Avaya Solution & Interoperability Test Lab

Application Notes for Configuring AudioCodes nCite with Avaya SIP Enablement Services and Avaya Communication Manager to Support SIP Trunking - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring AudioCodes nCite with Avaya SIP Enablement Services and Avaya Communication Manager.

AudioCodes nCite is a SIP session border controller (SBC) that manages and protects the flow of SIP signaling and related media across an untrusted network. The compliance testing focused on telephony scenarios between two enterprise sites connected via a SIP trunk across an untrusted network.

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.

1. Introduction

These Application Notes describe the procedures for configuring AudioCodes nCite with Avaya SIP Enablement Services (SES) and Avaya Communication Manager.

AudioCodes nCite is a SIP session border controller (SBC) that manages and protects the flow of SIP signaling and related media across an untrusted network. The compliance testing focused on telephony scenarios between two enterprise sites connected via a SIP trunk across an untrusted network.

1.1. Configuration

Figure 1 illustrates the test configuration. The test configuration shows two enterprise sites connected via a SIP trunk across an untrusted IP network. Both sites have a Juniper Networks Netscreen-50 firewall at the edge of the network restricting unwanted traffic between the untrusted network and the enterprise. No Network Address Translation (NAT) is being performed by the Netscreen-50 in this configuration. nCite uses two physical interfaces to connect to the firewall in the demilitarized zone (DMZ) of the enterprise. One interface is used for nCite's public side and the other interface is used for the private side. On the public interface, three IP addresses are assigned to nCite. One is a private IP address assigned to the physical interface and two are public virtual addresses; one used for signaling and one used for media. On the private interface, two IP addresses are assigned to nCite. Both are private IP addresses; one is assigned to the physical interface and also used for signaling and the other is used for media (**see Table 1**). nCite supports only 1G Ethernet interfaces, so a 10M/100M/1G Layer 2 switch is used between nCite and the firewall to convert the 1G interfaces of nCite to the 100M interfaces of the firewall. The firewall will allow incoming SIP and RTP traffic directed to nCite. Outbound traffic will be unrestricted.

Two separate nCite models were used for the compliance test. An nCite 4000 was used at the main site and an nCite 1000 was used at the branch. Each nCite SBC is connected to the same management LAN which is separate from the local LAN at each site. Also connected to this common management LAN is the nCite EMS and a Windows PC. The Windows PC is used to access the EMS and perform centralized management for both nCite SBCs.

All SIP traffic flows through nCite at each site. In this manner, nCite can protect the local site's infrastructure from any SIP-based attacks. The voice communication across the untrusted network uses SIP over UDP and RTP for the media streams. All non-SIP traffic bypasses nCite and flows directly between the untrusted network and the private LAN of the enterprise if permitted by the firewall.

Located at the main site on the private LAN side of the firewall is an Avaya SES and an Avaya S8300 Server running Avaya Communication Manager in an Avaya G700 Media Gateway. Avaya IA 770 Intuity Audix is also running on the Avaya S8300 Server. Endpoints include an Avaya 4600 Series IP Telephone (with SIP firmware), an Avaya 4600 Series IP Telephone (with H.323 firmware), an Avaya 9600 Series Telephone (with H.323 firmware), an Avaya 9600 Series Telephone running Avaya one-X Deskphone Edition SIP firmware, an Avaya one-X Desktop Edition, an Avaya 6408D Digital Telephone, and an Avaya 6210 Analog Telephone. An ISDN-PRI trunk connects the media gateway to the PSTN. The PSTN numbers assigned to the ISDN-PRI trunk at the main site are mapped to telephone extensions at the main site. There are two Windows PCs on site; one is used as a TFTP/HTTP server and the other is used to manage nCite.

Located at the branch site on the private LAN side of the firewall is an Avaya SES and an Avaya S8300 Server running Avaya Communication Manager in an Avaya G350 Media Gateway. Avaya IA 770 Intuity Audix is also running on the Avaya S8300 Server. Endpoints include an Avaya 4600 Series IP Telephone (with SIP firmware), an Avaya 4600 Series IP Telephone (with H.323 firmware), an Avaya 9600 Series Telephone running Avaya one-X Deskphone Edition SIP software, and Avaya one-X Desktop Edition. The site also has a TFTP/HTTP server.

The SIP endpoints located at both sites are registered to the local Avaya SES. Each enterprise has a separate SIP domain: ***business.com*** for the main site and ***dev4.com*** for the branch. SIP telephones at both sites use the local TFTP/HTTP server to obtain their configuration files.

All calls originating from Avaya Communication Manager at the main site and destined for the branch will be routed through the on-site Avaya SES to the on-site nCite via the data firewall and from nCite to the untrusted IP network via the data firewall. Once across the untrusted network, the call enters the branch site via the data firewall located there and routed to the local nCite. From nCite, the call is routed to Avaya SES via the data firewall and finally to Avaya Communication Manager. Calls from the branch to the main site follow this same path in the reverse order.

For interoperability, direct IP to IP media (also known as media shuffling) must be disabled on both SIP trunks in Avaya Communication Manager (see **Section 3.1, Step 3**). This will result in VoIP resources being used in the Avaya Media Gateway for the duration of each SIP call.

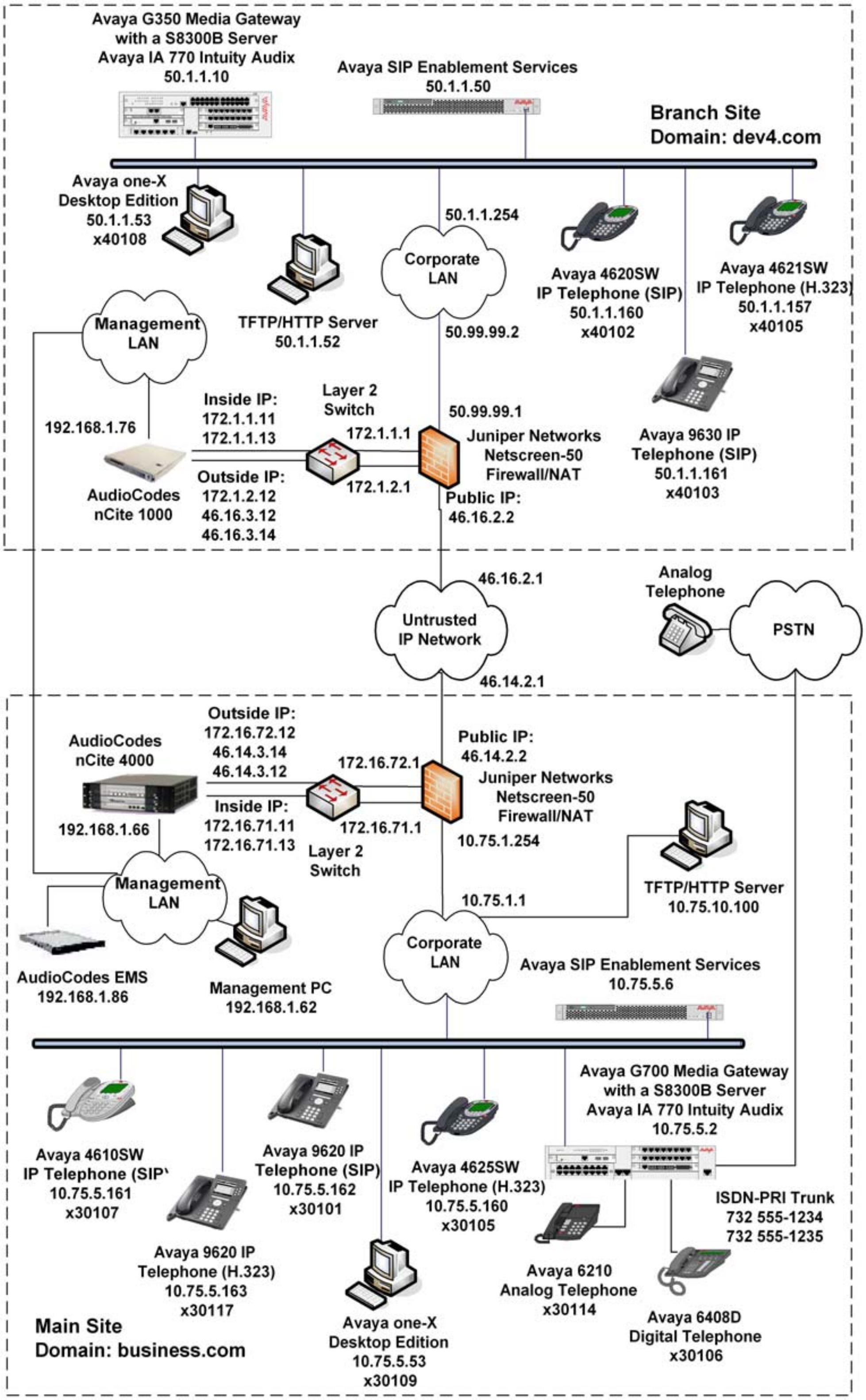


Figure 1: nCite SIP Trunking Test Configuration

nCite Interface Description	IP Address (Main)	IP Address (Branch)
External physical interface	172.16.72.12	172.1.2.12
External SIP signaling interface	46.14.3.14	46.16.3.14
External RTP media interface	46.14.3.12	46.16.3.12
Internal physical interface	172.16.71.11	172.1.1.11
Internal SIP signaling interface	172.16.71.11	172.1.1.11
Internal RTP media interface	172.16.71.13	172.1.1.13

Table 1: nCite IP Addresses

2. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8300B Server with Avaya G700 Media Gateway Avaya IA 770 Intuity Audix	Avaya Communication Manager 4.0.1 Service Pack (R014x.00.0.731.2-14300)
Avaya S8300B Server with Avaya G350 Media Gateway Avaya IA 770 Intuity Audix	Avaya Communication Manager 4.0.1 Service Pack (R014x.00.0.731.2-14300)
Avaya S8500B Server	Avaya SIP Enablement Services 4.0
Avaya 4610SW IP Telephone Avaya 4620SW IP Telephones	SIP version 2.2.2
Avaya 4621SW IP Telephones Avaya 4625SW IP Telephones	H.323 version 2.8.3
Avaya 9620 IP Telephones Avaya 9630 IP Telephones	Avaya one-X Deskphone Edition SIP 1.0.1 (SIP96xx_1_0_2_2.bin)
Avaya one-X Desktop Edition	2.1 (Build 70)
Avaya 6408D Digital Telephone	-
Avaya 6210 Analog Telephone	-
Analog Telephone	-
Windows PCs (Management PC and TFTP/HTTP Server)	Windows XP Professional SP 2
Juniper Networks Netscreen-50 (main site)	5.4.0r1.0
Juniper Networks Netscreen-50 (branch site)	5.4.0r6.0
AudioCodes nCite 1000	3.4.3.P3
AudioCodes nCite 4000	3.4.3.P3
AudioCodes nCite EMS	3.4.3.P3

Table 2: Equipment List

3. Configure Avaya Communication Manager

This section describes the Avaya Communication Manager configuration at the main site to support the network shown in **Figure 1**. It assumes the procedures necessary to support SIP and connectivity to Avaya SES have been performed as described in [3]. It also assumes that an off-PBX station (OPS) has been configured on Avaya Communication Manager for each SIP endpoint in the configuration as described in [3] and [4].

This section is divided into two parts. **Section 3.1** will summarize the user-defined parameters used in the installation procedures that are important to understanding the solution as a whole. It will not attempt to show the installation procedures in their entirety. It will also describe any deviations from the standard procedures, if any.

Section 3.2 will describe procedures beyond the initial SIP installation procedures that are necessary for interoperating with nCite.

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.

This configuration must be repeated for Avaya Communication Manager at the branch using values appropriate for the branch from **Figure 1**. This includes but is not limited to the IP addresses, SIP domain and user extensions.

3.1. Summary of Initial SIP Installation

This section summarizes the applicable user-defined parameters used during the SIP installation procedures.

Step	Description
1.	**IP network region** The Avaya S8300 Server, Avaya SES and IP (H.323/SIP) endpoints were located in a single IP network region (IP network region 1) using the parameters described below. Use the **display ip-network-region** command to view these settings. The example below shows the values used for the compliance test. ▪ **Authoritative Domain**: ***business.com*** This field was configured to match the domain name configured on Avaya SES. This name will appear in the "From" header of SIP messages originating from this IP region. ▪ **Name**: ***Default*** Any descriptive name may be used. ▪ **Intra-region IP-IP Direct Audio**: *yes* **Inter-region IP-IP Direct Audio**: *yes* By default, IP-IP direct audio (media shuffling) is enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. Shuffling can be further restricted at the trunk level on the **Signaling Group** form. ▪ **Codec Set**: ***1*** The codec set contains the set of codecs available for calls within this IP network region. This includes SIP calls since all necessary components are within the same region.

```
display ip-network-region 1                                     Page   1 of  19
                               IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: business.com
    Name: Default
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: 3329
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
```

Step	Description
2.	**Codecs** IP codec set 1 was used for the compliance test. Multiple codecs were listed in priority order to allow the codec used by a specific call to be negotiated during call establishment. The list includes the codecs the enterprise wishes to support within the normal trade-off of bandwidth versus voice quality. The example below shows the values used in the compliance test. It should be noted that when testing the use of G.729AB, G.711MU was removed from the list.

```
display 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: G.729AB           n         2        20
 3:
```

Step	Description
3.	**Signaling Group** For the compliance test, signaling group 1 was used for the signaling group associated with the SIP trunk group between Avaya Communication Manager and Avaya SES. Signaling group 1 was configured using the parameters highlighted below. All other fields were set as described in [3]. ▪ **Near-end Node Name**: ***procr*** This node name maps to the IP address of the Avaya S8300 Server. Node names are defined using the **change node-names ip** command. ▪ **Far-end Node Name**: ***SES*** This node name maps to the IP address of Avaya SES. ▪ **Far-end Network Region**: ***1*** This defines the IP network region which contains Avaya SES. ▪ **Far-end Domain**: blank This domain will default to the domain specified in the IP network region form in **Step 1.** This domain is sent in the "To" header of SIP messages of calls using this signaling group. ▪ **Direct IP-IP Audio Connections**: ***n*** For interoperability, this field must be set to ***n*** to disable media shuffling on the SIP trunk.

```
display signaling-group 1
                                SIGNALING GROUP

 Group Number: 1              Group Type: sip
                        Transport Method: tls



   Near-end Node Name: procr                Far-end Node Name: SES
 Near-end Listen Port: 5061               Far-end Listen Port: 5061
                                       Far-end Network Region: 1
       Far-end Domain:

                                            Bypass If IP Threshold Exceeded? n

         DTMF over IP: rtp-payload           Direct IP-IP Audio Connections? n
                                                       IP Audio Hairpinning? n
 Enable Layer 3 Test? n
 Session Establishment Timer(min): 3
```

Step	Description

4. **Trunk Group**

For the compliance test, trunk group 1 was used for the SIP trunk group between Avaya Communication Manager and Avaya SES. Trunk group 1 was configured using the parameters highlighted below. All other fields were set as described in [3].

- **Signaling Group**: ***1*** This field is set to the signaling group shown in the previous step.
- **Number of Members: *24*** This field represents the number of trunks in the SIP trunk group. It determines how many simultaneous SIP calls can be supported by the configuration. Each SIP call between two SIP endpoints (whether internal or external) requires two SIP trunks for the duration of the call. Thus, a call from a SIP telephone to another SIP telephone will use two SIP trunks. A call between a non-SIP telephone and a SIP telephone will only use one trunk.

```
display trunk-group 1                                           Page   1 of  21
                                TRUNK GROUP

Group Number: 1                    Group Type: sip           CDR Reports: y
  Group Name: SES Trk Grp                 COR: 1        TN: 1        TAC: 101
   Direction: two-way        Outgoing Display? n
 Dial Access? n                                    Night Service:
Queue Length: 0
Service Type: tie                   Auth Code? n

                                                       Signaling Group: 1
                                                     Number of Members: 24
```

5. **Trunk Group – continued**

On **Page 3**:

- Verify the **Numbering Format** field is set to ***public***. This field specifies the format of the calling party number sent to the far-end.
- The default values may be retained for the other fields.

```
display trunk-group 1                                           Page   3 of  21
TRUNK FEATURES
          ACA Assignment? n            Measured: none
                                                          Maintenance Tests? y



                     Numbering Format: public
                                                UUI Treatment: service-provider


                                                Replace Unavailable Numbers? n


 Show ANSWERED BY on Display? y
```

Step	Description
6.	**Public Unknown Numbering** Public unknown numbering defines the calling party number to be sent to the far-end. An entry was created for the trunk group defined in **Step 4**. In the example shown below, all calls originating from a 5-digit extension beginning with 3 and routed across trunk group 1 will be sent as a 5 digit calling number. This calling party number is sent to the far-end in the SIP “From” header.

```
change public-unknown-numbering 0                               Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext           Trk       CPN             CPN
Len Code          Grp(s)    Prefix          Len
                                                     Total Administered: 5
 5  3             1                         5           Maximum Entries: 240
```

3.2. Configure SIP Trunk and Routing to the Branch Site

To communicate to the branch site, a second SIP trunk with the appropriate call routing must be configured on Avaya Communication Manager. This SIP trunk will be used to route SIP calls to Avaya SES that are destined for the branch site SIP domain.

Step	Description
1.	**Signaling Group** For the compliance test, signaling group 6 was used for the signaling group associated with the SIP trunk group defined for branch site calls (see **Step 2**). Signaling group 6 was configured using the same parameters as signaling group 1 in **Section 3.1** with the exception of the far-end domain. The **Far-end Domain** field is set to the domain of the branch site Avaya SES, ***dev4.com***.

```
display signaling-group 6
                                SIGNALING GROUP

 Group Number: 6              Group Type: sip
                        Transport Method: tls


   Near-end Node Name: procr                Far-end Node Name: SES
 Near-end Listen Port: 5061               Far-end Listen Port: 5061
                                        Far-end Network Region: 1
       Far-end Domain: dev4.com

                                             Bypass If IP Threshold Exceeded? n


         DTMF over IP: rtp-payload            Direct IP-IP Audio Connections? n
                                                        IP Audio Hairpinning? n
 Enable Layer 3 Test? n
 Session Establishment Timer(min): 3
```

Step	Description
2.	**Trunk Group** For the compliance test, trunk group 6 was used for the SIP trunk group defined for branch site calls. Trunk group 6 was configured using the same parameters as trunk group 1 in **Section 3.1** except the **Signaling Group** field is set to ***6***. This includes the settings on **Page 3** of the trunk group form (not shown).

```
display trunk-group 6                                           Page   1 of  21
                                TRUNK GROUP

Group Number: 6                   Group Type: sip           CDR Reports: y
  Group Name: Site2SES                   COR: 1        TN: 1        TAC: 106
   Direction: two-way       Outgoing Display? n
 Dial Access? n                                Night Service:
Queue Length: 0
Service Type: tie                  Auth Code? n

                                                    Signaling Group: 6
                                                  Number of Members: 10
```

Step	Description
3.	**Public Unknown Numbering** A new entry was created for the trunk group defined in **Step 2**. In the example shown below, all calls originating from a 5-digit extension beginning with 3 and routed across trunk group 6 will be sent as a 5-digit calling number. This calling party number is sent to the far-end in the SIP “From” header.

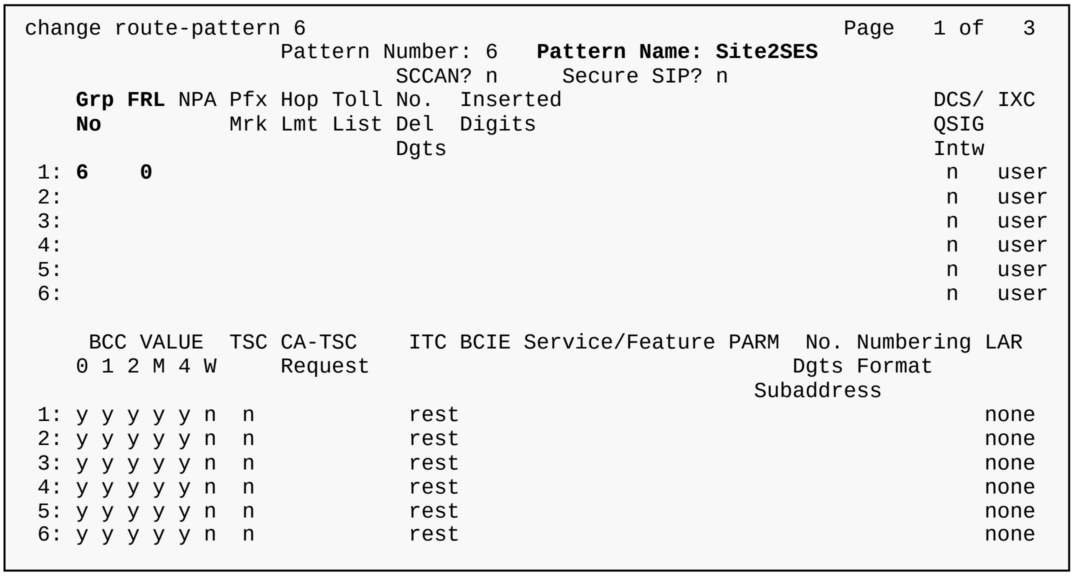
```
change public-unknown-numbering 0                               Page   1 of   2
                      NUMBERING - PUBLIC/UNKNOWN FORMAT
                                           Total
Ext Ext            Trk       CPN            CPN
Len Code           Grp(s)    Prefix         Len
                                                      Total Administered: 5
 5  3              1                        5            Maximum Entries: 240
 5  3              6                        5
```

Step	Description
4.	**Automatic Alternate Routing** Automatic Alternate Routing (AAR) was used to route calls to the branch site. In the example shown, numbers that begin with 4 and are 5 digits long use route pattern 6. Route pattern 6 routes calls to the SIP trunk defined for branch site calls.

```
display aar analysis 4                                          Page   1 of   2
                             AAR DIGIT ANALYSIS TABLE
                                                         Percent Full:    3

          Dialed           Total     Route    Call   Node   ANI
          String          Min  Max  Pattern   Type   Num    Reqd
    4                     5    5     6        aar           n
```

Step	Description
5.	**Route Pattern** For the compliance test, route pattern 6 was used for calls destined for the branch site. Route pattern 6 was configured using the parameters highlighted below. ▪ **Pattern Name**: Any descriptive name. ▪ **Grp No**: ***6*** This field is set to the trunk group number defined in **Step 2**. ▪ **FRL**: ***0*** This field is the Facility Restriction Level of the trunk. It must be set to an appropriate level to allow authorized users to access the trunk. The level of 0 is the least restrictive.



```
change route-pattern 6                                          Page   1 of   3
                    Pattern Number: 6   Pattern Name: Site2SES
                             SCCAN? n     Secure SIP? n
    Grp FRL NPA Pfx Hop Toll No.  Inserted                             DCS/ IXC
    No          Mrk Lmt List Del  Digits                               QSIG
                             Dgts                                      Intw
 1: 6    0                                                              n   user
 2:                                                                     n   user
 3:                                                                     n   user
 4:                                                                     n   user
 5:                                                                     n   user
 6:                                                                     n   user

     BCC VALUE  TSC CA-TSC    ITC BCIE Service/Feature PARM  No. Numbering LAR
    0 1 2 M 4 W     Request                                 Dgts Format
                                                         Subaddress
 1: y y y y y n  n            rest                                         none
 2: y y y y y n  n            rest                                         none
 3: y y y y y n  n            rest                                         none
 4: y y y y y n  n            rest                                         none
 5: y y y y y n  n            rest                                         none
 6: y y y y y n  n            rest                                         none
```

4. Configure Avaya SIP Enablement Services

This section covers the configuration of Avaya SES at the main site. Avaya SES is configured via an Internet browser using the administration web interface. It is assumed that the Avaya SES software and the license file have already been installed on the server. During the software installation, an installation script is run from the Linux shell of the server to specify the IP network properties of the server along with other parameters. In addition, it is assumed that the setup screens of the administration web interface have been used to initially configure Avaya SES. For additional information on these installation tasks, refer to [5].

Each SIP endpoint used in the compliance test that registers with Avaya SES requires that a user and media server extension be created on Avaya SES. This configuration is not directly related to the interoperability of nCite so it is not included here. These procedures are covered in [5].

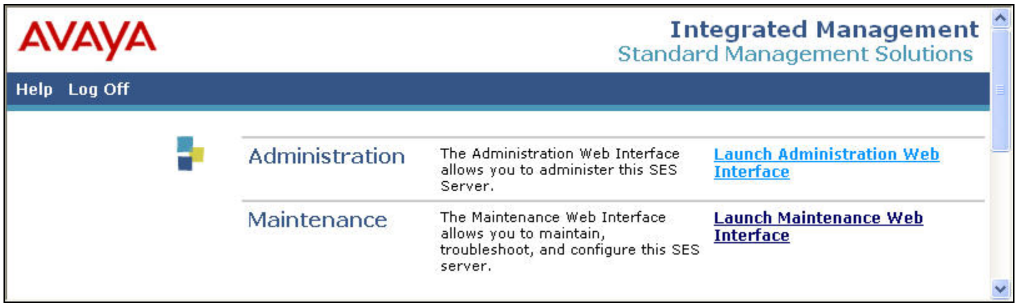
This section is divided into two parts. **Section 4.1** will summarize some of the user-defined parameters used in the installation procedures that are important to understanding the solution as a whole. It will not attempt to show the installation procedures in their entirety. It will also describe any deviations from the standard procedures, if any.

Section 4.2 will describe procedures beyond the initial SIP installation procedures that are necessary for interoperating with nCite.

This configuration must be repeated for Avaya SES at the branch using values appropriate for the branch from **Figure 1**. This includes but is not limited to the IP addresses, SIP domain and user extensions.

4.1. Summarize Initial Configuration Parameters

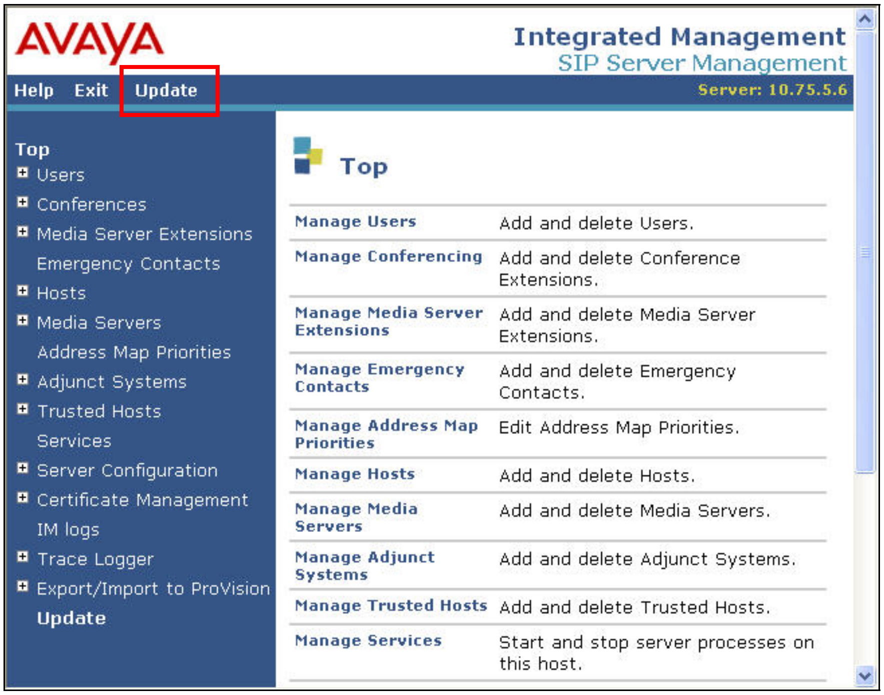
This section summarizes the applicable user-defined parameters used during the SIP installation procedures.

Step	Description
1.	**Login** Access the Avaya SES administration web interface by entering [http://<*ip-addr*>/admin]() as the URL in an Internet browser, where <*ip-addr*> is the IP address of the Avaya SES server. Log in with the appropriate credentials and then select the **Launch Administration Web Interface** link from the main page as shown below.  AVAYA Integrated Management Standard Management Solutions Help Log Off Administration The Administration Web Interface allows you to administer this SES Server. Launch Administration Web Interface Maintenance The Maintenance Web Interface allows you to maintain, troubleshoot, and configure this SES server. Launch Maintenance Web Interface

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>2.</td><td>

Top Page
The Avaya SES **Top** page will be displayed as shown below.

If any changes are made within Avaya SES, an **Update** link appears in the menu options at the top of the page. It is necessary to click this link to commit the pending changes to the database.



Manage Users	Add and delete Users.
Manage Conferencing	Add and delete Conference Extensions.
Manage Media Server Extensions	Add and delete Media Server Extensions.
Manage Emergency Contacts	Add and delete Emergency Contacts.
Manage Address Map Priorities	Edit Address Map Priorities.
Manage Hosts	Add and delete Hosts.
Manage Media Servers	Add and delete Media Servers.
Manage Adjunct Systems	Add and delete Adjunct Systems.
Manage Trusted Hosts	Add and delete Trusted Hosts.
Manage Services	Start and stop server processes on this host.

</td></tr>
<tr><td>3.</td><td>

Initial Configuration Parameters
As part of the Avaya SES installation and initial configuration procedures, the following parameters were defined. Although these procedures are out of the scope of these Application Notes, the values used in the compliance test are shown below for reference. After each parameter is a brief description of how to view the value from the Avaya SES administration home page shown in the previous step.

- SIP Domain: ***business.com***
  (To view, navigate to **Server Configuration→System Parameters**)

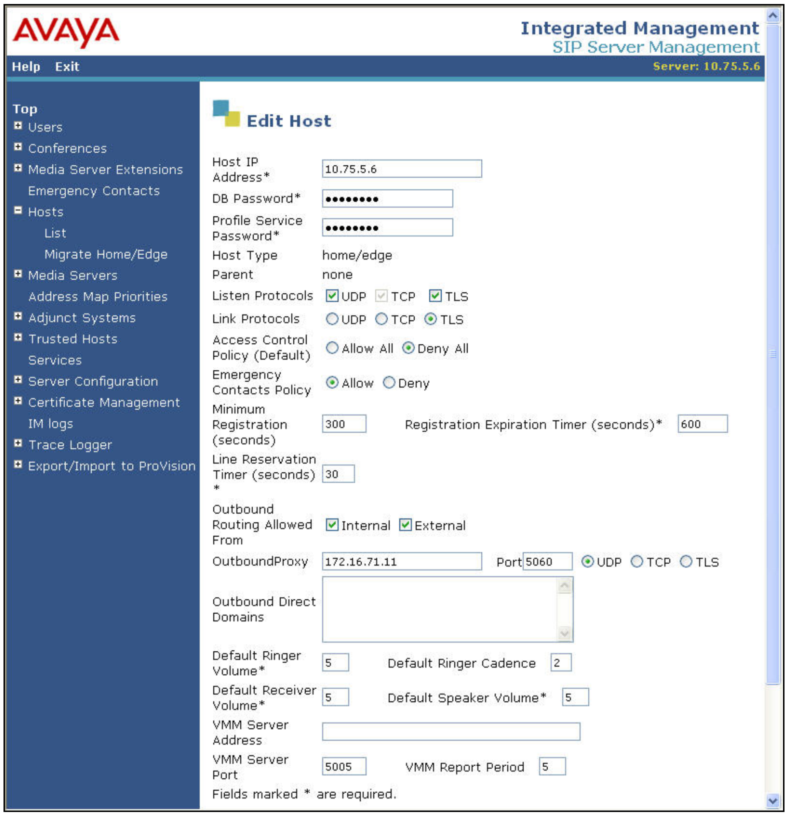
- Host (SES IP address): ***10.75.5.6***
- Host Type: ***home/edge***
  (To view, navigate to **Host→List**; click **Edit**)

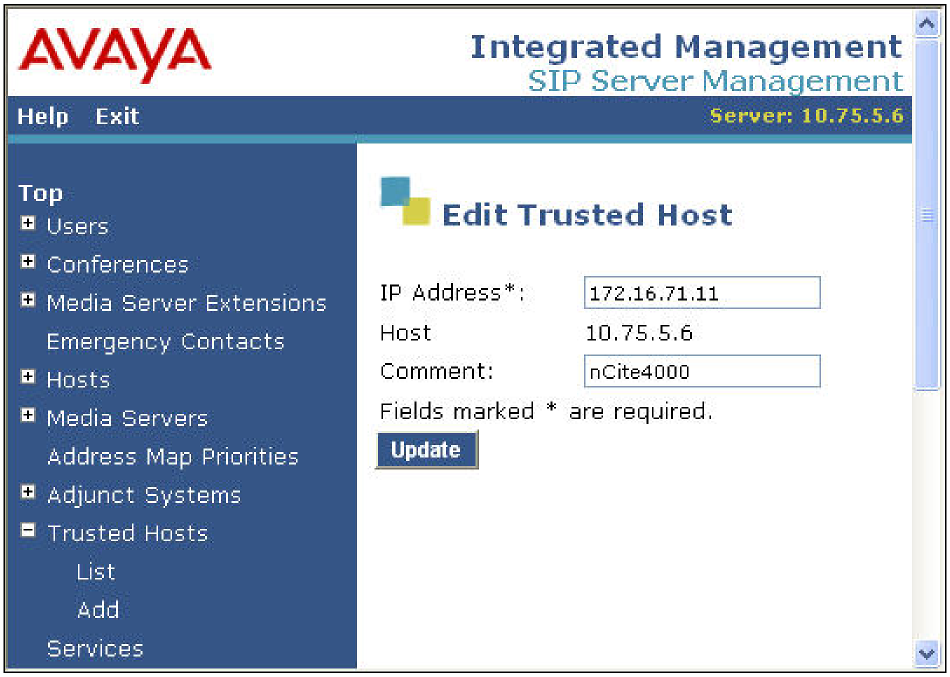
- Media Server (Avaya Communication Manager) Interface Name: ***CMeast***
- SIP Trunk Link Type: ***TLS***
- SIP Trunk IP Address (Avaya S8300B Server IP address): ***10.75.5.2***
  (To view, navigate to **Media Server→List**; click **Edit**)

</td></tr>
</table>

4.2. nCite Specific Configuration

This section describes additional Avaya SES configuration necessary for interoperating with nCite.

Step	Description
1.	**Outbound Proxy** The outbound proxy of Avaya SES was set to the local nCite IP address. When Avaya SES receives a call request (INVITE message) with a destination containing a foreign domain (e.g., ***dev4.com***), Avaya SES will perform a DNS look-up on this domain. If no DNS server is present (as in the compliance test), the DNS look-up will fail and Avaya SES will route the call to the outbound proxy (the local nCite). The local nCite will then be responsible for routing the call to the remote nCite at the other site. To view the proxy settings, navigate to **Hosts→Lists** in the left pane. Select the **Edit** link next to the host name of Avaya SES (not shown). In the **Edit Host** window that appears, the following was configured: • **Outbound Routing Allowed From**: Both ***Internal*** and ***External*** were checked. • **Outbound Proxy**: IP address of the local nCite. **Port** field was set to ***5060***. The **UDP** radio button was selected.  Integrated Management SIP Server Management Help Exit Top Users Conferences Media Server Extensions Emergency Contacts Hosts List Migrate Home/Edge Media Servers Address Map Priorities Adjunct Systems Trusted Hosts Services Server Configuration Certificate Management IM logs Trace Logger Export/Import to ProVision Server: 10.75.5.6 Edit Host Host IP Address*: 10.75.5.6 DB Password*: •••••••• Profile Service Password*: •••••••• Host Type: home/edge Parent: none Listen Protocols: ☑ UDP ☑ TCP ☑ TLS Link Protocols: ○ UDP ○ TCP ● TLS Access Control Policy (Default): ○ Allow All ● Deny All Emergency Contacts Policy: ● Allow ○ Deny Minimum Registration (seconds)*: 300 Registration Expiration Timer (seconds)*: 600 Line Reservation Timer (seconds)*: 30 Outbound Routing Allowed From: ☑ Internal ☑ External OutboundProxy: 172.16.71.11 Port 5060 ● UDP ○ TCP ○ TLS Outbound Direct Domains: Default Ringer Volume*: 5 Default Ringer Cadence: 2 Default Receiver Volume*: 5 Default Speaker Volume*: 5 VMM Server Address: VMM Server Port: 5005 VMM Report Period: 5 Fields marked * are required.

Step	Description
2.	**Trusted Host** The IP address of nCite must be configured as a trusted host in Avaya SES so that SIP messages from nCite are not challenged by Avaya SES. To view the trusted host settings, navigate to **Trusted Hosts → Edit** from the left pane of the Avaya SES window. The **Edit Trusted Host** screen will appear. The parameters are described below: • **IP Address**: The IP address of nCite. • **Comment**: Any descriptive comment.  AVAYA Integrated Management SIP Server Management Help Exit Server: 10.75.5.6 Top Users Conferences Media Server Extensions Emergency Contacts Hosts Media Servers Address Map Priorities Adjunct Systems Trusted Hosts List Add Services Edit Trusted Host Update IP Address*: 172.16.71.11 Host 10.75.5.6 Comment: nCite4000 Fields marked * are required.

Step	Description
3.	**Media Server Address Map**

A media server address map is needed to route calls from the remote site to a non-SIP phone at the local site. This is because neither the caller nor the called party is a registered user on Avaya SES with a media server extension assigned to it. Thus, Avaya SES does not know to route this call to Avaya Communication Manager. Thus to accomplish this task, a media server address map is created.

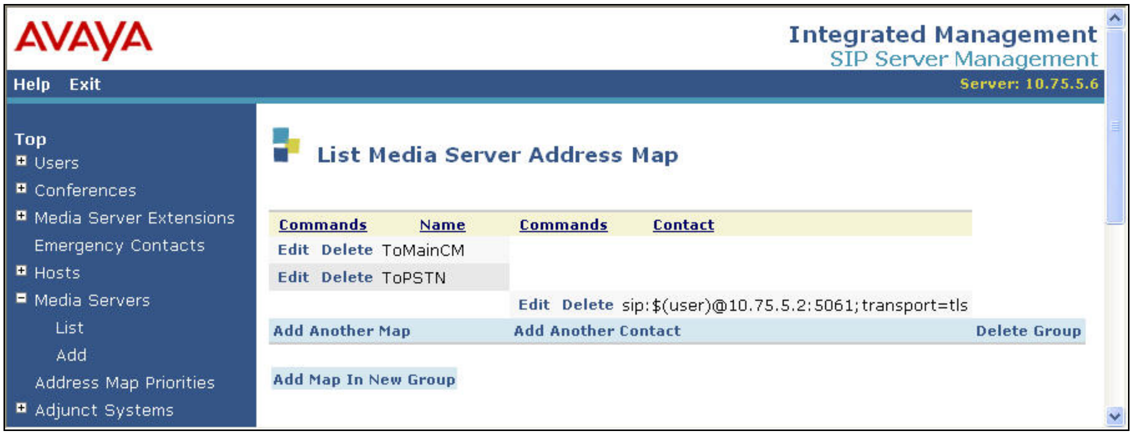
To configure a media server address map:

- Navigate to **Media Server→List** in the left pane. In the **List Media Servers** window that appears (not shown), click on the **Map** link next to the host name of the Avaya S8300 Server running Avaya Communication Manager.
- The **List Media Server Address Map** window will appear as shown below. If no other maps exist, click **Add Map In New Group**. If adding another map for the same media server, click **Add Another Map**. In either case, a window similar to the one shown in **Step 4** will appear, for entering the map data.

The example below shows the media server address map for the main site, named ***ToMainCM***, after it was created. For simplicity, the media server address map was configured to match all calls dialed with a 5 digit number beginning with 3. To view or edit the contents of the map, click the **Edit** link next to the map name (see **Step 4**).

After configuring the map, the initial **Contact** information is populated automatically and directs the calls to the IP address of the Avaya S8300 Server (***10.75.5.2***) using port ***5061*** and ***TLS*** as the transport protocol. The user portion in the original request URI is substituted for ***$(user)***. For the compliance test, the **Contact** field for the media server address map is displayed as:

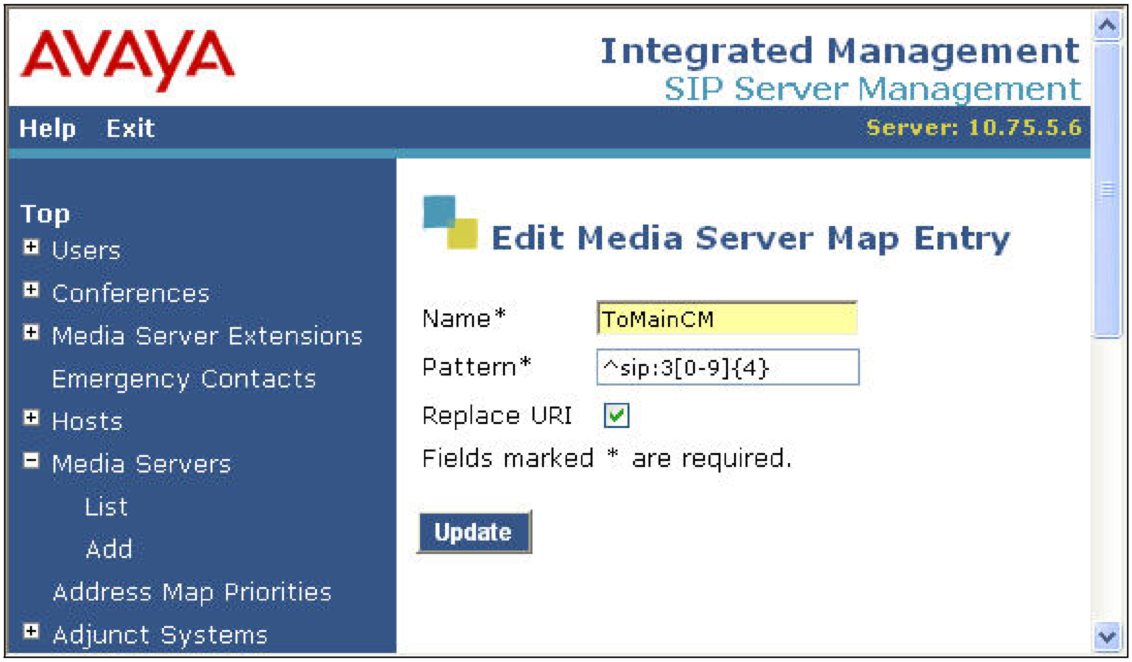
```
sip:$(user)@10.75.5.2:5061;transport=tls
```



List Media Server Address Map

Commands	Name	Commands	Contact
Edit Delete	ToMainCM		
Edit Delete	ToPSTN		
		Edit Delete	sip:$(user)@10.75.5.2:5061;transport=tls
Add Another Map		Add Another Contact	Delete Group

Add Map In New Group

Step	Description
4.	**Media Server Address Map – continued** The content of the media server address map is described below. - **Name**: Contains any descriptive name - **Pattern**: Contains an expression to define the matching criteria for calls to be routed from the remote site to the local Avaya Communication Manager. The example below shows the expression used in the compliance test. This expression will match any URI that begins with ***sip:3*** followed by any digit between ***0-9*** for the next ***4*** digits. Additional information on the syntax used for address map patterns can be found in [5]. - **Replace URI**: Check the box. If any changes are made, click **Update**.  Integrated Management SIP Server Management Help Exit Server: 10.75.5.6 Top Users Conferences Media Server Extensions Emergency Contacts Hosts Media Servers List Add Address Map Priorities Adjunct Systems Update **Edit Media Server Map Entry** Name* ToMainCM Pattern* ^sip:3[0-9]{4} Replace URI ☑ Fields marked * are required.

5. Configure the Avaya SIP Telephones

The SIP telephones at each site will use the local Avaya SES as the call server. The table below shows an example of the SIP telephone networking settings for each site.

	Main Site	**Branch**
Extension	30107	40103
IP Address	10.75.5.161	50.1.1.161
Subnet Mask	255.255.255.0	255.255.255.0
Router	10.75.5.1	50.1.1.254
File Server	10.75.10.100	50.1.1.52
DNS Server	0.0.0.0	0.0.0.0
SIP Domain	business.com	dev4.com
Call Server or SIP Proxy Server	10.75.5.6	50.1.1.50

6. Configure Juniper Networks Netscreen-50

This section describes the Juniper Networks NetScreen-50 configuration at the main site. It must be repeated for the Netscreen-50 at the branch using values appropriate for the branch from **Figure 1**. This section assumes the NetScreen-50 has been installed as described in [7] and starts with the factory defaults. The complete configuration file for the main site is included in **Appendix A**. The configuration for the branch site 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 10.75.1.254/24
ns50-> set interface ethernet1 manage-ip 10.75.1.254
ns50-> set interface ethernet1 route
```

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 46.14.2.2/24`
	`ns50-> set interface ethernet3 route`

4.	**DMZ Zone**
	Statically administer the two Ethernet interfaces in the DMZ zone. It is not necessary to specifically set the interface mode to ***route*** versus ***nat*** as was done in **Step 2** and **3**. These interfaces will always route when bound to the DMZ zone, independent of the interface mode setting.
	`ns50-> set interface ethernet2 zone dmz`
	`ns50-> set interface ethernet2 ip 172.16.71.1/24 zone dmz`
	`ns50-> set interface ethernet4 zone dmz`
	`ns50-> set interface ethernet4 ip 172.16.72.1/24 zone dmz`

5.	**Static Route**
	Define a static route to reach the networks which are not directly attached.
	`ns50-> set vrouter trust-vr route 10.75.10.0/24 interface ethernet1 gateway 10.75.1.1`
	`ns50-> set vrouter trust-vr route 10.75.5.0/24 interface ethernet1 gateway 10.75.1.1`
	`ns50-> set vrouter trust-vr route 46.14.3.0/24 interface ethernet4 gateway 172.16.72.12`
	`ns50-> set vrouter trust-vr route 50.1.1.0/24 interface ethernet3 gateway 46.14.2.1`
	`ns50-> set vrouter trust-vr route 46.16.3.0/24 interface ethernet3 gateway 46.14.2.1`

6.	**Default Route** Define a default static route for any traffic that does not match any of the static routes defined in the previous step. `ns50-> set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 46.14.2.1`
7.	**Clear SIP ALG** Disable the internal SIP Application Layer Gateway provided by the NetScreen-50. `ns50-> unset alg sip enable`
8.	**Save Configuration** Save the configuration. `ns50-> save`

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>9.</td><td>

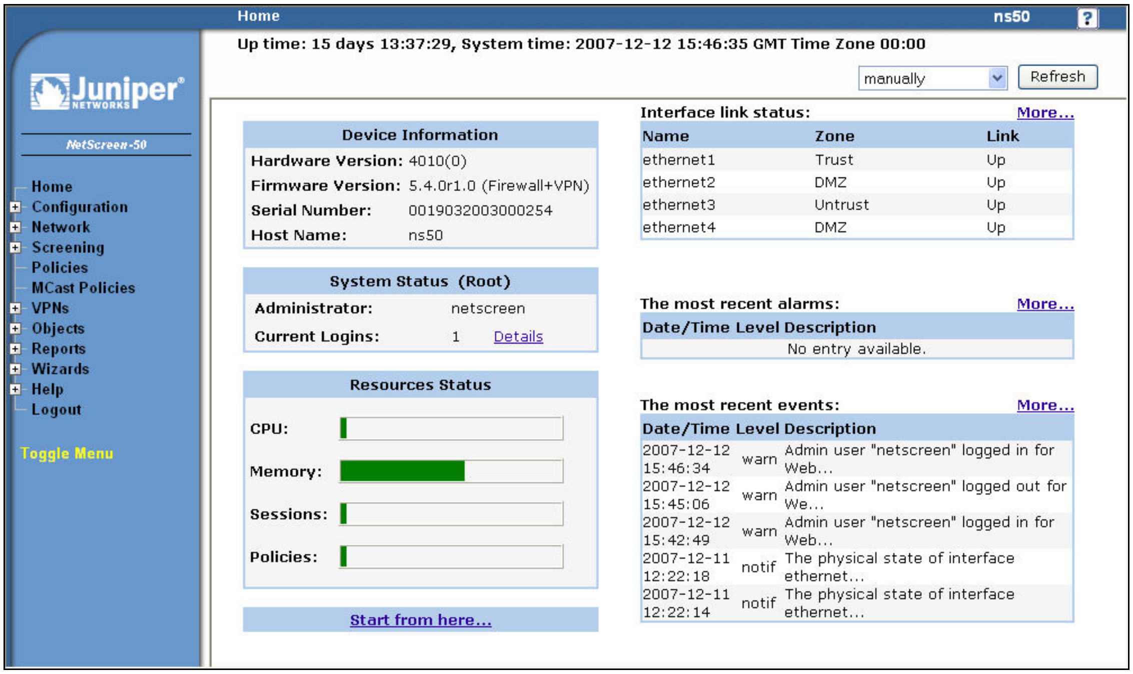
Login to the Web interface.

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.

</td></tr>
<tr><td>10.</td><td>

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.



Up time: 15 days 13:37:29, System time: 2007-12-12 15:46:35 GMT Time Zone 00:00

Device Information

Hardware Version: 4010(0)
Firmware Version: 5.4.0r1.0 (Firewall+VPN)
Serial Number: 0019032003000254
Host Name: ns50

System Status (Root)

Administrator: netscreen
Current Logins: 1 Details

Resources Status

CPU:
Memory:
Sessions:
Policies:

Interface link status:

<table>
<tr><th>Name</th><th>Zone</th><th>Link</th></tr>
<tr><td>ethernet1</td><td>Trust</td><td>Up</td></tr>
<tr><td>ethernet2</td><td>DMZ</td><td>Up</td></tr>
<tr><td>ethernet3</td><td>Untrust</td><td>Up</td></tr>
<tr><td>ethernet4</td><td>DMZ</td><td>Up</td></tr>
</table>

The most recent alarms:

<table>
<tr><th>Date/Time</th><th>Level</th><th>Description</th></tr>
<tr><td colspan="3">No entry available.</td></tr>
</table>

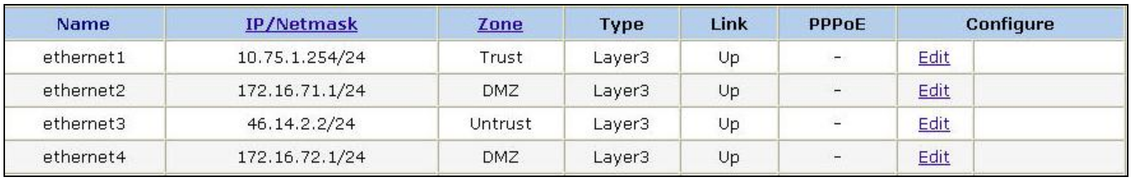
The most recent events:

<table>
<tr><th>Date/Time</th><th>Level</th><th>Description</th></tr>
<tr><td>2007-12-12 15:46:34</td><td>warn</td><td>Admin user "netscreen" logged in for Web...</td></tr>
<tr><td>2007-12-12 15:45:06</td><td>warn</td><td>Admin user "netscreen" logged out for We...</td></tr>
<tr><td>2007-12-12 15:42:49</td><td>warn</td><td>Admin user "netscreen" logged in for Web...</td></tr>
<tr><td>2007-12-11 12:22:18</td><td>notif</td><td>The physical state of interface ethernet...</td></tr>
<tr><td>2007-12-11 12:22:14</td><td>notif</td><td>The physical state of interface ethernet...</td></tr>
</table>

</td></tr>
<tr><td>11.</td><td>

Interfaces

To view the interfaces configured in **Steps 2 - 4**, navigate to **Network→Interfaces** from the left pane.



<table>
<tr><th>Name</th><th>IP/Netmask</th><th>Zone</th><th>Type</th><th>Link</th><th>PPPoE</th><th>Configure</th></tr>
<tr><td>ethernet1</td><td>10.75.1.254/24</td><td>Trust</td><td>Layer3</td><td>Up</td><td>-</td><td>Edit</td></tr>
<tr><td>ethernet2</td><td>172.16.71.1/24</td><td>DMZ</td><td>Layer3</td><td>Up</td><td>-</td><td>Edit</td></tr>
<tr><td>ethernet3</td><td>46.14.2.2/24</td><td>Untrust</td><td>Layer3</td><td>Up</td><td>-</td><td>Edit</td></tr>
<tr><td>ethernet4</td><td>172.16.72.1/24</td><td>DMZ</td><td>Layer3</td><td>Up</td><td>-</td><td>Edit</td></tr>
</table>

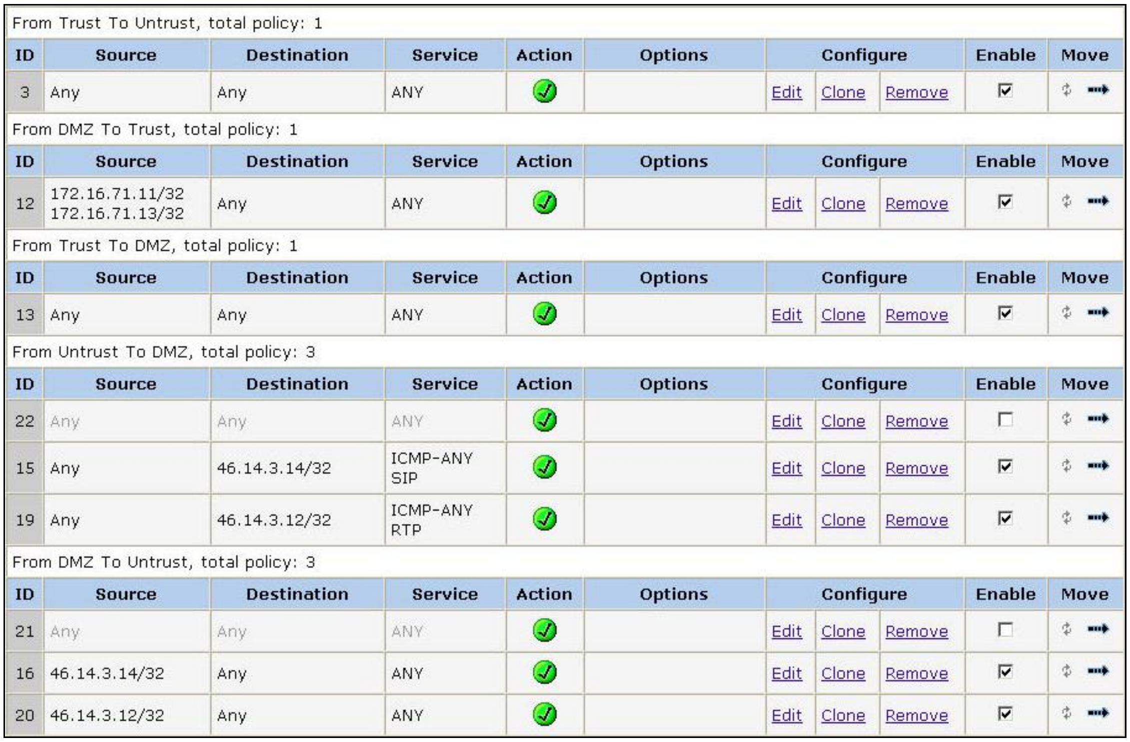
</td></tr>
</table>

Step	Description
12.	**Policies** Policies define the traffic that is allowed to flow through the firewall. To configure a policy, navigate to **Policies** in the left pane. Each policy is created by selecting a **From** zone and a **To** zone from the pull-downs at the top of the **Policies** page and clicking the **New** button. A new page is opened (not shown) where the policy information can be entered and submitted. **Steps 2 – 4** have previously defined the following: • Trust zone: Connects to the private enterprise LAN. • DMZ zone: Connects to nCite. • Untrust zone: Connects to the public untrusted IP network. These zones are used to define the policies used in the compliance test as shown in the next step.

Step	Description
13.	**Policies – continued**

The policies used in the compliance test are summarized as follows:

- Policy 3 and 13: Traffic is unrestricted in the direction of Trust to Untrust, and Trust to DMZ.
- Policy 12: Any traffic from either nCite private address (signaling or media) is allowed from the DMZ to the Trust zone.
- Policy 15: SIP and ICMP traffic (for pings) to the nCite public IP address used for signaling is allowed from the Untrust to DMZ zones. The ICMP traffic is not required for the compliance test.
- Policy 19: RTP and ICMP traffic (for pings) to the nCite public IP address used for media is allowed from the Untrust to DMZ zones. The ICMP traffic is not required for the compliance test.
- Policy 16: Any traffic from the nCite public IP address used for signaling is allowed from the DMZ to Untrust zone.
- Policy 20: Any traffic from the nCite public IP address used for media is allowed from the DMZ to Untrust zone.



From Trust To Untrust, total policy: 1

ID	Source	Destination	Service	Action	Options	Configure	Enable	Move
3	Any	Any	ANY	✓		Edit Clone Remove	☑	

From DMZ To Trust, total policy: 1

ID	Source	Destination	Service	Action	Options	Configure	Enable	Move
12	172.16.71.11/32 172.16.71.13/32	Any	ANY	✓		Edit Clone Remove	☑	

From Trust To DMZ, total policy: 1

ID	Source	Destination	Service	Action	Options	Configure	Enable	Move
13	Any	Any	ANY	✓		Edit Clone Remove	☑	

From Untrust To DMZ, total policy: 3

ID	Source	Destination	Service	Action	Options	Configure	Enable	Move
22	Any	Any	ANY	✓		Edit Clone Remove	☐	
15	Any	46.14.3.14/32	ICMP-ANY SIP	✓		Edit Clone Remove	☑	
19	Any	46.14.3.12/32	ICMP-ANY RTP	✓		Edit Clone Remove	☑	

From DMZ To Untrust, total policy: 3

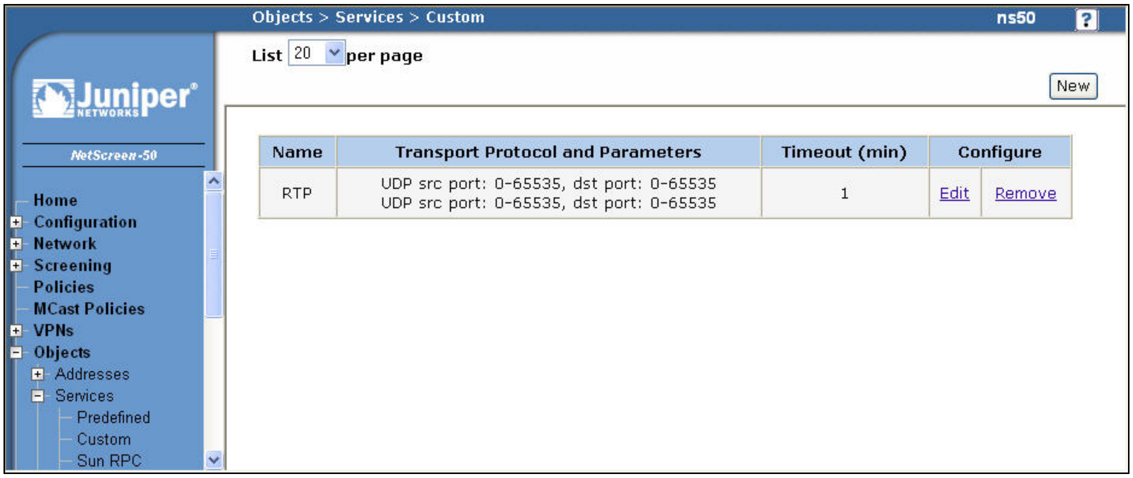
ID	Source	Destination	Service	Action	Options	Configure	Enable	Move
21	Any	Any	ANY	✓		Edit Clone Remove	☐	
16	46.14.3.14/32	Any	ANY	✓		Edit Clone Remove	☑	
20	46.14.3.12/32	Any	ANY	✓		Edit Clone Remove	☑	

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>14.</td><td>

Services

The services used in the policies in **Step 12** were standard services defined by the firewall with the exception of the service called RTP. RTP does not use a set of well known ports, so a custom service was created to define the ports and transport protocol used by the service RTP. To create a custom service, navigate to **Objects→Services→Custom** from the left pane. Click on the **New** button. A new page is opened (not shown) where the policy information can be entered and submitted.

The table below shows the custom service named RTP used for the compliance test. For simplicity, the source port and the destination port was defined as any valid UDP port. The range of ports used can be further restricted as long as the range of ports is compatible to the range used by nCite and Avaya SES. Even though the range of ports used for the compliance test was large, the firewall policy only allows this traffic to a single host (nCite).



<table>
<tr><th>Name</th><th>Transport Protocol and Parameters</th><th>Timeout (min)</th><th colspan="2">Configure</th></tr>
<tr><td>RTP</td><td>UDP src port: 0-65535, dst port: 0-65535
UDP src port: 0-65535, dst port: 0-65535</td><td>1</td><td>Edit</td><td>Remove</td></tr>
</table>

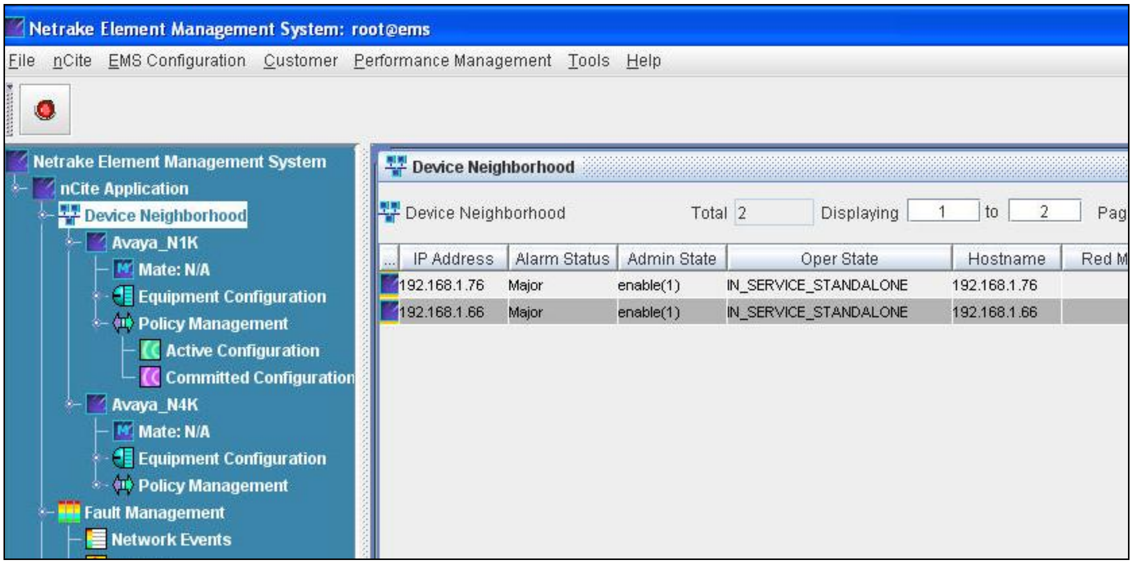
</td></tr>
</table>

7. Configure AudioCodes nCite

This section covers the configuration of the nCite at both sites. It is assumed that the nCite software has already been installed. For additional information on these installation tasks, refer to [8].

In each step, the values are summarized for both sites. However, only a single screenshot example from the main site configuration is shown in each step. All configuration for both nCite SBCs is done via the nCite Element Management System (EMS).

A conceptual view of the configuration of the nCite internal components is shown in **Appendix C**.

Step	Description
1.	**Login to the EMS** Enter the IP address of the EMS with port 9090 into the URL of a web browser (e.g., **http://192.168.1.86:9090**). Log in with appropriate credentials. An opening page will appear showing the devices available in the **Device Neighborhood**. The example below shows two devices; one named ***Avaya_N1K*** and the other named ***Avaya_N4K***. ***Avaya_N1K*** represents the nCite at the branch site and ***Avaya_N4K*** represents the nCite at the main site. The configuration of these devices is stored in the policy of each device. To list the available policies, navigate to **nCite→Policy Configuration** from the menu bar at the top of the page. To view or edit a policy, right-click the policy for the device of interest in the list and select **Modify** (not shown). A policy configuration screen will appear (see **Step 2**). The remaining steps are performed from within this policy configuration window. 

Total 2 Displaying 1 to 2 Pag

...	IP Address	Alarm Status	Admin State	Oper State	Hostname	Red M
	192.168.1.76	Major	enable(1)	IN_SERVICE_STANDALONE	192.168.1.76	
	192.168.1.66	Major	enable(1)	IN_SERVICE_STANDALONE	192.168.1.66	

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>2.</td><td>

Virtual Routing Domains (VRD)

Each device was configured with two virtual routing domains. One domain is for the outside/public side of the device and the other is for the inside/private side of the device. The names of both routing domains for each site are summarized as follows:

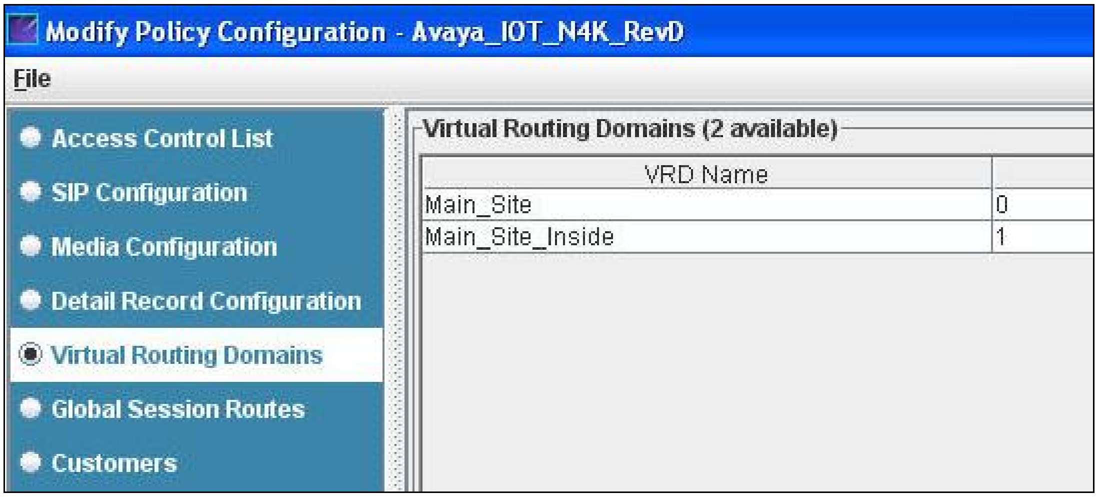
Main site (Domain # – Domain Name):

- VRD 0 (outside) – Main_Site
- VRD 1 (inside) – Main_Site_Inside

Branch site (Domain # – Domain Name):

- VRD 0 (outside) – Branch_Site
- VRD 1 (inside) – Branch_Site_Inside

The example below shows the two domains for the main site. To access the configuration contained within a VRD (**Steps 3 – 12**), select the VRD name in the right pane and click the **View** or **Modify** button at the bottom of the page (not shown).



Virtual Routing Domains (2 available)

<table>
<tr><th>VRD Name</th><th></th></tr>
<tr><td>Main_Site</td><td>0</td></tr>
<tr><td>Main_Site_Inside</td><td>1</td></tr>
</table>

</td></tr>
</table>

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>3.</td><td>

Session Target (ST)

Within each VRD, a session target was created. A session target defines an external SIP destination known to that routing domain. The names of each of the session targets for both sites are summarized as follows:

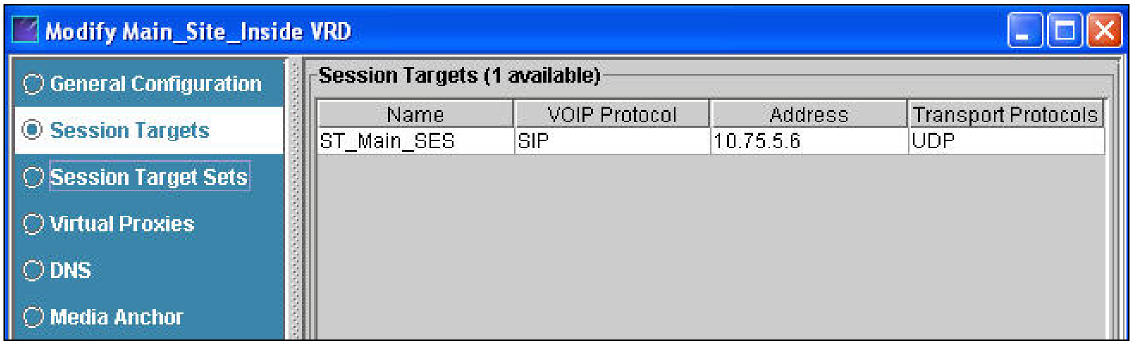
Main site (Domain – Session Target):

- Main_Site (VRD) – ST_Branch_Site
- Main_Site_Inside (VRD) – ST_Main_SES

Branch site (Domain – Session Target):

- Branch_Site (VRD) – ST_Main_Site
- Branch_Site_Inside (VRD) – ST_Branch_SES

The example below shows the session target for the private routing domain (named ***Main_Site_Inside***) at the main site. To access the session target configuration (**Steps 4 – 5**), select the session target name in the right pane and click the **View** or **Modify** button at the bottom of the page (not shown).



Session Targets (1 available)

Name	VOIP Protocol	Address	Transport Protocols
ST_Main_SES	SIP	10.75.5.6	UDP

</td></tr>
</table>

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>4.</td><td>

Session Target – Continued

Each session target was configured using the same parameters as the example below with the exception of the name and IP address. The IP addresses of the session targets for both sites are summarized as follows:

<table>
<tr><td>

Main site (Session Target – IP addr):

- ST_Branch_Site – 46.16.3.14 (Branch nCite outside signaling IP)
- ST_Main_SES – 10.75.5.6 (Main SES)

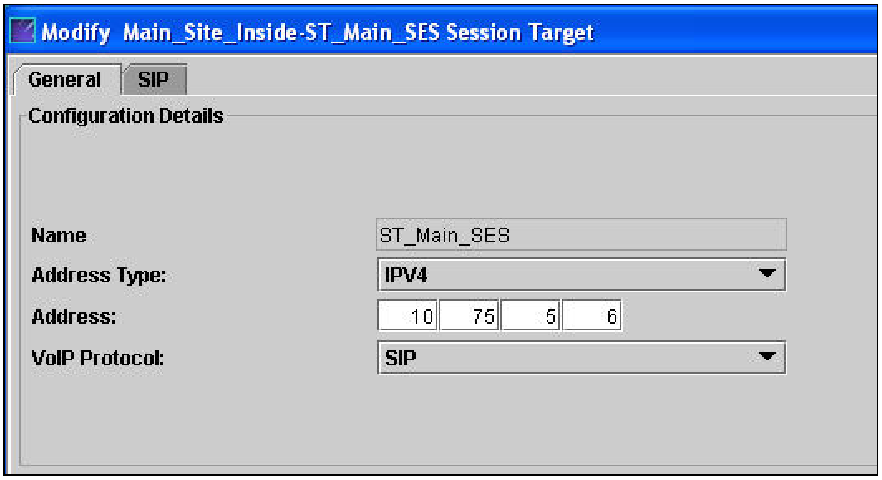
</td><td>

Branch site (Session Target – IP addr):

- ST_Main_Site – 46.14.3.14 (Main nCite outside signaling IP)
- ST_Branch_SES – 50.1.1.50 (Branch SES)

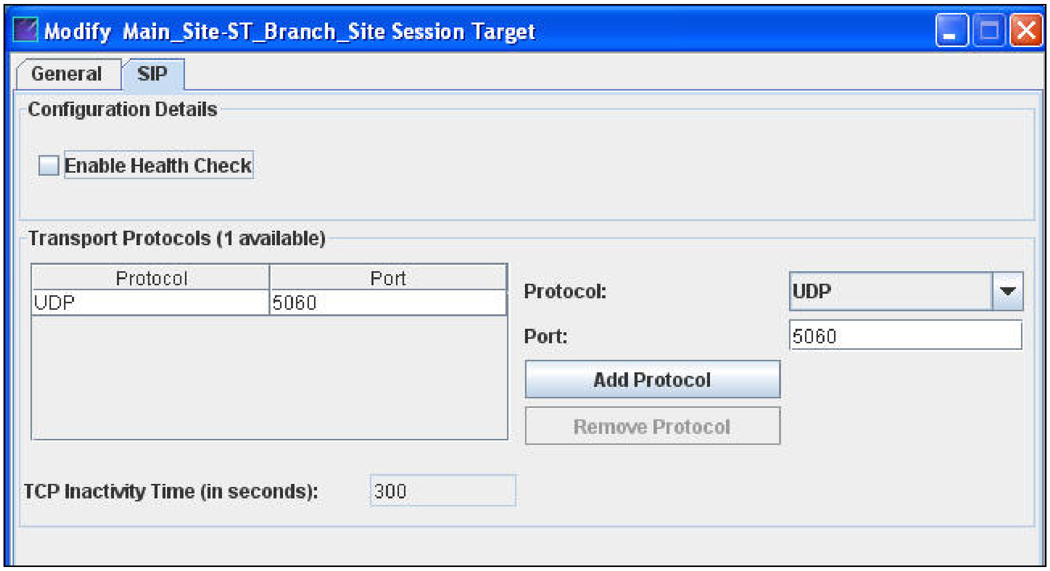
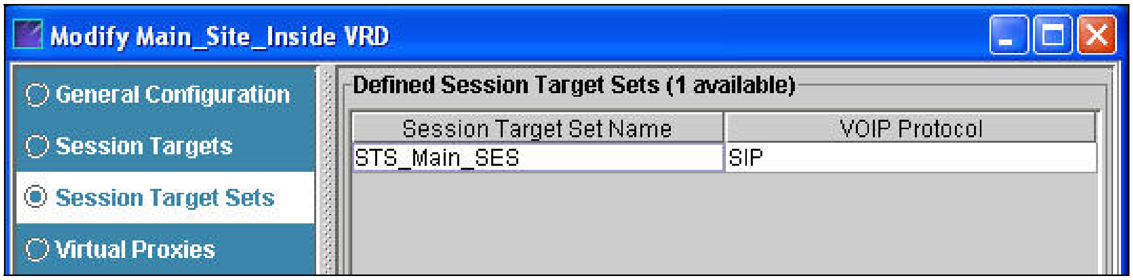
</td></tr>
</table>

The example below shows the **General** parameters of the session target named ***ST_Main_SES*** at the main site.



Name: ST_Main_SES
Address Type: IPV4
Address: 10 75 5 6
VoIP Protocol: SIP

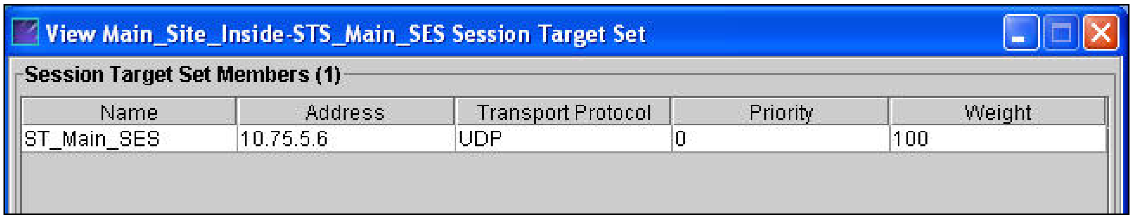
</td></tr>
</table>

Step	Description
5.	**Session Target – Continued** On the **SIP** tab, the **Protocol** field was set to ***UDP*** and the **Port** field was set to ***5060***. This was set the same for all session targets. Modify Main_Site-ST_Branch_Site Session Target General SIP Configuration Details ☐ Enable Health Check Transport Protocols (1 available) Protocol | Port UDP | 5060 Protocol: UDP Port: 5060 Add Protocol Remove Protocol TCP Inactivity Time (in seconds): 300
6.	**Session Target Set (STS)** Session Targets may be grouped into sets for redundancy or load sharing. In the compliance test, each session target set included a single session target. The session target in each STS at both sites are summarized as follows: Main site (STS – Session Target): • STS_Branch_Site - ST_Branch_Site • STS_Main_SES - ST_Main_SES Branch site (STS – Session Target): • STS_Main_Site - ST_Main_Site • STS_Branch_SES - ST_Branch_SES The example below shows the STS which contains the session target pointing to the SES at the main site. To access the STS configuration (**Step 7**), select the STS name in the right pane and click the **View** or **Modify** button at the bottom of the page (not shown). Modify Main_Site_Inside VRD ○ General Configuration ○ Session Targets ● Session Target Sets ○ Virtual Proxies Defined Session Target Sets (1 available) Session Target Set Name | VOIP Protocol STS_Main_SES | SIP

Step | **Description**

7. **Session Target Set –Continued**

The STS configuration shows the list of session targets in the set. The example below shows the single session target in the STS named ***STS_Main_SES***. This session target was defined in **Steps 3 - 5**.



View Main_Site_Inside-STS_Main_SES Session Target Set

Session Target Set Members (1)

Name	Address	Transport Protocol	Priority	Weight
ST_Main_SES	10.75.5.6	UDP	0	100

8. **Virtual Proxies (VP)**

A virtual proxy was created for each routing domain. Each virtual proxy defines an internal SIP proxy for the routing domain. The names of each of the virtual proxies for both sites are summarized as follows:

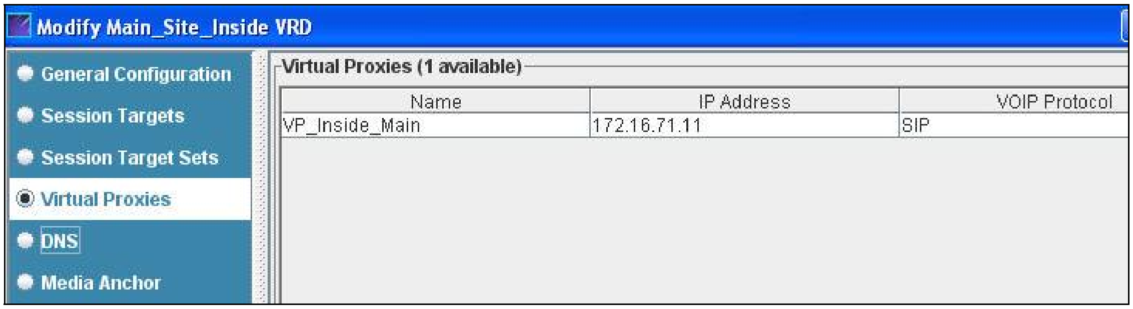
Main site (Domain – Virtual Proxy):

- Main_Site (VRD) – VP_Main_Site
- Main_Site_Inside (VRD) – VP_Inside_Main

Branch site (Domain – Virtual Proxy):

- Branch_Site (VRD) – VP_Branch_Site
- Branch_Site_Inside (VRD) – VP_Inside_Branch

The example below shows the virtual proxy for the private routing domain at the main site.



Virtual Proxies (1 available)

Name	IP Address	VOIP Protocol
VP_Inside_Main	172.16.71.11	SIP

Step | **Description**

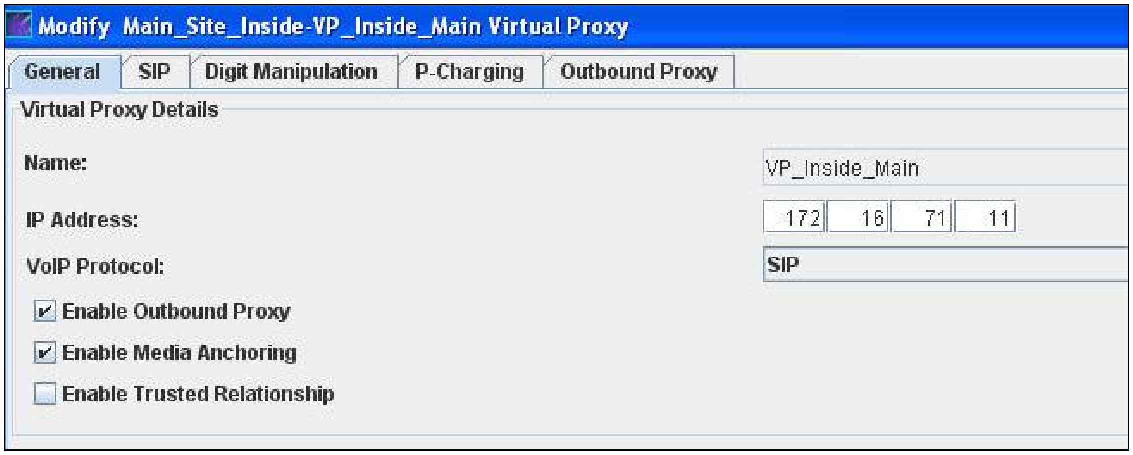
9. **Virtual Proxies – Continued**

Each virtual proxy was configured using the same parameters in the example below with the exception of the name and IP address. The IP addresses of each of the virtual proxies for both sites are summarized as follows:

Main site (Virtual Proxy – IP addr):
- VP_Main_Site – 46.14.3.14 (Main nCite outside signaling IP)
- VP_Inside_Main – 172.16.71.11 (Main nCite inside signaling IP)

Branch site (Virtual Proxy – IP addr):
- VP_Branch_Site – 46.16.3.14 (Branch nCite outside signaling IP)
- VP_Inside_Branch – 172.1.1.11 (Branch nCite inside signaling IP)

The example below shows the **General** tab of the virtual proxy named ***VP_Inside_Main*** at the main site.



Name: VP_Inside_Main

IP Address: 172 16 71 11

VoIP Protocol: SIP

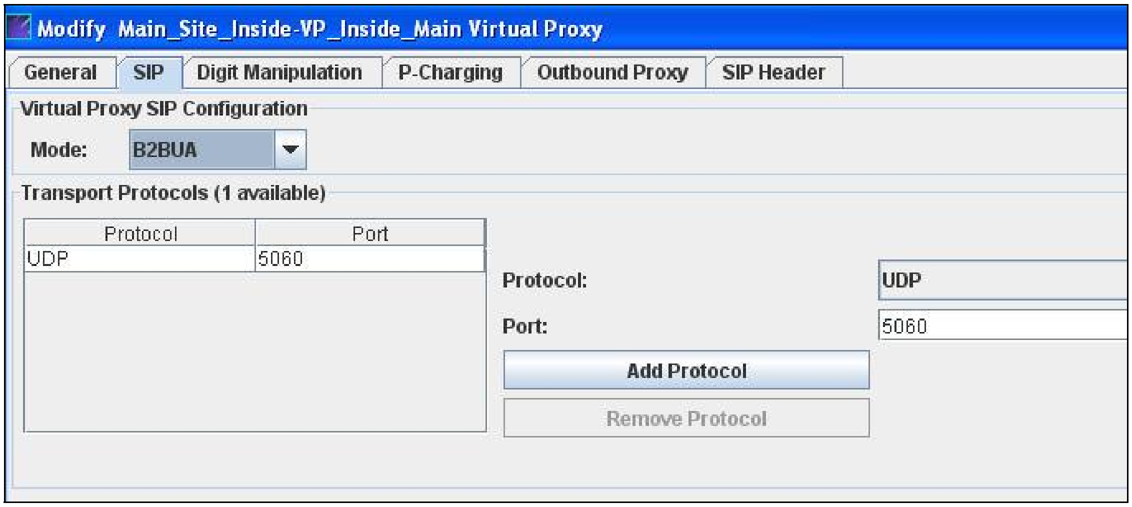
☑ Enable Outbound Proxy

☑ Enable Media Anchoring

☐ Enable Trusted Relationship

10. **Virtual Proxies – Continued**

On the **SIP** tab, the **Mode** field was set to ***B2BUA***, the **Protocol** field was set to ***UDP*** and the **Port** field was set to ***5060***. The same settings were used for all virtual proxies.

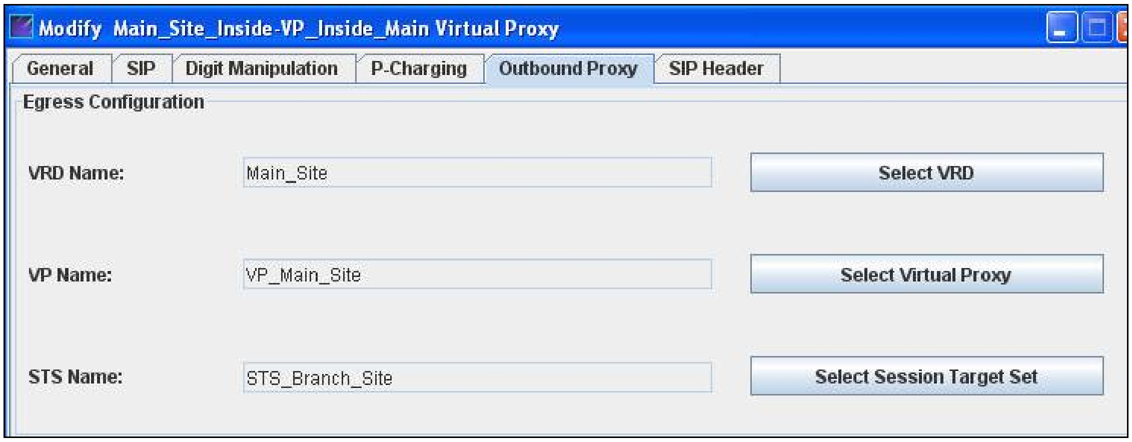

Modify Main_Site_Inside-VP_Inside_Main Virtual Proxy
General
SIP
Digit Manipulation
P-Charging
Outbound Proxy
SIP Header
Virtual Proxy SIP Configuration
Transport Protocols (1 available)
Add Protocol
Remove Protocol

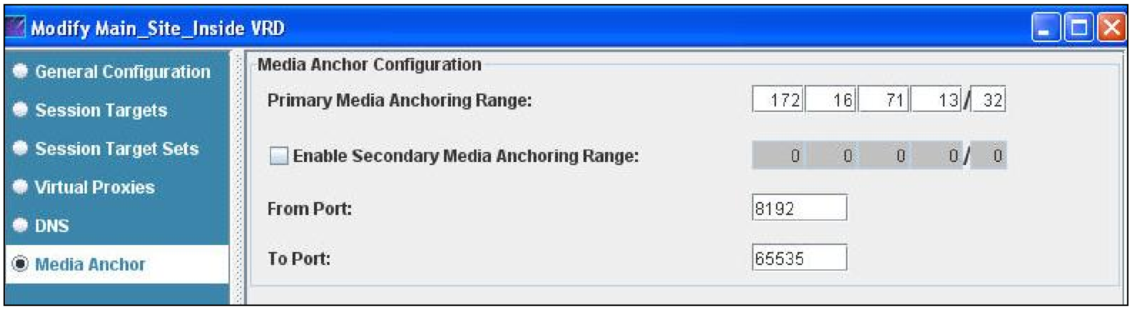
Mode: B2BUA

Protocol	Port
UDP	5060

Protocol: UDP

Port: 5060

Step	Description
11.	**Virtual Proxies – Continued** Each virtual proxy is configured with an outbound proxy that defines the next hop for outbound SIP traffic. On the **Outbound Proxy** tab, the **VRD Name**, **VP Name** and **STS Name** fields all refer to the parameters of the outbound proxy. In the case of the compliance test, the outbound proxy was the virtual proxy in the other routing domain on the same SBC. The outbound proxy fields for each of the virtual proxies at both sites are summarized as follows: Main site (Virtual Proxy): • VP_Main_Site VRD Name: Main_Site_Inside VP Name: VP_Inside_Main STS Name: STS_Main_SES • VP_Inside_Main VRD Name: Main_Site VP Name: VP_Main_Site STS Name: STS_Branch_Site Branch site (Virtual Proxy): • VP_Branch_Site VRD Name: Branch_Site_Inside VP Name: VP_Inside_Branch STS Name: STS_Branch_SES • VP_Inside_Branch VRD Name: Branch_Site VP Name: VP_Branch_Site STS Name: STS_Main_Site The example below shows the **Outbound Proxy** tab of the virtual proxy named ***VP_Inside_Main*** at the main site.  Modify Main_Site_Inside-VP_Inside_Main Virtual Proxy General SIP Digit Manipulation P-Charging Outbound Proxy SIP Header Egress Configuration Select VRD Select Virtual Proxy Select Session Target Set VRD Name: Main_Site VP Name: VP_Main_Site STS Name: STS_Branch_Site

Step	Description
12.	**Media Anchor** A media anchor was created for each routing domain. Each media anchor defines the IP address the routing domain uses for processing RTP media streams. Each media anchor was configured with the same parameters as the example below with the exception of the IP address. The IP addresses of each of the media anchors for both sites are summarized as follows: Main site (Domain – Media Anchor): • Main_Site (VRD) – 46.14.3.12 • Main_Site_Inside (VRD) – 172.16.71.13 Branch site (Domain – Media Anchor): • Branch_Site (VRD) – 46.16.3.12 • Branch_Site_Inside (VRD) – 172.1.1.13 The example below shows the media anchor for the private routing domain at the main site.  Modify Main_Site_Inside VRD General Configuration Session Targets Session Target Sets Virtual Proxies DNS Media Anchor Media Anchor Configuration Primary Media Anchoring Range: 172 16 71 13 / 32 ☐ Enable Secondary Media Anchoring Range: 0 0 0 0 / 0 From Port: 8192 To Port: 65535

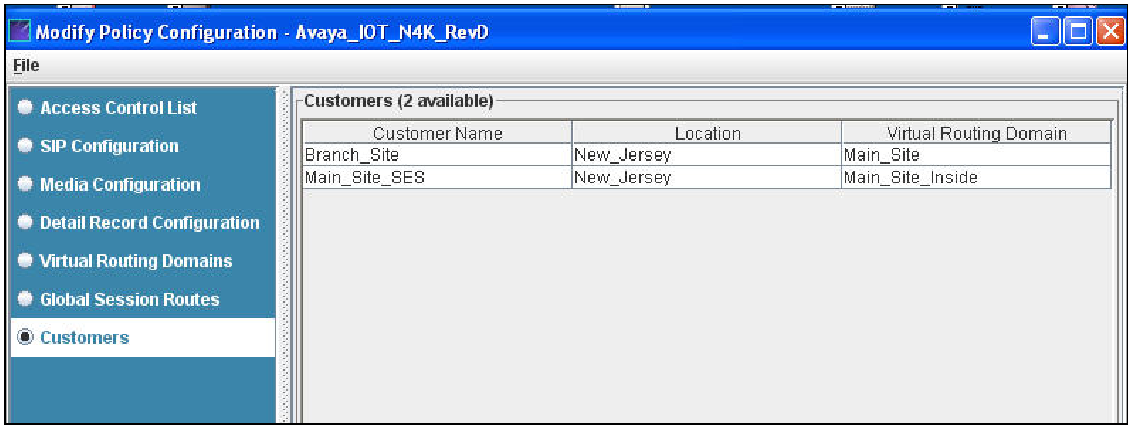
Step	Description
13.	**Customers**

Two customers were created for each nCite. A customer defines what IP addresses are allowed to access the SBC and any characteristics of those customers that may impact the operation of the SBC. The customer is also associated with a particular VRD. The names of the customers for both VRDs at each site are summarized as follows:

Main site (Domain – Customer):
- Main_Site (VRD) – Branch_Site
- Main_Site_Inside (VRD) – Main_Site_SES

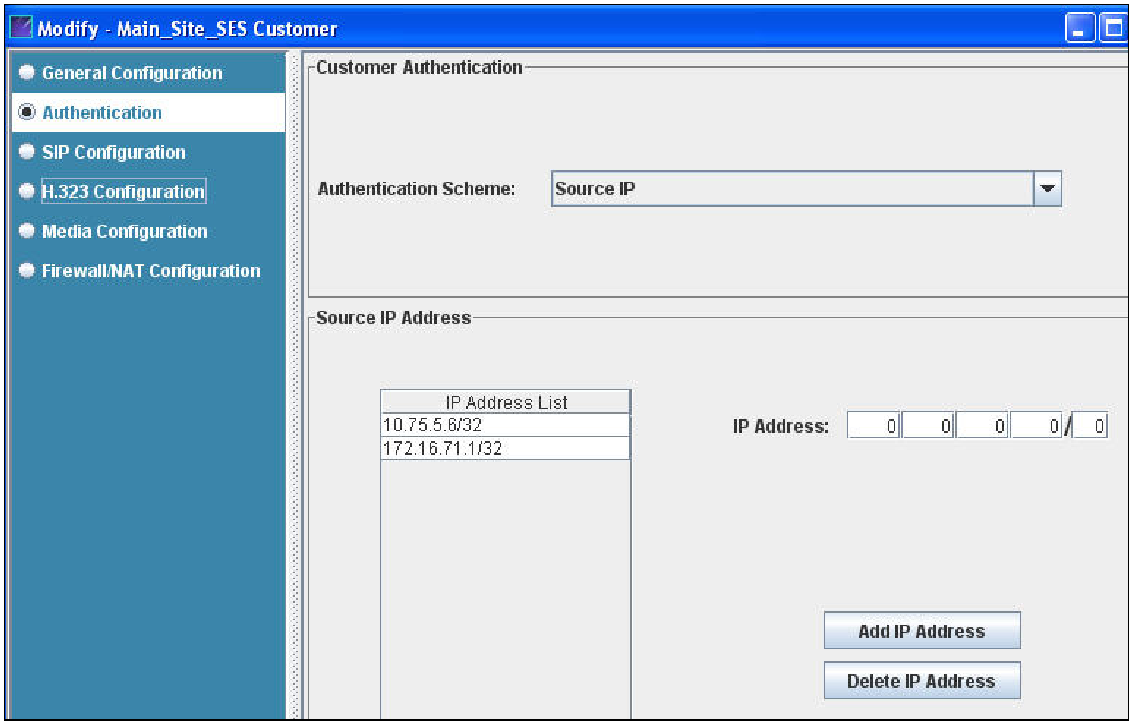
Branch site (Domain – Customer):
- Branch_Site (VRD) – Main_Site
- Branch_Site_Inside (VRD) – Branch_Site_SES

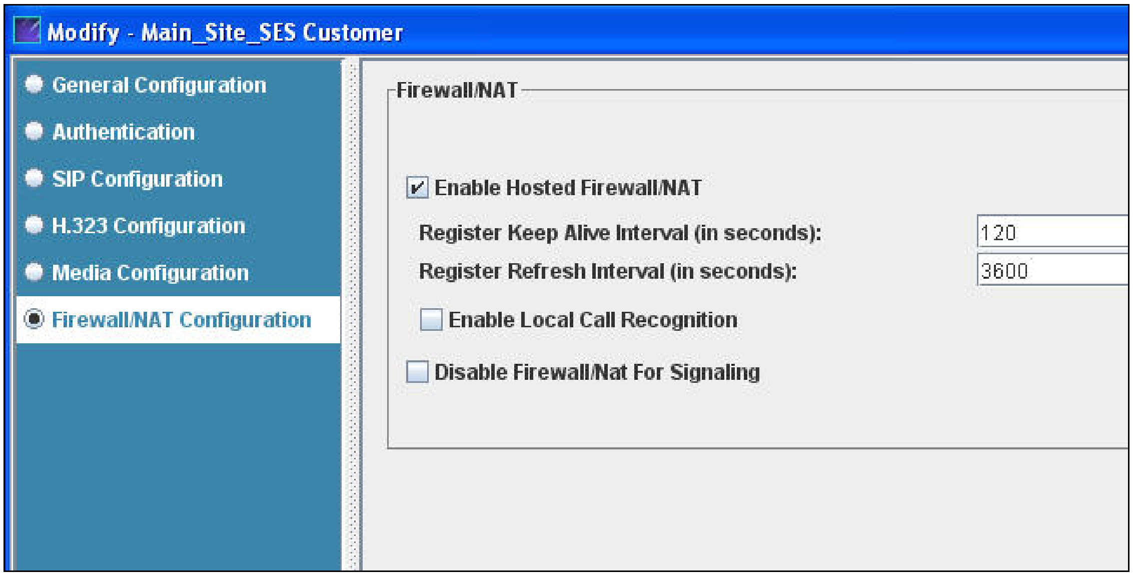
The example below shows the customers for the private routing domain at the main site. To access the customer configuration (**Steps 14 – 15**), select the customer name in the right pane and click the **View** or **Modify** button at the bottom of the page (not shown).



Customers (2 available)

Customer Name	Location	Virtual Routing Domain
Branch_Site	New_Jersey	Main_Site
Main_Site_SES	New_Jersey	Main_Site_Inside

Step	Description
14.	**Customers – Continued** The customers were configured the same as the example below with the exception of the IP addresses for each customer. The list of IP addresses include both the session target in that routing domain (see **Step 4**) as well as the IP address of the Netscreen-50 firewall connected to that routing domain (see **Figure 1**). The IP addresses of each of the customers at both sites are summarized as follows: Main site (Customer – Allowable IPs): • Branch_Site – 46.16.3.14, 172.1.2.1 • Main_Site_SES – 10.75.5.6, 172.16.71.1 Branch site (Customer – Allowable IPs): • Main_Site – 46.14.3.14, 172.16.72.1 • Branch_Site_SES – 50.1.1.50, 172.1.1.1 The example below shows IP addresses for the customer ***Main_Site_SES*** at the main site.  Modify - Main_Site_SES Customer Customer Authentication Authentication Scheme: Source IP Source IP Address IP Address List 10.75.5.6/32 172.16.71.1/32 IP Address: 0 0 0 0 / 0 General Configuration Authentication SIP Configuration H.323 Configuration Media Configuration Firewall/NAT Configuration Add IP Address Delete IP Address

Step	Description
15.	**Customers – Continued** Each customer was configured with NAT traversal enabled by checking the checkbox next to **Enable Hosted Firewall/NAT**. This feature is typically enabled at customer installations because it may not be known if a NAT device is located somewhere in the network. If NAT traversal is not required, enabling this feature has no adverse affect on SBC operation. In the case of the compliance test, the feature was enabled but no NAT traversal was performed in the network.  Modify - Main_Site_SES Customer General Configuration Authentication SIP Configuration H.323 Configuration Media Configuration Firewall/NAT Configuration Firewall/NAT ☑ Enable Hosted Firewall/NAT Register Keep Alive Interval (in seconds): 120 Register Refresh Interval (in seconds): 3600 ☐ Enable Local Call Recognition ☐ Disable Firewall/Nat For Signaling

8. Interoperability Compliance Testing

This section describes the compliance testing used to verify the interoperability of AudioCodes nCite with Avaya SIP Enablement Services and Avaya Communication Manager using SIP trunking. This section covers the general test approach and the test results.

8.1. General Test Approach

The general test approach was to make calls between the two sites using various codec settings and exercising common PBX features.

8.2. Test Results

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

- Successful registrations of endpoints at the main and branch sites.
- Calls from both SIP and non-SIP endpoints between sites.
- G.711u and G.729AB codec support
- Proper recognition of DTMF transmissions by navigating voicemail menus.
- Proper operation of voicemail with message waiting indicators (MWI).
- PBX features including Hold, Transfer, Call Waiting, Call Forwarding and Conference.

- Extended telephony features using Avaya Communication Manager Feature Name Extensions (FNE) such as Conference On Answer, Call Park, Call Pickup, Automatic Redial and Send All Calls. For more information on FNEs, please refer to [4].
- Proper system recovery after an nCite restart and loss of IP connection.

The following observations were made during the compliance test:

- For interoperability, direct IP to IP media (also known as media shuffling) must be disabled on each SIP trunk signaling group in Avaya Communication Manager (see **Section 3.1, Step 3** and **Section 3.2, Step 1**). This will result in VoIP resources being used in the Avaya Media Gateway for the duration of each SIP call.

9. Verification Steps

The following steps may be used to verify the configuration:

- From the Avaya Communication Manager SAT, use the **status signaling-group** command to verify that the SIP signaling group is in-service.
- From the Avaya Communication Manager SAT, use the **status trunk-group** command to verify that the SIP trunk group is in-service.
- From the Avaya SES web administration interface, verify that all endpoints are registered with the local Avaya SES. To view, navigate to **Users→Registered Users**.
- Verify that calls can be placed from both SIP and non-SIP endpoints between sites.

10. Support

For technical support on nCite, contact AudioCodes via the support link at www.audiocodes.com.

11. Conclusion

AudioCodes nCite passed compliance testing with the observations listed in **Section 8.2**. These Application Notes describe the procedures required to configure AudioCodes nCite to interoperate with Avaya SIP Enablement Services and Avaya Communication Manager to support SIP trunking between enterprise locations as shown in **Figure 1**.

12. Additional References

[1] *Feature Description and Implementation For Avaya Communication Manager*, Doc # 555-245-205, Issue 5.0, February 2007.
[2] *Administrator Guide for Avaya Communication Manager*, Doc # 03-300509, Issue 3.1, February 2007.
[3] *SIP support in Avaya Communication Manager Running on the Avaya S3800, S8400, S8500 Series and S8700 Series Media Server*, Doc # 555-245-206, Issue 6.1, March 2007.
[4] *Avaya Extension to Cellular and Off-PBX Station (OPS) Installation and Administration Guide Release 3.0*, version 6.0, Doc # 210-100-500, Issue 9, June 2005.
[5] *Installing and Administering SIP Enablement Services*, Doc# 03-600768, Issue 4, May 2007.
[6] *Avaya IA 770 INTUITY AUDIX Messaging Application*, Doc # 11-300532, May 2005.
[7] *Concepts and Examples ScreenOS Reference Guide*, Release 5.4.0, Rev.B.
[8] *AudioCodes nCite Installation Guide (230-5210-31).*
[9] *AudioCodes nCite Administration Guide (010-5310-31).*

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

Product documentation for Netscreen products may be found at http://www.juniper.net.

Product documentation for nCite can be obtained from AudioCodes. Contact AudioCodes using the contact link at http://www.audiocodes.com.

Appendix A: Main Site 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
set service "RTP" protocol udp src-port 0-65535 dst-port 0-65535
set service "RTP" + udp src-port 0-65535 dst-port 0-65535
unset alg sip enable
unset alg sip enable
unset alg mgcp enable
unset alg sccp enable
unset alg sunrpc enable
unset alg msrpc enable
unset alg sql enable
unset alg rtsp enable
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 0
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 id 100 "L2-mgt" L2 28
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 "V1-Trust" reassembly-for-alg
set zone "V1-Untrust" reassembly-for-alg
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"
set interface "ethernet4" zone "DMZ"
set interface vlan1 ip 192.168.1.250/24
set interface vlan1 route
set interface ethernet1 ip 10.75.1.254/24
set interface ethernet1 route
set interface ethernet2 ip 172.16.71.1/24
set interface ethernet2 nat
set interface ethernet3 ip 46.14.2.2/24
set interface ethernet3 route
set interface ethernet4 ip 172.16.72.1/24
set interface ethernet4 nat
unset interface vlan1 bypass-others-ipsec
unset interface vlan1 bypass-non-ip
set interface vlan1 ip manageable
set interface ethernet1 ip manageable
set interface ethernet2 ip manageable
set interface ethernet3 ip manageable
set interface ethernet4 ip manageable
set interface ethernet3 manage ping
set interface ethernet3 manage telnet
set interface ethernet3 manage web
set interface ethernet4 manage telnet
set interface ethernet4 manage web
set zone L2-mgt manage telnet
set zone L2-mgt manage web
unset zone V1-Trust manage ping
unset zone V1-Trust manage ssh
unset zone V1-Trust manage telnet
unset zone V1-Trust manage snmp
unset zone V1-Trust manage ssl
unset zone V1-Trust manage web
set interface "ethernet3" mip 46.14.2.12 host 172.16.72.12 netmask
255.255.255.255 vr "trust-vr"
set interface "ethernet3" mip 46.14.2.52 host 10.75.10.52 netmask
255.255.255.255 vr "trust-vr"
set interface "ethernet3" mip 46.14.2.100 host 10.75.10.100 netmask
255.255.255.255 vr "trust-vr"
unset flow no-tcp-seq-check
set flow tcp-syn-check
set console timeout 30
set pki authority default scep mode "auto"
set pki x509 default cert-path partial
set address "Trust" "10.75.5.52/32" 10.75.5.52 255.255.255.255
set address "Trust" "46.14.2.12/32" 46.14.2.12 255.255.255.255
set address "Trust" "46.14.2.52/32" 46.14.2.52 255.255.255.255
set address "Untrust" "20.20.1.10/24" 20.20.1.10 255.255.255.0
set address "Untrust" "20.20.1.11/24" 20.20.1.11 255.255.255.0
set address "DMZ" "172.16.71.11/32" 172.16.71.11 255.255.255.255
set address "DMZ" "172.16.71.12/32" 172.16.71.12 255.255.255.255
set address "DMZ" "172.16.71.13/24" 172.16.71.13 255.255.255.0
set address "DMZ" "172.16.71.13/32" 172.16.71.13 255.255.255.255
set address "DMZ" "172.16.71.2/32" 172.16.71.2 255.255.255.255
set address "DMZ" "172.16.72.12/32" 172.16.72.12 255.255.255.255
set address "DMZ" "20.20.1.10/24" 20.20.1.10 255.255.255.0
set address "DMZ" "46.14.3.12/32" 46.14.3.12 255.255.255.255
set address "DMZ" "46.14.3.14/32" 46.14.3.14 255.255.255.255
set ike respond-bad-spi 1
unset ike ikeid-enumeration
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 url protocol websense
exit
set policy id 3 name "allow all" from "Trust" to "Untrust"  "Any" "Any" "ANY" 
permit
set policy id 3
exit
set policy id 6 name "Allow TFTP" from "Untrust" to "Trust"  "Any" 
"MIP(46.14.2.52)" "ICMP-ANY" permit
set policy id 6 disable
set policy id 6
set service "TFTP"
exit
set policy id 12 name "DMZ-Trust" from "DMZ" to "Trust"  "172.16.71.11/32" "Any" 
"ANY" permit
set policy id 12
set src-address "172.16.71.13/32"
exit
set policy id 13 name "Trust-DMZ" from "Trust" to "DMZ"  "Any" "Any" "ANY" 
permit
set policy id 13
exit
set policy id 22 from "Untrust" to "DMZ"  "Any" "Any" "ANY" permit
set policy id 22 disable
set policy id 22
exit
set policy id 15 from "Untrust" to "DMZ"  "Any" "46.14.3.14/32" "ICMP-ANY" 
permit
set policy id 15
set service "SIP"
exit
set policy id 21 from "DMZ" to "Untrust"  "Any" "Any" "ANY" permit
set policy id 21 disable
set policy id 21
exit
set policy id 16 from "DMZ" to "Untrust"  "46.14.3.14/32" "Any" "ANY" permit
set policy id 16
exit
set policy id 17 from "Untrust" to "Trust"  "Any" "MIP(46.14.2.100)" "DHCP-
Relay" permit
set policy id 17
set service "FTP"
set service "HTTP"
set service "HTTPS"
set service "ICMP-ANY"
set service "TFTP"
exit
set policy id 18 from "Untrust" to "Trust"  "Any" "Any" "ANY" permit
set policy id 18
exit
set policy id 19 from "Untrust" to "DMZ"  "Any" "46.14.3.12/32" "ICMP-ANY"
permit
set policy id 19
set service "RTP"
exit
set policy id 20 from "DMZ" to "Untrust"  "46.14.3.12/32" "Any" "ANY" permit
set policy id 20
exit
set monitor cpu 100
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 10.75.10.0/24 interface ethernet1 gateway 10.75.1.1
set route 10.75.5.0/24 interface ethernet1 gateway 10.75.1.1
set route 0.0.0.0/0 interface ethernet3 gateway 46.14.2.1 preference 20
permanent
set route 50.1.1.0/24 interface ethernet3 gateway 46.14.2.1 preference 20
permanent
set route 46.14.3.0/24 interface ethernet4 gateway 172.16.72.12 preference 20
set route 46.16.3.0/24 interface ethernet3 gateway 46.14.2.1 preference 20
exit
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
exit
```

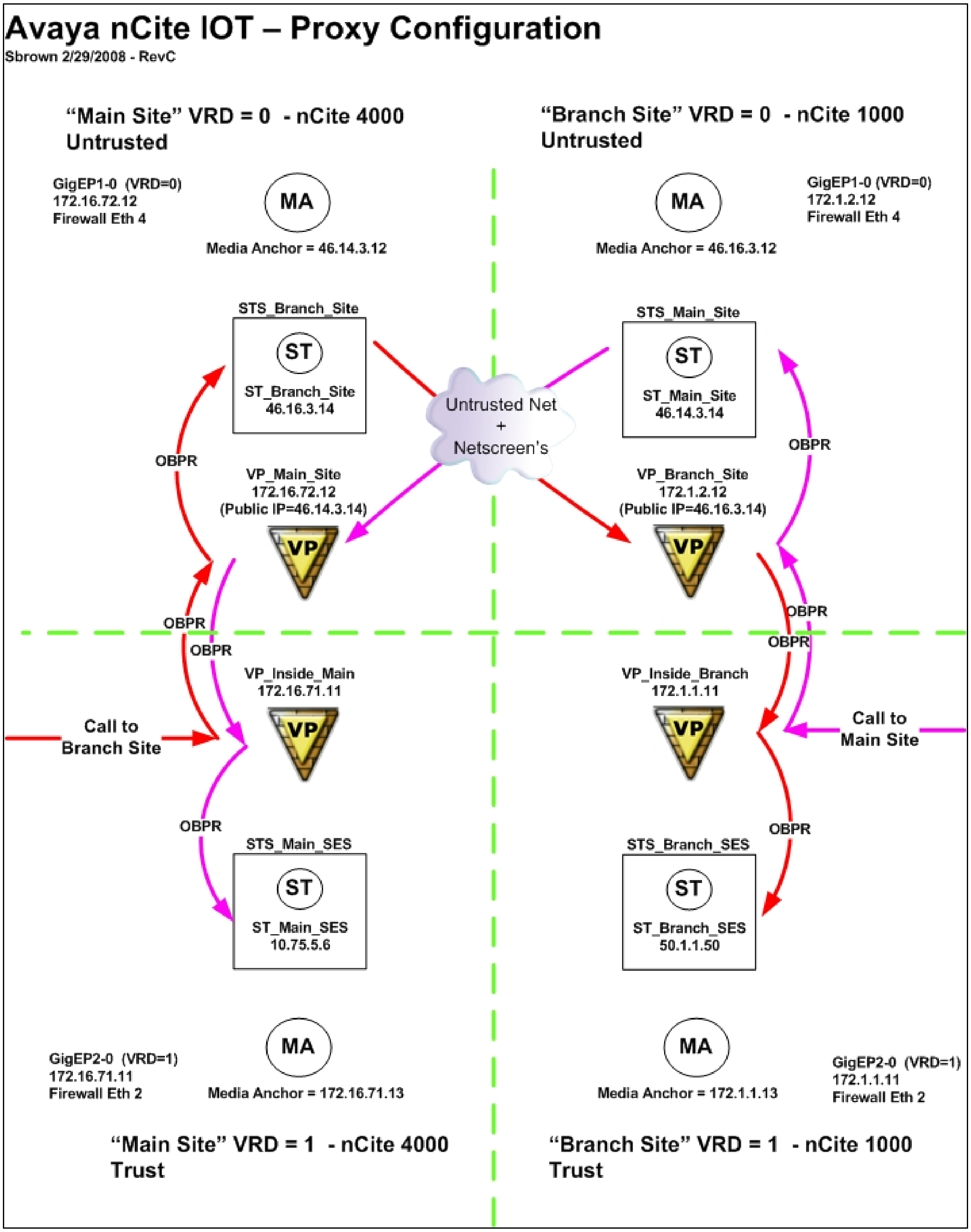
Appendix B: Branch Site NetScreen-50 Configuration File

Included below is the Juniper Networks NetScreen-50 configuration file used during the compliance testing at the branch 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
set service "RTP" protocol udp src-port 0-65535 dst-port 0-65535
set service "RTP" + udp src-port 0-65535 dst-port 0-65535
unset alg sip enable
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"
set interface "ethernet4" zone "DMZ"
unset interface vlan1 ip
set interface ethernet1 ip 50.99.99.1/24
set interface ethernet1 route
set interface ethernet2 ip 172.1.1.1/24
set interface ethernet2 nat
set interface ethernet3 ip 46.16.2.2/24
set interface ethernet3 route
set interface ethernet4 ip 172.1.2.1/24
set interface ethernet4 nat
unset interface vlan1 bypass-others-ipsec
unset interface vlan1 bypass-non-ip
set interface ethernet1 ip manageable
set interface ethernet2 ip manageable
set interface ethernet3 ip manageable
set interface ethernet4 ip manageable
set interface ethernet2 manage telnet
set interface ethernet2 manage web
set interface ethernet3 manage ping
set interface ethernet3 manage telnet
set interface ethernet3 manage web
set interface ethernet4 manage telnet
set interface "ethernet3" mip 46.16.2.12 host 172.1.2.12 netmask 255.255.255.255
vr "trust-vr"
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 address "DMZ" "172.1.1.11/32" 172.1.1.11 255.255.255.255
set address "DMZ" "172.1.1.12/32" 172.1.1.12 255.255.255.255
set address "DMZ" "172.1.1.13/32" 172.1.1.13 255.255.255.255
set address "DMZ" "172.1.2.12/32" 172.1.2.12 255.255.255.255
set address "DMZ" "46.16.2.12/32" 46.16.2.12 255.255.255.255
set address "DMZ" "46.16.2.14/32" 46.16.2.14 255.255.255.255
set address "DMZ" "46.16.3.12/32" 46.16.3.12 255.255.255.255
set address "DMZ" "46.16.3.14/32" 46.16.3.14 255.255.255.255
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 url protocol websense
exit
set policy id 1 from "Trust" to "Untrust"  "Any" "Any" "ANY" permit
set policy id 1
exit
set policy id 2 from "Untrust" to "Trust"  "Any" "Any" "ANY" permit
set policy id 2 disable
set policy id 2
exit
set policy id 3 from "Trust" to "DMZ"  "Any" "Any" "ANY" permit log
set policy id 3
exit
set policy id 4 from "DMZ" to "Trust"  "172.1.1.11/32" "Any" "ANY" permit log
set policy id 4
set src-address "172.1.1.13/32"
```

```
exit
set policy id 9 from "DMZ" to "Untrust"  "Any" "Any" "ANY" permit
set policy id 9 disable
set policy id 9
exit
set policy id 5 from "DMZ" to "Untrust"  "46.16.3.14/32" "Any" "ANY" permit
set policy id 5
exit
set policy id 10 from "Untrust" to "DMZ"  "Any" "Any" "ANY" permit
set policy id 10 disable
set policy id 10
exit
set policy id 6 from "Untrust" to "DMZ"  "Any" "46.16.3.14/32" "ICMP-ANY" permit
set policy id 6
set service "SIP"
exit
set policy id 7 from "Untrust" to "DMZ"  "Any" "46.16.3.12/32" "ICMP-ANY" permit
set policy id 7
set service "RTP"
exit
set policy id 8 from "DMZ" to "Untrust"  "46.16.3.12/32" "Any" "ANY" permit
set policy id 8
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 50.1.1.0/24 interface ethernet1 gateway 50.99.99.2
set route 0.0.0.0/0 interface ethernet3 gateway 46.16.2.1
set route 46.16.3.0/24 interface ethernet4 gateway 172.1.2.12 preference 20
set route 46.14.3.0/24 interface ethernet3 gateway 46.16.2.1 preference 20
exit
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
exit
```

Appendix C: nCite Configuration – Conceptual View



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.