



## IPSec VPN for SonicWall PRO 2040 to X-family

<b>Document Version:</b>	1.4
<b>Publication Date:</b>	18 February 2009
<b>Description:</b>	Configuring site-to-site VPNs from SonicWall to 3Com X-family
<b>Product:</b>	3Com X-family
<b>3Com TOS Version:</b>	2.5.0.6688 or later
<b>SonicWall PRO 2040 Software Version:</b>	SonicOS Enhanced 3.2.0.0-43e

# 1 Overview

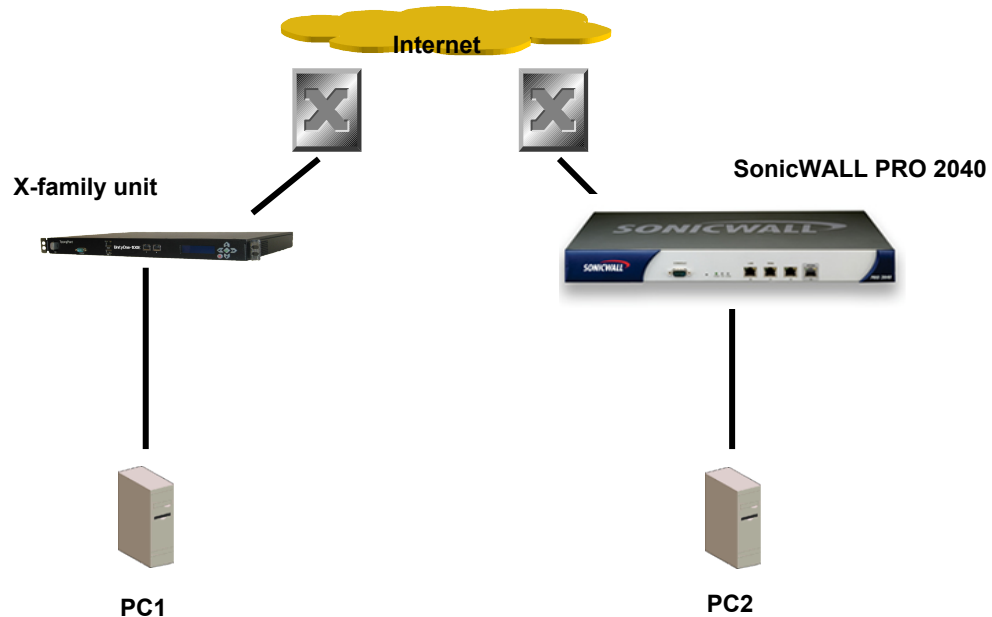
This technical note describes how to setup IPSec VPN tunnels between a 3Com X-family device and the SonicWall PRO 2040.

Both Main Mode and Aggressive Mode deployments are shown. Main Mode is more secure and hence is recommended when both sites have a static IP address. Aggressive mode can be used if one IP address is dynamic.

This document only describes "shared-secret/pre-shared-key" setup, not the alternative method using X.509 certificates.

# 2 Connection

This diagram shows the SonicWall PRO 2040 and an X-family unit connected via the Internet – actually a simple router in my configuration. Each device has a PC connected to its LAN interface – to be used both for configuration and for testing purposes.



**Addresses are:**

Device	Interface	Address	Mask	Gateway
Router	1 (to X-family unit)	10.10.20.1	255.255.255.0	
Router	2 (to SonicWALL)	10.10.10.1	255.255.255.0	
X-family	external	10.10.20.147	255.255.255.0	10.10.10.1
SonicWALL	external	10.10.10.147	255.255.255.0	10.10.20.1

			0	
PC1		192.168.1.100	255.255.255.0	192.168.1.254
PC2		192.168.22.10	255.255.255.0	192.168.22.254

## 3 Pre-Requisite Configuration

### 3.1 3Com X-family Pre-requisite Configuration

#### 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]: sta  
IP address []: 10.10.20.147  
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	10.10.20.147	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.

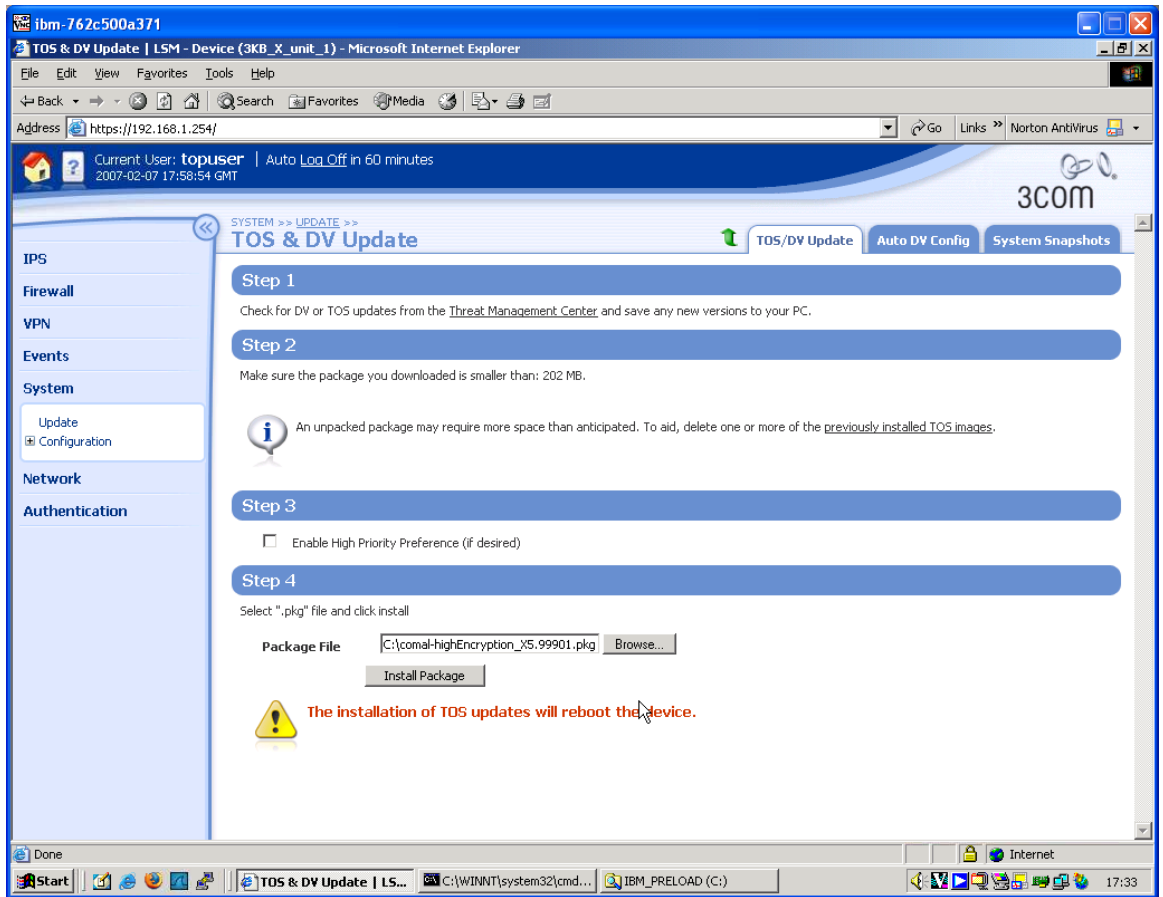
**Firewall rules** - the firewall rules in the factory default configuration will be sufficient - specifically this one:

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

### 3.1.2 Load the High Encryption Token

When delivered from the factory, the X-family devices are capable of encryption levels up to a key size of 64 bits (e.g. DES). To enable higher encryption key sizes to be used (e.g. 3DES, AES) a High Encryption "token" package must be loaded onto the device. This package is only available to approved end users in approved locations.

1. Acquire the High Encryption package 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 High Encryption package on PC1. Click "Install Package".



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

### 3.2 SonicWALL PRO 2040 Pre-Requisite Configuration

1. From factory defaults, PC2 must either be set to DHCP at the start or must have an IP address in the range 192.168.1.2-254.
2. Open a browser on PC2, connect to <https://192.168.1.254> and login to the SonicWALL GUI.
3. Click the Network button on the left.
4. On the Network screen, click the "Setup Wizard" button.
5. Complete the wizard as follows:

**Note: The certificate error shown in each of the following seven screen shots is due to using Internet Explorer 7. Do not use IE7 as it will cause problems later in configuration of the VPNs. Use either IE6 or Firefox 2.0.**

**SonicWALL - Setup Wizard - Windows Internet Explorer**

https://192.168.22.254/wizSetupPass.html Certificate Error

### Step 1: Change Password

You must change the administrator password for your SonicWALL.

Please select a strong password. A strong password should be a combination of numbers and letters up to 32 characters long.

The password you select will be case-sensitive. It should not be a word that appears in the dictionary, and it should not contain personal information such as birthdates, names of relatives, or license plate numbers. It should be something easy to remember, but difficult to guess, such as "11k3ch33s3".

**Note: The password will be set as entered before. If you wish to change your password again, enter the new information and click Next.**

Old Password:

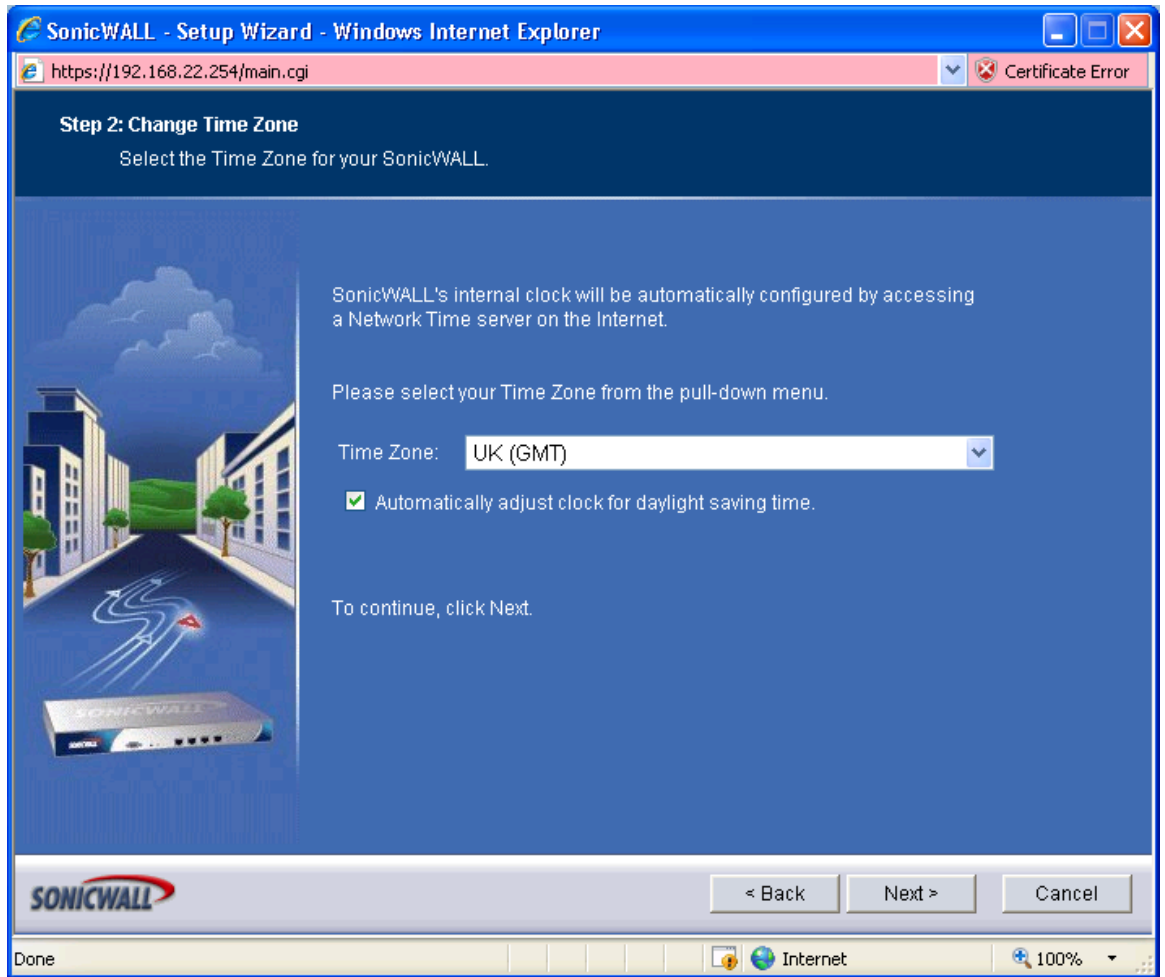
New Password:

Confirm:

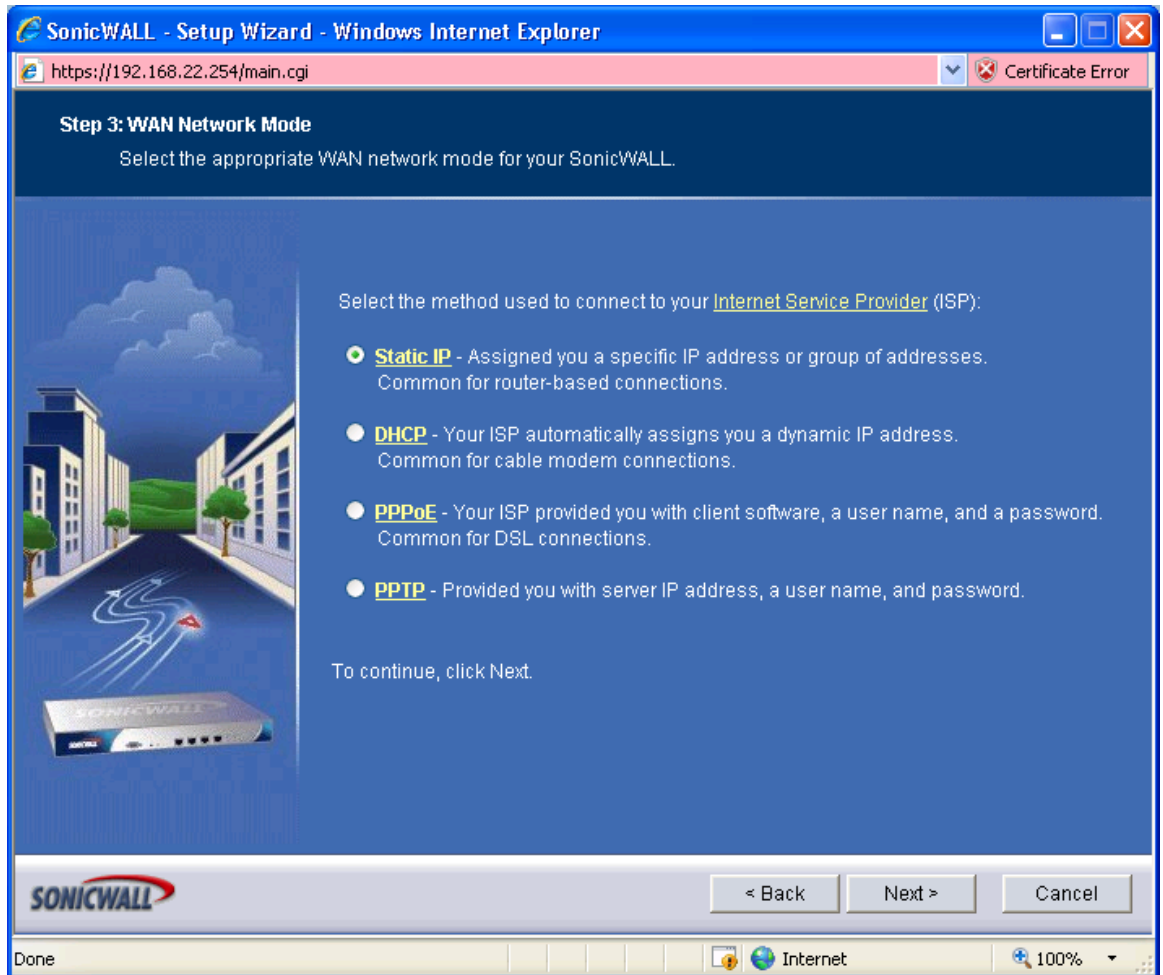
To continue, click Next.

**SONICWALL** < Back Next > Cancel

Done Internet 100%







SonicWALL - Setup Wizard - Windows Internet Explorer

https://192.168.22.254/main.cgi

Certificate Error

**Step 4: WAN Network Mode: NAT Enabled**

Fill in the following network settings to get to the Internet.

You will need to fill in the following fields to connect to the Internet. All these values must be entered as numerical IP addresses (such as 10.50.128.52). If you do not have the information, please contact your [ISP](#).

SonicWALL WAN IP Address: 10.10.10.147

WAN Subnet Mask: 255.255.255.0

Gateway (Router) Address: 10.10.10.1

DNS Server Address: 10.10.10.1

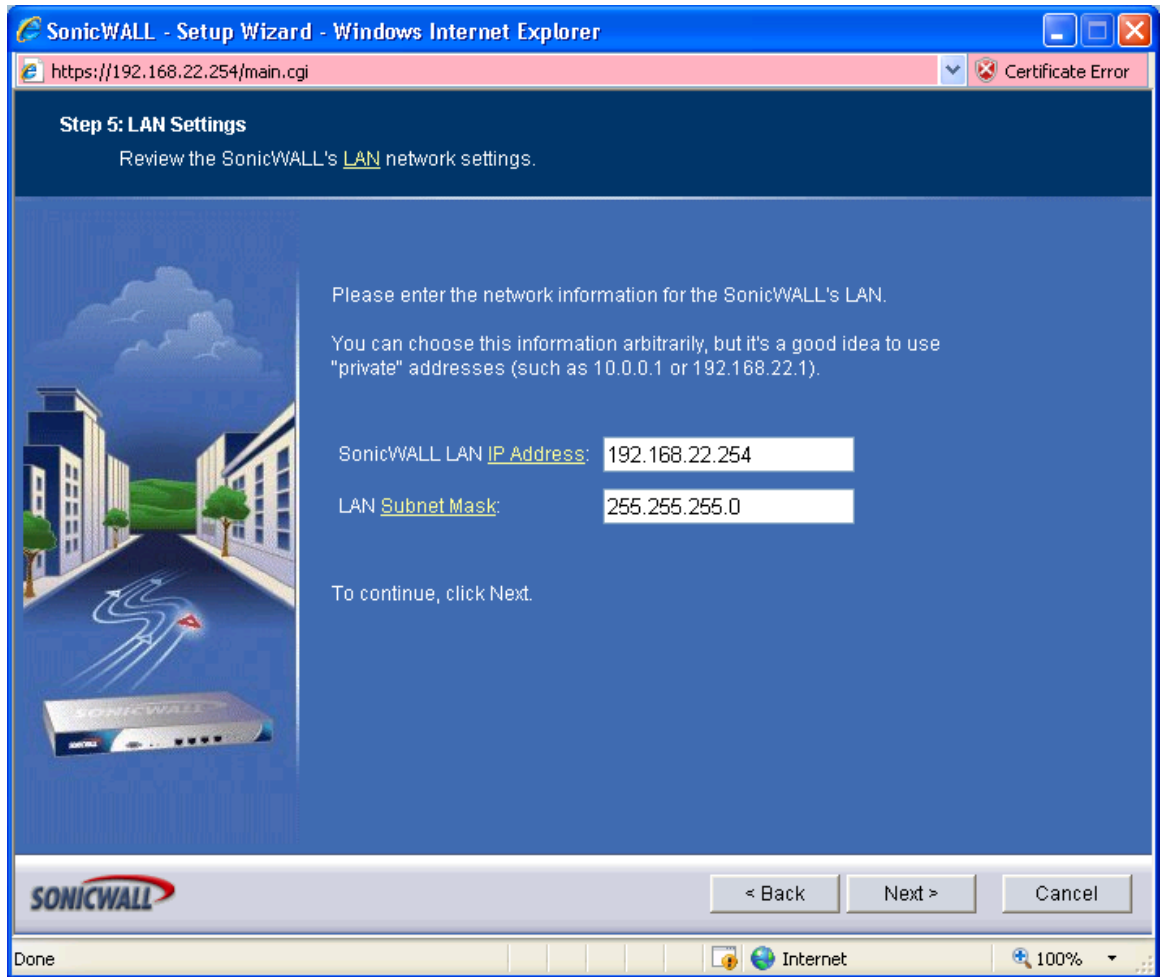
DNS Server Address #2 (optional):

To continue, click Next.

SonicWALL

< Back Next > Cancel

Done Internet 100%



SonicWALL - Setup Wizard - Windows Internet Explorer

https://192.168.22.254/main.cgi

**Step 6: LAN DHCP Settings**  
You can enable and configure your SonicWALL's DHCP Server on the LAN.

If you wish to use SonicWALL's [DHCP Server](#) on the LAN, check the "Enable DHCP Server on LAN" checkbox below and enter a range of IP addresses to assign to the network devices.

The address range must be in the same subnet as the SonicWALL Web Management address, currently **192.168.22.254/255.255.255.0**.

The range below already exists. You may change it here if you wish.

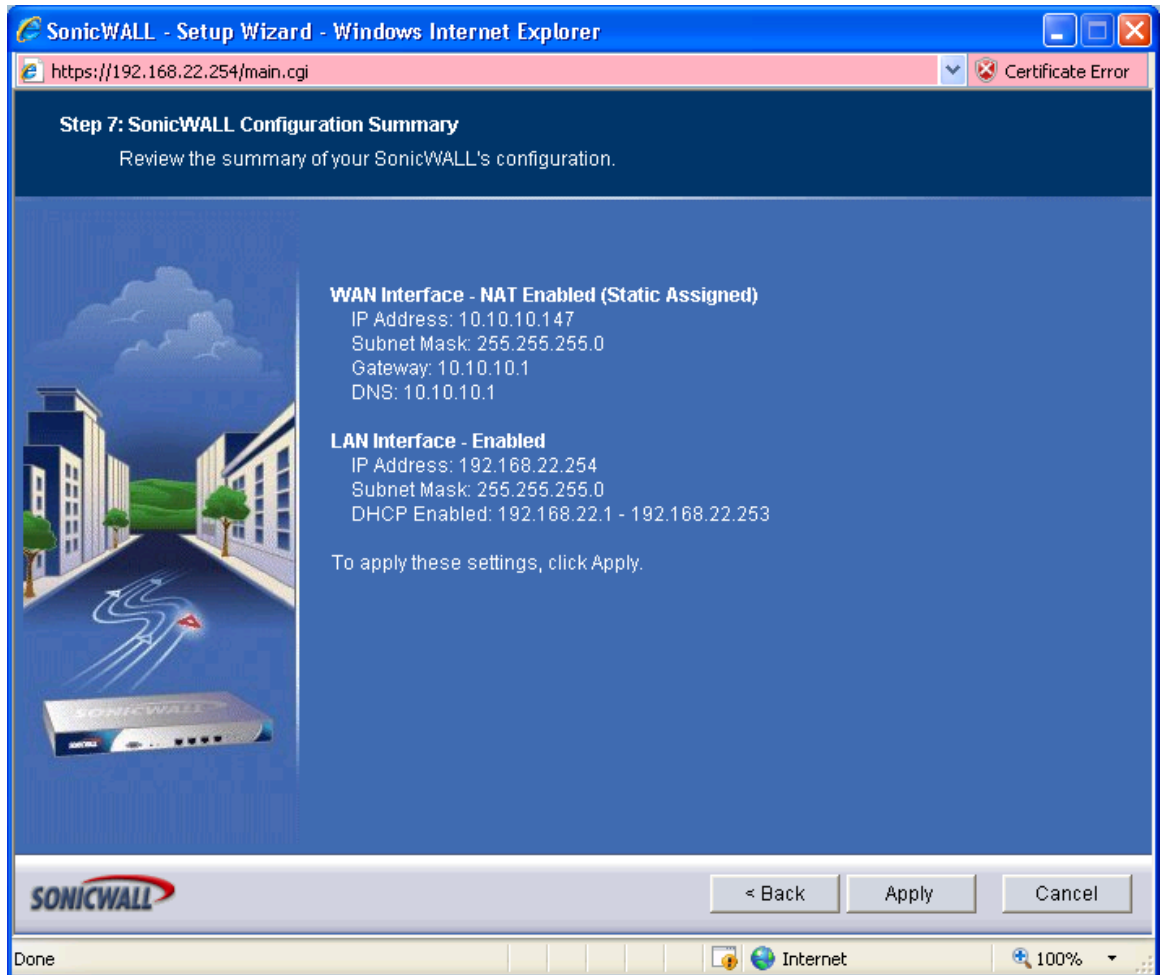
Enable DHCP Server on LAN

LAN Address Range:  to

To continue, click Next.

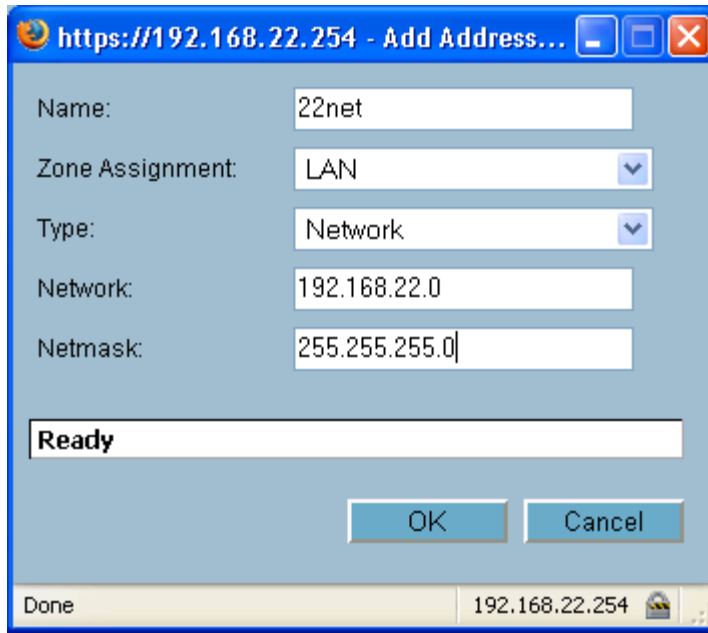
**SONICWALL** < Back Next > Cancel

Done Internet 100%



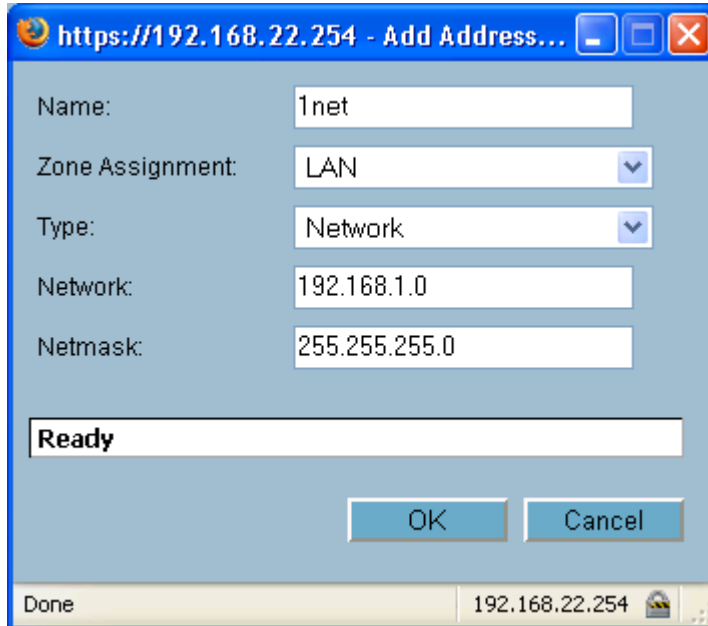
...and click the Apply button.

6. Create address groups for the local subnets each end of the VPN tunnel. Go to Network -> Address Objects and scroll to the bottom of the page. Click on the "Add" button to add an address object. Complete the form as shown below:



..and click the OK button.

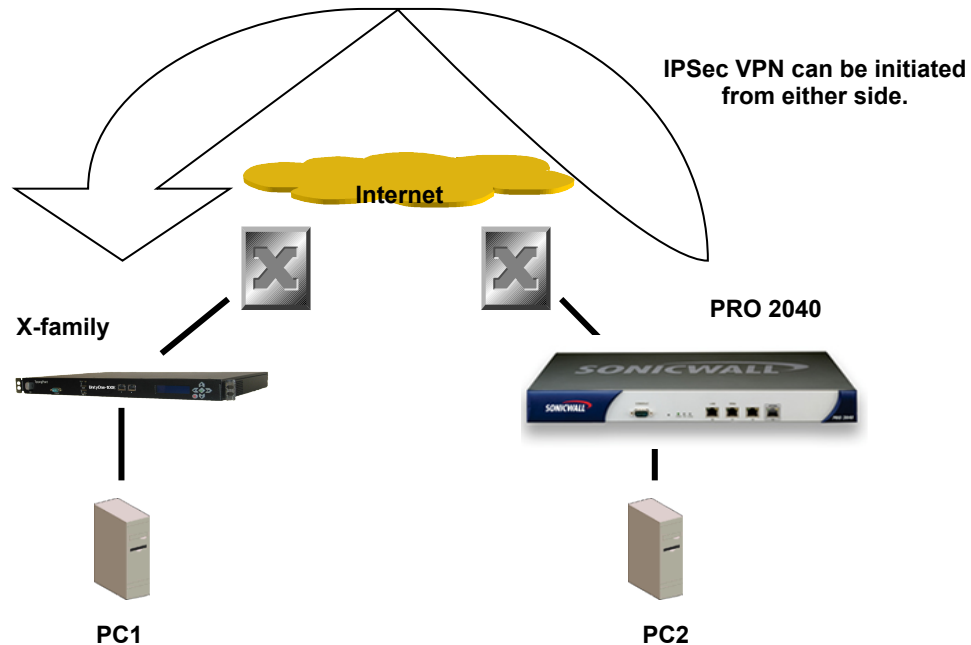
7. Repeat for the other address object.



...and click the OK button.

## 4 Configuring Main Mode Tunnel

This example shows how to configure an IPsec tunnel using Main Mode between the 3Com X-family and a SonicWall PRO 2040. Main Mode is the recommended setting when both devices have static IP addresses that can be accessed from the public internet.



### Key Setup Information

Keying Mode	IKE
IKE Mode	Main Mode
SA Authentication Method	Pre-shared Key
Keying Group	DH (Diffie Hellman) Group 2
Encryption and Data Integrity	3DES-SHA1

## 4.1 3Com X-family VPN Configuration

1. Open a browser on PC1, connect to <https://192.168.1.254> and login as the user you set up during the OBE.
2. Navigate to VPN -> IKE Proposals. You will see one default proposal for DES-SHA1-PSK but we do not want to use this as it does not provide a suitably high level of security so click on the "Create IKE Proposal" button to create a new proposal. Complete the form that opens as shown below.

The screenshot shows a web browser window titled "Create IKE Proposal | LSM - Device (3KB\_X\_unit\_1) - Microsoft Internet Explorer". The address bar shows <https://192.168.1.254/>. The user is logged in as "topuser" with an auto-logout in 60 minutes. The page title is "VPN >> Create IKE Proposal".

**IKE Phase 1 Setup**

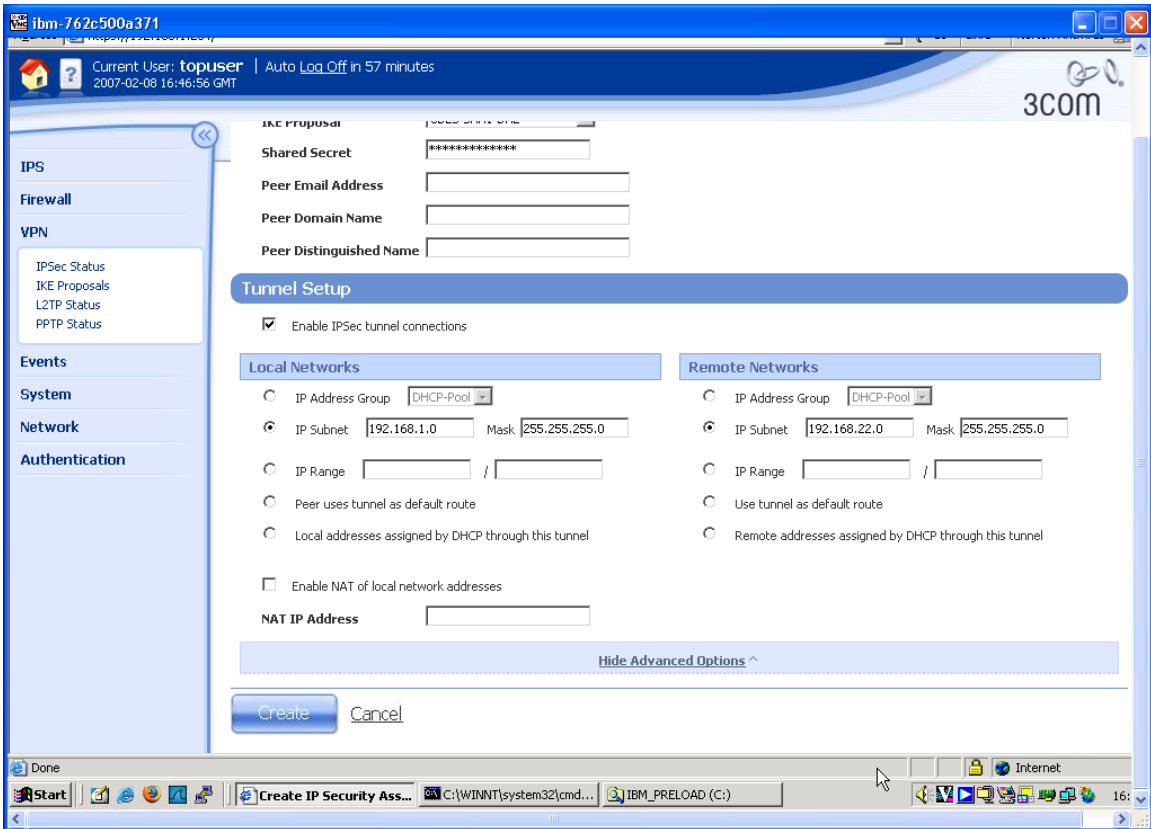
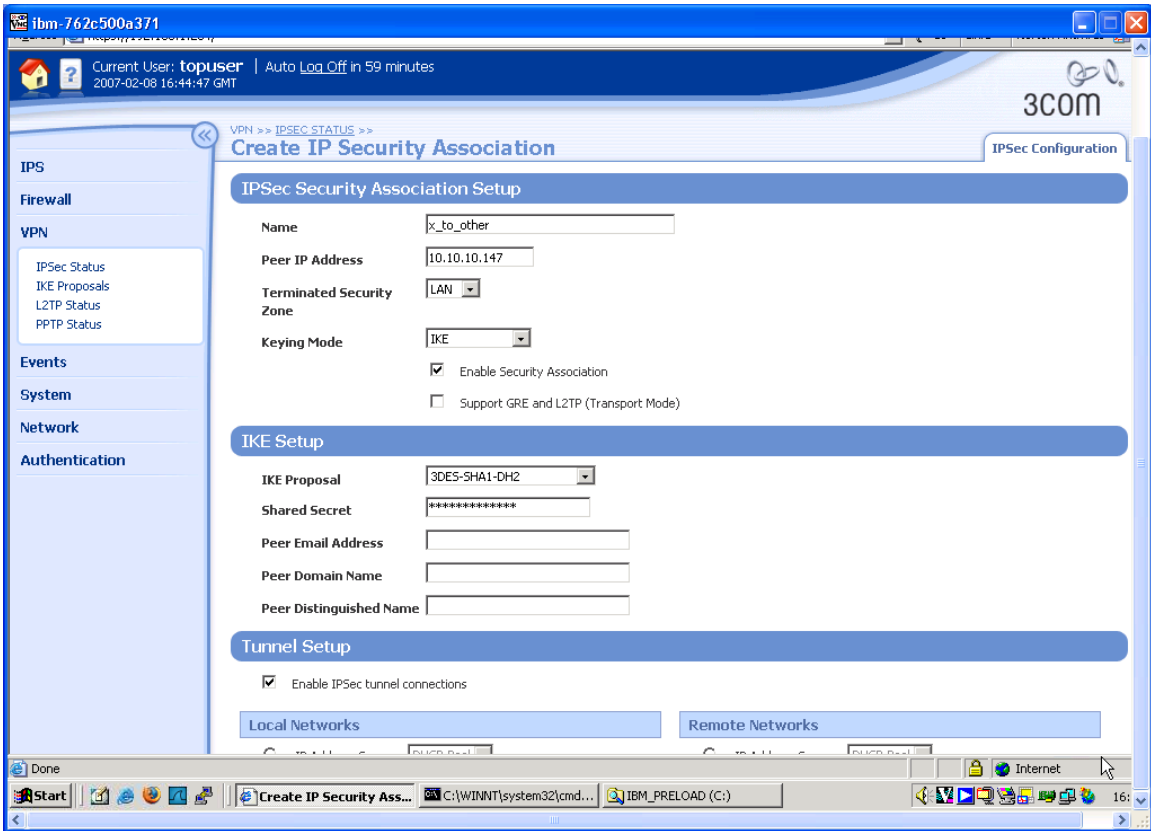
- Proposal Name: 3DES-SHA1-DH2
- Encryption: 3DES-CBC
- Integrity: SHA-1
- Diffie-Hellman Group: 2 (1024 bits)
- Lifetime: 28800 seconds
- Authentication Type: Pre-Shared Key
- Options:
  - Enable Aggressive Mode
  - Enable NAT Traversal
  - Enable Dead Peer Detection
  - Automatically connect on system start-up
  - Delete Phase 2 SA when Phase 1 SA terminates

**IKE Phase 2 Setup**

- Encryption: ESP 3DES-CBC
- Integrity: ESP SHA-1-HMAC
- Lifetime: 3600 seconds
- Diffie-Hellman Group: 2 (1024 bits)
- Enable Perfect Forward Secrecy

3. Click "Create" to save the new IKE Proposal.
4. Navigate to VPN -> IPSEC Status and click on the "IPSEC Configuration" tab.
5. Click the Enable IPSEC Global VPNs checkbox and click the Apply button.
6. On the IPSEC Configuration screen you will see one Security Association called "Default" displayed but we will not be using this as it is mainly used with IPsec clients on remote PCs, so click the Create IPsec Association button to create a new Security Association. Complete the form that opens as shown below – there are two screen grabs because the form is too large to fit in a single screen. Note also that the "Shared Secret" string entered here must be at least 8 characters and must be exactly the same as the shared secret entered on the peer device.





7. Click "Create" to save the new Security Association.

## 4.2 SonicWall PRO 2040 Configuration

1. Open a browser on PC2, connect to <https://192.168.22.254> and login to the SonicWall GUI.
2. Click on "VPN" to open up the submenu.
3. Click on "Settings" in the submenu and click on the checkbox "Enable VPNs" to check it.
4. On the same screen, under VPN Policies, click the "Add" button and complete the forms provided as shown below. Use the tabs at the top of the screen to move from the "General" page to the "Network", "Proposals" and "Advanced" pages in turn. Note that the "Shared Secret" string entered here must be at least 8 characters and must be exactly the same as the shared secret entered on the peer device.

https://192.168.22.254 - VPN Policy - Mozilla Firefox

General Network Proposals Advanced

### Security Policy

Authentication Method: IKE using Preshared Secret

Name: X-family\_to\_SonicWALL

IPsec Primary Gateway Name or Address: 10.10.20.147

IPsec Secondary Gateway Name or Address:

### IKE Authentication

Shared Secret: \*

Confirm Shared Secret: \*  Mask Shared Secret

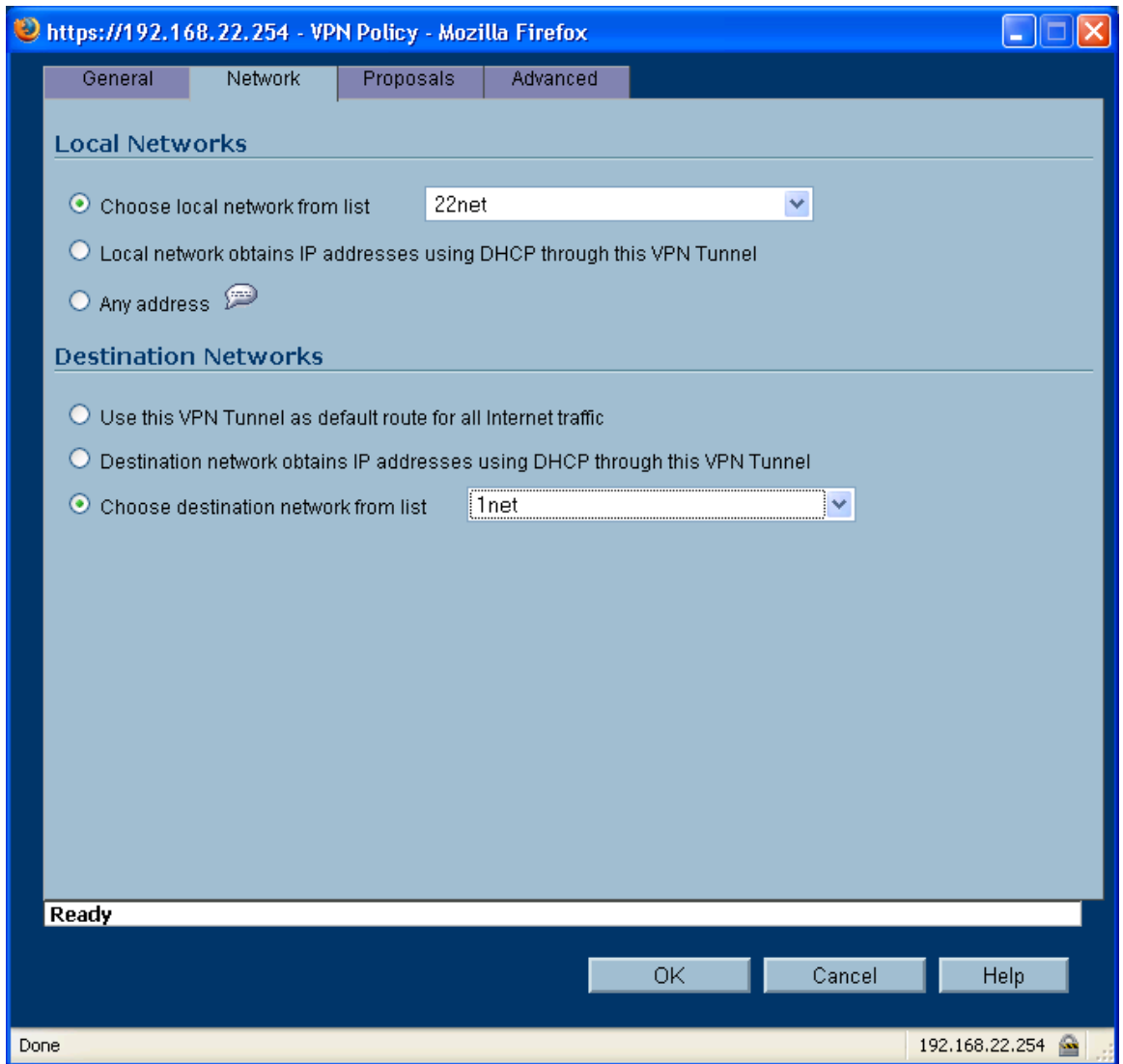
Local IKE ID: IP Address 10.10.10.147

Peer IKE ID: IP Address 10.10.20.147

Ready

OK Cancel Help

Done 192.168.22.254



The screenshot shows a web browser window titled "https://192.168.22.254 - VPN Policy - Mozilla Firefox". The browser displays the configuration page for a VPN policy, with the "Advanced" tab selected. The page is divided into two main sections: "IKE (Phase 1) Proposal" and "Ipsec (Phase 2) Proposal".

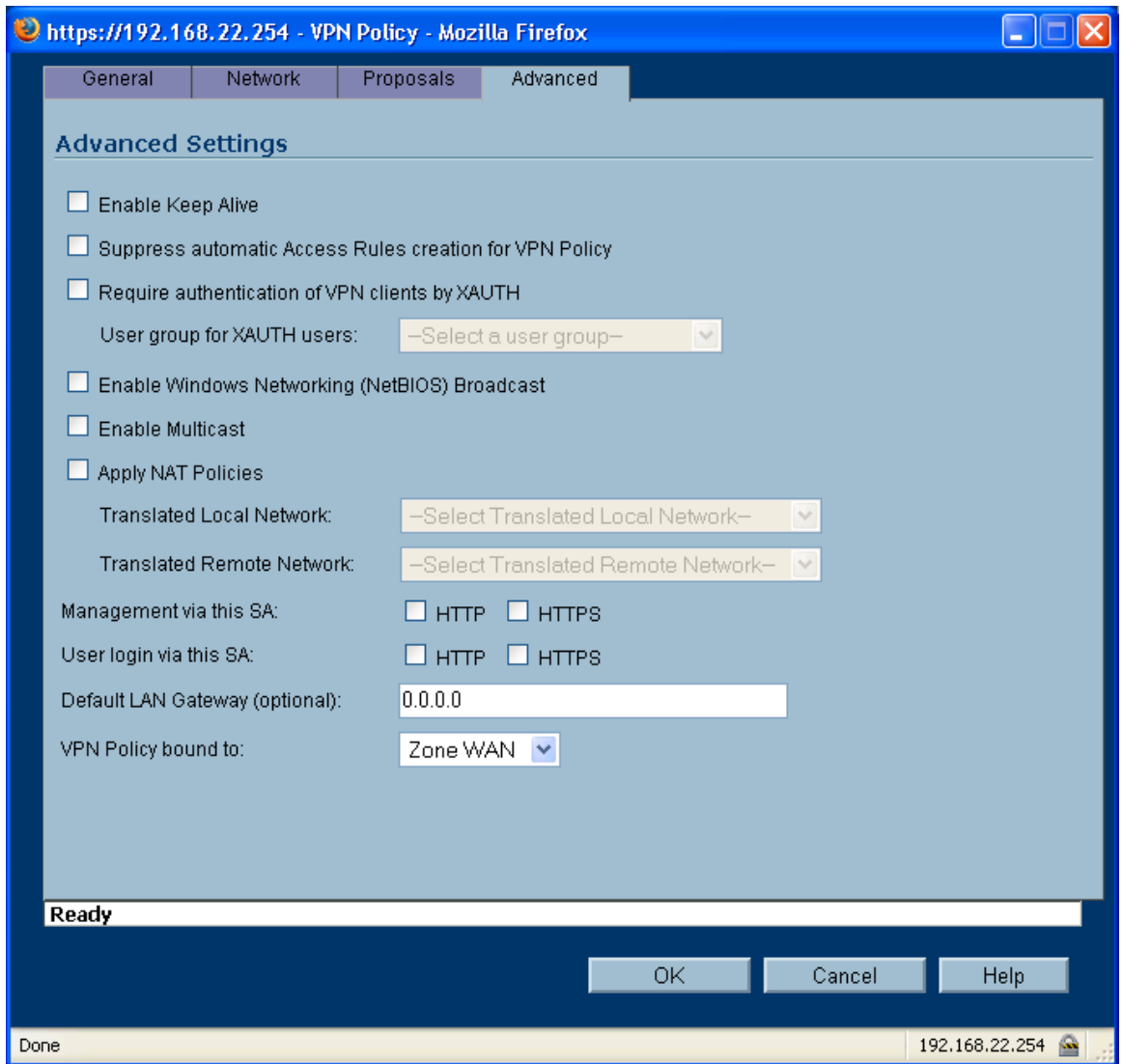
**IKE (Phase 1) Proposal**

- Exchange: Main Mode
- DH Group: Group 2
- Encryption: 3DES
- Authentication: SHA1
- Life Time (seconds): 28800

**Ipsec (Phase 2) Proposal**

- Protocol: ESP
- Encryption: 3DES
- Authentication: SHA1
- Enable Perfect Forward Secrecy
- DH Group: Group 2
- Life Time (seconds): 28800

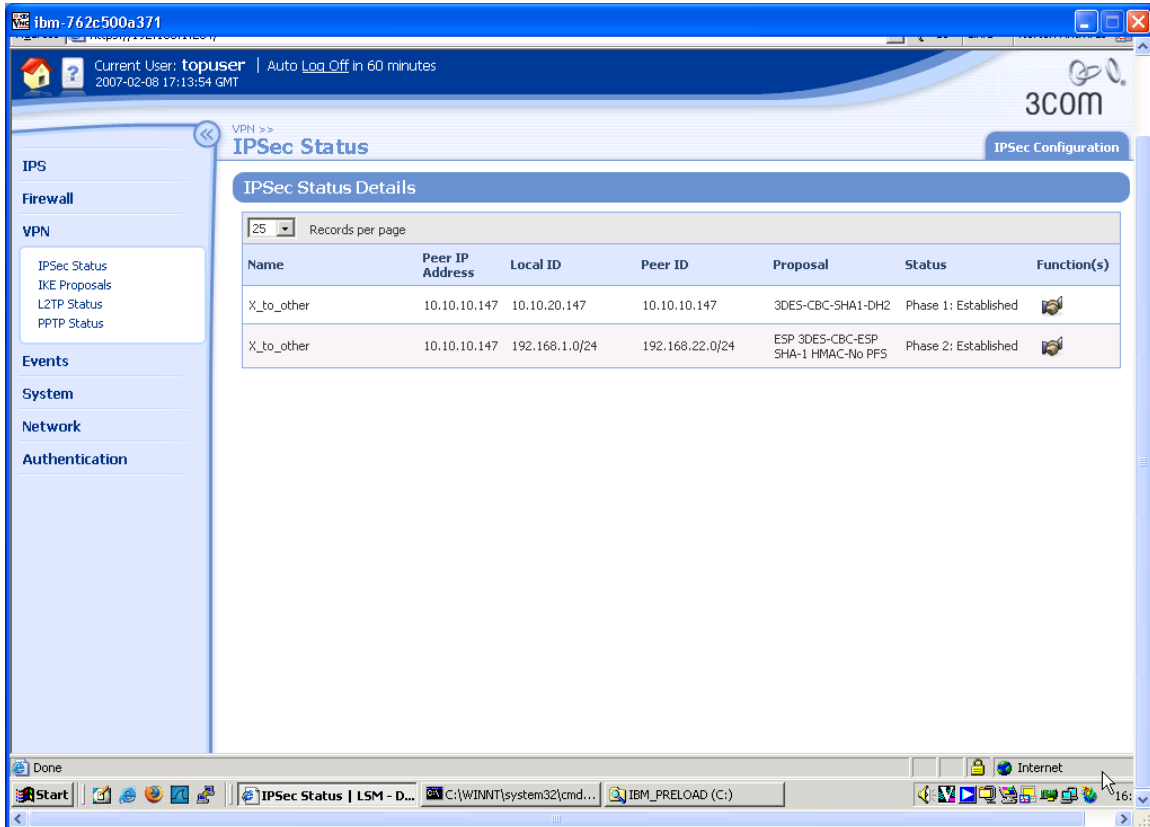
At the bottom of the configuration area, there is a "Ready" status bar. Below the configuration area are three buttons: "OK", "Cancel", and "Help". The browser's status bar at the very bottom shows "Done" on the left and "192.168.22.254" on the right.



5. Click on "OK" to save the new VPN Policy.

## 4.3 Testing the VPN with data

1. Ping from PC1 to PC2 - this will bring up the tunnel which should look like this on the IPSec Status screen of the X-family. One or two pings may be lost while the tunnel establishes but then all subsequent pings should be successful.



The screenshot displays the SonicWall management interface for an X-family device. The main content area is titled "IPSec Status" and shows a table of active VPN tunnels. The table has the following columns: Name, Peer IP Address, Local ID, Peer ID, Proposal, Status, and Function(s). Two tunnels are listed, both with a status of "Phase 2: Established".

Name	Peer IP Address	Local ID	Peer ID	Proposal	Status	Function(s)
X_to_other	10.10.10.147	10.10.20.147	10.10.10.147	3DES-CBC-SHA1-DH2	Phase 1: Established	
X_to_other	10.10.10.147	192.168.1.0/24	192.168.22.0/24	ESP 3DES-CBC-ESP SHA-1 HMAC-No PFS	Phase 2: Established	

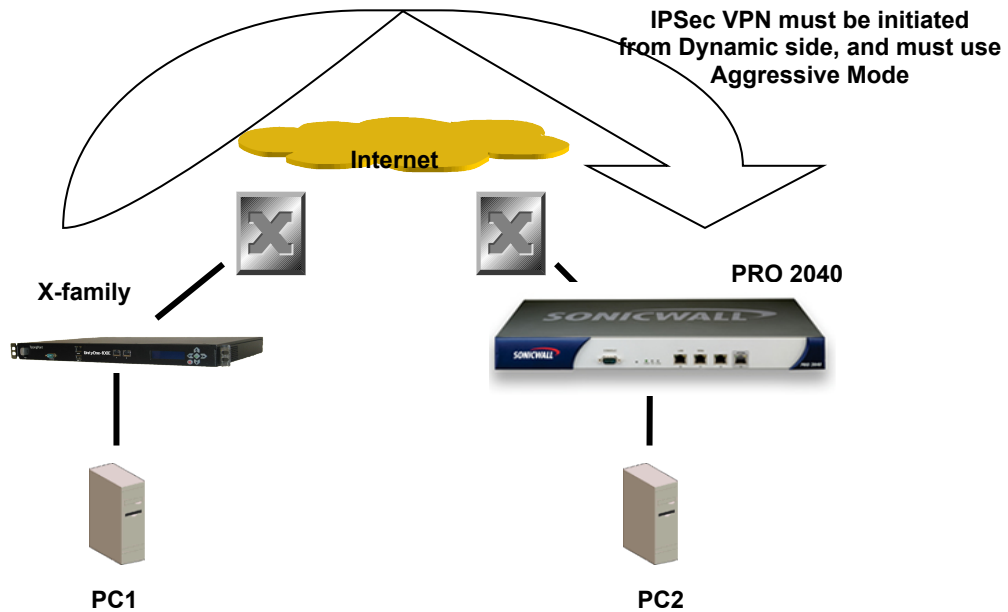
## 5 Aggressive Mode Tunnel

This example shows how to configure an IPsec tunnel using Aggressive Mode between the 3Com X-family and a SonicWall PRO 2040. Aggressive Mode must be used when one side of the VPN tunnel has a variable (dynamic) WAN IP address. While Aggressive Mode can be used even if both sides have a Static WAN IP address, Main Mode is recommended as the tunnel will be more secure.

The X-family receives a dynamic IP address (through PPPoE, PPTP, DHCP or L2TP) from the Internet Service Provider. The X-family must initiate the VPN back to the SonicWall, and the tunnel must use Aggressive Mode IKE.

### Key Setup Information

Keying Mode	IKE
IKE Mode	Aggressive Mode with Perfect Forward Secrecy
SA Authentication Method	Pre-shared Key
Keying Group DH	DH (Diffie Hellman) Group 2
Encryption and Data Integrity	3DES-SHA1



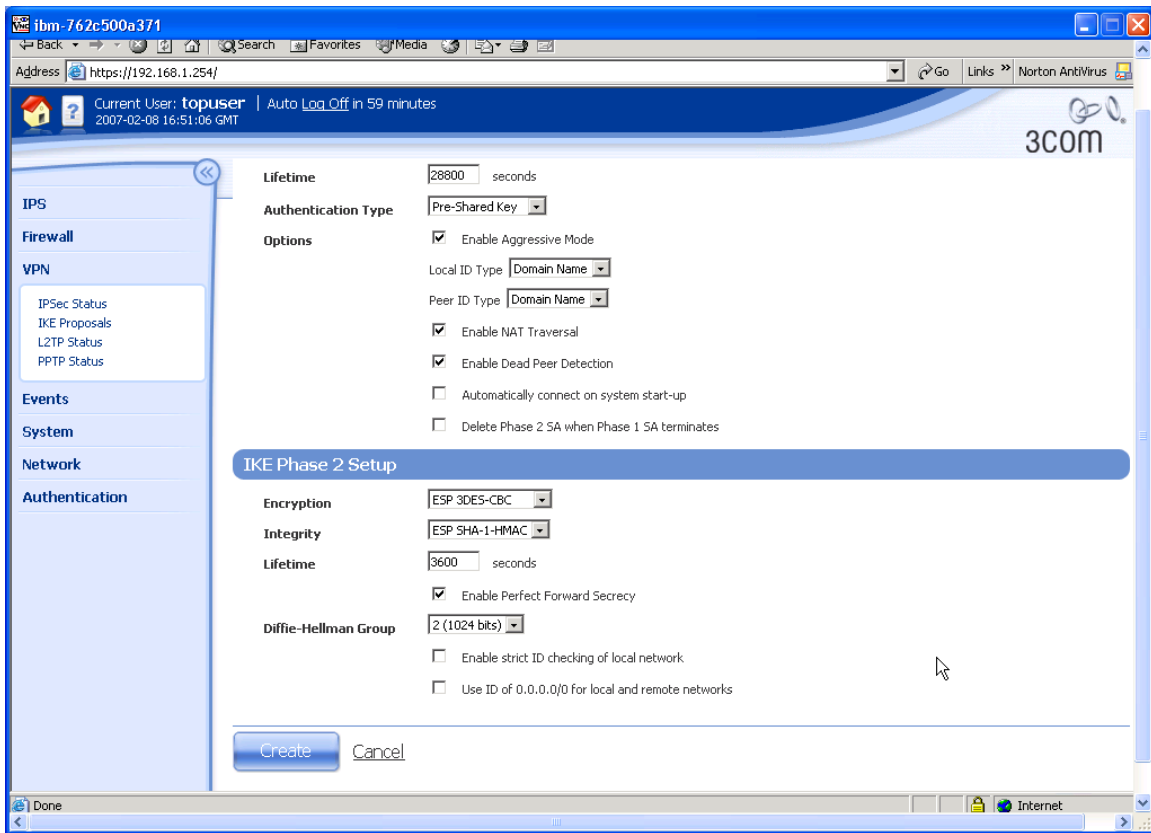
## 5.1 3Com X-family Configuration

1. Open a browser on PC1, connect to <https://192.168.1.254> and login as the user you set up during the OBE.
2. Navigate to VPN -> IKE Proposals. You will see one default proposal for DES-SHA1-PSK but we do not want to use this as it does not provide a suitably high level of security so click on the "Create IKE Proposal" button to create a new proposal. Complete the form that opens as shown below. (There are two screen grabs because the setup page is too large for a single screen).

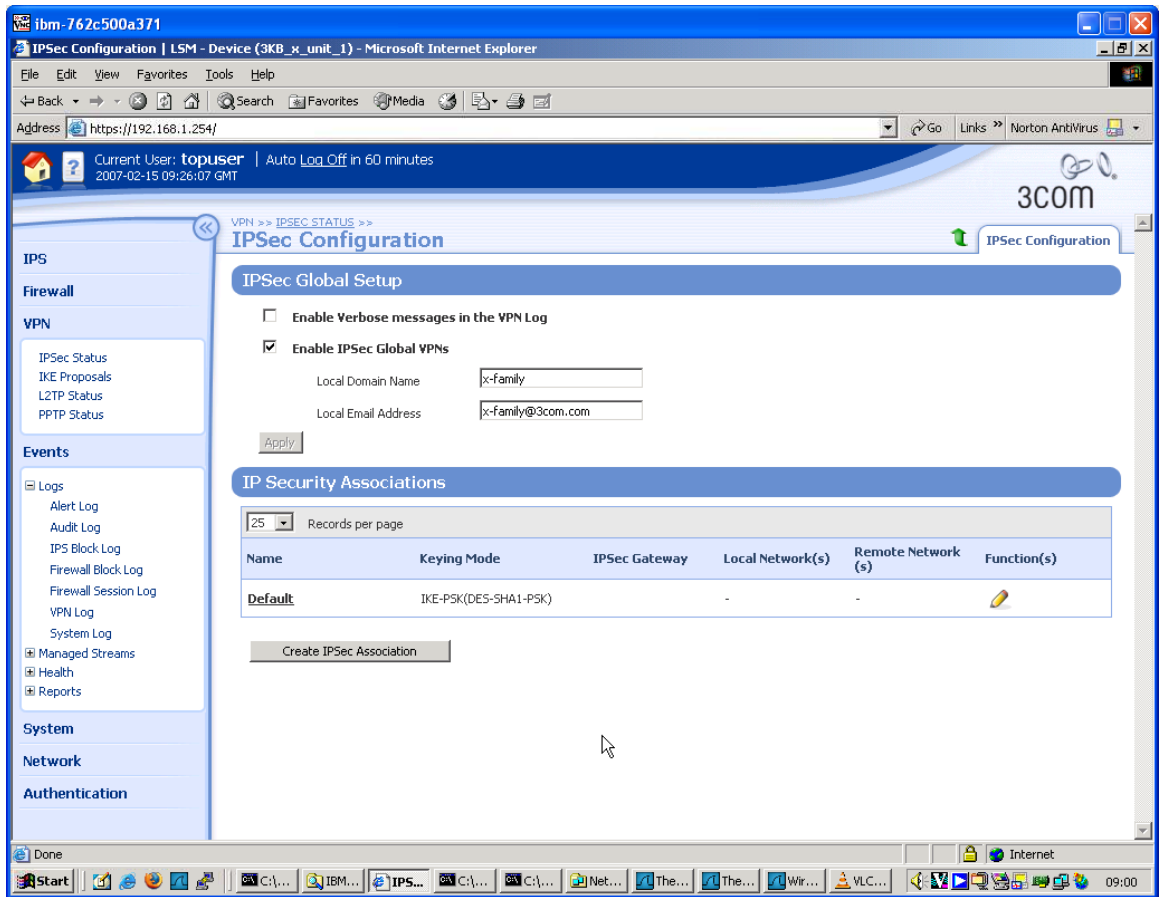
The screenshot displays the SonicWall web interface for configuring an IKE proposal. The browser window title is 'IBM-762c500a371' and the address bar shows 'https://192.168.1.254/'. The user is logged in as 'topuser' with an auto-logout timer of 58 minutes. The page title is 'Create IKE Proposal' under the 'VPN' menu. The configuration is split into two sections:

- IKE Phase 1 Setup:**
  - Proposal Name: 3DES-SHA1-DH2-AGG-PFS
  - Encryption: 3DES-CBC
  - Integrity: SHA-1
  - Diffie-Hellman Group: 2 (1024 bits)
  - Lifetime: 28800 seconds
  - Authentication Type: Pre-Shared Key
  - Options:
    - Enable Aggressive Mode
    - Local ID Type: Domain Name
    - Peer ID Type: Domain Name
    - Enable NAT Traversal
    - Enable Dead Peer Detection
    - Automatically connect on system start-up
    - Delete Phase 2 SA when Phase 1 SA terminates
- IKE Phase 2 Setup:**
  - Encryption: ESP 3DES-CBC
  - Integrity: ESP SHA-1-HMAC
  - Lifetime: 3600 seconds

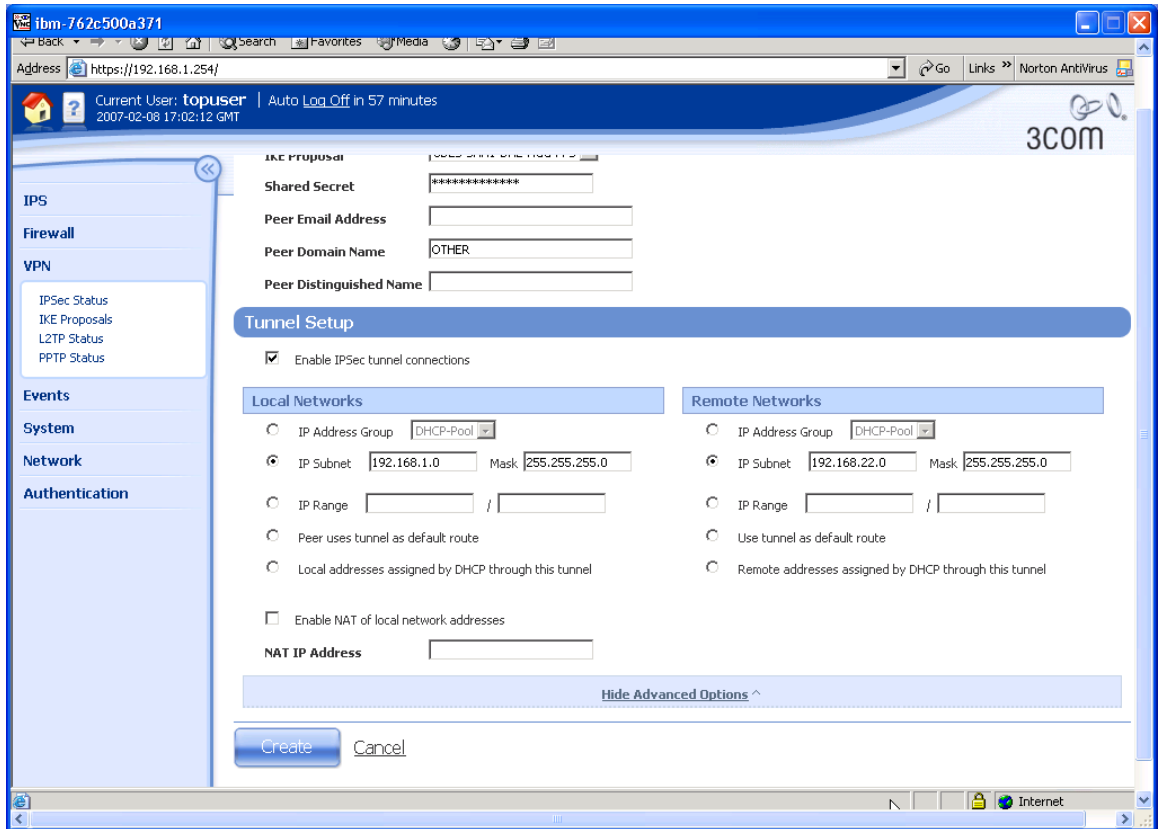
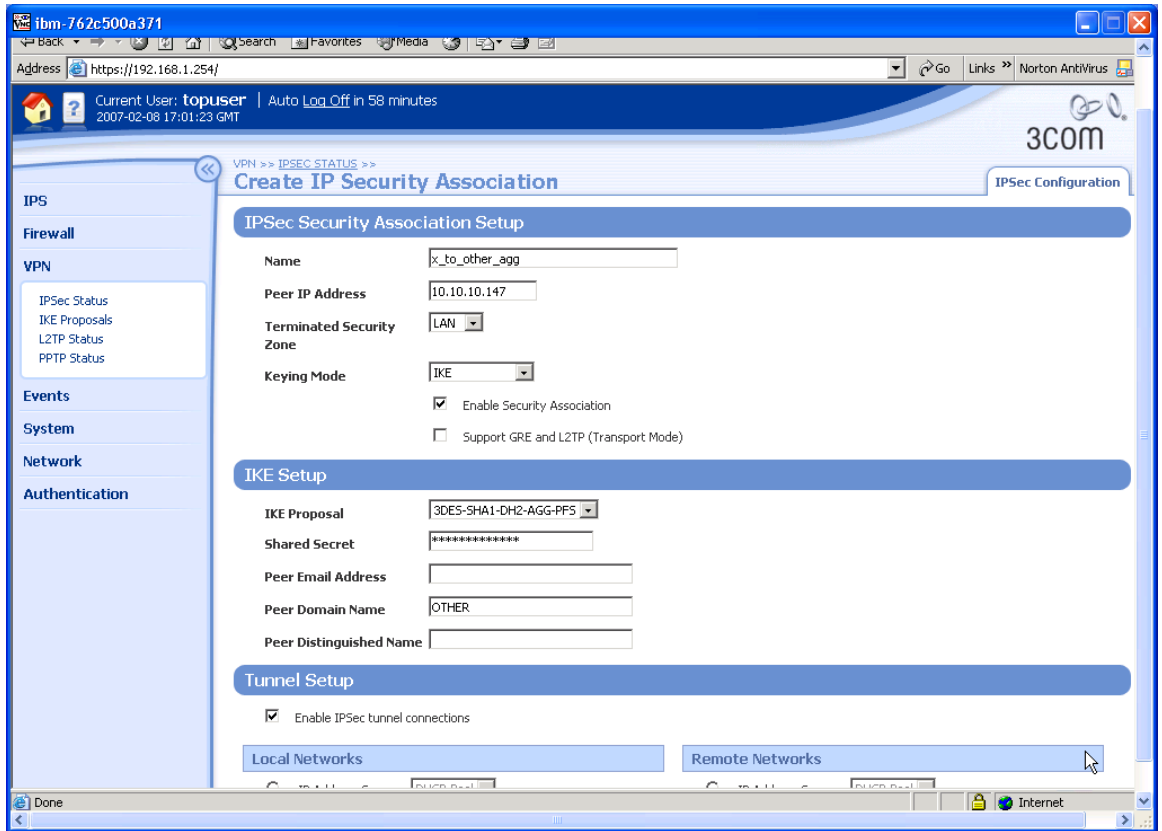




3. Click "Create" to save the new IKE Proposal.
4. Navigate to VPN -> IPSEC Status and click on the "IPSEC Configuration" tab.
5. Configure the upper part of the screen as shown below.



6. Click the Apply button to save the changes.
7. On the IPSEC Configuration screen you will see one Security Association called "Default" displayed but we will not be using this as it is mainly used with IPsec clients on remote PCs, so click the Create IPsec Association button to create a new Security Association. Complete the form that opens as shown below – there are two screen grabs because the form is too large to fit in a single screen. Note that the "Shared Secret" string entered here must be at least 8 characters and must be exactly the same as the shared secret entered on the peer device.



8. Click "Create" to create the Security Association.

## 5.2 SonicWall PRO 2040 Configuration

1. Open a browser on PC2, connect to <https://192.168.22.254> and login to the SonicWall GUI.
2. Click on "VPN" to open up the submenu.
3. Click on "Settings" in the submenu and click on the checkbox "Enable VPNs" to check it.
4. On the same screen, under VPN Policies, click the "Add" button and complete the forms provided as shown below. Use the tabs at the top of the screen to move from the "General" page to the "Network", "Proposals" and "Advanced" pages in turn. Note that the peer IP address is set to 0.0.0.0 because we do not know what it will be as it is a dynamic IP address allocated via DHCP, PPPoE etc. Note also that the "Shared Secret" string entered here must be at least 8 characters and must be exactly the same as the shared secret entered on the peer device.

https://192.168.22.254 - VPN Policy - Mozilla Firefox

General Network Proposals Advanced

**Security Policy**

Authentication Method: IKE using Preshared Secret

Name: X-family\_to\_SonicWall

IPsec Primary Gateway Name or Address: 0.0.0.0

IPsec Secondary Gateway Name or Address: 0.0.0.0

Shared Secret: shared-secret

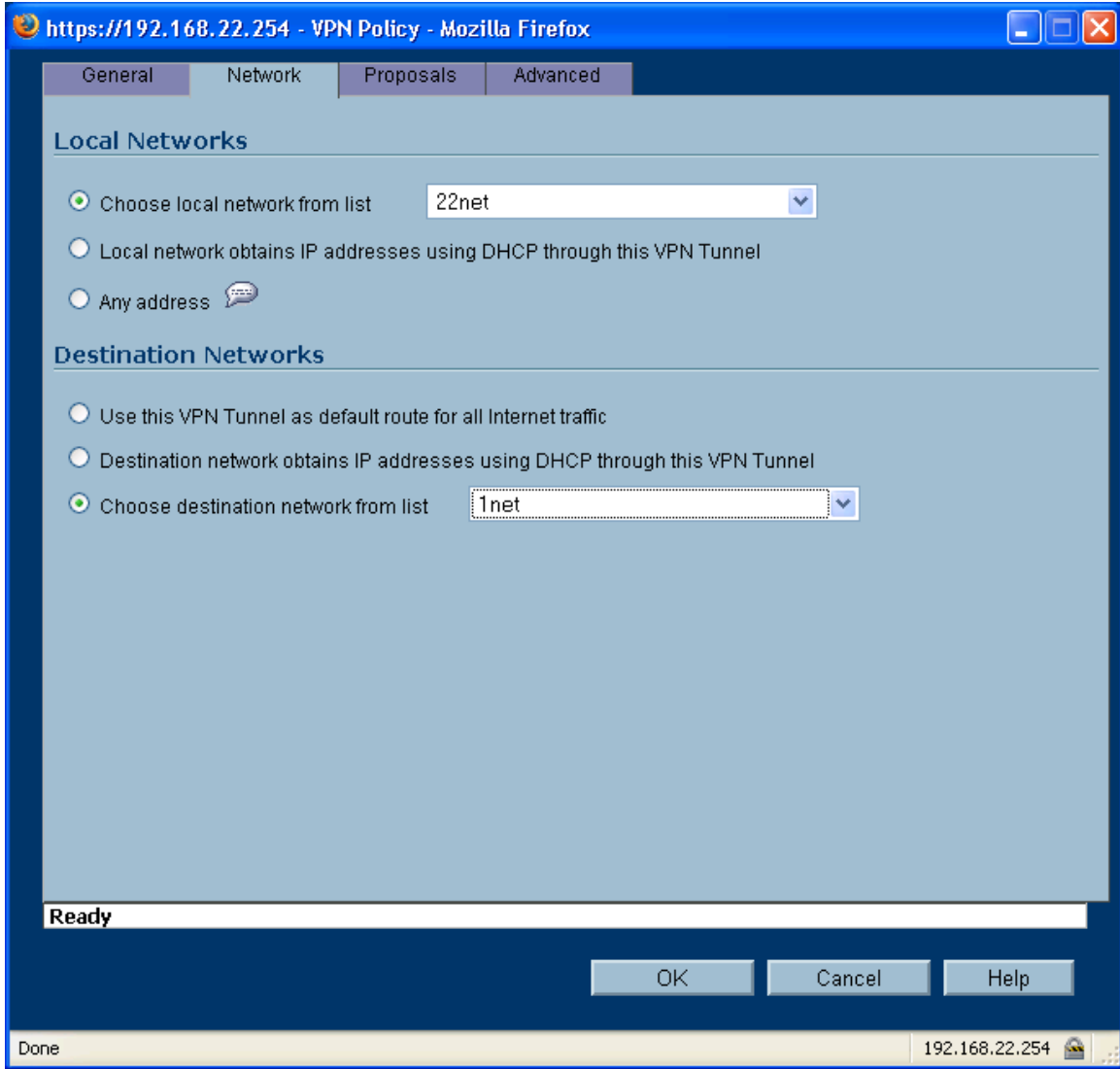
Local IKE ID: Domain Name OTHER

Peer IKE ID (optional): Domain Name x-family

Ready

OK Cancel Help

Done 192.168.22.254



The screenshot shows a web browser window titled "https://192.168.22.254 - VPN Policy - Mozilla Firefox". The browser window contains a configuration interface for a VPN policy. The interface has four tabs: "General", "Network", "Proposals", and "Advanced". The "Advanced" tab is selected. The configuration is divided into two sections: "IKE (Phase 1) Proposal" and "Ipsec (Phase 2) Proposal".

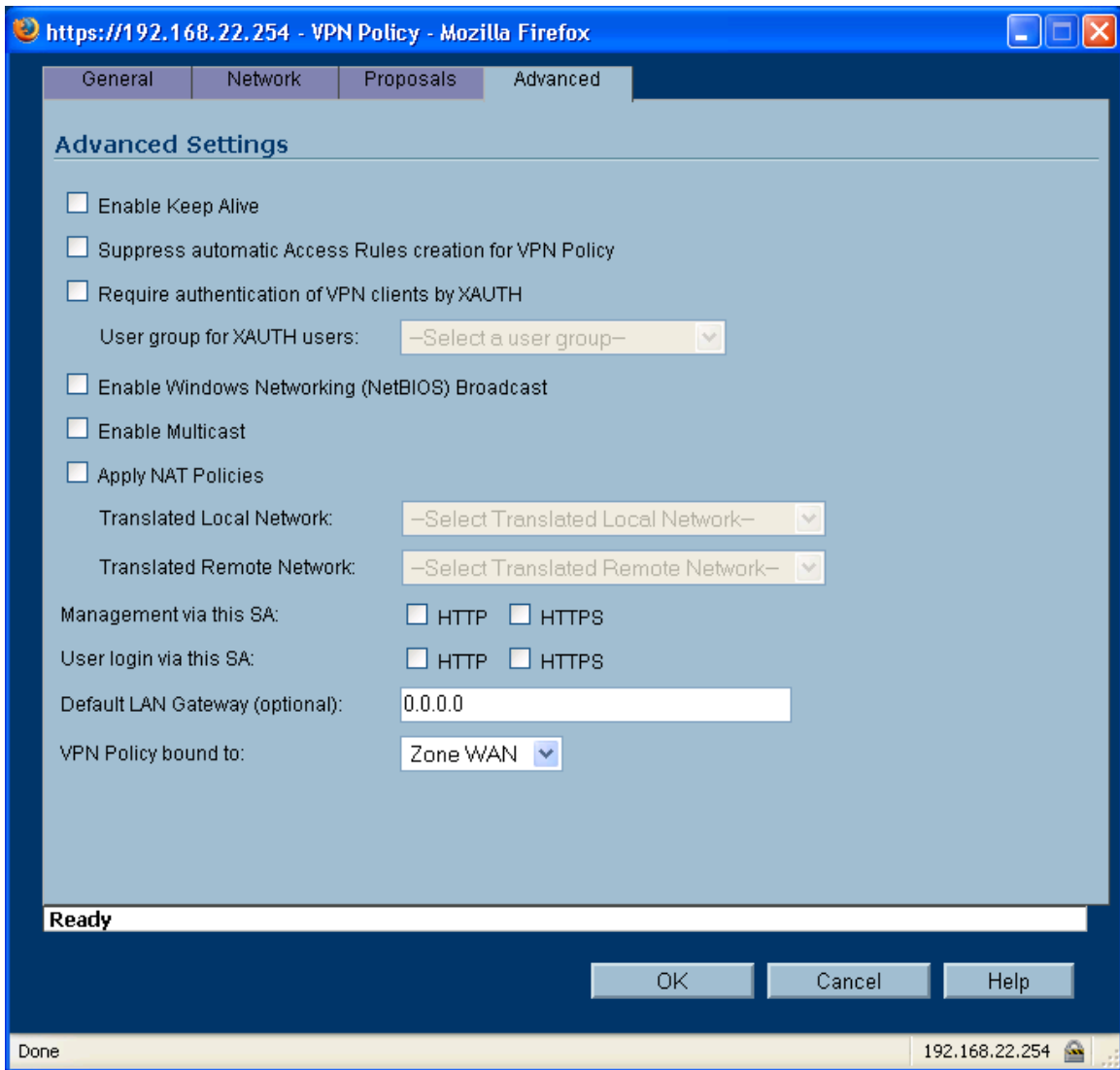
**IKE (Phase 1) Proposal**

- Exchange: Aggressive Mode
- DH Group: Group 2
- Encryption: 3DES
- Authentication: SHA1
- Life Time (seconds): 28800

**Ipsec (Phase 2) Proposal**

- Protocol: ESP
- Encryption: 3DES
- Authentication: SHA1
- Enable Perfect Forward Secrecy
- DH Group: Group 2
- Life Time (seconds): 28800

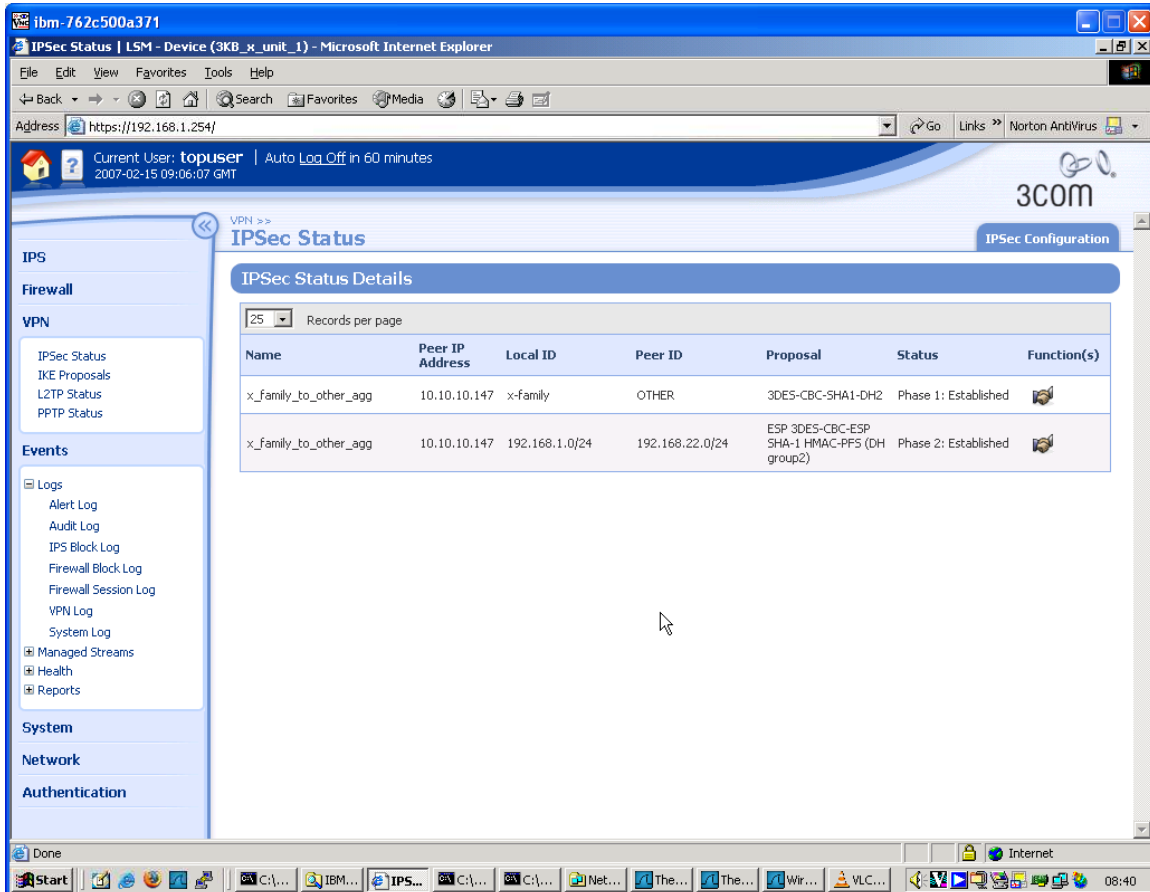
At the bottom of the configuration area, there is a status bar that says "Ready". Below the status bar are three buttons: "OK", "Cancel", and "Help". The browser's status bar at the very bottom shows "Done" on the left and "192.168.22.254" on the right.



5. Click on "OK" to save the new VPN Policy.

## 5.3 Testing the VPN with data

- Ping from PC1 to PC2 - this will bring up the tunnel which should look like this on the IPSec Status screen of the X-family. One or two pings may be lost while the tunnel establishes but then all subsequent pings should be successful. N.B. The direction of the initial ping (PC1 to PC2) is important as the X-family must be the initiator. This is because the IP address of the X-family is not known to the SonicWall.



The screenshot shows the SonicWall management interface in a Microsoft Internet Explorer browser window. The page title is "IPSec Status" and the URL is "https://192.168.1.254/". The user is logged in as "topuser". The interface displays the "IPSec Status Details" section, which contains a table with two rows of established VPN tunnels. The table has columns for Name, Peer IP Address, Local ID, Peer ID, Proposal, Status, and Function(s).

Name	Peer IP Address	Local ID	Peer ID	Proposal	Status	Function(s)
x_family_to_other_agg	10.10.10.147	x-family	OTHER	3DES-CBC-SHA1-DH2	Phase 1: Established	
x_family_to_other_agg	10.10.10.147	192.168.1.0/24	192.168.22.0/24	ESP 3DES-CBC-ESP SHA-1 HMAC-PFS (DH group2)	Phase 2: Established	



## 6 Appendix – Configuration Files

Here are textual configuration files for both devices for reference purposes.

### 6.1 Main Mode

#### 6.1.1 "show conf" file for X-family

```
3KB_X_unit_1# show conf
interface ethernet 3 1
    negotiate
    duplex full
    linespeed 100
    no shutdown
    exit
interface ethernet 3 2
    negotiate
    duplex full
    linespeed 100
    no shutdown
    exit
interface ethernet 3 3
    negotiate
    duplex full
    linespeed 100
    no shutdown
    exit
interface ethernet 3 4
    negotiate
    duplex full
    linespeed 100
    no shutdown
    exit
interface ethernet 3 5
    negotiate
    duplex full
    linespeed 100
    no shutdown
    exit
interface ethernet 3 6
    negotiate
    duplex full
    linespeed 100
    no shutdown
    exit
interface settings poll-interval 2000
interface settings detect-mdi enable
interface settings mdi-mode mdix
host name "3KB_X_unit_1"
host location "Lab"
host ip-filter permit any icmp
host ip-filter permit any ip
no autody
user options max-attempts 5
user options expire-period 90
user options expire-action expire
```

```
user options lockout-period 5
user options attempt-action lockout
user options security-level 2
high-availability disable
high-availability heartbeat 4 100 2
high-availability id 4098
clock timezone GMT
clock dst
log audit select general
log audit select login
log audit select logout
log audit select user
log audit select time
log audit select policy
log audit select update
log audit select boot
log audit select report
log audit select host
log audit select configuration
log audit select oam
log audit select sms
log audit select server
log audit select segment
log audit select high-availability
log audit select monitor
log audit select ip-filter
log audit select conn-table
log audit select host-communication
log audit select tse
category-settings -profile "Default Security Profile" vulnerabilities
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" exploits
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" security-policy
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" reconnaissance
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" virus
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" spyware
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" identity-theft
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" traffic-normal
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" network-equipment
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" p2p
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" im
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" streaming-media
enable - action-set "Recommended"
notify-contact "Management Console" 1
notify-contact "Remote System Log" 1
default-alert-sink period 1
server ssh
server no http
```

```
server https
server browser-check
monitor threshold memory      -major  90 -critical  95
monitor threshold disk        -major  90 -critical  95
monitor threshold temperature -major  92 -critical  94
monitor disable power-supply
no service-access
tse adaptive-filter mode automatic
tse afc-severity warning
tse connection-table timeout 1800
tse logging-mode conditional -threshold 1.0 -period 600
tse quarantine duration 60
email-rate-limit 10
zone update LAN vlan-id 1
zone update LAN port 3/1
zone update LAN mtu 1500
zone update LAN addresses disable
zone update LAN vpn-tunnel-access enable
zone update VPN vlan-id 4
zone update VPN port none
zone update VPN mtu 1500
zone update VPN addresses disable
zone update VPN vpn-tunnel-access enable
zone update WAN vlan-id 3
zone update WAN port 3/6
zone update WAN mtu 1500
zone update WAN addresses disable
zone update WAN vpn-tunnel-access enable
address-groups update DHCP-Pool range 192.168.1.1 192.168.1.20
authentication privilege-groups update Allow_VPN_access vpn-client-
access
authentication privilege-groups update RADIUS
authentication radius default-privilege-group RADIUS
authentication radius server primary 0.0.0.0 port 1812 shared-secret
***** au
th-method chap
authentication radius server secondary none
authentication radius disable
authentication radius user-authentication enable
authentication radius vpn-clients enable
authentication radius retries 3
authentication radius timeout 2
web-filtering default-rule block
web-filtering filter-action block-and-log
web-filtering filter-service cache expiry 24
web-filtering filter-service cache size 2097152
web-filtering filter-service block adult
web-filtering filter-service block gambling
web-filtering filter-service block violence
web-filtering filter-service block criminal
web-filtering filter-service block hacking
web-filtering filter-service block weapons
web-filtering filter-service block drugs
web-filtering filter-service block hate
web-filtering filter-service permit advertisement
web-filtering filter-service permit computing
web-filtering filter-service permit food
web-filtering filter-service permit politics
```

```
web-filtering filter-service permit hosting
web-filtering filter-service permit lifestyle
web-filtering filter-service permit dating
web-filtering filter-service permit reference
web-filtering filter-service permit sex-education
web-filtering filter-service permit sports
web-filtering filter-service permit usenet
web-filtering filter-service permit arts
web-filtering filter-service permit education
web-filtering filter-service permit games
web-filtering filter-service permit health
web-filtering filter-service permit careers
web-filtering filter-service permit vehicles
web-filtering filter-service permit photos
web-filtering filter-service permit religion
web-filtering filter-service permit search
web-filtering filter-service permit streaming-media
web-filtering filter-service permit email
web-filtering filter-service permit chat
web-filtering filter-service permit finance
web-filtering filter-service permit glamour
web-filtering filter-service permit hobbies
web-filtering filter-service permit kids
web-filtering filter-service permit news
web-filtering filter-service permit real-estate
web-filtering filter-service permit proxies
web-filtering filter-service permit shopping
web-filtering filter-service permit travel
web-filtering filter-service disable
web-filtering manual-filter disable
dhcp-server addresses group DHCP-Pool
dhcp-server enable
dhcp-server bootp disable
dhcp-server lease-duration 60
dhcp-server dns default
dhcp-server wins primary 0.0.0.0
dhcp-server wins secondary 0.0.0.0
dhcp-server nbx 0.0.0.0
dhcp-server relay disable
dns use-external-dns enable
interface virtual add 1 internal
interface virtual internal 1 ip 192.168.1.254 netmask 255.255.255.0
interface virtual internal 1 ha-mgmt-ip 0.0.0.0
interface virtual internal 1 nat external-ip
interface virtual internal 1 rip disable
interface virtual internal 1 rip send-mode v2-multicast
interface virtual internal 1 rip receive-mode all
interface virtual internal 1 rip auth disable
interface virtual internal 1 rip split-horizon enable
interface virtual internal 1 rip poison-reverse enable
interface virtual internal 1 rip advertise-routes enable
interface virtual internal 1 igmp disable
interface virtual internal 1 pim-dm disable
interface virtual internal 1 zone add LAN
interface virtual internal 1 zone add VPN
interface virtual add 2 external
interface virtual external 2 type static 10.10.20.147 netmask
255.255.255.0
```

```
interface virtual external 2 ha-mgmt-ip 0.0.0.0
interface virtual external 2 rip disable
interface virtual external 2 rip send-mode disable
interface virtual external 2 rip receive-mode disable
interface virtual external 2 rip auth disable
interface virtual external 2 rip split-horizon disable
interface virtual external 2 rip poison-reverse disable
interface virtual external 2 rip advertise-routes disable
interface virtual external 2 igmp disable
interface virtual external 2 pim-dm disable
interface virtual external 2 zone add WAN
firewall schedule update working-day days -mtwtf- from 0800 to 1800
firewall service update 3com-nbx udp port 2093 to 2096
firewall service update audio-call-control tcp port 1731
firewall service update dhcp-client udp port 68
firewall service update dhcp-server udp port 67
firewall service update dns-tcp tcp port 53
firewall service update dns-udp udp port 53
firewall service update finger-tcp tcp port 79
firewall service update ftp tcp port 21
firewall service update gopher-tcp tcp port 70
firewall service update gre gre
firewall service update h323 tcp port 1720
firewall service update http tcp port 80
firewall service update https tcp port 443
firewall service update igmp igmp
firewall service update ike udp port 500
firewall service update imap tcp port 143
firewall service update imapv3 tcp port 220
firewall service update ipsec-ah ah
firewall service update ipsec-esp esp
firewall service update kerberos-tcp tcp port 88
firewall service update kerberos-udp udp port 88
firewall service update l2tp udp port 1701
firewall service update ldap-tcp tcp port 389
firewall service update ldap-udp udp port 389
firewall service update lotus-notes-domino tcp port 1352
firewall service update lpr tcp port 515
firewall service update nat-t-ipsec udp port 4500
firewall service update nbname tcp port 137
firewall service update netbios-tcp tcp port 137 to 139
firewall service update netbios-udp udp port 137 to 139
firewall service update netmeeting tcp port 1720
firewall service update nfsd-tcp tcp port 2049
firewall service update nfsd-udp udp port 2049
firewall service update nntp tcp port 119
firewall service update ntp udp port 123
firewall service update pim-dm pim
firewall service update ping icmp port 8
firewall service update pop3 tcp port 110
firewall service update portmapper-tcp tcp port 111
firewall service update portmapper-udp udp port 111
firewall service update pptp-tcp tcp port 1723
firewall service update radius-accounting udp port 1813
firewall service update radius-auth udp port 1812
firewall service update rexec tcp port 512
firewall service update rip udp port 520
firewall service update rlogin tcp port 513
```

```
firewall service update rsh tcp port 514
firewall service update rtsp tcp port 554
firewall service update sip-tcp tcp port 5060
firewall service update sip-udp udp port 5060
firewall service update smb tcp port 445
firewall service update sms-client tcp port 10042
firewall service update sms-trap tcp port 8162 to 8163
firewall service update smtp tcp port 25
firewall service update snmp-request udp port 161
firewall service update snmp-trap udp port 162
firewall service update ssh tcp port 22
firewall service update syslog udp port 514
firewall service update t120 tcp port 1503
firewall service update telnet tcp port 23
firewall service update tftp udp port 69
firewall service update traceroute icmp port 8
firewall service update uucp udp port 540
firewall service update vnc-browser tcp port 5800
firewall service update vnc-viewer tcp port 5900
firewall service update x-windows tcp port 6000 to 6063
firewall service-group update dns dns-tcp dns-udp
firewall service-group update email pop3 smtp imap imapv3
firewall service-group update ipsec ike ipsec-ah ipsec-esp
firewall service-group update ldap ldap-udp ldap-tcp
firewall service-group update management https ssh ping snmp-request
firewall service-group update netmeeting h323 audio-call-control t120
firewall service-group update network-protocols dns-tcp dns-udp dhcp
server
firewall service-group update nfs portmapper-tcp portmapper-udp nfsd-tcp
nfsd-udp
firewall service-group update pptp pptp-tcp gre
firewall service-group update secure-management https ssh
firewall service-group update sip sip-tcp sip-udp
firewall service-group update sms-config http https sms-client snmp-
request ssh
firewall service-group update sms-get ntp sms-trap
firewall service-group update snmp snmp-request snmp-trap
firewall service-group update vnc vnc-browser vnc-viewer
firewall service-group update voice 3com-nbx sip-tcp sip-udp
firewall service-group update vpn-protocols pptp-tcp l2tp gre ike nat-t-
ipsec
firewall rule update 1 permit LAN WAN ANY
firewall rule update 1 schedule always timeout 30 logging disable
firewall rule update 1 src-addr all
firewall rule update 1 dst-addr all
firewall rule update 1 bandwidth disable
firewall rule update 1 authentication disable
firewall rule update 1 position 1
firewall rule update 1 comment "Allow LAN unrestricted access to WAN"
firewall rule update 1 remote-logging disable
firewall rule enable 1
firewall rule update 2 permit WAN this-device vpn-protocols
firewall rule update 2 schedule always timeout 30 logging disable
firewall rule update 2 src-addr all
firewall rule update 2 dst-addr all
firewall rule update 2 bandwidth disable
firewall rule update 2 authentication disable
firewall rule update 2 position 2
```

```
firewall rule update 2 comment "Allow VPN termination"
firewall rule update 2 remote-logging disable
firewall rule enable 2
firewall rule update 3 permit LAN this-device management
firewall rule update 3 schedule always timeout 30 logging disable
firewall rule update 3 src-addr all
firewall rule update 3 dst-addr all
firewall rule update 3 bandwidth disable
firewall rule update 3 authentication disable
firewall rule update 3 position 3
firewall rule update 3 comment "Allow management access from LAN"
firewall rule update 3 remote-logging disable
firewall rule enable 3
firewall rule update 4 permit LAN this-device network-protocols
firewall rule update 4 schedule always timeout 30 logging disable
firewall rule update 4 src-addr all
firewall rule update 4 dst-addr all
firewall rule update 4 bandwidth disable
firewall rule update 4 authentication disable
firewall rule update 4 position 4
firewall rule update 4 comment "Allow DNS and DHCP from LAN"
firewall rule update 4 remote-logging disable
firewall rule enable 4
firewall rule update 200 permit ANY ANY ANY
firewall rule update 200 schedule always timeout 30 logging disable
firewall rule update 200 src-addr all
firewall rule update 200 dst-addr all
firewall rule update 200 bandwidth disable
firewall rule update 200 authentication disable
firewall rule update 200 position 5
firewall rule update 200 comment ""
firewall rule update 200 remote-logging disable
firewall rule enable 200
firewall alg sip services ANY
firewall alg sip sdp-port-range ANY
routing rip disable update-timer 30
routing multicast igmp disable
routing multicast pim-dm disable query-interval 30 prune-timeout 180
vpn ike add DES-SHA1-PSK
vpn ike proposal DES-SHA1-PSK phase1-encryption des-cbc
vpn ike proposal DES-SHA1-PSK phase1-integrity sha1
vpn ike proposal DES-SHA1-PSK phase1-dh-group 1
vpn ike proposal DES-SHA1-PSK phase1-lifetime 28800
vpn ike proposal DES-SHA1-PSK auth-type psk
vpn ike proposal DES-SHA1-PSK aggressive-mode disable
vpn ike proposal DES-SHA1-PSK local-id-type ip
vpn ike proposal DES-SHA1-PSK peer-id-type ip
vpn ike proposal DES-SHA1-PSK ca-cert ANY
vpn ike proposal DES-SHA1-PSK nat-t disable
vpn ike proposal DES-SHA1-PSK dpd enable
vpn ike proposal DES-SHA1-PSK auto-connect disable
vpn ike proposal DES-SHA1-PSK tight-phase2-control enable
vpn ike proposal DES-SHA1-PSK phase2-encryption des-cbc
vpn ike proposal DES-SHA1-PSK phase2-integrity esp-sha1-hmac
vpn ike proposal DES-SHA1-PSK phase2-lifetime 3600
vpn ike proposal DES-SHA1-PSK pfs disable
vpn ike proposal DES-SHA1-PSK phase2-dh-group 1
vpn ike proposal DES-SHA1-PSK phase2-zero-id disable
```

```
vpn ike proposal DES-SHA1-PSK phase2-strict-id-check disable
vpn ike add 3DES-SHA1-DH2
vpn ike proposal 3DES-SHA1-DH2 phase1-encryption 3des-cbc
vpn ike proposal 3DES-SHA1-DH2 phase1-integrity sha1
vpn ike proposal 3DES-SHA1-DH2 phase1-dh-group 2
vpn ike proposal 3DES-SHA1-DH2 phase1-lifetime 28800
vpn ike proposal 3DES-SHA1-DH2 auth-type psk
vpn ike proposal 3DES-SHA1-DH2 aggressive-mode disable
vpn ike proposal 3DES-SHA1-DH2 local-id-type ip
vpn ike proposal 3DES-SHA1-DH2 peer-id-type ip
vpn ike proposal 3DES-SHA1-DH2 ca-cert ANY
vpn ike proposal 3DES-SHA1-DH2 nat-t enable
vpn ike proposal 3DES-SHA1-DH2 dpd enable
vpn ike proposal 3DES-SHA1-DH2 auto-connect disable
vpn ike proposal 3DES-SHA1-DH2 tight-phase2-control disable
vpn ike proposal 3DES-SHA1-DH2 phase2-encryption 3des-cbc
vpn ike proposal 3DES-SHA1-DH2 phase2-integrity esp-sha1-hmac
vpn ike proposal 3DES-SHA1-DH2 phase2-lifetime 3600
vpn ike proposal 3DES-SHA1-DH2 pfs disable
vpn ike proposal 3DES-SHA1-DH2 phase2-dh-group 2
vpn ike proposal 3DES-SHA1-DH2 phase2-zero-id disable
vpn ike proposal 3DES-SHA1-DH2 phase2-strict-id-check disable
vpn ipsec enable
vpn ipsec add Default
vpn ipsec sa Default disable
vpn ipsec sa Default key ike proposal DES-SHA1-PSK shared-secret
*****
vpn ipsec sa Default transport enable
vpn ipsec sa Default peer 0.0.0.0
vpn ipsec sa Default zone LAN
vpn ipsec sa Default tunnel enable
vpn ipsec add X_to_other
vpn ipsec sa X_to_other key ike proposal 3DES-SHA1-DH2 shared-secret
*****
vpn ipsec sa X_to_other transport disable
vpn ipsec sa X_to_other peer 10.10.10.147
vpn ipsec sa X_to_other zone LAN
vpn ipsec sa X_to_other tunnel remote subnet 192.168.22.0 netmask
255.255.255.0
vpn ipsec sa X_to_other tunnel local subnet 192.168.1.0 netmask
255.255.255.0
vpn ipsec sa X_to_other tunnel nat disable
vpn ipsec sa X_to_other tunnel enable
vpn ipsec sa X_to_other enable
vpn l2tp addresses none
vpn l2tp zone LAN
vpn l2tp dns relay
vpn l2tp encryption enable
vpn l2tp disable
vpn pptp addresses none
vpn pptp zone LAN
vpn pptp dns relay
vpn pptp encryption enable
vpn pptp disable
ntp peer
ntp server
ntp duration 5
ntp offset 1
```



```
ntp fast enable
ntp disable
ramdisk sync-interval sys 30
ramdisk sync-interval audit 30
ramdisk sync-interval block -1
ramdisk sync-interval alert -1
ramdisk sync-interval firewallsession -1
ramdisk sync-interval firewallblock -1
ramdisk sync-interval vpn -1
sms v2
sms no must-be-ip
no sms
sms no remote-deploy
session timeout 20 -persist
3KB_X_unit_1#
```

### 6.1.2 SonicWall PRO 2040 configuration file

There does not seem to be an easy way to dump the entire config as a text file – so here is the VPN configuration only.

```
PRO 2040 Enhanced> show vpn policy
```

```
Policy: WAN GroupVPN
Key Mode: Pre-shared
Pre Shared Secret: shared-secret
Proposals:
IKE: Aggressive Mode, 3DES SHA, DH Group 2, 28800 seconds
IPSEC: ESP, 3DES SHA, No PFS, 28800 seconds
Advanced:
Allow NetBIOS OFF, Allow Multicast OFF
Management: HTTP OFF, HTTPS OFF
Lan Default GW: 0.0.0.0
Require XAUTH: ON, User Group: Trusted Users
Client:
Cache XAUTH Settings: Never
Virtual Adapter Settings: None
Allow Connections To: Split Tunnels
Set Default Route OFF, Require GSC OFF
Use Default Key OFF
```

```
Policy: WLAN GroupVPN (Disabled)
Key Mode: Pre-shared
Pre Shared Secret: 391D190BD059C7DE
Proposals:
IKE: Aggressive Mode, 3DES SHA, DH Group 2, 28800 seconds
IPSEC: ESP, 3DES SHA, No PFS, 28800 seconds
Advanced:
Allow NetBIOS OFF, Allow Multicast OFF
Management: HTTP ON, HTTPS ON
Lan Default GW: 0.0.0.0
Require XAUTH: ON, User Group: Trusted Users
Client:
Cache XAUTH Settings: Single Session
Virtual Adapter Settings: None
Allow Connections To: All Secured Gateways
Set Default Route ON, Require GSC OFF
Use Default Key ON
```

```

Policy: X_unit_to_SonicWall
Key Mode: Pre-shared
Primary GW: 10.10.20.147
Secondary GW: 0.0.0.0
Pre Shared Secret: shared-secret
IKE ID:
Local: IP Address 10.10.10.147
Peer: IP Address 10.10.20.147
Network:
Local: 22netRemote: 1net
Proposals:
IKE: Main Mode, 3DES SHA, DH Group 2, 28800 seconds
IPSEC: ESP, 3DES SHA, No PFS, 28800 seconds
Advanced:
Keepalive OFF, Add Auto-Rule ON, Allow NetBIOS OFF
Allow Multicast OFF
Management: HTTP OFF, HTTPS OFF
User Login: HTTP OFF, HTTPS OFF
Lan Default GW: 0.0.0.0
Require XAUTH: OFF
Bound To: Zone WAN

```

```
PRO 2040 Enhanced> show vpn sa
```

```

Policy: X_unit_to_SonicWall
IKE SAs
GW: 10.10.10.147:500 --> 10.10.20.147:500
Main Mode, 3DES SHA, DH Group 2, Initiator
Cookie: 0x7fe9119c8276a968 (I), 0x23320c97b2370c4c (R)
Lifetime: 28800 seconds (28741 seconds remaining)

```

```

IPsec SAs
GW: 10.10.10.147:500 --> 10.10.20.147:500
(192.168.22.0 - 192.168.22.255) --> (192.168.1.0 - 192.168.1.255)
ESP, 3DES SHA, In SPI 0xc7cb44c2, Out SPI 0xe09a93f6
Lifetime: 28800 seconds (28740 seconds remaining)
PRO 2040 Enhanced>

```

## 6.2 Aggressive Mode

### 6.2.1 "show conf" file for X505

```

3KB_x_unit_1# show conf
interface ethernet 3 1
    negotiate
    duplex full
    linespeed 100
    no shutdown
    exit
interface ethernet 3 2
    negotiate
    duplex full
    linespeed 100
    no shutdown
    exit
interface ethernet 3 3

```

```
    negotiate
    duplex full
    linespeed 100
    no shutdown
    exit
interface ethernet 3 4
    negotiate
    duplex full
    linespeed 100
    no shutdown
    exit
interface ethernet 3 5
    negotiate
    duplex full
    linespeed 100
    no shutdown
    exit
interface ethernet 3 6
    negotiate
    duplex full
    linespeed 100
    no shutdown
    exit
interface settings poll-interval 2000
interface settings detect-mdi enable
interface settings mdi-mode mdix
host name "3KB_x_unit_1"
host location "Lab"
host ip-filter permit any icmp
host ip-filter permit any ip
no autodv
user options max-attempts 5
user options expire-period 90
user options expire-action expire
user options lockout-period 5
user options attempt-action lockout
user options security-level 2
high-availability disable
high-availability heartbeat 4 100 2
high-availability id 4098
clock timezone GMT
clock dst
log audit select general
log audit select login
log audit select logout
log audit select user
log audit select time
log audit select policy
log audit select update
log audit select boot
log audit select report
log audit select host
log audit select configuration
log audit select oam
log audit select sms
log audit select server
log audit select segment
log audit select high-availability
```

```
log audit select monitor
log audit select ip-filter
log audit select conn-table
log audit select host-communication
log audit select tse
category-settings -profile "Default Security Profile" vulnerabilities
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" exploits
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" security-policy
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" reconnaissance
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" virus
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" spyware
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" identity-theft
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" traffic-normal
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" network-equipment
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" p2p
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" im
enable - action-set "Recommended"
category-settings -profile "Default Security Profile" streaming-media
enable - action-set "Recommended"
notify-contact "Management Console" 1
notify-contact "Remote System Log" 1
default-alert-sink period 1
server ssh
server no http
server https
server browser-check
monitor threshold memory -major 90 -critical 95
monitor threshold disk -major 90 -critical 95
monitor threshold temperature -major 92 -critical 94
monitor disable power-supply
no service-access
tse adaptive-filter mode automatic
tse afc-severity warning
tse connection-table timeout 1800
tse logging-mode conditional -threshold 1.0 -period 600
tse quarantine duration 60
email-rate-limit 10
zone update LAN vlan-id 1
zone update LAN port 3/1
zone update LAN mtu 1500
zone update LAN addresses disable
zone update LAN vpn-tunnel-access enable
zone update VPN vlan-id 4
zone update VPN port none
zone update VPN mtu 1500
zone update VPN addresses disable
zone update VPN vpn-tunnel-access enable
zone update WAN vlan-id 3
```

```
zone update WAN port 3/6
zone update WAN mtu 1500
zone update WAN addresses disable
zone update WAN vpn-tunnel-access enable
address-groups update DHCP-Pool range 192.168.1.1 192.168.1.20
authentication privilege-groups update Allow_VPN_access vpn-client-
access
authentication privilege-groups update RADIUS
authentication radius default-privilege-group RADIUS
authentication radius server primary 0.0.0.0 port 1812 shared-secret
***** auth-method chap
authentication radius server secondary none
authentication radius disable
authentication radius user-authentication enable
authentication radius vpn-clients enable
authentication radius retries 3
authentication radius timeout 2
web-filtering default-rule block
web-filtering filter-action block-and-log
web-filtering filter-service cache expiry 24
web-filtering filter-service cache size 2097152
web-filtering filter-service block adult
web-filtering filter-service block gambling
web-filtering filter-service block violence
web-filtering filter-service block criminal
web-filtering filter-service block hacking
web-filtering filter-service block weapons
web-filtering filter-service block drugs
web-filtering filter-service block hate
web-filtering filter-service permit advertisement
web-filtering filter-service permit computing
web-filtering filter-service permit food
web-filtering filter-service permit politics
web-filtering filter-service permit hosting
web-filtering filter-service permit lifestyle
web-filtering filter-service permit dating
web-filtering filter-service permit reference
web-filtering filter-service permit sex-education
web-filtering filter-service permit sports
web-filtering filter-service permit usenet
web-filtering filter-service permit arts
web-filtering filter-service permit education
web-filtering filter-service permit games
web-filtering filter-service permit health
web-filtering filter-service permit careers
web-filtering filter-service permit vehicles
web-filtering filter-service permit photos
web-filtering filter-service permit religion
web-filtering filter-service permit search
web-filtering filter-service permit streaming-media
web-filtering filter-service permit email
web-filtering filter-service permit chat
web-filtering filter-service permit finance
web-filtering filter-service permit glamour
web-filtering filter-service permit hobbies
web-filtering filter-service permit kids
web-filtering filter-service permit news
web-filtering filter-service permit real-estate
```

```
web-filtering filter-service permit proxies
web-filtering filter-service permit shopping
web-filtering filter-service permit travel
web-filtering filter-service disable
web-filtering manual-filter disable
dhcp-server addresses group DHCP-Pool
dhcp-server enable
dhcp-server bootp disable
dhcp-server lease-duration 60
dhcp-server dns default
dhcp-server wins primary 0.0.0.0
dhcp-server wins secondary 0.0.0.0
dhcp-server nbx 0.0.0.0
dhcp-server relay disable
dns use-external-dns enable
interface virtual add 1 internal
interface virtual internal 1 ip 192.168.1.254 netmask 255.255.255.0
interface virtual internal 1 ha-mgmt-ip 0.0.0.0
interface virtual internal 1 nat external-ip
interface virtual internal 1 rip disable
interface virtual internal 1 rip send-mode disable
interface virtual internal 1 rip receive-mode disable
interface virtual internal 1 rip auth disable
interface virtual internal 1 rip split-horizon disable
interface virtual internal 1 rip poison-reverse disable
interface virtual internal 1 rip advertise-routes enable
interface virtual internal 1 igmp disable
interface virtual internal 1 pim-dm disable
interface virtual internal 1 zone add LAN
interface virtual internal 1 zone add VPN
interface virtual add 2 external
interface virtual external 2 type static 10.10.20.147 netmask
255.255.255.0
interface virtual external 2 ha-mgmt-ip 0.0.0.0
interface virtual external 2 rip disable
interface virtual external 2 rip send-mode v2-multicast
interface virtual external 2 rip receive-mode all
interface virtual external 2 rip auth disable
interface virtual external 2 rip split-horizon enable
interface virtual external 2 rip poison-reverse enable
interface virtual external 2 rip advertise-routes disable
interface virtual external 2 igmp disable
interface virtual external 2 pim-dm disable
interface virtual external 2 zone add WAN
default-gateway 10.10.20.1
firewall schedule update working-day days -mtwtf- from 0800 to 1800
firewall service update 3com-nbx udp port 2093 to 2096
firewall service update audio-call-control tcp port 1731
firewall service update dhcp-client udp port 68
firewall service update dhcp-server udp port 67
firewall service update dns-tcp tcp port 53
firewall service update dns-udp udp port 53
firewall service update finger-tcp tcp port 79
firewall service update ftp tcp port 21
firewall service update gopher-tcp tcp port 70
firewall service update gre gre
firewall service update h323 tcp port 1720
firewall service update http tcp port 80
```

```
firewall service update https tcp port 443
firewall service update igmp igmp
firewall service update ike udp port 500
firewall service update imap tcp port 143
firewall service update imapv3 tcp port 220
firewall service update ipsec-ah ah
firewall service update ipsec-esp esp
firewall service update kerberos-tcp tcp port 88
firewall service update kerberos-udp udp port 88
firewall service update l2tp udp port 1701
firewall service update ldap-tcp tcp port 389
firewall service update ldap-udp udp port 389
firewall service update lotus-notes-domino tcp port 1352
firewall service update lpr tcp port 515
firewall service update nat-t-ipsec udp port 4500
firewall service update nbname tcp port 137
firewall service update netbios-tcp tcp port 137 to 139
firewall service update netbios-udp udp port 137 to 139
firewall service update netmeeting tcp port 1720
firewall service update nfsd-tcp tcp port 2049
firewall service update nfsd-udp udp port 2049
firewall service update nntp tcp port 119
firewall service update ntp udp port 123
firewall service update pim-dm pim
firewall service update ping icmp port 8
firewall service update pop3 tcp port 110
firewall service update portmapper-tcp tcp port 111
firewall service update portmapper-udp udp port 111
firewall service update pptp-tcp tcp port 1723
firewall service update radius-accounting udp port 1813
firewall service update radius-auth udp port 1812
firewall service update rexec tcp port 512
firewall service update rip udp port 520
firewall service update rlogin tcp port 513
firewall service update rsh tcp port 514
firewall service update rtsp tcp port 554
firewall service update sip-tcp tcp port 5060
firewall service update sip-udp udp port 5060
firewall service update smb tcp port 445
firewall service update sms-client tcp port 10042
firewall service update sms-trap tcp port 8162 to 8163
firewall service update smtp tcp port 25
firewall service update snmp-request udp port 161
firewall service update snmp-trap udp port 162
firewall service update ssh tcp port 22
firewall service update syslog udp port 514
firewall service update t120 tcp port 1503
firewall service update telnet tcp port 23
firewall service update tftp udp port 69
firewall service update traceroute icmp port 8
firewall service update uucp udp port 540
firewall service update vnc-browser tcp port 5800
firewall service update vnc-viewer tcp port 5900
firewall service update x-windows tcp port 6000 to 6063
firewall service-group update dns dns-tcp dns-udp
firewall service-group update email pop3 smtp imap imapv3
firewall service-group update ipsec ike ipsec-ah ipsec-esp
firewall service-group update ldap ldap-udp ldap-tcp
```

```
firewall service-group update management https ssh ping snmp-request
firewall service-group update netmeeting h323 audio-call-control t120
firewall service-group update network-protocols dns-tcp dns-udp dhcp-
server
firewall service-group update nfs portmapper-tcp portmapper-udp nfsd-tcp
nfsd-udp
firewall service-group update pptp pptp-tcp gre
firewall service-group update secure-management https ssh
firewall service-group update sip sip-tcp sip-udp
firewall service-group update sms-config http https sms-client snmp-
request ssh
firewall service-group update sms-get ntp sms-trap
firewall service-group update snmp snmp-request snmp-trap
firewall service-group update vnc vnc-browser vnc-viewer
firewall service-group update voice 3com-nbx sip-tcp sip-udp
firewall service-group update vpn-protocols pptp-tcp l2tp gre ike nat-t-
ipsec
firewall rule update 1 permit LAN WAN ANY
firewall rule update 1 schedule always timeout 30 logging disable
firewall rule update 1 src-addr all
firewall rule update 1 dst-addr all
firewall rule update 1 bandwidth disable
firewall rule update 1 authentication disable
firewall rule update 1 position 1
firewall rule update 1 comment "Allow LAN unrestricted access to WAN"
firewall rule update 1 remote-logging disable
firewall rule enable 1
firewall rule update 2 permit WAN this-device vpn-protocols
firewall rule update 2 schedule always timeout 30 logging disable
firewall rule update 2 src-addr all
firewall rule update 2 dst-addr all
firewall rule update 2 bandwidth disable
firewall rule update 2 authentication disable
firewall rule update 2 position 2
firewall rule update 2 comment "Allow VPN termination"
firewall rule update 2 remote-logging disable
firewall rule enable 2
firewall rule update 3 permit LAN this-device management
firewall rule update 3 schedule always timeout 30 logging disable
firewall rule update 3 src-addr all
firewall rule update 3 dst-addr all
firewall rule update 3 bandwidth disable
firewall rule update 3 authentication disable
firewall rule update 3 position 3
firewall rule update 3 comment "Allow management access from LAN"
firewall rule update 3 remote-logging disable
firewall rule enable 3
firewall rule update 4 permit LAN this-device network-protocols
firewall rule update 4 schedule always timeout 30 logging disable
firewall rule update 4 src-addr all
firewall rule update 4 dst-addr all
firewall rule update 4 bandwidth disable
firewall rule update 4 authentication disable
firewall rule update 4 position 4
firewall rule update 4 comment "Allow DNS and DHCP from LAN"
firewall rule update 4 remote-logging disable
firewall rule enable 4
firewall rule update 5 permit LAN this-device rip
```



```
firewall rule update 5 schedule always timeout 30 logging disable
firewall rule update 5 src-addr all
firewall rule update 5 dst-addr all
firewall rule update 5 bandwidth disable
firewall rule update 5 authentication disable
firewall rule update 5 position 5
firewall rule update 5 comment ""
firewall rule update 5 remote-logging disable
firewall rule enable 5
firewall rule update 6 permit LAN this-device pim-dm
firewall rule update 6 schedule always timeout 30 logging disable
firewall rule update 6 src-addr all
firewall rule update 6 dst-addr all
firewall rule update 6 bandwidth disable
firewall rule update 6 authentication disable
firewall rule update 6 position 6
firewall rule update 6 comment ""
firewall rule update 6 remote-logging disable
firewall rule enable 6
firewall alg sip services ANY
firewall alg sip sdp-port-range ANY
routing rip enable update-timer 30
routing multicast igmp disable
routing multicast pim-dm disable query-interval 30 prune-timeout 180
vpn ike local-id email x-family@3com.com
vpn ike local-id domain x-family
vpn ike add DES-SHA1-PSK
vpn ike proposal DES-SHA1-PSK phase1-encryption des-cbc
vpn ike proposal DES-SHA1-PSK phase1-integrity sha1
vpn ike proposal DES-SHA1-PSK phase1-dh-group 1
vpn ike proposal DES-SHA1-PSK phase1-lifetime 28800
vpn ike proposal DES-SHA1-PSK auth-type psk
vpn ike proposal DES-SHA1-PSK aggressive-mode disable
vpn ike proposal DES-SHA1-PSK local-id-type ip
vpn ike proposal DES-SHA1-PSK peer-id-type ip
vpn ike proposal DES-SHA1-PSK ca-cert ANY
vpn ike proposal DES-SHA1-PSK nat-t disable
vpn ike proposal DES-SHA1-PSK dpd enable
vpn ike proposal DES-SHA1-PSK auto-connect disable
vpn ike proposal DES-SHA1-PSK tight-phase2-control enable
vpn ike proposal DES-SHA1-PSK phase2-encryption des-cbc
vpn ike proposal DES-SHA1-PSK phase2-integrity esp-sha1-hmac
vpn ike proposal DES-SHA1-PSK phase2-lifetime 3600
vpn ike proposal DES-SHA1-PSK pfs disable
vpn ike proposal DES-SHA1-PSK phase2-dh-group 1
vpn ike proposal DES-SHA1-PSK phase2-zero-id disable
vpn ike proposal DES-SHA1-PSK phase2-strict-id-check disable
vpn ike add 3DES-SHA1-DH2
vpn ike proposal 3DES-SHA1-DH2 phase1-encryption 3des-cbc
vpn ike proposal 3DES-SHA1-DH2 phase1-integrity sha1
vpn ike proposal 3DES-SHA1-DH2 phase1-dh-group 2
vpn ike proposal 3DES-SHA1-DH2 phase1-lifetime 28800
vpn ike proposal 3DES-SHA1-DH2 auth-type psk
vpn ike proposal 3DES-SHA1-DH2 aggressive-mode disable
vpn ike proposal 3DES-SHA1-DH2 local-id-type ip
vpn ike proposal 3DES-SHA1-DH2 peer-id-type ip
vpn ike proposal 3DES-SHA1-DH2 ca-cert ANY
vpn ike proposal 3DES-SHA1-DH2 nat-t enable
```

```
vpn ike proposal 3DES-SHA1-DH2 dpd enable
vpn ike proposal 3DES-SHA1-DH2 auto-connect disable
vpn ike proposal 3DES-SHA1-DH2 tight-phase2-control disable
vpn ike proposal 3DES-SHA1-DH2 phase2-encryption 3des-cbc
vpn ike proposal 3DES-SHA1-DH2 phase2-integrity esp-sha1-hmac
vpn ike proposal 3DES-SHA1-DH2 phase2-lifetime 3600
vpn ike proposal 3DES-SHA1-DH2 pfs disable
vpn ike proposal 3DES-SHA1-DH2 phase2-dh-group 2
vpn ike proposal 3DES-SHA1-DH2 phase2-zero-id disable
vpn ike proposal 3DES-SHA1-DH2 phase2-strict-id-check disable
vpn ike add 3DES-SHA1-DH2-AGG-PFS
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS phase1-encryption 3des-cbc
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS phase1-integrity sha1
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS phase1-dh-group 2
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS phase1-lifetime 28800
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS auth-type psk
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS aggressive-mode enable
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS local-id-type domain
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS peer-id-type domain
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS ca-cert ANY
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS nat-t enable
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS dpd enable
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS auto-connect disable
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS tight-phase2-control disable
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS phase2-encryption 3des-cbc
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS phase2-integrity esp-sha1-hmac
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS phase2-lifetime 3600
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS pfs enable
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS phase2-dh-group 2
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS phase2-zero-id disable
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS phase2-strict-id-check disable
vpn ipsec enable
vpn ipsec add Default
vpn ipsec sa Default disable
vpn ipsec sa Default key ike proposal DES-SHA1-PSK shared-secret
*****
vpn ipsec sa Default transport enable
vpn ipsec sa Default peer 0.0.0.0
vpn ipsec sa Default zone LAN
vpn ipsec sa Default tunnel enable
vpn ipsec add x_family_to_other_agg
vpn ipsec sa x_family_to_other_agg key ike proposal 3DES-SHA1-DH2-AGG-
PFS shared-secret ***** peer-id OTHER
vpn ipsec sa x_family_to_other_agg transport disable
vpn ipsec sa x_family_to_other_agg peer 10.10.10.147
vpn ipsec sa x_family_to_other_agg zone LAN
vpn ipsec sa x_family_to_other_agg tunnel remote subnet 192.168.22.0
netmask 255
.255.255.0
vpn ipsec sa x_family_to_other_agg tunnel local subnet 192.168.1.0
netmask 255.2
55.255.0
vpn ipsec sa x_family_to_other_agg tunnel nat disable
vpn ipsec sa x_family_to_other_agg tunnel enable
vpn ipsec sa x_family_to_other_agg enable
vpn l2tp addresses none
vpn l2tp zone LAN
vpn l2tp dns relay
```

```
vpn l2tp encryption enable
vpn l2tp disable
vpn pptp addresses none
vpn pptp zone LAN
vpn pptp dns relay
vpn pptp encryption enable
vpn pptp disable
ntp peer
ntp server 161.71.52.200:123
ntp duration 5
ntp offset 1
ntp fast enable
ntp enable
ramdisk sync-interval sys 30
ramdisk sync-interval audit 30
ramdisk sync-interval block -1
ramdisk sync-interval alert -1
ramdisk sync-interval firewallsession -1
ramdisk sync-interval firewallblock -1
ramdisk sync-interval vpn -1
sms v2
sms no must-be-ip
no sms
sms no remote-deploy
session timeout 20 -persist
3KB_x_unit_1#
```

## 6.2.2 SonicWall PRO 2040 configuration file

There does not seem to be an easy way to dump the entire config as a text file – so here is the VPN configuration only.

```
PRO 2040 Enhanced> show vpn policy
Policy: WAN GroupVPN
  Key Mode: Pre-shared
  Pre Shared Secret: sharedkey

  Proposals:
  IKE: Aggressive Mode, 3DES SHA, DH Group 2, 28800 seconds
  IPSEC: ESP, 3DES SHA, No PFS, 28800 seconds

  Advanced:
  Allow NetBIOS OFF, Allow Multicast OFF
  Management: HTTP OFF, HTTPS OFF
  Lan Default GW: 0.0.0.0
  Require XAUTH: ON, User Group: Trusted Users

  Client:
  Cache XAUTH Settings: Never
  Virtual Adapter Settings: None
  Allow Connections To: Split Tunnels
  Set Default Route OFF, Require GSC OFF
  Use Default Key OFF

Policy: WLAN GroupVPN (Disabled)
  Key Mode: Pre-shared
  Pre Shared Secret: 391D190BD059C7DE
```

Proposals:  
IKE: Aggressive Mode, 3DES SHA, DH Group 2, 28800 seconds  
IPSEC: ESP, 3DES SHA, No PFS, 28800 seconds

Advanced:  
Allow NetBIOS OFF, Allow Multicast OFF  
Management: HTTP ON, HTTPS ON  
Lan Default GW: 0.0.0.0  
Require XAUTH: ON, User Group: Trusted Users

Client:  
Cache XAUTH Settings: Single Session  
Virtual Adapter Settings: None  
Allow Connections To: All Secured Gateways  
Set Default Route ON, Require GSC OFF  
Use Default Key ON

Policy: X-family\_to\_SonicWall  
Key Mode: Pre-shared  
Primary GW: 0.0.0.0  
Secondary GW: 0.0.0.0  
Pre Shared Secret: shared-secret

IKE ID:  
Local: Domain Name OTHER  
Peer: Domain Name x-family

Network:  
Local: 22net Remote: 1net

Proposals:  
IKE: Aggressive Mode, 3DES SHA, DH Group 2, 28800 seconds  
IPSEC: ESP, 3DES SHA, PFS: DH Group 2, 28800 seconds

Advanced:  
Keepalive OFF, Add Auto-Rule ON, Allow NetBIOS OFF  
Allow Multicast OFF  
Management: HTTP OFF, HTTPS OFF  
User Login: HTTP OFF, HTTPS OFF  
Lan Default GW: 0.0.0.0  
Require XAUTH: OFF  
Bound To: Zone WAN

PRO 2040 Enhanced> show vpn sa

Policy: X-family\_to\_SonicWall  
IKE SAs

GW: 10.10.10.147:500 --> 10.10.20.147:500  
Aggressive Mode, 3DES SHA, DH Group 2, Responder  
Cookie: 0x8d1189d7bfda58f4 (I), 0x03a9407f82b0947f (R)  
Lifetime: 28800 seconds (27902 seconds remaining)

IPsec SAs

GW: 10.10.10.147:500 --> 10.10.20.147:500  
(192.168.22.0 - 192.168.22.255) --> (192.168.1.0 -  
192.168.1.255)  
ESP, 3DES SHA, In SPI 0xba921950, Out SPI 0x95fa06d5

Lifetime: 3600 seconds (2701 seconds remaining)

PRO 2040 Enhanced>