



**STORMSHIELD**



TECHNICAL NOTE

**STORMSHIELD NETWORK SECURITY**

# IPSEC VPN: HUB AND SPOKE CONFIGURATION

Product concerned: SNS 1 and higher versions

Date: June 19, 2019

Reference: sns-en-IPSec\_VPN\_Hub\_And\_Spoke\_Technical\_Note



# Table of contents

IPSec VPN: Hub and Spoke Configuration .....	3
Architectures shown .....	3
Case no. 1: internal traffic via IPSec tunnels .....	3
Case no.2: all traffic via IPSec tunnels .....	3
Configuration requirements .....	5
Case no.1: internal traffic via IPSec tunnels .....	6
Configuring the Hub site .....	6
Creating the Site_Spoke_A peer .....	6
Creating the Site_Spoke_B peer .....	6
Creating tunnels .....	7
Filtering rules .....	7
NAT rule .....	8
Configuring the satellite sites Spoke A and Spoke B .....	8
Defining the IPSec peer .....	8
Creating tunnels .....	9
Filter rules .....	9
NAT rule .....	10
Case no.2: all traffic via IPSec tunnels .....	11
Configuring the central Hub site .....	11
Defining IPSec peers .....	11
Creating tunnels .....	11
Filtering rules .....	12
NAT rule .....	12
Configuring the satellite sites Spoke A and Spoke B .....	12
Defining the IPSec peer .....	12
Creating tunnels .....	13
Filter rules .....	13
Checking the tunnel setup .....	15
Via the Stormshield Network administration suite .....	15
Information and diagnosis tools in console mode .....	16
showSPD command .....	16
showSAD command .....	16
Incident resolution - Common errors .....	17



# IPSec VPN: Hub and Spoke Configuration

## Architectures shown

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

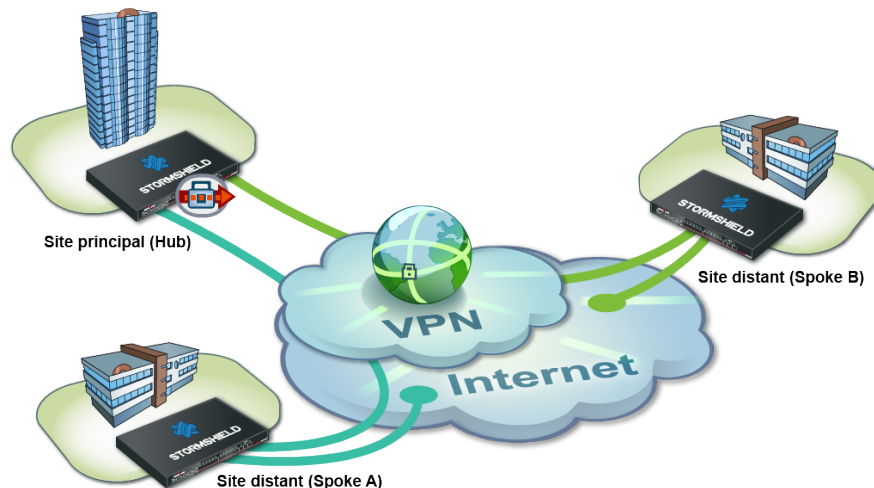
For details on operations regarding the PKI, please refer to the tutorial “IPSec VPN - authentication by certificate”.

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.

Please note that in the configuration we will describe in this document, each remote site owns only one local network.

### Case no. 1: internal traffic via IPSec tunnels

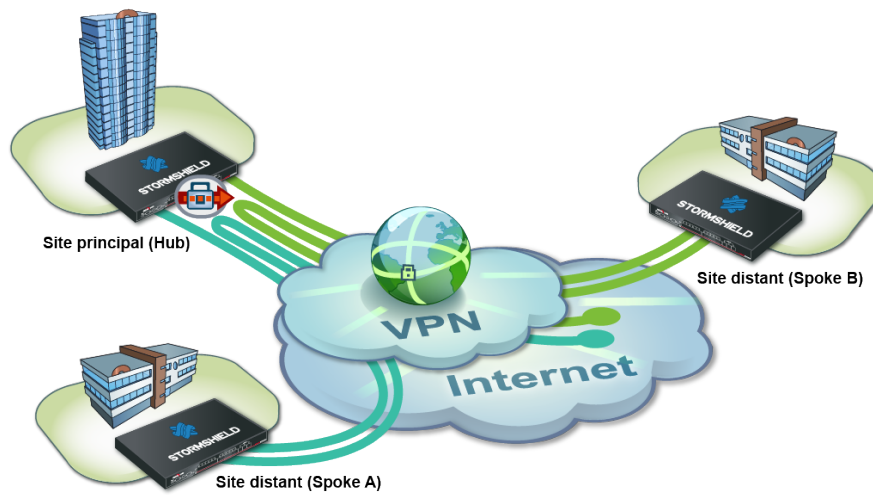
Only internal traffic between the three sites (Hub, Spoke A and Spoke B) goes through tunnels via the Hub. Internet traffic is managed locally on each site.



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:

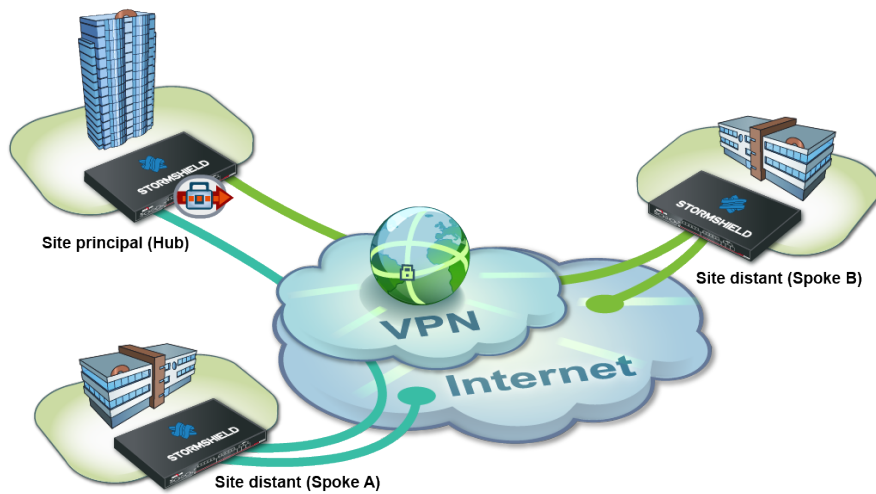
- the public IP address of the Hub Firewall: Pub\_FW\_Hub,
- the local network of the Hub site: Private\_Net\_Hub,
- the public IP address of the Spoke A Firewall: Pub\_FW\_Spoke\_A,
- the local network of the Spoke A site: Private\_Net\_Spoke\_A,
- the public IP address of the Spoke B Firewall: Pub\_FW\_Spoke\_B,
- the local network of the Spoke B site: Private\_Net\_Spoke\_B.

Check that your PKI has been set up:

- There is a certificate 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: internal traffic via IPsec tunnels

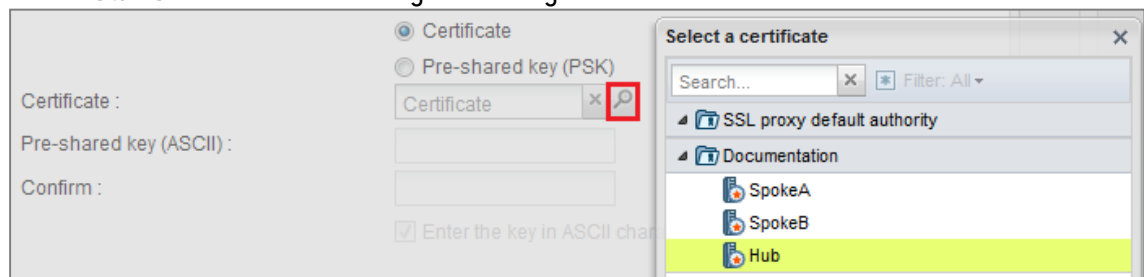


### Configuring the Hub site

#### Creating the Site\_Spoke\_A peer

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.



#### Creating the Site\_Spoke\_B peer

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.

ENCRIPTION POLICY - TUNNELS					
PEERS IDENTIFICATION ENCRYPTION PROFILES					
(8) Hub & Spoke - Internal Activate this policy Edit					
SITE-TO-SITE (GATEWAY-GATEWAY) ANONYMOUS - MOBILE USERS					
Searched text x + Add x Delete Up Down Cut Copy Insert					
Line	Stat...	Local network	Peer	Remote network	Encryption profile
1		Tunnel pour le trafic de Spoke A vers Spoke B			
2	on	Private_Net_Spoke_A	Site_Spoke_B	Private_Net_Spoke_B	GoodEncryption
3		Tunnel pour le trafic de Spoke B vers Spoke A			
4	on	Private_Net_Spoke_B	Site_Spoke_A	Private_Net_Spoke_A	GoodEncryption
5		Tunnel pour le trafic de Hub vers Spoke A			
6	on	Private_Net_Hub	Site_Spoke_A	Private_Net_Spoke_A	GoodEncryption
7		Tunnel pour le trafic de Hub vers Spoke B			
8	on	Private_Net_Hub	Site_Spoke_B	Private_Net_Spoke_B	GoodEncryption

## 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		NAT																									
Searched text								+ New rule		Delete		Up		Down		Expand all		Collapse all		Cut		Copy		Paste			
	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection																				
Accès au réseau de Hub depuis Spoke A et Spoke B (trafic entrant)																											
1	on	pass	Private_Net_Spoke_A Private_Net_Spoke_B via IPsec VPN tunnel	Private_Net_Hub	Any		IPS																				
Accès aux réseaux de Spoke A et Spoke B depuis Hub (trafic sortant)																											
2	on	pass	Private_Net_Hub	Private_Net_Spoke_A Private_Net_Spoke_B	Any		IPS																				
Accès de Spoke A au réseau de Spoke B (trafic traversant)																											
3	on	pass	Private_Net_Spoke_A via IPsec VPN tunnel	Private_Net_Spoke_B	Any		IPS																				
Accès de Spoke B au réseau de Spoke A (trafic traversant)																											
4	on	pass	Private_Net_Spoke_B via IPsec VPN tunnel	Private_Net_Spoke_A	Any		IPS																				
Accès Internet local du site Hub (trafic sortant)																											
5	on	pass	Private_Net_Hub	Internet	http https dns		IPS																				
Administration du FW																											
6	on	pass	Any	Any	Admin_srv		IPS																				

## NAT rule

To allow hosts on the network Private\_Net\_Hub to access the internet, create the following NAT rule:

FILTERING		NAT						
Searched text		<a href="#">+ New rule</a> <a href="#">Delete</a> <a href="#">Up</a> <a href="#">Down</a> <a href="#">Expand all</a> <a href="#">Collapse all</a> <a href="#">Cut</a> <a href="#">Copy</a> <a href="#">Paste</a>						
	Status	Source	Destination	Dest. port	Traffic after translation			
		Original traffic (before translation)			Source	Src. port	Destination	Dest. port
1	on	Private_Net_Hub	Internet interface: out	Any	Pub_FW_Hub	ephemeral	Any	Options

## 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.

## Defining the IPsec peer

### Spoke A site

Following the method described in the paragraph [Configuring the Hub site / Defining IPsec 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 [Configuring the Hub site / Defining IPsec 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 [Configuring the Hub site / Creating tunnels](#), create the two tunnels needed:

SITE-TO-SITE (GATEWAY-GATEWAY)					
ANONYMOUS - MOBILE USERS					
Line	Stat...	Local network	Peer	Remote network	Encryption profile
1		Tunnel pour le trafic entre Spoke A et Hub			
2	on	Private_Net_Spoke_A	Site_FW_Hub	Private_Net_Hub	GoodEncryption
3		Tunnel pour le trafic entre Spoke A et Spoke B			
4	on	Private_Net_Spoke_A	Site_FW_Hub	Private_Net_Spoke_B	GoodEncryption

### Spoke B site

Following the method described in the paragraph [Configuring the Hub site / Creating tunnels](#), create the two tunnels needed:

SITE-TO-SITE (GATEWAY-GATEWAY)					
ANONYMOUS - MOBILE USERS					
Line	Stat...	Local network	Peer	Remote network	Encryption profile
1		Tunnel pour le trafic entre Spoke B et Hub			
2	on	Private_Net_Spoke_B	Site_FW_Hub	Private_Net_Hub	GoodEncryption
3		Tunnel pour le trafic entre Spoke B et Spoke A			
4	on	Private_Net_Spoke_B	Site_FW_Hub	Private_Net_Spoke_A	GoodEncryption

## Filter 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:

FILTERING							
NAT							
Searched text							
+ New rule - Delete - Up - Down - Expand all - Collapse all - Cut - Copy - Paste							
Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	
Accès de Spoke A aux réseaux de Hub et Spoke B (trafic sortant)							
1	on	pass	Private_Net_Spoke_A	Private_Net_Hub Private_Net_Spoke_B	Any	IPS	
Accès de Hub et Spoke B au réseau de Spoke A (trafic entrant)							
2	on	pass	Private_Net_Hub Private_Net_Spoke_B via IPsec VPN tunnel	Private_Net_Spoke_A	Any	IPS	
Accès Internet local du site Spoke A (trafic sortant)							
3	on	pass	Private_Net_Spoke_A	Internet	http https dns	IPS	
Administration du Firewall							
4	on	pass	Any	Any	Admin_srv	IPS	



## 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:

FILTERING NAT							
Searched text							
	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
Accès de Spoke B aux réseaux de Hub et Spoke A (trafic sortant)							
1	on	pass	Private_Net_Spoke_B	Private_Net_Spoke_A Private_Net_Hub	Any		IPS
Accès de Hub et Spoke A au réseau de Spoke B (trafic entrant)							
2	on	pass	Private_Net_Spoke_A Private_Net_Hub via IPsec VPN tunnel	Private_Net_Spoke_B	Any		IPS
Accès Internet local du site Spoke B (trafic sortant)							
3	on	pass	Private_Net_Spoke_B	Internet	http https dns		IPS
Administration du Firewall							
4	on	pass	Any	Any	Admin_srv		IPS

## NAT rule

### Spoke A site

To allow hosts on the network Private\_Net\_Spoke\_A to access the internet, create the following NAT rule:

FILTERING NAT									
Searched text									
	Status	Source	Destination	Dest. port	Traffic after translation				
					Source	Src. port	Destination	Dest. port	Options
1	on	Private_Net_Spoke_A	Internet interface: out	Any	Pub_FW_Spoke_A	ephemeral	Any		

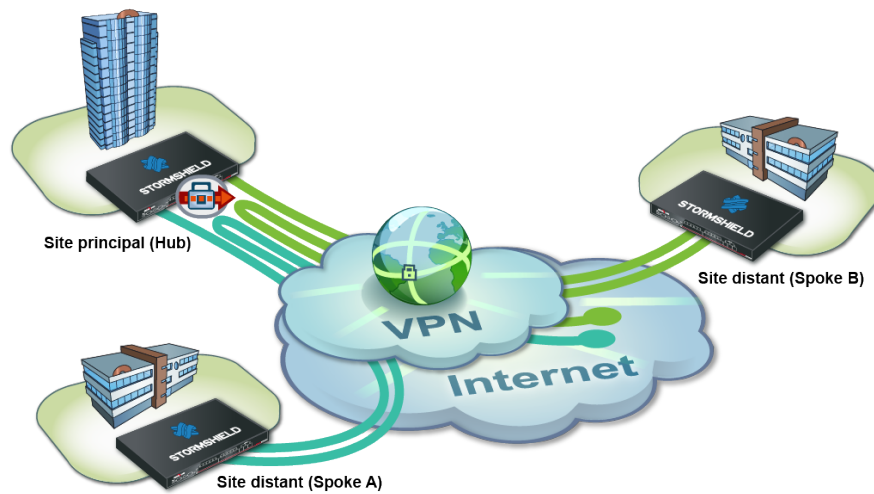
### Spoke B site

To allow hosts on the network Private\_Net\_Spoke\_B to access the internet, create the following NAT rule:

FILTERING NAT									
Searched text									
	Status	Source	Destination	Dest. port	Traffic after translation				
					Source	Src. port	Destination	Dest. port	Options
1	on	Private_Net_Spoke_B	Internet interface: out	Any	Pub_FW_Spoke_B	ephemeral	Any		



## Case no.2: all traffic via IPsec tunnels



### Configuring the central Hub site

#### Defining IPsec peers

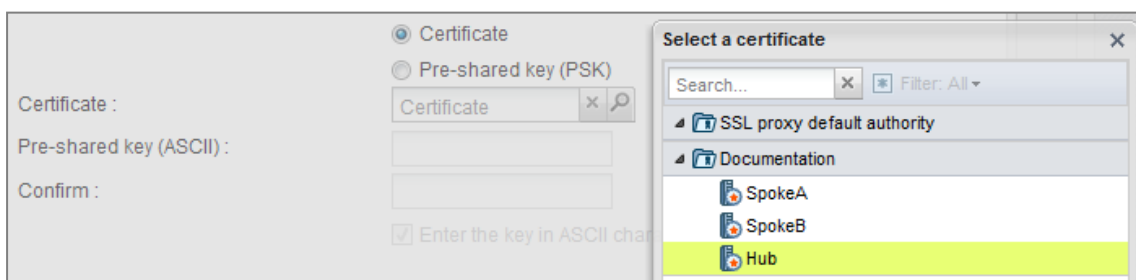
Following the method described in the paragraph [Configuring the Hub site / Defining IPsec peers](#) in Case no. 1, create both peers Site\_Spoke\_A and Site\_Spoke\_B.

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 [Configuring the Hub site / Creating tunnels](#) in Case no. 1 to define the following VPN tunnels:



SITE-TO-SITE (GATEWAY-GATEWAY)		ANONYMOUS - MOBILE USERS			
Line	Stat...	Local network	Peer	Remote network	Encryption profile
1		Tunnel pour l'ensemble du trafic entre tous les autres réseaux (Spoke B, Hub, Internet) et Spoke A			
2	on	all	Site_Spoke_A	Private_Net_Spoke_A	GoodEncryption
3		Tunnel pour l'ensemble du trafic entre tous les autres réseaux (Spoke A, Hub, Internet) et Spoke B			
4	on	all	Site_Spoke_B	Private_Net_Spoke_B	GoodEncryption

## 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		NAT				
	Status	Action	Source	Destination	Dest. port	Security inspection
Accès de Spoke A et Spoke B au réseau de Hub (trafic entrant)						
1	on	pass	Private_Net_Spoke_A Private_Net_Spoke_B via IPsec VPN tunnel	Private_Net_Hub	Any	IPS
Accès de Hub aux réseaux de Spoke A et Spoke B (trafic sortant)						
2	on	pass	Private_Net_Hub	Private_Net_Spoke_A Private_Net_Spoke_B	Any	IPS
Accès de Spoke A au réseau de Spoke B (trafic traversant)						
3	on	pass	Private_Net_Spoke_A via IPsec VPN tunnel	Private_Net_Spoke_B	Any	IPS
Accès de Spoke B au réseau de Spoke A (trafic traversant)						
4	on	pass	Private_Net_Spoke_B via IPsec VPN tunnel	Private_Net_Spoke_A	Any	IPS
Accès de Hub, Spoke A et Spoke B à Internet						
5	on	pass	Private_Net_Spoke_A Private_Net_Spoke_B Private_Net_Hub	Internet	http https dns	IPS
Administration du Firewall						
6	on	pass	Any	Firewall_bridge	Admin_srv	IPS

## NAT rule

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

FILTERING		NAT							
	Status	Source	Destination	Dest. port	Source	Src. port	Destination	Dest. port	Options
1	on	Private_Net_Hub Private_Net_Spoke_A Private_Net_Spoke_B	Internet interface: out	Any	Pub_FW_Hub	ephemeral	Any		

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

## Configuring the satellite sites Spoke A and Spoke B

### Defining the IPsec peer

#### Spoke A site

Following the method described in the paragraph [Configuring the Hub site / Defining IPsec 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 [Configuring the Hub site / Defining IPSec 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 [Configuring the Hub site / Creating tunnels](#) in Case no. 1 to define the following VPN tunnel:

SITE-TO-SITE (GATEWAY-GATEWAY)					
ANONYMOUS - MOBILE USERS					
Searched text X + Add - X Delete   Up Down   Cut Copy Insert					
Line	Stat...	Local network	Peer	Remote network	Encryption profile
1		Tunnel pour l'ensemble du trafic entre Spoke A et les autres réseaux (Spoke B, Hub, Internet)			
2	on	Private_Net_Spoke_A	Site_FW_Hub	all	GoodEncryption

### Spoke B site

Follow the method described in the paragraph [Configuring the Hub site / Creating tunnels](#) in Case no. 1 to define the following VPN tunnel:

SITE-TO-SITE (GATEWAY-GATEWAY)					
ANONYMOUS - MOBILE USERS					
Searched text X + Add - X Delete   Up Down   Cut Copy Insert					
Line	Stat...	Local network	Peer	Remote network	Encryption profile
1		Tunnel pour l'ensemble du trafic entre Spoke B et les autres réseaux (Spoke A, Hub, Internet)			
2	on	Private_Net_Spoke_B	Site_FW_Hub	all	GoodEncryption

## Filter 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):



FILTERING		NAT																							
Searched text								+ New rule ▾		Delete		↑ Up		↓ Down		Expand all		Collapse all		Cut		Copy		Paste	
	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection																		
Accès de Spoke A aux réseaux de Hub et Spoke B (trafic sortant)																									
1	● on	pass	Private_Net_Spoke_A	Private_Net_Hub Private_Net_Spoke_B	Any		IPS																		
Accès de Hub et Spoke B au réseau de Spoke A (trafic entrant)																									
2	● on	pass	Private_Net_Hub Private_Net_Spoke_B via IPsec VPN tunnel	Private_Net_Spoke_A	Any		IPS																		
Accès à Internet du site Spoke A via le site Hub (trafic sortant)																									
3	● on	pass	Private_Net_Spoke_A	Internet	http https dns		IPS																		
Administration du Firewall																									
4	● on	pass	Any	Any	Admin_srv		IPS																		

## 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		NAT						
Searched text <input type="text" value="x"/>								
+ New rule ▾ × Delete   ↑ Up ↓ Down   Expand all Collapse all   Cut Copy Paste								
	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	
Accès de Spoke B aux réseaux de Hub et Spoke A (trafic sortant)								
1	● on	pass	Private_Net_Spoke_B	Private_Net_Spoke_A Private_Net_Hub	Any		IPS	
Accès de Hub et Spoke A au réseau de Spoke B (trafic entrant)								
2	● on	pass	Private_Net_Spoke_A Private_Net_Hub via IPsec VPN tunnel	Private_Net_Spoke_B	Any		IPS	
Accès à Internet du site Spoke B via le site Hub (trafic sortant)								
3	● on	pass	Private_Net_Spoke_B	Internet	http https dns		IPS	
Administration du Firewall								
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:

i

Vue d'ensemble

Console

Tableau de bord

Evénements

Management de...

Machines

Interfaces

Qualité de Service

Utilisateurs

Quarantaine - B...

Tunnels VPN

Actualiser

Rechercher:

Source	Octets	Destination	Etat	Durée de vie	Authenticatio	Chiffrement
Pub_FW_Hub	11,06 Ko	5,28 Ko Pub_FW_Spoke_A	mature	2m 20sec	hmac-sha1	3des-cbc

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
10:20:49	Information	1	Pub_FW_Hub	Pub_FW_Spoke_B	DPD support detected				0x8b44ebe0933b4060/0x0000000000000000	responder
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	Authenticatio	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/192.168.0.70-192.168.0.71/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/192.168.0.71-192.168.0.70/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:

```
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

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”.



**STORMSHIELD**

[documentation@stormshield.eu](mailto:documentation@stormshield.eu)

*All images in this document are for representational purposes only, actual products may differ.*

*Copyright © Stormshield 2019. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.*