TheGreenBow IPSec VPN Client to 3Com X-family

Document Version:	1.0
Publication Date:	12th June 2007
Description:	TheGreenBow IPSec VPN Client to 3Com X-family
Product:	3Com X-family
3Com TOS Version:	2.5.1.6827
TheGreenBow VPN Client version:	4.00.007
Underlying Windows OS	Windows XP Version 5.1 (Build 2600.xpsp_sp2_gdr.070227-2254 : Service Pack 2).

Introduction

This document explains how to configure the 3Com X-family devices to terminate a “TheGreenBow” VPN IPSec Client.

These instructions assume that your corporate network is attached to the LAN security zone of the X-family, and that external (Internet) traffic is on the WAN security zone.

Table of Contents

1 OVERVIEW 3

2 NETWORK CONFIGURATION 3

3 PRE-REQUISITE CONFIGURATION 4

3.1.1 Initial Setup via the OBE 4

3.1.2 Load the Strong Encryption Package (Recommended) 7

4 CONFIGURING IPSEC WITH PRE-SHARED KEY (PSK) 8

4.1 High-level steps … 8

4.2 3Com X-family Configuration 8

4.3 TheGreenBow VPN Client Configuration 11

5 CONFIGURING IPSEC WITH X.509 DIGITAL CERTIFICATE 15

5.1 Recommended (High Security) Method 15

5.1.1 High Level Steps 15

5.1.2 Creating and Loading the Certificates 15

5.2 Alternative Method Using Open-Source Tools 16

5.2.1 Create the Certificates on the Certificate Server. 16

5.2.2 Load the certificates onto the X-family 25

5.2.3 Configure the X-Family VPN to use the Certificate. 26

5.2.4 Install and configure TheGreenBow VPN Client 27

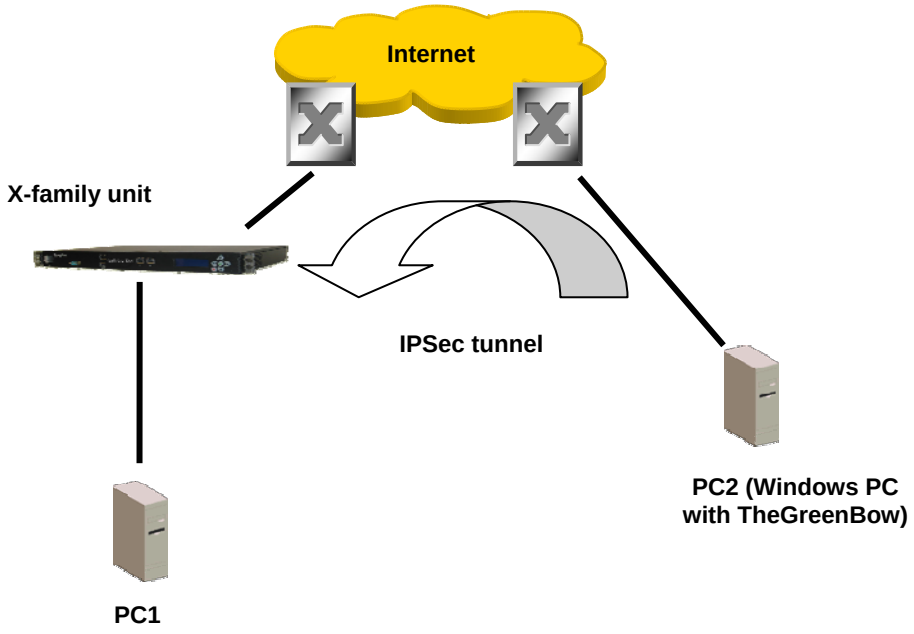
6 TROUBLESHOOTING IPSEC TUNNELS 33

1 Overview

Third-party IPSec VPN Clients like “TheGreenBow” provide a simple way to configure an IPSec secure tunnel to another device. “TheGreenBow” will run on any Microsoft Windows operating system from Windows 98 to Windows XP SP2 and a version is in development that will work on Windows Vista.

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 Network Configuration



IP Addresses for this example setup are:

Device	Interface	Address	Mask	Gateway
Router	1 (to X-family unit)	10.10.10.1	255.255.255.0	
Router	2 (to PC2)	10.10.20.1	255.255.255.0	
X-family	External	10.10.10.146	255.255.255.0	10.10.10.1
PC1		192.168.1.100	255.255.255.0	192.168.1.254
PC2		10.10.20.200	255.255.255.0	10.10.20.1

3 Pre-Requisite Configuration

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

3.1.1 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
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.

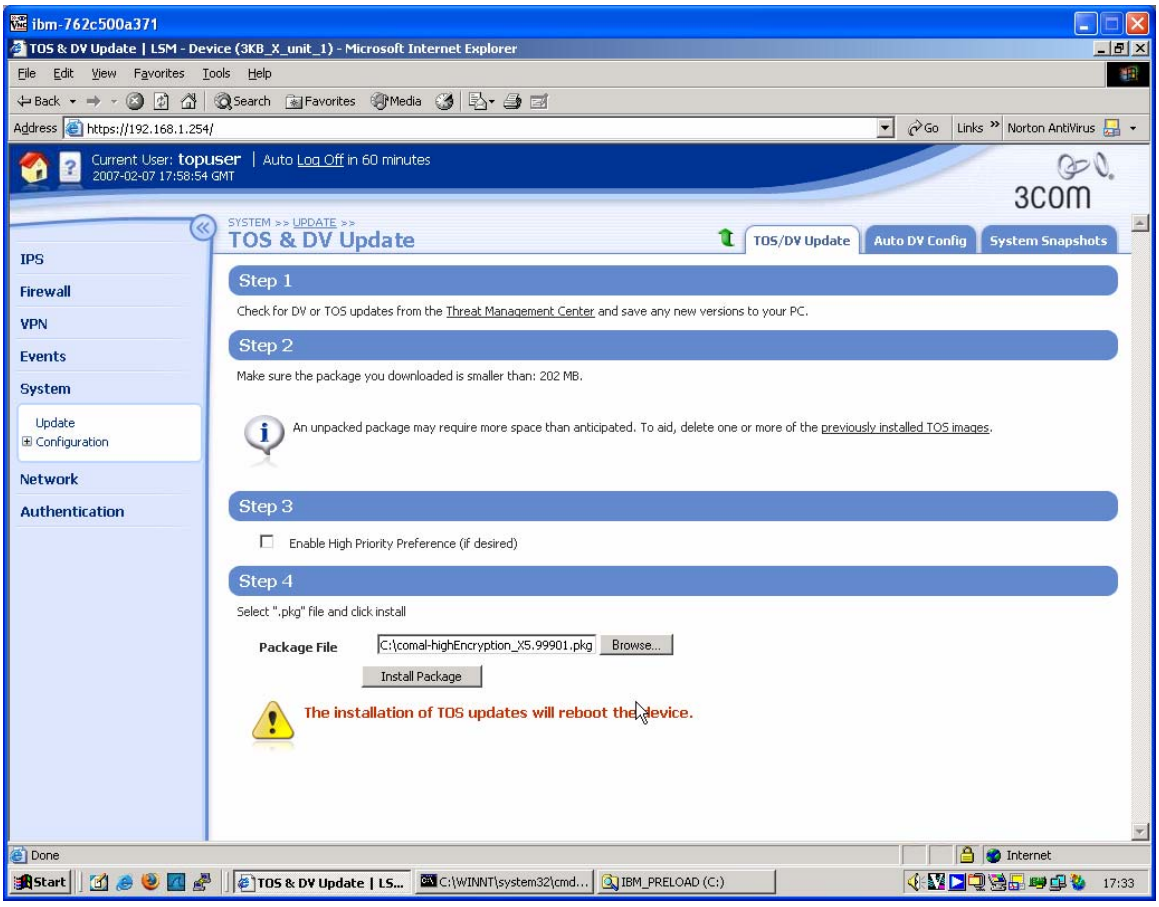
Firewall rules – the firewall rules in the factory default configuration will be sufficient – specifically this one:

```
2        permit       WAN          this-device       vpn-protocols
```


3.1.2 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.

4 Configuring IPSec with Pre-Shared Key (PSK)

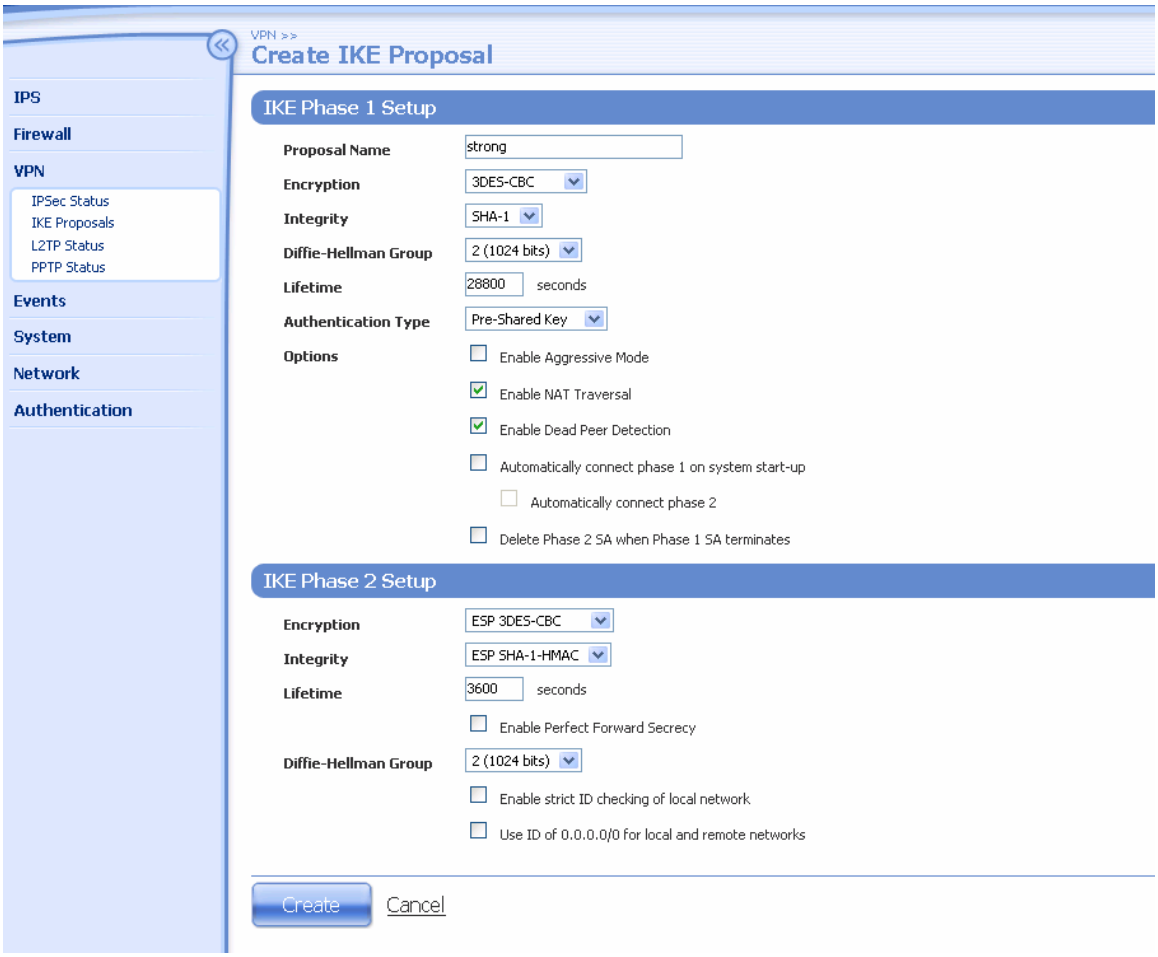
4.1 High-level steps …

Configuring IPSec with PSK consists of:

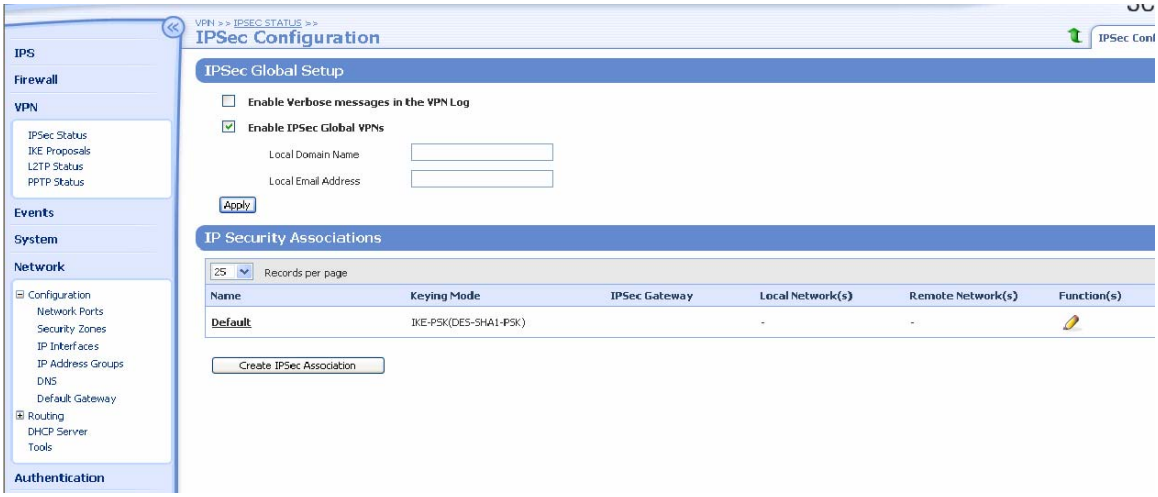
- Configure a strong encryption IKE proposal on the X-family (recommended).
- Enable IPSec VPNs on the X-family.
- Configure the Default Security Association on the X-family.
- Configure firewall rules to allow IPSec to the X-family WAN interface.
- Download and Install “TheGreenBow” VPN Client onto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

4.2 3Com X-family Configuration

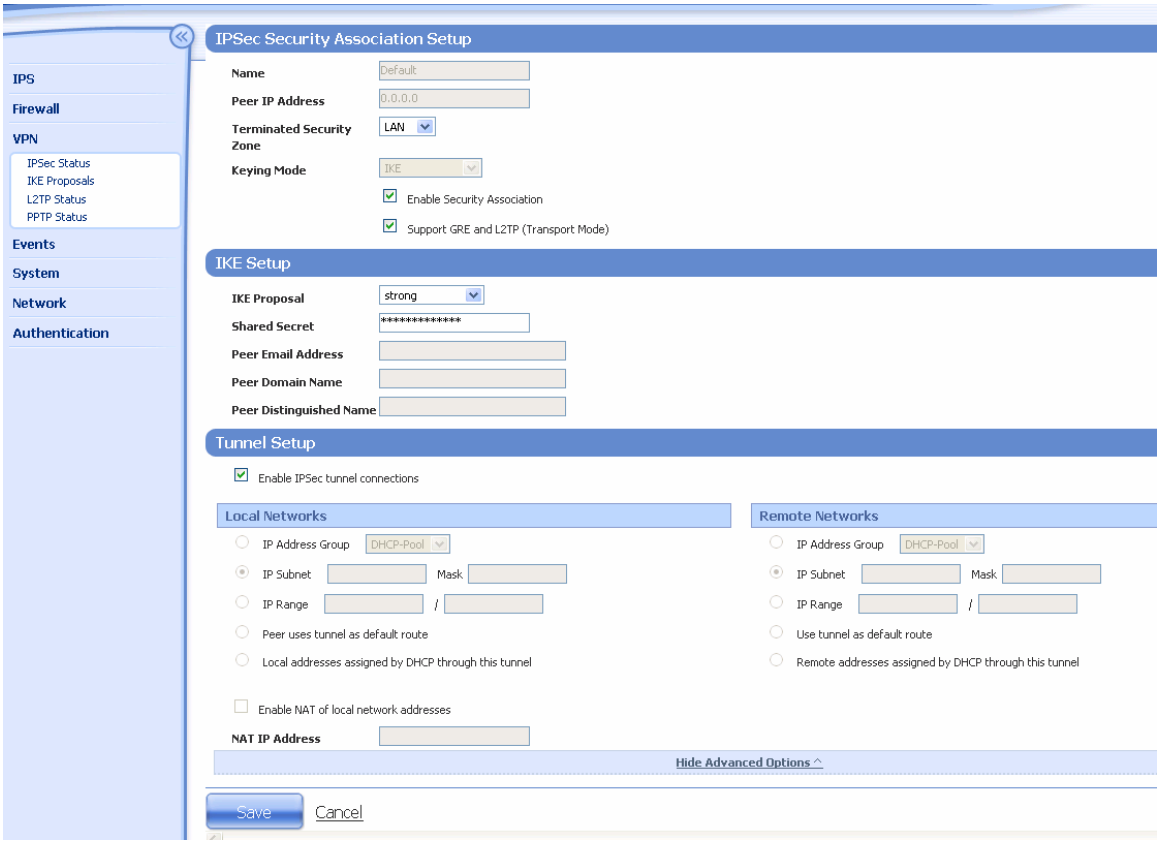
1) Login to your X-family web interface (LSM).
2) Create a strong encryption IKE Proposal on the X-family:
   a) Navigate to VPN > IKE Proposals and click on **Create New Proposal**.
   b) Complete the form as shown below and click **Create**. (This is an example using 3DES encryption, AES encryption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



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**.



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 zone[1].

b) Ensure that there is a policy rule allowing this-device to send ANY protocol to ANY zone [2].

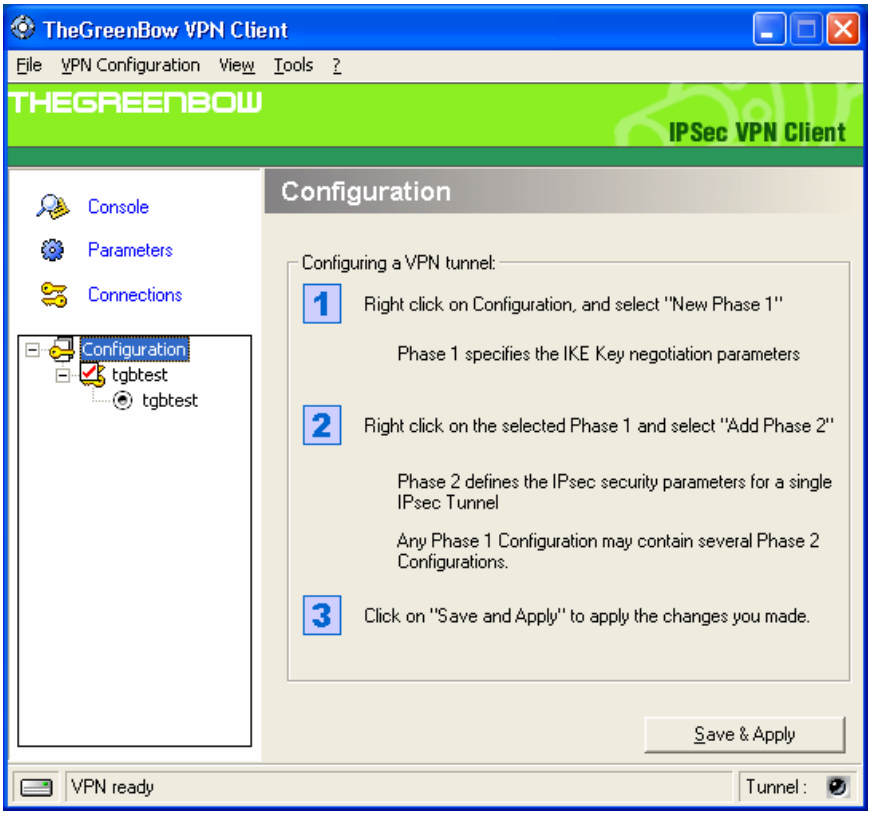
The X-family is now configured.

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

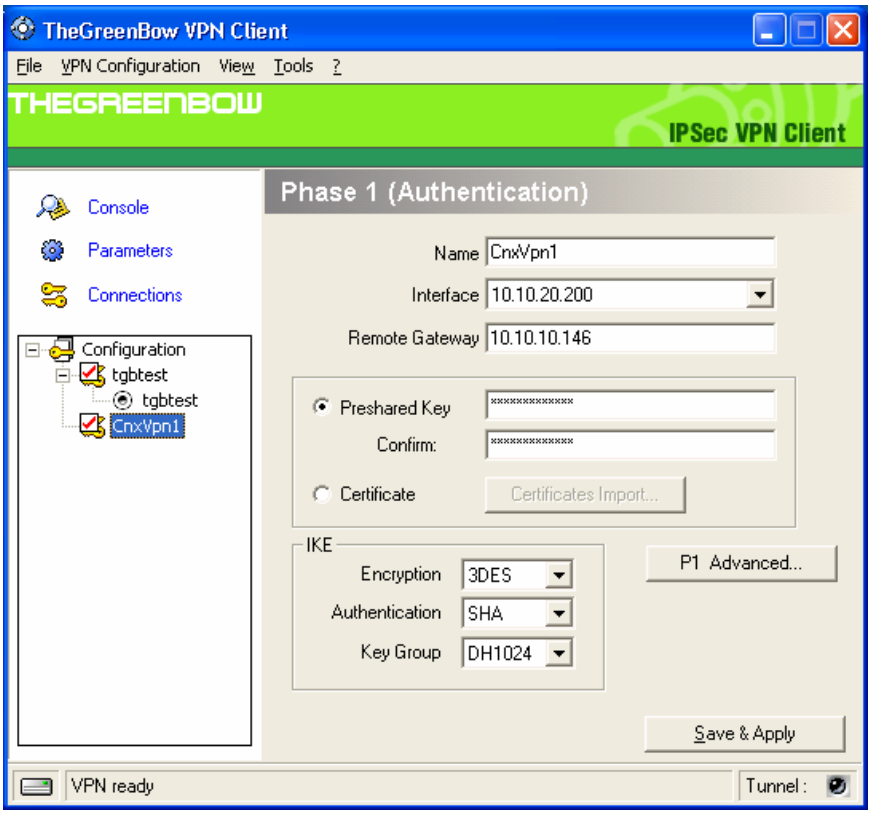
[2] There is a "hidden" firewall rule that enables this, unless a "DENY" rule has been specified in the firewall table that overrules it.

4.3 TheGreenBow VPN Client Configuration

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.

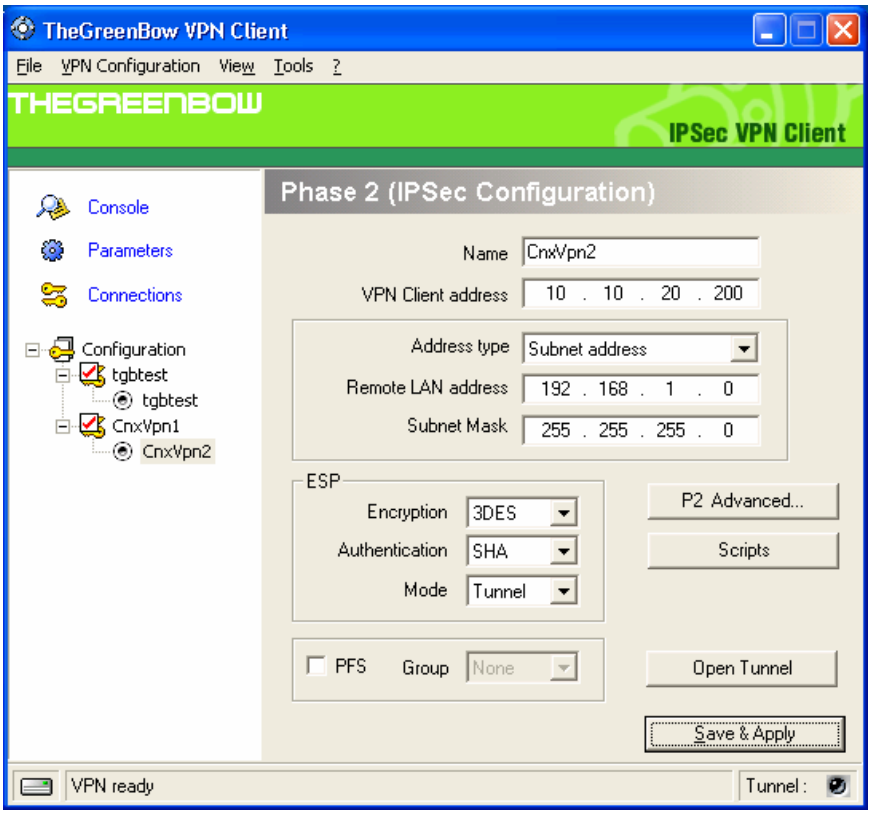


4. Follow Step 1 and complete the form as shown below. The pre-shared key must match the Shared Secret entered on the X-family device earlier.



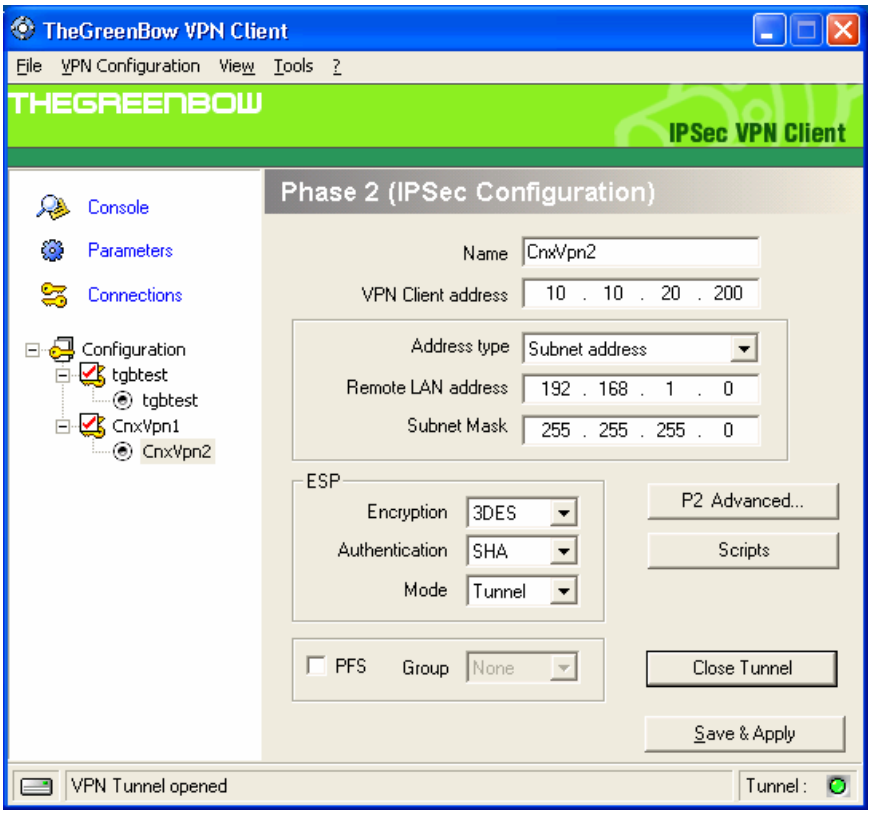
Click **Save & Apply**.

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



Click **Save & Apply**.

6. Click the **Open Tunnel** button. The tunnel should open. If it does not, clicking on the **Console** hyperlink will open a console window that will show debug information.
   When the tunnel is open, the TheGreenBow display will be like this:



…and the X-family IPSec VPN > IPSec Status screen will look like this:

Also, PC1 should be able to ping PC2 and vice versa.

5 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.

5.1 Recommended (High Security) Method

5.1.1 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.

5.1.2 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.

5.2 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.

5.2.1 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
        X509v3 extensions:
            X509v3 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=t
est@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=t
est@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-----
MIIDpzCCAxCgAwIBAgIBATANBgkqhkiG9w0BAQQFADCBizELMAkGA1UEBhMCR0Ix
EDAOBgNVBAgTB0VuZ2xhbmQxDzANBgNVBAcTBkxvbmRvbjENMAsGA1UEChMEM0Nv
bTEVMBMGA1UECxMMVGlwcGluZ1BvaW5OMQOwCwYDVQQDEwRNeUNBMSQwIgYJKoZI
hvcNAQkBFhV0ZXN0QHRpcHBpbmdwb2ludC5jb20wHhcNMDYwNDEwMDk0MjE4WhcN
MDcwNDEwMDk0MjE4WjCBizELMAkGA1UEBhMCR0IxEDAOBgNVBAgTB0VuZ2xhbmQx
DzANBgNVBAcTBkxvbmRvbjENMAsGA1UEChMEM0NvbTEVMBMGA1UECxMMVGlwcGlu
Z1BvaW5OMQOwCwYDVQQDEwRYNTA1MSQwIgYJKoZIhvcNAQkBFhV0ZXN0QHRpcHBp
bmdwb2ludC5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAJ85o/EDKYL9
lZwAxRYUyc38oP/yCNOtfb2CMDHsQ0Y3sKdJcgylA/P54mhEMalaVH6IaLh6ONaT
Kq3tOSkgJOZYsDQC1Tfyhy/2vsxbWCnWShUtwWoyRWgj3ERIyFkiv1hOEueIi9uM
ljg41JB1Z12MlgQTLO1WewhvYJcK1uUpAgMBAAGjggEXMIIBEzAJBgNVHRMEAjAA
MCwGCWCGSAGG+EIBDQQfFh1PcGVuU1NMIEdlbmVyYXRlZCBDZXJ0aWZpY2F0ZTAd
BgNVHQ4EFgQUAk5iXsnE1P1pXDwULnFFyVKZr6AwgbgGA1UdIwSBsDCBrYAUv3P5
BSUUtrfMvhNSbccIGgPqTDShgZGkgY4wgYsxCzAJBgNVBAYTAkdCMRAwDgYDVQQI
EwdFbmdsYW5kMQ8wDQYDVQQHEwZMb25kb24xDTALBgNVBAoTBDNDb20xFTATBgNV
BAsTDFRpcHBpbmdQb2ludDENMAsGA1UEAxMETXlDQTEkMCIGCSqGSIb3DQEJARYV
dGVzdEB0aXBwaW5ncG9pbnQuY29tggEAMA0GCSqGSIb3DQEBBAUAA4GBADHytJgQ
ymPkULivoPdudZIYiM5Rh5IWj9AhEIGHEAIl5Bok8PfHLD6/r4Z8YbdQbTLsp6rY
UBc8PtQwWiEnz7sVf6Y1M2YfocMSo9C8V9hDxo51ILeZ3iUQ2WkxhGOFMBUECEUg
ClrN2hhXpFUAUUVSGCP5UzsPH2jFgD7z73oS
-----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=t
est@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:
```



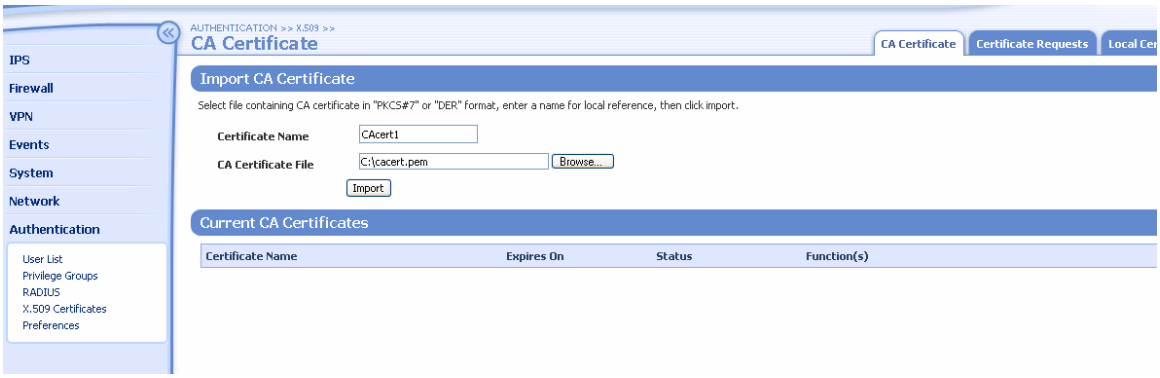
```
                    97:56:b2:3c:e4:af:46:d6:d6:b1:1b:f6:4e:40:65:
                    fb:ab:92:7f:8a:9a:48:1d:28:46:e7:81:ec:85:58:
                    8f:1d:70:36:bf:2f:05:2d:a0:ef:7d:47:e4:9d:a7:
                    1f:a2:0e:76:5f:ce:60:f0:76:ae:2c:16:f6:f1:a9:
                    73:df:99:be:35:8c:e9:3a:10:87:e5:ae:a4:93:33:
                    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=t
est@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-----
MIIDsjCCAxugAwIBAgIBAjANBgkqhkiG9w0BAQQFADCBizELMAkGA1UEBhMCR0Ix
EDAOBgNVBAgTB0VuZ2xhbmQxDzANBgNVBAcTBkxvbmRvbjENMAsGA1UEChMEM0Nv
bTEVMBMGA1UECxMMVGlwcGluZ1BvaW50MQ0wCwYDVQQDEwRNeUNBMSQwIgYJKoZI
hvcNAQkBFhV0ZXN0QHRpcHBpbmdwb2ludC5jb20wHhcNMDYwNDEwMDk1NjQxWhcN
MDcwNDEwMDk1NjQxWjCBljELMAkGA1UEBhMCR0IxETAPBgNVBAgTCFNjb3RsYW5k
MRIwEAYDVQQHEwlFZGluYnVyZ2gxDTALBgNVBAoTBDNDb20xFTATBgNVBAsTDFRp
cHBpbmdQb2ludDEUMBIGA1UEAxMLTDJUUCBDbGllbnQxJDAiBgkqhkiG9w0BCQEW
FXVzZXJAdGlwcGluZ3BvaW50LmNvbTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkC
gYEAs15lXEUP1vetUQlfq9G9tSgKhuBIggZNSndd2xBM5CVSFvJ1mI+5LYhgy26X
VrI85K9G1taxG/ZOQGX7q5J/ippIHShG54HshViPHXA2vy8FLaDvfUfknacfog52
X85g8HauLBb28alz35m+NYzpOhCH5a6kkzOTWwhadvfbpKECAwEAAaOCARcwggET
MAkGA1UdEwQCMAAwLAYJYIZIAYb4QgENBB8WHU9wZW5TUOwgR2VuZXJhdGVkIENl
cnRpZmljYXRlMB0GA1UdDgQWBBTEwe2oihb5b5WPXCbM3g6a8IGV1jCBuAYDVR0j
BIGwMIGtgBS/c/kFJRS2t8y+E1JtxwgaA+pMNKGBkaSBjjCBizELMAkGA1UEBhMC
R0IxEDAOBgNVBAgTB0VuZ2xhbmQxDzANBgNVBAcTBkxvbmRvbjENMAsGA1UEChME
M0NvbTEVMBMGA1UECxMMVGlwcGluZ1BvaW50MQ0wCwYDVQQDEwRNeUNBMSQwIgYJ
KoZIhvcNAQkBFhV0ZXN0QHRpcHBpbmdwb2ludC5jb22CAQAwDQYJKoZIhvcNAQEE
BQADgYEAZgR4B+7617hsGpPRT9y18D8pDRzVOe49cneJbKSwMP/jLKWptjWCIQVQ
issFbRQsEgPgehvPKYEle5m7dH6I4b8eam7cSq8TMnm7GVgpmvNQ/BDw+qooUM9a
```



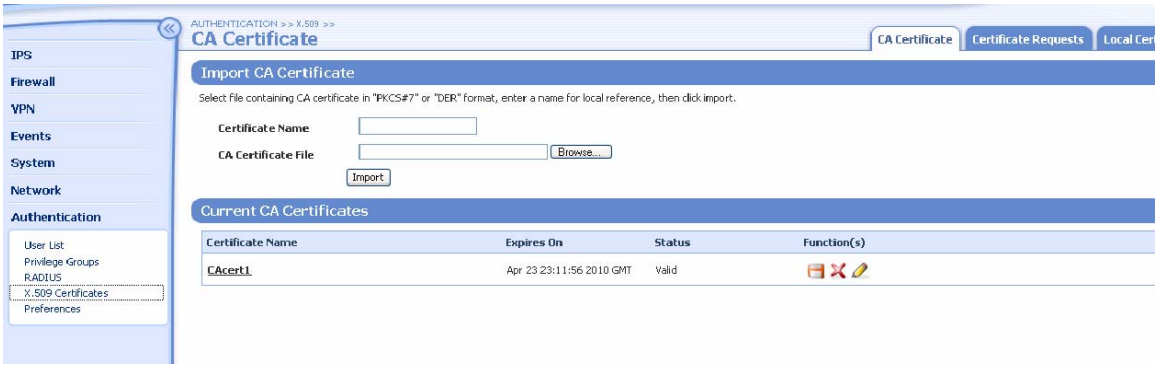
```
4+HOW1Q/89wXAcXr3yju+65TQXjEXZ94qTdkVzc3TdbYQYF15Ko=
-----END CERTIFICATE-----
Signed certificate is in newcert.pem
[test]:
[test]:
[test]: ################################################################
[test]: # Convert to PKCS#12 incorporating CA and Local Certificates #
[test]: ################################################################
[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]:
```


5.2.2 Load the certificates onto the X-family

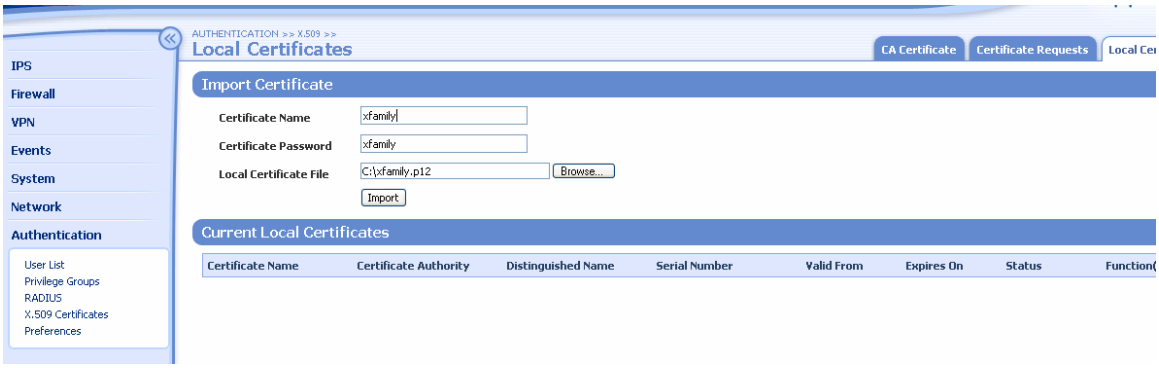
1. Copy the cacert.pem CA certificate file and the X-family.p12 local certificate file to your X-family management PC.
2. Import the CA certificate onto the X-family



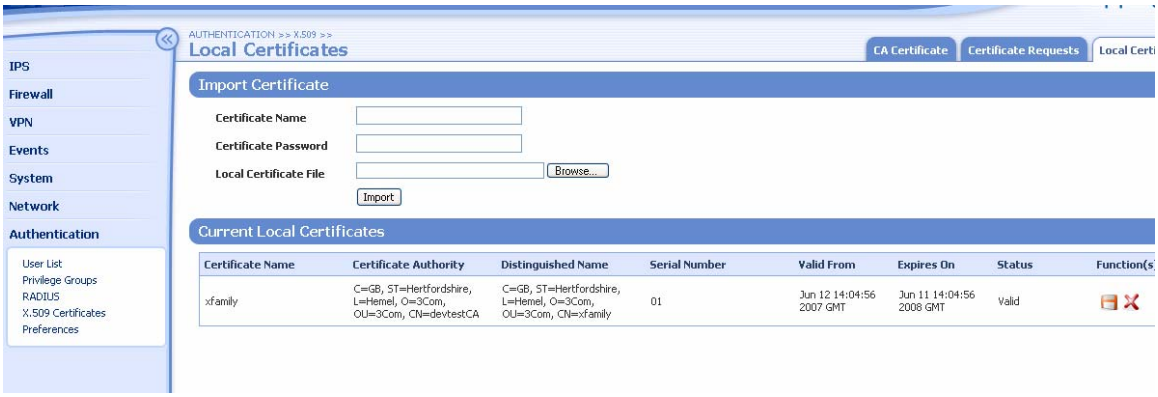
Status of imported Certificate should be “Valid”.



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

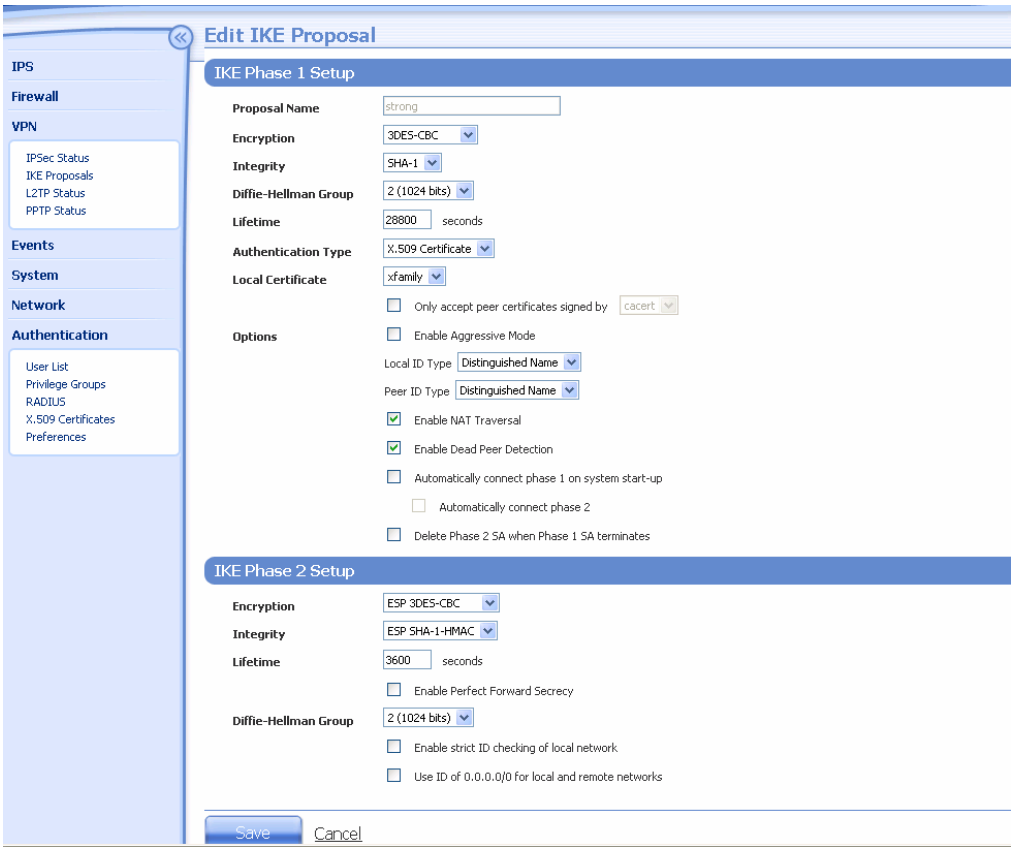


The certificate should appear in the Local Certificates tab and status should be “Valid”.



5.2.3 Configure the X-Family VPN to use the Certificate.

1) Configure the X-Family for Pre-Shared Key as shown in Section 4.2.
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.)



Click **Save**.

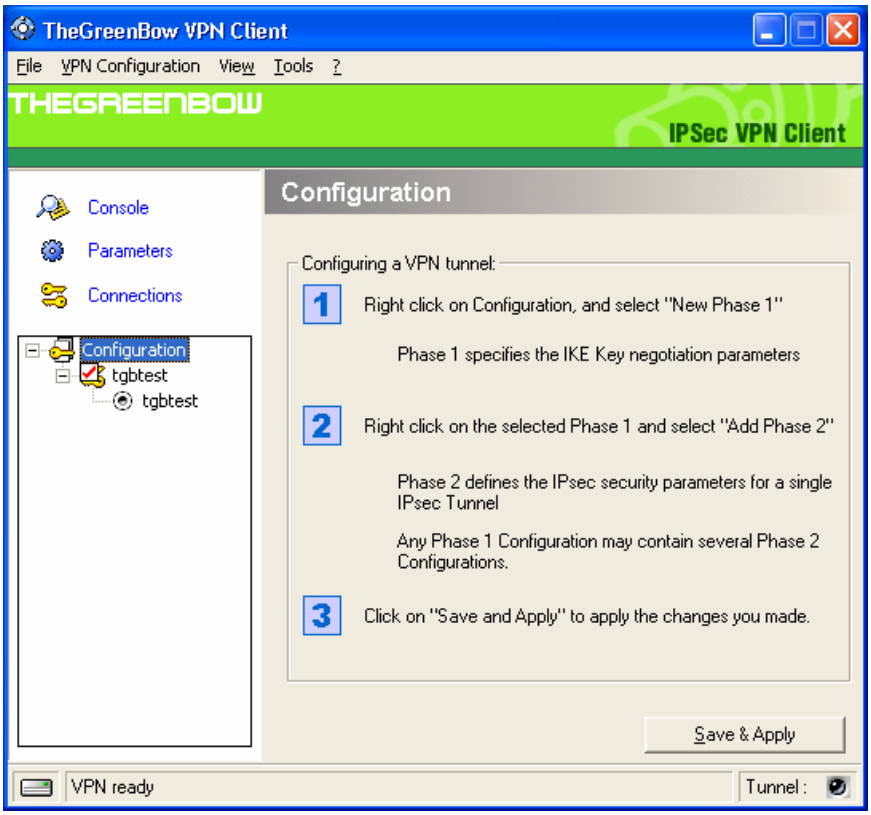
The X-family device is now ready to use certificates.

5.2.4 Install and configure TheGreenBow VPN Client

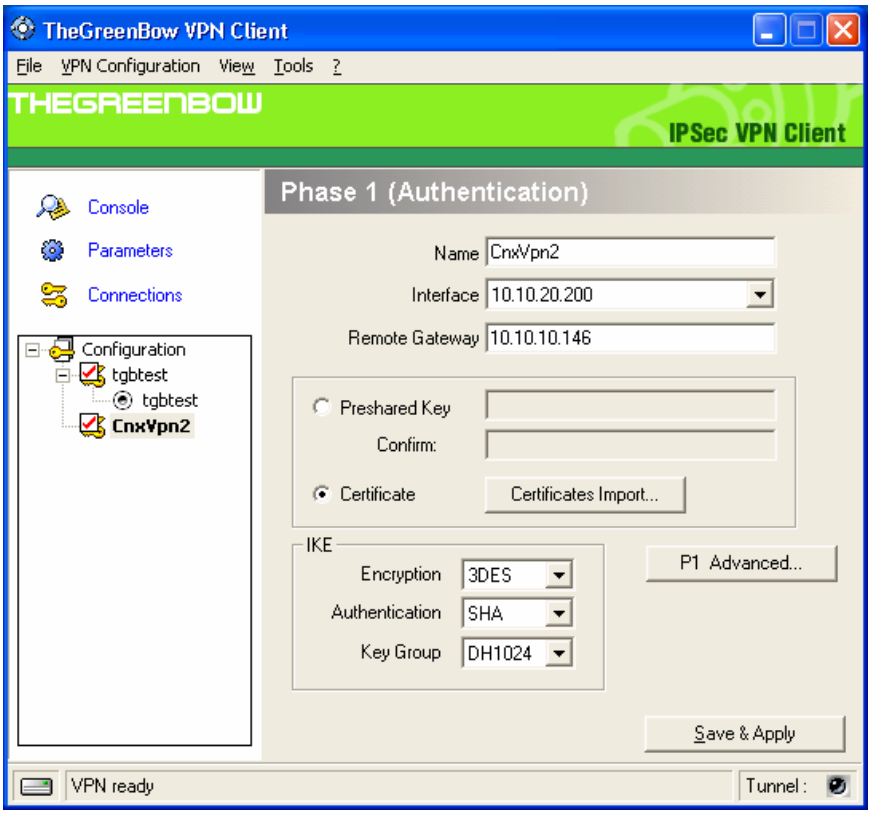
1. Download and Install the TheGreenBow VPN Client.

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.

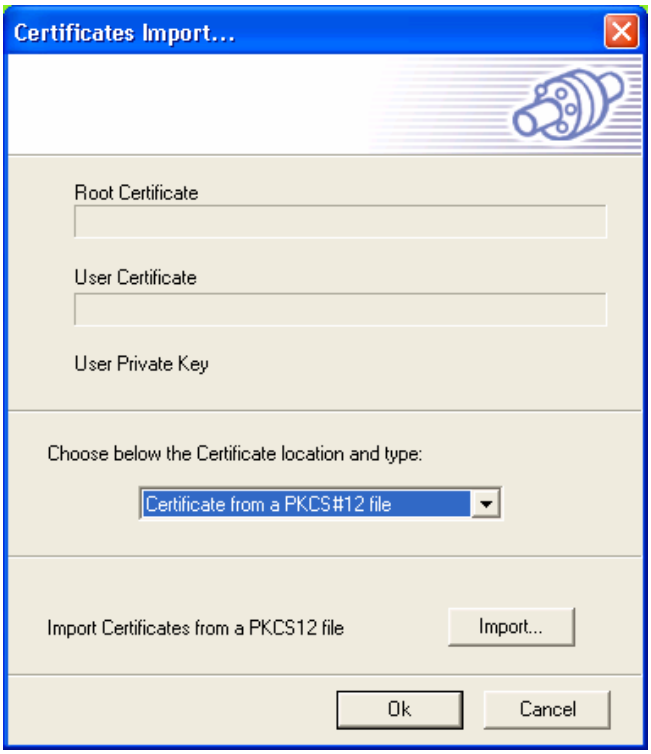
2. Copy the PKS#12 file to the TheGreenBow PC.
3. Start up TheGreenBow and click on Configuration. The instructions for setting up a connection are displayed as shown below.



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

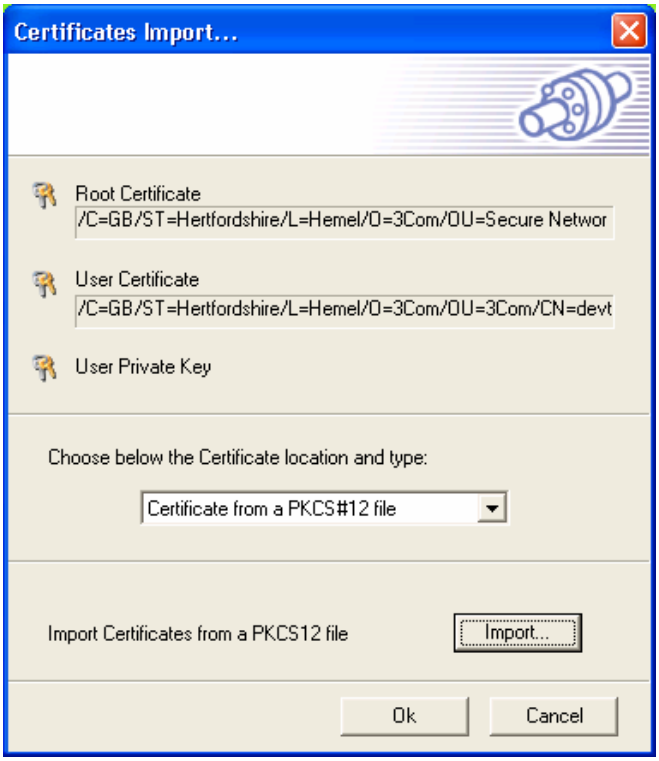


5. Click on **Certificates Import…** Complete the form as shown below.

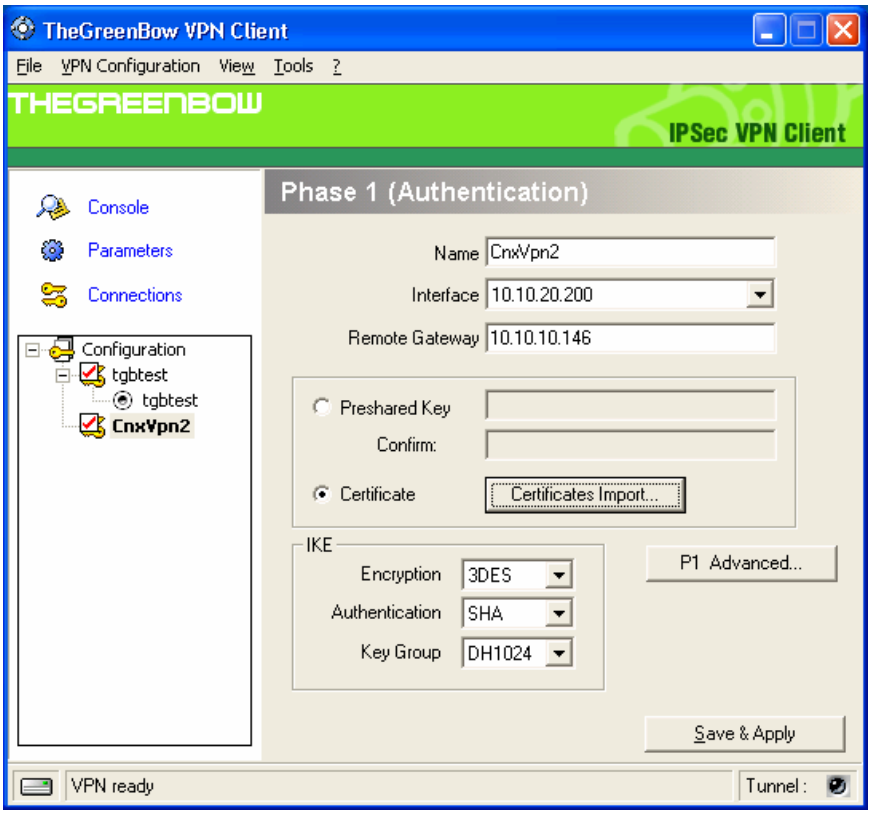


6. Click **Import**, browse to the PKS#12 certificate file on the PC and click **Open**. Enter the password of the PKS#12 file and click **OK**.

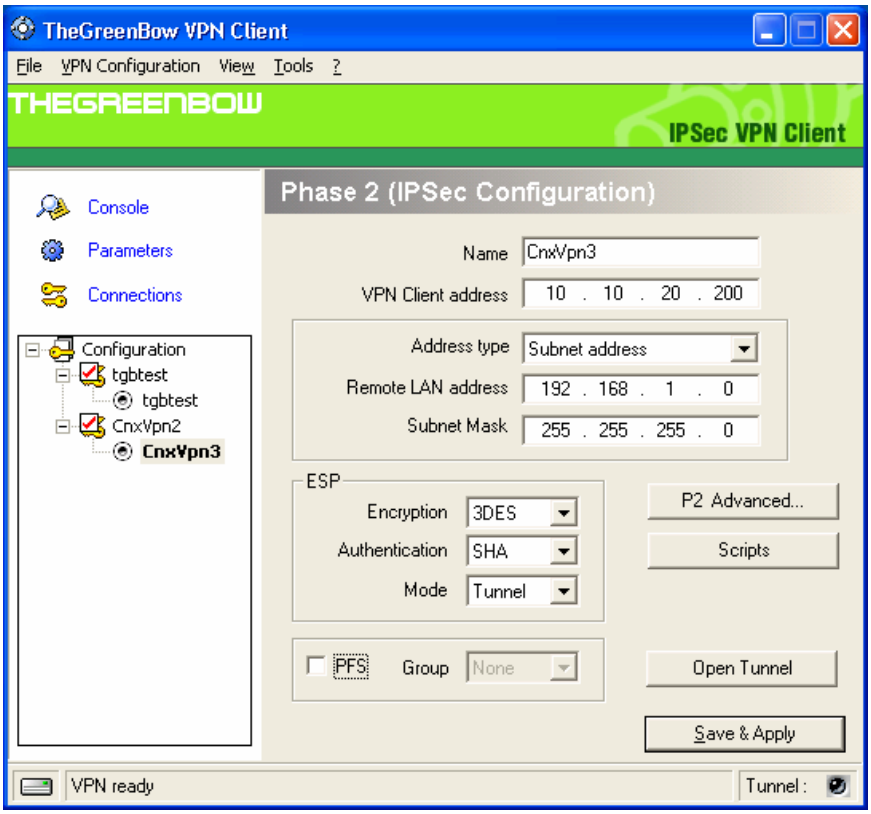
7. The form should now display details of the imported certificate and the root certificate that was used to sign it, as shown below.



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

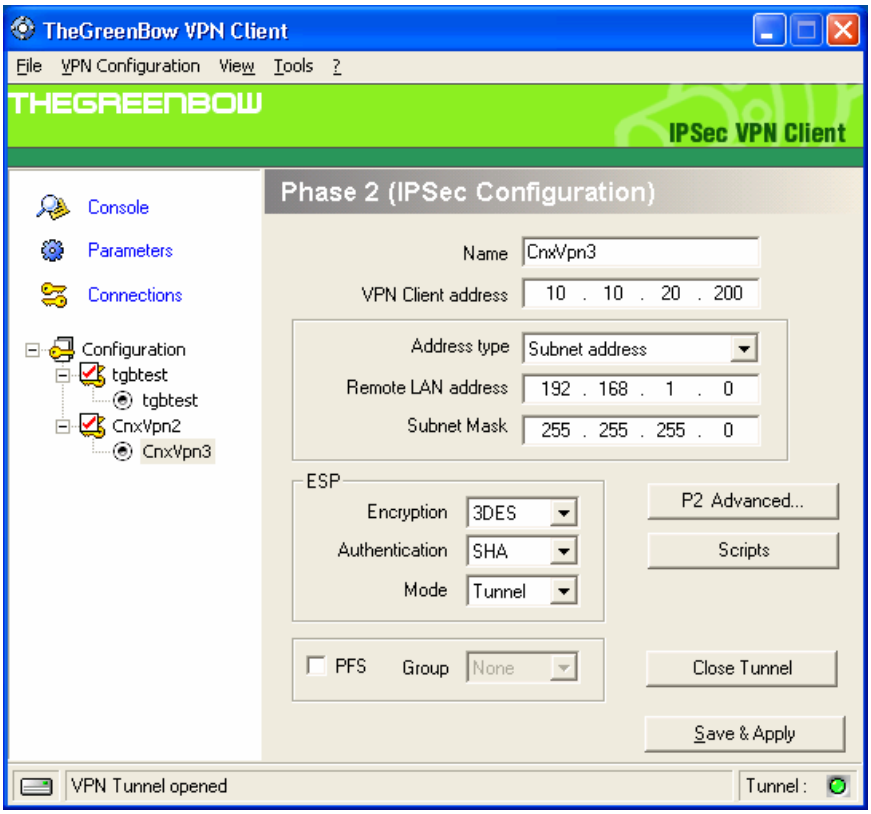


9. Click **Save & Apply**. Right click on the Phase 1 you just created (CnxVpn2 in my case) and select “Add Phase 2”. Complete the form as shown below.



10. Click **Save & Apply**.

11. Click the **Open Tunnel** button. The tunnel should open. If it does not, clicking on the **Console** hyperlink will open a console window that will show debug information.
    When the tunnel is open, the TheGreenBow display will be like this:



…and the X-family VPN > IPSec Status screen will look like this:

Also, PC1 should be able to ping PC2 and vice versa.

6 Troubleshooting IPSec Tunnels

The following is a list of things to check if the IPSec tunnel cannot be established or does not operate correctly:

a) On the X-family – ensure that the Strong Encryption package has been loaded (this shows on the LSM home screen as “Encryption: 256 bit” at the bottom of the Product Specification column).
b) On the X-family - ensure that the default IPSec SA is set to:
   - SA enabled
   - Phase 1 and 2 encryption set to 3DES (or AES 128)
   - Phase 1 and 2 authentication set to SHA1
   - Phase 1 Diffie-Hellman set to 2
   - Phase 2 Tunnel enabled
   - Phase 2 PFS **not** enabled.
c) Check the firewall policy rules allow:
   - Service IPSec from the WAN zone to this-device.
   - Service IKE from the WAN zone to this-device.
   - From this-device to ANY for ANY service. (There is an implicit “hidden” rule for this so no explicit rule is required unless an explicit deny rule has been added to the table).

   It is worth checking the Block Log on the X-family to see if the connection is being refused. This may require you to enable “Logging” on the Block rules in the firewall that you suspect may be blocking the request.

If you are using Pre-Shared Key:

a) Ensure that the X-family is using exactly the same Shared-Secret/Pre-Shared Key character string as TheGreenBow. Shared-Secrets/Pre-shared Keys on the X-family must be at least eight characters long.

If you are using X.509 certificates:

a) On X-family - ensure that the correct certificate name is selected on the IKE proposal.
b) On both - ensure that the certificate is signed by a trusted CA. Failure to do this may result in TheGreenBow refusing to use the certificate for IPSec connections.

