Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Borderware SIPassure with Avaya SIP Enablement Services and Avaya Communication Manager to Support Remote Users - Issue 1.0

Abstract

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

Borderware SIPassure is a SIP security gateway that manages and protects the flow of SIP signaling and related media across an untrusted network. The compliance testing focused on telephony scenarios between remote SIP endpoints and the SIP infrastructure at a main site across an untrusted network secured by SIPassure.

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

1. Introduction

These Application Notes describe the procedure for configuring Borderware SIPassure with Avaya SIP Enablement Services (SES) and Avaya Communication Manager.

Borderware SIPassure is a SIP security gateway that manages and protects the flow of SIP signaling and related media across an untrusted network. The compliance testing focused on telephony scenarios between remote SIP endpoints and the SIP infrastructure at a main site across an untrusted network secured by SIPassure.

1.1. Configuration

Figure 1 illustrates the test configuration. The test configuration shows two sites connected by an untrusted IP network. The main office has a SIPassure at the edge of the network and the branch office does not. The remote SIP endpoints will direct SIP and RTP traffic to the public IP address of SIPassure. SIPassure in return will direct SIP and RTP traffic on behalf of these endpoints to Avaya SES. SIPassure uses its private LAN IP address to communicate with Avaya SES. In this manner, SIPassure can protect the main site infrastructure from any SIP-based attacks. The voice communication across the untrusted network uses SIP over UDP and RTP for the media streams.

Located at the main office is an Avaya SES and an Avaya S8300 Server running Avaya Communication Manager in an Avaya G700 Media Gateway. Endpoints include two Avaya 4600 Series IP Telephones (with SIP firmware), an Avaya 4600 Series IP Telephone (with H.323 firmware), an Avaya 6408D+ Digital Telephone, and an Avaya 6210 Analog Telephone. An ISDN-PRI trunk connects the media gateway to the PSTN. One PSTN number assigned to the ISDN-PRI trunk at the main office is mapped to a telephone extension at the main office. The other is mapped to a telephone extension at the branch office.

The Avaya 4600 Series IP Telephone is registered to Avaya Communication Manager and the Avaya 4600 Series SIP Telephones are registered directly to Avaya SES. All calls originating from Avaya Communication Manager at the main office and destined for the branch office will be routed through the on-site Avaya SES, SIPassure and across the untrusted IP network.

Located at the branch office are two Avaya 4600 Series SIP Telephones. These telephones register with Avaya SES through SIPassure. These telephones use the public IP address of SIPassure at the main office as their configured server. SIPassure will forward any registration messages it receives from the remote endpoints to Avaya SES. All calls originating from the branch office are routed across the untrusted IP network, through SIPassure and Avaya SES to Avaya Communication Manager at the main office.

All SIP telephones at both sites use the TFTP server at the main site to obtain their configuration files. All non-SIP traffic (including these TFTP transfers) bypasses SIPassure and flows through a parallel connection through the untrusted network which would be protected by a traditional data firewall.

For interoperability, direct IP to IP media (also known as media shuffling) must be disabled on the SIP trunk in Avaya Communication Manager (see **Section 3, Step 6**). This will result in VoIP resources being used in the Avaya Media Gateway for the duration of each SIP call.

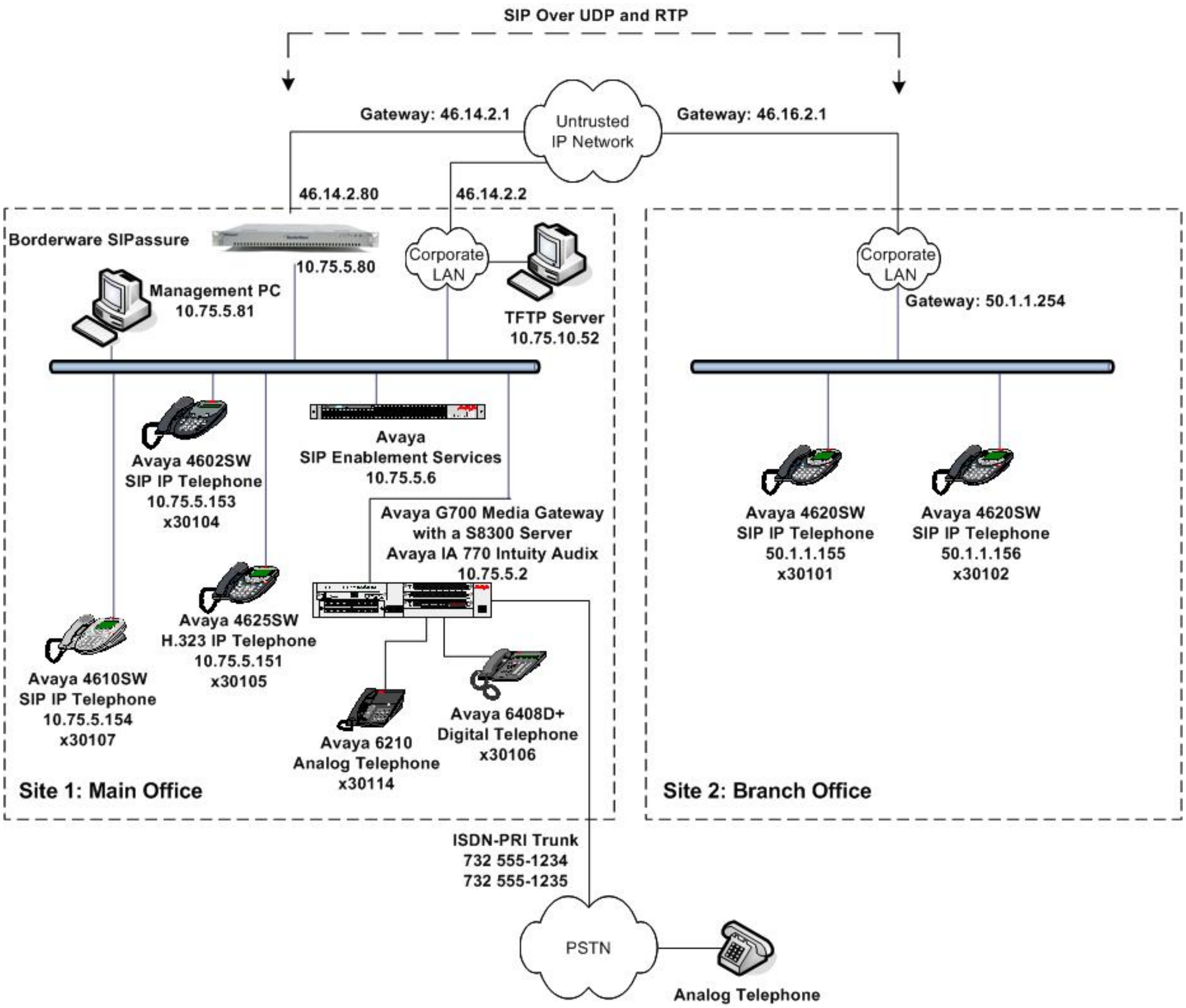


Figure 1: SIPassure Test Configuration

2. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8300 Server with Avaya G700 Media Gateway Avaya IA 770 Intuity Audix	Avaya Communication Manager 4.0 Service Pack (R014x.00.0.730.5-13566)
Avaya SIP Enablement Services	3.1.2
Avaya 4602SW IP Telephone Avaya 4610SW IP Telephone Avaya 4620SW IP Telephones	SIP version 2.2.2
Avaya 4625SW IP Telephone	H.323 version 2.7
Avaya 6408D+ Digital Telephone	-
Avaya 6210 Analog Telephone	-
Analog Telephone	-
Windows PCs (Management PC and TFTP Server)	Windows XP Professional
Borderware SIPassure	3.0.1 (Build 3.0.7) with Update 1

3. Configure Avaya Communication Manager

This section describes the Avaya Communication Manager configuration to support SIP. It is typically comprised of two parts. The first part is the configuration of the SIP connection to Avaya SES required of any Avaya SES installation. The second part describes the configuration of Off-PBX stations (OPS) for each SIP endpoint. The configuration of the OPS stations is not directly related to the interoperability of SIPassure, so it is not included here. The procedure for configuring OPS stations can be found in [4].

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

Step	Description
1.	Use the **display system-parameters customer-options** command to verify that sufficient SIP trunk capacity exists. On **Page 2**, verify that the number of SIP trunks supported by the system is sufficient for the number of SIP trunks needed. 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. The license file installed on the system controls the maximum permitted. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to make the appropriate changes.

```
display system-parameters customer-options                      Page   2 of  10
                                OPTIONAL FEATURES

IP PORT CAPACITIES                                             USED
                     Maximum Administered H.323 Trunks: 100   32
           Maximum Concurrently Registered IP Stations: 100   0
             Maximum Administered Remote Office Trunks: 0     0
Maximum Concurrently Registered Remote Office Stations: 0     0
              Maximum Concurrently Registered IP eCons: 0     0
  Max Concur Registered Unauthenticated H.323 Stations: 0     0
                  Maximum Video Capable H.323 Stations: 0     0
                   Maximum Video Capable IP Softphones: 0     0
                       Maximum Administered SIP Trunks: 100   44

   Maximum Number of DS1 Boards with Echo Cancellation: 0     0
                             Maximum TN2501 VAL Boards: 0     0
                     Maximum Media Gateway VAL Sources: 0     0
           Maximum TN2602 Boards with 80 VoIP Channels: 0     0
          Maximum TN2602 Boards with 320 VoIP Channels: 0     0
   Maximum Number of Expanded Meet-me Conference Ports: 0     0

        (NOTE: You must logoff & login to effect the permission changes.)
```

Step	Description
2.	In order to support SIP the following features must be enabled. Use the **display system-parameters customer-options** command to verify that the following fields have been set to ***y***. **Page 4**: **Enhanced EC500?** ***y*** **Page 4**: **ISDN-PRI?** ***y*** **Page 4**: **IP trunks?** ***y*** If a required feature is not enabled, contact an authorized Avaya sales representative to make the appropriate changes.

Step	Description

3.	Use the **change node-names ip** command to assign the node name and IP address for Avaya SES. In this case, ***SES*** and ***10.75.5.6*** are being used, respectively. The node name ***SES*** will be used throughout the other configuration forms of Avaya Communication Manager. In this example, ***procr*** and ***10.75.5.2*** are the name and IP address assigned to the Avaya S8300 Server.
	
	`change node-names ip                                        Page   1 of   2`
	`                                  IP NODE NAMES`
	`    Name              IP Address`
	`SES                 10.75.5.6`
	`default             0.0.0.0`
	`myaudix             10.75.5.7`
	`procr               10.75.5.2`

Step	Description
4.	Use the **change ip-network-region *n*** command, where ***n*** is the number of the region to be changed, to define the connectivity settings for all VoIP resources and IP endpoints within the region. Select an IP network region that will contain the Avaya SES server. The association between this IP network region and the Avaya SES server will be done on the **Signaling Group** form as shown in **Step 6**. In the case of the compliance test, the same IP network region that contains the Avaya S8300 Server and Avaya IP Telephones was selected to contain the Avaya SES server. By default, the Avaya S8300 Server and IP telephones are in IP network region 1. On the **IP Network Region** form: ▪ The **Authoritative Domain** field is configured to match the domain name configured on Avaya SES. In this configuration, the domain name is ***business.com***. This name will appear in the "From" header of SIP messages originating from this IP region. ▪ Enter a descriptive name for the **Name** field. ▪ By default, **IP-IP Direct Audio** (shuffling) is enabled to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya G700 Media Gateway. This is true for both intra-region and inter-region IP-IP Direct Audio. Shuffling can be further restricted at the trunk level on the **Signaling Group** form. ▪ The **Codec Set** is set to the number of the IP codec set to be used for calls within this IP network region. If different IP network regions are used for the Avaya S8300 Server and the Avaya SES server, then **Page 3** of each **IP Network Region** form must be used to specify the codec set for inter-region communications. ▪ The default values can be used for all other fields.

```
change 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
5.	Use the **change ip-codec-set *n*** command, where ***n*** is the codec set value specified in **Step 4**, to enter the supported audio codecs. Multiple codecs can be listed in priority order to allow the codec to be negotiated during call establishment. The list should include 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.

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

                          IP Codec Set

    Codec Set: 1

    Audio        Silence      Frames   Packet
    Codec        Suppression  Per Pkt  Size(ms)
 1: G.711MU          n          2        20
 2: G.729AB          n          2        20
 3:
```

Step	Description
6.	Use the **add signaling-group *n*** command, where ***n*** is the number of an unused signaling group, to create the SIP signaling group as follows: ▪ Set the **Group Type** field to ***sip***. ▪ The **Transport Method** field will default to ***tls*** (Transport Layer Security). TLS is the only link protocol that is supported for communication between Avaya SES and Avaya Communication Manager. ▪ Specify the Avaya S8300 Server (node name ***procr***) and the Avaya SES server (node name ***SES***) as the two ends of the signaling group in the **Near-end Node Name** and the **Far-end Node Name** fields, respectively. These field values are taken from the **IP Node Names** form shown in **Step 3**. For alternative configurations that use a C-LAN board, the near (local) end of the SIP signaling group will be the C-LAN board instead of the Avaya S8300 Server. ▪ Ensure that the TLS port value of ***5061*** is configured in the **Near-end Listen Port** and the **Far-end Listen Port** fields. ▪ In the **Far-end Network Region** field, enter the IP network region value assigned in the **IP Network Region** form in **Step 4**. This defines which IP network region contains the Avaya SES server. If the **Far-end Network Region** field is different from the near-end network region, the preferred codec will be selected from the IP codec set assigned for the inter-region connectivity for the pair of network regions. ▪ Enter the domain name of Avaya SES in the **Far-end Domain** field. In this configuration, the domain name is ***business.com***. This domain is specified in the Uniform Resource Identifier (URI) of the SIP "To" header in the INVITE message. ▪ The **Direct IP-IP Audio Connections** field is set to ***n***. For interoperability, this field (also know as media shuffling) must be disabled for the SIP trunk. ▪ The **DTMF over IP** field must be set to the default value of ***rtp-payload*** for a SIP trunk. This value enables Avaya Communication Manager to send DTMF transmissions using RFC 2833. ▪ The default values for the other fields may be used.

```
add signaling-group 1                                           Page   1 of   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: business.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): 120
```

Step	Description
7.	Add a SIP trunk group by using the **add trunk-group *n*** command, where ***n*** is the number of an unused trunk group. For the compliance test, trunk group number 1 was chosen. On **Page 1**, set the fields to the following values: ▪ Set the **Group Type** field to ***sip***. ▪ Choose a descriptive **Group Name**. ▪ Specify an available trunk access code (**TAC**) that is consistent with the existing dial plan. ▪ Set the **Service Type** field to ***tie***. ▪ Specify the signaling group associated with this trunk group in the **Signaling Group** field as previously specified in **Step 6**. ▪ Specify the **Number of Members** supported by this SIP trunk group. As mentioned earlier, 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. ▪ The default values may be retained for the other fields.

```
add 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
```

Step	Description
8.	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.

```
add 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
9.	Use the **change public-unknown-numbering 0** command to define the full calling party number to be sent to the far-end. Add an entry for the trunk group defined in **Step 7**. 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 will be 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: 4
 5  3              1                        5           Maximum Entries: 240
 5  3              99                       5
```

Step	Description
10.	Create a route pattern that will use the SIP trunk that connects to Avaya SES. This route pattern will be used as a default route for SIP calls in **Step 11**. Some transfer scenarios using alpha-numeric handles (i.e., user names) instead of extensions require a default route pattern. These call scenarios were not tested as part of the compliance test, however, the creation of this default route pattern is included here for completeness. To create a route pattern, use the **change route-pattern *n*** command, where ***n*** is the number of an unused route pattern. Enter a descriptive name for the **Pattern Name** field. Set the **Grp No** field to the trunk group number created for the SIP trunk. Set the Facility Restriction Level (**FRL**) field to a level that allows access to this trunk for all users that require it. The value of ***0*** is the least restrictive level. The default values may be retained for all other fields.

```
change route-pattern 1                                          Page   1 of   3
                    Pattern Number: 3   Pattern Name: SIP
                             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: 1    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 3 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
```

Step	Description
11.	Use the **change locations** command to assign the default SIP route pattern to the location. All IP endpoints, both local and remote, are part of a single logical location in Avaya Communication Manager with the default name of ***Main*** and shown in the example below. Enter the route pattern number from the previous step in the **Proxy Sel Rte Pat** field. The default values may be retained for all other fields.

```
change locations                                                Page   1 of   4
                                   LOCATIONS

                ARS Prefix 1 Required For 10-Digit NANP Calls? y

 Loc  Name           Timezone Rule  NPA  ARS  Atd      Disp   Prefix   Proxy Sel
 No                   Offset             FAC  FAC      Parm              Rte Pat
 1:  Main            + 00:00   0                        1                  1
 2:                      :
 3:                      :
```

Step	Description
12.	Automatic Route Selection (ARS) is used to route calls to the PSTN. In the compliance test, PSTN numbers that begin with 1732 were used for testing. Use the **change ars analysis *n*** command to add an entry in the ARS Digit Analysis Table for the dialed string beginning with ***n***. In the example shown, PSTN numbers that begin with 1732 and 11 digits long use route pattern 2. Route pattern 2 routes calls to the ISDN-PRI trunk between the main site and the PSTN shown in **Figure 1**. The configuration of the PRI trunk is beyond the scope of these Application Notes.

```
change ars analysis 1732                                        Page   1 of   2
                             ARS DIGIT ANALYSIS TABLE
                                   Location:  all          Percent Full:    3

          Dialed          Total     Route    Call   Node   ANI
          String         Min  Max  Pattern   Type   Num    Reqd
    1732                 11   11     2       fnpa          n
    174                  11   11    deny     fnpa          n
    175                  11   11    deny     fnpa          n
    176                  11   11    deny     fnpa          n
    177                  11   11    deny     fnpa          n
```

Step	Description
13.	To map a PSTN number to a station at the main or branch office, use the **change inc-call-handling-trmt trunk-group *n*** command, where ***n*** is the trunk group number connected to the PSTN from the Avaya G700 Media Gateway. The compliance test used trunk group 2 to connect to the PSTN. This trunk group configuration is not shown in these Application Notes. The example below shows two incoming 11-digit numbers being deleted and replaced with the extension number of the desired station.

```
change inc-call-handling-trmt trunk-group 2                     Page   1 of   3
                          INCOMING CALL HANDLING TREATMENT
 Service/      Called    Called      Del Insert          Per Call Night
 Feature        Len      Number                          CPN/BN   Serv
 tie             11 17325551234      11  30104
 tie             11 17325551235      11  30101
```

4. Configure Avaya SES

This section covers the configuration of Avaya SES. 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].

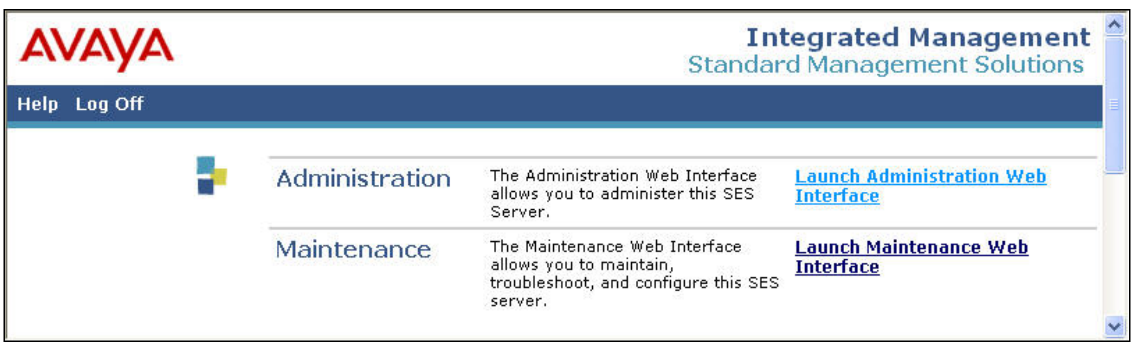
Each SIP endpoint used in the compliance test, requires that a user and media server extension be created on Avaya SES. This configuration is not directly related to the interoperability of SIPassure so it is not included here. These procedures are covered in [5].

SIPassure registers to Avaya SES on behalf of each of the remote users by serving as a proxy of the registration request from the remote endpoint to Avaya SES. Thus, SIPassure appears as a set of endpoints to Avaya SES. As a result, no outbound proxy settings, address maps or trusted host settings are required on Avaya SES to route calls to or to support the remote users.

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>1.</td><td>

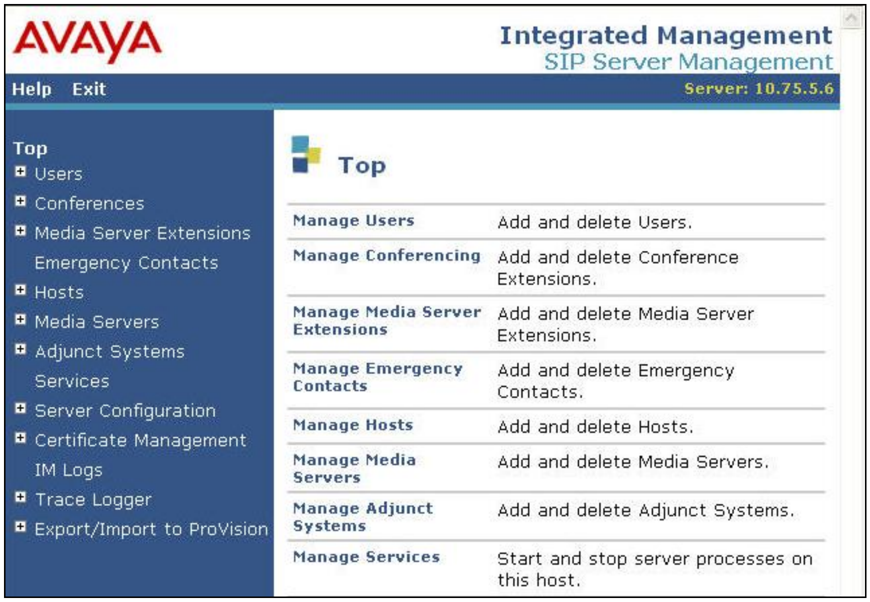
Access the Avaya SES administration web interface by entering http://<*ip-addr*>/admin as the URL in an Internet browser, where <*ip-addr*> is the IP address of the Avaya SES server.

Log in with the appropriate credentials and then select the **Launch Administration Web Interface** link from the main page as shown below.



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

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>2.</td><td>The Avaya SES administration home page will be displayed as shown below.



</td></tr>
<tr><td>3.</td><td>After making changes within Avaya SES, it is necessary to commit the database changes using the Update link that appears when changes are pending. Perform this step by clicking on the Update link found in the bottom of the blue navigation bar on the left side of any of the Avaya SES administration pages as shown below. It is recommended that this be done after making any changes.

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

Step	Description
4.	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*** (To view, navigate to **Host→List**; Click **Edit**) • Media Server (Avaya Communication Manager) Interface Name: ***CMeast*** (To view, navigate to **Media Server→List**; Click **Edit**) • SIP Trunk IP Address (Avaya S8300 Server IP address): ***10.75.5.2*** (To view, navigate to **Media Server→List**; Click **Edit**)

5. Configure the Avaya SIP Telephones

The SIP telephones at the main office will use Avaya SES as the call server. The SIP telephones at the branch site will use the public IP address of SIPassure as the call server.

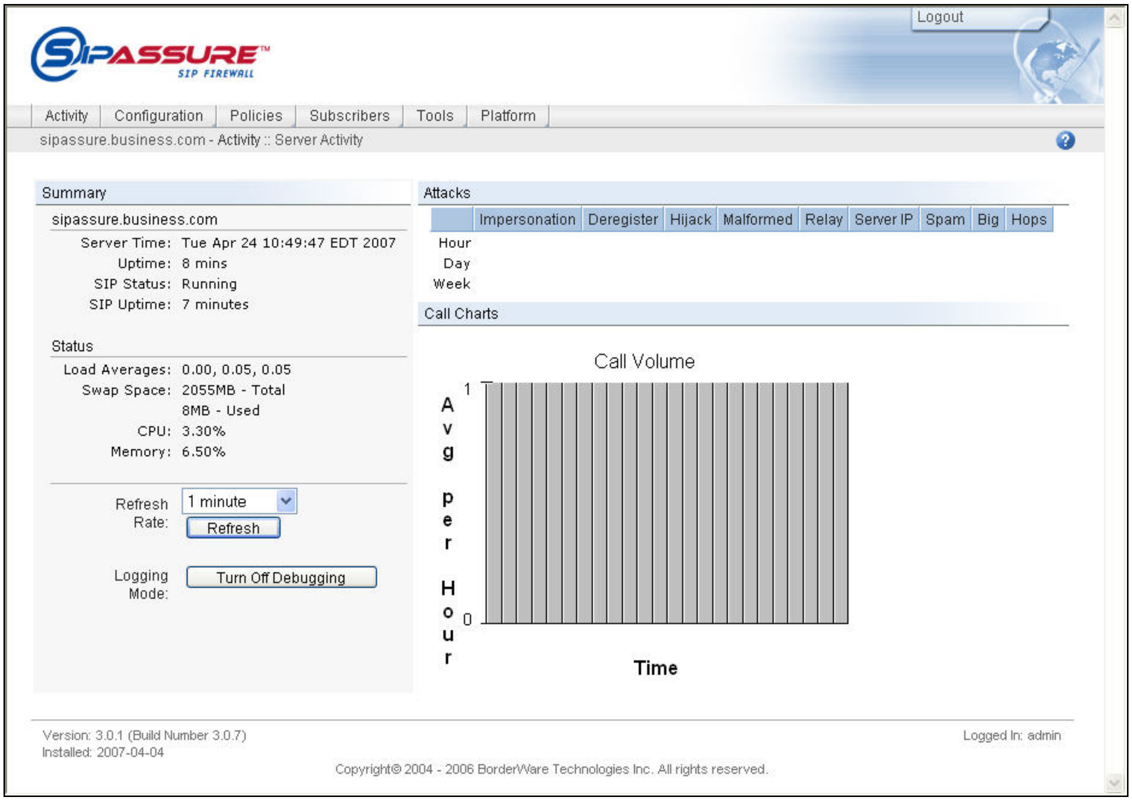
The table below shows an example of the SIP telephone networking settings for both the main and branch offices.

	Main Site	**Branch Site**
IP Address	10.75.5.153	50.1.1.155
Subnet Mask	255.255.255.0	255.255.255.0
Call Server	10.75.5.6	46.14.2.80
Router	10.75.5.1	50.1.1.254
File Server	10.75.10.52	10.75.10.52

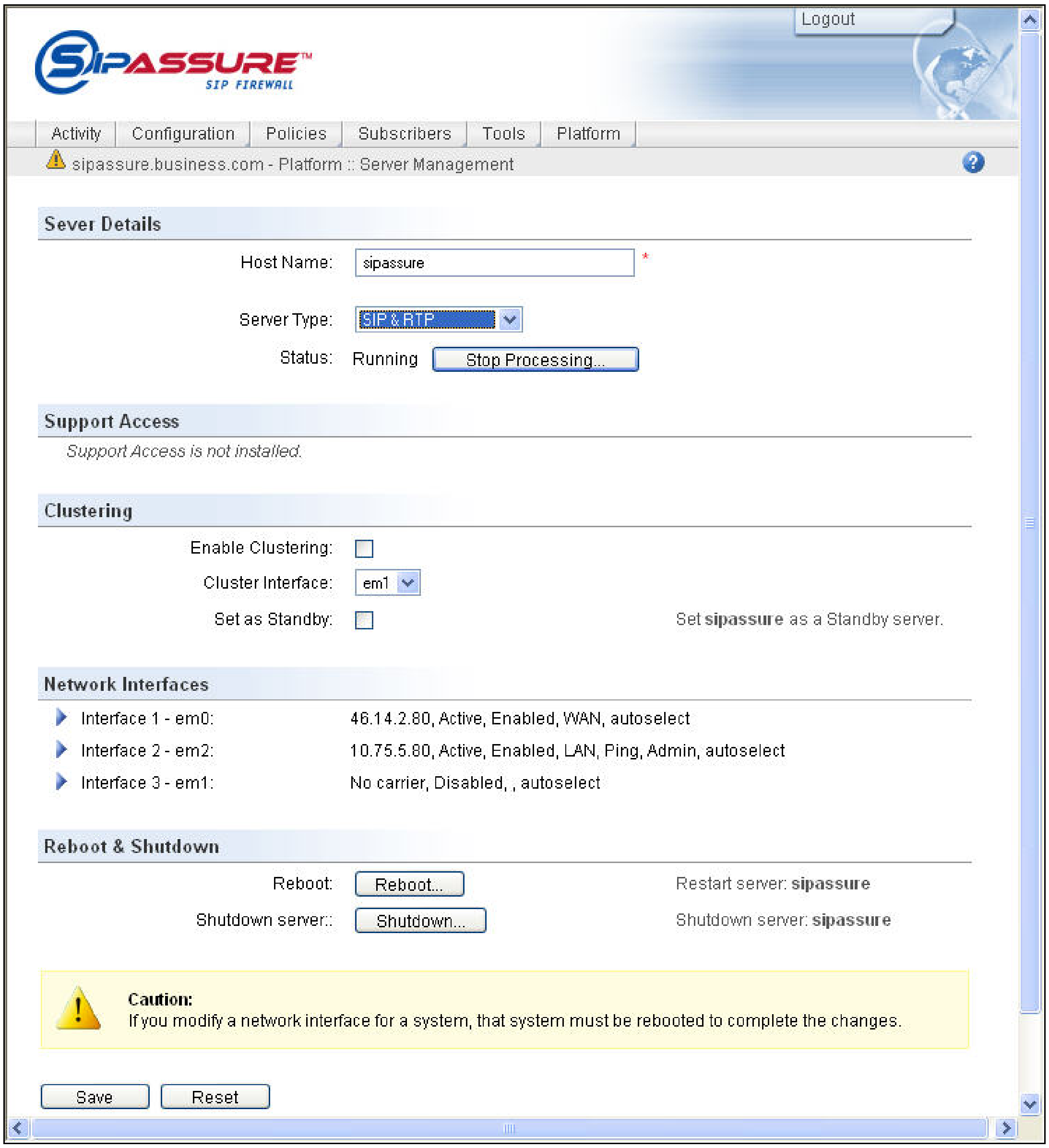
6. Configure Borderware SIPassure

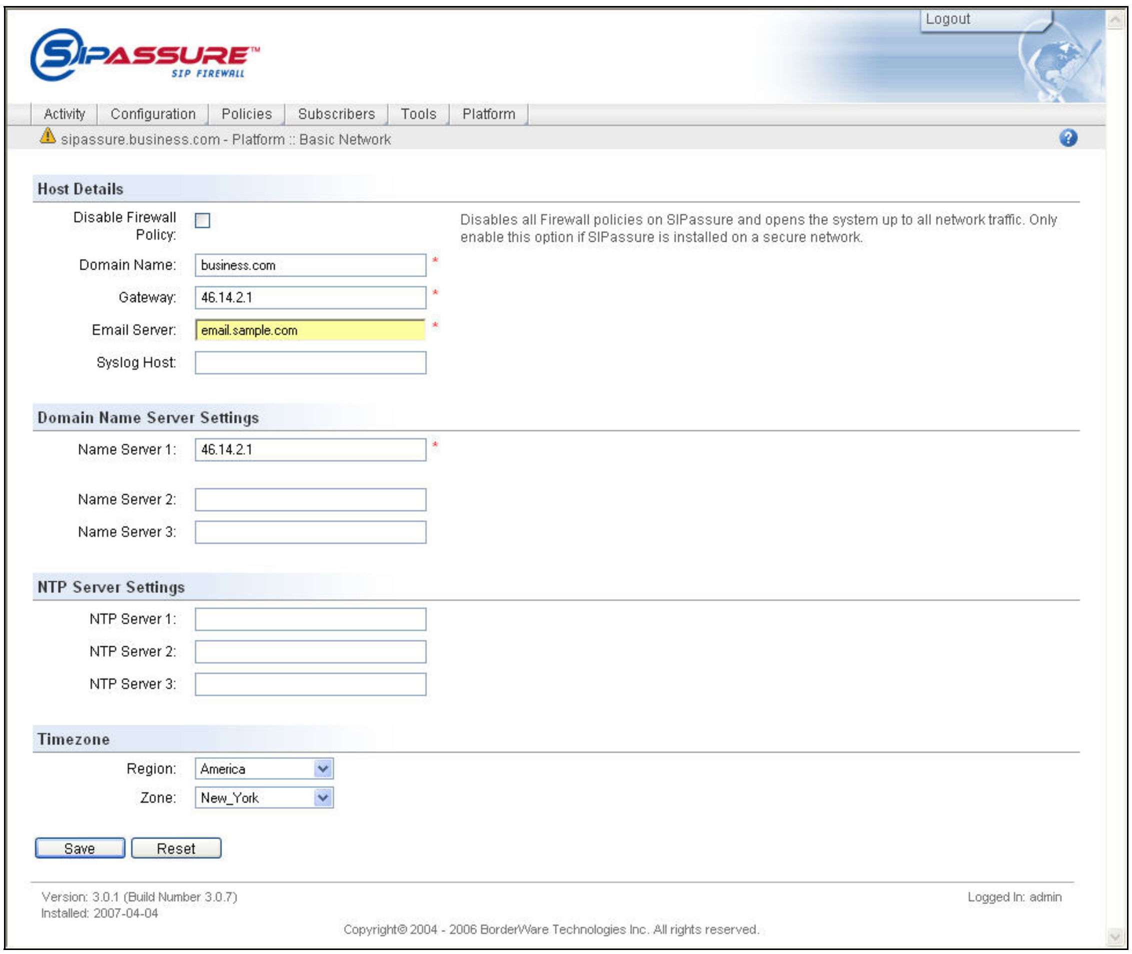
This section covers the configuration of SIPassure. It is assumed that the SIPassure software has already been installed. For additional information on these installation tasks, refer to [7].

Step	Description
1.	SIPassure is configured via a web browser. To access the web interface, enter http://<*ip-addr*> in the address field of the web browser, where <*ip-addr*> is the IP address of SIPassure. Log in with the appropriate credentials. The main page will appear as shown below.



Step	Description
2.	The initial server parameters are configured as part of the installation procedures. This includes the server name, server type and both public and private IP addresses. For details on these procedures see [7]. To view these settings, navigate from the **Platform** tab to **Platform→Server Management**. The example below shows the settings used for the compliance test. The **Host Name** was set to ***sipassure***. The **Server Type** was set to ***SIP & RTP***. **Interface - em0** was set to the WAN (public) IP address and **Interface - em2** was set to the LAN (private) IP address. The default values were used for the remaining fields. If any values were modified, click **Save**.

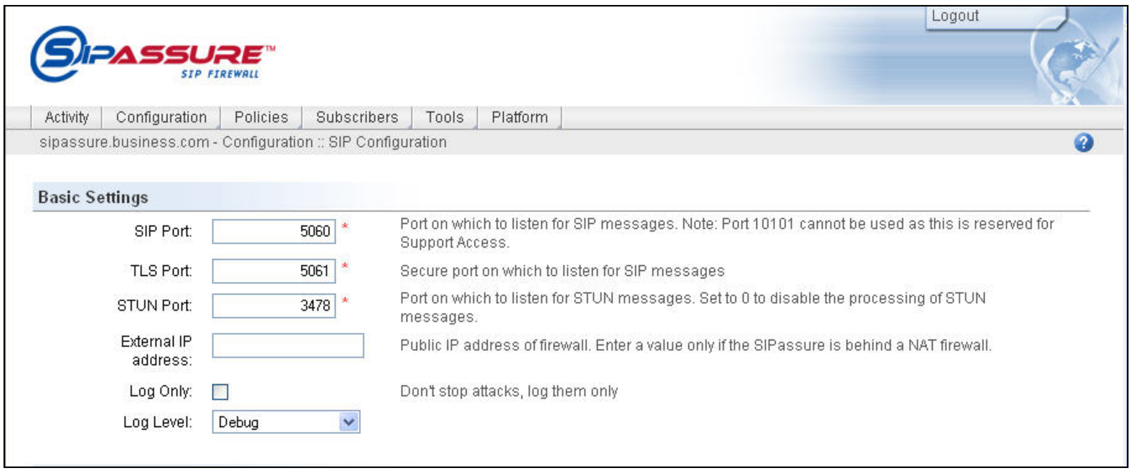


Step	Description
3.	Additional parameters configured during installation can be viewed by navigating from the **Platform** tab to **Platform→Basic Network**. The **Domain Name** field was set to the SIP domain of Avaya SES as shown in **Section 4**, **Step 4**. The **Gateway** field was set to the default gateway for the public IP interface. No email server or DNS server was used in the compliance test. However, SIPassure requires entries in these fields, so an arbitrary value was entered for each. The email server is needed for the customer to receive notifications of software updates that have been uploaded and not yet installed. In a redundant configuration, it is also used to send notifications that a failover has occurred. In a production environment, the DNS server would be used to resolve host names within the VoIP network. If a NTP server is used, it should be set to the same clock source (NTP server) as Avaya SES and Avaya Communication Manager. The default values can be used for the remaining fields. If any values were modified, click **Save**. 

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

Basic Settings
To configure or verify the basic settings, navigate from the **Configuration** tab to **Configuration→SIP**. Verify the **SIP Port** field is set to the default value of ***5060***. This is the port which SIPassure will listen for SIP messages. Verify the **TLS Port** field is set to the default value of ***5061***. This is the port which SIPassure will listen for secure SIP messages using TLS. The **Log Level** field was set to ***Debug*** for the testing. Normally, it would be set to the default value of ***Error*** to reduce the amount of logging under normal conditions.

The default values can be used for the remaining fields. Scroll down to configure additional parameters.



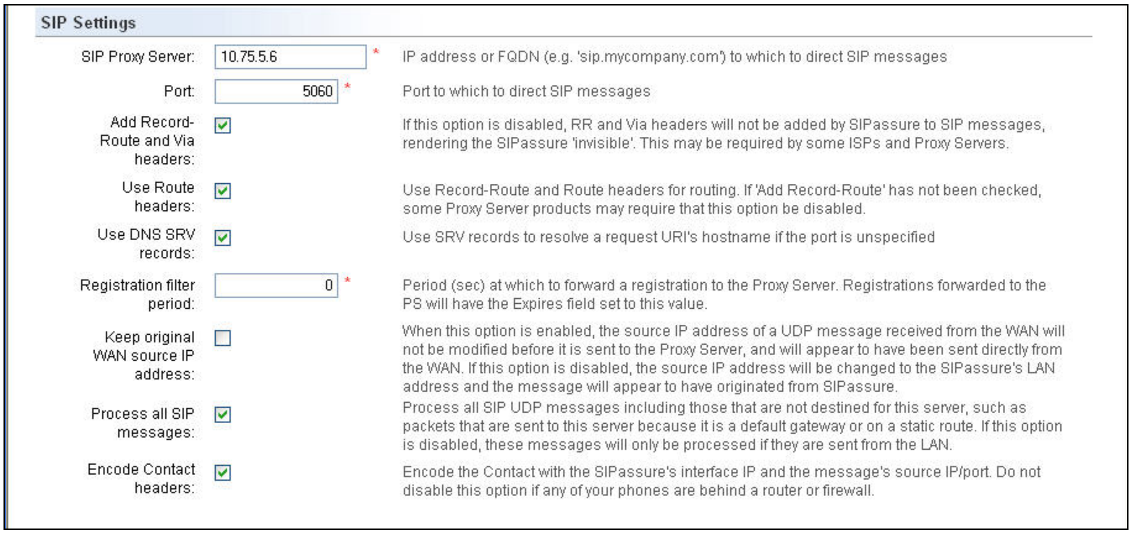
</td></tr>
</table>

<table>
<tr><th>Step</th><th>Description</th></tr>
<tr><td>5.</td><td>

SIP Settings

Set the **SIP Proxy Server** to the IP address of Avaya SES. Verify the **Port** field is set to the default value of ***5060***. This is the port which SIPassure will send SIP signaling messages. Check the **Process all SIP messages** box.

The default values can be used for the remaining fields. Scroll down to configure additional parameters.

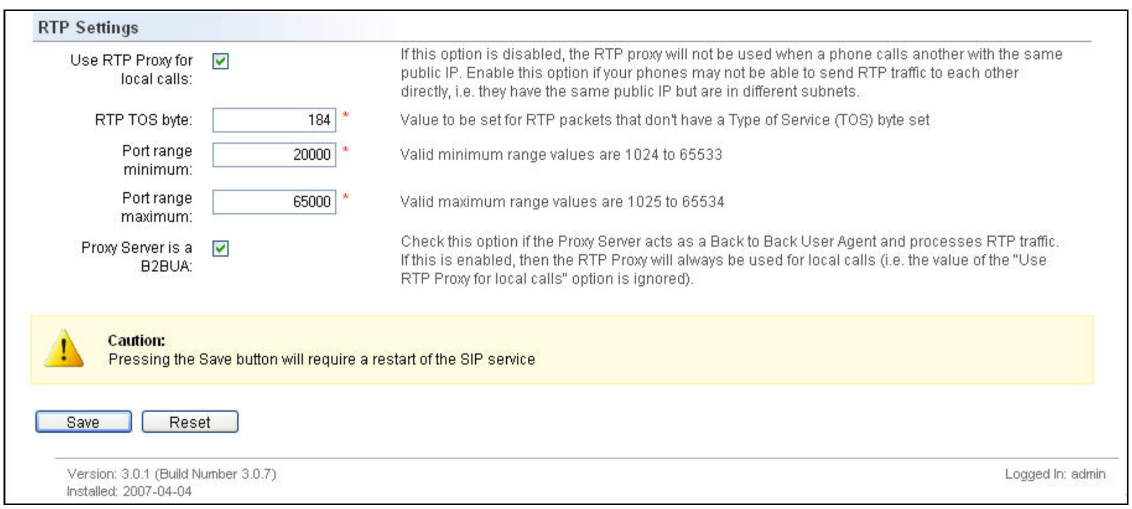


</td></tr>
<tr><td>6.</td><td>

RTP Settings

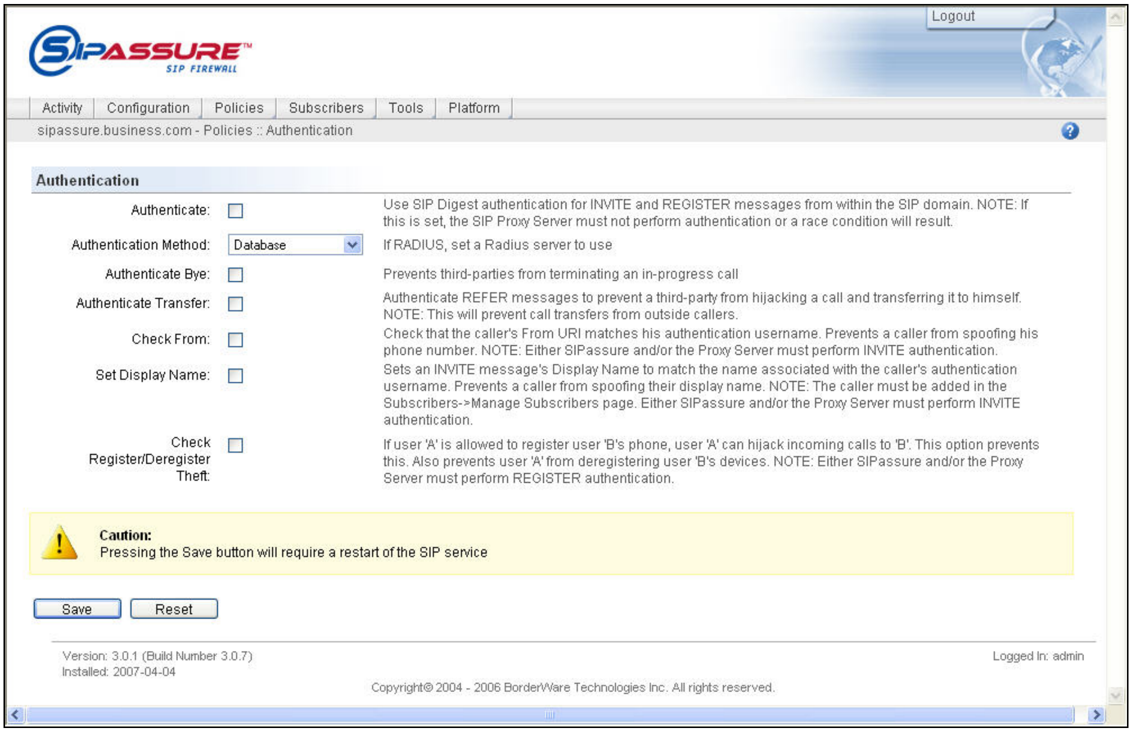
Check the **Use RTP Proxy for local calls** box. Check the **Proxy Server is a B2BUA** box.

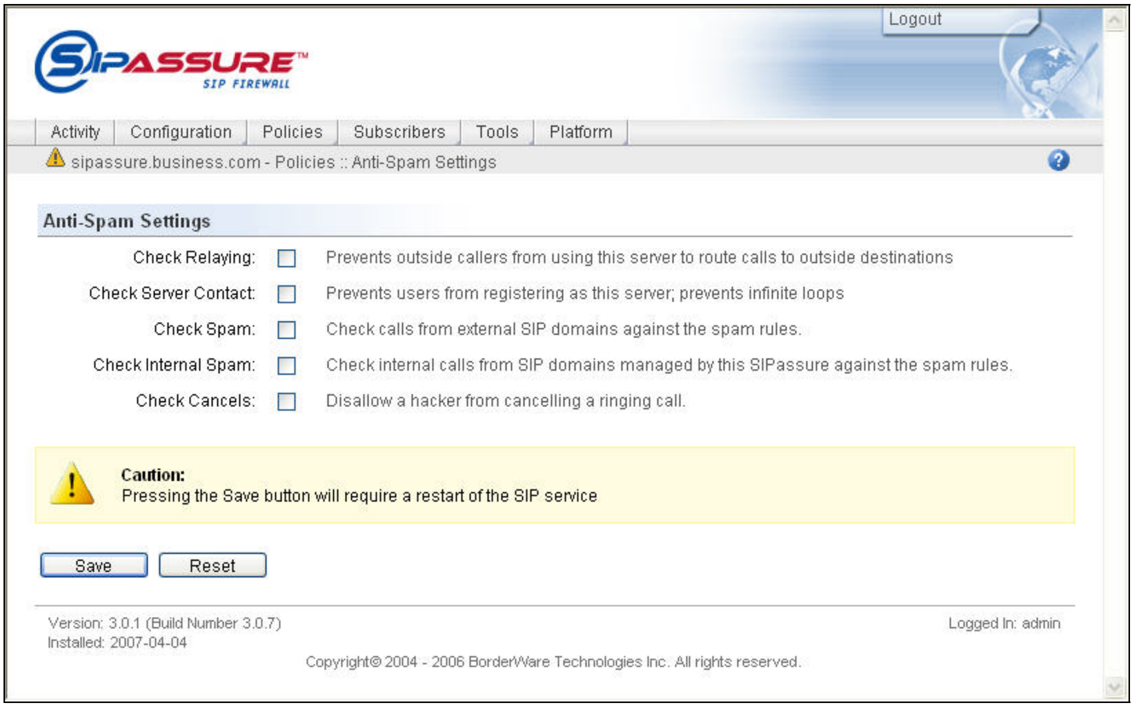
The default values can be used for the remaining fields. Click **Save**.



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

Step	Description
7.	**SIP Domain** Navigate from the **Configuration** tab to **Configuration→SIP Domains**. The compliance test used a single SIP domain which was entered during installation (see **Step 3**). This form may be used to add additional domains. The example below shows the single domain used by the compliance test. 

Step	Description
8.	**Authentication** Navigate from the **Policies** tab to **Policies→Authentication**. Uncheck the **Authentication** box since Avaya SES will authenticate the caller. The default values can be used for the remaining fields. Click **Save**. 

Step	Description
9.	**Anti-Spam Settings** The Anti-Spam Settings were disabled for the compliance test. To configure these settings, navigate to **Policies** tab to **Policies→Anti-Spam Settings**. The example below shows all the settings were unchecked. However, for a customer installation, Borderware highly recommends that Anti-Spam protection be enabled to allow normal call traffic and flag or block abnormal calling patterns. For more information on how to configure the Anti-Spam settings, see [9]. 

7. Interoperability Compliance Testing

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

7.1. General Test Approach

The general test approach was to make calls through SIPassure using various codec settings and exercising common PBX features. Calls were made between the branch office and the main office, between the branch office and the PSTN, and within the branch site.

7.2. Test Results

SIPassure 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 offices.
- Calls between the branch office and SIP endpoints at the main office.
- Calls between the branch office and non-SIP endpoints at the main office.
- Calls between the branch office and the PSTN.
- Intra-branch calls
- 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 a SIPassure 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 the SIP trunk in Avaya Communication Manager (see **Section 3, Step 6**). This will result in VoIP resources being used in the Avaya Media Gateway for the duration of each SIP call.
- For interoperability, local SIP endpoints must register with SES and do not have the option to register through SIPassure as the remote endpoints do. Thus, SIPassure will not be able to protect Avaya SES and Avaya Communication Manager from SIP attacks from internal users.

8. 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 remote endpoints are registered with Avaya SES using the private IP address of SIPassure. To view, navigate to **Users→Registered Users**.
- Verify that calls can be placed between the branch office and SIP endpoints at the main office.
- Verify that calls can be placed between the branch office and non-SIP endpoints at the main office.
- Verify that calls can be placed between the branch office and the PSTN.
- Verify that calls can be placed between endpoints at the branch office.

9. Support

For technical support on SIPassure, contact the Borderware reseller or distributor from where SIPassure was purchased.

10. Conclusion

Borderware SIPassure passed compliance testing with the observations listed in **Section 7.2**. These Application Notes describe the procedures required to configure Borderware SIPassure to interoperate with Avaya SIP Enablement Services and Avaya Communication Manager to support remote users as shown in **Figure 1**.

11. 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] *Borderware SIPassure Installation Guide*, Version 3.0, September 21, 2006.

[8] *Borderware SIPassure Quick Install Guide*, October 6, 2006.

[9] *Borderware SIPassure Users Guide*, Version 3.0, August 11, 2006.

[10] *Borderware SIPassure Update 3 Release Notes*, October 19, 2006.

[11] *Borderware SIPassure Update 3.0.7 Release Notes*, pending completion.

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

Product documentation for SIPassure can be obtained from a Borderware reseller or distributor.

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 Developer*Connection* Program at devconnect@avaya.com.