

Avaya Solution & Interoperability Test Lab

Configuring the Juniper Networks SSG Security Platform and Steel-Belted Radius Authentication Server to Support Avaya VPNremote Phones – Issue 1.0

Abstract

These Application Notes describe the steps for configuring the Juniper Networks SSG security platform and Steel-Belted Radius authentication server to support Avaya VPNremote Phones. The Juniper Networks SSG, running the ScreenOS operating system, provides the secure termination of IPSec VPN tunnels with Avaya VPNremote Phones and functions as a RADIUS client for VPNremote Phone user authentication. The Juniper Networks Steel-Belted Radius, functioning as a RADIUS server, provides authentication of VPNremote Phone users as well as IP address assignment for Avaya VPNremote Phones.

The sample configuration presented in these Application Notes enables network administrators to easily map individual Avaya VPNremote Phones to specific Network Regions of Avaya Communication Manager. Unique Network Region parameters can then be assigned to different groups of VPNremote Phones. One example where this might be useful is to assign VPNremote Phones used over broadband Internet connections with limited available bandwidth the G.729a voice codec while VPNremote Phones used over broadband Internet connections with sufficient bandwidth the G.711 voice codec.

©2007 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the steps for configuring the Juniper Networks SSG security platform and Steel-Belted Radius authentication server to support Avaya VPNremote Phones. The Juniper Networks SSG, running the ScreenOS operating system, provides the secure termination of IPSec VPN tunnels with Avaya VPNremote Phones and functions as a RADIUS client for VPNremote Phone user authentication. The Juniper Networks Steel-Belted Radius, functioning as a RADIUS server, provides authentication of VPNremote Phone users as well as IP address assignment for Avaya VPNremote Phones.

The sample configuration presented in these Application Notes enables network administrators to easily map individual Avaya VPNremote Phones to specific Network Regions of Avaya Communication Manager. Unique Network Region parameters can then be assigned to different groups of VPNremote Phones. One example where this might be useful is to assign VPNremote Phones used over broadband Internet connections with limited available bandwidth the G.729a voice codec while VPNremote Phones used over broadband Internet connections with sufficient bandwidth the G.711 voice codec.

The mapping of VPNremote Phones to a specific Network Region is accomplished by using Avaya Communication Managers IP Address Mapping capability combined with Juniper Steel-Belted Radius IP Address Pool assignment. Specifically, two user profiles are created on the Juniper Steel-Belted Radius server. Each profile is associated with an IP address Pool which contains a unique range of IP addresses to be assigned to the VPNremote Phones. Each of these unique IP address ranges are mapped to a Network Region in Avaya Communication Manager, one Network Region is configured with an IP Codec Set of G.711 and the other Network Region is configured with an IP Codec Set of G.729a. Each VPNremote Phone user account created in the Juniper Steel-Belted Radius server is assigned to one of the user profiles which will determine the Network Region the VPNremote Phone is associated with and the voice codec the VPNremote Phone will use.

The configuration steps described in these Application Notes utilize a Juniper SSG model 520M. However, these configuration steps can be applied to Juniper NetScreen and ISG platforms using the ScreenOS version specified in **Table 1**.

2. Network Topology

The sample network implemented for these Application Notes is shown in **Figure 1.** The Main Campus location contains the Juniper SSG 520M functioning as perimeter security device and VPN head-end. The Avaya Phone File Server and Avaya WebLM License Manager are running on the same physical server while the Juniper Steel-Belted Radius server is running on a stand-alone server within the trusted enterprise LAN. The Avaya S8710 Servers and Avaya G650 Media Gateway are also located at the Main Campus within the trusted enterprise LAN.

The ‘call out’ boxes included in **Figure 1** list the VPNremote Phone user accounts, user profile associations and IP address Pool mapping as configured in the Steel-Belted Radius server as well as the IP address to Network Region Mapping of Avaya Communication Server.

©2007 Avaya Inc. All Rights Reserved.

The Avaya VPNremote Phones are located in public Internet accessible locations, typically home networks with broadband Internet connectivity, and are configured to establish an IPSec tunnel to the Public (untrusted) interface of the Juniper SSG 520M. The Juniper SSG 520M communicates with the Steel-Belted Radius server for user authentication and IP address assignment. This assigned IP address, also known as the inner address, will be used by the VPNremote Phone when communicating inside the IPSec tunnel and in the private corporate network to Avaya Communication Manager. Once the IPSec tunnel is established, the VPNremote Phone accesses the Avaya Phone File Server and Avaya WebLM server. The VPNremote Phone then initiates an H.323 registration with Avaya Communication Manager.

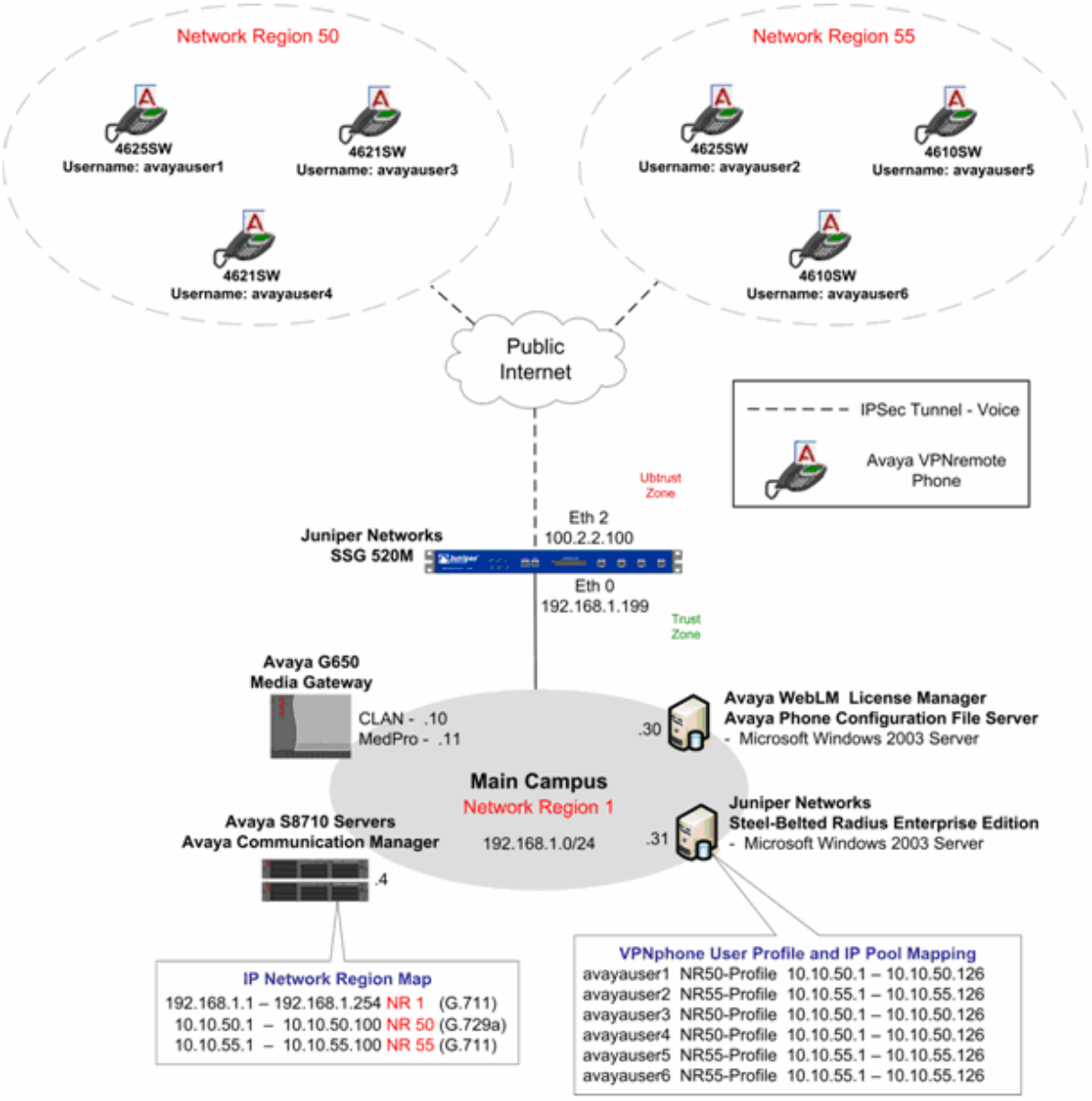


Figure 1 - Network Diagram

©2007 Avaya Inc. All Rights Reserved.

3. Equipment and Software Validated

The information in these Application Notes is based on the software and hardware versions list in **Table 1** below.

Equipment	Software Version
Avaya S8710 Servers	Avaya Communication Manager 3.1.2 (R013x.01.2.632.1)
Avaya G650 Media Gateway IPSI (TN2312BP) C-LAN (TN799DP) MedPro (TN2302AP)	 FW 022 (HW6) FW 016 (HW1) FW 108 (HW12)
Avaya 4610SW IP Telephones	R2.3.2 – **Release 2** (a10bVPN232_1.bin)
Avaya 4621SW IP Telephones	R2.3.2 – **Release 2** (a20bVPN232_1.bin)
Avaya 4625SW IP Telephones	R2.5.2 – **Release 2** (a25VPN252_1.bin)
Juniper Networks SSG 520M	ScreenOS 5.4.0r2.0
Juniper Networks Steel-Belted Radius Enterprise Edition	Version 6.0

Table 1 – Software/Hardware Version Information

4. Juniper Networks SSG 520M Configuration

This section describes the steps necessary to configure the Juniper SSG 520M to support IPSec VPN termination of Avaya VPNremote Phones. The configuration steps below utilize the Web User Interface (WebUI) of the Juniper SSG 520M. These Application Notes assume the basic administration and network interface configuration of the Juniper SSG 520M has been performed and network connectivity to both the Trusted and Untrusted security zones exists. For the sample configuration, interface 'Ethernet 0/0' of the Juniper SSG 520M is configured to a Trust security zone facing the internal corporate network while interface 'Ethernet 0/2' is configured to an Untrust security zone facing the public internet (see the Juniper SSG interface summary below). The Avaya VPNremote Phone interacts with 'Ethernet 0/2' when establishing an IPSec Tunnel.

The following areas are covered in this section.

1. WebUI Log In
2. Configuring a Default Route
3. Authentication Server Configuration
4. IKE User Configuration
5. IKE User Group Configuration
6. AutoKey IKE Gateway Configuration - Phase 1
7. AutoKey IKE VPN Tunnel Configuration - Phase 2

©2007 Avaya Inc. All Rights Reserved.

8. Security Policies

4.1. WebUI Log In

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



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

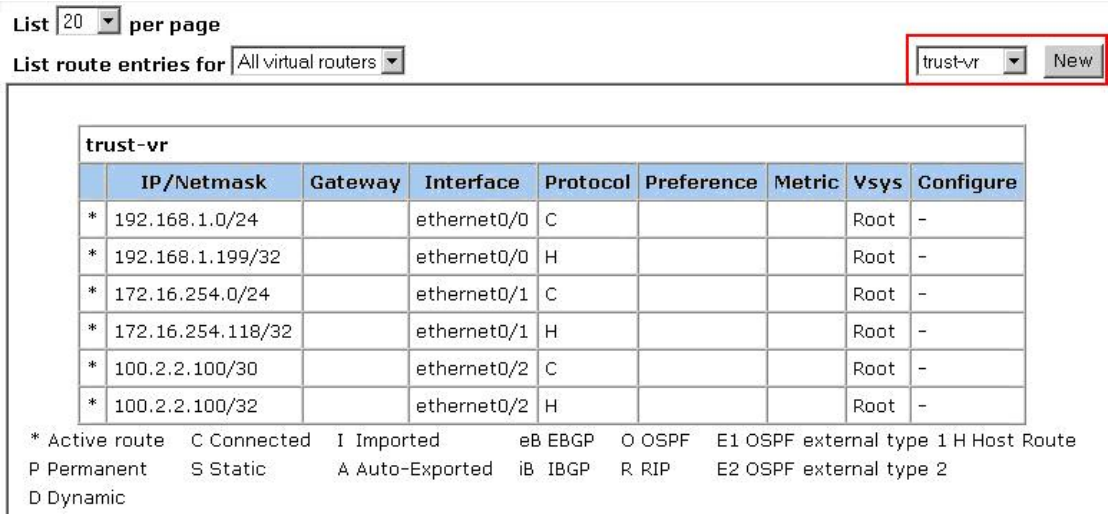
Device Information	
Hardware Version:	0(0)
Firmware Version:	5.4.0r2.0 (Firewall+VPN)
Serial Number:	JN1090890ADA
Host Name:	SSG520M

©2007 Avaya Inc. All Rights Reserved.

4.2. Configuring a Default Route

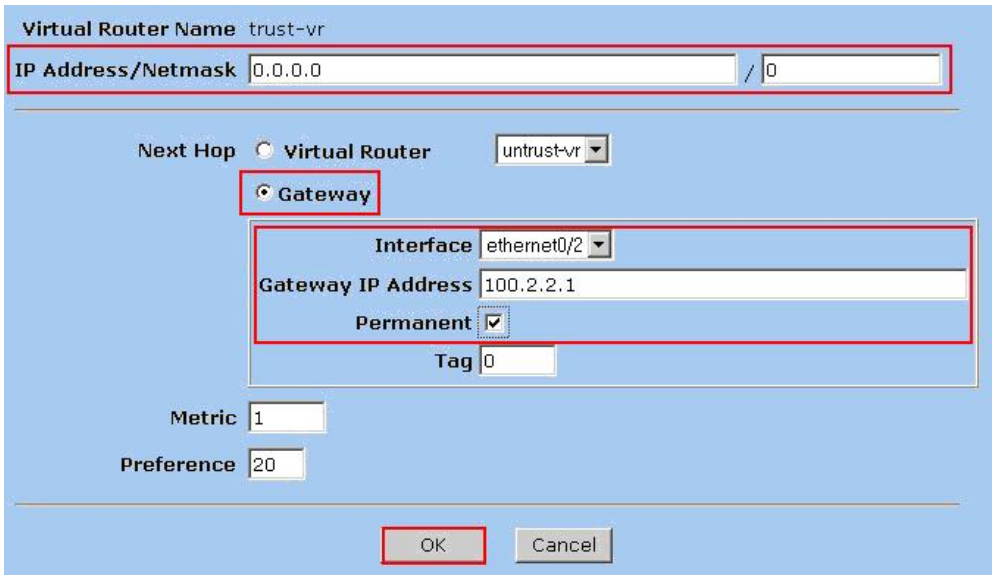
The sample configuration uses a static default route entry to interface Ethernet 0/2 in the Untrust zone.

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 click **New**.



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 of interface Ethernet 0/2 to the public internet.



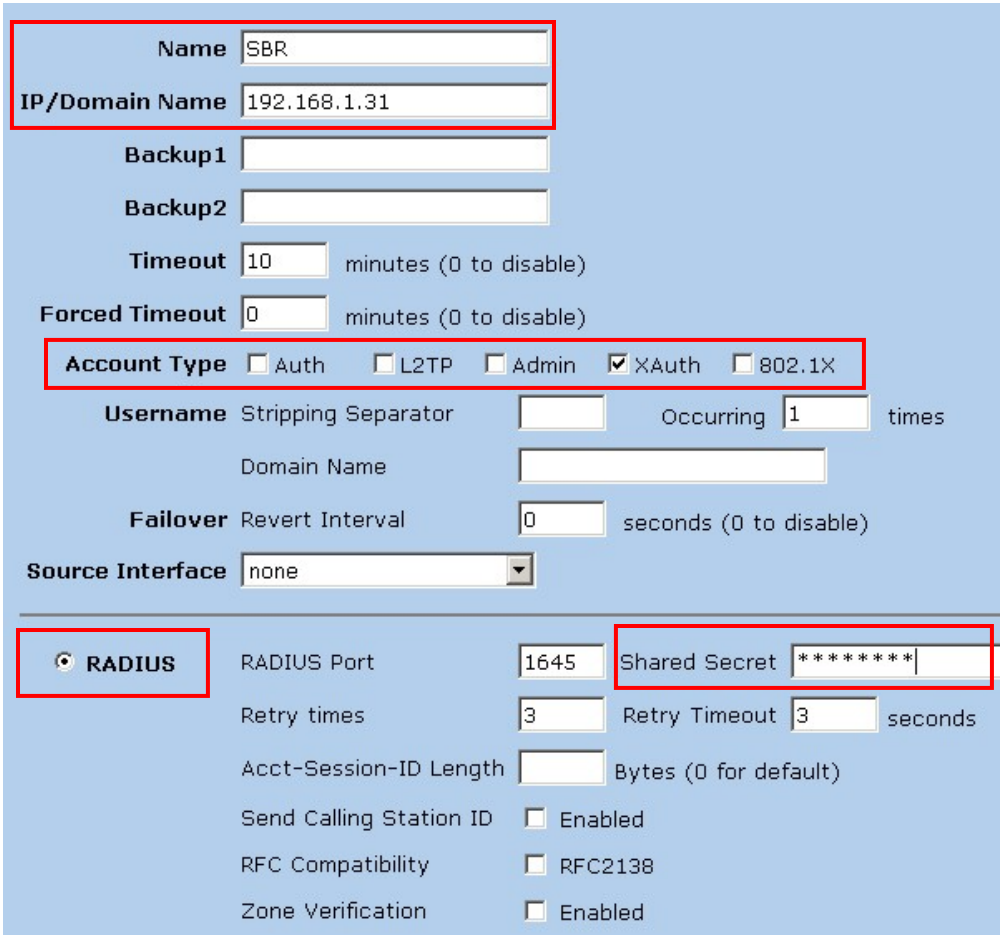
©2007 Avaya Inc. All Rights Reserved.

4.3. Authentication Server Configuration

The Juniper SSG 520M running ScreenOS includes a local authentication server for user authentication. To use an external authentication server, such as Steel-Belted Radius, the SSG 520M must be configured to communicate with the external authentication server as described below.

From the left navigation menu, select **Configuration → Auth → Auth Servers → New**. From the New Auth Server window that appears, enter the following information. Click **OK** when complete (not shown).

- **Name:** Name of the authentication server.
- **IP / Domain Name:** Host name or IP address of the authentication server for the SSG 520M to communicate with.
- **Account Type:** Check **XAuth** to support the XAuth protocol used by Avaya VPNphones.
- **RADIUS:** Select the RADIUS button to specify the authentication server will use the RADIUS protocol.
- **Shared Secret:** Text string used to authenticate with the RADIUS server. The same text string must match the RADIUS server.



©2007 Avaya Inc. All Rights Reserved.

4.4. IKE User Configuration

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.

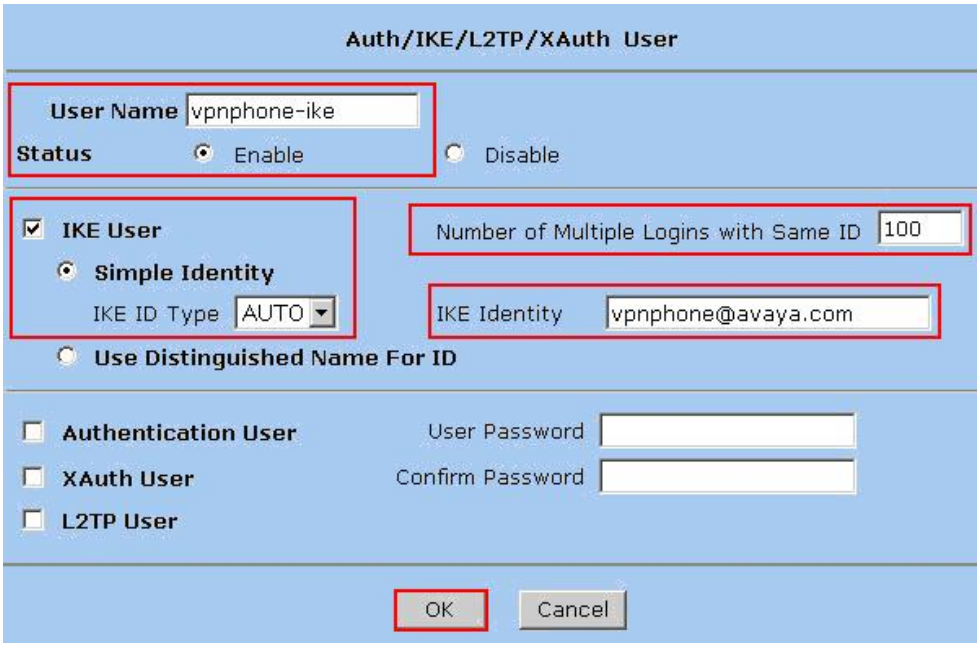
The following steps create an IKE user to be used by Avaya VPNremote Phones for IKE authentication.

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.

   Choose a descriptive name for the **User Name** field.

   The **Number of Multiple Logins with Same ID** parameter specifies the number of endpoints that can concurrently establish IPSec tunnels using this identity. This number must equal or exceed the number of Avaya VPNremote Phones simultaneously 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 Section 6, the Group Name field of the Avaya VPNremote Phone must match this IKE Identity string. The IKE Identity string vpnphone@avaya.com is used in these Application Notes however any email address string can be used.



©2007 Avaya Inc. All Rights Reserved.

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

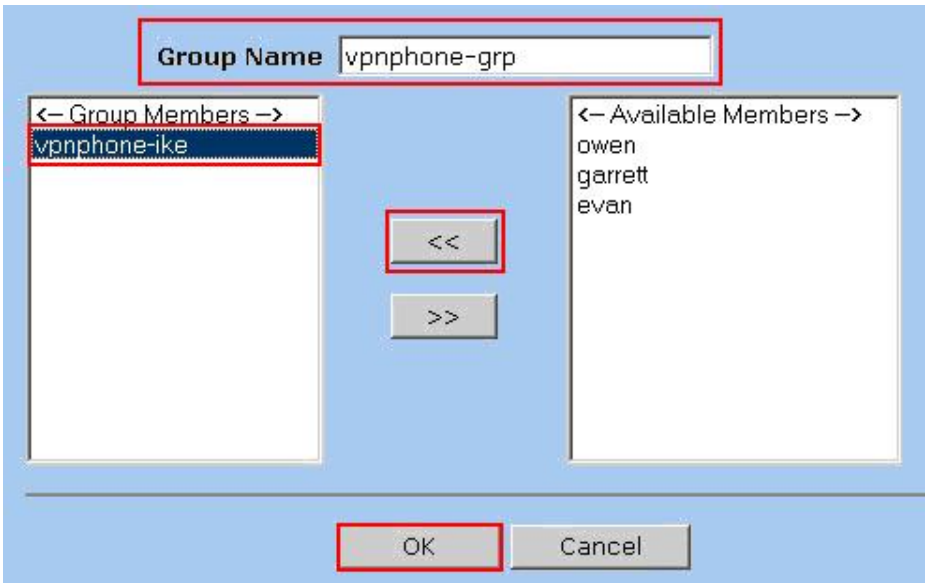
Name	Type	Group	Status	Identity	Configure	
vpnphone-ike	IKE	-	Enabled	vpnphone@avaya.com	Edit	Remove

4.5. IKE 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 polices for each individual user.

From the left navigation menu, select **Objects → User → Local Groups → New**.

Enter a descriptive **Group Name**. Select the vpnphone-ike user name 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.



©2007 Avaya Inc. All Rights Reserved.

4.6. VPN Configuration

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

- Phase 1 covers how the Avaya VPNremote Phone and the Juniper SSG will securely negotiate and handle the building of the tunnel.
- 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 2 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 2 – IKE P1 /P2 Proposals

4.6.1. AutoKey IKE Gateway Configuration - Phase 1

1. 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**. Selecting a Security Level of **Custom** provides access to a more complete list of proposals available on this Juniper SSG. Selecting **Dialup User Group** associates the Group **vpnphone-grp** created in Section 4.6 to this IKE gateway.

   Enter an ASCII text string for the **Preshared Key** that will match the text entered on the Avaya VPNremote Phone.

   Outgoing Interface is the interface which terminates the VPN tunnel.

   Select **Advanced** to access additional configuration options.

©2007 Avaya Inc. All Rights Reserved.



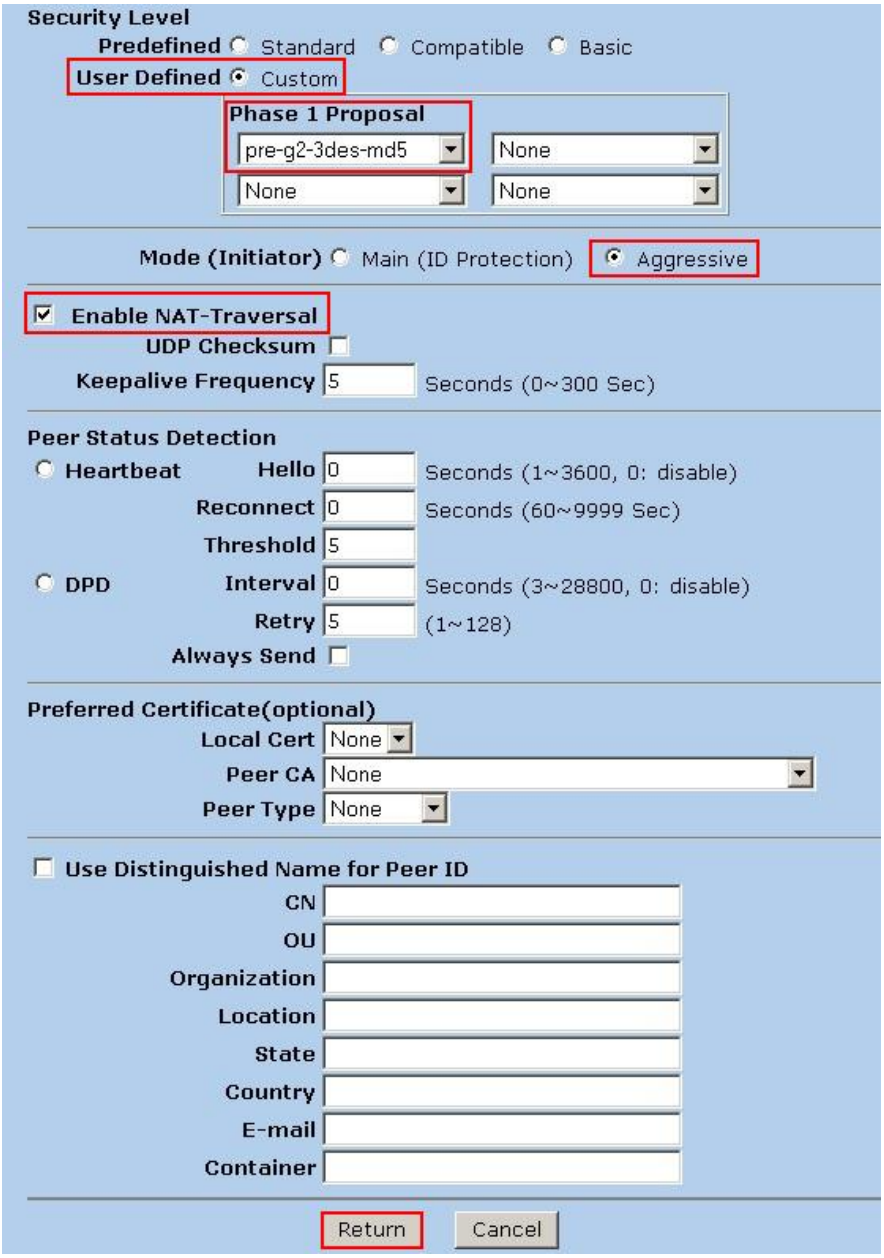
2. Configure the highlighted fields shown below. All remaining fields can be left as default. Select **Return** to complete the advanced configuration, and then **OK** to save.

   Select Security Level of **Custom** and the appropriate **Phase 1 Proposal** from the drop-down menu. Refer to **Table 2 – IKE P1 / P2 Proposals**.

   Mode of **Aggressive** 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.

©2007 Avaya Inc. All Rights Reserved.



3. Because the IKE group was selected in Step 1 above, a pop-up window is displayed as a reminder to enable the XAuth server. Under the SSG Authentication Server configuration in Section 4.3, XAuth was selected for the Account Type to use with Steel-Belted Radius. Select **OK**.



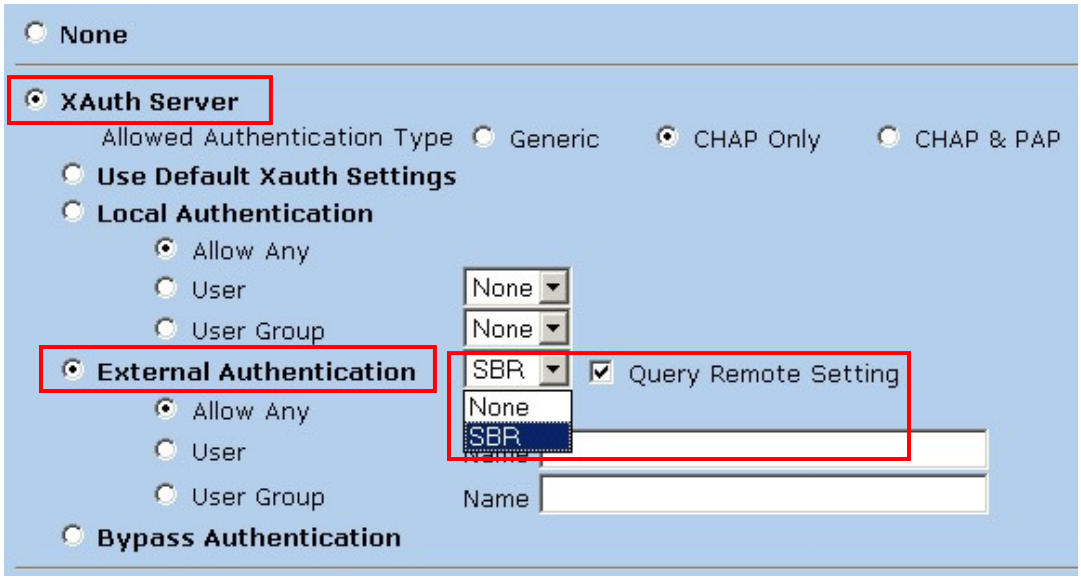
©2007 Avaya Inc. All Rights Reserved.

4. The **AutoKey Advanced → Gateway** list page displays the new gateway.

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

5. Click **Xauth** for the new gateway entry.

   Select **XAuth Server** and **CHAP Only** for Allowed Authentication Type. Select **External Authentication** then the name of the authentication server created in Section 4.3. Select the **Query Remote Setting** check box then click **OK** (not shown).



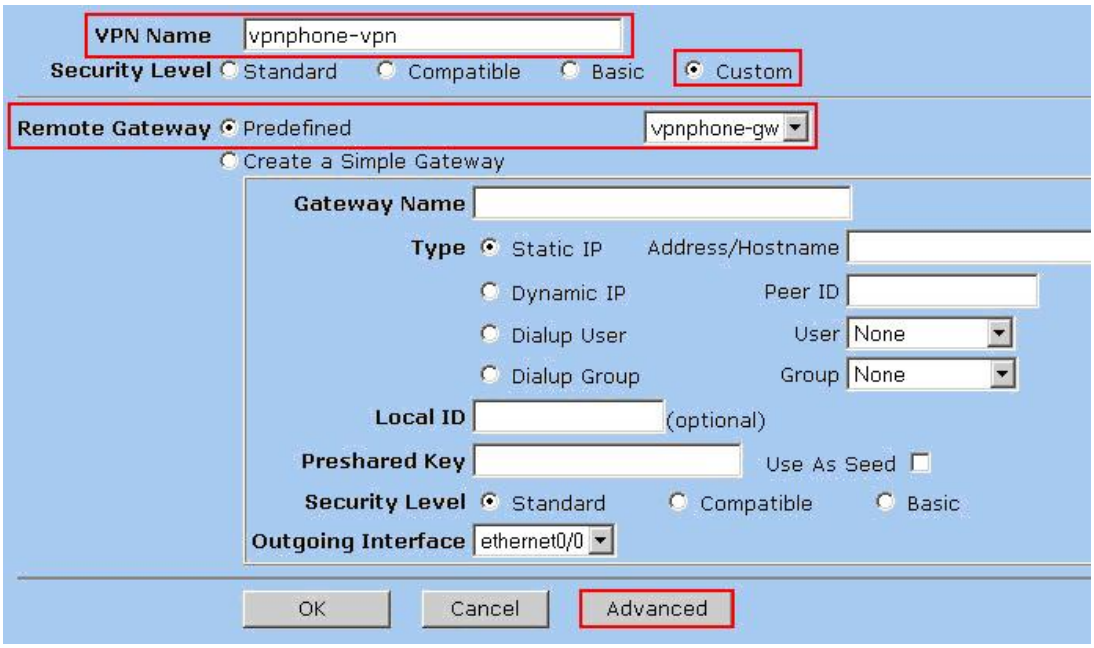
4.6.2. AutoKey IKE VPN Tunnel Configuration - Phase 2

1. From the left navigation menu, select **VPNs → AutoKey IKE → New**. Configure the highlighted fields shown below. All remaining fields can be left as default.

   Provide a descriptive **VPN Name**. Selecting a Security Level of **Custom** provides access to a more complete list of proposals available on the Juniper SSG. Select **Predefined** for Remote Gateway and then select the Remote Gateway name entered in Section 4.6.1, **vpnphone-gw**, from the drop-down menu.

   Select **Advanced** to access additional configuration options.

©2007 Avaya Inc. All Rights Reserved.



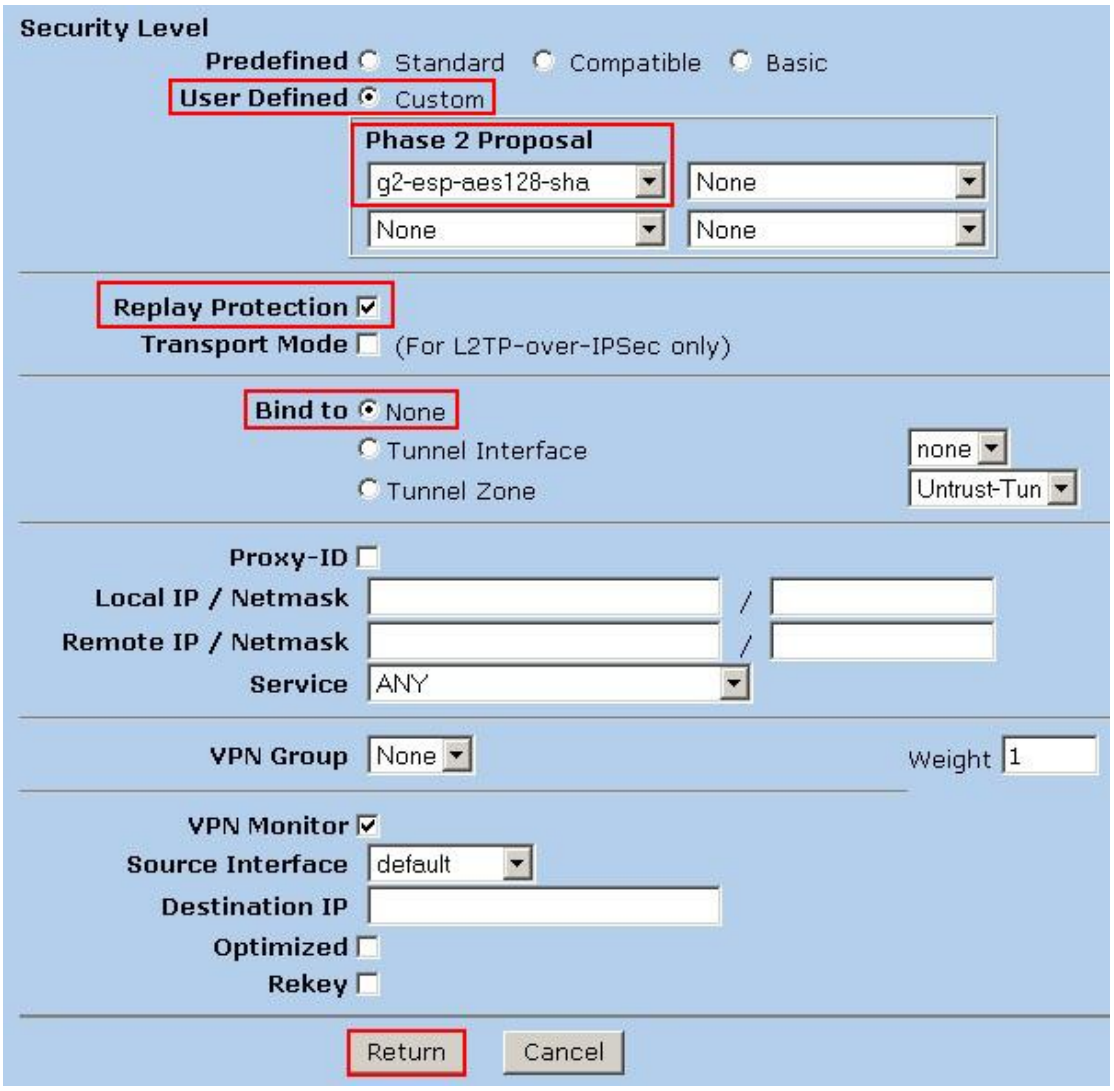
2. Configure the highlighted fields shown below. All remaining fields can be left as default. Select **Return** to complete the advanced configuration, and then **OK** to save.

   Select the appropriate **Phase 2 Proposal** from the drop-down menu. Refer to **Table 2 – IKE P1 / P2 Proposals**.

   Replay Protection 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.

   Bind to None uses the outgoing interface, Ethernet 0/2, for all VPN tunnel traffic.

©2007 Avaya Inc. All Rights Reserved.



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

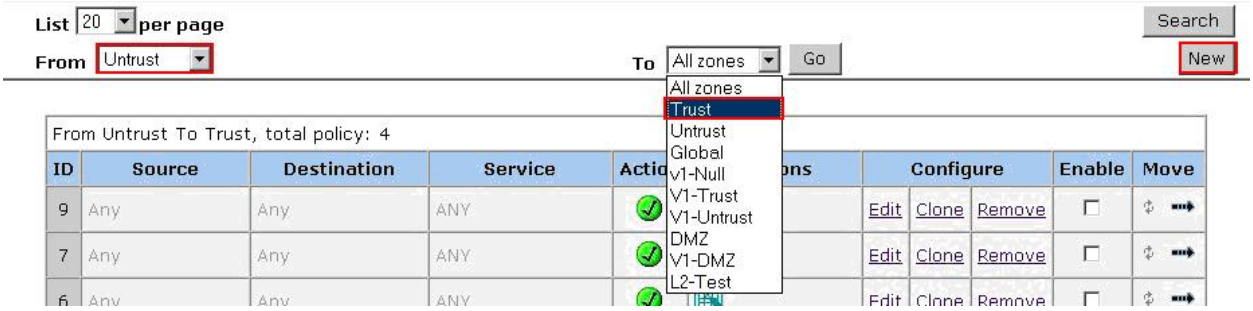
Name	Gateway	Security	Monitor	Configure	
vpnphone-vpn	vpnphone-gw	Custom	On	Edit	Remove

©2007 Avaya Inc. All Rights Reserved.

4.7. Security Policies

1. From the left navigation menu select **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. 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.

   Selecting Dial-Up VPN from the **Source Address** drop-down menu and Any from the **Destination Address** defines the VPN tunnel as the traffic originator.

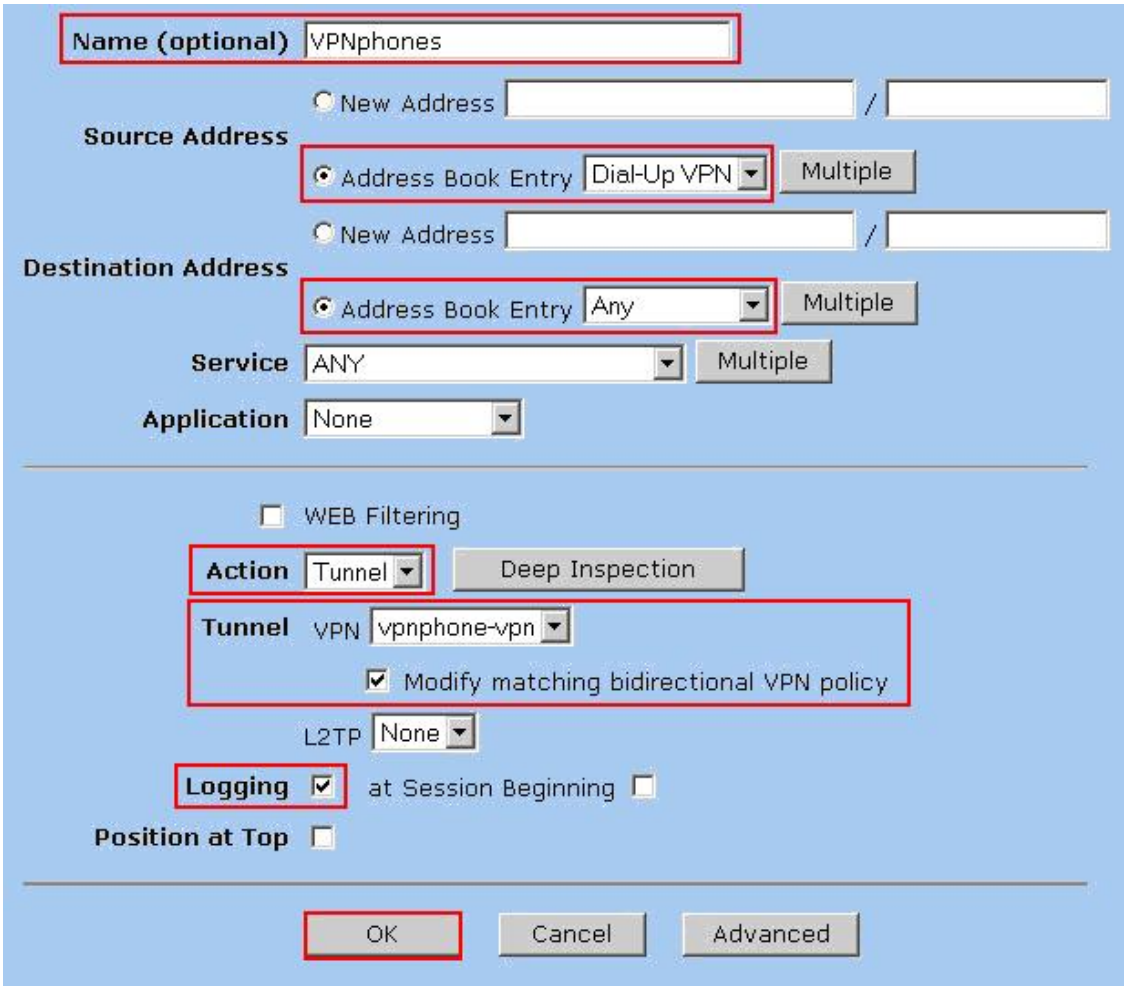
   Selecting Tunnel from the **Action** field drop-down menu indicates the action the SSG will take against traffic that matches the first three criteria of the policy: Source Address, Destination Address, and Service. All matching traffic will be associated with a particular VPN tunnel specified in the **Tunnel** field.

   Selecting 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.

   Enabling **Logging** will generate syslog events associated with this policy.

©2007 Avaya Inc. All Rights Reserved.



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

From Untrust To Trust, total policy: 1										
ID	**Source**	**Destination**	**Service**	**Action**	**Options**	**Configure**			**Enable**	**Move**
1	Dial-Up VPN	Any	ANY			Edit	Clone	Remove	☑	
From Trust To Untrust, total policy: 1										
ID	**Source**	**Destination**	**Service**	**Action**	**Options**	**Configure**			**Enable**	**Move**
2	Any	Dial-Up VPN	ANY			Edit	Clone	Remove	☑	

©2007 Avaya Inc. All Rights Reserved.

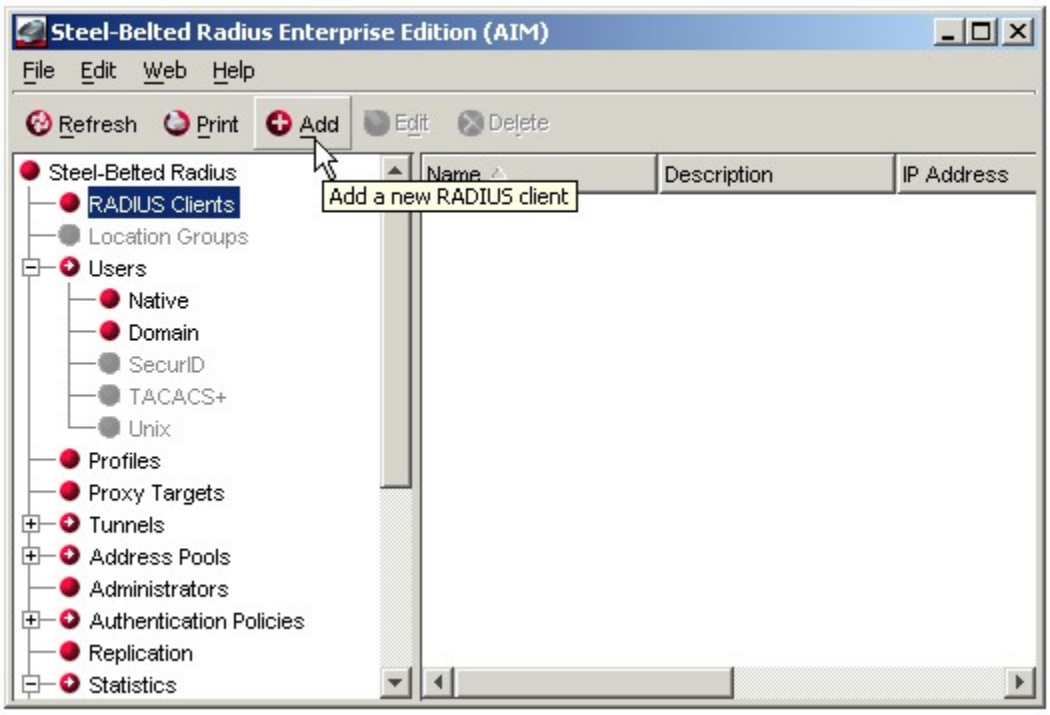
5. Juniper Networks Steel-Belted Radius Configuration

The following areas are covered in this section.

1. RADIUS Client
2. IP Address Pools
3. User Profiles
4. User Accounts

5.1. RADIUS Client

1. Start the Steel-Belted Radius Administration application and select **RADIUS Clients** from the left navigation window. Click **Add** on the top tool bar.



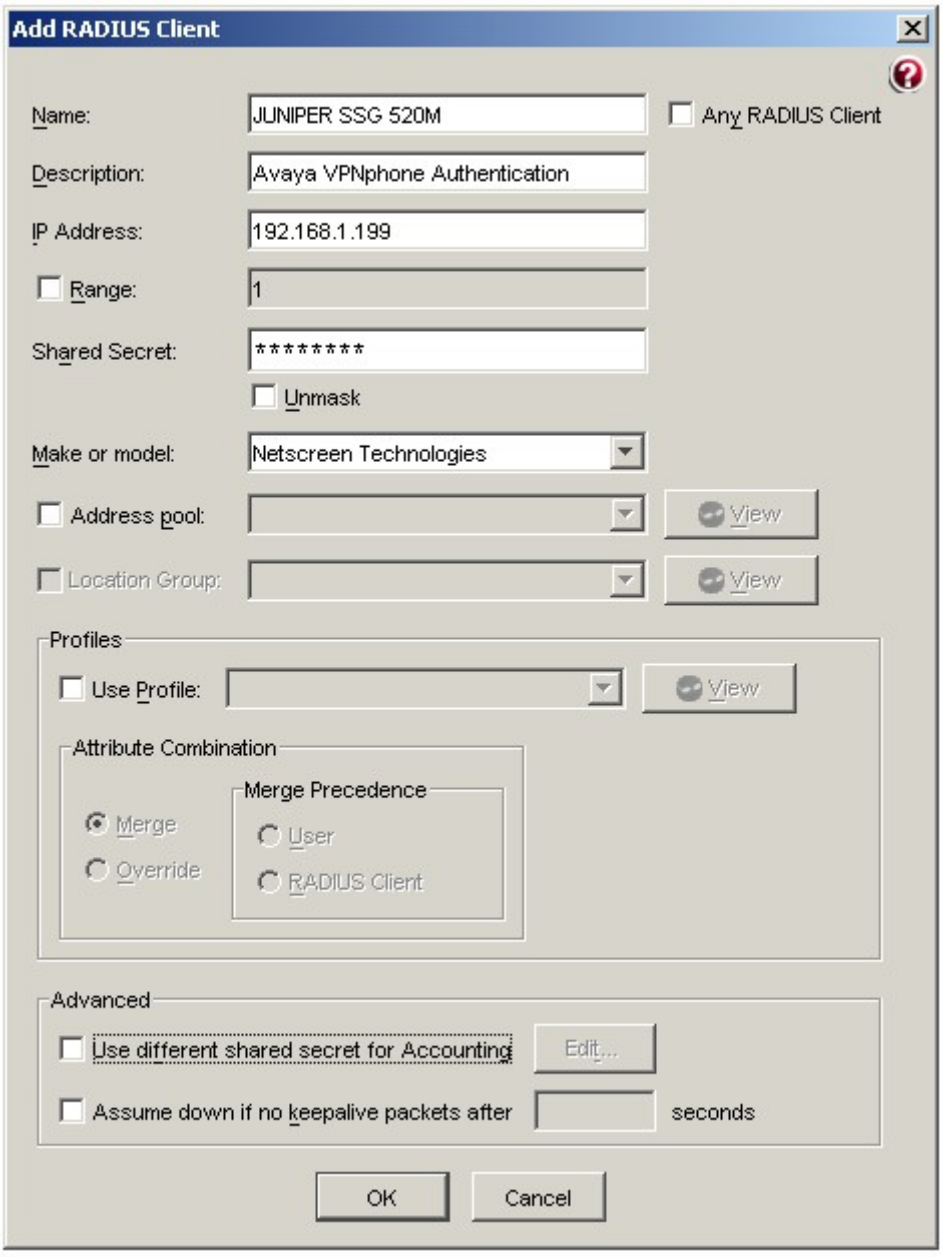
2. From the Add RADIUS Client window enter the following information:

- **Name:** Name of the RADIUS client.
- **Description:** A description of the RADIUS client for easy identification.
- **IP Address:** Host name or IP address of RADIUS client for Steel-Belted Radius to communicate with. The Juniper SSG is used in the sample configuration.
- **Shared Secret:** Text string used to authenticate with the RADIUS client. The same text string must match the RADIUS client.

©2007 Avaya Inc. All Rights Reserved.

- **Make or model:** Identifies the RADIUS client to determine the available RADIUS attributes. In the sample configuration, the Juniper SSG 520M is the RADIUS client, therefore **Netscreen Technologies** is used.

All remaining fields can be left at default values. Click **OK**

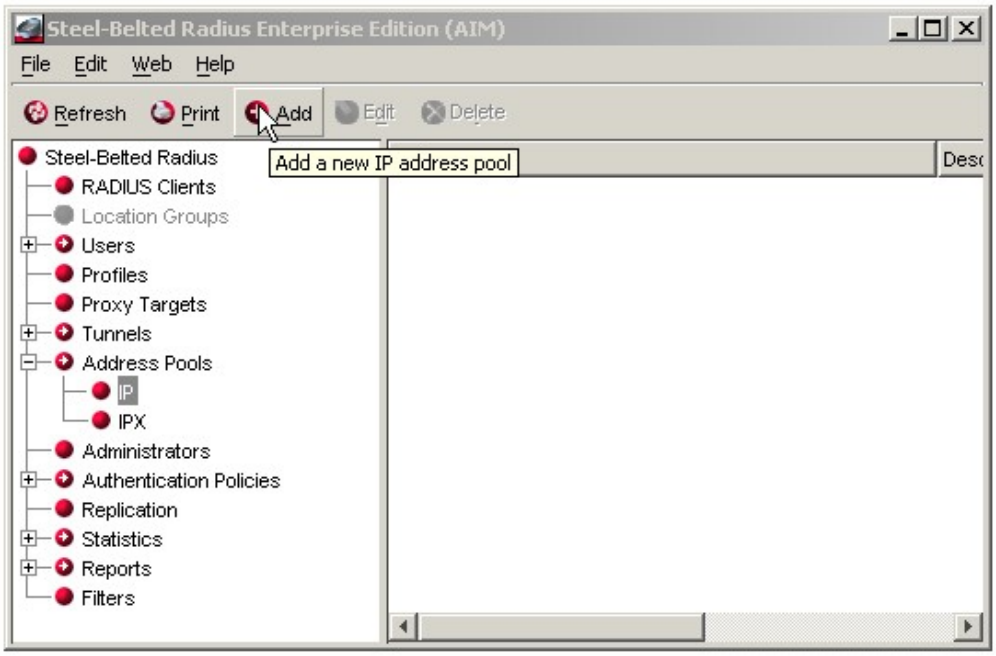


©2007 Avaya Inc. All Rights Reserved.

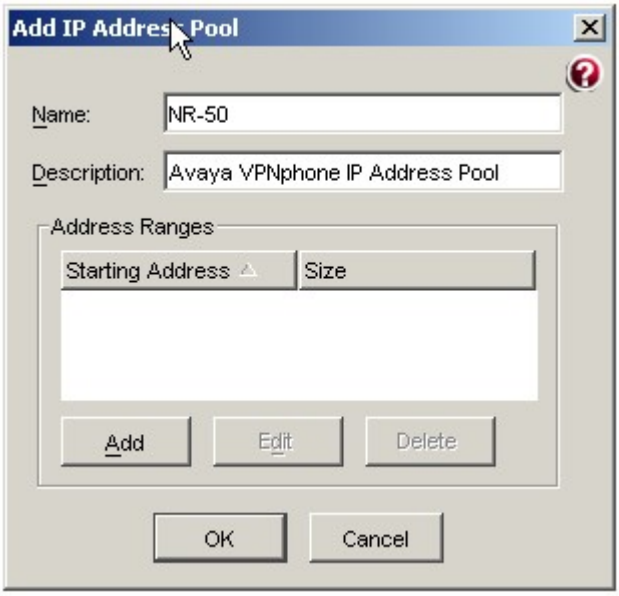
5.2. IP Address Pools

Two IP address pools are created in the sample configuration, one named NR-50 and one named NR-55. The steps below show the creation of the NR-50 address pool. Follow the same steps to create additional address pools as needed.

1. From the Steel-Belted Radius Administration GUI, expand **Address Pools** then select **IP** from the left navigation window. Click **Add** on the top tool bar.

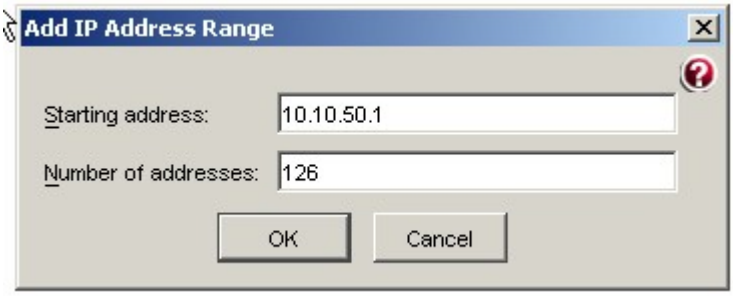


2. Enter a **Name** and **Description** for the new address pool then click **Add**.



©2007 Avaya Inc. All Rights Reserved.

3. Enter the starting IP address and number of addresses to include in the pool. The IP address used in the sample configuration for NR-50 included 126 addresses to match a Netmask of 255.255.255.128. Click **OK** to save this address range entry.



4. Click **OK** to save the new address pool.

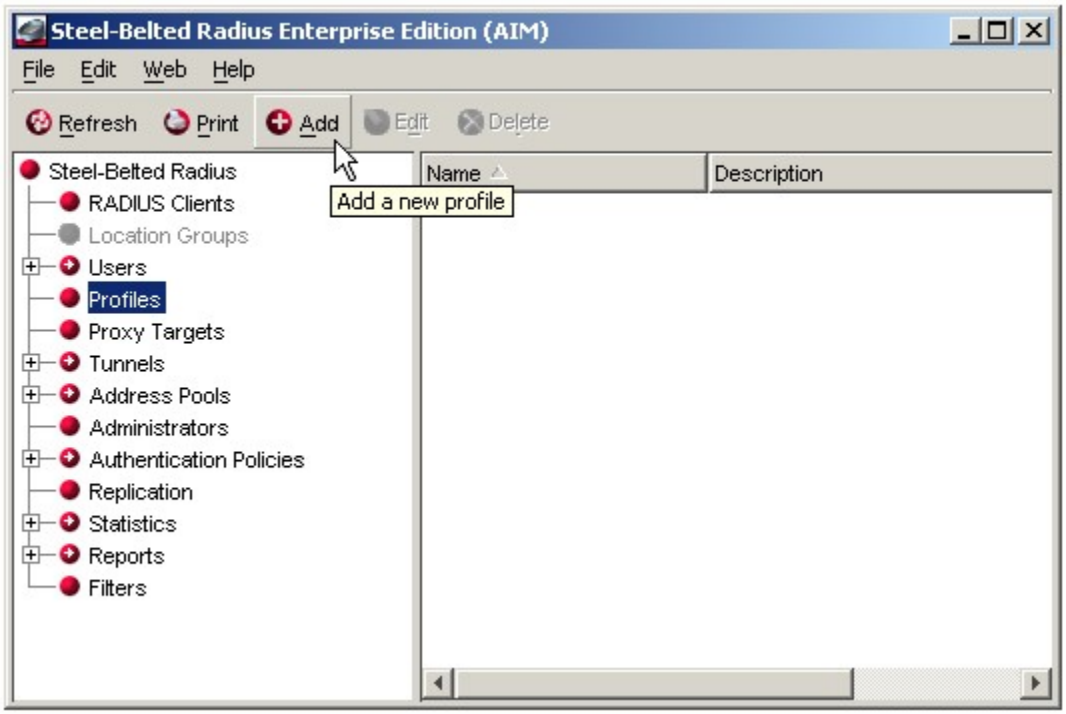


5.3. User Profiles

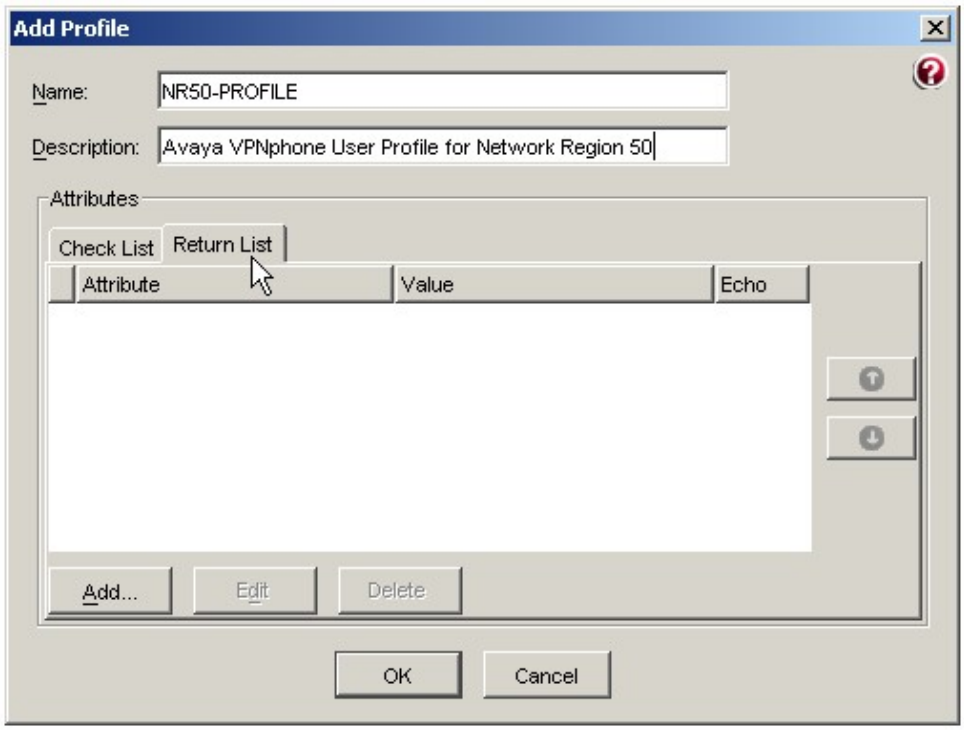
Two user profiles are created in the sample configuration, AVAYA-VPNPHONE-NR50 and AVAYA-VPNPHONE-NR55. The steps below show the creation of the AVAYA-VPNPHONE-NR50 user profile. Follow the same steps to create additional user profiles as needed.

1. From the Steel-Belted Radius Administration GUI, select **Profiles** from the left navigation window. Click **Add** on the top tool bar.

©2007 Avaya Inc. All Rights Reserved.

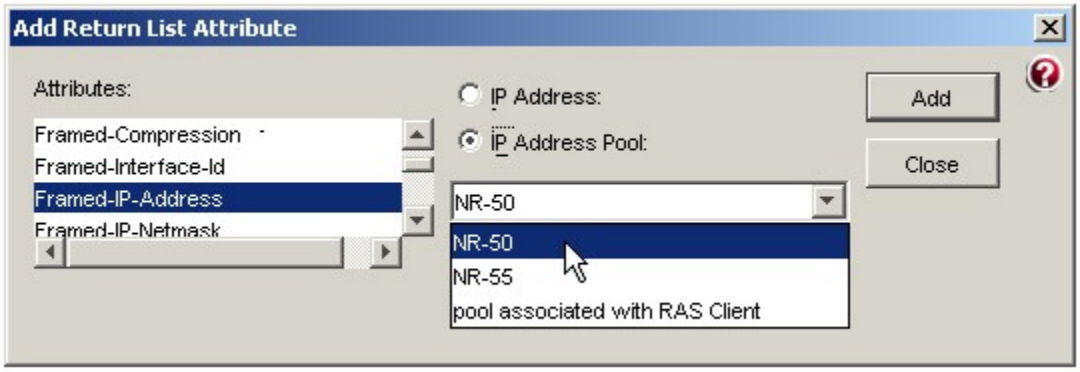


2. From the Add Profile window, enter the new profile **Name** and **Description**. Click the **Return List** tab then **Add**. The Check List tab specifies attributes the RADIUS server looks for in messages coming from RADIUS clients. The Return List tab specifies attributes the RADIUS server includes in messages being sent back to RADIUS clients.

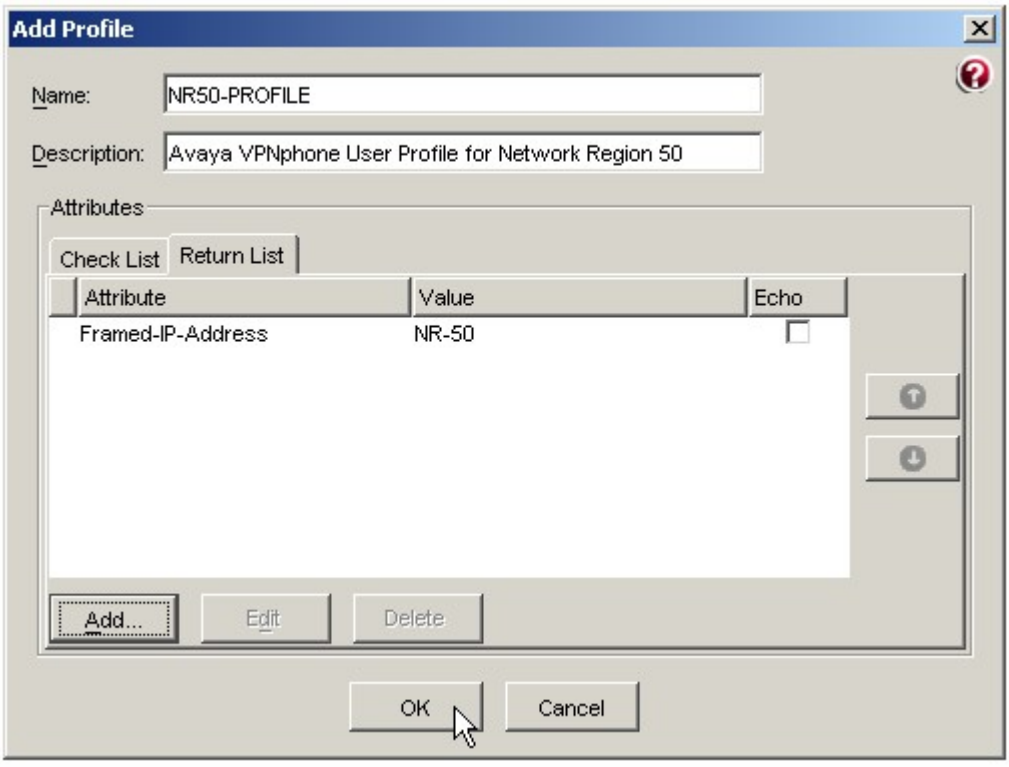


©2007 Avaya Inc. All Rights Reserved.

3. From the Add Return List Attribute window, select **Framed-IP-Address** from the Attributes list. Select the **IP Address Pool** radio button. From the dorp-down list, select the name of the IP Address Pool, created in Section 5.2, for which this user profile is to be associated with. Click **Add** then **Close**.



4. The Add Profile window is re-activated. Click **OK** to save.



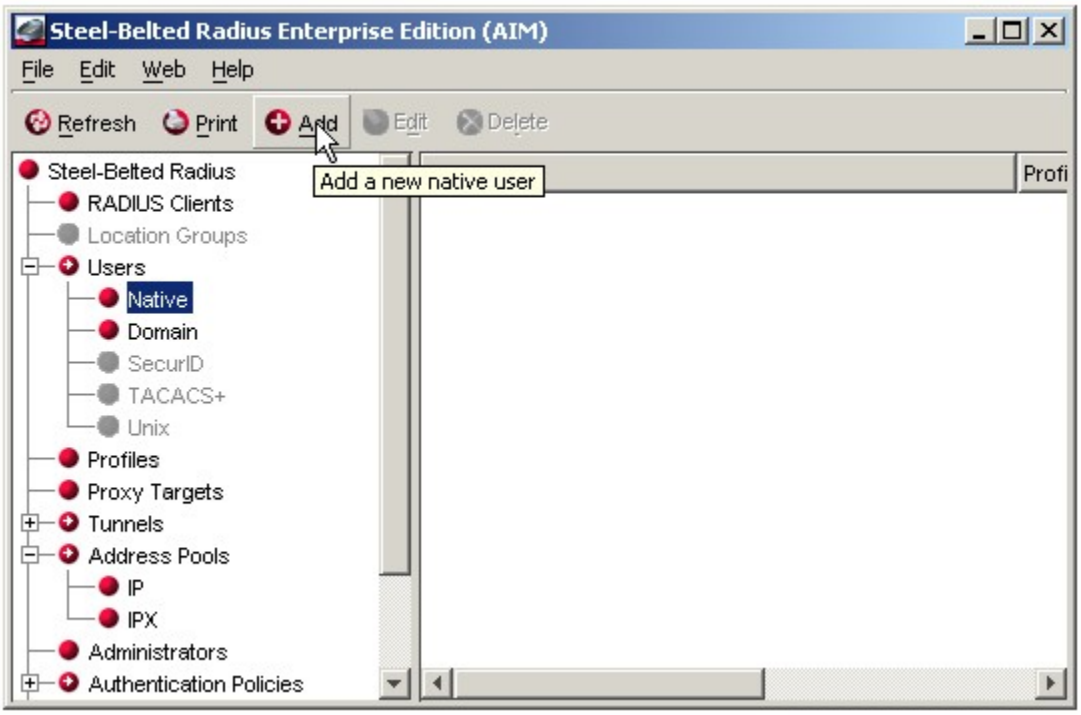
©2007 Avaya Inc. All Rights Reserved.

5.4. User Accounts

Six user accounts are created in the sample configuration, avayauser1 through avayauser6. The steps below show the creation of the avayauser1 user account. Follow the same steps to create additional user accounts as needed.

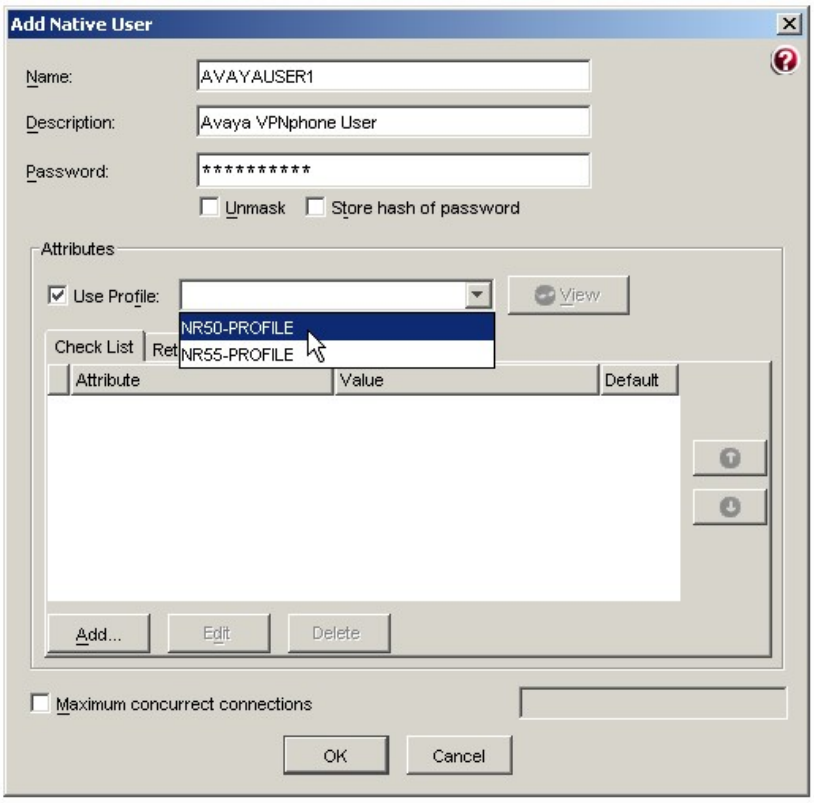
Note: the text of the user name entered in Steel-Belted Radius shows as caps, however the name is not case sensitive i.e., the user name entered on the VPNremote Phone can be entered as all lower case.

1. From the Steel-Belted Radius Administration GUI, expand **User** then select **Native** from the left navigation window. Click **Add** on the top tool bar.

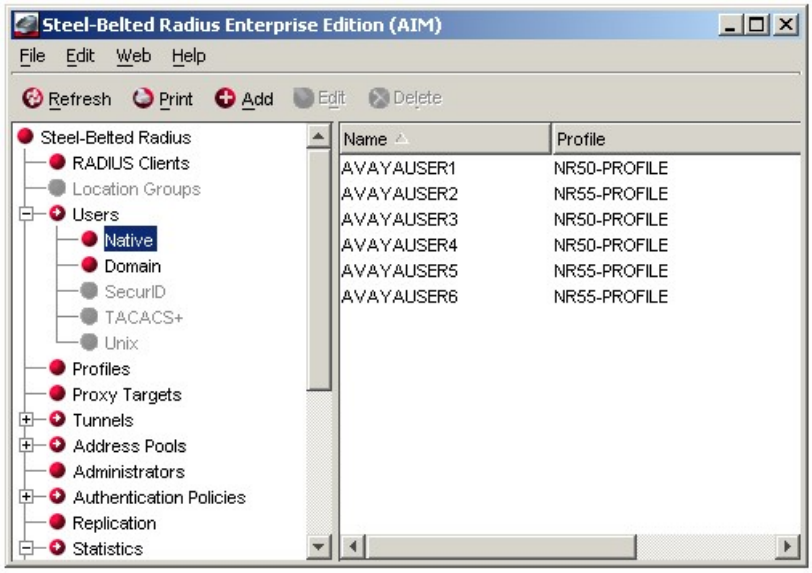


©2007 Avaya Inc. All Rights Reserved.

2. From the Add Native User window, enter the new user **Name**, **Description** and **Password**. Click the **Use Profile** check box and select the profile this user is to be associated with from the drop-down list. Click **OK.**



3. The new user accounts are listed in the Steel-Belted Radius Administration GUI under **User → Native** with the associated profile of each user as shown below.



©2007 Avaya Inc. All Rights Reserved.

6. Avaya VPNremote Phone Configuration

6.1. VPNremote Phone Firmware

The Avaya VPNremote Phone firmware must be installed on the phone prior to the phone being deployed in the remote location. See [4] and [5] for details on installing VPNremote Phone firmware. The firmware version of Avaya IP telephones can be identified by viewing the version displayed on the phone upon boot up or when the phone is operational by pressing 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 **Table 1,** 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 for all VPNremote Phone parameters with the exception of the WebLM License Manager URL. The WebLM License Manager URL cannot be set from the local phone configuration menu as of the firmware release used in these Application Notes and must be set from a centralized HTTP/TFTP server. The **NVWEBLMURL** variable of the 46xxvpnsetting.txt script file located on the HTTP/TFTP sever defines the WebLM License Manger URL, that the VPNremote Phones use to acquire a license. See [3], [4] and [6] for additional information.

The following shows the **NVWEBLMURL** setting used in the 46xxvpnsetting.txt script file for these Application Notes:

SET NVWEBLMURL http://192.168.1.30:8080/webLM/LicenseServer

The following steps describe how to configure the VPNremote Phone VPN parameters locally from the telephone.

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

   a. **During Telephone Boot:**

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

      ```
      DHCP
      * to program
      ```


©2007 Avaya Inc. All Rights Reserved.

When the * key is pressed, several configuration parameters are presented such as the phone's IP address, the Call Server's IP address, etc. Press the # key to accept the current settings, or enter an appropriate value and press the # key. 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 the VPNremote Phone is in an operational state, 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 following 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. The configuration values for the VPNremote Phone of user avayauser1, used in the sample configuration, are shown in **Table 3** below.

Note: The values entered below are case sensitive.

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

Configuration Options	Value	Description
Server:	**100.2.2.100**	IP address of the SSG Public interface
User Name:	**avayauser1**	User created in Steel-Belted Radius (Section 5.4)
Password:	********	Must match user password entered in Steel-Belted Radius (Section 5.4)
Group Name:	**vpnphone@avaya.com**	IKE Identity created in SSG (Section 4.4)

©2007 Avaya Inc. All Rights Reserved.

Configuration Options	Value	Description
Group PSK:	******** (avaya123)	Must match pre-shared key entered in SSG (Section 4.6.1)
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**	Default value to enable NAT traversal
Syslog Server:	-	Locally log phone events
IKE Parameters:	**DH2-3DES-MD5**	Must match IKE SA set in SSG (Section 4.6)
IKE ID Type:	**USER-FQDN**	Specifies the format of the Group Name
Diffie-Hellman Grp	**2**	Can be set to "Detect" to accept SSG settings
Encryption Alg:	**3DES**	Can be set to "Any" to accept SSG settings
Authentication Alg:	**MD5**	Can be set to "Any" to accept SSG settings
IKE Xchg Mode:	**Aggressive**	Mode used for Phase 1 Negotiations
IKE Config Mode:	**Enable**	Enables IKE
IPSec Parameters:	**DH2-AES128-SHA1**	Must match IPSec proposals set in SSG (Section 4.6)
Encryption Alg:	**AES-128**	Can be set to "Any" to accept SSG settings
Authentication Alg:	**SHA1**	Can be set to "Any" to accept SSG settings
Diffie-Hellman Grp	**2**	Can be set to "Detect" to accept SSG settings
Protected Net:		
Remote Net #1:	**0.0.0.0/0**	Access to all private nets
Copy TOS:	**Yes**	RE-write TOS bit setting to outside IP header for QoS
File Srvr:	**192.168.1.30**	TFTP/HTTP Phone File Srv
Connectivity Check:	**First Time**	Test initial IPSec connectivity

Table 3 – VPNremote Phone Configuration

©2007 Avaya Inc. All Rights Reserved.

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

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

   - Avaya Security Gateway
   - Cisco Xauth with PSK
   - Juniper Xauth with PSK
   - Generic PSK

   Press the button aligned with the **Juniper Xauth with PSK** profile option then press the **Done** soft button.

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

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

7. Avaya Communication Manager Configuration

All the commands discussed in this section are executed on Avaya Communication Manager using the System Access Terminal (SAT). This section assumes that basic configuration on Avaya Communication Manager has been completed.

7.1. VPNremote Phone Configuration

An Avaya VPNremote Phone is configured the same as other IP telephones within Avaya Communication Manager. 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.

For additional information regarding Avaya Communication Manager configuration refer to [1].

©2007 Avaya Inc. All Rights Reserved.

7.2. IP Codec Sets Configuration

Two IP codec sets are utilized in the sample configuration, one offering the G.711 codec and one offering the G.729a codec.

Use the **change ip-codec-set 1** command to define the G.711 codec as shown below.

```
change ip-codec-set 1                                          Page   1 of   2

                         IP Codec Set

   Codec Set: 1

   Audio        Silence      Frames   Packet
   Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU          n         2        20
 2:
 3:
```

Use the **change ip-codec-set 2** command to define the G.729a codec as shown below.

```
change ip-codec-set 2                                          Page   1 of   2

                         IP Codec Set

   Codec Set: 2

   Audio        Silence      Frames   Packet
   Codec        Suppression  Per Pkt  Size(ms)
 1: G.729A           n         2        20
 2:
 3:
```

Use the **list ip-codec-set** command to verify the codec assignments.

```
list ip-codec-set

                              IP CODEC SETS

Codec  Codec 1     Codec 2     Codec 3     Codec 4     Codec 5
Set

  1    G.711MU
  2    G.729A
```


©2007 Avaya Inc. All Rights Reserved.

7.3. IP Network Map Configuration

Three Network Regions are utilized in the sample configuration; Network Region 1, Network Region 50 and Network Region 55 as shown in Figure 1. Network Region 1 is associated with devices on the Main Campus network. Network Region 50 and 55 are associated with VPNremote Phones. VPNremote Phones mapped to Network Region 50 are assigned an IP codec set containing the G.711 codec, IP codec set 1 in the sample configuration. VPNremote Phones mapped to Network Region 55 are assigned an IP codec set containing the G.729a codec, IP codec set 2 in the sample configuration.

Use the **change ip-network-map** command to define the IP addresses mapped to Network Region 50 and 55 as shown below. Refer to Figure 1 and the Steel-Belted Radius IP Address Pools in Section 5.2.

```
change ip-network-map                                          Page   1 of  32
                        IP ADDRESS MAPPING

                                                                Emergency
                                      Subnet                    Location
 From IP Address  (To IP Address   or Mask)  Region    VLAN    Extension
 10 .10 .50 .1    10 .10 .50 .126             50       n
 10 .10 .55 .1    10 .10 .55 .126             55       n
    .   .   .        .   .   .                          n
    .   .   .        .   .   .                          n
```


©2007 Avaya Inc. All Rights Reserved.

7.4. IP Network Regions Configuration

7.4.1. Network Region 1

Use the **change ip-network-region 1** command to configure Network Region 1 parameters. Configure the highlighted fields shown below. All remaining fields can be left as default.

Select a descriptive a **Name**. The **Intra-region** and **Inter-region IP-IP Direct Audio** fields determine the flow of RTP audio packets, setting to yes enables the most efficient audio path be taken. **Codec Set** 1 is used for Network Region 1 as shown in Figure 1.

```
change ip-network-region 1                                    Page   1 of  19


                              IP NETWORK REGION
  Region: 1
Location: 1       Authoritative Domain: avaya.com
    Name: Main Campus
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                     IP Audio Hairpinning? y
   UDP Port Max: 3029
DIFFSERV/TOS PARAMETERS                 RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                     RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```


©2007 Avaya Inc. All Rights Reserved.

Page 3 defines the codec set to use for intra-region and inter-region calls. Avaya VPNremote Phones are mapped to Network Region 50 or 55.

- Calls within IP Network Region 1 use Codec Set 1 (G.711).
- Calls between Network Region 1 and VPNremote Phones in Network Region 50 use Codec Set 1 (G.711).
- Calls between Network Region 1 and VPNremote Phones in Network Region 55 use Codec Set 2 (G.729a).

```
change ip-network-region 1                                    Page   3 of  19

                   Inter Network Region Connection Management

 src dst  codec  direct                                    Dynamic CAC
 rgn rgn   set    WAN    WAN-BW-limits  Intervening-regions    Gateway   IGAR
 1   1     1
 -
 1   50    1       y           :NoLimit                                   n
 -
 1   55    2       y           :NoLimit                                   n
```

7.4.2. Network Region 50

Use the **change ip-network-region 50** command to configure Network Region 50 parameters. Configure the highlighted fields shown below. All remaining fields can be left as default.

```
change ip-network-region 50                                   Page   1 of  19
                              IP NETWORK REGION
  Region: 50
Location:         Authoritative Domain:
    Name: VPNphone G.711
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                        IP Audio Hairpinning? y
   UDP Port Max: 3028
```

Page 3 defines the codec set to use for intra-region and inter-region calls. Avaya VPNremote Phones are mapped to Network Region 50 or 55.

- Calls between VPNremote Phones in Network Region 50 and Network Region 1 use Codec Set 1 (G.711).
- Calls between VPNremote Phones within Network Region 50 use Codec Set 1 (G.711).
- Calls between VPNremote Phones in Network Region 50 and VPNremote Phones in Network Region 55 use Codec Set 2 (G.729a).

©2007 Avaya Inc. All Rights Reserved.

```
change ip-network-region 50                                    Page   3 of  19

                  Inter Network Region Connection Management

 src dst  codec  direct                                      Dynamic CAC
 rgn rgn   set    WAN    WAN-BW-limits  Intervening-regions    Gateway   IGAR
 50  1     1       y           :NoLimit                                    n
 -
 50  50    1
 -
 50  55    2       y           :NoLimit                                    n
```

7.4.3. Network Region 55

Use the **change ip-network-region 55** command to configure Network Region 55 parameters. Configure the highlighted fields shown below. All remaining fields can be left as default.

```
change ip-network-region 55                                    Page   1 of  19
                             IP NETWORK REGION
  Region: 55
Location:         Authoritative Domain:
    Name: VPNphone G.729a
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 2              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                       IP Audio Hairpinning? y
   UDP Port Max: 3028
```

Page 3 defines the codec set to use for intra-region and inter-region calls. Avaya VPNremote Phones are mapped to Network Region 50 or 55.

- Calls between VPNremote Phones in Network Region 55 and Network Region 1 use Codec Set 2 (G.729a).
- Calls between VPNremote Phones within Network Region 55 use Codec Set 2 (G.729a).
- Calls between VPNremote Phones in Network Region 55 and VPNremote Phones in Network Region 50 use Codec Set 2 (G.729a).

```
change ip-network-region 55                                    Page   3 of  19

                  Inter Network Region Connection Management

 src dst  codec  direct                                      Dynamic CAC
 rgn rgn   set    WAN    WAN-BW-limits  Intervening-regions    Gateway   IGAR
 55  1     2       y           :NoLimit                                    n
 -
 50  50    2       y           :NoLimit                                    n
 -
 55  55    2
```


©2007 Avaya Inc. All Rights Reserved.

8. Verification

8.1. VPNremote Phone IPSec Statistics

Once the Avaya VPNremote Phone establishes an IPSec tunnel, registers with Avaya Communication Manager and becomes functional (dial-tone), statistics of the IPSec tunnel can be accessed including the Inner IP address assigned by Steel-Belted Radius.

To access the IPSec stats from the telephone keypad, press the **OPTIONS** hard button (with √ icon). From the telephone keypad, press the ► hard button until the **VPN Status…** option appears. Select **VPN Status…** The VPN statistics of the active IPSec tunnel will be 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 the VPNremote phone used in the sample configuration.

VPN Status…	
PKT S/R	**448/419**
FRAG RCVD	**0**
Comp/Decomp	**0/0**
Auth Failures	**0**
Recv Errors	**0**
Send Errors	**0**
Gateway	**100.2.2.100**
Outer IP	**172.16.12.8**
Inner IP	**10.10.50.21**
Gateway Version	**0.0.0**
Inactivity Timeout	**0**
AES128-SHA-1 days	

8.2. Avaya Communication Manager "list registered-ip-stations"

The Avaya Communication Manager **list registered-ip-stations** command, run from the SAT, can be used to verify the registration status of the VPNremote Phones and associated parameters as highlighted below. Included is the Network Region the Phone has been mapped too.

```
list registered-ip-stations

                          REGISTERED IP STATIONS

Station  Set     Product    Prod  Station         Net Orig    Gatekeeper     TCP
Ext      Type    ID         Rel   IP Address      Rgn Port    IP Address     Skt
50003    4625    IP_Phone   2.500 10.10.50.21     50          192.168.1.10    y
24074    4610    IP_Phone   2.300 10.10.55.52     55          192.168.1.10    y
50020    4602+   IP_Phone   2.300 192.168.1.242   1           192.168.1.10    y
```


©2007 Avaya Inc. All Rights Reserved.

8.3. Avaya Communication Manager "status station"

The Avaya Communication Manager **status station *nnn*** command, where ***nnn*** is a station extension of a VPNremote Phone, can be run from the SAT to verify the current status of an administered station. The **Service State: in-service/off-hook** shown on Page 1 below indicates the VPNremote Phone with extension 50003 is participating in an active call.

```
status station 50003                                          Page   1 of   6
                            GENERAL STATUS
     Administered Type: 4625              Service State: in-service/off-hook
        Connected Type: 4625           TCP Signal Status: connected
             Extension: 50003
                  Port: S00004        Parameter Download: complete
            Call Parked? no                SAC Activated? no
      Ring Cut Off Act? no             CF Destination Ext:
Active Coverage Option: 1

          EC500 Status: N/A        Off-PBX Service State: N/A
       Message Waiting:
   Connected Ports: S00029


 User Cntrl Restr: none                        HOSPITALITY STATUS
Group Cntrl Restr: none                      Awaken at:
                                              User DND: not activated
                                             Group DND: not activated
                                          Room Status: non-guest room
```

Page 4, abridged below, displays the audio status of an **active call between two VPNremote Phones in different Network Regions**. The highlighted fields shown below indicate the following:

- **Other-end IP Addr** and **Set-end IP Addr** values are from the Steel-Belted Radius IP Address Pools indicating the call is between VPNremote Phones.
- The **G.729A** codec is being used.
- Station 50003 is mapped to **Network Region 50** while far-end station is mapped to **Network Region 55**.
- Audio RTP packets are going direct (**ip-direct**) between VPNremote Phones.

```
status station 50003                                          Page   4 of   6

                                AUDIO CHANNEL
                                Port: S00004
                  Switch                        IP                      IP
                  Port     Other-end IP Addr :Port   Set-end IP Addr:Port
G.729A      Audio:          10. 10. 55.  52  :2138    10. 10. 50. 21:2934
        Node Name:
   Network Region:          55                        50
   Audio Connection Type: ip-direct
```


©2007 Avaya Inc. All Rights Reserved.

Page 4, abridged below, displays the audio status of an **active call between a VPNremote Phone and a Main Campus IP telephone**. The highlighted fields indicate the following:

- Other-end IP Addr value indicates the call is with an IP telephone at the Main Campus.
- The **G.711** codec is being used.
- Station 50003 is mapped to **Network Region 50** while far-end station is mapped to **Network Region 1**.
- Audio RTP packets are going direct (**ip-direct**) between VPNremote Phone and campus Phone.

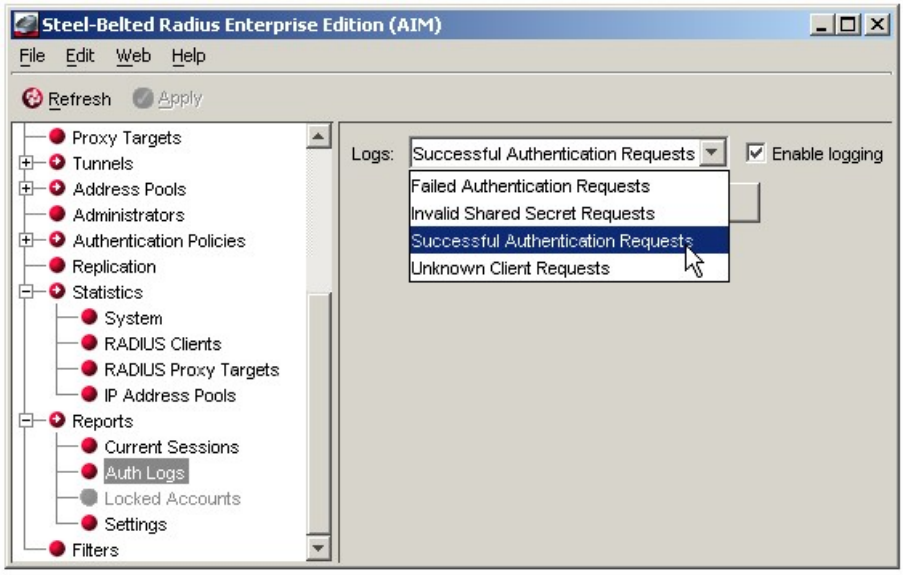
```
status station 50003                                          Page   4 of   6

                                AUDIO CHANNEL
                                Port: S00004
                  Switch                        IP                      IP
                  Port     Other-end IP Addr :Port   Set-end IP Addr:Port
G.711       Audio:          192.168.  1.242   :2678    10. 10. 50. 21:2934
        Node Name:
   Network Region:          1                         50
   Audio Connection Type: ip-direct
```

8.4. Juniper Steel-Belted Radius Authentication Logs

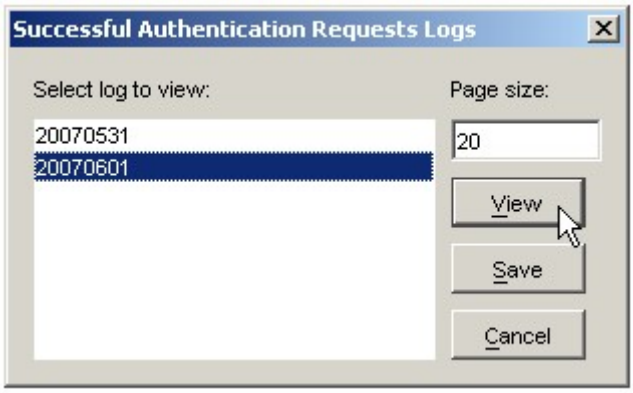
The Steel-Belted Radius server maintains authentication logs of several types. The following shows how to access these logs:

1. From the Steel-Belted Radius Administration GUI, expand **Reports** then select **Auth Logs** from the left navigation window. Select the desired log type from the drop-down list then click **View**. The **Successful Authentication Requests** log has been selected below.

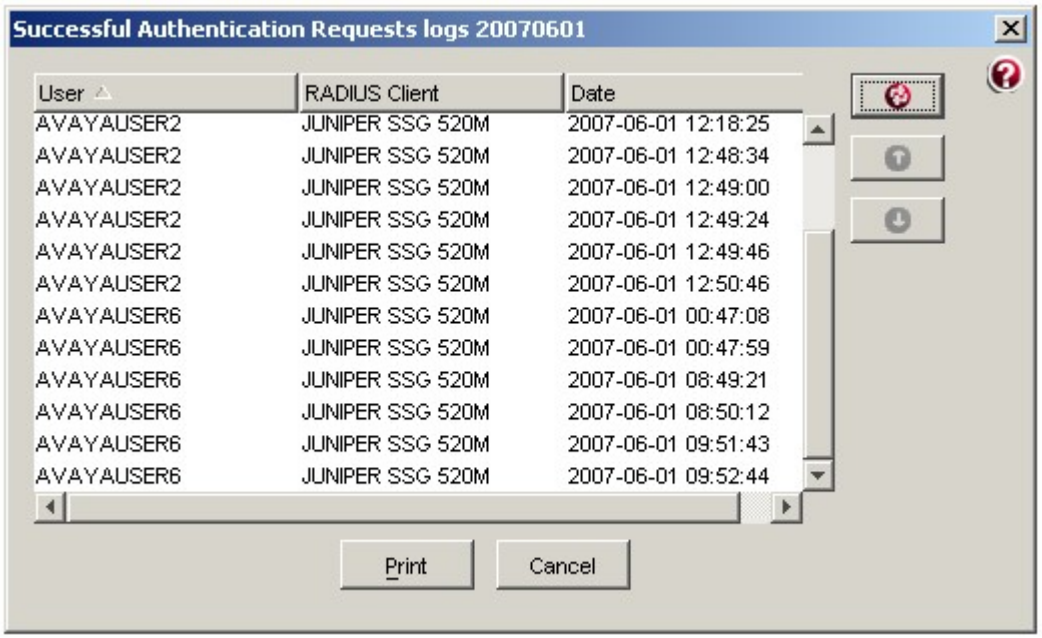


©2007 Avaya Inc. All Rights Reserved.

2. Steel-Belted Radius can be configured to maintain several days worth of logs. Shown below is a pop-up window offering the available logs stored on the Steel-Belted Radius server. Select the desired log date then click **View**.



3. The Successful Authentication Requests log is displayed for the selected date similar to the display below.



9. Conclusion

The Avaya VPNremote Phone combined with the Juniper Networks SSG security platform and the Juniper Networks Steel-Belted Radius authentication platform provides a secure and reliable solution for remote worker telephony over a broadband Internet connection. The flexibility offered by the Steel-Belted Radius server enables Network Region mapping of VPNremote Phones within Avaya Communication Manager to accommodate individual VPNremote Phone user network environments.

©2007 Avaya Inc. All Rights Reserved.

10. References

Avaya Application Notes and additional resources can be found at the following web address http://www.avaya.com/gcm/master-usa/en-us/resource/. Avaya Product Support web site can be found at the following web address http://support.avaya.com/.

[1] ***Administrators Guide for Avaya Communication Manager,***
Doc ID: 03-300509 Issue: 3.1

[2] ***4600 Series IP Telephone Release 2.8 LAN Administrator Guide,***
Doc ID: 555-233-507 Issue: 6

[3] ***VPNremote for the 4600 Series IP Telephone Release 2.0 Administrator Guide,***
Doc ID: 19-600753 Issue: 2

[4] ***VPNremote for 4600 Series IP Telephone Installation and Deployment Guide***
Doc ID: 1022006 Issue: 1

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

[6] ***Application Notes for Configuring Avaya WebLM License Manager for Avaya VPNremote™ Phone Release 2 – Issue 1.0***

[7] **Juniper Networks SSG 500 Series Product Page**
http://www.juniper.net/products_and_services/firewall_slash_ipsec_vpn/ssg_500_series/index.html

[8] **Juniper Networks Steel-Belted Radius Product Page**
http://www.juniper.net/products_and_services/aaa_and_802_1x/steel_belted_radius/index.html

©2007 Avaya Inc. All Rights Reserved.

©2007 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