IPSec VPN for OfficeConnect 3CR858-91 to “X” unit

Document Version:	1.2
Publication Date:	22 January 2007
Description:	Configuring site-to-site VPNs from OfficeConnect Cable/DSL Router 3CR858-91 to 3Com “X” unit
Product:	3Com “X” unit
3Com TOS Version:	2.5.0.6682
OfficeConnect 3CR858-91 Software Version:	V1.091-168 (Sep 28 2006 12:06:53)

1 Overview

This technical note describes how to setup IPSec VPN tunnels between a 3Com "X" unit and the OfficeConnect 3CR858-91.

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.

2 Pre-Configuration before setting up VPNs

2.1 3Com "X" unit Pre-Configuration

2.1.1 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).

```
Would you like to modify the host management port options? <Y,[N]>:
Would you like to modify timekeeping options? <Y,[N]>:
Would you like to modify the network deployment mode? <Y,[N]>:
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]: c
Enter the number of the entry you want to change []: 2
Mode (static, dhcp, pppoe, pptp, l2tp) [dhcp]: static
IP address []: 10.0.0.146
Mask [255.255.255.0]:
Virtual interfaces:

Id  Type      Mode    IP Address       Subnet Mask      NAT
 1  internal  static  192.168.1.254    255.255.255.0    external-ip
 2  external  static  10.0.0.146       255.255.255.0    disable
 3  <empty>
 4  <empty>
 5  <empty>
 6  <empty>

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

Would you like to modify default gateway? <Y,[N]>:
Would you like to modify security zones? <Y,[N]>:
Would you like to modify security zone to virtual interface mapping? <Y,[N]>:
Would you like to configure DNS? <Y,[N]>:
```

```
Would you like to modify firewall policy rules? <Y,[N]>:y
The current state of firewall rules is as follows:

 ID       Action       Source       Destination       Service                E
 1        permit       LAN          WAN               ANY                    X
 2        permit       WAN          this-device       vpn-protocols          X
 3        permit       LAN          this-device       management             X
 4        permit       LAN          this-device       network-protocols      X
Key: (E)nabled
Modifying the firewall rules via this wizard resets the rules to a
default state and allows you to configure basic policies for Internet access,
web filtering, and device management.

Do you want to continue? <Y,[N]>:
Would you like to enable SMS-based configuration? <Y,[N]>:
Would you like to modify the Web and CLI Server options? <Y,[N]>:
Would you like to restrict SMS access? <Y,[N]>:
Would you like to modify the Ethernet ports? <Y,[N]>:
Would you like to modify the default Email contact? <Y,[N]>:

PG_DUT#
```

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.

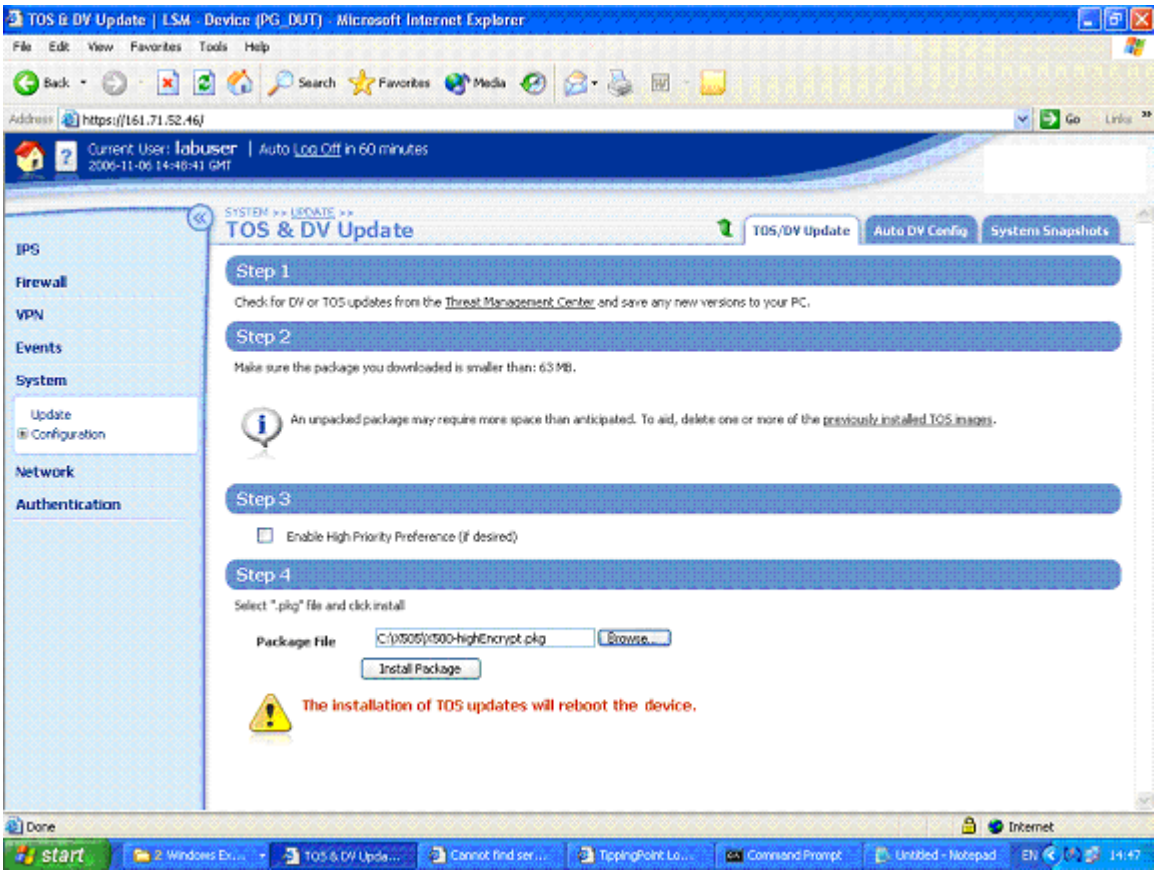
Firewall rules – the firewall rules in the factory default configuration will be sufficient – specifically this one:

2 permit WAN this-device vpn-protocols

2.1.2 Load the High Encryption Token

When delivered from the factory, the "X" units 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.

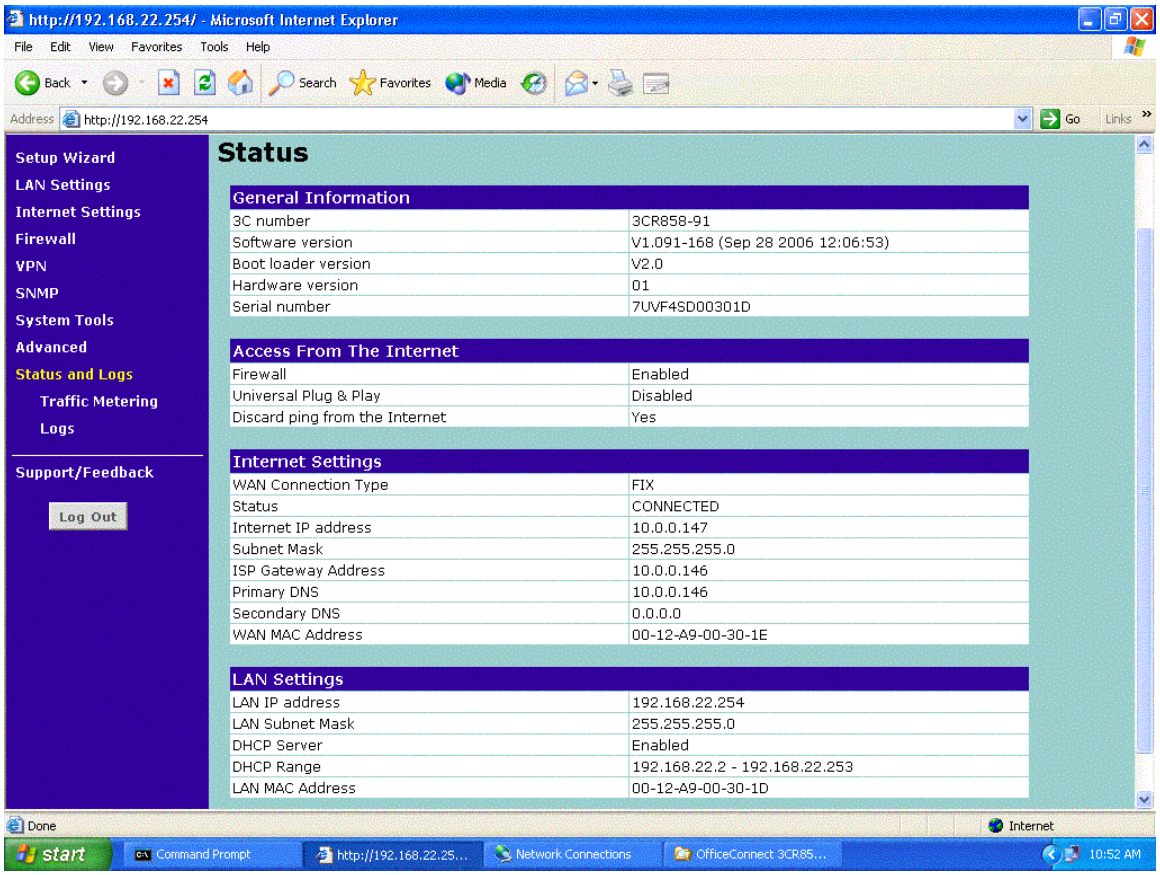
1. Acquire the High Encryption package from the TMC and load it onto PC1.
2. Open a browser on PC1, connect to https://192.168.1.254 and login as the user you set up during the OBE.
3. Navigate to System -> Update, open the "TOS/DV Update" tab and complete the form as shown below with the path of the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



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

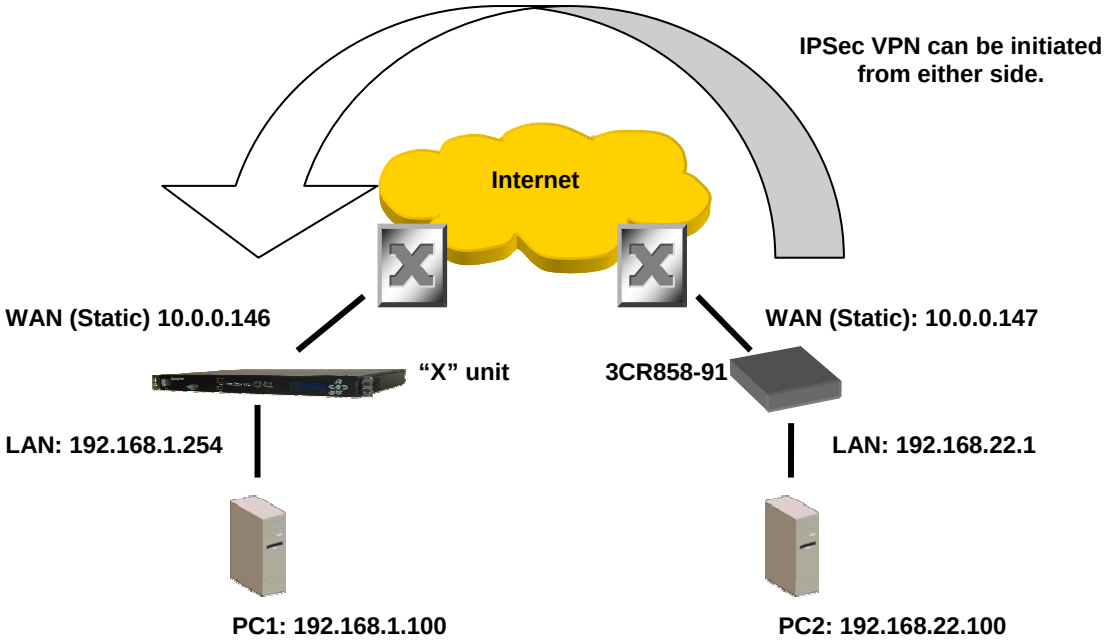
2.2 OfficeConnect 3CR858-91 Pre-Configuration

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://192.168.1.1 and login to the OfficeConnect GUI as "admin".
3. The setup wizard will run. Set the password and time options as required and select static for the Connection Type. Set the IP address to be 10.0.0.147, subnet mask to 255.255.255.0 and gateway to 10.0.0.146. On the next screen set the DNS address to 10.0.0.146. On the LAN Settings screen set the IP address to 192.168.22.254 and change the IP Pool end address to be 253 - leave the rest at defaults. Just click OK on the two popups that appear – do **not** change the IP address on your browser at this time. Click Apply on the final screen.
4. Change the address on PC2 to be 192.168.22.100 subnet 255.255.255.0 gateway 192.168.22.254.
5. Open a browser on PC2, connect to https://192.168.22.1 and login to the OfficeConnect GUI. The Status page should be as shown below:



3 Configuring Main Mode Tunnel

This example shows how to configure an IPSec tunnel using Main Mode between the "X" unit and a OfficeConnect 3CR858-91. Main Mode is the recommended setting when both devices have static IP addresses that can be accessed from the public internet.

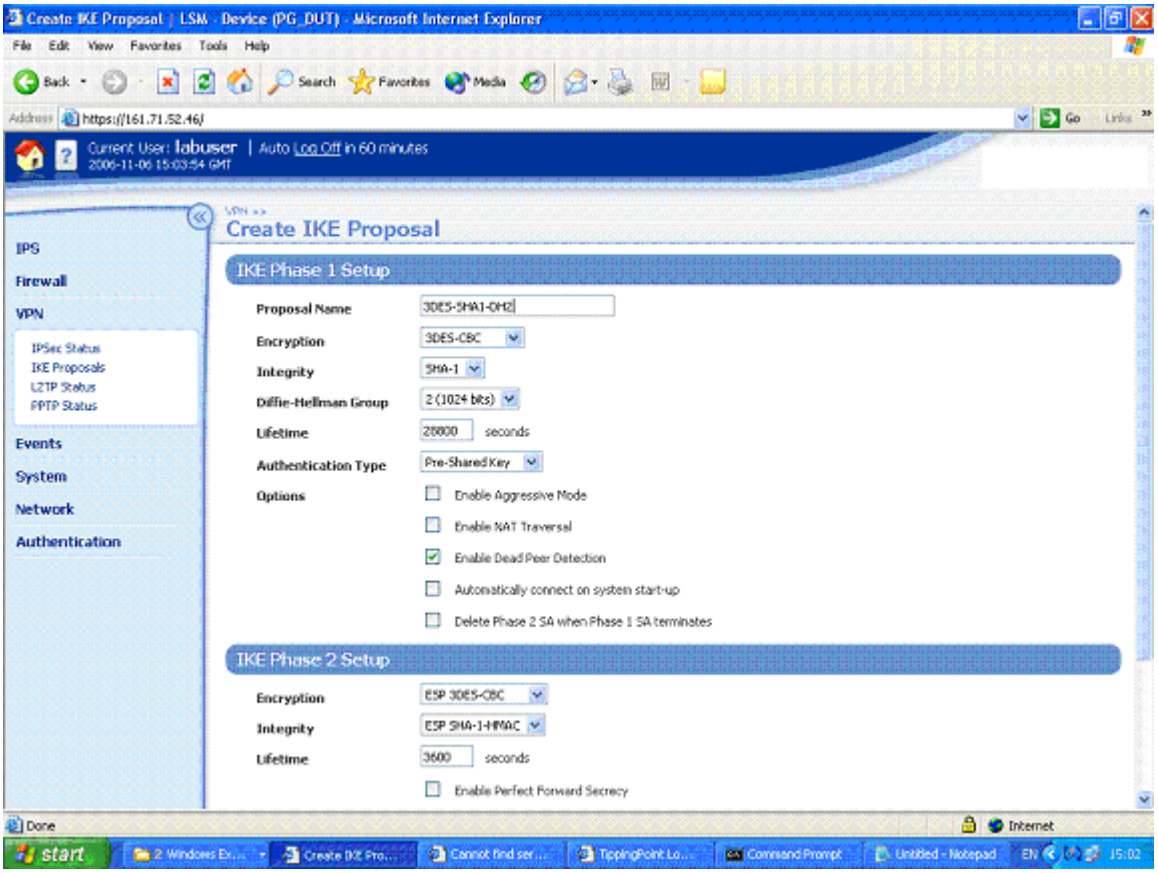


Key Setup Information

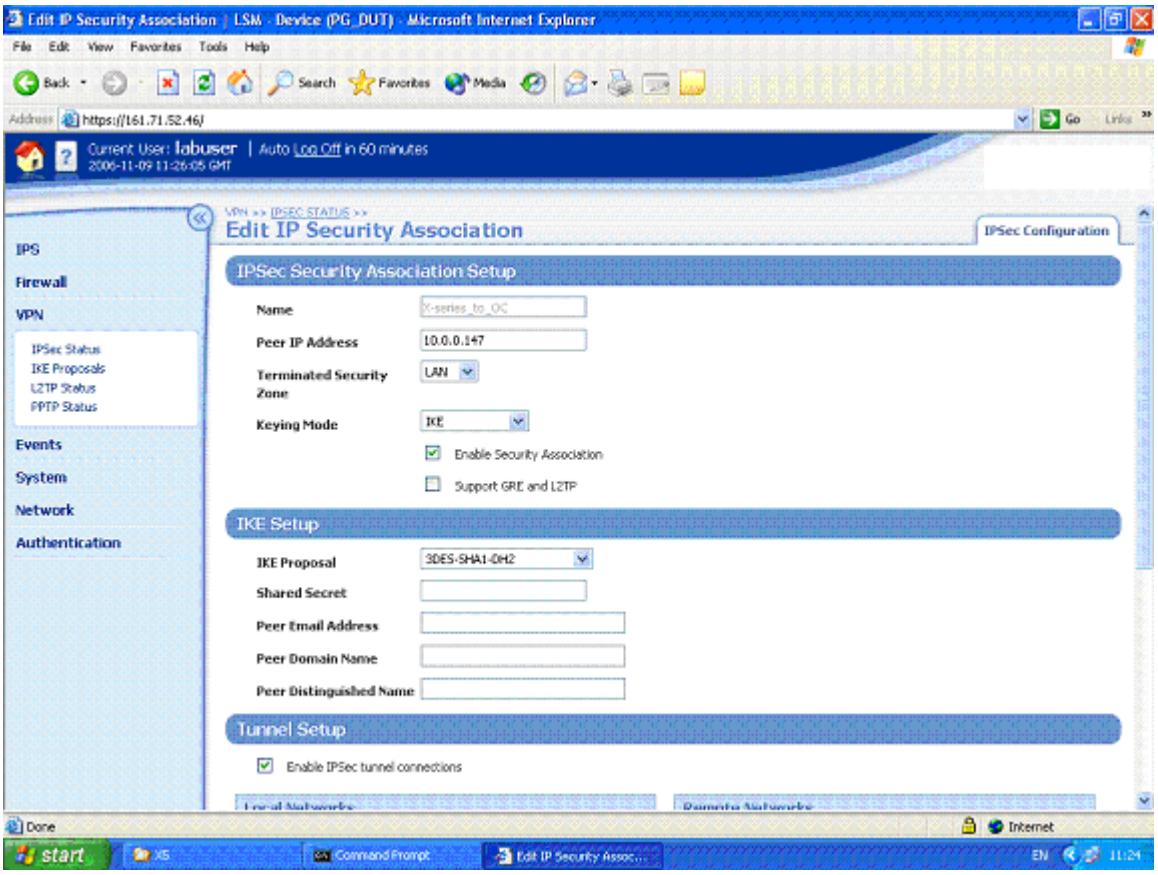
Keying Mode	IKE
IKE Mode	Main Mode
SA Authentication Method	Pre-shared Key
Keying Group DH	DH (Diffie Hellman) Group 2
Encryption and Data Integrity	3DES-SHA1

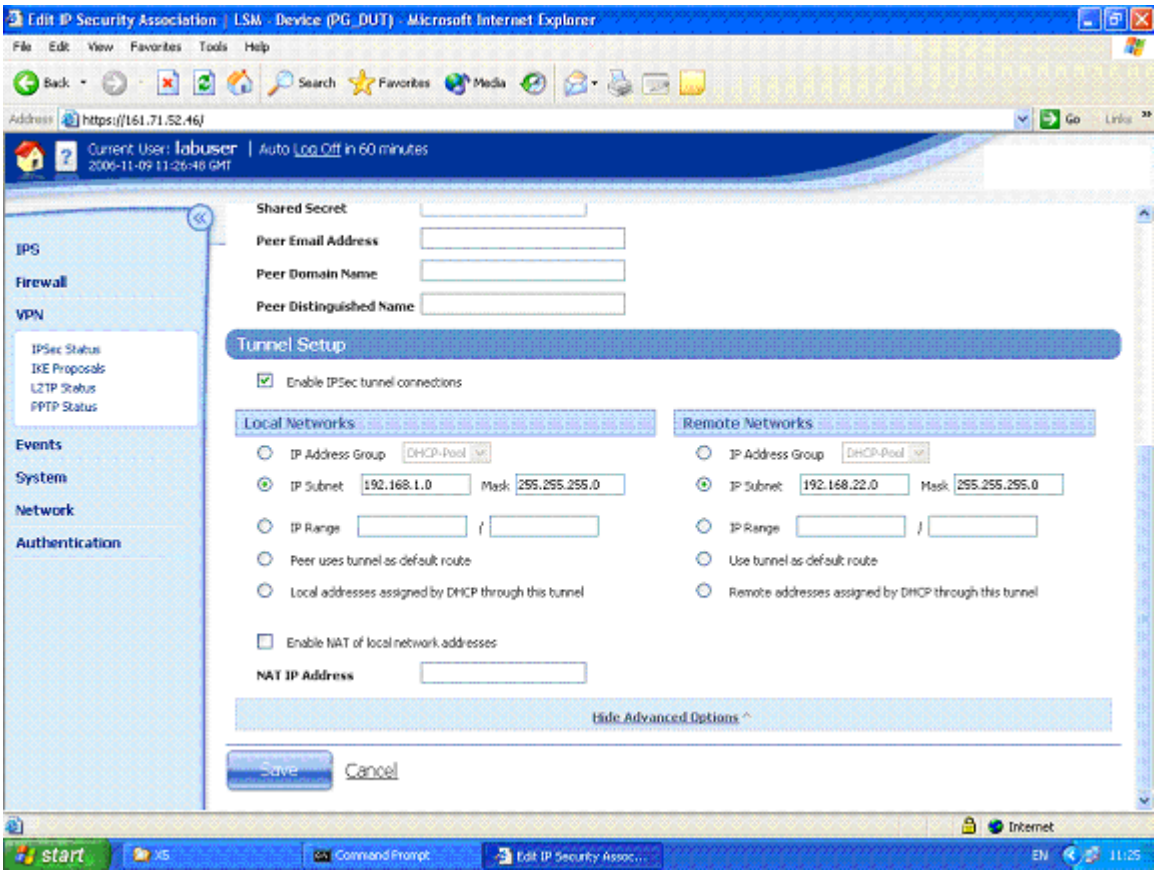
3.1 3Com "X" unit VPN Configuration

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 (type X_unit@3com.com in the "Local Email Address" box if you will be configuring aggressive mode) 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.

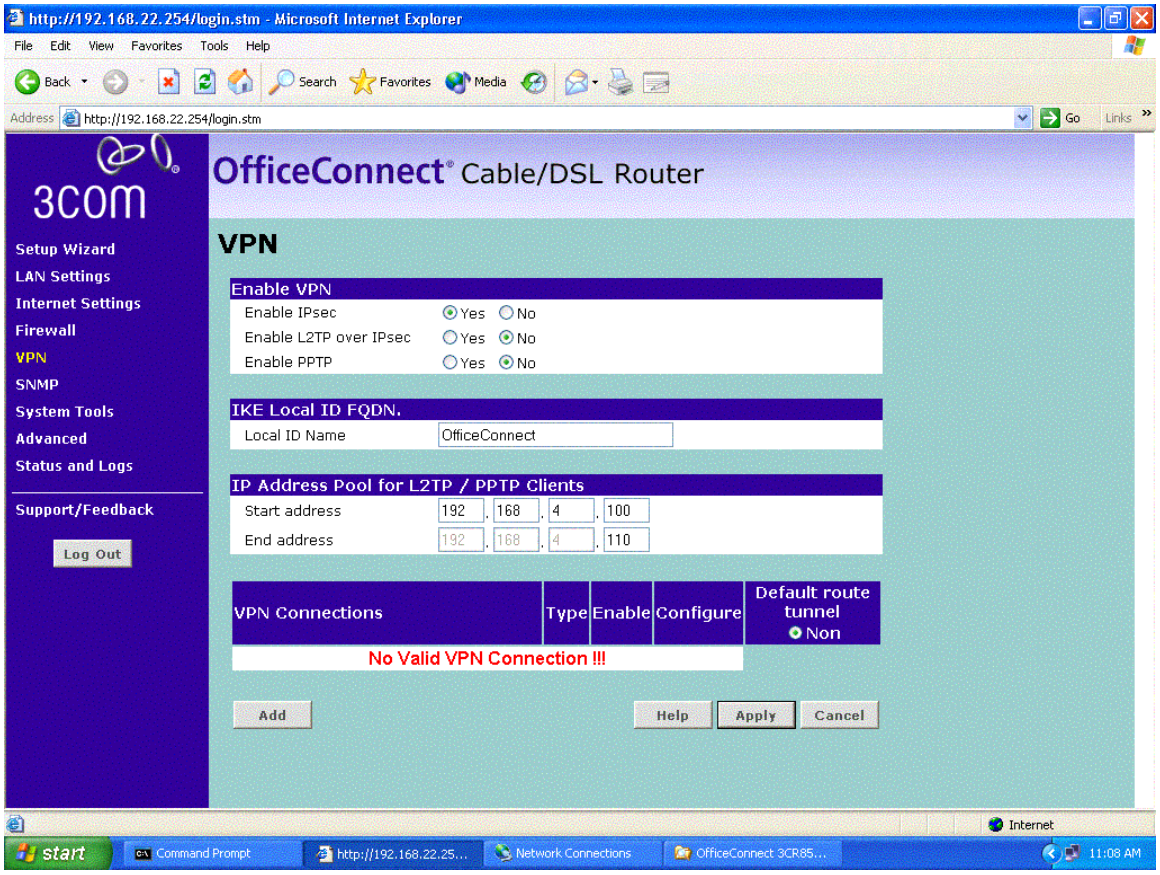

Edit IP Security Association | LSM - Device (PG_DUT) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
https://161.71.52.46/
Current User: labuser | Auto Log Off in 60 minutes
2006-11-09 11:26:05 GMT
IPS
Firewall
VPN
IPSec Status
IKE Proposals
L2TP Status
PPTP Status
Events
System
Network
Authentication
VPN >> IPSEC STATUS >>
Edit IP Security Association
IPSec Configuration
IPSec Security Association Setup
Name
X-series_to_OC
Peer IP Address
10.0.0.147
Terminated Security Zone
LAN
Keying Mode
IKE
Enable Security Association
Support GRE and L2TP
IKE Setup
IKE Proposal
3DES-SHA1-DH2
Shared Secret
Peer Email Address
Peer Domain Name
Peer Distinguished Name
Tunnel Setup
Enable IPSec tunnel connections
Done
Internet
start
Command Prompt
Edit IP Security Assoc...
EN
11:24



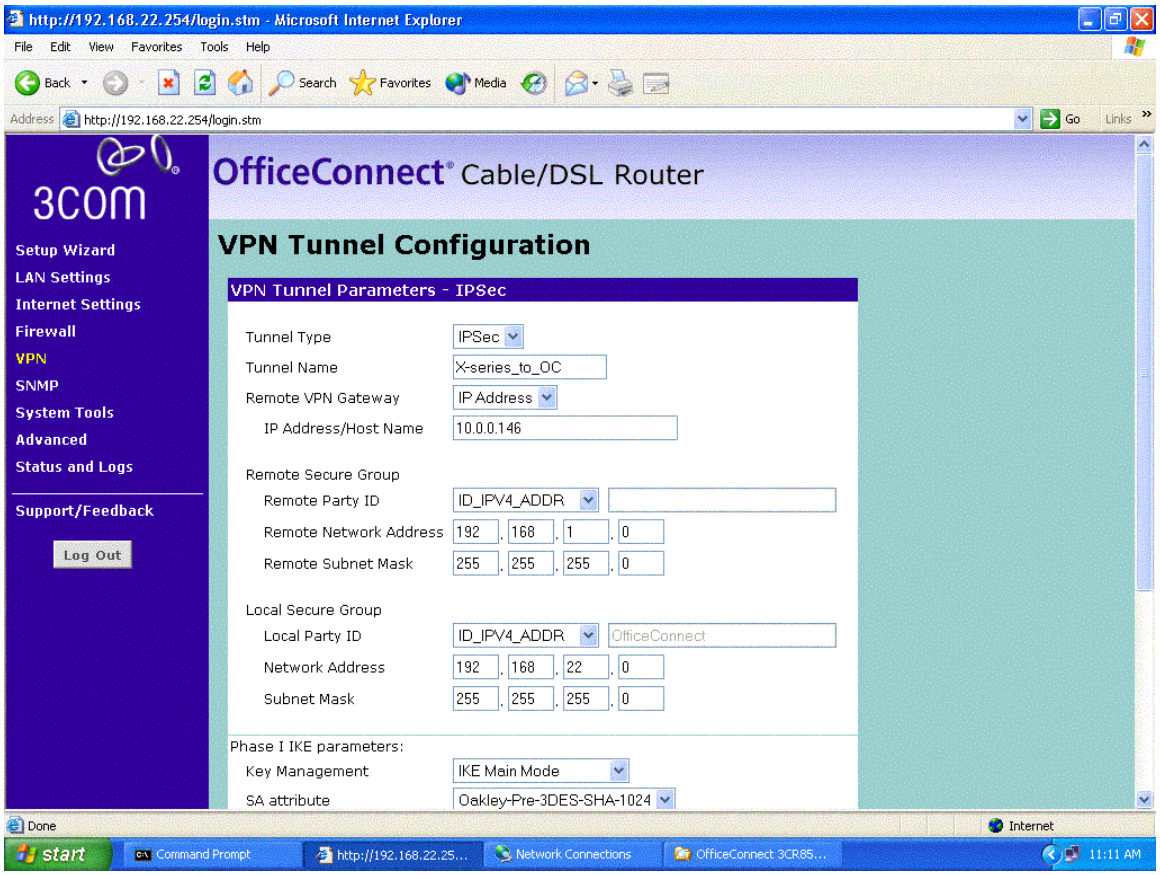
7. Click "Create" to save the new Security Association.

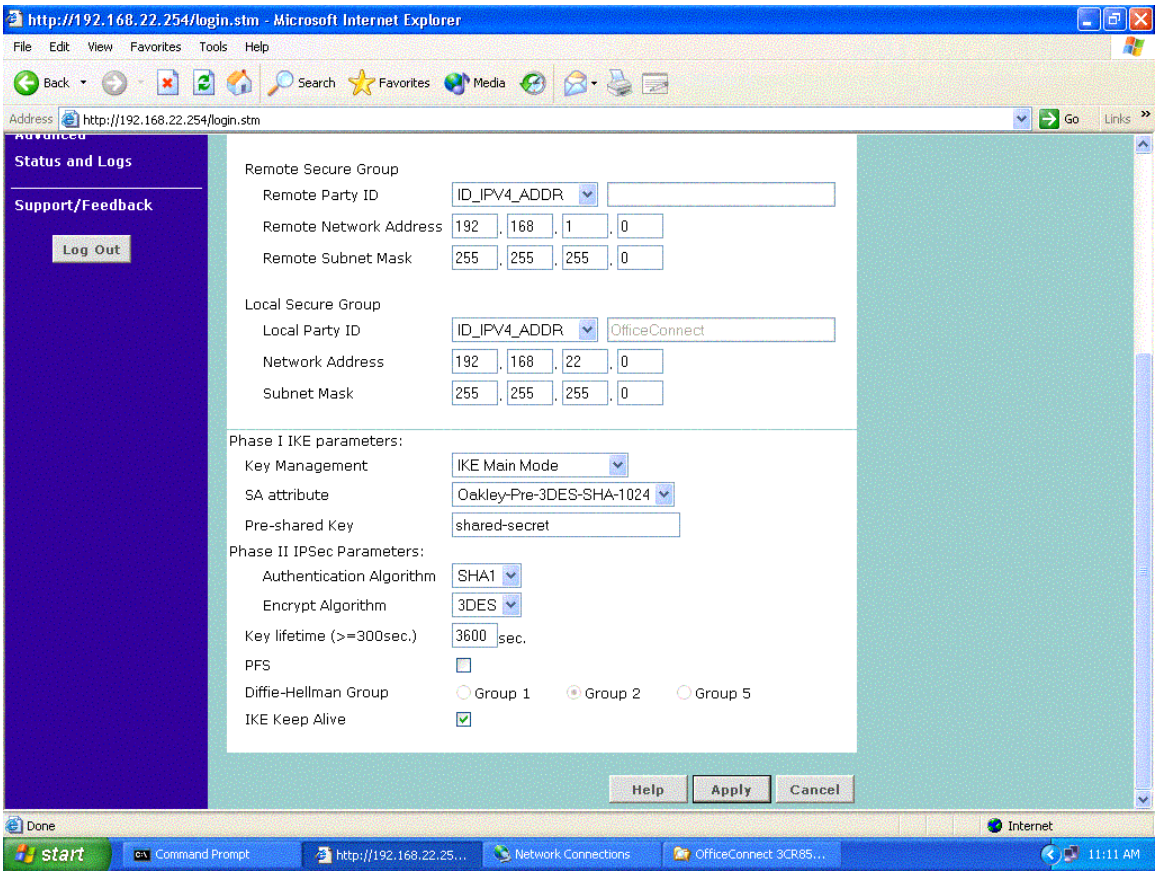
3.2 OfficeConnect 3CR858-91 Configuration

8. Open a browser on PC2, connect to https://192.168.22.1 and login to the OfficeConnect GUI.
9. Click on "VPN" to open up the global VPN page. Configure it as shown below and click "Apply".



10. Click on the "Add" button to create a VPN Connection. Complete the form provided as shown below (the form is more than one screen log so there are two screen grabs below – one for the upper part of the form and one for the lower part).

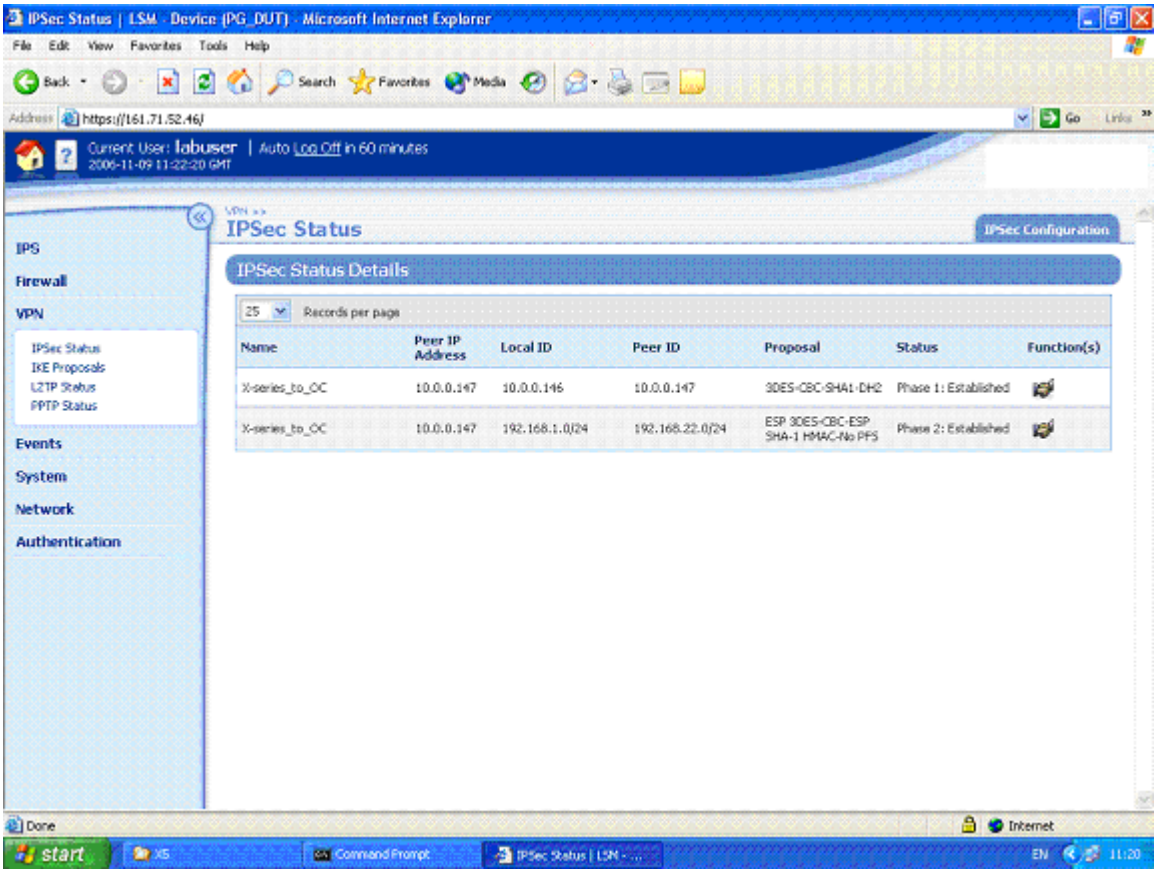

http://192.168.22.254/login.stm - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.22.254/login.stm
Go Links
3com
OfficeConnect® Cable/DSL Router
Setup Wizard
LAN Settings
Internet Settings
Firewall
VPN
SNMP
System Tools
Advanced
Status and Logs
Support/Feedback
Log Out
VPN Tunnel Configuration
VPN Tunnel Parameters - IPSec
Tunnel Type IPSec
Tunnel Name X-series_to_OC
Remote VPN Gateway IP Address
IP Address/Host Name 10.0.0.146
Remote Secure Group
Remote Party ID ID_IPV4_ADDR
Remote Network Address 192 . 168 . 1 . 0
Remote Subnet Mask 255 . 255 . 255 . 0
Local Secure Group
Local Party ID ID_IPV4_ADDR OfficeConnect
Network Address 192 . 168 . 22 . 0
Subnet Mask 255 . 255 . 255 . 0
Phase I IKE parameters:
Key Management IKE Main Mode
SA attribute Oakley-Pre-3DES-SHA-1024
Done
Internet
start
Command Prompt
http://192.168.22.25...
Network Connections
OfficeConnect 3CR85...
11:11 AM



11. Click on "Apply" to save the new VPN Connection.

3.3 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" unit. One or two pings may be lost while the tunnel establishes but then all subsequent pings should be successful.



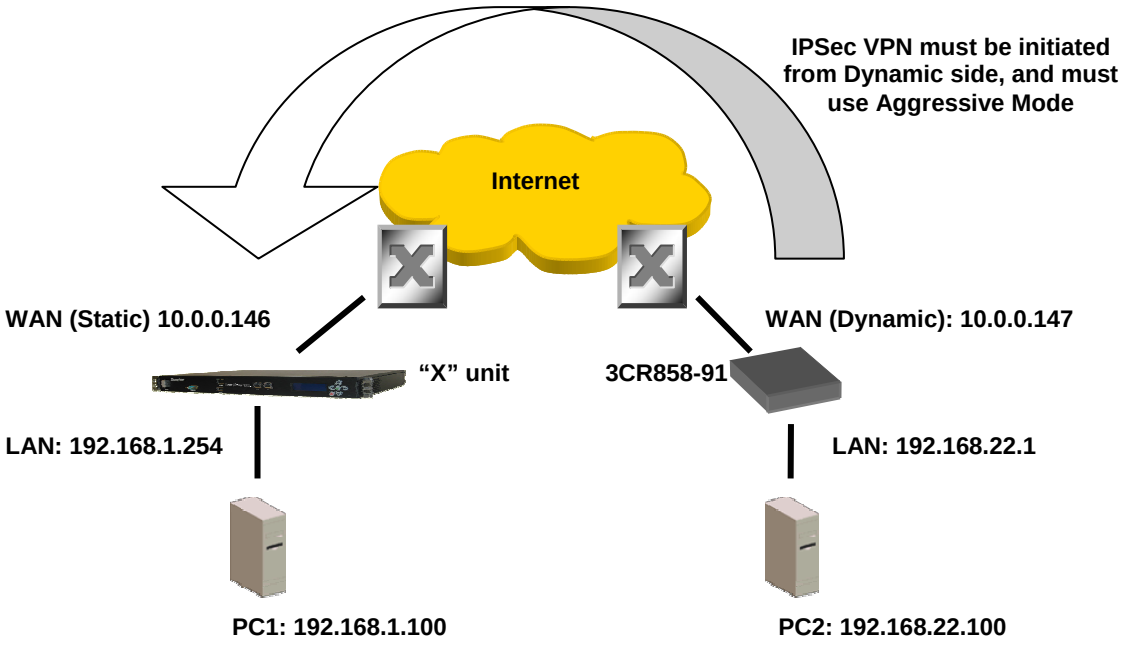
4 Aggressive Mode Tunnel

This example shows how to configure an IPSec tunnel using Aggressive Mode between the "X" unit and a OfficeConnect 3CR858-91. 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 OfficeConnect receives a dynamic IP address (through PPPoE, PPTP, DHCP or L2TP) from the Internet Service Provider. The OfficeConnect must initiate the VPN back to the "X" unit, and the tunnel must use Aggressive Mode IKE.

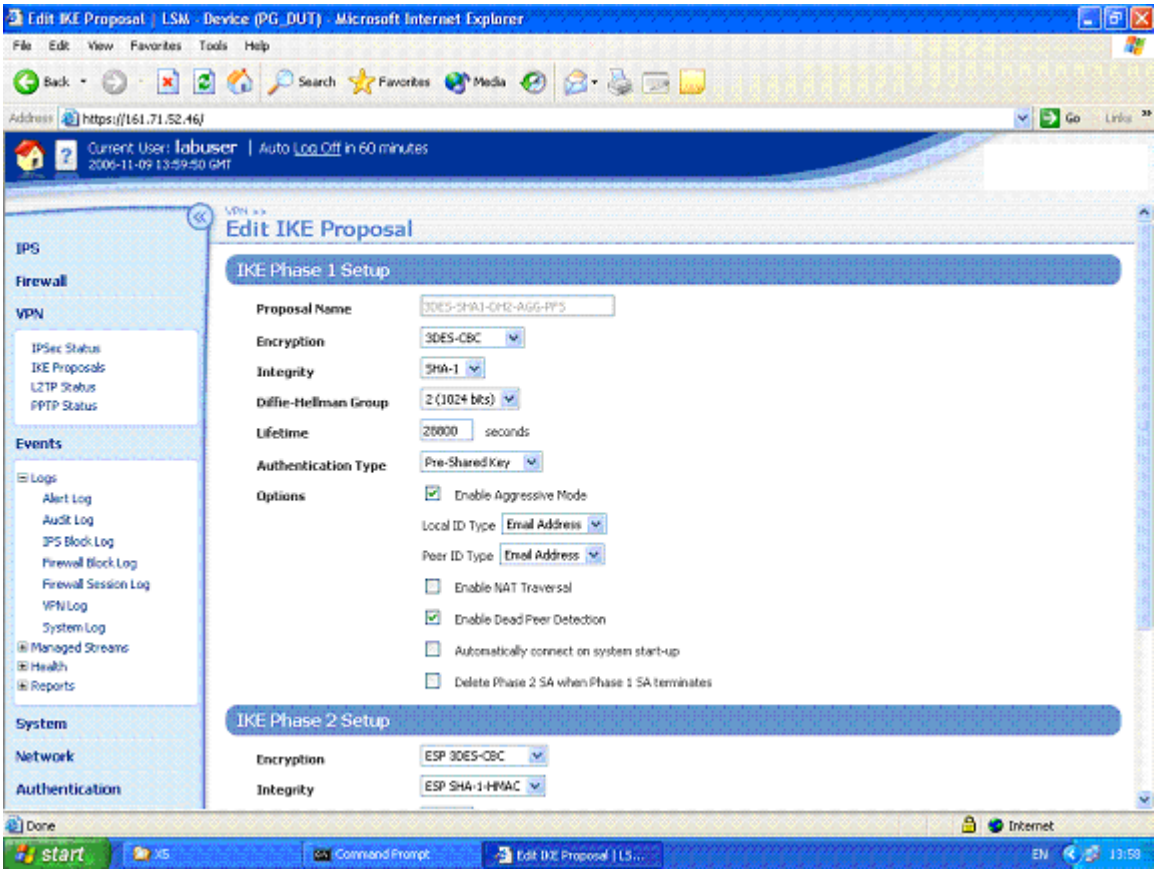
Key Setup Information

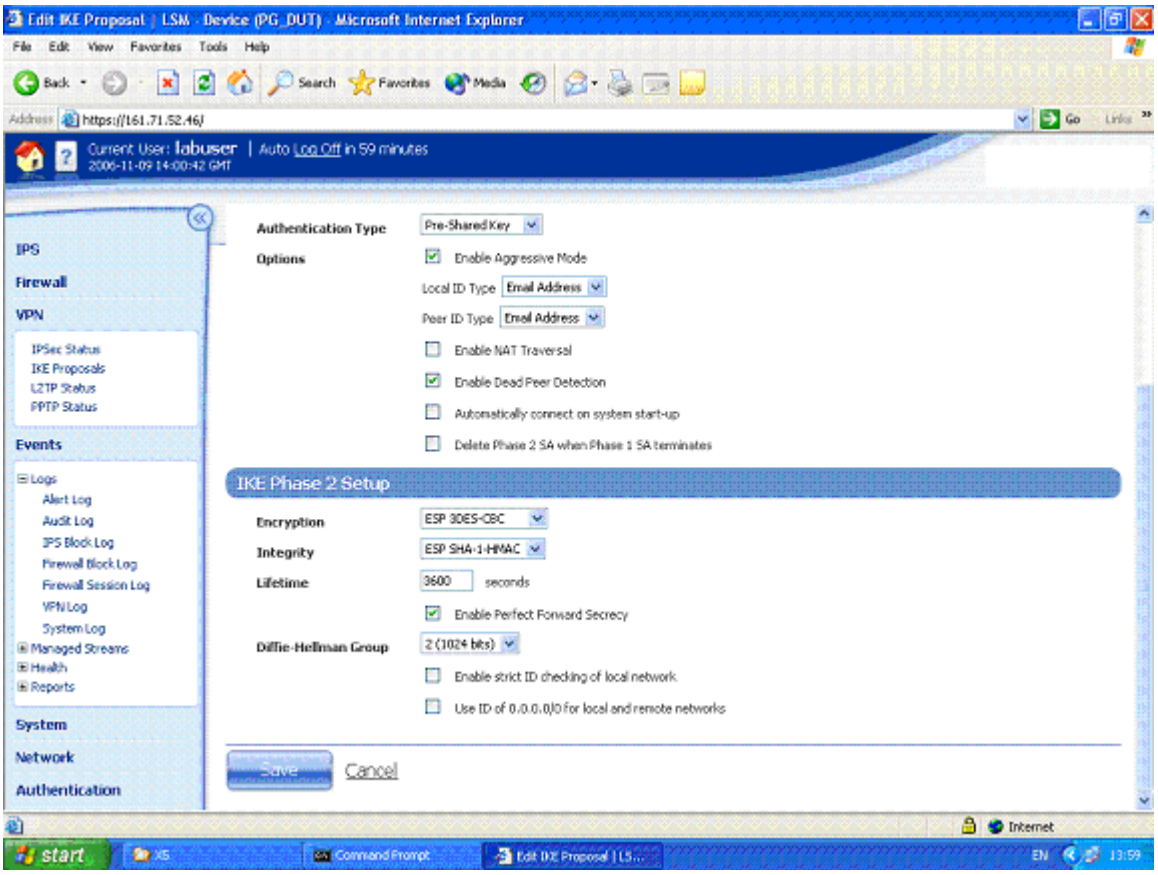
Keying Mode	IKE
IKE Mode	Aggressive Mode with Perfect Forward Secrecy
SA Authentication Method	Pre-shared Key
Keying Group DH	DH (Diffie Hellman) Group 2
Encryption and Data Integrity	3DES-SHA1



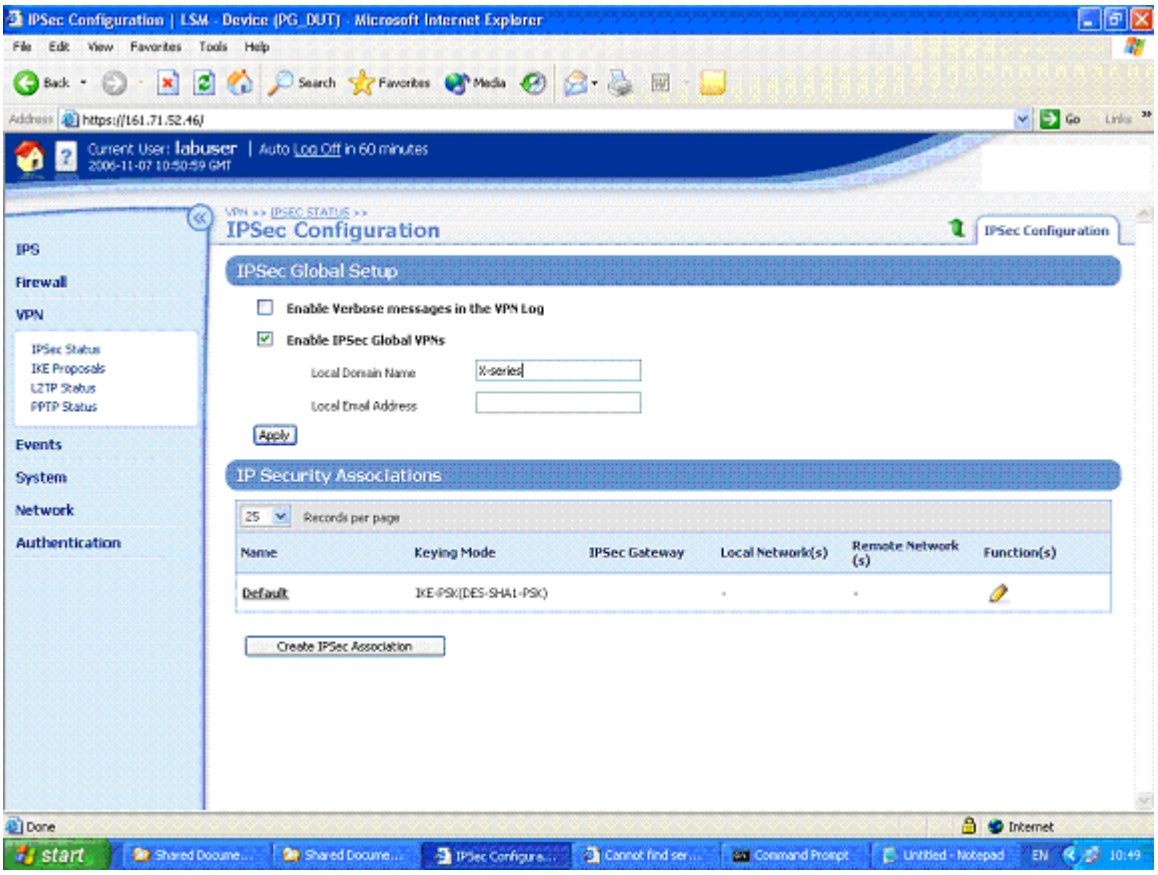
4.1 3Com "X" unit Configuration

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).

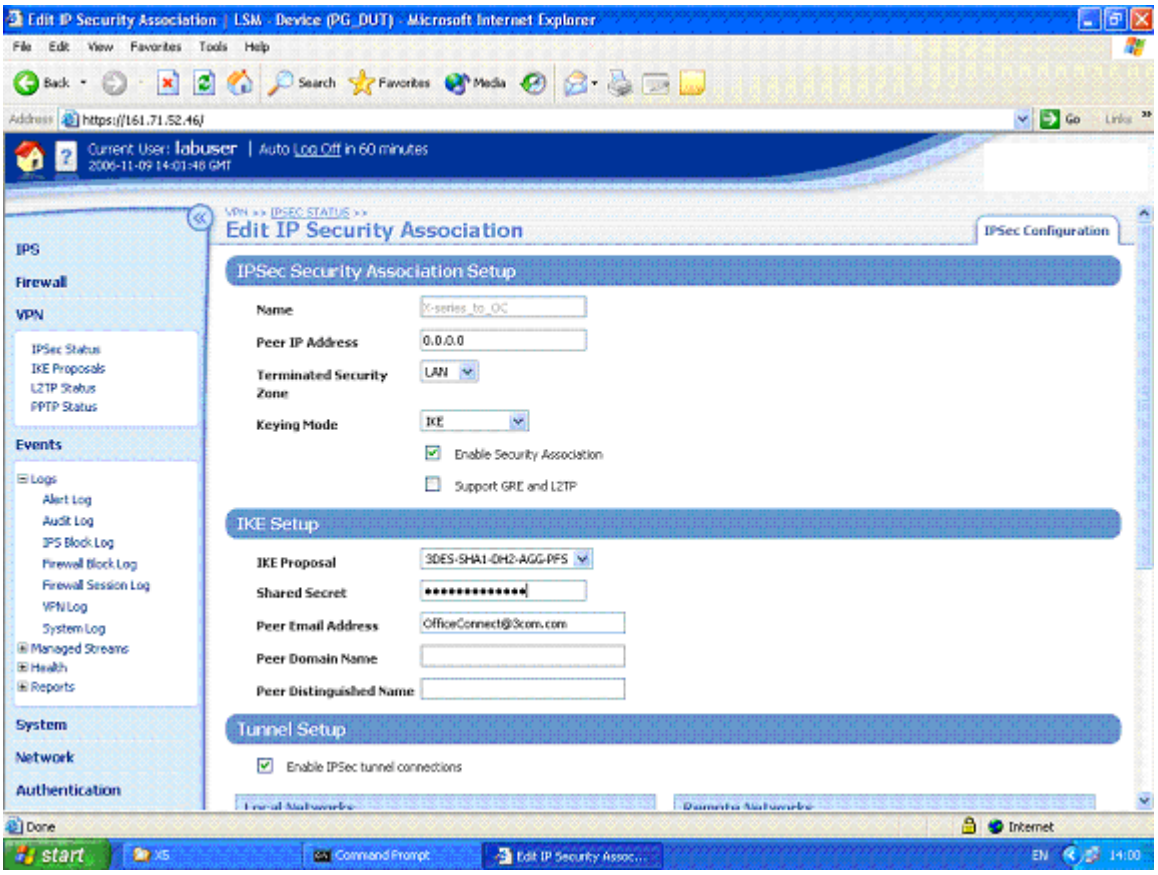


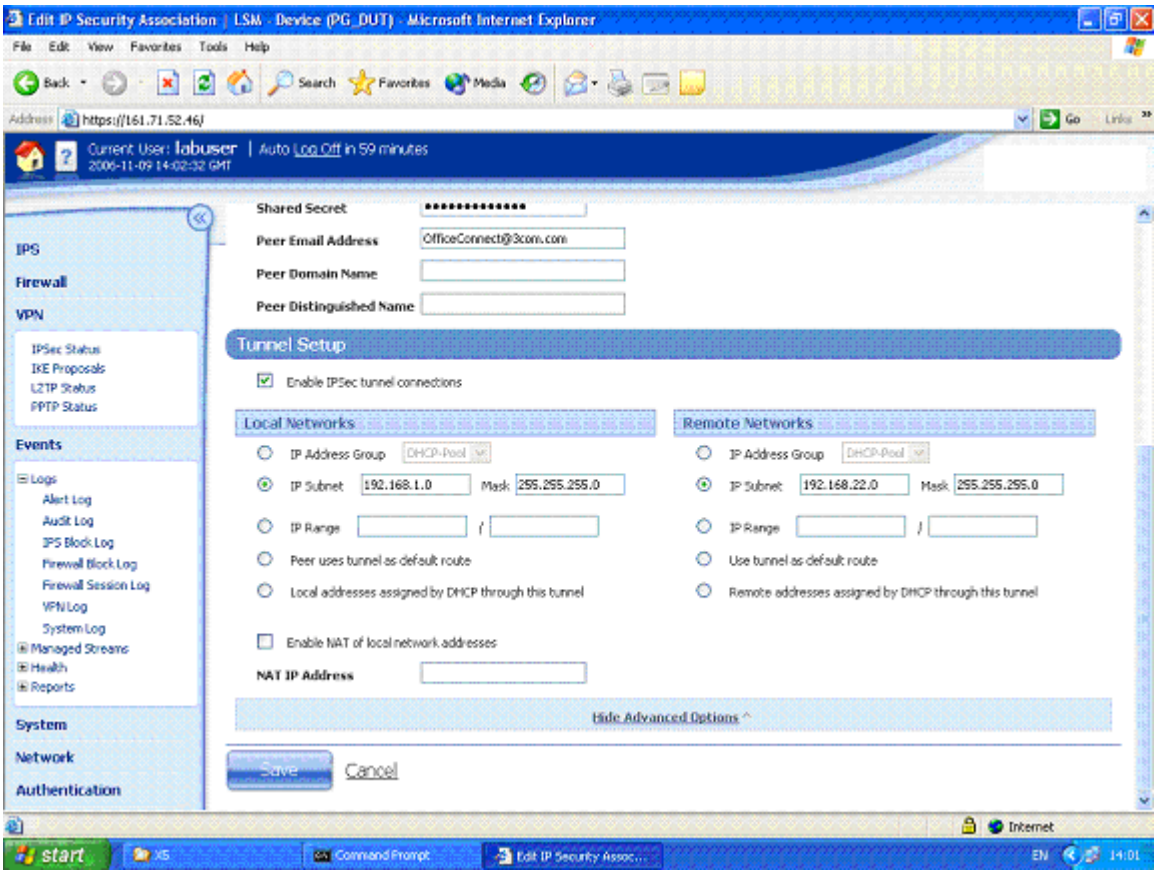


3. Click "Create" to save the new IKE Proposal.
4. Navigate to VPN -> IPSEC Status and click on the "IPSEC Configuration" tab.
5. Configure the upper part of the screen as shown below.



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 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.

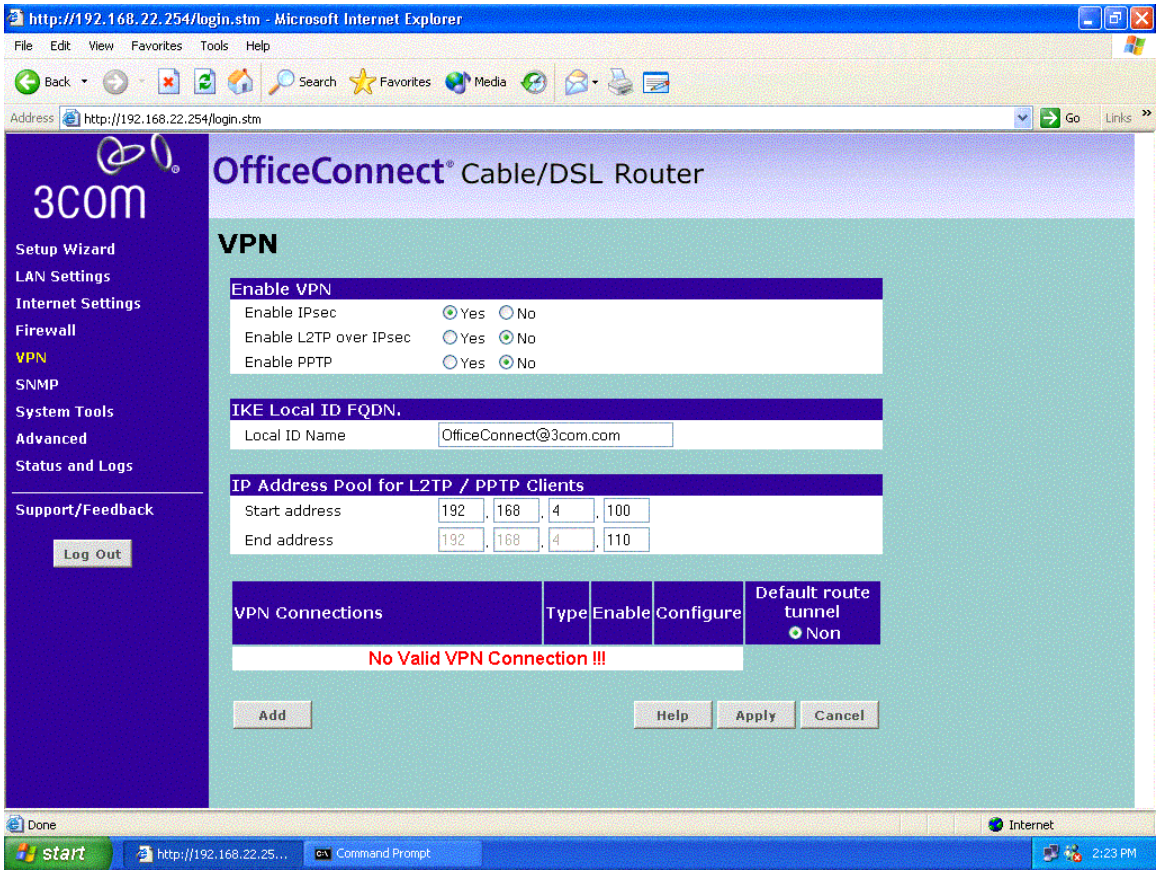

Edit IP Security Association | LSM - Device (PG_DUT) - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
https://161.71.52.46/
Current User: labuser | Auto Log Off in 60 minutes
2006-11-09 14:01:46 GMT
IPS
Firewall
VPN
IPSec Status
IKE Proposals
L2TP Status
PPTP Status
Events
Logs
Alert Log
Audit Log
IPS Block Log
Firewall Block Log
Firewall Session Log
VPN Log
System Log
Managed Streams
Health
Reports
System
Network
Authentication
VPN >> IPSEC STATUS >>
Edit IP Security Association
IPSec Configuration
IPSec Security Association Setup
Name
X-series_to_OC
Peer IP Address
0.0.0.0
Terminated Security Zone
LAN
Keying Mode
IKE
Enable Security Association
Support GRE and L2TP
IKE Setup
IKE Proposal
3DES-SHA1-DH2-AGG-PFS
Shared Secret
Peer Email Address
OfficeConnect@3com.com
Peer Domain Name
Peer Distinguished Name
Tunnel Setup
Enable IPSec tunnel connections
Done
Internet
start
Command Prompt
Edit IP Security Assoc...
EN
14:00



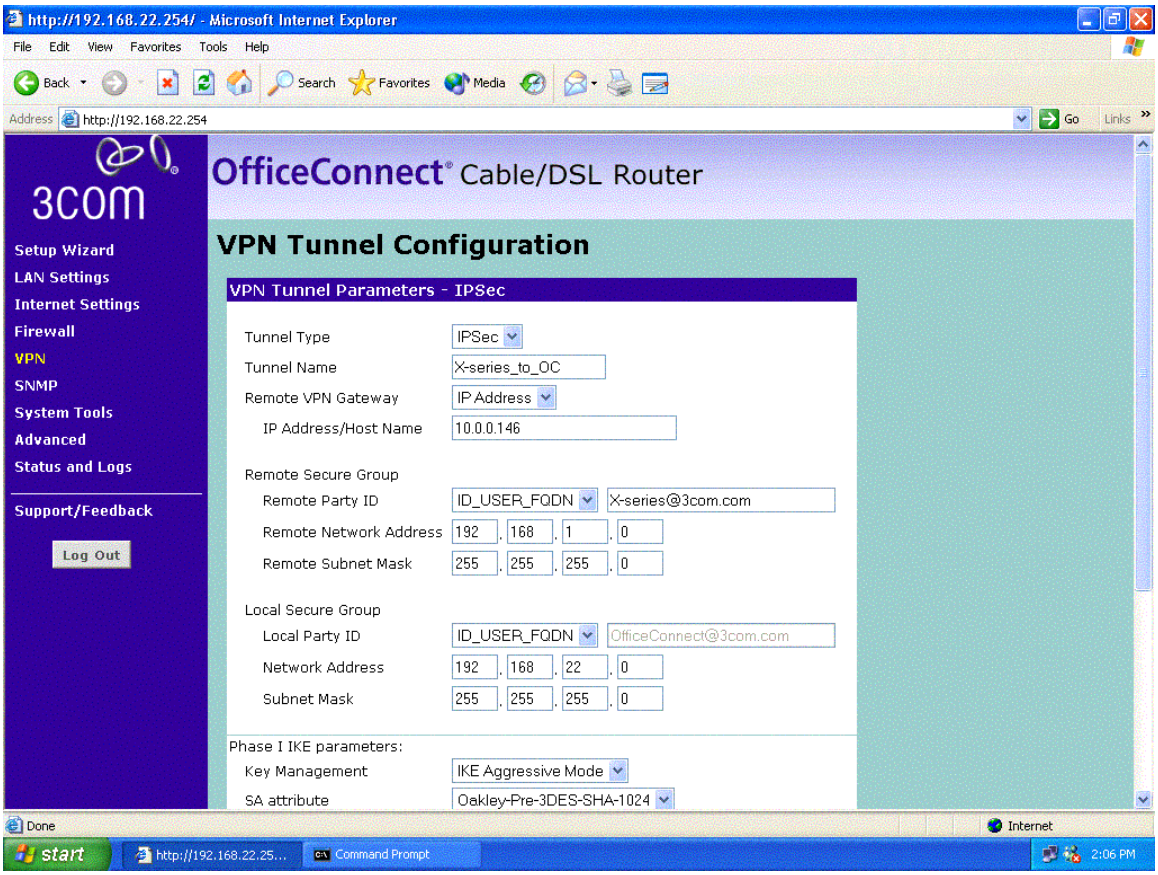
8. Click "Create" to create the Security Association.

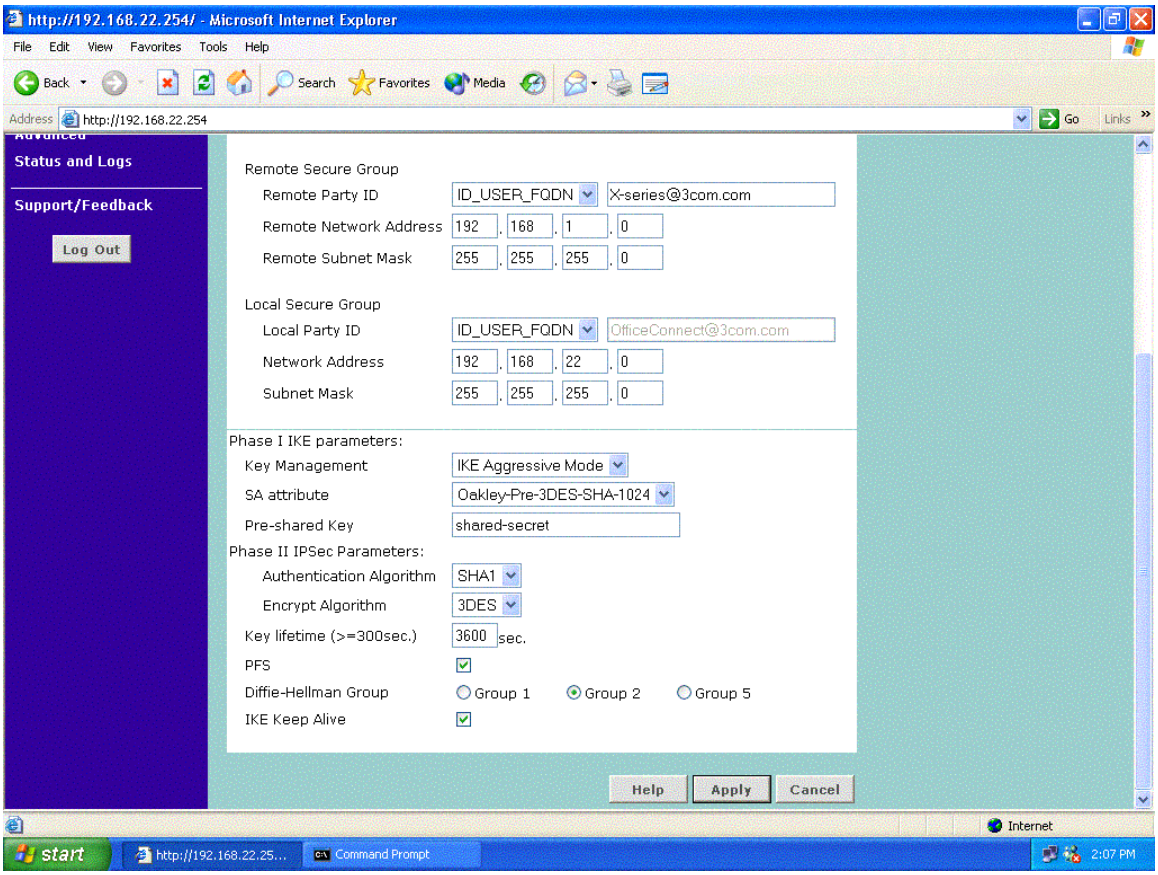
4.2 OfficeConnect 3CR858-91 Configuration

1. Open a browser on PC2, connect to https://192.168.22.1 and login to the OfficeConnect GUI.
2. Click on "VPN" to open up the global VPN page. Configure it as shown below and click "Apply".



3. Click on the "Add" button to create a VPN Connection. Complete the form provided as shown below (the form is more than one screen log so there are two screen grabs below – one for the upper part of the form and one for the lower part).

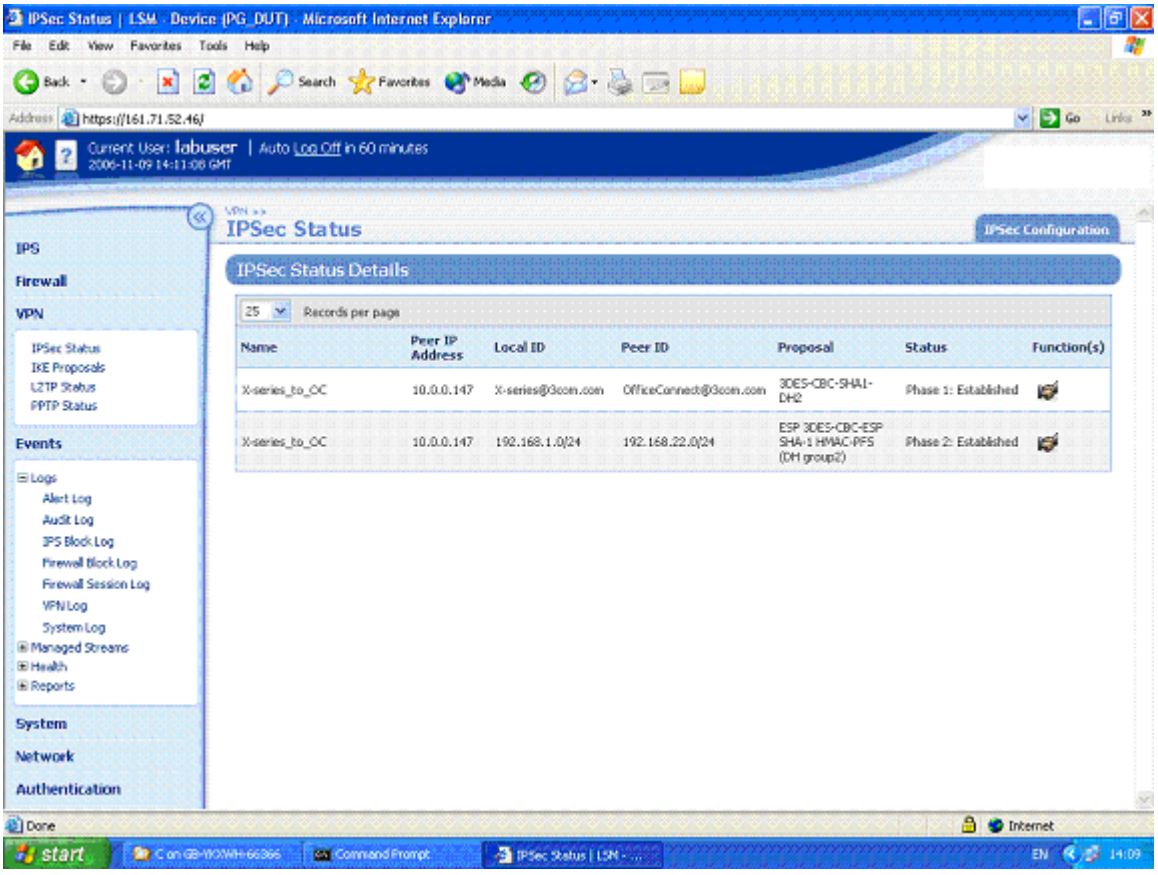

http://192.168.22.254/ - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.22.254
Go Links
3com
OfficeConnect® Cable/DSL Router
Setup Wizard
LAN Settings
Internet Settings
Firewall
VPN
SNMP
System Tools
Advanced
Status and Logs
Support/Feedback
Log Out
VPN Tunnel Configuration
VPN Tunnel Parameters - IPSec
Tunnel Type IPSec
Tunnel Name X-series_to_OC
Remote VPN Gateway IP Address
IP Address/Host Name 10.0.0.146
Remote Secure Group
Remote Party ID ID_USER_FQDN X-series@3com.com
Remote Network Address 192 . 168 . 1 . 0
Remote Subnet Mask 255 . 255 . 255 . 0
Local Secure Group
Local Party ID ID_USER_FQDN OfficeConnect@3com.com
Network Address 192 . 168 . 22 . 0
Subnet Mask 255 . 255 . 255 . 0
Phase I IKE parameters:
Key Management IKE Aggressive Mode
SA attribute Oakley-Pre-3DES-SHA-1024
Done
Internet
start
http://192.168.22.25...
Command Prompt
2:06 PM



4. Click on "Apply" to save the new VPN Connection.

4.3 Testing the VPN with data

1. Ping from PC2 to PC1 - this will bring up the tunnel which should look like this on the IPSec Status screen of the "X" unit. 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 (PC2 to PC1) is important as the OfficeConnect must be the initiator. This is because the IP address of the OfficeConnect is not known to the "X" unit.



5 Appendix – Configuration Files

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

5.1 Main Mode

5.1.1 “show conf” file for X505

```
 interface mgmtEthernet
    ip 161.71.52.46
    mask 255.255.255.0
    exit
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 settings poll-interval 2000
interface settings detect-mdi enable
interface settings mdi-mode mdix
host name "DUT"
host location "3Com Lab"
host ip-filter permit any icmp
host ip-filter permit any ip
default-gateway 0.0.0.0
no autodv
sntp primary 192.43.244.18
sntp secondary 192.5.41.40
sntp duration 60
sntp offset 1
sntp port 123
sntp timeout 1
sntp retries 3
```

```
no sntp
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
segment "LAN-WAN" create "LAN" "WAN"
high-availability no ip
high-availability disable
clock timezone CST
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 cva
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 attack-protection enable -action-set "Recommended"
category-settings reconnaissance    enable -action-set "Recommended"
category-settings security-policy   enable -action-set "Recommended"
category-settings informational     enable -action-set "Recommended"
category-settings network-equipment enable -action-set "Recommended"
category-settings traffic-normal    enable -action-set "Recommended"
category-settings misuse-abuse      enable -action-set "Recommended"
notify-contact "SMS" 1
notify-contact "Remote System Log" 1
notify-contact "Management Console" 1
notify-contact "LSM" 1
default-alert-sink period 1
server no 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  72 -critical  74
```

```
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
no nms
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 4
zone update WAN mtu 1500
zone update WAN addresses disable
zone update WAN vpn-tunnel-access enable
zone update LAN2 vlan-id 2
zone update LAN2 port 3 2
zone update LAN2 mtu 1500
zone update LAN2 addresses disable
zone update LAN2 vpn-tunnel-access enable
zone update LAN3 vlan-id 5
zone update LAN3 port 3 3
zone update LAN3 mtu 1500
zone update LAN3 addresses disable
zone update LAN3 vpn-tunnel-access enable
address-groups update dhcp-pool range 192.168.1.101 192.168.1.200
authentication privilege-groups update Allow_VPN_access vpn-client-access
authentication privilege-groups update RADIUS
authentication radius disable
content-filtering filter-service filter-action block-and-log
content-filtering filter-service default-rule deny
content-filtering filter-service server america
content-filtering filter-service deny adult
content-filtering filter-service deny gambling
content-filtering filter-service deny violence
content-filtering filter-service deny criminal
content-filtering filter-service deny hacking
content-filtering filter-service deny weapons
content-filtering filter-service deny drugs
content-filtering filter-service deny hate
content-filtering filter-service allow advertisement
content-filtering filter-service allow computing
content-filtering filter-service allow food
content-filtering filter-service allow politics
content-filtering filter-service allow hosting
```

```
content-filtering filter-service allow lifestyle
content-filtering filter-service allow dating
content-filtering filter-service allow reference
content-filtering filter-service allow sex-education
content-filtering filter-service allow sports
content-filtering filter-service allow usenet
content-filtering filter-service allow arts
content-filtering filter-service allow education
content-filtering filter-service allow games
content-filtering filter-service allow health
content-filtering filter-service allow careers
content-filtering filter-service allow vehicles
content-filtering filter-service allow photos
content-filtering filter-service allow religion
content-filtering filter-service allow search
content-filtering filter-service allow streaming-media
content-filtering filter-service allow email
content-filtering filter-service allow chat
content-filtering filter-service allow finance
content-filtering filter-service allow glamour
content-filtering filter-service allow hobbies
content-filtering filter-service allow kids
content-filtering filter-service allow news
content-filtering filter-service allow real-estate
content-filtering filter-service allow proxies
content-filtering filter-service allow shopping
content-filtering filter-service allow travel
content-filtering filter-service disable
content-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
interface virtual add 1 internal
interface virtual internal 1 ip 192.168.1.1 netmask 255.255.255.0
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 enable query-interval 125 query-timeout 250 ma
x-query-time 10
interface virtual internal 1 pim-dm enable
interface virtual internal 1 zone add LAN
interface virtual internal 1 zone add LAN2
```

```
interface virtual internal 1 zone add VPN
interface virtual internal 1 zone add LAN3
interface virtual add 2 external
interface virtual external 2 type static 10.0.0.146 netmask 255.255.255.0 gw 10.
0.0.147
interface virtual external 2 full-transparent disable
interface virtual external 2 dns-server 10.0.0.145
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 enable
interface virtual external 2 igmp disable
interface virtual external 2 pim-dm disable
interface virtual external 2 zone add WAN
policy schedule update working-day days -mtwtf- from 0800 to 1800
policy service update 3com-nbx udp port 2093 to 2096
policy service update aol-tcp tcp port 5190 to 5193
policy service update aol-udp udp port 5190 to 5193
policy service update audio-call-control tcp port 1731
policy service update chargen-tcp tcp port 19
policy service update chargen-udp udp port 19
policy service update dhcp-client udp port 68
policy service update dhcp-server udp port 67
policy service update discard-udp udp port 9
policy service update discard-tcp tcp port 9
policy service update dns-tcp tcp port 53
policy service update dns-udp udp port 53
policy service update echo-tcp tcp port 7
policy service update echo-udp udp port 7
policy service update finger-tcp tcp port 79
policy service update ftp tcp port 21
policy service update gopher-tcp tcp port 70
policy service update gre gre
policy service update h323 tcp port 1720
policy service update http tcp port 80
policy service update https tcp port 443
policy service update icmp-ping icmp port 8
policy service update igmp igmp
policy service update ike udp port 500
policy service update imap tcp port 143
policy service update imapv3 tcp port 220
policy service update internet-locator tcp port 389
policy service update ipsec-ah ah
policy service update ipsec-esp esp
policy service update irc tcp port 194
policy service update itunes-tcp tcp port 3689
policy service update itunes-udp udp port 5353
policy service update kerberos-tcp tcp port 88
policy service update kerberos-udp udp port 88
policy service update l2tp udp port 1701
```

```
policy service update ldap-tcp tcp port 389
policy service update ldap-udp udp port 389
policy service update lotus-notes-domino tcp port 1352
policy service update lpr tcp port 515
policy service update msn-tcp tcp port 1863
policy service update msn-udp udp port 1863
policy service update nat-t-ipsec udp port 4500
policy service update nbname tcp port 137
policy service update netbios-tcp tcp port 137 to 139
policy service update netbios-udp udp port 137 to 139
policy service update netmeeting tcp port 1720
policy service update nfsd-tcp tcp port 2049
policy service update nfsd-udp udp port 2049
policy service update nntp tcp port 119
policy service update ntp udp port 123
policy service update pc-anywhere-tcp tcp port 5631
policy service update pim-dm pim
policy service update ping icmp port 8
policy service update pop3 tcp port 110
policy service update portmapper-tcp tcp port 111
policy service update portmapper-udp udp port 111
policy service update pptp-tcp tcp port 1723
policy service update radius-accounting udp port 1813
policy service update radius-auth udp port 1812
policy service update realaudio tcp port 7070
policy service update rexec tcp port 512
policy service update rip udp port 520
policy service update rlogin tcp port 513
policy service update rsh tcp port 514
policy service update rtsp tcp port 554
policy service update sip-tcp tcp port 5060
policy service update sip-udp udp port 5060
policy service update smb tcp port 445
policy service update sms-trap tcp port 8162 to 8163
policy service update smtp tcp port 25
policy service update snmp-request udp port 161
policy service update snmp-trap udp port 162
policy service update ssh tcp port 22
policy service update ssh-udp udp port 22
policy service update syslog udp port 514
policy service update t120 tcp port 1503
policy service update talk udp port 517 to 518
policy service update telnet tcp port 23
policy service update tftp udp port 69
policy service update traceroute icmp port 8
policy service update uls tcp port 522
policy service update uucp udp port 540
policy service update vnc tcp port 5800
policy service update wais tcp port 210
policy service update x-windows tcp port 6000 to 6063
policy service-group update aol aol-tcp aol-udp
policy service-group update dns dns-tcp dns-udp
policy service-group update email pop3 smtp imap imapv3
```

```
policy service-group update ipsec ike ipsec-ah ipsec-esp
policy service-group update ldap ldap-udp ldap-tcp
policy service-group update msn-messenger msn-udp msn-tcp
policy service-group update netmeeting h323 audio-call-control t120
policy service-group update nfs portmapper-tcp portmapper-udp nfsd-tcp nfsd-udp
policy service-group update pptp pptp-tcp gre
policy service-group update secure-management https ssh
policy service-group update sip sip-tcp sip-udp
policy service-group update snmp snmp-request snmp-trap
policy service-group update voice 3com-nbx sip-tcp sip-udp
policy service-group update vpn-protocols pptp-tcp l2tp gre ike nat-t-ipsec
policy service-group update sms-config https snmp-request ssh
policy service-group update sms-get ntp sms-trap
policy service-group update lan2-prot http icmp-ping telnet
policy rule update 5 allow LAN WAN ANY
policy rule update 5 schedule always timeout 30 logging disable
policy rule update 5 src-addr all
policy rule update 5 dst-addr all
policy rule update 5 bandwidth disable
policy rule update 5 authentication disable
policy rule update 5 position 1
policy rule update 5 comment ""
policy rule enable 5
policy rule update 6 allow LAN2 WAN ANY
policy rule update 6 schedule always timeout 30 logging disable
policy rule update 6 src-addr all
policy rule update 6 dst-addr all
policy rule update 6 bandwidth disable
policy rule update 6 authentication disable
policy rule update 6 position 2
policy rule update 6 comment ""
policy rule enable 6
policy rule update 17 allow VPN LAN2 ANY
policy rule update 17 schedule always timeout 30 logging disable
policy rule update 17 src-addr all
policy rule update 17 dst-addr all
policy rule update 17 bandwidth disable
policy rule update 17 authentication disable
policy rule update 17 position 3
policy rule update 17 comment ""
policy rule enable 17
policy rule update 19 allow LAN this-device secure-management
policy rule update 19 schedule always timeout 30 logging disable
policy rule update 19 src-addr all
policy rule update 19 dst-addr all
policy rule update 19 bandwidth disable
policy rule update 19 authentication disable
policy rule update 19 position 4
policy rule update 19 comment ""
policy rule enable 19
policy rule update 20 allow LAN2 this-device secure-management
policy rule update 20 schedule always timeout 30 logging disable
policy rule update 20 src-addr all
```

```
policy rule update 20 dst-addr all
policy rule update 20 bandwidth disable
policy rule update 20 authentication disable
policy rule update 20 position 5
policy rule update 20 comment ""
policy rule enable 20
policy rule update 7 allow VPN WAN ANY
policy rule update 7 schedule always timeout 30 logging disable
policy rule update 7 src-addr all
policy rule update 7 dst-addr all
policy rule update 7 bandwidth disable
policy rule update 7 authentication disable
policy rule update 7 position 6
policy rule update 7 comment ""
policy rule enable 7
policy rule update 8 allow LAN3 WAN ANY
policy rule update 8 schedule always timeout 30 logging disable
policy rule update 8 src-addr all
policy rule update 8 dst-addr all
policy rule update 8 bandwidth disable
policy rule update 8 authentication disable
policy rule update 8 position 7
policy rule update 8 comment ""
policy rule enable 8
policy rule update 18 allow LAN LAN2 ANY
policy rule update 18 schedule always timeout 30 logging disable
policy rule update 18 src-addr all
policy rule update 18 dst-addr all
policy rule update 18 bandwidth disable
policy rule update 18 authentication disable
policy rule update 18 position 8
policy rule update 18 comment ""
policy rule enable 18
policy rule update 11 allow VPN LAN ANY
policy rule update 11 schedule always timeout 30 logging disable
policy rule update 11 src-addr all
policy rule update 11 dst-addr all
policy rule update 11 bandwidth disable
policy rule update 11 authentication disable
policy rule update 11 position 9
policy rule update 11 comment ""
policy rule enable 11
policy rule update 15 allow LAN VPN ANY
policy rule update 15 schedule always timeout 30 logging disable
policy rule update 15 src-addr all
policy rule update 15 dst-addr all
policy rule update 15 bandwidth disable
policy rule update 15 authentication disable
policy rule update 15 position 10
policy rule update 15 comment ""
policy rule enable 15
policy rule update 16 allow WAN this-device vpn-protocols
policy rule update 16 schedule always timeout 30 logging disable
```

```
policy rule update 16 src-addr all
policy rule update 16 dst-addr all
policy rule update 16 bandwidth disable
policy rule update 16 authentication disable
policy rule update 16 position 11
policy rule update 16 comment ""
policy rule enable 16
policy rule update 13 allow this-device WAN vpn-protocols
policy rule update 13 schedule always timeout 30 logging disable
policy rule update 13 src-addr all
policy rule update 13 dst-addr all
policy rule update 13 bandwidth disable
policy rule update 13 authentication disable
policy rule update 13 position 12
policy rule update 13 comment ""
policy rule enable 13
policy rule update 21 allow ANY ANY ANY
policy rule update 21 schedule always timeout 30 logging disable
policy rule update 21 src-addr all
policy rule update 21 dst-addr all
policy rule update 21 bandwidth disable
policy rule update 21 authentication disable
policy rule update 21 position 13
policy rule update 21 comment ""
policy rule enable 21
policy rule update 22 deny ANY ANY ANY
policy rule update 22 schedule always timeout 30 logging disable
policy rule update 22 src-addr all
policy rule update 22 dst-addr all
policy rule update 22 bandwidth disable
policy rule update 22 authentication disable
policy rule update 22 position 14
policy rule update 22 comment ""
policy rule enable 22
routing rip disable update-timer 30
routing multicast igmp enable
routing multicast pim-dm enable 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 2
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 enable
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 2
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 disable
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 ipsec enable
vpn ipsec add Default
vpn ipsec sa Default key ike proposal DES-SHA1-PSK
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 subnet 0.0.0.0 netmask 0.0.0.0
vpn ipsec sa Default peer-default-route disable
vpn ipsec sa Default disable
vpn ipsec add LAN1-22NET
vpn ipsec sa LAN1-22NET key ike proposal 3DES-SHA1-DH2 shared-secret ********
vpn ipsec sa LAN1-22NET transport disable
vpn ipsec sa LAN1-22NET peer 10.0.0.147
vpn ipsec sa LAN1-22NET zone LAN
vpn ipsec sa LAN1-22NET tunnel subnet 192.168.22.0 netmask 255.255.255.0
vpn ipsec sa LAN1-22NET peer-default-route disable
vpn ipsec sa LAN1-22NET 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
ramdisk sync-interval message 30
ramdisk sync-interval audit 30
ramdisk sync-interval block -1
ramdisk sync-interval alert -1
```

```
ramdisk sync-interval peer -1
ramdisk sync-interval traffic -1
sms v2
sms no v3
sms no must-be-ip
no sms
session timeout 20 -persist
DUT#
```

5.1.2 OfficeConnect 3CR858-91 configuration file

There is no method to dump the configuration as a text file.

5.2 Aggressive Mode

5.2.1 "show conf" file for X505

```
interface mgmtEthernet
    ip 161.71.52.46
    mask 255.255.255.0
    default-gateway 0.0.0.0
    exit
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 settings poll-interval 2000
interface settings detect-mdi enable
interface settings mdi-mode mdix
host name "PG_DUT"
host location "Hemel shared 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  72 -critical  74
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 3/4
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 4194304
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 10.0.0.146 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 10.0.0.147
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 ANY 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 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 local-id email X_unit@3com.com
vpn ike local-id domain X_unit
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-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 email
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS peer-id-type email
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS ca-cert ANY
vpn ike proposal 3DES-SHA1-DH2-AGG-PFS nat-t disable
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 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 disable
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_unit_to_OC
vpn ipsec sa X_unit_to_OC key ike proposal 3DES-SHA1-DH2-AGG-PFS shared-
secret ******** peer-id OfficeConnect@3com.com
vpn ipsec sa X_unit_to_OC transport disable
vpn ipsec sa X_unit_to_OC peer 0.0.0.0
```

```
vpn ipsec sa X_unit_to_OC zone LAN
vpn ipsec sa X_unit_to_OC tunnel remote subnet 192.168.22.0 netmask
255.255.255.0
vpn ipsec sa X_unit_to_OC tunnel local subnet 192.168.1.0 netmask
255.255.255.0
vpn ipsec sa X_unit_to_OC tunnel nat disable
vpn ipsec sa X_unit_to_OC tunnel enable
vpn ipsec sa X_unit_to_OC 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
```

5.2.2 OfficeConnect 3CR858-91 configuration file

There is no method to dump the configuration as a text file.