IPSec VPN for Netscreen NS25 to 3Com X-family

Document Version:	1.4
Publication Date:	18 February 2009
Description:	Configuring site-to-site VPNs from Netscreen to 3Com X-family
Product:	3Com X-family
3Com TOS Version:	2.5.0.6688 or later
Netscreen NS25 Software Version:	5.0.0r8.0 (Firewall+VPN)

1 Overview

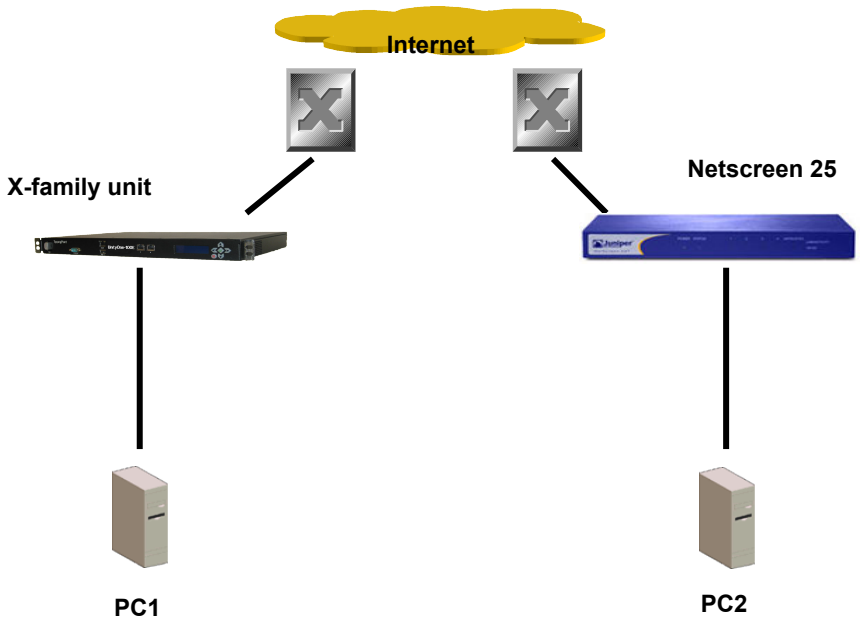
This technical note describes how to setup IPSec VPN tunnels between a 3Com X-family and the Netscreen NS25.

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 Netscreen NS25 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 Netscreen)	10.10.10.1	255.255.255.0	
X-family	external	10.10.20.147	255.255.255.0	10.10.10.1
Netscreen	external	10.10.10.147	255.255.255.	10.10.20.1

			0	
PC1		192.168.1.100	255.255.255.0	192.168.1.254
PC2		192.168.22.100	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.

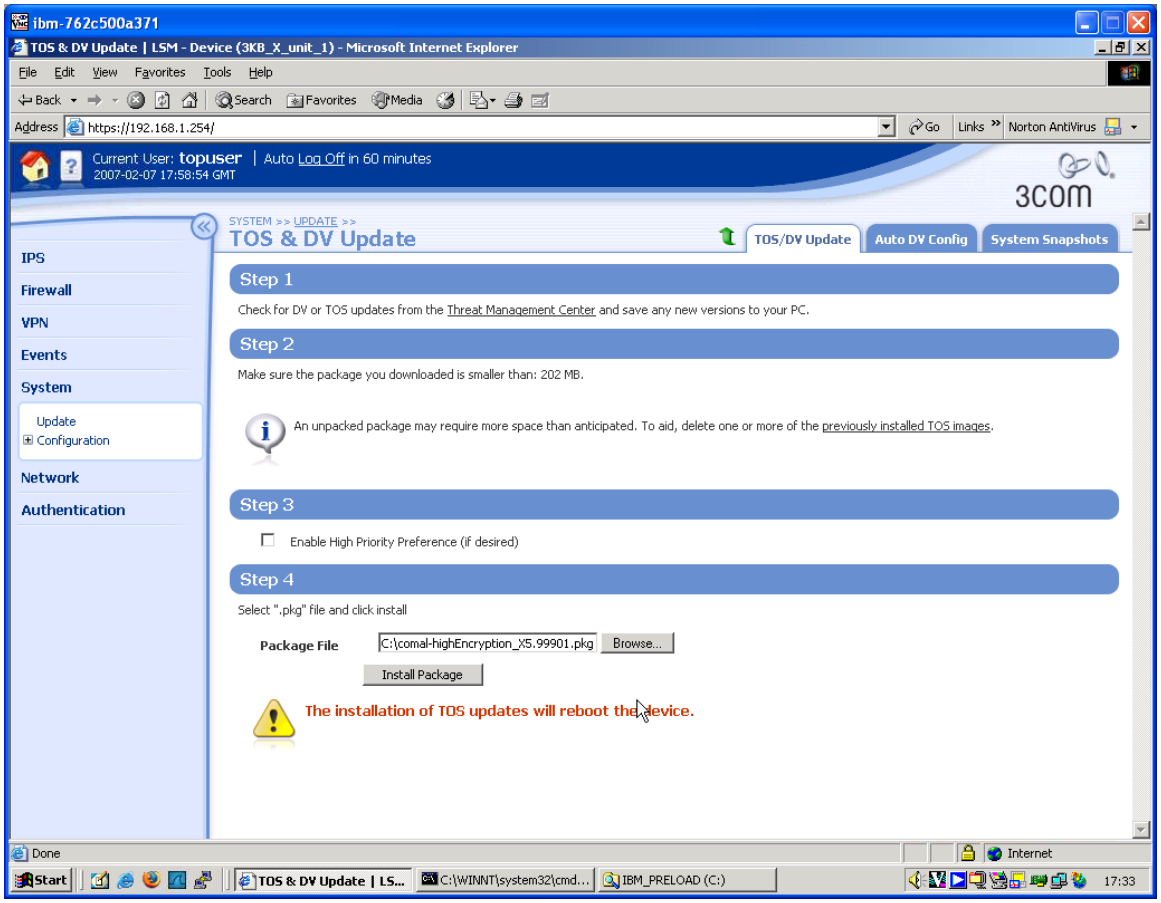
Firewall rules – the firewall rules in the factory default configuration will be sufficient – specifically this one:

```
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.

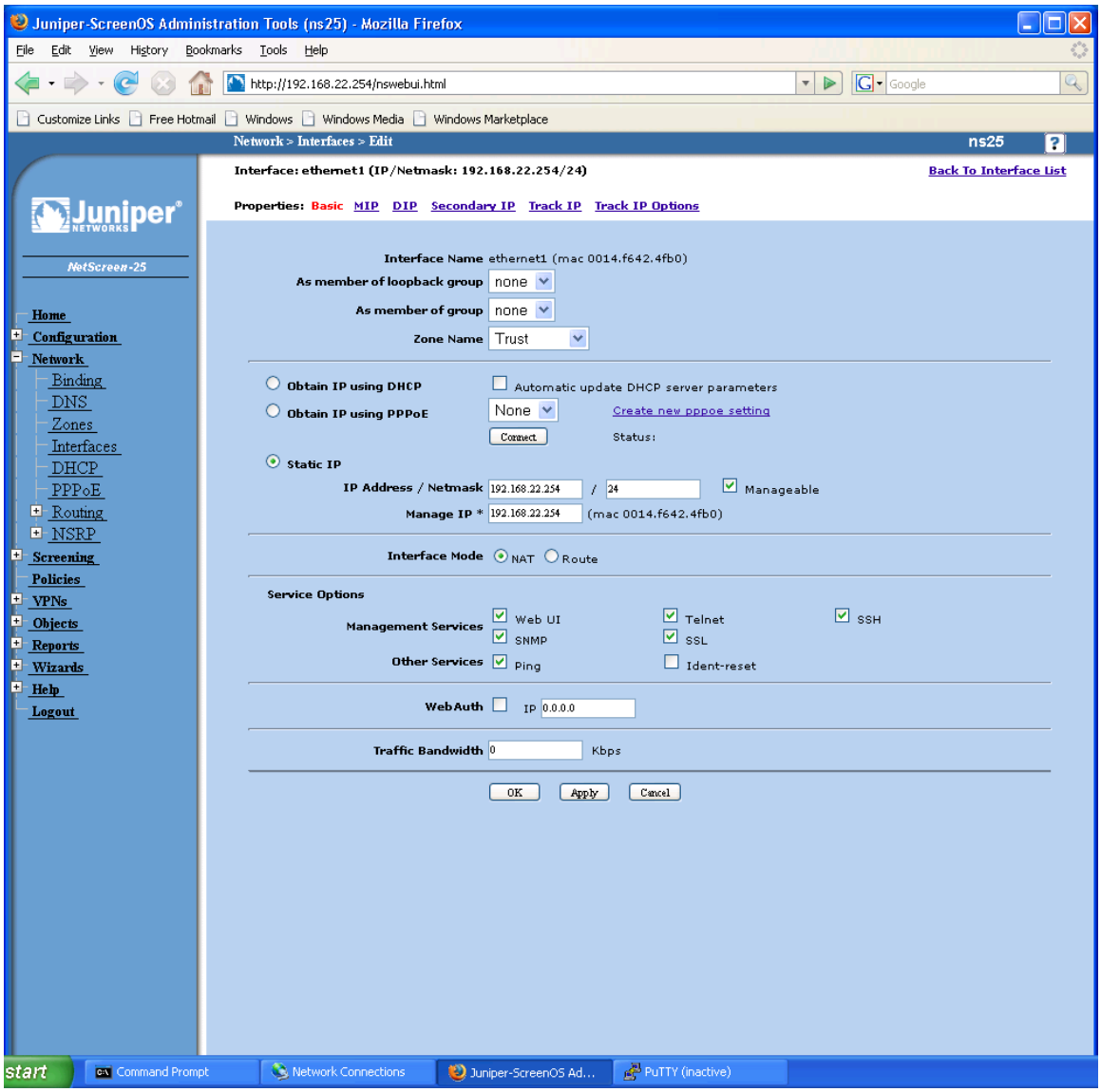
1. Acquire the High Encryption package from the TMC and load it onto PC1.
2. Open a browser on PC1, connect to https://192.168.1.254 and login as the user you set up during the OBE.
3. Navigate to System -> Update, open the "TOS/DV Update" tab and complete the form as shown below with the path of the 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.

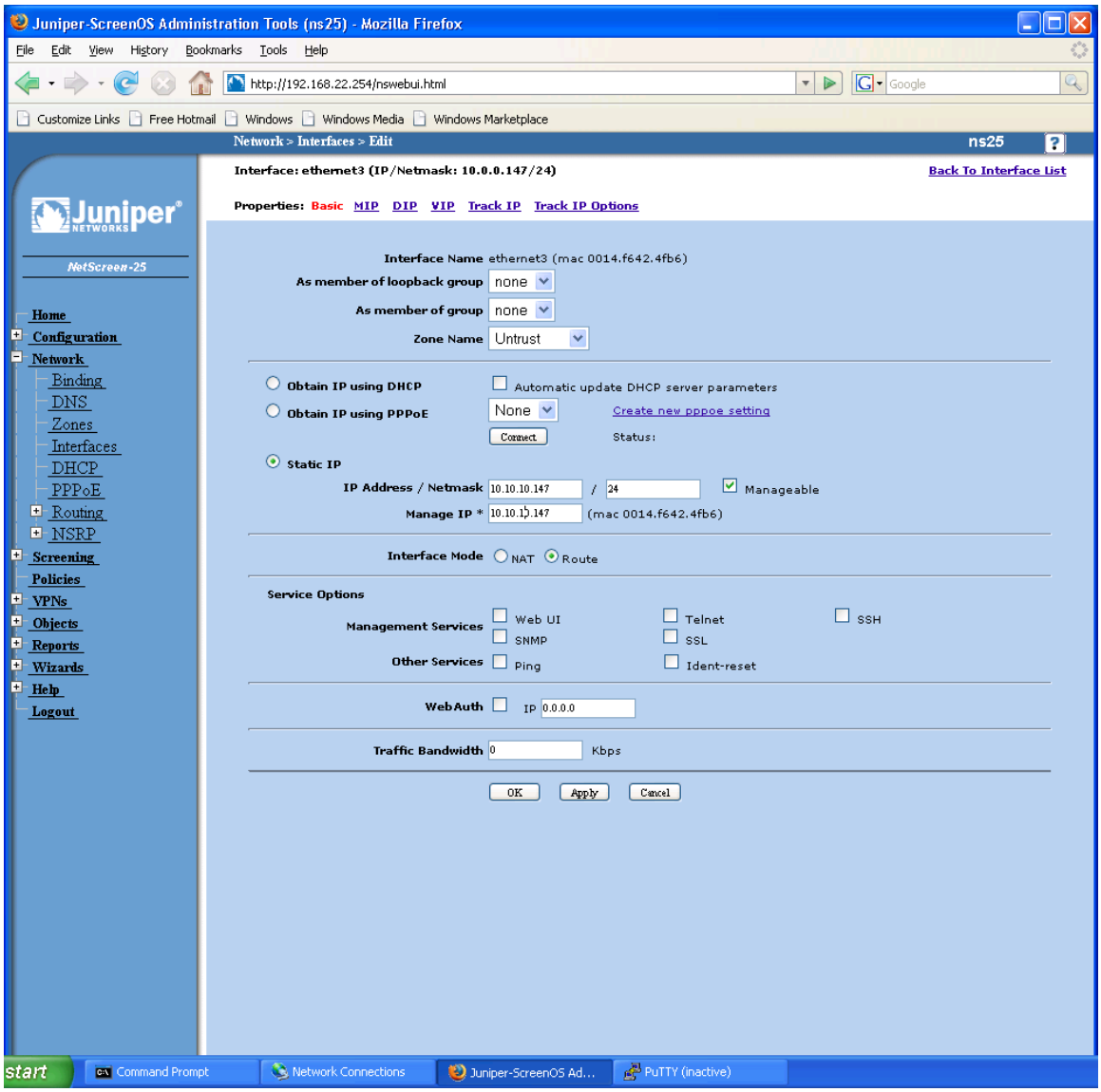
3.2 Netscreen NS25 Pre-Requisite Configuration

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 http://192.168.1.254 and login to the Netscreen GUI.
3. Click the + sign next to “Network” at the left of the screen and click “Interfaces” on the submenu that appears. In the screen that is presented click “edit” next to the interface “ethernet 1”. Complete the screen as shown below and click OK.

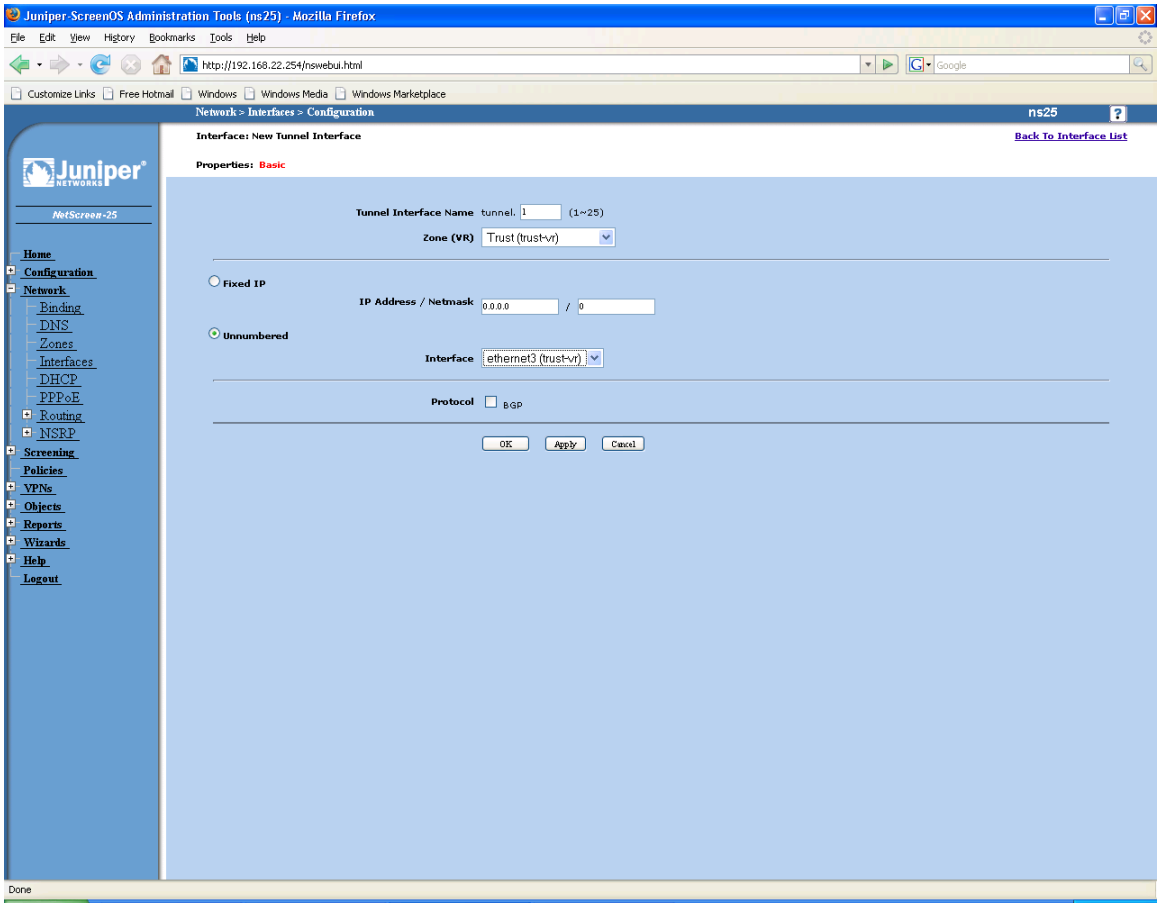


4. The management connection to the Netscreen will be lost. Change the IP address of PC2 to 192.168.22.100 and reconnect to the new Netscreen management address http://192.168.22.254.

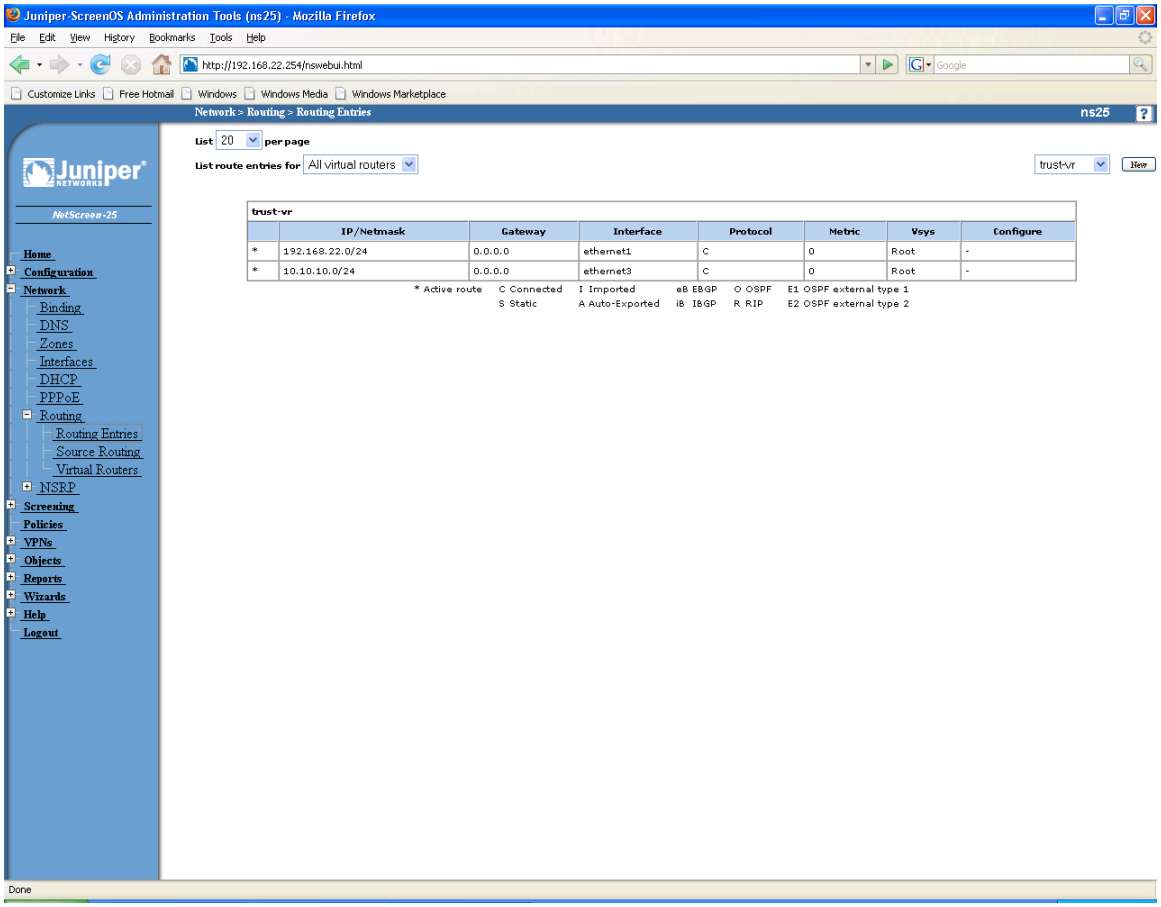
5. Login and return to the Network -> Interfaces screen. This time click the edit next to interface Ethernet 3, complete the form as shown below and click OK.



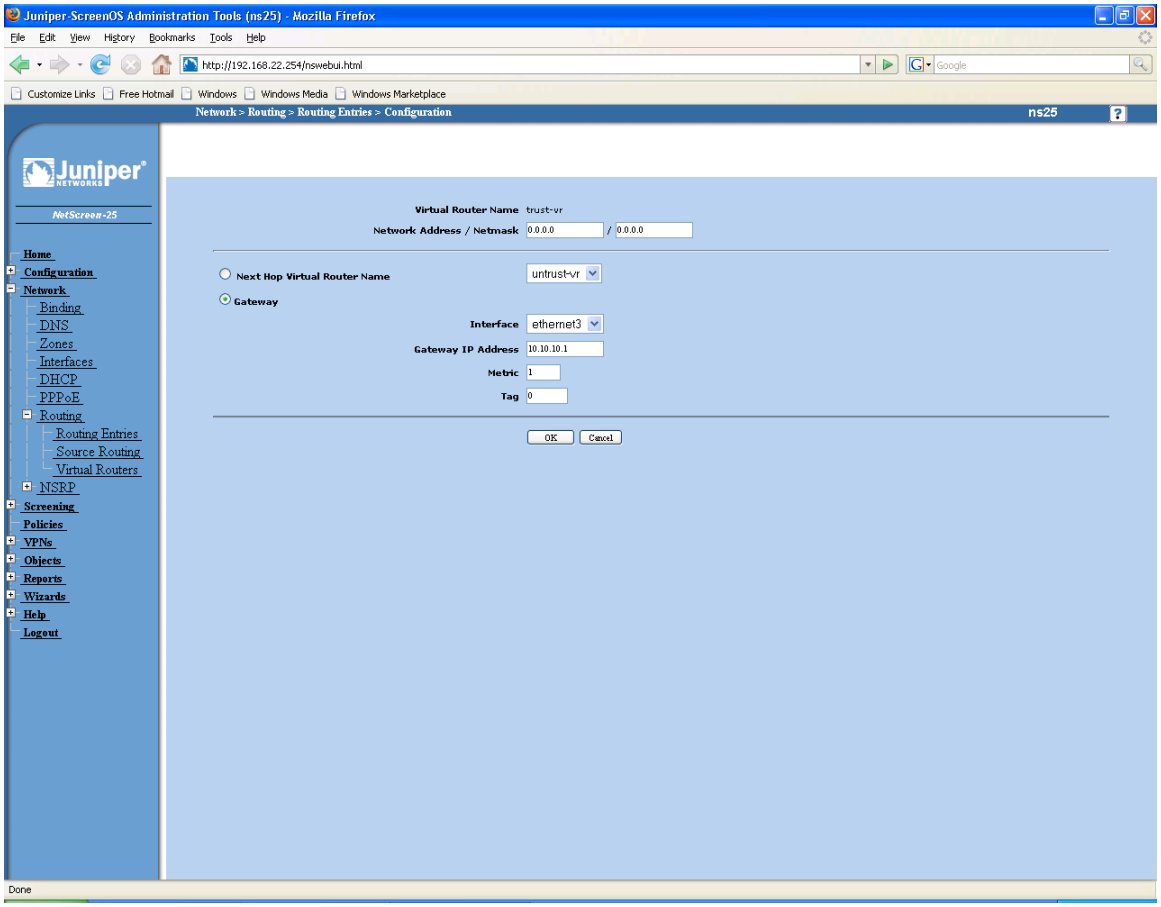
6. Return to the Network -> Interfaces screen. This time go to the top right of the screen, set the drop-down menu to "Tunnel IF" and click the "New" button next to it. Complete the form as shown below and click "OK". This will create the tunnel interface that can be used by the VPNs that are configured later.



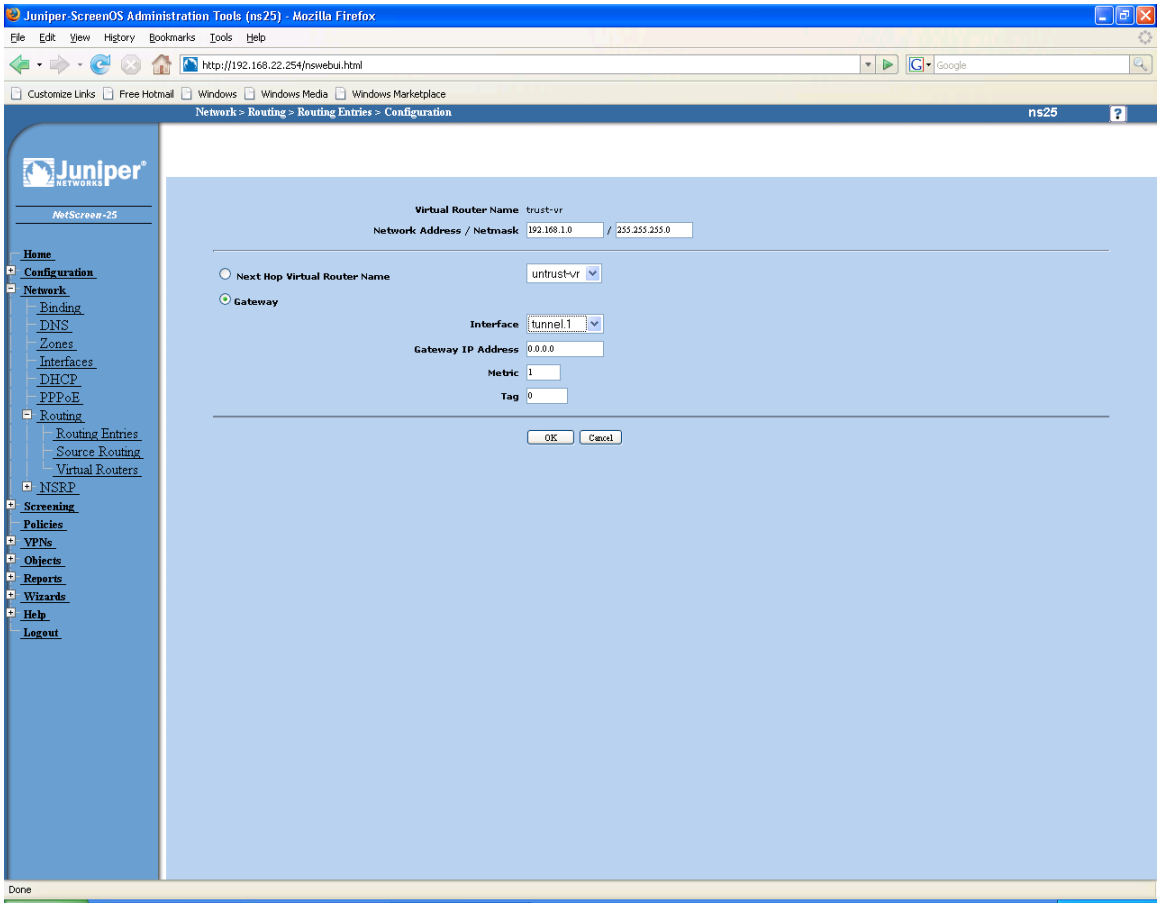
7. The Netscreen device does not have a default gateway setting, so a Routing entry must be created for a default route. Navigate to Network -> Routing -> Routing Entries. This will contain two default entries for the internal and external networks as shown below.



8. Ensure that "trust-vr" is shown in the top right drop-down window and click the "New" button. Complete the form as shown below and click the OK button.

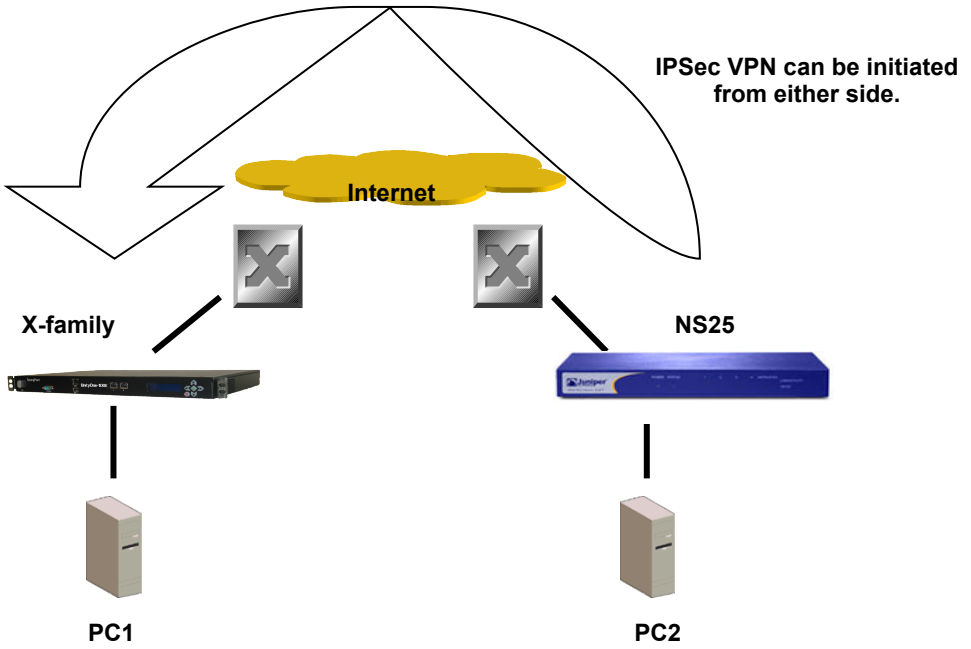


9. Finally, we need a route to cause traffic to flow down the VPN tunnel. Ensure that "trust-vr" is shown in the top right and click the "New" button. Complete the form as shown below and click the OK button.


Juniper-ScreenOS Administration Tools (ns25) - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.22.254/nswebui.html
Customize Links Free Hotmail Windows Windows Media Windows Marketplace
Network > Routing > Routing Entries > Configuration
ns25
Juniper NETWORKS
NetScreen-25
Home
Configuration
Network
Binding
DNS
Zones
Interfaces
DHCP
PPPoE
Routing
Routing Entries
Source Routing
Virtual Routers
NSRP
Screening
Policies
VPNs
Objects
Reports
Wizards
Help
Logout
Virtual Router Name trust-vr
Network Address / Netmask 192.168.1.0 / 255.255.255.0
Next Hop Virtual Router Name untrust-vr
Gateway
Interface tunnel.1
Gateway IP Address 0.0.0.0
Metric 1
Tag 0
OK Cancel
Done

4 Configuring Main Mode Tunnel

This example shows how to configure an IPSec tunnel using Main Mode between the X-family and a Netscreen NS25. Main Mode is the recommended setting when both devices have static IP addresses that can be accessed from the public internet.

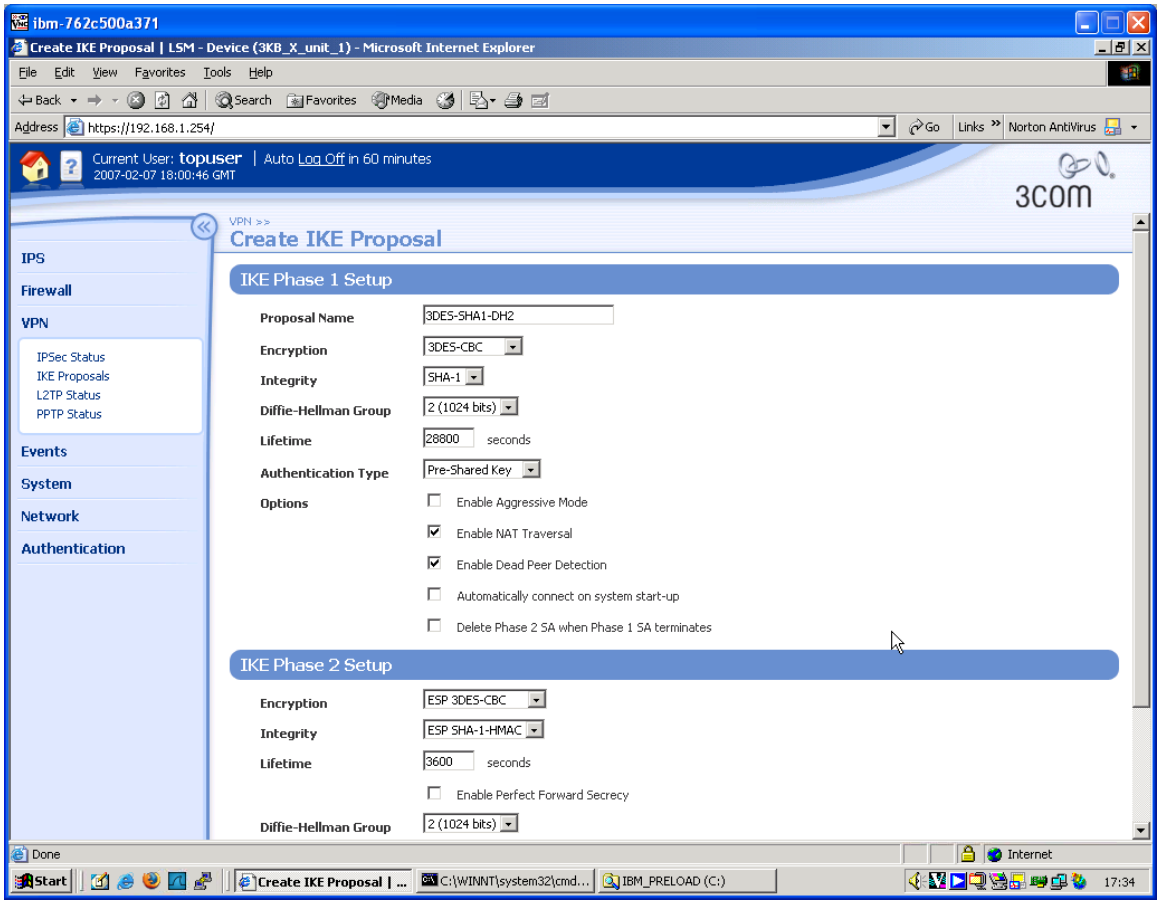


Key Setup Information

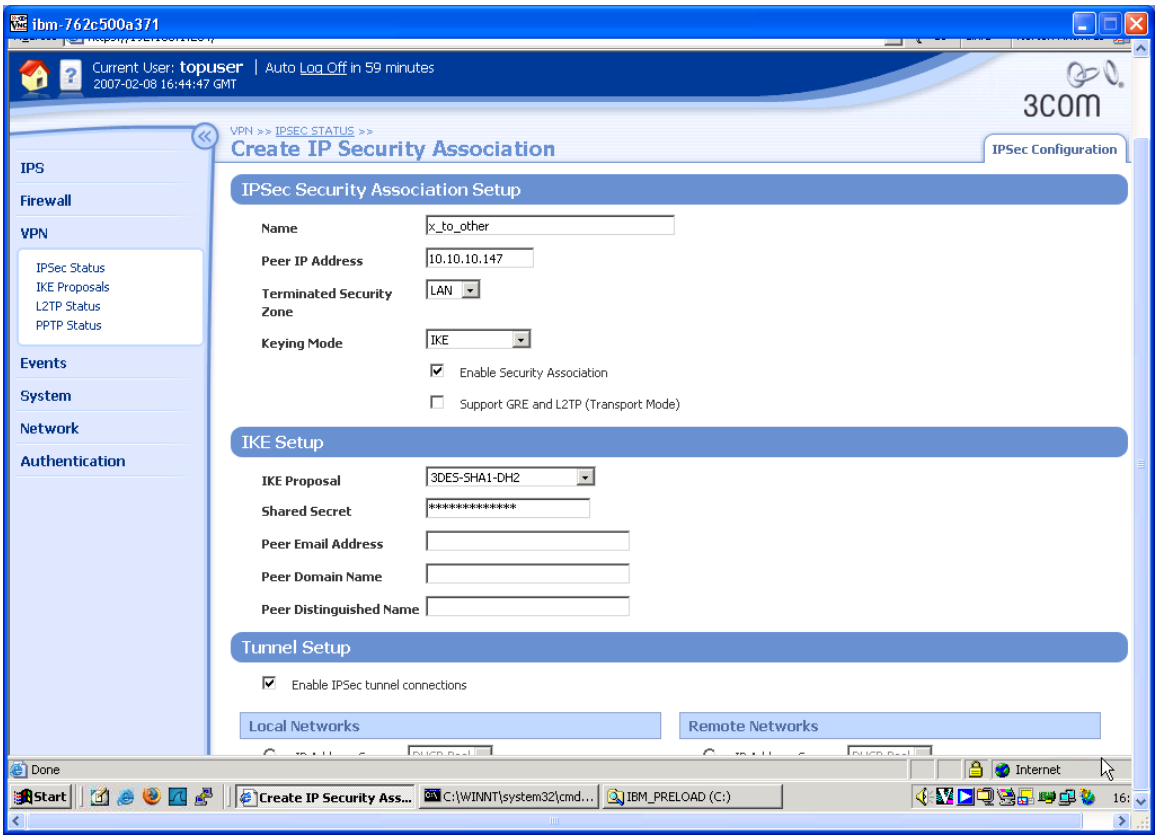
Keying Mode	IKE
IKE Mode	Main Mode
SA Authentication Method	Pre-shared Key
Keying Group DH	DH (Diffie Hellman) Group 2
Encryption and Data Integrity	3DES-SHA1

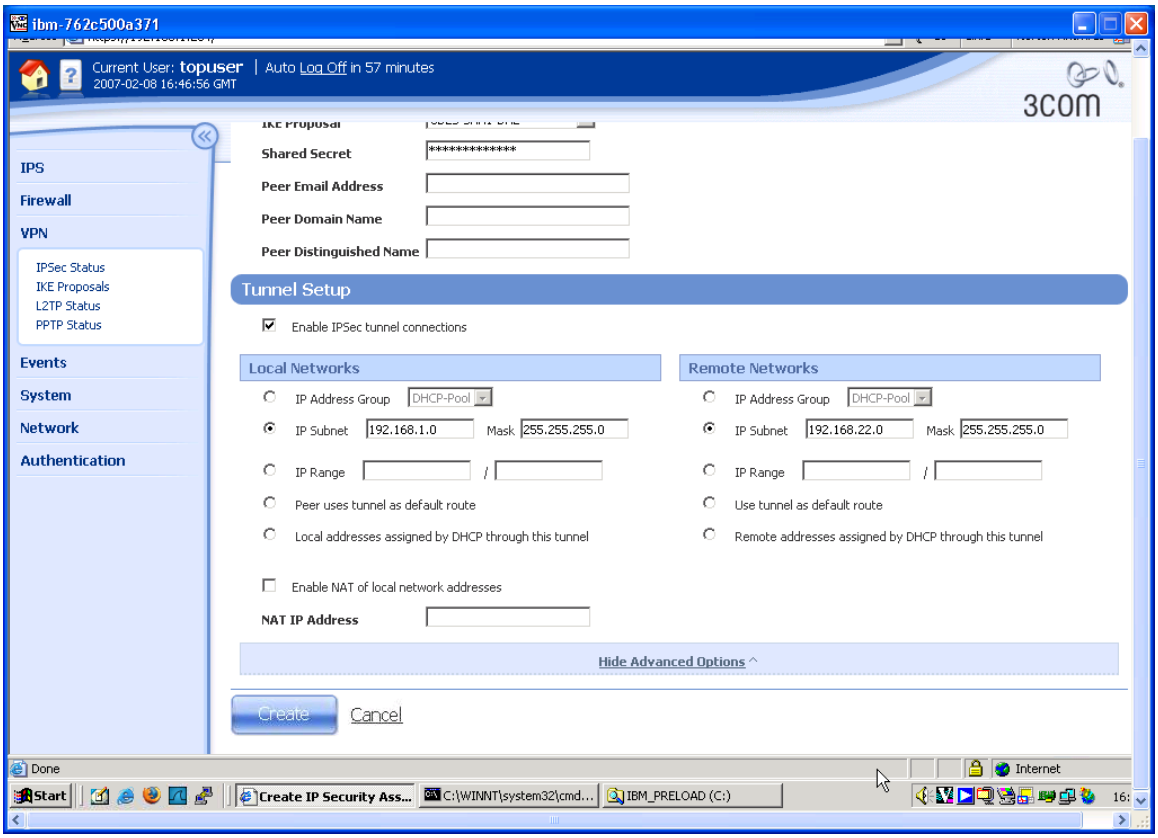
4.1 3Com X-family VPN Configuration

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.



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.

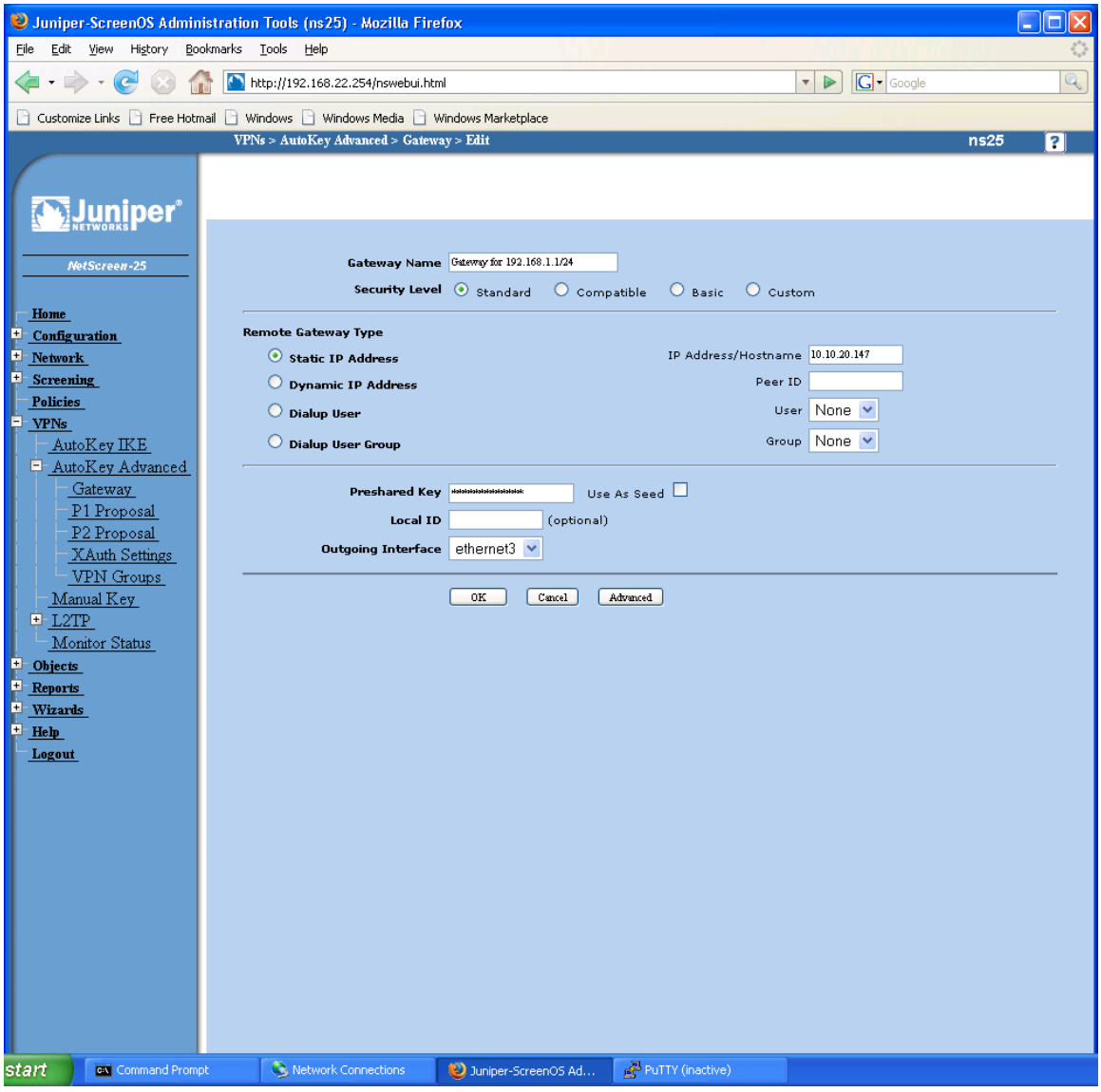




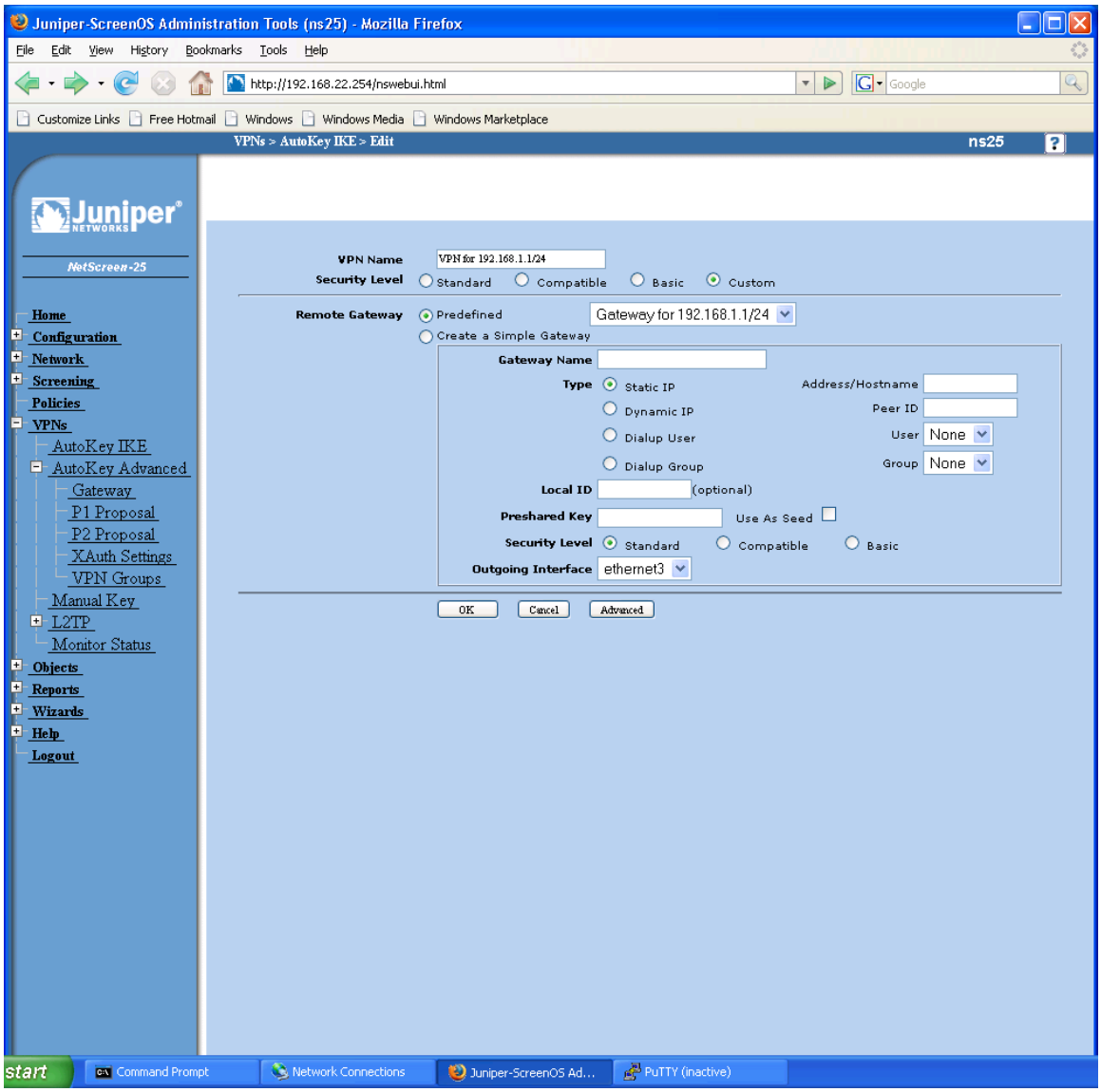
7. Click "Create" to save the new Security Association.

4.2 Netscreen NS25 Configuration

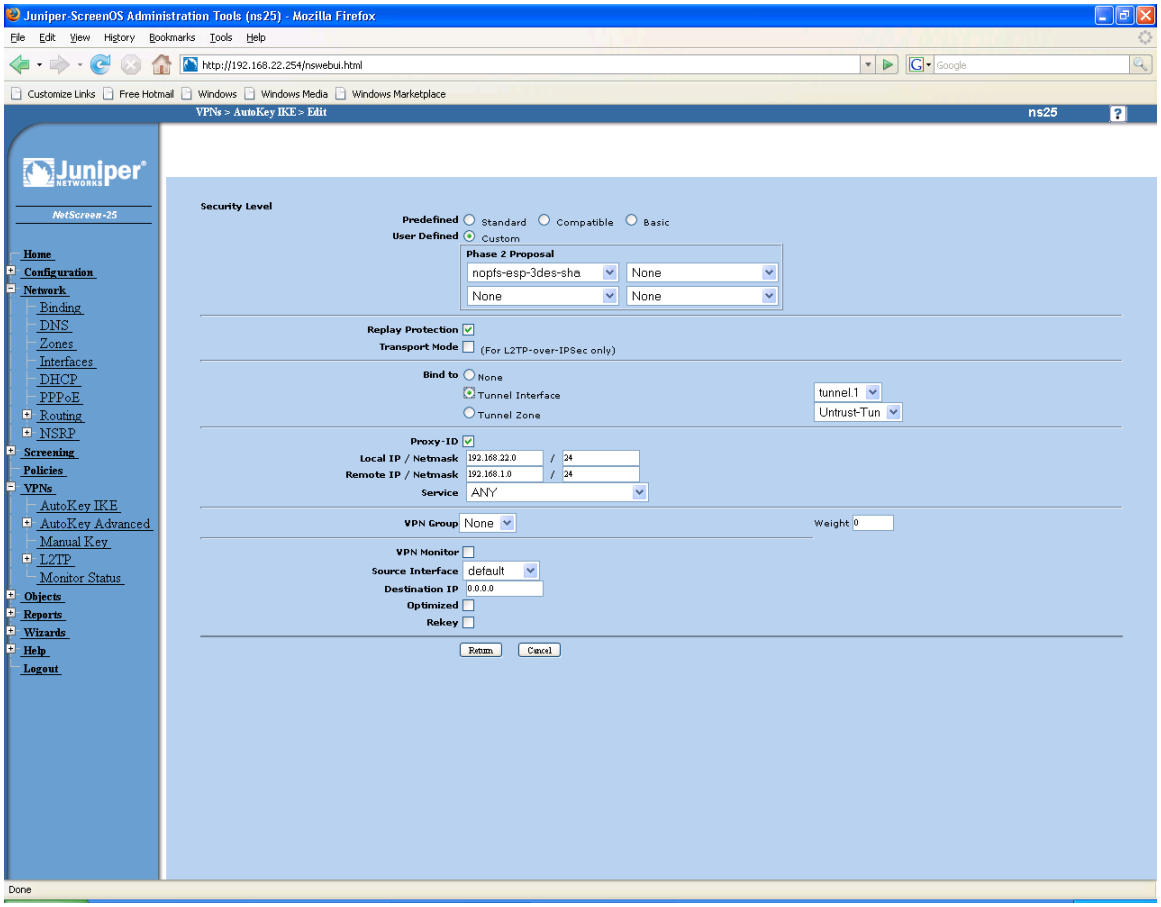
1. Open a browser on PC2, connect to https://192.168.22.254 and login to the Netscreen GUI as user "netscreen" with password "netscreen".
2. Click on the + sign to the left of "VPNs" to open up the submenus.
3. Click on the + sign to the left of "AutoKey Advanced" in the new submenu to open up another submenu.
4. Click on "Gateway" in the new submenu and click the "New" button to create a new gateway. Complete the form as shown below. Note that the "Preshared Key" string entered here must be at least 8 characters and must be exactly the same as the shared secret entered on the peer device.



5. Click on "OK" to save the new Gateway.
6. Click on "AutoKey IKE". On the screen that opens click on "New" to create a new Security Association and complete the form as shown below.



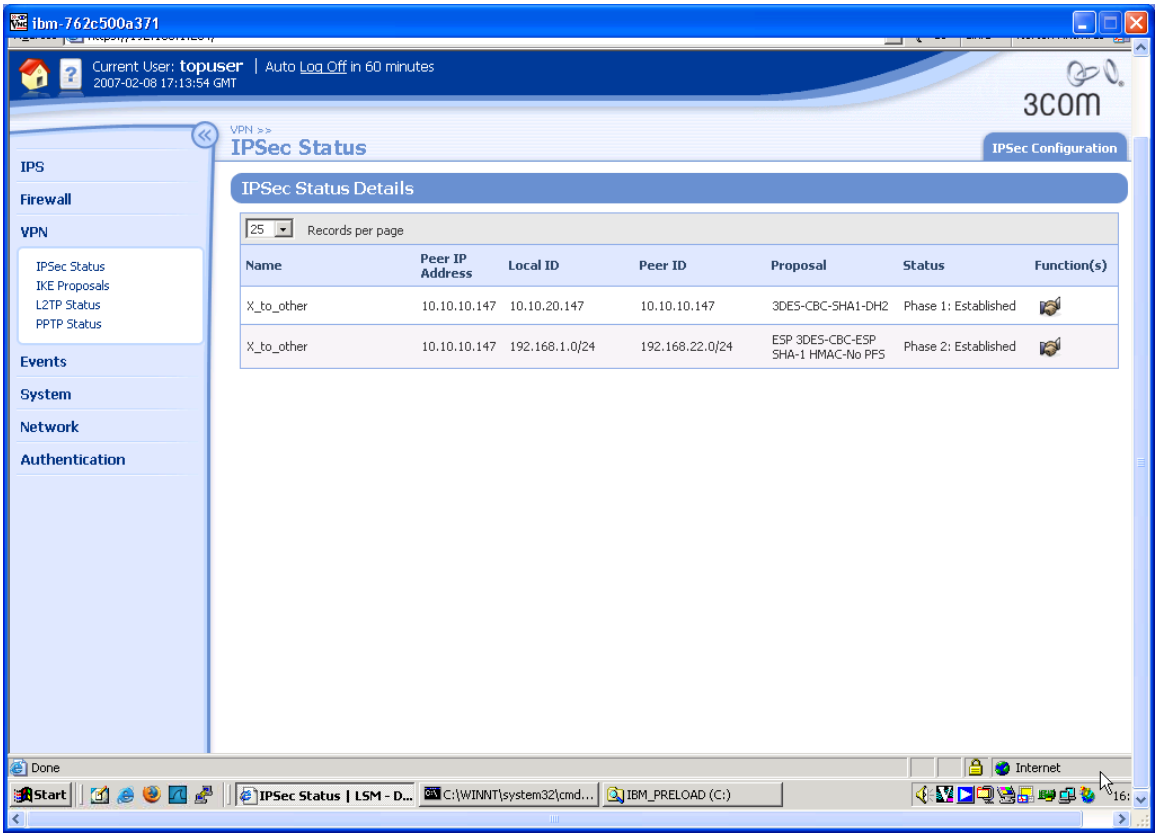
7. Click on "Advanced" and fill in the new form as show below.



8. Click on "Return" at the bottom of the form and then click on "OK" on the previous form to save the changes.

4.3 Testing the VPN with data

8. Ping from PC2 to PC1 - 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.



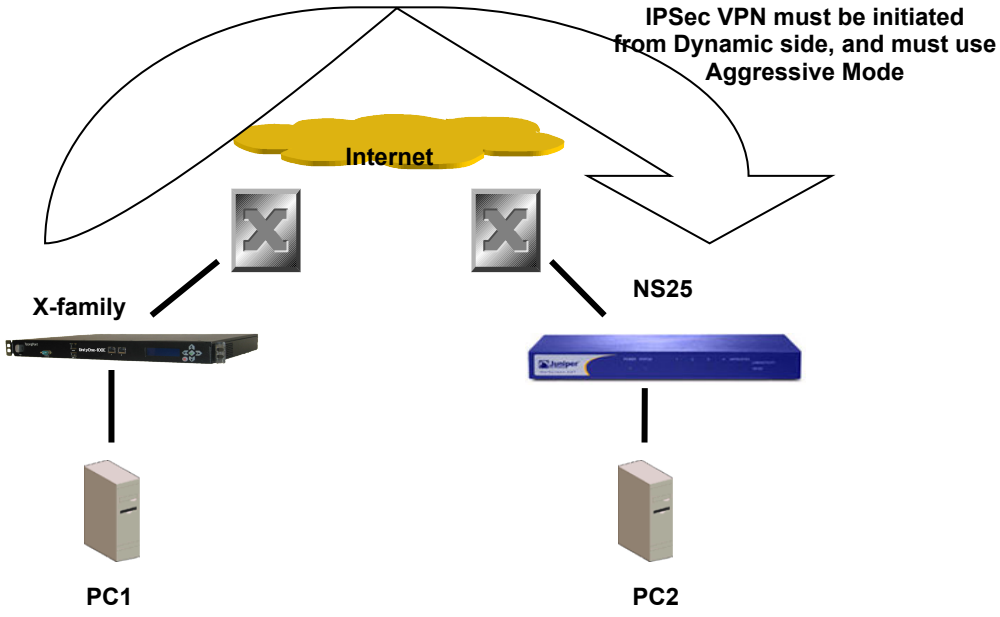
5 Aggressive Mode Tunnel

This example shows how to configure an IPSec tunnel using Aggressive Mode between the X-family and a Netscreen NS25. 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 Netscreen, and the tunnel must use Aggressive Mode IKE.

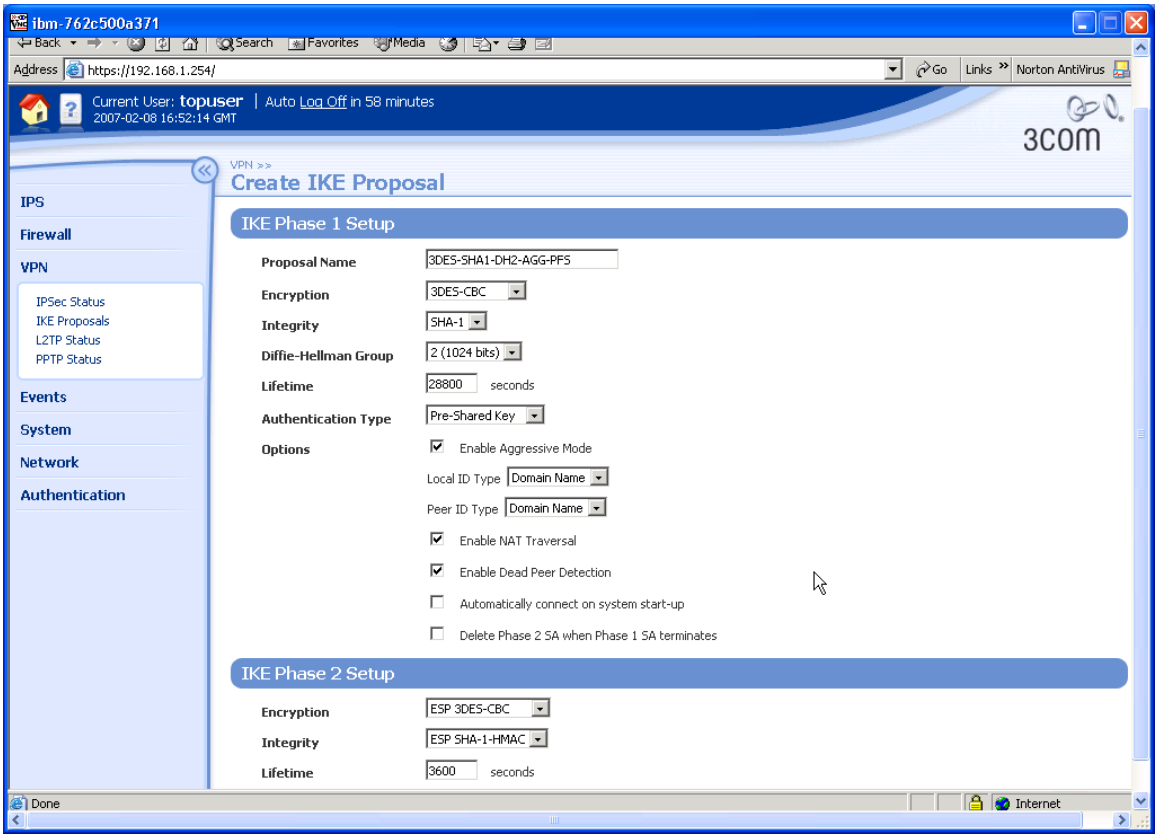
Key Setup Information

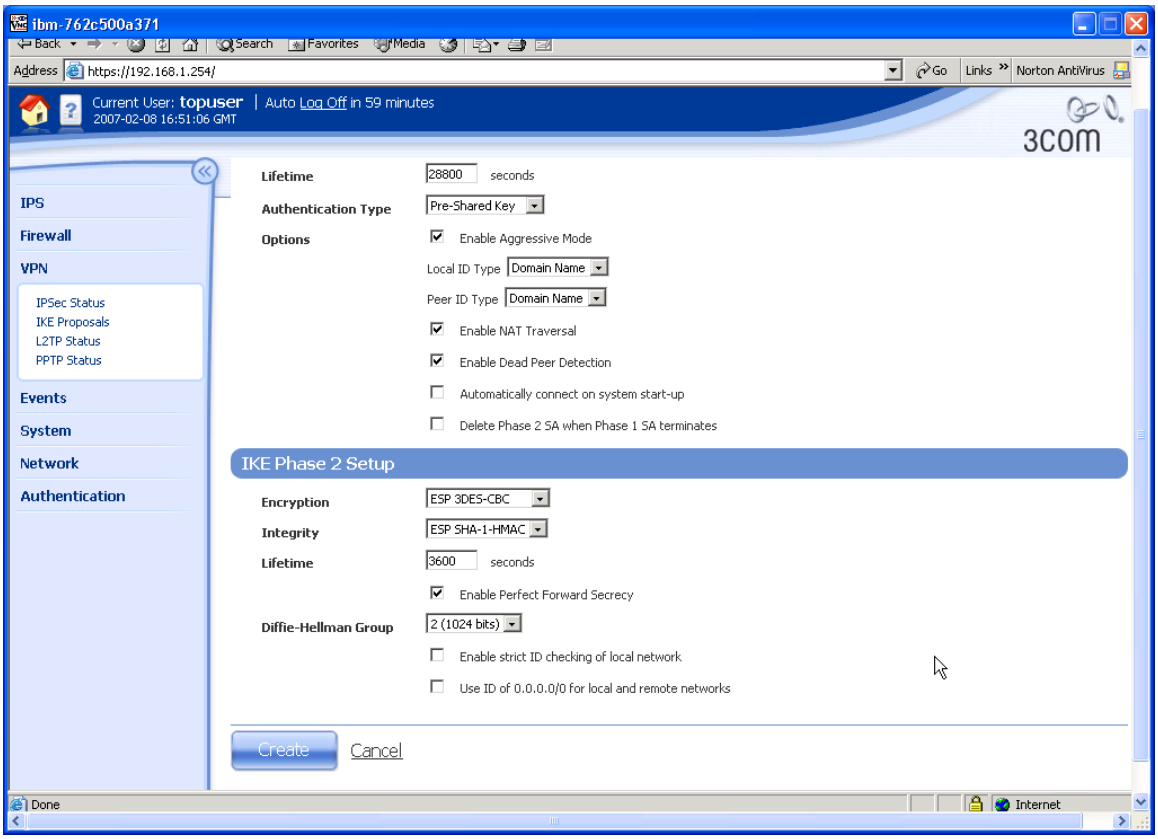
Keying Mode	IKE
IKE Mode	Aggressive Mode with Perfect Forward Secrecy
SA Authentication Method	Pre-shared Key
Keying Group DH	DH (Diffie Hellman) Group 2
Encryption and Data Integrity	3DES-SHA1



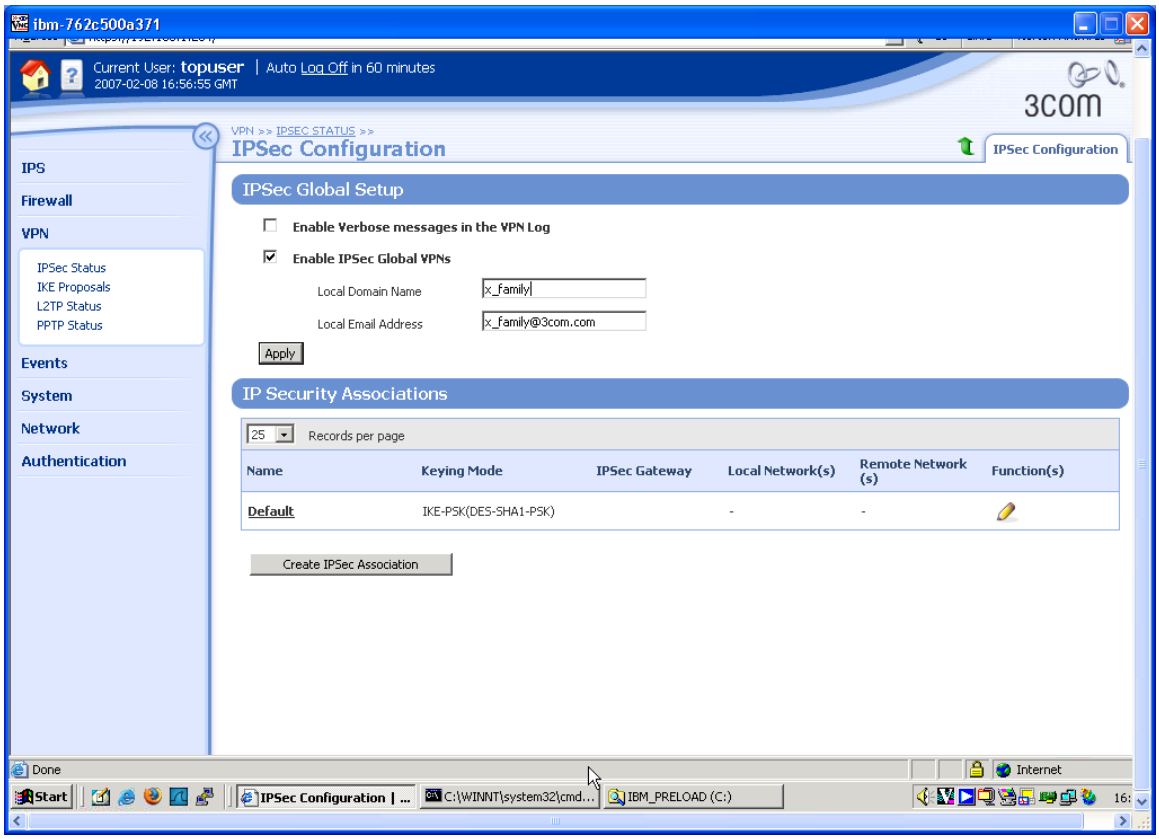
5.1 3Com X-family Configuration

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).

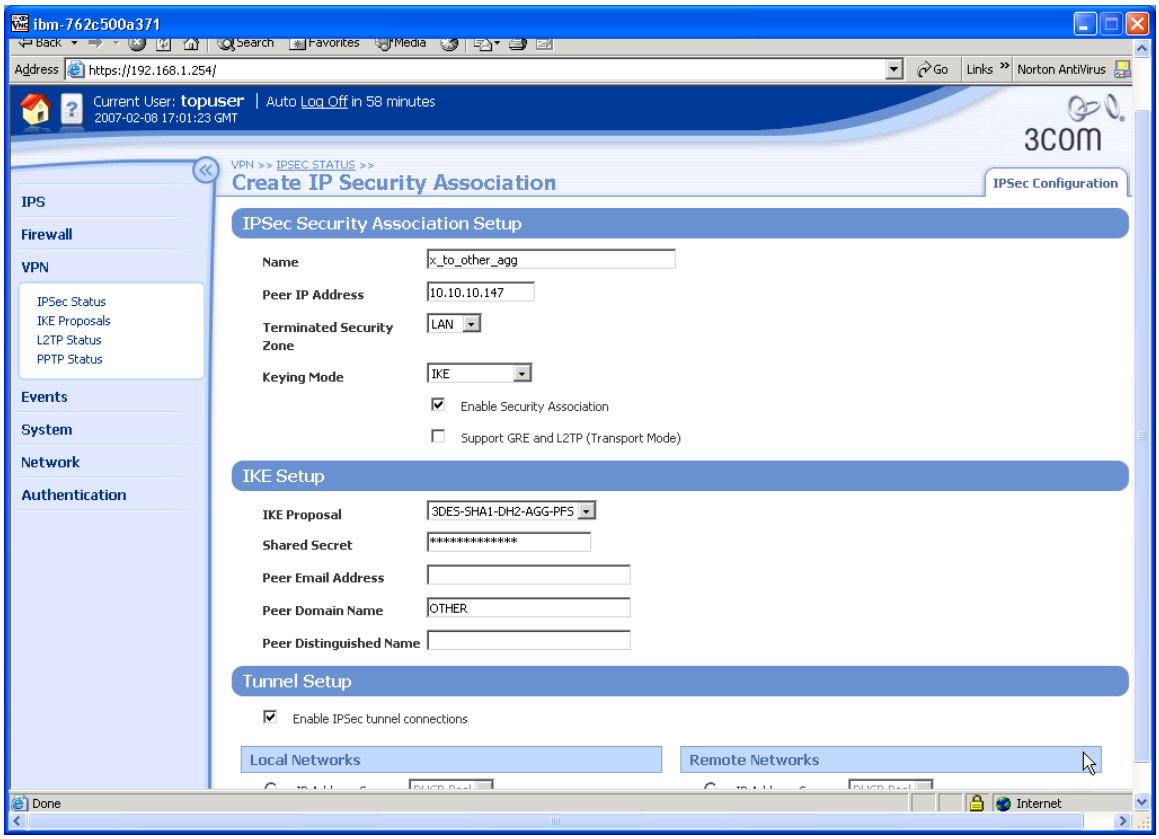


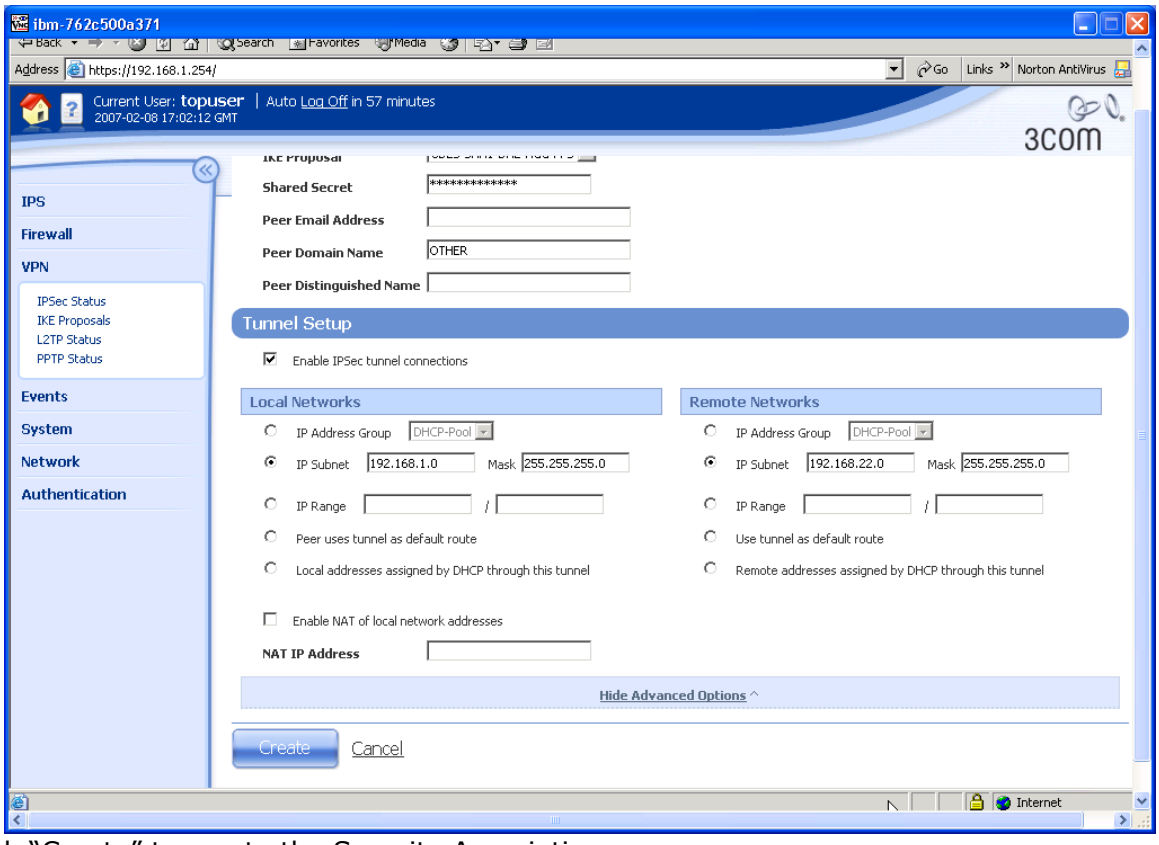


3. Click "Create" to save the new IKE Proposal.
4. Navigate to VPN -> IPSEC Status and click on the "IPSEC Configuration" tab.
5. Configure the upper part of the screen as shown below.



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.

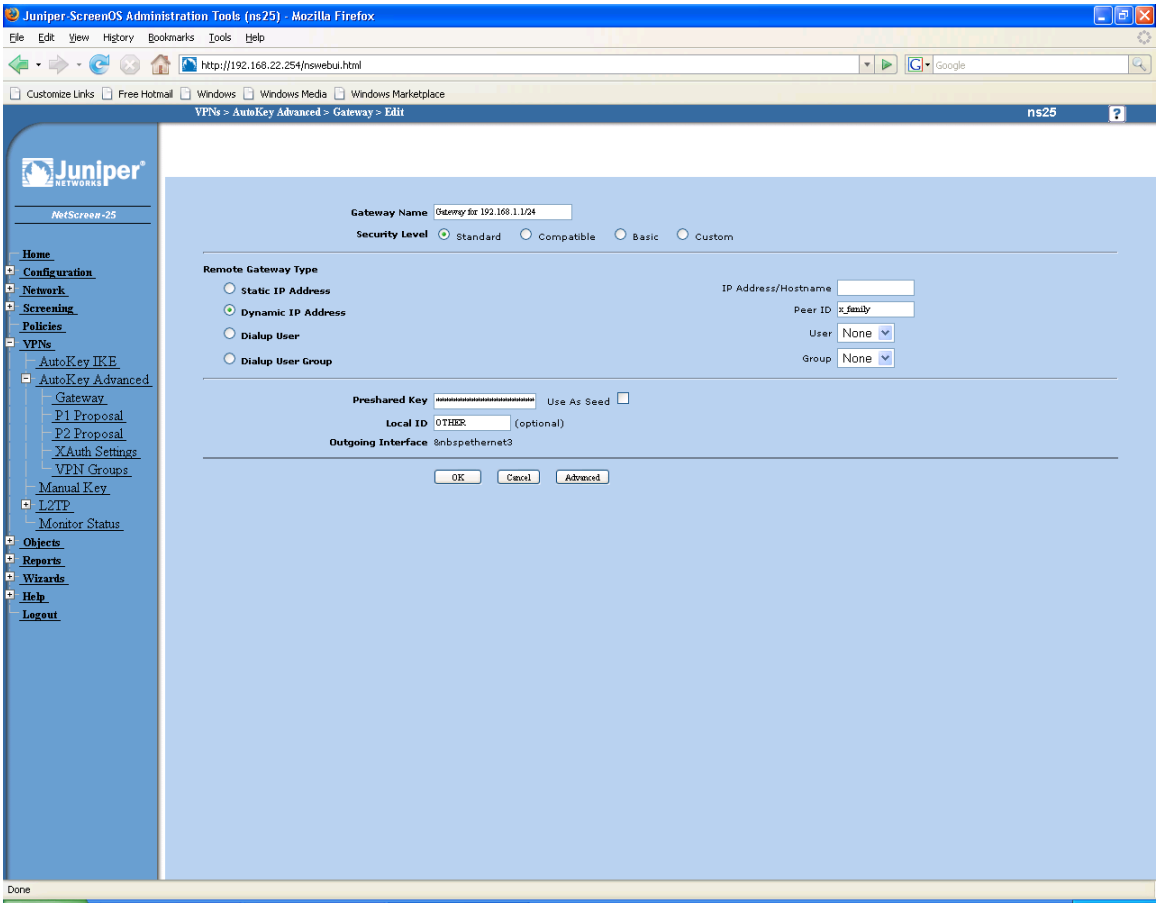




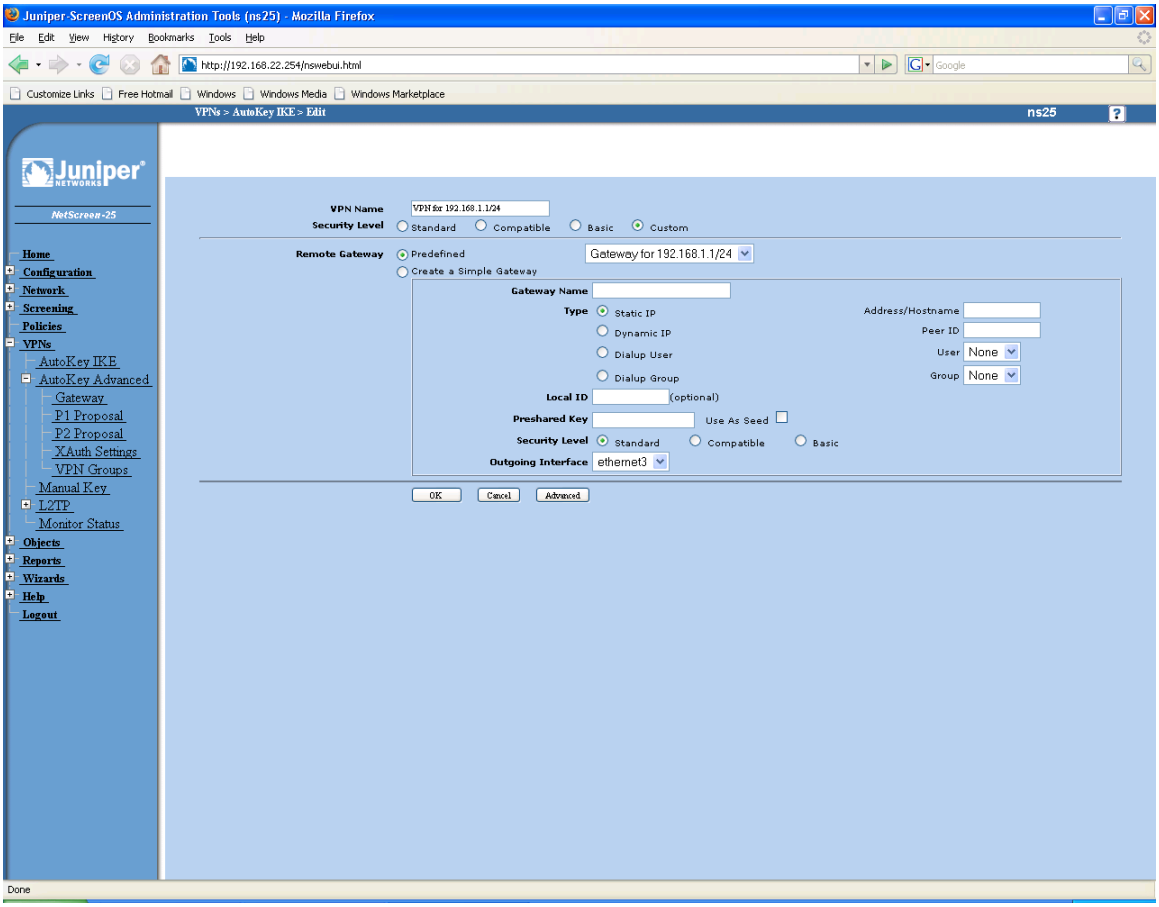
8. Click "Create" to create the Security Association.

5.2 Netscreen NS25 Configuration

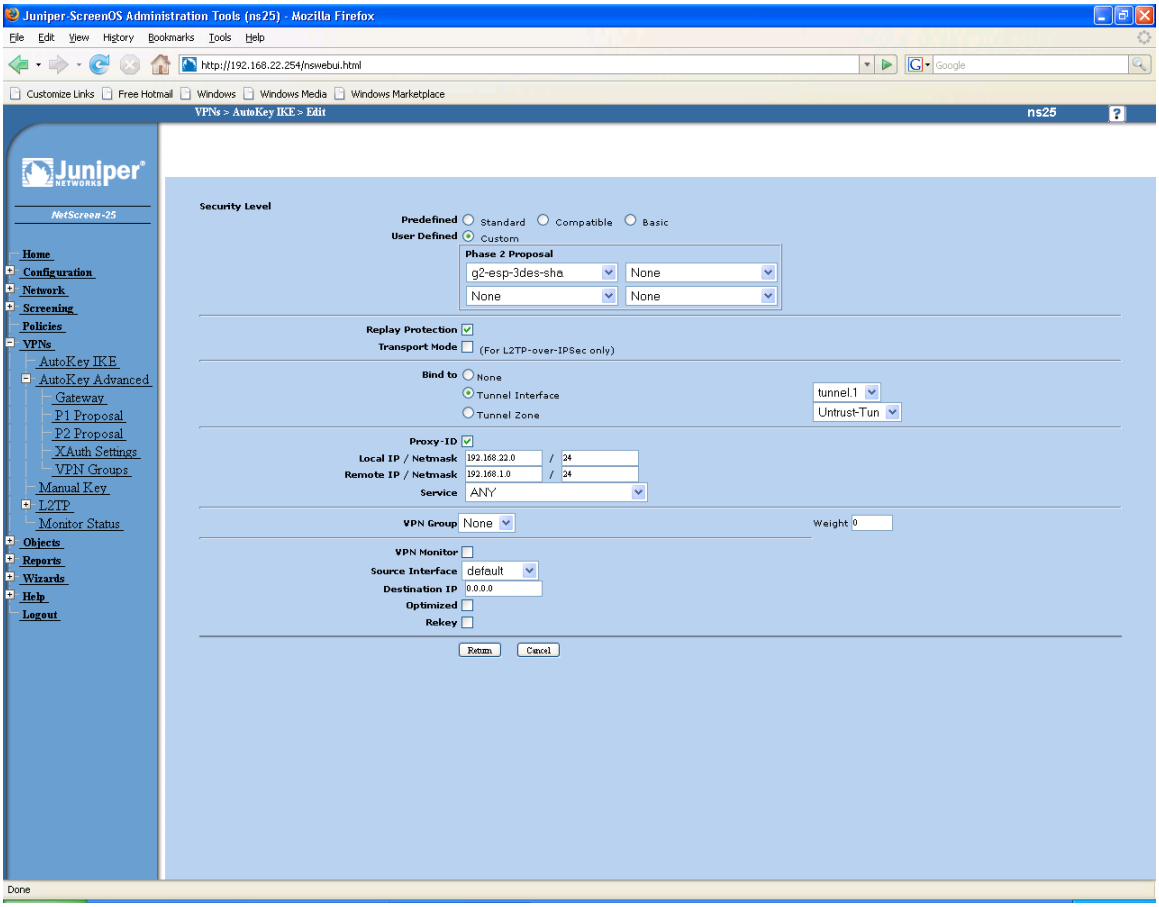
1. Open a browser on PC2, connect to https://192.168.22.254 and login to the Netscreen GUI as user "netscreen" with password "netscreen".
2. Click on the + sign to the left of "VPNs" to open up the submenus.
3. Click on the + sign to the left of "AutoKey Advanced" in the new submenu to open up another submenu.
4. Click on "Gateway" in the new submenu and click the "New" button to create a new gateway. Complete the form as shown below. Note that the peer IP address is blank 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 "Preshared Key" string entered here must be at least 8 characters and must be exactly the same as the shared secret entered on the peer device.



5. Click on "OK" to save the new Gateway.
6. Click on "AutoKey IKE". On the screen that opens click on "New" to create a new Security Association and complete the form as shown below.



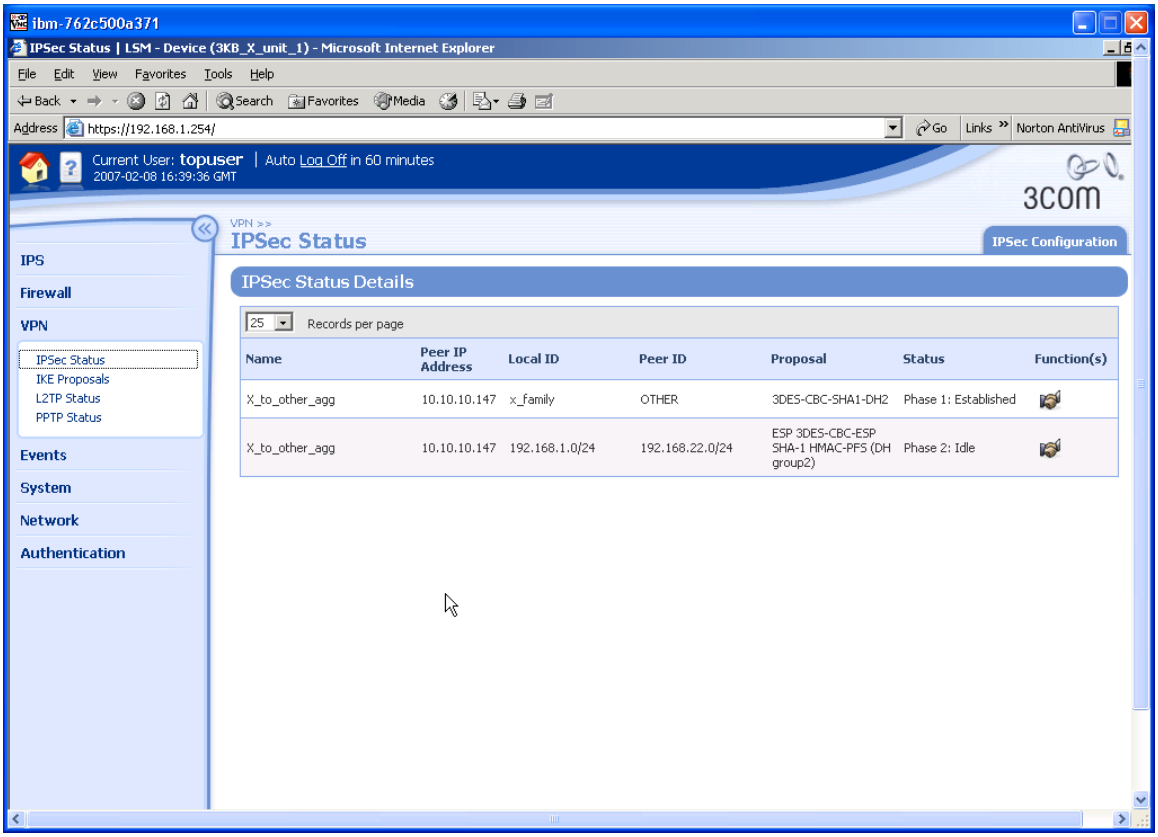
9. Click on "Advanced" and fill in the new form as show below.



10. Click on "Return" at the bottom of the form and then click on "OK" on the previous form to save the changes.

5.3 Testing the VPN with data

7. 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. Note that the tunnel will not come up if PC2 pings PC1 as the Netscreen does not know the IP address of the X-family device.



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 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
******** 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 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 rule update 7 permit ANY ANY ping
firewall rule update 7 schedule always timeout 30 logging disable
firewall rule update 7 src-addr all
firewall rule update 7 dst-addr all
firewall rule update 7 bandwidth disable
firewall rule update 7 authentication disable
firewall rule update 7 position 7
firewall rule update 7 comment ""
firewall rule update 7 remote-logging disable
firewall rule enable 7
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
vpn ipsec sa x_family_to_other key ike proposal 3DES-SHA1-DH2 shared-
secret ****
****
vpn ipsec sa x_family_to_other transport disable
vpn ipsec sa x_family_to_other peer 10.10.10.147
vpn ipsec sa x_family_to_other zone LAN
vpn ipsec sa x_family_to_other tunnel remote subnet 192.168.22.0 netmask
255.255
.255.0
vpn ipsec sa x_family_to_other tunnel local subnet 192.168.1.0 netmask
255.255.2
55.0
vpn ipsec sa x_family_to_other tunnel nat disable
vpn ipsec sa x_family_to_other tunnel enable
vpn ipsec sa x_family_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 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#
```

6.1.2 Netscreen NS25 configuration file

```
ns25-> get config
get config
Total Config size 2756:
set clock timezone 0
set vrouter trust-vr sharable
unset vrouter "trust-vr" auto-route-export
set auth-server "Local" id 0
set auth-server "Local" server-name "Local"
set auth default auth server "Local"
set admin name "labuser"
set admin password "nO1/IYrfC4ZOcjlEUsbITpLtn2EQ1n"
set admin auth timeout 10
set admin auth server "Local"
set admin format dos
set zone "Trust" vrouter "trust-vr"
set zone "Untrust" vrouter "trust-vr"
set zone "DMZ" vrouter "trust-vr"
set zone "VLAN" vrouter "trust-vr"
set zone "Trust" tcp-rst
set zone "Untrust" block
unset zone "Untrust" tcp-rst
set zone "MGT" block
set zone "DMZ" tcp-rst
set zone "VLAN" block
set zone "VLAN" tcp-rst
set zone "Untrust" screen tear-drop
set zone "Untrust" screen syn-flood
set zone "Untrust" screen ping-death
```

```
set zone "Untrust" screen ip-filter-src
set zone "Untrust" screen land
set zone "V1-Untrust" screen tear-drop
set zone "V1-Untrust" screen syn-flood
set zone "V1-Untrust" screen ping-death
set zone "V1-Untrust" screen ip-filter-src
set zone "V1-Untrust" screen land
set interface "ethernet1" zone "Trust"
set interface "ethernet2" zone "Null"
set interface "ethernet3" zone "Untrust"
set interface "tunnel.1" zone "Trust"
unset interface vlan1 ip
set interface ethernet1 ip 192.168.22.254/24
set interface ethernet1 nat
set interface ethernet3 ip 10.10.10.147/24
set interface ethernet3 route
set interface tunnel.1 ip unnumbered interface ethernet1
unset interface vlan1 bypass-others-ipsec
unset interface vlan1 bypass-non-ip
set interface ethernet1 ip manageable
set interface ethernet3 ip manageable
set interface ethernet3 manage ping
set hostname ns25
set ike gateway "Gateway for 192.168.1.1/24" address 10.10.20.147 Main
outgoing-interface

"ethernet3" preshare "g/dqSAKkNiW6Vis+hJCVLLcK5jnThXew6A==" sec-level
standard
set ike gateway "Gateway for 192.168.1.1/24" cert peer-ca all
set ike respond-bad-spi 1
set vpn "VPN for 192.168.1.1/24" gateway "Gateway for 192.168.1.1/24"
replay tunnel idletime

0 proposal "nopfs-esp-3des-sha"
set vpn "VPN for 192.168.1.1/24" id 1 bind interface tunnel.1
set pki authority default scep mode "auto"
set pki x509 default cert-path partial
set policy id 1 from "Trust" to "Untrust"  "Any" "Any" "ANY" permit
set policy id 2 from "Untrust" to "Trust"  "Any" "Any" "ANY" permit
set vpn "VPN for 192.168.1.1/24" proxy-id local-ip 192.168.22.0/24
remote-ip 192.168.1.0/24

"ANY"
set ssh version v2
set config lock timeout 5
set snmp port listen 161
set snmp port trap 162
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset add-default-route
set route  0.0.0.0/0 interface ethernet3 gateway 10.10.10.1
set route  192.168.1.0/24 interface tunnel.1
exit
ns25->
```

6.2 Aggressive Mode

6.2.1 "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 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
******** 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 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 rule update 7 permit ANY ANY ping
firewall rule update 7 schedule always timeout 30 logging disable
firewall rule update 7 src-addr all
firewall rule update 7 dst-addr all
firewall rule update 7 bandwidth disable
firewall rule update 7 authentication disable
firewall rule update 7 position 7
firewall rule update 7 comment ""
firewall rule update 7 remote-logging disable
firewall rule enable 7
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
vpn ipsec sa x_family_to_other key ike proposal 3DES-SHA1-DH2-AGG-PFS
shared-sec
ret ******** peer-id OTHER
vpn ipsec sa x_family_to_other transport disable
vpn ipsec sa x_family_to_other peer 10.10.10.147
vpn ipsec sa x_family_to_other zone LAN
vpn ipsec sa x_family_to_other tunnel remote subnet 192.168.22.0 netmask
255.255
.255.0
vpn ipsec sa x_family_to_other tunnel local subnet 192.168.1.0 netmask
255.255.2
55.0
vpn ipsec sa x_family_to_other tunnel nat disable
vpn ipsec sa x_family_to_other tunnel enable
vpn ipsec sa x_family_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 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 Netscreen NS25 configuration file

```
ns25-> get config
Total Config size 2841:
set clock timezone 0
set vrouter trust-vr sharable
unset vrouter "trust-vr" auto-route-export
set auth-server "Local" id 0
set auth-server "Local" server-name "Local"
set auth default auth server "Local"
set admin name "labuser"
set admin password "nO1/IYrfC4ZOcjlEUsbITpLtn2EQ1n"
set admin auth timeout 10
set admin auth server "Local"
set admin format dos
set zone "Trust" vrouter "trust-vr"
set zone "Untrust" vrouter "trust-vr"
set zone "DMZ" vrouter "trust-vr"
set zone "VLAN" vrouter "trust-vr"
set zone "Trust" tcp-rst
set zone "Untrust" block
unset zone "Untrust" tcp-rst
set zone "MGT" block
set zone "DMZ" tcp-rst
set zone "VLAN" block
set zone "VLAN" tcp-rst
set zone "Untrust" screen tear-drop
set zone "Untrust" screen syn-flood
set zone "Untrust" screen ping-death
set zone "Untrust" screen ip-filter-src
set zone "Untrust" screen land
set zone "V1-Untrust" screen tear-drop
set zone "V1-Untrust" screen syn-flood
```

```
set zone "V1-Untrust" screen ping-death
set zone "V1-Untrust" screen ip-filter-src
set zone "V1-Untrust" screen land
set interface "ethernet1" zone "Trust"
set interface "ethernet2" zone "Null"
set interface "ethernet3" zone "Untrust"
set interface "tunnel.1" zone "Trust"
unset interface vlan1 ip
set interface ethernet1 ip 192.168.22.254/24
set interface ethernet1 nat
set interface ethernet3 ip 10.10.10.147/24
set interface ethernet3 route
set interface tunnel.1 ip unnumbered interface ethernet1
unset interface vlan1 bypass-others-ipsec
unset interface vlan1 bypass-non-ip
set interface ethernet1 ip manageable
set interface ethernet3 ip manageable
set interface ethernet3 manage ping
set hostname ns25
set ike gateway "Gateway for 192.168.1.1/24" address 0.0.0.0 id
"x_family" Main local-id

"OTHER" outgoing-interface "ethernet3" preshare
"g/dqSAKkNiW6Vis+hJCVLLcK5jnThXew6A=="

sec-level standard
set ike gateway "Gateway for 192.168.1.1/24" cert peer-ca all
unset ike gateway "Gateway for 192.168.1.1/24" nat-traversal
set ike respond-bad-spi 1
set vpn "VPN for 192.168.1.1/24" gateway "Gateway for 192.168.1.1/24"
replay tunnel idletime

0 proposal "g2-esp-3des-sha"
set vpn "VPN for 192.168.1.1/24" id 1 bind interface tunnel.1
set pki authority default scep mode "auto"
set pki x509 default cert-path partial
set policy id 1 from "Trust" to "Untrust"  "Any" "Any" "ANY" permit
set policy id 2 from "Untrust" to "Trust"  "Any" "Any" "ANY" permit
set vpn "VPN for 192.168.1.1/24" proxy-id local-ip 192.168.22.0/24
remote-ip 192.168.1.0/24

"ANY"
set ssh version v2
set config lock timeout 5
set snmp port listen 161
set snmp port trap 162
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset add-default-route
set route  0.0.0.0/0 interface ethernet3 gateway 10.10.10.1
set route  192.168.1.0/24 interface tunnel.1
exit
ns25->
```