TECHNICAL NOTE
STORMSHIELD NETWORK SECURITY

IPSEC VPN: HUB AND SPOKE CONFIGURATION

Product concerned: SNS 3.x, SNS 4.x

Document last updated: December 9, 2019

Reference: sns-en-IPSec_VPN_Hub_And_Spoke_Technical_Note

Table of contents

Getting started

The authentication method chosen for this tutorial is based on certificates.

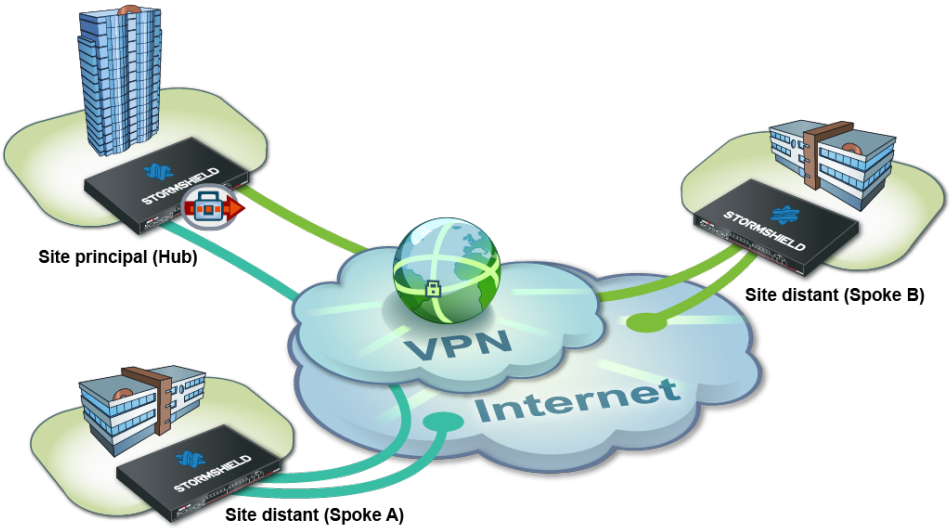
For details on operations regarding the PKI, please refer to the tutorial “IPsec VPN - authentication by certificate”.

Further on in this document, the central site will be named “Hub”, and both satellite sites will be represented by “Spoke A” and “Spoke B”. Needless to say, this type of architecture is not restricted to just two satellite sites.

Architectures shown

Case no. 1: internal traffic via IPsec tunnels

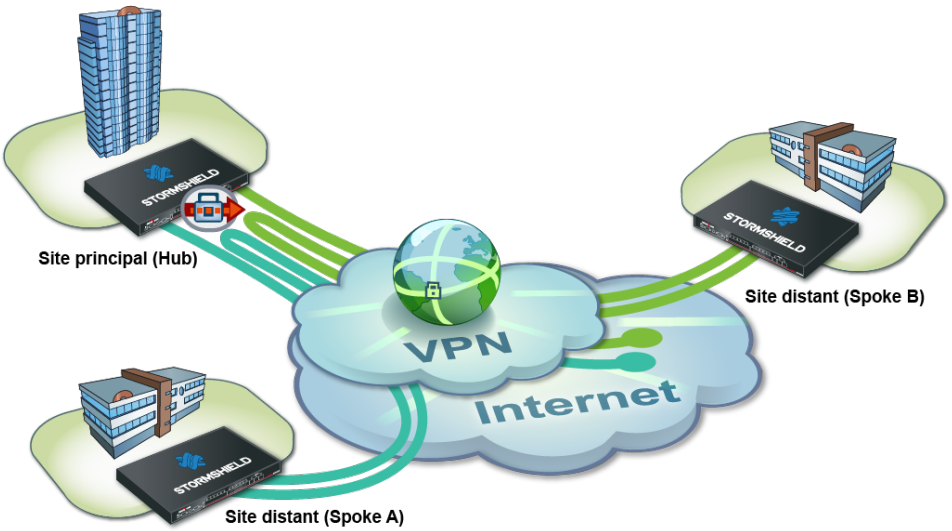
Only internal traffic between the three sites (Hub, Spoke A and Spoke B) goes through tunnels via the Hub. Internet traffic is managed locally on each site.



This infrastructure may sometimes be preferred over the one presented in case no.2 for economic reasons, in particular: centralized internet access on the Hub may require a lot of throughput and end up being much costlier than a set of lower-capacity internet access channels.

Case no.2: all traffic via IPsec tunnels

All the traffic goes through the Hub through tunnels. Internet access is centralized at the Hub level.



This infrastructure presents the advantage of the centrally managing internet access and the associated security policy.

Configuration requirements

In this tutorial, the private networks of the 3 sites will be distinct (example: 192.168.0.0/24, 192.168.1.0/24 and 192.168.2.0/24).

The necessary network objects have been created on each of the sites to interlink:

- the public IP address of the Hub Firewall: Pub_FW_Hub,
- the local network of the Hub site: Private_Net_Hub,
- the public IP address of the Spoke A Firewall: Pub_FW_Spoke_A,
- the local network of the Spoke A site: Private_Net_Spoke_A,
- the public IP address of the Spoke B Firewall: Pub_FW_Spoke_B,
- the local network of the Spoke B site: Private_Net_Spoke_B.

Check that your PKI has been set up:

- There is a certification authority (CA),
- Certificates have been created for the Firewalls,
- The respective certificates have been imported on the Firewalls of the Spoke sites,
- The CA has been added to the list of trusted CAs on each of the Firewalls to interlink.

Case no.1: configuring the central site (Hub)

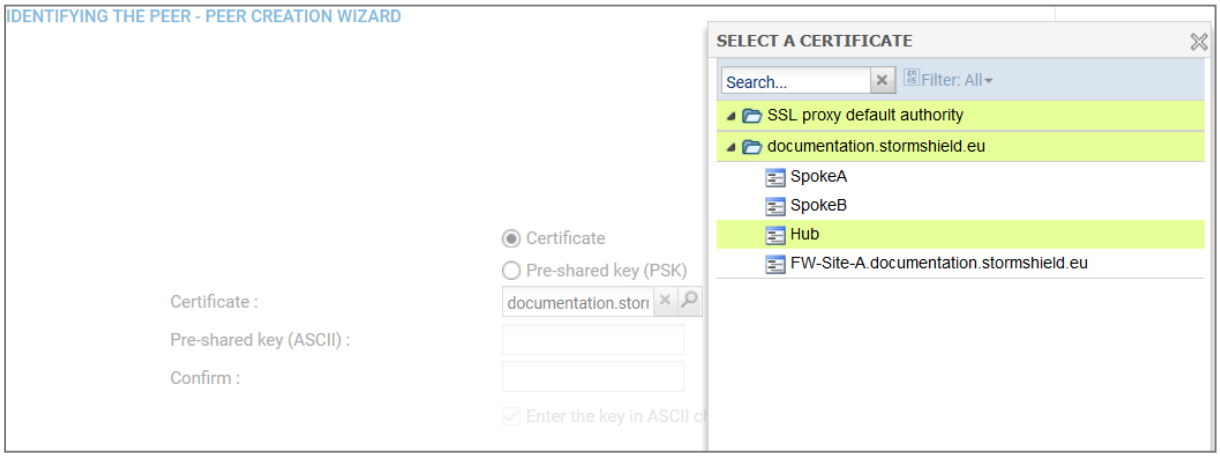
On the Hub site you will have to:

- Creating the Site_Spoke_A and Site_Spoke_B peers,
- Creating tunnels,
- Creating filtering rules,
- Creating NAT rule.

Creating the Site_Spoke_A and Site_Spoke_B peers

In the menu **Configuration** > **VPN** > **IPsec VPN** > **Peers** tab:

1. Click on **Add.**
2. Choose **New remote site**.
   The wizard will ask you to select the remote gateway. In this case, this gateway will be the public address of the Firewall on the Spoke A site (object **Pub_FW_Spoke_A**).
3. By default, the name of the peer will be created by adding a prefix "Site_" to this object name; this name can be customized. Press **Enter**.
4. Next, select the **Certificate** method.
5. Click on the magnifying glass next to the **Certificate** field
6. Select the certificate corresponding to the Hub Firewall.
   The **Trusted CA** field is automatically entered by the certificate.
7. In the same way, create the Site_Spoke_B peer using the following values:
   - **Remote gateway**: the Firewall of the Spoke B site (object Pub_FW_Spoke_B),
   - **Certificate**: the certificate of the Hub Firewall.



Creating tunnels

In the menu **Configuration** > **VPN** > **IPsec VPN** > **Encryption policy – Tunnels** tab:

1. Click on **Add.**
2. Select **Site-to-site tunnel**.

3. Follow the instructions in the wizard to define the tunnel meant for traffic between the sites Spoke A and Spoke B:
   - In the field **Local network**, select **Private_Net_Spoke_A**,
   - In the field **Peer selection**, select **Site_Spoke_B**,
   - In the field **Remote network**, select **Private_Net_Spoke_B**,
   - Click **Finish**.
4. Do the same thing to create the three other 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.

SITE-TO-SITE (GATEWAY-GATEWAY) | ANONYMOUS - MOBILE USERS

Searched text | Add | Delete | Up | Down | Cut | Copy | Paste

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	

Creating filtering rules

Define the filtering rules needed for exchanges between Spoke sites, Spoke sites and the Hub as well as local traffic to the Internet:

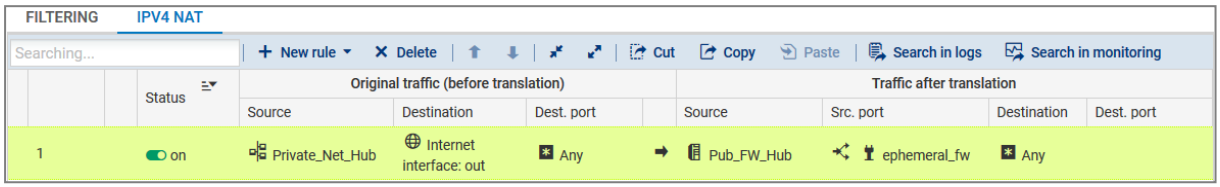
FILTERING | IPV4 NAT

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

	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
Traffic from Spoke 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

Creating NAT rule

To allow hosts on the network Private_Net_Hub to access the internet, create the following NAT rule:



Case no.1: configuring the satellite sites Spoke A and Spoke B

In a Hub and Spoke configuration, a satellite site only knows one IPsec peer: the Firewall of the Hub site.

- Defining the IPsec peer,
- Creating tunnels,
- Creating filtering rules,
- Creating NAT rule.

Defining the IPsec peer

Spoke A site

Following the method described in the paragraph Creating the Site_Spoke_A and Site_Spoke_B peers, create the peer Site_FW_Hub using the following values:

- **remote gateway**: Firewall of the Hub (object **Pub_FW_Hub**),
- **certificate**: the certificate of the Spoke A Firewall.

Spoke B site

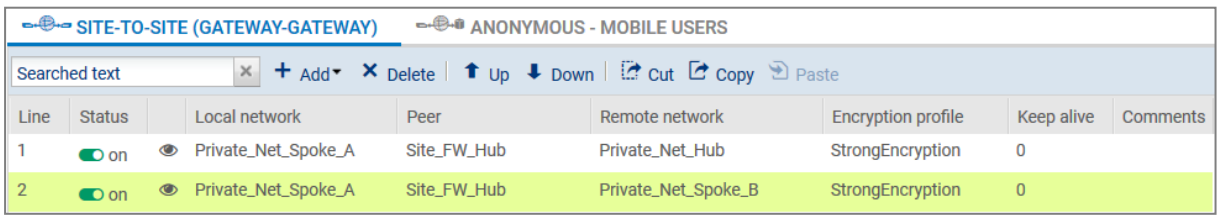
Following the method described in the paragraph Creating the Site_Spoke_A and Site_Spoke_B peers, create the peer Site_FW_Hub using the following values:

- **remote gateway**: Firewall of the Hub (object **Pub_FW_Hub**),
- **certificate**: the certificate of the Spoke B Firewall.

Creating tunnels

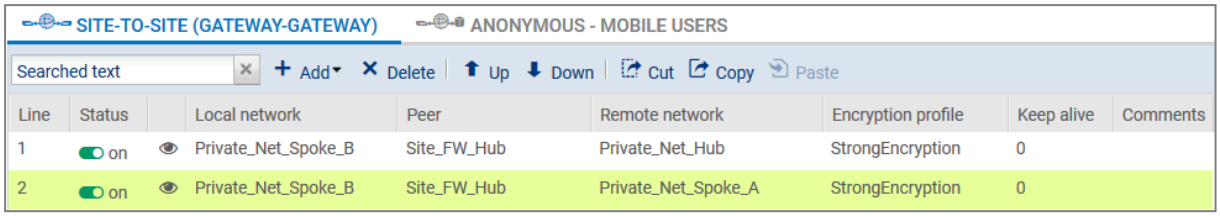
Spoke A site

Following the method described in the paragraph Creating tunnels, create the two tunnels needed:



Spoke B site

Following the method described in the paragraph Creating tunnels, create the two tunnels needed:

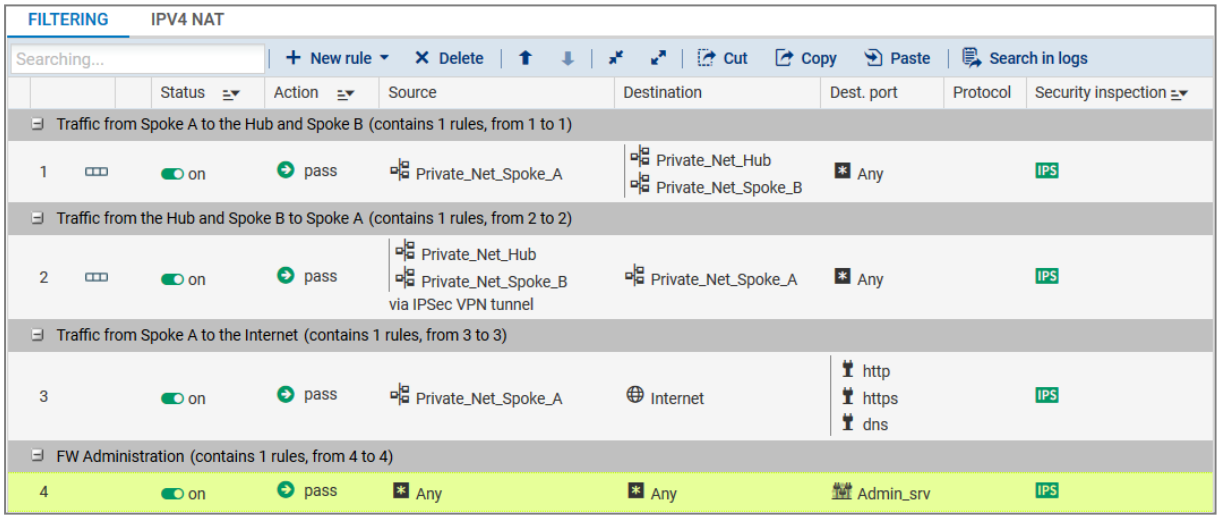


Creating filtering rules

In this tutorial, traffic between private networks is voluntarily not specified (destination port: ANY). To optimize performance (save bandwidth and machine resources), it is important to refine the filtering on satellite sites (authorized protocols, ports, etc) in order to prevent unnecessary packets from going through the tunnels. This filtering policy will also be on the Hub site.

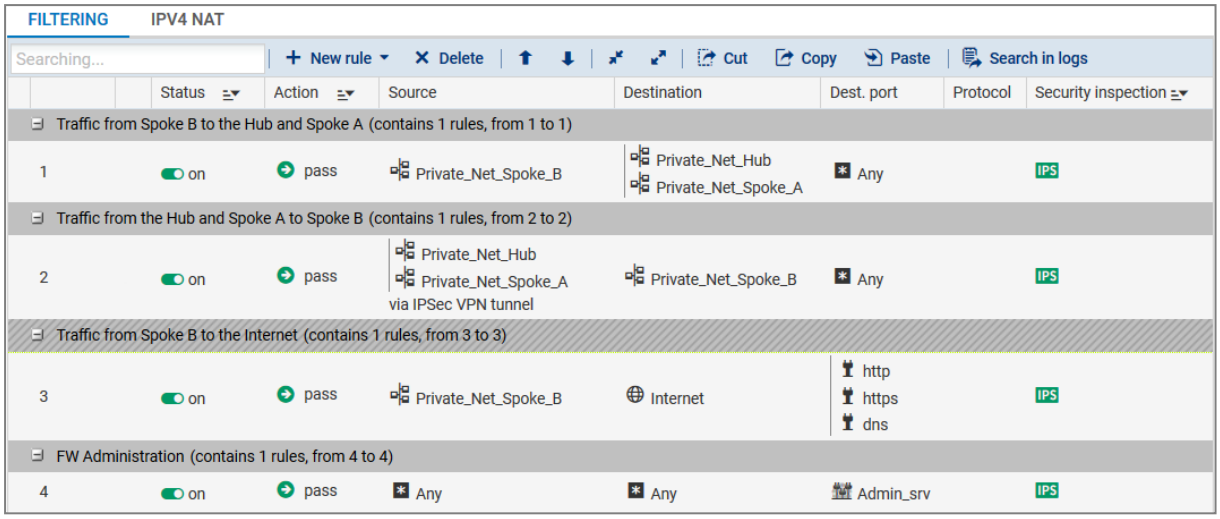
Spoke A site

Define the filtering rules needed for exchanges between Spoke A and Spoke B, Spoke A and the Hub as well as local traffic to the Internet:



Spoke B site

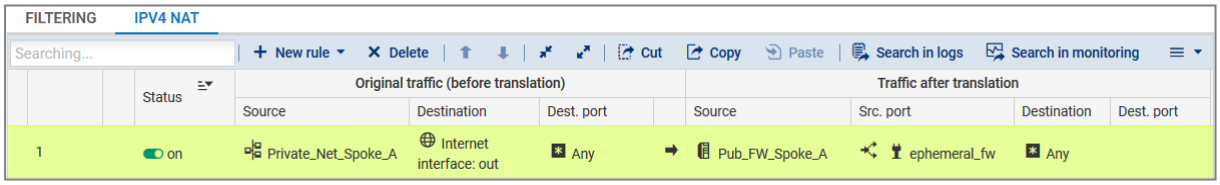
Define the filtering rules needed for exchanges between Spoke B and Spoke A, Spoke B and the Hub as well as local traffic to the Internet:



Creating NAT rule

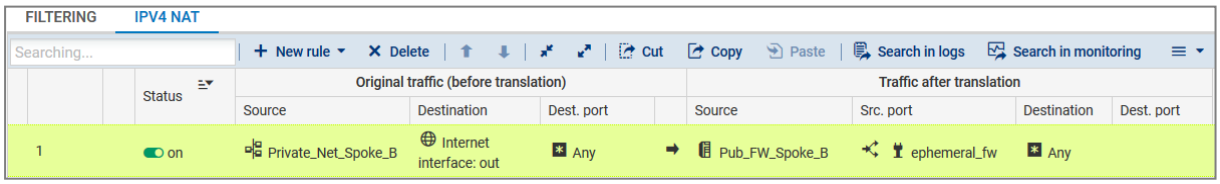
Spoke A site

To allow hosts on the network Private_Net_Spoke_A to access the internet, create the following NAT rule:



Spoke B site

To allow hosts on the network Private_Net_Spoke_B to access the internet, create the following NAT rule:



Case no.2: configuring the central site (Hub)

On the Hub site you will have to:

- Defining the IPsec peer,
- Creating tunnels,
- Creating filtering rules,
- Creating NAT rule.

Defining the IPsec peer

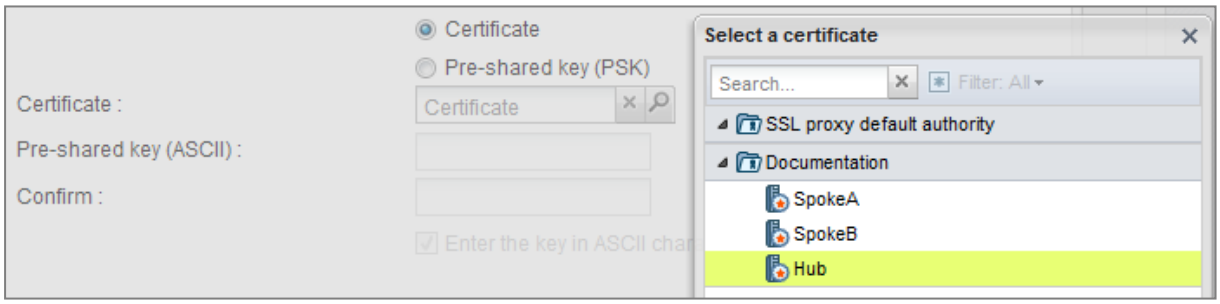
Following the method described in the paragraph Creating the Site_Spoke_A and Site_Spoke_B peers in Case no. 1, create both peers Site_Spoke_A and Site_Spoke_B.

To define Site_Spoke_A, use the following values:

- **remote gateway**: Firewall of the Spoke A site (object Pub_FW_Spoke_A),
- **Certificate**: the certificate of the Hub Firewall.

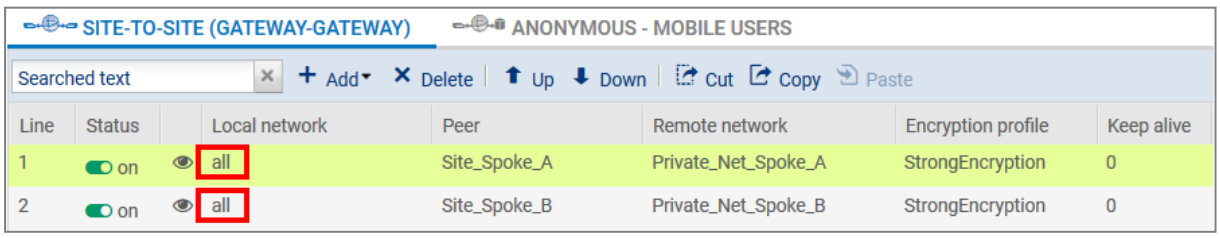
To define Site_Spoke_B:

- **remote gateway**: Firewall of the Spoke B site (object Pub_FW_Spoke_B),
- **Certificate**: the certificate of the Hub Firewall.



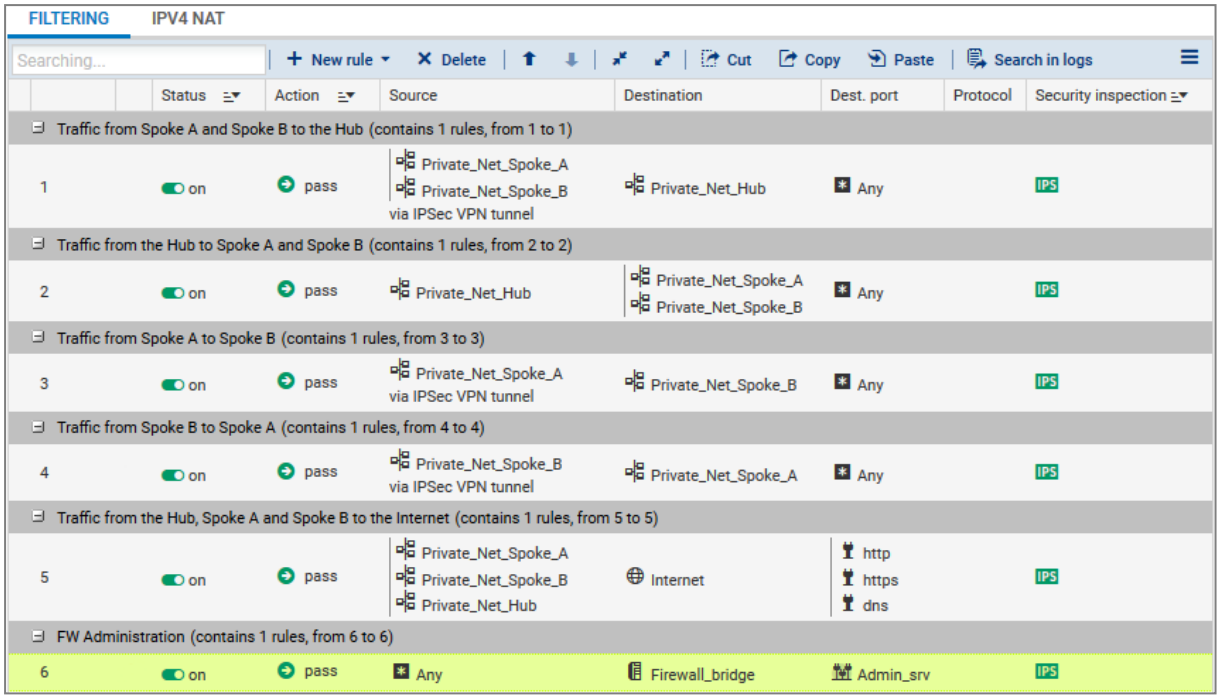
Creating tunnels

Follow the method described in the paragraph Creating tunnels in Case no. 1 to define the following VPN tunnels:



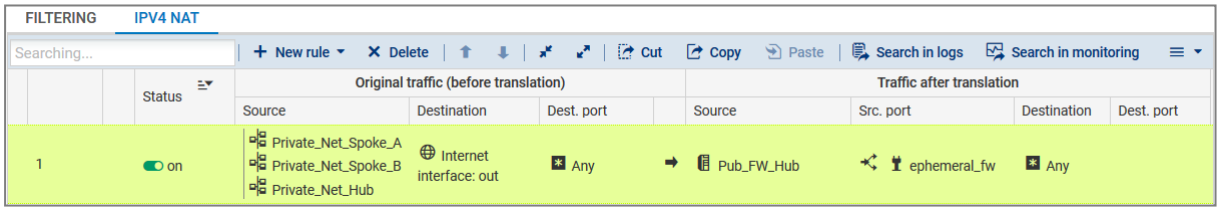
Creating filtering rules

Define the filtering rules needed for exchanges between Spoke sites, Spoke sites and the Hub as well as local traffic to the Internet:



Creating NAT rule

To allow all hosts on private networks to access the internet, create the following NAT rule:



Sources have been indicated individually in this rule, but obviously groups will need to be used once the number of satellite sites increases.

Case no.2: configuring the satellite sites Spoke A and Spoke B

In a Hub and Spoke configuration, a satellite site only knows one IPsec peer: the Firewall of the Hub site.

- Defining the IPsec peer,
- Creating tunnels,
- Creating filtering rules.

Defining the IPsec peer

Spoke A site

Following the method described in the paragraph Creating the Site_Spoke_A and Site_Spoke_B peers in Case no. 1, create the peer Site_FW_Hub using the following values:

- **remote gateway**: Firewall of the Hub (object **Pub_FW_Hub**),
- **certificate**: the certificate of the Spoke A Firewall.

Spoke B site

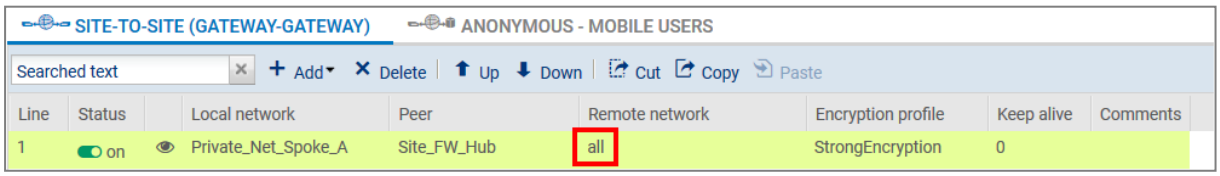
Following the method described in the paragraph Creating the Site_Spoke_A and Site_Spoke_B peers in Case no. 1, create the peer Site_FW_Hub using the following values:

- **remote gateway**: Firewall of the Hub (object **Pub_FW_Hub**),
- **certificate**: the certificate of the Spoke B Firewall.

Creating tunnels

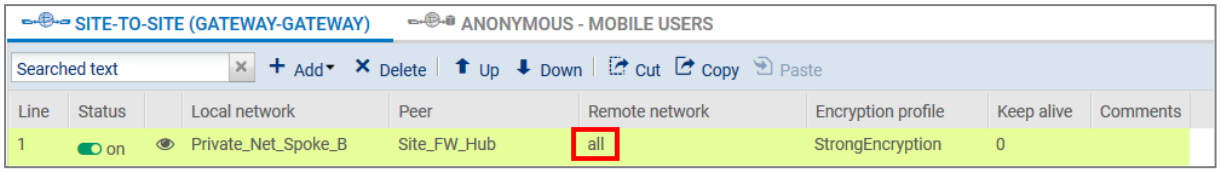
Spoke A site

Follow the method described in the paragraph Creating tunnels in Case no. 1 to define the following VPN tunnel:



Spoke B site

Follow the method described in the paragraph Creating tunnels in Case no. 1 to define the following VPN tunnel:

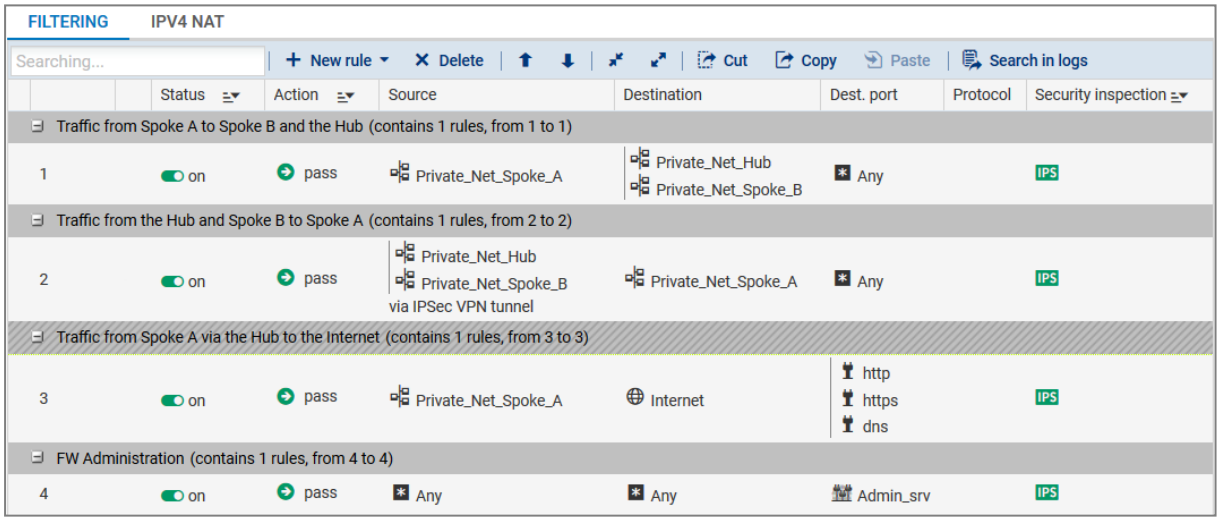


Creating filtering rules

In this tutorial, traffic between private networks is voluntarily not specified (destination port: ANY). To optimize performance (save bandwidth and machine resources), it is important to refine the filtering on satellite sites (authorized protocols, ports, etc) in order to prevent unnecessary packets from going through the tunnels. This filtering policy will also be on the Hub site.

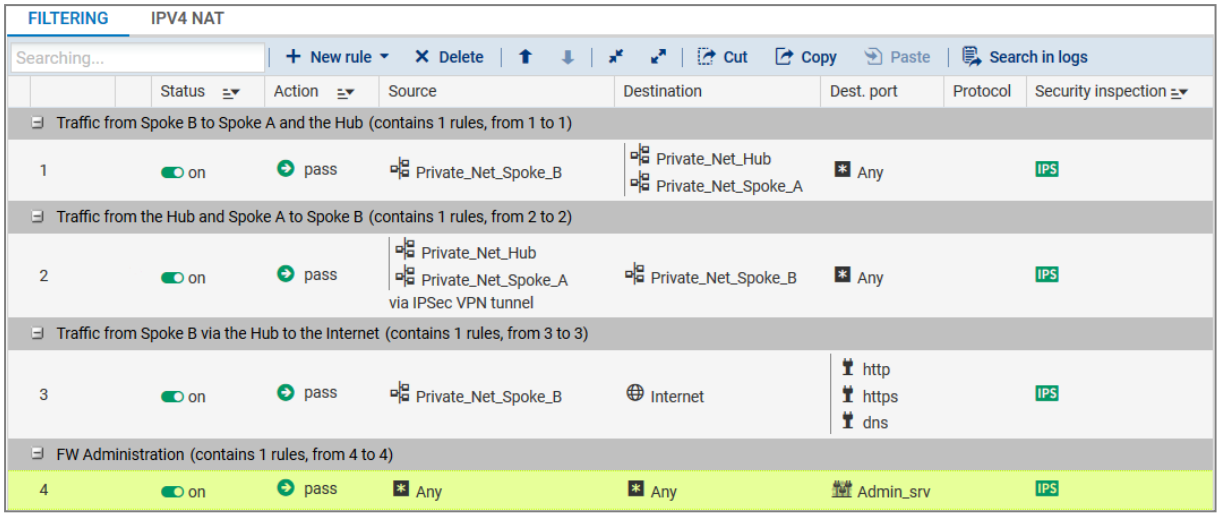
Spoke A site

Define the filtering rules needed for exchanges between Spoke A and Spoke B, Spoke A and the Hub as well as local traffic to the Internet (centralized on the Hub):



Spoke B site

Define the filtering rules needed for exchanges between Spoke B and Spoke A, Spoke B and the Hub as well as local traffic to the Internet (centralized on the Hub):



FILTERING | IPV4 NAT

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

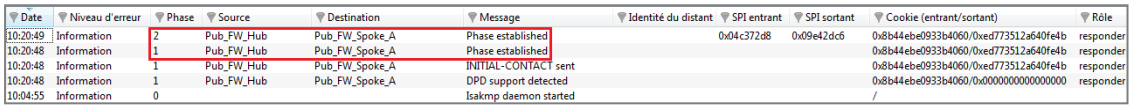
	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
Traffic from Spoke B to Spoke A and the Hub (contains 1 rules, from 1 to 1)							
1	on	pass	Private_Net_Spoke_B	Private_Net_Hub Private_Net_Spoke_A	Any		IPS
Traffic from the Hub and Spoke A to Spoke B (contains 1 rules, from 2 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

Checking the tunnel setup

From a client workstation located on the Spoke A site, first of all set up a connection to a host on the Hub site (using a ping for example, if you have allowed ICMP in all filtering rules), in order to test the setup of the first tunnel (Spoke A to Hub).

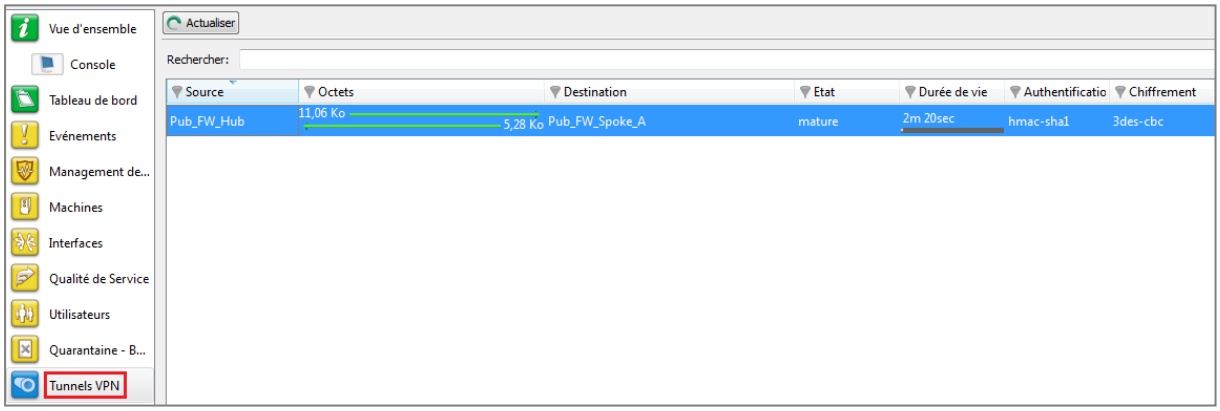
Via the Stormshield Network administration suite

Launch Stormshield Network Real-Time Monitor, log on to the Firewall of the Hub site through the program and click on the module **Logs** > **VPN**. Check that phases 1 and 2 took place correctly (message “Phase established”):



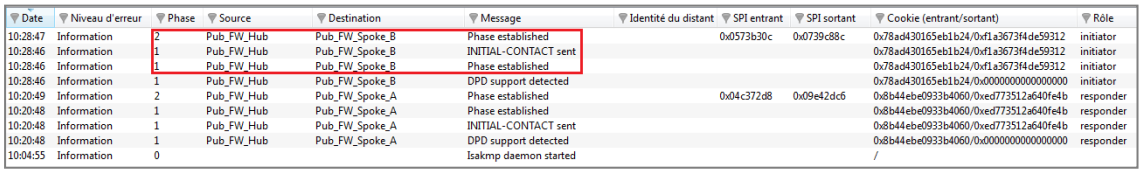
Date	Niveau d'erreur	Phase	Source	Destination	Message	Identité du distant	SPI entrant	SPI sortant	Cookie (entrant/sortant)	Rôle
10:20:49	Information	2	Pub_FW_Hub	Pub_FW_Spoke_A	Phase established		0x04c372d8	0x09e42dc6	0x8b44ebe0933b4060/0xed773512a640fe4b	responder
10:20:48	Information	1	Pub_FW_Hub	Pub_FW_Spoke_A	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				/	

In the module **VPN Tunnels**, you can also view the first tunnel as well as the amount of data exchanged:



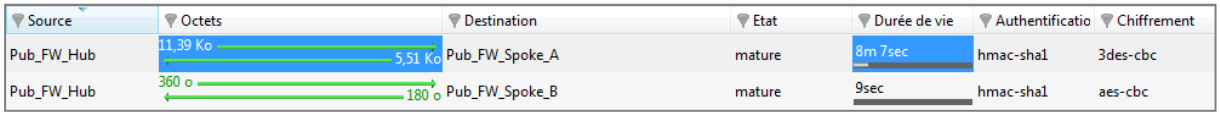
From the same client workstation on the Spoke A site, set up a connection to a host on the Spoke B site, in order to test the setup of the second tunnel (Hub to Spoke B).

In the module **Logs > VPN** in Stormshield Network Real-Time Monitor, check that phases 1 and 2 took place correctly (message “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				/	

In the module **VPN tunnels**, you can now see both tunnels:



Source	Octets	Destination	Etat	Durée de vie	Authentificatio	Chiffrement
Pub_FW_Hub	11,39 Ko / 5,51 Ko	Pub_FW_Spoke_A	mature	8m 7sec	hmac-sha1	3des-cbc
Pub_FW_Hub	360 o / 180 o	Pub_FW_Spoke_B	mature	9sec	hmac-sha1	aes-cbc

Information and diagnosis tools in console mode

showSPD command

The command *showSPD* displays the active IPsec policy on the Firewall. Its result will be the same whether tunnels have been set up or not.

In Case no.2 of this tutorial (all traffic via IPsec tunnel), executing this command on the Spoke A Firewall will return the following result:

```
>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/[illegible]/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/[illegible]/unique#16385
        spid=71 seq=0 pid=62800
        refcnt=1
```

The following information will be found:

- The local network and the remote network: "**192.168.0.0**/24 [any] **0.0.0.0**/0 [any]",
- The direction of the tunnel: "**out** ipsec",
- The IP addresses of the IPsec gateways: "esp/tunnel/**local address – remote address**",
- The ID of the Security Association (SA): "unique#**16385**".

showSAD command

The command *showSAD* lists the security information of SAs (Security Associations) set up on an IPsec gateway. Such information will be available only when tunnels have been set up.

In Case no.2 of this tutorial (all traffic via IPsec tunnel), executing this command on the Spoke A Firewall will return the following result:

```
[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
```

The following information will be found:

- IP address of the sending gateway – IP address of the receiving gateway.
- The SPI (Security Parameter Index): "spi=169172253 (**0x0a155d1d**)". The SPI is identified according to the direction of the SA displayed. As such, for an SA described in the direction remote IP – local IP, the SPI indicated is the incoming SPI. It therefore allows identifying incoming traffic.
- The encryption method used: "E: **3des-cbd**",
- The authentication method used: "A: **hmac-sha1**",
- The state of the tunnel: "state=**mature**". This state can be mature (the tunnel has been set up correctly: the SA is available and usable), larval (the SA is being negotiated) or dying (the SA's lifetime has expired and it will be renegotiated when the traffic requires it).
- The date/time the tunnel was set up and the current date/time,
- The number of bytes exchanged. current: **8840** (bytes).

Incident resolution - Common errors

- If you have chosen to use authentication by certificate, please refer to the section "Incident resolution - Common errors" in the tutorial "IPsec VPN – Authentication by certificate".
- If you have opted for authentication by pre-shared key, please refer to the section "Incident resolution - Common errors" in the tutorial "IPsec VPN – Authentication by pre-shared key".

Further reading

Additional information and responses to questions you may have are available in the Stormshield knowledge base (authentication required).

STORMSHIELD

documentation@stormshield.eu