

# TheGreenBow IPSec VPN Client Configuration Guide

## **3COM X-FAMILY**

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

**IPSec VPN Router Configuration** 

TH	E	6	P	-	E		129	N	949519293	
				1						

Doc.Ref	tgbvpn_ug_3comX_en
Doc.version	1.0 – Jun.2007
VPN version	2.5.1.6827

### Table of contents

1	In	itroduction	. 3
	1.1	Goal of this document	. 3
	1.2	VPN Network topology	. 3
	1.3	3COM X-FAMILY Restrictions	. 3
	1.4	3COM X-FAMILY VPN Security Appliance	. 3
2	30	COM X-FAMILY VPN configuration	. 4
	2.1	Pre-Requisite Configuration	. 4
	2.2	Configuring IPSec with Pre-Shared Key (PSK)	. 7
	2.3	Configuring IPSec with X.509 Digital Certificate	10
3	T	heGreenBow IPSec VPN Client configuration	21
-	3.1	VPN Client Phase 1 (IKE) Configuration	21
	3.2	VPN Client Phase 2 (IPSec) Configuration	22
	3.3	Configure the VPN Client for connection to the 3Com Family Using PSK	23
	3.4	Configure the VPN Client for Connection to the X-family using Certificates	25
	3.5	Open IPSec VPN tunnels	28
4	Т	ools in case of trouble	30
	4.1	A good network analyser: ethereal	30
	4.2	Turn on Detailed Logging on the 3Com X-family	30
5	V	PN IPSec Traubleshaating	32
U	51	« PAYLOAD MALEORMED » error (wrong Phase 1 [SA])	32
	5.2	«INVALID COOKIF » error	32
	5.3	« no keystate » error	32
	5.4	« received remote ID other than expected » error	32
	5.5	« NO PROPOSAL CHOSEN » error	33
	5.6	« INVALID ID INFORMATION » error	33
	5.7	I clicked on "Open tunnel", but nothing happens	33
	5.8	The VPN tunnel is up but I can't ping I	33
6	С	ontacts	35

Doc.Ref	tgbvpn_ug_3comX_en
Doc.version	1.0 – Jun.2007
VPN version	2.5.1.6827

### 1 Introduction

### 1.1 Goal of this document

This configuration guide describes how to configure TheGreenBow IPSec VPN Client with a 3Com X-family Security Appliance such as an X5 or X506.

### 1.2 VPN Network topology

In our VPN network example (diagram hereafter), we will connect TheGreenBow IPSec VPN Client to the LAN behind the 3COM X-FAMILY Security Appliance. 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 3COM X-FAMILY Restrictions

None. Example main mode connections without Perfect Forward Secrecy (PFS) using Pre-shared Secret Key (PSK) or X.509 certificates are described in this document, but other options such as aggressive mode, NAT-T, PFS etc. are available if required.

### 1.4 3COM X-FAMILY VPN Security Appliance

Our tests and VPN configuration have been conducted with 3COM X-FAMILY firmware release version 2.5.1.6827.

The 3Com X-family of security appliances are firewall devices which incorporate routing, VPN, and the awardwinning TippingPoint Intrusion Protection System as well as many other security features.

THECOECOECOLI DAO 14 0 10 10 10 10 10 10 10 10 10 10 10 10 1	Doc.Ref	tgbvpn_ug_3comX_en
	Doc.version	1.0 – Jun.2007
	VPN version	2.5.1.6827

### 2 3COM X-FAMILY VPN configuration

This section describes how to build an IPSec VPN configuration suitable for terminating TheGrrenBow VPN Client on your 3COM X-FAMILY Security Appliance.

TheGreenBow can offer a choice of using a Pre-shared Secret Key (PSK) or a X.509 Digital Certificate to secure the IPSec VPN. Both are shown in the following examples.

### 2.1 Pre-Requisite Configuration

The following configuration steps are required before the X-family device can be configured to terminate IPSec connections from TheGreenBow. The instructions assume that the X-family device is at default settings.

#### Initial Setup via the OBE

Setup the user account and then set the basic configuration as follows. The dialogue shown is the OBE ("Out of Box Experience") on the Command Line Interface – this could also be set up using the OBE on the Graphical User Interface).

Your super-user account has been created.

```
You may continue initial configuration by logging into your device. After logging in, you will be asked for additional information.
```

```
Login: topuser
```

Password: t0p--us3r

Entering Setup wizard...

Enter Host Name [myhostname]: 3KB\_X\_unit\_1

Enter Host Location [room/rack]: Lab

Host Name: 3KB\_X\_unit\_1

Host Location: Lab

Enter [A]ccept, [C]hange, or [E]xit without saving [C]: **a** 

Timekeeping options allow you to set the time zone, enable or disable daylight saving time, and configure or disable NTP.

Would you like to modify timekeeping options? <Y,[N]>:

The X-Series device may be configured into a number of well known network deployments.

Would you like to modify the network deployment mode? <Y,[N]>:

Virtual interfaces define how this device integrates with the IP layer 3 network. You must configure one virtual interface for every IP subnet that is directly connected to the X-Series device. For example, you need one for the WAN connection (external virtual interface) and one for every directly connected network subnet (internal virtual interfaces).

Would you like to modify virtual interfaces? <Y,[N]>: $\mathbf{y}$ 

Virtual interfaces:

Id	Туре	Mode	IP Address	Subnet Mask	NAT
1	internal	static	192.168.1.254	255.255.255.0	external-ip
2	external	dhcp			disable

Т	HEGREERBOU	Doc.Ref Doc.version VPN version	tgbvpn_ug_3comX_en 1.0 – Jun.2007 2.5.1.6827
3	<empty></empty>		
4	<empty></empty>		
5	<empty></empty>		
б	<empty></empty>		
Ente	er [A]ccept, [C]hange, [R]emove or [E]xit with	out saving	[C]:
Ente	er the number of the entry you want to change	[]: <b>2</b>	
Mode	e (static, dhcp, pppoe, pptp, l2tp) [dhcp]: <b>st</b> a	atic	

Mask [255.255.255.0]:

IP address []: 10.10.10.146

Virtual interfaces:

Id	Туре	Mode	IP Address	Subnet Mask	NAT
1	internal	static	192.168.1.254	255.255.255.0	external-ip

- 2 external static 10.10.10.146 255.255.255.0 disable
- 3 <empty>
- 4 <empty>
- 5 <empty>
- 6 <empty>

Enter [A]ccept, [C]hange, [R]emove or [E]xit without saving [C]: **a** You must configure a default gateway manually if external virtual interface is static.

Would you like to modify default gateway? <Y,[N]>:y

Default Gateway [0.0.0.0]: 10.10.20.1

Security zones enable you to section your network logically into security domains. As network traffic travels between zones, it is routed and security-scanned by the firewall and IPS according to the policies you define. You need to create security zones that naturally map onto your intended network security boundaries. A security zone may or may not be connected (mapped) to a virtual interface.

Would you like to modify security zones? <Y,[N]>:

Would you like to modify security zone to virtual interface mapping? <Y,[N]>: DNS (Domain Name Service) is a system which translates computer hostnames to IP addresses. The X-Series device requires DNS configuration in order to perform web filtering.

Would you like to configure DNS? <Y,[N]>:

Firewall policy rules control the flow of network traffic between security zones. Firewall policy rules control traffic flow based on source and destination security zones and network protocol. Would you like to modify firewall policy rules? <Y,[N]>: SMS-based configuration allows the device to retrieve the configuration for a secure management VPN to the SMS system. This ensures that

TUECDEEDEGU DAOSIOSO	Doc.Ref	tgbvpn_ug_3comX_en
	Doc.version	1.0 – Jun.2007
	VPN version	2.5.1.6827

the device can be managed securely from the SMS
Would you like to enable SMS-based configuration? <Y,[N]>:
If you wish to run this wizard again, use the 'setup' command.
3KB\_X\_unit\_1#

Notes:

Virtual Interfaces - There are two virtual interfaces (external and internal) set up as factory default. The only configuration required on them is to set the IP addresses. (In the example, I have kept the internal IP address as default and changed the external IP address).

Security Zones – The factory default configuration sets the LAN security zone to be on Port 1 and linked to the internal Virtual Interface. The WAN security zone is on the last port (Port 4 on an X505 or port 6 on the X506 and X5) and is linked to the external virtual interface. No change is needed to this.

Firewall rules – the firewall rules in the factory default configuration will be sufficient – specifically this one:

2 permit WAN this-device vpn-protocols

### Load the Strong Encryption Package (Recommended)

For compliance with export regulations, the X-family devices are shipped from the factory with encryption types with keys below 64 bits (i.e. DES). This will work with TheGreenBow, but weak encryption is no longer considered suitable for the protection of commercial VPNs. To enable higher encryption key sizes to be used (e.g. 3DES, AES) a Strong Encryption package must be loaded onto the device. This package is only available to approved end users in approved locations.

- 1. Acquire the appropriate Strong Encryption package for your X-family device from the TMC and load it onto PC1.
- 2. Open a browser on PC1, connect to <a href="https://192.168.1.254">https://192.168.1.254</a> and login as the user you set up during the OBE.
- Navigate to System -> Update, open the TOS/DV Update tab and complete the form as shown below with the path of the Strong Encryption package on PC1. Click Install Package.

THECOECOECOE ON 101010101	Doc.Ref	tgbvpn_ug_3comX_en
	Doc.version	1.0 – Jun.2007
	VPN version	2.5.1.6827

🚾 ibm-762c500a371	
TOS & DV Update   LSM - Device (3KB_X_unit_1) - Microsoft Internet Explorer	- 문 ×
<u>Eile Edit Yiew Favorites Iools H</u> elp	100 A
🕁 Back 🔹 🤿 🖌 🗿 🚰 🦓 Search 📾 Favorites 🎯 Media 🧭 🔂 - 🎒 🗃	
Address 🗃 https://192.168.1.254/	💌 🔗 Go 🛛 Links 🌺 Norton AntiVirus 🛃 🕶
Current User: topuser   Auto Log Off in 60 minutes 2007-02-07 17:58:54 GMT	Scom
	30011
TOS & DV Update	1 TOS/DV Update Auto DV Config System Snapshots
IPS Court	
Firewall Step 1	
VPN Check for DV or TOS updates from the <u>Threat Management Center</u> and save an	y new versions to your PC.
Events Step 2	
System Make sure the package you downloaded is smaller than: 202 MB.	
Update Configuration	id, delete one or more of the <u>previously installed TOS images</u> .
Network	
Authentication Step 3	
Enable High Priority Preference (if desired)	
Step 4	
Select ".pkg" file and click install	
Backage File Circonal-biotEncryption X5 99901 pkg Browse	1
Polikage File	-
The installation of TOS updates will reboot the dev	vice.
	<b>T</b>
🙆 Done	🔒 🔮 Internet
😹 Start 🛛 🛃 🕭 🥮 📶 🖑 🛛 🎼 TOS & DY Update   L.S 🖾 C:\WINNT\system32\cmd 🔯 IBM_PRI	ELOAD (C:) 🛛 🤄 🔀 🖬 🗐 🛱 🥸 17:33

The package will be installed and the X-family device will reboot. The X-family device is ready to set up the VPN.

### 2.2 Configuring IPSec with Pre-Shared Key (PSK)

#### High-level steps ...

Configuring IPSec with PSK consists of:

- Configure a strong encryption IKE proposal on the X-family (recommended).
- Enable IPSec VPNs on the X-family.
- Configure the Default Security Association on the X-family.
- Configure firewall rules to allow IPSec to the X-family WAN interface.
- Download and Install "TheGreenBow" VPN Client onto PC2.
- Configure "TheGreenBow" VPN Client.

#### 3Com X-family Configuration

- 1) Login to your X-family web interface (LSM).
- 2) Create a strong encryption IKE Proposal on the X-family:
  - a) Navigate to VPN > IKE Proposals and click on **Create New Proposal**.
    - b) Complete the form as shown below and click **Create**. (This is an example using 3DES encryption, AES encryption could be used instead).

Doc.Ref	tgbvpn_ug_3comX_en
Doc.version	1.0 – Jun.2007
VPN version	2.5.1.6827

a	VPN >>	
e	Create IKE Propo	sal
IPS	IKE Phase 1 Setup	
Firewall	Proposal Name	strong
VPN	Encryption	3DE5-CBC
IPSec Status	Integrity	SHA-1 V
L2TP Status	Diffie-Hellman Group	2 (1024 bits) 🗸
PPTP Status	Lifetime	28800 seconds
Events	Authentication Type	Pre-Shared Key
System	Options	Enable Aggressive Mode
Network		
Authentication		
		Automatically connect phase 1 on system scart-up
		Delete Phase 2 SA when Phase 1 SA terminates
	IKE Phase 2 Setup	
	Encryption	ESP 3DES-CBC
	Integrity	ESP SHA-1-HMAC 💌
	Lifetime	3600 seconds
		Enable Perfect Forward Secrecy
	Diffie-Hellman Group	2 (1024 bits) 💌
		Enable strict ID checking of local network
		Use ID of 0.0.0.0/0 for local and remote networks
	Create <u>Cancel</u>	

- 3) Enable IPSec VPNs.
  - a) Click VPN > IPSec/IKE Status > IPSEC Configuration in the navigation menu.
  - b) Click **Enable IPSec Global VPNs**. Since the tunnel will be Main Mode there is no need to supply a Local Domain Name or Local Email Address. Click **Apply**.

	VPN >> IPSEC STATUS >>					00
IPS	IPSec Configurati	on				1 IPSec Cor
Firewall	IPSec Global Setup					
VPN	Enable Verbose mes	sages in the VPN Log				
IPSec Status IKE Proposals L2TP Status PPTP Status	Enable IPSec Global     Local Domain Name     Local Email Address	VPNs           5				
Events	Apply					
System	IP Security Associati	ons				
Network	25 💌 Records per page					
	Name	Keying Mode	IPSec Gateway	Local Network(s)	Remote Network(s)	Function(s)
Network Ports Security Zones	Default	IKE-PSK(DES-SHA1-PSK)		-		0
IP Interfaces IP Address Groups DN5 Default Gateway B Routing DHCP Server Tools	Create IPSec Association					
Authentication	1					

- 4) In the same dialog, configure the Default SA encryption parameters.
  - Note: The default SA is always present and cannot be deleted
  - a) Click the pencil icon next to the Security Association called "Default".
  - b) Click the **Enable Security Association** checkbox.

Doc.Ref	tgbvpn_ug_3comX_en
Doc.version	1.0 – Jun.2007
VPN version	2.5.1.6827

- c) Select the security zone to terminate IPSec connections onto this should be LAN in this example.
- d) The "Keying mode" should already be IKE.
- e) Select the IKE Proposal from the pull-down list. (Note: Only DES encryption will initially be available. It is recommended that a 3DES-SHA1-PSK IKE proposal is created and used for higher security. However, this requires that the X-family Strong Encryption package has been downloaded onto the unit, before a 3DES IKE proposal may be created.)
- f) Enter the shared secret to be used. Note the shared secret will be masked and it must be at least eight characters long. Make a note of the shared secret as it must match the shared secret used by the VPN Client.
- g) Ensure that the **Enable IPSec tunnel connections** checkbox is checked.
- h) Click Save. Note the screen may not update but the Save has occurred.

(«	IPSec Security Assoc	iation Setup		
IPS	Name	Default		
Firewall	Peer IP Address	0.0.0.0		
VPN	Terminated Security	LAN 💌		
IPSec Status	Zone Keying Mode	IKE		
IKE Proposals	keying lode			
PPTP Status				
Events		Support GRE and L21P (Transport Mode)		
System	IKE Setup			
Network	IKE Proposal	strong 💌		
Authentication	Shared Secret	****		
	Peer Email Address			
	Peer Domain Name			
	Peer Distinguished Name			
	Tunnel Setup			
	Enable IPSec tunnel con	nections		
	Local Networks			Remote Networks
	IP Address Group	HCP-Pool		O IP Address Group DHCP-Pool
	IP Subnet	Mask		IP Subnet     Mask
	O IP Range			IP Range /
	O Peer uses tunnel as def	ault route		O Use tunnel as default route
	<ul> <li>Local addresses assigned</li> </ul>	ed by DHCP through this tunnel		<ul> <li>Remote addresses assigned by DHCP through this tunnel</li> </ul>
	Enable NAT of local network	vork addresses		
	NAT IP Address		Hido & Jure	and Onlines A
			<u>riide Advan</u>	
	Save Cancel			

6) Check Firewall Policies.

If you are using multiple security zones, and/or have changed the terminating zone from LAN, and/or have change the policy rules for traffic allowed to the X-family from the WAN, you should perform this step.

### Note: Remember that the firewall rule table is ordered with traffic being matched top to bottom.

- a) Ensure that there is a policy rule allowing the IPSec tunnel traffic to the *WAN* security zone<sup>1</sup>.
- b) Ensure that there is a policy rule allowing this-device to send ANY protocol to ANY zone<sup>2</sup>.

The X-family is now configured.

<sup>&</sup>lt;sup>1</sup> The default Service Group vpn-protocols and default firewall rules will allow this. Protocols required are ike and nat-t-ipsec.

 $<sup>^{2}</sup>$  There is a "hidden" firewall rule that enables this, unless a "DENY" rule has been specified in the firewall table that overrules it.

THECOECODON Hotostotot	Doc.Ref	tgbvpn_ug_3comX_en
	Doc.version	1.0 – Jun.2007
	VPN version	2.5.1.6827

### 2.3 Configuring IPSec with X.509 Digital Certificate

X.509 Digital Certificates provide a stronger level of authentication and security than Pre-Shared Key (PSK) for IPSec connections. X.509 uses Public Key Infrastructure (PKI) encryption mechanisms to ensure full privacy without the need to exchange a private key.

To deploy a VPN client solution using X.509, two certificates are generated by a trusted Certificate Authority (CA) – one for the Windows VPN client, and one for the X-family device terminating the IPSec connection. The certificates uniquely identify each end point of the connection, ensuring that each end point can know with certainty that the partner is who they say they are. If not using a 3<sup>rd</sup> party Certificate Authority you can still generate certificates that are *self signed* through readily available tools.

### Recommended (High Security) Method

### High Level Steps

The recommended high level steps for using X.509 certificates with TheGreenBow IPSec VPN client are:

- Generate certificates for use on the X-family and the TheGreenBow VPN client machine.
  - o Generate the self-signed CA certificate.
  - Create a local certificate request on the X-family, copy it to the certificate machine and sign it with the CA certificate.
  - Create a local certificate request on the TheGreenBow PC, copy it to the certificate server and sign it with the CA certificate.
- On the X-family:
  - Install the signed CA and local certificates.
  - Associate the local certificate with the IKE proposal.
  - Associate the IKE proposal with the IPSec Default Security Association.
  - Ensure the Default Security Association is using tunnel mode.
- On TheGreenBow client PC:
  - Create the TheGreenBow IPSec client connection, selecting to use certificates for IPSec authentication.
  - o Install the signed CA and IPSec client local certificates.

### Creating and Loading the Certificates

Three certificates are required for this configuration:

• A CA certificate. This is created on the certificate server and installed on both the X-family and the TheGreenBow client PC.

The certificates used by TheGreenBow for IPSec *must* be signed or TheGreenBow will fail the IPSec main mode negotiation. When Windows XP negotiates the main mode IPSec tunnel with the X-family box, it exchanges the list of Certificate Authorities (CA's) it will accept certificates from. A CA certificate must be installed in Windows XP to authenticate the local L2TP client certificate. The X-family can use a similar scheme.

### • A Local certificate on the X-family.

The Local certificate request is created on the X-family, is signed by the shared CA and is used to authenticate the IPSec server within the X-family.

### • A Local certificate for the TheGreenBow VPN client.

The Personal certificate request created on the TheGreenBow PC is signed by the shared CA and is used to authenticate the TheGreenBow IPSec client.

THECDEEDEGI 1040140304	Doc.Ref	tgbvpn_ug_3comX_en
	Doc.version	1.0 – Jun.2007
	VPN version	2.5.1.6827

It is strongly advised that the Local Certificates are generated through a PKI setup (e.g. the Windows Certificate Server that ships in Windows 200x Server) ensuring that private keys are not exposed on the network. The signing process could be performed by a trusted CA server such as Verisign or Thawte. This is outside the scope of this document however.

Note that X-family does not currently support an automated certificate enrolment protocol.

#### Alternative Method Using Open-Source Tools

To demonstrate the techniques, this document will use the OpenSSL utility on a Linux platform to generate selfsigned certificates in PKS#12 format.

The following example creates the certificates using the CA wrapper normally available in the /etc/pki/tls/misc/CA directory, and openSSL. Once the CA certificate is created, the example signs a local certificate request created on the certificate server using the created CA certificate.

#### Create the Certificates on the Certificate Server.

The following dialogue generates a single root (CA) certificate plus two PKS#12 files for the X-family device and TheGreenBow client. Make sure that you make a note of the "PEM Pass Phrase" (I used "xfamily") and the PKS#12 export password(s) (I used "xfamily" again). You will need the PEM pass phrase several times during the certificate generation sequence and you will need the export password when you import the PKS#12 file onto the X-family and onto the TheGreenBow client. Note that the pass phrase and password must only use letters and numbers (i.e. no spaces or special characters) – otherwise there will be problems when importing the local certificate into the X-family device.

```
[test]:
[test]: openssl version
OpenSSL 0.9.7a Feb 19 2003
[test]:
[test]: # create the CA certificate #
[test]:
[test]: ./CA -newca
./CA -newca
CA certificate filename (or enter to create)
Making CA certificate ...
Generating a 1024 bit RSA private key
..++++++
....++++++
writing new private key to './demoCA/private/./cakey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
_ _ _ _ _
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
- - - - -
Country Name (2 letter code) [GB]:
State or Province Name (full name) [Berkshire]:England
Locality Name (eg, city) [Newbury]:London
Organization Name (eg, company) [My Company Ltd]:3Com
```

Doc.Ref	tgbvpn_ug_3comX_en
Doc.version	1.0 – Jun.2007
VPN version	2.5.1.6827

```
Organizational Unit Name (eg, section) []:3Com
Common Name (eg, your name or your server's hostname) []:MyCA
Email Address []:test@3Com.com
[test]:
[test]:
[test]: # create Local Certificate request for the X-family #
test1:
[test]: ./CA -newreq
Generating a 1024 bit RSA private key
...++++++
.+++++
writing new private key to 'newreq.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
Country Name (2 letter code) [GB]:
State or Province Name (full name) [Berkshire]:England
Locality Name (eg, city) [Newbury]:London
Organization Name (eg, company) [My Company Ltd]:3Com
Organizational Unit Name (eg, section) []:3Com
Common Name (eg, your name or your server's hostname) []:X505
Email Address []:test@3Com.com
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Request (and private key) is in newreq.pem
[test]:
[test]:
[test]: # Sign the X-family Local Certificate request #
[test]:
[test]:./CA -sign
Using configuration from /usr/share/ssl/openssl.cnf
Enter pass phrase for ./demoCA/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
       Serial Number: 1 (0x1)
       Validity
          Not Before: Apr 10 09:42:18 2006 GMT
          Not After : Apr 10 09:42:18 2007 GMT
       Subject:
                                 = GB
          countryName
```

THECOECOECOM	Doc.Ref	tgbvpn_ug_3comX_en
	Doc.version	1.0 – Jun.2007
	VPN version	2.5.1.6827

	stateOrProvinceName	= England
	localityName	= London
	organizationName	= 3Com
	organizationalUnitName	= 3Com
	commonName	= X505
X I	emailAddress	= test@3Com.com
Χ.:	509V3 extensions:	
	Netscape Comment:	
	OpenSSL Generated Certifi	cate
	X.509v3 Subject Kev Ident	ifier:
	02:4E:62:5E:C9:C4:D4:FD:6	9:5C:3C:14:2E:71:45:C9:52:99:AF:A0
	X.509v3 Authority Key Ide	ntifier:
keyid:BF:7	3:F9:05:25:14:B6:B7:CC:BE:1	3:52:6D:C7:08:1A:03:EA:4C:34
DirName:/C	-GR/ST-England/L-London/0-3	Com/OU-3Com/CN-MyCA/emailAddress-test@
3Com.com		
	serial:00	
Sign the co	e is to be certified until , ertificate? [y/n]:y	Apr 10 09:42:18 2007 GMT (365 days)
1 out of 1	contificato poquesto conti	fied commit? [u/n]u
Write out (	detabase with 1 new entries	iied, commit? [y/n]y
Data Base I	Indated	
Certificate	2:	
Data:		
Vei	rsion: 3 (0x2)	
Sei	rial Number: 1́ (Ox1)	
Sig	gnature Algorithm: md5WithR	SAEncryption
Is	suer: C=GB, ST=England, L=L	ondon, O=3Com, OU=3Com,
CN=MyCA/ema	ailAddress=test@3Com.com	
Val	lidity	
	Not Before: Apr 10 09:42:	18 2006 GMT
0.1	Not After : Apr 10 09:42:	18 2007 GMT
	bject: C=GB, SI=England, L= billddpoop=toot02Com com	London, U=300m, UU=300m,
	aiiAddress-testestom.com	
501	Public Key Algorithm: rsa	Encryption
	BSA Public Key: (1024 bit	
	Modulus (1024 bit):	)
	00:9f:39:a3:f1:03	:29:82:fd:95:9c:00:c5:16:14:
	c9:cd:fc:a0:ff:f2	:08:d3:ad:7d:bd:82:30:31:ec:
	43:46:37:b0:a7:49	:72:0c:a5:03:f3:f9:e2:68:44:
	31:a9:5a:54:7e:88	:68:b8:7a:38:d6:93:2a:ad:ed:
	d1:29:20:24:e6:58	:b0:34:02:d5:37:f2:87:2f:f6:
	be:cc:5b:58:29:d6	:4a:15:2d:c1:6a:32:45:68:23:
	dc:44:48:c8:59:22	:bf:58:4e:12:e7:88:8b:db:8c:
	96:38:38:d4:90:75	:67:5d:8c:96:04:13:2c:ed:56:
	7b:08:6f:60:97:0a	:00:05:29
V	Exponent: 65537 (UX10)	JUT)
Χ.:	DOBAD EXTENSIONS:	

THECOELOODU	Doc.Ref	tgbvpn_ug_3comX_en
	Doc.version	1.0 – Jun.2007
	VPN version	2.5.1.6827
X.509v3 Basic Constraints:		
CA:FALSE		
Netscape Comment:		
OpenSSL Generated Certificate		
X.509v3 Subiect Kev Identifier:		
02:4E:62:5E:C9:C4:D4:FD:69:5C:3C:14:2	E:71:45:C9:	52:99:AF:A0
X.509v3 Authority Key Identifier:		
keyid:BF:73:F9:05:25:14:B6:B7:CC:BE:13:52:6D:C7:08	B:1A:03:EA:	4C:34
DirName:/C=GB/ST=England/L=London/O=3Com/OU=3Com/	CN=MyCA/ema	ailAddress=test@
3Com.com		
serial:00		
Signature Algorithm: md5WithRSAEncryption		
31:f2:b4:98:10:ca:63:e4:50:b8:af:a0:f7:6e	:75:92:18:8	38:
ce:51:87:92:16:8f:d0:21:10:81:87:10:02:25	:e4:1a:24:f	<sup>-</sup> 0:
f7:c7:2c:3e:bf:af:86:7c:61:b7:50:6d:32:ec	:a7:aa:d8:5	50:
17:3c:3e:d4:30:5a:21:27:cf:bb:15:7f:a6:35	:33:66:1f:a	11:
c3:12:a3:d0:bc:57:d8:43:c6:8e:75:20:b7:99	:de:25:10:c	19:
69:31:84:63:85:30:15:04:08:45:20:0a:5a:cd	:da:18:57:a	14:
55:00:51:45:52:18:23:f9:53:3b:0f:1f:68:c5	:80:3e:f3:e	ef:
7a:12		
BEGIN CERTIFICATE		
MIIDpzCCAxCgAwIBAgIBATANBgkqhkiG9w0BAQQFADCBizELM	AkGA1UEBhMC	CROIX
EDAOBgNVBAgTBOVuZ2xhbmQxDzANBgNVBAcTBkxvbmRvbjENM/	AsGA1UEChME	MON∨
bTEVMBMGA1UECxMMVGlwcGluZ1BvaW50MQ0wCwYDVQQDEwRNet	JNBMSQwIgYJ	IKoZI
hvcNAQkBFhV0ZXN0QHRpcHBpbmdwb2ludC5jb20wHhcNMDYwN	DEwMDkOMjE4	WhcN
MDcwNDEwMDkOMjE4WjCBizELMAkGA1UEBhMCROIxEDAOBgNVB	AgTB0VuZ2xh	nbmQx
DzANBgNVBAcTBkxvbmRvbjENMAsGA1UEChMEMONvbTEVMBMGA	IUECxMMVGlw	vcGlu
Z1BvaW50MQ0wCwYDVQQDEwRYNTA1MSQwIgYJKoZIhvcNAQkBFI	hVOZXNOQHRp	осНВр
bmdwb21udC5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJA	GBAJ850/ED	OKYL9
1ZwAxRYUyc38oP/yCNOtfb2CMDHsQ0Y3sKdJcgy1A/P54mhEMa	alaVH6IaLh6	SONaT
Kq3t0SkgJ0ZYsDQC1Tfyhy/2vsxbWCnWShUtwWoyRWgj3ERIy	-kiv1h0Euel	19uM
1]g41JB1212M1gQ1L01WewhvYJcK1uUpAgMBAAG]ggEXM11BE	ZAJBGNVHRME	A]AA
MCwGCWCGSAGG+EIBDQQ+Fh1PcGVuU1NMIEdIbmVyYXRIZCBD2	(JOaWZpY2FC	021Ad
BgNVHQ4EFgQUAk51XsnE1P1pXDwULnFFyVKZr6AwgbgGA1Ud1	VSBSDCBrYAL	Jv3P5
BSUUTTTMVNNSbccIGgPqIDSngZGKgY4wgYsxCzAJBgNVBAYIA		
		BGNV
BASIDFRPCHBPDMQQD21udDENMASGATUEAXMETXIDQTEKMCIGG		
dGVZdEBUaXBwaw5ncG9pbnQuY29TggEAMA0GC5qG51b3DQEBB/		TJgu mcnV
ymPkULIVOPdudZIYIMSRN5IWJ9ANEIGHEAIISBOK8PIHLD6/N		Sport
	VKXIIGUFINIBUE	CEUg
END CERTIFICATE		
Signed Certificate is in newcert.pem		
[tost]. [tost]: ####################################	4 # # # # # # # # # #	
[test]: # Convert to PKCS#12 incomponeting CA and	10001 Cort	
[tost], # convert to PRCo#12 incorporating CA and	100ar Cerl	.1110ales #
[test]: ####################################	****	***
[[test], opened pleased overant in newcent rem in	akov nownos	nom contfile
ldomoCA/casest per out Vfemily s12	ikey newred	Phem - centitite
Enten neen nhneen for newner nerr		
Lincer pass philase for newred.pem:		

٦		E	G	F	E	É	D	B	M	681116

Doc.Ref	tgbvpn_ug_3comX_en
Doc.version	1.0 – Jun.2007
VPN version	2.5.1.6827

Enter Export Password: Verifying - Enter Export Password: [test]: [test]: [test]: # create the TheGreenBow Local certificate request # [test]: [test]: ./CA -newreq [test]: Generating a 1024 bit RSA private key .....++++++ .....++++++ writing new private key to 'newreq.pem' Enter PEM pass phrase: Verifying - Enter PEM pass phrase: You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank. - - - - -Country Name (2 letter code) [GB]: State or Province Name (full name) [Berkshire]:Scotland Locality Name (eg, city) [Newbury]:Edinburgh Organization Name (eg, company) [My Company Ltd]:3Com Organizational Unit Name (eg, section) []:3Com Common Name (eg, your name or your server's hostname) []:TheGreenBow Email Address []:user@3Com.com Please enter the following 'extra' attributes to be sent with your certificate request A challenge password []: An optional company name []: Request (and private key) is in newreq.pem [test]: [test]: [test]: # Sign the TheGreenBow Local Certificate request # [test]: [test]:./CA -sign Using configuration from /usr/share/ssl/openssl.cnf Enter pass phrase for ./demoCA/private/cakey.pem: Check that the request matches the signature Signature ok Certificate Details: Serial Number: 2 (0x2) Validity Not Before: Apr 10 09:56:41 2006 GMT Not After : Apr 10 09:56:41 2007 GMT Subject: countryName = GB stateOrProvinceName = Scotland

TLECDEEDE®U 040440404	Doc.Ref	tgbvpn_ug_3comX_en
	Doc.version	1.0 – Jun.2007
	VPN version	2.5.1.6827

1 ] . + N	– Estimburgh
localityName	
organizationName	= 300m
organizationalunitwame	
commonName	= L2IP Client
emailAddress	= user@3Com.com
X.509v3 extensions:	
X.509v3 Basic Constraints	
CA:FALSE	
Netscape Comment:	
OpenSSL Generated Certific	cate
X.509v3 Subject Key Ident:	Ltier:
C4:C1:ED:A8:8A:16:F9:6F:9	5:8F:5C:26:CC:DE:0E:9A:F0:81:95:D6
X.509v3 Authority Key Iden	itifier:
keyid:BF:73:F9:05:25:14:B6:B7:CC:BE:13	3:52:6D:C7:08:1A:03:EA:4C:34
DirName:/C=GB/ST=England/L=London/0=30	Com/OU=3Com/CN=MyCA/emailAddress=test@
3Com.com	
serial:00	
Certificate is to be certified until / Sign the certificate? [y/n]:y	Apr 10 09:56:41 2007 GMT (365 days)
1 out of 1 certificate requests certificate out database with 1 new entries Data Base Updated Certificate: Data:	fied, commit? [y/n]y
Version: $3 (0x2)$	
Serial Number: $2 (0x2)$	
Signature Algorithm: md5WithD9	3 A Encryption
Issuer: C=GB_ST=England L=L	$\Delta A = 3 C \circ m$ $O = 3 C \circ m$
CN=MyCA/emailAddress=test03Com com	
Validity	
Not Before: Apr 10 09:56:4	11 2006 GMT
Not After : Apr 10 09:56:4	11 2007 GMT
Subject: C=GB, ST=Scotland, L	=Edinburgh, 0=3Com, 0U=3Com, CN=L2TP
Client/emailAddress=user@3Com.com	
Subject Public Key Info:	
Public Kev Algorithm: rsal	Encryption
RSA Public Kev: (1024 bit	)
Modulus (1024 bit):	
00:b3:5e:65:5c:45	:0f:d6:f7:ad:51:09:5f:ab:d1:
bd:b5:28:0a:86:e0	:48:82:06:4d:4a:77:5d:db:10:
4c:e4:25:52:16:f2	:75:98:8f:b9:2d:88:60:cb:6e:
97:56:b2:3c:e4:af	:46:d6:d6:b1:1b:f6:4e:40:65:
fb:ab:92:7f:8a:9a	:48:1d:28:46:e7:81:ec:85:58:
8f:1d:70:36:bf:2f	:05:2d:a0:ef:7d:47:e4:9d:a7:
1f:a2:0e:76:5f:ce	:60:f0:76:ae:2c:16:f6:f1:a9:
73:df:99:be:35:8c	:e9:3a:10:87:e5:ae:a4:93:33:
93:5b:08:5a:76:f7	:db:a4:a1
Exponent: 65537 (0x100	001)
X.509v3 extensions:	
X.509v3 Basic Constraints	

THEGREEDBOU

Doc.Ref	tgbvpn_ug_3comX_en
Doc.version	1.0 – Jun.2007
VPN version	2.5.1.6827

CA: FALSE Netscape Comment: **OpenSSL Generated Certificate** X.509v3 Subject Key Identifier: C4:C1:ED:A8:8A:16:F9:6F:95:8F:5C:26:CC:DE:0E:9A:F0:81:95:D6 X.509v3 Authority Key Identifier: keyid:BF:73:F9:05:25:14:B6:B7:CC:BE:13:52:6D:C7:08:1A:03:EA:4C:34 DirName:/C=GB/ST=England/L=London/O=3Com/OU=3Com/CN=MyCA/emailAddress=test@ 3Com.com serial:00 Signature Algorithm: md5WithRSAEncryption 66:04:78:07:ee:fa:d7:b8:6c:1a:93:d1:4f:dc:b5:f0:3f:29: Od:1c:d5:d1:ee:3d:72:77:89:6c:a4:b0:30:ff:e3:2c:a5:a9: b6:35:82:21:05:50:8a:cb:05:6d:14:2c:12:03:e0:7a:1b:cf: 29:81:25:7b:99:bb:74:7e:88:e1:bf:1e:6a:6e:dc:4a:af:13: 32:79:bb:19:58:29:9a:f3:50:fc:10:f0:fa:aa:28:50:cf:5a: e3:e1:ce:5b:54:3f:f3:dc:17:01:c5:eb:df:28:ee:fb:ae:53: 41:78:c4:5d:9f:78:a9:37:64:57:37:37:4d:d6:d8:41:81:75: e4:aa ----BEGIN CERTIFICATE----MIIDsjCCAxugAwIBAgIBAjANBgkqhkiG9w0BAQQFADCBizELMAkGA1UEBhMCR0Ix EDAOBgNVBAgTB0VuZ2xhbmQxDzANBgNVBAcTBkxvbmRvbjENMAsGA1UEChMEMONv bTEVMBMGA1UECxMMVG1wcG1uZ1BvaW50MQ0wCwYDVQQDEwRNeUNBMSQwIgYJKoZI hvcNAQkBFhV0ZXN0QHRpcHBpbmdwb21udC5jb20wHhcNMDYwNDEwMDk1NjQxWhcN MDcwNDEwMDk1NjQxWjCB1jELMAkGA1UEBhMCR0IxETAPBgNVBAgTCFNjb3RsYW5k MRIwEAYDVQQHEw1FZG1uYnVyZ2gxDTALBgNVBAoTBDNDb20xFTATBgNVBAsTDFRp cHBpbmdQb21udDEUMBIGA1UEAxMLTDJUUCBDbG11bnQxJDAiBqkqhkiG9w0BCQEW FXVzZXJAdG1wcG1uZ3BvaW50LmNvbTCBnzANBgkghkiG9w0BAQEFAA0BjQAwgYkC gYEAs151XEUP1vetUQlfq9G9tSgKhuBIggZNSndd2xBM5CVSFvJ1mI+5LYhqv26X VrI85K9G1taxG/Z0QGX7q5J/ippIHShG54HshViPHXA2vy8FLaDvfUfknacfog52 X85g8HauLBb28a1z35m+NYzp0hCH5a6kkz0TWwhadvfbpKECAwEAAa0CARcwggET MAkGA1UdEwQCMAAwLAYJYIZIAYb4QgENBB8WHU9wZW5TU0wgR2VuZXJhdGVkIEN1 cnRpZmljYXR1MB0GA1UdDgQWBBTEwe2oihb5b5WPXCbM3g6a8IGV1jCBuAYDVR0j BIGwMIGtgBS/c/kFJRS2t8y+E1JtxwgaA+pMNKGBkaSBjjCBizELMAkGA1UEBhMC R0IxEDAOBgNVBAgTB0VuZ2xhbmQxDzANBgNVBAcTBkxvbmRvbjENMAsGA1UEChME MONvbTEVMBMGA1UECxMMVG1wcG1uZ1BvaW50MQ0wCwYDVQQDEwRNeUNBMSQwIgYJ KoZIhvcNAQkBFhV0ZXN0QHRpcHBpbmdwb21udC5jb22CAQAwDQYJKoZIhvcNAQEE BQADgYEAZgR4B+7617hsGpPRT9v18D8pDRzV0e49cneJbKSwMP/jLKWptjWCIQVQ issFbRQsEgPgehvPKYEle5m7dH6I4b8eam7cSq8TMnm7GVgpmvNQ/BDw+qooUM9a 4+HOW1Q/89wXAcXr3yju+65TQXjEXZ94qTdkVzc3TdbYQYF15Ko= ----END CERTIFICATE----Signed certificate is in newcert.pem [test]: [test]: [test]: # Convert to PKCS#12 incorporating CA and Local Certificates # [test]: [test]:openssl pkcs12 -export -in newcert.pem -inkey newreq.pem -certfile demoCA/cacert.pem -out thegreenbow.p12 Enter pass phrase for newreq.pem: Enter Export Password:

THECOECODON I Jaso 1 Jose 1 Jos	Doc.Ref	tgbvpn_ug_3comX_en
	Doc.version	1.0 – Jun.2007
	VPN version	2.5.1.6827

```
Verifying - Enter Export Password:
[test]:
[test]:ls *.p12
thegreenbow.p12 Xfamily.p12
[test]:
```

Load the certificates onto the X-family

- 1. Copy the cacert.pem CA certificate file and the X-family.p12 local certificate file to your X-family management PC.
- 2. Import the CA certificate onto the X-family

	AUTHENTICATION >> X.509 >>			CA Certificate	Certificate Requests
IPS	or cortinue				
Firewall	Import CA Certificate				
VPN	Select file containing CA certificate in "PK	.S#7" or "DER" format, enter a name for local i	reference, then click import.		
Events	Certificate Name CAcer	:1	_		
System	CA Certificate File	art.pem Browse	]		
Network	Import				
Authentication	Current CA Certificates				
User List	Certificate Name	Expires On	Status	Function(s)	
Privilege Groups RADIU5 X.509 Certificates Preferences					

Status of imported Certificate should be "Valid".

				CA Certificate	Certificate Requests	
IPS						
Firewall	Import CA Certificate					
VPN	Select file containing CA certificate in "PKCS#	17" or "DER" format, enter a name for local reference	e, then click import.			
Events	Certificate Name					
System	CA Certificate File	Browse				
Network	Import					
Authentication	Current CA Certificates					
User List	Certificate Name	Expires On	Status	Function(s)		
Privilege Groups RADIUS	CAcert1	Apr 23 23:11:56 2010 GMT	Valid			
X.509 Certificates Preferences						

3. Import the local certificate into the X-family. Use the certificate password that you noted when creating the certificate earlier.

IPS	AUTHENTICATION >> X.509 >> Local Certificates	5				CA Certificate	Certificate Requests	Local Cei
Firewall	Certificate Name	xfamily						
Events	Certificate Password	xfamily						
System	Local Certificate File	C:\xfamily.p12	Browse					
Network	Current Local Certif	icates						
User List Privilege Groups RADIU5 X.509 Certificates Preferences	Certificate Name	Certificate Authority	Distinguished Name	Serial Number	¥alid From	Expires On	Status	Function(

THECOECOECO	Doc.Ref	tgbvpn_ug_3comX_en
	Doc.version	1.0 – Jun.2007
	VPN version	2.5.1.6827

The certificate should appear in the Local Certificates tab and status should be "Valid".

IPS Firewall	Import Certificate						tincate Request	
VPN	Certificate Name							
Events	Certificate Password							
System	Local Certificate File		Browse					
Network		Import						
Authentication	Current Local Certi	ficates						
User List	Certificate Name	Certificate Authority	Distinguished Name	Serial Number	Valid From	Expires On	Status	Function(s
RADIUS X.509 Certificates Preferences	xfamily	C=GB, ST=Hertfordshire, L=Hemel, O=3Com, OU=3Com, CN=devtestCA	C=GB, ST=Hertfordshire, L=Hemel, O=3Com, OU=3Com, CN=xfamily	01	Jun 12 14:04:56 2007 GMT	Jun 11 14:04:56 2008 GMT	Valid	Ξ×

Configure the X-Family VPN to use the Certificate.

- 1) Configure the X-Family for Pre-Shared Key as shown in Section 2.2.
- 2) Edit the IKE proposal.
  - a) Navigate toVPN > IKE Proposals.
  - b) Click the pencil icon next to the new IKE Proposal that uses strong encryption.
  - c) Change the "Authentication Type" pulldown to "X.509 Certificate" and select the imported certificate name. (There will only be one certificate in the list.)

(«	) Edit IKE Proposa	
IPS	IKE Phase 1 Setup	
Firewall	Proposal Name	strong
VPN	Encryption	3DES-CBC
IPSec Status	Integrity	SHA-1 💌
L2TP Status	Diffie-Hellman Group	2 (1024 bits) 💌
PPTP Status	Lifetime	28800 seconds
Events	Authentication Type	X.509 Certificate 💌
System	Local Certificate	xfamily 🔽
Network		Only accept peer certificates signed by cacert
Authentication	Options	Enable Aggressive Mode
User List		Local ID Type Distinguished Name 💌
Privilege Groups RADIUS		Peer ID Type Distinguished Name
X.509 Certificates Preferences		Enable NAT Traversal
		Enable Dead Peer Detection
		Automatically connect phase 1 on system start-up
		Automatically connect phase 2
		Delete Phase 2 SA when Phase 1 SA terminates
	IKE Phase 2 Setup	
	Encryption	ESP 3DES-CBC
	Integrity	ESP SHA-1-HMAC 💌
	Lifetime	3600 seconds
		Enable Perfect Forward Secrecy
	Diffie-Hellman Group	2 (1024 bits) 🔻
		Enable strict ID checking of local network
		Use ID of 0.0.0.0/0 for local and remote networks
	Save <u>Cancel</u>	

#### Click Save.

The X-family VPN is now ready to use certificates.

THECOECOECOE CON 1040140104	Doc.Ref	tgbvpn_ug_3comX_en
	Doc.version	1.0 – Jun.2007
	VPN version	2.5.1.6827

THECOECOD CON 040140304	Doc.Ref	tgbvpn_ug_3comX_en
	Doc.version	1.0 – Jun.2007
	VPN version	2.5.1.6827

### 3 TheGreenBow IPSec VPN Client configuration

### 3.1 VPN Client Phase 1 (IKE) Configuration

📀 TheGreenBow VPN Client		
<u>File VPN Configuration T</u> ools	2	
THEGREENBOW	IPSer VPN Client	
<ul> <li>Console</li> <li>Parameters</li> <li>Connections</li> </ul>	Phase 1 (Authentication) Name CnxVpn1	The remote VPN Gateway IP address is either an explicit IP address, or a DNS
Configuration	Remote Gateway gateway.mydomain.com	- abcdefqh abcdefqh
	IKE Encryption DES  P1 Advanced Authentication SHA  Key Group DH768	
	Save & Apply	
VPN Tunnel active	Tunnel: 💟	

Phase 1 configuration

THECOECOECOE COLH 049419104	Doc.Ref	tgbvpn_ug_3comX_en
	Doc.version	1.0 – Jun.2007
	VPN version	2.5.1.6827

### 3.2 VPN Client Phase 2 (IPSec) Configuration

📀 TheGreenBow ¥PN Client		
<u>File VPN Configuration Iools</u>		You may define a static virtual IP address here.
🔎 Console	Phase 2 (IPSec Configuration)	If you use 0.0.0.0, you will have error "Local-ID" is missing. It does not prevent you from
Parameters	Name CnxVpn1	establishing a tunnel
S Connections	VPN Client address 1 . 0 . 0 . 1954	5
Configuration	Address type Single address  Remote host address  Subnet Mask  C . O . O . 1 ESP Encryption DES  Authentication MD5 Mode Tunnel	Enter the IP address (and subnet mask) of the remote LAN.
	PFS Group None Close Tunnel	
	Save & Apply	
VPN Tunnel active	Tunnel: O	

### Phase 2 Configuration

You may notice that we have selected SHA as authentication algorithm despite that fact MD5 algorithm is used for phase 2 in 3COM X-FAMILY advanced settings. The real authentication algorithm used is defined in main configuration page of the 3COM X-FAMILY router settings.

THECOECOE COL 040140104	Doc.Ref	tgbvpn_ug_3comX_en
	Doc.version	1.0 – Jun.2007
	VPN version	2.5.1.6827

### 3.3 Configure the VPN Client for connection to the 3Com Family Using PSK

- 1. Go to <u>http://www.thegreenbow.com</u> and download the VPN Client software. Note: The software is available for 30 day evaluation after which you must either buy it or cease using it.
- 2. Follow the instructions to install TheGreenBow on your Windows PC.
- 3. Start up TheGreenBow and click on **Configuration**. The instructions for setting up a connection are displayed as shown below.



4. Follow Step 1 and complete the form as shown below. The pre-shared key must match the Shared Secret entered on the X-family device earlier.



Click Save & Apply.

THECOECOECOE (1) 1040410304	Doc.Ref	tgbvpn_ug_3comX_en
	Doc.version	1.0 – Jun.2007
	VPN version	2.5.1.6827

5. Follow Step 2 and complete the form as shown below.

TheGreenBow VPN Clie	nt 📃 🗖 🔀
<u>File VPN Configuration View</u>	Tools ?
THEGREENBOW	
	IPSec VPN Client
💫 Console	Phase 2 (IPSec Configuration)
🎯 Parameters	Name CnxVpn2
😂 Connections	VPN Client address 10 . 10 . 20 . 200
Configuration tgbtest CnzVpn1 CnzVpn2	Address type Subnet address Remote LAN address  192 . 168 . 1 . 0 Subnet Mask  255 . 255 . 0
	ESP Encryption 3DES Authentication SHA Mode Tunnel
	F PFS Group None Open Tunnel
	Save & Apply
VPN ready	Tunnel: 🥑

Click Save & Apply.

TUECDEEDDGIII 040140104	Doc.Ref	tgbvpn_ug_3comX_en
	Doc.version	1.0 – Jun.2007
	VPN version	2.5.1.6827

### 3.4 Configure the VPN Client for Connection to the X-family using Certificates

- 1. Download and Install the TheGreenBow VPN Client.
  - a) Go to <u>http://www.thegreenbow.com</u> and download the VPN Client software. Note: The software is available for 30 day evaluation after which you must either buy it or cease using it.
  - b) Follow the instructions to install TheGreenBow on your Windows PC.
- 2. Copy the PKS#12 file to the TheGreenBow PC.
- 3. Start up TheGreenBow and click on Configuration. The instructions for setting up a connection are displayed as shown below.



4. Follow Step 1 and complete the form as shown below.



Doc.Ref	tgbvpn_ug_3comX_en
Doc.version	1.0 – Jun.2007
VPN version	2.5.1.6827

5. Click on **Certificates Import...** Complete the form as shown below.

Certificates Import 🛛 🗙
E
Root Certificate
User Certificate
User Private Key
Choose below the Certificate location and type:
Import Certificates from a PKCS12 file Import
Ok Cancel

6. Click **Import**, browse to the PKS#12 certificate file on the PC and click **Open**. Enter the password of the PKS#12 file and click **OK**.

PKCS12 file password	$\mathbf{X}$
	Ð
Please enter the file passwo	ord below:
OK	Cancel

7. The form should now display details of the imported certificate and the root certificate that was used to sign it, as shown below.

THECDEEDEMIlia 14 1010	Doc.Ref	tgbvpn_ug_3comX_en
	Doc.version	1.0 – Jun.2007
	VPN version	2.5.1.6827

ertificates Import 🛛 🗙			
63)			
Root Certificate /C=GB/ST=Hertfordshire/L=Hemel/0=3Com/0U=Secure Networ			
User Certificate     /C=GB/ST=Hertfordshire/L=Hemel/0=3Com/0U=3Com/CN=devt			
The Osei Linkate Key			
Choose below the Certificate location and type:			
Certificate from a PKCS#12 file			
Import Certificates from a PKCS12 file			
Ok Cancel			

8. Click OK, which will return you to here:

TheGreenBow VPN Cli	ent 🔲 🗖 🔀						
Eile VPN Configuration View	Tools ?						
	IPSec VPN client						
🚕 Console	Phase 1 (Authentication)						
🔯 Parameters	Name CnxVpn2						
😂 Connections	Interface 10.10.20.200						
Configuration	Remote Gateway       10.10.10.146         Preshared Key						
	<u>S</u> ave & Apply						
VPN ready	Tunnel: 🥑						

9. Click Save & Apply.
 10. Right click on the Phase 1 you just created (CnxVpn2 in my case) and select "Add Phase 2". Complete the form as shown below.

Doc.Ref	tgbvpn_ug_3comX_en
Doc.version	1.0 – Jun.2007
VPN version	2.5.1.6827

🔄 TheGreenBow VPN Client							
<u>File VPN Configuration View</u>	Tools ?						
THEGREENBOW							
	IPSEC VPN C	lient					
😣 Console	Phase 2 (IPSec Configuration)						
Parameters	Name CnxVpn3						
😂 Connections	VPN Client address 10 . 10 . 20 . 200						
Configuration	Address type Subnet address Remote LAN address 192 . 168 . 1 . 0 Subnet Mask 255 . 255 . 0 ESP Encryption 3DES Authentication SHA Mode Tunnel						
	C PFS Group None C Open Tunnel						
	Save & Apply						
VPN ready	Tunne	: Ø					

#### 11. Click Save & Apply.

### 3.5 Open IPSec VPN tunnels

Once both 3COM X-FAMILY router and TheGreenBow IPSec VPN Client have been configured accordingly, you are ready to open VPN tunnels

1. Click on "Save & Apply" to take into account all modifications we've made on your VPN Client configuration

2. Click on "**Open Tunnel**", or generate traffic that will automatically open a secure IPSec VPN Tunnel (e.g. ping, IE browser)

3. Select "Connections" to see opened VPN Tunnels

4. Select "**Console**" if you want to access to the IPSec VPN logs and adjust filters to display less IPSec messaging. The following example shows a successful connection between TheGreenBow IPSec VPN Client and a Microsoft Windows 2000 Server.

	- Incip						
No Time Source Destination Protocol Info							
1 0.000000 192.168.1.3 192.168.1.2 ISAKMP Identity Protection (Main Mode)							
2 0.153567 192.168.1.2 192.168.1.3 ISAKMP Identity Protection (Main Mode)							
3 0.205363 192.168.1.3 192.168.1.2 ISAKMP Identity Protection (Main Mode)							
4 0.257505 192.168.1.2 192.168.1.3 ISAKMP Identity Protection (Main Mode)							
5 0.300882 192.168.1.3 192.168.1.2 ISAKMP Identity Protection (Main Mode)							
6 0.310186 192.168.1.2 192.168.1.3 ISAKMP Identity Protection (Main Mode)							
7 0.313742 192.168.1.3 192.168.1.2 ISAKMP Quick Mode							
8 0.321913 192.168.1.2 192.168.1.3 ISAKMP Quick Mode							
9 0.323741 192.168.1.3 192.168.1.2 ISAKMP Quick Mode							
10 0.334980 192.168.1.2 192.168.1.3 ISAKMP Quick Mode							
11 0.691160 192.168.1.3 192.168.1.2 ESP ESP (SPI=0x919bfabc)							
12 1.692568 192.168.1.3 192.168.1.2 ESP ESP (SPI=0x919bfabc)							
13 1.693164 192.168.1.2 192.168.1.3 ESP ESP (SPI=0x53a5925e)							
14 2.693600 192.168.1.3 192.168.1.2 ESP ESP (SPI=0x919bfabc)							
15 2.694026 192.168.1.2 192.168.1.3 ESP ESP (SPI=0x53a5925e)							
Herame 1 (142 hytes on wire 142 hytes cantured)							
E sthernet II src. 00:50:04.ad/52:73 pst. 00:10:65:07:25.ff							

...and the X-family IPSec VPN > IPSec Status screen will look like this (PSK):

THECOECODOU 1040110101	Doc.Ref	tgbvpn_ug_3comX_en
	Doc.version	1.0 – Jun.2007
	VPN version	2.5.1.6827

PS IPSec Status PS IPSec Status PS IPSec Status PN PN PSec Status Per PAddress Local ID Per ID Proposal Default 0.0.0.0 10.10.10.146 0.0.0.0 30ES-CBC-SHA1-DH2 Phase 1 Default 0.10.20.200 192.168.1.0/24 10.10.20.200 ESP 30ES-CBC-SPA1 Phase 2 Vents Vents Vents Vents Configuration Network Ports Configuration Configuration Network Ports Configuration Co	IPSec Con
PS IPSec Status Details  IPSec Status PN  IPSec Status PP  Poposal  IPSec Status Per Page  IPSec Status Per Page  Peer IP Address Local ID  Peer ID  Proposal Status Default  0.0.0.0  10.10.10.146  0.0.0.0  3DES-CBC-SHA1-DH2 Phase 1  Default  10.10.20.200  192.168.1.0/24  10.10.20.200  ESP 3DES-CBC-ESP SHA-1 Phase 2	Function
irevall  PPN  IPSec Status IRE Proposals L27P Status Vents  Anne Peer IP Address Local ID Peer ID Proposal Status Default 0.0.0.0 10.10.10.146 0.0.0.0 3DES-CBC-SHA1-DH2 Phase 1 Default 0.10.20.200 192.168.1.0/24 10.10.20.200 ESP 3DES-CBC-ESP SHA1 Phase 2 Phase	Function(
IPSec Status       Name       Peer IP Address       Local ID       Peer ID       Proposal       Status         IXE Proposals L2TP Status       Default       0.0.0.0       10.10.10.146       0.0.0.0       3DES-CBC-SHA1-DH2       Phase 1         Default       10.10.20.200       192.168.1.0/24       10.10.20.200       ESP 3DES-CBC-SEP SHA-1 HMAC-No PFS       Phase 2         System       Configuration       Network Ports       Supervision       Supervision       Supervision         Network Ports       Configuration       Network Ports       Supervision       Supervision       Supervision	Function(
IPSec Status     Name     Peer IP Address     Local ID     Peer ID     Proposal     Status       IXE Proposals     L27P Status     Default     0.0.0.0     10.10.10.146     0.0.0.0     3DES-CBC-SHA1-DH2     Phase 1       L27P Status     PPTP Status     Default     10.10.20.200     192.168.1.0/24     10.10.20.200     ESP 3DES-CBC-SHA1-DH2     Phase 1       System     Pervork     Configuration     Network Ports     Network Ports     Network     Ne	Function(s
IKE Proposals         Default         0.0.0.0         10.10.10.146         0.0.0.0         3DE5-CBC-SHA1-DH2         Phase 1           L2TP Status         PPTP Status         Default         10.10.20.200         192.168.1.0/24         10.10.20.200         ESP 30E5-CBC-SFA1-DH2         Phase 1           Vertors         System         HMAC-No PF5         HMAC-No PF5         Phase 2           Vertork         Gonfiguration         Network Ports         Vertor         Vertor         Vertork	
PPTP Status     Default     10.10.20.200     192.166.1.0/24     10.10.20.200     ESP 30ES-CBC-ESP SHA-1     Phase 2       System     HMAC-No PFS     HMAC-No PFS     HMAC-No PFS     Phase 2       Vetwork     Configuration     Network Ports     Network     Network	Idle 💕
Events System System Configuration Network Ports	Established 💕
Bystem Setwork Ports	
Network Configuration Network Ports	
Configuration     Network Ports	
Terry has been	
Security Zones	
IP Interfaces	
IP Address Groups	
DNS	
Default Gateway	
B Routing	
DHCP Server	
Tools	
Authentication	

#### ... or this (X.509 Certificates)



Doc.Ref	tgbvpn_ug_3comX_en
Doc.version	1.0 – Jun.2007
VPN version	2.5.1.6827

### 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: 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 tools 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.

### 4.2 Turn on Detailed Logging on the 3Com X-family

- 1. Login to the management GUI and navigate to VPN > IPSec Status > IPSec Configuration tab.
- 2. Click the Enable Verbose messages in the VPN Log checkbox and click Apply.

	VPN >> IPSEC STATUS >> IPSec Configurati	on				1 IPSec Conf
IPS						
Firewall	IPSec Global Setup					
VPN	🗹 Enable Verbose mes	sages in the ¥PN Log				
IPSec Status IKE Proposals L2TP Status PPTP Status	Enable IPSec Global     Local Domain Name     Local Email Address	VPNs				
Events	Apply					
System	IP Security Association	ons				
Network	25 💌 Records per page					
Authentication	Name	Keying Mode	IPSec Gateway	Local Network(s)	Remote Network(s)	Function(s)
	<u>Default</u>	IKE-X.509(strong)		<b>5</b> 0	<b>N</b>	0
	Create IPSec Association					

- 3. Navigate to Events > Logs > VPN Log and click Reset to clear it.
- 4. Try to connect (either by clicking Connect Tunnel on the VPN Client or by pinging from the client to PC1 on the LAN side of the X-family).
- 5. View the VPN Log for debug information. The following is an example of some of the log entries from a single successful connection.

Doc.Ref	tgbvpn_ug_3comX_en
Doc.version	1.0 – Jun.2007
VPN version	2.5.1.6827

0	EVENTS >	> LOGS >>				
e	Y VPN		<u>sh</u> in 19 seconds			
IPS						
Firewall	VPN	Log Functions				
VPN	-	Download 🥿 Reset				
Events	VPN	Log Entries				
E Logs	50	Records per page				<<   <   1 - 39 of 39 entries  >
Alert Log Audit Log	Log ID	Log Entry Time	Severity Level	SourceIP:Port	DestIP:Port	Message
Firewall Block Log	10167	2007-06-13 12:29:16	INFO			Log Files Reset
Firewall Session Log	10168	3 2007-06-13 12:29:25	INFO	10.10.20.200:500	10.10.10.146:500	Main mode responder received message 1
VPN Log System Log	10169	2007-06-13 12:29:25	INFO	10.10.20.200:500	10.10.10.146:500	Rcvd Msg, 160 bytes: HDR[MM], [ 5A(52) VENDOR_ID(20) VENDOR_ID(20) VENDOR_ID(20) VENDOR_ID(20)] , cookies: CDA1C5F38308C8A8 / 00000000000000, msg id: 0
⊞ Managed Streams ⊞ Health	10170	0 2007-06-13 12:29:25	INFO	10.10.20.200:500	10.10.10.146:500	Proposal 1 protocol ISAKMP, 1 transforms
■ Reports	10171	2007-06-13 12:29:25	INFO	10.10.20.200:500	10.10.10.146:500	Transform 0 KEY_IKE:TRIPLEDES_CBC   SHA_HASH   RSA_SIGNATURE   DH_GROUP_2(MODP_1024)   SECONDS
System	10172	2 2007-06-13 12:29:25	INFO	10.10.20.200:500	10.10.10.146:500	Peer supports NAT-T: Draft 2
Network	10173	3 2007-06-13 12:29:25	INFO	10.10.20.200:500	10.10.10.146:500	Peer supports NAT-T: Draft 3
Authentication	10174	2007-06-13 12:29:25	INFO	10.10.20.200:500	10.10.10.146:500	Peer supports DPD
	10175	5 2007-06-13 12:29:25	INFO	10.10.20.200:500	10.10.10.146:500	Local phase 1 ID: IPV4_ADDR10.10.10.146
	10176	5 2007-06-13 12:29:25	INFO	10.10.20.200:500	10.10.10.146:500	Responder started IKE phase 1, main mode
	10177	2007-06-13 12:29:25	INFO	10.10.10.146:500	10.10.20.200:500	Outgoing msg, 120 bytes: HDR[MM], [SA(52) VENDOR_ID(20) VENDOR_ID(20)] , cookies: C0A1C5F3B308C6A8 / 011C749A65C6F013, msg id: 0
	10178	3 2007-06-13 12:29:25	INFO	10.10.10.146:500	10.10.20.200:500	Main mode responder sent message 1
	10179	2007-06-13 12:29:25	INFO	10.10.20.200:500	10.10.10.146:500	Main mode responder received message 2
	10180	2007-06-13 12:29:25	INFO	10.10.20.200:500	10.10.10.146:500	Rcvd Msg, 338 bytes: HDR[MM], [ KE(132) NONCE(20) CERT_REQ(110) NAT-D-PRIVATE(24) NAT-D-PRIVATE(24)] cookies: COA1CSF38308C8A8 / 011C749A65C6F013, msg id: 0
	10181	2007-06-13 12:29:25	INFO	10.10.10.146:500	10.10.20.200:500	Peer IP seen: 10.10.20,200, Local IP: 10.10.10.146
	10182	2007-06-13 12:29:25	INFO	10.10.10.146:500	10.10.20.200:500	Outgoing msg, 340 bytes: HDR[MM], [ KE(132) NONCE(20) CERT_REQ(110) NAT-D-PRIVATE(24) NAT-D-PRIVATE(  , cookies: CDA1C5F38308C8A8 / 011C749A65C6F013, msg id: 0
	10183	3 2007-06-13 12:29:25	INFO	10.10.10.146:500	10.10.20.200:500	Main mode responder sent message 2
	10184	2007-06-13 12:29:25	INFO	10.10.20.200:500	10.10.10.146:500	Main mode responder received message 3
	10185	5 2007-06-13 12:29:25	INFO	10.10.20.200:500	10.10.10.146:500	Rcvd Msg, 1108 bytes: HDR[MM], *[ ID(115) CERT(831) SIG(132)]] , cookies: COA1C5F3B308C8A8 / 011C749A65C6F013, msg id: 0

THECOEEDOGH BADATOLO	Doc.Ref	tgbvpn_ug_3comX_en
	Doc.version	1.0 – Jun.2007
	VPN version	2.5.1.6827

### 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 connection 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 (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.

Doc.Ref	tgbvpn_ug_3comX_en
Doc.version	1.0 – Jun.2007
VPN version	2.5.1.6827

### 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)
                                                                           phase
122626
            Default
                          (SA
                                                                SEND
                                                                                             Ouick
                                                                                                        Mode
                                                                                      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

THEGREEDBOU	Doc.Ref	tgbvpn_ug_3comX_en
	Doc.version	1.0 – Jun.2007
	VPN version	2.5.1.6827

- 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.

THE	5R	EÉ	n	1011116	H
		49			

Doc.Ref	tgbvpn_ug_3comX_en
Doc.version	1.0 – Jun.2007
VPN version	2.5.1.6827

### 6 Contacts

News and updates on TheGreenBow web site : <u>http://www.thegreenbow.com</u>

Technical support by email at <a href="mailto:support@thegreenbow.com">support@thegreenbow.com</a>

Sales contacts at +33 1 43 12 39 37 ou by email at info@thegreenbow.com

Product Information, User guides etc. for 3Com X-family on the 3Com website: http://www.3com.com

3Com Knowledgebase at: http://knowledgebase.3com.com