Avaya Solution & Interoperability Test Lab

Configuring the NETGEAR FVX538 ProSafe VPN Firewall as an IPSec VPN Head-end to Support the Avaya VPNremote Phone and Avaya Phone Manager Pro with Avaya IP Office – Issue 1.0

Abstract

These Application Notes describe the steps for configuring the NETGEAR FVX538 ProSafe VPN Firewall for Avaya IP Office to support Avaya VPNremote Phone and Phone Manager Pro. This solution can be used for a remote worker who wants to use a multi-button telephone and have the same functionality as a local telephone co-located with the IP Office. The sample configuration presented in these Application Notes utilizes a policy-based IPSec VPN and XAuth enhanced authentication. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab and at the request of the Solutions Marketing Team.

Table of Contents

1. Introduction

These Application Notes describe the steps for configuring the NETGEAR FVX538 ProSafe VPN Firewall for Avaya IP Office to support Avaya VPNremote Phone and Phone Manager Pro. Steps for configuring the NETGEAR FVX538 ProSafe VPN Firewall with a policy-based IPSec VPN and XAuth enhanced authentication to support the Avaya VPNremote Phone and Phone Manager Pro are described in this document.

The solution described in these Application Notes is an integral part of the Unified Communications – Small Business Edition, which provides a remote worker the same functionality as a local worker telephone co-located with the IP Office. The solution specific components are:

- **Avaya VPNremote Phone for remote IP Office user**
- **Avaya Phone Manager Pro (in telecommuter mode)**
- **NETGEAR FVX538 ProSafe VPN Firewall**
- **NETGEAR ProSafe VPN Client**

1.1. Avaya VPNremote Phone for remote IP Office users

The Avaya VPNremote Phone is a software based IPSec Virtual Private Network (VPN) client integrated into the firmware of an Avaya 4600 or 5600 Series IP Telephone. This capability allows the Avaya IP Telephone to be plugged in and used over a secure IPSec VPN from any broadband Internet connection. End users experience the same IP telephony features as if they were using the telephone in the office.

Avaya IP Office 500 supports Avaya IP Telephone models 4610SW, 5610SW, 4620SW, 5620SW, 4621SW and 5621SW with Avaya VPNremote Phone firmware. Any of the above mentioned Avaya IP Telephones can be converted to an Avaya VPNremote Phone, as described in [1], and [2]. For a VPN solution, the IP Office VPN Phone license is required along with the Avaya VPNremote Phone firmware.

1.2. Avaya Phone Manager Pro (in Telecommuter mode)

In this mode, a user running Phone Manager Pro on a PC with a data connection to the IP Office, (via VPN), is able to have calls routed to a telephone number specified when starting Phone Manager. When the user makes a call using Phone Manager, IP Office will call the user's specified telephone number and, when answered, make the outgoing call for the user. Similarly, incoming calls to the user's extension on IP Office are routed to the remote number. The Hot Desk feature of IP Office will be used with Phone Manager Pro. The Phone Manager Pro user will have an internal IP Office extension with a hard phone. While the user is logged in to Phone Manager as a telecommuter, the physical phone is logged off.

The NETGEAR ProSafe VPN client is used by the remote user to securely connect to the corporate IP network for telephony and data access.

1.3. NETGEAR FVX538 ProSafe VPN Firewall

The sample network provided in these Application Notes implements the following features of the NETGEAR FVX538:

- **Policy-Based IPSec VPN**
  The policy-based VPN feature of the NETGEAR FVX538 allows a VPN Tunnel to be directly associated with a security policy as opposed to a route-based VPN being bound to a logical VPN Tunnel interface. Since no network exists beyond a VPN client end-point, policy-based VPN tunnels are a good choice for VPN end-point configurations, such as the Avaya VPNremote Phone and NETGEAR ProSafe VPN Client.
- **XAuth User Authentication**
  The XAuth protocol enables the NETGEAR FVX538 to authenticate the individual users of the VPNremote Phone. The NETGEAR ProSafe VPN Client was configured to use pre-shared key and not XAuth user authentication. The XAuth user authentication is in addition to the IKE IPSec VPN authentication. The IKE and XAuth authentication steps are as follows:

Step 1. **Phase 1 negotiations:** the NETGEAR FVX538 authenticates the Avaya VPNremote Phone by matching the IKE ID and pre-shared key sent by the Avaya VPNremote Phone. If there is a match, the NETGEAR FVX538 XAuth process begins.

Step 2. **XAuth:** the NETGEAR FVX538 XAuth server prompts the Avaya VPNremote Phone for user credentials (username and password).

Step 3. **Phase 2 negotiations:** Once the XAuth user authentication is successful, Phase 2 negotiations begin.

- **XAuth Dynamic IP Address Assignment**
  The XAuth protocol enables the NETGEAR FVX538 appliance to dynamically assign IP addresses from a configured IP Address pool range.

2. Network Topology

The sample network implemented for these Application Notes is shown in **Figure 1.** The corporate IP network location contains the NETGEAR FVX538 functioning as a perimeter security device and VPN head-end. The corporate IP network also has the Avaya IP Office 500 and the Avaya IP Office VoiceMail Pro server.

The Avaya VPNremote Phones are located in the public network and configured to establish an IPSec tunnel to the Public IP address of the NETGEAR FVX538. The NETGEAR FVX538 will assign IP addresses to Avaya VPNremote Phones. The assigned IP addresses, also known as the inner addresses, will be used by Avaya VPNremote Phones when communicating inside the IPSec tunnel and in the private corporate network to Avaya IP Office 500.

The Phone Manager Pro PC is located in the public network and configured to establish an IPSec tunnel to the Public IP address of the NETGEAR FVX538. The NETGEAR ProSafe VPN client is used to securely connect to the corporate IP network for telephony and data access.

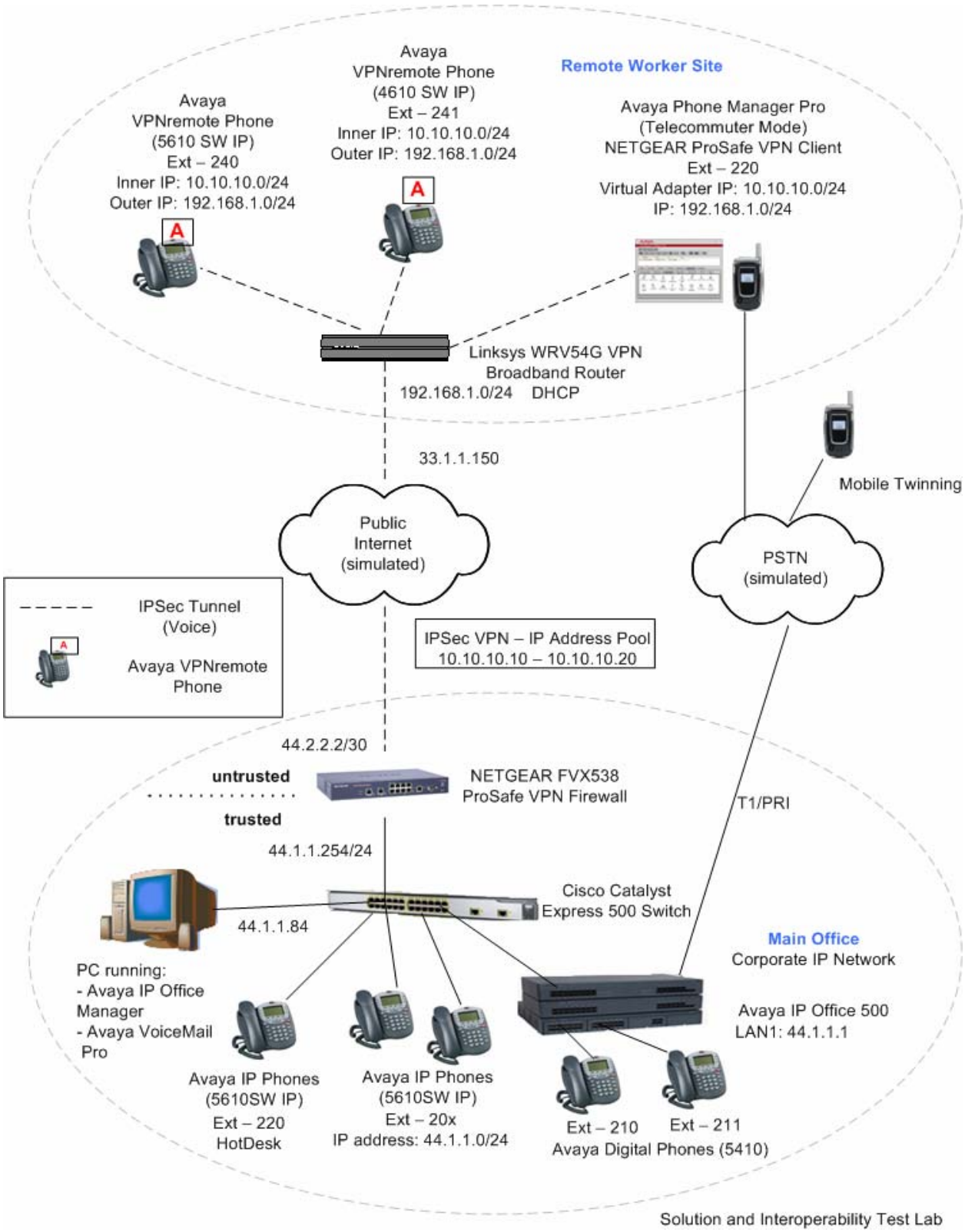


Figure 1: Unified Communications Small Business Edition for Small Office using Avaya IP Office

3. Equipment and Software Validated

The following equipment and software/firmware were used for the sample configuration provided:

Device Description	Versions Tested
Avaya IP Office 500	4.1.9
Avaya IP Office Manager	6.1.9
Avaya IP Office Voicemail Pro	4.1.27
Avaya Phone Manager Pro	4.1.14
Avaya 5410 Digital Telephones	---
Avaya 5610 IP Telephones	i10d01a2824.bin
Avaya VPNremote Phone (4610SW)	a10bVPN23252.bin
Avaya VPNremote Phone (5610SW)	i10bVPN23252.bin
NETGEAR FVX538 ProSafe VPN Firewall	2.1.3-17
NETGEAR ProSafe VPN Client	10.8.0 Build 20
Linksys WRV54G VPN Broadband Router	2.39.2
Cisco Catalyst Express 500 Switch	12.2(25)FY

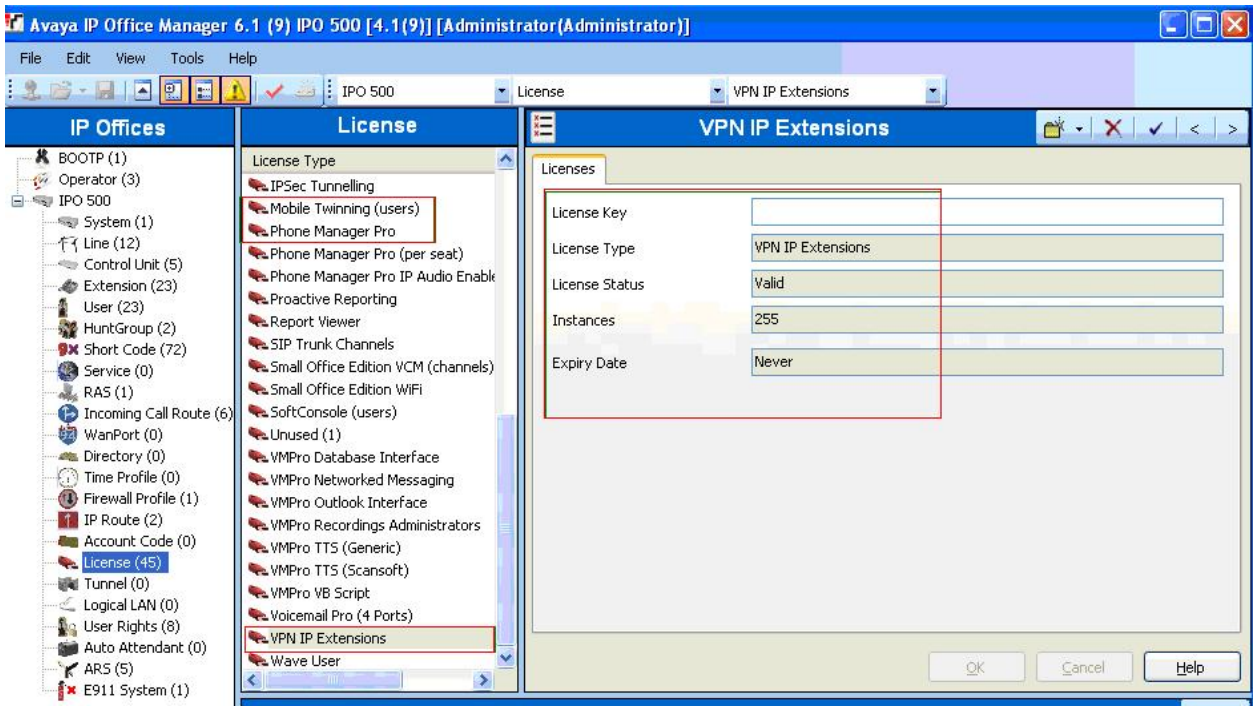
Table 1 – Equipment and Software Validated

4. IP Office Configuration

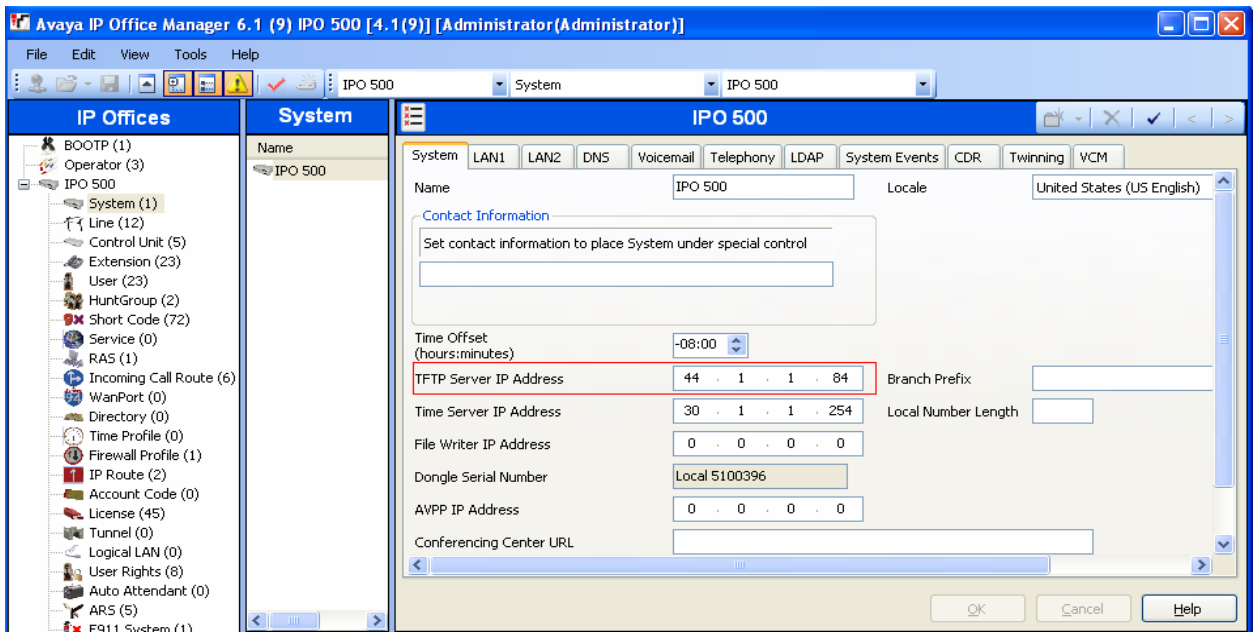
This section describes the IP Office configuration required to support VPNremote Phones and Phone Manager Pro extensions and users. All the commands discussed in this section are executed using the IP Office Manager program. This section assumes that basic configuration on Avaya IP Office has already been completed. For additional information regarding the administration of Avaya IP Office, refer to [3].

Log in to the IP Office Manager PC. Select **Start → Programs → IP Office → Manager** to launch the Manager application. Log in to the Manager application using the appropriate credentials.

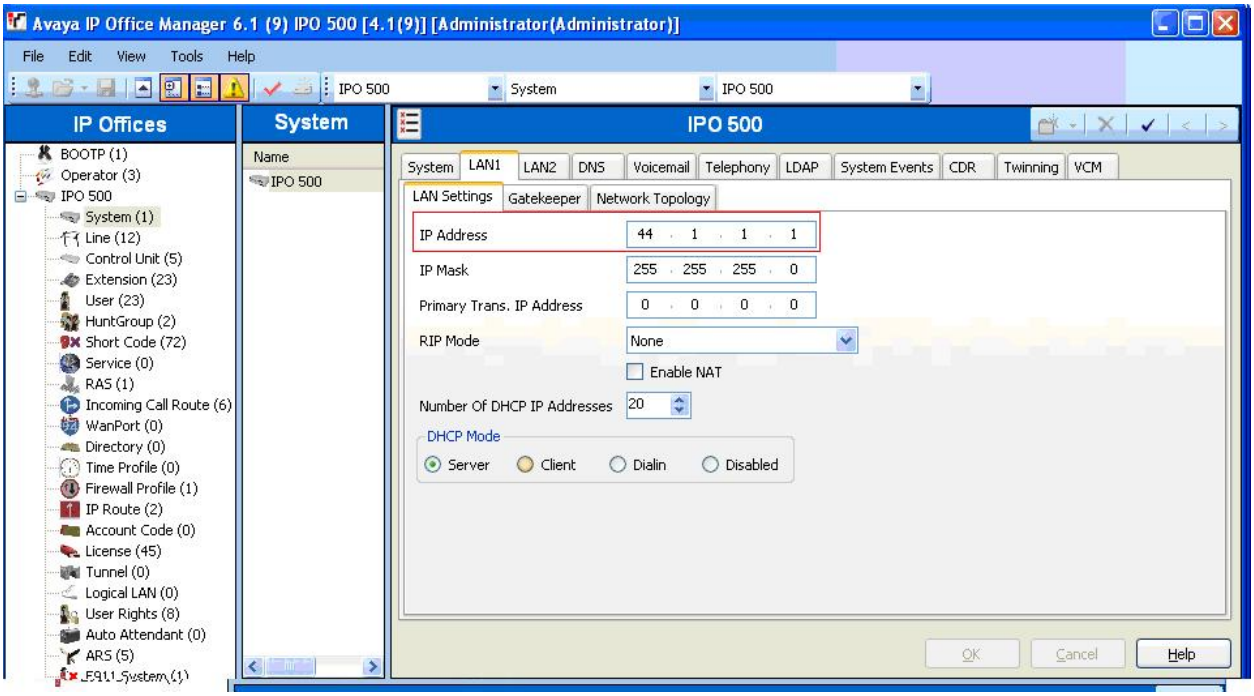
1. *Verify the licenses.* In IP Office Manager, select **License** in the left panel. Verify that IP Office has the correct licenses for **VPN IP Extensions**, **Phone Manager Pro** and **Mobile Twinning (users)**. If not, contact Avaya or an authorized Avaya business partner.



2. *Verify the TFTP Server IP Addresses.* In IP Office Manager, select **System** in the left panel. Double-click on **System**. Verify the **TFTP Server IP Address** in the right hand panel **System** tab.

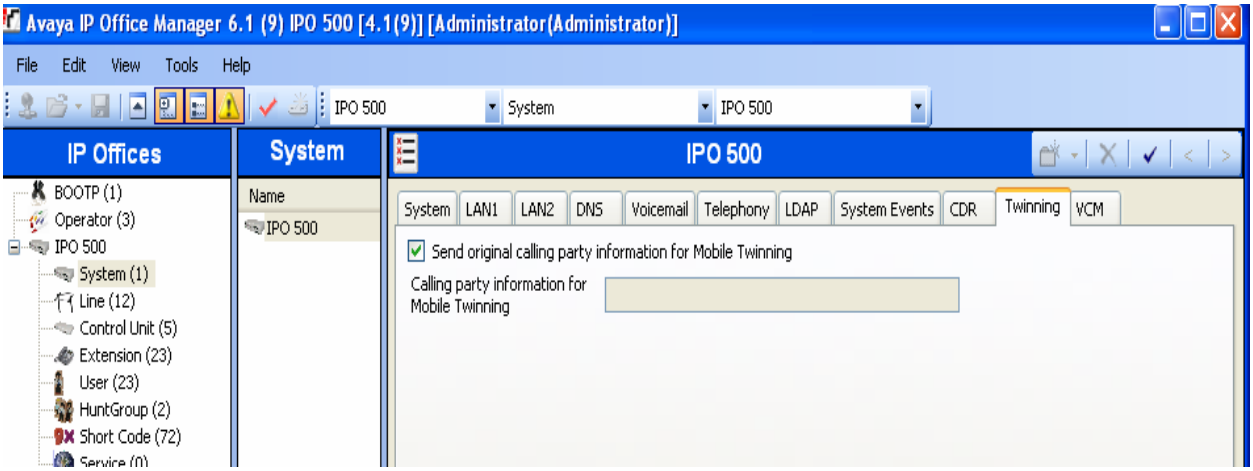


3. *Verify the IP Addresses.* In IP Office Manager, select **System** in the left panel. Double-click on **System**. Verify the **IP Address** in the right hand panel **LAN1 → LAN Settings** tab.



4. *Configure the system level twinning feature.* In IP Office Manager, select **System** in the left panel. Double-click on **System**.

   Select the **Twinning** tab. Enable **Send original calling party information for Mobile Twinning**. Press the **OK** button (not shown).



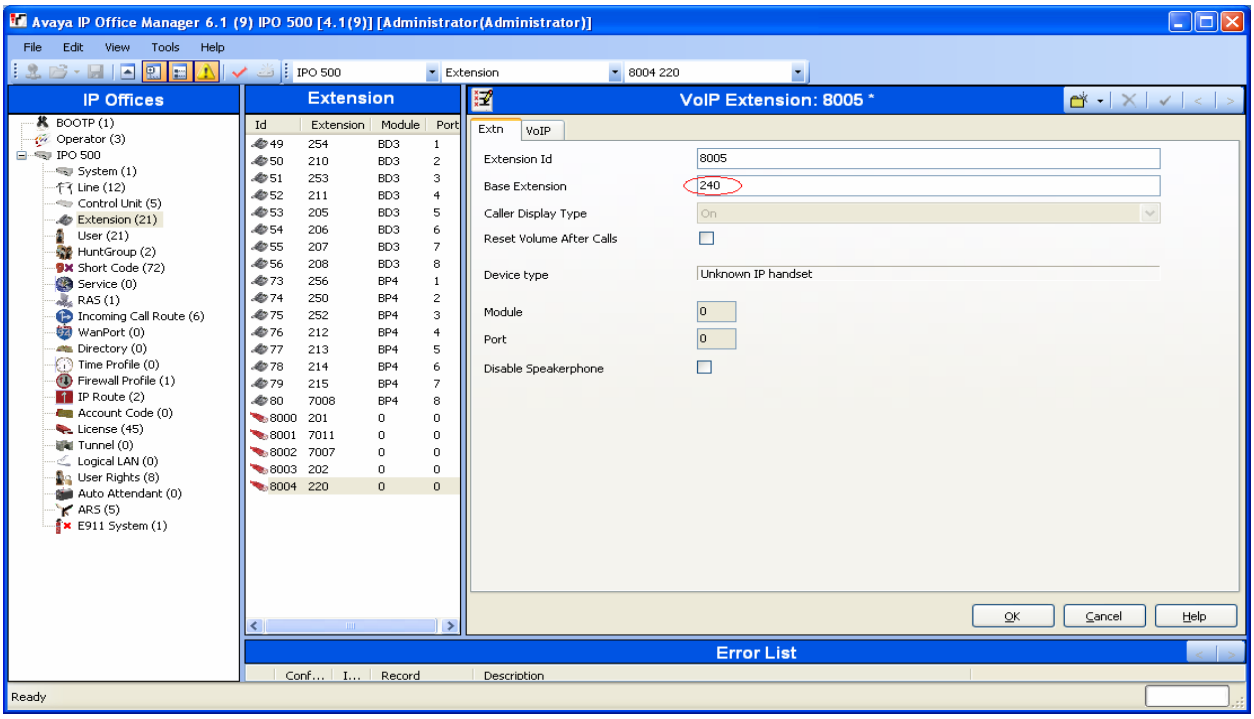
5. *Configure an extension for the VPNremote Phone.* An Avaya VPNremote Phone is administered the same as other Avaya IP telephones within Avaya IP Office. Even though the Avaya VPNremote Phone is physically located outside of the corporate network, the Avaya VPNremote Phone will behave the same as other Avaya IP telephones located on the corporate LAN, once the VPN tunnel has been established.

   In IP Office Manager, select **Extension** in the left panel. In the right panel, click on **Create a New Record** icon  .

   From the pull down menu, select **VoIP Extension**.

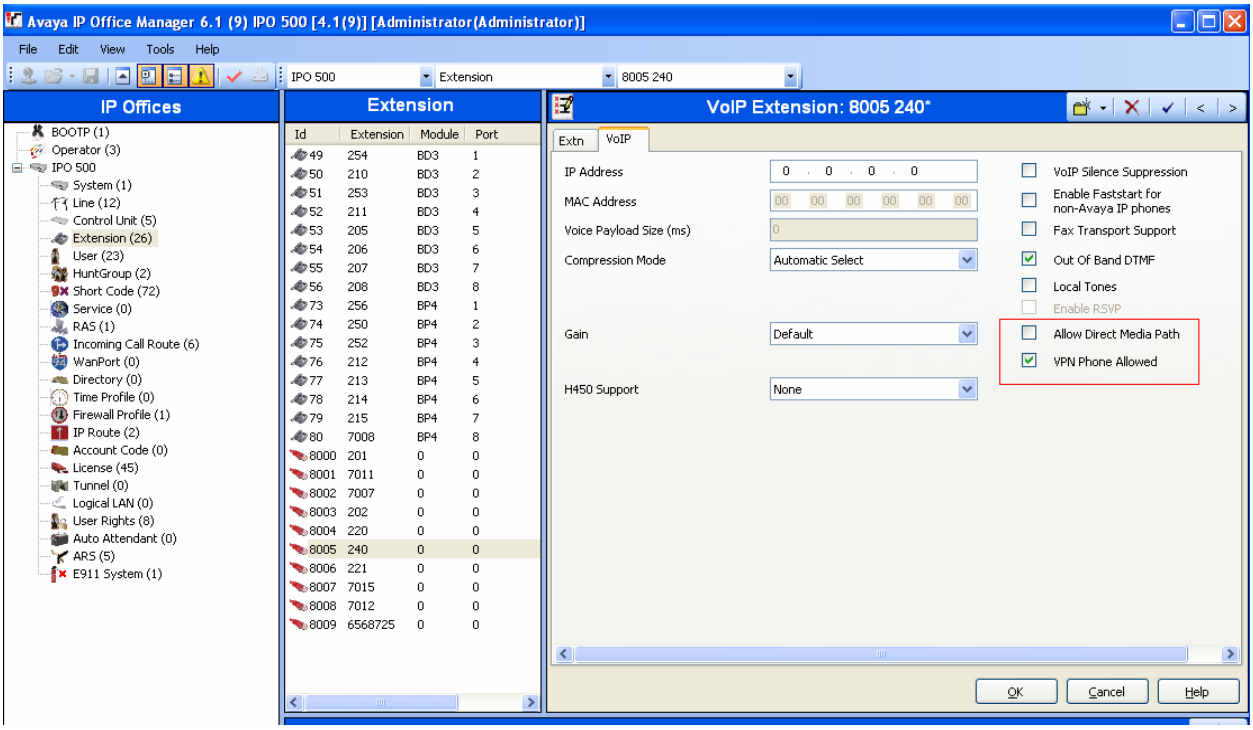
   The VoIP Extension screen will appear in the right panel.

   - Enter a unique **Base Extension** number in the **Extn** tab as shown below.



   In the **VoIP** tab:

   - Enable the **VPN Phone Allowed** option.
   - Un-check the **Allow Direct Media Path** option.
   - Accept default values for all other fields.



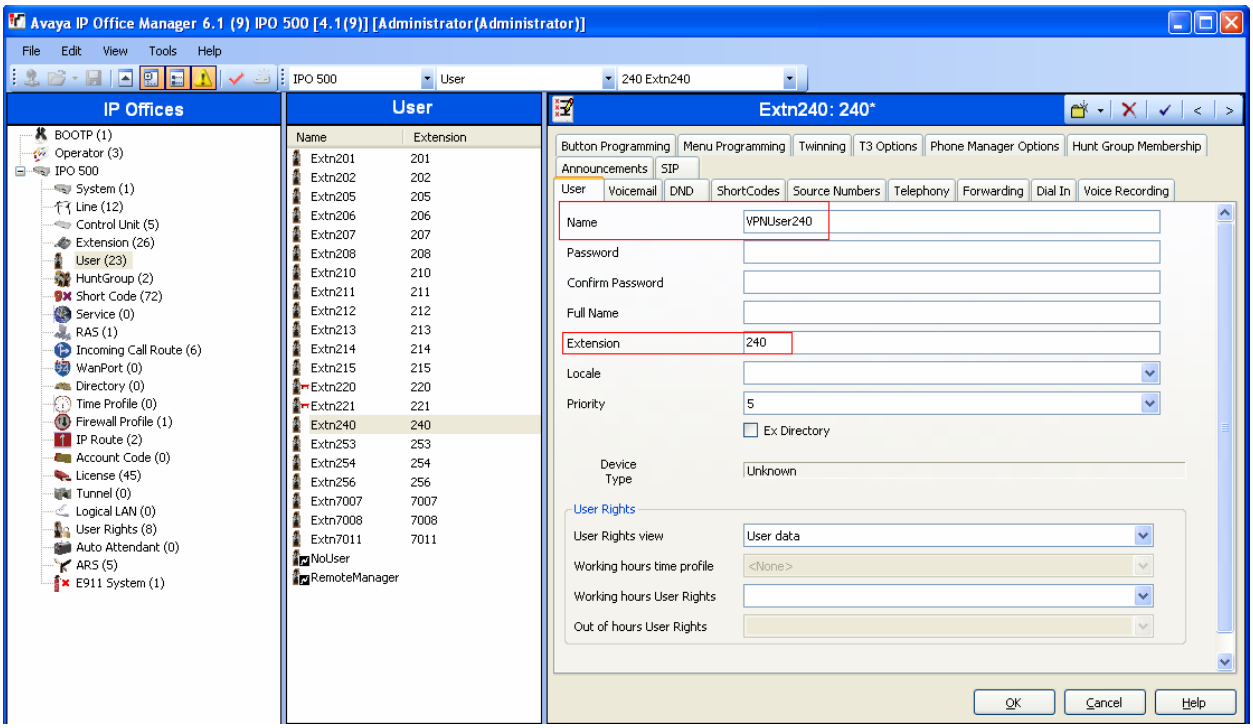
Press the **OK** button.

6. *Configure a user for the VPNremote Phone.* In IP Office Manager, select **User** in the left panel.

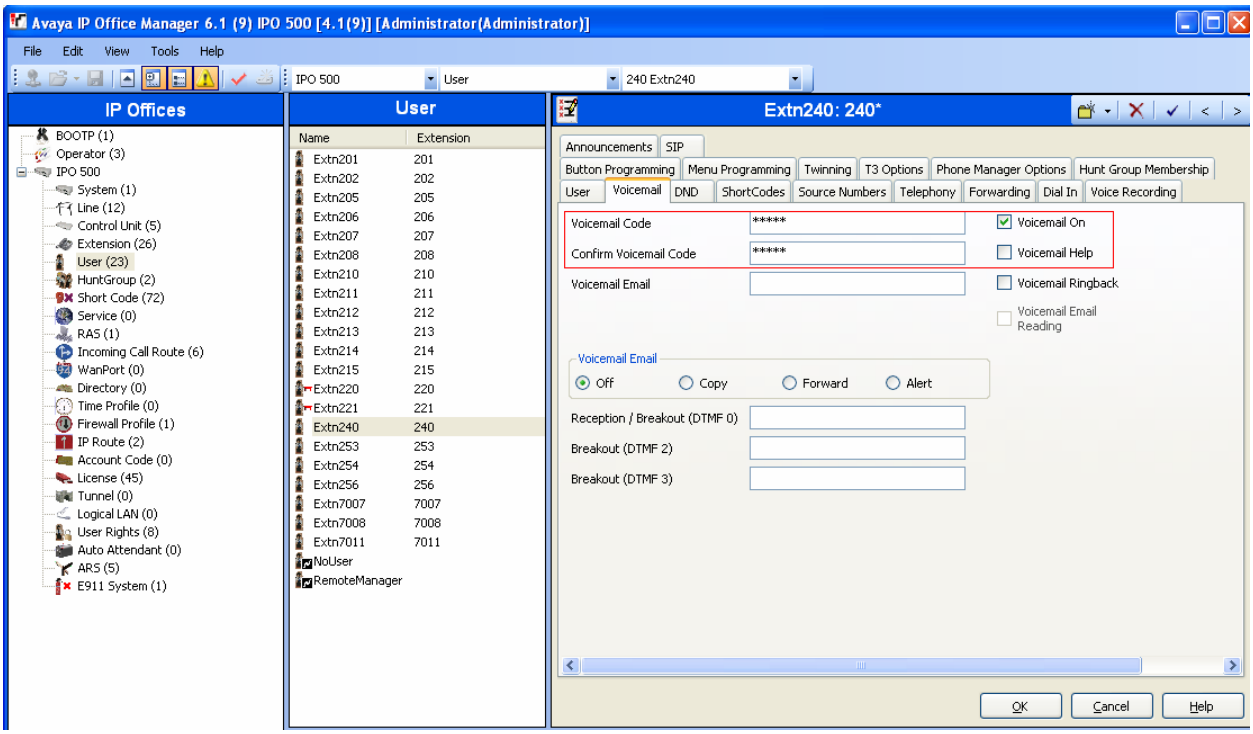
   In the right panel, click on the **Create a New Record** icon  .

   From the pull down menu, select **User**.

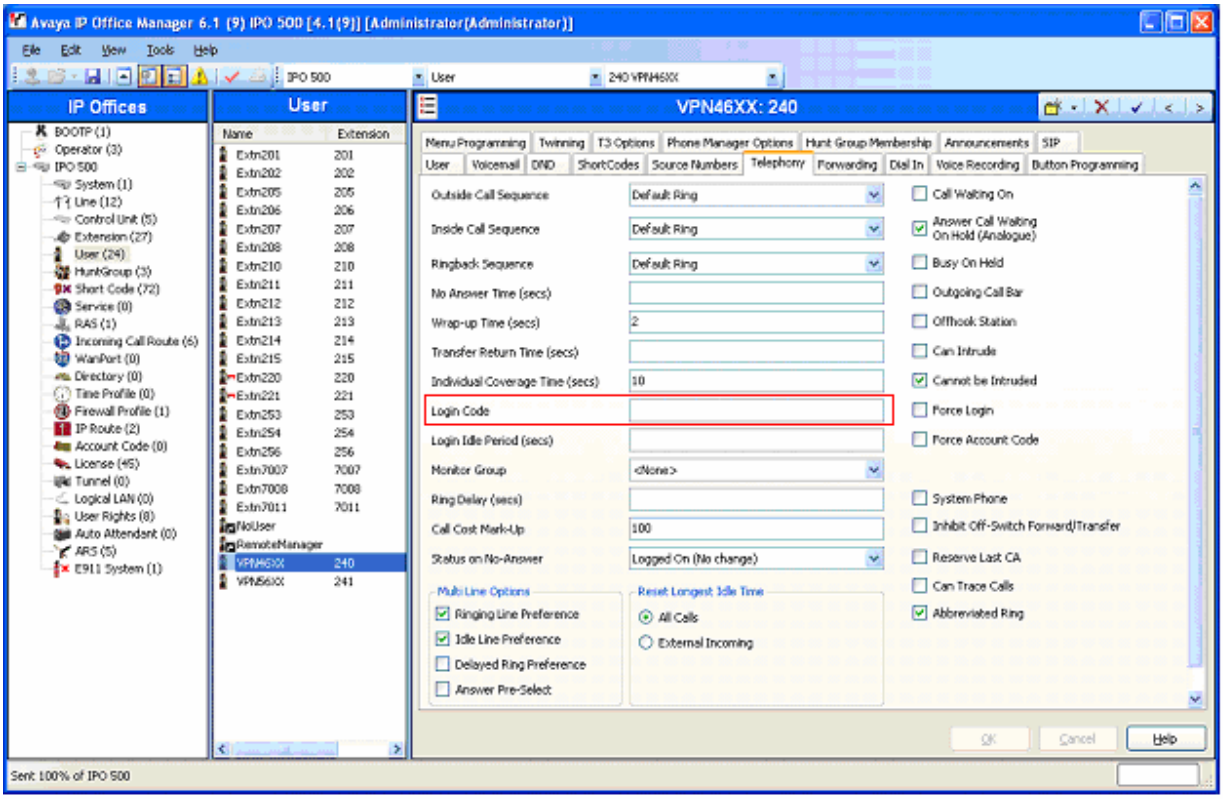
   In the **User** tab, enter a unique **Name** and the **Extension Number** created in **Step 5.**



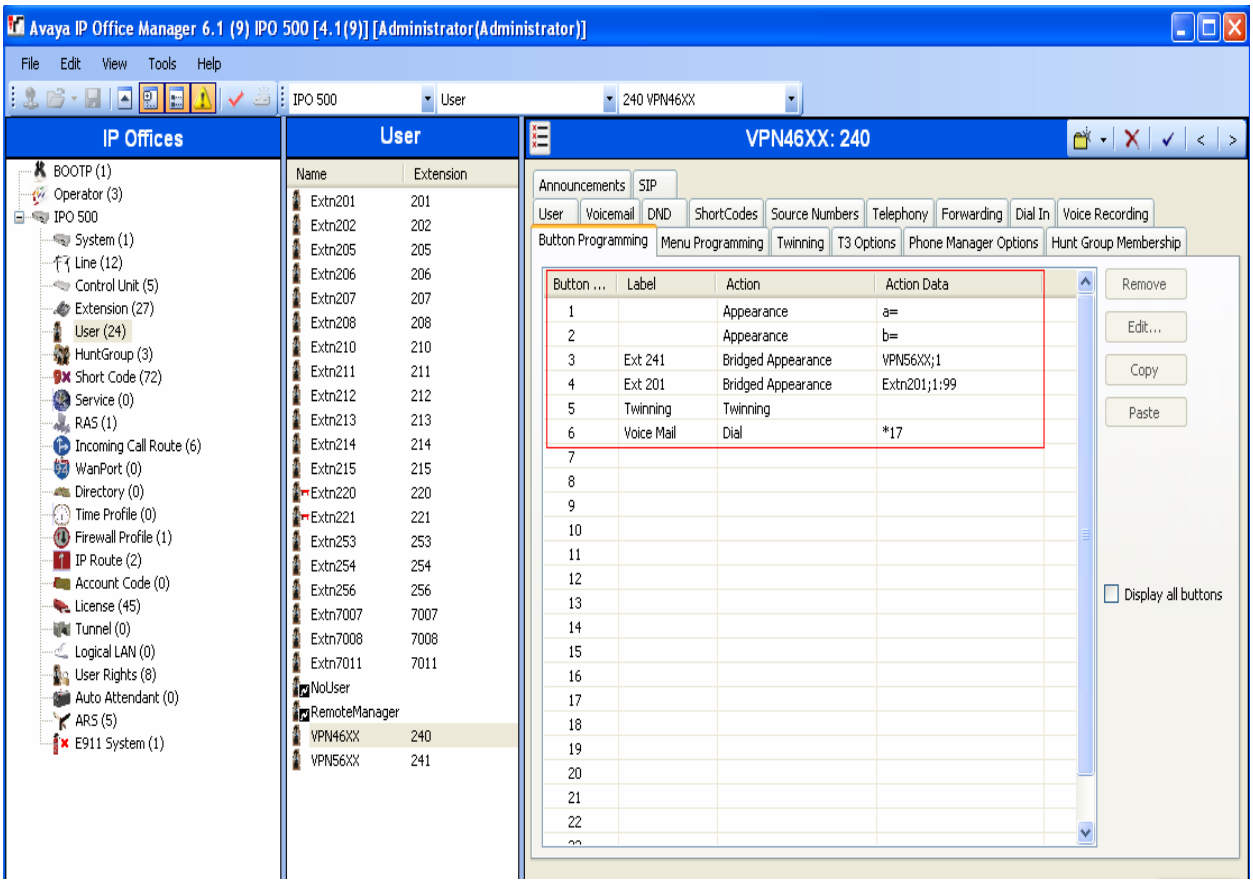
In the **Voicemail** tab, check the **Voicemail On** option and enter the **Voicemail Code**.



In the **Telephony** tab, enter a password if desired in the **Login Code** field. This is the same password that will be used to log in a VPNremote phone in **Step 4** of **Section 6.2** or the Phone Manager Pro user in **Step 2** of **Section 8**.

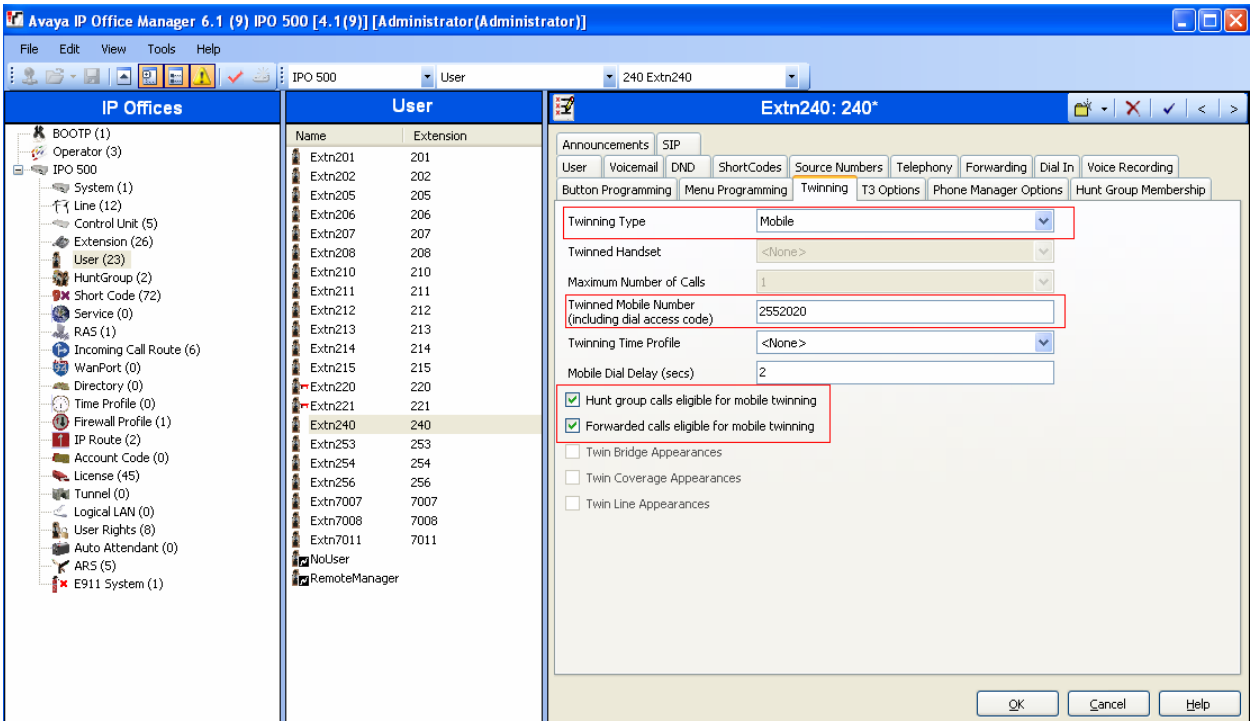


In the **Button Programming** tab, program the buttons as needed. An example is shown below.



In the **Twinning** tab,

- Select **Mobile** for **Twinning Type**.
- Enter the telephone number for **Twinned Mobile Number**.
- Enable the **Hunt group calls eligible for mobile twinning** option.
- Enable the **Forwarded calls eligible for mobile twinning** option.



Press the **OK** button.

7. *Configure an extension that will be used by the IP Office telephone at the Main Office and Phone Manager Pro.* A Phone Manager Pro extension is administered the same as other Avaya IP telephones within Avaya IP Office.

   In IP Office Manager, select **Extension** in the left panel. In the right panel, click on **Create a New Record** icon  .

   From the pull down menu, select **VoIP Extension**. The **VoIP Extension** screen will appear in the right panel, as shown in **Step 5**.
   - Enter a unique **Base Extension** number in the **Extn** tab.

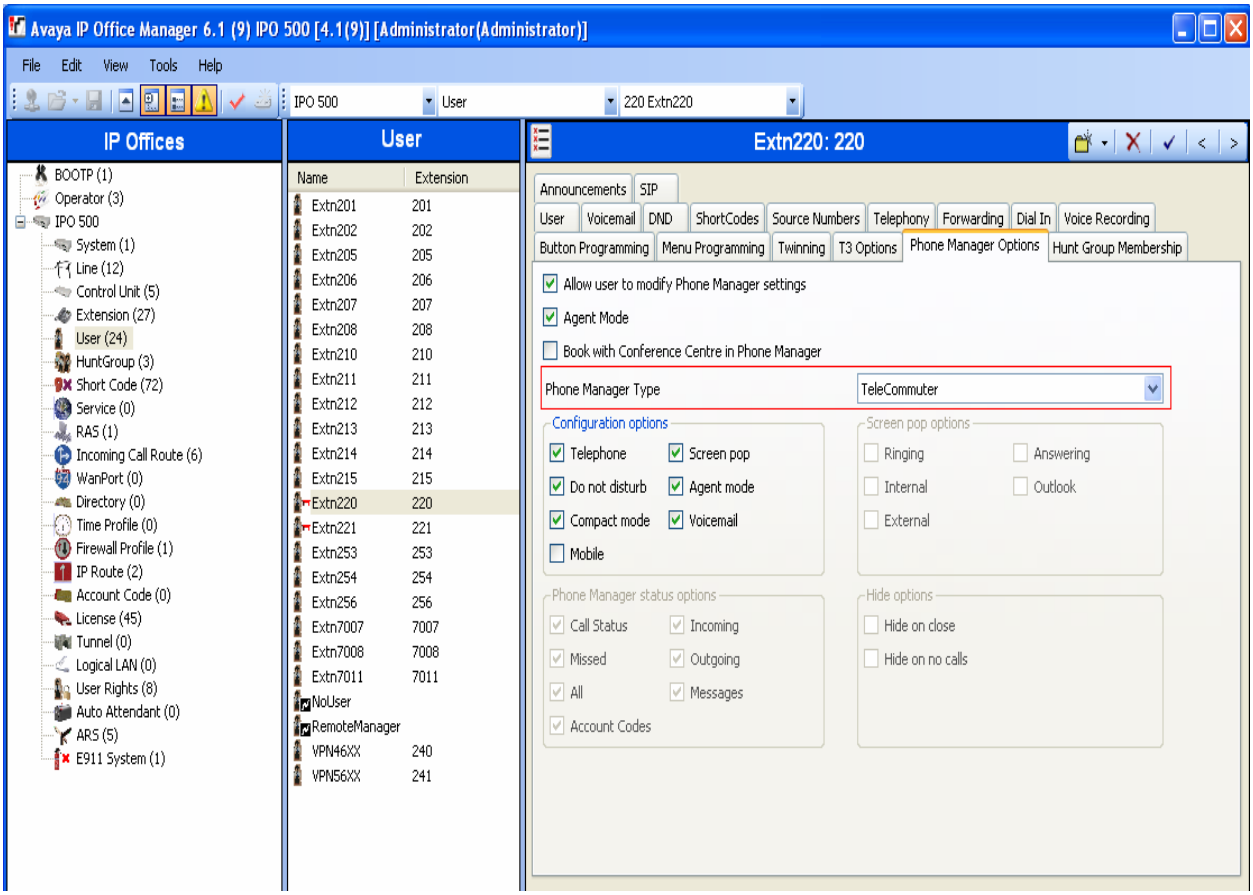
   In the **VoIP** tab:
   - Accept the default values.

   Press the **OK** button.

8. *Configure a user that will be used by the IP Office telephone at the Main Office and Phone Manager Pro.* In IP Office Manager, select **User** in the left panel. In the right panel, click on the **Create a New Record** icon  .
From the pull down menu, select **User**.

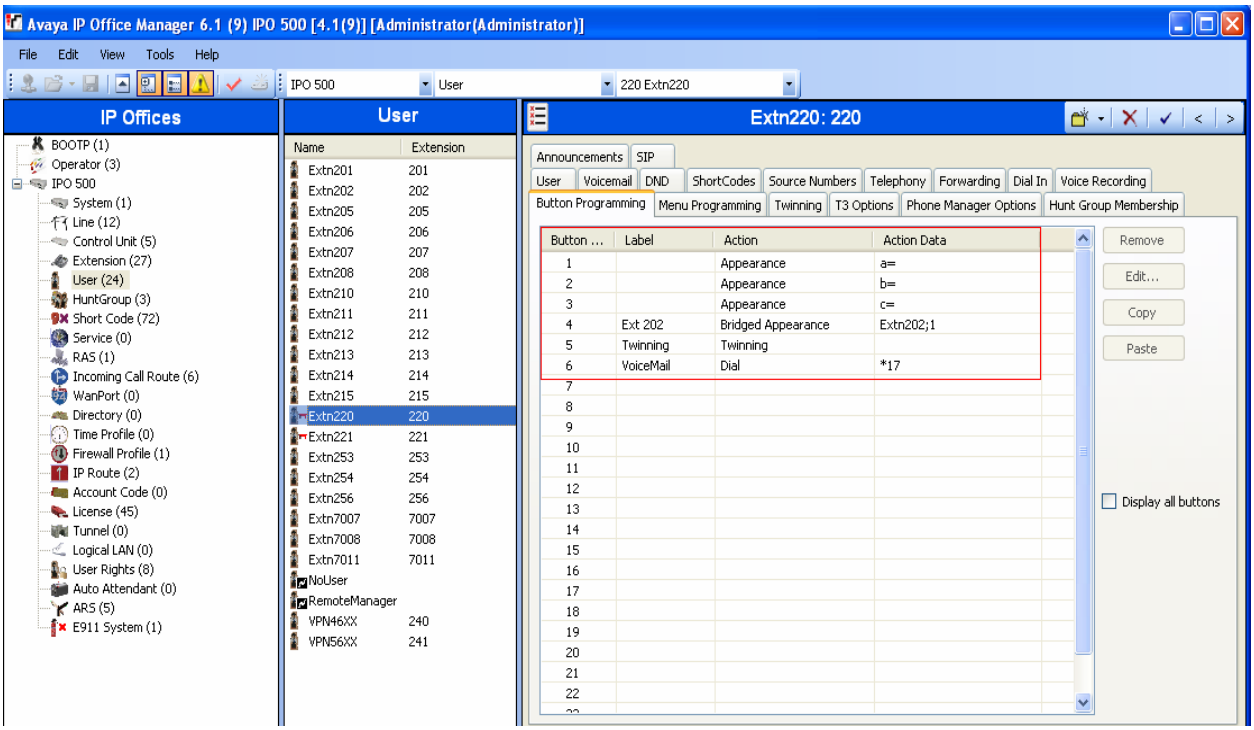
In the **User** tab, enter a unique **Name** and the **Extension Number** created in **Step 7**.

In the **Phone Manager Options** tab, select the **Phone Manager Type** as **Telecommuter**.



Follow the same steps as described in **Step 6** for the **Voicemail** and **Twinning** tabs.

In the **Button Programming** tab, program the buttons as needed. An example is shown below.



Note: The Users configured with Phone Manager Telecommuter option will have  in the left panel next to the User Name. This denotes a Hot Desk user. The Phone Manager User has an internal IP Office extension. While logged in to Phone Manager as a telecommuter, the internal IP Office extension is logged off. The internal IP Office extension is logged in automatically after the user exits Phone Manager.

9. *Save the configuration.* In IP Office Manager, use the  icon to save the configuration and load the saved configuration on the IP Office.

5. NETGEAR FVX538 Configuration

5.1. VPN

Setting up the VPN tunnel encryption and authentication is a two-phase process.

- Phase 1 covers how the Avaya VPNremote Phone and NETGEAR ProSafe VPN Client will securely negotiate and handle the building of the tunnel with the NETGEAR FVX538.
- Phase 2 sets up how the data passing through the tunnel will be encrypted at one end and decrypted at the other. This process is carried out on both sides of the tunnel.

Table 1 provides the IKE Proposals used in the sample configuration for the Avaya VPNremote Phones.

Phase	Encryption/ Authentication Method	Diffie-Hellman Group	Encryption Algorithm	Hash Algorithm	Life Time (sec)
[redacted]					
P1	Pre-Shared Key	2	3DES	SHA-1	432000
P2	ESP	2	3DES	SHA-1	432000

Table 2 – Avaya VPNremote Phones IKE P1/P2 Proposals

Table 2 provides the IKE Proposals used in the sample configuration for the NETGEAR ProSafe VPN Client.

Phase	Encryption/ Authentication Method	Diffie-Hellman Group	Encryption Algorithm	Hash Algorithm	Life Time (sec)
[redacted]					
P1	Pre-Shared Key	2	3DES	SHA-1	28800
P2	ESP	2	3DES	SHA-1	3600

Table 3 – NETGEAR ProSafe VPN Client IKE P1/P2 Proposals

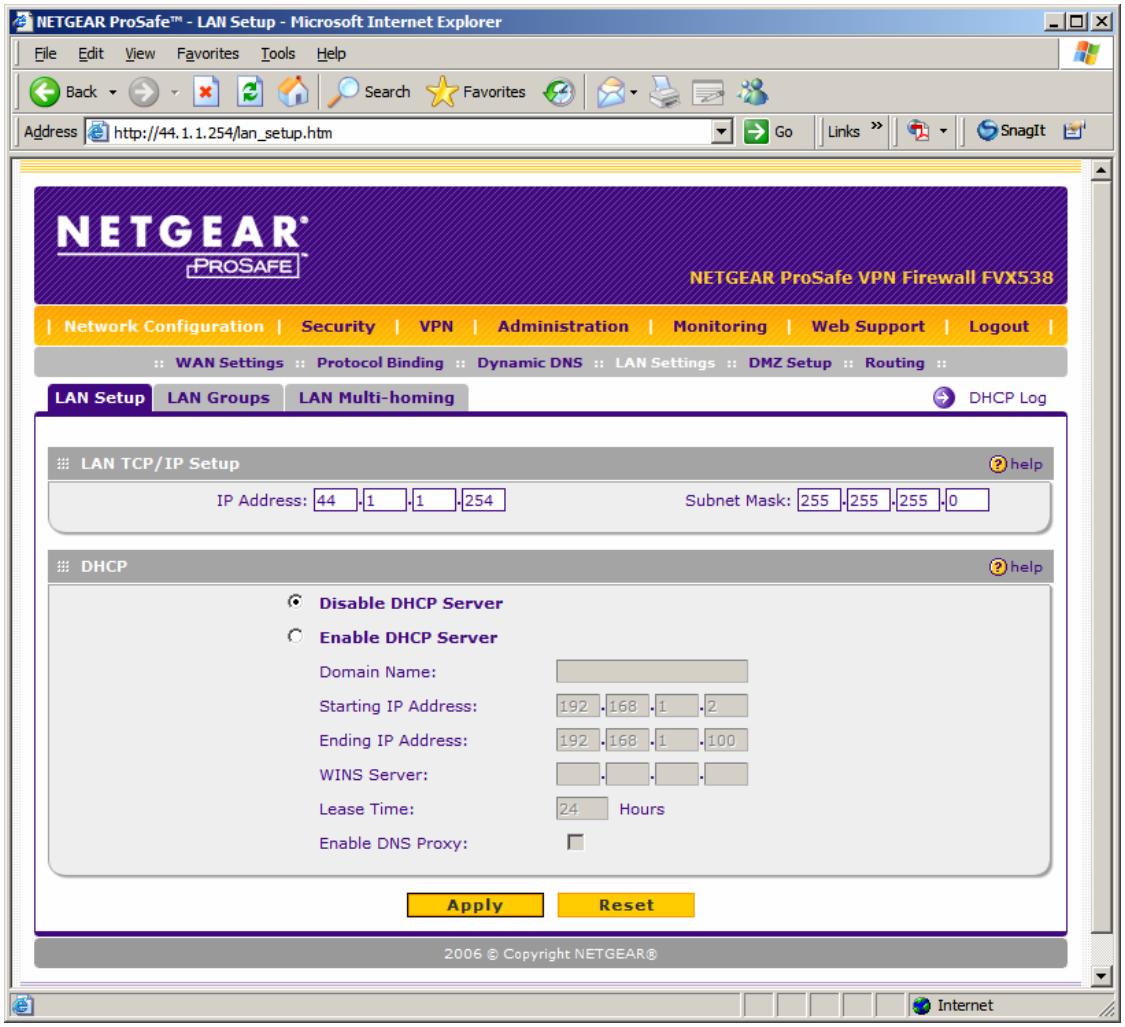
5.2. Access NETGEAR FVX538

1. From a web browser, enter http://<IP address of the NETGEAR FVX538>, the IP address of the local interface of the NETGEAR FVX538. Log in using the appropriate credentials.

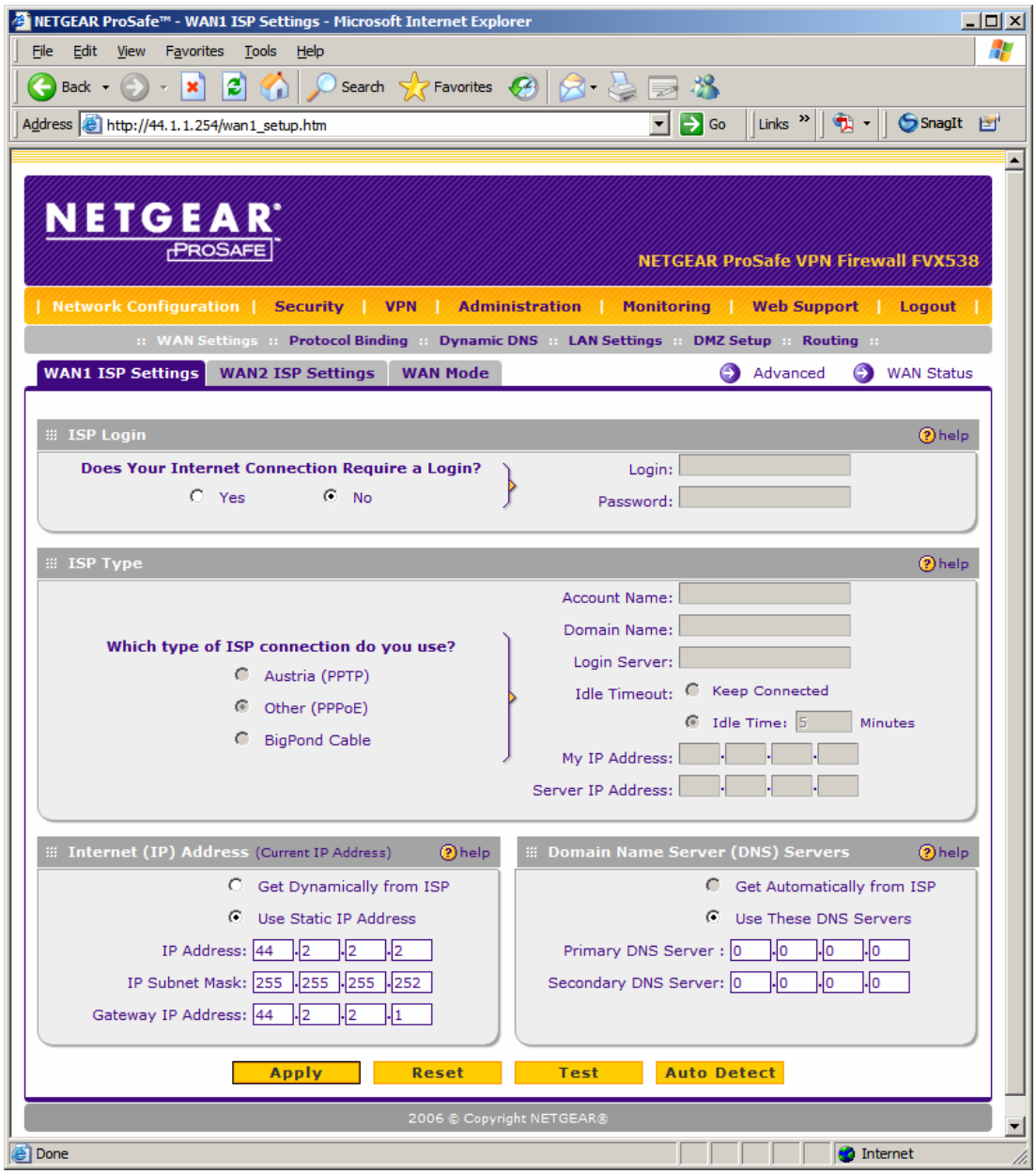
5.3. Configure NETGEAR FVX538 Ethernet Interfaces

The steps below configure the IP addresses of the local and WAN Ethernet interfaces for the configuration shown in **Figure 1**. The Avaya VPNremote Phone and the NETGEAR ProSafe VPN Client will use the IP address of the WAN Ethernet interface to establish an IPSec Tunnel.

1. *Configure IP address of the LAN interface*. Select **Network Configuration → LAN Settings → LAN Setup** from the top menu bar. Assign IP address **44.1.1.254** with a subnet mask of **255.255.255.0** for the LAN interface of the NETGEAR FVX538. Disable the DHCP Server.



2. *Configure the IP address of the WAN interface*. Select **Network Configuration → WAN1 ISP Settings** from the top menu bar. Assign IP address **44.2.2.2** with a subnet mask of **255.255.255.252** for the WAN interface of the NETGEAR FVX538.

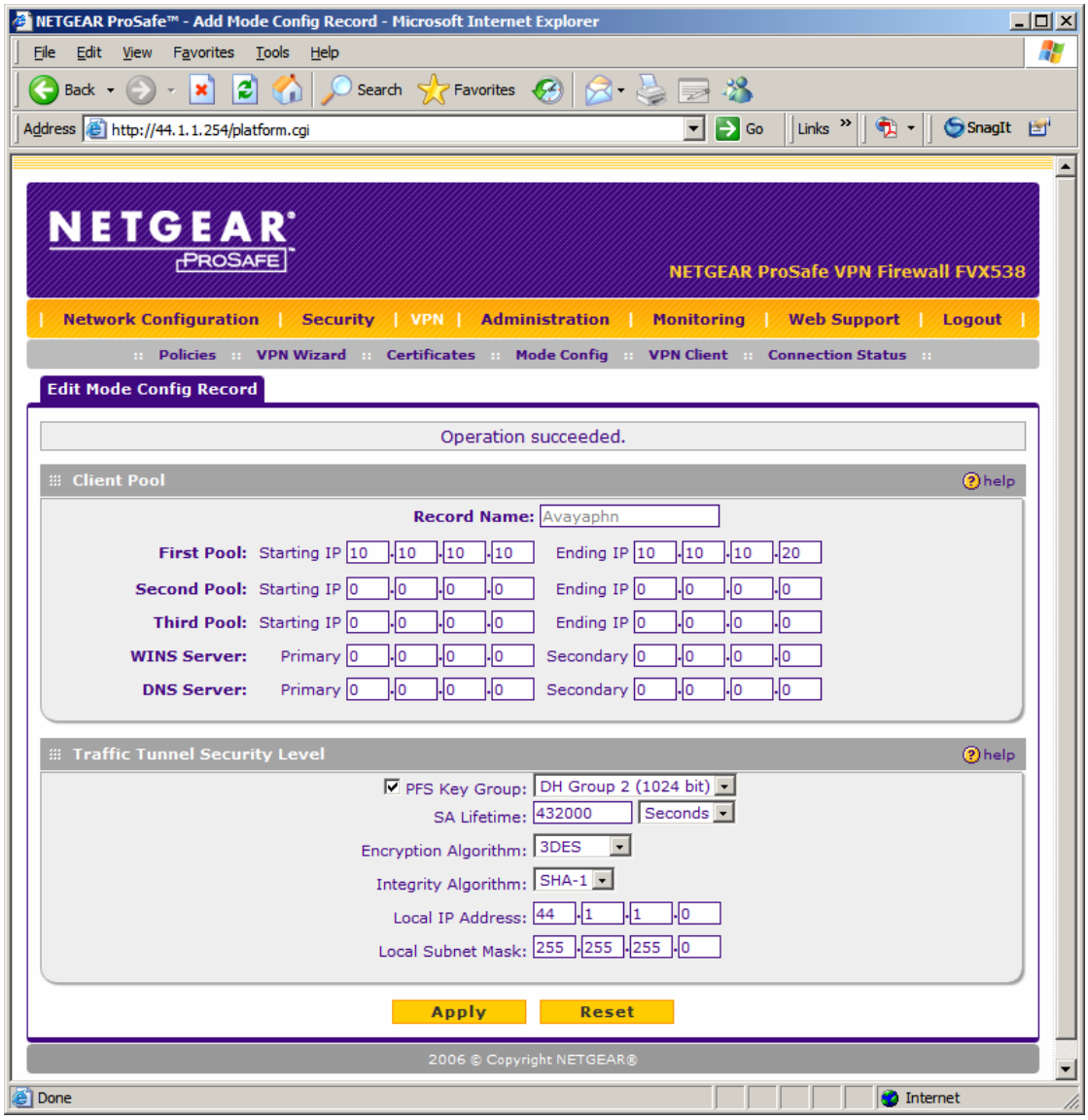


5.4. Mode Config Record

The Mode Config record is used to define the pool of IP addresses that will be used by the Avaya VPNremote Phone as well as the authentication and encryption method to use for tunnel traffic by the NETGEAR FVX538. Select **VPN → Mode Config** from the top menu bar to create a Mode Config record.

Enter the following information:

- **Record Name**: Enter a name (e.g., **Avayaphn**) for the Mode Config record.
- **First Pool**: Enter the range of IP addresses for the pool.
- **PFS Key Group**: Select the hashing algorithm.
- **SA Lifetime**: Enter the time in seconds for Phase 2 renegotiation. Avaya recommends setting this value to **432000** seconds or 5 days.
- **Encryption Algorithm**: Select the encryption algorithm for the tunnel.
- **Integrity Algorithm**: Select the integrity algorithm for the tunnel.
- **Local IP Address**: Enter the subnet of the IP Office located in the private or trusted side.
- **Local Subnet Mask**: Enter the subnet mask of the IP Office located in the private or trusted side.



5.5. IKE Policy

Create an IKE policy for phase 1 negotiation by selecting **VPN → Policies → IKE Policies** from the top menu bar. Enter the following information:

Mode Config Record

- **Do you want to use Mode Config Record?**: Select **Yes**.
- **Select Mode Config Record**: Select the Mode Config record (e.g., **Avayaphn**) created in **Step 5.4**.

General

- **Policy Name**: Enter a name for the IKE policy.
- **Exchange Mode**: Select **Aggressive**.

Local

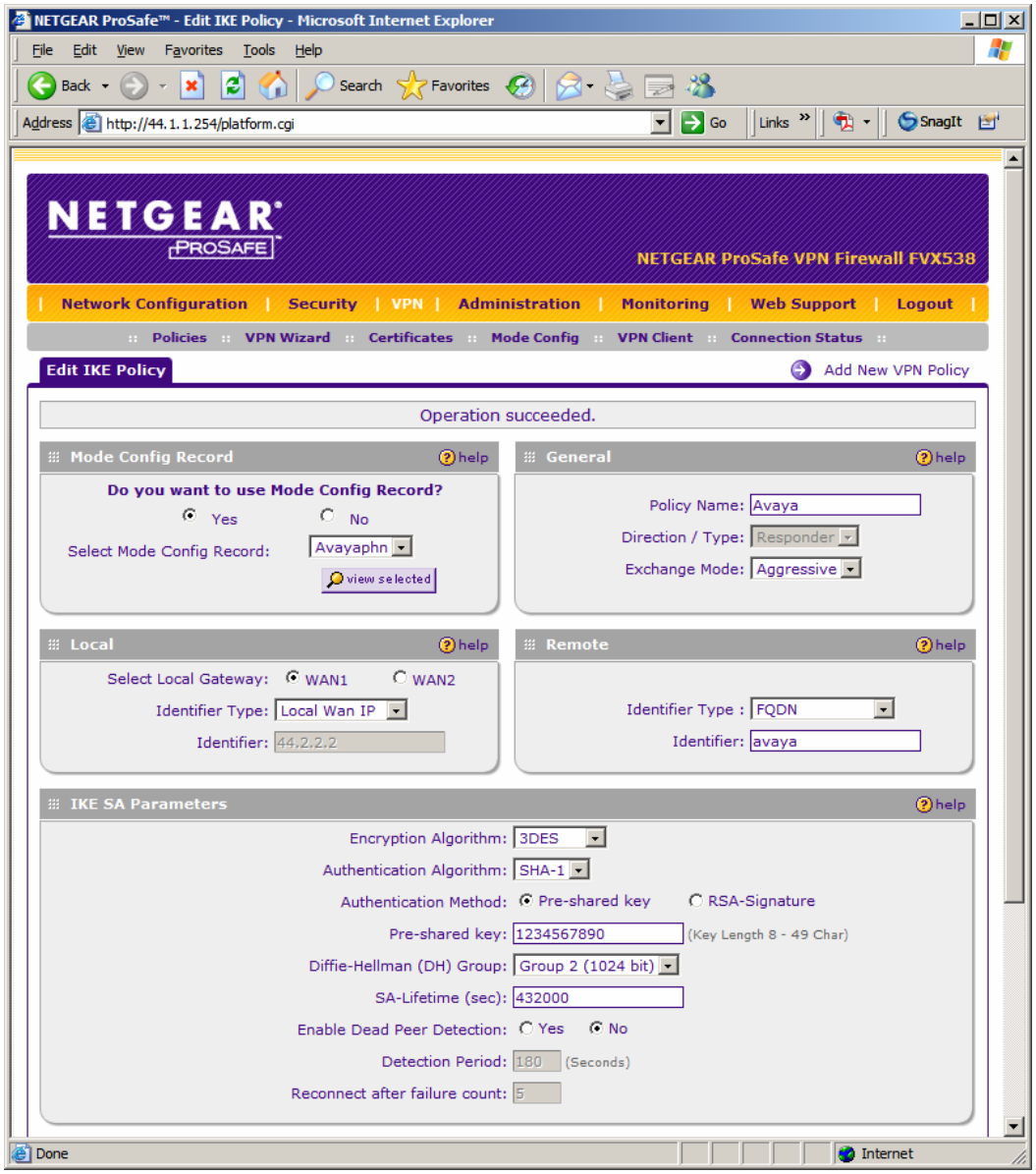
- **Select Local Gateway**: Select **WAN1**.
- **Identifier Type**: Select **Local Wan IP**.

Remote

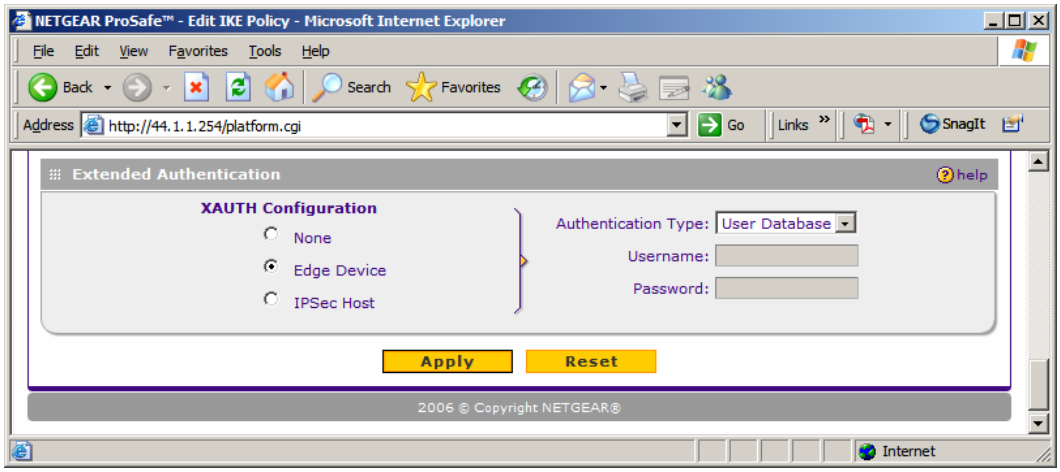
- **Identifier Type**: Select **FQDN**.
- **Identifier**: Enter the "Group Name" that will be used by the Avaya VPNremote phone to establish the VPN tunnel in **Step 3** of **Section 6.2**.

IKE SA Parameters

- **Encryption Algorithm**: Select the encryption algorithm.
- **Authentication Algorithm**: Select the authentication algorithm.
- **Authentication Method**: Select **Pre-shared key**.
- **Pre-shared key**: Enter the "Group PSK" that will be used by the Avaya VPNremote phone in **Step 3** of **Section 6.2**.
- **Diffie-Hellman (DH) Group**: Select the DH Group.
- **SA-Lifetime (sec)**: Enter the time in seconds for Phase 2 renegotiation. Avaya recommends setting this value to **432000** seconds or 5 days.
- **Enable Dead Peer Detection**: Select **No**.
- **XAUTH Configuration**: Select **Edge Device**.
- **Authentication Type**: Select **User Database**. The VPN clients stored in the user database of the NETGEAR FVX538 will be used for authentication. The VPN clients will be defined in **Step 5.6**.



The bottom half of the IKE policy screen is shown below.

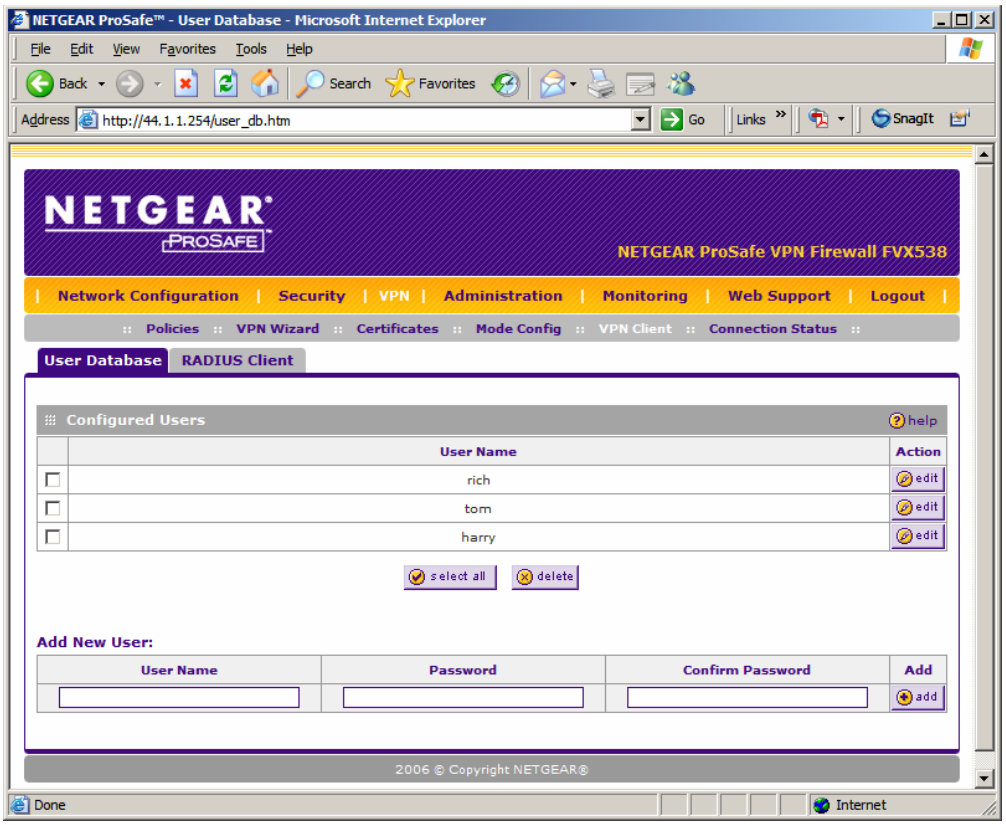


5.6. Xauth User

Add a user that will be used by the Avaya VPNremote phone for authentication by selecting **VPN → VPN Client** from the top menu.

- **User Name**: Enter the name of the user.
- **Password**: Enter the password for the user.
- **Confirm Password**: Enter the password again.

Click **add**.



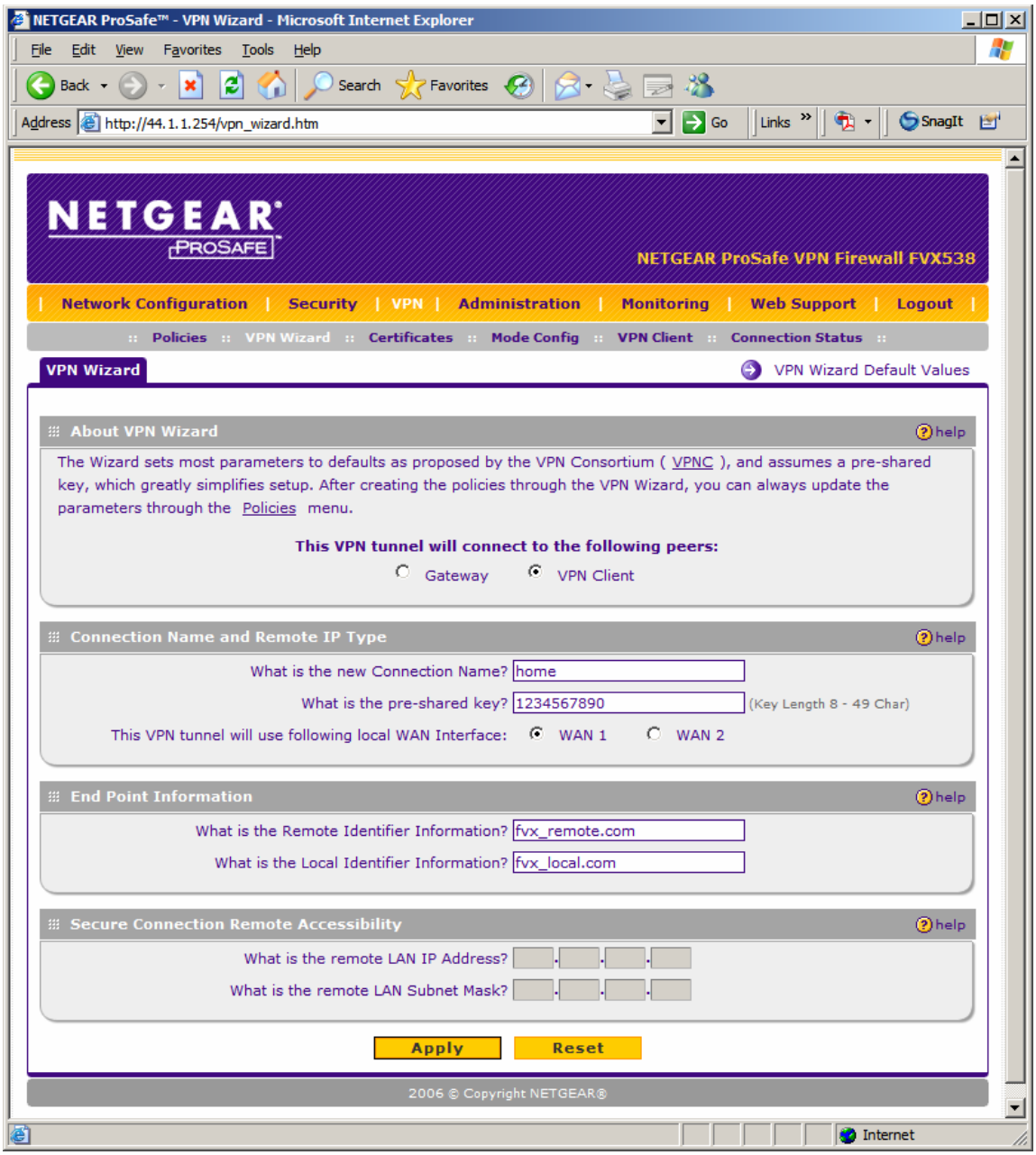
5.7. VPN Policy

The VPN policy will be used by the NETGEAR ProSafe VPN client to establish a tunnel to the NETGEAR FVX538. Create a new VPN policy by selecting **VPN → VPN Wizard**. Enter the following information:

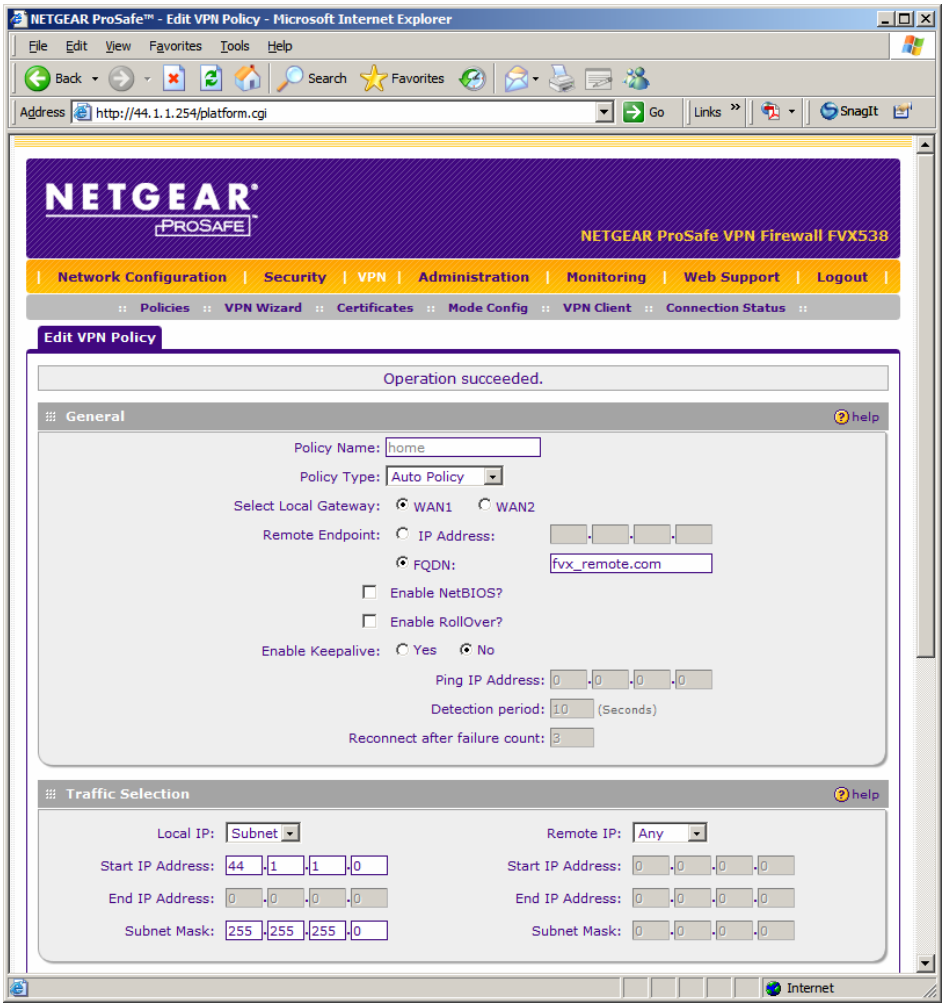
- **This VPN tunnel will connect to the following peers**: Select **VPN Client**.
- **What is the new Connection Name?**: Enter a name for the VPN policy.
- **What is the pre-shared key?**: Enter the key that will be used by the NETGEAR ProSafe VPN client for authentication.
- **This VPN tunnel will use following local WAN Interface**: Select **WAN 1**.
- **What is the Remote Identifier Information?**: Enter the arbitrary **Domain Name** which will be used in **Step 2** of **Section 7**.

- **What is the Local Identifier Information?**: Enter the arbitrary **Domain Name** which will be used in **Step 1** of **Section 7**.

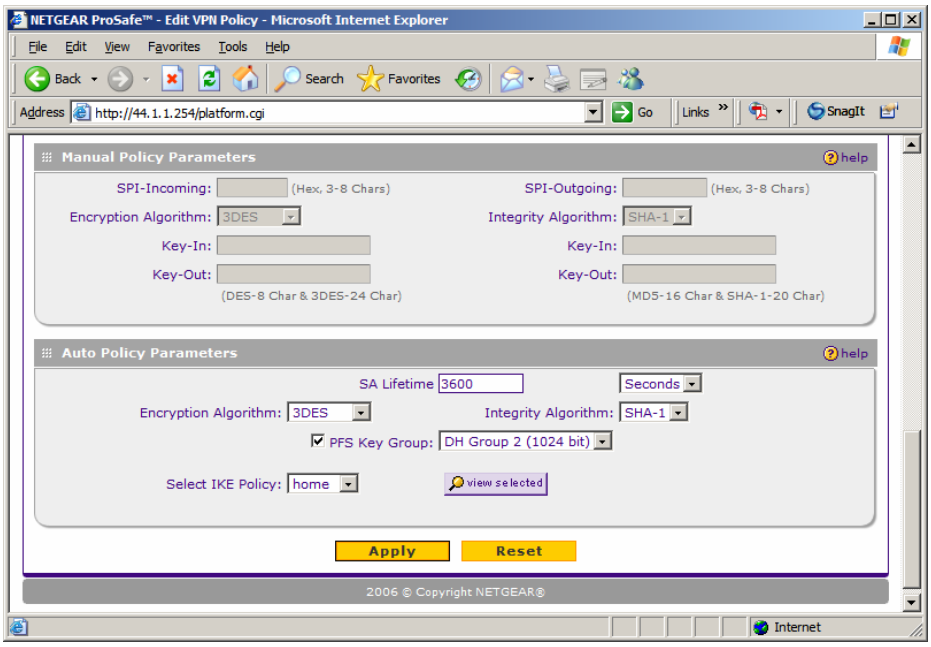
Click **Apply**.



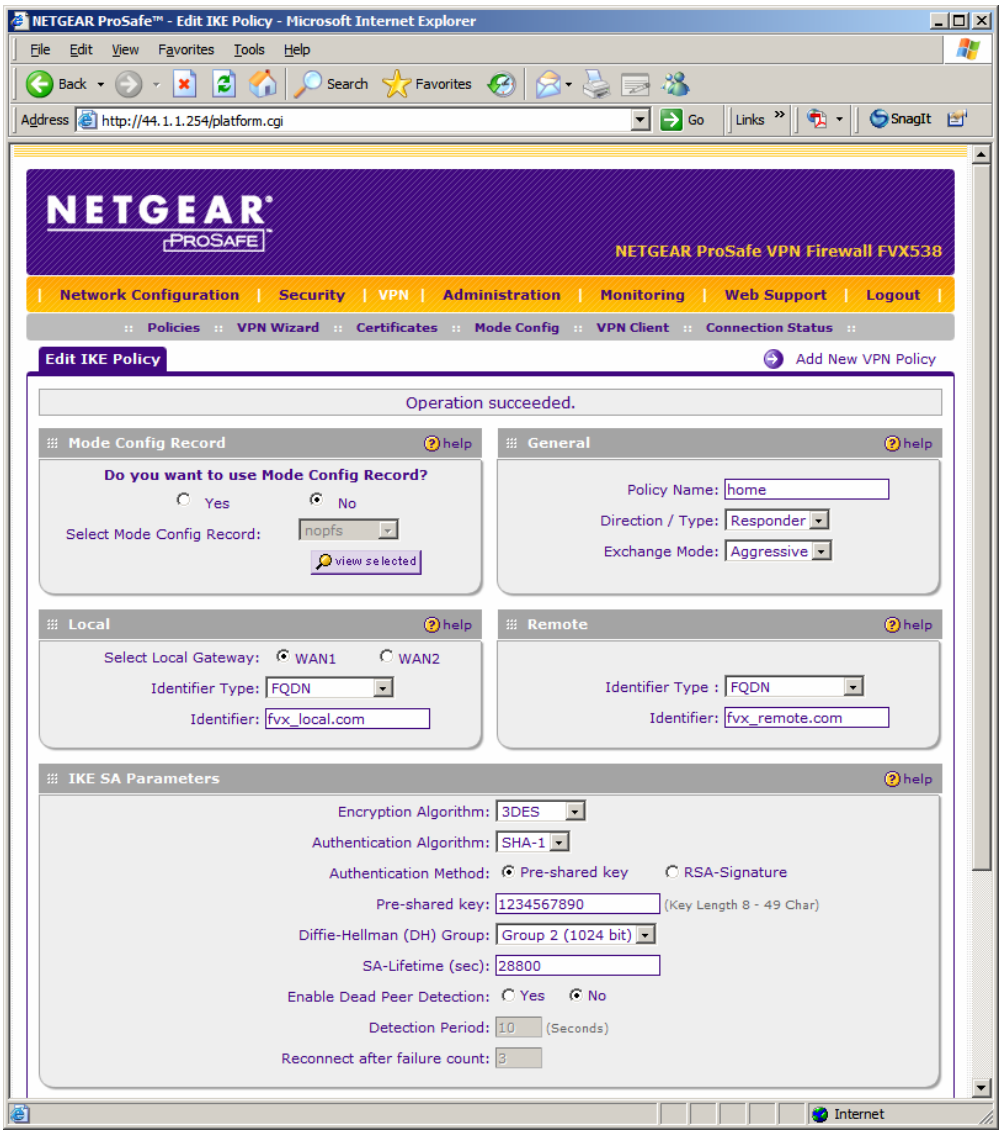
The following VPN policy is created automatically and is shown below.



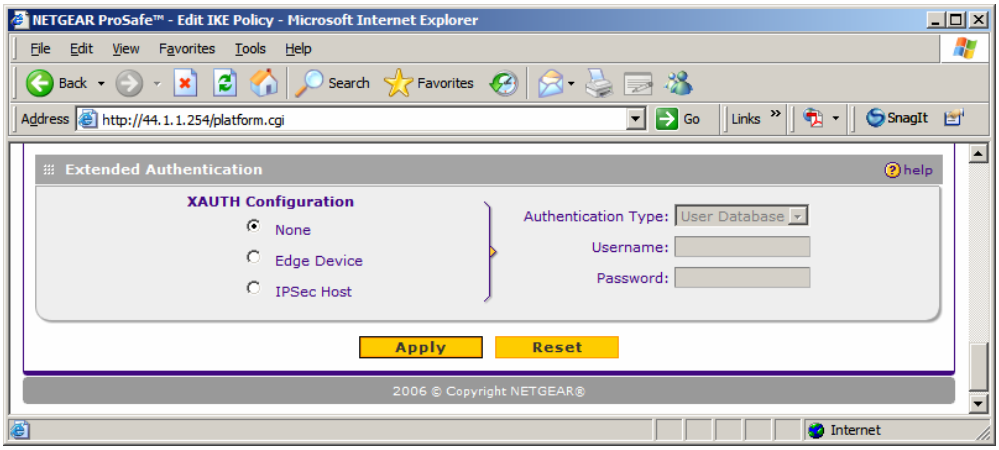
The bottom half of the VPN policy is shown below.



The following IKE policy is created automatically and is shown below.



The bottom half of the IKE policy is shown below.



6. Avaya VPNremote Phone Configuration

6.1. Avaya VPNremote Phone Firmware

The Avaya VPNremote Phone firmware must be installed on the phone prior to the phone being deployed in the remote location. Refer to [1] and [2] for details on installing Avaya VPNremote Phone firmware. The firmware version of Avaya VPNremote Phone can be identified by viewing the version displayed on the phone upon boot up or when the phone is operational by selecting the **Options** hard button → **View IP Settings** soft button → **Miscellaneous** soft button → ► hard button. The Application file name displayed denotes the installed firmware version.

As displayed in **Table 1**, Avaya VPNremote Phone firmware includes the letters **VPN** in the name. This allows for easy identification of firmware versions incorporating VPN capabilities.

6.2. Configuring Avaya VPNremote Phone

The Avaya VPNremote Phone configuration can be administered centrally from an HTTP/TFTP server or locally on the phone. These Application Notes utilize the local phone configuration method. Refer to [1] and [2] for details on a centralized configuration.

1. There are two methods available to access the **VPN Configuration Options** menu from the Avaya VPNremote Phone.

   a. **During Telephone Boot:**

   During Avaya VPNremote Phone boot up, the option to press the * key to enter the local configuration mode is displayed on the telephone screen as shown below.

   ```
   DHCP
   * to program
   ```

   When the * key is pressed, several configuration parameters are presented such as the phones IP Address, the Call Server IP Address, etc. Press # to accept the current settings or set to an appropriate value. The final configuration option displayed is the VPN Start Mode option shown below. Press the * key to enter the VPN Options menu.

   ```
   VPN Start Mode: Boot
   *=Modify  #=OK
   ```

b. During Telephone Operation:

While Avaya VPNremote Phone is in an operational state, i.e. registered with IP Office, press the following key sequence on the telephone to enter VPN configuration mode:

Mute-V-P-N-M-O-D-# (Mute-8-7-6-6-6-3-#)

The follow is displayed:

```
VPN Start Mode: Boot
*=Modify  #=OK
```

Press the ***** key to display the VPN Options menu.

2. The Avaya VPNremote Phone can interoperate with several VPN head-end vendors. The Avaya VPNremote Phone must be told which VPN head-end vendor will be used so the appropriate protocol dialogs can take place. This is done by setting the **VPN Configuration Profile** on the Avaya VPNremote Phone.

Press the **Profile** soft button at the bottom of the Avaya VPNremote Phone display while in the VPN Options mode. The **VPN Configuration Profile** options, shown below, are displayed. If a Profile other than **Juniper Xauth with PSK** is already chosen, press the Modify soft button to display the following list:

- **Avaya Security Gateway**
- **Cisco Xauth with PSK**

  .
  .
  .
- **Juniper Xauth with PSK**
- **Nortel Contivity**

Press the button adjacent to the **Juniper Xauth with PSK** profile option then press the **Done** soft button. **Juniper Xauth with PSK** must be used instead of the **Generic PSK** profile because the sample network is using Xauth authentication.

3. The VPN configuration options menu is displayed. For a detailed description of each VPN configuration option, refer to [1] and [2].

The configuration values of one of the Avaya VPNremote Phones used in the sample configuration are shown in **Table 4** below.

Note: The values entered below are case sensitive.

Press the ► hard button on the telephone to access the next screen of configuration options. Phone models with larger displays (e.g., 4621) will present more configuration options per page.

Configuration Options	Value	Description
Server:	**44.2.2.2**	IP address of the NETGEAR FVX538 (WAN interface configured in **Step 2** of **Section 5.3**).
User Name:	**rich**	User created in **Section 5.6**.
Password:	********	Must match user password entered in **Section 5.6**.
Group Name:	**avaya**	Must match the "Remote Identifier" entered in **Section 5.5**.
Group PSK:	**1234567890**	Must match the "Pre-shared key" entered in **Section 5.5**.
VPN Start Mode	**BOOT**	IPSec tunnel dynamically starts on phone power up.
Password Type	**Save in Flash**	User is not prompted at phone boot up.
Encapsulation	**4500-4500**	This default value enables NAT Traversal.
Syslog Server	-	
IKE Parameters	**DH2-3DES-SHA1**	
IKE ID Type:	**FQDN**	
Diffie-Hellman Grp:	**2**	Can be set to "Detect" to accept VPN Concentrator settings.
Encryption Alg	**3DES**	Can be set to "Any" to accept VPN Concentrator settings.
Authentication Alg	**SHA1**	Can be set to "Any" to accept VPN Concentrator settings.
IKE Xchg Mode	**Aggressive**	
IKE Config Mode:	**Enable**	
XAUTH	**Enable**	
Cert Expiry Check	**Disable**	
Cert DN Check	**Disable**	
IPSec Parameters	**DH2-3DES-SHA1**	
Encryption Alg	**3DES**	Can be set to "Any" to accept VPN Concentrator settings.
Authentication Alg	**SHA1**	Can be set to "Any" to accept VPN Concentrator settings.

Configuration Options	Value	Description
Diffie-Hellman Grp:	**2**	Can be set to "Detect" to accept VPN Concentrator settings.
Protected Nets		
Remote Net #1:	**44.1.1.0/24**	Access to IP Office subnet.
Copy TOS:	**Yes**	Maintain phone TOS setting on Corp. Network for QoS.
File Srvr:	**44.1.1.84**	TFTP File Server.
Connectivity Check:	**Always**	Always test IPSec connectivity.
Qtest	**Disable**	Can be set to either Enable or Disable to allow user access to QTest feature.

Table 4 – Avaya VPNremote Phone Configuration

When all VPN configuration options have been set, press the **Done** soft button. The following is displayed. Press # to save the configuration and reboot the phone.

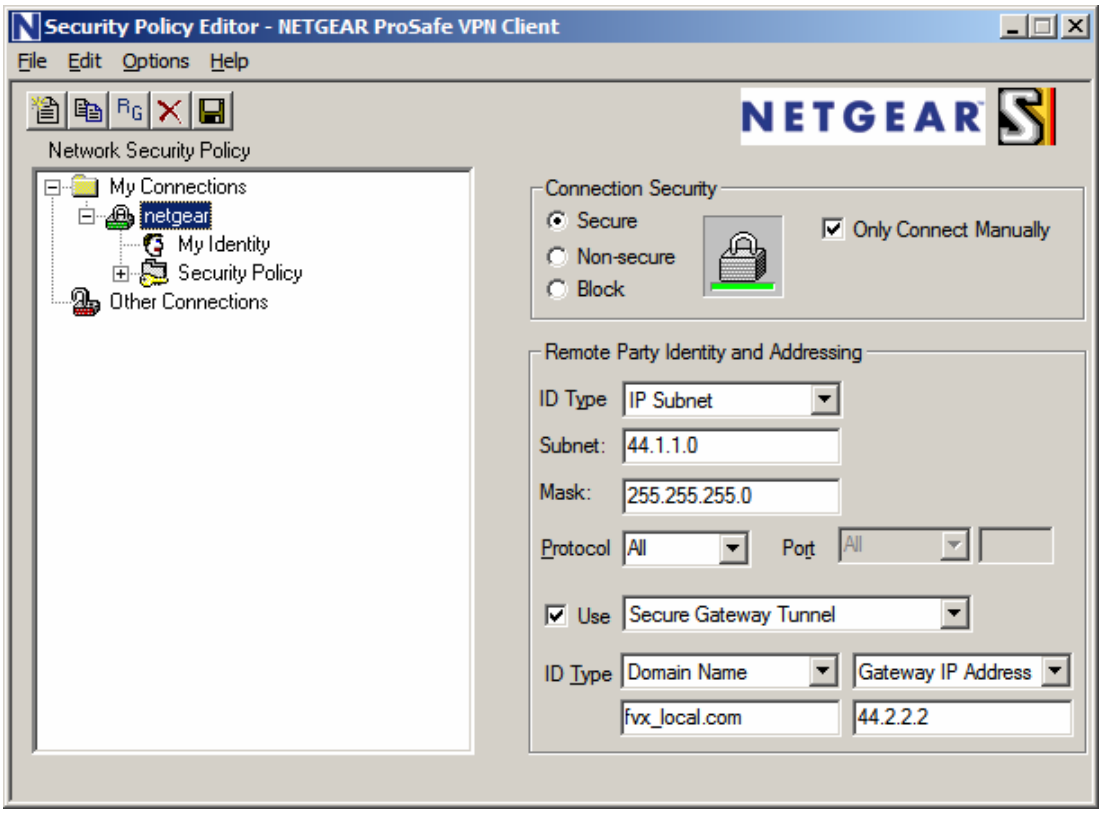
```
Save new values ?
*=no  #=yes
```

4. After the phone reboots, enter the **Base Extension**, administered in **Step 5** of **Section 4**, as the **Extension** when prompted. Enter the **Login Code**, administered in **Step 6** of **Section 4** as the **Password** when prompted.

7. NETGEAR ProSafe VPN Client Configuration

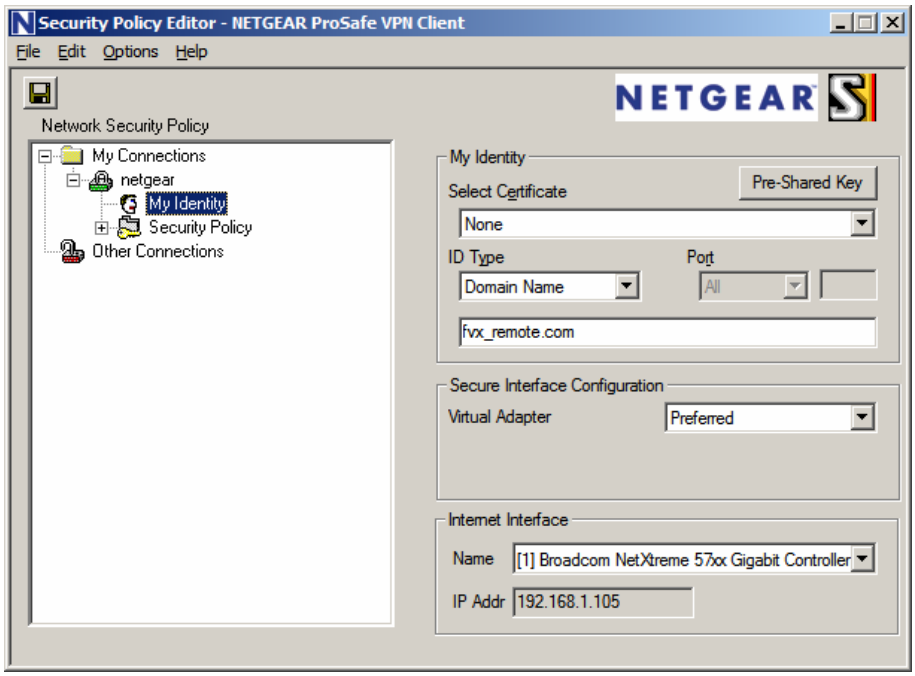
This section shows the configuration of the NETGEAR ProSafe VPN Client.
This section assumes that the NETGEAR ProSafe VPN Client software is already installed on the client desktop.

1. Launch the NETGEAR ProSafe VPN Client Security Policy Editor by selecting **Start → All Programs → NETGEAR ProSafe VPN Client** (Security Policy Editor. Right click the folder My Connections and select Add (Connection (not shown). Provide a descriptive name for the new connection. netgear was used in the sample configuration. Configure the fields shown below.
   - Select **Secure** for **Connection Security**.
   - Select **IP Subnet** for **ID Type**.
   - Enter **44.1.1.0** in the **Subnet** field and **255.255.255.0** in the **Mask** field.
   - Select **All** in the **Protocol** field.
   - Check the **Use** box and select **Secure Gateway Tunnel** from the drop down menu.
   - Enter **fvx_local.com** as the arbitrary **Domain Name** in the **ID Type** field. This must match the **Local Identifier** entered in **Section 5.7**.
   - Enter **44.2.2.2**, the IP address of the NETGEAR FVX538 public interface, as the **Gateway IP Address**.

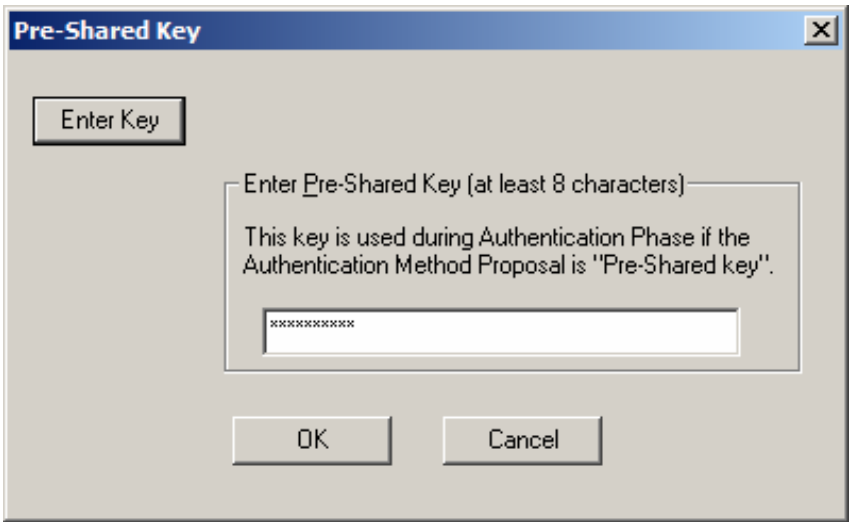


2. Expand the **netgear** folder and select **My Identity**. Configure the fields shown below.
   - Select **None** for the **Select Certificate** field.
   - Select **Domain Name** for the **ID Type** field and enter arbitrary domain **fvx_remote.com**. This must match the **Remote Identifier** in **Section 5.7**.
   - Select **Preferred** for the **Virtual Adapter** field.
   - Select the network interface in the **Internet Interface** field.

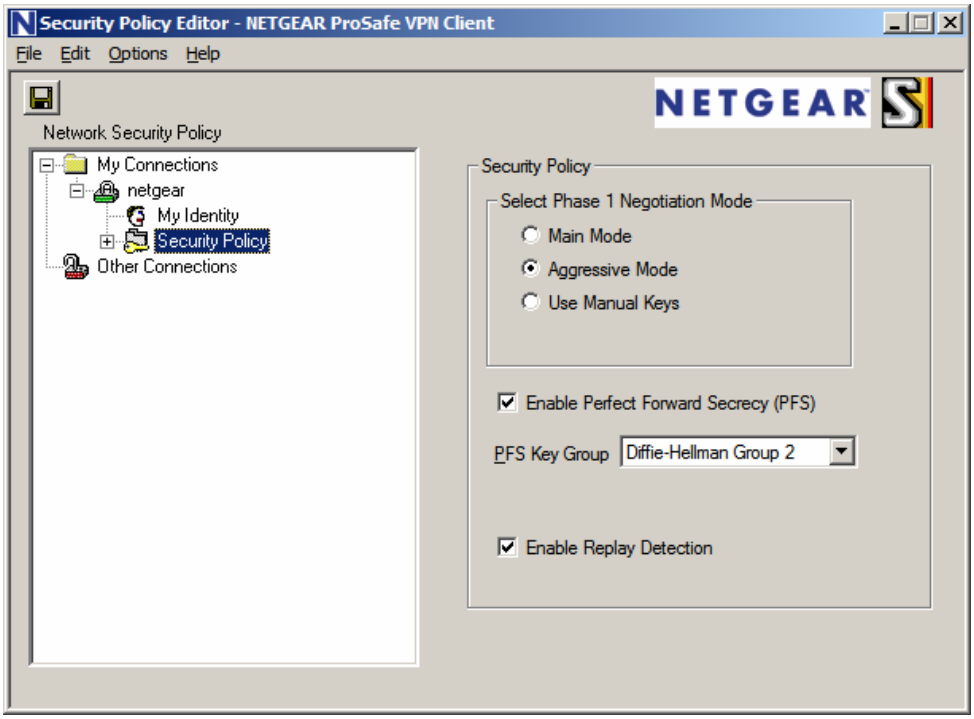
   All remaining fields can be left as the defaults. Click **Pre-Shared Key** to continue.



3. Click **Enter Key** and type the Pre-Shared Key. This must match the Pre-shared Key entered in **Section 5.7**. Click **OK**.

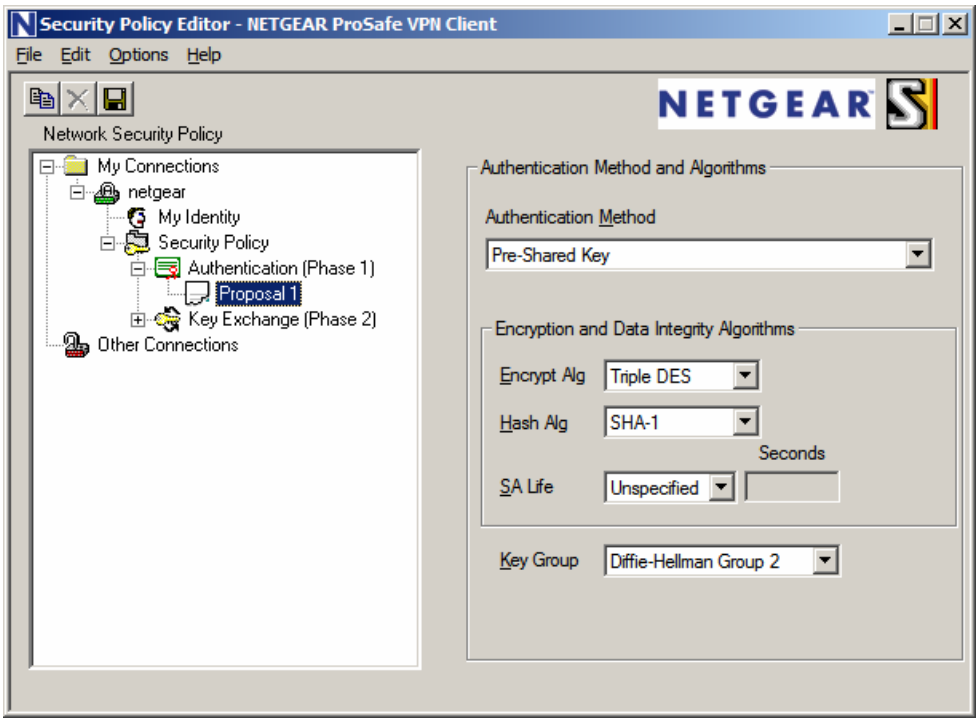


4. Select **Security Policy**. Configure the fields shown below.
    - Select **Aggressive Mode** for **Select Phase 1 Negotiation Mode**.
    - Check **Enable Perfect Forward Secrecy (PFS)**.
    - Select PFS Key Group. Refer to **Section 5.7**.
    - Check the **Enable Replay Detection** box.



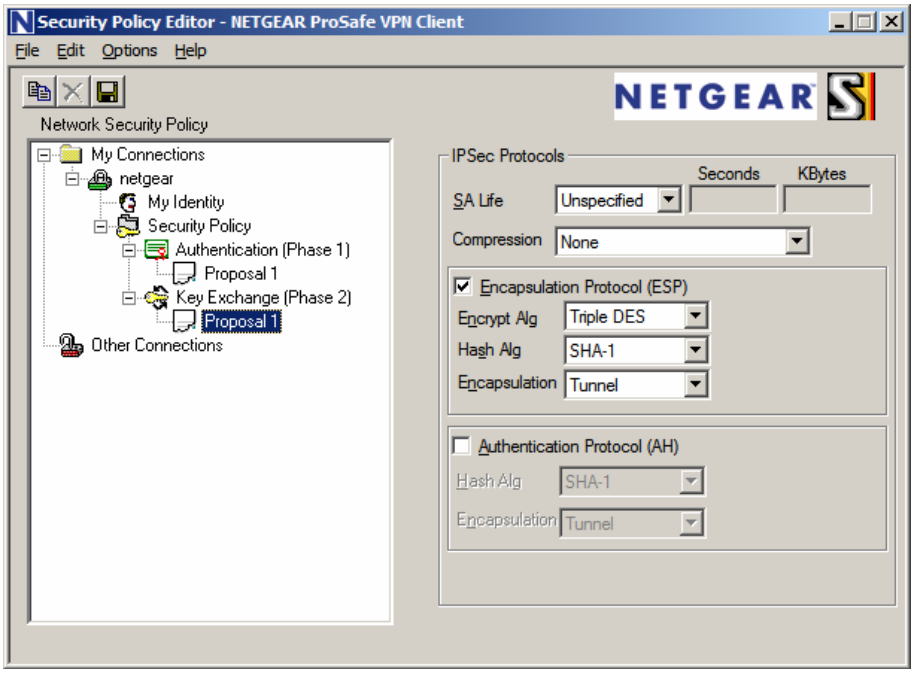
5. Expand the folder **Security Policy → Authentication (Phase 1)** and select **Proposal 1**. Configure the highlighted fields shown below.

- Select **Pre-Shared Key** for the **Authentication Method** field.
- Select **Triple DES** for the **Encrypt Alg** field.
- Select **SHA-1** for the **Hash Alg** field.
- Select **Unspecified** for the **SA Life** field.
- Select **Diffie-Hellman Group 2** for the **Key Group** field.



6. Expand the folder **Security Policy → Key Exchange (Phase 2)** and select **Proposal 1**. Configure the fields shown below. All remaining fields can be left as the defaults.

- Check the **Encapsulation Protocol (ESP)** box.
- Select **Triple DES** for **Encrypt Alg** field.
- Select **SHA-1** for the **Hash Alg** field.
- Select **Tunnel** for the **Encapsulation** field.

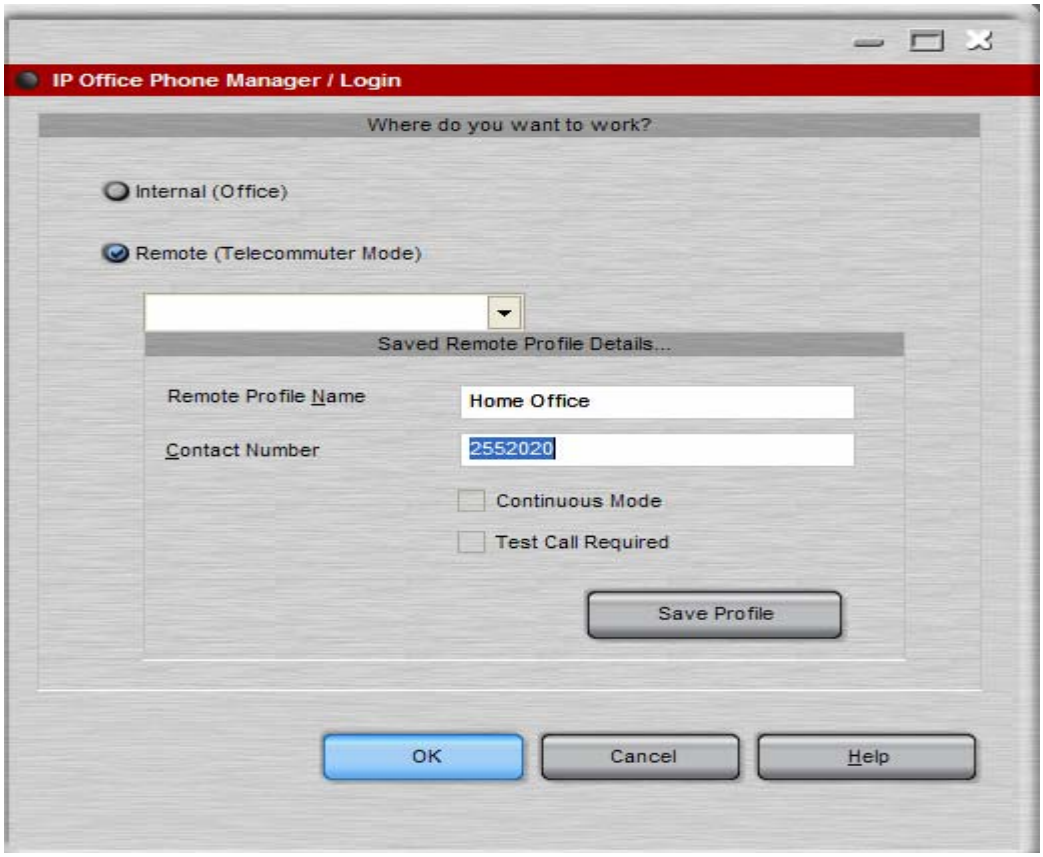


From the menu, select **File → Save** to save the configuration.

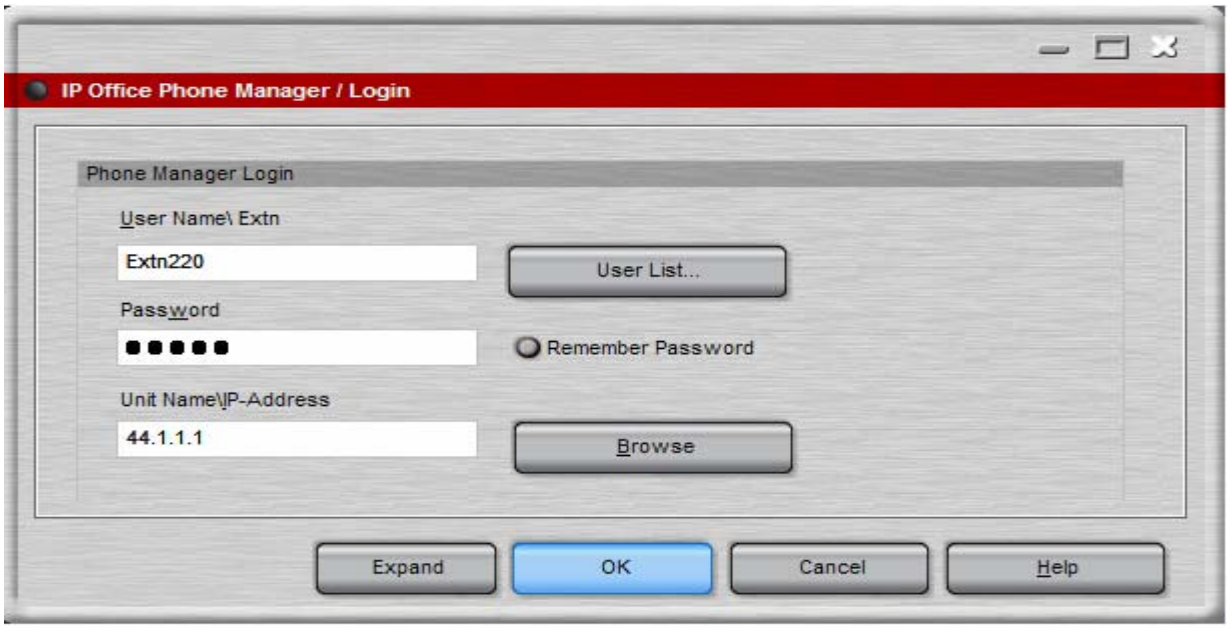
8. Phone Manager Pro Configuration

Log in to the PC and select **Start → Programs → IP Office → Phone Manager** to launch the application.

1. In IP Office Phone Manager **Where do you want to work?** screen:
   - Select **Remote (Telecommuter Mode)**
   - Enter a descriptive **Remote Profile Name**
   - Enter the telephone number in **Contact Number** field, as it would be dialed from any IP Office extension. In these Application Notes, **2552020** is the number of a PSTN phone used by the telecommuter.
   - Accept the default values for **Continuous Mode** and **Test Call Required**.
   - Click on **Save Profile**.
   - Click on **OK**.



2. In the **IP Office Phone Manager / Login** screen, enter:
   - **User Name\Extn**
   - **Password**. This password must match the **Login Code** administered in **Step 6** of **Section 4**.
   - Enter the **LAN1 IP Address** of IP Office, from **Step 3** of **Section 4**, in the **Unit Name\IP-Address** field.
   - Click on **OK**.



Note: The User configured with Phone Manager Telecommuter option is a Hot Desk user, as mentioned in **Section 4, Step 8**. When a user logs in using Phone Manager Pro, the internal IP Office extension will be logged off. The internal IP Office extension is logged in automatically after the user exits Phone Manager.

9. Verification

9.1. VPNremote Phone VPN Status

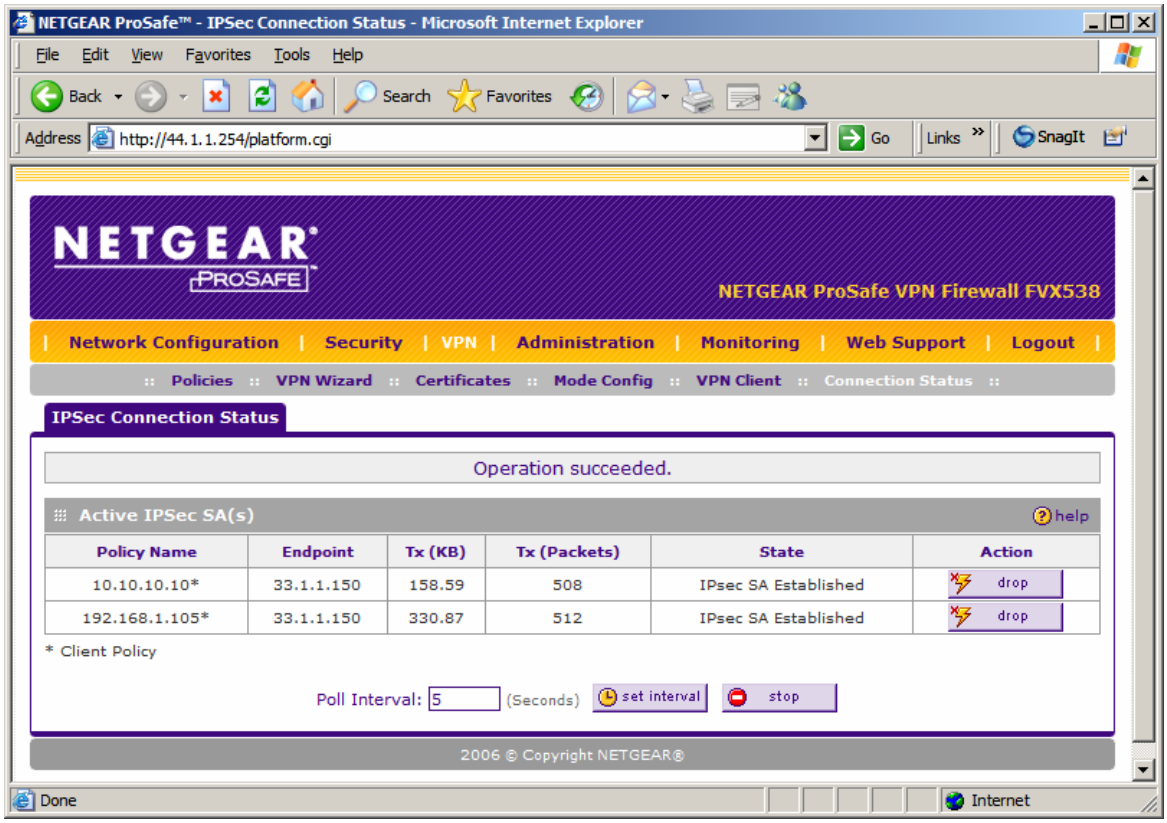
VPN status is available after the Avaya VPNremote Phone establishes an IPSec tunnel, registers with IP Office and becomes functional. From the telephone keypad, press the **OPTIONS** hard button (√ icon), then press the ► hard button to access the next screen. Select the **VPN Status…** option. Two screens of IPSec tunnel statistics are displayed. Use the ► hard button to access the next screen. Press the **Refresh** soft button to update the displayed statistics.

The statistics from Avaya VPNremote Phone used in the sample configuration are shown below.

VPN Status…	
PKT S/R	**474/574**
FRAG RCVD	**0**
Comp/Decomp	**0/0**
Auth Failures	**0**
Recv Errors	**0**
Send Errors	**0**
Gateway	**44.2.2.2**
Outer IP	**192.168.1.101**
Inner IP	**10.10.10.10**
Gateway Version	**KAME/raccoon..**
Inactivity Timeout	**0**
	DH2-3DES-SHA-120 hrs

9.2. NETGEAR FVX538 Debug and Logging

On the NETGEAR FVX538 WebUI, select **VPN → Connection Status** from the top menu bar. The following screenshot shows the connection status of the VPN tunnels.



On the NETGEAR FVX538 WebUI, select **Monitoring → VPN Logs** from the top menu bar. The NETGEAR FVX538 VPN Log shown below contains the IKE Phase1, IKE Phase2 and XAuth events logged as an Avaya VPNremote Phone establishes an IPSec tunnel. The screen below shows the events of a single Avaya VPNremote Phone successfully establishing an IPSec tunnel.

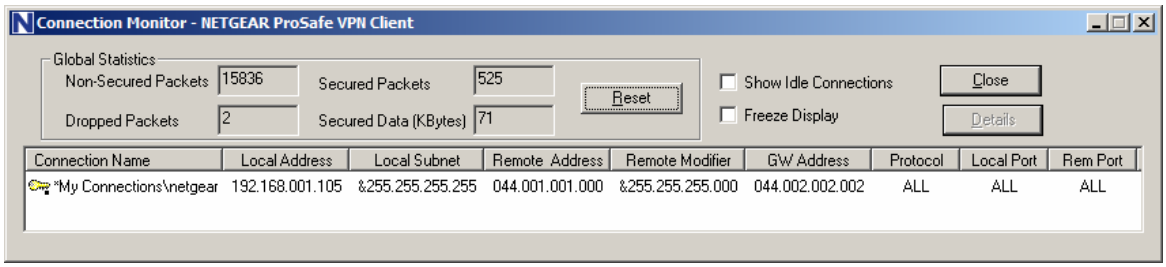
```
1970 Jan  1 00:01:43 [FVX538] [IKE] Remote configuration for identifier "avaya" found_
1970 Jan  1 00:01:43 [FVX538] [IKE] Received request for new phase 1 negotiation:
44.2.2.2[500]<=>33.1.1.150[2070]_
1970 Jan  1 00:01:43 [FVX538] [IKE] Beginning Aggressive mode._
1970 Jan  1 00:01:43 [FVX538] [IKE] Received unknown Vendor ID_
1970 Jan  1 00:01:43 [FVX538] [IKE] Received Vendor ID: draft-ietf-ipsec-nat-t-ike-02__
1970 Jan  1 00:01:43 [FVX538] [IKE] Received unknown Vendor ID_
                - Last output repeated 2 times -
1970 Jan  1 00:01:43 [FVX538] [IKE] Received Vendor ID: draft-ietf-ipsra-isakmp-xauth-06.txt_
1970 Jan  1 00:01:43 [FVX538] [IKE] For 33.1.1.150[2070], Selected NAT-T version: draft-ietf-
ipsec-nat-t-ike-02_
1970 Jan  1 00:01:45 [FVX538] [IKE] Floating ports for NAT-T with peer 33.1.1.150[4500]_
1970 Jan  1 00:01:45 [FVX538] [IKE] NAT-D payload matches for 44.2.2.2[4500]_
1970 Jan  1 00:01:45 [FVX538] [IKE] NAT-D payload does not match for 33.1.1.150[4500]_
1970 Jan  1 00:01:45 [FVX538] [IKE] NAT detected: Peer is behind a NAT device_
1970 Jan  1 00:01:45 [FVX538] [IKE] Sending Xauth request to 33.1.1.150[4500]_
1970 Jan  1 00:01:45 [FVX538] [IKE] ISAKMP-SA established for 44.2.2.2[4500]-33.1.1.150[4500]
with spi:1ff20d555c1aea7a:31c367d492a950f0_
1970 Jan  1 00:01:45 [FVX538] [IKE] Received attribute type "ISAKMP_CFG_REPLY" from
33.1.1.150[4500]_
1970 Jan  1 00:01:45 [FVX538] [IKE] Login succeeded for user "rich"_
1970 Jan  1 00:01:45 [FVX538] [IKE] Received attribute type "ISAKMP_CFG_REQUEST" from
33.1.1.150[4500]_
1970 Jan  1 00:01:45 [FVX538] [IKE] 10.10.10.10 IP address is assigned to remote peer
33.1.1.150[4500]_
1970 Jan  1 00:01:45 [FVX538] [IKE] Ignored attribute 5_
1970 Jan  1 00:01:45 [FVX538] [IKE] Ignored attribute 6_
1970 Jan  1 00:01:47 [FVX538] [IKE] Responding to new phase 2 negotiation:
44.2.2.2[0]<=>33.1.1.150[0]_
1970 Jan  1 00:01:47 [FVX538] [IKE] Ignore INITIAL-CONTACT notification from 33.1.1.150[4500]
because it is only accepted after phase1._
1970 Jan  1 00:01:47 [FVX538] [IKE] Using IPsec SA configuration: 44.1.1.0/24<-
>10.10.10.0/24_
1970 Jan  1 00:01:47 [FVX538] [IKE] Adjusting peer's encmode 61443(61443)->Tunnel(1)_
1970 Jan  1 00:01:49 [FVX538] [IKE] IPsec-SA established[UDP encap 4500->4500]: ESP/Tunnel
33.1.1.150->44.2.2.2 with spi=251917329(0xf03f411)_
1970 Jan  1 00:01:49 [FVX538] [IKE] IPsec-SA established[UDP encap 4500->4500]: ESP/Tunnel
44.2.2.2->33.1.1.150 with spi=1478768541(0x5824379d)_
```

The NETGEAR FVX538 VPN Log shown below contains the IKE Phase1, IKE Phase2 events logged as a NETGEAR ProSafe VPN Client establishes an IPSec tunnel.

```
1970 Jan  1 00:26:15 [FVX538] [IKE] Remote configuration for identifier "fvx_remote.com"
found_
1970 Jan  1 00:26:15 [FVX538] [IKE] Received request for new phase 1 negotiation:
44.2.2.2[500]<=>33.1.1.150[500]_
1970 Jan  1 00:26:15 [FVX538] [IKE] Beginning Aggressive mode._
1970 Jan  1 00:26:15 [FVX538] [IKE] Received unknown Vendor ID_
                - Last output repeated 2 times -
1970 Jan  1 00:26:15 [FVX538] [IKE] Received Vendor ID: draft-ietf-ipsra-isakmp-xauth-
06.txt_
1970 Jan  1 00:26:15 [FVX538] [IKE] Received unknown Vendor ID_
1970 Jan  1 00:26:15 [FVX538] [IKE] Received Vendor ID: draft-ietf-ipsec-nat-t-ike-02__
1970 Jan  1 00:26:15 [FVX538] [IKE] For 33.1.1.150[500], Selected NAT-T version: draft-
ietf-ipsec-nat-t-ike-02_
1970 Jan  1 00:26:16 [FVX538] [IKE] Floating ports for NAT-T with peer 33.1.1.150[27701]_
1970 Jan  1 00:26:16 [FVX538] [IKE] NAT-D payload matches for 44.2.2.2[4500]_
1970 Jan  1 00:26:16 [FVX538] [IKE] NAT-D payload does not match for 33.1.1.150[27701]_
1970 Jan  1 00:26:16 [FVX538] [IKE] Ignore REPLAY-STATUS notification from
33.1.1.150[27701]._
1970 Jan  1 00:26:16 [FVX538] [IKE] Ignore INITIAL-CONTACT notification from
33.1.1.150[27701] because it is only accepted after phase1._
1970 Jan  1 00:26:16 [FVX538] [IKE] NAT detected: Peer is behind a NAT device_
1970 Jan  1 00:26:16 [FVX538] [IKE] ISAKMP-SA established for 44.2.2.2[4500]-
33.1.1.150[27701] with spi:0329354c4ce217e2:1bd3e066bf94373c_
1970 Jan  1 00:26:16 [FVX538] [IKE] Sending Informational Exchange: notify payload[INITIAL-
CONTACT]_
1970 Jan  1 00:26:16 [FVX538] [IKE] Responding to new phase 2 negotiation:
44.2.2.2[0]<=>33.1.1.150[0]_
1970 Jan  1 00:26:16 [FVX538] [IKE] Using IPsec SA configuration: 44.1.1.0/24<->0.0.0.0/0
from fvx_remote.com_
1970 Jan  1 00:26:16 [FVX538] [IKE] No policy found, generating the policy :
192.168.1.105/32[0] 44.1.1.0/24[0] proto=any dir=in_
1970 Jan  1 00:26:16 [FVX538] [IKE] Adjusting peer's encmode 61443(61443)->Tunnel(1)_
1970 Jan  1 00:26:16 [FVX538] [IKE] IPsec-SA established[UDP encap 27701->4500]: ESP/Tunnel
33.1.1.150->44.2.2.2 with spi=186021828(0xb1677c4)_
1970 Jan  1 00:26:16 [FVX538] [IKE] IPsec-SA established[UDP encap 4500->27701]: ESP/Tunnel
44.2.2.2->33.1.1.150 with spi=3180860194(0xbd981322)_
```

9.3. NETGEAR ProSafe VPN Client Debug and Logging

Launch the NETGEAR ProSafe Log Viewer by selecting **Start → All Programs → NETGEAR ProSafe VPN Client → Connection Monitor**. The NETGEAR ProSafe VPN Client Connection Monitor can be used to determine the connection status of the IPSec VPN tunnel.



Launch the NETGEAR ProSafe VPN Client Log Viewer by selecting **Start → All Programs → NETGEAR ProSafe VPN Client → Log Viewer**. The NETGEAR ProSafe VPN Client Log Viewer shown below contains the IKE Phase1, IKE Phase2 events logged as an IPSec tunnel is established.

```
2-21: 14:22:15.895
 2-21: 14:22:15.895 My Connections\netgear - Initiating IKE Phase 1 (IP
ADDR=44.2.2.2)
 2-21: 14:22:16.161 My Connections\netgear - SENDING>>>> ISAKMP OAK AG (SA, KE, NON,
ID, VID 6x)
 2-21: 14:22:16.598 My Connections\netgear - RECEIVED<<< ISAKMP OAK AG (SA, KE, NON,
ID, HASH, VID 3x, NAT-D 2x, VID)
 2-21: 14:22:16.598 My Connections\netgear - Peer is NAT-T draft-02 capable
 2-21: 14:22:16.598 My Connections\netgear - NAT is detected for Client
 2-21: 14:22:16.598 My Connections\netgear - Floating to IKE non-500 port
 2-21: 14:22:16.739 My Connections\netgear - SENDING>>>> ISAKMP OAK AG *(HASH, NAT-D
2x, NOTIFY:STATUS_REPLAY_STATUS, NOTIFY:STATUS_INITIAL_CONTACT)
 2-21: 14:22:16.739 My Connections\netgear - Established IKE SA
 2-21: 14:22:16.739 My Connections\netgear -   MY COOKIE 3 29 35 4c 4c e2 17 e2
 2-21: 14:22:16.739 My Connections\netgear -   HIS COOKIE 1b d3 e0 66 bf 94 37 3c
 2-21: 14:22:16.973 My Connections\netgear - Initiating IKE Phase 2 with Client IDs
(message id: 5EE6A314)
 2-21: 14:22:16.973 My Connections\netgear -   Initiator = IP ADDR=192.168.1.105,
prot = 0 port = 0
 2-21: 14:22:16.973 My Connections\netgear -   Responder = IP
SUBNET/MASK=44.1.1.0/255.255.255.0, prot = 0 port = 0
 2-21: 14:22:16.973 My Connections\netgear - SENDING>>>> ISAKMP OAK QM *(HASH, SA,
NON, KE, ID 2x)
 2-21: 14:22:16.973 My Connections\netgear - RECEIVED<<< ISAKMP OAK INFO *(HASH,
NOTIFY:STATUS_INITIAL_CONTACT)
 2-21: 14:22:17.286 My Connections\netgear - RECEIVED<<< ISAKMP OAK QM *(HASH, SA,
NON, KE, ID 2x)
 2-21: 14:22:17.286 My Connections\netgear - Filter entry 3 added: SECURE
192.168.001.105&255.255.255.255  044.001.001.000&255.255.255.000  044.002.002.002
 2-21: 14:22:17.286 My Connections\netgear - SENDING>>>> ISAKMP OAK QM *(HASH)
 2-21: 14:22:17.333 My Connections\netgear - Loading IPSec SA (Message ID = 5EE6A314
OUTBOUND SPI = B1677C4 INBOUND SPI = BD981322)
```

10. Testing

The interoperability testing focused on verifying interoperability between the Avaya VPNremote Phone and Phone Manager Pro in Telecommuter mode and the Avaya IP Office using the configuration shown in **Figure 1**.

The following features were successfully tested in this configuration:

1. Basic operations that include call origination, termination, hold, transfer, and conference functionality.
2. Voicemail and Message Waiting Indication
3. Hunt Group operation at the Avaya VPNremote Phone and Phone Manager Pro.
4. Bridged and Line Appearance buttons at the Avaya VPNremote Phone.
5. Mobile Twinning at the Avaya VPNremote Phone.

A remote worker when using the Phone Manager Pro in telecommuter mode **does not** have the same functionality as a telephone co-located with the IP office. **Phone Manager Pro limitations are**:

1. Single Line appearance.
2. No bridged call appearances at the Phone Manager Pro or of the Phone Manager Pro extension at other IP Office users when in this mode.
3. The Mobile Twinning feature is not available when using the Phone Manager Pro.

11. Troubleshooting

This section offers some common configuration mismatches to assist in troubleshooting.

11.1. Incorrect User Name or Password

- **Avaya VPNremote Phone display:**
  The display shows the following:
  Retrying in 7200 Secs
  Invalid password OR user name
  Press Edit to modify VPN
  Press MORE to see details

  Press the **More** soft button to display the following:
  Showing Error 1/1
  Invalid password OR user name
  Error Code: 3997700:0
  Module:IKECFG:430

- **NETGEAR FVX538 WebUI: Monitoring → VPN Logs**

```
1970 Jan  1 00:07:11 [FVX538] [IKE] Remote configuration for identifier "avaya"
found_
1970 Jan  1 00:07:11 [FVX538] [IKE] Received request for new phase 1 negotiation:
44.2.2.2[500]<=>33.1.1.150[2070]_
1970 Jan  1 00:07:11 [FVX538] [IKE] Beginning Aggressive mode._
1970 Jan  1 00:07:11 [FVX538] [IKE] Received unknown Vendor ID_
1970 Jan  1 00:07:11 [FVX538] [IKE] Received Vendor ID: draft-ietf-ipsec-nat-t-ike-
02__
1970 Jan  1 00:07:11 [FVX538] [IKE] Received unknown Vendor ID_
                - Last output repeated 2 times -
1970 Jan  1 00:07:11 [FVX538] [IKE] Received Vendor ID: draft-ietf-ipsra-isakmp-
xauth-06.txt_
1970 Jan  1 00:07:11 [FVX538] [IKE] For 33.1.1.150[2070], Selected NAT-T version:
draft-ietf-ipsec-nat-t-ike-02_
1970 Jan  1 00:07:13 [FVX538] [IKE] Floating ports for NAT-T with peer
33.1.1.150[4500]_
1970 Jan  1 00:07:13 [FVX538] [IKE] NAT-D payload matches for 44.2.2.2[4500]_
1970 Jan  1 00:07:13 [FVX538] [IKE] NAT-D payload does not match for
33.1.1.150[4500]_
1970 Jan  1 00:07:13 [FVX538] [IKE] NAT detected: Peer is behind a NAT device_
1970 Jan  1 00:07:13 [FVX538] [IKE] Sending Xauth request to 33.1.1.150[4500]_
1970 Jan  1 00:07:13 [FVX538] [IKE] ISAKMP-SA established for 44.2.2.2[4500]-
33.1.1.150[4500] with spi:3f03ccbff2fe21e2:de07e15640ea38b8_
1970 Jan  1 00:07:13 [FVX538] [IKE] Received attribute type "ISAKMP_CFG_REPLY" from
33.1.1.150[4500]_
1970 Jan  1 00:07:13 [FVX538] [IKE] 0.0.0.0 IP address has been released by remote
peer._
1970 Jan  1 00:07:13 [FVX538] [IKE] Login failed for user "joe"_
1970 Jan  1 00:07:13 [FVX538] [IKE] Sending Informational Exchange: delete payload[]_
1970 Jan  1 00:07:13 [FVX538] [IKE] Failed to find proper address pool with id -1_
1970 Jan  1 00:07:13 [FVX538] [IKE] an undead schedule has been deleted: 'ph1_main'._
1970 Jan  1 00:07:13 [FVX538] [IKE] Received mode config from 33.1.1.150[4500], but
we do not have ISAKMP-SA._
```

- **NETGEAR ProSafe VPN Client → Log Viewer**

```
2-21: 15:35:40.254
 2-21: 15:35:40.254 My Connections\netgear - Initiating IKE Phase 1 (IP
ADDR=44.2.2.2)
 2-21: 15:35:40.536 My Connections\netgear - SENDING>>>> ISAKMP OAK AG (SA, KE, NON,
ID, VID 6x)
 2-21: 15:35:40.958 My Connections\netgear - RECEIVED<<< ISAKMP OAK AG (SA, KE, NON,
ID, HASH, VID 3x, NAT-D 2x, VID)
 2-21: 15:35:40.958 My Connections\netgear - Peer is NAT-T draft-02 capable
 2-21: 15:35:40.958 My Connections\netgear - NAT is detected for Client
 2-21: 15:35:40.958 My Connections\netgear - Floating to IKE non-500 port
 2-21: 15:35:41.067 My Connections\netgear - Hash Payload is incorrect.
 2-21: 15:35:41.067 My Connections\netgear - SENDING>>>> ISAKMP OAK INFO (HASH,
NOTIFY:INVALID_HASH_INFO)
 2-21: 15:35:41.067 My Connections\netgear - Discarding IKE SA negotiation
 2-21: 15:35:41.067 My Connections\netgear -   MY COOKIE 81 23 24 aa b1 9c d5 d
 2-21: 15:35:41.067 My Connections\netgear -   HIS COOKIE 3b 33 1c f4 13 87 5 16
```

11.2. Mismatched Phase 1 Proposal

- **Avaya VPNremote Phone display:**
  `Retrying in 30 Secs`
  `IKE Phase1 no response`
  `Press EDIT to modify VPN`
  `Press MORE to see details`

  Press the **More** soft button to display the following:
  `Showing Error 1/2`
  `Error Code: 3997700:0`
  `Module:IKMPD:142`

  Press the **Next** soft button to display the following:
  `Showing Error 2/2`
  `Error Code: 3997700:0`
  `Module:IKECFG:459`

- **NETGEAR FVX538 WebUI: Monitoring → VPN Logs**

```
1970 Jan  1 00:27:40 [FVX538] [IKE] Remote configuration for identifier "avaya"
found_
1970 Jan  1 00:27:40 [FVX538] [IKE] Received request for new phase 1 negotiation:
44.2.2.2[500]<=>33.1.1.150[2070]_
1970 Jan  1 00:27:40 [FVX538] [IKE] Beginning Aggressive mode._
1970 Jan  1 00:27:40 [FVX538] [IKE] Received unknown Vendor ID_
1970 Jan  1 00:27:40 [FVX538] [IKE] Received Vendor ID: draft-ietf-ipsec-nat-t-
ike-02__
1970 Jan  1 00:27:40 [FVX538] [IKE] Received unknown Vendor ID_
                - Last output repeated 2 times -
1970 Jan  1 00:27:40 [FVX538] [IKE] Received Vendor ID: draft-ietf-ipsra-isakmp-
xauth-06.txt_
1970 Jan  1 00:27:40 [FVX538] [IKE] For 33.1.1.150[2070], Selected NAT-T version:
draft-ietf-ipsec-nat-t-ike-02_
1970 Jan  1 00:27:40 [FVX538] [IKE] Rejected phase 1 proposal as Peer's hashtype
"MD5" mismatched with Local "SHA"._
1970 Jan  1 00:27:40 [FVX538] [IKE] No suitable proposal found for
33.1.1.150[2070]._
1970 Jan  1 00:27:40 [FVX538] [IKE] Failed to get valid proposal for
33.1.1.150[2070]._
```

- **NETGEAR ProSafe VPN Client → Log Viewer**

```
2-21: 16:14:13.051 My Connections\netgear - Initiating IKE Phase 1 (IP
ADDR=44.2.2.2)
 2-21: 16:14:13.239 My Connections\netgear - SENDING>>>> ISAKMP OAK AG (SA, KE,
NON, ID, VID 6x)
 2-21: 16:14:28.567 My Connections\netgear - message not received!
Retransmitting!
 2-21: 16:14:28.567 My Connections\netgear - SENDING>>>> ISAKMP OAK AG
(Retransmission)
 2-21: 16:14:43.708 My Connections\netgear - message not received!
Retransmitting!
 2-21: 16:14:43.708 My Connections\netgear - SENDING>>>> ISAKMP OAK AG
(Retransmission)
 2-21: 16:14:58.739 My Connections\netgear - message not received!
Retransmitting!
 2-21: 16:14:58.739 My Connections\netgear - SENDING>>>> ISAKMP OAK AG
(Retransmission)
 2-21: 16:15:13.739 My Connections\netgear - Exceeded 3 IKE SA negotiation
attempts
```

11.3. Mismatched Phase 2 Proposal

- **Avaya VPNremote Phone display:**

  `Retrying in 30 Secs`
  `IKE Phase2 no response`
  `Press EDIT to modify VPN`
  `Press MORE to see details`

  Press the **More** soft button to display the following:

  `Showing Error 1/2`
  `IKE Phase2 proposal mismatch`
  `Error Code: 3997698:14`
  `Module:NOTIFY:444`

Press the **Next** soft button to display the following:

```
Showing Error 2/2
IKE Phase2 no response
Error Code: 3997700:0
Module:IKECFG:1184
```

- **NETGEAR FVX538 WebUI: Monitoring → VPN Logs**

```
1970 Jan  1 00:57:32 [FVX538] [IKE] Remote configuration for identifier "avaya"
found_
1970 Jan  1 00:57:32 [FVX538] [IKE] Received request for new phase 1 negotiation:
44.2.2.2[500]<=>33.1.1.150[2070]_
1970 Jan  1 00:57:32 [FVX538] [IKE] Beginning Aggressive mode._
1970 Jan  1 00:57:32 [FVX538] [IKE] Received unknown Vendor ID_
1970 Jan  1 00:57:32 [FVX538] [IKE] Received Vendor ID: draft-ietf-ipsec-nat-t-ike-
02__
1970 Jan  1 00:57:32 [FVX538] [IKE] Received unknown Vendor ID_
                - Last output repeated 2 times -
1970 Jan  1 00:57:32 [FVX538] [IKE] Received Vendor ID: draft-ietf-ipsra-isakmp-
xauth-06.txt_
1970 Jan  1 00:57:32 [FVX538] [IKE] For 33.1.1.150[2070], Selected NAT-T version:
draft-ietf-ipsec-nat-t-ike-02_
1970 Jan  1 00:57:34 [FVX538] [IKE] Floating ports for NAT-T with peer
33.1.1.150[4500]_
1970 Jan  1 00:57:34 [FVX538] [IKE] NAT-D payload matches for 44.2.2.2[4500]_
1970 Jan  1 00:57:34 [FVX538] [IKE] NAT-D payload does not match for
33.1.1.150[4500]_
1970 Jan  1 00:57:34 [FVX538] [IKE] NAT detected: Peer is behind a NAT device_
1970 Jan  1 00:57:34 [FVX538] [IKE] Sending Xauth request to 33.1.1.150[4500]_
1970 Jan  1 00:57:34 [FVX538] [IKE] ISAKMP-SA established for 44.2.2.2[4500]-
33.1.1.150[4500] with spi:a618784f357856ae:4facabc6c9e2d690_
1970 Jan  1 00:57:34 [FVX538] [IKE] Received attribute type "ISAKMP_CFG_REPLY" from
33.1.1.150[4500]_
1970 Jan  1 00:57:34 [FVX538] [IKE] Login succeeded for user "rich"_
1970 Jan  1 00:57:34 [FVX538] [IKE] Received attribute type "ISAKMP_CFG_REQUEST" from
33.1.1.150[4500]_
1970 Jan  1 00:57:34 [FVX538] [IKE] 10.10.10.10 IP address is assigned to remote peer
33.1.1.150[4500]_
1970 Jan  1 00:57:34 [FVX538] [IKE] Ignored attribute 5_
1970 Jan  1 00:57:34 [FVX538] [IKE] Ignored attribute 6_
1970 Jan  1 00:57:36 [FVX538] [IKE] Responding to new phase 2 negotiation:
44.2.2.2[0]<=>33.1.1.150[0]_
1970 Jan  1 00:57:36 [FVX538] [IKE] Ignore INITIAL-CONTACT notification from
33.1.1.150[4500] because it is only accepted after phase1._
1970 Jan  1 00:57:36 [FVX538] [IKE] Using IPsec SA configuration: 44.1.1.0/24<-
>10.10.10.0/24_
1970 Jan  1 00:57:36 [FVX538] [IKE] Adjusting peer's encmode 61443(61443)->Tunnel(1)_
1970 Jan  1 00:57:36 [FVX538] [IKE] Peer's Proposal:_
1970 Jan  1 00:57:36 [FVX538] [IKE] (proto_id=ESP spisize=4 spi=d84b94af
spi_p=00000000 encmode=Tunnel reqid=0:0)_
1970 Jan  1 00:57:36 [FVX538] [IKE] (trns_id=3DES encklen=0 authtype=hmac-md5)_
1970 Jan  1 00:57:36 [FVX538] [IKE] Local Proposal:_
1970 Jan  1 00:57:36 [FVX538] [IKE] (proto_id=ESP spisize=4 spi=00000000
spi_p=00000000 encmode=Tunnel reqid=4500:4500)_
1970 Jan  1 00:57:36 [FVX538] [IKE] (trns_id=3DES encklen=0 authtype=hmac-sha)_
1970 Jan  1 00:57:36 [FVX538] [IKE] Phase 2 proposal by 33.1.1.150[0] did not match._
1970 Jan  1 00:57:36 [FVX538] [IKE] No suitable policy found for 33.1.1.150[0]_
1970 Jan  1 00:57:36 [FVX538] [IKE] Sending Informational Exchange: notify
payload[NO-PROPOSAL-CHOSEN]_
1970 Jan  1 00:57:36 [FVX538] [IKE] Responding to new phase 2 negotiation:
44.2.2.2[0]<=>33.1.1.150[0]_
1970 Jan  1 00:57:36 [FVX538] [IKE] Ignore INITIAL-CONTACT notification from
33.1.1.150[4500] because it is only accepted after phase1._
1970 Jan  1 00:57:36 [FVX538] [IKE] Using IPsec SA configuration: 44.1.1.0/24<-
>10.10.10.0/24_
```

- **NETGEAR ProSafe VPN Client → Log Viewer**

```
2-21: 16:26:25.739 My Connections\netgear - Initiating IKE Phase 1 (IP ADDR=44.2.2.2)
 2-21: 16:26:25.989 My Connections\netgear - SENDING>>>> ISAKMP OAK AG (SA, KE, NON,
ID, VID 6x)
 2-21: 16:26:26.411 My Connections\netgear - RECEIVED<<< ISAKMP OAK AG (SA, KE, NON,
ID, HASH, VID 3x, NAT-D 2x, VID)
 2-21: 16:26:26.411 My Connections\netgear - Peer is NAT-T draft-02 capable
 2-21: 16:26:26.411 My Connections\netgear - NAT is detected for Client
 2-21: 16:26:26.411 My Connections\netgear - Floating to IKE non-500 port
 2-21: 16:26:26.520 My Connections\netgear - SENDING>>>> ISAKMP OAK AG *(HASH, NAT-D
2x, NOTIFY:STATUS_REPLAY_STATUS, NOTIFY:STATUS_INITIAL_CONTACT)
 2-21: 16:26:26.520 My Connections\netgear - Established IKE SA
 2-21: 16:26:26.520 My Connections\netgear -   MY COOKIE b1 2d 5c c8 4f ba 14 1a
 2-21: 16:26:26.520 My Connections\netgear -   HIS COOKIE 33 de 7c 5f 3c ff b1 aa
 2-21: 16:26:26.676 My Connections\netgear - Initiating IKE Phase 2 with Client IDs
(message id: 3DECF9A5)
 2-21: 16:26:26.676 My Connections\netgear -   Initiator = IP ADDR=192.168.1.105, prot
= 0 port = 0
 2-21: 16:26:26.676 My Connections\netgear -   Responder = IP
SUBNET/MASK=44.1.1.0/255.255.255.0, prot = 0 port = 0
 2-21: 16:26:26.676 My Connections\netgear - SENDING>>>> ISAKMP OAK QM *(HASH, SA,
NON, KE, ID 2x)
 2-21: 16:26:26.676 My Connections\netgear - RECEIVED<<< ISAKMP OAK INFO *(HASH,
NOTIFY:STATUS_INITIAL_CONTACT)
 2-21: 16:26:26.879 My Connections\netgear - RECEIVED<<< ISAKMP OAK INFO *(HASH,
NOTIFY:NO_PROPOSAL_CHOSEN)
 2-21: 16:26:26.879 My Connections\netgear - Discarding IPSec SA negotiation
 2-21: 16:26:26.895 My Connections\netgear - Discarding IKE SA negotiation
 2-21: 16:26:26.895 My Connections\netgear - Deleting IKE SA (IP ADDR=44.2.2.2)
 2-21: 16:26:26.895 My Connections\netgear -   MY COOKIE b1 2d 5c c8 4f ba 14 1a
 2-21: 16:26:26.895 My Connections\netgear -   HIS COOKIE 33 de 7c 5f 3c ff b1 aa
 2-21: 16:26:26.895 My Connections\netgear - SENDING>>>> ISAKMP OAK INFO *(HASH, DEL)
```

12. Conclusion

The Avaya VPNremote Phone and Phone Manager Pro combined with NETGEAR FVX538 ProSafe VPN Firewall and NETGEAR ProSafe VPN client provide a secure solution for remote worker telephony over broadband Internet connection.

13. Definitions and Abbreviations

The following terminology is used throughout this document.

DHCP	Dynamic Host Configuration Protocol
IKE	Internet Key Exchange (An IPSec control protocol)
ISAKMP	Internet Security Association and Key Management Protocol
IPSec	Internet Protocol Security
MD5	Message Digest 5
NAT	Network Address Translation
PFS	Perfect Forward Secret
Phase 1	IKE negotiations used to create an ISAKMP security association.
Phase 2	IKE negotiations used to create IPSec security associations.
RTP	Real-Time Transport Protocol
SA	Security Association
SHA-1	Secure Hash Algorithm 1
VPN	Virtual Private Network

14. References

Avaya Application Notes and Resources Web Site:

http://www.avaya.com/gcm/master-usa/en-us/resource/index.htm

Avaya Product Support Web Site:

http://support.avaya.com/japple/css/japple?PAGE=Home

[1] ***Application Notes for Converting an Avaya 4600 Series IP Telephone to an Avaya VPNremote Phone – Issue 1.0***.

[2] ***Avaya VPNremote for the 4600 Series IP Telephones Release 2.1 Administrator Guide***, Doc ID: 19-600753, Issue 3, June 2007

[3] ***Administrators Guide for Avaya IP Office***, Doc ID: 39DHB0002UKAA, October 2007.

[4] ***IP Office 4.1 Phone Manager User Guide***, Doc ID: 15-600988 Issue 16c, October, 2007.

NETGEAR Product Support Web Site:

http://www.netgear.com

[5] ***NETGEAR FVX538 ProSafe VPN Firewall 200 Installation Guide***, 201-10595-02, June 2006.

[6] ***NETGEAR FVX538 ProSafe VPN Firewall 200 Reference Manual***, v1.0, 202-10062-04, August 2006.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.