Avaya Solution and Interoperability Test Lab

Configuring an Avaya IP Telephone at a Remote Site served by an Avaya IP Office over a Virtual Private Network Implemented between a NetGear ProSafe VPN Firewall FVS114 and FVX538 - Issue 1.0

Abstract

These Application Notes describe a configuration that supports a remote worker’s use of an Avaya 5600 series IP Telephone served by an Avaya IP Office IP412 at the main office through a Virtual Private Network (VPN) implemented with a NetGear ProSafe VPN Firewall FVS114 and FVX538. The VPN spans from the NetGear FVS114 at the remote worker site to the NetGear FVX538 in the main office over a simulated internet to provide secure connectivity. This solution can be used for a remote worker who wants to use a multi-button telephone and have the same functionality (for example, Message Waiting Indication) as a telephone co-located with the IP Office.

Since the Internet Service Providers generally do not provide guarantees for bandwidth, delay, jitter or loss, the quality of service to the user in a real world configuration cannot be guaranteed.

1. Introduction

Figure 1 shows the tested configuration. The Main Office Avaya IP Office IP412 provides business telephony service to both the main site and the remote site. The Avaya 5620SW at the remote site registers to the IP Office over an IPsec Virtual Private Network implemented between the NetGear devices. Avaya softConsole and PC Softphone were used during the testing.

Feature operation provided to the remote user was similar to feature operation for any Avaya IP Telephone user. The quality of the voice connection cannot be guaranteed, since the Internet Service Providers typically do not guarantee the performance of the underlying packet service.

These Application Notes focus on the configuration needed to support the telephony features in a given environment. Some aspects of configuration, such as the firewall configuration for non-voice traffic, are simplified.

This document does not describe the configuration of the Cisco 6015 IP DSL switch and the Cisco 7500 Router. For an example of a similar configuration, see item [2] in Section 10.

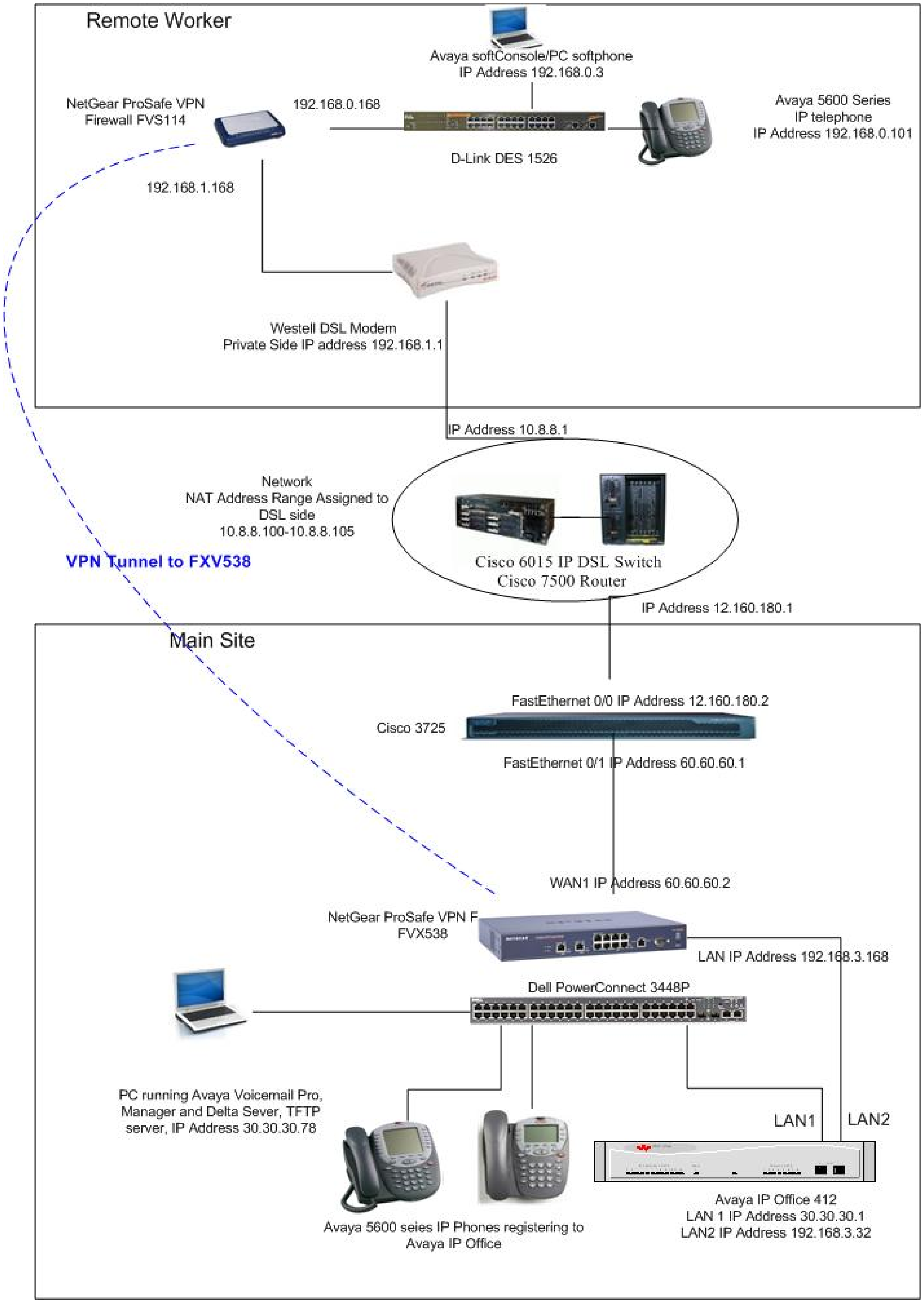


Figure 1 - Network Configuration Diagram

1.1. IP Office Features

The configuration presented in this document uses the IP Office Hot Desking feature. This allows a user to easily switch from an office phone to the remote phone with the ability to have one telephone number by logging into the telephone of choice. A user can go to either the office phone or the remote phone and log in (via a short code). Once the user has successfully logged in, the functionality that is available is provided (for example message waiting, programmed buttons and feature access). Once the user is done working, the user can log out. Calls to the logged out user receive coverage or busy treatment.

The following features were successfully tested in this configuration:

1. Message Waiting Indication for the Hot Desk Extension at the remote phone.
2. Call Recording at the remote phone.
3. Call Intrude capability from a user at Main Site to the remote phone.
4. Delta Server information for the remote phone user. The Compact Business Center (CBC), Compact Contact Center (CCC) and SMDR applications use this information.
5. User and Hunt Group button operation at the remote phone.
6. Bridged and Line Appearance buttons at the remote phone.

Note: The Call Listen capability on IP Office is not available on the remote phone. This is the same restriction as other IP telephones registered to an IP Office.

2. Equipment and Software Validated

The following hardware and software versions were used for this configuration:

Equipment	Version
Avaya IP Office 412	3.1(65)
Avaya Delta Server	3.1.5
Avaya IP Office Voicemail Pro	3.1.16
Avaya softConsole	3.1.16
Avaya PC Softphone	3.1.15
Avaya 5602SW, 5610SW and 5620SW IP Telephones	2.3
NetGear ProSafe VPN Firewall FVS114	V1.1_01
NetGear ProSafe VPN Firewall FXV538	V1.6.49
Cisco 3725 Router	OS version 12.2(8r)T2 Software (fc1)
Dell PowerConnect 3448P switch	1.0.0.112
Westell 2200 DSL Modem	01.06.53
D-Link DES 1526 switch	1.00 2.001.002 (protocol)

Table 1 - Equipment and Versions Validated

3. Configure Avaya IP Office IP 412 at the Main Site

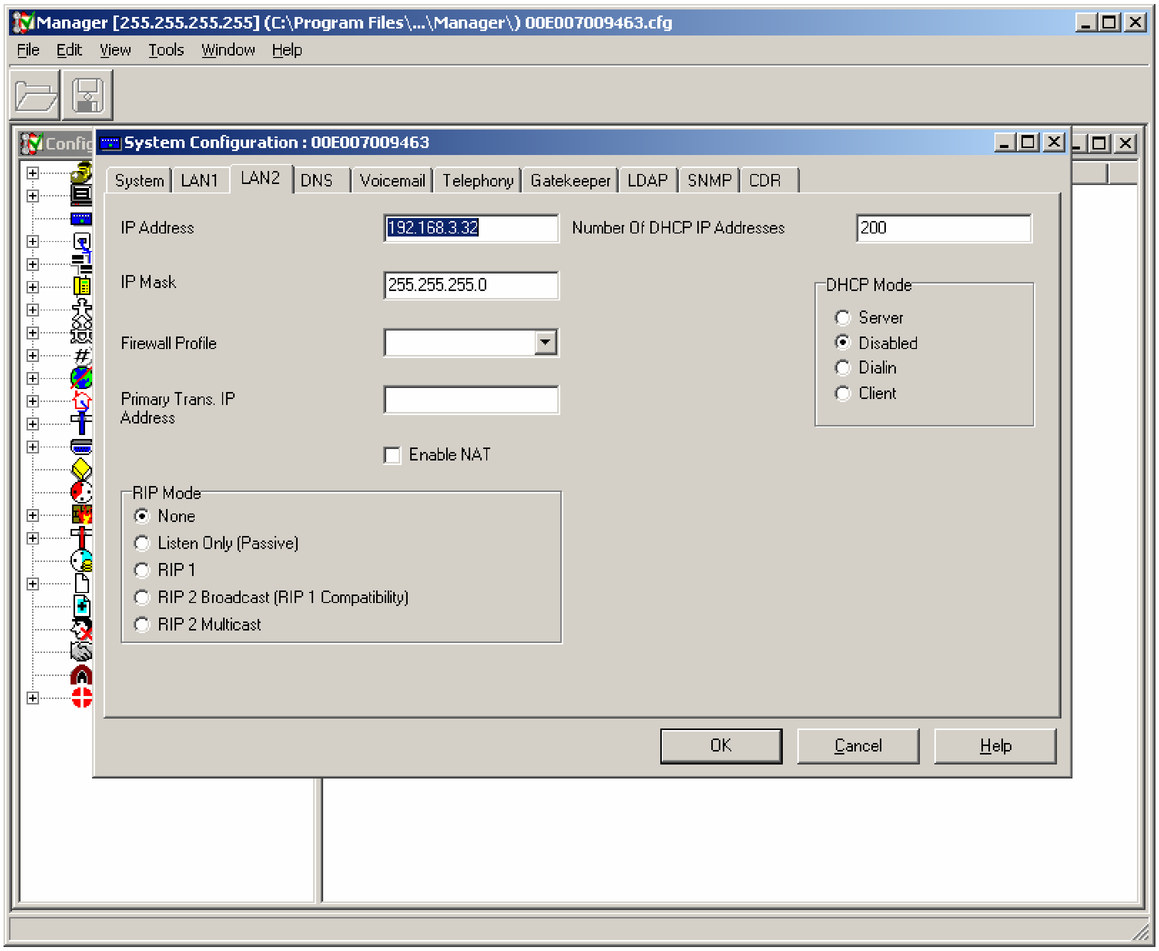
This section describes the IP Office configuration at the Main Site. This includes configuring:

1. An IP Extension,
2. A Hot Desk User,
3. A default IP Route to the NetGear ProSafe VPN firewall FVX538,
4. Short Codes for the ExtnLogin and ExtnLogout features.

IP Office is configured via the IP Office Manager program. Log into the IP Office Manager PC and select **Start** → **Programs** → **IP Office** → **Manager** to launch the Manager application. Log into the Manager application using the appropriate credentials.

1. *Configure the LAN2 IP Address.* In IP Office Manager, select **System** in the left panel. Double-click on the entry in the right panel.

   Select the **LAN2** Tab. Enter an **IP Address** and **Mask** and set the **DHCP Mode** to **Disabled**. Press the **OK** button.


Manager [255.255.255.255] (C:\Program Files\...\Manager\) 00E007009463.cfg
File Edit View Tools Window Help
Confic
System Configuration : 00E007009463
System | LAN1 | LAN2 | DNS | Voicemail | Telephony | Gatekeeper | LDAP | SNMP | CDR
OK
Cancel
Help

IP Address: 192.168.3.32

IP Mask: 255.255.255.0

Firewall Profile:

Primary Trans. IP Address:

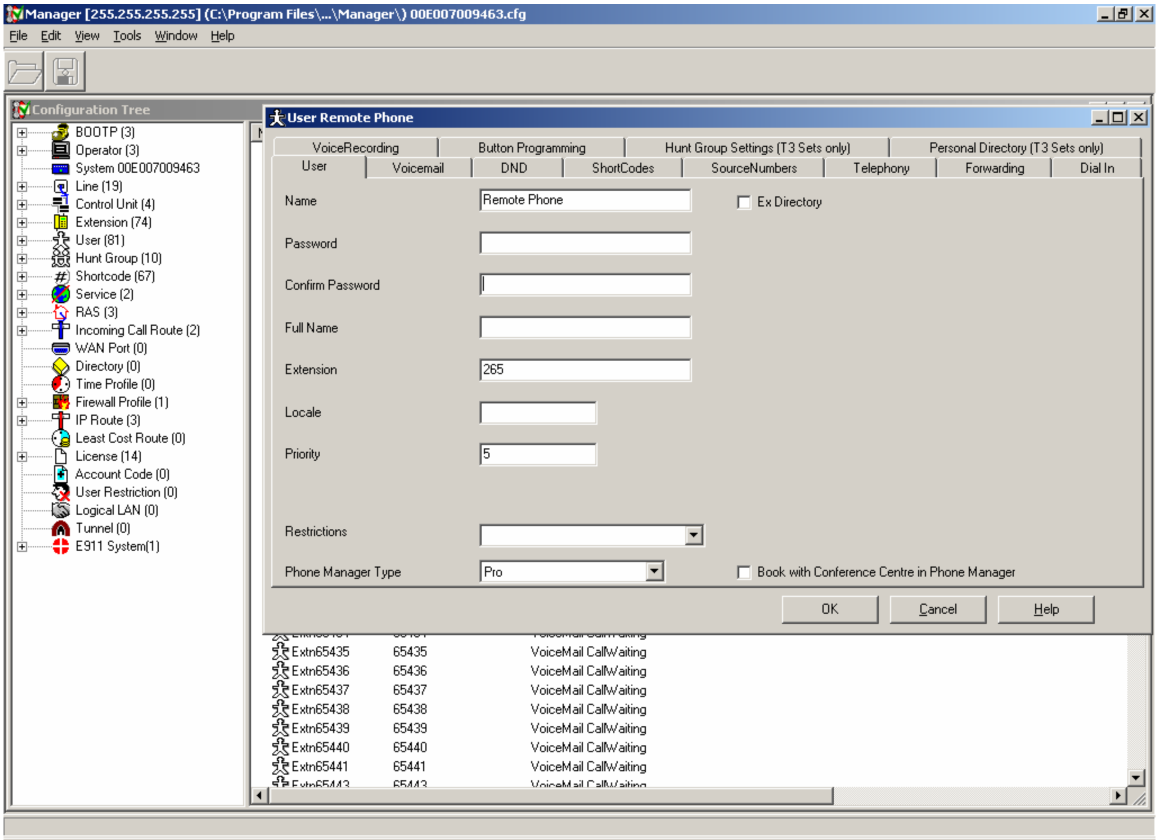
□ Enable NAT

Number Of DHCP IP Addresses: 200

DHCP Mode
○ Server
● Disabled
○ Dialin
○ Client

RIP Mode
● None
○ Listen Only (Passive)
○ RIP 1
○ RIP 2 Broadcast (RIP 1 Compatibility)
○ RIP 2 Multicast

2. *Configure a user for the remote phone.* In IP Office Manager, select **User** in the left panel. In the right panel, right click and select the **New** option. Enter a unique **Name** and **Extension** number. Select the appropriate **Phone Manager Type**. Press the **OK** button.



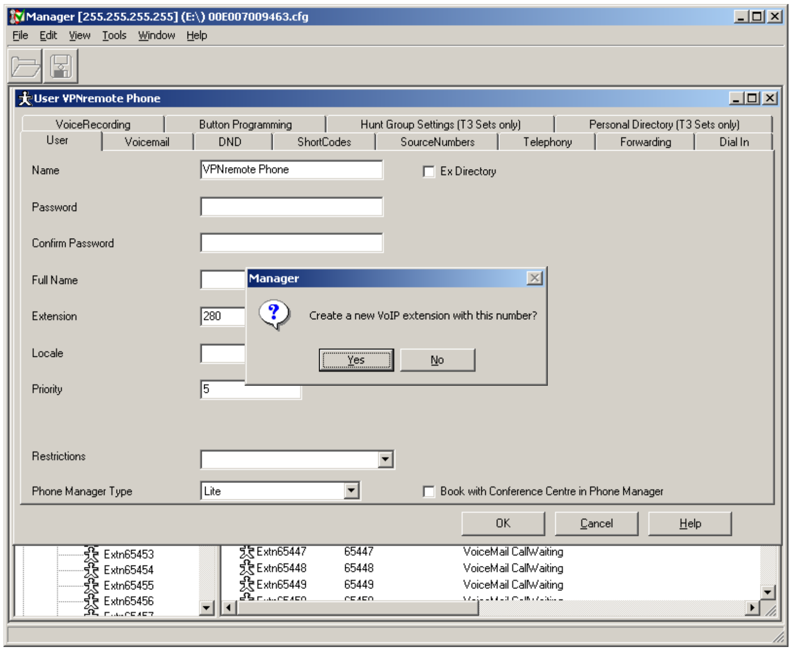
Name	Remote Phone
Password	
Confirm Password	
Full Name	
Extension	265
Locale	
Priority	5
Restrictions	
Phone Manager Type	Pro

□ Ex Directory

□ Book with Conference Centre in Phone Manager

Extn65435	65435	VoiceMail CallWaiting
Extn65436	65436	VoiceMail CallWaiting
Extn65437	65437	VoiceMail CallWaiting
Extn65438	65438	VoiceMail CallWaiting
Extn65439	65439	VoiceMail CallWaiting
Extn65440	65440	VoiceMail CallWaiting
Extn65441	65441	VoiceMail CallWaiting
Extn65443	65443	VoiceMail CallWaiting

3. *Complete the user*. Choose the **Yes** option for creating a new VoIP extension. This will create a default IP Extension for the user.



Manager [255.255.255.255] (E:\) 00E007009463.cfg

User VPNremote Phone

Name: VPNremote Phone

□ Ex Directory

Password:

Confirm Password:

Full Name:

Extension: 280

Locale:

Priority: 5

Restrictions:

Phone Manager Type: Lite

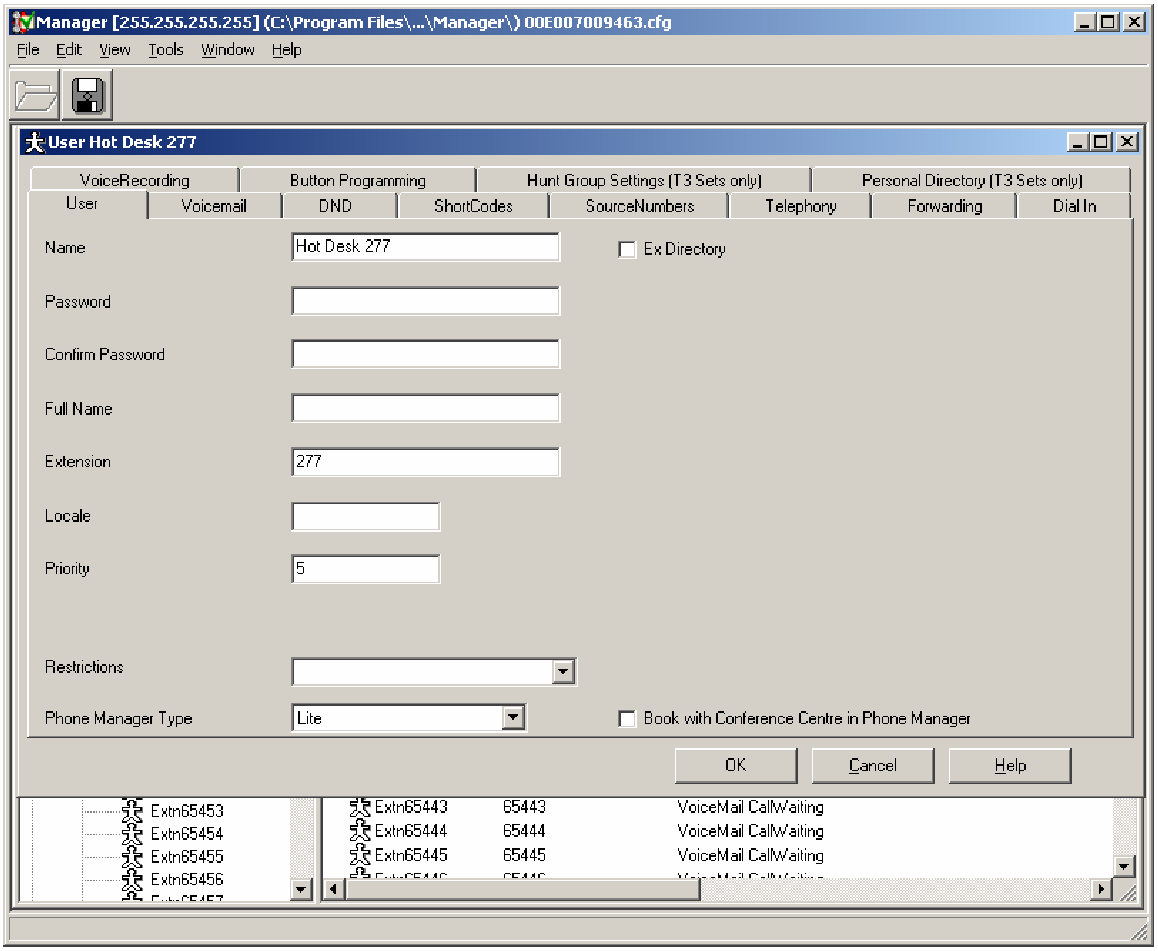
□ Book with Conference Centre in Phone Manager

Manager

Create a new VoIP extension with this number?

Extn65447	65447	VoiceMail CallWaiting
Extn65448	65448	VoiceMail CallWaiting
Extn65449	65449	VoiceMail CallWaiting

4. *Create a Hot Desk User*. Select **User** in the left panel. In the right panel, right click and select the **New** option. Enter a unique **Name** and a unique **Extension** number. Set other parameters as needed.



Name: Hot Desk 277

□ Ex Directory

Password:

Confirm Password:

Full Name:

Extension: 277

Locale:

Priority: 5

Restrictions:

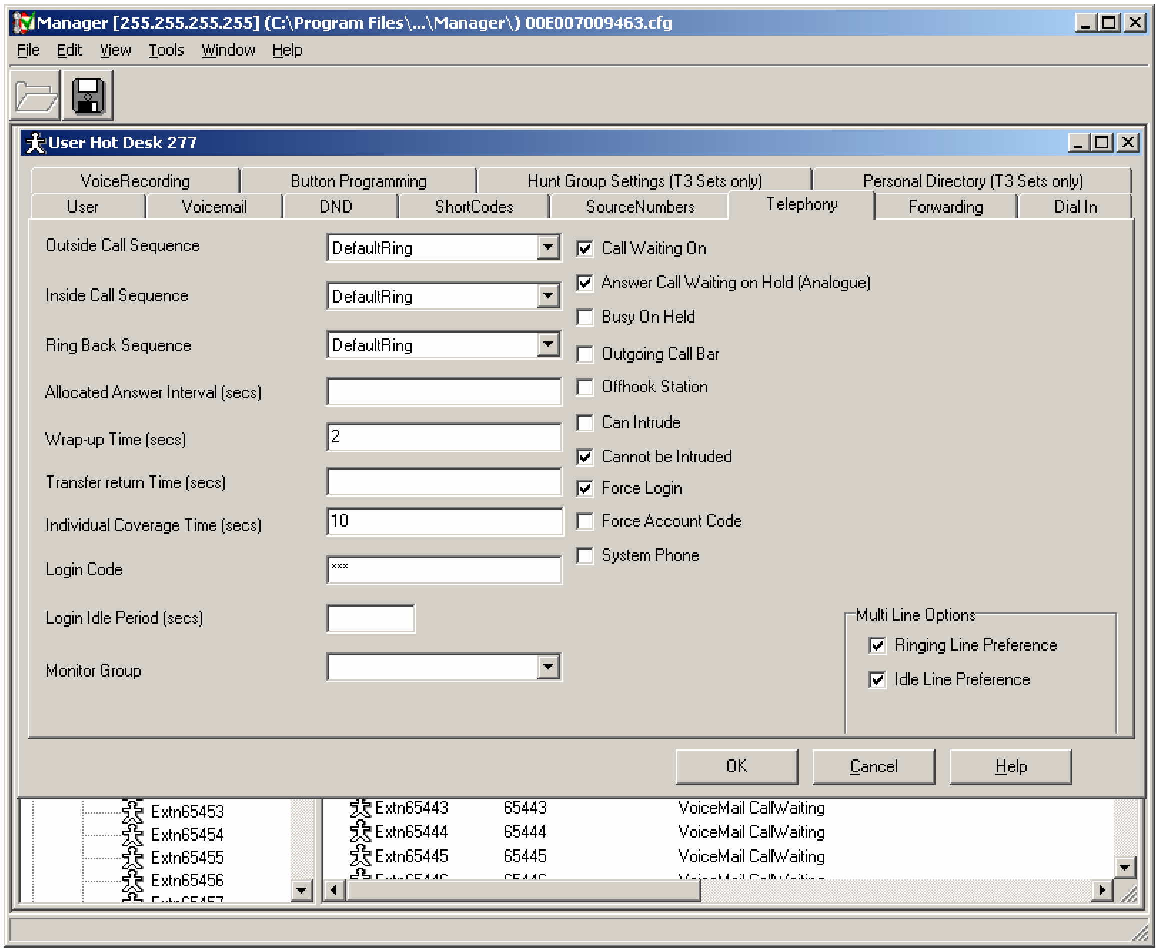
Phone Manager Type: Lite

□ Book with Conference Centre in Phone Manager

Extn65453
Extn65454
Extn65455
Extn65456

Extn65443 65443 VoiceMail CallWaiting
Extn65444 65444 VoiceMail CallWaiting
Extn65445 65445 VoiceMail CallWaiting

5. *Configure the Hot Desking options.* Select the **Telephony** tab. Check the **Force Login** box and enter a **Login Code.** The **Login Code** text box displays a “*” for each number in the code. Set other parameters as needed. Press the **OK** button.


Manager [255.255.255.255] (C:\Program Files\...\Manager\) 00E007009463.cfg
File Edit View Tools Window Help
User Hot Desk 277
VoiceRecording
Button Programming
Hunt Group Settings (T3 Sets only)
Personal Directory (T3 Sets only)
User
Voicemail
DND
ShortCodes
SourceNumbers
Telephony
Forwarding
Dial In
OK
Cancel
Help

Outside Call Sequence: DefaultRing
Inside Call Sequence: DefaultRing
Ring Back Sequence: DefaultRing
Allocated Answer Interval (secs):
Wrap-up Time (secs): 2
Transfer return Time (secs):
Individual Coverage Time (secs): 10
Login Code: ***
Login Idle Period (secs):
Monitor Group:

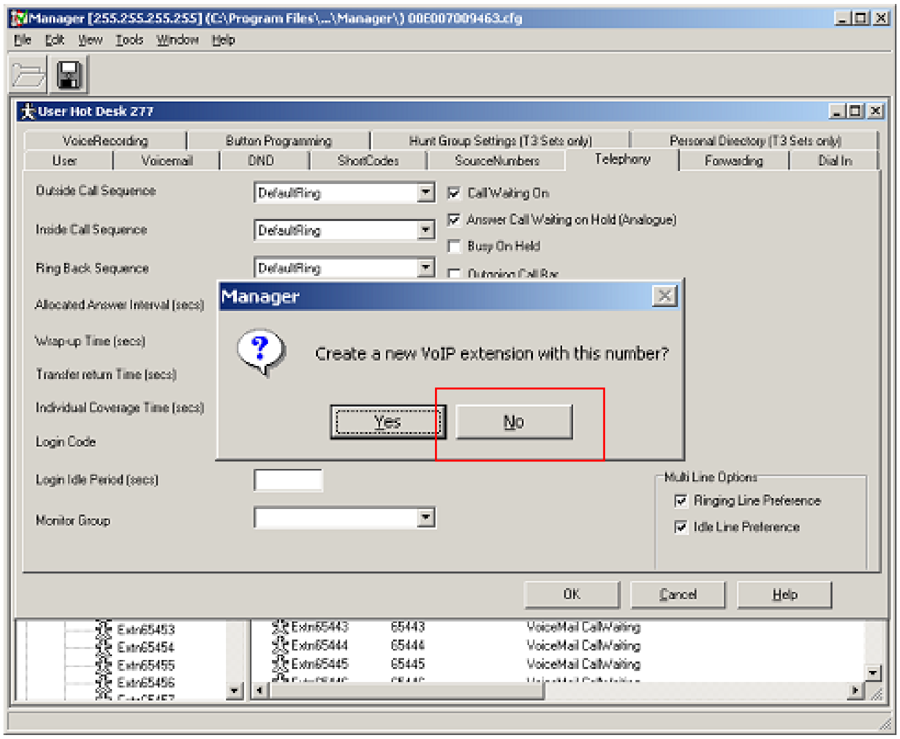
☑ Call Waiting On
☑ Answer Call Waiting on Hold (Analogue)
☐ Busy On Held
☐ Outgoing Call Bar
☐ Offhook Station
☐ Can Intrude
☑ Cannot be Intruded
☑ Force Login
☐ Force Account Code
☐ System Phone

Multi Line Options
☑ Ringing Line Preference
☑ Idle Line Preference

Extn65453
Extn65454
Extn65455
Extn65456

Extn65443	65443	VoiceMail CallWaiting
Extn65444	65444	VoiceMail CallWaiting
Extn65445	65445	VoiceMail CallWaiting

6. *Complete the user*. Choose the **No** option for creating a new VoIP extension. This allows the user to be accessed easily at any telephone. Choose the **Yes** option when asked **Are you sure?**


Manager [255.255.255.255] (C:\Program Files\...\Manager\) 00E007009463.cfg
File Edit View Tools Window Help
User Hot Desk 277
VoiceRecording
Button Programming
Hunt Group Settings (T3 Sets only)
Personal Directory (T3 Sets only)
User
Voicemail
DND
ShortCodes
SourceNumbers
Telephony
Forwarding
Dial In
Allocated Answer Interval (secs)
Wrap-up Time (secs)
Transfer return Time (secs)
Individual Coverage Time (secs)
Login Code
Login Idle Period (secs)
Monitor Group
☐ Outgoing Call Bar
Yes
No
OK
Cancel
Help

Outside Call Sequence: DefaultRing

Inside Call Sequence: DefaultRing

Ring Back Sequence: DefaultRing

☑ Call Waiting On

☑ Answer Call Waiting on Hold (Analogue)

☐ Busy On Held

Multi Line Options

☑ Ringing Line Preference

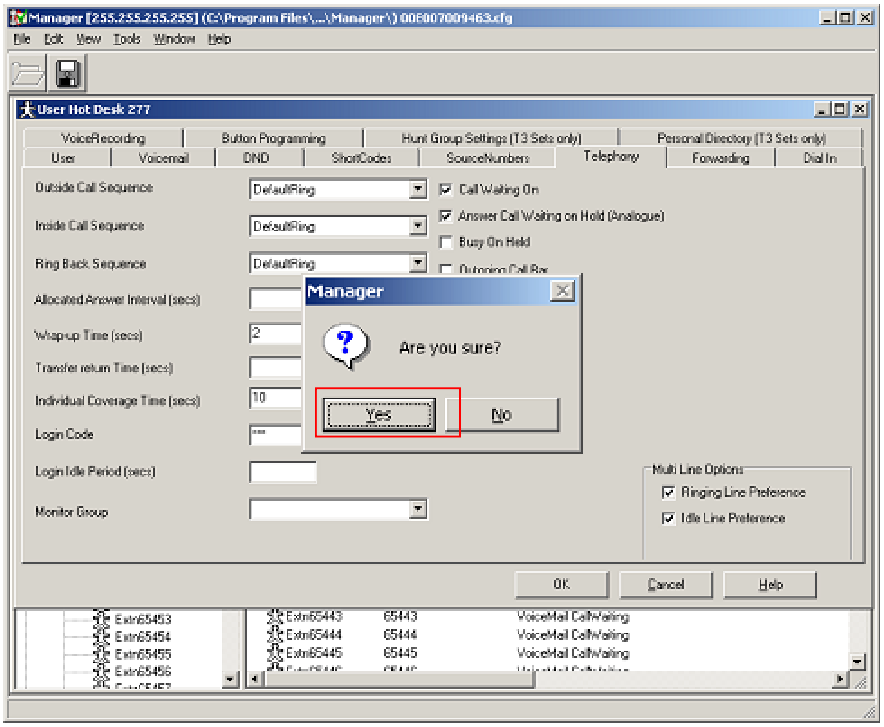
☑ Idle Line Preference

Manager

Create a new VoIP extension with this number?

Extn65453
Extn65454
Extn65455
Extn65456

Extn65443	65443	VoiceMail CallWaiting
Extn65444	65444	VoiceMail CallWaiting
Extn65445	65445	VoiceMail CallWaiting


Manager [255.255.255.255] (C:\Program Files\...\Manager\) 00E007009463.cfg
File Edit View Tools Window Help
User Hot Desk 277
VoiceRecording
Button Programming
Hunt Group Settings (T3 Sets only)
Personal Directory (T3 Sets only)
User
Voicemail
DND
ShortCodes
SourceNumbers
Telephony
Forwarding
Dial In
Allocated Answer Interval (secs)
Transfer return Time (secs)
Login Idle Period (secs)
Monitor Group
☐ Outgoing Call Bar
Yes
No
OK
Cancel
Help

Outside Call Sequence: DefaultRing

Inside Call Sequence: DefaultRing

Ring Back Sequence: DefaultRing

Wrap-up Time (secs): 2

Individual Coverage Time (secs): 10

Login Code: ***

☑ Call Waiting On

☑ Answer Call Waiting on Hold (Analogue)

☐ Busy On Held

Multi Line Options

☑ Ringing Line Preference

☑ Idle Line Preference

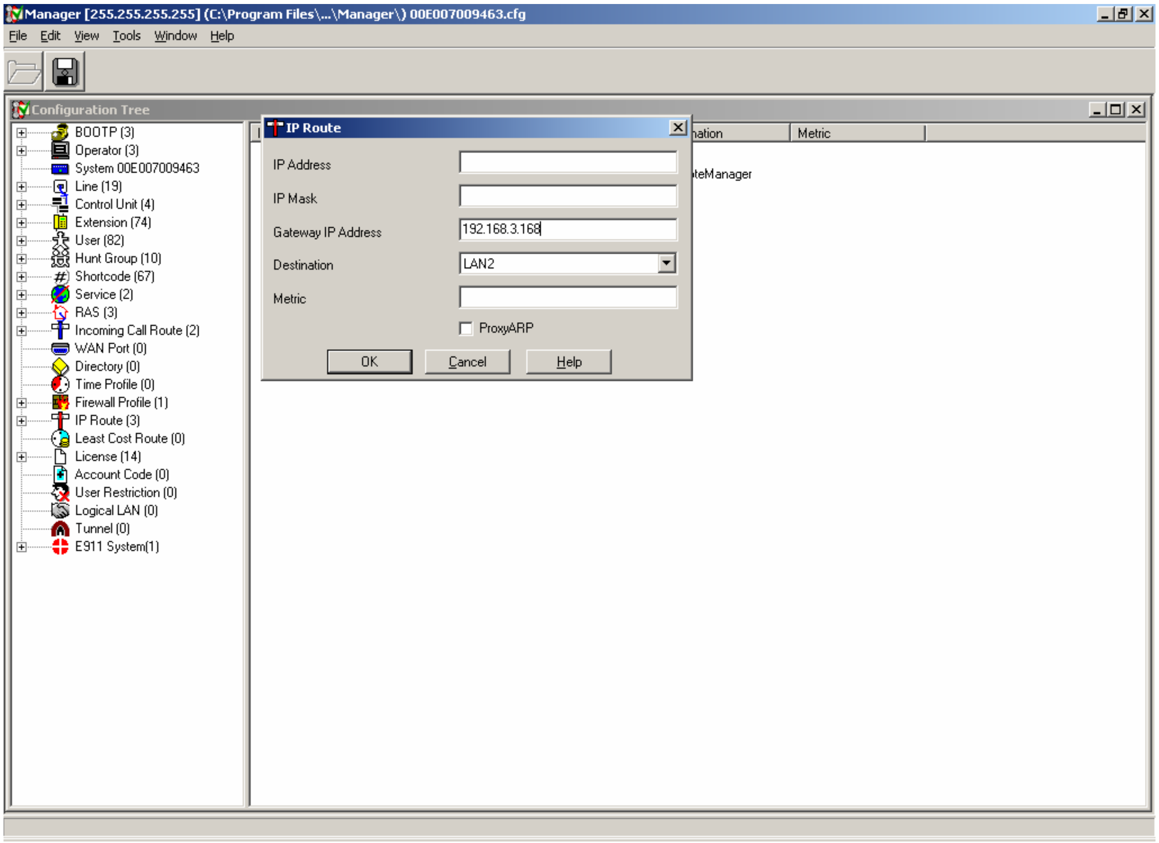
Manager

Are you sure?

Extn65453
Extn65454
Extn65455
Extn65456

Extn65443	65443	VoiceMail CallWaiting
Extn65444	65444	VoiceMail CallWaiting
Extn65445	65445	VoiceMail CallWaiting

7. *Make the NetGear ProSafe VPN Firewall FVX538 the default IP Route*. In IP Office Manager, select **IP Route** in the left panel. In the right panel, right click and select the **New** option. Enter the NetGear ProSafe VPN Firewall FVX538 LAN IP Address in the **Gateway IP Address** field and select LAN2 as the **Destination**. Retain all other default values. Press the **OK** button.



IP Address

IP Mask

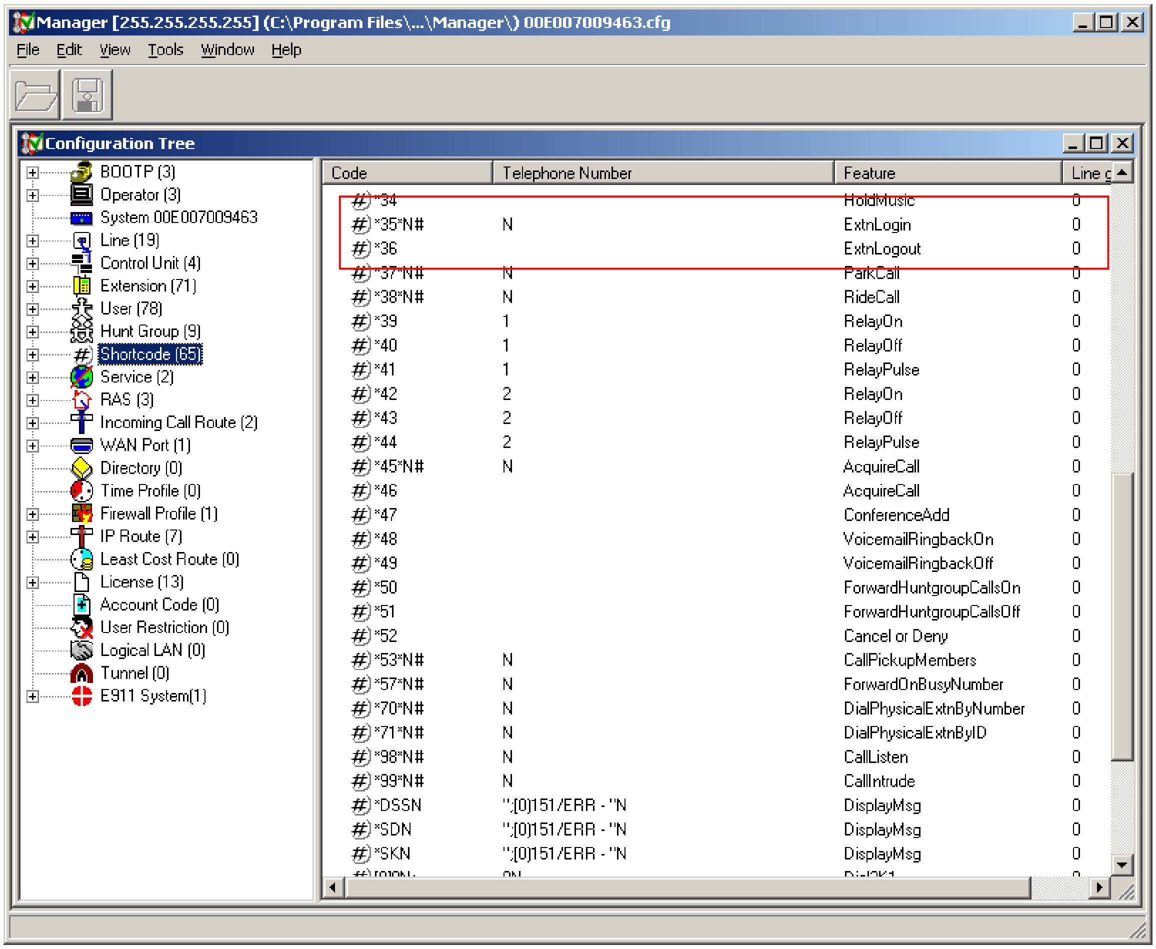
Gateway IP Address 192.168.3.168

Destination LAN2

Metric

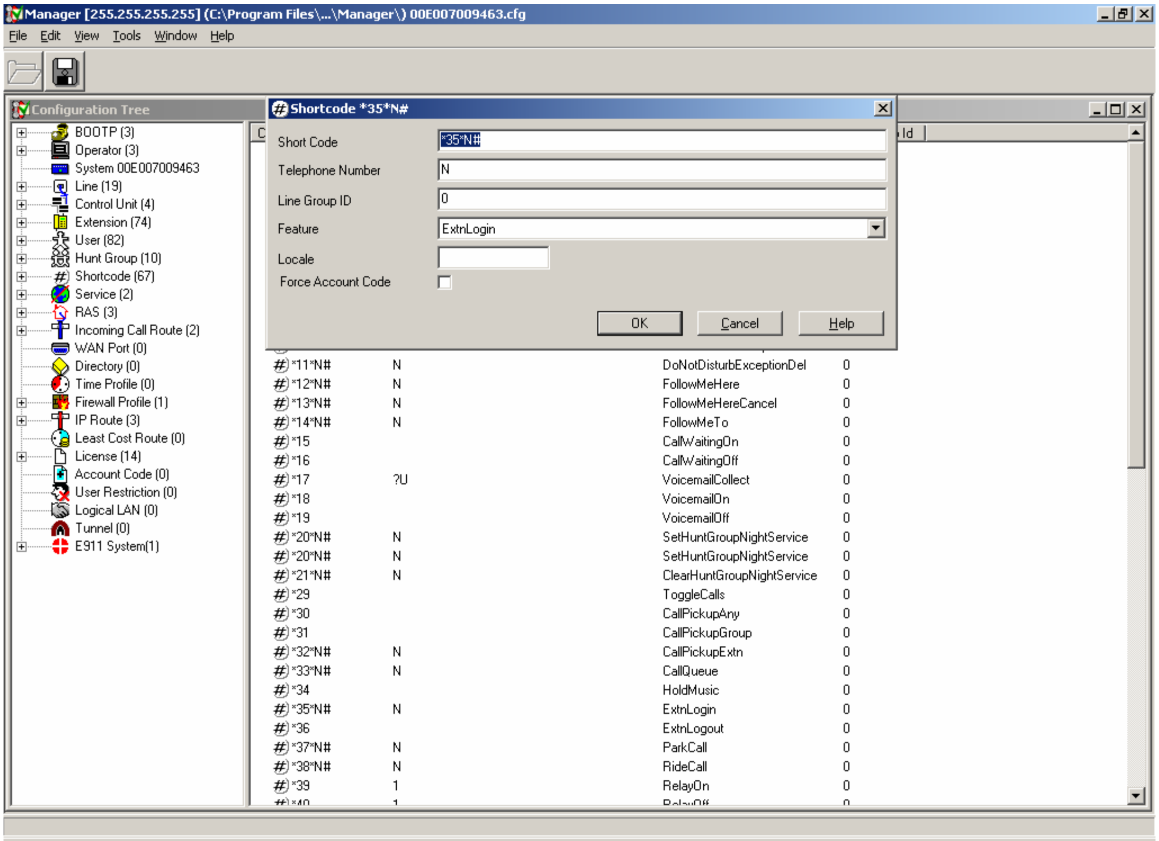
☐ ProxyARP

8. *Check to see if there are ExtnLogin and ExtnLogout shortcodes*. In the IP Office Manager Configuration Tree, click on **Shortcode** in the in the left panel. In the right panel, check to see if the **ExtnLogin** and **ExtnLogout** shortcodes exist. The defaults are shown below.



Code	Telephone Number	Feature	Line g
*34		HoldMusic	0
*35*N#	N	ExtnLogin	0
*36		ExtnLogout	0
*37*N#	N	ParkCall	0
*38*N#	N	RideCall	0
*39	1	RelayOn	0
*40	1	RelayOff	0
*41	1	RelayPulse	0
*42	2	RelayOn	0
*43	2	RelayOff	0
*44	2	RelayPulse	0
*45*N#	N	AcquireCall	0
*46		AcquireCall	0
*47		ConferenceAdd	0
*48		VoicemailRingbackOn	0
*49		VoicemailRingbackOff	0
*50		ForwardHuntgroupCallsOn	0
*51		ForwardHuntgroupCallsOff	0
*52		Cancel or Deny	0
*53*N#	N	CallPickupMembers	0
*57*N#	N	ForwardOnBusyNumber	0
*70*N#	N	DialPhysicalExtnByNumber	0
*71*N#	N	DialPhysicalExtnByID	0
*98*N#	N	CallListen	0
*99*N#	N	CallIntrude	0
*DSSN	";[0]151/ERR - "N	DisplayMsg	0
*SDN	";[0]151/ERR - "N	DisplayMsg	0
*SKN	";[0]151/ERR - "N	DisplayMsg	0

9. *If the shortcode is not present, add an ExtnLogin shortcode*. In the right panel right-click and select **New**. Set the **Feature** and **Telephone Number**, as shown below. Select a unique code for the **Short Code** field. The code must end with a "*N#". Press the **OK** button. In this case, the "N" represents a string of dialed digits; the extension number, a "*" and the login code entered in Step 5 of this section. The user logs in by dialing ***35*extension number*login code*#**.



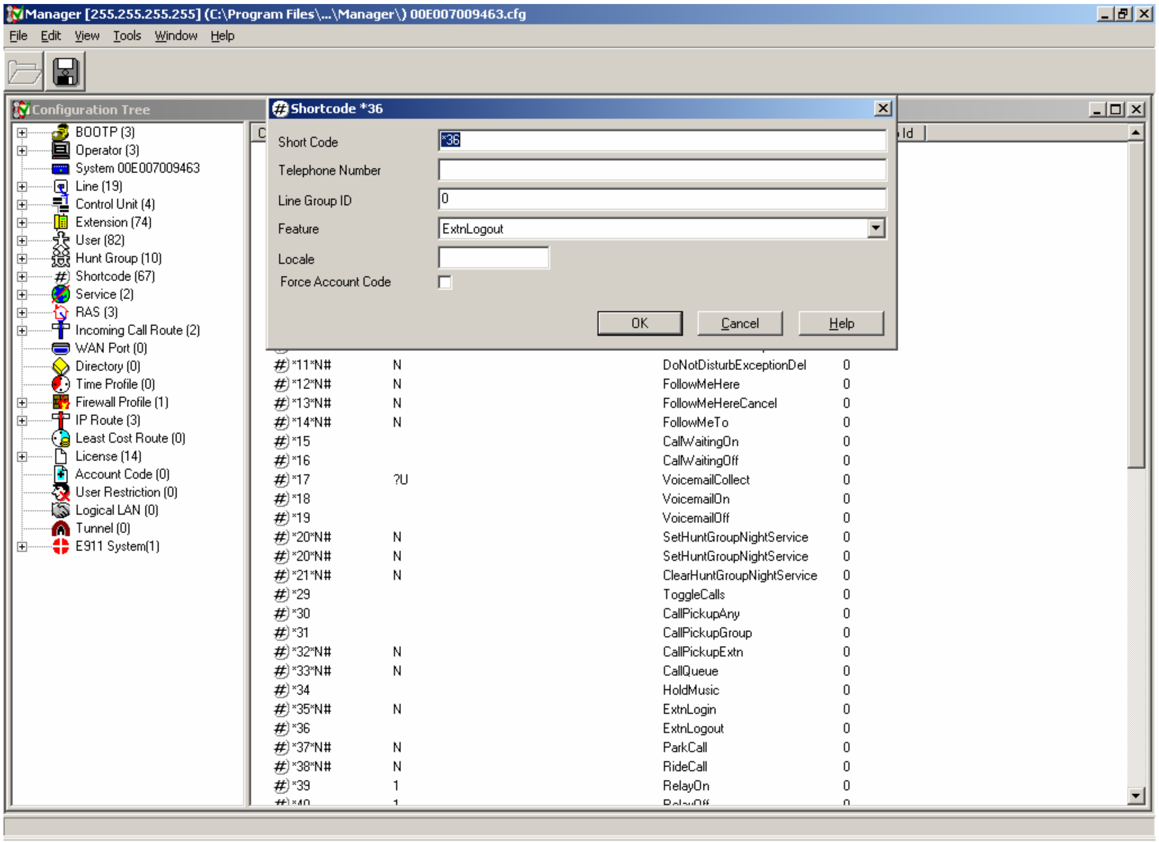
Shortcode *35*N#

Short Code: *35*N#
Telephone Number: N
Line Group ID: 0
Feature: ExtnLogin
Locale:
Force Account Code: □

OK | Cancel | Help

*11*N#	N	DoNotDisturbExceptionDel	0
*12*N#	N	FollowMeHere	0
*13*N#	N	FollowMeHereCancel	0
*14*N#	N	FollowMeTo	0
*15		CallWaitingOn	0
*16		CallWaitingOff	0
*17	?U	VoicemailCollect	0
*18		VoicemailOn	0
*19		VoicemailOff	0
*20*N#	N	SetHuntGroupNightService	0
*20*N#	N	SetHuntGroupNightService	0
*21*N#	N	ClearHuntGroupNightService	0
*29		ToggleCalls	0
*30		CallPickupAny	0
*31		CallPickupGroup	0
*32*N#	N	CallPickupExtn	0
*33*N#	N	CallQueue	0
*34		HoldMusic	0
*35*N#	N	ExtnLogin	0
*36		ExtnLogout	0
*37*N#	N	ParkCall	0
*38*N#	N	RideCall	0
*39	1	RelayOn	0
*40	1	RelayOff	0

10. *If the shortcode is not present, add an ExtnLogout shortcode.* In the right panel right click and select **New**. Set the **Feature**, as shown below. Select a unique code for the **Short Code** field. Press the **OK** button.



Short Code: *36

Telephone Number:

Line Group ID: 0

Feature: ExtnLogout

Locale:

Force Account Code: □

*11*N#	N	DoNotDisturbExceptionDel	0
*12*N#	N	FollowMeHere	0
*13*N#	N	FollowMeHereCancel	0
*14*N#	N	FollowMeTo	0
*15		CallWaitingOn	0
*16		CallWaitingOff	0
*17	?U	VoicemailCollect	0
*18		VoicemailOn	0
*19		VoicemailOff	0
*20*N#	N	SetHuntGroupNightService	0
*20*N#	N	SetHuntGroupNightService	0
*21*N#	N	ClearHuntGroupNightService	0
*29		ToggleCalls	0
*30		CallPickupAny	0
*31		CallPickupGroup	0
*32*N#	N	CallPickupExtn	0
*33*N#	N	CallQueue	0
*34		HoldMusic	0
*35*N#	N	ExtnLogin	0
*36		ExtnLogout	0
*37*N#	N	ParkCall	0
*38*N#	N	RideCall	0
*39	1	RelayOn	0
*40	1	RelayOff	0

4. Configure the NetGear ProSafe VPN Firewall FVX538 at the Main Site

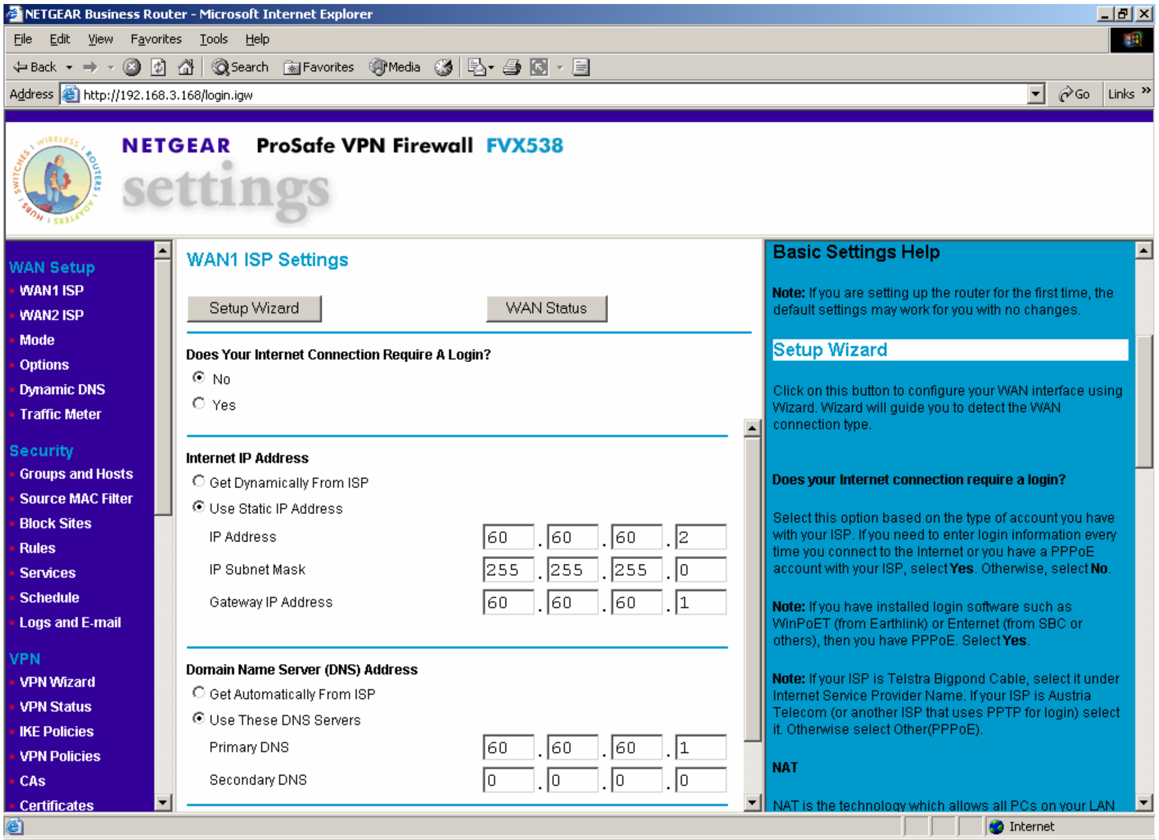
This section describes the NetGear ProSafe VPN Firewall FVX538 configuration at Main Site. The configuration includes:

- Configuring the WAN mode for Network Address Translation (NAT)
- Configuring an IP Route for the IP Office LAN1 Subnet
- Configuring a VPN

To configure the NetGear ProSafe VPN Firewall FVX538, open a web browser and enter the IP Address of the NetGear ProSafe VPN Firewall FVX538 in the Address field. This document assumes the IP Address of the LAN has been set.

1. *Configure the WAN ISP Settings.* Select **WAN Setup-> WAN1 ISP**.

   Select the appropriate option, which is provided by the ISP in the **Does You Internet Connection Require a Login?** field. In the Internet IP Address section, enter the **IP Address** and **Subnet Mask** of the FVX538 in the fields and enter the IP Address of the Cisco 3725 connection in the **Gateway IP Address** field. Press the **Apply** button.



WAN1 ISP Settings

Does Your Internet Connection Require A Login?

● No
○ Yes

Internet IP Address

○ Get Dynamically From ISP
● Use Static IP Address

IP Address	60 . 60 . 60 . 2
IP Subnet Mask	255 . 255 . 255 . 0
Gateway IP Address	60 . 60 . 60 . 1

Domain Name Server (DNS) Address

○ Get Automatically From ISP
● Use These DNS Servers

Primary DNS	60 . 60 . 60 . 1
Secondary DNS	0 . 0 . 0 . 0

Basic Settings Help

Note: If you are setting up the router for the first time, the default settings may work for you with no changes.

Setup Wizard

Click on this button to configure your WAN interface using Wizard. Wizard will guide you to detect the WAN connection type.

Does your Internet connection require a login?

Select this option based on the type of account you have with your ISP. If you need to enter login information every time you connect to the Internet or you have a PPPoE account with your ISP, select **Yes**. Otherwise, select **No**.

Note: If you have installed login software such as WinPoET (from Earthlink) or Enternet (from SBC or others), then you have PPPoE. Select **Yes**.

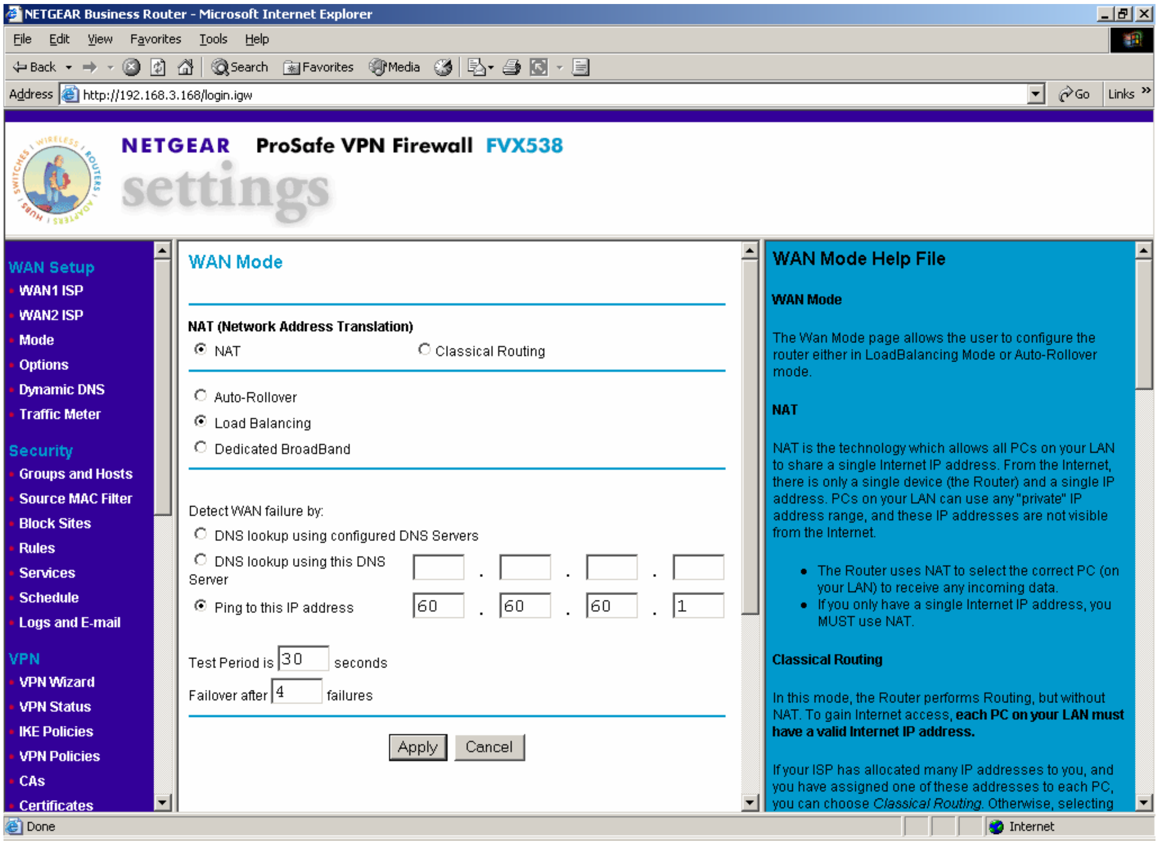
Note: If your ISP is Telstra Bigpond Cable, select it under Internet Service Provider Name. If your ISP is Austria Telecom (or another ISP that uses PPTP for login) select it. Otherwise select Other(PPPoE).

NAT

NAT is the technology which allows all PCs on your LAN

2. *Configure the WAN Mode.* Select **WAN Setup-> Mode**.

   Select the **NAT** option for **NAT (Network Address Translation)**. Select **Ping to this IP Address** for the **Detect WAN failure by:** option. Enter the IP Address of the Cisco 3725. Press the **Apply** button.



WAN Mode

NAT (Network Address Translation)

● NAT ○ Classical Routing

○ Auto-Rollover
● Load Balancing
○ Dedicated BroadBand

Detect WAN failure by:

○ DNS lookup using configured DNS Servers
○ DNS lookup using this DNS Server ___ . ___ . ___ . ___
● Ping to this IP address 60 . 60 . 60 . 1

Test Period is 30 seconds

Failover after 4 failures

WAN Mode Help File

WAN Mode

The Wan Mode page allows the user to configure the router either in LoadBalancing Mode or Auto-Rollover mode.

NAT

NAT is the technology which allows all PCs on your LAN to share a single Internet IP address. From the Internet, there is only a single device (the Router) and a single IP address. PCs on your LAN can use any "private" IP address range, and these IP addresses are not visible from the Internet.

- The Router uses NAT to select the correct PC (on your LAN) to receive any incoming data.
- If you only have a single Internet IP address, you MUST use NAT.

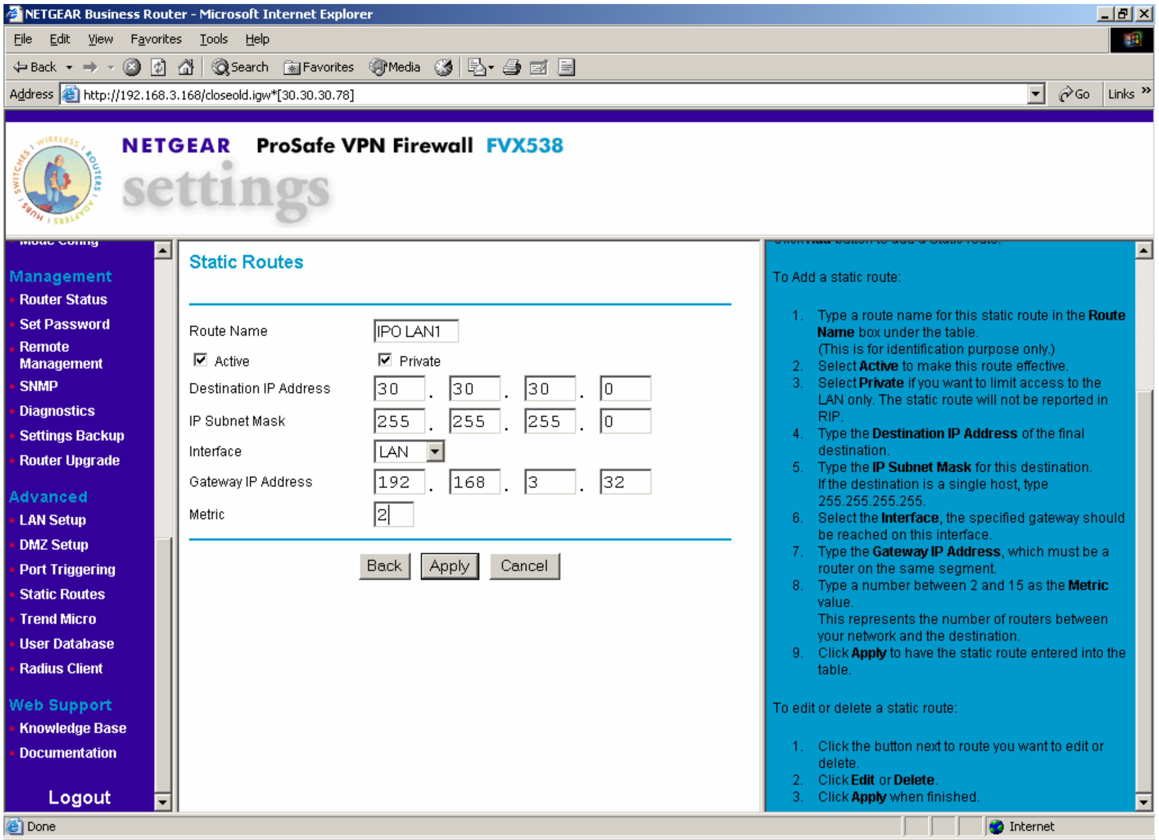
Classical Routing

In this mode, the Router performs Routing, but without NAT. To gain Internet access, **each PC on your LAN must have a valid Internet IP address.**

If your ISP has allocated many IP addresses to you, and you have assigned one of these addresses to each PC, you can choose *Classical Routing*. Otherwise, selecting

3. *Configure a static IP Route for the IP Office LAN1 subnet.* Select **Advanced->Static Routes**. Press the **Add** button.

   Enter a unique name for the **Route Name**. Check the **Active** and **Private** boxes. This ensures that the route will be used and not reported in RIP tables. Enter the IP Office LAN1 Subnet in the **Destination IP Address** field. Enter the appropriate Subnet Mask in the **IP Subnet Mask** field. Select LAN in the **Interface** field. Enter the Avaya IP Office 412 LAN2 IP Address in the **Gateway IP Address** field. Enter the **Metric** as shown below. Press the **Apply** button.



Static Routes

Route Name	IPO LAN1
☑ Active	☑ Private
Destination IP Address	30 . 30 . 30 . 0
IP Subnet Mask	255 . 255 . 255 . 0
Interface	LAN
Gateway IP Address	192 . 168 . 3 . 32
Metric	2

To Add a static route:

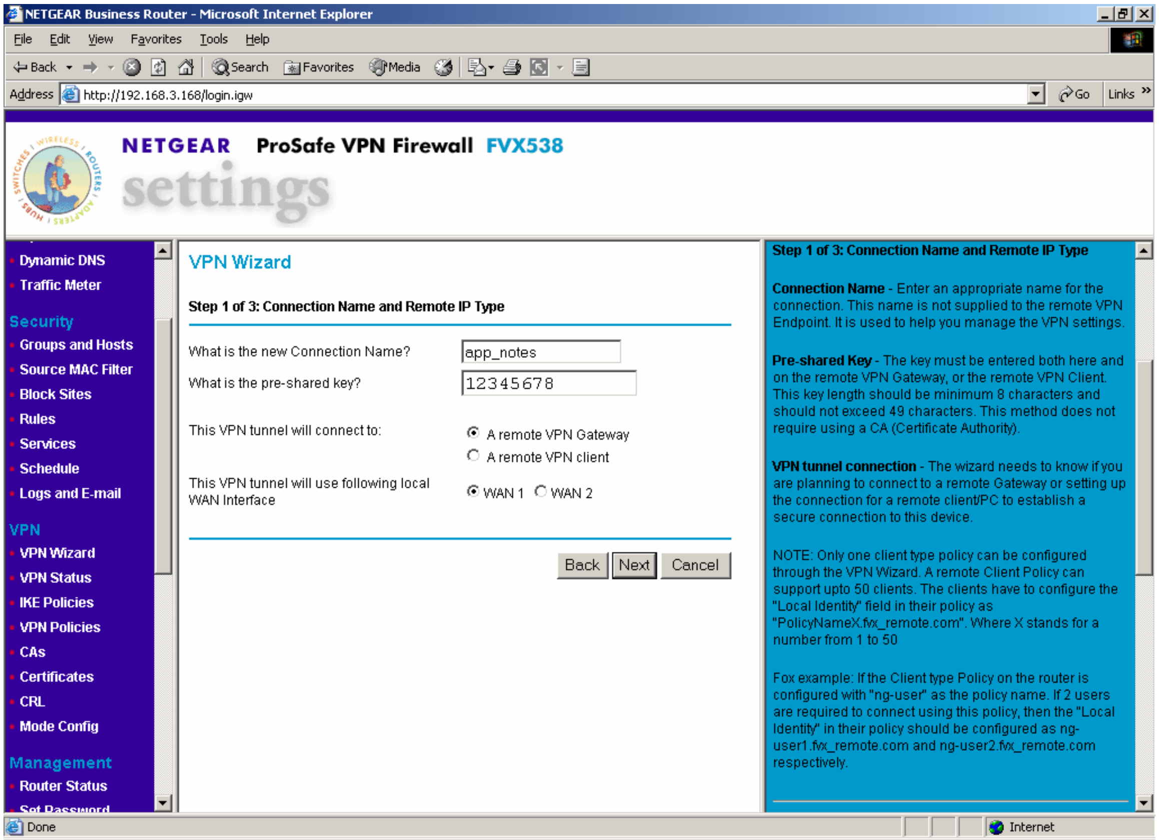
1. Type a route name for this static route in the **Route Name** box under the table.
   (This is for identification purpose only.)
2. Select **Active** to make this route effective.
3. Select **Private** if you want to limit access to the LAN only. The static route will not be reported in RIP.
4. Type the **Destination IP Address** of the final destination.
5. Type the **IP Subnet Mask** for this destination.
   If the destination is a single host, type 255.255.255.255.
6. Select the **Interface**, the specified gateway should be reached on this interface.
7. Type the **Gateway IP Address**, which must be a router on the same segment.
8. Type a number between 2 and 15 as the **Metric** value.
   This represents the number of routers between your network and the destination.
9. Click **Apply** to have the static route entered into the table.

To edit or delete a static route:

1. Click the button next to route you want to edit or delete.
2. Click **Edit** or **Delete**.
3. Click **Apply** when finished.

4. *Add a VPN*. Select **VPN->VPN Wizard**. Press the **Next** button.

Enter a unique name in the **What is the new Connection Name?** field. Enter a text string in the **What is the pre-shared key?** field. Select the **A remote VPN Gateway** for the **This VPN tunnel will connect to** field. Select WAN1 for the **This VPN tunnel will use the following local WAN 1 Interface** field. Press the **Next** button.



VPN Wizard

Step 1 of 3: Connection Name and Remote IP Type

What is the new Connection Name? app_notes

What is the pre-shared key? 12345678

This VPN tunnel will connect to: ● A remote VPN Gateway ○ A remote VPN client

This VPN tunnel will use following local WAN Interface ● WAN 1 ○ WAN 2

Back Next Cancel

Step 1 of 3: Connection Name and Remote IP Type

Connection Name - Enter an appropriate name for the connection. This name is not supplied to the remote VPN Endpoint. It is used to help you manage the VPN settings.

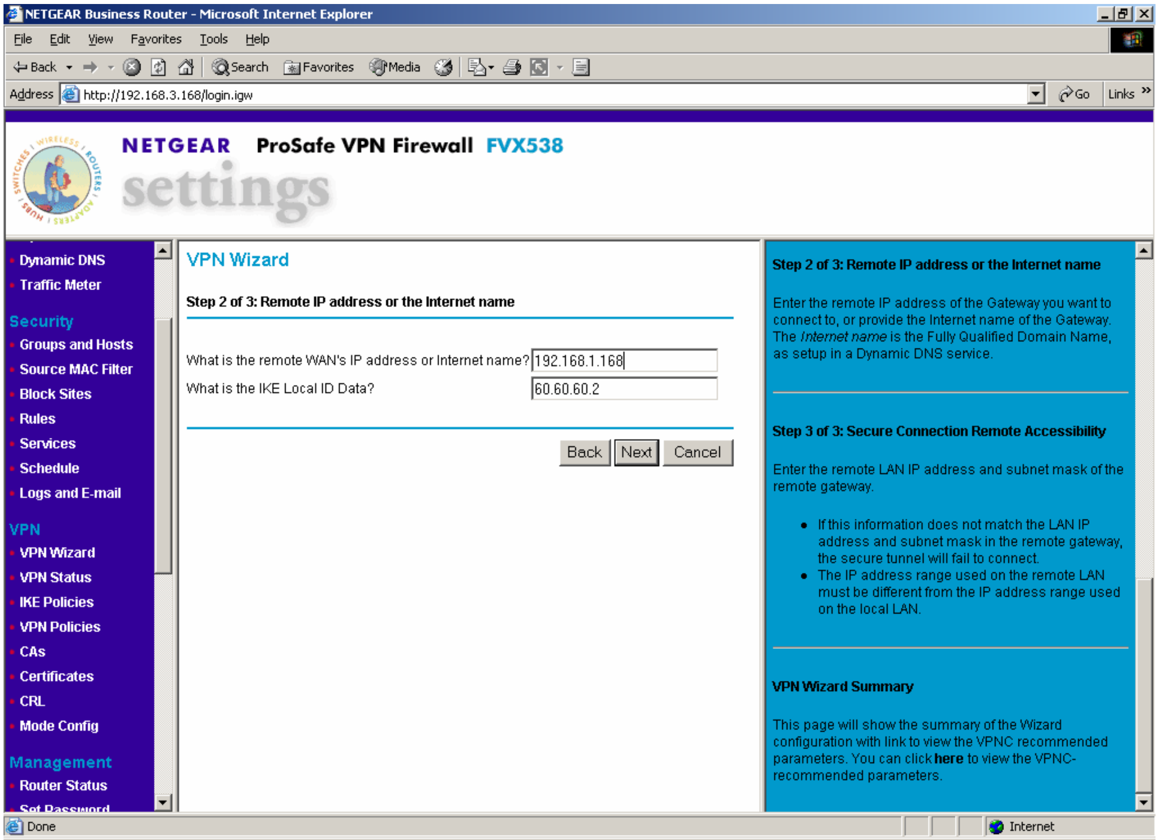
Pre-shared Key - The key must be entered both here and on the remote VPN Gateway, or the remote VPN Client. This key length should be minimum 8 characters and should not exceed 49 characters. This method does not require using a CA (Certificate Authority).

VPN tunnel connection - The wizard needs to know if you are planning to connect to a remote Gateway or setting up the connection for a remote client/PC to establish a secure connection to this device.

NOTE: Only one client type policy can be configured through the VPN Wizard. A remote Client Policy can support upto 50 clients. The clients have to configure the "Local Identity" field in their policy as "PolicyNameX.fvx_remote.com". Where X stands for a number from 1 to 50

Fox example: If the Client type Policy on the router is configured with "ng-user" as the policy name. If 2 users are required to connect using this policy, then the "Local Identity" in their policy should be configured as ng-user1.fvx_remote.com and ng-user2.fvx_remote.com respectively.

5. *Configure the IP Address of the Remote End of the tunnel*. Enter the WAN IP Address of the NetGear ProSafe VPN Firewall FVS114 in the **What is the remote WAN's IP address or the Internet name** field. The actual IP address of the remote site WAN is placed in this field and not the NAT'd version. The **What is the IKE Local ID Data** field is pre-populated with the FVX538 WAN1 IP Address and does not have to be changed. Press the **Next** button.



VPN Wizard

Step 2 of 3: Remote IP address or the Internet name

What is the remote WAN's IP address or Internet name? 192.168.1.168

What is the IKE Local ID Data? 60.60.60.2

Step 2 of 3: Remote IP address or the Internet name

Enter the remote IP address of the Gateway you want to connect to, or provide the Internet name of the Gateway. The *Internet name* is the Fully Qualified Domain Name, as setup in a Dynamic DNS service.

Step 3 of 3: Secure Connection Remote Accessibility

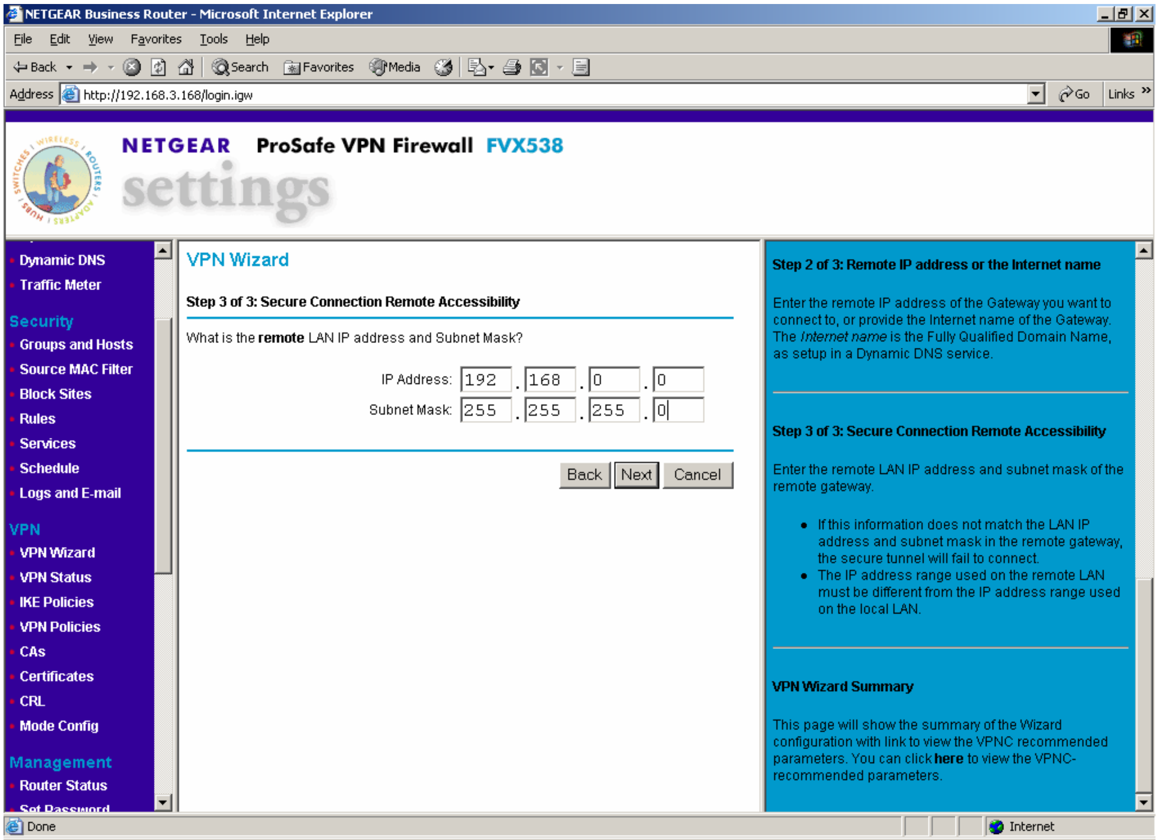
Enter the remote LAN IP address and subnet mask of the remote gateway.

- If this information does not match the LAN IP address and subnet mask in the remote gateway, the secure tunnel will fail to connect.
- The IP address range used on the remote LAN must be different from the IP address range used on the local LAN.

VPN Wizard Summary

This page will show the summary of the Wizard configuration with link to view the VPNC recommended parameters. You can click **here** to view the VPNC-recommended parameters.

6. *Configure the Remote subnet of the VPN*. Enter the LAN subnet of the NetGear ProSafe VPN Firewall FVS114 in the **IP Address** field and the Subnet Mask of the LAN Subnet in the **Subnet Mask** field. Press the **Next** button.



VPN Wizard

Step 3 of 3: Secure Connection Remote Accessibility

What is the **remote** LAN IP address and Subnet Mask?

IP Address: 192 . 168 . 0 . 0

Subnet Mask: 255 . 255 . 255 . 0

Step 2 of 3: Remote IP address or the Internet name

Enter the remote IP address of the Gateway you want to connect to, or provide the Internet name of the Gateway. The *Internet name* is the Fully Qualified Domain Name, as setup in a Dynamic DNS service.

Step 3 of 3: Secure Connection Remote Accessibility

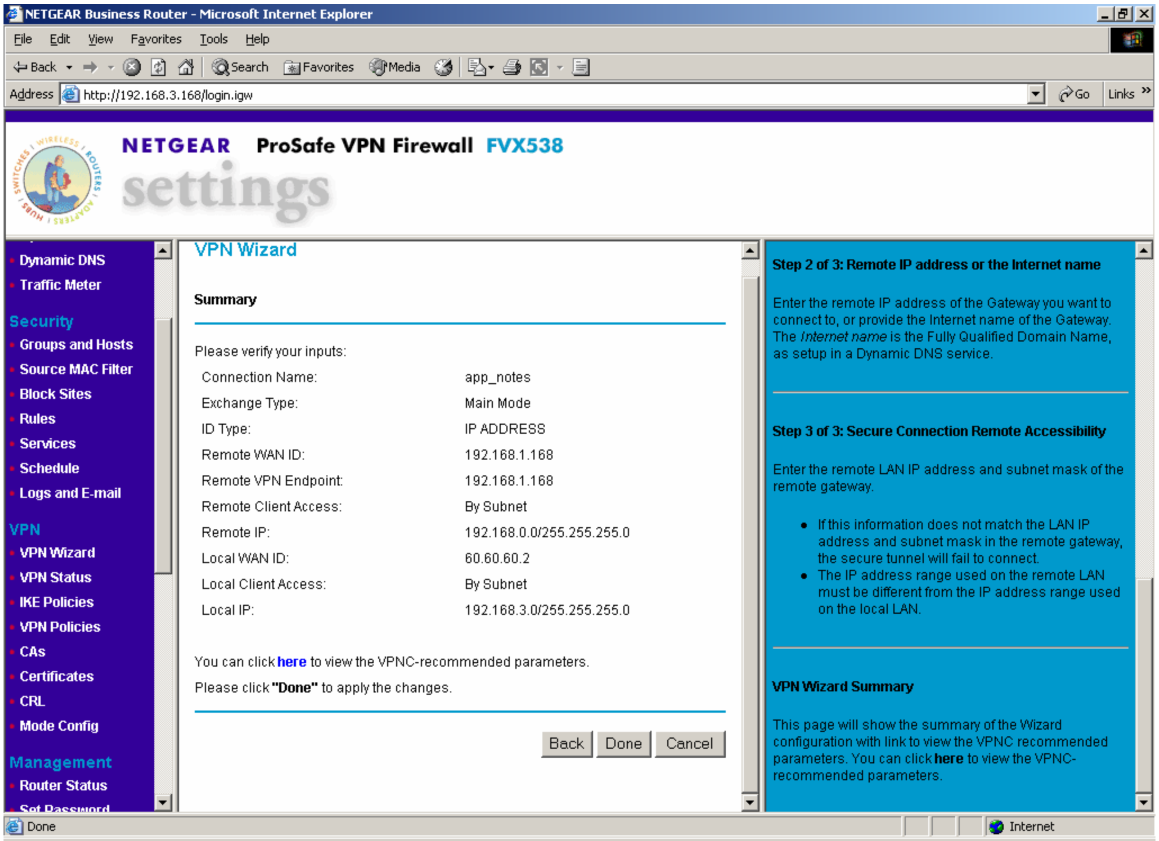
Enter the remote LAN IP address and subnet mask of the remote gateway.

- If this information does not match the LAN IP address and subnet mask in the remote gateway, the secure tunnel will fail to connect.
- The IP address range used on the remote LAN must be different from the IP address range used on the local LAN.

VPN Wizard Summary

This page will show the summary of the Wizard configuration with link to view the VPNC recommended parameters. You can click **here** to view the VPNC-recommended parameters.

7. *Complete the VPN*. Verify all the settings. Press the **Done** button.



VPN Wizard

Summary

Please verify your inputs:

Connection Name:	app_notes
Exchange Type:	Main Mode
ID Type:	IP ADDRESS
Remote WAN ID:	192.168.1.168
Remote VPN Endpoint:	192.168.1.168
Remote Client Access:	By Subnet
Remote IP:	192.168.0.0/255.255.255.0
Local WAN ID:	60.60.60.2
Local Client Access:	By Subnet
Local IP:	192.168.3.0/255.255.255.0

You can click **here** to view the VPNC-recommended parameters.

Please click **"Done"** to apply the changes.

Back Done Cancel

Step 2 of 3: Remote IP address or the Internet name

Enter the remote IP address of the Gateway you want to connect to, or provide the Internet name of the Gateway. The *Internet name* is the Fully Qualified Domain Name, as setup in a Dynamic DNS service.

Step 3 of 3: Secure Connection Remote Accessibility

Enter the remote LAN IP address and subnet mask of the remote gateway.

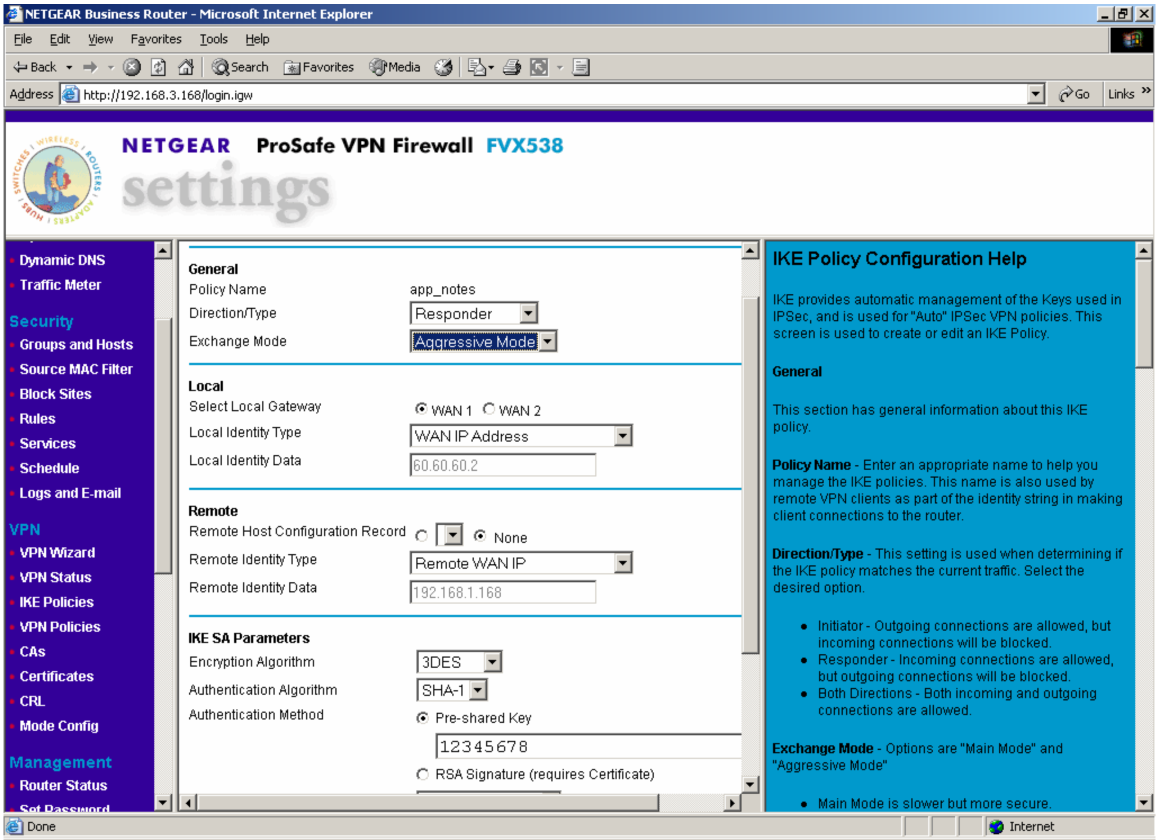
- If this information does not match the LAN IP address and subnet mask in the remote gateway, the secure tunnel will fail to connect.
- The IP address range used on the remote LAN must be different from the IP address range used on the local LAN.

VPN Wizard Summary

This page will show the summary of the Wizard configuration with link to view the VPNC recommended parameters. You can click **here** to view the VPNC-recommended parameters.

8. *Modify the IKE policy*. Select **VPN->IKE Policies**. Select the radio button for the VPN policy created in Steps 3-6 and press the **Edit** button.

   Select **Aggressive Mod**e for the **Exchange Mode** and **Responder** for the **Direction/Type**. Scroll down and press the **Apply** button. Using Aggressive mode provides more security.



General
Policy Name app_notes
Direction/Type Responder
Exchange Mode Aggressive Mode

Local
Select Local Gateway ● WAN 1 ○ WAN 2
Local Identity Type WAN IP Address
Local Identity Data 60.60.60.2

Remote
Remote Host Configuration Record ○ ● None
Remote Identity Type Remote WAN IP
Remote Identity Data 192.168.1.168

IKE SA Parameters
Encryption Algorithm 3DES
Authentication Algorithm SHA-1
Authentication Method ● Pre-shared Key
12345678
○ RSA Signature (requires Certificate)

IKE Policy Configuration Help

IKE provides automatic management of the Keys used in IPSec, and is used for "Auto" IPSec VPN policies. This screen is used to create or edit an IKE Policy.

General

This section has general information about this IKE policy.

Policy Name - Enter an appropriate name to help you manage the IKE policies. This name is also used by remote VPN clients as part of the identity string in making client connections to the router.

Direction/Type - This setting is used when determining if the IKE policy matches the current traffic. Select the desired option.

- Initiator - Outgoing connections are allowed, but incoming connections will be blocked.
- Responder - Incoming connections are allowed, but outgoing connections will be blocked.
- Both Directions - Both incoming and outgoing connections are allowed.

Exchange Mode - Options are "Main Mode" and "Aggressive Mode"

- Main Mode is slower but more secure.

9. *Disable the H323 Application Layer Gateway*. Telnet to the FVX538 LAN IP Address. Login with the appropriate credentials. Enter the commands as shown below.

```
FVX538: />cd config
FVX538: /config> cd algs
FVX538: /config/algs> disable h323
```

This completes the configuration of the NetGear ProSafe VPN Firewall FVX538.

5. Configure the NetGear ProSafe VPN Firewall FVS114 at the Remote Site

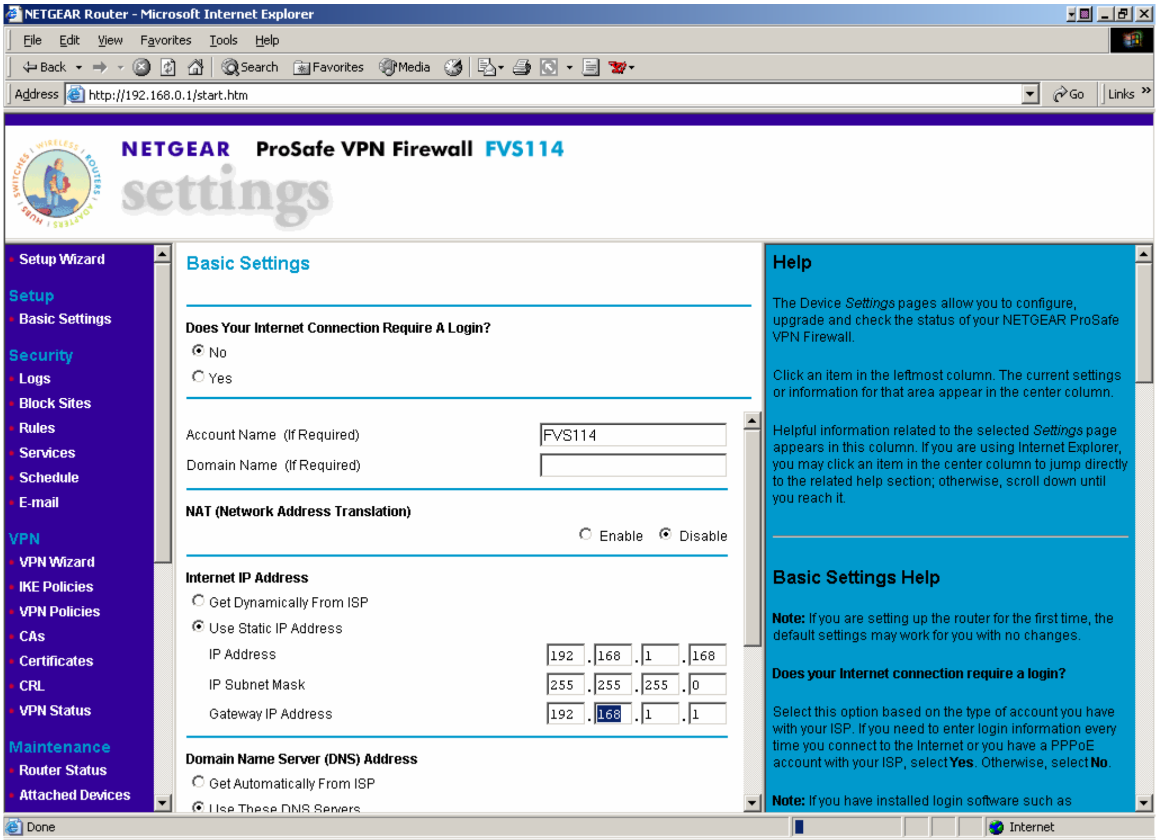
This section describes the NetGear ProSafe VPN Firewall FVS114 configuration at the Remote Site. The configuration includes:

- Configuring the WAN
- Configuring a VPN

To configure the NetGear ProSafe VPN Firewall FVS114, open a web browser and enter the IP Address of the NetGear ProSafe VPN Firewall FVS114 in the Address field. This document assumes the IP Address of the LAN has been set.

1. *Configure the WAN.* Select **Setup->Basic Settings**.

   Enter the WAN IP Address in the **IP Address** field and the Westell DSL modem IP Address in the **Gateway IP Address** field. Scroll down and press the **Apply** button.



Basic Settings

Does Your Internet Connection Require A Login?

● No

○ Yes

Account Name (If Required) FVS114

Domain Name (If Required)

NAT (Network Address Translation) ○ Enable ● Disable

Internet IP Address

○ Get Dynamically From ISP

● Use Static IP Address

IP Address 192 . 168 . 1 . 168

IP Subnet Mask 255 . 255 . 255 . 0

Gateway IP Address 192 . 168 . 1 . 1

Domain Name Server (DNS) Address

○ Get Automatically From ISP

● Use These DNS Servers

Help

The Device *Settings* pages allow you to configure, upgrade and check the status of your NETGEAR ProSafe VPN Firewall.

Click an item in the leftmost column. The current settings or information for that area appear in the center column.

Helpful information related to the selected *Settings* page appears in this column. If you are using Internet Explorer, you may click an item in the center column to jump directly to the related help section; otherwise, scroll down until you reach it.

Basic Settings Help

Note: If you are setting up the router for the first time, the default settings may work for you with no changes.

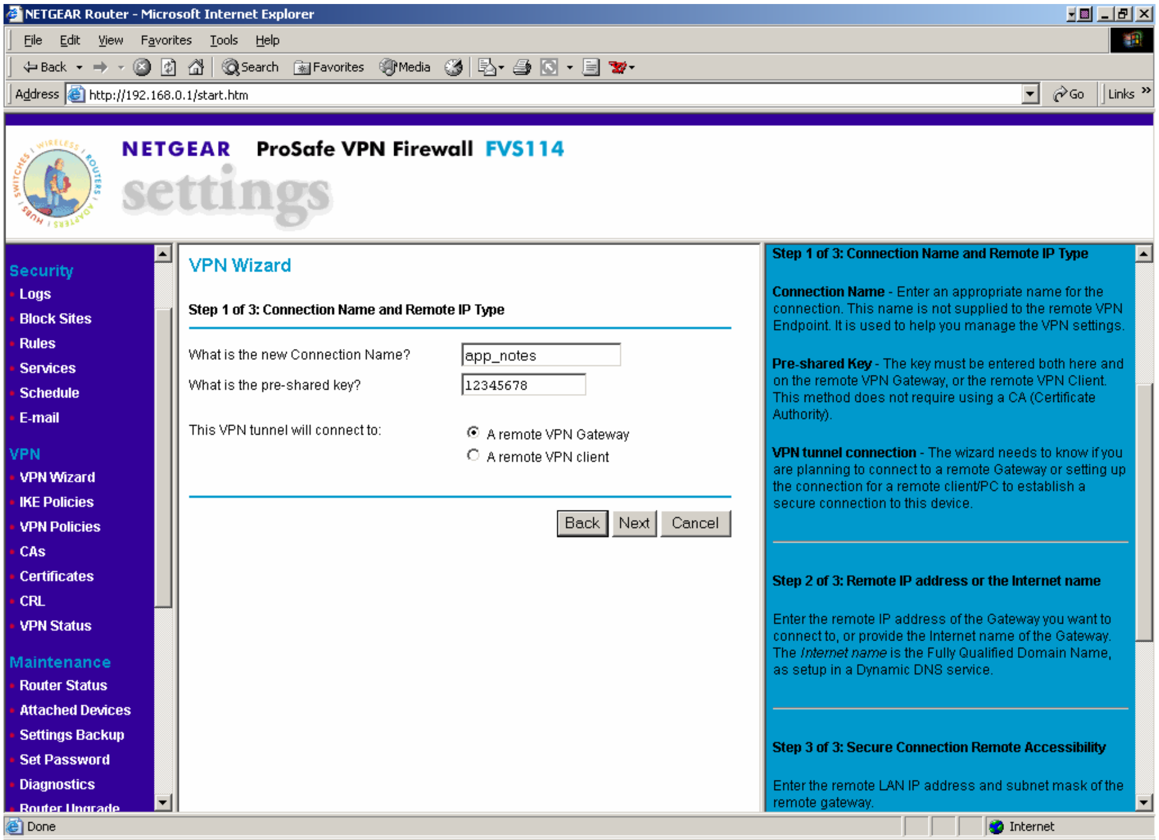
Does your Internet connection require a login?

Select this option based on the type of account you have with your ISP. If you need to enter login information every time you connect to the Internet or you have a PPPoE account with your ISP, select **Yes**. Otherwise, select **No**.

Note: If you have installed login software such as

2. *Add a VPN*. Select **VPN->VPN Wizard**. Press the **Next** button.

   Enter a unique name in the **What is the new Connection Name?** field. Enter a text string in the **What is the pre-shared key?** field. Select the **A remote VPN Gateway** for the **This VPN tunnel will connect to** field. Press the **Next** button.



VPN Wizard

Step 1 of 3: Connection Name and Remote IP Type

What is the new Connection Name? app_notes

What is the pre-shared key? 12345678

This VPN tunnel will connect to:
● A remote VPN Gateway
○ A remote VPN client

Step 1 of 3: Connection Name and Remote IP Type

Connection Name - Enter an appropriate name for the connection. This name is not supplied to the remote VPN Endpoint. It is used to help you manage the VPN settings.

Pre-shared Key - The key must be entered both here and on the remote VPN Gateway, or the remote VPN Client. This method does not require using a CA (Certificate Authority).

VPN tunnel connection - The wizard needs to know if you are planning to connect to a remote Gateway or setting up the connection for a remote client/PC to establish a secure connection to this device.

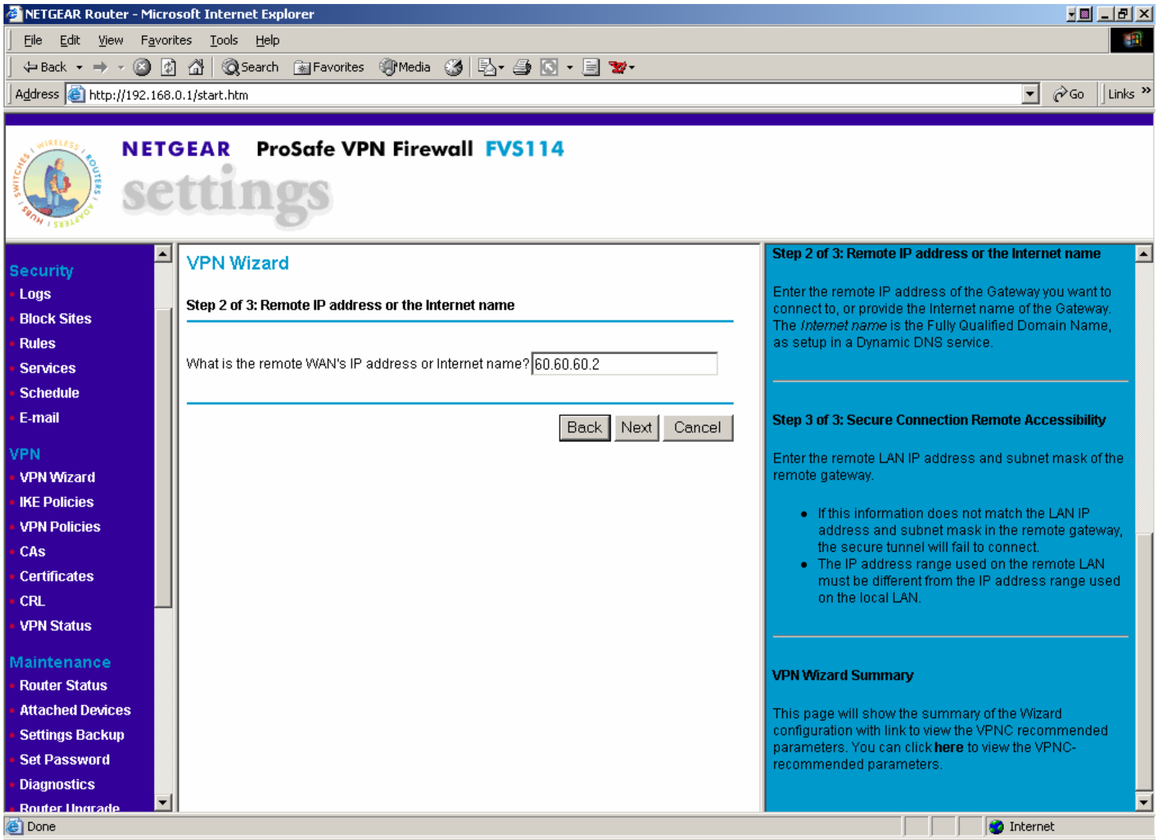
Step 2 of 3: Remote IP address or the Internet name

Enter the remote IP address of the Gateway you want to connect to, or provide the Internet name of the Gateway. The *Internet name* is the Fully Qualified Domain Name, as setup in a Dynamic DNS service.

Step 3 of 3: Secure Connection Remote Accessibility

Enter the remote LAN IP address and subnet mask of the remote gateway.

3. *Configure the IP Address of the Remote End of the tunnel*. Enter the WAN IP Address of the NetGear ProSafe VPN Firewall FVX538 in the **What is the remote WAN's IP address or the Internet name?** field. Press the **Next** button.



VPN Wizard

Step 2 of 3: Remote IP address or the Internet name

What is the remote WAN's IP address or Internet name? 60.60.60.2

Step 2 of 3: Remote IP address or the Internet name

Enter the remote IP address of the Gateway you want to connect to, or provide the Internet name of the Gateway. The *Internet name* is the Fully Qualified Domain Name, as setup in a Dynamic DNS service.

Step 3 of 3: Secure Connection Remote Accessibility

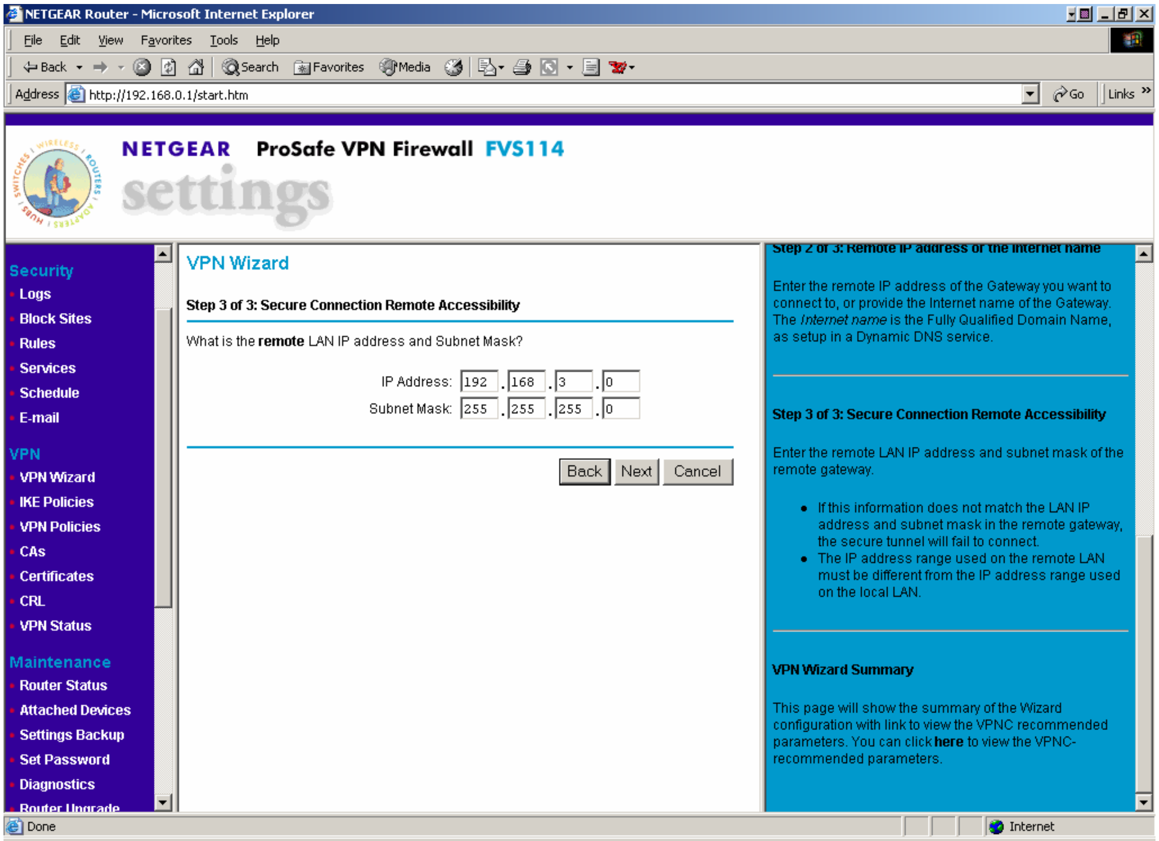
Enter the remote LAN IP address and subnet mask of the remote gateway.

- If this information does not match the LAN IP address and subnet mask in the remote gateway, the secure tunnel will fail to connect.
- The IP address range used on the remote LAN must be different from the IP address range used on the local LAN.

VPN Wizard Summary

This page will show the summary of the Wizard configuration with link to view the VPNC recommended parameters. You can click **here** to view the VPNC-recommended parameters.

4. *Configure the Remote end of the VPN.* Enter the LAN subnet of the NetGear ProSafe VPN Firewall FVX538 in the **IP Address** field and the Subnet Mask of the LAN Subnet in the **Subnet Mask** field. Press the **Next** button.



VPN Wizard

Step 3 of 3: Secure Connection Remote Accessibility

What is the **remote** LAN IP address and Subnet Mask?

IP Address: 192 . 168 . 3 . 0

Subnet Mask: 255 . 255 . 255 . 0

Back Next Cancel

Step 2 of 3: Remote IP address or the Internet name

Enter the remote IP address of the Gateway you want to connect to, or provide the Internet name of the Gateway. The *Internet name* is the Fully Qualified Domain Name, as setup in a Dynamic DNS service.

Step 3 of 3: Secure Connection Remote Accessibility

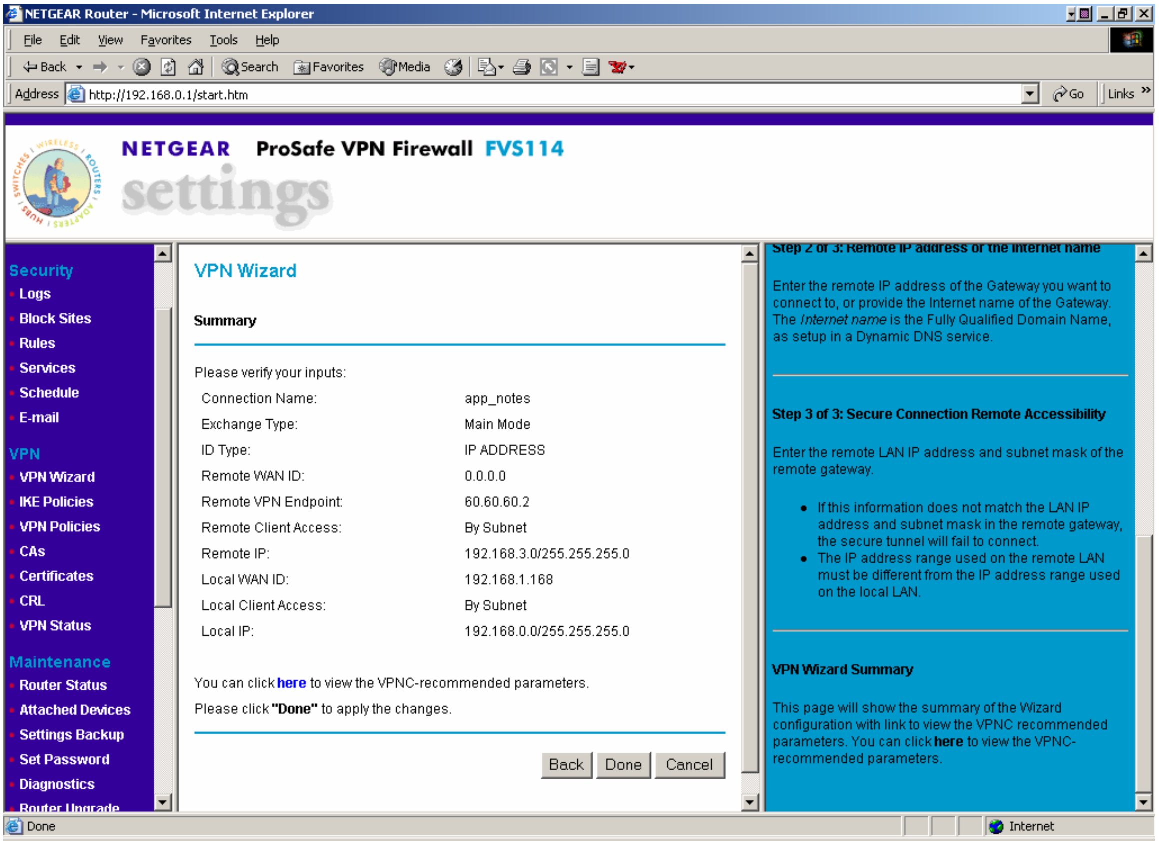
Enter the remote LAN IP address and subnet mask of the remote gateway.

- If this information does not match the LAN IP address and subnet mask in the remote gateway, the secure tunnel will fail to connect.
- The IP address range used on the remote LAN must be different from the IP address range used on the local LAN.

VPN Wizard Summary

This page will show the summary of the Wizard configuration with link to view the VPNC recommended parameters. You can click **here** to view the VPNC-recommended parameters.

5. *Complete the VPN*. Verify all the settings. Press the **Done** button.



VPN Wizard

Summary

Please verify your inputs:

Connection Name:	app_notes
Exchange Type:	Main Mode
ID Type:	IP ADDRESS
Remote WAN ID:	0.0.0.0
Remote VPN Endpoint:	60.60.60.2
Remote Client Access:	By Subnet
Remote IP:	192.168.3.0/255.255.255.0
Local WAN ID:	192.168.1.168
Local Client Access:	By Subnet
Local IP:	192.168.0.0/255.255.255.0

You can click **here** to view the VPNC-recommended parameters.

Please click **"Done"** to apply the changes.

Step 2 of 3: Remote IP address or the Internet name

Enter the remote IP address of the Gateway you want to connect to, or provide the Internet name of the Gateway. The *Internet name* is the Fully Qualified Domain Name, as setup in a Dynamic DNS service.

Step 3 of 3: Secure Connection Remote Accessibility

Enter the remote LAN IP address and subnet mask of the remote gateway.

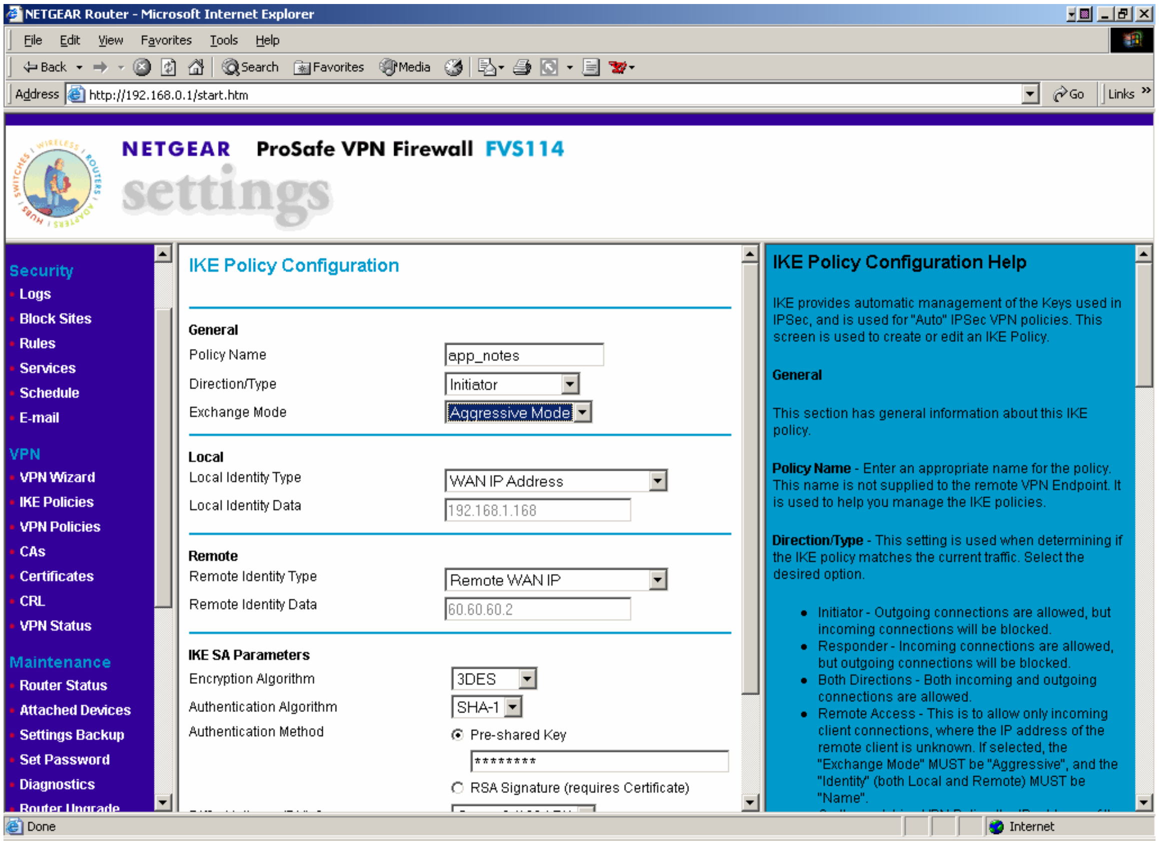
- If this information does not match the LAN IP address and subnet mask in the remote gateway, the secure tunnel will fail to connect.
- The IP address range used on the remote LAN must be different from the IP address range used on the local LAN.

VPN Wizard Summary

This page will show the summary of the Wizard configuration with link to view the VPNC recommended parameters. You can click **here** to view the VPNC-recommended parameters.

6. *Modify the IKE policy*. Select **VPN->IKE** Policies. Select the radio button for the VPN policy created in Steps 2-5 and press the **Edit** button.

   Select Initiator for the **Direction/Type** and Aggressive Mode for the **Exchange Mode**. Scroll down and press the **Apply** button. Using Aggressive mode provides more security.



IKE Policy Configuration

General

Policy Name	app_notes
Direction/Type	Initiator
Exchange Mode	Aggressive Mode

Local

Local Identity Type	WAN IP Address
Local Identity Data	192.168.1.168

Remote

Remote Identity Type	Remote WAN IP
Remote Identity Data	60.60.60.2

IKE SA Parameters

Encryption Algorithm	3DES
Authentication Algorithm	SHA-1
Authentication Method	● Pre-shared Key ******** ○ RSA Signature (requires Certificate)

IKE Policy Configuration Help

IKE provides automatic management of the Keys used in IPSec, and is used for "Auto" IPSec VPN policies. This screen is used to create or edit an IKE Policy.

General

This section has general information about this IKE policy.

Policy Name - Enter an appropriate name for the policy. This name is not supplied to the remote VPN Endpoint. It is used to help you manage the IKE policies.

Direction/Type - This setting is used when determining if the IKE policy matches the current traffic. Select the desired option.

- Initiator - Outgoing connections are allowed, but incoming connections will be blocked.
- Responder - Incoming connections are allowed, but outgoing connections will be blocked.
- Both Directions - Both incoming and outgoing connections are allowed.
- Remote Access - This is to allow only incoming client connections, where the IP address of the remote client is unknown. If selected, the "Exchange Mode" MUST be "Aggressive", and the "Identity" (both Local and Remote) MUST be "Name".

This completes the configuration of the NetGear ProSafe VPN Firewall FVS114.

6. Configure the Cisco 3725 Router at the Main Site

This section describes the configuration for the Cisco 3725 router, which resides at Main Site and connects to the network and the NetGear ProSafe VPN Firewall FVX538.

The following steps were followed to configure the Cisco 3725 Router:

1. Configuring the Ethernet interface connected to the NetGear ProSafe VPN Firewall FVX538.
2. Configuring the Ethernet interface connected to the Network.
3. Configuring IP Routes for:
   - IP Office LAN2 Subnet.
   - Default static IP route.

1. *Connect to the Cisco 3725 Router with its serial cable.* Run a terminal emulator, such as HyperTerminal with settings of 9600Kb/s, 8 data bits, 1 stop bit and no parity. Set the flow control to none and change the emulation mode to VT100.

2. *Configure one Ethernet connection for the Network.*

```
DGK-3725>enable
DGK-3725#configure
Configuring from terminal, memory, or network? [terminal] terminal
DGK-3725(config)#interface FastEthernet 0/1
DGK-3725(config-if)#ip address 60.60.60.2 255.255.255.0
```

3. *Configure one Ethernet connection for the Network.*

```
DGK-3725(config)#interface FastEthernet 0/0
DGK-3725(config-if)#ip address 12.160.180.2 255.255.255.0
```

4. *Configure an ip route for the IP Office 412 LAN2 Subnet*

```
DGK-3725(config)#ip route 192.168.3.0 255.255.255.0 60.60.60.2
```

5. *Configure a default ip route to the Network.*

```
DGK-3725(config)#ip route 0.0.0.0 0.0.0.0 12.160.180.1
```

7. Remote Avaya 5620SW IP Telephone

Enter the following to manually configure the Avaya IP telephone:

- Press the "*" at the appropriate time during power up.
- At an idle registered phone, press:
    i. "HOLD"
    ii. A D D R # (2 3 3 7 #).

At the prompts, enter the following data to repeat this configuration:

Prompt	**Data**	**Meaning**
Phone=	192.168.0.101	The IP Telephone's IP Address
CallSv=	192.168.3.32	The IP Office LAN2 IP address
CallSvPort=	1719	The registration port
Router=	192.168.0.1	The LAN IP Address of the NetGear FVS114
Mask=	255.255.255.0	The subnet mask
FileSv=	30.30.30.78	The File Server for IP Telephone firmware updates (typically the IP Office Manager PC)
802.1Q=	Off	Deactivates VLAN/Layer 2 priority tagging
Save Changes	#	OK to accept values (and restart the phone) if necessary.

Alternatively, if the remote device can be configured to use VLAN tagging, the 802.1Q= entry can be set to "On" and the appropriate VLAN tag entered.

8. Verification and Troubleshooting

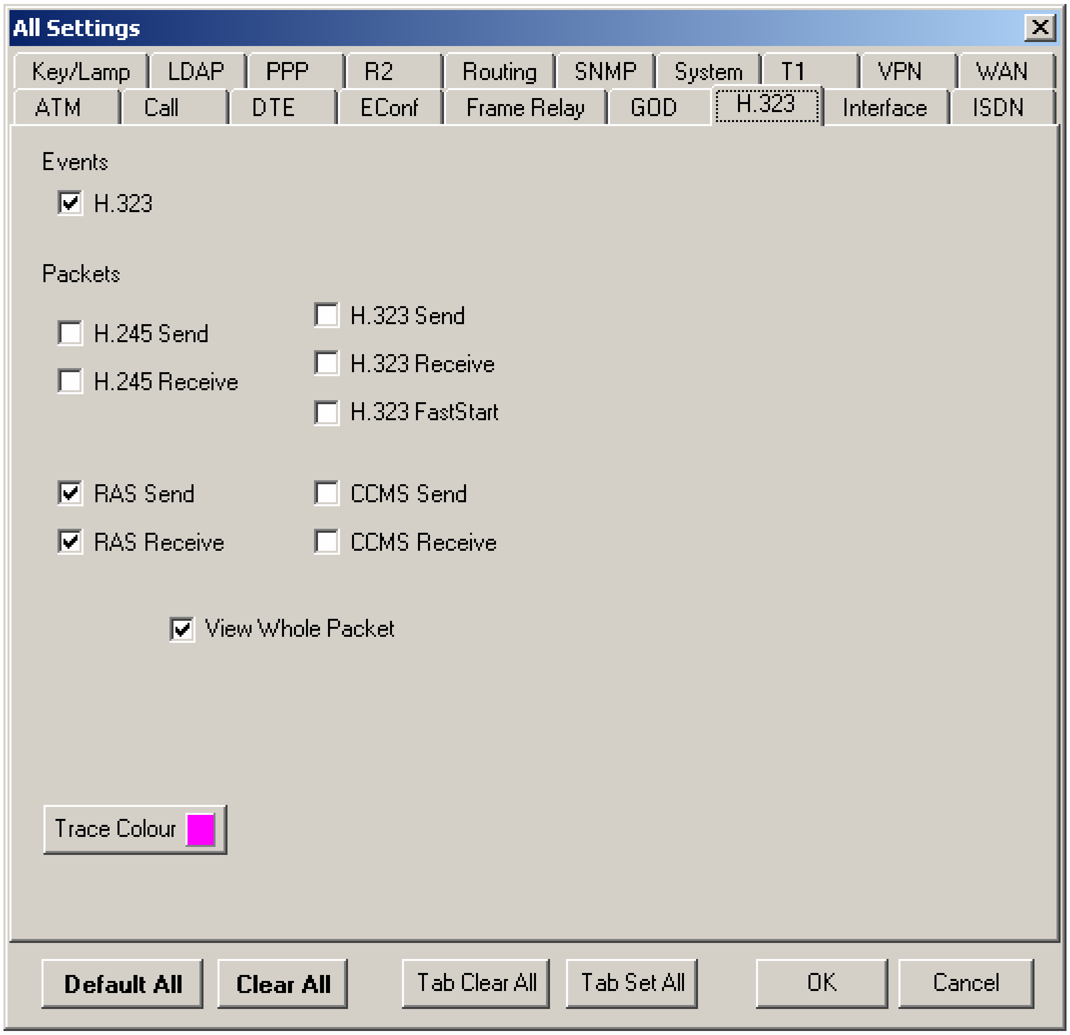
8.1. Phone Troubleshooting

If the Remote Phone displays:	Explanation	Actions
Bad Router	The remote phone cannot "ping" the router.	Verify that the cables are connected and the IP Addressing and appropriate routes have been configured for the IP Addresses.
Discover aaa.bbb.ccc.ddd	This means that the remote phone is not receiving a H.323 gatekeeper confirm response from the aaa.bbb.ccc.ddd IP Address, which must be the IP Office 412 LAN2 IP Address.	• Check that the appropriate IP routes are administered for the Avaya IP Office, the NetGear FVX538 and the Cisco 3725 • Check to see that the VPN Tunnel is up between the sites.
Partial display on IP Phone. No dial tone received when offhook	The phone has successfully completed registration, but subsequent messages (e.g. on/off hook) are blocked.	Ensure that the Application Layer Gateway is disabled on the NetGear FVX538. Telnet to the FVX538 LAN IP Address. Login with the appropriate credentials. Enter the commands as shown in Section 8.4.1. If the **h323** entry shows **Enabled**, follow Step 8 in Section 4.

8.2. Avaya IP Office Troubleshooting

Troubleshooting can be done for the IP Office via the IP Office System Monitor application. Log into the IP Office Monitor PC and select **Start → Programs → IP Office → Monitor** to launch the IP Office System Monitor application. Log into the application using the appropriate credentials.

Select **Trace Options** under the **Filters** Menu. Select the **H.323** tab and configure as illustrated below.



Events

☑ H.323

Packets

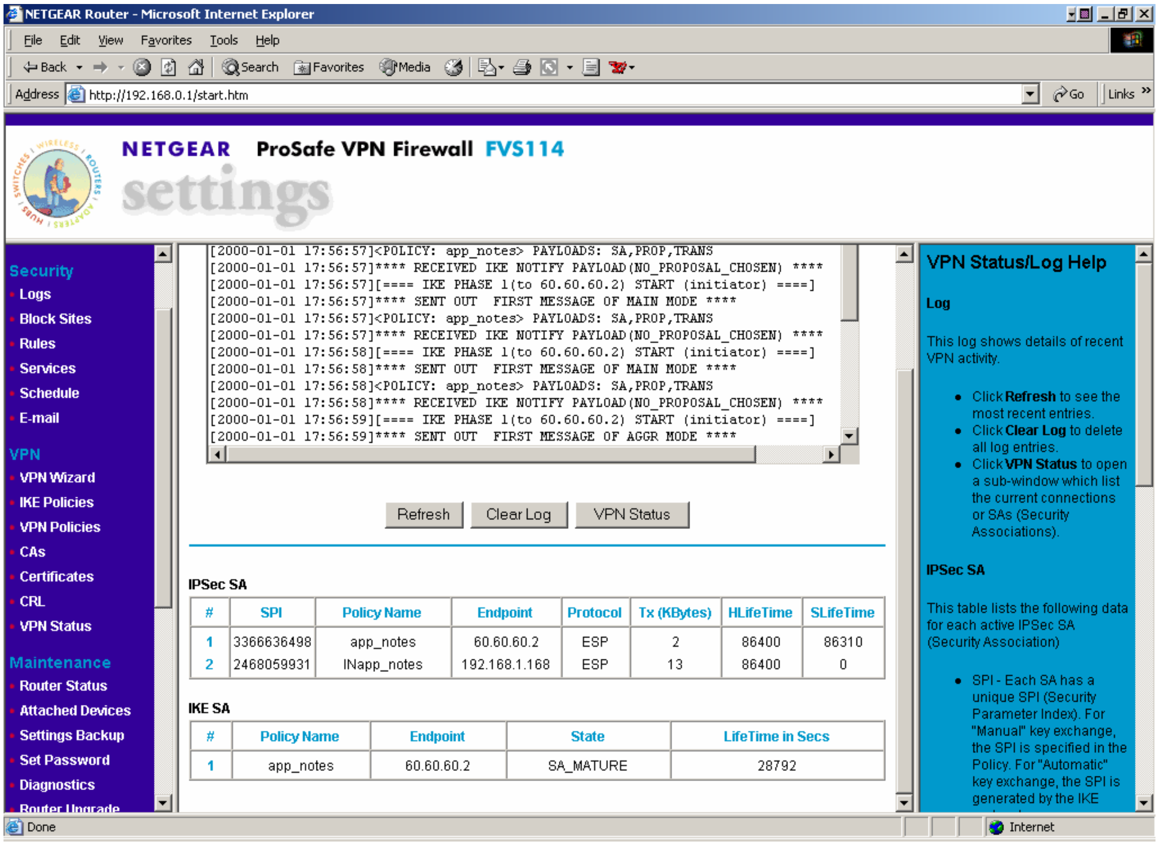
☐ H.245 Send
☐ H.245 Receive
☐ H.323 Send
☐ H.323 Receive
☐ H.323 FastStart
☑ RAS Send
☑ RAS Receive
☐ CCMS Send
☐ CCMS Receive

☑ View Whole Packet

When the system is configured correctly, the trace will show the H.323 Registration messages to and from the remote phone to the IP Office.

8.3. NetGear ProSafe FXS114 VPN Troubleshooting

Select **VPN->VPN Status** to see that the VPN tunnel is operational. The log provides information about the VPN tunnel and will give information about why it is not up (for example a timeout, or policy mismatch).



```
[2000-01-01 17:56:57]<POLICY: app_notes> PAYLOADS: SA,PROP,TRANS
[2000-01-01 17:56:57]**** RECEIVED IKE NOTIFY PAYLOAD(NO_PROPOSAL_CHOSEN) ****
[2000-01-01 17:56:57][==== IKE PHASE 1(to 60.60.60.2) START (initiator) ====]
[2000-01-01 17:56:57]**** SENT OUT  FIRST MESSAGE OF MAIN MODE ****
[2000-01-01 17:56:57]<POLICY: app_notes> PAYLOADS: SA,PROP,TRANS
[2000-01-01 17:56:57]**** RECEIVED IKE NOTIFY PAYLOAD(NO_PROPOSAL_CHOSEN) ****
[2000-01-01 17:56:58][==== IKE PHASE 1(to 60.60.60.2) START (initiator) ====]
[2000-01-01 17:56:58]**** SENT OUT  FIRST MESSAGE OF MAIN MODE ****
[2000-01-01 17:56:58]<POLICY: app_notes> PAYLOADS: SA,PROP,TRANS
[2000-01-01 17:56:58]**** RECEIVED IKE NOTIFY PAYLOAD(NO_PROPOSAL_CHOSEN) ****
[2000-01-01 17:56:59][==== IKE PHASE 1(to 60.60.60.2) START (initiator) ====]
[2000-01-01 17:56:59]**** SENT OUT  FIRST MESSAGE OF AGGR MODE ****
```

IPSec SA

#	SPI	Policy Name	Endpoint	Protocol	Tx (KBytes)	HLifeTime	SLifeTime
1	3366636498	app_notes	60.60.60.2	ESP	2	86400	86310
2	2468059931	INapp_notes	192.168.1.168	ESP	13	86400	0

IKE SA

#	Policy Name	Endpoint	State	LifeTime in Secs
1	app_notes	60.60.60.2	SA_MATURE	28792

VPN Status/Log Help

Log

This log shows details of recent VPN activity.

- Click **Refresh** to see the most recent entries.
- Click **Clear Log** to delete all log entries.
- Click **VPN Status** to open a sub-window which list the current connections or SAs (Security Associations).

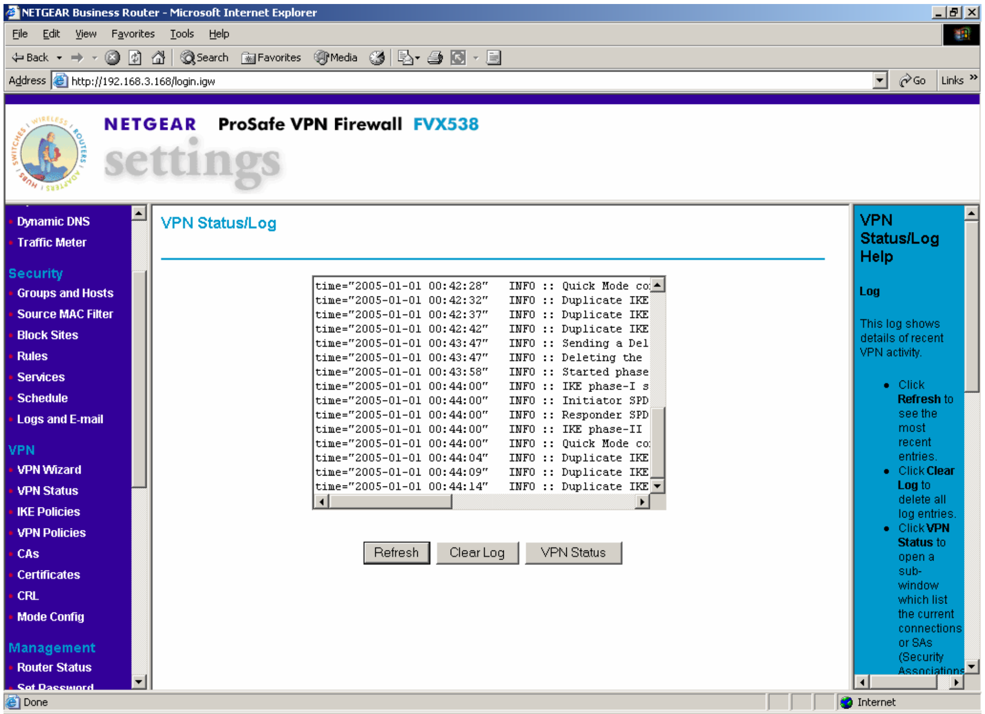
IPSec SA

This table lists the following data for each active IPSec SA (Security Association)

- SPI - Each SA has a unique SPI (Security Parameter Index). For "Manual" key exchange, the SPI is specified in the Policy. For "Automatic" key exchange, the SPI is generated by the IKE

8.4. NetGear ProSafe FVX538 VPN Troubleshooting

Select **VPN->VPN Status** to see VPN information. The log provides information about the VPN tunnel and will give information about the VPN being down (for example a timeout, or policy mismatch).



VPN Status/Log

```
time="2005-01-01 00:42:28"   INFO :: Quick Mode co
time="2005-01-01 00:42:32"   INFO :: Duplicate IKE
time="2005-01-01 00:42:37"   INFO :: Duplicate IKE
time="2005-01-01 00:42:42"   INFO :: Duplicate IKE
time="2005-01-01 00:43:47"   INFO :: Sending a Del
time="2005-01-01 00:43:47"   INFO :: Deleting the
time="2005-01-01 00:43:58"   INFO :: Started phase
time="2005-01-01 00:44:00"   INFO :: IKE phase-I s
time="2005-01-01 00:44:00"   INFO :: Initiator SPD
time="2005-01-01 00:44:00"   INFO :: Responder SPD
time="2005-01-01 00:44:00"   INFO :: IKE phase-II
time="2005-01-01 00:44:00"   INFO :: Quick Mode co
time="2005-01-01 00:44:04"   INFO :: Duplicate IKE
time="2005-01-01 00:44:09"   INFO :: Duplicate IKE
time="2005-01-01 00:44:14"   INFO :: Duplicate IKE
```

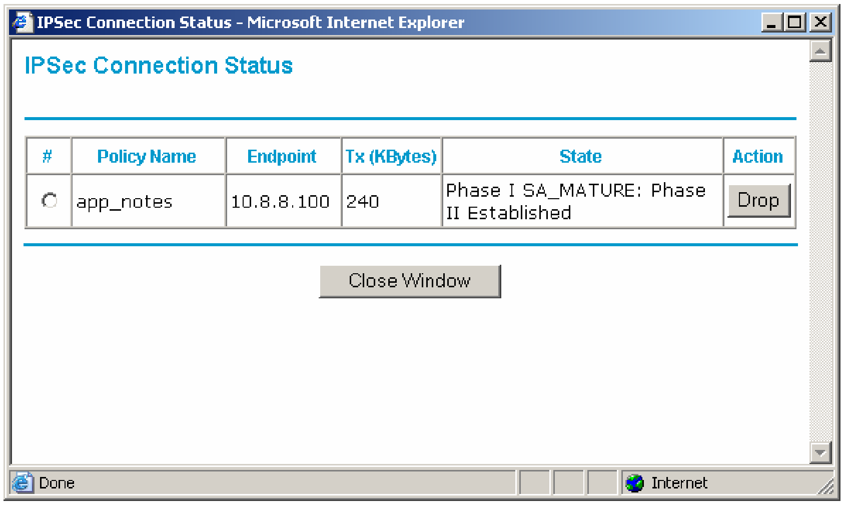
VPN Status/Log Help

Log

This log shows details of recent VPN activity.

- Click **Refresh** to see the most recent entries.
- Click **Clear Log** to delete all log entries.
- Click **VPN Status** to open a sub-window which list the current connections or SAs (Security Associations

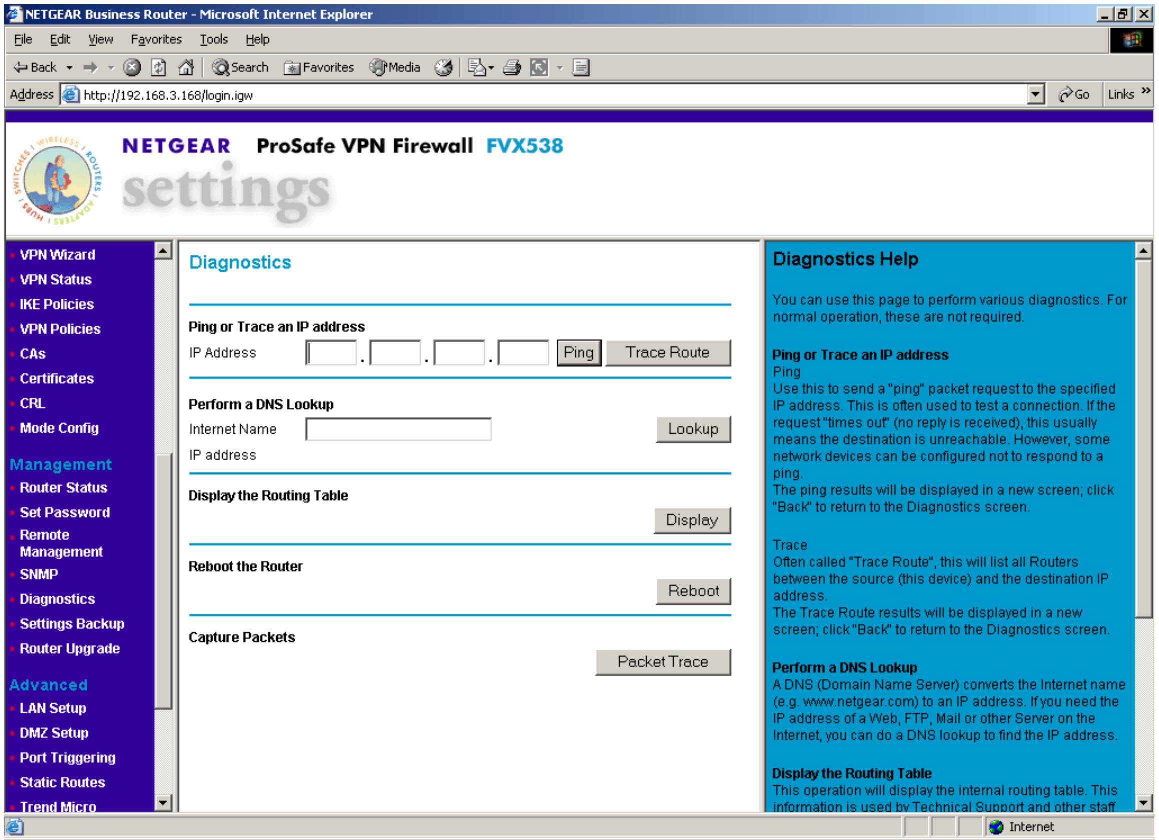
Pressing the **VPN Status** button displays the VPN connection information. The NAT version of the FSV114 WAN IP Address is what will be displayed as the endpoint.



IPSec Connection Status

#	Policy Name	Endpoint	Tx (KBytes)	State	Action
○	app_notes	10.8.8.100	240	Phase I SA_MATURE: Phase II Established	Drop

There is a mechanism to ping different endpoint under **Management->Diagnostics**. The packet trace can also be used to see what packets are on the LAN or WAN interfaces.



Diagnostics

Ping or Trace an IP address

IP Address [ ] . [ ] . [ ] . [ ] Ping Trace Route

Perform a DNS Lookup

Internet Name [ ] Lookup

IP address

Display the Routing Table

Display

Reboot the Router

Reboot

Capture Packets

Packet Trace

Diagnostics Help

You can use this page to perform various diagnostics. For normal operation, these are not required.

Ping or Trace an IP address

Ping

Use this to send a "ping" packet request to the specified IP address. This is often used to test a connection. If the request "times out" (no reply is received), this usually means the destination is unreachable. However, some network devices can be configured not to respond to a ping.

The ping results will be displayed in a new screen; click "Back" to return to the Diagnostics screen.

Trace

Often called "Trace Route", this will list all Routers between the source (this device) and the destination IP address.

The Trace Route results will be displayed in a new screen; click "Back" to return to the Diagnostics screen.

Perform a DNS Lookup

A DNS (Domain Name Server) converts the Internet name (e.g. www.netgear.com) to an IP address. If you need the IP address of a Web, FTP, Mail or other Server on the Internet, you can do a DNS lookup to find the IP address.

Display the Routing Table

This operation will display the internal routing table. This information is used by Technical Support and other staff

8.4.1. Application Layer Gateway Settings

Verify the Application Layer is disabled with the following commands.

```
FVX538: />cd config
FVX538: /config> cd algs
FVX538: /config/algs> show

AlgName                 Status
h323          :          Disabled
tcpsip5061    :          Enabled
tcpsip5620    :          Enabled
msgudp        :          Enabled
```

9. Conclusion

These Application Notes describe the configuration of a remote Avaya IP Telephone served by an Avaya IP Office over a NetGear Virtual Private Network. The configuration was tested successfully.

10. References

1. Product documentation for Avaya IP Office may be found at: http://marketingtools.avaya.com/knowledgebase/.

2. *Application Notes for the Configuring an Avaya G250 Media Gateway as a VPN IKE Responder for a Cisco 877 Access Router and an Avaya G350 Media Gateway* http://devconnect.avaya.com.

3. NetGear product documentation can be found at http://www.netgear.com.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com