



**STORMSHIELD**



TECHNICAL NOTE

**STORMSHIELD NETWORK SECURITY**

# IPSEC VPN: AUTHENTICATION BY CERTIFICATE

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

Document last updated: December 9, 2019

Reference: [sns-en-IPSec\\_VPN\\_Authentication\\_Certificates\\_Technical\\_Note](#)



# Table of contents

- Getting started ..... 3
- Implementation ..... 4
  - Configuring the main site ..... 4
    - Creating network objects ..... 4
    - Creating the PKI infrastructure ..... 4
    - Creating IPsec tunnels ..... 6
    - Setting up filtering rules ..... 8
  - Configuring remote sites A and B ..... 9
    - Creating network objects ..... 10
    - Importing elements for authentication ..... 10
    - Creating IPsec tunnels ..... 11
    - Setting up filtering rules ..... 12
- Checking the tunnel setup ..... 14
  - Checking in Stormshield Network Realtime Monitor ..... 14
  - Incident resolution - Common errors ..... 14
- Further reading ..... 17



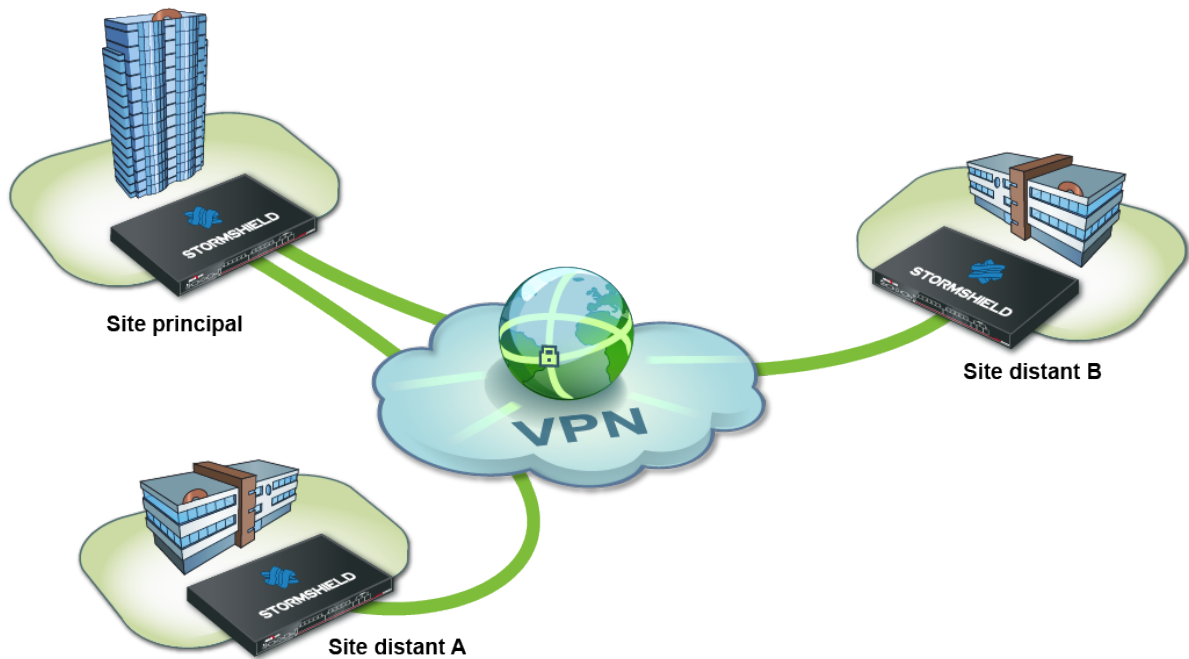
## Getting started

You wish to securely link up the various sites of your company currently linked via the Internet.

To do so, you need to create a site-to-site IPsec VPN star configuration. The authentication method shown in this tutorial is based on the verification of certificates (authentication by pre-shared key can also be set up).

This document describes the configuration to create, so that you can allow client workstations on two remote sites to access an intranet server on the main site through this tunnel in HTTP. Needless to say, this architecture is not restricted to just three sites.

The certification authority will be hosted by one of three IPsec gateways involved, the IPS-Firewall of the main site.





## Implementation

The purpose of this section is to describe the configuration needed on the various firewalls participating in the IPsec VPN.

### Configuring the main site

On the main site you will have to:

- Create the network objects of every site to connect,
- Create the PKI infrastructure,
- Create IPsec tunnels,
- Set up filtering rules.

### Creating network objects

The creation of an IPsec VPN connection between these three entities requires at least seven network objects:

- the local network of the main site: **Private\_Net\_Main\_Site**,
- the public address of the main Firewall: **Pub\_Main\_FW**,
- the local network of remote site A: **Private\_Net\_Site\_A**,
- the public address of the Firewall on remote site A: **Pub\_FW\_Site\_A**,
- the local network of remote site B: **Private\_Net\_Site\_B**,
- the public address of the Firewall on remote site B: **Pub\_FW\_Site\_B**,
- the intranet server to contact on the main site: **Intranet\_server**.

These objects have to be defined on each Firewall to interlink, in the menu: **Configuration > Objects > Network objects**.

### Creating the PKI infrastructure

#### Certification authority (CA)


In the menu **Configuration > Objects > Certificates and PKI**:

1. Click on **Add > Root Authority**.
2. Fill in the various required fields in the wizard:
  - **CN**: the name of your certification authority,
  - **ID**: the name entered in the CN field is suggested by default,
  - **Organization (O)**. Example: the name of your company,
  - **Organizational unit (OU)**. Example: the name of the CA user's department,
  - **State or province (ST)**,
  - **Country (C)**.



### CREATE ROOT AUTHORITY

#### CERTIFICATE AUTHORITY PROPERTIES



CN:

Identifier:

#### Authority attributes

Organization:

Organizational unit:

City (L):

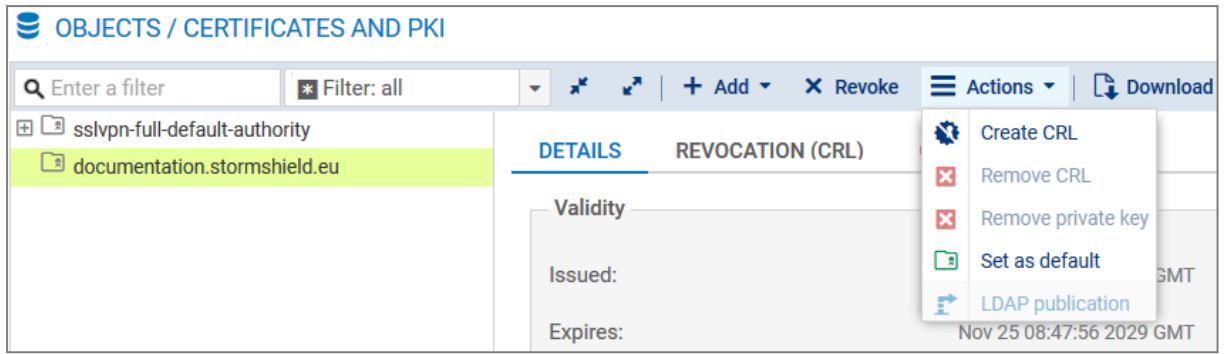
State (ST):

Country:

3. Fill in the following fields:
  - **Password** (necessary when creating certificates),
  - **E-mail address** (optional),
  - **Key size** (2048 bytes by default),
  - **Validity** (365 days by default).
4. You can define the URIs of CRL (Certificate revocation lists) distribution points.

### Certificate revocation lists (CRL)

1. In the menu **Configuration > Objects > Certificates and PKI**:
2. Select your CA and click on **Actions > Create a CRL**.
3. The wizard will ask you for the password to the certification authority. Enter it and click on **Create a CRL** to confirm.
4. Next, download the CRL (file in PEM format) in order to import it later on remote Firewalls.



### Certificate of the main Firewall

In the menu **Configuration > Objects > Certificates and PKI**:

1. Click on **Add > Server identity**.
2. Fill in the field **Fully qualified domain name** with the FQDN of the main Firewall. The **ID** field suggests the same name by default.
3. Indicate the duration of the **Validity** and the **Key size**.
4. Click on the magnifying glass next to the **Certification authority** field and select your CA to sign this certificate.
5. Enter the password of the certification authority. The attributes of the certificate are imported automatically; you can however modify them.
6. The wizard will display a summary of the certificate. Click on **Finish** to close it.

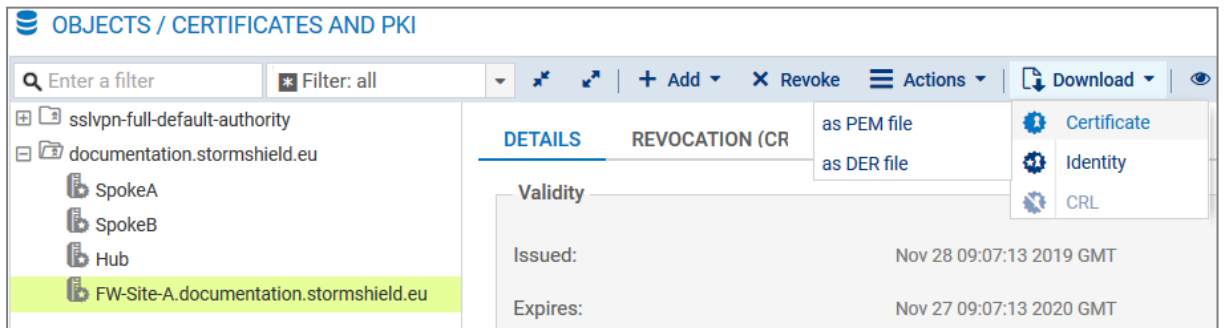
### Certificates of remote Firewalls

Create server certificates for the remote Firewalls by following the [method described earlier](#).

### Exporting security data of remote sites

In the menu **Configuration > Objects > Certificates and PKI**:

1. Select the certificate of one of the remote Firewalls.
2. Click on **Download > Certificate** and choose the desired file.
3. After entering a password to protect it, download the certificate by clicking on the hyperlink.
4. Save it on your administration workstation.
5. Follow the same steps to export the certificate of the second remote Firewall.



## Creating IPsec tunnels

### Adding the CA to the list of trusted CAs

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

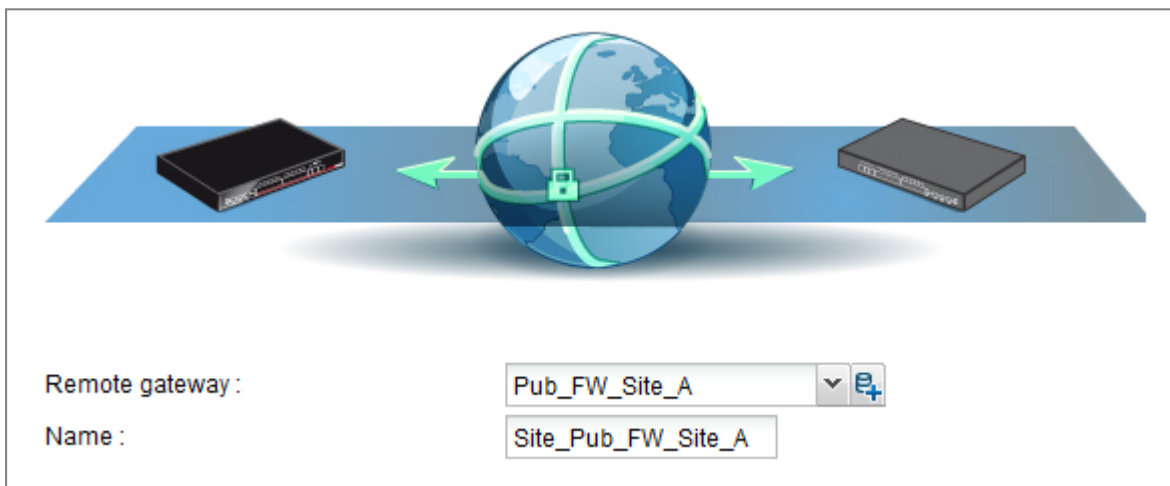


1. Under *Approved certificate authorities*, click on **Add**.
2. Select your CA.
3. Save.

### Creating IPsec peers

In the menu **Configuration > VPN > IPsec VPN**, select the *Peers* tab.

1. Click on **Add**.
2. Click on **New IKEv1 remote site** or **New IKEv2 remote site** depending on the IKE protocol version you use.
3. The wizard will then ask you to select the remote gateway. In this case, this gateway will be the public address of the first remote Firewall (object **Pub\_FW\_Site\_A**).  
By default, the name of the peer will be created by adding a prefix "Site\_" to this object name; this name can be customized.



4. Press **Enter**.
5. Check the **Certificate** checkbox.
6. Click on the magnifying glass next to the **Certificate** field.
7. Select the one corresponding to the main Firewall.  
The **Trusted CA** field is automatically entered by the certificate.
8. The wizard will display a summary of the peer you have just created.
9. Click on **Finish** to close this window.
10. Click again on **Finish** to close the wizard.
11. Repeat all the steps to create the IPsec peer for remote site B.

### Selecting the encryption policy and adding the VPN tunnel

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

1. Select the encryption policy you wish to configure.
2. You can rename it later by clicking on **Edit**.
3. Next, click on **Add** to define the IPsec tunnels.
4. Select the **Star configuration** model.  
A wizard will automatically launch.
5. In the **Local network** field, select your object **Private\_Net\_Main\_Site**.



- In the **Remote sites** table, click on **Add** to select the first peer by associating its network (Site\_Pub\_FW\_Site\_A and Private\_Net\_Site\_A). Peers can be created directly in this wizard by clicking on >> then **Create a peer**.
- Repeat the operation for the second peer (Site\_Pub\_FW\_Site\_B and Private\_Net\_Site\_B).

Local network :  
Private\_Net\_Main\_Site

REMOTE SITES

Peer selection	Remote networks
Site_Pub_FW_Site_A	Private_Net_Site_A
Site_Pub_FW_Site_B	Private_Net_Site_B

**! IMPORTANT**  
Ensure that you do not select the **Treat IPsec interfaces as internal interfaces** checkbox (applies to all tunnels). This option would prevent the setup of tunnels between remote sites and the main site (it can only be used in a Hub & Spoke configuration). If you have selected it by mistake, go to the **Advanced properties** window in the **Inspection profiles** module (**Application protection** menu) and unselect **Treat IPsec interfaces as internal interfaces (applies to all tunnels - remote networks will need to be explicitly legitimized)**.

- Validate by clicking on **Finish**.  
The IPsec tunnels are now defined on the main site and the tunnels will be automatically enabled (**Status "on"**).
- You can now click on **Enable** this policy.

ENCRYPTION POLICY - TUNNELS							
(1) IPsec 01 <span>Activate this policy</span> <span>Edit</span> <span>Disable policy</span>							
SITE-TO-SITE (GATEWAY-GATEWAY)				ANONYMOUS - MOBILE USERS			
Searched text <span>+ Add</span> <span>× Delete</span> <span>↑ Up</span> <span>↓ Down</span> <span>Cut</span> <span>Copy</span> <span>Paste</span>							
Line	Status	Local network	Peer	Remote network	Encryption profile	Keep alive	
1	✳	Star configuration: start					
2	on	Private_Net_Main_Site	Site_Pub_FW_Site_A	Private_Net_Site_A	StrongEncryption	0	
3	on	Private_Net_Main_Site	Site_Pub_FW_Site_B	Private_Net_Site_B	StrongEncryption	0	
4	✳	Star configuration: end					

### Setting up filtering rules

The VPN tunnel is meant to interlink two remote sites securely, but its purpose is not to filter traffic between these two entities. Filtering rules therefore need to be set up in order to





authorize only necessary traffic between identified source and destination hosts.

In the menu **Configuration > Security policy > Filtering and NAT:**

1. Select your filtering policy.
2. In the **Filtering** tab, click on the menu **New rule > Standard rule**.
3. Fill in the **Action, Source, Destination** and **Destination port** fields.

For better security, you can create a more restrictive rule on the Firewall that hosts the intranet server by specifying the source of the packets. To do so, when selecting the traffic source, indicate the value "IPsec VPN tunnel" in the field **Via** (*Advanced properties* tab):

The screenshot shows the configuration interface for a filtering rule. On the left is a sidebar with tabs: General, Action, Source (highlighted), Destination, Port - Protocol, and Inspection. The main area is titled 'SOURCE' and has three sub-tabs: GENERAL, GEOLOCATION / REPUTATION, and ADVANCED PROPERTIES (highlighted). Under 'Advanced properties', there are three fields: 'Source port' with a list containing 'Any' and '+ Add' / '- Delete' buttons; 'Via' with a dropdown menu set to 'IPSec VPN tunnel'; and 'source DSCP' with a dropdown menu set to 'All'.

In the case presented, client workstations located on remote sites must be able to connect in HTTP to the intranet server located on the local network of the main site (rule no. 1). You can also temporarily add, for example, ICMP to test the setup of the tunnel more easily (rule no. 2).

The filtering rules on the main site will look like this:

FILTERING IPV4 NAT									
	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comments	
1	on	pass	Private_Net_Site_A Private_Net_Site_B via IPSec VPN tunnel	Intranet_Server	http		IPS	Created on ...	
2	on	pass	Private_Net_Site_A Private_Net_Site_B via IPSec VPN tunnel	Intranet_Server	Any	icmp	IPS	Created on ...	
3	on	pass	Any	Firewall_bridge	Admin_srv		IPS	Created on ...	

**NOTE**  
The advanced features on Firewalls (use of proxies, security inspection profiles, etc) can of course be implemented in these filtering rules.

### Configuring remote sites A and B

On each remote site you will have to:

- Create the network objects of the local and the main sites,
- Import CRL and certificate of the local firewall,



- Create IPsec tunnels,
- Setting up filtering rules.

## Creating network objects

Define the five network objects needed through the menu: **Configuration > Objects > Network objects**.

On remote site A:

- The local network of the main site: **Private\_Net\_Main\_Site**,
- The public address of the main Firewall: **Pub\_Main\_FW**,
- The local network of remote site A: **Private\_Net\_Site\_A**,
- The public address of the Firewall on remote site A: **Pub\_FW\_Site\_A**,
- The intranet server to contact on the main site: **Intranet\_server**.

On remote site B:

- The local network of the main site: **Private\_Net\_Main\_Site**,
- The public address of the main Firewall: **Pub\_Main\_FW**,
- The local network of remote site B: **Private\_Net\_Site\_B**,
- The public address of the Firewall on remote site B: **Pub\_FW\_Site\_B**,
- The intranet server to contact on the main site: **Intranet\_server**.

## Importing elements for authentication

### Importing the certificate of each remote firewall

In the menu **Configuration > Objects > Certificates and PKI**:

1. Click on **Add > Import a file**.
2. Select the certificate corresponding to the Firewall and enter its password.



### IMPORT FILE

File to import:  ...

File format:  
 P12  
 DER  
 PEM

File password:

What to import:  
 All  
 Certificate(s)  
 Private key(s)  
 CRL  
 CA

Overwrite existing content

### Importing the CRL

In the menu **Configuration > Objects > Certificates and PKI**:

1. Click on **Add > Import a file**.
2. Select the CRL file exported earlier and enter its password.

## Creating IPsec tunnels

### Adding the CA to the list of trusted CAs

Please refer to the section **Configuring the main site**, under [Adding the CA to list of trusted authorities](#).

### Creating the IPsec peer

On each remote site, define the IPsec peer of the main site.

To do so, please refer to the section **Configuring the main site**, under [Creating IPsec peers](#).

The objects to select are the following:

On remote site A:

- **Local network**: **Private\_Net\_Site\_A**,
- **Peer field**: **Pub\_Main\_FW**,
- **Remote networks field**: **Private\_Net\_Main\_Site**.



On remote site B:

- **Local network:** Private\_Net\_Site\_B,
- **Peer field:** Pub\_Main\_FW,
- **Remote networks field:** Private\_Net\_Main\_Site.

### Selecting the encryption policy and adding the VPN tunnel

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

1. Select the encryption policy you wish to configure.
2. You can rename it later by clicking on **Edit**.
3. Click on **Add** to define the IPsec tunnel.
4. Select the **Site-to-site tunnel** model.
5. Fill in the fields in the wizard with the values adapted to each remote site.

On remote site A:

- **Local network:** Private\_Net\_Site\_A,
- **Remote network:** Private\_Net\_Main\_Site,
- **Remote gateway:** Pub\_Main\_FW,
- **Certificate:** the certificate created for the remote Firewall on site A.

On remote site B:

- **Local network:** Private\_Net\_Site\_B,
- **Remote network:** Private\_Net\_Main\_Site,
- **Remote gateway:** Pub\_Main\_FW,
- **Certificate:** the certificate created for the remote Firewall on site B.

### Setting up filtering rules

In the menu **Configuration > Security policy > Filtering and NAT:**

1. Select your filtering policy.
2. In the **Filtering** tab, click on the menu **New rule > Standard rule**.
3. Fill in the **Action, Source, Destination** and **Destination port** fields.

In the case presented, client workstations located on remote sites must be able to connect in HTTP to the intranet server located on the local network of the main site (rule no. 1). You can also temporarily add, for example, ICMP to test the setup of the tunnel more easily (rule no. 2).

The filtering rules will look like this:

On remote site A:

FILTERING IPv4 NAT									
Searching...									
	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection	Comments	
1	on	pass	Private_Net_Site_A	Intranet_Server	http		IPS	Created on ...	
2	on	pass	Private_Net_Site_A	Intranet_Server	Any	icmp	IPS	Created on ...	
3	on	pass	Any	Firewall_bridge	Admin_srv		IPS	Created on ...	



On remote site B:

FILTERING IPV4 NAT									
Searching...									
	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection		Comments
1	on	pass	Private_Net_Site_B	Intranet_Server	http		IPS		Created on ...
2	on	pass	Private_Net_Site_B	Intranet_Server	Any	icmp	IPS		Created on ...
3	on	pass	Any	Firewall_bridge	Admin_srv		IPS		Created on ...



# Checking the tunnel setup

From a client workstation located on each remote site, enter the URL of your intranet site in a web browser. For example: [http://intranet\\_site\\_name](http://intranet_site_name).

If you have allowed ICMP in the filter rules, you can also ping from the workstation to the intranet server.

## Checking in Stormshield Network Realtime Monitor

1. Launch Stormshield Network Real-Time Monitor.
2. Log on to the Firewall of the main site through the program.
3. Click on the module **Logs > VPN**.
4. Check that phases 1 and 2 took place correctly (message "Phase established"):

Error level	Phase	Source	Destination	Message	F	In SPI	Out SPI	Cookie (in/out)	Role
Information	2	Pub_Main_FW	Pub_FW_Site_A	Phase established	0x0b177225	0x0327a8f0	0x07ba826eae24b615/0x227a3bd376801377	0x07ba826eae24b615/0x227a3bd376801377	responder
Information	1	Pub_Main_FW	Pub_FW_Site_A	INITIAL-CONTACT received				0x07ba826eae24b615/0x227a3bd376801377	responder
Information	1	Pub_Main_FW	Pub_FW_Site_A	Phase established				0x07ba826eae24b615/0x227a3bd376801377	responder

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

Source	Bytes	Destination	Status	Lifetime	Authentication	Encryption
Pub_Main_FW	200.64 KB / 57.18 KB	Pub_FW_Site_A	mature	2m 41sec	hmac-sha1	aes-cbc

If this is not the case, look up the section [Incident resolution - Common errors](#) below.

## Incident resolution - Common errors

Further on in this section, the Firewall of the remote site is called the "initiator", as it initiates the setup of the tunnel for the chosen example. As for the Firewall of the main site, it is called the "responder".

**Symptom:** The tunnel between the appliances has been set up but no traffic seems to go through it.

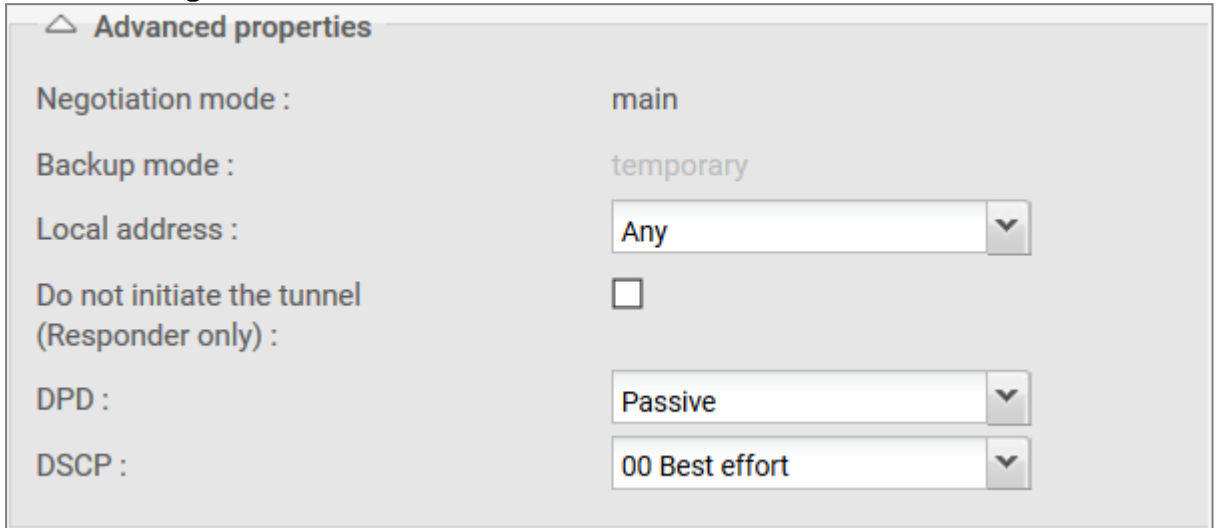
**Solution:** Check your filter rules. Also check the routing between the hosts (client workstation, intranet server) and their respective gateways (static routing or default gateway).

**Symptom:** The tunnel cannot be set up.

- No message appears in the module Logs > VPN in Stormshield Network Real-Time Monitor on the "initiator" Firewall.
- No message appears in the module Logs > VPN in Stormshield Network Real-Time Monitor on the "responder" Firewall.

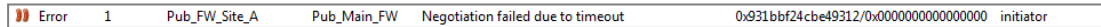


**Solution:** Check the routing between the hosts (client workstation, intranet server) and their respective gateways (static routing or default gateway). Check your filter rules on the “initiator”. Also ensure that the “initiator”’s tunnel is not in “responder only” mode (Peers tab in the menu **Configuration > VPN > IPsec VPN**).



**Symptom:** The tunnel cannot be set up.

- A message “Negotiation failed due to timeout” in phase 1 appears in the module **Logs > VPN** in Stormshield Network Real-Time Monitor on the “initiator” Firewall



- No message appears in the module **Logs > VPN** in Stormshield Network Real-Time Monitor on the “responder” Firewall.

**Solution:** The remote IPsec gateway (“responder”) is not responding to requests. Check that the IPsec VPN policy has been enabled on the “responder” Firewall. Check that the objects corresponding to tunnel endpoints have been entered with the right IP addresses.

**Symptom:** The tunnel cannot be set up.

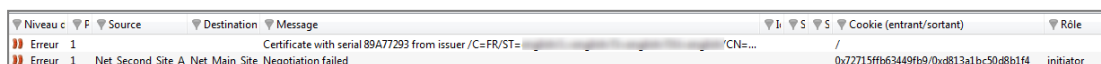
- The messages “Negotiation failed” and “Certificate with serial XXX from issuer YYY: unable to get local issuer certificate” in phase 1 appear in the module **Logs > VPN** in Stormshield Network Real-Time Monitor on the “responder” Firewall



**Solution:** the “responder” Firewall cannot verify the validity of the “initiator” Firewall’s certificate. Ensure that you have indeed defined the CA as the trusted CA on the “responder” (Identification tab in the menu **Configuration > VPN > IPsec VPN**).

**Symptom:** The tunnel cannot be set up.

- The messages “Negotiation failed” and “Certificate with serial XXX from issuer YYY: unable to get local issuer certificate” in phase 1 appear in the module **Logs > VPN** in Stormshield Network Real-Time Monitor on the “initiator” Firewall





**Solution:** the “initiator” Firewall cannot verify the validity of the “responder” Firewall’s certificate. Ensure that you have indeed defined the CA as the trusted CA on the “initiator” (Identification tab in the menu **Configuration > VPN > IPsec VPN**).





## Further reading

---

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



**STORMSHIELD**

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