

TECHNICAL NOTE STORMSHIELD NETWORK SECURITY

LEVEL 2 ENCAPSULATION

Product concerned: SNS 2.3 and higher, SNS 3.x Date: April 21, 2021 Reference: sns-en-level_2_encapsulation_technical_note





Table of contents

Introduction	. 3
Architectures shown	4
Case 1: bringing together two sites sharing the same address range	. 4
Case 2: transporting VLAN in a GRE tunnel	. 4
Case 1: bringing together two sites sharing the same address range	. 6
Configuring the firewall on Site A	. 6
Creating the GRETAP interface	6
Creating IPsec tunnels	6
Configuring the firewall on Site B	′
Creating the GRETAP Interface	(
Verifying tuppels	0 Q
GRE tunnels	. 9
Encrypted GRE tunnel in an IPsec tunnel	9
Case 2: transporting VLAN in a GRE tunnel	.11
Configuring the firewall on Site A	11
Creating the GRETAP interface	. 11
Creating IPsec tunnels	. 13
Creating VLANs	. 13
Lonfiguring the firewall on Site B	.15
Creating The GRETAP Interface	. 15
Creating II Sec turners	16
Verification	.16



Introduction

From firmware version 2.x onwards, Stormshield Network firewalls can encapsulate Level 2 traffic in GRE (Generic Routing Encapsulation) tunnels based on GRETAP interfaces. Since GRE tunnels are not encrypted natively, exchanges can be secured by making GRE traffic go through IPSec.

The use of GRE tunnels based on GRETAP interfaces makes it possible, for instance, to link sites with the same address range through a bridge. DHCP services can therefore be shared between both sites. This kind of tunnel also allows transporting VLANs identified and explicitly declared on the firewalls between two sites



Architectures shown

Case 1: bringing together two sites sharing the same address range



This section of the technical note sets out the scenario of a company seeking to link two sites sharing an identical address range through a bridge. Services, for example DHCP, and shared network resources will therefore be considered local services, regardless of the site. To secure exchanges, GRE traffic will be encrypted in an IPsec tunnel.

🕦 NOTE

IP addresses assigned to devices on both sites must of course be unique.

Case 2: transporting VLAN in a GRE tunnel



This section of the technical note sets out the scenario of a company seeking to share two VLANs between two sites through a GRE tunnel secured by encryption (IPSec). It covers the specific configurations in the creation of GRETAP interfaces, IPSec tunnels, VLAN settings and their attachment to GRETAP interfaces.

🕕 IMPORTANT

A bridge is needed for each VLAN transported. It is therefore essential that you ensure the firewall supports the number of bridges planned.

The system property command (Système > Console CLI menu) allows you to get this information:



	CONSOLE CLI
	SYSIEM : System commands USER : User related functions VERSION : Display server version
	system property
	[Result]
	Type=Firewall
	Model=V50-A
	MachineType=amd64
	Version=
	ASQVersion=7.3.0
	SerialNumber=V50XXA3E0000017
	MTUmax=9198
	LACP=0
	Bridge=8
ľ	



Case 1: bringing together two sites sharing the same address range

Configuring the firewall on Site A

Creating the GRETAP interface

In the **Network** > **Interfaces** module, click on **Add** and select **Add a interface**. Enter the following mandatory fields:

Global configuration

Name: assign a name to the GRETAP interface (gretap in the example).

Interface Configuration

Bridge: select an existing bridge on the firewall. This may be a bridge created by the default configuration or a bridge created specifically for this purpose.

🕦 NOTE

Bridges cannot be created in the GRETAP interface creation wizard.

🕦 NOTE

It is possible to not assign any bridge to the interface by selecting the option **Create an inactive GRETAP interface**. The interface can then be enabled later by moving it to a bridge.

GRETAP tunnel configuration

Tunnel source: select the physical interface through which GRE traffic will travel on the firewall. In the example given, this is the **Firewall out** interface.

Tunnel destination: select an object bearing the public IP address of the remote firewall (**Remote_ Firewall** in the example).

Click on Finish then Apply to confirm the creation of the GRETAP interface.

Creating IPsec tunnels

In the *Encryption policy - Tunnels* tab of the **VPN** > **IPsec VPN** module, click on **Add** and select **Site-to-site tunnel**. Fill in the various fields suggested by the tunnel creation wizard and confirm:

Local network: select the physical interface bearing the GRE tunnel (Firewall_out in the example).

Remote network: select an object bearing the public IP address of the remote firewall.

Peer selection: create (or select it if it exists) a peer whose remote gateway will be an object bearing the public IP address of the remote firewall.



🕦 NOTE

For further detail on how to create a peer using authentication by pre-shared key or certificates, please refer to the documents *IPsec VPN - Authentication by pre-shared key* and *IPsec VPN - Authentication by certificate*.

🕦 NOTE

The version of the IKE protocol for this peer has to be the same as:

the one used on the remote firewall,

the one for the peers used in the other rules of the IPsec policy in question.

In order to prevent the setup of IPsec tunnels for protocols other than GRE and thereby preventing the encryption of traffic such as ICMP (ping), the GRE protocol can be specified in the **Protocol** column. If this column does not display, roll your mouse over the title of any column and expand the pop-up menu by clicking on the arrow. Select **Columns** then check **Protocol**:

(8)	IPsec and C	GRE 🔽 🖌 Activate	e this policy Edit - 🛄			
-@	SITE-TO-SI	TE (GATEWAY-GATEWAY)	ANONYMOUS - MOBILE USE	RS		
Search	ied text	× 🕂 Add - 🕻	3 Delete 🕇 Up 👃 Down 💣	Cut 😭 Copy 🔄		
Line	Status	Local network	Peer	Remote network	 Encryption profile 	Comment
1	🔵 on	Firewall_out	Site_RemoteFW	RemoteFW	Ag↓ Sort Ascending	
					ZA↓ Sort Descending	
					Columns 🕨	
						V Local network
						Peer
						Remote network
						Protocol
						Encryption profile
						Keep alive

The IPsec VPN policy will therefore resemble:

-										
	(8)	IPsec and G	RE	👻 🧸 Activat	e this policy Edit - 🛄					
-	@	SITE-TO-SI	te (Ga	ATEWAY-GATEWAY)	ANONYMOUS - MOBIL	LE USERS				
	arob	ad taxt		X 📥 Add 🚽	🖸 Delete 🕈 IIn 📕 Down	Cut R Co				
	sarci	eutext				Cor 🖉 Co	py rusic			
Li	ne	Status		Local network	Peer	Remote r	network F	rotocol	Encryption profile	Comment
1		🔵 on	۲	Firewall_out	Site_RemoteFW	RemoteF	W g	re	GoodEncryption	

🕦 NOTE

Since the firewall initiated the sending of GRE network packets, filter rules therefore do not need to be created for this protocol.

Configuring the firewall on Site B

Creating the GRETAP interface

Following the method used on site A's firewall, create the GRETAP interface:



Global configuration

Name: assign a name to the GRETAP interface

Interface configuration

Bridge: select an existing bridge on the firewall. This may be a bridge created by the default configuration or a bridge created specifically for this purpose.

GRETAP tunnel configuration

Tunnel source: select the physical interface through which GRE traffic will travel on the firewall. In the example given, this is the **Firewall out** interface.

Tunnel destination: select an object bearing the public IP address of the remote firewall (**Remote_ Firewall** in the example).

Click on Finish then Apply to confirm the creation of the interface.

Creating IPsec tunnels

Following the method used for creating the IPsec tunnel on site A's firewall, define a tunnel with the following values:

- Local network: select the physical interface bearing the GRE tunnel (Firewall_out in the example).
- **Remote network**: select an object bearing the public IP address of the remote firewall (**Remote**_ **Firewall** in the example).
- **Peer selection**: create (or select it if it exists) a peer whose remote gateway will be an object bearing the public IP address of the remote firewall.

🕦 NOTE

The version of the IKE protocol for this peer has to be the same as:

- the one used on the remote firewall,
- the one for the peers used in the other rules of the IPsec policy in question.

Select **GRE** in the **Protocol** column of the IPsec rule in order to restrict the use of the tunnel to GRE traffic.

The IPsec VPN policy will therefore resemble:

	(8)	IPsec and GI	RE	👻 🤱 Activat	e this policy Edit - 🛄					
	- ®	SITE-TO-SIT	E (GA	ATEWAY-GATEWAY)	⊷-@+■ ANONYMOUS - MO	DBILE USERS	s			
s	earch	ed text		× 🕂 Add -	🛛 Delete 🕇 Up 👃 Dov	vn 💣 Cu	ut 😭 Copy 🧐 Pa			
L	ine	Status		Local network	Peer		Remote network	Protocol	Encryption profile	Comment
1		🔵 on	۲	Firewall_out	Site_RemoteFW		RemoteFW	gre	GoodEncryption	



🕦 NOTE

Since the firewall initiated the sending of GRE network packets, filter rules therefore do not need to be created for this protocol.

Verifying tunnels

GRE tunnels

To check the operational status of the unencrypted GRE tunnel between both firewalls, disable the IPsec rule on each site by setting its status to **off** and enable the IPsec policy:

A (8)	IPsec and G	RE	✓ ▲ Activate this	oolicy Edit - 🛄			
	SITE-TO-SIT	E (GA	TEWAY-GATEWAY)	ANONYMOUS - MOBILE USEF	κs		
Search	ied text		× 🕂 Add - 🔀 Del	ete 🕇 Up 🤳 Down 💣 C	Cut 😭 Copy 🧐 Pa		
Line	Status		Local network	Peer	Remote network	Protocol	Encryption profile
4	a off		Eirowall out	Site DemotoFW	DomotoEW/	010	CoodEconviction

From a workstation located on the local network of Site A, ping a machine located on the local network of Site B. This machine should respond to requests.

Encrypted GRE tunnel in an IPsec tunnel

On each firewall, enable the IPsec rule by setting its status to on and enable the IPsec policy:

A (8)	Psec and G	GRE 🔽 🖌 Activate th	nis policy Edit - 🛄			
@	SITE-TO-SI	TE (GATEWAY-GATEWAY)	- @ ANONYMOUS - MOBILE U	JSERS		
Search	hed text	× 🕂 Add - 🔀	Delete 🕇 Up 👃 Down [🚰 Cut 😭 Copy 🔄 Pa	iste	
Line	Status	Local network	Peer	Remote network	Protocol	Encryption profile
1	🔵 on	Firewall_out	Site_RemoteFW	RemoteFW	gre	GoodEncryption

From a workstation located on the local network of Site A, send a ping from a machine located on the local network of Site B. This machine should respond to requests.

Verifying in SN Real-Time Monitor

The status of the IPsec tunnel can be viewed in the *IPsec VPN tunnels* tab in the **VPN** tunnels module in SN Real-Time Monitor:

Γ	IPSec VPN tunnels SSL VPN tunnels	3				
	Actions Search: 					
	Source Bytes	Destination	🔻 Status	🔻 Lifetime	Authentication	F Encryption
	Firewall_out	RemoteFWPublic1	mature	1m 7sec	hmac-sha1	aes-cbc

Logs regarding the setup of IPsec tunnels can be looked up in the Logs > VPN module:



Sea	arch:														
7	Firewall	🛡 Date	Frror level	💎 Phase	Source	Destination	♥ Message	Peer identity	🛡 In SPI	🛡 Out SPI	🔻 Cookie (in/out)	🛡 Role	Remote net	work	Local network
19	2.168.56.250	12:50	Information	1	Firewall_out	RemoteFWPublic1	IKE SA established				0x08d261bf9431821e/0x2a92b95115d9d4d4	initiator			
19	2.168.56.250	12:50	Information	2	Firewall_out	RemoteFWPublic1	IPSEC SA established		0xc874d01c	0xceb52e32	0x08d261bf9431821e/0x2a92b95115d9d4d4	initiator	10. /32[gre]	10.)/32[gre]
19	2.168.56.250	12:50	Information	1	Firewall_out	RemoteFWPublic1	IKE SA established				0x1bac5337bb8ad6d1/0x059fedec578fb01e	responde	r		
19	2.168.56.250	12:50	Information	2	Firewall_out	RemoteFWPublic1	IPSEC SA established		0xc44b35ac	0xc94c0482	0x1bac5337bb8ad6d1/0x059fedec578fb01e	responde	r 10. /32[gre]	10. /32[gre]

Verifying in the firewall web interface

In the firewall's web administration interface, you can display logs and reports to verify that your configuration operates correctly.



Case 2: transporting VLAN in a GRE tunnel

Configuring the firewall on Site A

Creating the GRETAP interface

Creation

In the **Network** > **Interfaces** module, click on **Add** and select **Add a interface**. Enter the following mandatory fields:

Global configuration

Name: assign a name to the GRETAP interface (Gretap VLAN in the example).

Interface Configuration

Bridge: select the option **Create an inactive GRETAP interface**. The interface will be enabled thereafter and assigned with a dedicated IP address.

🕦 NOTE

Not attaching the GRETAP interface to a bridge makes it possible to authorize only network packets through the GRE tunnel from VLANs attached to this interface (VLAN10 and 20 in the example).

GRETAP tunnel configuration

Tunnel source: select the physical interface through which GRE traffic will travel on the firewall. In the example given, this is the **Firewall_out** interface.

Tunnel destination: select an object bearing the public IP address of the remote firewall (**Remote_ Firewall** in the example).

Click on **Finish** then **Apply** to confirm the creation of the GRETAP interface.



The GretapVLAN interface created will then appear grayed out (inactive) in the list of interfaces:

Caarab	X + Add - 🖸 Dalata 🔚 🔚 Mixed viz	aw - Show all- 🔿 Chack usaga
Search		ew • Show all • 🐨 Check usage
p PL ondge	CONFIGURATION OF THE INTERFACE	ADVANCED CONFIGURATION
dmz1	Name :	GretapVLAN
m dmz2	Comments :	
GretapVLAN	VLANs attached to the interface :	
	Color :	•
	This interface is :	internal (protected)
	GRETAP tunnel address	
	Tunnel source :	Firewall_out
	Tunnel destination :	RemoteFW Y
	- Address range	
	Address range	
		None (interface disabled)

Activation

In the tab *Configuration of the interface*, assign an IP address to the GRETAP interface by selecting **Fixed IP (static)** then entering the IP address and network mask. Confirm the configuration by clicking on **Apply**. The GRETAP interface will then be enabled. In this example, the IP address and network selected have the values 192.168.44.1 and 255.255.255.252 respectively:

⊳ ∎-t <mark>a</mark> bridge	CONFIGURATION OF THE INTERFACE	ADVANCED CONFIGURATION	
im out			
im dmz1	Name :	GretapVLAN	
m dmz2	Comments :		
GretapVLAN	VLANs attached to the interface :		
	Color		
	This interface is :	internal (protected)	
	CRETAR tunnel address		
	Tunnel source :	Firewall out	
	Tunnel destination :	Pameta[]//	
	runner destination .	Remoterw	
	Address range		
		None (Interface disabled)	
		Oynamic IP (obtained by DHCP)	
		Address range inherited from the bridge	
		Select a bridge	
		Fixed IP (static)	
	🕂 Add 🔀 Delete		
	IP address		Network mask
	192.168.44.1		255.255.255.252
	L		



Creating IPsec tunnels

To create the IPsec tunnel on Site A's firewall, please refer to the section Creating the IPsec tunnel in Case 1.

🕦 NOTE

Since the firewall initiated the sending of GRE network packets, filter rules therefore do not need to be created for this protocol.

Creating VLANs

Creating VLAN 10

In the **Network** > **Interfaces** menu, click on **Add** then **Add a VLAN**. In the first window of the wizard, select the option **VLAN attached to 2 interfaces** (crossing VLAN).

Next, fill in the fields in the various windows of the wizard as follows:

VLAN ID	
Name :	vlan_10
VLAN ID :	10 🗘
Color :	
VLAN address range	
VLAN address range —	Use an existing bridge
— VLAN address range —— Bridge :	O Use an existing bridge Select a bridge ✓
VLAN address range	 Use an existing bridge Select a bridge Create a new bridge
VLAN address range	 Use an existing bridge Select a bridge Create a new bridge BridgeVlan10

VLAN ID

- Name: choose a name for this VLAN (vlan_10 in the example).
- VLAN ID: select the 802.1q identifier associated with the VLAN (10 in the example).

VLAN address range

- Select Create a new bridge and assign a name to this bridge (BridgeVlan10 in the example).
- IPv4 address: leave the default dynamic IP assignment (DHCP) then confirm and click on Next.

Incoming VLAN ID		
Name :	vlan_10_1	
Interface :	in	~
This interface is :	internal (protected)	*
Name :	vlan_10_2	
Interface :	GretapVLAN	~
This interface is :	internal (protected)	*

Incoming VLAN ID

- Name: select a name for the VLAN attached to the interface for incoming traffic. By default, this should be the name of the VLAN selected in the first window with the addition of the suffix "_1" (vlan_10_1 in the example).
- Interface: select the interface through which packets belonging to the VLAN will enter the firewall. In the example, since the hosts are on the internal network, this will be the in interface.
- This interface is: specify that the VLAN has to be considered as an internal (protected) interface.

Outgoing VLAN ID

- Name: select a name for the VLAN attached to the interface for outgoing traffic. By default, this should be the name of the VLAN selected in the first window with the addition of the suffix "2" (vlan_102 in the example).
- Interface: select the GRETAP interface through which packets belonging to the VLAN will leave the firewall. In the example, this would be the **GretapVLAN** interface.
- This interface is: specify that the VLAN has to be considered as an internal (protected) interface.

After having confirmed the configuration, the VLANs and their associated bridges can be seen in the list of interfaces:

Search ×	
▷ ■C ⁰ bridge	
⊿ ∎C BridgeVlan10	
m vlan_10_1	
m vlan_10_2	

Creating VLAN 20

To create the second VLAN that needs to be transported through the GRE tunnel, follow the method described in the paragraph Creating VLAN 10 using the following values:

<u>VLAN ID</u>

• Name: vlan_20 in the example.



• VLAN ID: 20 in the example.

VLAN address range

- Select Create a new bridge. Name: BridgeVlan20 in the example.
- IPv4 address: Dynamic IP (DHCP).

Incoming VLAN ID

- Name: vlan 20 1 in the example.
- Interface: in in the example.
- This interface is: specify that the VLAN has to be considered as an internal (protected) interface.

Outgoing VLAN ID

- Name: vlan 20 2 in the example.
- Interface: GretapVLAN in the example.
- This interface is: specify that the VLAN has to be considered as an internal (protected) interface.

By clicking on the GRETAP interface, you will be able to check that both VLANs vlan_10_2 and vlan_ 20_2 have been attached to it:

Search	× + Add -	w ▼ Show all ▼ 💿 Check usage
▷ ••••••••••••••••••••••••••••••••••••	CONFIGURATION OF THE INTERFACE	ADVANCED CONFIGURATION
BridgeVlan10 BridgeVlan20	Name :	GretapVLAN
GretapVLAN	VLANs attached to the interface :	vlan_10_2, vlan_20_2
	Color :	
	This interface is :	internal (protected)
	GRETAP tunnel address	
	Tunnel source :	Firewall_out 👻
	Tunnel destination :	RemoteFW Y

Configuring the firewall on Site B

Creating the GRETAP interface

To create the GRETAP interface on the firewall of site B, please follow the method explained in the paragraph **Creating the GRETAP interface** on site A. For the example shown, the values used will be the following:

- **IP address:** 192.168.44.2.
- Mask: 255.255.255.252.



Creating IPsec tunnels

To create the IPsec tunnel on Site B's firewall, please refer to the section Creating the IPsec tunnel in Case 1.

🕦 NOTE

Since the firewall initiated the sending of GRE network packets, filter rules therefore do not need to be created for this protocol.

Creating VLAN

To create VLAN 10 and 20 and assign them to the GRETAP interface on the second firewall, follow the method described in the paragraph Creating VLAN for the firewall on Site A.

Verification

From a machine on Site A belonging to VLAN 10 or VLAN 20, ping a machine on Site B belonging to the same VLAN: the machine on Site B should respond to requests.

It is also possible to check whether VLAN are indeed being transported through the tunnel by creating a network capture on the incoming interface of the tunnel on Site B's firewall. In this case, captured network packets will show the GRE protocol encapsulating the transported VLAN (VLAN 20 in the example).

15:41:06.019669 00:90:fb:2c:5d:b2 > 00:0d:b4:0c:c6:b6, ethertype IPv4 (0x0800), length 108: 172.16.3.1 > 172.16.2.1: GREv0, proto TEB (0x6558), length 74: 18:03:73:8b:51:d8 > 01:00:5e:00:00:fc, ethertype 802.1Q (0x8100), length 70: vlan 20) p 0, ethertype IPv4, 192.168.1.10.50677 > 224.0.0.252.5355: UDP, length 24





documentation@stormshield.eu

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

Copyright © Stormshield 2021. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.