

TheGreenBow IPSec VPN Client Configuration Guide

IPCop 1.4.16

WebSite: Contact: http://www.thegreenbow.com support@thegreenbow.com

IPSec VPN Router Configuration



Doc.Ref	tgbvpn_ug_ipcop_en
Doc.version	1.0 - Oct 2007
VPN version	4.x

Table of contents

1	Introduction	3
	I.1 Goal of this document	3
	I.2 VPN Network topology	3
	I.3 IPCop VPN Gateway product info	3
n	Sotting up IDCon 1.4.14	1
Ζ	Selling up IPCop 1.4.10	4
	2.1 Piepdilly IPCUPS built	4 E
		J
3	Setting up TheGreenBow IPSec VPN Client	9
	3.1 VPN Client Phase 1 Configuration	9
	3.2 VPN Client Phase 2 Configuration	. 11
1	Teals in case of trouble	10
4	1 UUIS III Lase of Il Ouble	. IJ 12
	F. T. A YOOU HEIWOIK allalysel. ethereal	. 13
5	VPN IPSec Troubleshooting	. 14
	5.1 « PAYLOAD MALFORMED » error (wrong Phase 1 [SA])	. 14
	5.2 « INVALID COOKIE » error	. 14
	5.3 « no keystate » error	. 14
	5.4 « received remote ID other than expected » error	. 14
	5.5 « NO PROPOSAL CHOSEN » error	. 15
	5.6 « INVALID ID INFORMATION » error	. 15
	5.7 I clicked on "Open tunnel", but nothing happens	. 15
	5.8 The VPN tunnel is up but I can't ping !	. 15
,		47
6	Contacts	. 17

TH	E	6	R	1000	Ē		M	684	181
				1					

Doc.Ref	tgbvpn_ug_ipcop_en
Doc.version	1.0 - Oct 2007
VPN version	4.x

1 Introduction

1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPSec VPN Client with a free Linux distribution firewall downloadable from http://www.ipcop.org

This document is not a tutorial about IPCop installation as there are many "Howto" available on the internet.

1.2 VPN Network topology

In our VPN network example (diagram hereafter), we will connect TheGreenBow IPSec VPN Client to the LAN behind the IPCop firewall. The VPN Client is connected to the Internet with a DSL connection or from a LAN. All the addresses in this document are given for example purpose.

The network configuration chosen for IPCop is GREEN+ RED interfaces (LAN+WAN).

A Road Warrior connection also needs to be configured. The following example makes use of these values:

• External IP of the IPCop (red interface):

IP Subnet behind the green interface (LAN):

mygateway.dyndns.org (or public IP address) 172.16.0.0/255.255.255.0



1.3 IPCop VPN Gateway product info

It is critical that users find all necessary information about IPCop VPN Gateway. All product info, User Guide and knowledge base for the IPCop VPN Gateway can be found on the IPCop website: <u>http://ipcop.org</u>

IPCop Product page: <u>http://ipcop.org/index.php?module=pnWikka&tag=IPCop14xFeatures</u> IPCop User Guide: <u>http://ipcop.org/index.php?module=pnWikka&tag=IPCopDocumentation</u>

IPCop FAQ/Knowledge Base: <u>http://ipcop.org/index.php?name=FAQ</u>

THECOECOECOE (10404040404	Doc.Ref	tgbvpn_ug_ipcop_en
	Doc.version	1.0 - Oct 2007
	VPN version	4.x

2 Setting up IPCop 1.4.16

2.1 Preparing IPCop's built

This section describes how to build an IPSec VPN configuration with your IPCop VPN router.

Once connected to your IPCop VPN gateway, go to VPNs tab.

STSIEM	HOME The bad packets stop here.
SYSTEM & STATU	S + NETWORK + SERVICES + FIREWALL + VPNS + LOGS +
	ipcop.localdomain
	Connect Disconnect Refresh
	Current profile: cegetel
	IP Address: 84.6.24.40 IPCop's Hostname:
	11:12:56 up 11:11, 0 users, load average: 0.01, 0.02, 0.00
	(i)

THECOEÉDOMI 1040410404	Doc.	Ref tgbvpn_ug_	ipcop_en
	Doc.	version 1.0 - Oct 200)7
	VPN	version 4.x	

lobal settings				
olic IP or FQDN	for RED interface or <%d	efaultroute>: dyndns	Enabled:	
erride default M	ITU: •			
lay before laund	ching VPN (seconds): 🍽	0		
start net-to-net	vpn when remote peer IP	changes (dyndns), it helps DPD: 🗌		
JTO DEBUG = cr	rypt: 🗌 , parsing: 🗹 , er	mitting: 🗹 , control: 🗹 , klips: 🗹 , dns:	🗹, nat_t: 🗹	
This field may	cha blask			
This field may If required, th	y be blank. his delay can be used to a	llow Dynamic DNS updates to propagate p	roperly. 60 is a common	Save
This field may If required, the value when R	y be blank. his delay can be used to a .ED is a dynamic IP.	llow Dynamic DNS updates to propagate p	properly, 60 is a common	Save
This field may If required, th value when R	y be blank. nis delay can be used to a .ED is a dynamic IP.	llow Dynamic DNS updates to propagate p	roperly. 60 is a common	Save
This field may If required, th value when R	y be blank. nis delay can be used to a ED is a dynamic IP. tus and control:	llow Dynamic DNS updates to propagate p	rroperly. 60 is a common	Save
This field may If required, the value when R onnection state Name	y be blank. nis delay can be used to a ED is a dynamic IP, tus and control: Type	llow Dynamic DNS updates to propagate p Common Name	roperly. 60 is a common Remark	Save Status Action
This field may If required, the value when R onnection star Name	y be blank. his delay can be used to a ED is a dynamic IP. tus and control: Type	llow Dynamic DNS updates to propagate p Common Name	roperly. 60 is a common Remark	Save Status Action
This field may If required, the value when R connection sta	y be blank. nis delay can be used to a ED is a dynamic IP. tus and control: Type	llow Dynamic DNS updates to propagate p Common Name	roperly. 60 is a common Remark	Save Status Action
This field may If required, the value when R connection state Name	y be blank. nis delay can be used to a ED is a dynamic IP. tus and control: Type	llow Dynamic DNS updates to propagate p Common Name	Remark	Save Status Action
This field may If required, the value when R connection state Name egend: P Er	y be blank. nis delay can be used to a ED is a dynamic IP. tus and control: Type	Ilow Dynamic DNS updates to propagate p Common Name	Remark	Save Status Action
This field may If required, ti value when R connection sta Name egend: \checkmark Er \Box D	y be blank. his delay can be used to a ED is a dynamic IP. tus and control: Type nabled (click to disable) isabled (click to enable)	Ilow Dynamic DNS updates to propagate p Common Name Show Certificate Show Certificate	Remark	Save Status Action
This field may If required, ti value when R connection stat Name egend: \checkmark Er D	y be blank. his delay can be used to a ED is a dynamic IP. tus and control: Type nabled (click to disable) isabled (click to enable)	Ilow Dynamic DNS updates to propagate p Common Name Show Certificate Download Certificate	Remark	Save Status Action

Press "Add" to configure a Roadwarrior connection

2.2 Setting up a Roadwarrior VPN Connection

Choose "Host-to-Net" VPN and press "Add".

Connection Type: ioinst-to-Net Virtual Private Network (RoadWarrior) Net-to-Net Virtual P <u>rivate N</u> etwork	Connection Type	
Net-to-Net Virtual Private Network	Connection Type: Diost-to-Net Virtual Private Network (RoadWarrior)	
	Net-to-Net Virtual Private Network	

Doc.Ref	tgbvpn_ug_ipcop_en
Doc.version	1.0 - Oct 2007
VPN version	4.x

connection:			
Name:	FirstVpn	Enabled:	V
Host IP address:	RED (Remote Host/IP: •	
Local Subnet:	172.16.0.0/255.255.255.0	Remote subnet:	
Local ID: • (e.g.: @xy.example.com)	test@user.com	Remote ID: 🍳	
Dead Peer Detection action:	clear 💌 🤉		
Remark: 🍳			

0	Use a Pre-Shared Key:	abcdef	
0	Upload a sertificate request:		
0	Upload a certificate:		Parcourir
0	Upload PKCS12 file PKCS12 File Password:		
0	Peer is identified by either IPV4_ADDR, FQDN, USER_FQDN or DER_ASN1_DN string in Remote ID field		
0	Generate a certificate:		
	User's Full Name or System Hostname:		
	User's E-mail Address: 🍳		
	User's Department: •		
	Organization Name: 🌑	TheGreenBow	
	City: •		
	State or Province: •		
	Country:	France	~
	Subject Alt Name (subjectAltName=email:*,URI:*,DNS:*,RID:*)		
	PKCS12 File Password:		
	PKCS12 File Password:(confirmation)		
_			

TLECDEEDERIH 0404/040	Doc.Ref	tgbvpn_ug_ipcop_en
	Doc.version	1.0 - Oct 2007
	VPN version	4.x

In connection, enter the name for this remote connection, RED interface and local subnet are already chosen, check "edit advanced configuration"

In authentication, choose "Use a Pre-Shared Key (PSK)" and enter a password that will be used in the VPNs.

Press "Save" to go on the "Advanced" settings screen:

Compression:		Nat Traversal:	
IKE Encryption:	AES (256 bit) AES (128 bit) 3DES Twofish (256 bit)	IKE Integrity:	SHA2 (512) SHA2 (256) SHA MD5
IKE Lifetime:	1 hours	IKE Grouptype:	MODP-2048 A MODP-1536 MODP-1024 MODP-768
ESP Encryption:	AES (256 bit) AES (128 bit) 3DES Twofish (256 bit)	ESP Integrity:	SHA2 (512) SHA2 (256) SHA1 MD5
ESP Keylife:	8 hours	ESP Grouptype:	Phase1 Group 💌

Choose algorithms, DH group, and lifetimes for IKE and ESP and press "Save".

Your Roadwarrior connection is now defined on VPN main screen:

		20 0 0 0 0 0 0 1 0 1 0 1 0 1		Doonton	igovpri_ug	<u>_'Poop_</u>
		0011101		Doc.version	1.0 - Oct 20	007
1				VPN versior	1 4.x	
Global set	ttings					
Public IP or	FODN for RED interface or <%	lefaultroute>: dvndns		Enabled: 🔽		
Override del	fault MTU: 🌒					
Delay before	e launching VPN (seconds): 🍽	0				
Delay before	e launching VPN (seconds): 🍽	0				
Delay before Restart net-t	e launching VPN (seconds): •• o-net vpn when remote peer IP	changes (dyndns), it helps DPD:				
Delay before	e launching VPN (seconds): ••	0 changes (dyndns), it helps DPD:				
Delay before Restart net-t PLUTO DEBU	e launching VPN (seconds): ●● o-net vpn when remote peer IP IG = crypt: □, parsing: ☑, e	0 • changes (dyndns), it helps DPD: mitting: 던 , control: 단 , klips: 단	. dns: 🗹 , nat_t:	V		
Delay before Restart net-t PLUTO DEBU	e launching VPN (seconds): ●● Io-net vpn when remote peer IP IG = crypt: □, parsing: ☑, e	0 changes (dyndns), it helps DPD: mitting: 🗹 , control: 🗹 , klips: 🖸	□ 2, dns: ♥, nat_t:	V		
Delay before Restart net-t PLUTO DEBU This fie	e launching VPN (seconds): ●● Io-net vpn when remote peer IP IG = crypt: □, parsing: ☑, e Id may be blank. ired, this delay can be used to a	0 changes (dyndns), it helps DPD: mitting: , control: , klips: allow Dynamic DNS updates to pro	, dns: , nat_t:	I is a common	Sava	
Delay before Restart net-t PLUTO DEBU This fie UT frequi value w	e launching VPN (seconds): ●● io-net vpn when remote peer IP IG = crypt: □, parsing: ♥, e Id may be blank. ired, this delay can be used to a when RED is a dynamic IP.	0 changes (dyndns), it helps DPD: mitting: , control: , klips: sllow Dynamic DNS updates to pro	□ , dns: ☑, nat_t: pagate properly. 60	₽ is a common	Save	
Delay before Restart net-t PLUTO DEBU This fie Value w	e launching VPN (seconds): ●● io-net vpn when remote peer IP IG = crypt: □, parsing: ☑, e Id may be blank. ired, this delay can be used to a when RED is a dynamic IP.	0 • changes (dyndns), it helps DPD: mitting: , control: , klips: allow Dynamic DNS updates to pro	□ 2, dns: ☑, nat_t: pagate properly. 60	▼ is a common	Save	
Delay before Restart net-t PLUTO DEBU This fie This fie Connection	e launching VPN (seconds): ●● Io-net vpn when remote peer IP IG = crypt: □, parsing: ♥, e Id may be blank. Ired, this delay can be used to a when RED is a dynamic IP. In status and control:	0 • changes (dyndns), it helps DPD: mitting: , control: , klips: allow Dynamic DNS updates to pro	□ 2, dns: ☑, nat_t: pagate properly. 60	v is a common	Save	
Delay before Restart net-t PLUTO DEBU This fie If requivalue w Connection Name	e launching VPN (seconds): •• co-net vpn when remote peer IP IG = crypt: , parsing: , e Id may be blank. ired, this delay can be used to a when RED is a dynamic IP. on status and control: Type	0 changes (dyndns), it helps DPD: mitting: , control: , klips: allow Dynamic DNS updates to pro	, dns: ♥, nat_t: pagate properly. 60	✓ is a common	Save	Action
Delay before Restart net-t PLUTO DEBU This fie This fie This fie Connection Name	e launching VPN (seconds): •• co-net vpn when remote peer IP IG = crypt: , parsing: , e Id may be blank. Ired, this delay can be used to a when RED is a dynamic IP. on status and control: Type	0 changes (dyndns), it helps DPD: mitting: , control: , klips: allow Dynamic DNS updates to pro Common Name	, dns: ♥, nat_t: pagate properly. 60	is a common	Save Status	Action
Delay before Restart net-t PLUTO DEBU This fie This fie This fie Connection Name	e launching VPN (seconds): •• co-net vpn when remote peer IP IG = crypt: , parsing: , e Id may be blank. ired, this delay can be used to a when RED is a dynamic IP. on status and control: Type	0 • changes (dyndns), it helps DPD: mitting: , control: , klips: allow Dynamic DNS updates to pro Common Name	pagate properly. 60	is a common	Save	Action
Delay before Restart net-t PLUTO DEBU This fie This fie This fie Connection Name	e launching VPN (seconds): ●● io-net vpn when remote peer IP IG = crypt: □, parsing: ☑, e Id may be blank. ired, this delay can be used to a when RED is a dynamic IP. on status and control: Type	0 changes (dyndns), it helps DPD: mitting: , control: , klips: allow Dynamic DNS updates to pro Common Name	□ 2, dns: ☑, nat_t: pagate properly. 60	v is a common Remark	Save Status	Action
Delay before Restart net-t PLUTO DEBU This file This file This file Connection Name	e launching VPN (seconds): ●● Io-net vpn when remote peer IP IG = crypt: □, parsing: ☑, e Id may be blank. Ired, this delay can be used to a when RED is a dynamic IP. Don status and control: Type Host (PSK).	0 changes (dyndns), it helps DPD: mitting: , control: , klips: sllow Dynamic DNS updates to pro Common Name	□ 2, dns: ☑, nat_t: pagate properly. 60	v is a common Remark	Save Status	Action
Delay before Restart net-t PLUTO DEBU This fie This fie This fie Connection Name FirstVpn Legend:	e launching VPN (seconds): •• co-net vpn when remote peer IP IG = crypt:, parsing: _/_, e Id may be blank. ired, this delay can be used to a when RED is a dynamic IP. on status and control: Type Host (PSK) Enabled (click to disable)	0 changes (dyndns), it helps DPD: mitting: , control: , klips: allow Dynamic DNS updates to pro Common Name	, dns: ♥, nat_t: pagate properly. 60	v is a common Remark	Save Status	Action
Delay before Restart net-t PLUTO DEBU This fie This fie This fie Connection Name FirstVpn Legend:	e launching VPN (seconds): •• io-net vpn when remote peer IP IG = crypt: , parsing: , e Id may be blank. ired, this delay can be used to a when RED is a dynamic IP. on status and control: Type Host (PSK) Host (PSK) Disabled (click to disable) Disabled (click to enable)	0 changes (dyndns), it helps DPD: mitting: , control: , klips: allow Dynamic DNS updates to pro Common Name Show Certificate Download Certificate	 , dns: ♥, nat_t: pagate properly. 60 Edit	v is a common Remark	Save Status	Action

On connection status and control, click on the download certificate icon and save it (in our example it is named tgb1.p12)

IPCop VPN Configuration is finished.

Doc.Ref	tgbvpn_ug_ipcop_en
Doc.version	1.0 - Oct 2007
VPN version	4.x

3 Setting up TheGreenBow IPSec VPN Client

3.1 VPN Client Phase 1 Configuration

Right click on Configuration in TheGreenBow IPSec VPN Client and select "Add Phase 1".

TheGreenBow VPN Cli	ent 📃 🗖 🔀
Eile VPN Configuration View	<u>I</u> ools <u>?</u>
THEGREENBOL	IPSec VPN Client
🔑 Console	Phase 1 (Authentication)
Parameters	Name ipcop_config
S Connections	Interface 172.16.0.106
Configuration	Remote Gateway tgbzone.dyndns.biz Preshared Key Confirm: Confirm: Confirm: Certificate Certificate Certificate IKE Encryption AES 128 P1 Advanced P1 Advanced
	Save & Apply
VPN ready	Tunnel: 🥑

Make sure you put in the area of Preshared Key "abcdef" as in the IPCop's config. Choose "P1 Advanced":

Doc.Ref	tgbvpn_ug_ipcop_en
Doc.version	1.0 - Oct 2007
VPN version	4.x

Phase1 Advanced		
		S
Advanced features		
🔲 Config Mode	Redund.GW	
C Aggressive Mode	NAT-T	Automatic 💽
X-Auth		
🗖 X-Auth Popup	Login	
Hybrid Mode	Password	
Local and Remote ID		
Chaese the ty	pe of ID:	Set the value for the ID:
	X	test@user.com
Remote ID	•	
	[Ok Cancel

Local ID can be defined as Email and depends on the type ID type defined on routers. Put the Email address for the value of the ID. Nothing is needed in Remote ID. Press "Ok".

THECDEEDEMI 104040404	Doc.Ref	tgbvpn_ug_ipcop_en
	Doc.version	1.0 - Oct 2007
	VPN version	4.x

3.2 VPN Client Phase 2 Configuration

Create a Phase2 by right-clicking on Phase1:

TheGreenBow VPN Clie	nt 📃 🗖 🔀
<u>File VPN Configuration Tools</u>	2
THEGREENBOW	IPSec VPN Client
🔑 Console	Phase 2 (IPSec Configuration)
Parameters	Name CnxVpn1
S Connections	VPN Client address 0 . 0 . 0 . 0
Configuration	Address upe Subnet address
	ESP Encryption AES 128 Authentication SHA Mode Tunnel
	Save & Apply
VPN Tunnel opened	Tunnel: 🧿

Modify Address type by choosing subnet address, and add the remote LAN address and mask (must match what was defined on IPCop)

Algorithms, PFS and DH group must match IPCop settings in advanced screen in section 2.2 of this document.

The VPN Client address must not belong to the remote subnet range. In our example, we chose 0.0.0.0 meaning the VPN Client address is the physical address of the machine dynamically assigned by ISP (from a hotel for example).

If the roadwarrior tries to connect from a LAN which address is 172.16.0.0, the VPN tunnel won't establish correctly. In this case you must specify an IP address in another range (10.0.0.1 for example, or 192.168.0.1 or whatever private IP address you wish)

Phase2 advanced is used to enter alternate DNS and/or wins servers addresses from the ones the VPN Client is using prior to establish the tunnel.

THECOEÉDOCH 040140304	Doc.Ref	tgbvpn_ug_ipcop_en
	Doc.version	1.0 - Oct 2007
	VPN version	4.x

Successful console log for this VPN tunnel:

VPN Console ACTIVE		
VPN Console ACTIVE Save Stop Clear 20071024 100934 Default (SA ipcop_config-P1) SEND phase 1 Main Mode [SA] [VID] [VID 20071024 100935 Default (SA ipcop_config-P1) RECV phase 1 Main Mode [SA] [VID] [VID 20071024 100935 Default (SA ipcop_config-P1) SEND phase 1 Main Mode [KEY_EXCH] [N 20071024 100935 Default (SA ipcop_config-P1) RECV phase 1 Main Mode [KEY_EXCH] [N 20071024 100935 Default (SA ipcop_config-P1) RECV phase 1 Main Mode [HASH] [ID] 20071024 100935 Default (SA ipcop_config-P1) RECV phase 1 Main Mode [HASH] [ID] 20071024 100935 Default (SA ipcop_config-P1) RECV phase 1 Main Mode [HASH] [ID] 20071024 100935 Default (SA ipcop_config-P1) RECV phase 1 Main Mode [HASH] [ID] 20071024 100935 Default (SA ipcop_config-P1) RECV phase 1 Main Mode [HASH] [ID] 20071024 100935 Default (SA ipcop_config-P1) RECV phase 1 Main Mode [HASH] [ID] 20071024 100935 Default (SA ipcop_config-P1) RECV phase 1 Main Mode [HASH] [ID] 20071024 100935 Default (SA ipcop_config-P1) RECV phase 2 Quick Mode [HAS] 20071024 100936 Default (SA ipcop_config-CnxVpn1-P2) SEND phase 2 Quick Mode [HAS] 20071024 100936 Default (SA ipcop_config-CnxVpn1-P2) SEND phase 2 Quick Mode [HAS] 20071024 100936 Default (SA ipcop_config-CnxVpn1-P2) SEND phase 2 Quick Mode [HAS] 20071024 100936 Default (SA ipcop_config-CnxVpn1-P2) SEND phase 2 Quick Mode [HAS] 20071024 100936 Default (SA ipcop_config-CnxVpn1-P2) SEND phase 2 Quick Mode [HAS] 20071024 100936 Default (SA ipcop_config-CnxVpn1-P2) SEND phase 2 Quick Mode [HAS] 20071024 100936 Default (SA ipcop_config-CnxVpn1-P2) SEND phase 2 Quick Mode [HAS] 20071024 100936 Default (SA ipcop_config-CnxVpn1-P2) SEND phase 2 Quick Mode [HAS] 20071024 100936 Default (SA ipcop_config-CnxVpn1-P2) SEND phase 2 Quick Mode [HAS] 20071024 100936 Default (SA ipcop_config-CnxVpn1-P2) SEND phase 2 Quick Mode [HAS] 20071024 100936 Default (SA ipcop_config-CnxVpn1-P2) SEND phase 2 Quick Mode [HAS] 20071024 100936 Default (SA ipcop_config-CnxVpn1-P2) SEND phase 2 Quick Mode [HAS] 20071024 100936 Default (SA ipcop_conf] [VID] [VID] [VID] NONCE] [NAT_D] [NAT IONCE] [NAT_D] [NAT IONCE] [NAT_D] [NAT SH] [SA] [KEY_EXCH] [I SH]	_D] _D] NONCE] [ID] [ID] NONCE] [ID] [ID]
	Current line : 10	max. lines : 10000

THE	5R	EE	NB	8311781

Doc.Ref	tgbvpn_ug_ipcop_en
Doc.version	1.0 - Oct 2007
VPN version	4.x

4 Tools in case of trouble

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

4.1 A good network analyser: ethereal

Ethereal 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 <u>http://www.ethereal.com/</u>. It can be used to follow protocol exchange between two devices. For installation and use details, read its specific documentation.

Doc.Ref	tgbvpn_ug_ipcop_en
Doc.version	1.0 - Oct 2007
VPN versior	4.x

5 VPN IPSec Troubleshooting

5.1 « PAYLOAD MALFORMED » error (wrong Phase 1 [SA])

114920 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [SA][VID] 114920 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [NOTIFY] 114920 Default exchange_run: exchange_validate failed 114920 Default dropped message from 195.100.205.114 port 500 due to notification type PAYLOAD_MALFORMED 114920 Default SEND Informational [NOTIFY] with PAYLOAD_MALFORMED error

If you have an « PAYLOAD MALFORMED » error you might have a wrong Phase 1 [SA], check if the encryption algorithms are the same on each side of the VPN tunnel.

5.2 « INVALID COOKIE » error

115933 Default message_recv: invalid cookie(s) 5918ca0c2634288f 7364e3e486e49105 115933 Default dropped message from 195.100.205.114 port 500 due to notification type INVALID_COOKIE 115933 Default SEND Informational [NOTIFY] with INVALID_COOKIE error

If you have an « INVALID COOKIE » error, it means that one of the endpoint is using a SA that is no more in use. Reset the VPN tunnel on each side.

5.3 « no keystate » error

115315 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [SA][VID] 115317 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [SA][VID] 115317 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [KEY][NONCE] 115319 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [KEY][NONCE] 115319 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY] 115319 Default ipsec_get_keystate: no keystate in ISAKMP SA 00B57C50

Check if the preshared key is correct or if the local ID is correct (see « Advanced » button). You should have more information in the remote endpoint logs.

5.4 « received remote ID other than expected » error

120348 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [SA][VID] 120349 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [SA][VID] 120349 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [KEY][NONCE] 120351 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [KEY][NONCE] 120351 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY] 120351 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [ID][HASH][NOTIFY] 120351 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [ID][HASH][NOTIFY] 120351 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [ID][HASH][NOTIFY] 120351 Default ike_phase_1_recv_ID: received remote ID other than expected support@thegreenbow.fr

The « Remote ID » value (see « Advanced » Button) does not match what the remote endpoint is expected.

THEGREEDBOU	Doc.Ref	tgbvpn_ug_ipcop_en
	Doc.version	1.0 - Oct 2007
	VPN version	4.x

5.5 « NO PROPOSAL CHOSEN » error

115911 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [SA][VID] 115913 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [SA][VID] 115913 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [KEY][NONCE] 115915 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [KEY][NONCE] 115915 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY] 115915 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [ID][HASH][NOTIFY] 115915 Default phase 1 done: initiator id c364cd70: 195.100.205.112, responder id c364cd72: 195.100.205.114, src: 195.100.205.112 dst: 195.100.205.114 CNXVPN1-CNXVPN1-P2) 115915 Default (SA SEND phase 2 Ouick Mode [SA][KEY][ID][HASH][NONCE] 115915 Default RECV Informational [HASH][NOTIFY] with NO_PROPOSAL_CHOSEN error 115915 Default RECV Informational [HASH][DEL] 115915 Default CNXVPN1-P1 deleted

If you have an « NO PROPOSAL CHOSEN » error, check that the « Phase 2 » encryption algorithms are the same on each side of the VPN Tunnel.

Check « Phase 1 » algorithms if you have this:

115911 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [SA][VID] 115911 Default RECV Informational [NOTIFY] with NO_PROPOSAL_CHOSEN error

5.6 « INVALID ID INFORMATION » error

```
122623 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode[SA][VID]122625 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode[SA][VID]122625 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode[KEY][NONCE]
122626 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [KEY][NONCE]
122626 Default (SA CNXVPN1-P1) SEND phase 1 Main Mode [ID][HASH][NOTIFY]
122626 Default (SA CNXVPN1-P1) RECV phase 1 Main Mode [ID][HASH][NOTIFY]
122626 Default phase 1 done: initiator id c364cd70: 195.100.205.112, responder id
c364cd72: 195.100.205.114, src: 195.100.205.112 dst: 195.100.205.114
                                  CNXVPN1-CNXVPN1-P2)
122626
            Default
                          (SA
                                                                SEND
                                                                                             Ouick
                                                                                                        Mode
                                                                           phase
                                                                                      2
[SA][KEY][ID][HASH][NONCE]
122626 Default RECV Informational [HASH][NOTIFY] with INVALID_ID_INFORMATION error
122626 Default RECV Informational [HASH][DEL]
122626 Default CNXVPN1-P1 deleted
```

If you have an «INVALID ID INFORMATION » error, check if « Phase 2 » ID (local address and network address) is correct and match what is expected by the remote endpoint.

Check also ID type ("Subnet address" and "Single address"). If network mask is not check, you are using a IPV4_ADDR type (and not a IPV4_SUBNET type).

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

Read logs of each VPN tunnel endpoint. IKE requests can be dropped by firewalls. An IPSec Client uses UDP port 500 and protocol ESP (protocol 50).

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 Phase 2 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

Doc.Ref	tgbvpn_ug_ipcop_en
Doc.version	1.0 - Oct 2007
VPN version	4.x

- If you still cannot ping, follow ICMP traffic on VPN server LAN interface and on LAN computer interface (with Ethereal 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 ethereal (http://www.ethereal.com) on one of your target computer. You can check that your pings arrive inside the LAN.

THEG	SRE	ÉR	11.6311961

Doc.Ref	tgbvpn_ug_ipcop_en
Doc.version	1.0 - Oct 2007
VPN version	4.x

6 Contacts

News and updates on TheGreenBow web site: <u>http://www.thegreenbow.com</u> Technical support by email at <u>support@thegreenbow.com</u> Sales contacts by email at <u>sales@thegreenbow.com</u>