



## **Configuring the Juniper SSG 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 Juniper Secure Services Gateway 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 worker 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 at the Avaya Solution and Interoperability Test Lab at the request of the Solutions Marketing Team.

## Table of Contents

<b>1. Introduction.....</b>	<b>4</b>
1.1. Avaya VPNremote Phone for remote IP Office users .....	4
1.2. Avaya Phone Manager Pro (in Telecommuter mode) .....	4
1.3. Juniper Secure Services Gateway 5 (SSG5) .....	5
<b>2. Network Topology.....</b>	<b>6</b>
<b>3. Equipment and Software Validated .....</b>	<b>8</b>
<b>4. IP Office Configuration.....</b>	<b>8</b>
<b>5. Juniper SSG 5 Configuration .....</b>	<b>18</b>
5.1. Access SSG 5 .....	18
5.2. Configure Juniper SSG Ethernet Interfaces .....	19
5.3. IP Address Pool.....	22
5.4. Routes .....	23
5.4.1. Configure Default Route .....	23
5.4.2. Configure Route to IP Pool Address range .....	24
5.5. Local User Configuration .....	25
5.5.1. IKE User for VPNremote Phone.....	26
5.5.2. IKE User for Juniper NetScreen-Remote .....	27
5.5.3. XAuth User .....	28
5.6. Local User Group Configuration .....	29
5.6.1. IKE User Group for VPNremote Phone .....	29
5.6.2. IKE User Group for Juniper NetScreen-Remote .....	30
5.6.3. XAuth User Group .....	30
5.7. VPN.....	32
5.7.1. AutoKey IKE Gateway Configuration – Phase 1 .....	32
5.7.2. AutoKey IKE VPN Tunnel Configuration – Phase 2 .....	36
5.8. XAuth Configuration .....	40
5.8.1. XAuth Server Defaults.....	40
5.8.2. Enable XAuth Authentication for AutoKey IKE gateway for VPNremote Phone.....	41
5.8.3. Enable XAuth Authentication for AutoKey IKE gateway for Juniper NetScreen-Remote VPN Client .....	42
5.9. H.323 ALG .....	43
5.10. Security Policies.....	43
<b>6. Avaya VPNremote Phone Configuration.....</b>	<b>46</b>
6.1. Avaya VPNremote Phone Firmware .....	46
6.2. Configuring Avaya VPNremote Phone .....	46
<b>7. Juniper NetScreen – Remote VPN Client Configuration.....</b>	<b>50</b>
<b>8. Phone Manager Pro Configuration.....</b>	<b>56</b>
<b>9. Verification .....</b>	<b>58</b>
9.1. VPNremote Phone Qtest .....	58
9.2. VPNremote Phone IPSec stats .....	58
9.3. Juniper SSG Debug and Logging .....	59
9.4. Juniper NetScreen-Remote Log Viewer .....	61

<b>10.</b>	<b>Testing.....</b>	<b>61</b>
<b>11.</b>	<b>Troubleshooting .....</b>	<b>62</b>
11.1.	Incorrect User Name or Password .....	62
11.2.	Mismatched Phase 1 Proposal .....	62
11.3.	Mismatched Phase 2 Proposal .....	63
<b>12.</b>	<b>Conclusion .....</b>	<b>64</b>
<b>13.</b>	<b>Definitions and Abbreviations .....</b>	<b>65</b>
<b>14.</b>	<b>References.....</b>	<b>65</b>

# 1. Introduction

These Application Notes describe the steps for configuring the Juniper Secure Services Gateway for Avaya IP Office to support Avaya VPNremote Phone and Phone Manager Pro. Steps for configuring the Juniper Secure Services Gateway 5 Security Platform 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 sample configuration presented in these Application Notes utilizes a shared IKE Group ID to streamline the VPN configuration and management, IP Network Region segmentation to logically group and administer VPNremote Phones and NAT-T for IPSec traversal of Network Address Translation devices.

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)**
- **Juniper Secure Services Gateway 5**
- **Juniper NetScreen – Remote Windows 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 IP 4600 or 5600 Series 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 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 their calls routed to a telephone number they specify 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 logged in to Phone Manager as a telecommuter, the internal IP Office extension is logged off.

Juniper NetScreen-Remote Windows VPN client is used by the remote user to securely connect to the corporate IP network for telephony and data access.

### 1.3. Juniper Secure Services Gateway 5 (SSG5)

The sample network provided in these Application Notes implements the following features of the Juniper SSG 5:

- **Policy-Based IPSec VPN**

The policy-based VPN feature of the Juniper SSG 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. Because no network exists beyond a VPN client end-point, policy-based VPN tunnels are a good choice for VPN end-point configurations such as with the Avaya VPNremote Phone and Juniper NetScreen-Remote Windows VPN Client.

- **XAuth User Authentication**

The XAuth protocol enables the Juniper SSG to authenticate the individual users of the VPNremote Phone and Phone Manager Pro. 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 Juniper SSG authenticates the Avaya VPNremote Phone and Juniper NetScreen-Remote Windows VPN Client by matching the IKE ID and pre-shared key sent by the Avaya VPNremote Phone and Juniper NetScreen-Remote Windows VPN Client. If there is a match, the Juniper SSG XAuth process begins.

**Step 2. XAuth:** the Juniper SSG XAuth server prompts the Avaya VPNremote Phone and Juniper NetScreen-Remote Windows VPN Client 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 Juniper SSG appliance to dynamically assign IP addresses from a configured IP Address pool range.

- **Shared IKE Group ID**

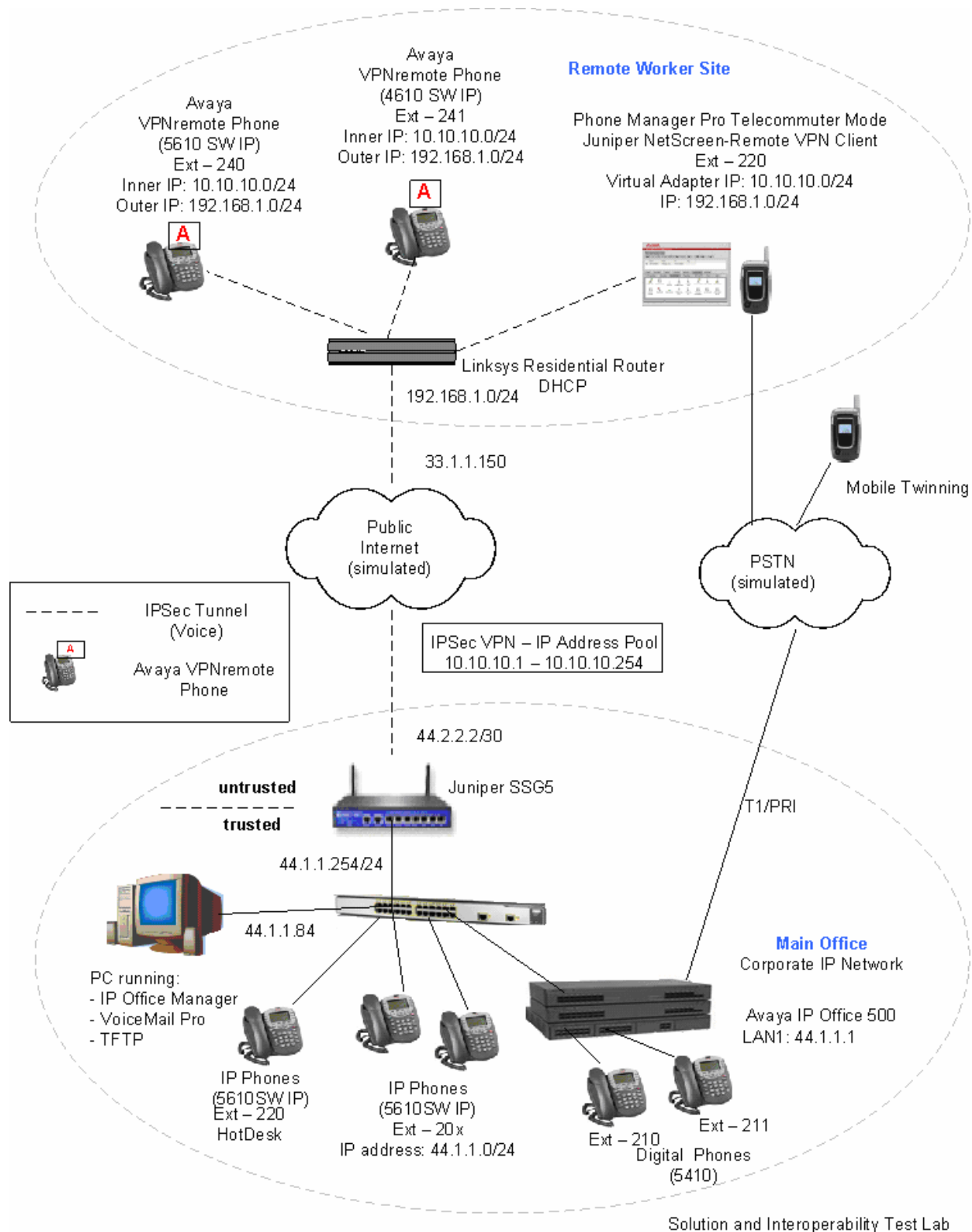
The shared IKE ID feature of the Juniper SSG appliance facilitates the deployment of a large number of dialup IPSec VPN users. With this feature, the security device authenticates multiple dialup VPN users using a single group IKE ID and pre-shared key. Thus, it provides IPSec protection for large remote user groups through a common VPN configuration. XAuth user authentication must be used when implementing Shared IKE Group ID.

## 2. Network Topology

The sample network implemented for these Application Notes is shown in **Figure 1**. The Corporate IP Network location contains the Juniper Secure Services Gateway 5 (SSG5) functioning as a perimeter security device and VPN head-end. The Corporate IP Network also has the Avaya IP Office 500 and the 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 SSG5. The SSG5 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 SSG5. The Juniper NetScreen-Remote Windows 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 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
Juniper Secure Services Gateway 5	6.0.0r3.0 (Firewall + VPN)
Linksys Wireless- G VPN Broadband Router	2.39.2
Juniper NetScreen – Remote Windows VPN Client	Build 10 10.8.1

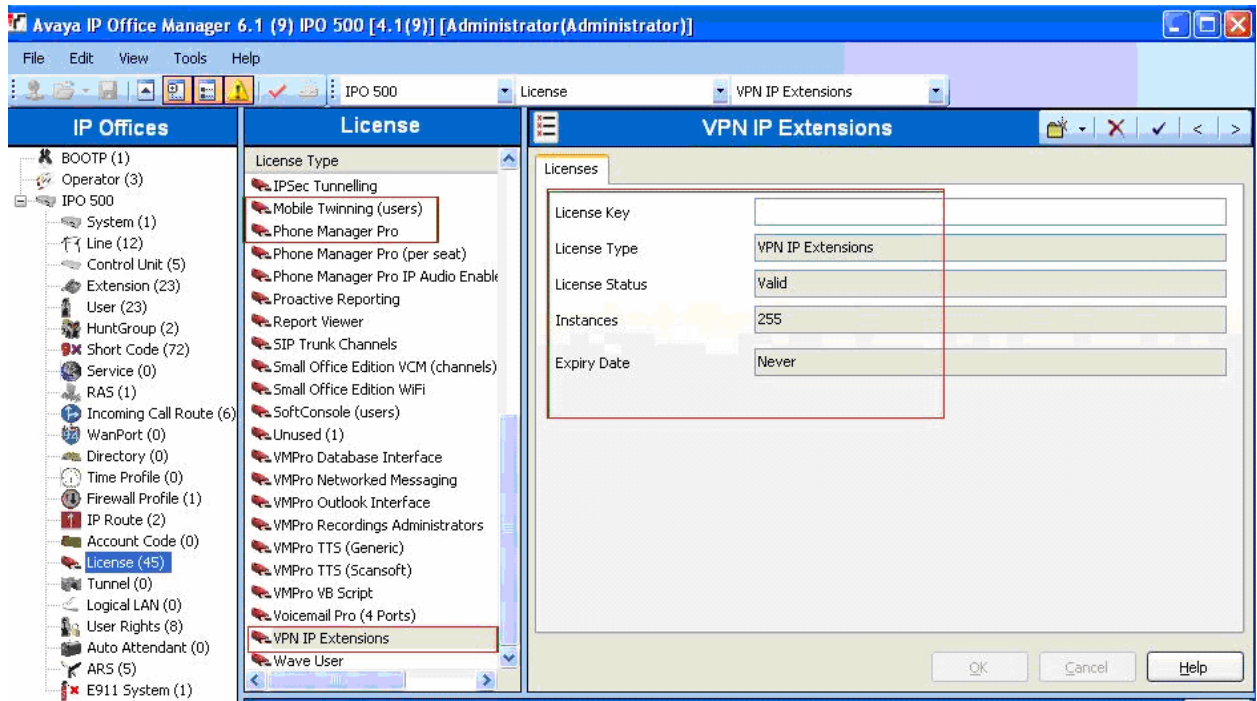
### 4. IP Office Configuration

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].

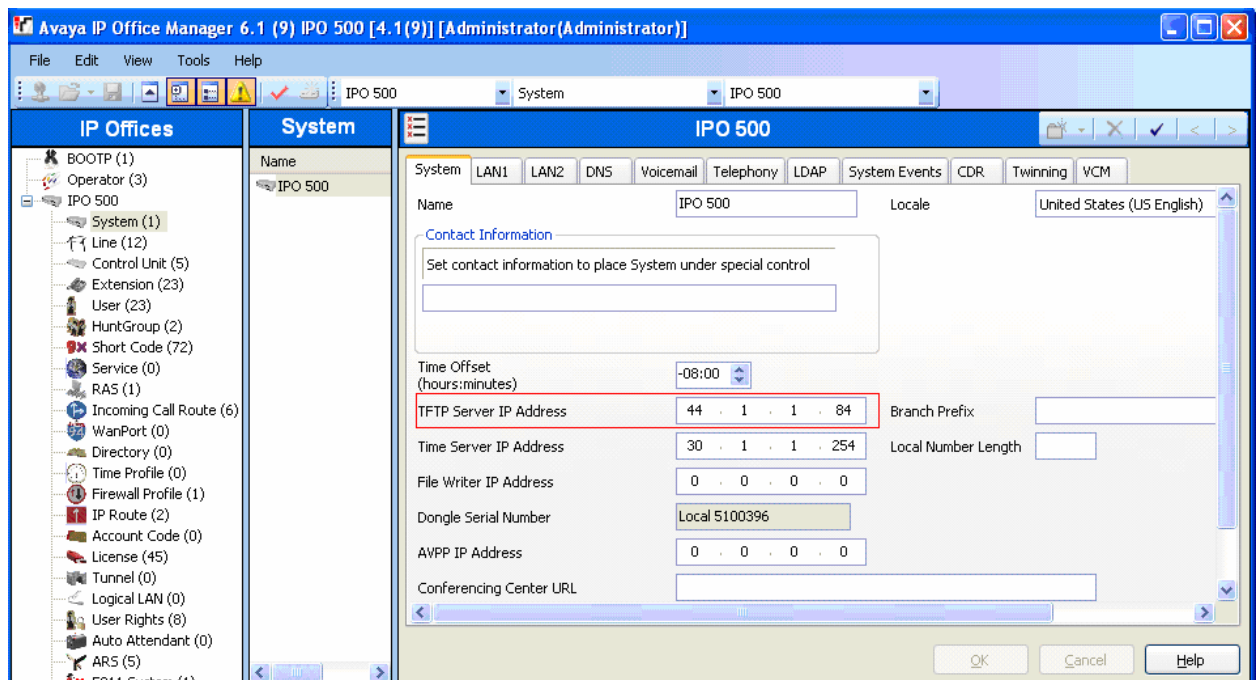
Log into the IP Office Manager PC and select **Start** → **Programs** → **IP Office** → **Manager** to launch the Manager application. Log into the Manager application using the appropriate credentials.

1. *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 they are not valid, contact your Avaya sales team or business partner.

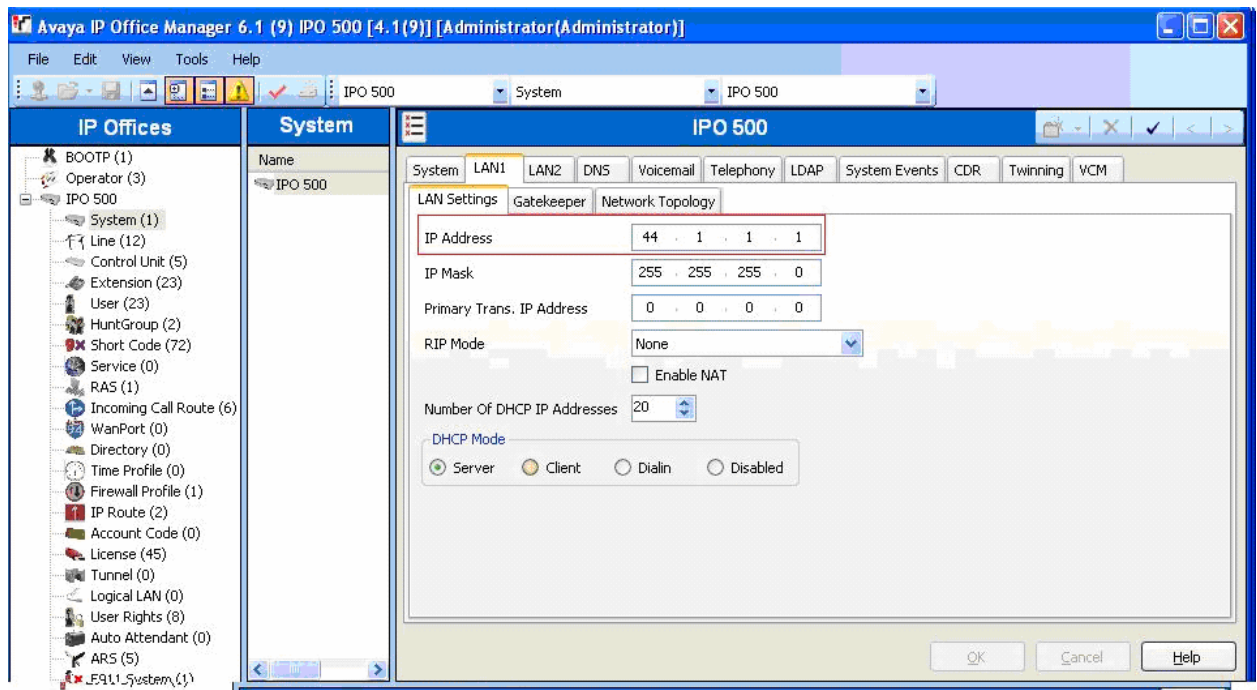




2. *Verify the TFTP Server IP Addresses.* In IP Office Manager, select **System** in the left panel. Double-click on **System**. Verify the **TFTP Server IP Address** in the right hand panel **System** Tab.

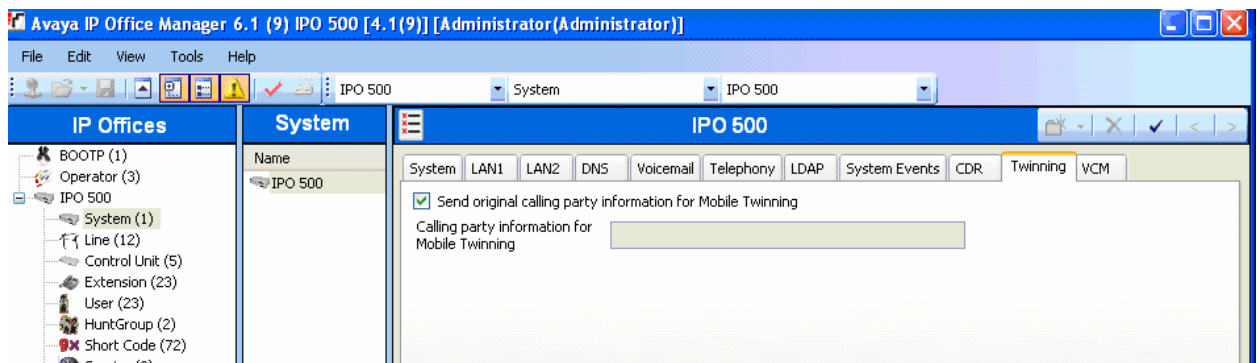


3. *Verify the IP Addresses.* In IP Office Manager, select **System** in the left panel. Double-click on **System**. Verify the **IP Address** in the right hand panel **LAN1 → LAN Settings** Tab.




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.



5. *Configure an extension for the VPN remote Phone.* An Avaya VPNremote Phone is administered the same as other Avaya IP telephones within Avaya IP Office. Even

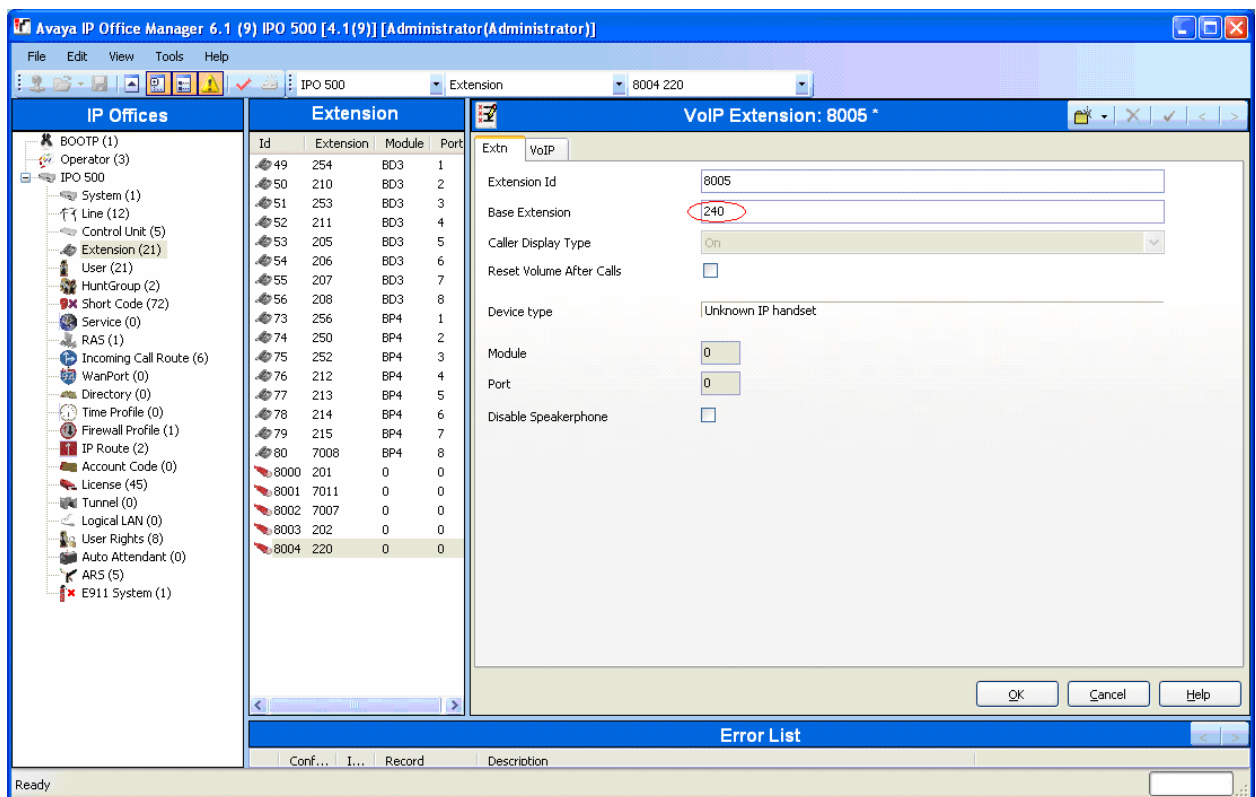
though the Avaya VPNremote Phone is physically located outside of the corporate network, the Avaya VPNremote Phone will behave the same as other Avaya IP telephones located locally on the corporate LAN once the VPN tunnel has been established.

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**.

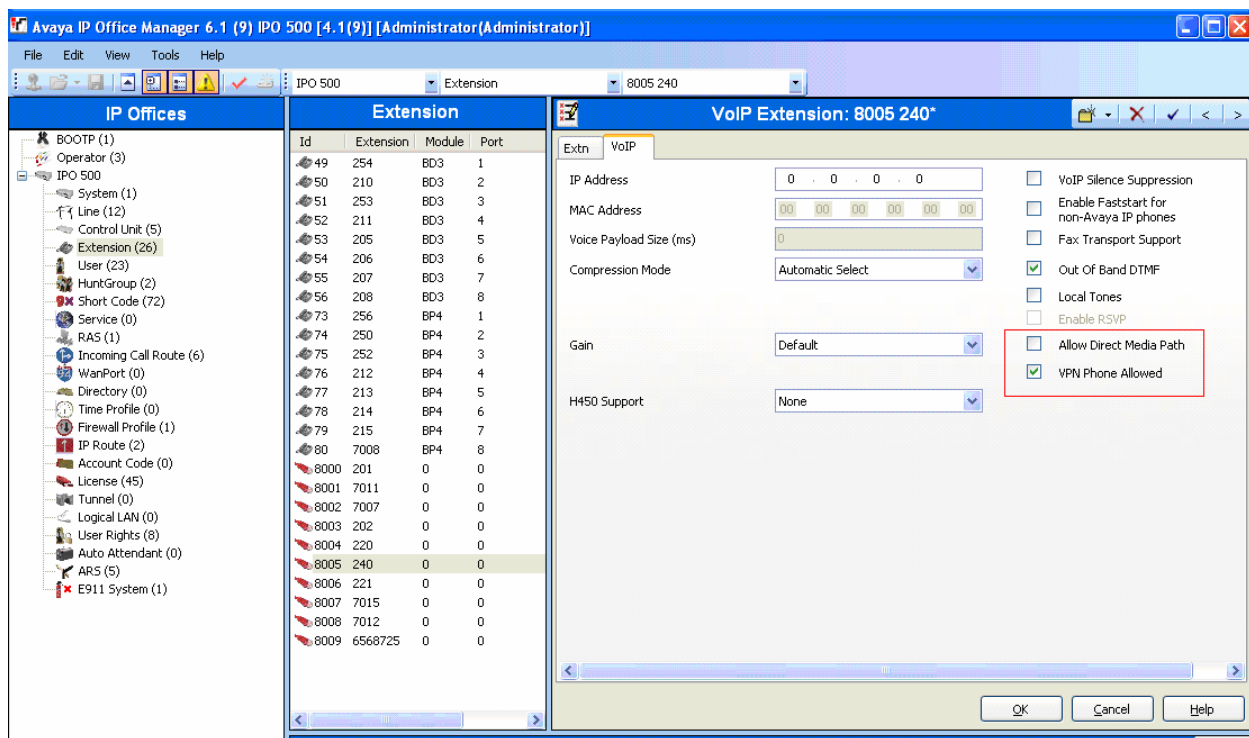
The **VoIP Extension** screen will appear in the right panel.

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



In the **VoIP** Tab:

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



Press the **OK** button.

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

In the right panel, click on **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**.

Avaya IP Office Manager 6.1 (9) IPO 500 [4.1(9)] [Administrator/Administrator]

File Edit View Tools Help

IPO 500 User 240 Extn240

**IP Offices**

- BOOTP (1)
- Operator (3)
- IPO 500
  - System (1)
  - Line (12)
  - Control Unit (5)
  - Extension (26)
  - User (23)
  - HuntGroup (2)
  - Short Code (72)
  - Service (0)
  - RAS (1)
  - Incoming Call Route (6)
  - WanPort (0)
  - Directory (0)
  - Time Profile (0)
  - Firewall Profile (1)
  - IP Route (2)
  - Account Code (0)
  - License (45)
  - Tunnel (0)
  - Logical LAN (0)
  - User Rights (8)
  - Auto Attendant (0)
  - ARS (5)
  - E911 System (1)

**User**

Name	Extension
Extn201	201
Extn202	202
Extn205	205
Extn206	206
Extn207	207
Extn208	208
Extn210	210
Extn211	211
Extn212	212
Extn213	213
Extn214	214
Extn215	215
Extn220	220
Extn221	221
Extn240	240
Extn253	253
Extn254	254
Extn256	256
Extn7007	7007
Extn7008	7008
Extn7011	7011
NoUser	
RemoteManager	

**Extn240: 240\***

Button Programming Menu Programming Twinning T3 Options Phone Manager Options Hunt Group Membership

Announcements SIP

User Voicemail DND ShortCodes Source Numbers Telephony Forwarding Dial In Voice Recording

Name: VPNUser240

Password:

Confirm Password:

Full Name:

Extension: 240

Locale:

Priority: 5

☐ Ex Directory

Device Type: Unknown

**User Rights**

User Rights view: User data

Working hours time profile: <None>

Working hours User Rights:

Out of hours User Rights:

OK Cancel Help

In the **Voicemail** Tab, check the **Voicemail On** and enter the **Voicemail Code**.

Avaya IP Office Manager 6.1 (9) IPO 500 [4.1(9)] [Administrator/Administrator]

File Edit View Tools Help

IPO 500 User 240 Extn240

**IP Offices**

- BOOTP (1)
- Operator (3)
- IPO 500
  - System (1)
  - Line (12)
  - Control Unit (5)
  - Extension (26)
  - User (23)
  - HuntGroup (2)
  - Short Code (72)
  - Service (0)
  - RAS (1)
  - Incoming Call Route (6)
  - WanPort (0)
  - Directory (0)
  - Time Profile (0)
  - Firewall Profile (1)
  - IP Route (2)
  - Account Code (0)
  - License (45)
  - Tunnel (0)
  - Logical LAN (0)
  - User Rights (8)
  - Auto Attendant (0)
  - ARS (5)
  - E911 System (1)

**User**

Name	Extension
Extn201	201
Extn202	202
Extn205	205
Extn206	206
Extn207	207
Extn208	208
Extn210	210
Extn211	211
Extn212	212
Extn213	213
Extn214	214
Extn215	215
Extn220	220
Extn221	221
Extn240	240
Extn253	253
Extn254	254
Extn256	256
Extn7007	7007
Extn7008	7008
Extn7011	7011
NoUser	
RemoteManager	

**Extn240: 240\***

Announcements SIP

Button Programming Menu Programming Twinning T3 Options Phone Manager Options Hunt Group Membership

User Voicemail DND ShortCodes Source Numbers Telephony Forwarding Dial In Voice Recording

Voicemail Code: \*\*\*\*\*

Confirm Voicemail Code: \*\*\*\*\*

Voicemail Email:

☒ Voicemail On

☐ Voicemail Help

☐ Voicemail Ringback

☐ Voicemail Email Reading

**Voicemail Email**

☒ Off ☐ Copy ☐ Forward ☐ Alert

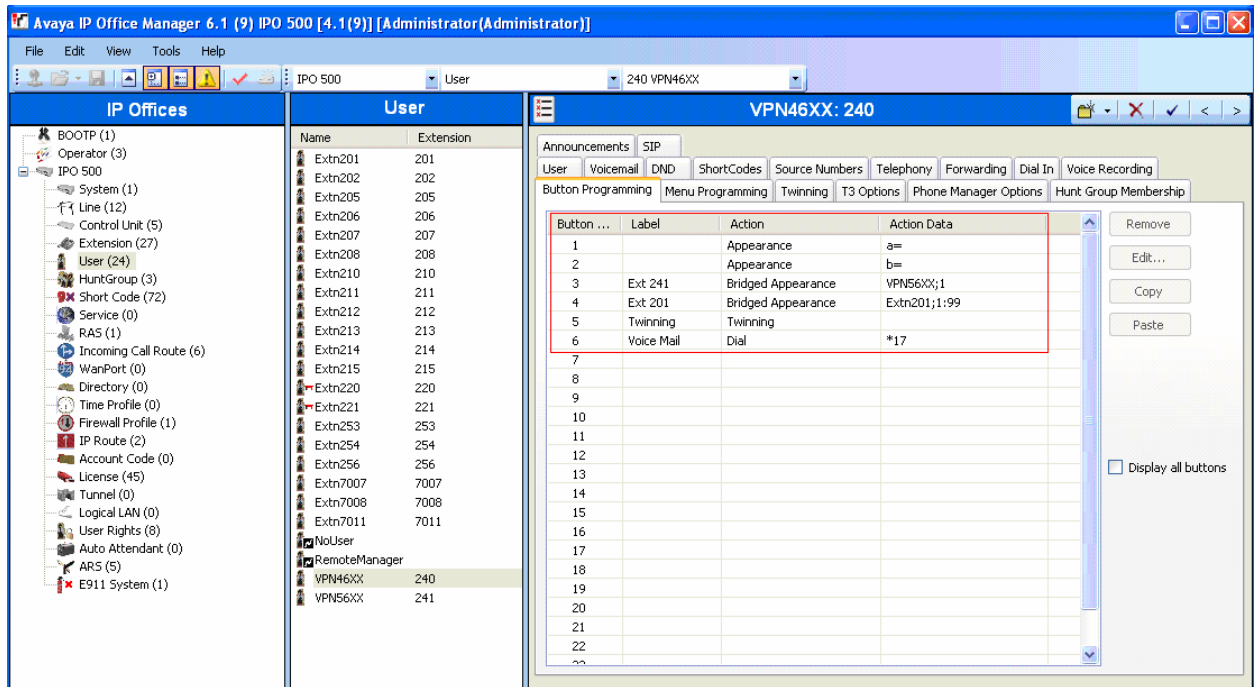
Reception / Breakout (DTMF 0):

Breakout (DTMF 2):

Breakout (DTMF 3):

OK Cancel Help

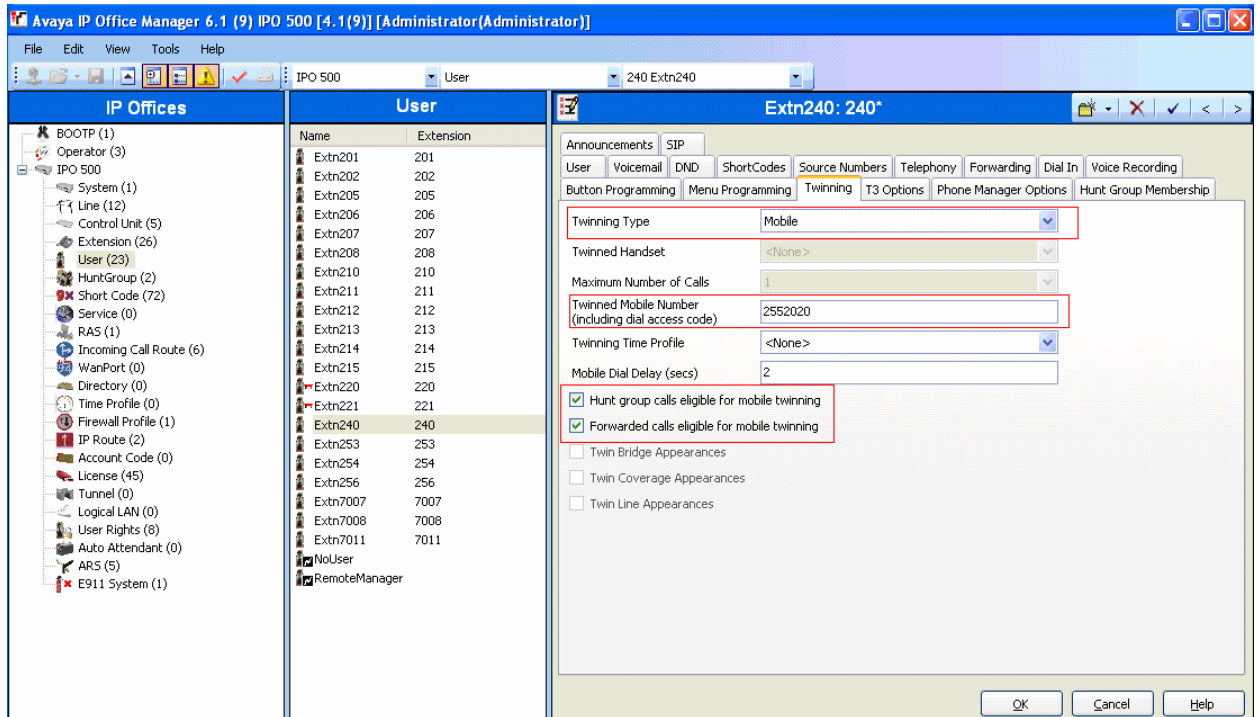
In the **Button Programming** Tab, program the buttons as needed. Shown below is a sample used in these Application Notes.



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**
- Enable **Forwarded calls eligible for mobile twinning**





Press the **OK** button.

7. *Configure an extension for the 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**.


**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:

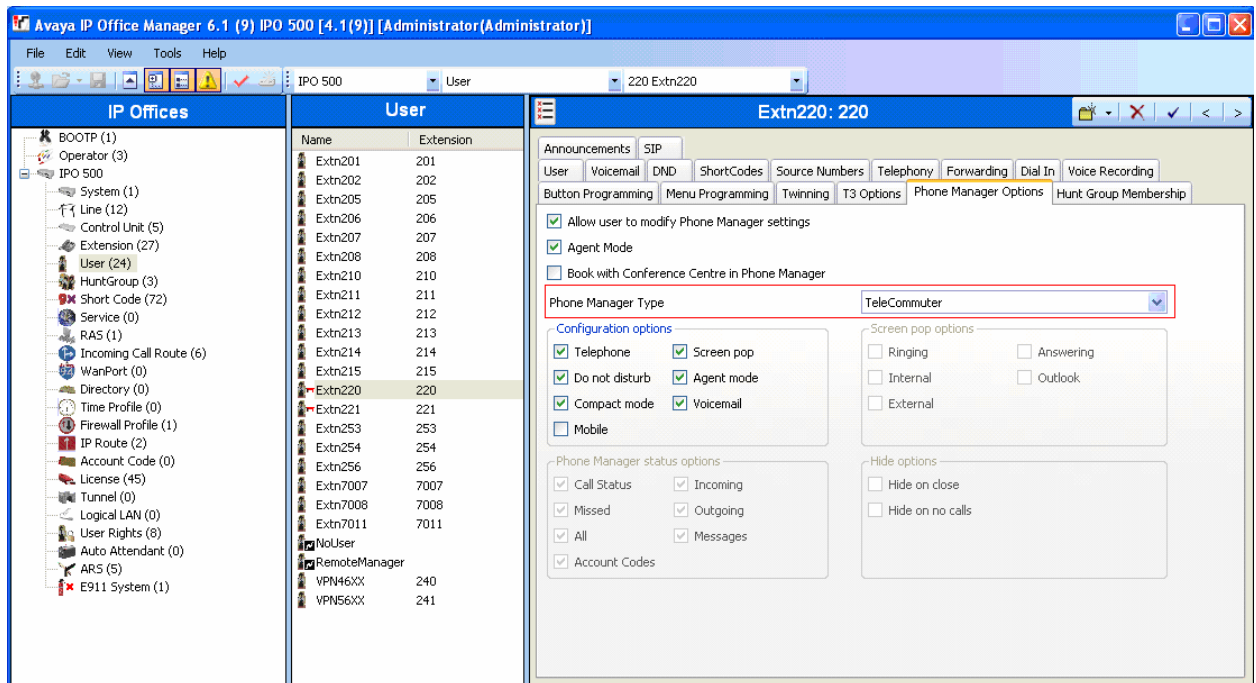
- Accept the default values.

Press the **OK** button.

8. *Configure a user for the Phone Manager Pro.* In IP Office Manager, select **User** in the left panel. In the right panel, click on **Create a New Record** icon . From the pull down menu, select **User**.

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

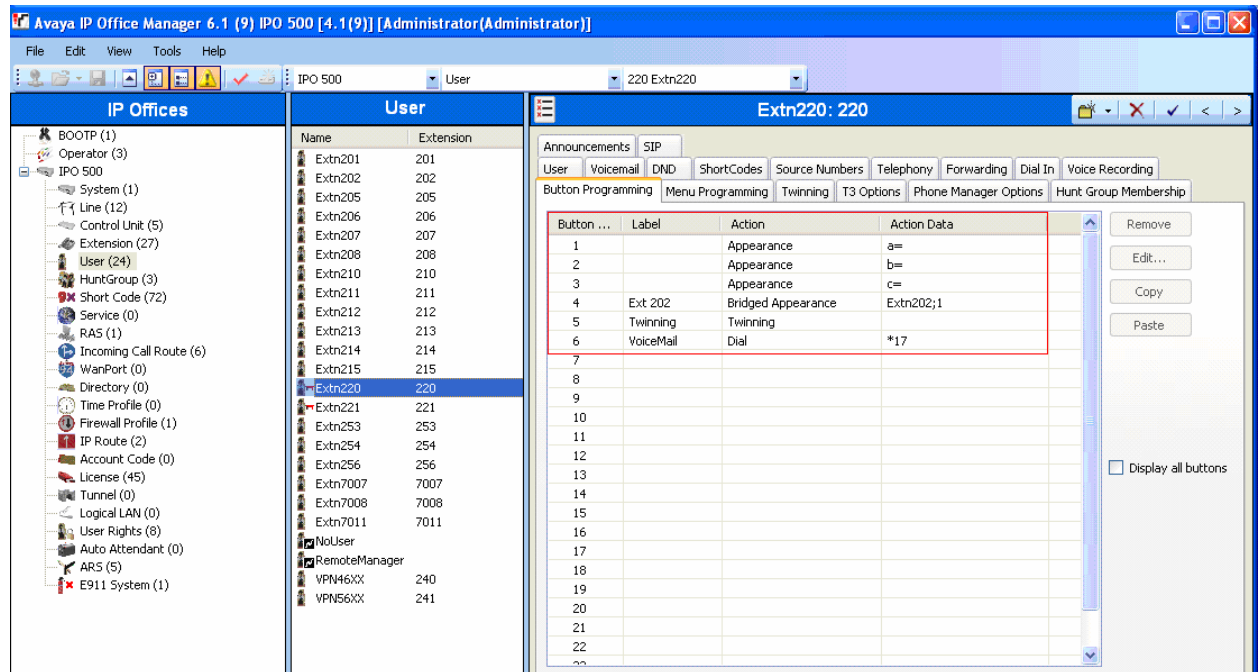
In the **Phone Manager Options** Tab, select the Phone Manager Type as **Telecommuter**.




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



In the **Button Programming** Tab, program the buttons as needed. Shown below is a sample used in these Application Notes.



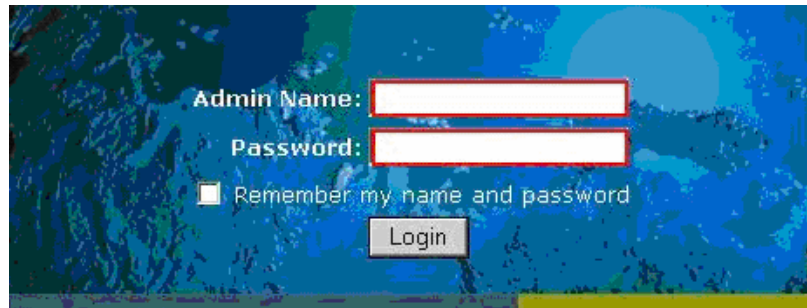
Note: The Users configured with Phone Manager Telecommuter option will have  in the left panel next to the User Name. This denotes a Hot Desk user. The Phone Manager User has an internal IP Office extension. While logged in to Phone Manager as a telecommuter, the internal IP Office extension is logged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

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

## 5. Juniper SSG 5 Configuration

### 5.1. Access SSG 5

1. From a web browser, enter the URL of the Juniper SSG WebUI management interface, <https://<IP address of the SSG>>, and the following login screen appears. Log in using a user name with administrative privileges.

The image shows the login interface of the Juniper SSG WebUI. It features a blue background with a subtle pattern. The login form is centered and includes the following elements: a label 'Admin Name:' followed by a text input field; a label 'Password:' followed by a text input field; a checkbox labeled 'Remember my name and password'; and a 'Login' button below the password field.

2. The Juniper SSG WebUI administration home page appears upon successful login. Note the ScreenOS Firmware Version.

My ssg5-serial-wlan	
Hardware Version:	710(0)
Firmware Version:	6.0.0r3.0 (Firewall+VPN)
Serial Number:	0162062006000005
Host Name:	ssg5-serial-wlan

## 5.2. Configure Juniper SSG Ethernet Interfaces

The steps below configured ethernet 0/0 to an Untrust security zone facing the public internet and bgroup0 to a Trust security zone facing the internal corporate network. The Avaya VPNremote Phone and Juniper NetScreen-Remote VPN Client will interact with ethernet 0/0 when establishing an IPSec Tunnel.

### Configure ethernet 0/0:

1. From the left navigation menu, select **Network > Interfaces**.  
The **Network Interfaces List** screen appears. The IP address is already populated for ethernet0/0. Select **Edit** for ethernet 0/0 to configure additional parameters.

Name	IP/Netmask	Zone	Type	Link	PPPoE	Configure
bgroup0	44.1.1.254/24	Trust	Layer3	Up	-	<a href="#">Edit</a>
ethernet0/2				Up	-	<a href="#">Edit</a>
ethernet0/3				Down	-	<a href="#">Edit</a>
ethernet0/4				Down	-	<a href="#">Edit</a>
ethernet0/5				Down	-	<a href="#">Edit</a>
ethernet0/6				Down	-	<a href="#">Edit</a>
bgroup1	0.0.0.0/0	Null	Unused	Down	-	<a href="#">Edit</a>
bgroup2	0.0.0.0/0	Null	Unused	Down	-	<a href="#">Edit</a>
bgroup3	0.0.0.0/0	Null	Unused	Down	-	<a href="#">Edit</a>
ethernet0/0	44.2.2.2/24	Untrust	Layer3	Up	-	<a href="#">Edit</a>
ethernet0/1	0.0.0.0/0	DMZ	Layer3	Down	-	<a href="#">Edit</a>
serial0/0	0.0.0.0/0	Null	Unused	Down	-	<a href="#">Edit</a>
vlan1	0.0.0.0/0	VLAN	Layer3	Down	-	<a href="#">Edit</a>
wireless0/0	192.168.2.1/24	Trust	Layer3	Up	-	<a href="#">Edit</a> <a href="#">Deactivate</a>
wireless0/1	0.0.0.0/0	Null	Unused	Down	-	<a href="#">Edit</a>
wireless0/2	0.0.0.0/0	Null	Unused	Down	-	<a href="#">Edit</a>
wireless0/3	0.0.0.0/0	Null	Unused	Down	-	<a href="#">Edit</a>

2. From the ethernet 0/0 properties page, configure the highlighted fields shown below. All remaining fields can be left as default. Select **OK** to save.

Because ethernet0/0 is in the Untrust zone and not configured as manageable, all service options are disabled.

Interface Name ethernet0/0 0014.f69b.aec0

Zone Name **Untrust**

☐ Obtain IP using DHCP
 ☐ Automatic update DHCP server parameters

☐ Obtain IP using PPPoE
 **None** [Create new pppoe setting](#)

☒ **Static IP**

IP Address / Netmask **44.2.2.2** / **24** ☐ Manageable  
 Manage IP \* **44.2.2.2** 0014.f69b.aec0

Interface Mode ☐ NAT ☒ **Route**

Block Intra-Subnet Traffic ☐

**Service Options**

Management Services ☐ Web UI ☐ Telnet ☐ SSH  
☐ SNMP ☐ SSL

Other Services ☐ Ping ☐ Path MTU(IPv4) ☐ Ident-reset

Maximum Transfer Unit(MTU) Admin MTU **0** Bytes (Operating MTU: 1500; Default MTU: 1500)

DNS Proxy ☐

NTP Server ☐

WebAuth ☐ IP Address **0.0.0.0** ☐ SSL Only

Traffic Bandwidth Egress Maximum Bandwidth **0** Kbps  
 Ingress Maximum Bandwidth **0** Kbps

## Configure bgroup0 Interface:

- From the **Network Interfaces List** screen, select **Edit** for bgroup0

Name	IP/Netmask	Zone	Type	Link	PPPoE	Configure
bgroup0	44.1.1.254/24	Trust	Layer3	Up	-	<a href="#">Edit</a>
ethernet0/2				Up	-	<a href="#">Edit</a>
ethernet0/3				Down	-	<a href="#">Edit</a>
ethernet0/4				Down	-	<a href="#">Edit</a>
ethernet0/5				Down	-	<a href="#">Edit</a>
ethernet0/6				Down	-	<a href="#">Edit</a>
bgroup1	0.0.0.0/0	Null	Unused	Down	-	<a href="#">Edit</a>
bgroup2	0.0.0.0/0	Null	Unused	Down	-	<a href="#">Edit</a>
bgroup3	0.0.0.0/0	Null	Unused	Down	-	<a href="#">Edit</a>
ethernet0/0	44.2.2.2/24	Untrust	Layer3	Up	-	<a href="#">Edit</a>

2. From the bgroup0 properties page, configure the highlighted fields shown below. All remaining fields can be left as default. Select **OK** to save.

bgroup0 connects to the private corporate network making it a trusted interface. It is placed in the **Trust** security zone of the Juniper SSG. In the **Service Options** enable **Management Services** and **Other Services** as shown below.

Interface Name bgroup0 0014.f69b.aecb

Zone Name Trust

☐ Obtain IP using DHCP ☐ Automatic update DHCP server parameters

☐ Obtain IP using PPPoE None [Create new pppoe setting](#)

☒ Static IP

IP Address / Netmask 44.1.1.254 / 24 ☒ Manageable

Manage IP \* 44.1.1.254 0014.f69b.aecb

Interface Mode ☐ NAT ☒ Route

Block Intra-Subnet Traffic ☐

Service Options

Management Services ☒ Web UI ☒ Telnet ☒ SSH

☒ SNMP ☒ SSL

Other Services ☒ Ping ☐ Path MTU(IPv4) ☐ Ident-reset

Maximum Transfer Unit(MTU) Admin MTU 0 Bytes (Operating MTU: 1500; Default MTU: 1500)

DNS Proxy ☐

NTP Server ☐

WebAuth ☐ IP Address 0.0.0.0 ☐ SSL Only

Traffic Bandwidth Egress Maximum Bandwidth 0 Kbps

Ingress Maximum Bandwidth 0 Kbps

OK Apply Cancel

### 5.3. IP Address Pool

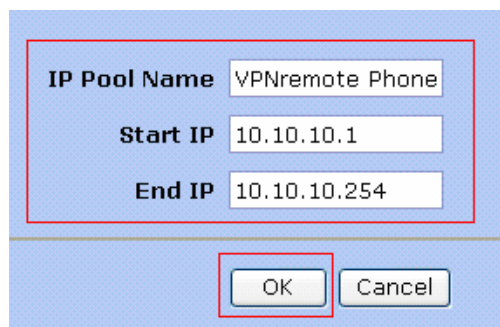
The XAuth protocol enables the Juniper SSG to dynamically assign IP addresses from a configured IP Address pool range to IPSec clients such as the Avaya VPNremote Phone and Juniper NetScreen-Remote Windows VPN Client.

The following steps create the IP Address Pool:

1. From the left navigation menu, select **Objects > IP Pools**.  
On the IP Pools list page, select **New**.
2. From the IP Pools Edit page, populate the highlighted fields shown below then select **OK** to save.

The **IP Pool Name** is a descriptive name for this IP Pool. Once configured, this name will appear in the **IP Pool Name** drop-down menu of **Section 5.8.1**.

Ensure the IP address range does not conflict with addresses used throughout the corporate trusted network.



3. The IP Pools list page displays the new address pool entry.

Name	Start IP	End IP	In use	Configure	
VPNremote Phone	10.10.10.1	10.10.10.254	0	<a href="#">Edit</a>	<a href="#">Remove</a>



## 5.4. Routes

The sample configuration requires a default route entry be added to the Juniper SSG routing table.

### 5.4.1. Configure Default Route

1. From the left navigation menu, select **Network > Routing > Destination**  
The Route Entries screen similar to the one below appears.

Select **trust-vr** from drop down menu then **New**

List 20 per page  
List route entries for All virtual routers

trust-vr

	IP/Netmask	Gateway	Interface	Protocol	Preference	Metric	Vsys	Configure
*	44.2.2.0/24		ethernet0/0	C			Root	-
*	44.2.2.2/32		ethernet0/0	H			Root	-
*	192.168.2.0/24		wireless0/0	C			Root	-
*	192.168.2.1/32		wireless0/0	H			Root	-
*	44.1.1.0/24		bgroup0	C			Root	-
*	44.1.1.254/32		bgroup0	H			Root	-

\* Active route   C Connected   I Imported   eB EBGP   O OSPF   E1 OSPF external type 1 H Host Route  
P Permanent   S Static   A Auto-Exported   iB IBGP   R RIP   E2 OSPF external type 2  
D Dynamic   N NHRP

2. Configure the highlighted fields shown below. All remaining fields can be left as default. Select **OK** to save.

The 0.0.0.0/0 network indicates the default route when no other matches existing in the routing table. The route is going to the next hop out interface ethernet 0/0 to the public Internet.

Virtual Router Name trust-vr

IP Address/Netmask 0.0.0.0 / 0

Next Hop ☐ Virtual Router ☒ Gateway

Virtual Router: untrust-vr

Interface ethernet0/0

Gateway IP Address 44.2.2.1

Permanent ☒

Tag 0

Metric 1

Preference 20

OK Cancel

## 5.4.2. Configure Route to IP Pool Address range

1. From the Route Entries screen, select **trust-vr** from the drop down menu then select **New**.
2. Configure the highlighted fields shown below. All remaining fields can be left as default. Select **OK** to save.
  - The **IP Address / Netmask** is the network used for the IP Address Pool in **Section 5.3**.
  - The **Gateway IP Address** specifies the next hop route of the Trusted corporate network. In the sample configuration, it is the IP address of the Avaya IP Office.

The screenshot displays the configuration interface for a Virtual Router named 'trust-vr'. The 'IP Address/Netmask' field is set to '10.10.10.1 / 24'. The 'Next Hop' section has 'Virtual Router' selected, with 'untrust-vr' chosen from the dropdown. The 'Gateway' option is selected, and its configuration box shows 'Interface' as 'bgroup0', 'Gateway IP Address' as '44.1.1.1', 'Permanent' checked, and 'Tag' as '0'. The 'Metric' is set to '1' and 'Preference' to '20'. The 'OK' button is highlighted with a red box.

Virtual Router Name	trust-vr
IP Address/Netmask	10.10.10.1 / 24
Next Hop	<input type="radio"/> Virtual Router <input type="radio"/> Gateway
Virtual Router	untrust-vr
Gateway	<div>Interface: bgroup0 Gateway IP Address: 44.1.1.1 Permanent: <input checked="" type="checkbox"/> Tag: 0</div>
Metric	1
Preference	20
<div>OK Cancel</div>	



## 5.5. Local User Configuration

There are two different user types: IKE users and XAuth users.

IKE users are typically associated with a device such as the Avaya VPNremote Phone and are used to authenticate the actual device during the establishment of the IPSec tunnel. For the sample configuration two IKE users will be created, one for Avaya VPNremote Phones and one for Juniper NetScreen-Remote Windows VPN Clients to support Phone Manager Pro.

XAuth users are remotely authenticated users who access a head-end security gateway via an AutoKey IKE VPN tunnel.

In the sample configuration, three groups are created:

- A XAuth group called remoteuser-grp containing all XAuth user accounts (tom, dick, harry). The XAuth group is associated with each “VPN”. **Section 5.8.2** describes steps for vpnphones. **Section 5.8.3** describes steps for netscreen-remote. This will allow the users like tom, dick and harry logins to be used by either the VPNremote Phones and Juniper NetScreen-Remote Windows VPN clients.
- An IKE group containing the IKE user vpnphone-ike used for VPNphone tunnels
- Another IKE group containing the IKE user Jane used for the netscreen-remote tunnels.

### 5.5.1. IKE User for VPNremote Phone

The following steps create an IKE user to be used by Avaya VPNremote Phones for IKE authentication.

1. From the left navigation menu, select **Objects > User > Local > New**.  
Configure the highlighted fields shown below. All remaining fields can be left as default. Select **OK** to save.
  - The **Number of Multiple Logins with Same ID** parameter specifies the number of end-points that can concurrently establish IPsec tunnels using this identity. This number must equal or exceed the number of Avaya VPNremote Phones accessing this Juniper SSG.
  - **IKE Identity**, combined with a Pre-Shared Key, is used to identify the end-point when an initial IKE Phase one dialog begins. The format of the IKE Identity used is of an email address. As described in **Step 2 of Section 6.2**, the Group Name field of the Avaya VPNremote Phone must match this IKE Identity string. **vpnphone@avaya.com** is used in these Application Notes however any email address string can be used.

Auth/IKE/XAuth/L2TP User

User Name: vpnphone-ike  
Status: ☒ Enable

Groups: vpnphone-grp  
☐ Disable

☒ IKE User  
☒ Simple Identity  
IKE ID Type: AUTO  
☐ Use Distinguished Name For ID

Number of Multiple Logins with Same ID: 25  
IKE Identity: vpnphone@avaya.com

☐ Authentication User  
☐ XAuth User  
☐ L2TP User

User Password:   
Confirm Password:

OK Cancel

2. The local Users list page displays the new IKE user:

Name	Type	Group	Status	Identity	Configure	
vpnphone-ike	IKE	-	Enabled	vpnphone@avaya.com	<a href="#">Edit</a>	<a href="#">Remove</a>

### 5.5.2. IKE User for Juniper NetScreen-Remote

The following steps create an IKE user to be used by Juniper NetScreen-Remote Windows VPN client for IKE authentication.

1. From the left navigation menu, select **Objects > User > Local > New**.  
Configure the highlighted fields shown below. All remaining fields can be left as default. Select **OK** to save.
  - The **Number of Multiple Logins with Same ID** parameter specifies the number of end-points that can concurrently establish IPsec tunnels using this identity.
  - **IKE Identity**, combined with a Pre-Shared Key, is used to identify the end-point when an initial IKE Phase one dialog begins. The format of the IKE Identity used is of an email address. As described in **Section 7 Step 2**, the **Email Address** field of the Juniper NetScreen-Remote Security Policy Editor must match this IKE Identity string.  
**vpn@avaya.com** is used in these Application Notes however any email address string can be used.

**Auth/IKE/XAuth/L2TP User**

**User Name** jane

**Status** ☒ Enable ☐ Disable

**Groups:** netscreen-remote-grp

☒ **IKE User**

☒ **Simple Identity**

**IKE ID Type** AUTO

☐ **Use Distinguished Name For ID**

**Number of Multiple Logins with Same ID** 25

**IKE Identity** vpn@avaya.com

☐ **Authentication User**

☐ **XAuth User**

☐ **L2TP User**

**User Password**

**Confirm Password**

**OK** **Cancel**

### 5.5.3. XAuth User

The XAuth server of the Juniper SSG provides the authentication of the XAuth users. Three XAuth user accounts – **tom**, **dick**, and **harry** are created in the sample configuration for users of the Avaya VPNremote Phones and Juniper NetScreen-Remote. The following steps create a user account for **tom**. Follow the same steps to create accounts for **dick** and **harry**.

The users of the Avaya VPNremote Phone will need to be supplied with their user name and password. Users will be prompted on the phone display to enter this information as the Avaya VPNremote Phone establishes the IPSec tunnel or the password can be stored in the VPNremote Phones flash memory, see **Section 6.2** for additional details.

In the sample configuration, XAuth users belong to both IKE User groups. This enables the users to use both VPNremote Phones and Juniper NetScreen-Remote Windows VPN client with the same user name and password.

1. From the left navigation menu, select **Objects > User > Local > New**. Configure the highlighted fields shown below. All remaining fields can be left as default. Select **OK** to save.

Follow the same steps for each additional user.

**Auth/IKE/XAuth/L2TP User**

User Name: tom

Status: ☒ Enable ☐ Disable

☐ IKE User Number of Multiple Logins with Same ID: 1

☐ Simple Identity

☐ Use Distinguished Name For ID

☐ Authentication User

☒ XAuth User

☐ L2TP User

User Password:

Confirm Password:

**L2TP/XAuth Remote Settings** ( Remote IP: 0.0.0.0 )

IP Pool: None

Static IP: 0.0.0.0

Primary DNS IP: 0.0.0.0

Primary WINS IP: 0.0.0.0

Secondary DNS IP: 0.0.0.0

Secondary WINS IP: 0.0.0.0

OK Cancel

2. The local Users list page displays the new XAuth users:

Name	Type	Group	Status	Identity
dick	XAuth	remoteuser-grp	Enabled	-
harry	XAuth	remoteuser-grp	Enabled	-
jane	IKE	netscreen-remote-grp	Enabled	vpn@avaya.com
tom	XAuth	remoteuser-grp	Enabled	-
vpnphone-ike	IKE	vpnphone-grp	Enabled	vpnphone@avaya.com

## 5.6. Local User Group Configuration

User groups have the benefit of being able to create one policy for the user group and that policy automatically applies to all members of a group. This eliminates the need to create policies for each individual user.

The sample configuration includes two different types of User Groups: IKE and XAuth. The IKE users and XAuth users created in **Section 5.5** must now be added to an IKE Group and an XAuth Group respectfully.

### 5.6.1. IKE User Group for VPNremote Phone

1. From the left navigation menu, select **Objects > User > Local Groups > New**.
  - Enter a descriptive **Group Name**.
  - Select the user name entered in **Section 5.5.1** from the **Available Members** column on the right.
  - Select the << icon to move the user name to the **Group Members** column on the left.
  - Select **OK** to save.

The screenshot shows a configuration window for creating a new local group. At the top, the 'Group Name' field is populated with 'vpnphone-grp'. Below this, there are two lists: 'Group Members' on the left and 'Available Members' on the right. The 'Group Members' list contains 'vpnphone-ike'. The 'Available Members' list contains 'tom', 'dick', and 'harry'. Between the two lists are two buttons: '<<' and '>>'. The '<<' button is highlighted with a red box. At the bottom of the window, there are 'OK' and 'Cancel' buttons, with the 'OK' button also highlighted by a red box.

## 5.6.2. IKE User Group for Juniper NetScreen-Remote

1. From the left navigation menu, select **Objects > User > Local Groups > New**.
  - Enter a descriptive **Group Name**.
  - Select the user name entered in **Section 5.5.2** from the **Available Members** column on the right.
  - Select the << icon to move the user name to the **Group Members** column on the left.
  - Select **OK** to save.

The screenshot shows a configuration window for creating a new IKE User Group. At the top, there is a text field labeled "Group Name" containing the text "netscreen-remote-grp". Below this, there are two list boxes. The left list box is titled "<- Group Members ->" and contains the name "jane". The right list box is titled "<- Available Members ->" and is currently empty. Between the two list boxes are two buttons: "<<" and ">>". At the bottom of the window are two buttons: "OK" and "Cancel". Red rectangular boxes highlight the "Group Name" field, the "<<" button, and the "OK" button.

## 5.6.3. XAuth User Group

1. From the left navigation menu, select **Objects > User > Local Groups > New**.
  - Enter a descriptive **Group Name**. In the Sample Configuration, **remoteuser-grp** is used.
  - Select the tom, dick and harry user names from the **Available Members** column on the right. Select the << icon to move the user name to the **Group Members** column on the left.
  - Select **OK** to save.

**Group Name** remoteuser-grp

<- Group Members ->

tom  
dick  
harry

<<

>>

<- Available Members ->

tom  
dick  
harry

---

OK

Cancel

## 5.7. VPN

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

- Phase 1 covers how the Avaya VPNremote Phone and Juniper NetScreen-Remote Windows VPN Client will securely negotiate and handle the building of the tunnel with Juniper SSG.
- 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 including the proposal name used by the Juniper SSG.

Phase	Encryption/ Authentication Method	Diffie- Hellman Group	Encryption Algorithm	Hash Algorithm	Life Time (sec)	SSG Proposal Name
P1	Pre-Shared Key	2	3DES	MD5	28800	pre-g2-3des-md5
P2	ESP	2	AES128	SHA-1	3600	g2-esp-aes128-sha

**Table 1 – IKE P1 /P2 Proposals**

### 5.7.1. AutoKey IKE Gateway Configuration – Phase 1

**1. Configuration for VPNremote Phone:**

From the left navigation menu, select **VPNs > AutoKey Advanced > Gateway**.

Select **New**. Configure the highlighted fields shown below. All remaining fields can be left as default.

- Provide a descriptive **Gateway Name**. In the Sample Configuration, **vpnphone-gw** is used.
- Select **Remote Gateway**
- Select **Dialup User Group**. For **Group** select the IKE Group created for the VPNremote Phone in **Section 5.6.1** from the drop down list. For the sample configuration , **vpnphone-grp** was used.
- Select **Advanced** to access additional configuration options.



Gateway Name

☒ Remote Gateway

☐ Static IP Address IP Address/Hostname   
☐ Dynamic IP Address Peer ID   
☐ Dialup User User   
☒ Dialup User Group Group   
☐ ACVPN-Dynamic Local ID   
☐ ACVPN-Profile

OK Cancel **Advanced**

2. *Configuration for VPNremote Phone:*

Configure the highlighted fields shown on the next page. All remaining fields can be left as default. Select **Return** to complete the advanced configuration, and then **OK** to save.

- Enter an ASCII text string for a **Preshared Key** that will match the text entered on the Avaya VPNremote Phone as described in **Section 6.2, Step 2**.
- Select **Outgoing Interface** (from the drop down menu), the interface which terminates the VPN tunnel.
- Select **Security Level** of Custom.
- Select appropriate **Phase 1 Proposal** from the drop down menu. Refer to **Table 1 – IKE P1 / P2 Proposals**.
- **Aggressive Mode** must be used for end-point negotiation such as the Avaya VPNremote Phone.
- **Enable NAT-Traversal** allows IPSec traffic after Phase 2 negotiations are complete to traverse a Network Address Translation (NAT) device. The Juniper SSG first checks if a NAT device is present in the path between itself and the Avaya VPNremote Phone. If a NAT device is detected, the Juniper SSG uses UDP to encapsulate each IPSec packet.

Use As Seed ☐  
 Local ID  (optional)  
 Outgoing Interface

---

**Security Level**  
 Predefined ☐ Standard ☐ Compatible ☐ Basic  
 User Defined ☒ Custom

**Phase 1 Proposal**  

<input type="text" value="pre-g2-3des-md5"/>	<input type="text" value="None"/>
<input type="text" value="None"/>	<input type="text" value="None"/>

---

Mode (Initiator) ☐ Main (ID Protection) ☒ Aggressive

---

☒ Enable NAT-Traversal

UDP Checksum ☐  
 Keepalive Frequency  Seconds (0~300 Sec)

---

**Peer Status Detection**  
☐ Heartbeat
 

Hello	<input type="text" value="0"/>	Seconds (1~3600, 0: disable)
Reconnect	<input type="text" value="0"/>	Seconds (60~9999 Sec)
Threshold	<input type="text" value="5"/>	(2~9999)
Interval	<input type="text" value="0"/>	Seconds (3~28800, 0: disable)
Retry	<input type="text" value="5"/>	(1~127)

  
☐ DPD
 

Always Send	<input type="checkbox"/>
-------------	--------------------------

3. *Configuration for Juniper NetScreen-Remote Windows VPN Client:*

From the left navigation menu, select **VPNs > AutoKey Advanced > Gateway**.

Select **New**. Configure the highlighted fields shown below. All remaining fields can be left as default.

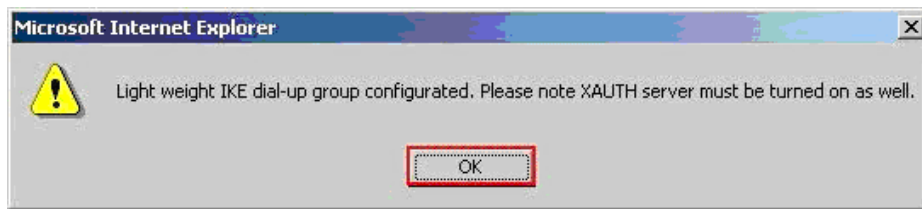
- Provide a descriptive **Gateway Name**. In the Sample Configuration, **netscreen-remote-gw** is used.
- Select **Dialup User Group** that associates with the **Group netscreen-remote-grp** created in **Section 5.6.2** to this IKE gateway.
- Select **Remote Gateway**
- Select **Dialup User Group**. For **Group** select the IKE Group created for the NetScreen-Remote client in **Section 5.6.2** from the drop down list. For the sample configuration , **netscreen-remote-grp** was used.
- Select **Advanced** to access additional configuration options.

4. *Configuration for Juniper NetScreen-Remote Windows VPN Client:*

Configure the highlighted fields shown on the next page. All remaining fields can be left as default. Select **Return** to complete the advanced configuration, and then **OK** to save.

- Enter an ASCII text string for a **Preshared Key** that will match the text entered on the Juniper NetScreen-Remote, as described in **Section 7, Step 3**.

5. Because the IKE group was selected in Step 1 above, a pop-up window similar to the one below is displayed as a reminder to enable the XAuth server. **Section 5.8** provides the XAuth server configuration. Select **OK**.



6. The **AutoKey Advanced > Gateway** list page displays the new gateway.

Name	Peer Type	Address/ID/User Group	Local ID	Security Level	Configure	
netscreen-remote-gw	Dialup	netscreen-remote-grp	-	Custom	<a href="#">Edit</a>	<a href="#">Xauth</a>
vpnphone-gw	Dialup	vpnphone-grp	-	Custom	<a href="#">Edit</a>	<a href="#">Xauth</a>

### 5.7.2. AutoKey IKE VPN Tunnel Configuration – Phase 2

1. *Configuration for VPNremote Phone:*

From the left navigation menu, select **VPNs > AutoKey IKE**.

Select **New**. Configure the highlighted fields shown below. All remaining fields can be left as default.

- Provide a descriptive **VPN Name**.
- Select **Predefined** for **Remote Gateway** and select the Remote Gateway name entered in **Section 5.7.1** from the drop-down menu. For the sample configuration it will be **vpnphone-gw** for VPNremote phones.
- Select **Advanced** to access additional configuration options.

A screenshot of a web-based configuration form for 'AutoKey IKE VPN Tunnel Configuration'. The form has a light blue background. At the top, there is a 'VPN Name' field with the value 'vpnphone-vpn'. Below it, the 'Remote Gateway' section is active, showing 'Predefined' selected with a radio button and 'vpnphone-gw' in a dropdown menu. Underneath, there are several configuration options: 'Gateway Name' (empty), 'Type' (Static IP selected), 'Address/Hostname' (empty), 'Dynamic IP' (radio button), 'Peer ID' (empty), 'Dialup User' (radio button), 'User' (None selected in dropdown), 'Dialup Group' (radio button), 'Group' (None selected in dropdown), 'Local ID' (empty), 'Preshared Key' (empty), 'Use As Seed' (checkbox), 'Security Level' (Standard selected), 'Compatible' (radio button), 'Basic' (radio button), 'Outgoing Interface' (ethernet0/0 selected), 'Gateway' (None selected in dropdown), 'Tunnel Towards Hub' (dropdown), 'Binding to Tunnel' (None selected in dropdown). At the bottom, there are three buttons: 'OK', 'Cancel', and 'Advanced'. The 'Advanced' button is highlighted with a red rectangular box.

2. Configure the highlighted fields shown below. All remaining fields can be left as default. Select **Return** to complete the advanced configuration, and then **OK** to save.

- Select **Security Level** of Custom.
- Select appropriate **Phase 2 Proposal** from the drop down menu. Refer to **Table 1 – IKE P1 / P2 Proposals**.
- Check **Replay Protection**. This protects the encrypted IPSec traffic from man-in-the-middle replay attacks by including a sequence number with each IKE negotiation between the IKE endpoints.
- Check **Bind to None**. This uses the outgoing interface, ethernet 0/0, for all VPN tunnel traffic.
- Check **VPN Monitor**.

The screenshot displays a VPN configuration window with the following sections and highlighted fields:

- Security Level**: Radio buttons for Predefined (Standard, Compatible, Basic) and User Defined (Custom). The **Custom** option is selected and highlighted with a red box.
- Phase 2 Proposal**: A table with two columns. The first column has a dropdown menu with "g2-esp-aes128-sha" selected, highlighted by a red box. The second column has two dropdown menus, both set to "None".
- Replay Protection**: A checkbox that is checked, highlighted by a red box.
- Transport Mode**: A checkbox labeled "(For L2TP-over-IPSec only)" which is unchecked.
- Bind to**: Radio buttons for Tunnel Interface and Tunnel Zone. The **None** option is selected and highlighted by a red box.
- Proxy-ID**: A checkbox which is unchecked.
- Local IP / Netmask**: Two text input fields.
- Remote IP / Netmask**: Two text input fields.
- Service**: A dropdown menu set to "ANY".
- VPN Group**: A dropdown menu set to "None".
- Weight**: A text input field set to "1".
- VPN Monitor**: A checkbox that is checked, highlighted by a red box.
- Source Interface**: A dropdown menu set to "default".
- Destination IP**: A text input field.
- Optimized**: An unchecked checkbox.
- Rekey**: An unchecked checkbox.
- Buttons**: "Return" and "Cancel" buttons at the bottom, with "Return" highlighted by a red box.

3. *Configuration for Juniper NetScreen-Remote VPN Client:*

From the left navigation menu, select **VPNs > AutoKey IKE**.

Select **New**. Configure the highlighted fields shown below. All remaining fields can be left as default.

- Provide a descriptive **VPN Name**.
- Select **Predefined** for **Remote Gateway** and select the Remote Gateway name entered in **Section 5.7.1, Step 3** from the drop-down menu. For the sample configuration it will be **netscreen-remote-gw**.
- Select **Advanced** to access additional configuration options.

The screenshot shows the configuration window for a Juniper NetScreen VPN client. The 'VPN Name' field is set to 'netscreen-remote-vpn'. The 'Remote Gateway' section is expanded, showing 'Predefined' selected and 'netscreen-remote-gw' chosen from the dropdown. The 'Advanced' button is highlighted with a red box.

**VPN Name** netscreen-remote-vpn

**Remote Gateway** ☒ Predefined netscreen-remote-gw ☐ Create a Simple Gateway

**Gateway Name**

**Type** ☒ Static IP Address/Hostname   
☐ Dynamic IP Peer ID   
☐ Dialup User User   
☐ Dialup Group Group

**Local ID**  (optional)

**Preshared Key**  Use As Seed ☐

**Security Level** ☒ Standard ☐ Compatible ☐ Basic

**Outgoing Interface** ethernet0/0

**Gateway**  **Tunnel Towards Hub**

**Binding to Tunnel**

☐ ACVPN-Dynamic  
☐ ACVPN-Profile

OK Cancel **Advanced**

4. Configure the highlighted fields shown below. All remaining fields can be left as default. Select **Return** to complete the advanced configuration, and then **OK** to save.

- Select **Security Level** of Custom.
- Select appropriate **Phase 2 Proposal** from the drop down menu. Refer to **Table 1 – IKE P1 / P2 Proposals**.
- Check **Replay Protection**.
- Check **Bind to None**.
- Check **VPN Monitor**.

**Security Level**

Predefined ☐ Standard ☐ Compatible ☐ Basic

User Defined ☒ Custom

**Phase 2 Proposal**

g2-esp-aes128-sha  None

None  None

**Replay Protection** ☒

**Transport Mode** ☐ (For L2TP-over-IPSec only)

**Bind to** ☒ None

☐ Tunnel Interface

☐ Tunnel Zone

**Proxy-ID** ☐

**Local IP / Netmask**  /

**Remote IP / Netmask**  /

**Service** ANY

**VPN Group** None  **Weight** 0

**VPN Monitor** ☒

**Source Interface** default

**Destination IP** default

**Optimized** ☐

**Rekey** ☐

**Return** **Cancel**

3. The **AutoKey IKE** list page displays the new IKE VPN:

Name	Gateway	Security	Monitor	Configure
netscreen-remote-vpn	netscreen-remote-gw	Custom	On	<a href="#">Edit</a>
vpnphone-vpn	vpnphone-gw	Custom	On	<a href="#">Edit</a>

## 5.8. XAuth Configuration

The Juniper SSG has a “local” XAuth server integrated within the ScreenOS operating system. Alternatively, an external Radius server can be used.

These Application Notes implement the “local” ScreenOS XAuth server. The following steps configure the default and IKE gateway specific settings of the local XAuth server.

### 5.8.1. XAuth Server Defaults

1. From the left navigation menu, select **VPNs > AutoKey Advanced > XAuth Settings**. Configure the highlighted fields shown below. All remaining fields can be left as default. Select **Apply** when complete.
  - Select the **IP Pool Name** created in **Section 5.3** from the drop down menu. This defines the IP Address range used when IP addresses are dynamically assigned to the Avaya VPNremote Phone and the Juniper NetScreen-Remote VPN Client by the XAuth server during IKE setup.
  - Enter the **DNS** and **WINS** server IP addresses if applicable. .

Reserve Private IP for XAuth User 480 Minutes

Default Authentication Server Local

Query Client Settings on Default Server ☐

CHAP ☐

IP Pool Name VPNremote Phone

DNS Primary Server IP 30.1.1.7

DNS Secondary Server IP 0.0.0.0

WINS Primary Server IP 0.0.0.0

WINS Secondary Server IP 0.0.0.0

Apply Cancel



## 5.8.2. Enable XAuth Authentication for AutoKey IKE gateway for VPNremote Phone

1. From the left navigation menu, select **VPNs > AutoKey Advanced > Gateway**. The list page displays the IKE gateway created in **Section 5.7.1** as shown below.

Select **Xauth** under the **Configure** column for the vpnphone-gw IKE gateway.

Name	Peer Type	Address/ID/User Group	Local ID	Security Level	Configure	
vpnphone-gw	Dialup	vpnphone-grp	-	Custom	<a>Edit</a>	<a>Xauth</a>

2. Configure the highlighted fields shown below. All remaining fields can be left as default. Select **OK** when complete to save settings.
  - Check **XAuth Server** with **Allowed Authentication Type** of **CHAP only**.
  - Select **User Group** from the drop down menu. This is the XAuth user group created in **Section 5.6.3**. For the sample configuration it will be **remoteuser-grp**.

☐ None

☒ **XAuth Server**

Allowed Authentication Type ☐ Generic ☒ **CHAP Only** ☐ CHAP & PAP

☐ Use Default Xauth Settings

☒ **Local Authentication**

☐ Allow Any

☐ User

☒ **User Group**

☐ **External Authentication**  ☐ Query Remote Setting

☒ Allow Any

☐ User

☐ User Group

☐ **Bypass Authentication**

☒ **XAuth Client**

Allowed Authentication Type ☐ Any ☐ CHAP Only ☐ SecurID

User Name

Password

Update DHCP Server ☐

Prefix Delegation to IPv6 Interfaces ☐

Interface	SLA ID	SLA Length	Action
<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value="0"/>	<input type="button" value="Add"/>
No entry available			

### 5.8.3. Enable XAuth Authentication for AutoKey IKE gateway for Juniper NetScreen-Remote VPN Client

1. From the left navigation menu, select **VPNs > AutoKey Advanced > Gateway**. The list page displays the IKE gateway created in **Section 5.7.1** as shown below.

Select **Xauth** under the **Configure** column for the vpnphone-gw IKE gateway.

Name	Peer Type	Address/ID/User Group	Local ID	Security Level	Configure	
netscreen-remote-gw	Dialup	netscreen-remote-grp	-	Custom	<a href="#">Edit</a>	<a href="#">Xauth</a>

2. Configure the highlighted fields shown below. All remaining fields can be left as default. Select **OK** when complete to save settings.
  - Check **XAuth Server** with **Allowed Authentication Type** of **Generic**.
  - Select **User Group** from the drop down menu. This is the XAuth user group created in **Section 5.6.3**. For the sample configuration it will be **remoteuser-grp**.

☐ None

☒ **XAuth Server**

Allowed Authentication Type ☒ Generic ☐ CHAP Only ☐ CHAP & PAP

☐ Use Default Xauth Settings

☒ **Local Authentication**

☐ Allow Any

☐ User

☒ **User Group**

☐ **External Authentication**  ☐ Query Remote Setting

☐ Allow Any

☐ User

☐ User Group

☐ **Bypass Authentication**

☐ **XAuth Client**

Allowed Authentication Type ☐ Any ☐ CHAP Only ☐ SecurID

User Name

Password

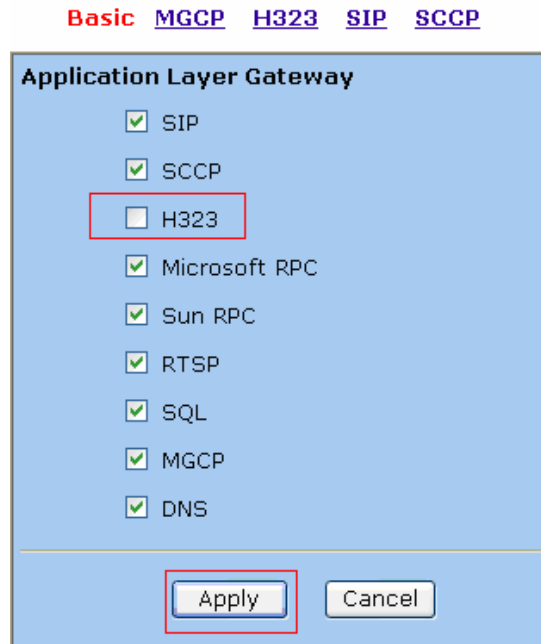
Update DHCP Server ☐

Prefix Delegation to IPv6 Interfaces

Interface	SLA ID	SLA Length	Action
<input type="text" value=""/>	<input type="text" value=""/>	<input type="text" value="0"/>	<input type="button" value="Add"/>
No entry available			

## 5.9. H.323 ALG

1. From the left navigation menu, select **Security > ALG**. Un-check the **H323** check box to globally disable the H.323 Application Layer Gateway.



## 5.10. Security Policies

1. From the left navigation menu select **Policy > Policies**. Any currently configured security policies are displayed.

Create a security policy for traffic flowing from the **Untrust** zone to the **Trust** zone. On the top of the **Policies** page select **Untrust** on the **From** drop-down menu and **Trust** on the **To** drop-down menu. Select the **New** button on top right corner of page to create the new security policy.

2. *Configuration for Avaya VPNremote Phone:*

Configure the highlighted fields shown below. All remaining fields can be left as default. Select **OK** when complete to save settings.

- Enter a descriptive policy **Name** to easily identify this policy in the policy list and logs.
- Select **Dial-Up VPN** from the Source Address drop down list and **Any** from the **Destination Address** drop down list. This defines the VPN tunnel as the traffic originator.
- Select **Tunnel** from the Action field drop-down list. This indicates the action the SSG will take against traffic that matches the first three criteria of the policy: Source Address, Destination Address, and Service. All matching traffic will be associated with a particular VPN Tunnel specified in the Tunnel field.
- Select **vpnphone-vpn** from the Tunnel VPN drop down menu associates the VPNremote Phone VPN tunnel to the Action.
- Check the **Modify matching bidirectional VPN policy** to have the SSG create a matching VPN policy for traffic flowing in the opposite direction.
- Check **Logging**.

**Name (optional)** VPNphones

**Source Address**  
☐ New Address /  
☒ Address Book Entry Dial-Up VPN Multiple

**Destination Address**  
☐ New Address /  
☒ Address Book Entry Any Multiple

**Service** ANY Multiple

**Application** None

☐ WEB Filtering

**Action** Tunnel

**Tunnel** VPN vpnphone-vpn  
☒ Modify matching bidirectional VPN policy

L2TP None

**Logging** ☒ at Session Beginning ☐

**Position at Top** ☐

OK Cancel Advanced

3. *Configuration for Juniper NetScreen-Remote VPN Client:*  
Configure the highlighted fields shown below. All remaining fields can be left as default. Select **OK** when complete to save settings.

**Name (optional)** netscreen-remote-vpn

**Source Address**  
☐ New Address /  
☒ Address Book Entry Dial-Up VPN Multiple

**Destination Address**  
☐ New Address /  
☒ Address Book Entry Any Multiple

**Service** ANY Multiple

**Application** None

☐ WEB Filtering

**Action** Tunnel

**Tunnel** VPN netscreen-remote-vpn  
☒ Modify matching bidirectional VPN policy

L2TP None

**Logging** ☒ at Session Beginning ☐

OK Cancel Advanced

4. The Policies list page displays the new Dial-Up VPN policy:

From Untrust To Trust, total policy: 2										
ID	Source	Destination	Service	Action	Options	Configure			Enable	Move
3	Dial-Up VPN	Any	ANY			<a href="#">Edit</a>	<a href="#">Clone</a>	<a href="#">Remove</a>	<input checked="" type="checkbox"/>	
1	Dial-Up VPN	Any	ANY			<a href="#">Edit</a>	<a href="#">Clone</a>	<a href="#">Remove</a>	<input checked="" type="checkbox"/>	
From Trust To Untrust, total policy: 2										
ID	Source	Destination	Service	Action	Options	Configure			Enable	Move
4	Any	Dial-Up VPN	ANY			<a href="#">Edit</a>	<a href="#">Clone</a>	<a href="#">Remove</a>	<input checked="" type="checkbox"/>	
2	Any	Dial-Up VPN	ANY			<a href="#">Edit</a>	<a href="#">Clone</a>	<a href="#">Remove</a>	<input checked="" type="checkbox"/>	

## 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 → **Right arrow** hard button. The Application file name displayed denotes the installed firmware version.

As displayed in Section 3, 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 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, e.g. registered with Avaya Communication Manager, 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 enter the VPN Options menu.

2. 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 2** 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:	<b>44.2.2.2</b>	IP address of the Juniper SSG5 (untrusted interface)
User Name:	<b>tom</b>	User created in <b>Section 5.5.3</b>
Password:	<b>*****</b>	Must match user password entered in <b>Section 5.5.3</b>
Group Name:	<b>vpnphone@avaya.com</b>	Must match the <b>IKE Identity</b> entered in <b>Section 5.5.1</b>
Group PSK:	<b>1234567890</b>	Must match the <b>Pre-shared Key</b> entered in <b>Section 5.7.1, Step 2</b>
VPN Start Mode:	<b>BOOT</b>	IPSec tunnel dynamically starts on Phone power up.
Password Type:	<b>Save in Flash</b>	User is not prompted at phone boot up.
Encapsulation	<b>4500-4500</b>	This default value enables NAT Traversal
Syslog Server:	-	
<b>IKE Parameters:</b>	<b>DH2-ANY-ANY</b>	

<b>Configuration Options</b>	<b>Value</b>	<b>Description</b>
IKE ID Type:	<b>User-FQDN</b>	
Diffie-Hellman Grp	<b>2</b>	Can be set to “Detect” to accept VPN Concentrator settings
Encryption Alg:	<b>ANY</b>	Can be set to “Any” to accept VPN Concentrator settings
Authentication Alg:	<b>ANY</b>	Can be set to “Any” to accept VPN Concentrator settings
IKE Xchg Mode:	<b>Aggressive</b>	
IKE Config Mode:	<b>Enable</b>	
Xauth	<b>Enable</b>	
Cert Expiry Check	<b>Disable</b>	
Cert DN Check	<b>Disable</b>	
<b>IPSec Parameters:</b>	<b>DH2-ANY-ANY</b>	
Encryption Alg:	<b>ANY</b>	Can be set to “Any” to accept VPN Concentrator settings
Authentication Alg:	<b>ANY</b>	Can be set to “Any” to accept VPN Concentrator settings
Diffie-Hellman Grp	<b>2</b>	Can be set to “Detect” to accept VPN Concentrator settings
<b>Protected Net:</b>		
Remote Net #1:	<b>0.0.0.0/0</b>	Access to all private nets
File Svr:	<b>44.1.1.84</b>	TFTP File Srv
Connectivity Check:	<b>First Time</b>	Test initial IPSec connectivity
Copy TOS:	<b>Yes</b>	Maintain phone TOS setting on Corp Network for QoS
QTest	<b>Disable</b>	Can be either Enable or Disable to allow user access to QTest feature.

**Table 2 – Avaya VPNremote Phone Configuration**



3. The Avaya VPNremote Phone can interoperate with several VPN head-end vendors. 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 Avaya VPNremote Phone.

Press the **Profile** soft button at the bottom of Avaya VPNremote Phones 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 aligned with 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.

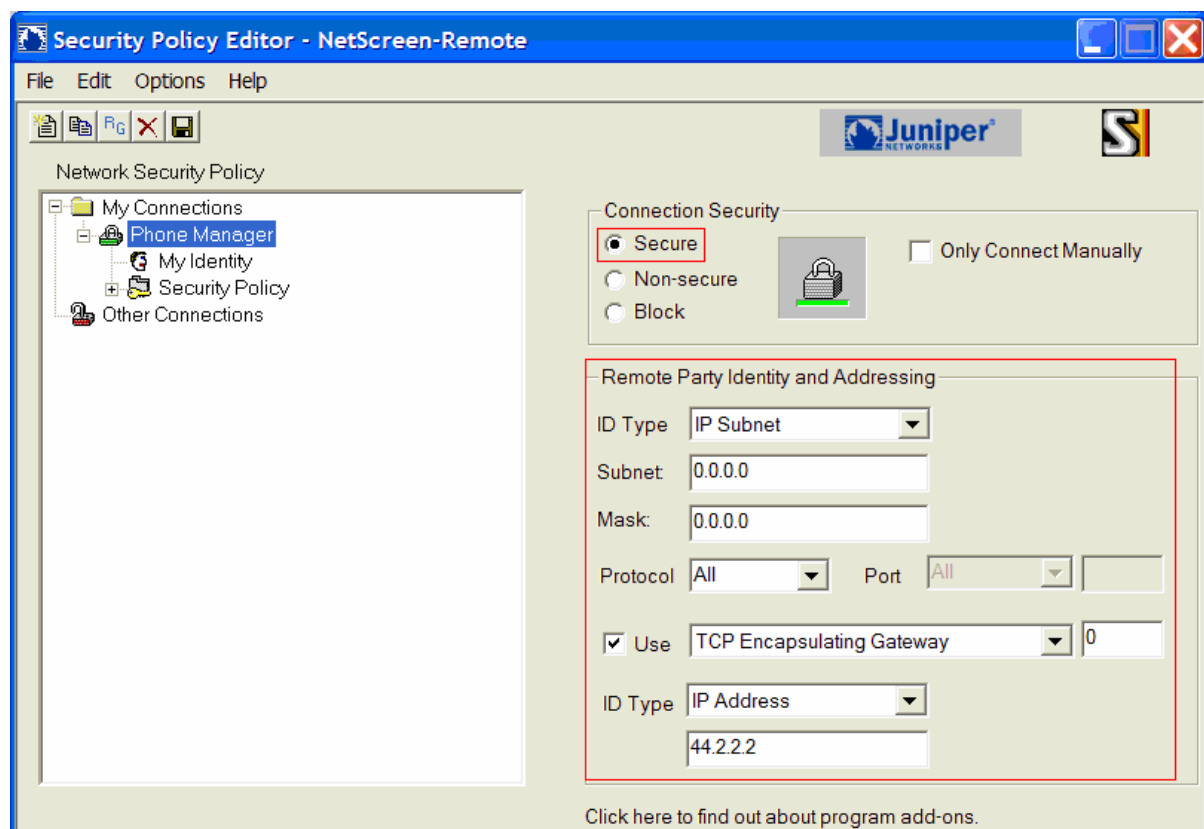
When all VPN configuration options have been set, press the **Done** soft button. The following is displayed. Press **#** to save the configuration and reboot the phone.

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

## 7. Juniper NetScreen – Remote VPN Client Configuration

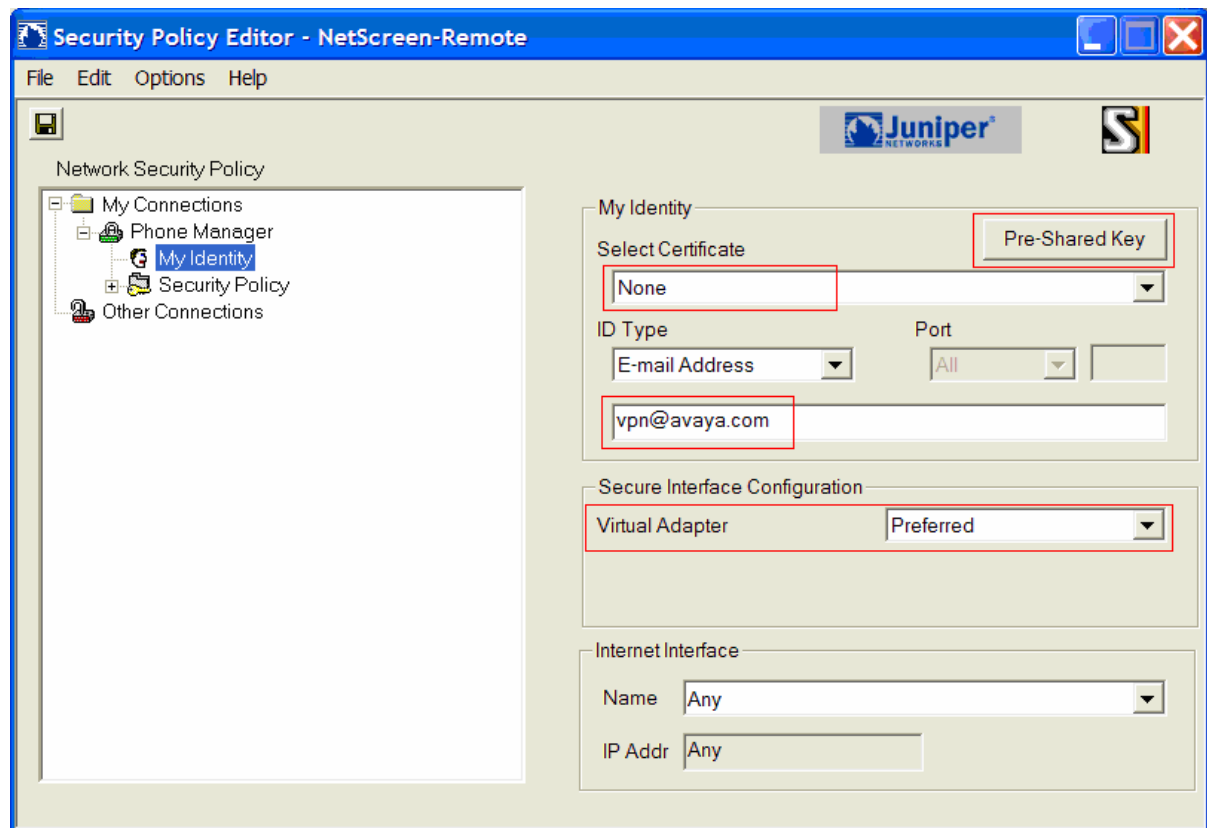
This section shows the configuration of the Juniper NetScreen – Remote Windows VPN client. This section assumes that Juniper NetScreen – Remote VPN Client software is already installed on the client desktop.

1. Launch the NetScreen-Remote Security Policy Editor by selecting **Start > Programs > NetScreen-Remote > Security Policy Editor**. Right click the folder **My Connections** and select **Add > Connection** (not shown). Provide a descriptive name for the new connection. **PhoneManager** was using in the sample configuration. Configure the highlighted fields shown below.
  - Select **Secure** for **Connection Security**.
  - Select **IP Subnet** for **ID Type**.
  - Enter **0.0.0.0** in the field **Subnet** and **0.0.0.0** in the field **Mask**.
  - Select **All** in the **Protocol**.
  - Check the **Use** box and select **TCP Encapsulating Gateway** from the drop down menu.
  - Select **IP Address** in the field **ID Type** and enter **44.2.2.2** (IP address of the SSG5 public interface) as the tunnel endpoint IP address.

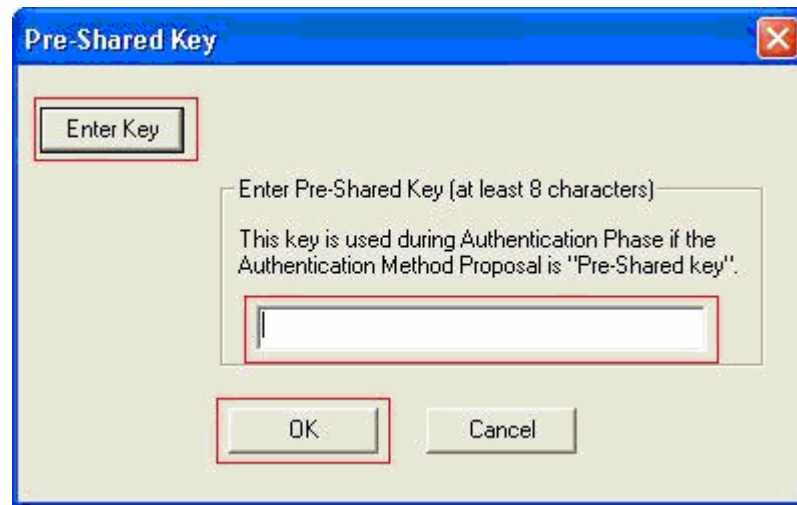


2. Expand the **Phone Manager** folder and select **My Identity**. Configure the highlighted fields shown below.
  - Select **E-mail Address** for **ID Type** field and enter [vpn@avaya.com](mailto:vpn@avaya.com). This should match the IKE Identity created in **Section 5.5.2, Step 1**.
  - Select **Preferred** for **Virtual Adapter** field.

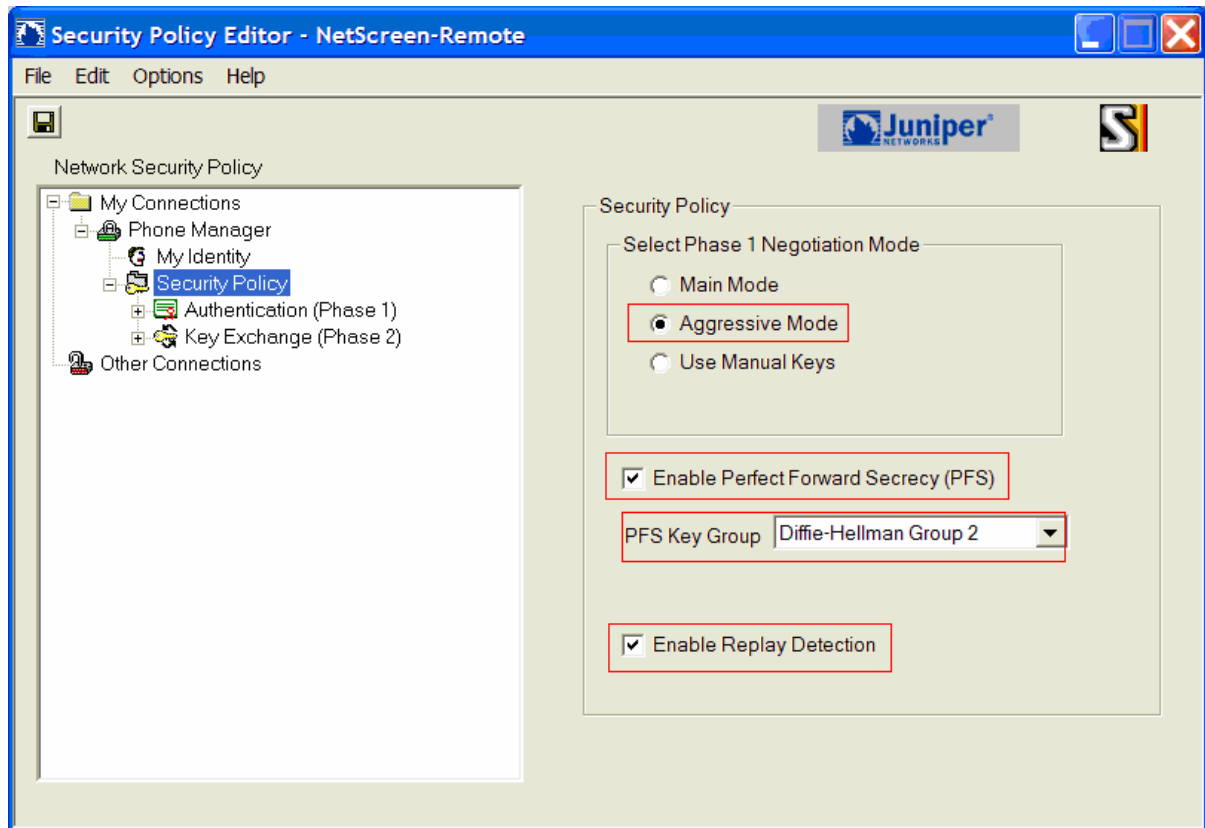
All remaining fields can be left as the defaults. Click **Pre-Shared Key** to continue.



3. Click **Enter Key** and type the Pre-Shared Key. This should match the Preshared Key entered in **Section 5.7.1, Step 4**. Click **OK**.

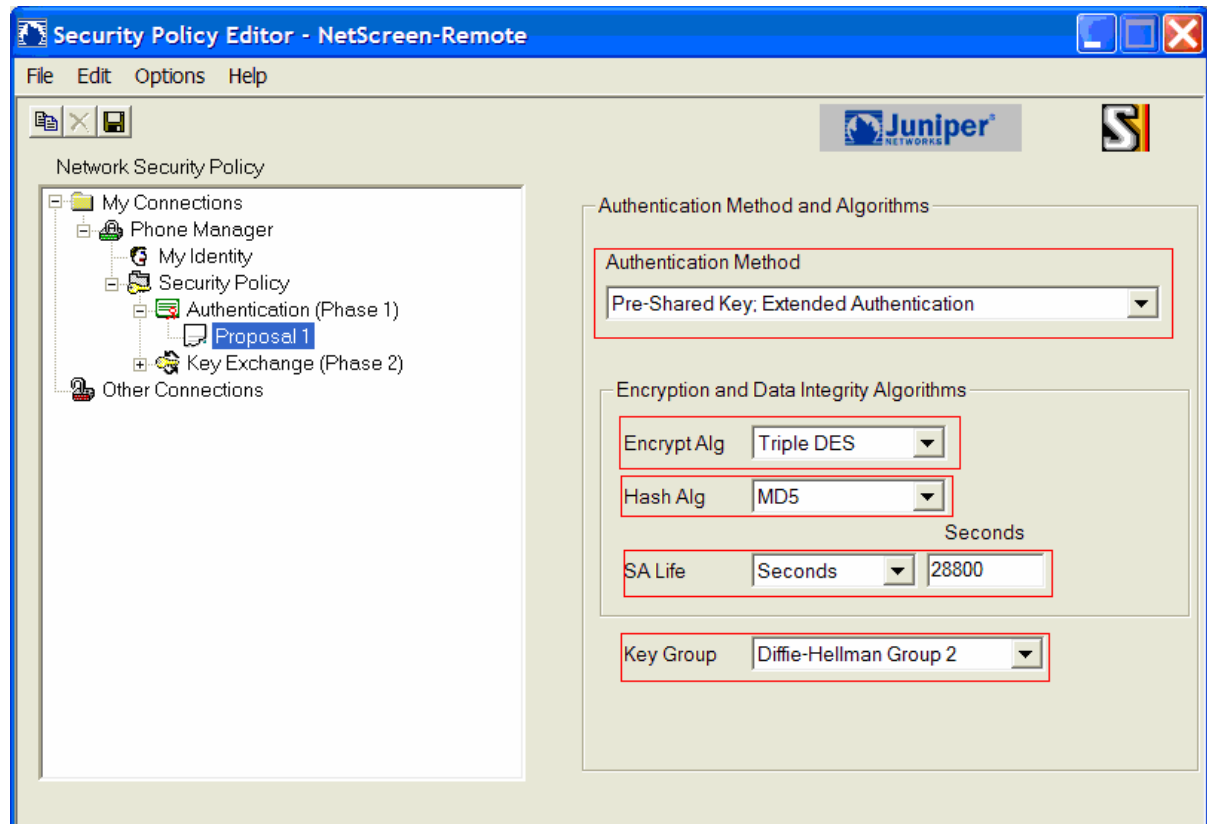


4. Select **Security Policy**. Configure the highlighted fields shown below.
- Select **Aggressive Mode** for **Select Phase 1 Negotiation Mode**.
  - Check **Enable Perfect Forward Secrecy (PFS)**.
  - Select PFS Key Group. Refer to **Section 5.7 Table 1 – IKE P1/P2 Proposals**.
  - Check **Enable Replay Detection** field.



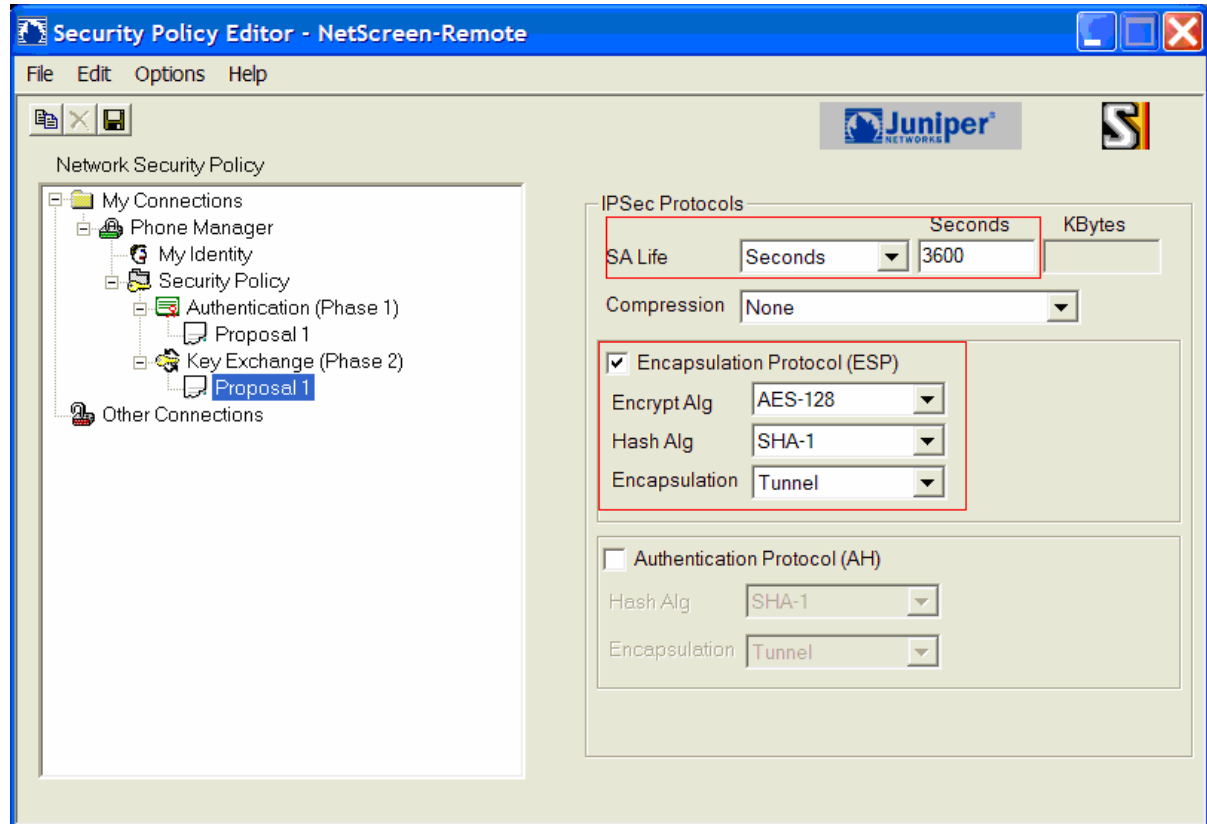
5. Expand folder **Security Policy > Authentication (Phase 1)** and select **Proposal 1**. Configure the highlighted fields shown below.
- Select **Pre-Shared Key; Extended Authentication** for **Authentication Method** field.
  - Select **Triple DES** for **Encrypt Alg** field.
  - **MD5** for **Hash Alg** field.
  - Select **Seconds** for SA Life, and enter **28800**.
  - Select **Diffie-Hellman Group 2** for **Key Group** field.

Refer to **Section 5.7 Table 1 – IKE P1/P2 Proposals** for Encrypt Alg and Hash Alg field.



6. Expand folder **Security Policy > Key Exchange (Phase 2)** and select **Proposal 1**. Configure the highlighted fields shown below. All remaining fields can be left as the defaults.
- Check **Encapsulation Protocol (ESP)** field.
  - Select **AES-128** for **Encrypt Alg** field.
  - Select **SHA-1** for **Hash Alg** field.
  - Select **Tunnel** for **Encapsulation** field.

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



## 8. Phone Manager Pro Configuration

Log into 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.
  - Accept the default values for Continuous Mode and Test Call Required.
  - Click on **Save Profile**.
  - Click on **OK**.

IP Office Phone Manager / Login

Where do you want to work?

☐ Internal (Office)

☒ Remote (Telecommuter Mode)

▼

Saved Remote Profile Details...

Remote Profile Name: Home Office

Contact Number: 2552020

☐ Continuous Mode

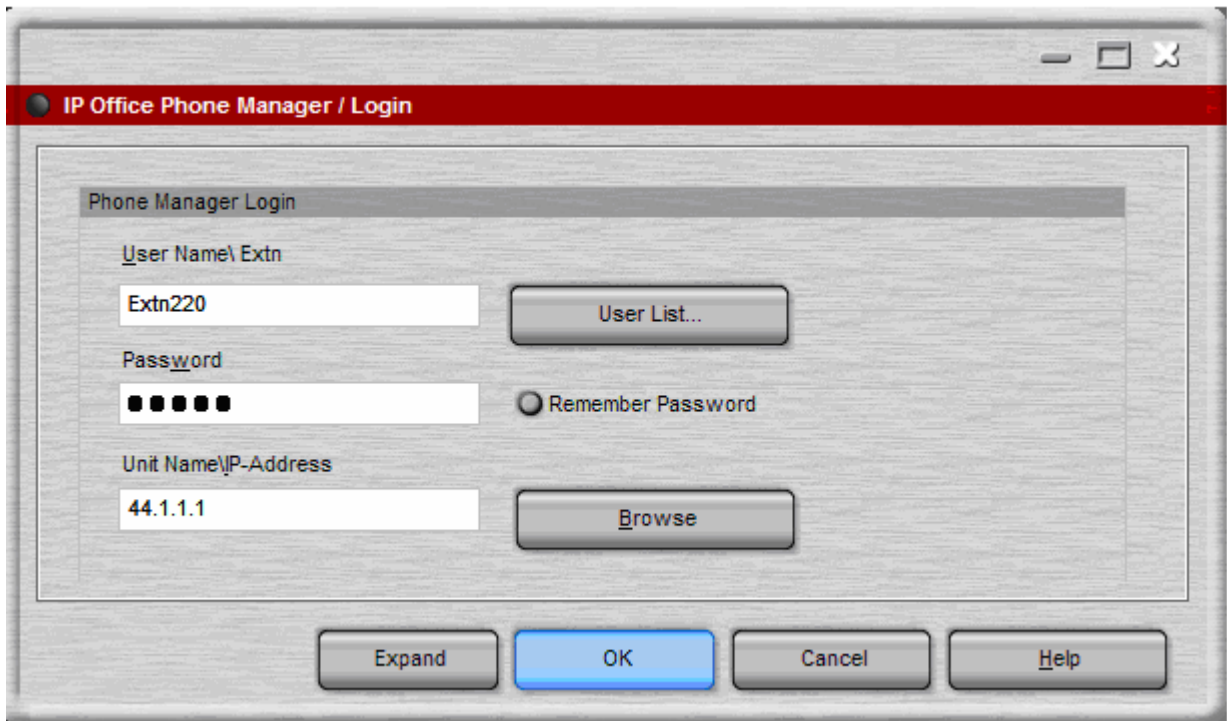
☐ Test Call Required

Save Profile

OK Cancel Help



2. In the **IP Office Phone Manager/Login** screen, enter:
- **User Name\Extn**
  - **Password**
  - Enter the IP Address of IP Office in the **Unit Name\IP-Address** field
  - Click on **OK**.



The screenshot shows a Windows-style dialog box titled "IP Office Phone Manager / Login". Inside the dialog, there is a section titled "Phone Manager Login". This section contains three text input fields: "User Name\ Extn" with the value "Extn220", "Password" with masked characters "•••••", and "Unit Name\IP-Address" with the value "44.1.1.1". To the right of the "User Name\ Extn" field is a button labeled "User List...". To the right of the "Password" field is a radio button labeled "Remember Password". To the right of the "Unit Name\IP-Address" field is a button labeled "Browse". At the bottom of the dialog, there are four buttons: "Expand", "OK" (highlighted in blue), "Cancel", and "Help".

Note: The User configured with Phone Manager Telecommuter option is a Hot Desk user, as mentioned in **Section 4, Step 8**. When a user will log-in at the Phone Manager, the internal IP Office extension will be logged off.

## 9. Verification

### 9.1. VPNremote Phone Qtest

Using a feature of the Avaya VPNremote Phone called **Quality test** or **Qtest**, the VPNremote Phone can test the network connection to the VPN head-end gateway to characterize the voice quality an end user is likely to experience.

Once the Avaya VPNremote Phone establishes an IPSec tunnel, registers with Avaya Communication Manager and becomes functional, enter the Avaya VPNremote Phone VPN configuration mode as described in **Section 6**. Select the **Qtest** soft button to enter the Qtest menu. Select the **Start** soft button to start Qtest. Note the reported statistics to determine the network connection quality.

### 9.2. VPNremote Phone IPSec stats

Once the Avaya VPNremote Phone establishes an IPSec tunnel, registers with Avaya Communication Manager and becomes functional, from the telephone keypad, press the **OPTIONS** hard button (√ icon). From the telephone keypad, press the telephone ► hard button to access the next screen. Select the **VPN Status...** option. There are two screens of IPSec tunnel statistics displayed. Use the ► hard button to access the next screen. Press the **Refresh** soft button to update the displayed statistics.

The list below shows the statistics from Avaya VPNremote Phone used in the sample configuration.

VPN Status...	
<b>PKT S/R</b>	<b>47/39</b>
<b>FRAG RCVD</b>	<b>4</b>
<b>Comp/Decomp</b>	<b>0/0</b>
<b>Auth Failures</b>	<b>0</b>
<b>Recv Errors</b>	<b>0</b>
<b>Send Errors</b>	<b>0</b>
<b>Gateway</b>	<b>44.2.2.2</b>
<b>Outer IP</b>	<b>192.168.1.103</b>
<b>Inner IP</b>	<b>10.10.10.1</b>
<b>Gateway Version</b>	<b>UNKNOWN</b>
<b>Inactivity Timeout</b>	<b>0</b>
<b>DH2-AES-SHA-60mins</b>	

### 9.3. Juniper SSG Debug and Logging

From the Juniper SSG WebUI, select **Reports > System Log > Event** from the left navigation menu.

The Juniper SSG System 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 a tunnel. The screen below is in reverse chronological order. Please refer to the time stamp.

Date / Time	Level	Description
2002-07-22 15:50:16	info	IKE 33.1.1.150 Phase 2 msg ID df86e7eb: Completed negotiations with SPI 2cecccc8, tunnel ID 32771, and lifetime 3600 seconds/0 KB.
2002-07-22 15:50:16	info	IKE 33.1.1.150 Phase 2 msg-id df86e7eb: Completed for user vpnphone@avaya.com.
2002-07-22 15:50:15	info	IKE 33.1.1.150: Received initial contact notification and removed Phase 1 SAs.
2002-07-22 15:50:15	info	IKE 33.1.1.150: Received initial contact notification and removed Phase 2 SAs.
2002-07-22 15:50:15	info	IKE 33.1.1.150: Received a notification message for DOI 1 24578 INITIAL-CONTACT.
2002-07-22 15:50:15	info	IKE 33.1.1.150 Phase 2 msg ID df86e7eb: Responded to the peer's first message from user vpnphone@avaya.com.
2002-07-22 15:50:14	info	IKE 33.1.1.150: XAuth login was passed for gateway vpnphone-gw, username tom, retry: 0, Client IP Addr 10.10.10.1, IPPool name: VPNremote Phone, Session-Timeout: 0s, Idle-Timeout: 0s.
2002-07-22 15:50:14	info	IKE 33.1.1.150: XAuth login was refreshed for username tom at 10.10.10.1/255.255.255.255.
2002-07-22 15:50:14	info	IKE 33.1.1.150 Phase 1: Completed Aggressive mode negotiations with a 28800-second lifetime.
2002-07-22 15:50:14	info	IKE 33.1.1.150 Phase 1: Completed for user vpnphone@avaya.com.
2002-07-22 15:50:14	info	IKE<33.1.1.150> Phase 1: IKE responder has detected NAT in front of the remote device.
2002-07-22 15:50:13	info	IKE 33.1.1.150 Phase 1: Responder starts AGGRESSIVE mode negotiations.

From the Juniper SSG Command Line Interface (CLI), the ScreenOS **debug ike basic** and **debug ike detail** commands are useful for troubleshooting ISAKMP (IKE) tunnel setup (e.g., detect mis-matched proposals, can't find gateway, etc.).

The **get ike cookies** command is also useful in getting status on existing IKE negotiations by displaying the completed IKE Phase 1 negotiations as shown below.

Following will be displayed when there are no active Phase 1 Security Associations:

```
ssg5-serial-wlan-> get ike cookies
```

```
Active: 0, Dead: 0, Total 0
```

Following will be displayed when there is one active Phase 1 Security Association:

```
ssg5-serial-wlan-> get ike cookies

Active: 1, Dead: 0, Total 1

1017182f/0006, 33.1.1.150:4500->44.2.2.2:4500, PRESHR/grp2/3DES/MD5, xchg(4)
(vpnphone-gw/grp1/usr1)
resent-tmr 322 lifetime 28800 lt-recv 432000 nxt_rekey 28130 cert-expire 0
responder, err cnt 0, send dir 1, cond 0x0
nat-traversal map:
  keepalive frequency 5 sec
  nat-t udp checksum disabled
  local pri ip 44.2.2.2
  local pri ike port 4500
  local pub ip 0.0.0.0
  local pub ike port 0
  remote pri ip 0.0.0.0
  remote pri ike port 4500
  remote pub ip 33.1.1.150
  remote pub ike port 4500
  internal ip 0.0.0.0
  internal port 0
  natt proto 17
ike heartbeat : disabled
ike heartbeat last rcv time: 0
ike heartbeat last snd time: 0
XAUTH status: 100
DPD seq local 0, peer 0

ssg5-serial-wlan->
```

## 9.4. Juniper NetScreen-Remote Log Viewer

The Juniper NetScreen-Remote Log Viewer shown below contains the IKE Phase1, IKE Phase2 and XAuth events logged as an IPSec tunnel is established.

```
1-25: 18:44:57.421 My Connections\Phone Manager - RECEIVED<<< ISAKMP OAK TRANS *(Retransmission)
1-25: 18:44:57.859 My Connections\Phone Manager - SENDING>>>> ISAKMP OAK TRANS *(HASH, ATTR)
1-25: 18:44:57.859 My Connections\Phone Manager - RECEIVED<<< ISAKMP OAK TRANS *(HASH, ATTR)
1-25: 18:44:57.859 My Connections\Phone Manager - Received Private DNS Address = IP ADDR=30.1.1.7
1-25: 18:44:57.859 My Connections\Phone Manager - Received Private IP Address = IP ADDR=10.10.10.26
1-25: 18:44:58.171 Virtual Interface constructed for local interface 10.10.10.26
1-25: 18:44:58.187 Virtual Interface added: 10.10.10.26/255.255.255.255 on ISDN "SafeNet VA miniport".
1-25: 18:44:58.187 Clearing arp for adapter 786436
1-25: 18:44:58.203 My Connections\Phone Manager - SENDING>>>> ISAKMP OAK TRANS *(HASH, ATTR)
1-25: 18:44:58.359 My Connections\Phone Manager - Initiating IKE Phase 2 with Client IDs (message id: 2630E6E9)
1-25: 18:44:58.359 My Connections\Phone Manager - Initiator = IP ADDR=10.10.10.26, prot = 0 port = 0
1-25: 18:44:58.359 My Connections\Phone Manager - Responder = IP SUBNET/MASK=0.0.0.0/0.0.0.0, prot = 0 port = 0
1-25: 18:44:58.359 My Connections\Phone Manager - SENDING>>>> ISAKMP OAK QM *(HASH, SA, NON, KE, ID 2x)
1-25: 18:44:58.359 My Connections\Phone Manager - RECEIVED<<< ISAKMP OAK TRANS *(HASH, ATTR)
1-25: 18:44:58.359 My Connections\Phone Manager - IKE Extended Authentication successful.
1-25: 18:44:58.359 My Connections\Phone Manager - Setting compliance status to OK.
1-25: 18:44:58.359 My Connections\Phone Manager - Calling UpdateBypassRecordsForCompliance - OK.
1-25: 18:44:58.359 My Connections\Phone Manager - SENDING>>>> ISAKMP OAK TRANS *(HASH, ATTR)
1-25: 18:44:58.406 My Connections\Phone Manager - RECEIVED<<< ISAKMP OAK QM *(HASH, SA, NON, KE, ID 2x)
1-25: 18:44:58.406 My Connections\Phone Manager - Filter entry 3 added: SECURE 010.010.010.026&255.255.255.255 000.000.000.000&000.000.000
1-25: 18:44:58.406 Route 0.0.0.0/0.0.0.0->10.10.10.26 added.
1-25: 18:44:58.421 Route 44.2.2.2->192.168.1.1 added.
1-25: 18:44:58.421 My Connections\Phone Manager - SENDING>>>> ISAKMP OAK QM *(HASH)
1-25: 18:44:58.468 My Connections\Phone Manager - Loading IPSec SA (Message ID = 2630E6E9 OUTBOUND SPI = 2CECCDC6 INBOUND SPI = 5
1-25: 18:44:58.468
```

## 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**.

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 button 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 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:**

Initial display shows the following:

```
Enter Username and Password
Password:
```

After a short period of time with no input (5 minutes) the display shows the following:

```
Invalid password OR user name
```

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

```
Error Code: 3997700:0
Module: IKECFG:478
```

- **Juniper SSG WebUI: Reports > System Log > Event**

Date / Time	Level	Description
2002-07-22 16:16:53	info	IKE 33.1.1.150: XAuth login expired and was terminated for username tom at 10.10.10.1/255.255.255.255>.
2002-07-22 16:16:39	info	IKE 33.1.1.150 Phase 1: Aborted negotiations because the time limit has elapsed. (0000/269948975)
2002-07-22 16:16:39	info	IKE 33.1.1.150: XAuth login failed for gateway vpnphone-gw, username N/A, retry: 3, timeout: 1.
2002-07-22 16:14:33	info	IKE 33.1.1.150 Phase 1: Completed Aggressive mode negotiations with a 28800-second lifetime.
2002-07-22 16:14:33	info	IKE 33.1.1.150 Phase 1: Completed for user vpnphone@avaya.com.
2002-07-22 16:14:33	info	IKE<33.1.1.150> Phase 1: IKE responder has detected NAT in front of the remote device.
2002-07-22 16:14:32	info	IKE 33.1.1.150 Phase 1: Responder starts AGGRESSIVE mode negotiations.

### 11.2. Mismatched Phase 1 Proposal

- **Avaya VPNremote Phone display:**

```
IKE Phase1 no response
```

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

```
Error Code: 3997700:0
Module: IKMPD:142
```

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

```
Error Code: 3997700:0
Module: IKECFG:459
```

- **Juniper SSG WebUI: Reports > System Log > Event**

Date / Time	Level	Description
2002-07-22 16:39:02	info	Rejected an IKE packet on ethernet0/0 from 33.1.1.150:2070 to 44.2.2.2:500 with cookies c45c44e65d844c98 and c544ba3b69fb8d08 because There were no acceptable Phase 1 proposals.
2002-07-22 16:39:02	info	IKE 33.1.1.150 Phase 1: Responder starts AGGRESSIVE mode negotiations.
2002-07-22 16:38:59	info	Rejected an IKE packet on ethernet0/0 from 33.1.1.150:2070 to 44.2.2.2:500 with cookies c45c44e65d844c98 and e3c622a127b3b0dd because There were no acceptable Phase 1 proposals.
2002-07-22 16:38:59	info	IKE 33.1.1.150 Phase 1: Responder starts AGGRESSIVE mode negotiations.
2002-07-22 16:38:57	info	Rejected an IKE packet on ethernet0/0 from 33.1.1.150:2070 to 44.2.2.2:500 with cookies c45c44e65d844c98 and 095810ad9959f9b7 because There were no acceptable Phase 1 proposals.
2002-07-22 16:38:57	info	IKE 33.1.1.150 Phase 1: Responder starts AGGRESSIVE mode negotiations.
2002-07-22 16:38:55	info	Rejected an IKE packet on ethernet0/0 from 33.1.1.150:2070 to 44.2.2.2:500 with cookies c45c44e65d844c98 and ee0e928f920c8eb1 because There were no acceptable Phase 1 proposals.
2002-07-22 16:38:55	info	IKE 33.1.1.150 Phase 1: Responder starts AGGRESSIVE mode negotiations.
2002-07-22 16:38:53	info	Rejected an IKE packet on ethernet0/0 from 33.1.1.150:2070 to 44.2.2.2:500 with cookies c45c44e65d844c98 and 616d39c38567acab because There were no acceptable Phase 1 proposals.
2002-07-22 16:38:53	info	IKE 33.1.1.150 Phase 1: Responder starts AGGRESSIVE mode negotiations.
2002-07-22 16:36:14	notif	All logged events or alarms were cleared by admin netscreen

- **Juniper NetScreen-Remote > Log Viewer**

```

1-25: 18:47:43.484 My Connections\Phone Manager - Initiating IKE Phase 1 (IP ADDR=44.2.2.2)
1-25: 18:47:44.609 My Connections\Phone Manager - SENDING>>>> ISAKMP OAK AG (SA, KE, NON, ID, VID 6x)
1-25: 18:47:44.625 My Connections\Phone Manager - RECEIVED<<<< ISAKMP OAK INFO (NOTIFY:NO_PROPOSAL_CHOSEN)
1-25: 18:47:44.625 My Connections\Phone Manager - Discarding IKE SA negotiation
1-25: 18:47:48.984

```

## 11.3. Mismatched Phase 2 Proposal

- **Avaya VPNremote Phone display:**

**IKE Phase2 proposal mismatch**

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

```

IKE Phasel1 send notify
Error Code: 3997698:14
Module:NOTIFY:444

```

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

```

IKE Phase2 no response
Error Code: 3997700:0
Module:IKECFG:1184

```

- **Juniper SSG WebUI: Reports > System Log > Event**

Date / Time	Level	Description
2002-07-22 16:44:26	info	IKE 33.1.1.150 Phase 2 msg ID 0b3dfca0: Negotiations have failed.
2002-07-22 16:44:26	info	IKE 33.1.1.150 Phase 2 msg ID 0b3dfca0: Negotiations have failed for user vpnphone@avaya.com.
2002-07-22 16:44:26	info	Rejected an IKE packet on ethernet0/0 from 33.1.1.150:4500 to 44.2.2.2:4500 with cookies 8b629ff48139dc7c and 25d7fc38f2cd5ed9 because There were no acceptable Phase 2 proposals..
2002-07-22 16:44:26	info	IKE 33.1.1.150 Phase 2 msg ID 0b3dfca0: Responded to the peer's first message from user vpnphone@avaya.com.
2002-07-22 16:44:25	info	IKE 33.1.1.150: XAuth login was passed for gateway vpnphone-gw, username tom, retry: 0, Client IP Addr 10.10.10.1, IPPool name: VPNremote Phone, Session-Timeout: 0s, Idle-Timeout: 0s.
2002-07-22 16:44:25	info	IKE 33.1.1.150: XAuth login was refreshed for username tom at 10.10.10.1/255.255.255.255.
2002-07-22 16:44:25	info	IKE 33.1.1.150 Phase 1: Completed Aggressive mode negotiations with a 28800-second lifetime.
2002-07-22 16:44:25	info	IKE 33.1.1.150 Phase 1: Completed for user vpnphone@avaya.com.
2002-07-22 16:44:25	info	IKE<33.1.1.150> Phase 1: IKE responder has detected NAT in front of the remote device.
2002-07-22 16:44:23	info	IKE 33.1.1.150 Phase 1: Responder starts AGGRESSIVE mode negotiations.

## - Juniper NetScreen-Remote > Log Viewer

```

1-25: 18:51:47.328 My Connections\Phone Manager - SENDING>>>> ISAKMP OAK TRANS *(HASH, ATTR)
1-25: 18:51:47.484 My Connections\Phone Manager - Initiating IKE Phase 2 with Client IDs (message id: 87C9E3FF)
1-25: 18:51:47.484 My Connections\Phone Manager - Initiator = IP ADDR=10.10.10.26, prot = 0 port = 0
1-25: 18:51:47.484 My Connections\Phone Manager - Responder = IP SUBNET/MASK=0.0.0.0/0.0.0.0, prot = 0 port = 0
1-25: 18:51:47.484 My Connections\Phone Manager - SENDING>>>> ISAKMP OAK QM *(HASH, SA, NON, KE, ID 2x)
1-25: 18:51:47.484 My Connections\Phone Manager - RECEIVED<<<< ISAKMP OAK TRANS *(HASH, ATTR)
1-25: 18:51:47.484 My Connections\Phone Manager - IKE Extended Authentication successful.
1-25: 18:51:47.484 My Connections\Phone Manager - Setting compliance status to OK.
1-25: 18:51:47.484 My Connections\Phone Manager - Calling UpdateBypassRecordsForCompliance - OK.
1-25: 18:51:47.484 My Connections\Phone Manager - SENDING>>>> ISAKMP OAK TRANS *(HASH, ATTR)
1-25: 18:51:47.500 My Connections\Phone Manager - RECEIVED<<<< ISAKMP OAK INFO *(HASH, NOTIFY:NO_PROPOSAL_CHOSEN)
1-25: 18:51:47.500 My Connections\Phone Manager - Discarding IPSec SA negotiation
1-25: 18:51:47.500 My Connections\Phone Manager - Discarding IKE SA negotiation
1-25: 18:51:47.500 My Connections\Phone Manager - Deleting IKE SA (IP ADDR=44.2.2.2)
1-25: 18:51:47.500 My Connections\Phone Manager - MY COOKIE f3 e6 4a 68 94 64 74 1
1-25: 18:51:47.500 My Connections\Phone Manager - HIS COOKIE ad 94 b 7b 21 c6 29 45
1-25: 18:51:47.500 My Connections\Phone Manager - SENDING>>>> ISAKMP OAK INFO *(HASH, DEL)
1-25: 18:51:49.984
1-25: 18:51:49.984 My Connections\Phone Manager - Initiating IKE Phase 1 (IP ADDR=44.2.2.2)
1-25: 18:51:50.140 My Connections\Phone Manager - SENDING>>>> ISAKMP OAK AG (SA, KE, NON, ID, VID 6x)
1-25: 18:51:50.187 My Connections\Phone Manager - RECEIVED<<<< ISAKMP OAK AG (SA, VID 4x, KE, NON, ID, HASH, VID, NAT-D 2x)
1-25: 18:51:50.187 My Connections\Phone Manager - Peer supports Dead Peer Detection Version 1.0
1-25: 18:51:50.187 My Connections\Phone Manager - Dead Peer Detection enabled
1-25: 18:51:50.187 My Connections\Phone Manager - Peer is NAT-T draft-02 capable
1-25: 18:51:50.187 My Connections\Phone Manager - Dead Peer Detection enabled
1-25: 18:51:50.187 My Connections\Phone Manager - NAT is detected for Client
1-25: 18:51:50.187 My Connections\Phone Manager - Floating to IKE non-500 port
1-25: 18:51:50.296 My Connections\Phone Manager - SENDING>>>> ISAKMP OAK AG *(HASH, NAT-D 2x, NOTIFY:STATUS_REPLAY_STATU
1-25: 18:51:50.296 My Connections\Phone Manager - Established IKE SA
1-25: 18:51:50.296 My Connections\Phone Manager - MY COOKIE d0 24 e9 98 7f f3 91 7a
1-25: 18:51:50.296 My Connections\Phone Manager - HIS COOKIE eb 7e 6b 6d b8 d2 fd e7
1-25: 18:51:50.296 My Connections\Phone Manager - RECEIVED<<<< ISAKMP OAK TRANS *(HASH, ATTR)
1-25: 18:51:56.484 My Connections\Phone Manager - RECEIVED<<<< ISAKMP OAK TRANS *(Retransmission)
1-25: 18:52:02.500 My Connections\Phone Manager - RECEIVED<<<< ISAKMP OAK TRANS *(Retransmission)

```

## 12. Conclusion

The Avaya VPNremote Phone and Phone Manager Pro combined with Juniper SSG5 and NetScreen-Remote Windows VPN client provide a secure solution for remote worker telephony over broadband Internet connection.



## 13. Definitions and Abbreviations

The following terminology is used through out this document.

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

## 14. References

**Avaya Application Notes and Resources Web Site:**

<http://www.avaya.com/gcm/master-usa/en-us/resource/>

**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.

**Juniper Networks Product Support Web Site:**

<http://www.juniper.net/techpubs/>:

- [5] **Juniper Networks: Concepts & Examples ScreenOS Reference Guide; Volume 5: Virtual Private Networks Release 5.4.0, Rev. A**  
[http://www.juniper.net/techpubs/software/screenos/screenos5.4.0/CE\\_v5.pdf](http://www.juniper.net/techpubs/software/screenos/screenos5.4.0/CE_v5.pdf)
- [6] **Secure Services Gateway (SSG) 500 Series Hardware Installation and Configuration Guide ScreenOS Version 5.4.0**  
[http://www.juniper.net/techpubs/hardware/netscreen-systems/netscreen-systems54/SSG\\_HW\\_revA.pdf](http://www.juniper.net/techpubs/hardware/netscreen-systems/netscreen-systems54/SSG_HW_revA.pdf)
- [7] **Juniper Netscreen-Remote VPN Client Administrator's Guide, Version 8.7, P/N 093-1635-000, Rev. B.**
- [8] **Juniper Networks SSG 500 Series Product Page**  
[http://www.juniper.net/products\\_and\\_services/firewall\\_slash\\_ipsec\\_vpn/ssg\\_500\\_series/index.html](http://www.juniper.net/products_and_services/firewall_slash_ipsec_vpn/ssg_500_series/index.html)

---

**©2008 Avaya Inc. All Rights Reserved.**

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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 Solution & Interoperability Test Lab at [interoplabnotes@list.avaya.com](mailto:interoplabnotes@list.avaya.com).