Indexemblant Indexemblant Indexemblant Indexemblant Indexemblant Indexemblant Indexemblant Indexemblant Indexemblant Indexemblant Indexemblant Indexemblant Indexemblant <th></th>	
Certiguetton Totols ? Certiguetton Totols ? Control Child SA Child SA Prove Sharring Prove Testing Connections Prove Vision Child SA Address type One of a distance Control Child SA Prove Sharring Connections Prove Vision Child SA Dot 0 · 0 · 0 · 0 · 0 · 0 · 0 · 0 · 0 · 0	
Tunnel: Child SA Remote Sharing IPV4	- 0
Init Configuration Init Solution	
Image: Solution of the sectors	VPN CLIENT
Image: Solution of the solutio	
S8. Address type Noneclatures Reporte LAN address type 0	
Remote LAV address 0 0 0 0 Subnet mask 0 0 0 0 Request configuration from the gateway Pred Key Pred Key Cryptography Encryption AES CBC 255 Integrity 5H42 384 0 Diffe Helman FH14 (MODP 2048) Child SA Lifetime 1800 sec. Password	
Image: Cryptography Encrypton AES CBC 256 Integrity SH42 384 Diffe Helman DH14 (MODP 2048) Chid SA Lifetime Isso Chid SA Lifetime 1800 Sec. Sec.	
Cryptography Encryption AES CBC 255 Integrity SH42 384 Diffe Helman DH14 (MODP 2048) Lifetime Chid SA Lifetime 1800 sec.	
Encryption AES CBC 255 \vee Integrity SH42 384 \vee Diffe-Helman DH14 (MODP 2048) \vee Lifetime Child SA Lifetime 1800 sec. Encryption AES CBC 256 \vee Password Multiple AUTH support Encryption AES CBC 256 \vee Pencesan SH42 384 \vee Encryption AES CBC 256 \vee Pencesan SH42 384 \vee	
Integrity SH42 384 \v Diffe-Helman DH14 (MODP 2048) \v Lifetime	
Diffe-Helman DH14 (MODP 2048) v Lifetime	
Lifetime	
Child SA Lifetime 1800 sec. Encryption AES CBC 256 Penceation SH42 384 Key Group Dirti4 (MODP 2048) V	
Child SA Lifetime 1800 sec. Encryption AES CBC 256 Penciation SH42 384 Key Group Dirtie (MODP 2048)	
Menotation (SHA2.384 V Key Group (Dirtis@n000#2048) V	
Key Group DH14 (MODP 2048) V	
Clent ready	
Cieurseph	
XRA (sans DHT# (skobs sore) A	
Distance of the second se	

TheGreenBow IPsec VPN Client

Configuration Guide STORMSHIELD

Website: www.thegreenbow.com Contact: support@thegreenbow.com

Property of TheGreenBow - Sistech S.A. © 2018

Configuration Guide

Table of Contents

1	Intro	oduction	3
	1.1	Goal of this document	3
	1.2	VPN Network topology	3
	1.3	STORMSHIELD Restrictions	3
	1.4	STORMSHIELD VPN Gateway	3
	1.5	STORMSHIELD VPN Gateway product info	3
2	STO	RMSHIELD VPN configuration	4
	2.1	Server Certificates	4
	2.2	Client Certificates	4
	2.3	Create VPN connections in STORMSHIELD	4
3	The	GreenBow IPsec VPN Client configuration	8
	3.1	VPN Client - IKE Auth Configuration	8
	3.2	VPN Client Phase 2 (Child SA) Configuration	9
	3.3	Open IPsec VPN tunnels1	0
4	Tool	s in case of trouble1	1
	4.1	A good network analyser: Wireshark1	1
5	VPN	IPsec Troubleshooting1	2
	5.1	"NO_PROPOSAL_CHOSEN" error (wrong IKE Auth)1	2
	5.2	"AUTHENTICATION_FAILED" error1	2
	5.3	"No user certificate available for the connexion" error1	2
	5.4	"Remote ID rejected" error1	2
	5.5	"NO_PROPOSAL_CHOSEN" error (wrong CHILD SA)1	2
	5.6	"FAILED_CP_REQUIRED" error1	3
	5.7	I clicked on "Open tunnel", but nothing happens1	3
	5.8	The VPN tunnel is up but I can't ping !1	3
6	Cont	acts1	4

2

1 Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPsec VPN Client software with a STORMSHIELD VPN router to establish VPN connections for remote access to corporate network.

1.2 VPN Network topology

In our VPN network example (diagram hereafter), we will connect TheGreenBow IPsec VPN Client software to the LAN behind the STORMSHIELD router. The VPN client is connected to the Internet with a DSL connection or through a LAN. All the addresses in this document are given for example purpose.



1.3 STORMSHIELD Restrictions

No known restrictions

1.4 STORMSHIELD VPN Gateway

Our tests and VPN configuration have been conducted with STORMSHIELD version 3.6.1.

1.5 STORMSHIELD VPN Gateway product info

It is critical that users find all necessary information about STORMSHIELD VPN Gateway. All product info, User Guide and knowledge base for the STORMSHIELD VPN Gateway can be found on the STORMSHIELD website: https://www.stormshield.com/

STORMSHIELD Product page	https://www.stormshield.com/
STORMSHIELD User Guide	https://documentation.stormshield.eu/SNS_v3/fr/Default.htm

2 STORMSHIELD VPN configuration

This section describes how to build an IPsec VPN configuration with your STORMSHIELD VPN router.

2.1 Server Certificates

Once connected to your STORMSHIELD VPN gateway, make sure you have Certificate authority and these certificates are created.

- CA Certificate : Certificate authority Certificate.
 - Server Certificate : Certificate of the STORMSHIELD machine, signed by above CA Certificate.

2.2 Client Certificates

- User Certificate : User Certificate to be imported to VPN Client.

It is possible to export ".p12" format file from STORMSHIELD.

2.3 Create VPN connections in STORMSHIELD

Once done, go to the menu Configuration > VPN > VPN IPsec > CORRESPONDANTE.

Create an IKEv2 tunnel and set as follows.



Set a name for the tunnel

ASSISTANT DE CRÉATION D'UN CORRESPONDANT NOMADE IKEV2	\approx
DÉFINITION DU TYPE D'IDENTIFICATION - ASSISTANT DE CRÉATION DE CORRESPONDANT NOMADE	
Nom de la configuration nomade : nomade_ikev2	
✓ Précédent Suivant >> X Annuler	

Select Certificate

ASSISTANT DE CRÉATION D'UN CORRESPONDANT NOMADE IKEV2	\approx
IDENTIFICATION DES CORRESPONDANTS - ASSISTANT DE CRÉATION DE CORRESPONDANT NOMADE	
AUTHENTIFICATION DU CORRESPONDANT	
Certificat	
○ Clé prépartagée (PSK)	
≪ Précédent Suivant >> ★ Annuler	

Select Server certificate

		Choisissez un certificat	8
		Rechercher × Filtre : Tous -	
		SSL proxy default authority	
		▲ (sslvpn-full-default-authority	
		b openvpnserver	
Certificat :	CASNS:sns.local × P	openvpnclient	
		A 🛅 CASNS	
		Client1	
		sns.local	
		client2	
		Client3	
		Client4	
		4 user4 user4	
		🚯 xauth	
Précédent	Suivant »		
			-
		Sélectionner 🛛 🗱 Annuler	

Chercher dans les corres			
♣ Ajouter	Correspondant:nomade ikev2		
Nom 🔺	-		
nomade_ikev2	Commentaire :		
mobile_ikev2_cert	Passerelle distante :		~ e.
nomade_ikev1_cert	Configuration de secours :	None	~
	Profil IKE :	GoodEncryption	*
	Version IKE :	IKEv2	¥
	Identification		
	Méthode d'authentification :	Certificat	*
	Certificat :	CASNS:sns.local	×P
	Local ID (Optionnel):	Saisir un identifian	t
		PSK	
	─ △ Configuration avancée		
	Mode de secours :	temporary	
	Adresse locale :	Any	*
	Ne pas initier le tunnel (Responder-only) :		
	DPD ·	Paceif	×

IKE Profile is set to Good encryption in this sample. This profile can be managed in "Profils de Chiffrement".

Add new mobile Policy.

Select "nomade_ikev2" tunnel which we created in above step (Page 5).

In wizard, select the network to be reached by VPN Client computer.

VPN IPSEC				
POLITIQUE DE CHIFFREMENT - TUNNELS COR	RESPONDANTS IDENTIFIC	ATION PROFILS DE C	HIFFRE	ASSISTANT DE POLITIQUE VPN IPSEC NOMADE
A (1) IPsec 01	cette politique Editer+ 🕒			
SITE À SITE (GATEWAY-GATEWAY)	B & ANONYME - UTILISATEUR	S NOMADES	_	
Sélectionnez le correspondant mobile :	nomad	le_ikev2 🗸	1	
Texte recherchi 🗶 💠 Ajouter 🕶 🔀 Supprimer	Monter I Descendre	Couper 🚰 Copie	· 50	
Ligne Etat Réseau local	Réseau nomade	Profil de chiffrement	Mode	
1 on Vietwork_proge	vpn_network	GoodEncryption		Cette politique rend accessible via un tunnel IPsec, les réseaux locaux aux utilisateurs autorisés. Tas cette configuration, les utilisateurs distants se connectent avec leur propre adresse IP ESSURCES LOCALES

Enable Mode config.

"vpn_network" is a pool of virtual address to be assigned for VPN Clients.

A (1)	IPsec 01	- AA	ctiver cette politique Editer - 🤅	E	
	SITE À SIT	E (GATEWAY-GATEWAY)	- 8 T ANONYME - UTILISATED	JRS NOMADES	
électio	onnez le co	orrespondant mobile :	nom	ade_ikev2 🔻	
Texte r	echerchi ×	🖌 🕂 Ajouter 🕶 🔀 Supp	orimer 🕇 Monter 👃 Descendr	re 💣 Couper 💣 Copie	er 🤄 Coller
Ligne	Etat	Réseau local	Réseau nomade	Profil de chiffrement	Mode config
1	🔵 on 👁	Network_bridge	vpn_network	GoodEncryption	🔵 on Ϛ Modifier
	Nom : N Adress Masqu	Network_bridge se IP : 192.168.175.0 e : 255.255.255.0	Nom : vpn_network Adresse IP : 192.168.10.0		

Once done, activate the IPsec policy.

Note : Firewall rules needs to be created for allowing IPsec traffic in "Filtrage" and "NAT".

- Allow Ports: UDP500 (isakmp) and UDP4500 (isakmp_natt) from Internet to Firewall.
- Allow also VPN traffic from "vpn_network" to "Network_bridge".

Please consult STORMSHIELD guide to create firewall rules.

3 TheGreenBow IPsec VPN Client configuration

This section describes the required configuration to connect to a STORMSHIELD VPN router via VPN connections.

To download the latest release of TheGreenBow IPsec VPN Client software, please go to **www.thegreenbow.com/vpn_down.html.**

3.1 VPN Client - IKE Auth Configuration

THEGREENBOW	Secure Connect	tions	
	To_Stormshield: IKE Auth		VPN PREMIUM
VPN Configuration K V1 K V1 K V1 K V1 Parameters K V2 K V2	Authentication Protocol Gateway Certi Remote Gateway Interface Any	ficate	The remote VPN Gateway IP address is either an explicit IP address or a DNS Name
	Remote Gateway mygate Authentication Preshared Key Confirm Confirm	way.dyndns.org	
	Cryptography		Multiple AUTH support
	Encryption Auto Authentication Auto Key Group Auto	~ ~	

Import the User certificate in Certificate tab, which you exported from the STORMSHIELD router.

This configuration is one example of what can be accomplished in term of User Authentication. You may want to refer to either the STORMSHIELD router user guide or TheGreenBow IPsec VPN Client software User Guide for more details on User Authentication options.

3.2 VPN Client Phase 2 (Child SA) Configuration

😌 TheGreenBow VPN Client			– 🗆 🗙
Configuration Tools ?			
THEGREENBOW	Secure Conne	ections	
	Tunnel: Child SA		VPN PREMIUM
VPN Configuration	Child SA Advanced Automation Re	mote Sharing	IPV4 IPV6
	VPN Client address	0.0.0.0	Virtual IP address
55L	Address type	Subnet address 🛛 🗸	address/subnet wi
	Remote LAN address	0.0.0.0	sent by Gatewa
	Subnet mask	0.0.0.0	through Mode C
		Request configuration from the	: gateway
	Cryptography		
	Encryption	Auto \checkmark	
	Integrity	Auto 🗸	
	Diffie-Hellman	Auto 🗸	
	Lifetime		
	Child SA Lifetime	1800 sec.	
VPN Client ready			

Child SA Configuration

3.3 **Open IPsec VPN tunnels**

Once both STORMSHIELD router and TheGreenBow IPsec VPN Client software have been configured accordingly, you are ready to open VPN tunnels. First make sure you enable your firewall with IPsec traffic.

- 1/ Select menu "Configuration" and "Save" to take into account all modifications we've made on your VPN Client configuration.
- 2/ Double Click on your Child SA tunnel name or Click "**Open**" button in Connection panel to open tunnel.
- 3/ Select menu "Tools" and "Console" if you want to access to the IPsec VPN logs. The following example shows a successful connection between TheGreenBow IPsec VPN Client and a STORMSHIELD VPN router.

4 Tools in case of trouble

Configuring an IPsec VPN tunnel can be a hard task. One missing parameter can prevent a VPN connection from being established. Some tools are available to find source of troubles during a VPN establishment.

4.1 A good network analyser: Wireshark

Wireshark is a free software that can be used for packet and traffic analysis. It shows IP or TCP packets received on a network card. This tool is available on website **www.wireshark.org**. It can be used to follow protocol exchange between two devices. For installation and use details, read its specific documentation (**www.wireshark.org/docs/**).

	isakmp					Expression + Appliquer ce filtre Appliquer ce filtre
No.		Time	Source	Destination	Protocol	Length Info
E	10	-18.903591	192.168.200.8	88.162.180.74	ISAKMP	1270 IKE_SA_INIT MID=00 Initiator Request
L	17	-14.932894	88.162.180.74	192.168.200.8	ISAKMP	1315 IKE_SA_INIT MID=00 Responder Response
	19	-14.901354	192.168.200.8	88.162.180.74	ISAKMP	102 IKE_AUTH MID=01 Initiator Request
	21	-14.842711	88.162.180.74	192.168.200.8	ISAKMP	102 IKE_AUTH MID=01 Responder Response
	227	-7.946751	192.168.200.8	88.162.180.74	ISAKMP	142 INFORMATIONAL MID=02 Initiator Request
	228	-7.946642	192.168.200.8	88.162.180.74	ISAKMP	142 INFORMATIONAL MID=03 Initiator Request
	236	-7.894043	88.162.180.74	192.168.200.8	ISAKMP	142 INFORMATIONAL MID=02 Responder Response
	237	-7.894042	88.162.180.74	192.168.200.8	ISAKMP	142 INFORMATIONAL MID=03 Responder Response

5 VPN IPsec Troubleshooting

5.1 "NO_PROPOSAL_CHOSEN" error (wrong IKE Auth)

```
20XX0913 16:08:53:387 TIKEV2_Tunnel SEND IKE_SA_INIT
[HDR][SA][NONCE][N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTINATION_IP)][KE][VID][N(FR
AGMENTATION_SUPPORTED)]
20XX0913 16:08:53:419 TIKEV2 Tunnel RECV IKE SA INIT [HDR][N(NO PROPOSAL CHOSEN)]
```

If you have an "NO_PROPOSAL_CHOSEN" error you might have a wrong Phase 1 [IKE Auth], check if the encryption algorithms are the same on each side of the VPN tunnel.

5.2 "AUTHENTICATION_FAILED" error

```
20XX0913 16:15:22:032 TIKEV2_Tunnel RECV IKE_AUTH [HDR] [N (AUTHENTICATION_FAILED)]
20XX0913 16:15:22:032 TIKEV2 Tunnel Remote endpoint sends error AUTHENTICATION FAILED
```

If you have an "AUTHENTICATION_FAILED" error, it means that the certificate or the preshared key is not matching. Check the Gateway if the user certificate or preshared key is valid.

5.3 "No user certificate available for the connexion" error

```
20XX0913 16:18:07:491 TIKEV2_TUNNEL RECV IKE_SA_INIT
[HDR][SA][KE][NONCE][N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTINATION_IP)][CERTREQ][
N(FRAGMENTATION_SUPPORTED)][N(MULTIPLE_AUTH_SUPPORTED)]
20XX0913 16:18:07:491 TIKEV2_TUNNEL IKE SA I-SPI 8D4467C52C91C316 R-SPI 9DF0F0E4A91F8867
20XX0913 16:18:07:491 TIKEV2_TUNNEL No user certificate available for the connexion
20XX0913 16:18:07:491 TIKEV2_TUNNEL Connection aborted.
```

Check if the certificate is selected or the Token (smartcard) is available on the computer.

5.4 "Remote ID rejected" error

20180913 16:24:32:087 TIKEV2_Tunnel ID types do not match. Expecting ID_RFC822_ADDR. Receiving ID_DER_ASN1_DN 20180913 16:24:32:087 TIKEV2 Tunnel Remote IDr rejected

The "Remote ID" value (see "Protocol" tab) does not match what the remote endpoint is expected.

5.5 "NO_PROPOSAL_CHOSEN" error (wrong CHILD SA)

```
20XX0913 16:25:14:933 TIKEV2 Tunnel SEND IKE SA INIT
[HDR] [SA] [NONCE] [N (NAT_DETECTION_SOURCE_IP) ] [N (NAT_DETECTION_DESTINATION_IP) ] [KE] [N (FRAGMEN
TATION SUPPORTED)]
20XX0913 16:25:15:118 TIKEV2 Tunnel RECV IKE SA INIT
[HDR][SA][KE][NONCE][N(NAT DETECTION SOURCE IP)][N(NAT DETECTION DESTINATION IP)][CERTREQ][
N(MULTIPLE AUTH SUPPORTED)]
20XX0913 16:25:15:118 TIKEV2 Tunnel IKE SA I-SPI E389FC49EE7078F1 R-SPI 00F37D557ED307FC
20XX0913 16:25:15:118 TIKEV2_Tunnel SEND IKE_AUTH
[HDR] [IDi] [CERTI] [CERTREQ] [AUTH] [CP] [SA] [TSi] [TSr] [N (INITIAL CONTACT)] [N (ESP TFC PADDING NOT
 SUPPORTED)]
20XX0913 16:25:15:165 TIKEV2 Tunnel RECV IKE AUTH
[HDR] [IDr] [CERT] [AUTH] [CP] [N (AUTH LIFETIME)] [N (NO PROPOSAL CHOSEN)]
20XX0913 16:25:15:165 TIKEV2 Tunnel IKE AUTH renewal in 1654 seconds (16:52:49)
20XX0913 16:25:15:165 TIKEV2 Tunnel SEND CHILD SA
[HDR] [SA] [NONCE] [KE] [TSi] [TSr] [N (ESP TFC PADDING NOT SUPPORTED)]
20XX0913 16:25:15:202 TIKEV2_Tunnel RECV CHILD_SA [HDR][N(NO_PROPOSAL_CHOSEN)]
20XX0913 16:25:15:202 TIKEV2_Tunnel Remote endpoint sends error NO_PROPOSAL_CHOSEN
20XX0913 16:25:15:202 TIKEV2_Tunnel SEND INFORMATIONAL [HDR][DELETE]
```

If you have an "NO_PROPOSAL_CHOSEN" error, check that the "Child SA" encryption algorithms are the same on each side of the VPN Tunnel.

5.6 "FAILED_CP_REQUIRED" error

```
20XX0913 16:29:46:780 TIKEV2_Tunnel RECV IKE_AUTH
[HDR][IDr][CERT][AUTH][N(AUTH_LIFETIME)][N(FAILED_CP_REQUIRED)][N(TS_UNACCEPTABLE)]
20180913 16:29:46:780 TIKEV2_Tunnel Remote endpoint sends error FAILED_CP_REQUIRED
20XX0913 16:29:46:780 TIKEV2_Tunnel Remote endpoint is expecting a configuration request
from the client
```

If you have an "FAILED_CP_REQUIRED" error, then the Gateway is configured to use Mode CP. Go to Traffic selectors and enable "Request configuration from the gateway".

5.7 I clicked on "Open tunnel", but nothing happens.

```
20XX1003 11:08:34:031 [VPNCONF] TGBIKE_STARTED received
20XX1003 11:21:34:379 TIKEV2_vRHEL75 SEND IKE_SA_INIT
[HDR][SA][NONCE][N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTINATION_IP)][KE]
20XX1003 11:21:39:397 TIKEV2_vRHEL75 SEND IKE_SA_INIT
[HDR][SA][NONCE][N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTINATION_IP)][KE]
20XX1003 11:21:44:409 TIKEV2_vRHEL75 SEND IKE_SA_INIT
[HDR][SA][NONCE][N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTINATION_IP)][KE]
20XX1003 11:21:44:409 TIKEV2_vRHEL75 SEND IKE_SA_INIT
[HDR][SA][NONCE][N(NAT_DETECTION_SOURCE_IP)][N(NAT_DETECTION_DESTINATION_IP)][KE]
20XX1003 11:21:49:423 TIKEV2 vRHEL75 3 attempts with no response. Aborting connection.
```

Read logs of each VPN tunnel endpoint. IKE requests can be dropped by firewalls. An IPsec Client uses UDP port 500.

Check if the remote server is online.

5.8 The VPN tunnel is up but I can't ping !

If the VPN tunnel is up, but you still cannot ping the remote LAN, here are a few guidelines:

- Check Child SA settings: VPN Client address and Remote LAN address. Usually, VPN Client IP address should not belong to the remote LAN subnet
- Once VPN tunnel is up, packets are sent with ESP protocol. This protocol can be blocked by firewall.
 Check that every device between the client and the VPN server does accept ESP
- Check your VPN server logs. Packets can be dropped by one of its firewall rules.
- Check your ISP support ESP and if the protocol 50 is allowed to pass traffic in your firewalls.
- If you still cannot ping, follow ICMP traffic on VPN server LAN interface and on LAN computer interface (with Wireshark for example). You will have an indication that encryption works.
- Check the "default gateway" value in VPN Server LAN. A target on your remote LAN can receive pings but does not answer because there is a no "Default gateway" setting.
- You cannot access to the computers in the LAN by their name. You must specify their IP address inside the LAN.
- We recommend you to install Wireshark (www.wireshark.org) on one of your target computer. You can check that your pings arrive inside the LAN.

6 Contacts

News and updates on TheGreenBow web site: www.thegreenbow.com

Technical support by email at: support@thegreenbow.com

Sales contacts by email at: sales@thegreenbow.com

Secure, Strong, Simple TheGreenBow Security Software