

STORMSHIELD



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	4
Architectures shown	5
Case no. 1: internal traffic via IPsec tunnels Case no.2: all traffic via IPsec tunnels	5 5
Configuration requirements	6
Case no.1: configuring the central site (Hub) Creating the Site_Spoke_A and Site_Spoke_B peers Creating tunnels Creating filtering rules Creating NAT rule	7 7 7 8 9
Case no.1: configuring the satellite sites Spoke A and Spoke B	10
Defining the IPsec peer Spoke A site Spoke B site Creating tunnels Spoke A site Spoke B site Creating filtering rules Spoke A site	10 10 10 10 10 10 10 11 11
Spoke B site	11
Creating NAI rule	12
Spoke B site	
Case no.2: configuring the central site (Hub)	13
Defining the IPsec peer	13
Creating fulles	13
Creating NAT rule	14
Case no.2: configuring the satellite sites Spoke A and Spoke B	15
Defining the IPsec peer	
Spoke A site Spoke B site	15
Creating tunnels	15
Spoke A site	15
Creating filtering rules	
Spoke A site	16
Spoke B site	16
Checking the tunnel setup	18
Via the Stormshield Network administration suite	
Information and diagnosis tools in console mode	19 19
showSAD command	
Incident resolution - Common errors	20









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.
- 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.

IDENTIFYING THE PEER - PEER CREATION WIZARD			
		SELECT A CERTIFICATE	\approx
		Search X EFilter: All -	
		SSL proxy default authority	
		documentation.stormshield.eu	
		E SpokeA	
		SpokeB	
	Certificate	📰 Hub	
	O Pre-shared key (PSK)	FW-Site-A.documentation.stormshield.eu	
Certificate :	documentation.stori $\times P$		
Pre-shared key (ASCII) :			
Confirm :			

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.

D+®+ 0	SITE-TO-SITE (GATEWAY-GATEWAY) ANONYMOUS - MOBILE USERS										
Search	Searched text × Add × × Delete 1 Up ↓ Down 1 🖾 Cut 🖸 Copy 🕑 Paste										
Line	Status		Local network	Peer	Remote network	Encryption profile	Keep alive	Comments			
1	💽 on	۲	Private_Net_Spoke_A	Site_Spoke_B	Private_Net_Spoke_B	StrongEncryption	0				
2	💽 on	۲	Private_Net_Spoke_B	Site_Spoke_A	Private_Net_Spoke_A	StrongEncryption	0				
3	💽 on	٢	Private_Net_Hub	Site_Spoke_A	Private_Net_Spoke_A	StrongEncryption	0				
4	💽 on	۲	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:

FIL	TERING	IPV4 NAT								
Sear	ching		+ New rule	✓ X Delete ↑ ↓	💉 🛃 🖻 Cut 🕑 C	opy 🕑 Paste	🛛 🛱 Search in logs 🛛 🚍			
		Status 🖃	Action =	Source	Destination	Dest. port	Protocol Security inspection			
Ξ	I Traffic from Spoke A and B to the Hub (contains 1 rules, from 1 to 1)									
1		on	🕄 🗎 pass	명 Private_Net_Spoke_A 명 Private_Net_Spoke_B via IPSec VPN tunnel	명 Private_Net_Hub	* Any	IPS			
Ξ	Traffic from	the Hub to Spoke	A and B (contain	s 1 rules, from 2 to 2)						
2		💽 on	🕤 🗎 pass	Private_Net_Hub	Private_Net_Spoke_A	* Any	IPS			
Ξ	Traffic from	Spoke A to Spoke	B (contains 1 ru	les, from 3 to 3)						
3		💽 on	🕤 🗎 pass	며불 Private_Net_Spoke_A via IPSec VPN tunnel	Private_Net_Spoke_B	* Any	IPS			
Ξ	Traffic from	Spoke B to Spoke	A (contains 1 ru	les, from 4 to 4)						
4		💽 on	🕤 🗎 pass	며불 Private_Net_Spoke_B via IPSec VPN tunnel	Private_Net_Spoke_A	* Any	IPS			
Ξ	Traffic from	the Hub to the Inte	ernet (contains 1	rules, from 5 to 5)						
5		 on 	pass	Pa Private_Net_Hub	Internet	T http T https T dns	IPS			
Ξ	FW Adminis	tration (contains 1	I 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:

FILT	ERING	IPV4 NAT								
Searching		+ New rule - X	Delete 1 🖡	* * B	Cut	🛃 Copy 🛛 🕑 Pa	aste 🕴 🗒 Search in logs	🚱 Search i	n monitoring	
	Ctatue =▼	Origin	al traffic (before trans	lation)		Traffic after translation				
		Status	Source	Destination	Dest. port		Source	Src. port	Destination	Dest. port
1		🜑 on	Private_Net_Hub	Internet interface: out	* Any	+	Pub_FW_Hub	🛠 🖠 ephemeral_fw	* Any	





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:

-	SITE-TO-SITE (GATEWAY-GATEWAY)									
Search	Searched text 🗙 + Add - X Delete 1 Up I Down 1 Ct Lt Copy Deste									
Line	Status		Local network	Peer	Remote network	Encryption profile	Keep alive	Comments		
1	💽 on	۲	Private_Net_Spoke_A	Site_FW_Hub	Private_Net_Hub	StrongEncryption	0			
2	🜑 on	٢	Private_Net_Spoke_A	Site_FW_Hub	Private_Net_Spoke_B	StrongEncryption	0			

Spoke B site

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





 +	SITE-TO-SITE (GATEWAY-GATEWAY) SHORE ANONYMOUS - MOBILE USERS									
Search	Searched text × Add × × Delete 1 Up I Down 1 C Cut C Copy 2 Paste									
Line	Status		Local network	Peer	Remote network	Encryption profile	Keep alive	Comments		
1	💽 on	۲	Private_Net_Spoke_B	Site_FW_Hub	Private_Net_Hub	StrongEncryption	0			
2	💽 on	۲	Private_Net_Spoke_B	Site_FW_Hub	Private_Net_Spoke_A	StrongEncryption	0			

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:

FILTERING	IPV4 NAT						
Searching		+ New rule	▼ X Delete ↑ ↓	📲 🖉 🚰 Cut 🖙 Co	py 🕑 Paste	🛛 🗒 Searc	h in logs
	Status ≞▼	Action =	Source	Destination	Dest. port	Protocol	Security inspection =-
I Traffic f	from Spoke A to the Hu	b and Spoke B (contains 1 rules, from 1 to 1)				
1 ===	on	pass	Private_Net_Spoke_A	Pivate_Net_Hub	* Any		IPS
E Traffic f	from the Hub and Spok	e B to Spoke A (contains 1 rules, from 2 to 2)				
2 ===	on	🕤 pass	며 Private_Net_Hub 며칠 Private_Net_Spoke_B via IPSec VPN tunnel	Private_Net_Spoke_A	* Any		IPS
E Traffic f	from Spoke A to the Int	ernet (contains 1	I rules, from 3 to 3)				
3	on	🕤 pass	Parivate_Net_Spoke_A	Internet	İ httpİ httpsİ dns		IPS
😑 🛛 FW Adr	ninistration (contains 1	I rules, from 4 to	4)				
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:





FILT	ERING	IPV4 NAT					
Searc	hing		+ New rule	▪ X Delete ↑ ↓ :	🦨 🖉 🚰 Cut 🛛 🗁 Co	py 🕑 Paste 🗒 Sea	rch in logs
		Status 🚉	Action =	Source	Destination	Dest. port Protocol	Security inspection =-
91	Traffic from	Spoke B to the Hu	ib and Spoke A (contains 1 rules, from 1 to 1)			
1		💽 on	pass	Private_Net_Spoke_B	Parivate_Net_Hub	* Any	IPS
91	Traffic from t	he Hub and Spok	e A to Spoke B (contains 1 rules, from 2 to 2)			
2		on	pass	명 Private_Net_Hub 명 Private_Net_Spoke_A via IPSec VPN tunnel	Private_Net_Spoke_B	X Any	IPS
	Traffic from	Spoke B to the Int	ernet (contains	1 rules, from 3 to 3)			
3		🔹 on	pass	Pa Private_Net_Spoke_B	Internet	I http I https I dns	IPS
Ð	FW Administ	ration (contains 1	1 rules, from 4 to	4)			
4		 on 	pass	* Any	* Any	Madmin_srv	IPS

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:

FILTERING	IPV4 NAT								
Searching		+ New rule - × De	elete 🕇 🖡	🗶 🖉 🕴 🗁 CL	rt	🔁 Copy 🛛 🕥 Paste	🗒 Search in logs 🛛	Search in moni	toring \equiv \bullet
Ctatua =*	Original	traffic (before transla	tion)			Traffic after transla	tion		
	Status	Source	Destination	Dest. port		Source	Src. port	Destination	Dest. port
1	💽 on	Private_Net_Spoke_A	Internet interface: out	* Any	+	Pub_FW_Spoke_A	🛠 🖠 ephemeral_fw	* Any	

Spoke B site

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

FILTERING	IPV4 NAT								
Searching		+ New rule - × De	lete 🕇 👢	💒 🖉 🗁 Cu	rt	🔁 Copy 🛛 🕑 Paste 🛛	🗒 Search in logs 🛛 🖥	Search in moni	toring \equiv \bullet
	Status =*	Original	traffic (before transla	tion)			Traffic after transla	tion	
	Status	Source	Destination	Dest. port		Source	Src. port	Destination	Dest. port
1	on	Private_Net_Spoke_B	Internet interface: out	* Any	•	Pub_FW_Spoke_B	⊀ Ï ephemeral_fw	* Any	







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.

	Oertificate	Select a certificate	×
	Pre-shared key (PSK)	Search X Filter: All -	
Certificate :	Certificate × P	SSL proxy default authority	
Pre-shared key (ASCII) :		In Documentation	
Confirm :		ᡖ SpokeA	
		🐌 SpokeB	
		Hub	

Creating tunnels

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

D+®+ 0	SITE-TO-SITE (GATEWAY-GATEWAY)							
Search	iearched text 🛛 🔺 + Add - 🎽 Delete 🕇 Up 🖡 Down 🛛 🔁 Cut 🖆 Copy 🕑 Paste							
Line	Status		Local network	Peer	Remote network	Encryption profile	Keep alive	
1	🜑 on	۲	all	Site_Spoke_A	Private_Net_Spoke_A	StrongEncryption	0	
2	💽 on	۲	all	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	▼ X Delete ↑ ↓	🗶 🛃 📴 Cut 🗁 Co	opy 🕑 Paste	🛛 🛱 Search in logs 🛛 🚍
	Status ≞•	Action =	Source	Destination	Dest. port	Protocol Security inspection =*
∃ Traffic f	from Spoke A and Spo	ke B to the Hub (contains 1 rules, from 1 to 1)			
1	💽 on	pass	명 Private_Net_Spoke_A 명 Private_Net_Spoke_B via IPSec VPN tunnel	며 Private_Net_Hub	* Any	IPS
Traffic f	from the Hub to Spoke	e A and Spoke B (contains 1 rules, from 2 to 2)			
2	 on 	\varTheta pass	며 Private_Net_Hub	Private_Net_Spoke_A	* Any	IPS
Traffic f	from Spoke A to Spoke	e B (contains 1 ru	les, from 3 to 3)			
3	 on 	\varTheta pass	P Private_Net_Spoke_A via IPSec VPN tunnel	P Private_Net_Spoke_B	* Any	IPS
I Traffic f	from Spoke B to Spoke	e A (contains 1 ru	les, from 4 to 4)			
4	💶 on	🕤 pass	명물 Private_Net_Spoke_B via IPSec VPN tunnel	Private_Net_Spoke_A	* Any	IPS
Traffic f	from the Hub, Spoke A	and Spoke B to t	he Internet (contains 1 rules, from	5 to 5)		
5	💽 on	pass	명 Private_Net_Spoke_A 명 Private_Net_Spoke_B 명 Private_Net_Hub	Internet	Ϊ http Ϊ https Ϊ dns	IPS
🗉 🛛 FW Adr	ministration (contains	1 rules, from 6 to	6)			
6	💽 on	🕤 pass	* Any	E Firewall_bridge	🕍 Admin_srv	IPS

Creating NAT rule

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

	FILTERING	IPV4 NAT								
S	earching		+ New rule - × De	lete 🕇 🕴	🗶 🛃 🖓 Cu	t	🔁 Copy 🛛 🕙 Paste 🛛	🗒 Search in logs 🛛 🗠	Search in monit	oring \equiv \bullet
		Status =*	Original	traffic (before transla	tion)			Traffic after translation	n	
		Status	Source	Destination	Dest. port		Source	Src. port	Destination	Dest. port
	1	🔍 on	Private_Net_Spoke_A P Private_Net_Spoke_B Private_Net_Hub	Internet interface: out	* Any	+	Pub_FW_Hub	✓ I ephemeral_fw	* Any	

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:

₽₩₽₩	SITE-TO	SITE	(GATEWAY-GATEWAY)	►+®+® ANONYMOUS	- MOBILE USERS			
Search	ed text		× + Add - × □	elete 🕇 Up 🖡 Down	n 🔄 Cut 🖸 Copy 👻 Pas	te		
Line	Status		Local network	Peer	Remote network	Encryption profile	Keep alive	Comments
1	🜑 on	۲	Private_Net_Spoke_A	Site_FW_Hub	all	StrongEncryption	0	

Spoke B site

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





-	■ SITE-TO	-SITE	(GATEWAY-GATEWAY)	⇔⊕+® ANONYMOUS	ANONYMOUS - MOBILE USERS					
Search	ned text		× + _{Add} - × □	Delete 🕇 Up 🖡 Down	n 🗁 Cut 🖆 Copy 👻 Pas	ste				
Line	Status		Local network	Peer	Remote network	Encryption profile	Keep alive	Comments		
1	🜑 on	۲	Private_Net_Spoke_B	Site_FW_Hub	all	StrongEncryption	0			

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):

FILTERIN	IG IPV4 NAT					
Searching		+ New rule	✓ X Delete ↑ ↓	🗶 🛃 🗁 Cut 🗁 Co	opy 🕙 Paste	🛱 Search in logs
	Status 🚉	Action =	Source	Destination	Dest. port	Protocol Security inspection =
∃ Traffi	c from Spoke A to Spoke	B and the Hub (contains 1 rules, from 1 to 1)			
1	on	pass	Parivate_Net_Spoke_A	Private_Net_Hub	* Any	IPS
∃ Traffi	c from the Hub and Spok	ke B to Spoke A (contains 1 rules, from 2 to 2)			
2	on	pass	P Private_Net_Hub P Private_Net_Spoke_B via IPSec VPN tunnel	P Private_Net_Spoke_A	* Any	IPS
∃ Traffi	c from Spoke A via the H	lub to the Interne	t (contains 1 rules, from 3 to 3)			
3	C on	pass	며 Private_Net_Spoke_A	Internet	i httpi httpsi dns	IPS
🗉 FW A	dministration (contains	1 rules, from 4 to	4)			
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	IPV4 NAT					
Searching		+ New rule	▪ X Delete ↑ ↓	🗚 🛃 🚰 Cut 🗁 Co	opy 🕑 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	* Any	IPS
∃ Traffic from	the Hub and Spol	ke A to Spoke B (contains 1 rules, from 2 to 2)			
2	 on 	pass	며 Private_Net_Hub 며칠 Private_Net_Spoke_A via IPSec VPN tunnel	P Private_Net_Spoke_B	* Any	IPS
I Traffic from	Spoke B via the H	lub to the Interne	t (contains 1 rules, from 3 to 3)			
3	 on 	pass	며 Private_Net_Spoke_B		httphttpsdns	IPS
😑 🛛 FW Admini	stration (contains	1 rules, from 4 to	4)			
4	🔍 on	🕤 pass	▲ Any	X 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	V 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	0×	x04c372d8	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				0x8b44ebe0933b4060/0x000000000000000	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:

Vue d'ensemble	C Actualiser							
Console	Rechercher:							
Tableau de bord	Source	🛡 Octets		Destination	🛡 Etat	🛡 Durée de vie	Authentificatio	💎 Chiffrement
Evénements	Pub_FW_Hub	11,06 Ko	5,28 Ko	Pub_FW_Spoke_A	mature	2m 20sec	hmac-sha1	3des-cbc
Management de								
Machines								
1 Interfaces								
Qualité de Service								
Utilisateurs								
Quarantaine - B								
Tunnels VPN								

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	V Source	Testination	🛡 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				0x8b44ebe0933b4060/0x000000000000000	responder
10:04:55	Information	0			Isakmp daemon started				/	

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

V 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/ - /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/ - /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:





10.2.50.253 10.40.3.71
esp mode=tunnel spi=219753044(0x0d192a54) regid=16386(0x00004002)
E: 3des-cbc 6093662d 55ec9528 818b6e7d 3f88d590 96a0d84a 80247f2c
A: hmac-sha1 e082ddd6 673a2af9 53d0b88f ea201de8 88c45da2
<pre>seq=0x00000031 replay=8 flags=0x00000000 state=mature</pre>
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
10.40.0.11.12.00.000
esp mode=tunnel spi=169172253(0x0a155d1d) regid=16385(0x00004001)
E: 3des-cbc c0100685 d48e5f27 686997d8 62d09ffb ed95d1c1 89cf9566
A: hmac-sha1 0fd9d769 f63ac3a0 62869791 4cca65a1 3445527d
<pre>seq=0x00000034 replay=8 flags=0x00000000 state=mature</pre>
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
<pre>sadb_seq=0 pid=29053 refcnt=2</pre>

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".







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







documentation@stormshield.eu

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

Copyright © Stormshield 2023. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.

