NOTE TECHNIQUE

STORMSHIELD NETWORK SECURITY

VPN IPSEC : CONFIGURATION HUB AND SPOKE

Produits concernés : SNS 3.x, SNS 4.x

Dernière mise à jour du document : 9 décembre 2019

Référence : sns-fr-VPN_IPSec_Hub_And_Spoke_Note_Technique

Table des matières

Avant de commencer

La méthode d'authentification choisie dans ce didacticiel est basée sur les certificats.

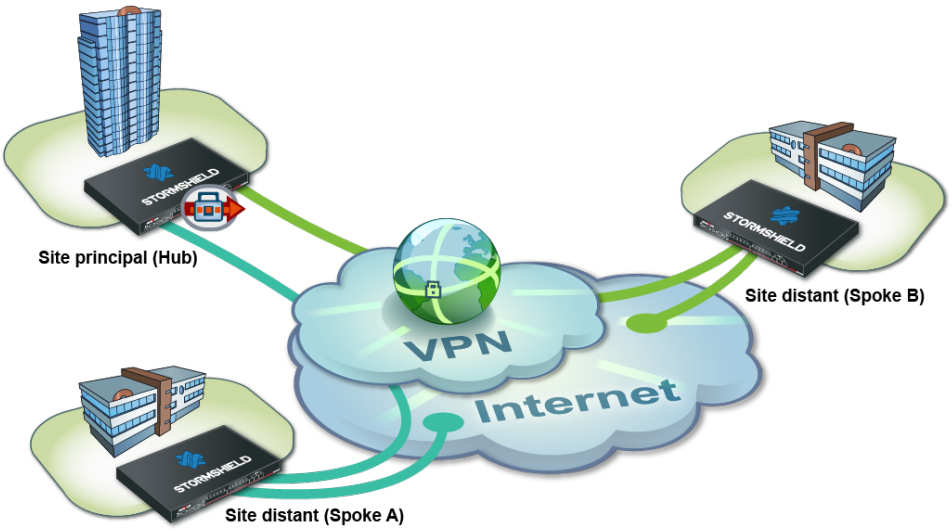
Pour le détail des opérations concernant la PKI, référez-vous au didacticiel « Mise en œuvre VPN IPsec - authentification par certificats ».

Dans la suite de ce document, le site central sera dénommé « Hub », les deux sites satellites étant représentés par « Spoke A » et « Spoke B ». Il est bien entendu que ce type d'architecture ne se limite pas à deux sites satellites.

Architectures présentées

Cas n° 1 : trafic interne via les tunnels IPsec

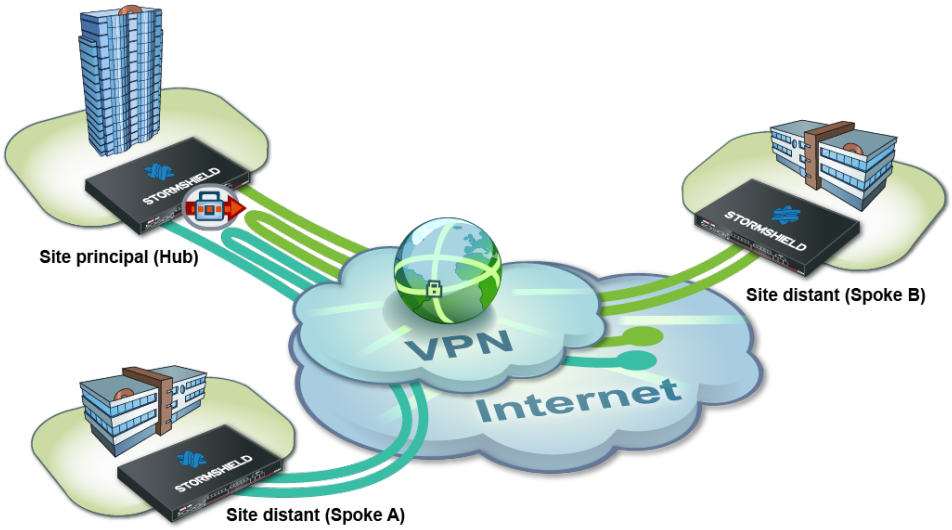
Seul le trafic interne entre les trois sites (Hub, Spoke A et Spoke B) passe au travers de tunnels via le Hub. Les flux Internet sont gérés localement sur chaque site.



Cette infrastructure peut parfois être préférée à celle présentée dans le cas n°2 pour des raisons économiques notamment: un accès internet centralisé sur le site Hub peut nécessiter un très gros débit et donc s'avérer plus onéreux qu'un ensemble d'accès Internet de capacité plus réduite.

Cas n°2 : trafic total via les tunnels IPsec

L'ensemble du trafic passe par le site Hub au travers de tunnels. L'accès Internet est centralisé au niveau du Hub.



Cette infrastructure présente l'avantage d'une gestion centralisée de l'accès Internet et de la politique de sécurité associée.

Prérequis de configuration

Dans ce didacticiel, les réseaux privés des 3 sites sont totalement distincts (exemple : 192.168.0.0/24, 192.168.1.0/24 et 192.168.2.0/24).

Les objets réseau nécessaires ont été créés sur chacun des sites à mettre en relation:

- l'adresse IP publique du Firewall Hub:Pub_FW_Hub,
- le réseau local du site Hub: Private_Net_Hub,
- l'adresse IP publique du Firewall Spoke A: Pub_FW_Spoke_A,
- le réseau local du site Spoke A: Private_Net_Spoke_A,
- l'adresse IP publique du Firewall Spoke B: Pub_FW_Spoke_B,
- le réseau local du site Spoke B: Private_Net_Spoke_B.

Vous avez mis en place votre PKI :

- Vous disposez d'une autorité de certification (CA),
- Vous avez créé les certificats des Firewalls,
- Vous avez importé sur les Firewalls des sites Spoke leur certificat respectif,
- Vous avez ajouté la CA dans les autorités de confiance sur chacun des Firewalls à mettre en relation.

Cas n°1 : paramétrer le site central (Hub)

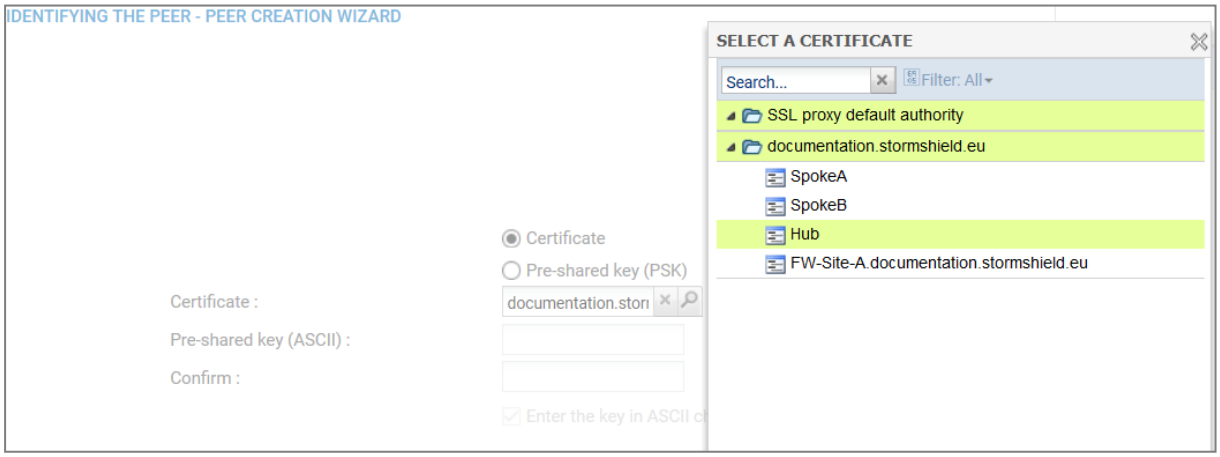
Sur le site Hub, il est nécessaire de :

- Créer les correspondants Site_Spoke_A et Site_Spoke_B,
- Créer les tunnels,
- Créer les règles de filtrage,
- Créer la règle de NAT.

Créer les correspondants Site_Spoke_A et Site_Spoke_B

Dans l'onglet **Correspondants** du menu **Configuration** > **VPN** > **VPN IPsec** :

1. Cliquez sur **Ajouter.**
2. Choisissez **Nouveau site distant**.
   L'assistant vous invite à sélectionner la passerelle distante. Ici, il s'agit de l'adresse publique du Firewall du site Spoke A (objet **Pub_FW_Spoke_A**).
3. Par défaut, le nom du correspondant est créé en préfixant cet objet avec « Site_ »; ce nom est personnalisable. Validez.
4. Choisissez la méthode **Certificat**.
5. Cliquez sur la loupe du champ **Certificat.**
6. Sélectionnez le certificat correspondant au Firewall Hub.
   Le champ **Autorité de confiance** est automatiquement fourni par le certificat.
7. Procédez à l'identique pour créer le correspondant Site_Spoke_B avec les valeurs suivantes :
   - **Passerelle distante** : le Firewall du site Spoke B (objet Pub_FW_Spoke_B),
   - **Certificat** : le certificat du Firewall Hub.

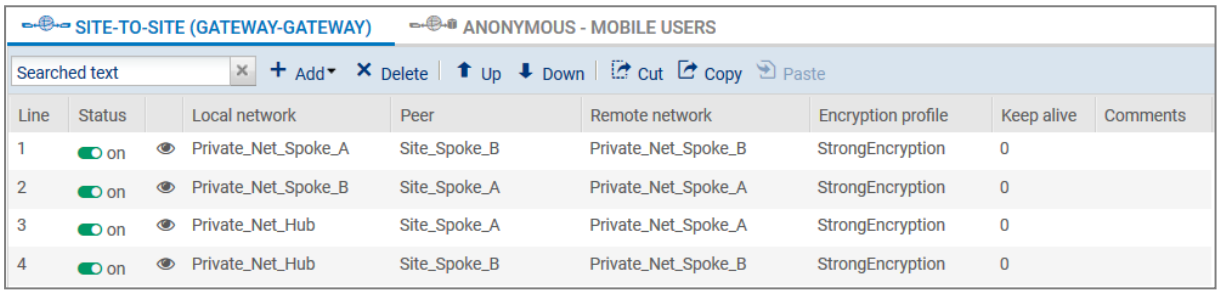


Créer les tunnels

Dans le menu **Configuration > VPN > VPN IPsec >** onglet **Politique de chiffrement – Tunnels :**

1. Cliquez sur **Ajouter.**
2. Choisissez **Tunnel site à site**.

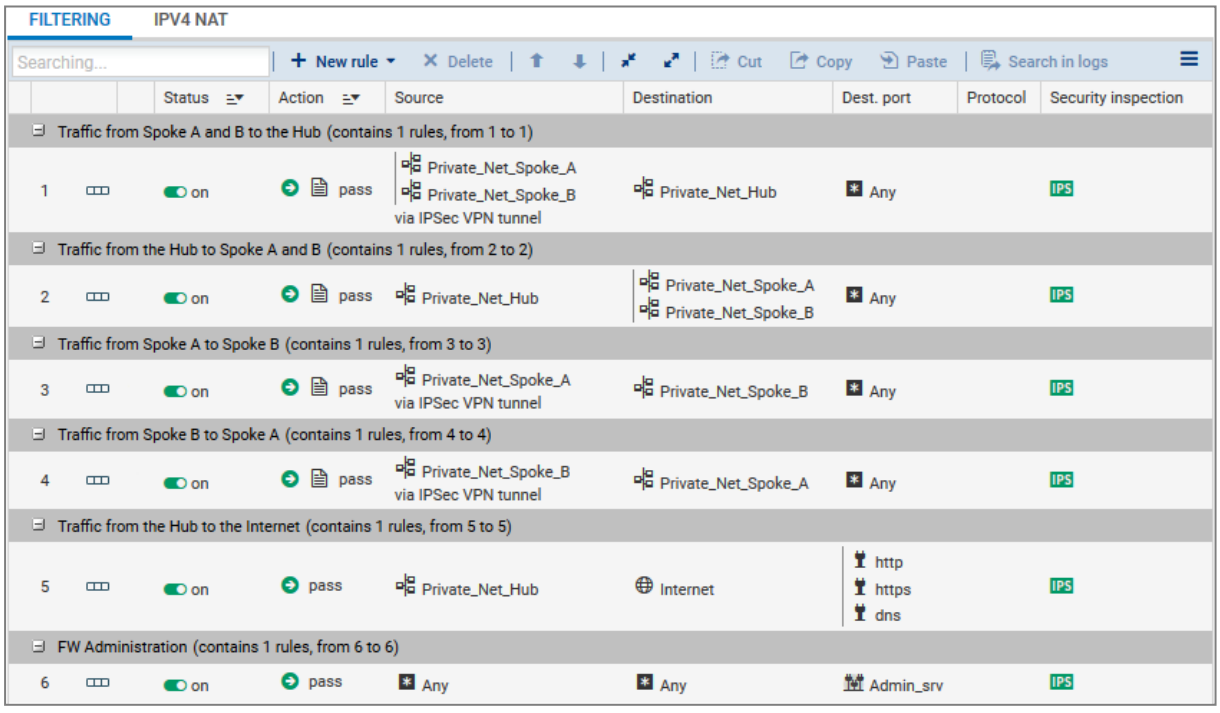
3. Suivez l'assistant pour définir le tunnel destiné au trafic entre sites Spoke A et Spoke B:
   - Dans le champ **Réseau local**, choisissez Private_Net_Spoke_A,
   - Dans le champ **Choix du correspondant**, sélectionnez Site_Spoke_B,
   - Dans le champ **Réseau distant**, choisissez Private_Net_Spoke_B,
   - Cliquez sur **Terminer**.
4. Procédez à l'identique pour créer les trois autres tunnels :
   - Private_Net_Spoke_B=> Site_Spoke_A => Private_Net_Spoke_A,
   - Private_Net_Hub => Site_Spoke_A => Private_Net_Spoke_A,
   - Private_Net_Hub => Site_Spoke_B=> Private_Net_Spoke_B.



Line	Status	Local network	Peer	Remote network	Encryption profile	Keep alive	Comments
1	on	Private_Net_Spoke_A	Site_Spoke_B	Private_Net_Spoke_B	StrongEncryption	0	
2	on	Private_Net_Spoke_B	Site_Spoke_A	Private_Net_Spoke_A	StrongEncryption	0	
3	on	Private_Net_Hub	Site_Spoke_A	Private_Net_Spoke_A	StrongEncryption	0	
4	on	Private_Net_Hub	Site_Spoke_B	Private_Net_Spoke_B	StrongEncryption	0	

Créer les règles de filtrage

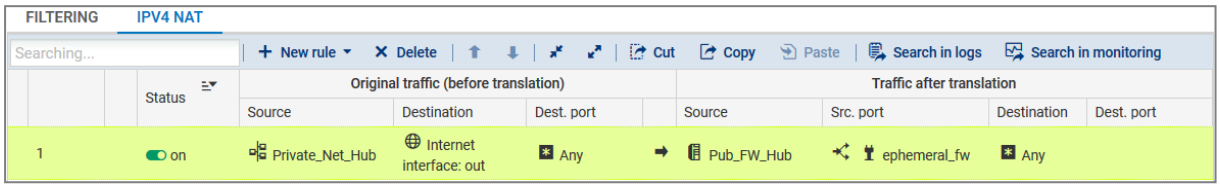
Définissez les règles de filtrage nécessaires au dialogue entre sites Spoke, sites Spoke et Hub ainsi qu'au trafic local vers Internet :



		Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
Traffic from Spoke A and B to the Hub (contains 1 rules, from 1 to 1)								
1		on	pass	Private_Net_Spoke_A Private_Net_Spoke_B via IPSec VPN tunnel	Private_Net_Hub	Any		IPS
Traffic from the Hub to Spoke A and B (contains 1 rules, from 2 to 2)								
2		on	pass	Private_Net_Hub	Private_Net_Spoke_A Private_Net_Spoke_B	Any		IPS
Traffic from Spoke A to Spoke B (contains 1 rules, from 3 to 3)								
3		on	pass	Private_Net_Spoke_A via IPSec VPN tunnel	Private_Net_Spoke_B	Any		IPS
Traffic from Spoke B to Spoke A (contains 1 rules, from 4 to 4)								
4		on	pass	Private_Net_Spoke_B via IPSec VPN tunnel	Private_Net_Spoke_A	Any		IPS
Traffic from the Hub to the Internet (contains 1 rules, from 5 to 5)								
5		on	pass	Private_Net_Hub	Internet	http https dns		IPS
FW Administration (contains 1 rules, from 6 to 6)								
6		on	pass	Any	Any	Admin_srv		IPS

Créer la règle de NAT

Pour permettre l'accès à Internet des machines du réseau Private_Net_Hub, créez la règle de NAT suivante :



Cas n°1 : paramétrer les sites satellites Spoke A et Spoke B

Dans une configuration de type Hub and Spoke, un site satellite ne connaît qu'un seul correspondant IPsec : le Firewall du site Hub.

- Définir le correspondant IPsec,
- Créer les tunnels,
- Créer les règles de filtrage,
- Créer la règle de NAT.

Définir le correspondant IPsec

Site Spoke A

En suivant la méthode décrite au paragraphe Créer les correspondants Site_Spoke_A et Site_Spoke_B, créez le correspondant Site_FW_Hub en utilisant les valeurs suivantes :

- **passerelledistante** : le Firewall du site Hub (objet Pub_FW_Hub),
- **certificat** : le certificat du Firewall Spoke A.

Site Spoke B

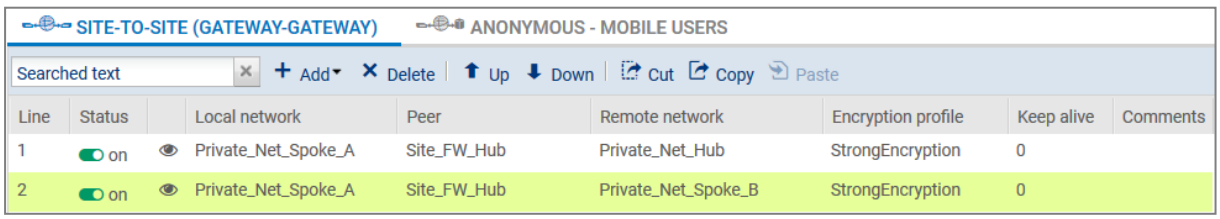
En suivant la méthode décrite au paragraphe Créer les correspondants Site_Spoke_A et Site_Spoke_B, créez le correspondant Site_FW_Hub en utilisant les valeurs suivantes :

- **passerelledistante** : le Firewall du site Hub (objet Pub_FW_Hub),
- **certificat** : le certificat du Firewall Spoke B.

Créer les tunnels

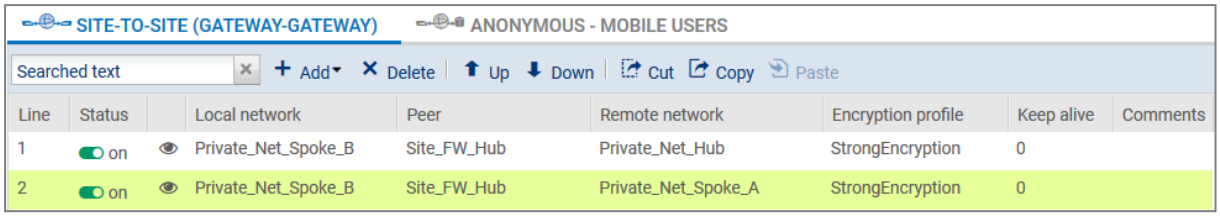
Site Spoke A

En suivant la méthode décrite au paragraphe Créer les tunnels, créez les deux tunnels nécessaires :



Site Spoke B

En suivant la méthode décrite au paragraphe Créer les tunnels, créez les deux tunnels nécessaires :

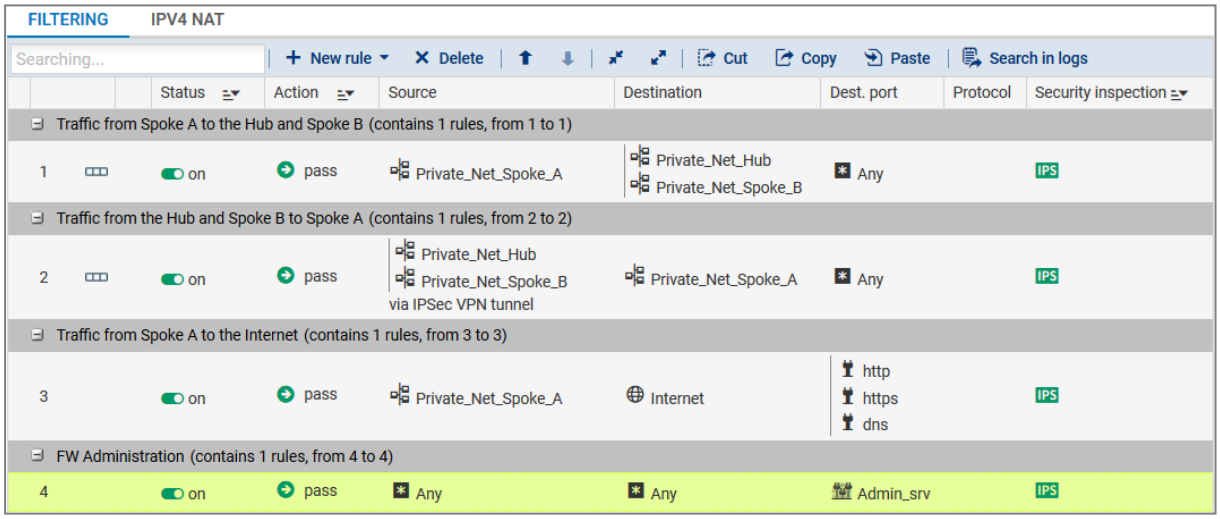


Créer les règles de filtrage

Dans ce didacticiel, le trafic entre les réseaux privés n'est volontairement pas précisé (port destination : ANY). Pour des raisons d'optimisation de performances (économie de bande passante et de ressources machine), il est important d'affiner le filtrage sur les sites satellites (protocoles, ports… autorisés) afin d'éviter de laisser transiter des paquets inutiles dans les tunnels. Cette politique de filtrage sera également présente sur le site Hub.

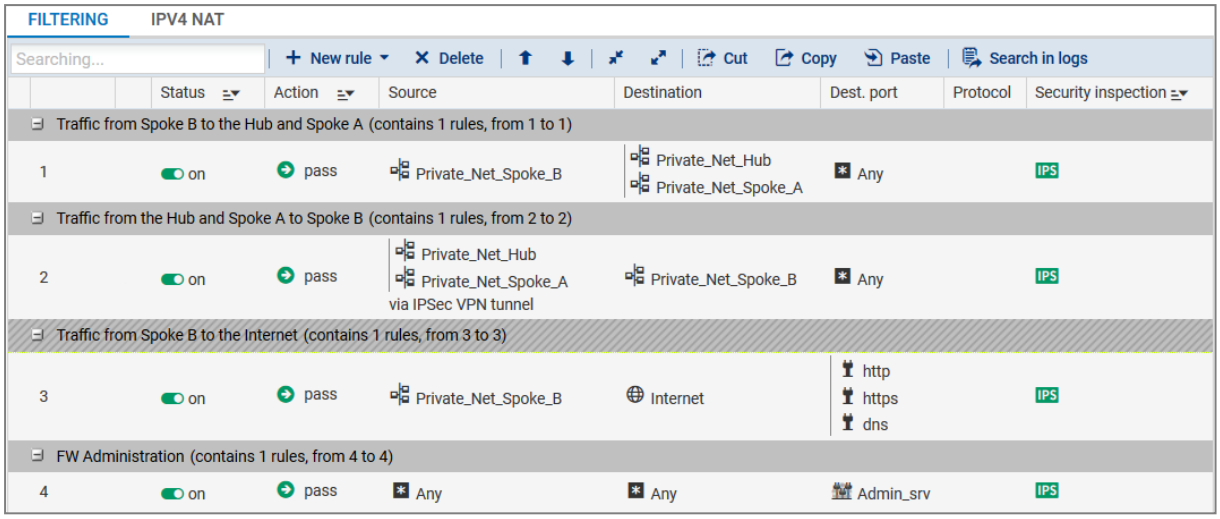
Site Spoke A

Définissez les règles de filtrage nécessaires au dialogue entre Spoke A et Spoke B, Spoke A et Hub ainsi qu'au trafic local vers Internet :



Site Spoke B

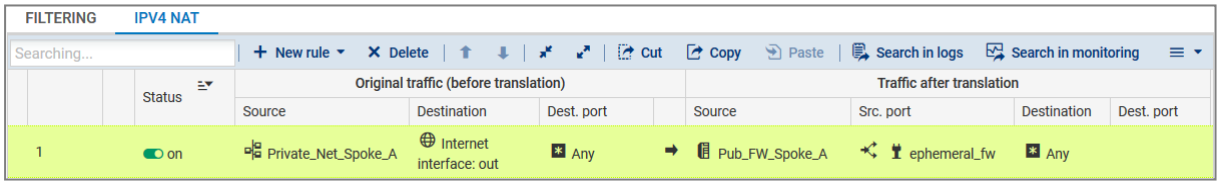
Définissez les règles de filtrage nécessaires au dialogue entre Spoke B et Spoke A, Spoke B et Hub ainsi qu'au trafic local vers Internet:



Créer la règle de NAT

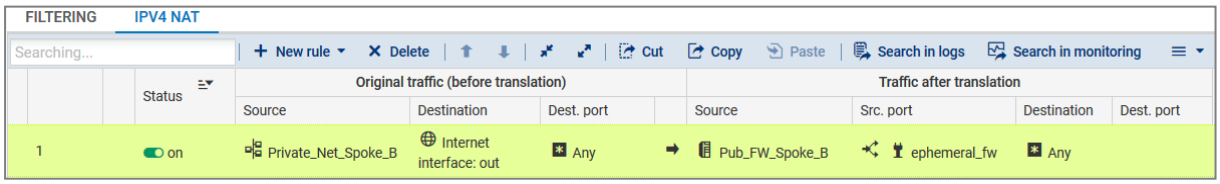
Site Spoke A

Pour permettre l'accès à Internet des machines du réseau Private_Net_Spoke_A, créez la règle de NAT suivante :



Site Spoke B

Pour permettre l'accès à Internet des machines du réseau Private_Net_Spoke_B, créez la règle de NAT suivante :



Cas n°2 : paramétrer le site central (Hub)

Sur le site Hub, il est nécessaire de :

- Définir le correspondant IPsec,
- Créer les tunnels,
- Créer les règles de filtrage,
- Créer la règle de NAT.

Définir le correspondant IPsec

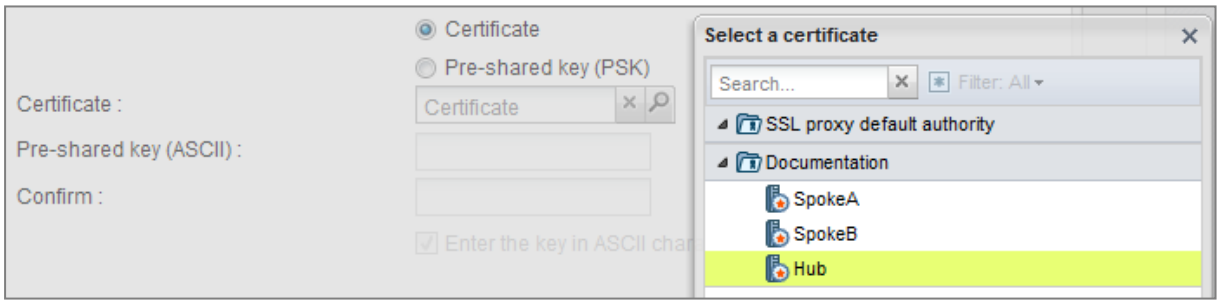
En suivant la méthode décrite au paragraphe Créer les correspondants Site_Spoke_A et Site_Spoke_B du Cas n°1, créez les deux correspondants Site_Spoke_A et Site_Spoke_B.

Pour définir Site_Spoke_A, utilisez les valeurs suivantes :

- **passerelle distante** : le Firewall du site Spoke A (objet Pub_FW_Spoke_A),
- **certificat** : le certificat du Firewall Hub.

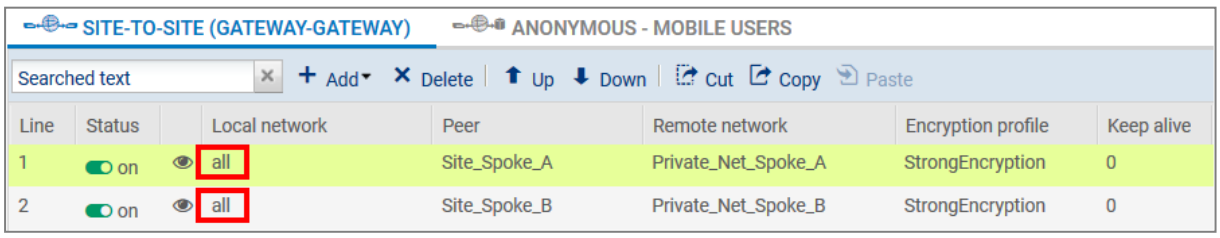
Pour définir Site_Spoke_B :

- **passerelle distante** : le Firewall du site Spoke B (objet Pub_FW_Spoke_B),
- **certificat** : le certificat du Firewall Hub.



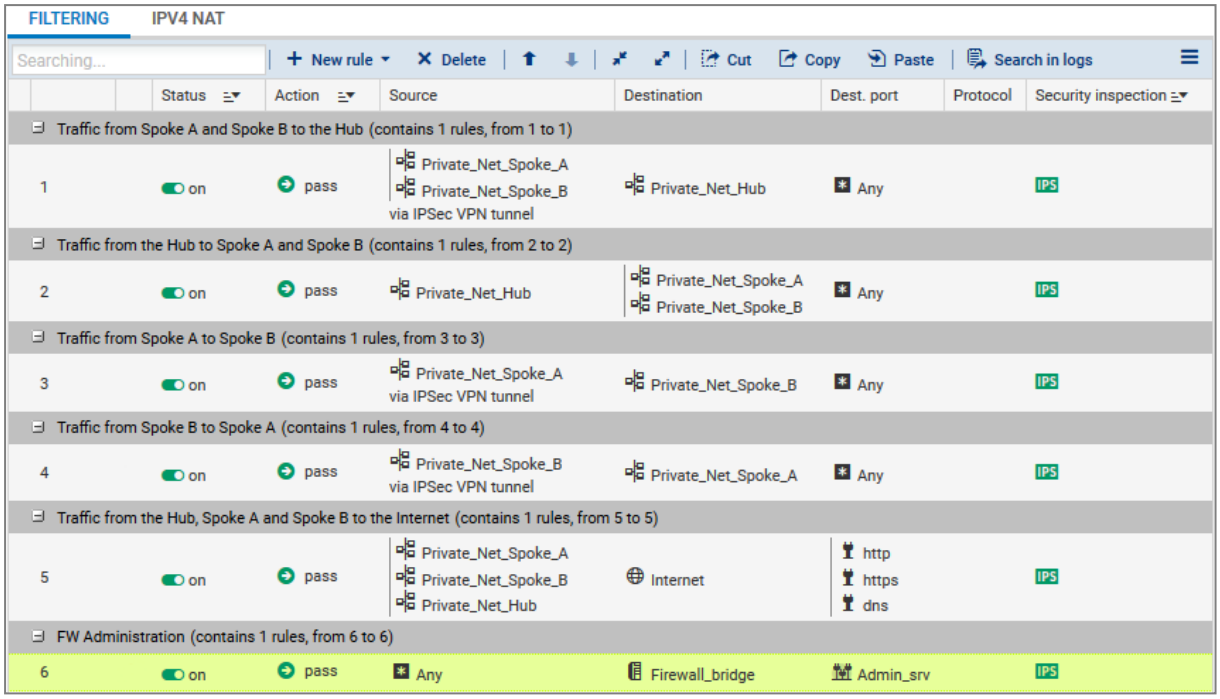
Créer les tunnels

Suivez la méthode décrite dans le paragraphe Créer les tunnels du Cas n°1 pour définir les VPN suivants :



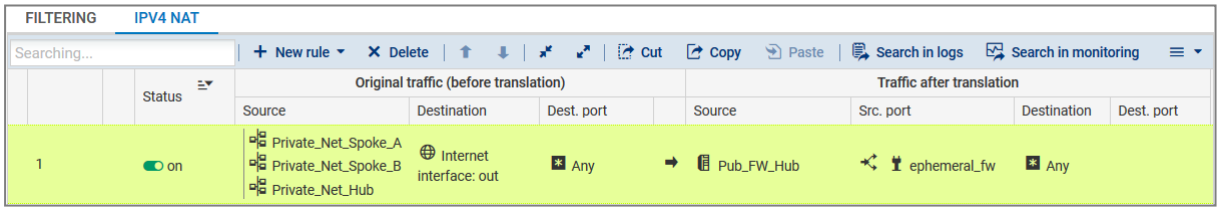
Créer les règles de filtrage

Définissez les règles de filtrage nécessaires au dialogue entre sites Spoke, sites Spoke et Hub ainsi qu'au trafic local vers Internet :



Créer la règle de NAT

Pour permettre l'accès à Internet de l'ensemble des machines des réseaux privés, créez la règle de NAT suivante :



Les sources ont été indiquées de manière unitaire dans cette règle, mais il est bien évident que l'emploi de groupes devient indispensable lorsque le nombre de sites satellites augmente.

Cas n°2 : paramétrer les sites satellites Spoke A et Spoke B

Dans une configuration de type Hub and Spoke, un site satellite ne connaît qu'un seul correspondant IPsec : le Firewall du site Hub.

- Définir le correspondant IPsec,
- Créer les tunnels,
- Créer les règles de filtrage.

Définir le correspondant IPsec

Site Spoke A

En suivant la méthode décrite au paragraphe Créer les correspondants Site_Spoke_A et Site_Spoke_B du Cas n°1, créez le correspondant Site_FW_Hub en utilisant les valeurs suivantes :

- **passerelledistante** : le Firewall du site Hub (objet Pub_FW_Hub),
- **certificat** : le certificat du Firewall Spoke A.

Site Spoke B

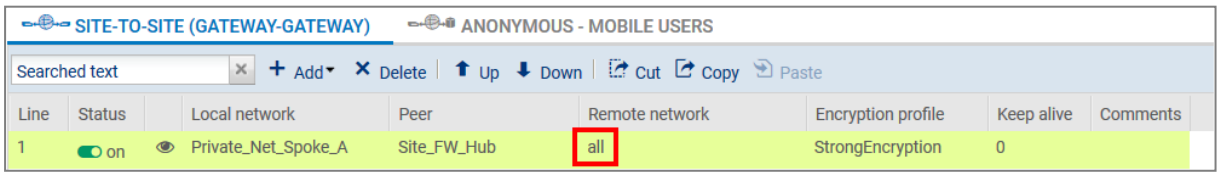
En suivant la méthode décrite au paragraphe Créer les correspondants Site_Spoke_A et Site_Spoke_B du Cas n°1, créez le correspondant Site_FW_Hub en utilisant les valeurs suivantes :

- **passerelledistante** : le Firewall du site Hub (objet Pub_FW_Hub),
- **certificat** : le certificat du Firewall Spoke B.

Créer les tunnels

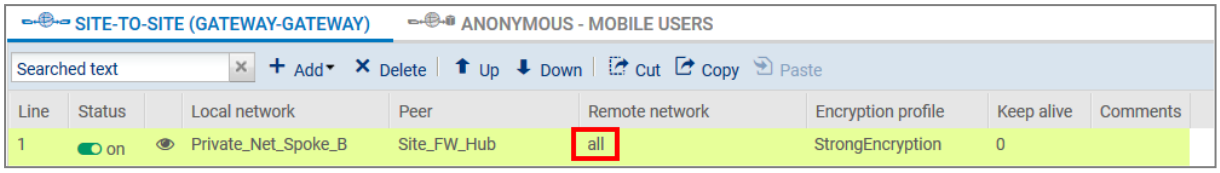
Site Spoke A

Suivez la méthode décrite dans le paragraphe Créer les tunnels du Cas n°1 pour définir le VPN suivant :



Site Spoke B

Suivez la méthode décrite dans le paragraphe Créer les tunnels du Cas n°1 pour définir le VPN suivant :

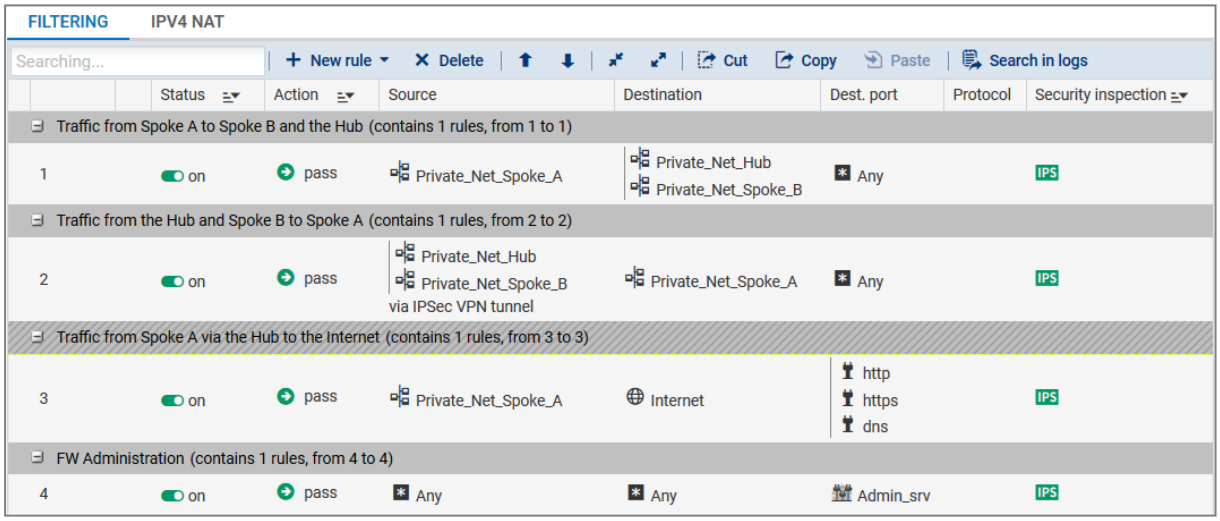


Créer les règles de filtrage

Dans ce didacticiel, le trafic entre les réseaux privés n'est volontairement pas précisé (port destination : ANY). Pour des raisons d'optimisation de performances (économie de bande passante et de ressources machine), il est important d'affiner le filtrage sur les sites satellites (protocoles, ports… autorisés) afin d'éviter de laisser transiter des paquets inutiles dans les tunnels. Cette politique de filtrage sera également présente sur le site Hub.

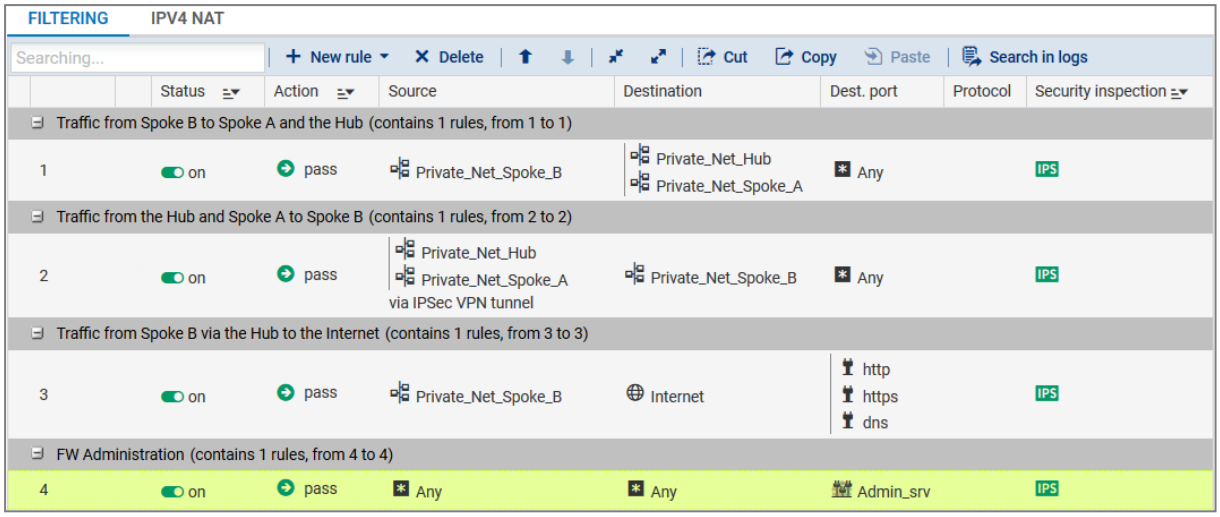
Site Spoke A

Définissez les règles de filtrage nécessaires au dialogue entre Spoke A et Spoke B, Spoke A et Hub ainsi qu'au trafic vers Internet (centralisé sur Hub) :



Site Spoke B

Définissez les règles de filtrage nécessaires au dialogue entre Spoke B et Spoke A, Spoke B et Hub ainsi qu'au trafic vers Internet (centralisé sur Hub) :



FILTERING | IPV4 NAT

Searching... | New rule | Delete | Cut | Copy | Paste | Search in logs

	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
Traffic from Spoke B to Spoke A and the Hub (contains 1 rules, from 1 to 1)							
1	on	pass	Private_Net_Spoke_B	Private_Net_Hub Private_Net_Spoke_A	Any		IPS
Traffic from the Hub and Spoke A to Spoke B (contains 1 rules, from 2 to 2)							
2	on	pass	Private_Net_Hub Private_Net_Spoke_A via IPSec VPN tunnel	Private_Net_Spoke_B	Any		IPS
Traffic from Spoke B via the Hub to the Internet (contains 1 rules, from 3 to 3)							
3	on	pass	Private_Net_Spoke_B	Internet	http https dns		IPS
FW Administration (contains 1 rules, from 4 to 4)							
4	on	pass	Any	Any	Admin_srv		IPS

Vérifier l'établissement des tunnels

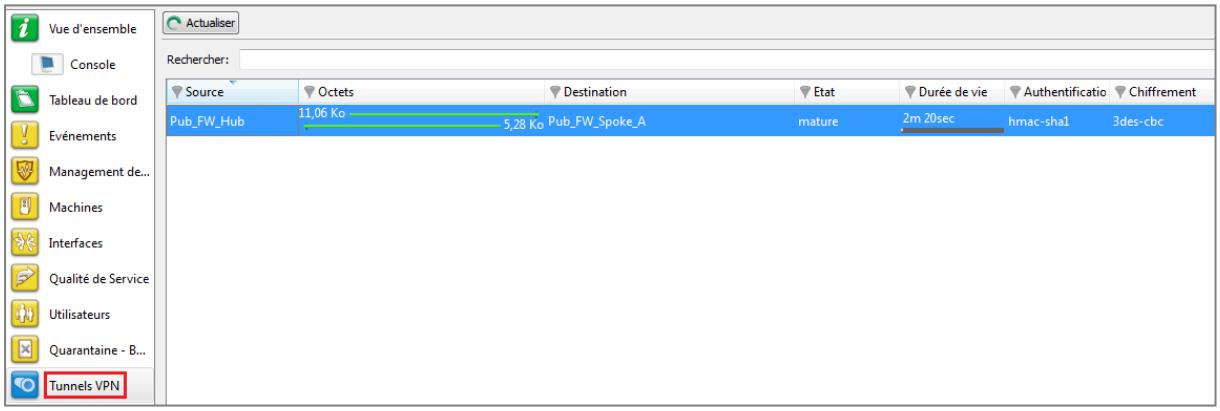
Depuis un poste client situé sur le site Spoke A, établissez tout d'abord une connexion vers une machine du site Hub (via un Ping par exemple, si vous avez autorisé le protocole ICMP dans l'ensemble des règles de filtrage), afin de tester l'établissement du premier tunnel (Spoke A vers Hub).

Via la suite d'administration Stormshield Network

Lancez Stormshield Network Real-Time Monitor, connectez-vous au Firewall du site Hub par le biais du logiciel et cliquez sur le module **Traces > VPN**. Vérifiez que les phases 1 et 2 se sont correctement déroulées (messages « Phase established ») :

Date	Niveau d'erreur	Phase	Source	Destination	Message	Identité du distant	SPI entrant	SPI sortant	Cookie (entrant/sortant)	Rôle
10:20:49	Information	2	Pub_FW_Hub	Pub_FW_Spoke_A	Phase established		0x04c372d8	0x09e42dc6	0x8b44ebe0933b4060/0xed773512a640fe4b	responder
10:20:48	Information	1	Pub_FW_Hub	Pub_FW_Spoke_A	Phase established				0x8b44ebe0933b4060/0xed773512a640fe4b	responder
10:20:48	Information	1	Pub_FW_Hub	Pub_FW_Spoke_A	INITIAL-CONTACT sent				0x8b44ebe0933b4060/0xed773512a640fe4b	responder
10:20:48	Information	1	Pub_FW_Hub	Pub_FW_Spoke_A	DPD support detected				0x8b44ebe0933b4060/0x0000000000000000	responder
10:04:55	Information	0			Isakmp daemon started				/	

Dans le module **Tunnels VPN,** vous pouvez également visualiser ce premier tunnel ainsi que la quantité de données échangées :

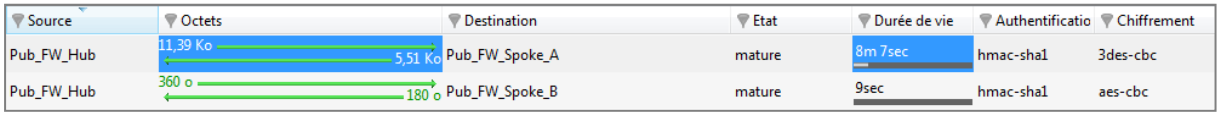


Depuis le même poste client du site Spoke A, établissez ensuite une connexion vers une machine du site Spoke B, afin de vérifier l'établissement du second tunnel (Hub vers Spoke B).

Dans le module **Traces > VPN** de Stormshield Network Real-Time Monitor, vérifiez que les phases 1 et 2 se sont correctement déroulées (messages « Phase established ») :

Date	Niveau d'erreur	Phase	Source	Destination	Message	Identité du distant	SPI entrant	SPI sortant	Cookie (entrant/sortant)	Rôle
10:28:47	Information	2	Pub_FW_Hub	Pub_FW_Spoke_B	Phase established		0x0573b30c	0x0739c88c	0x78ad430165eb1b24/0xf1a3673f4de59312	initiator
10:28:46	Information	1	Pub_FW_Hub	Pub_FW_Spoke_B	INITIAL-CONTACT sent				0x78ad430165eb1b24/0xf1a3673f4de59312	initiator
10:28:46	Information	1	Pub_FW_Hub	Pub_FW_Spoke_B	Phase established				0x78ad430165eb1b24/0xf1a3673f4de59312	initiator
10:28:46	Information	1	Pub_FW_Hub	Pub_FW_Spoke_B	DPD support detected				0x78ad430165eb1b24/0x0000000000000000	initiator
10:20:49	Information	2	Pub_FW_Hub	Pub_FW_Spoke_A	Phase established		0x04c372d8	0x09e42dc6	0x8b44ebe0933b4060/0xed773512a640fe4b	responder
10:20:48	Information	1	Pub_FW_Hub	Pub_FW_Spoke_A	Phase established				0x8b44ebe0933b4060/0xed773512a640fe4b	responder
10:20:48	Information	1	Pub_FW_Hub	Pub_FW_Spoke_A	INITIAL-CONTACT sent				0x8b44ebe0933b4060/0xed773512a640fe4b	responder
10:20:48	Information	1	Pub_FW_Hub	Pub_FW_Spoke_A	DPD support detected				0x8b44ebe0933b4060/0x0000000000000000	responder
10:04:55	Information	0			Isakmp daemon started				/	

Dans le module **Tunnels VPN,** vous pouvez désormais visualiser les deux tunnels :



Outils d'informations et de diagnostic en console

Commande showSPD

La commande *showSPD* présente la politique IPsec active sur le Firewall. Son résultat est identique, que des tunnels soient établis ou non.

Dans le cas N°2 de ce didacticiel (trafic total via tunnel IPsec), cette commande passée sur le Firewall Spoke A retourne le résultat suivant :

```
[redacted]>showSPD
0.0.0.0/0[any] 127.0.0.0/8[any] 255
        in none
        spid=67 seq=5 pid=62800
        refcnt=1
192.168.0.0/24[any] 192.168.0.0/24[any] 255
        in none
        spid=69 seq=4 pid=62800
        refcnt=1
0.0.0.0/0[any] 192.168.0.0/24[any] 255
        in ipsec
        esp/tunnel/[redacted]/unique#16386
        spid=72 seq=3 pid=62800
        refcnt=1
127.0.0.0/8[any] 0.0.0.0/0[any] 255
        out none
        spid=68 seq=2 pid=62800
        refcnt=1
192.168.0.0/24[any] 192.168.0.0/24[any] 255
        out none
        spid=70 seq=1 pid=62800
        refcnt=1
192.168.0.0/24[any] 0.0.0.0/0[any] 255
        out ipsec
        esp/tunnel/[redacted]/unique#16385
        spid=71 seq=0 pid=62800
        refcnt=1
```

On y retrouve notamment les informations suivantes :

- Le réseau local et le réseau distant : « **192.168.0.0**/24 [any] **0.0.0.0**/0 [any] »,
- Le sens du tunnel : « **out** ipsec »,
- Les adresses IP des passerelles IPsec : « esp/tunnel/**adresse locale** – **adresse distante** »,
- L'ID de l'Association de Sécurité (SA) : « unique#**16385** ».

Commande showSAD

La commande *showSAD* liste les informations de sécurité des SA (Security Associations – Associations de Sécurité) établies sur une passerelle IPsec. Ces informations ne sont disponibles que lorsque des tunnels sont établis.

Dans le cas N°2 de ce didacticiel (trafic total via tunnel IPsec), cette commande passée sur le Firewall Spoke A retourne le résultat suivant :

```
[redacted]
        esp mode=tunnel spi=219753044(0x0d192a54) reqid=16386(0x00004002)
        E: 3des-cbc  6093662d 55ec9528 818b6e7d 3f88d590 96a0d84a 80247f2c
        A: hmac-sha1  e082ddd6 673a2af9 53d0b88f ea201de8 88c45da2
        seq=0x00000031 replay=8 flags=0x00000000 state=mature
        created: Feb  3 16:09:16 2014   current: Feb  3 16:15:44 2014
        diff: 388(s)    hard: 3600(s)   soft: 2880(s)
        last: Feb  3 16:11:58 2014      hard: 0(s)      soft: 0(s)
        current: 9999(bytes)    hard: 0(bytes)  soft: 0(bytes)
        allocated: 49   hard: 0 soft: 0
        sadb_seq=1 pid=29053 refcnt=1
[redacted]
        esp mode=tunnel spi=169172253(0x0a155d1d) reqid=16385(0x00004001)
        E: 3des-cbc  c0100685 d48e5f27 686997d8 62d09ffb ed95d1c1 89cf9566
        A: hmac-sha1  0fd9d769 f63ac3a0 62869791 4cca65a1 3445527d
        seq=0x00000034 replay=8 flags=0x00000000 state=mature
        created: Feb  3 16:09:16 2014   current: Feb  3 16:15:44 2014
        diff: 388(s)    hard: 3600(s)   soft: 2880(s)
        last: Feb  3 16:11:58 2014      hard: 0(s)      soft: 0(s)
        current: 8840(bytes)    hard: 0(bytes)  soft: 0(bytes)
        allocated: 52   hard: 0 soft: 0
        sadb_seq=0 pid=29053 refcnt=2
```

On y retrouve notamment les informations suivantes :

- Adresse IP de la passerelle émettrice – Adresse IP de la passerelle réceptrice.
- Le SPI (Security Parameter Index) : « spi=169172253 **(0x0a155d1d)** ». Le SPI est identifié en fonction du sens de la SA affichée. Ainsi, pour une SA décrite dans le sens IP distante – IP locale, le SPI indiqué est le SPI entrant. Il permet alors d'identifier des flux entrants,
- La méthode de chiffrement utilisée : « E : **3des-cbd** »,
- La méthode d'authentification utilisée : « A: **hmac-sha1** »,
- L'état du tunnel : « state=**mature** ». Cet état peut être mature (le tunnel est correctement établi : la SA est disponible et utilisable), larval (la SA est en cours de négociation) ou dying (la SA est arrivée au terme de sa durée de vie et sera renégociée lorsque du trafic le nécessitera).
- La date/heure d'établissement du tunnel et la date/heure courantes,
- Le nombre d'octets échangés. current : **8840** (bytes).

Résolution d'incidents – Erreurs communes

- Si vous avez opté pour l'authentification par certificats, reportez-vous à la section « Résolution d'incidents – Erreurs communes » du didacticiel « Mise en œuvre d'un VPN IPsec – Authentification par certificats ».
- Si vous avez opté pour l'authentification par clé prépartagée, reportez-vous à la section « Résolution d'incidents – Erreurs communes » du didacticiel « Mise en œuvre d'un VPN IPsec – Authentification par clé prépartagée ».

Pour aller plus loin

Des informations complémentaires et réponses à vos éventuelles questions sont disponibles dans la base de connaissances Stormshield (authentification nécessaire).

documentation@stormshield.eu