Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Mobile Communication System (VPNremote Phone Option) with Clear Channel Satellite XtremeSat – Issue 1.0

Abstract

These Application Notes describe the procedures for configuring Avaya Mobile Communication System with Clear Channel Satellite XtremeSat.

Avaya Mobile Communication System (MCS) is a compact highly mobile full featured communication system designed for rapid deployment in disaster stricken or remote areas where other systems may have been damaged or do not exist. Avaya MCS can be connected to traditional and non-traditional networking facilities in a variety of ways. These Application Notes focus on the interoperability of Avaya MCS with the Clear Channel Satellite XtremeSat service to provide Internet connectivity via a satellite link. Using the Internet access provided by XtremeSat, an IPsec VPN tunnel can be established between Avaya Mobile Communication System and a main site to provide secure voice communication between the sites.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

©2008 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the procedures for configuring Avaya Mobile Communication System with Clear Channel Satellite XtremeSat.

Avaya Mobile Communication System is a compact highly mobile full featured communication system designed for rapid deployment in disaster stricken or remote areas where other systems may have been damaged or do not exist. Avaya MCS can be connected to traditional and non-traditional networking facilities in a variety of ways.

Depending on the application and deployment environment, Avaya MCS can be constructed using different Avaya system platforms and various equipment and networking options which are mounted in a rugged rack case and powered by an Uninterruptable Power Supply (UPS). For more details on the various options available with Avaya MCS, refer to [7].

For the VPN application described in these Application Notes, Avaya MCS consisted of the following:

- Avaya VPNremote Phones
- Avaya C363T-PWR Converged Stackable Switch
- EMS 2000 Series satellite interactive terminal (SIT) (required for satellite option)
- Very Small Aperture Terminal (VSAT) (required for satellite option)

In addition, a Linksys Broadband Firewall Router was used as a network address translation (NAT) device between the Clear Channel Satellite ISP and the private network provided as part of the Avaya MCS.

These Application Notes focus on the interoperability of Avaya MCS with the Clear Channel Satellite XtremeSat service to provide Internet connectivity via a satellite link. Using the Internet access provided by XtremeSat, an IPsec VPN tunnel can be established between each Avaya VPNremote Phone connected to Avaya MCS and a main site to provide secure voice communication between the main site and the remote users.

1.1. Configuration

Figure 1 illustrates the test configuration. The test configuration shows Avaya MCS at a remote site connected through XtremeSat to the Clear Channel Satellite earth station. The Clear Channel Satellite earth station can provide connectivity to the Internet and the PSTN for the users of the XtremeSat service. In the case of this VPN configuration, PSTN access is provided from the main site Avaya Media Gateway. Thus, the PSTN access provided by XtremeSat is not used and thus not shown in **Figure 1**. Voice is transmitted to the main site over IP through an IPsec VPN tunnel established with each Avaya VPNremote Phone. Data traffic from the PC connected to the Avaya VPNremote Phone does not pass through the VPN tunnel, but still is allowed to flow between the two sites or the Internet.

As previously mentioned, Avaya MCS can be constructed with several platform and equipment options. **Figure 1** shows Avaya MCS consisting of an Avaya C363T-PWR Converged Stackable Switch and a set of Avaya VPNremote Phones. The Avaya C363T-PWR Converged Stackable

©2008 Avaya Inc. All Rights Reserved.

Switch is connected to a port on the private side of a Linksys BEFSX41 Broadband Firewall Router. If four or less users need to be supported, then the Avaya VPNremote Phones can be connected directly to the Linksys router and the Avaya C363T-PWR Converged Stackable Switch can be removed from the configuration. The Internet port of the Linksys router then connects to the EMS 2000 Series satellite interactive terminal (SIT). Both the Internet port of the Linksys router and the SIT are assigned public IP addresses from the service provider (Clear Channel Satellite). For reasons of security, all public IP addresses referenced in these Application Notes have been replaced with IP addresses in the range of 192.168.100.0 to 192.168.110.254.

The SIT is connected directly via coax cable to the satellite dish. XtremeSat uses a small dish at the remote site known as a Very Small Aperture Terminal (VSAT) to communicate to the earth station at the other end using the Digital Video Broadcast Return Channel via Satellite (DVB-RCS) standard. XtremeSat supports two types of VSATs: a one meter fixed dish and a .76 meter auto-acquisition dish. The auto-acquisition dish is designed to automatically locate and lock on the satellite signal when powered up and deployed. Compliance testing was done with the fixed dish configuration.

At the main site is a Juniper Networks NetScreen-50 firewall which connects to an Avaya C363T-PWR Converged Stackable Switch. The NetScreen-50 in addition to being a firewall will also terminate the IPsec VPN at the main site. The Avaya C363T-PWR Converged Stackable Switch provides routing at the main site. Also connected to the switch is an Avaya G700 Media Gateway with Avaya S8300 Server running Avaya Communication Manager.

It should be noted that calls between the Avaya MCS and the main site will typically experience one to two seconds of delay. This is expected with the known latency of a satellite link. In addition, since the voice traffic is routed over the Internet, there is no mechanism to ensure that voice traffic is given priority over data traffic.

©2008 Avaya Inc. All Rights Reserved.

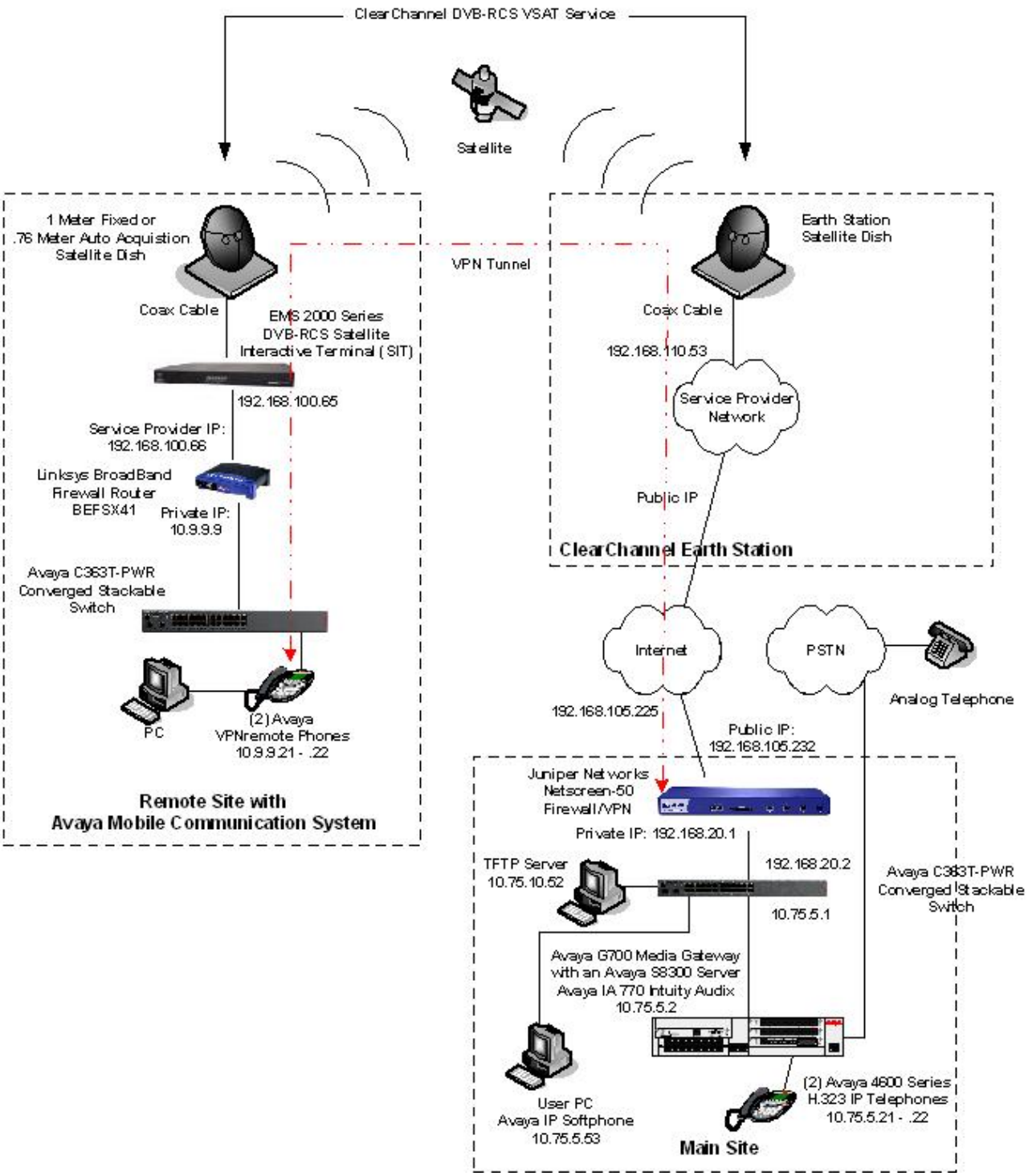


Figure 1: Avaya MCS VPNremote Phone Configuration

©2008 Avaya Inc. All Rights Reserved.

2. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8300 Server	Avaya Communication Manager 4.0.1 (with Avaya IA 770 Intuity Audix) (R014x.00.1.731.2) Service Pack 00.1.731.2-14330
Avaya G700 Media Gateway	26.33.0
Avaya C363T-PWR Converged Stackable Switch	4.5.14
Avaya VPNremote Phone	H323_VPN_232_4
Avaya 4620SW IP Telephone Avaya 4621SW IP Telephone	H.323 version 2.8
Avaya IP Softphone	6.0 (Build 6.0.0.25) on Windows XP Professional SP2
Juniper Networks NetScreen-50 Firewall / VPN	ScreenOS 5.4.0r3.0
Linksys BEFSX41 Broadband Firewall Router	1.50.18
Clear Channel Satellite XtremeSat • EMS 2000 Series (SIT) • VSAT	- V3009.R05 -

3. Configure Main Site Avaya Communication Manager

This section describes the configuration of Avaya Communication Manager at the main site. This section assumes Avaya S8300 Server has been installed using the procedures described in [1]. As part of these procedures, the Avaya C363T-PWR Converged Stackable Switch (IP interface 10.75.5.1 as shown in **Section 4**) was configured as the default gateway for the Avaya S8300 Server.

This section describes the configuration of the components necessary to support the Avaya VPNremote Phone. This includes the following components or services:

- IP network region
- IP codec set
- Stations

The configuration of Avaya Communication Manager was performed using the System Access Terminal (SAT). After the completion of the configuration, perform a **save translation** command to make the changes permanent.

©2008 Avaya Inc. All Rights Reserved.

Step	Description

1.	**IP Network Region**
	Determine the IP network region in which the Avaya VPNremote Phones will reside. The Avaya S8300 Server is located in the default IP network region 1. For simplicity, the Avaya VPNremote Phones were placed in this same network region for the compliance test. Codec set 1 was assigned to this region and **Intra-region** and **Inter-region IP-IP Direct Audio** was enabled. The example below shows the IP network region settings used for the compliance test.
	
	It should be noted that the Avaya VPNremote Phone Release Notes [9] specify that **IP-IP Direct Audio** (also known as shuffling) should be disabled when using a Juniper Networks Netscreen device at the enterprise. Otherwise, calls placed between Avaya VPNremote Phones may result in no audio. It was observed that it was not necessary to disable IP-IP Direct Audio for the specific configuration and test cases covered in the compliance test. However, if a user experiences no audio for calls between Avaya VPNremote Phones then IP-IP Direct Audio should be disabled in the IP network region where the Avaya VPNremote Phones reside.
	
	`display ip-network-region 1  Page 1 of 19`
	`IP NETWORK REGION`
	`Region: 1`
	`Location: Authoritative Domain:`
	`Name:`
	`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? n`
	`UDP Port Max: 3327`
	`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`

2.	**IP Codec Set**
	Define the codecs to be used. The compliance test was performed using both G.711MU and G.729AB during different parts of the test. The example below shows the setting for G.711MU.
	
	`display ip-codec-set 1  Page 1 of 2`
	`IP Codec Set`
	`Codec Set: 1`
	`Audio Codec  Silence Suppression  Frames Per Pkt  Packet Size(ms)`
	`1: G.711MU  n  2  20`
	`2:`

©2008 Avaya Inc. All Rights Reserved.

Step	Description
3.	**Stations** Add a station for each Avaya VPNremote Phone to be supported. The configuration of the station is the same as with any other Avaya IP H.323 Telephone. The example below shows the use of the **add station** command to add station 30121 which is one of the Avaya VPNremote Phones located at the remote site. The **Type** field is set to ***4620***. The **Port** field is set to ***IP***. The **Name** field should be set to a descriptive name for this user. The **Security Code** field contains the password used by the user to access the telephone. The **Coverage Path** field is set to the coverage path for Avaya IA 770 Intuity Audix. The configuration related to Avaya IA 770 Intuity Audix is beyond the scope of these Application Notes and thus is not shown.

```
add station 30121                                                Page   1 of   5
                                      STATION

Extension: 30121                          Lock Messages? n               BCC: 0
     Type: 4620                           Security Code: 1234             TN: 1
     Port: IP                           Coverage Path 1: 1               COR: 1
     Name: Tim                          Coverage Path 2:                 COS: 1
                                        Hunt-to Station:
STATION OPTIONS
                                             Time of Day Lock Table:
              Loss Group: 19          Personalized Ringing Pattern: 1
                                                Message Lamp Ext: 30121
            Speakerphone: 2-way               Mute Button Enabled? y
        Display Language: english                Expansion Module? n
 Survivable GK Node Name:
          Survivable COR: internal              Media Complex Ext:
   Survivable Trunk Dest? y                          IP SoftPhone? n



                                            Customizable Labels? y
```


©2008 Avaya Inc. All Rights Reserved.

4. Configure Main Site Avaya C363T-PWR Converged Stackable Switch

This section describes the Avaya C363T-PWR Converged Stackable Switch configuration. This section assumes the Avaya C363T-PWR has been installed using the procedures described in [6]. It is also assumed that the Avaya C363T-PWR Converged Stackable Switch has a router license installed. The complete media gateway configuration file is included in **Appendix A**.

Step	Description

1.	**Create VLANs**
	Create a VLAN for use by Avaya Communication Manager and the Avaya IP Telephones. The compliance test created **vlan *2*** with **name *V2*** for this purpose. Create a second VLAN for the TFTP server. The compliance test created **vlan *3*** with **name *V3*** for this purpose. Create a third VLAN for the private side of the NetScreen-50. The compliance test created **vlan *5*** with **name *V5*** for this purpose.
	
	`G360-1(super)# set vlan 2 name V2`
	`G360-1(super)# set vlan 3 name V3`
	`G360-1(super)# set vlan 5 name V5`

2.	**Create VLAN Names (Layer 3)**
	For the VLANs created in **Step 1,** VLAN names must be created for these VLAN IDs at the router level so that IP addresses may be assigned to them. The names may be different than those used in **Step 1**. The VLAN names at layer 2 and 3 are tied together by the VLAN ID.
	
	`G360-1(super)# session router`
	`Router-1(super)# set vlan 2 name voice`
	`Router-1(super)# set vlan 3 name data`
	`Router-1(super)# set vlan 5 name satellite`

3.	**Assign IP addresses**
	For each VLAN created in **Step 1**, create a layer 3 interface and assign an IP address consistent with **Figure 1**. The example below shows how to set these parameters for the layer 3 interfaces IPI2, IPI3 and IPI5.
	
	`G360-1(super)# session router`
	`Router -1(super)# interface IPI2`
	`Router -1(super-if:IPI2)# ip vlan 2`
	`Router -1(super-if:IPI2)# ip address 10.75.5.1 255.255.255.0`
	`Router -1(super-if:IPI2)# exit`
	`Router-1(super)# interface IPI3`
	`Router -1(super-if:IPI3)# ip vlan 3`
	`Router -1(super-if:IPI3)# ip address 10.75.10.1 255.255.255.0`
	`Router -1(super-if:IPI3)# exit`
	`Router-1(super)# interface IPI5`
	`Router -1(super-if:IPI5)# ip vlan 5`
	`Router -1(super-if:IPI5)# ip address 192.168.20.2 255.255.255.0`
	`Router -1(super-if:IPI5)# exit`

©2008 Avaya Inc. All Rights Reserved.

Step	Description

4.	**Default Gateway or Static Routes**
	Configure a default gateway or static routes such that traffic from the main site directed to the IP addresses of the remote site are sent to the Netscreen-50. For the compliance test, static routes were used for this purpose. The example below shows the setting of these static routes. The remote site uses two IP network addresses. The 10.9.9.0 address is the physical IP network address of the Avaya VPNremote Phones. The 100.100.100.0 address is a virtual IP network address assigned to the Avaya VPNremote Phones by the Netscreen-50 in **Section 5**.
	
	`G360-1(super)# ip route 10.9.9.0 255.255.255.0 192.168.20.1`
	`G360-1(super)# ip route 100.100.100.0 255.255.255.0 192.168.20.1`

5.	**Save Configuration** Use the **copy running-config startup-config** command to save the configuration. `G360-1(super)# copy running-config startup-config`

5. Configure Main Site Juniper Networks NetScreen-50

This section describes the Juniper Networks NetScreen-50 configuration including in particular the IPsec VPN tunnel setup. This section assumes the NetScreen-50 has been installed as described in [13] and starts with the factory defaults. The complete configuration file is included in **Appendix B**.

The Netscreen-50 can be configured using either the Command Line Interface (CLI) or the Web interface. This section will use the CLI to perform the initial basic setup of the device and then will switch to using the Web interface to complete the configuration.

Step	Description
1.	**Login** Using a terminal emulation application, connect to the console port using the following parameters: 9600 baud, 8 data bits, no parity, 1 stop bit, and no flow control. Log in with the appropriate user name and password.

2.	**Trusted Zone**
	Statically administer the trusted zone Ethernet interface. The NetScreen-50 trusted zone is the protected or private side of the firewall. The IP address was also enabled to perform management.
	
	`ns50-> set interface ethernet1 zone trust`
	`ns50-> set interface ethernet1 ip 192.168.20.1/24`
	`ns50-> set interface ethernet1 manage-ip 192.168.20.1`

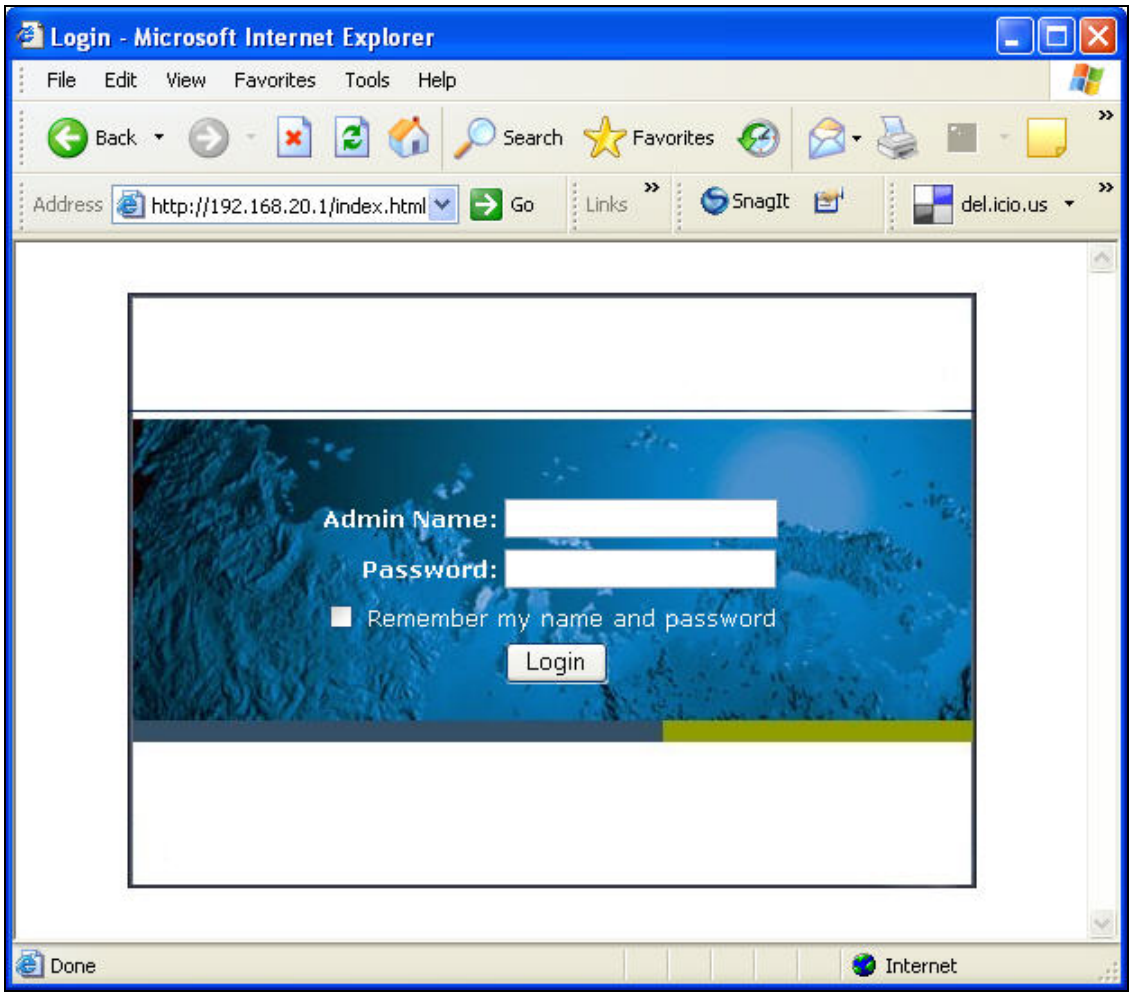
©2008 Avaya Inc. All Rights Reserved.

Step	Description

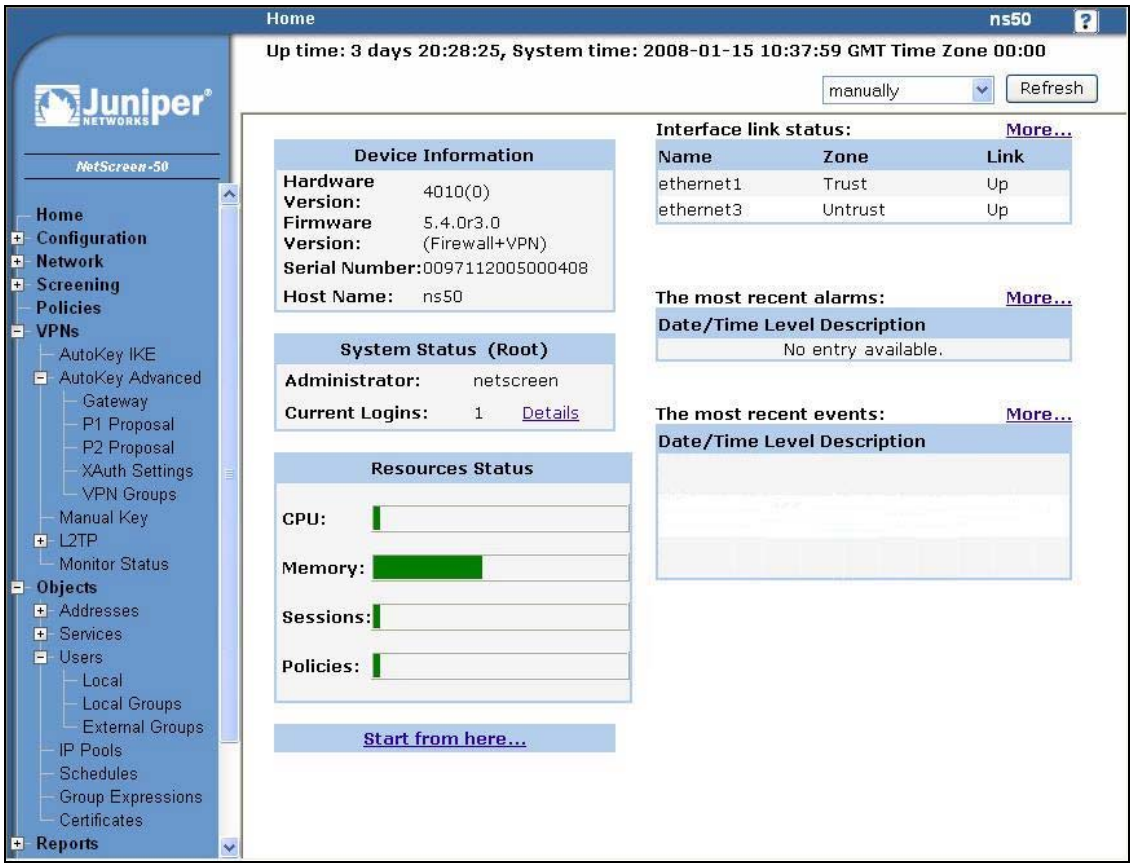
3.	**Untrusted Zone**
	Statically administer the untrusted zone Ethernet interface. The NetScreen-50 untrusted zone is the unprotected or public side of the firewall.
	
	`ns50-> set interface ethernet3 zone untrust`
	`ns50-> set interface ethernet3 ip 192.168.105.232/27`

4.	**Static Route** Define a static route to reach the trusted network which is not directly attached. `ns50-> set vrouter trust-vr route 10.75.0.0/16 interface ethernet1 gateway 192.168.20.2`
5.	**Default Route** Define a default static route for all outbound traffic. `ns50-> set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 192.168.105.225`
6.	**Clear H.323 ALG**
7.	**Save Configuration** Save the configuration. `ns50-> save`

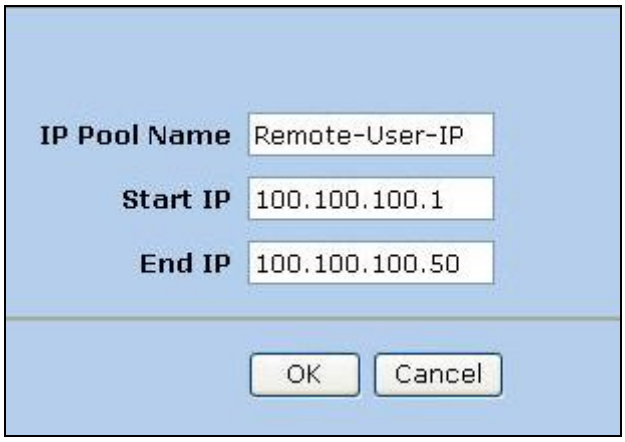
©2008 Avaya Inc. All Rights Reserved.

Step	Description
8.	**Login to the Web interface.** Enter the IP address of the private side of the Netscreen-50 as the destination address in a Web browser. At the login screen, provide the appropriate credentials. 

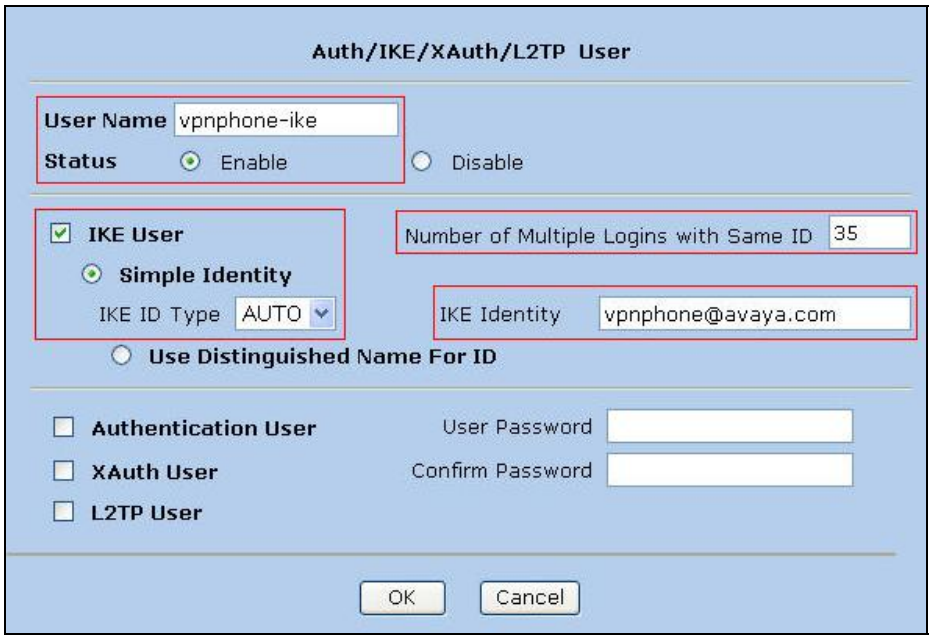
©2008 Avaya Inc. All Rights Reserved.

Step	Description
9.	**Home Page** The **Home** page appears as shown below. The menu tree in the left pane will be used to navigate through the remaining steps. 

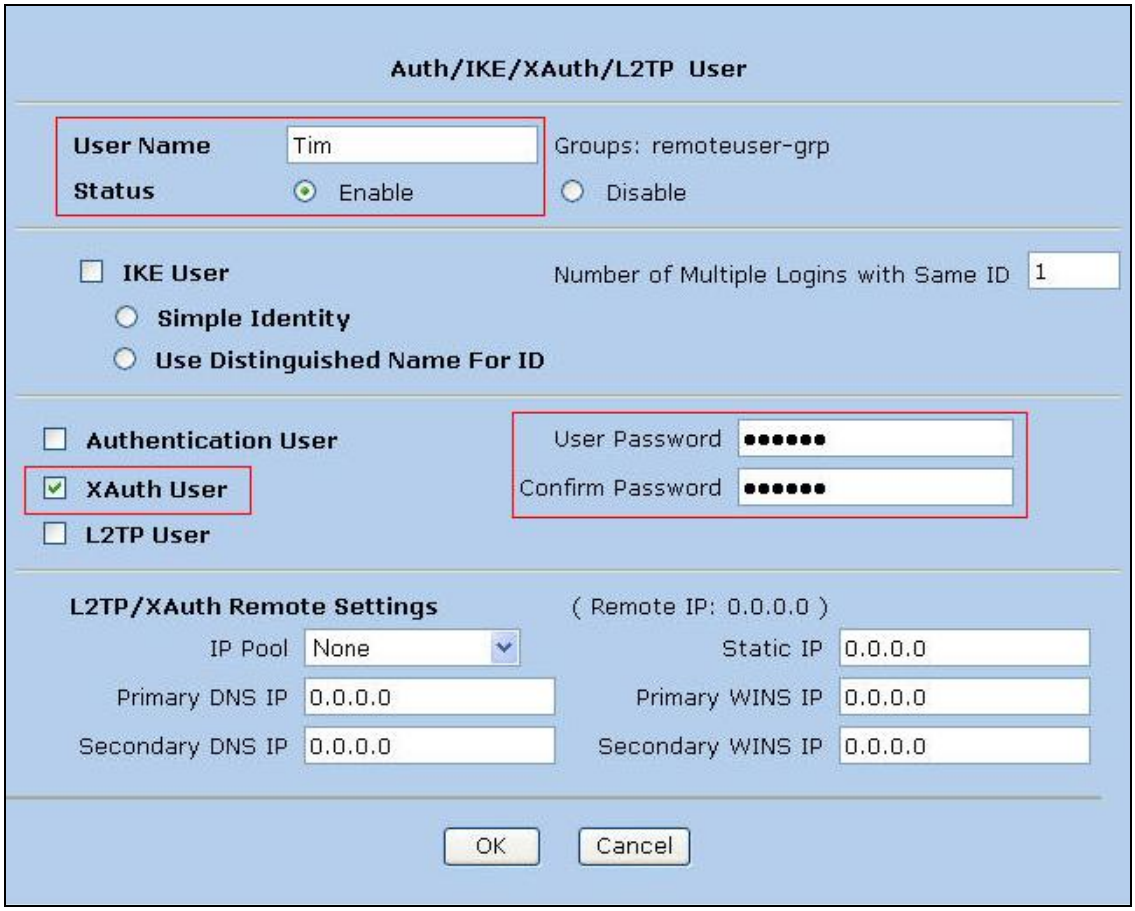
©2008 Avaya Inc. All Rights Reserved.

Step	Description
10.	**IP Address Pool** The XAuth protocol enables the Netscreen-50 to dynamically assign IP addresses from a configured IP Address pool range to IPSec clients such as the Avaya VPNremote Phones. The following steps create the IP Address Pool: From the left navigation menu, select **Objects > IP Pools**. On the **IP Pools** page (not shown), click **New**. Populate the 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 **Step 24**. Ensure the IP address range does not conflict with addresses used throughout the corporate trusted network.  The **IP Pools** page displays the new address pool entry. Name: Remote-User-IP; Start IP: 100.100.100.1; End IP: 100.100.100.50; In use: 0; Configure: Edit, Remove

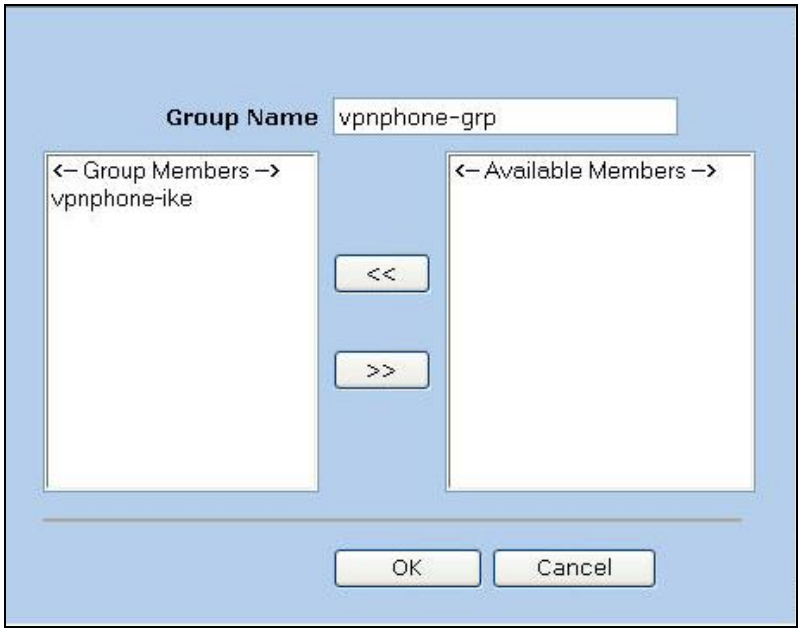
©2008 Avaya Inc. All Rights Reserved.

Step	Description
11.	**Local User Configuration - IKE User** The sample configuration includes 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. XAuth users are remotely authenticated users who access a head-end security gateway via an AutoKey IKE VPN tunnel. Thus, the authentication of IKE users is actually the authentication of an individual's device (e.g., Avaya VPNremote Phone); whereas the authentication of XAuth users is the authentication of the individual themselves. The following steps create an IKE user to be used by Avaya VPNremote Phones for IKE authentication. From the left navigation menu, select **Objects > Users > Local**. On the **Local Users** page (not shown), click **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 endpoints that can concurrently establish IPSec tunnels using this identity. This number must equal or exceed the number of Avaya VPNremote Phones accessing the Netscreen-50. **IKE Identity**, combined with a Pre-Shared Key**,** is used to identify the endpoint when an initial IKE Phase one dialog begins. The format of the IKE Identity is that of an email address. As described in **Section 9**, **Step 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. 

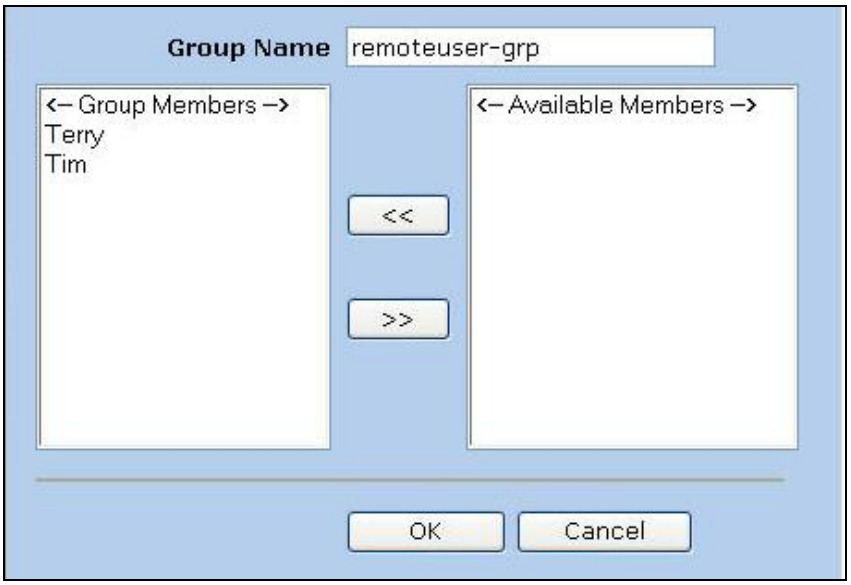
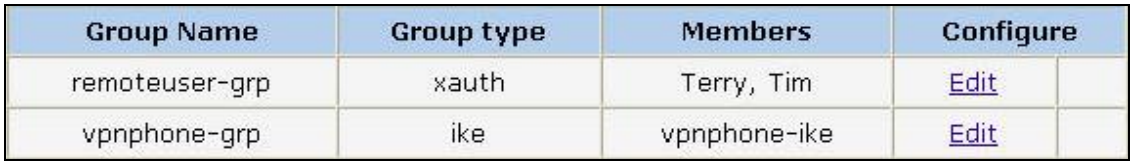
©2008 Avaya Inc. All Rights Reserved.

Step	Description
12.	**Local User Configuration - XAuth Users** Two XAuth user accounts, **Tim**, and **Terry** are created in the sample configuration for users of the Avaya VPNremote Phones. The following steps create a user account for **Tim**. Follow the same steps to create an account for **Terry**. The XAuth server of the Netscreen-50 provides the authentication of these users. The users of the Avaya VPNremote Phones 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 Avaya VPNremote Phones flash memory. See **Section 9**, **Step 2** for additional detail. From the left navigation menu, select **Objects > Users > Local**. On the **Local Users** page (not shown), click **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. 

©2008 Avaya Inc. All Rights Reserved.

Step	Description
13.	**Resulting Users** The resulting users created in **Steps 11** and **12** are shown below and can be displayed by navigating to **Objects** > **Users** > **Local**. | Name	Type	Group	Status	Identity	Configure	
---	---	---	---	---	---	---
Terry	XAuth	-	Enabled	-	Edit	Remove
Tim	XAuth	-	Enabled	-	Edit	Remove
vpnphone-ike	IKE	-	Enabled	vpnphone@avaya.com	Edit	Remove	 **Local User Group Configuration - IKE Group** 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. The sample configuration includes two different types of user groups: IKE and XAuth. The IKE users and XAuth users created in **Steps 11** and **12** must now be added to an IKE Group and a XAuth Group respectfully. To create a user group, select **Objects** > **Users** > **Local Groups** from the left navigation menu. On the **Local Groups** page (not shown), click **New**. Enter a descriptive **Group Name**. To add members to the group, select the user name in the **Available Members** column on the right, then click the << button to move the user name to the **Group Members** column on the left. The example below shows the IKE group. It contains a single user name: ***vpnphone-ike***. 

©2008 Avaya Inc. All Rights Reserved.

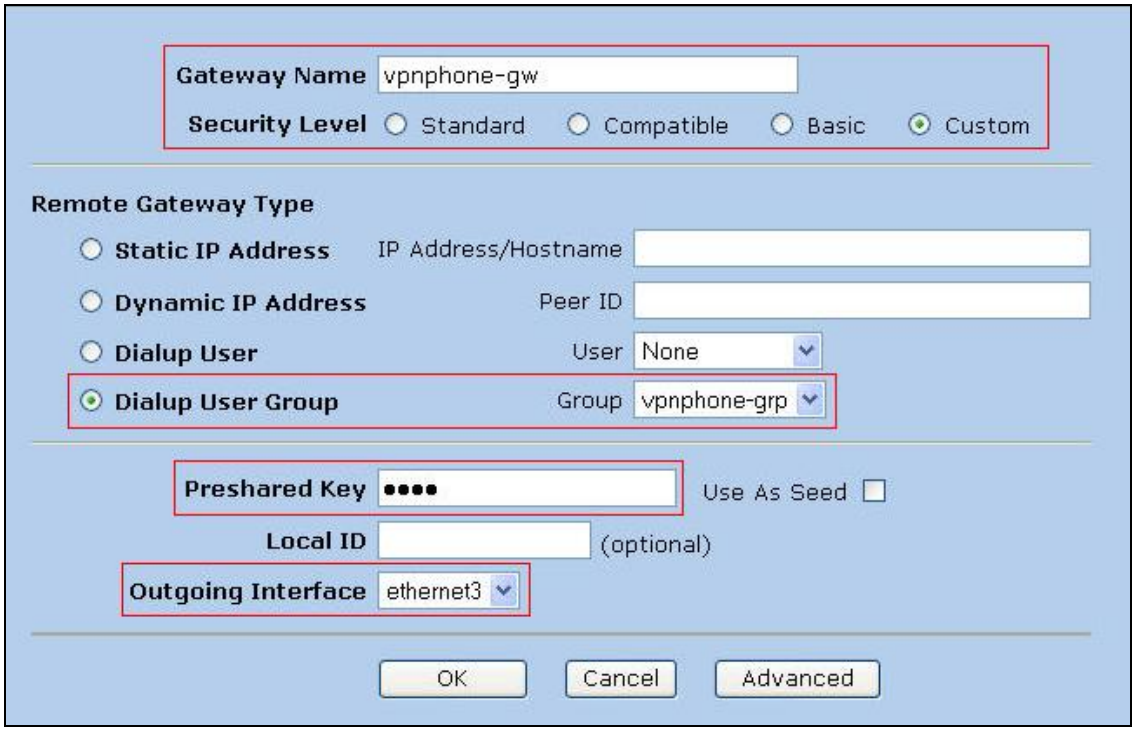
Step	Description
15.	**Local User Group Configuration - XAuth Group** Use the same procedures described in **Step 14** to create the group for the XAuth users. The example below shows the XAuth group used in the test configuration. 
16.	**Resulting Groups** The resulting groups created in **Steps 14** and **15** are shown below and can be displayed by navigating to **Objects** > **Users** > **Local Groups**. 

©2008 Avaya Inc. All Rights Reserved.

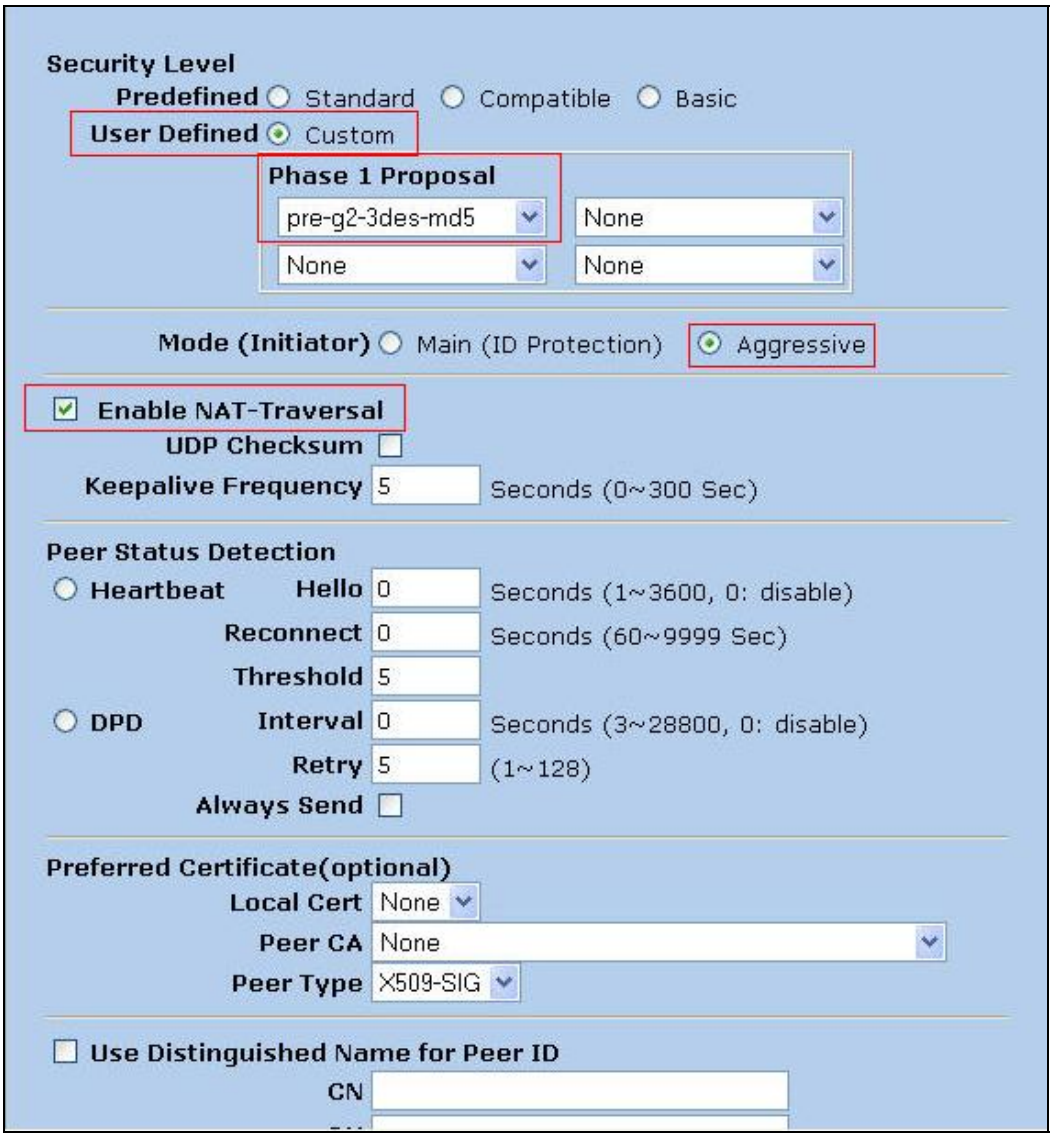
Step	Description
17.	**VPN** Setting up the VPN tunnel encryption and authentication is a two-phase process. • Phase 1 covers how the Avaya VPNremote Phone and the Netscreen-50 will securely negotiate and handle the building of the tunnel. • Phase 2 sets up how the data passing through the tunnel will be encrypted at one end and decrypted at the other. This process is carried out on both sides of the tunnel. The table below provides the IKE Proposals used in the sample configuration including the proposal name used by the Netscreen-50. This information will be used in **Steps 18 – 23** to configure the VPN on the Netscreen-50.

Phase	Encryption/ Authentication Method	Diffie-Hellman Group	Encryption Algorithm	Hash Algorithm	Life Time (sec)	Netscreen-50 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

©2008 Avaya Inc. All Rights Reserved.

Step	Description
18.	**AutoKey IKE Gateway Configuration – Phase 1** From the left navigation menu, select **VPNs > AutoKey Advanced > Gateway.** On the **AutoKey Advanced Gateway** page (not shown), click **New**. Configure the highlighted fields shown below. All remaining fields can be left as default. Provide a descriptive **Gateway Name**. Selecting ***Custom*** for the **Security Level** provides access to a more complete list of proposals available on the Netscreen-50. Selecting **Dialup User Group** associates the **Group *vpnphone-grp*** created in **Step 14** to this IKE gateway. Enter an ASCII text string for a **Preshared Key** that will match the text entered on the Avaya VPNremote Phone. The **Outgoing Interface** is the interface which terminates the VPN tunnel. Click the **Advanced** button to access additional configuration options. 

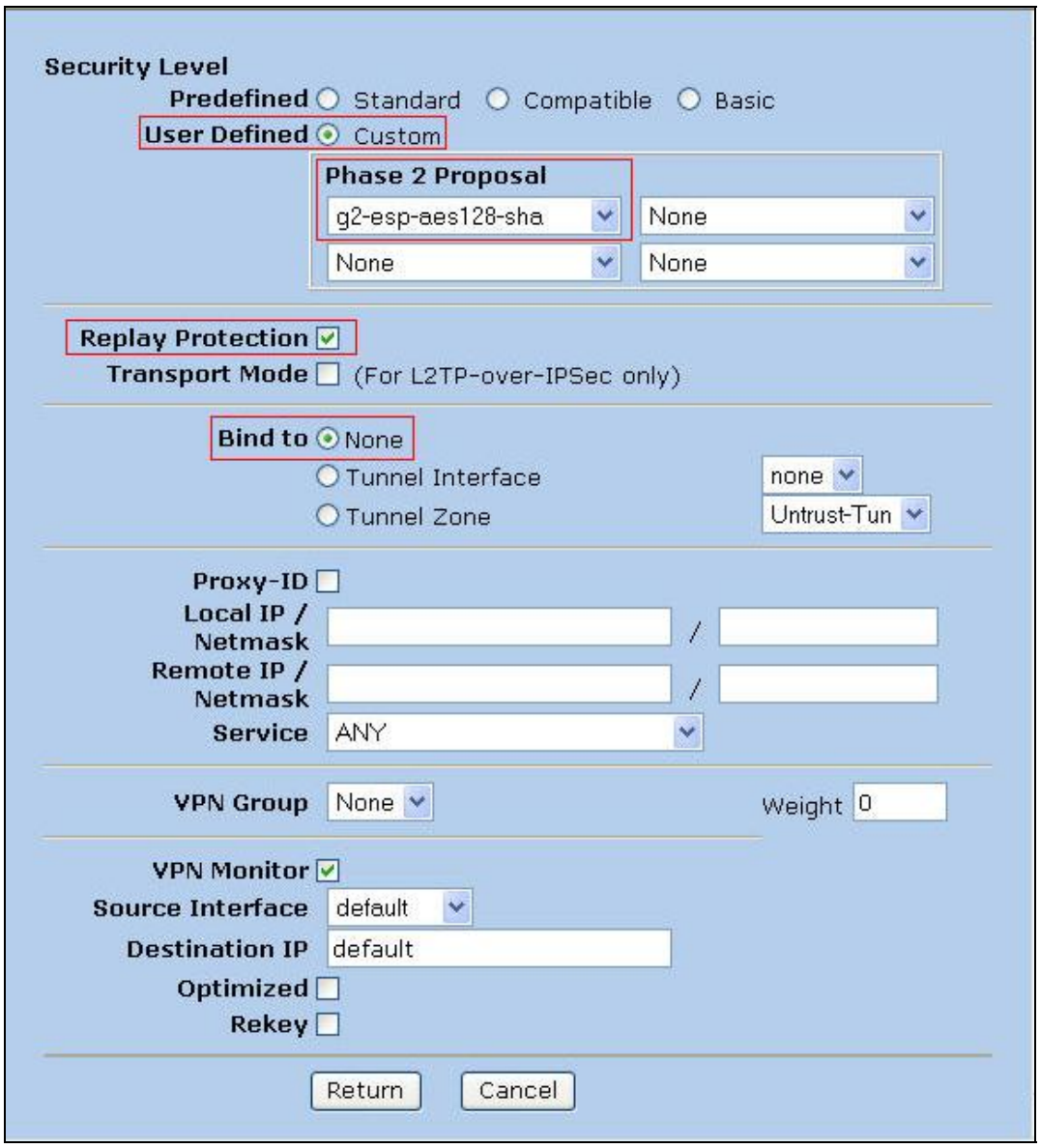
©2008 Avaya Inc. All Rights Reserved.

Step	Description
19.	**Phase 1 – Continued** Configure the highlighted fields shown below. All remaining fields can be left as default. Click the **Return** button at the bottom of the page (not shown) to complete the advanced configuration and then click the **OK** button on the previous page to save. Select ***Custom*** for **Security Level** and the appropriate **Phase 1 Proposal** from the drop-down menu. Refer to **Step 17**. **Mode** must be set to ***Aggressive*** for endpoint 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 Netscreen-50 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 Netscreen-50 uses UDP to encapsulate each IPSec packet. In the case of the compliance test, the Linksys router serves as a NAT device. 

©2008 Avaya Inc. All Rights Reserved.

Step	Description
20.	**Phase 1 Complete** The gateway configured in **Steps 18 – 19** can be displayed by navigating to **VPNs > AutoKey Advanced > Gateway**. Name | Peer Type | Address/ID/User Group | Local ID | Security Level | Configure vpnphone-gw | Dialup | vpnphone-grp | - | Custom | Edit Xauth -
21.	**AutoKey IKE VPN Tunnel Configuration – Phase 2** From the left navigation menu, select **VPNs > AutoKey IKE**. On the **AutoKey IKE** page (not shown), click **New**. Configure the highlighted fields shown below. All remaining fields can be left as default. Provide a descriptive **VPN Name**. Selecting ***Custom*** for the **Security Level** provides access to a more complete list of proposals available on the Netscreen-50. Select ***Predefined*** for **Remote Gateway** and then select the remote gateway name entered in **Step 18** from the drop-down menu (***vpnphone-gw***). Click the **Advanced** button to access additional configuration options. VPN Name: vpnphone-vpn Security Level: Standard / Compatible / Basic / Custom Remote Gateway: Predefined vpnphone-gw Create a Simple Gateway Gateway Name Type: Static IP — Address/Hostname Dynamic IP — Peer ID Dialup User — User None Dialup Group — Group None Local ID (optional) Preshared Key — Use As Seed Security Level: Standard / Compatible / Basic Outgoing Interface: ethernet1 OK Cancel Advanced

©2008 Avaya Inc. All Rights Reserved.

Step	Description
22.	**Phase 2 Continued** Configure the highlighted fields shown below. All remaining fields can be left as default. Click the **Return** button at the bottom of the page (not shown) to complete the advanced configuration and then click the **OK** button on the previous page to save. Select ***Custom*** for **Security Level** and the appropriate **Phase 2 Proposal** from the drop-down menu. Refer to **Step 17**. **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 1, for all VPN tunnel traffic. 

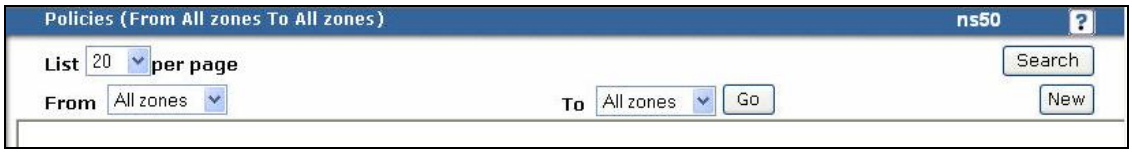
©2008 Avaya Inc. All Rights Reserved.

Step	Description
23.	**Phase 2 Complete** The VPN configured in **Steps 21 – 22** can be displayed by navigating to **VPNs > AutoKey IKE**. | Name	Gateway	Security	Monitor	Configure	
---	---	---	---	---	---
vpnphone-vpn	vpnphone-gw	Custom	On	Edit	- | |
24.	**XAuth Configuration – XAuth Server Settings** The Netscreen-50 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. This step configures the default settings of the local XAuth server. 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. Click **Apply** when complete. Select the **IP Pool Name** created in **Step 10** from the drop-down menu. This defines the IP Address range used when IP addresses are dynamically assigned to the Avaya VPNremote Phone by the XAuth server during IKE setup. Reserve Private IP for XAuth User: 480 Minutes Default Authentication Server: Local Query Client Settings on Default Server: ☐ CHAP: ☐ IP Pool Name: Remote-User-IP DNS Primary Server IP: 0.0.0.0 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

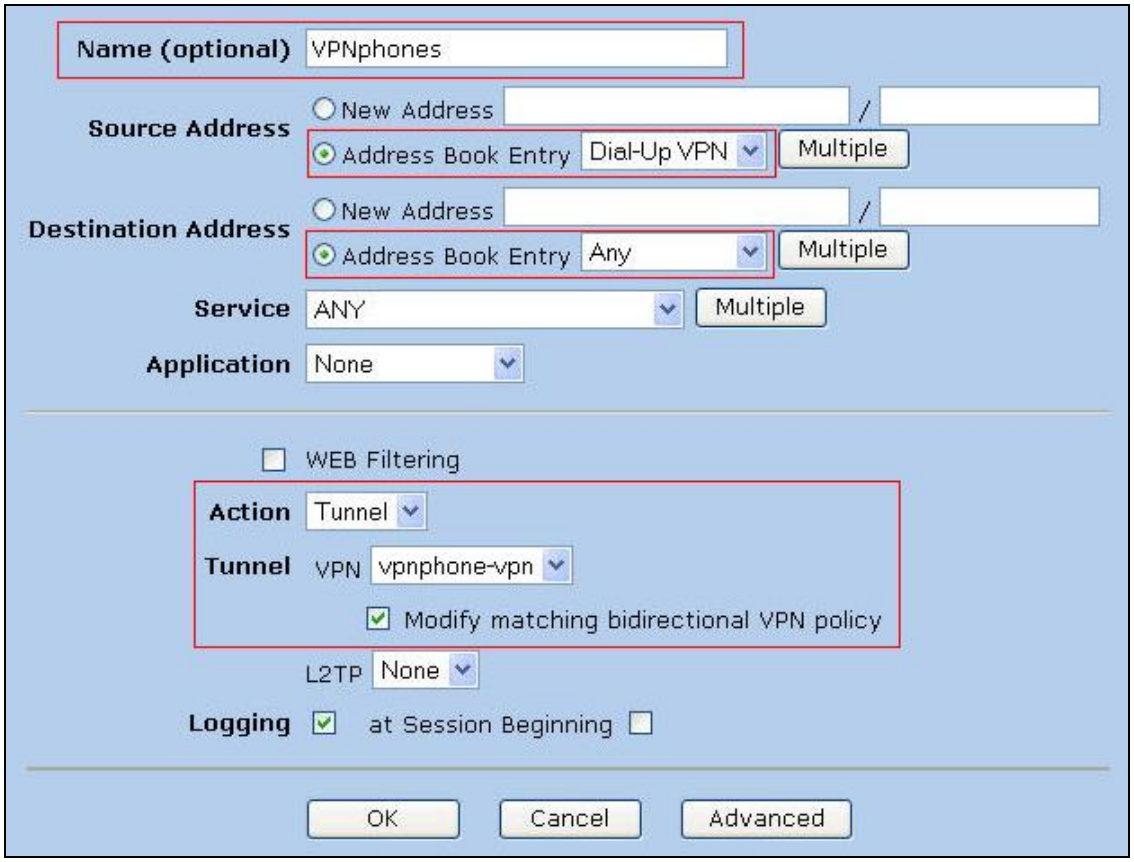
©2008 Avaya Inc. All Rights Reserved.

Step	Description
25.	**XAuth Configuration – IKE Gateway Settings** From the left navigation menu, select **VPNs** > **AutoKey Advanced** > **Gateway.** The IKE gateway created in **Steps 18 - 19** is displayed 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 | Edit | Xauth | -
26.	**XAuth Configuration – IKE Gateway Settings Continued** Configure the highlighted fields shown below. All remaining fields can be left as default. Click **OK** when complete to save settings. None XAuth Server Allowed Authentication Type: Generic, CHAP Only, CHAP & PAP Use Default Xauth Settings Local Authentication Allow Any User: None User Group: remoteuser-grp External Authentication: None, Query Remote Setting Allow Any User: Name User Group: Name 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 0 | Add No entry available OK | Apply | Cancel

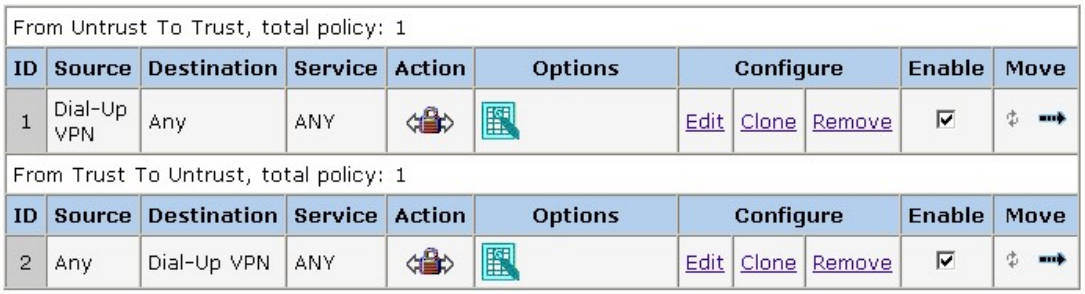
©2008 Avaya Inc. All Rights Reserved.

Step	Description
27.	**Policies** Security policies need to be created that will define what traffic is allowed to flow through the VPN tunnel. A policy was manually created for the traffic flowing from the Untrust zone to the Trust zone. Based on the options selected for this policy, the Netscreen-50 was instructed to create a matching policy for the Trust to Untrust direction. To create the policy in the Untrust to Trust direction, navigate to **Policies** from the left navigation menu. Any currently configured policies are displayed. On the top of the **Policies** page, select **Untrust** from the **From** drop-down menu and **Trust** from the **To** drop-down menu. Click the **New** button. 

©2008 Avaya Inc. All Rights Reserved.

Step	Description
28.	**Policies Continued** Configure the highlighted fields shown below. All remaining fields can be left as default. Enter a descriptive policy **Name** to easily identify this policy. The example below shows a policy for traffic that matches the criteria of **Source Address** of ***Dial-Up VPN***, any **Destination Address** and any **Service**. Selecting ***Dial-Up VPN*** as the **Source Address** defines the VPN tunnel as the traffic originator. The **Action** field defines the action to be taken when traffic matches the above criteria. Selecting ***Tunnel*** from the **Action** field drop-down menu indicates traffic will be allowed and associated with the particular VPN Tunnel specified in the **Tunnel VPN** field. Select ***vpnphone-vpn*** from the **Tunnel VPN** drop-down menu. This is the VPN tunnel defined for the Avaya VPNremote Phones. Check the **Modify matching bidirectional VPN policy** box to have the Netscreen-50 automatically create a matching VPN policy for traffic flowing in the opposite direction. Click **OK** to save. 

©2008 Avaya Inc. All Rights Reserved.

Step	Description
29.	**Policies Continued** The **Policies** page displays the new Dial-Up VPN policies.  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

6. Configure XtremeSat

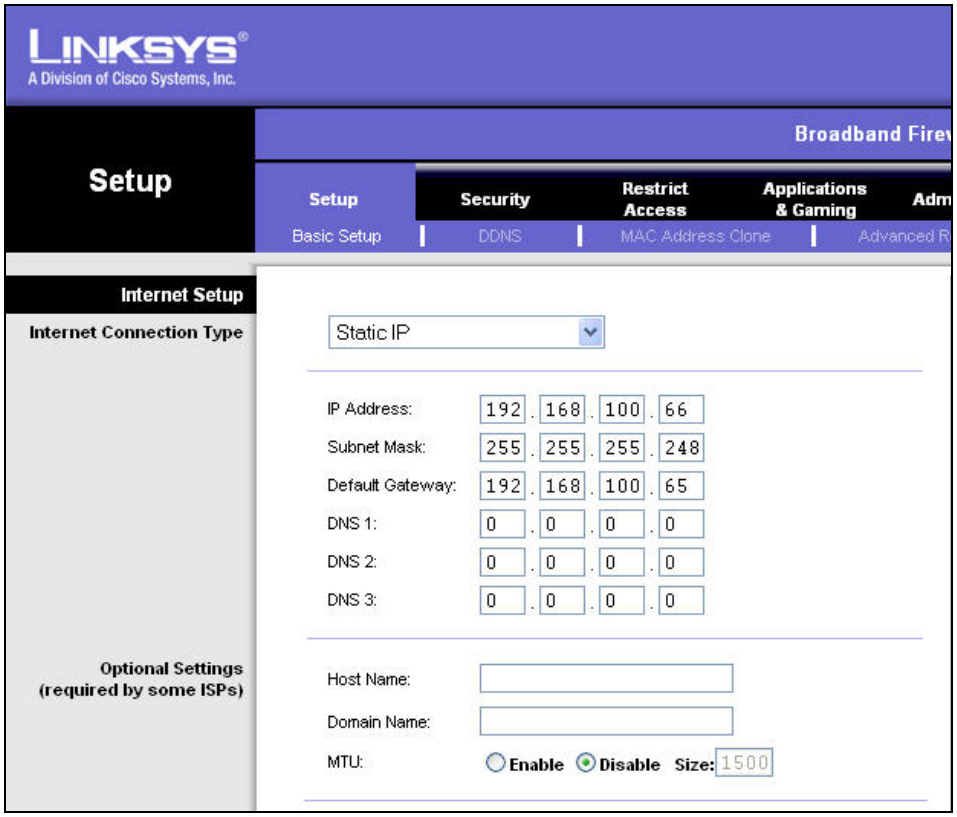
The configuration of XtremeSat is done by Clear Channel Satellite and is not expected to be done by the end user or a third party technician. This includes configuration of the SIT and dish alignment if using a fixed dish. The auto-acquisition dish does not require manual alignment. The auto-acquisition dish will automatically align with the satellite signal once it is powered up and deployed.

7. Configure Linksys BEFSX41 Broadband Firewall Router

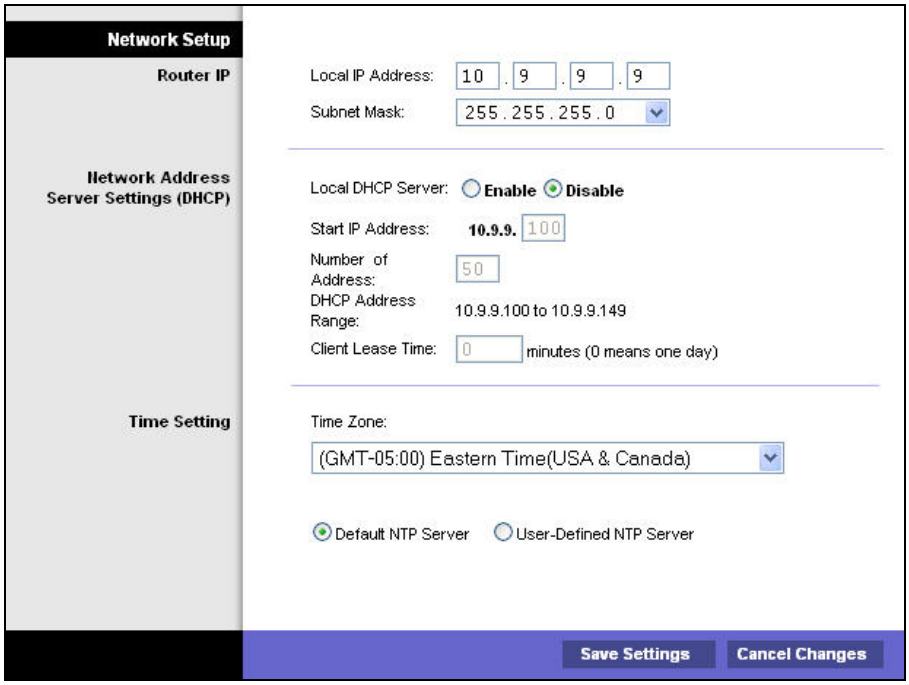
This section describes the configuration of the Linksys BEFSX41 Broadband Firewall Router. This section assumes the Linksys router has been installed as described in [12] and starts with the factory defaults.

Step	Description
1.	**Login** The Linksys router is configured via a Web interface. Connect a PC configured for DHCP to any port on the private side of the router. Launch a Web browser and enter the IP address of the Linksys router in the URL field. Log in with the appropriate user name and password.

©2008 Avaya Inc. All Rights Reserved.

Step	Description
2.	**Internet Setup** After log in the **Basic Setup** page is displayed. Under **Internet Setup**, select ***Static IP*** for the **Internet Connection Type**. Enter the values provided by Clear Channel Satellite for the **IP Address**, **Subnet Mask** and **Default Gateway** fields. 

©2008 Avaya Inc. All Rights Reserved.

Step	Description
3.	**Local Network Setup** Scroll down to the **Network Setup** section of the page. Enter an IP address for the router that will be used on the private side of the device in the **Local IP Address** field and a corresponding subnet mask in the **Subnet Mask** field. The Avaya VPNremote Phones will be configured with static IP addresses. Thus, disable the DHCP server of the router by clicking the **Disable** radio button next to the **Local DHCP Server** field. Select the appropriate **Time Zone** for the location from the pull-down menu. Default values can be used for all other fields. Click the **Save Settings** button to complete the configuration. 

8. Configure Avaya MCS – Avaya C363T-PWR Converged Stackable Switch

This section describes the Avaya C363T-PWR Converged Stackable Switch configuration as part of Avaya MCS. This section assumes the Avaya C363T-PWR has been installed using the procedures described in [6]. There is no additional configuration to be performed. The switch uses the factory defaults of all ports on a single VLAN (VLAN 1). No layer 3 routing is enabled.

©2008 Avaya Inc. All Rights Reserved.

9. Configure Avaya MCS – 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. The following steps describe how to configure the Avaya VPNremote Phone VPN parameters locally from the telephone.

Step	Description

1.	**VPN Options Menu Access**
	There are two methods available to access the **VPN Options** menu from the Avaya VPNremote Phone.
	
	During Telephone Boot:
	
	During the 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 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`
	
	During Telephone Operation:
	
	While the Avaya 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.

©2008 Avaya Inc. All Rights Reserved.

Step	Description
2.	**VPN Options** The **VPN Options** menu is displayed. The configuration values for the Avaya VPNremote Phone of user Tim, used in the sample configuration, are shown below. All values 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:	**192.168.105.232**	IP address of the Netscreen-50 public interface.
User Name:	**Tim**	User created in Netscreen-50 (**Section 5**, **Step 12**).
Password:	********	Must match user password entered in Netscreen-50 (**Section 5**, **Step 12**).
Group Name:	**vpnphone@avaya.com**	IKE Identity created in Netscreen-50 (**Section 5**, **Step 11**).
Group PSK:	********	Must match pre-shared key entered in Netscreen-50 (**Section 5**, **Step 18**).
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-Any-Any**	Must match IKE SA set in Netscreen-50 (**Section 5**, **Step 19**).
IKE ID Type:	**USER-FQDN**	Group Name format.
Diffie-Hellman Grp:	**2**	Can be set to "Detect" to accept Netscreen-50 settings.
Encryption Alg:	**Any**	When set to "Any", accept Netscreen-50 settings.
Authentication Alg:	**Any**	When set to "Any", accept Netscreen-50 settings.
IKE Xchg Mode:	**Aggressive**	Mode used for Phase 1 Negotiations.
IKE Config Mode:	**Enable**	Enables IKE.

©2008 Avaya Inc. All Rights Reserved.

Step	Description
3.	**VPN Configuration Options Continued**

Configuration Options	Value	Description
IPSec Parameters:	**DH2-Any-Any**	Must match IPSec proposals set in Netscreen-50 (**Section 5**, **Step 22**).
Encryption Alg:	**Any**	When set to "Any", accept Netscreen-50 settings.
Authentication Alg:	**Any**	When set to "Any", accept Netscreen-50 settings.
Diffie-Hellman Grp:	**2**	Can be set to "Detect" to accept Netscreen-50 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:	**10.75.10.52**	TFTP/HTTP file server.
Connectivity Check:	**First Time**	Test initial IPSec connectivity.
QTest	**Disable**	

4. **VPN Configuration Profile**

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

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

©2008 Avaya Inc. All Rights Reserved.

Step	Description

5.	**Save Configuration**
	When all VPN configuration options have been set, press the **Done** soft button. The following message is displayed. Press # to save the configuration and reboot phone.
	
	`Save new values ?`
	`*=no  #=yes`

10. Interoperability Compliance Testing

This section describes the compliance testing used to verify the interoperability of Clear Channel Satellite XtremeSat with Avaya Mobile Communication System with the VPNremote Phone option to support remote telephone users. This section covers the general test approach and the test results.

10.1. General Test Approach

The general test approach was to make varying types of calls through XtremeSat and exercise common PBX features. Calls were made between Avaya MCS and the main site. All functionality listed below was tested using the one meter fixed dish.

10.2. Test Results

XtremeSat passed compliance testing. The following features and functionality were verified. Any observations related to these tests are listed at the end of this section.

- Outbound calls from Avaya MCS to the main site.
- Inbound calls from the main site to Avaya MCS.
- Intra-site calls between Avaya MCS endpoints.
- PBX features including Hold, Transfer, Call Forwarding and Conference.
- Proper DTMF tone detection.
- Voice mail and message waiting indicators (MWI).
- Internet access.
- Proper system recovery after a SIT restart and loss of IP connection.

The following observations were made during the compliance test.

1. A noticeable delay of one to two seconds was experienced on each call. This is expected with the known latency of a satellite link.
2. Since the voice traffic is routed over the Internet, there is no mechanism to ensure that voice traffic is given priority over data traffic.
3. It was observed that it was not necessary to disable IP-IP Direct Audio for the specific configuration and test cases covered in the compliance test as was recommended in the Avaya VPNremote Phone Release Notes [9] when using a Juniper Networks Netscreen device at the enterprise. However, if a user experiences no audio for calls between Avaya VPNremote Phones then IP-IP Direct Audio should be disabled in the IP network region where the Avaya VPNremote Phones reside.

©2008 Avaya Inc. All Rights Reserved.

11. Verification Steps

The following steps may be used to verify the configuration:

- From a PC on the Internet, ping the public IP addresses of the SIT and Linksys router to verify data connectivity inward to the Linksys router.
- From a PC connected to the Avaya VPNremote Phone, ping the public IP addresses of the SIT and Linksys router to verify data connectivity outward to the Linksys router.
- From a PC connected to the Avaya VPNremote Phone, verify that a web browser can be used to access a public Internet website.
- From the Avaya Communication Manager SAT, use the **status station** command to verify that the Avaya VPNremote Phone is in-service.
- Verify that calls can be placed from an Avaya VPNremote Phone to the main site.
- Verify that calls can be placed from the main site to an Avaya VPNremote Phone.

12. Support

For technical support on XtremeSat, contact Clear Channel Satellite via the support link at www.clearchannelsatellite.net.

13. Conclusion

Clear Channel Satellite XtremeSat passed compliance testing. These Application Notes describe the procedures required to configure Avaya Mobile Communication System to interoperate with Clear Channel Satellite XtremeSat to support remote users using Avaya VPNremote Phones as shown in **Figure 1**.

©2008 Avaya Inc. All Rights Reserved.

14. Additional References

[1] *Installing and Upgrading the Avaya G700 Media Gateway and Avaya S8300 Media Server,* Doc # 555-234-100, Issue 10.2, May 2007.

[2] *Administrator Guide for Avaya Communication Manager*, Doc # 03-300509, Issue 3.1, February 2007.

[3] *Avaya IA 770 INTUITY AUDIX Messaging Application*, Doc # 11-300532, May 2005.

[4] *4600 Series IP Telephone Release 2.8 LAN Administrator Guide*, Doc # 555-233-507, Issue 6, February 2007.

[5] *Avaya IP Softphone Release 6.0 User Reference,* Issue 1, May 2007.

[6] *Installation and Configuration for the Avaya C360 Converged Stackable Switches Software Version 4.5,* Doc # 10-300503, Issue 2, July 2005.

[7] *Avaya Mobile Communication Overview*, http://www.avaya.com/gcm/master-usa/en-us/solutions/offers/mobile_communication_system.htm.

[8] *VPNremote for the 4600 Series IP Telephones Release 2.1 Administrator Guide*, Doc # 19-600753, Issue 3, June 2007.

[9] *Avaya VPNremote Phone Release Notes (vpnphone_readme.html)* located at the VPNremote Phone Download link, June 2007.

[10] *Configuring the Juniper Networks SSG Security Platform and Steel-Belted Radius Authentication Server to Support Avaya VPNremote Phones*, June 26, 2007.

[11] *Application Notes for Converting an Avaya 4600 Series IP Telephone to an Avaya VPNremote Phone*, May 17, 2007.

[12] *Linksys Broadband Firewall Router with 4-Port Switch/VPN Endpoint User Guide, Model BEFSX41.*

[13] *Concepts & Examples Screen0S Reference Guide,* Release 5.4.0 Rev B, January 2007.

Product documentation for Avaya products may be found at http://support.avaya.com.

Product documentation for the Linksys router can be obtained from http://www.linksys.com.

Product documentation for XtremeSat can be obtained from Clear Channel Satellite.

©2008 Avaya Inc. All Rights Reserved.

Appendix A: Avaya C363T-PWR Configuration File

Included below is the Avaya C363T-PWR Converged Stackable Switch configuration file used during the compliance testing for the switch at the main site. It can be displayed on the switch by using the **show run** command.

```
#!#$@ DO NOT REMOVE THIS LINE - Avaya Inc. C360 Switch - Router configuration

! Avaya Inc. C360 Switch - Router configuration
! version 4.5.14
set vlan       1 name "fw"
set vlan       2 name "voice"
set vlan       3 name "data"
set vlan       4 name "wan"
set vlan       5 name "satellite"
!
ip bootp-dhcp relay
!
interface "IPI1"
 ip vlan name "fw"
 ip address 10.75.1.1       255.255.255.0
 ip bootp-dhcp server 10.75.10.100
!
interface "IPI2"
 ip vlan name "voice"
 ip address 10.75.5.1       255.255.255.0
 ip bootp-dhcp server 10.75.10.100
!
interface "IPI3"
 ip vlan name "data"
 ip address 10.75.10.1      255.255.255.0
 ip bootp-dhcp server 10.75.10.100
!
interface "IPI5"
 ip vlan name "satellite"
 ip address 192.168.20.2    255.255.255.0
!
ip default-gateway 10.75.1.254     1 low
ip route   10.9.9.0        255.255.255.0   192.168.20.1    1 low
ip route   100.100.100.0   255.255.255.0   192.168.20.1    1 low
!#
!# End of Configuration File
```


©2008 Avaya Inc. All Rights Reserved.

Appendix B: NetScreen-50 Configuration File

Included below is the Juniper Networks NetScreen-50 configuration file used during the compliance testing at the main site. It can be displayed on the NetScreen-50 by using the **get configuration** command.

```
set clock timezone 0
set vrouter trust-vr sharable
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset auto-route-export
exit
unset alg h323 enable
set auth-server "Local" id 0
set auth-server "Local" server-name "Local"
set auth default auth server "Local"
set auth radius accounting port 1646
set admin name "netscreen"
set admin password "nKVUM2rwMUzPcrkG5sWIHdCtqkAibn"
set admin auth timeout 10
set admin auth server "Local"
set admin format dos
set zone "Trust" vrouter "trust-vr"
set zone "Untrust" vrouter "trust-vr"
set zone "DMZ" vrouter "trust-vr"
set zone "VLAN" vrouter "trust-vr"
set zone "Untrust-Tun" vrouter "trust-vr"
set zone "Trust" tcp-rst
set zone "Untrust" block
unset zone "Untrust" tcp-rst
set zone "MGT" block
set zone "DMZ" tcp-rst
set zone "VLAN" block
unset zone "VLAN" tcp-rst
set zone "Untrust" screen tear-drop
set zone "Untrust" screen syn-flood
set zone "Untrust" screen ping-death
set zone "Untrust" screen ip-filter-src
set zone "Untrust" screen land
set zone "V1-Untrust" screen tear-drop
set zone "V1-Untrust" screen syn-flood
set zone "V1-Untrust" screen ping-death
set zone "V1-Untrust" screen ip-filter-src
set zone "V1-Untrust" screen land
set interface "ethernet1" zone "Trust"
set interface "ethernet2" zone "DMZ"
set interface "ethernet3" zone "Untrust"
unset interface vlan1 ip
set interface ethernet1 ip 192.168.20.1/24
set interface ethernet1 nat
set interface ethernet3 ip 192.168.105.232/27
set interface ethernet3 route
unset interface vlan1 bypass-others-ipsec
unset interface vlan1 bypass-non-ip
```


©2008 Avaya Inc. All Rights Reserved.

```
set interface ethernet1 ip manageable
set interface ethernet3 ip manageable
set interface ethernet3 manage ping
unset flow no-tcp-seq-check
set flow tcp-syn-check
set pki authority default scep mode "auto"
set pki x509 default cert-path partial
set ippool "Remote-User-IP" 100.100.100.1 100.100.100.50
set user "Terry" uid 4
set user "Terry" type  xauth
set user "Terry" password "RR6xlSb9NLYIkVsSb7CXDP1SVOny4Unuxg=="
unset user "Terry" type auth
set user "Terry" "enable"
set user "Tim" uid 2
set user "Tim" type  xauth
set user "Tim" password "Hy8vHd0qNZnl08svuCC6SyN3Rcn+c304dQ=="
unset user "Tim" type auth
set user "Tim" "enable"
set user "vpnphone-ike" uid 1
set user "vpnphone-ike" ike-id u-fqdn "vpnphone@avaya.com" share-limit 35
set user "vpnphone-ike" type  ike
set user "vpnphone-ike" "enable"
set user-group "remoteuser-grp" id 2
set user-group "remoteuser-grp" user "Terry"
set user-group "remoteuser-grp" user "Tim"
set user-group "vpnphone-grp" id 1
set user-group "vpnphone-grp" user "vpnphone-ike"
set ike gateway "vpnphone-gw" dialup "vpnphone-grp" Aggr outgoing-interface
"ethernet3" preshare "pI5B+ehxNL1muns6zhCxYtrwu+nCoDhLDg==" proposal "pre-g2-
3des-md5"
unset ike gateway "vpnphone-gw" nat-traversal udp-checksum
set ike gateway "vpnphone-gw" nat-traversal keepalive-frequency 5
set ike gateway "vpnphone-gw" xauth server "Local" user-group "remoteuser-grp"
set ike gateway "vpnphone-gw" xauth server auth-method chap pap
unset ike gateway "vpnphone-gw" xauth do-edipi-auth
set ike respond-bad-spi 1
unset ike ikeid-enumeration
unset ike dos-protection
unset ipsec access-session enable
set ipsec access-session maximum 5000
set ipsec access-session upper-threshold 0
set ipsec access-session lower-threshold 0
set ipsec access-session dead-p2-sa-timeout 0
unset ipsec access-session log-error
unset ipsec access-session info-exch-connected
unset ipsec access-session use-error-log
set xauth lifetime 5
set xauth default ippool "Remote-User-IP"
set vpn "vpnphone-vpn" gateway "vpnphone-gw" replay tunnel idletime 0 proposal
"g2-esp-aes128-sha"
set vpn "vpnphone-vpn" monitor
set url protocol websense
exit
set policy id 1 name "VPNphones" from "Untrust" to "Trust"  "Dial-Up VPN" "Any"
"ANY" tunnel vpn "vpnphone-vpn" id 1 pair-policy 2 log
set policy id 1
exit
```


©2008 Avaya Inc. All Rights Reserved.

```
set policy id 2 name "VPNphones" from "Trust" to "Untrust"  "Any" "Dial-Up VPN"
"ANY" tunnel vpn "vpnphone-vpn" id 1 pair-policy 1 log
set policy id 2
exit
set nsmgmt bulkcli reboot-timeout 60
set ssh version v2
set config lock timeout 5
set snmp port listen 161
set snmp port trap 162
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset add-default-route
set route 192.168.1.0/24 interface ethernet1 gateway 192.168.20.2
set route 0.0.0.0/0 interface ethernet3 gateway 192.168.105.225
set route 10.75.0.0/16 interface ethernet1 gateway 192.168.20.2 preference 20
exit
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
exit
```


©2008 Avaya Inc. All Rights Reserved.

©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 DevConnect Program at devconnect@avaya.com.