



 **TheGreenBow IPsec VPN Client**
Configuration Guide
3COM X-FAMILY

WebSite: <http://www.thegreenbow.com>

Contact: support@thegreenbow.com

Table of contents

1	Introduction	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	3COM 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	TheGreenBow 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	Tools 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	VPN IPSec Troubleshooting	32
5.1	« PAYLOAD MALFORMED » error (wrong Phase 1 [SA])	32
5.2	« INVALID COOKIE » 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 !.....	33
6	Contacts.....	35

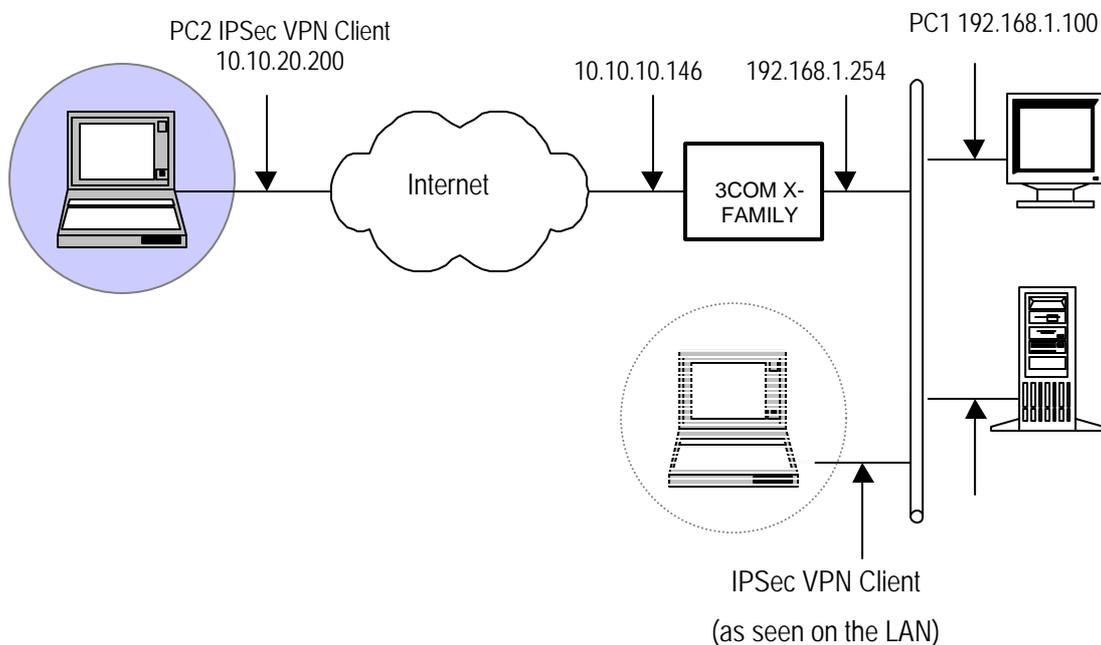
1 Introduction

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 award-winning TippingPoint Intrusion Protection System as well as many other security features.

2 3COM X-FAMILY VPN configuration

This section describes how to build an IPSec VPN configuration suitable for terminating TheGreenBow 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]>:**y**

Virtual interfaces:

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

```

3 <empty>
4 <empty>
5 <empty>
6 <empty>

```

Enter [A]ccept, [C]hange, [R]emove or [E]xit without saving [C]:

Enter the number of the entry you want to change []: **2**

Mode (static, dhcp, pppoe, pptp, l2tp) [dhcp]: **static**

IP address []: **10.10.10.146**

Mask [255.255.255.0]:

Virtual interfaces:

Id	Type	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

	Doc.Ref	tgvpn_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.

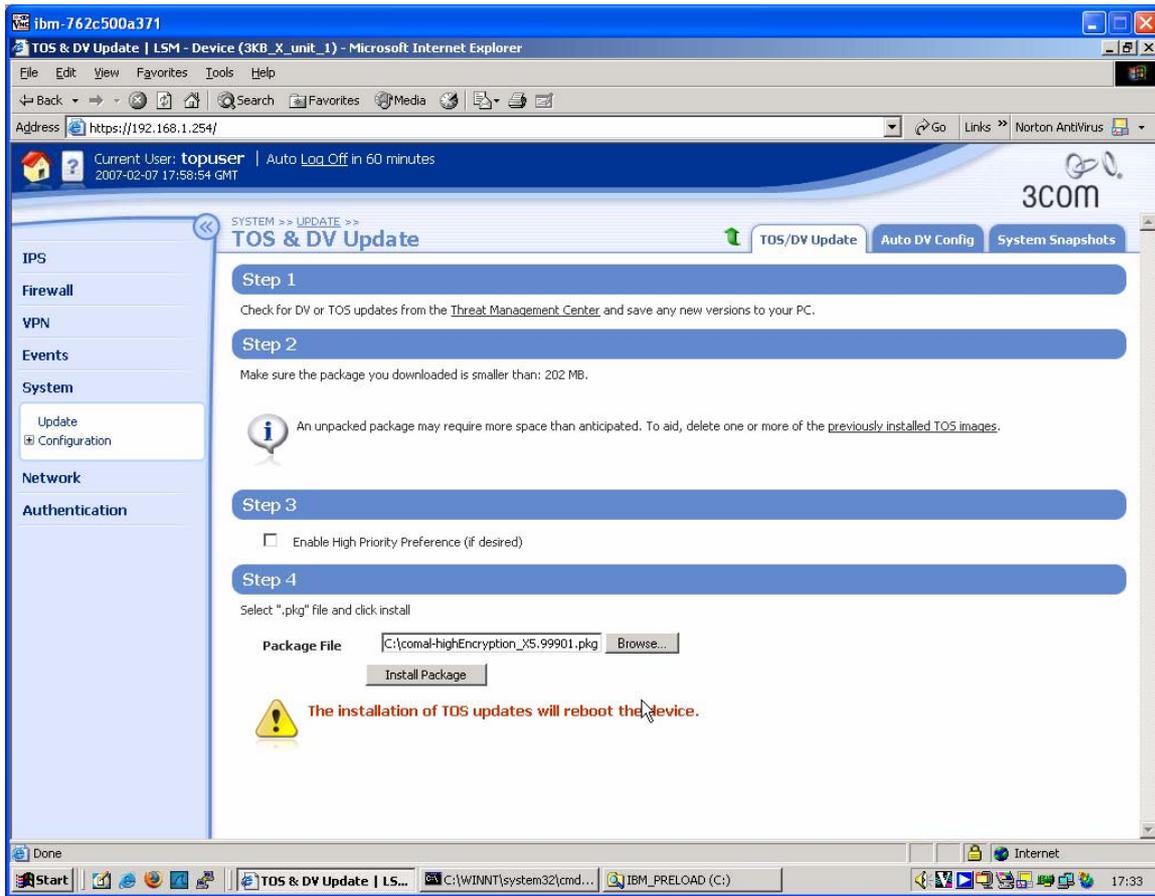
Firewall rules – the firewall rules in the factory default configuration will be sufficient – specifically this one:

```
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 <https://192.168.1.254> and login as the user you set up during the OBE.
3. 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**.



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).

VPN >> Create IKE Proposal

IKE Phase 1 Setup

Proposal Name:

Encryption:

Integrity:

Diffie-Hellman Group:

Lifetime: seconds

Authentication Type:

Options:

- Enable Aggressive Mode
- 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:

Integrity:

Lifetime: seconds

Diffie-Hellman Group:

Options:

- Enable Perfect Forward Secrecy
- Enable strict ID checking of local network
- Use ID of 0.0.0.0/0 for local and remote networks

- 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 >> IPsec Configuration

IPsec Global Setup

Enable Verbose messages in the VPN Log

Enable IPsec Global VPNs

Local Domain Name:

Local Email Address:

IP Security Associations

25 Records per page

Name	Keying Mode	IPsec Gateway	Local Network(s)	Remote Network(s)	Function(s)
Default	IKE-PSK(DES-SHA1-PSK)				

- 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.

- 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.

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 zone¹.
- b) Ensure that there is a policy rule allowing this-device to send ANY protocol to ANY zone².

The X-family is now configured.

¹ The default Service Group vpn-protocols and default firewall rules will allow this. Protocols required are ike and nat-t-ipsec.

² There is a “hidden” firewall rule that enables this, unless a “DENY” rule has been specified in the firewall table that overrules it.

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 3rd 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.
 - 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.
 - 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.

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 self-signed 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]: #####
[test]: # create the CA certificate #
[test]: #####
[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
```

```

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]: #####
[test]: # create Local Certificate request for the X-family #
[test]: #####
test]:
[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]: #####
[test]: # Sign the X-family Local Certificate request #
[test]: #####
[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:
        countryName = GB

```

```

stateOrProvinceName      = England
localityName             = London
organizationName         = 3Com
organizationalUnitName   = 3Com
commonName               = X505
emailAddress             = test@3Com.com
X.509v3 extensions:
X.509v3 Basic Constraints:
CA:FALSE
Netscape Comment:
OpenSSL Generated Certificate
X.509v3 Subject Key Identifier:
02:4E:62:5E:C9:C4:D4:FD:69:5C:3C:14:2E: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:C7:08:1A:03:EA:4C:34

DirName:/C=GB/ST=England/L=London/O=3Com/OU=3Com/CN=MyCA/emailAddress=test@
3Com.com

serial:00

Certificate is to be certified until Apr 10 09:42:18 2007 GMT (365 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 1 (0x1)
Signature Algorithm: md5WithRSAEncryption
Issuer: C=GB, ST=England, L=London, O=3Com, OU=3Com,
CN=MyCA/emailAddress=test@3Com.com
Validity
Not Before: Apr 10 09:42:18 2006 GMT
Not After : Apr 10 09:42:18 2007 GMT
Subject: C=GB, ST=England, L=London, O=3Com, OU=3Com,
CN=X505/emailAddress=test@3Com.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA 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:d6:e5:29
Exponent: 65537 (0x10001)
X.509v3 extensions:

```

```
X.509v3 Basic Constraints:
CA:FALSE
Netscape Comment:
OpenSSL Generated Certificate
X.509v3 Subject Key Identifier:
02:4E:62:5E:C9:C4:D4:FD:69:5C:3C:14:2E: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:C7:08:1A: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

```
31:f2:b4:98:10:ca:63:e4:50:b8:af:a0:f7:6e:75:92:18:88:
ce:51:87:92:16:8f:d0:21:10:81:87:10:02:25:e4:1a:24:f0:
f7:c7:2c:3e:bf:af:86:7c:61:b7:50:6d:32:ec:a7:aa:d8:50:
17:3c:3e:d4:30:5a:21:27:cf:bb:15:7f:a6:35:33:66:1f:a1:
c3:12:a3:d0:bc:57:d8:43:c6:8e:75:20:b7:99:de:25:10:d9:
69:31:84:63:85:30:15:04:08:45:20:0a:5a:cd:da:18:57:a4:
55:00:51:45:52:18:23:f9:53:3b:0f:1f:68:c5:80:3e:f3:ef:
7a:12
```

-----BEGIN CERTIFICATE-----

```
MIIDpzCCAxCGAwIBAgIBATANBgkqhkiG9w0BAQQFADCBIzELMAkGA1UEBhMCROIx
EDA0BgNVBAGTB0VuZ2xhbmQxZDZANBgNVBAcTBkxvbmRvbjENMAsGA1UEChMEMONv
bTEVMBMGA1UECxMMVG1wcGluZ1BvaW50MQ0wCwYDVQQDEwRNeUNBMSQwIgwYJKoZI
hvcNAQkBFhVOZXNOQHRpcHBpbmdwb2ludC5jb20wHhcNMDYwNDEwMDk0MjE4WWhcN
MDcwNDEwMDk0MjE4WjCBizELMAkGA1UEBhMCROIxEDA0BgNVBAGTB0VuZ2xhbmQx
ZDZANBgNVBAcTBkxvbmRvbjENMAsGA1UEChMEMONvbTEVMBMGA1UECxMMVG1wcGlu
Z1BvaW50MQ0wCwYDVQQDEwRYNTA1MSQwIgwYJKoZIhvcNAQkBFhVOZXNOQHRpcHBp
bmdwb2ludC5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgYOAMIGJAoGBAJ85o/EDKYL9
lZwAxRYUyc38oP/yCN0tfb2CMDHsQ0Y3sKdJcgylA/P54mhEMalaVH6IaLh60NaT
Kq3t0SkGJOZYsDQC1Tfyhy/2vsxbWCnWShUtwWoyRWgj3ERiyFkiv1hOEueIi9uM
lJg41JB1Z12MlgQTL01WewhvYJcK1uUpAgMBAAGjggEXMIIBEzAJBgNVHRMEAjAA
MCwGCWCGSAGG+EIBDQqFh1PcGVuU1NMIEdlbmVvYXRlZCZlZCZlZCZlZCZlZCZlZCZl
BgNVHQ4EFgQUAk5iXsnE1P1pXDwULnFFyVKZr6AwgbgGA1UdIwSBsDCBrYAUv3P5
BSUUtRfMvhNSbccIGgPqTDSHgZGkgY4wgYsxCzAJBgNVBAYTAkdCMRAwDgYDVQQI
EwdFbmdsYW5kMQ8wDQYDVQQHEwZMb25kb24xDTALBgNVBAoTBBDNDb20xFTATBgNV
BAsTDFRpcHBpbmdQb2ludDENMAsGA1UEAxMETXlDQTEKMCIGCSqGSIb3DQEJARYV
dGVzdEB0aXBwaW5ncG9pbmQuY29tggeAMA0GCSqGSIb3DQEBAUAA4GBADHyTJgQ
ymPkULivoPduZiYiM5Rh5IWj9AhEIGHEAI15Bok8PfHLD6/r4Z8YbdQbTLsp6rY
UBc8PtQwWiEnz7sVf6Y1M2YfocMS09C8V9hDxo51ILeZ3iUQ2WkxhGOFMBUECEUg
ClrN2hhXpFUUUUVSGCP5UzsPH2jFgD7z73oS
```

-----END CERTIFICATE-----

Signed certificate is in newcert.pem

```
[test]:
[test]:
[test]: #####
[test]: # Convert to PKCS#12 incorporating CA and Local Certificates #
[test]: #####
[test]:
[test]: openssl pkcs12 -export -in newcert.pem -inkey newreq.pem -certfile
demoCA/cacert.pem -out Xfamily.p12
Enter pass phrase for newreq.pem:
```

```

Enter Export Password:
Verifying - Enter Export Password:
[test]:
[test]:
[test]: #####
[test]: # create the TheGreenBow Local certificate request #
[test]: #####
[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]: #####
[test]: # Sign the TheGreenBow Local Certificate request #
[test]: #####
[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

```

```

localityName           = Edinburgh
organizationName       = 3Com
organizationalUnitName = 3Com
commonName              = L2TP Client
emailAddress            = user@3Com.com
X.509v3 extensions:
X.509v3 Basic Constraints:
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

Certificate is to be certified until Apr 10 09:56:41 2007 GMT (365 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 2 (0x2)
Signature Algorithm: md5WithRSAEncryption
Issuer: C=GB, ST=England, L=London, O=3Com, OU=3Com,
CN=MyCA/emailAddress=test@3Com.com
Validity
Not Before: Apr 10 09:56:41 2006 GMT
Not After : Apr 10 09:56:41 2007 GMT
Subject: C=GB, ST=Scotland, L=Edinburgh, O=3Com, OU=3Com, CN=L2TP
Client/emailAddress=user@3Com.com
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public Key: (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 (0x10001)
X.509v3 extensions:
X.509v3 Basic Constraints:

```

```
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:
0d: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-----
```

```
MIIDsjCCAxugAwIBAgIBAgjANBgkqhkiG9w0BAQQFADCBizELMAkGA1UEBhMCROIx
EDA0BgNVBAGTB0VuZ2xhbmQxZDZANBgNVBAcTBkxvbmRvb21udC5jb20wHhcNMDYw
NDEwMDk1NjQxWjCB1jELMAkGA1UEBhMCROIxETAPBgNVBAGTCFNjb3RsYW5k
MRIwEAYDVQQHEw1FZGluYnVyZ2gxDTALBgNVBAoTBDBDb20xFTATBgNVBAsTDFRr
cHBpmdQb21udDEUMBIGA1UEAxMLTDJUUUCBDBG11bnQxJDAiBgkqhkiG9w0BQCQEW
FXVzZXJAdGluZ3BvaW50LmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwYkCg
gYEA515XEUP1vetUQlfq9G9tSgKhuBIggZNSndd2xBM5CVSFvJ1mI+5LYhgy26X
VrI85K9G1taxG/ZOQGx7q5J/ippIHSg54HshViPHXA2vy8FLaDvfUfknacfog52
X85g8HauLBb28alz35m+NYzp0hCH5a6kkz0TWwhadvfbpKECAwEAAaOCARcwggET
MAkGA1UdEwQCMAAwLAYJYIZIAyb4QgENBB8WHU9wZW5TU0wgR2VuZXJhdGVkIENl
cnRpZmljYXR1MB0GA1UdDgQWBBTEwe2oihb5b5WPXCbM3g6a8IGV1jCBuAYDVROj
BIGwMIgtgBS/c/kFJRS2t8y+E1JtxwgaA+pMNKGBkaSBjjCBizELMAkGA1UEBhMC
ROIxEDA0BgNVBAGTB0VuZ2xhbmQxZDZANBgNVBAcTBkxvbmRvb21udC5jb22CAQAw
DQYJKoZIhvcNAQEEBQADgYEAZgR4B+7617hsGpPRT9y18D8pDRzV0e49cneJbKSwMP/j
LKWptjWCiQVQissFbRQsEgPgehVPKYEle5m7dH6I4b8eam7cSq8TMnm7GVgpmvNQ/B
Dw+qooUM9a4+HOW1Q/89wXAcXr3yju+65TQXjEXZ94qTdkVzc3TdbYQYF15Ko=
```

```
-----END CERTIFICATE-----
```

```
Signed certificate is in newcert.pem
```

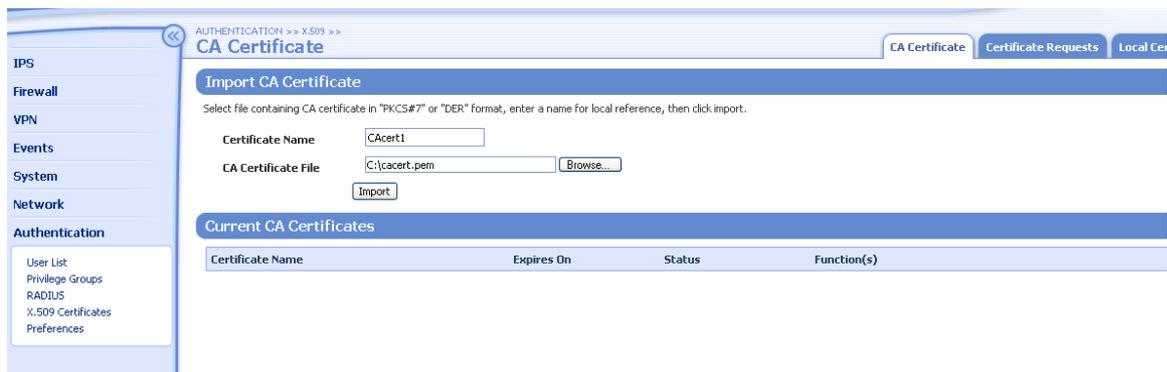
```
[test]:
[test]:
[test]: #####
[test]: # Convert to PKCS#12 incorporating CA and Local Certificates #
[test]: #####
[test]:
[test]:openssl pkcs12 -export -in newcert.pem -inkey newreq.pem -certfile
demoCA/cacert.pem -out thegreenbow.p12
Enter pass phrase for newreq.pem:
Enter Export Password:
```

```

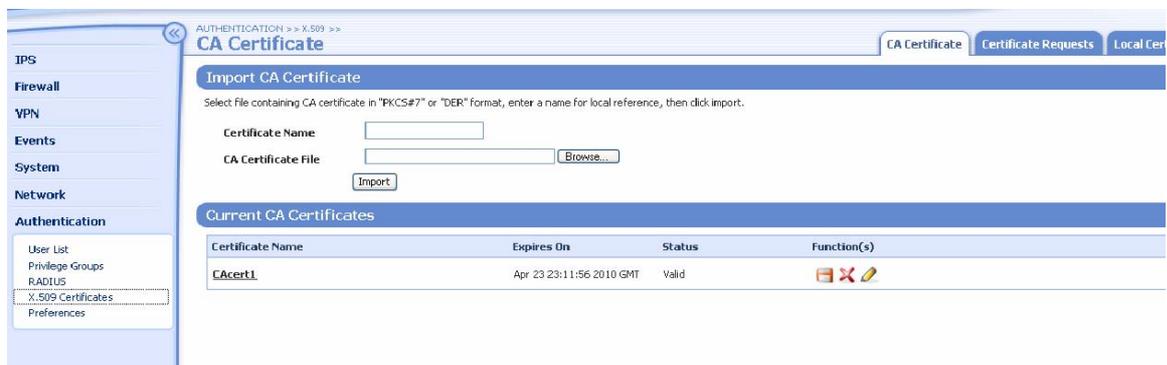
Verifying - Enter Export Password:
[test]:
[test]:ls *.p12
thegreenbow.p12  Xfamily.p12
[test]:
    
```

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



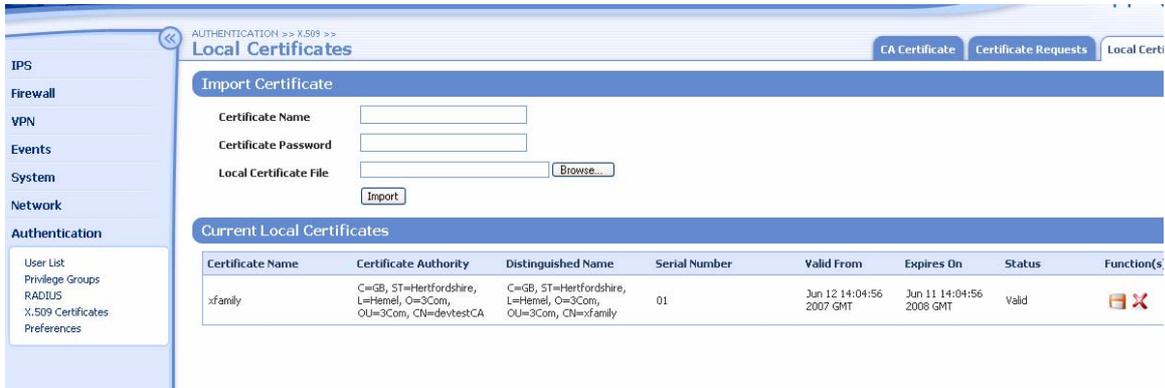
Status of imported Certificate should be “Valid”.



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

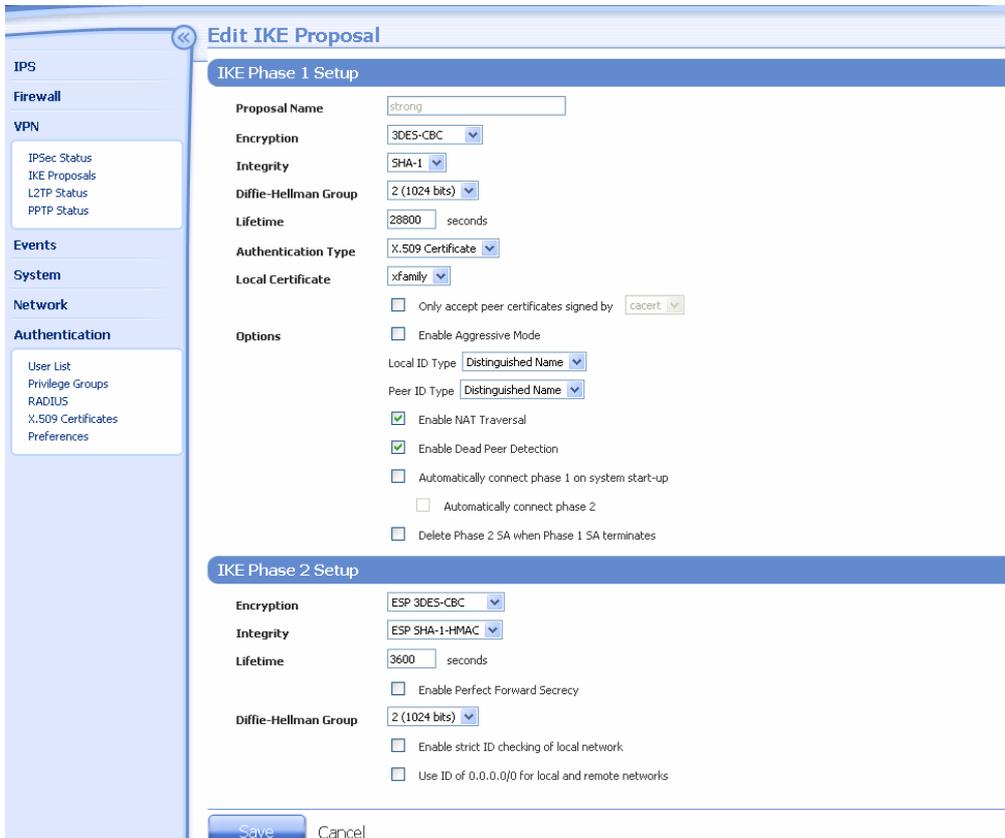


The certificate should appear in the Local Certificates tab and status should be “Valid”.



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 to VPN > 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.)



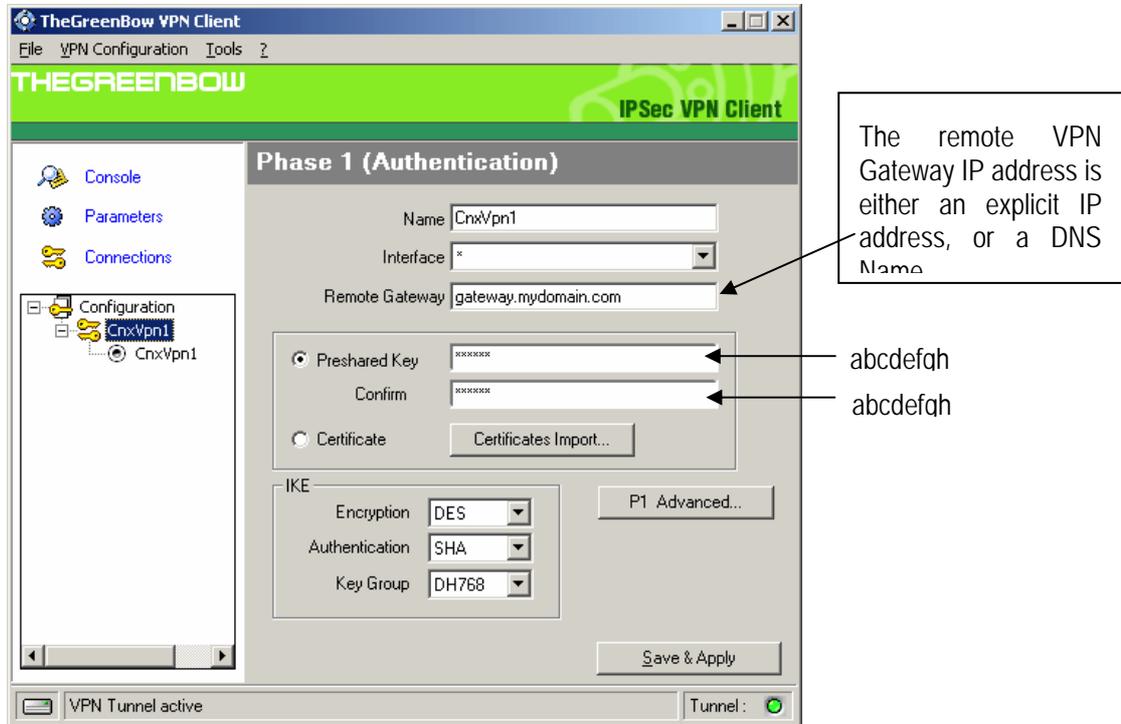
Click **Save**.

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

Doc.Ref	tgvpn_ug_3comX_en
Doc.version	1.0 – Jun.2007
VPN version	2.5.1.6827

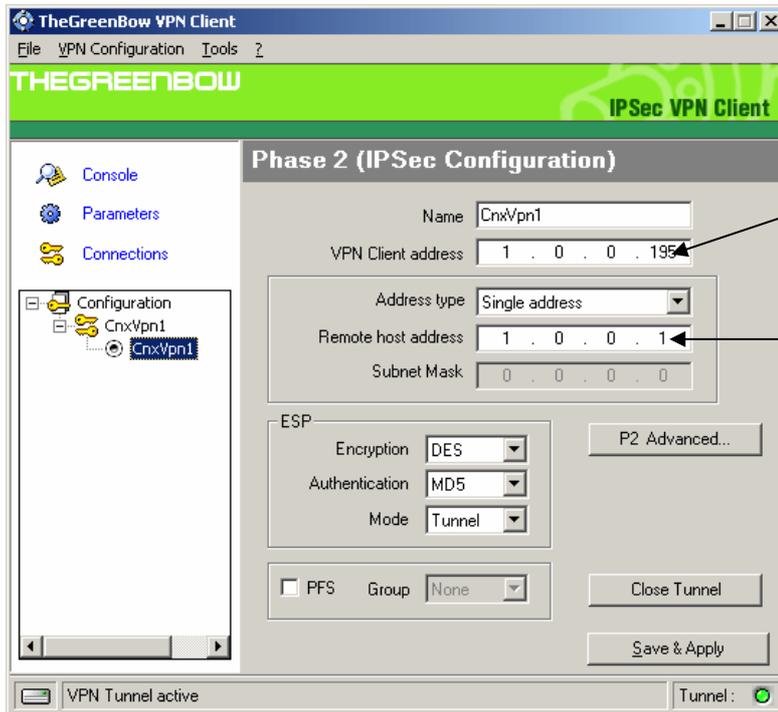
3 TheGreenBow IPsec VPN Client configuration

3.1 VPN Client Phase 1 (IKE) Configuration



Phase 1 configuration

3.2 VPN Client Phase 2 (IPSec) Configuration



You may define a static virtual IP address here.
If you use 0.0.0.0, you will have error "Local-ID" is missing. It does not prevent you from establishing a tunnel

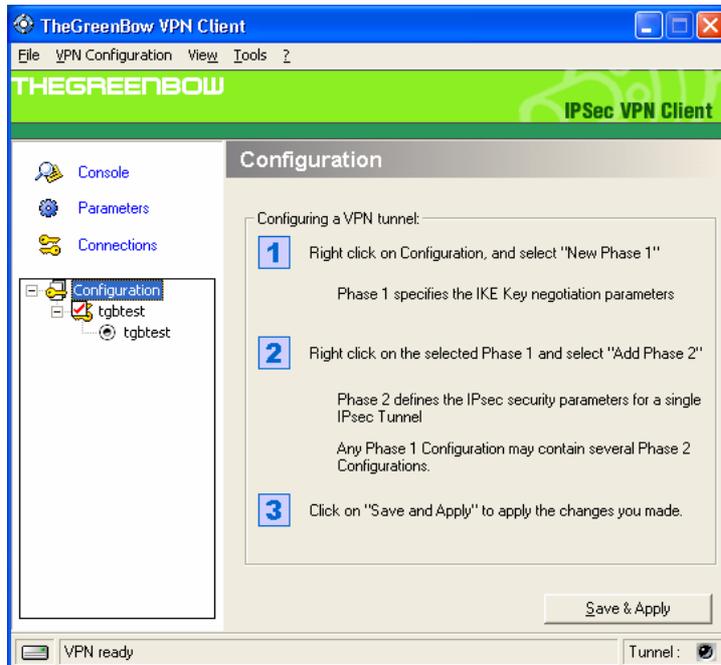
Enter the IP address (and subnet mask) of the remote LAN.

Phase 2 Configuration

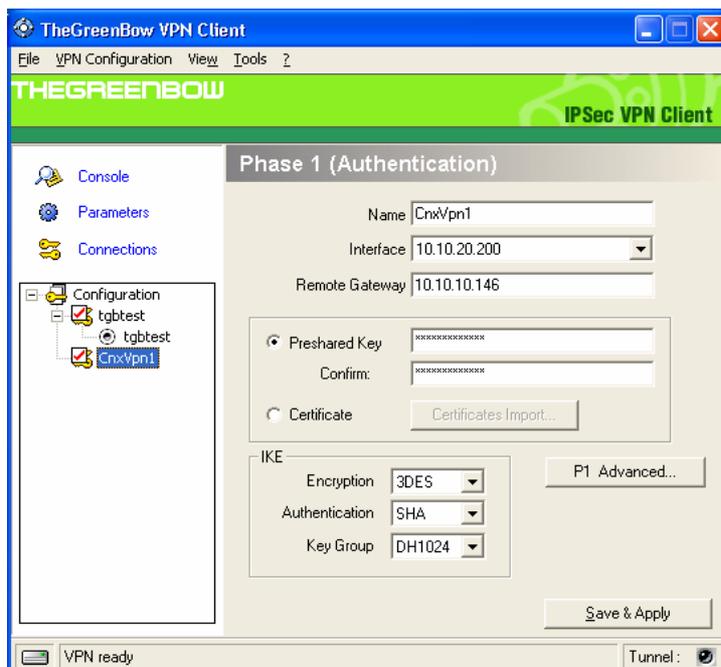
You may notice that we have selected SHA as authentication algorithm despite that fact MD5 algorithm is used for phase 2 in 3COM X-FAMILY advanced settings. The real authentication algorithm used is defined in main configuration page of the 3COM X-FAMILY router settings.

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

1. Go to <http://www.thegreenbow.com> 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.

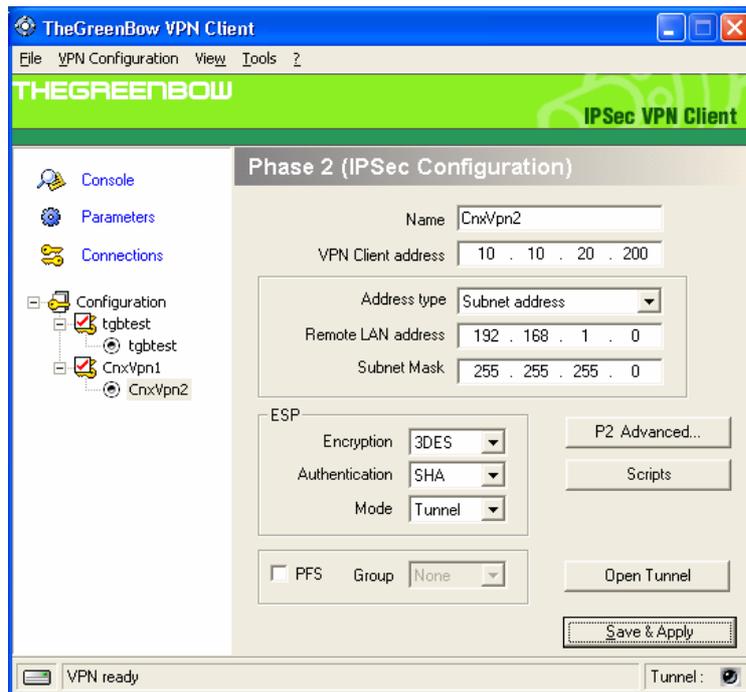


4. Follow Step 1 and complete the form as shown below. The pre-shared key must match the Shared Secret entered on the X-family device earlier.



Click **Save & Apply**.

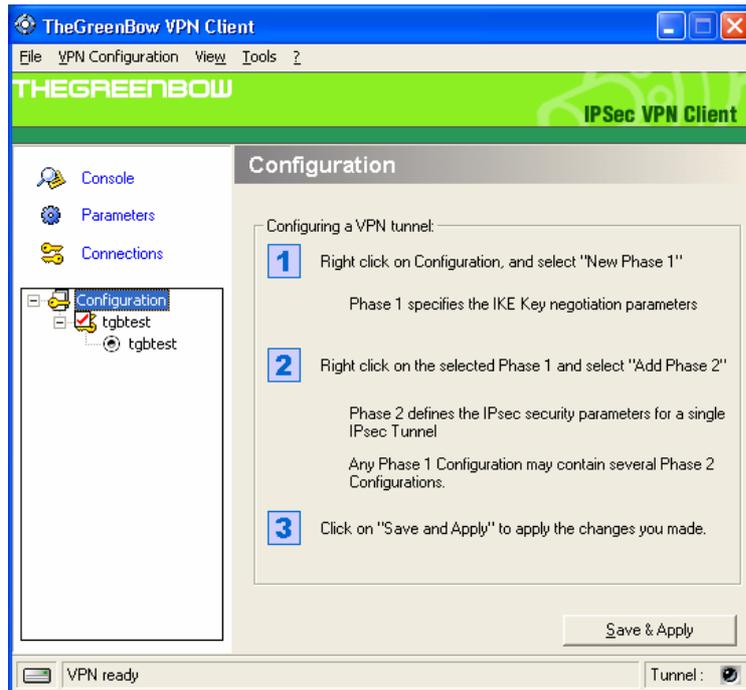
5. Follow Step 2 and complete the form as shown below.



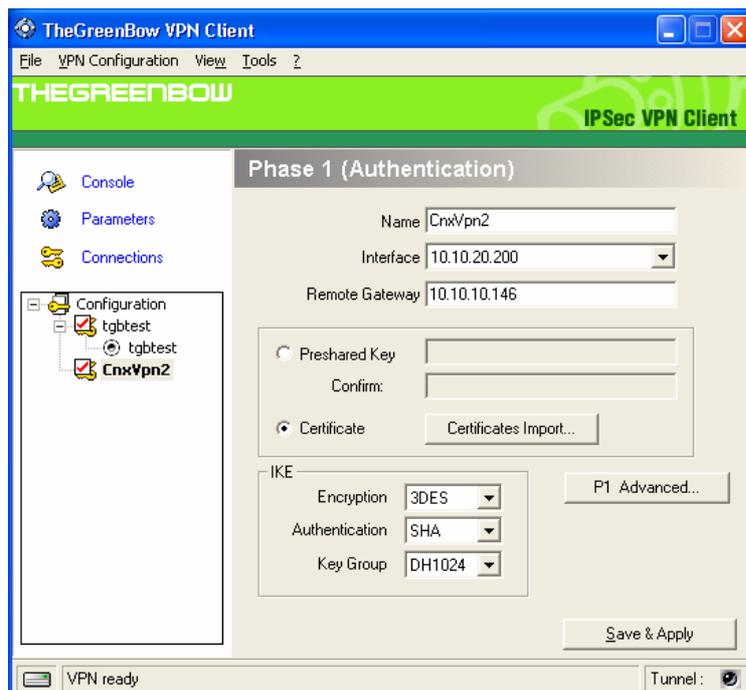
Click **Save & Apply**.

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

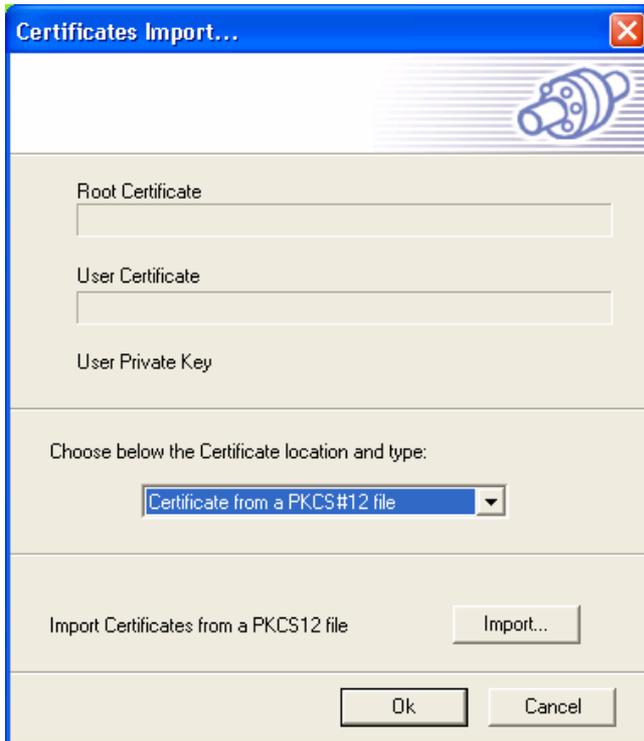
1. Download and Install the TheGreenBow VPN Client.
 - a) Go to <http://www.thegreenbow.com> and download the VPN Client software. Note: The software is available for 30 day evaluation after which you must either buy it or cease using it.
 - b) Follow the instructions to install TheGreenBow on your Windows 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.



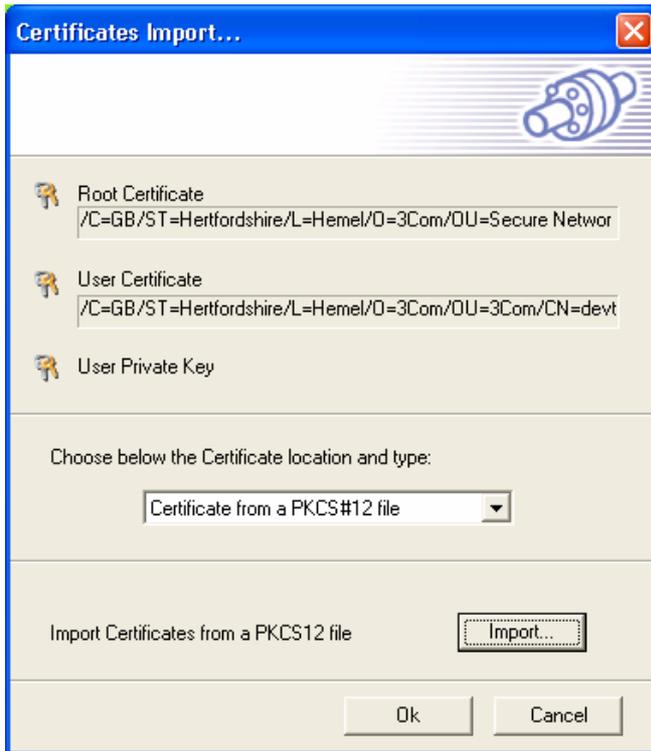
5. Click on **Certificates Import...** Complete the form as shown below.



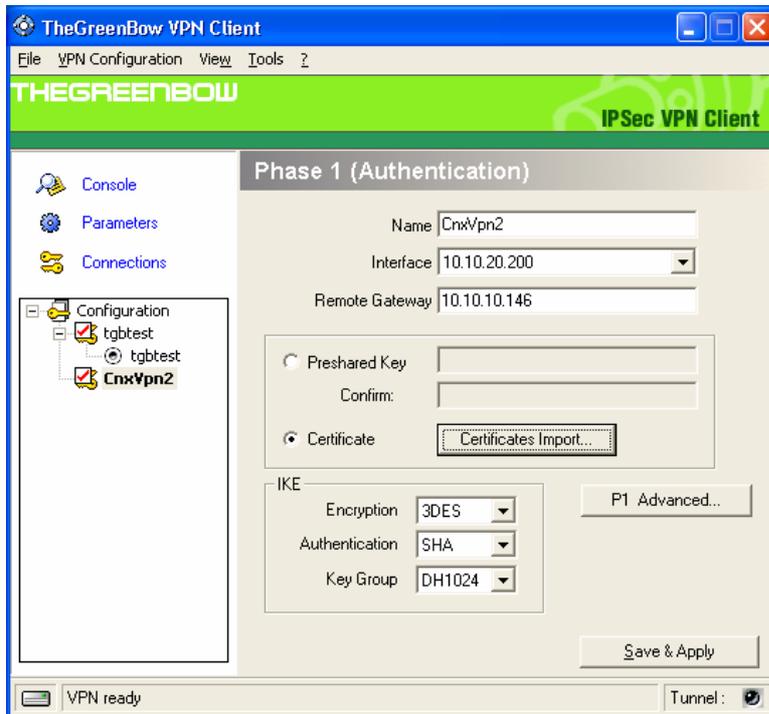
6. Click **Import**, browse to the PKS#12 certificate file on the PC and click **Open**. Enter the password of the PKS#12 file and click **OK**.



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

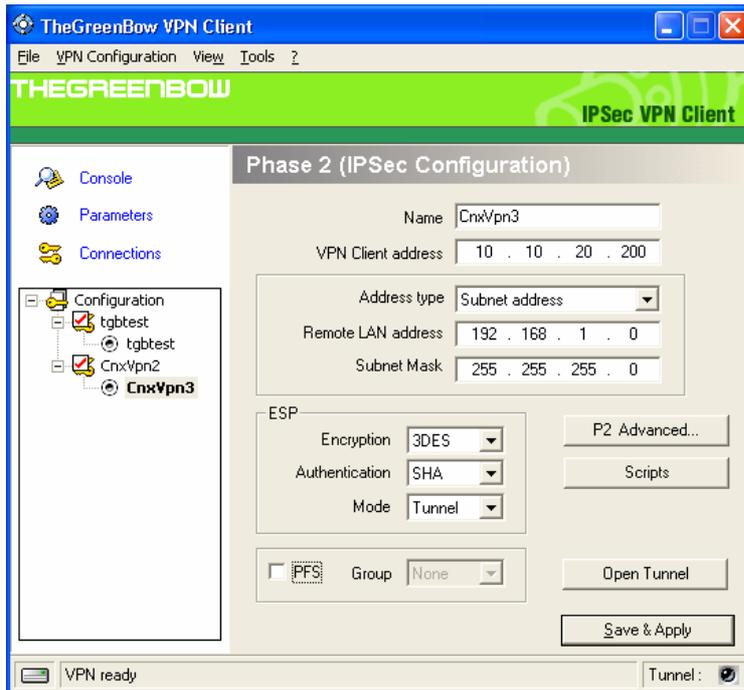


8. Click OK, which will return you to here:



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.



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.

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)

Frame 1 (142 bytes on wire, 142 bytes captured)
Ethernet II, Src: 00:50:04:ad:f2:73, Dst: 00:10:b5:07:2f:ff

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

VPN >> **IPSec Status** IPSec Config

IPSec Status Details

25 Records per page

Name	Peer IP Address	Local ID	Peer ID	Proposal	Status	Function(s)
Default	0.0.0.0	10.10.10.146	0.0.0.0	3DES-CBC-SHA1-DH2	Phase 1: Idle	
Default	10.10.20.200	192.168.1.0/24	10.10.20.200	ESP 3DES-CBC-ESP SHA-1 HMAC-No PFS	Phase 2: Established	

...or this (X.509 Certificates)

VPN >> **IPSec Status** IPSec Config

IPSec Status Details

25 Records per page

Name	Peer IP Address	Local ID	Peer ID	Proposal	Status	Function(s)
Default	0.0.0.0	C=GB, ST=Hertfordshire, L=Hemel, O=3Com, OU=3Com, CN=xfamily		3DES-CBC-SHA1-DH2	Phase 1: Idle	
Default	10.10.20.200	192.168.1.0/24	10.10.20.200	ESP 3DES-CBC-ESP SHA-1 HMAC-No PFS	Phase 2: Established	

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 <http://www.ethereal.com/>. 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**.



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.

EVENTS >> LOGS >> **VPN Log** Auto Refresh in 19 seconds

VPN Log Functions
[Download](#) [Reset](#)

VPN Log Entries

50 Records per page << < | 1 - 39 of 39 entries >

Log ID	Log Entry Time	Severity Level	SourceIP:Port	DestIP:Port	Message
10167	2007-06-13 12:29:16	INFO			Log Files Reset
10168	2007-06-13 12:29:25	INFO	10.10.20.200:500	10.10.10.146:500	Main mode responder received message 1
10169	2007-06-13 12:29:25	INFO	10.10.20.200:500	10.10.10.146:500	Rcvd Msg, 160 bytes: HDR[MM], [SA(52) VENDOR_ID(20) VENDOR_ID(20) VENDOR_ID(20) VENDOR_ID(20)], cookies: COA1C5F3B308C8A8 / 0000000000000000, msg id: 0
10170	2007-06-13 12:29:25	INFO	10.10.20.200:500	10.10.10.146:500	Proposal 1 -- protocol ISAKMP, 1 transforms
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
10172	2007-06-13 12:29:25	INFO	10.10.20.200:500	10.10.10.146:500	Peer supports NAT-T: Draft 2
10173	2007-06-13 12:29:25	INFO	10.10.20.200:500	10.10.10.146:500	Peer supports NAT-T: Draft 3
10174	2007-06-13 12:29:25	INFO	10.10.20.200:500	10.10.10.146:500	Peer supports DPD
10175	2007-06-13 12:29:25	INFO	10.10.20.200:500	10.10.10.146:500	Local phase 1 ID: IPV4_ADDR--10.10.10.146
10176	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: COA1C5F3B308C8A8 / 011C749A65C6F013, msg id: 0
10178	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: COA1C5F3B308C8A8 / 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(24)], cookies: COA1C5F3B308C8A8 / 011C749A65C6F013, msg id: 0
10183	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	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

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_rcv: 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 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 ike_phase_1_rcv_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.

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
115915 Default (SA CNXVPN1-CNXVPN1-P2) SEND phase 2 Quick 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
122626 Default (SA CNXVPN1-CNXVPN1-P2) SEND phase 2 Quick Mode
[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

- 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.

	Doc.Ref	tgvpn_ug_3comX_en
	Doc.version	1.0 – Jun.2007
	VPN version	2.5.1.6827

6 Contacts

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

Technical support by email at support@thegreenbow.com

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>