TECHNICAL NOTE
STORMSHIELD NETWORK SECURITY

IPSEC VPN: AUTHENTICATION BY PRE-SHARED KEY

Product concerned: SNS 1 and higher versions

Date: June 19, 2019

Reference: sns-en-IPSec_VPN_Authentication_Pre_Shared_Key_Technical_Note

Table of contents

IPSec VPN: Authentication by pre-shared key

You wish to securely link up two sites on your company network currently linked via the Internet. To do so, you need to create a site-to-site IPSec VPN (also known as "gateway to gateway").

The authentication method presented in this tutorial is based on the use of pre-shared keys (authentication by certificate can also be set up).

This document describes the VPN configuration to create, so that you can allow a client workstation on the remote site to access an intranet server on the main site through this tunnel in HTTP.

Implementation

Configuring the main site

Creating network objects

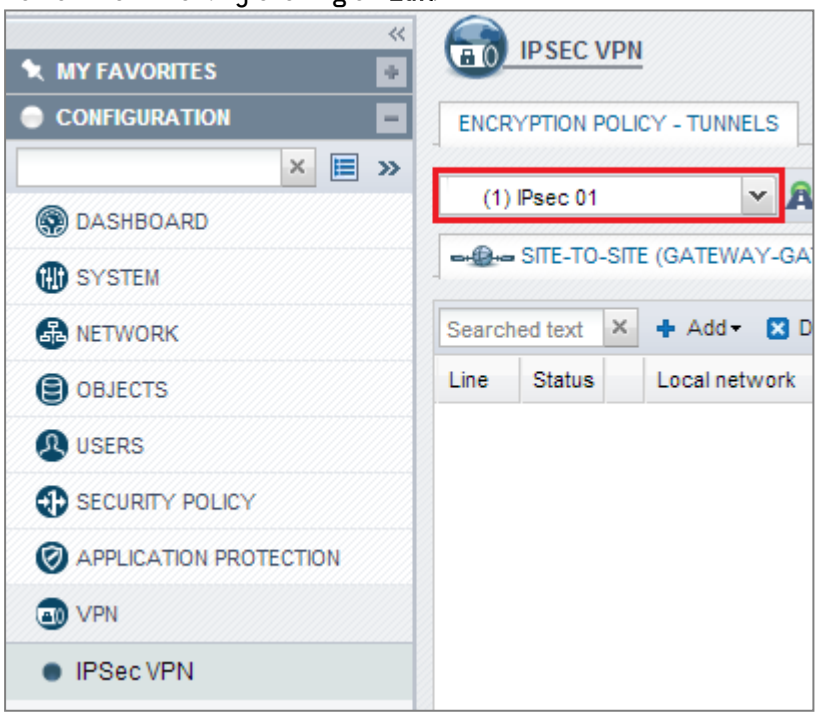
The creation of this site-to-site IPSec VPN connection requires at least five network objects:

- 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 the remote site: Private_Net_Remote_Site,
- the public address of the remote Firewall: Pub_Remote_FW,
- the intranet server to contact on the main site: Intranet_Server.

These objects can be defined in the menu: **Configuration > Objects** > **Network objects**.

Creating IPSec tunnels

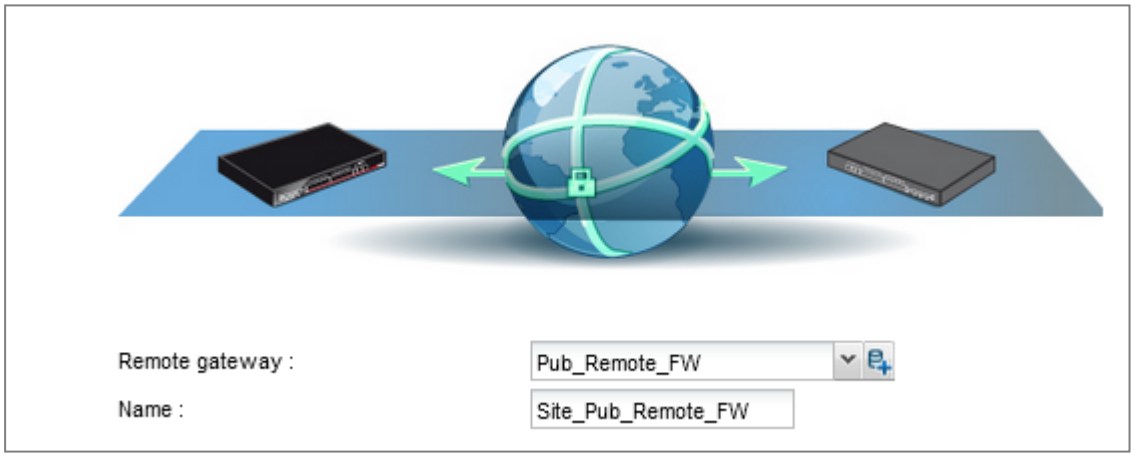
1. Click on **Configuration > VPN > IPSec VPN.**
2. Select the encryption policy you wish to configure.
   You can rename it by clicking on **Edit**.



3. Click on **Add > Site-to-site tunnel.**
   A wizard will automatically launch:
4. In the **Local network** field, select your object Private_Net_Main_Site.

5. In the **Remote network** field, select the object Private_Net_Remote_Site.

6. Next, select a peer.
   If the peer you wish to use does not yet exist, as in this example, you can create it by clicking on the hyperlink **Create a peer** (this step corresponds to the parameters that can be defined directly in the Peer tab in the menu **Configuration** > **VPN** > **IPSec VPN**).
7. The wizard will then ask you to select the remote gateway: in this current case, this is the public address of the remote Firewall (object Pub_Remote_FW). By default, the name of the peer will be created by adding a prefix "Site_" to this object name; this name can be customized:



8. Next, select the authentication method: select the method "Pre-shared key (PSK)".
9. In the fields **Pre-shared key (ASCII)** and **Confirm**, enter a complex password that will be exchanged between both sites in order to set up the IPSec tunnel, and then confirm.

NOTE

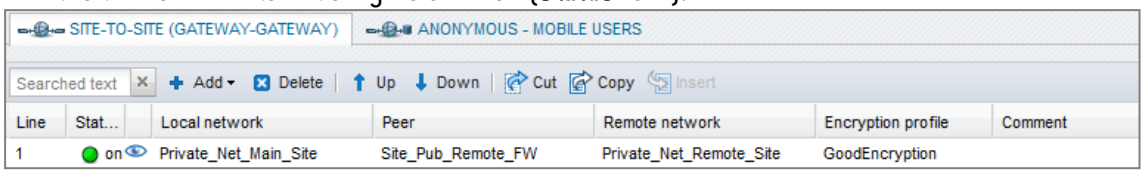
To define a pre-shared key that is sufficiently secure, you are advised to do the following:

- Keep to a minimum length of 8 characters,
- Use uppercase and lowercase letters, numbers and special characters,
- Do not use a word found in a dictionary for your password.

Example: 7f4V8!>Xdu.

10. The wizard will then show a summary of the peer that you have just created.
11. Click on **Finish** to close this window.

12. Click again on **Finish** to close the wizard. The IPSec tunnel is now defined on the main site and the tunnel will automatically be enabled (**Status** "on"):



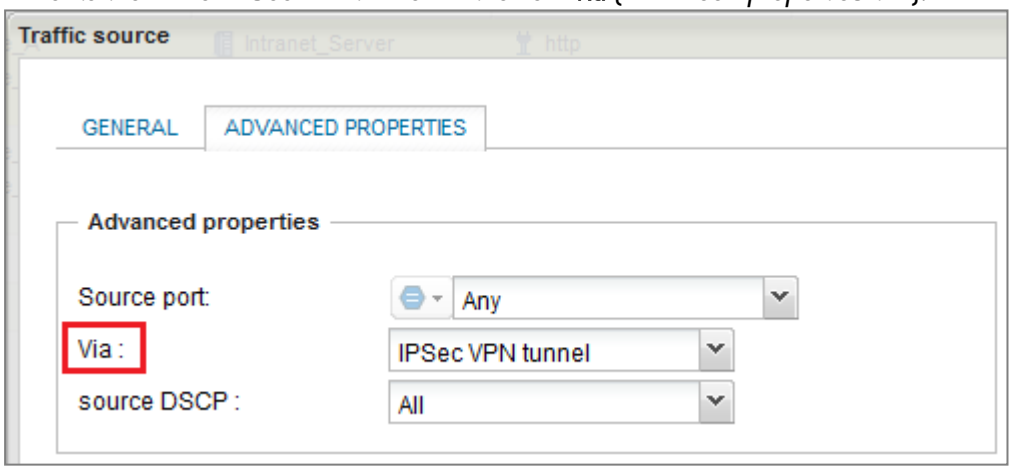
13. Click on **Enable this policy.**

Creating filtering rules

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

- Authorize only necessary traffic between identified source and destination hosts,
- Optimize performance (host resources, internet access bandwidth) by preventing unnecessary packets from setting up a tunnel.

1. In the menu **Configuration > Security policy > Filtering and NAT**, select your filtering policy.
2. In the **Filtering** tab, click on the menu **New rule > Standard rule**.
   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):



In the case presented, a client workstation located on the local network of the **remote site** 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 rule will look like this:

	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
1	on	pass	Private_Net_Remote_Site via IPSec VPN tunnel	Intranet_Server	http		IPS
2	on	pass	Private_Net_Remote_Site via IPSec VPN tunnel	Intranet_Server	Any	icmp	IPS
3	on	pass	Any	Firewall_bridge	Admin_srv		IPS

NOTE

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

Configuring the remote site

The aim of this section is to reproduce on the remote site a configuration symmetrical with the one created on the main Firewall.

Creating network objects

The objects are the same as those defined on the main Firewall. Please refer to section **Configuring the main site**, under Creating network objects.

Creating IPSec tunnels

Please refer to section **Configuring the main site**, under Creating the IPSec tunnel. For the remote site, the fields to be entered in the wizard will have the following values:

- **Local network:** Private_Net_Remote_Site,
- **Remote network:** Private_Net_Main_Site,
- **Remote gateway:** Pub_Main_FW,
- **Pre-shared key**: the same password as the one entered on the main Firewall.

Creating filtering rules

1. In the menu **Configuration > Security policy > Filtering and NAT**, select your filtering policy.
2. In the **Filtering** tab, click on the menu **New rule > Standard rule**.
   In the case presented, a client workstation located on the local network of the **remote site** 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 rule will look like this:

	Status	Action	Source	Destination	Dest. port	Protocol	Security inspection
1	on	pass	Private_Net_Remote_Site	Intranet_Server	http		IPS
2	on	pass	Private_Net_Remote_Site	Intranet_Server	Any	icmp	IPS
3	on	pass	Any	Firewall_bridge	Admin_srv		IPS

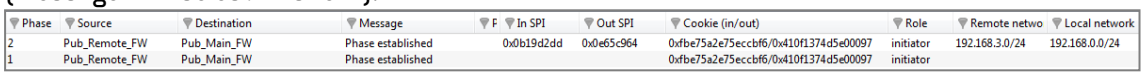
Checking the tunnel setup

From a client workstation located on the remote site, enter the URL of your intranet site in a web browser. For example: *http://intranet_site_name.*

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

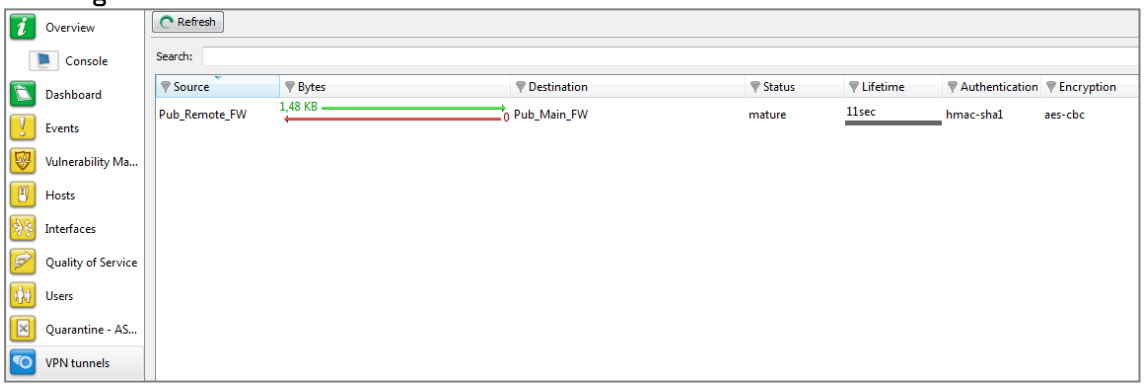
Checking in Stormshield Network Real-Time Monitor

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



Phase	Source	Destination	Message	F	In SPI	Out SPI	Cookie (in/out)	Role	Remote netwo	Local network
2	Pub_Remote_FW	Pub_Main_FW	Phase established		0x0b19d2dd	0x0e65c964	0xfbe75a2e75eccbf6/0x410f1374d5e00097	initiator	192.168.3.0/24	192.168.0.0/24
1	Pub_Remote_FW	Pub_Main_FW	Phase established				0xfbe75a2e75eccbf6/0x410f1374d5e00097	initiator		

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



If this is not the case, look up the section Incident resolution - Common errors.

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".

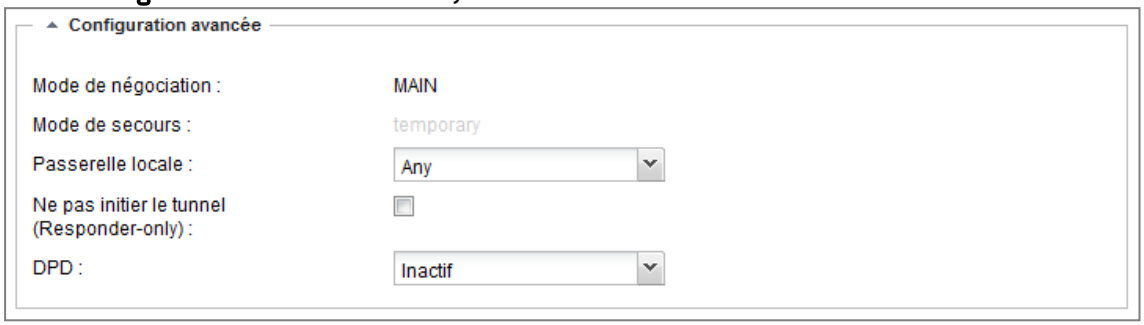
Symptom: The tunnel between the appliances has been set up but no traffic seems to go through it.

Solution: Check your filter rules on the "responder". 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.

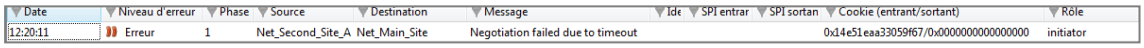
- No message appears in the module **Logs > VPN** in Stormshield Network Real-Time Monitor on the "initiator" Firewall.
- No message appears in the module **Logs > VPN** in Stormshield Network Real-Time Monitor on the "responder" Firewall.

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.

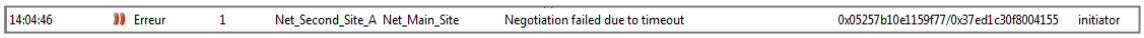


- No message appears in the module **Logs** > **VPN** in Stormshield Network Real-Time Monitor on the "responder" Firewall.

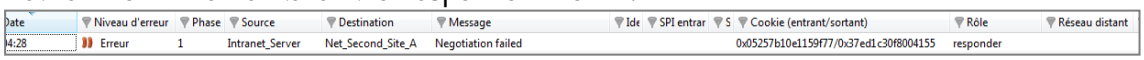
Solution: The remote IPSec gateway ("responder") is not responding to requests. Check that the IPSec VPN policy has been enabled on the "responder" Firewall. Check that the objects corresponding to tunnel endpoints have been entered with the right IP addresses (generally public IP addresses).

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.



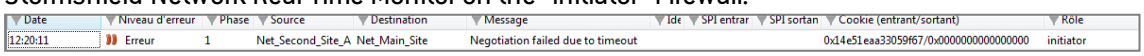
- A message "Negotiation failed" in phase 1 appears in the module **Logs** > **VPN** in Stormshield Network Real-Time Monitor on the "responder" Firewall.



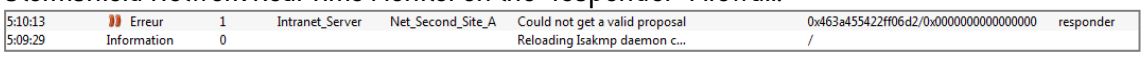
Solution: The appliances are attempting to negotiate but cannot seem to agree on an authentication policy. Check that the pre-shared key is the same on both Firewalls.

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.



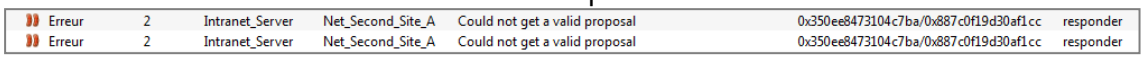
- A message "Could not get a valid proposal" in phase 1 appears in the module **Logs** > **VPN** in Stormshield Network Real-Time Monitor on the "responder" Firewall.



Solution: The appliances are attempting to negotiate but cannot seem to agree on an encryption policy in phase 1 (IKE). Check that the encryption profile is the same on both Firewalls (Diffie-Hellman group, maximum lifetime, etc.).

Symptom: The tunnel cannot be set up.

- A message "Could not get a valid proposal" in phase 2 appears in the module **Logs > VPN** in Stormshield Network Real-Time Monitor on the "responder" Firewall.



Erreur	2	Intranet_Server	Net_Second_Site_A	Could not get a valid proposal	0x350ee8473104c7ba/0x887c0f19d30af1cc	responder
Erreur	2	Intranet_Server	Net_Second_Site_A	Could not get a valid proposal	0x350ee8473104c7ba/0x887c0f19d30af1cc	responder

Solution: The appliances are attempting to negotiate but cannot seem to agree on an encryption policy in phase 2 (IPSec). Check that the encryption profile is the same on both Firewalls (authentication and encryption proposals, etc.).

documentation@stormshield.eu