdev = 37.715/39.927/42.139/2.212 ms
user@client-training:~$
```

Nous effectuons plusieurs ping depuis la machine de A vers les machines de la DMZ de B :

```
user@client-training:~$ ping 172.16.2.11
PING 172.16.2.11 (172.16.2.11) 56(84) bytes of data.
64 bytes from 172.16.2.11: icmp_seq=1 ttl=64 time=111 ms
64 bytes from 172.16.2.11: icmp_seq=2 ttl=64 time=86.3 ms
64 bytes from 172.16.2.11: icmp_seq=3 ttl=64 time=69.3 ms
^C
--- 172.16.2.11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 4ms
rtt min/avg/max/mdev = 69.301/88.977/111.286/17.242 ms
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=32.1 ms
64 bytes from 172.16.2.12: icmp_seq=2 ttl=64 time=113 ms
^C
--- 172.16.2.12 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 97ms
rtt min/avg/max/mdev = 32.081/72.566/113.051/40.485 ms
```

- Nous affichons les log IPsec VPN tunnels

Log de A :

Type	Status	Local traffic ...	Local gateway	Local ID	Remote gate...	Peer ID	Remote traffi...
Type : Site-to-site tunnels (4)							
	OK	Network_in	Firewall_out	192.36.253.10	Fw_B	192.36.253.20	Lan_in_B
	OK	Network_in	Firewall_out	192.36.253.10	Fw_B	192.36.253.20	Net_DMZ_B
	OK	Network_dm...	Firewall_out	192.36.253.10	Fw_B	192.36.253.20	Lan_in_B
	OK	Network_dm...	Firewall_out	192.36.253.10	Fw_B	192.36.253.20	Net_DMZ_B

Log de B :

 Actualiser Configurer le service VPN IPsec							
POLITIQUES							
Type	État	Extrémité d...	Passerelle l...	Local ID	Passerelle d...	ID du correspon...	Extrémité de...
Type : Tunnels site à site (4)							
	OK	Network_in	Firewall_out	192.36.253.20	Fw_A	192.36.253.10	Lan_in_A
	OK	Network_in	Firewall_out	192.36.253.20	Fw_A	192.36.253.10	Net_DMZ_A

8. Mise en place d'un tunnel basé sur des interfaces VTI

- Pour aller plus loin, nous avons réalisé une interconnexion via des tunnels VTI (Virtual Tunnel Interface).

IPSEC INTERFACES (VTI)		GRE INTERFACES		LOOPBACK	
Search		+ Add		X Delete 👁 Check usage	
Status	Name	IPv4 address	IPv4 mask	Comments	
Enabled	VTI_to_B	192.168.120.2	255.255.255.254		

Et B :

INTERFACES IPSEC (VTI)

INTERFACES GRE

LOOPBACK

Rechercher

+ Ajouter

✕ Supprimer

|

👁 Vérifier l'utilisation

État

⌵

Nom ↑

Adresse IPv4

Masque IPv4

Commentaire

🟢 Activé

VTI_to_A

192.168.120.1

255.255.255.254

Chaque pare-feu a reçu une adresse IP spécifique sur l'interface VTI, appartenant à un réseau distinct de ceux déjà configurés.

- Création des machines IP VTI A et B :

PROPERTIES

Object name:	mIP_VTI_B	
IPv4 address:	172.25.255.2	
MAC address:	01:23:45:67:89:ab (optional)	
Resolution		
☒ None (static IP) ☐ Automatic		
Comments:		

PROPRIÉTÉS

Nom de l'objet:	mIP_VTI_A	
Adresse IPv4:	172.25.255.1	
Adresse MAC:	01:23:45:67:89:ab (Facultatif)	
Résolution		
☒ Aucune (IP statique) ☐ Automatique		
Commentaire:		

▪ Création des réseaux IP VTI A et B :

CREATE AN OBJECT

Host

DNS name (FQDN)

Network

Address range

Router

Group

IP Protocol

Port

Object name:

IP_VTI_B

IPv4 addresses

Network IP address:

172.25.255.2/30

Example 192.168.0.0/16 or 192.168.0.0/255.255.0.0

Comments:

CRÉER UN OBJET

Machine

Nom DNS (FQDN)

Réseau

Plage d'adresses

Routeur

Groupe

Protocole IP

Port

Nom de l'objet:

IP_VTI_A

Adresses IPv4

Adresse IP de réseau:

172.25.255.1/30

Exemple 192.168.0.0/16 ou 192.168.0.0/255.255.0.0

Commentaire:

Nous avons ensuite configuré des routes statiques (ou du routage par politique - PBR) pour rediriger les flux utilisateurs à travers ces tunnels.

- Sur le correspondant A

STATIC ROUTES

Searching...					
Status	Destination network...	Interface	Address range	Gateway	Comments
on	Net_DMZ_B	VTI_to_B	172.16.2.0/24	mIP_VTI_B	
on	Net_in_B	VTI_to_B	192.168.2.0/24	mIP_VTI_B	

- Sur le correspondant B

ROUTES STATIQUES IPV4

ROUTAGE DYNAMIQUE

ROUTES DE RETOUR IPV4

Configuration générale

Passerelle par défaut (routeur):

Gw_default_B

ROUTES STATIQUES

Rechercher...					
État	Réseau de destinat...	Interface	Plan d'adressage	Passerelle	Commentaire
on	Net_DMZ_A	VTI_to_A	172.16.1.0/24	mIP_VTI_A	
on	Net_in_A	VTI_to_A	192.168.1.0/24	mIP_VTI_A	

- Enfin, des règles de filtrage adaptées ont été appliquées sur chaque VTI pour contrôler le trafic.

FILTERING NAT

Searching...										+ New rule ▾ × Delete ↑ ↓ ↻ ↺ ✂ Cut 📄 Copy 📄 Paste 🔍 Search in logs										☰
			Status ▾	Action ▾	Source	Destination	Dest. port	Protocol	Security inspection ▾	Co...										
1	🔌	🟢 on	➡ pass	🔌 Network_in	🔌 Net_in_B	🖱 Any		🛡 IPS		Cre...										
2	🔌	🟢 on	➡ pass	🔌 Network_in interface: VTI_to_B	🔌 Network_i	🖱 Any		🛡 IPS		Cre...										

FILTRAGE NAT

Rechercher...

Nouvelle règle

Supprimer

↑

↓

↶

↷

Couper

Copier

Coller

		État	Action	Source	Destination	Port dest.	Protocole	Inspection de s
1		on	passer	Network_in	Net_in_A	Any		IPS
2		on	passer	Net_in_A interface: VTI to	Network_in	Any		IPS

- Des tests de ping ont confirmé la bonne communication entre les deux extrémités via les interfaces virtuelles.

