



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Sipera Systems UC-Sec Secure Access Proxy with Avaya Aura® Session Manager and Avaya Aura® Communication Manager to Support Remote Users with and without NAT Traversal - Issue 1.1

Abstract

These Application Notes describe the procedures for configuring Sipera Systems UC-Sec Secure Access Proxy with Avaya Aura® Session Manager and Avaya Aura® Communication Manager to support Remote Users with and without NAT Traversal.

The Sipera Systems UC-Sec Secure Access Proxy is a SIP security appliance that manages and protects the flow of SIP signaling and related media across an un-trusted network. Compliance testing focused on remote Avaya SIP endpoints, with and without network address translation, traversing the un-trusted network through the Sipera UC-Sec Secure Access Proxy to the Avaya SIP infrastructure at the corporate site while the Sipera UC-Sec enforced Denial of Service policies.

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 Sipera Systems UC-Sec Appliance with Avaya Aura® Session Manager and Avaya Aura® Communication Manager to support Remote Users with and without NAT Traversal.

The Sipera Systems UC-Sec Secure Access Proxy (Sipera UC-Sec) is a SIP security appliance that manages and protects the flow of SIP signaling and related media across an un-trusted network. Compliance testing focused on remote Avaya SIP endpoints, with and without network address translation (NAT), traversing the un-trusted network through the Sipera UC-Sec Secure Access Proxy to the Avaya SIP infrastructure at the corporate site while the Sipera UC-Sec enforced Denial of Service (DoS) policies.

With all the benefits of VoIP/UC come all the threats of any new technology or application traversing untrusted networks. Sipera's UC-Sec allows enterprises to implement the following security measures to ensure remote users communicate securely and safely with all of the UC benefits of an office based employee.

Define and implement strong UC policies - Define rules for VoIP and UC traffic. Sipera's UC-Sec enforces these policies based on network, user, device, and time-of-day.

Integrate with existing infrastructure for strong access control - The Sipera UC-Sec solution offers strong access control by ensuring VoIP users and devices are authenticated against existing AAA or two-factor authentication servers.

Ensure signaling and media privacy - Traffic that passes over an untrusted network is susceptible to reconnaissance activities such as sniffing and eavesdropping attacks. Encryption, using TLS for signaling traffic and SRTP for media traffic, must ensure privacy without compromising performance. With the Sipera UC-Sec appliances, internal phones, media gateways, conference bridges, and call servers do not require upgrades to support encryption natively because UC-Sec terminates encrypted traffic from the public Internet and sends unencrypted streams to the private enterprise intranet.

Ensure and monitor voice and video quality - Sipera's real-time UC-Sec appliances offer deterministic performance with delays for media packets measured in hundreds of microseconds (even when encryption is involved and call volume grows) while reporting VoIP quality metrics such as latency and jitter.

Simplify firewall/NAT traversal - Employee home routers and Wi-Fi hotspots are usually not under the control of enterprises, so enterprises must place a security appliance in their enterprise demilitarized zones to solve far-end firewall/NAT traversal issues for VoIP deployments. Sipera's UC-Sec solution simplifies near-end NAT traversal using static rules that do not require updates when changes occur in the enterprise VoIP network.

Threat Mitigation – UC-Sec detects and mitigates thousands of attacks and security threats based on the most advanced library of vulnerabilities.

2. General Test Approach and Test Results

The general test approach was to make calls through Sipera UC-Sec while DoS policies are in place using various codec settings and exercising common and advanced PBX features. Calls were made between the remote users and the main site, between the remote users and the PSTN via the main site PSTN gateway, and between the remote users. Different types of remote endpoints were also tested.

2.1. Interoperability Compliance Testing

The compliance testing tested interoperability between the Sipera UC-Sec and Avaya Aura® Session Manager and Avaya Aura® Communication Manager by making calls between remote users and users at the main site. The following specific SIP telephony functions were tested in the test environment set up for the compliance test:

- Successful registration of remote user SIP endpoints on Session Manager through Sipera UC-Sec.
- Calls from remote users with and without NAT to users at the main site via Sipera UC-Sec.
- Calls from users at the main site to remote users with and without NAT via Sipera UC-Sec.
- PSTN calls to/from remote users with and without NAT via Sipera UC-Sec.
- Calls between remote users with and without NAT via Sipera UC-Sec.
- Basic call scenarios using G.711 and G.729 codecs
- SIPING-19 supplementary call features (including Hold, Transfer, Conference, Bridged Calls, etc.)
- Advanced call features provided via Feature Name Extensions (FNE) on Communication Manager (such as Call Forwarding, Call Park, Call Pickup, Automatic Redial, Send All Calls, etc.)
- Verified Voicemail and Message Waiting Indicator (MWI) for both Communication Manager Messaging and Avaya Modular Messaging
- Validated that the Sipera UC-Sec preserves the Layer 2 & 3 QoS values marked by the Avaya IP Telephones.

2.2. Test Results

All feature functionality, serviceability, and performance passed all test cases described in **Section 2.1**. VoIP traffic and voice features worked properly while traversing the un-trusted network through the Sipera UC-Sec Secure Access Proxy.

2.3. Support

Technical support for Sipera Systems UC-Sec Secure Access Proxy:

- Phone: (866) 861-3113
- Email: support@sipera.com

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows several remote users connected by different means to the unprotected IP network to access the SIP infrastructure at a main enterprise site.

The main site has a simulated firewall at the edge of the network restricting unwanted traffic between the un-trusted network and the enterprise. Also connected to the edge of the main site is a Sipera UC-Sec. The public side of the Sipera UC-Sec is connected to the un-trusted network and the private side is connected to the trusted corporate LAN. The Sipera UC-Sec is assigned two IP addresses for the private interfaces and one for the public.

All SIP traffic between the remote endpoints and the enterprise site flows through the Sipera UC-Sec. In this manner, the Sipera UC-Sec can protect the main site's infrastructure from any SIP-based attacks. In addition, HTTP transfers required by the remote endpoints to gather licensing or configuration data, also passes through the Sipera UC-Sec. All other traffic bypasses the Sipera UC-Sec and flows directly between the un-trusted network and the private LAN of the enterprise if permitted by the data firewall.

The network diagram shown in **Figure 1** illustrates the network environment used for the compliance test. The network consists of an Avaya Aura® Telephony Infrastructure including Avaya Aura® Communication Manager running on an Avaya S8300 Server with an Avaya G450 Media Gateway, an Avaya S8800 server running Avaya Aura® Session Manager, an Avaya S8800 server running Avaya Aura® System Manager, Avaya Modular Messaging, multiple Avaya 9600 Series H.323 and SIP Telephones, one Avaya 2420 Digital Telephone, one Avaya Analog Telephone and one Sipera Systems UC-Sec Secure Access Proxy. An ISDN-PRI trunk connects the media gateway to the PSTN. A PSTN number assigned to the ISDN-PRI trunk at the main site is mapped to a telephone extension at the main site or to a remote telephone extension depending on the test cases being executed. One computer is present in the network providing network services such as Radius, DHCP, HTTP, and TFTP.

The SIP endpoints located at the main site are registered to Session Manager. All calls originating from Communication Manager at the main site and destined for the remote users will be routed through the on-site Session Manager to the Sipera UC-Sec, and across the un-trusted IP network.

The remote users are comprised of the following endpoints:

- Avaya 9600 Series IP Telephones (with SIP firmware) connected directly to the un-trusted network.
- Avaya 9600 Series IP Telephone (with SIP firmware) connected behind a Netscreen-5GT firewall (SIP ALG disable).

The voice communication across the untrusted network for the Avaya 9600 Series IP Telephones uses SIP over TLS.

The remote users register with Session Manager through the Sipera UC-Sec. These telephones use the public IP address of Sipera UC-Sec at the main site as their configured server. The Sipera UC-Sec will forward any registration messages it receives from the remote endpoints to Session Manager. Thus, the Sipera UC-Sec appears to the Session Manager as a set of SIP endpoints. All calls originating from the remote users are routed across the untrusted IP network, Sipera UC-Sec and Session Manager to Communication Manager at the main site.

All SIP telephones, both local and remote, use the HTTP server at the main site to obtain their configuration files. The Sipera UC-Sec will perform any address translation of private IP addresses in the configuration files before sending the files to the remote endpoints. All SIP endpoints that registered to SM via the Sipera UC-Sec were configured with a third party certificate via the 46xxsetiings file TRUSTCERTS parameter. SIP endpoints that registered directly to SM did not have the TRUSTCERTS parameter configured. All SIP endpoints, both local and remote use the same SIP domain: **dev4.com**.

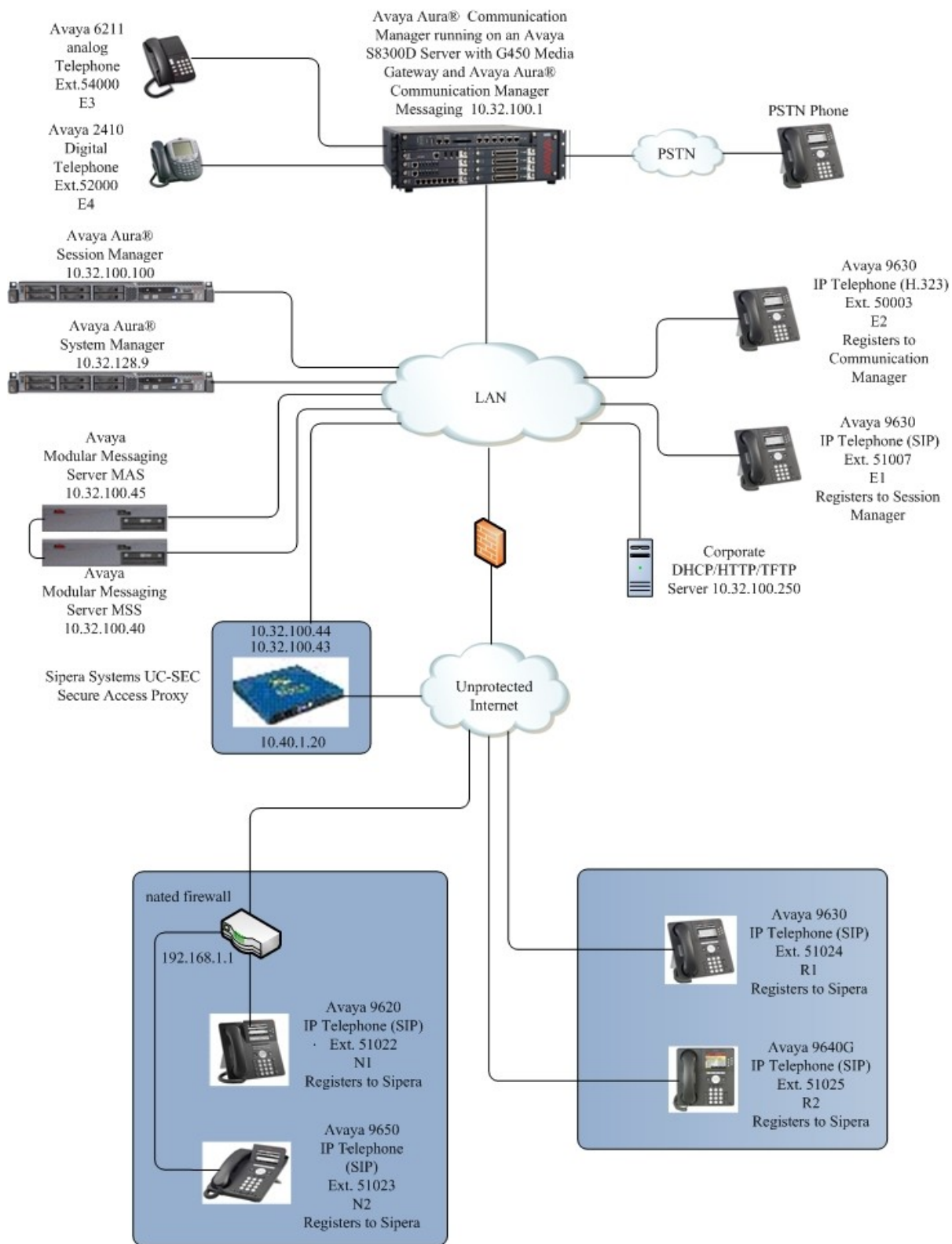


Figure 1: Avaya and Sipera Remote User Solution

4. Equipment and Software Validated

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

Equipment	Software/Firmware
<i>Avaya PBX Products</i>	
Avaya S8300 Server running Avaya Aura® Communication Manager	Avaya Aura® Communication Manager 6.0
Avaya G450 Media Gateway MGP MM712 DCP Media Module	30.13.2 HW9
<i>Avaya Aura® Session Manager</i>	
Avaya Aura® Session Manager	6.0
Avaya Aura® System Manager	6.0
<i>Avaya Messaging (Voice Mail) Products</i>	
Avaya Modular Messaging - Messaging Application Server (MAS)	5.2
Avaya Modular Messaging - Message Storage Server (MSS)	5.2
Avaya Aura® Communication Manager Messaging (CMM)	6.0
<i>Avaya Telephony Sets</i>	
Avaya 9600 Series IP Telephones	(H.323 3.1.1) and (SIP 2.6)
Avaya 2410 Digital Telephone	5.0
Avaya Analog Telephone	NA
<i>Sipera Systems Products</i>	
Sipera Systems UC-Sec Secure Access Proxy	v4.0 v4.0.4 (TLS Certificate Testing)
<i>Microsoft Products</i>	
DHCP/HTTP/TFTP Server	Microsoft Windows 2003 Server

5. Avaya Aura® Communication Manager and Avaya Aura® Session Manager

There is no Sipera UC-Sec specific configuration required on Avaya Aura® Communication Manager and Avaya Aura® Session Manager to support this solution. It is assumed that all Aura® Telephony components, appropriate licenses and authentication files have been configured already. Trunks, dial plans, etc., will not be covered in this document. For detailed information on the installation, maintenance, and configuration of Communication Manager and Session Manager, please references **Section 10, [1]** through **[3]**. Sections 5.1 and 5.2 are supplied for reference, no configuration is required.

5.1. Verify OPS and SIP Trunk Capacity

Using the SAT, verify that the Off-PBX Telephones (OPS) and SIP Trunks features are enabled on the **Optional Features** form. The license file installed on the system controls these options. If a required feature is not enabled, contact an authorized Avaya sales representative. On **Page 1**, verify that the number of OPS stations allowed in the system is sufficient for the number of SIP endpoints that will be deployed.

```
display system-parameters customer-options                               Page 1 of 11
                                OPTIONAL FEATURES

G3 Version: V16                                     Software Package: Enterprise
Location: 2                                          System ID (SID): 1
Platform: 28                                        Module ID (MID): 1

                                USED
                                Platform Maximum Ports: 6400 143
                                Maximum Stations: 2400 44
                                Maximum XMOBILE Stations: 2400 0
Maximum Off-PBX Telephones - EC500: 9600 5
Maximum Off-PBX Telephones - OPS: 9600 35
Maximum Off-PBX Telephones - PBFMC: 9600 0
Maximum Off-PBX Telephones - PVFMC: 9600 0
Maximum Off-PBX Telephones - SCCAN: 0 0
Maximum Survivable Processors: 313 0
```


5.2. Verify QoS on Communication Manager

IP networks were originally designed to carry data on a best-effort delivery basis, which meant that all traffic had equal priority and an equal chance of being delivered in a timely manner. As a result, all traffic had an equal chance of being dropped when congestion occurred. QoS is now utilized to prioritize VoIP traffic and should be implemented throughout the entire network.

In order to achieve prioritization of VoIP traffic, the VoIP traffic must be classified. The Avaya Aura® telephony infrastructure supports both IEEE 802.1p and DiffServ.

The DiffServ and 802.1p/Q values configured here will be downloaded to the Avaya H.323 IP wired and wireless Telephones via Communication Manager. Avaya SIP IP Telephones will get QoS settings by downloading the 46xxsettings file from the HTTP server (not shown in this document). For more information on QoS settings please refer to **Section 10**.

On **Page 1** of the **change ip-network-region** form, verify the Differentiated Services Code Points.

The Differentiated Services Code Point for **Call Control PHB Value** and **Audio PHB Value** are **46** and the **Call Control 802.1p Priority** and **Audio 802.1p Priority** are set to **6**.

```
change ip-network-region 1                                     Page 1 of 20
                                     IP NETWORK REGION
  Region: 1
Location:      Authoritative Domain: dev4.com
  Name: Main
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
Call Control PHB Value: 46
Audio PHB Value: 46
  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
```

5.3. Add SIP Users to Avaya Aura® Session Manager

Add SIP users corresponding to the remote users shown in **Figure 1**.

This section provides the procedures for configuring SIP users on the Session Manager.

Configuration is accomplished by accessing the browser-based GUI of Avaya Aura® System Manager using the URL “https://<ip-address>/SMGR”, where <ip-address> is the IP address of Avaya Aura® System Manager. Log in with the appropriate credentials.

To add new SIP users, expand **Users** and select **Manage Users** from left and select **New** button (not shown) on the right.

Enter values for the following required attributes for a new SIP user in the **General** section of the new user form.

- **Last Name:** Enter the last name of the user.
- **First Name:** Enter the first name of the user.

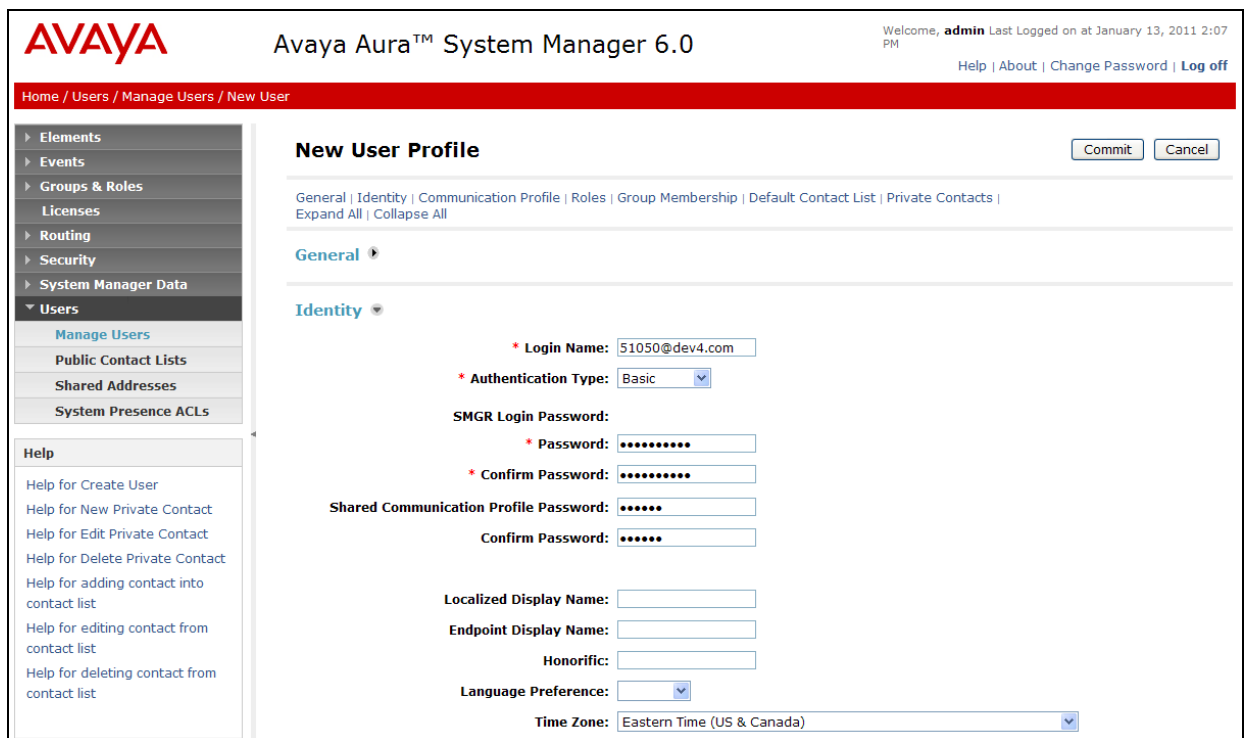
The screen below shows the information when adding a new SIP user to the sample configuration.

The screenshot displays the Avaya Aura System Manager 6.0 web interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura™ System Manager 6.0', and user information: 'Welcome, admin Last Logged on at January 13, 2011 2:07 PM'. A secondary navigation bar contains links for 'Help | About | Change Password | Log off'. The main content area has a breadcrumb trail: 'Home / Users / Manage Users / New User'. On the left, a sidebar menu shows various system components, with 'Users' expanded and 'Manage Users' selected. The main panel is titled 'New User Profile' and features a tabbed interface. The 'General' tab is active, showing input fields for 'Last Name' (containing 'Sipera'), 'First Name' (containing 'Sipera'), 'Middle Name', and 'Description'. 'Commit' and 'Cancel' buttons are located at the top right of the form.

Enter values for the following required attributes for a new SIP user in the **Identity** section of the new user form.

- **Login Name:** Enter `<extension>@<sip domain>` of the user (e.g., 51050@dev4.com).
- **Authentication Type:** Select *Basic*.
- **SMGR Login Password:** Enter the password which will be used to log into System Manager.
- **Confirm Password:** Re-enter the password from above.
- **Shared Communication Profile Password:** Enter the password that will be used by the SIP phone to log into Session Manager.
- **Confirm Password:** Re-enter the password from above.

The screen below shows the information when adding a new SIP user to the sample configuration.



The screenshot displays the 'New User Profile' form in the Avaya Aura System Manager 6.0 interface. The form is organized into several sections, with the 'Identity' section currently expanded. The 'General' section includes a 'Login Name' field with the value '51050@dev4.com' and an 'Authentication Type' dropdown set to 'Basic'. The 'SMGR Login Password' section contains 'Password' and 'Confirm Password' fields, both masked with dots. The 'Shared Communication Profile Password' section also has 'Password' and 'Confirm Password' fields, also masked. Below these are fields for 'Localized Display Name', 'Endpoint Display Name', 'Honorific', 'Language Preference' (a dropdown menu), and 'Time Zone' (set to 'Eastern Time (US & Canada)'). The left sidebar shows a navigation menu with options like 'Elements', 'Events', 'Groups & Roles', 'Licenses', 'Routing', 'Security', 'System Manager Data', and 'Users'. The top of the page shows the Avaya logo, the product name 'Avaya Aura™ System Manager 6.0', and a welcome message for the user 'admin'.

Scroll down to the **Communication Profile** section and select **New** to define a **Communication Profile** for the new SIP user. Enter values for the following required fields:

- **Name:** Enter name of communication profile.
- **Default:** Select field to indicate that this is the default profile.

Click **New** to define a **Communication Address** for the new SIP user. Enter values for the following required fields:

- **Type:** Select *Avaya SIP*.
- **Fully Qualified Address:** Enter extension number and select SIP domain.

The screen below shows the information when adding a new SIP user to the sample configuration. Click **Add**.

The screenshot displays the Avaya SIP user configuration interface. On the left is a sidebar with a 'Users' section containing 'Manage Users', 'Public Contact Lists', 'Shared Addresses', and 'System Presence ACLs'. Below this is a 'Help' section with links for creating, editing, and deleting users and contacts. The main content area is titled 'Identity' and contains three sections: 'Communication Profile', 'Communication Address', and a table for 'Communication Address' records. The 'Communication Profile' section has buttons for 'New', 'Delete', 'Done', and 'Cancel'. It shows a table with one record named 'Primary' and a 'Select : None' dropdown. Below this, the 'Name' field is set to 'Primary' and the 'Default' checkbox is checked. The 'Communication Address' section has buttons for 'New', 'Edit', and 'Delete'. It shows a table with columns 'Type', 'Handle', and 'Domain', and a message 'No Records found'. Below this, the 'Type' dropdown is set to 'Avaya SIP' and the 'Fully Qualified Address' field is set to '51050' with a domain dropdown set to 'dev4.com'. At the bottom right are 'Add' and 'Cancel' buttons.

Name
Primary

Select : None

* Name: Primary

Default : ☒

Type	Handle	Domain
No Records found		

Type: Avaya SIP

* Fully Qualified Address: 51050 @ dev4.com

Add Cancel

In the *Session Manager* section, configure the following:

- **Primary Session Manager:** Dev4 SM was used for testing
- **Origination Application Sequence:** DEV4 EVO was used for testing
- **Termination Application Sequence:** DEV4 EVO was used for testing
- **Home Location:** Dev4 Infrastructure was used for testing

Manage Users

Public Contact Lists

Shared Addresses

System Presence ACLs

Help

Help for Create User

Help for New Private Contact

Help for Edit Private Contact

Help for Delete Private Contact

Help for adding contact into contact list

Help for editing contact from contact list

Help for deleting contact from contact list

Communication Profile

New Delete Done Cancel

Name

Primary

Select : None

* Name:

Primary

Default :

☒

Communication Address

New Edit Delete

<input type="checkbox"/>	Type	Handle	Domain
<input type="checkbox"/>	Avaya SIP	51050	dev4.com

Select : All, None

☒ Session Manager Profile

* Primary Session Manager

Dev4 SM

Primary	Secondary	Maximum
39	0	39

Secondary Session Manager

(None)

Primary	Secondary	Maximum
---------	-----------	---------

Origination Application Sequence

DEV4 EVO

Termination Application Sequence

DEV4 EVO

Survivability Server

(None)

* Home Location

Dev4 Infrastructure

In the **Endpoint Profile** section, fill in the following fields:

- **System:** Select the managed element corresponding to Communication Manager.
- **Use Existing Endpoints:** If field is not selected, the station will automatically be added in Communication Manager.
- **Extension:** Enter extension number of SIP user.
- **Template:** Select template for type of SIP phone.
- **Port:** Enter *IP*.
- **Delete Endpoint on Unassign of Endpoint:** Enable field to automatically delete station when **Station Profile** is un-assigned from user.

Select **Commit** to complete the SIP user configuration. Repeat **Section 5.3** for each desired SIP user.

The screen below shows the information when adding a new SIP user to the sample configuration.

The screenshot displays a web-based configuration interface for a SIP user. The 'Endpoint Profile' section is active, indicated by a checked checkbox and a dropdown arrow. Below this, several fields are visible: 'System' is a dropdown menu set to 'Dev4-AACM'; 'Use Existing Endpoints' is an unchecked checkbox; 'Extension' is a text field containing '51050' with an 'Endpoint Editor' button to its right; 'Template' is a dropdown menu set to 'DEFAULT_9640SIP_CM_6_0'; 'Set Type' is a text field containing '9640SIP'; 'Security Code' is an empty text field; 'Port' is a text field containing 'IP' with a magnifying glass icon to its left; and 'Voice Mail Number' is an empty text field. Below these fields, the 'Delete Endpoint on Unassign of Endpoint from User' checkbox is checked. A horizontal separator line follows. Below the separator, the 'Messaging Profile' section is shown with an unchecked checkbox and a dropdown arrow. Further down, there are four expandable sections: 'Roles', 'Group Membership', 'Default Contact List', and 'Private Contacts', each with a dropdown arrow. At the bottom left, a legend indicates that an asterisk (*) denotes a required field. At the bottom right, there are 'Commit' and 'Cancel' buttons.

☒ Endpoint Profile ▾

* System Dev4-AACM ▾

Use Existing Endpoints ☐

* Extension 51050 Endpoint Editor

* Template DEFAULT_9640SIP_CM_6_0 ▾

Set Type 9640SIP

Security Code

* Port IP

Voice Mail Number

Delete Endpoint on Unassign of Endpoint from User ☒

☐ Messaging Profile ▾

Roles ▾

Group Membership ▾

Default Contact List ▾

Private Contacts ▾

* Required

Commit Cancel

6. Configure the Avaya SIP Telephones

The Avaya IP SIP telephones at the main site will register to Avaya Aura® Session Manager. The Avaya IP SIP telephones of the remote users will use the mapped public IP address of Sipera UC-Sec as the SIP server.

The tables below shows an example of the SIP telephone network settings for both the main site and the remote users. For complete details on configuring a specific endpoint type refer to **Section 10**. The Avaya SIP endpoints that directly register to the Avaya SM and to Avaya SM via the Sipera UC-Sec use different 46xxsetiings files. The 46xxsetiings file used for SIP endpoints registered to Avaya SM via the Sipera UC-Sec use the TRUSTCERTS parameter to download the third party certificate to the Avaya SIP endpoints.

Avaya IP Telephones at Main Site

	Main Site (9600 SIP)	Main Site (9600 H.323)
Extension	51007	50003
IP Address	10.32.75.100	10.32.75.101
Subnet Mask	255.255.255.0	255.255.255.0
SIP/H.323 Server	10.32.100.100	10.32.100.1
Router	10.32.75.254	10.32.75.254
File Server	10.32.100.250	10.32.100.250

Remote Avaya IP Telephones Using NAT

	Remote User N1 with NAT (9600 SIP)	Remote User N2 with NAT (9600 SIP)
Extension	51022	55023
IP Address	192.168.1.50	192.168.1.51
Subnet Mask	255.255.255.0	255.255.255.0
SIP Server	10.40.1.20	10.40.1.20
Router	192.168.1.1	192.168.1.1
File Server	10.32.100.250	10.32.100.250

Remote Avaya IP Telephones NO NAT

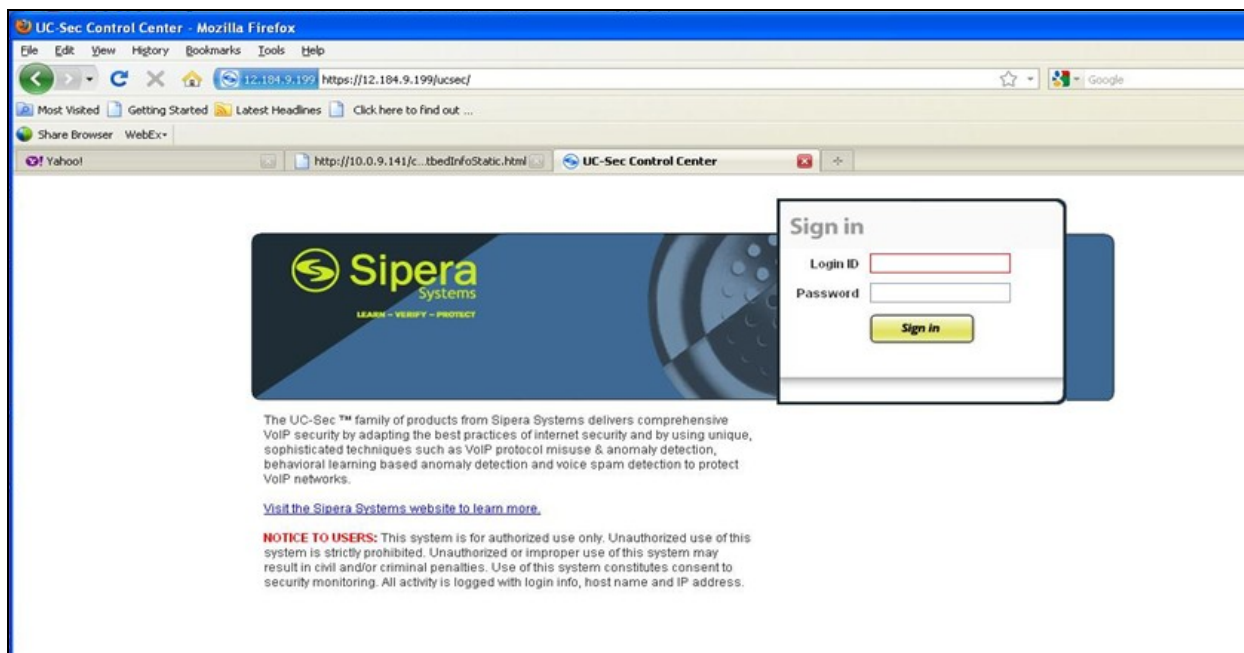
	Remote User R1 with NAT (9600 SIP)	Remote User R2 with NAT (9600 SIP)
Extension	51024	51025
IP Address	192.168.1.50	192.168.1.51
Subnet Mask	255.255.255.0	255.255.255.0
SIP Server	10.40.1.20	10.40.1.20
Router	192.168.1.1	192.168.1.1
File Server	10.40.1.20	10.40.1.20

7. Configure Sipera UC-Sec Secure Access Proxy

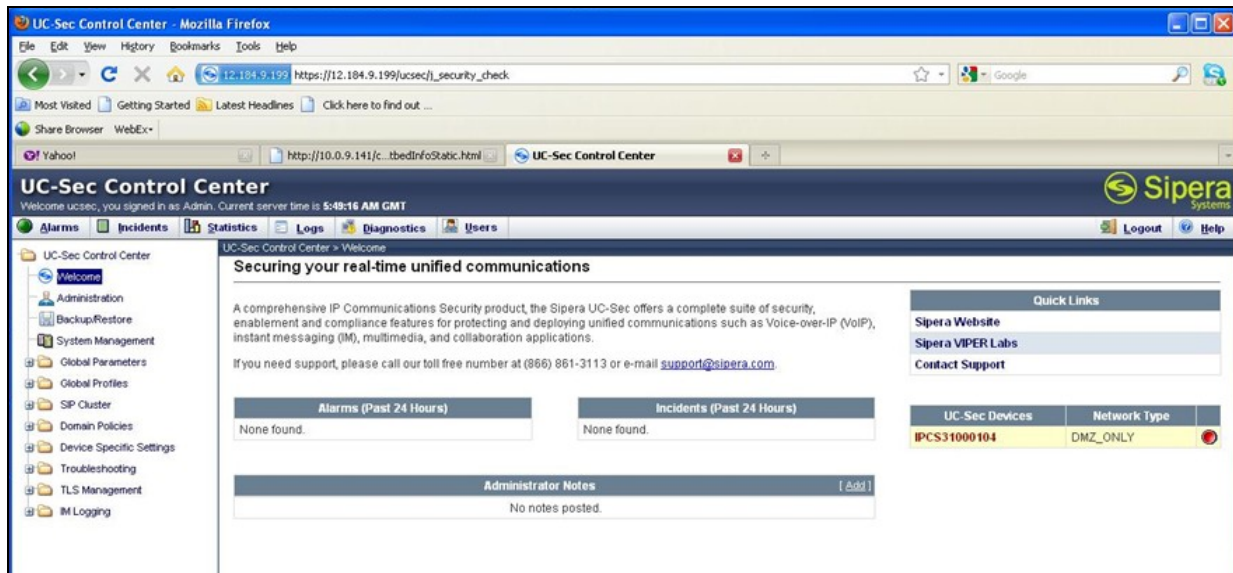
This section covers the configuration of the Sipera UC-Sec. It is assumed that the UC-Sec software has already been installed. For additional information on these configuration tasks, refer to **Section 10**, [9] and [10].

Use a WEB browser to access the UC-Sec web interface, enter `https://<ip-addr>/ucsec` in the address field of the web browser, where `<ip-addr>` is the management LAN IP address of UC-Sec.

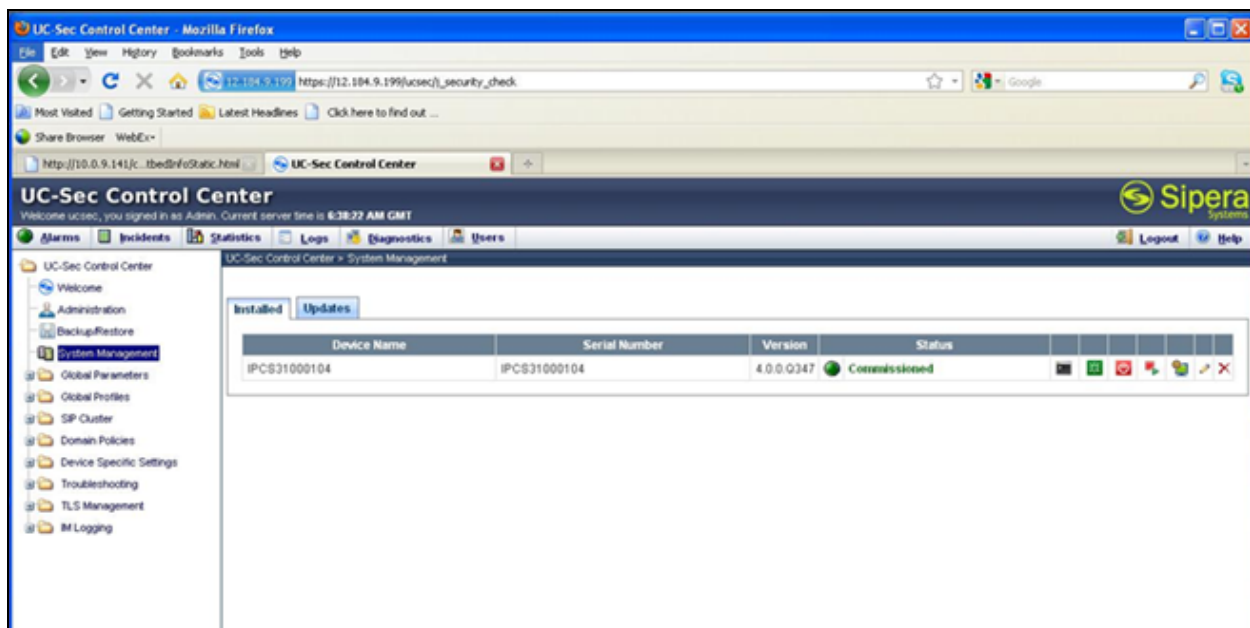
Log in with the appropriate credentials. Click **Sign In**.



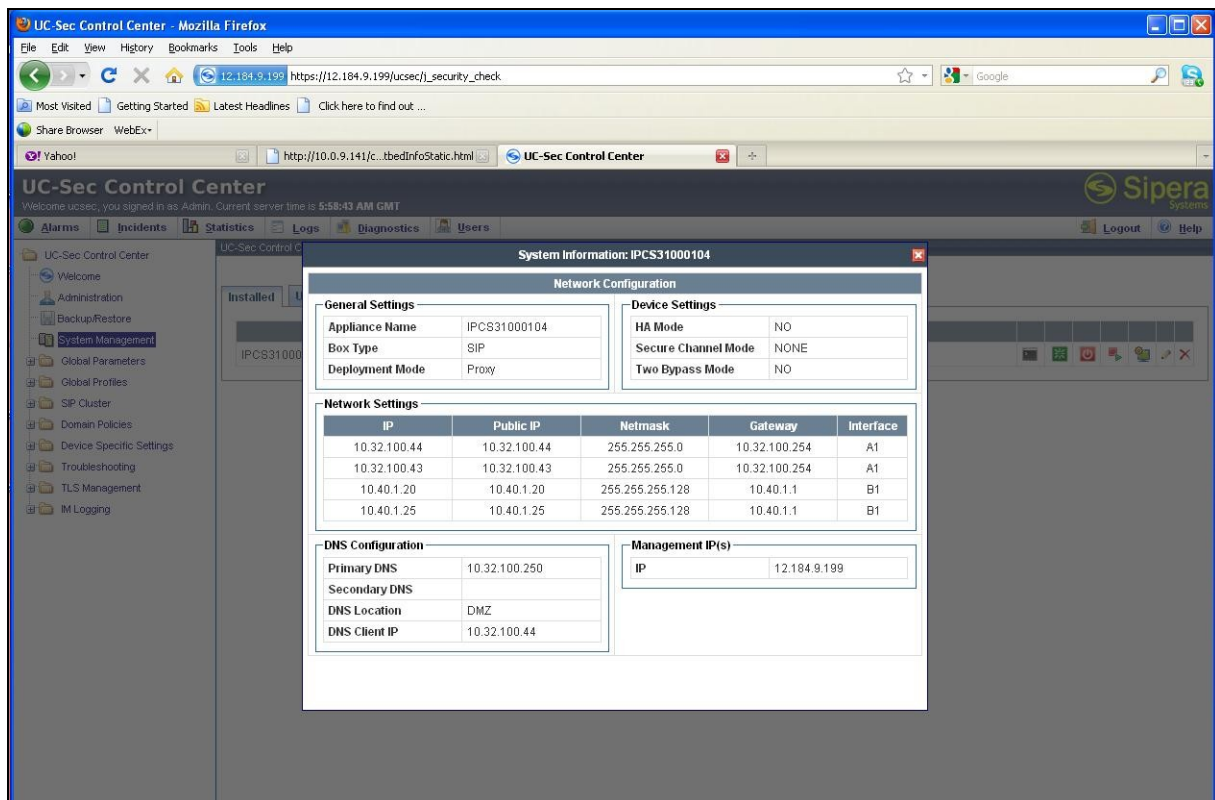
Step 2: The main page of the UC-Sec Control Center is displayed.



Step 3: To view system information that was configured during installation, navigate to **UC-Sec Control Center → System Management**. A list of installed devices is shown in the right pane. In the case of the compliance test, a single device named **IPCS310** is shown. To view the configuration of this device, click the monitor icon (the third icon from the right for the **IPCS310** device entry).



Step 4: The **System Information** screen shows the **Network Settings**, **DNS Configuration** and **Management IP** information provided during installation and corresponds to **Figure 1**. The compliance test did not use a DNS server, but an entry was required by UC-Sec. An arbitrary IP address was used for the **Primary DNS** field. The **Box Type** was set to **SIP** and the **Deployment Mode** was set to **Proxy**. Default values were used for all other fields.



Step 5: Signaling Interface

A signaling interface is created that maps a signaling interface name to an IP address and a set of ports and transport protocols that can be used on that interface.

To define a new signaling interface, navigate to **UC-Sec Control Center → Device Specific Settings → Signaling Interface**. Select the UC-Sec device name from the middle pane. Select the **Add Signaling Interface** button in the right pane. A new page is opened (not shown) where the new information can be entered and submitted.

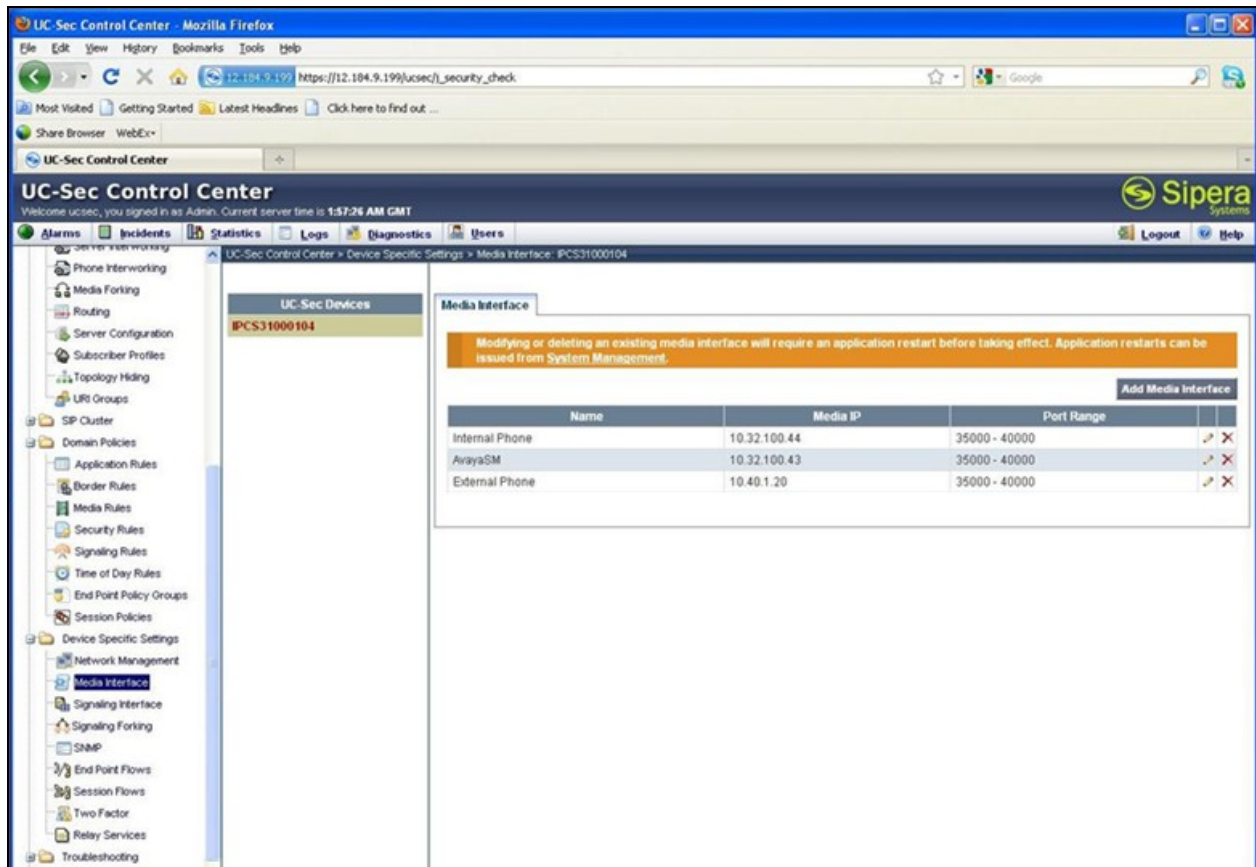
The example below shows two interfaces created for the compliance test, one for each of the IP addresses assigned to UC-Sec. The interface named **External phone** supports TLS. The **Avaya SM** interface supports TCP and/or UDP.

The screenshot shows the UC-Sec Control Center web interface in a Mozilla Firefox browser. The page title is "UC-Sec Control Center" and the URL is "https://12.104.9.199/ucsec/_security_check". The interface includes a navigation menu on the left with categories like "Alarms", "Incidents", "Statistics", "Logs", "Diagnostics", and "Users". The main content area is divided into two panes. The left pane, titled "UC-Sec Devices", lists "IPCS31000104". The right pane, titled "Signaling Interface", contains a table with two rows: "AvayaSM" and "External phone". The table has columns for Name, Signaling IP, TCP Port, UDP Port, TLS Port, and TLS Profile. An "Add Signaling Interface" button is located at the top right of the table.

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile
AvayaSM	10.32.100.43	5060	---	---	None
External phone	10.40.1.20	5060	5060	5061	signalling

Step 6: Media Interface

A media interface maps a media interface name to an IP address and a range of ports that can be used on that interface. Navigate to **UC-Sec Control Center → Device Specific Settings → Media Interface**. The settings used by the compliance test are shown below.



The screenshot shows the UC-Sec Control Center web interface in a Mozilla Firefox browser. The address bar shows the URL https://12.184.9.199/ucsec/_security_check. The page title is "UC-Sec Control Center" and the Siper Systems logo is in the top right. The left sidebar contains a navigation menu with categories like "Phone Interworking", "Routing", "Server Configuration", "Domain Policies", "Device Specific Settings", and "Troubleshooting". The "Media Interface" option under "Device Specific Settings" is selected. The main content area shows the "Media Interface" configuration for device "IPCS31000104". A warning message states: "Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management." Below this is a table with columns "Name", "Media IP", and "Port Range".

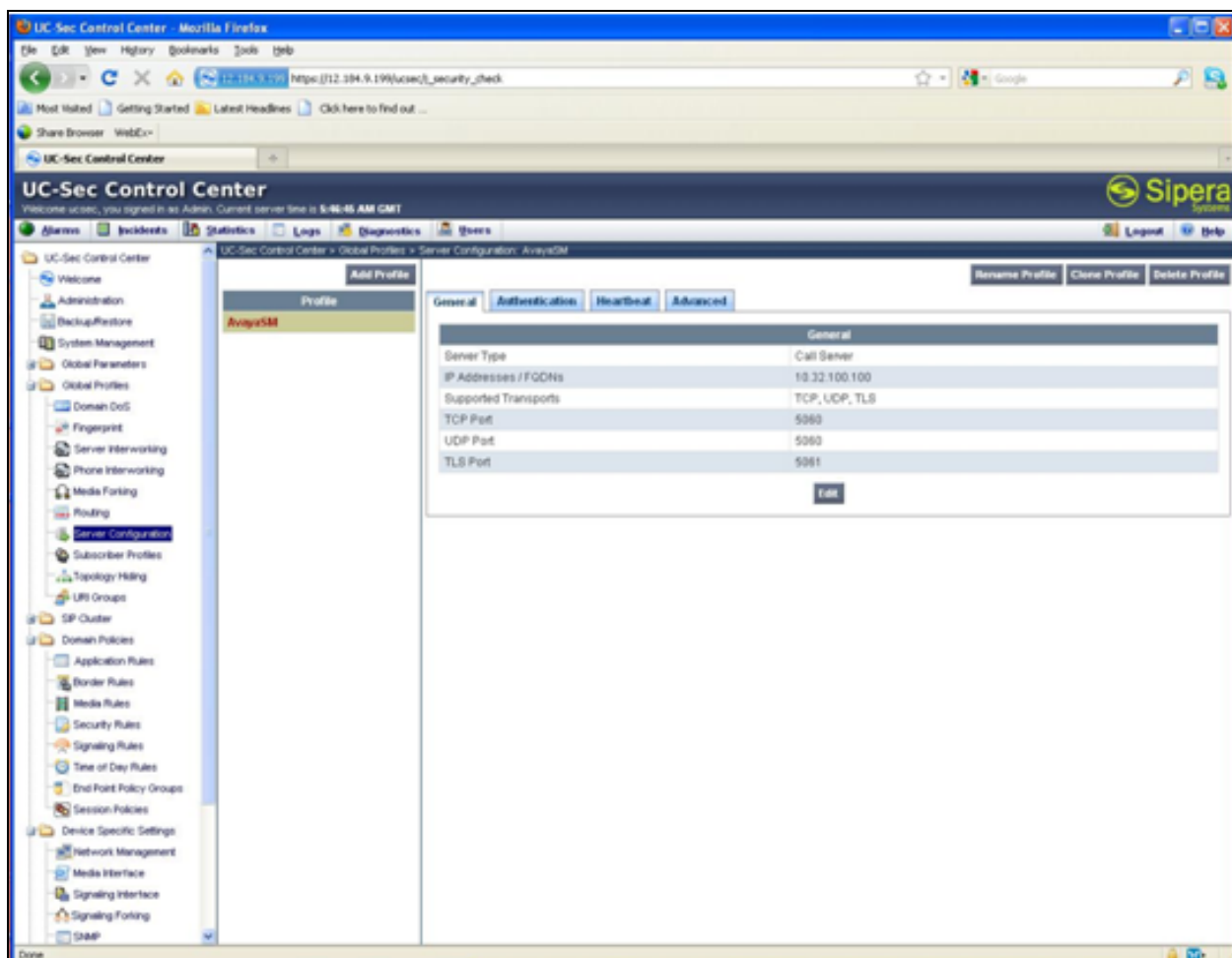
Name	Media IP	Port Range
Internal Phone	10.32.100.44	35000 - 40000
AvayaSM	10.32.100.43	35000 - 40000
External Phone	10.40.1.20	35000 - 40000

Step 7: Server Definition – General

A server configuration profile is created to define the characteristics of the Session Manager 6.0 to which the UC-Sec will communicate.

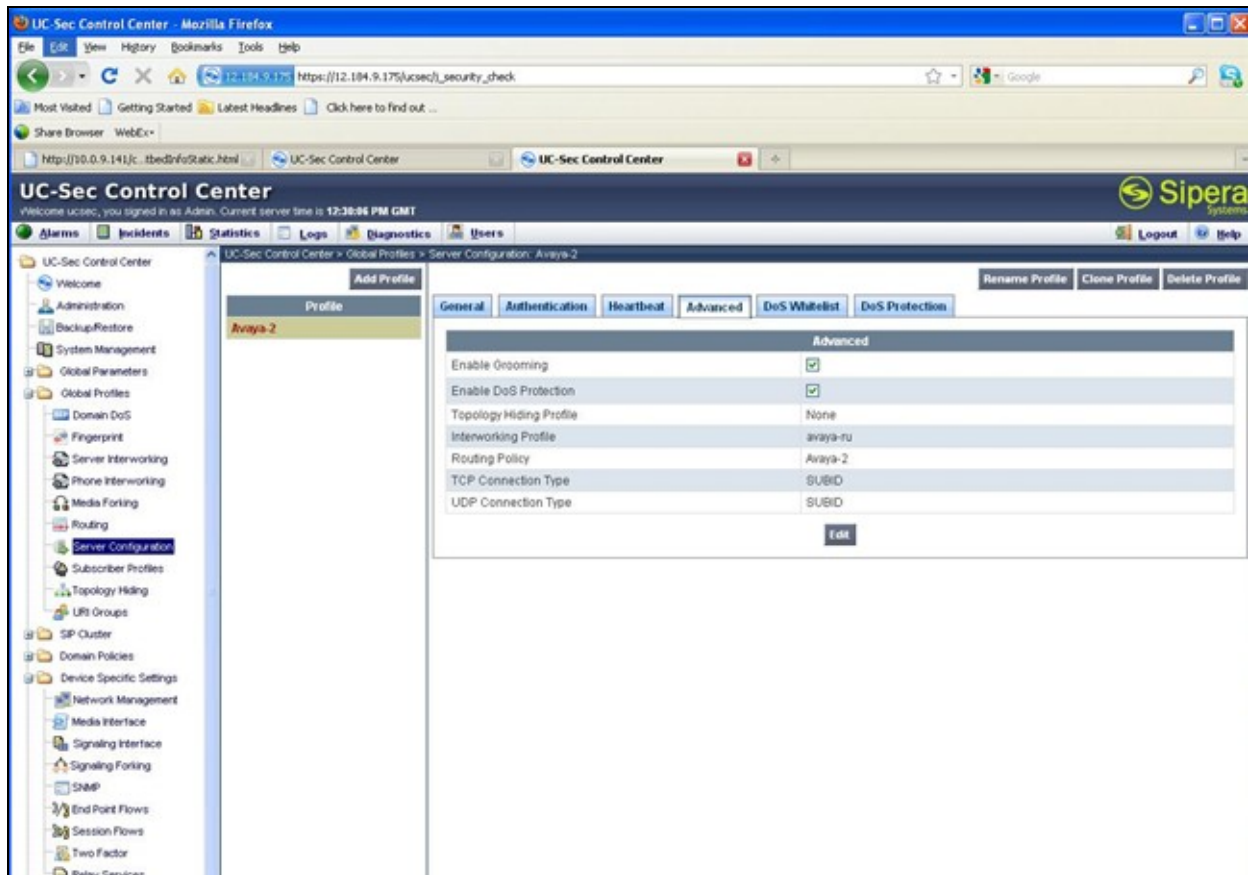
To define a new server configuration profile, navigate to **UC-Sec Control Center → Global Profiles → Server Configuration**. Select the **Add Profile** button in the middle pane to enter and submit the new information.

The example below shows the server configuration profile named **AvayaSM**, which was used for the compliance test. The General tab shows the **Server Type** as **Call Server** and the IP of the Session Manager SIP signaling interface (**10.32.100.100**) in the **IP Addresses/FQDNs** field. The remaining fields show the transport protocols and ports supported for traffic between UC-Sec and Session Manager.



Step 8: Server Definition – Advanced

On the **Advanced** tab, profiles are specified that will be applied to traffic between the UC-Sec and this server (Session Manager). The **Interworking** profiles are applied to traffic from the UC-Sec to the server and the Routing profile is applied to traffic to the UC-Sec from the server. These profiles, **Interworking** and **Routing**, are described in **Steps 9-10**. Grooming is also activated since the Session Manager only supports up to 6 TCP connections from different ports from the same IP address.



Step 9: Server – Interworking Profile

Server Interworking profile defines how SIP message headers and content (other than the IP addresses) may be manipulated for interoperability with different call servers.

To define a new interworking profile, navigate to **UC-Sec Control Center → Global Profiles → Server Interworking**. Select the **Add Profile** button in the middle pane to enter and submit the new information.

In the example below, multiple profiles are shown in the middle pane. Only the profile named **avaya-ru** was used for the compliance test. By highlighting this profile in the middle pane, its details are shown in the right pane. On the **Advanced** tab, **Hold Support** was changed to RFC2543 for interworking with the gateway used for testing with Analog and Digital phone (not shown). Default values were used for all other fields.

The screenshot displays the UC-Sec Control Center web interface. The left sidebar shows a navigation tree with 'Server Interworking' selected. The middle pane lists several interworking profiles: 'cs2100', 'avaya-ru' (highlighted), 'OCS-Edge-Server', 'cisco-ccm', 'cups', 'Sipera-Halo', and 'OCS-FrontEnd-Server'. The right pane shows the configuration details for the 'avaya-ru' profile, with the 'Advanced' tab selected. A warning message at the top of the right pane states: 'It is not recommended to edit the defaults, improper configuration will prevent Easy Config from working properly.'

General	
Hold Support	RFC2543
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261

Privacy	
Privacy Enabled	No
User Name	
P-Asserted-Identity	No
P-Preferred-Identity	No
Privacy Header	

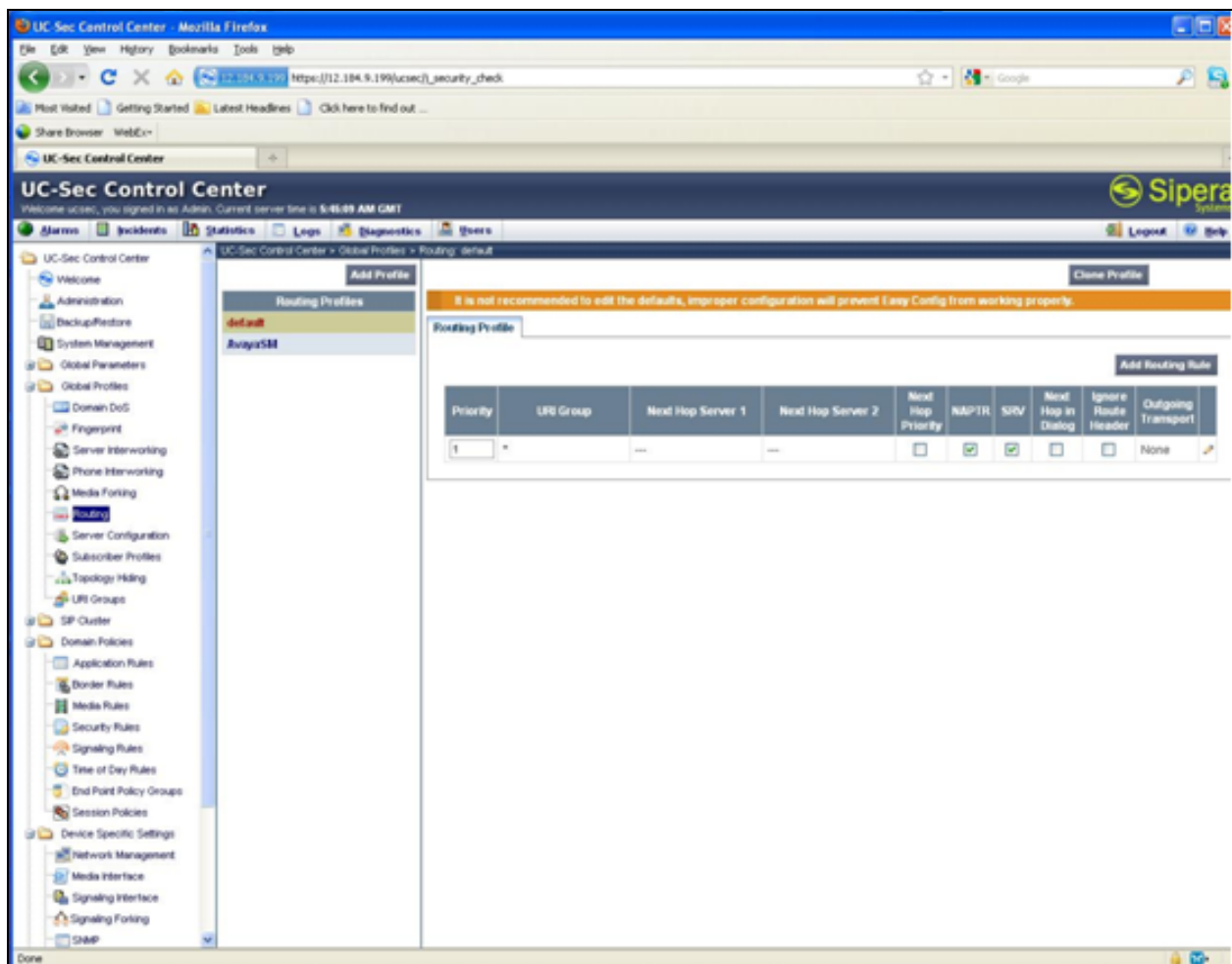
DTMF	
DTMF Support	None

Step 10: Server – Routing Profile

A routing profile defines how a call is to be routed. In this case, the routing profile is applied to calls from the server to UC-Sec.

To define a new routing profile, navigate to **UC-Sec Control Center → Global Profiles → Routing**. Select the **Add Profile** button in the middle pane to enter and submit the new information.

In the example below, two profiles are shown in the middle pane. Only the profiles named **default** and **AvayaSM** were used for the compliance test. By highlighting a profile in the middle pane, its details are shown in the right pane. The **AvayaSM** routing profile is described in **Step 17**. The **default** profile is shown below. The **default** profile is for routing traffic from the server destined for one of the remote endpoints. Thus, the routing profile is for all URI Groups (**URI Group = ***) and no server IP address is specified in **Next Hop Server 1** or **Next Hop Server 2** fields. To locate the destination address, the UC-Sec will use its internal database to identify the IP address associated with the destination extension in the SIP message.

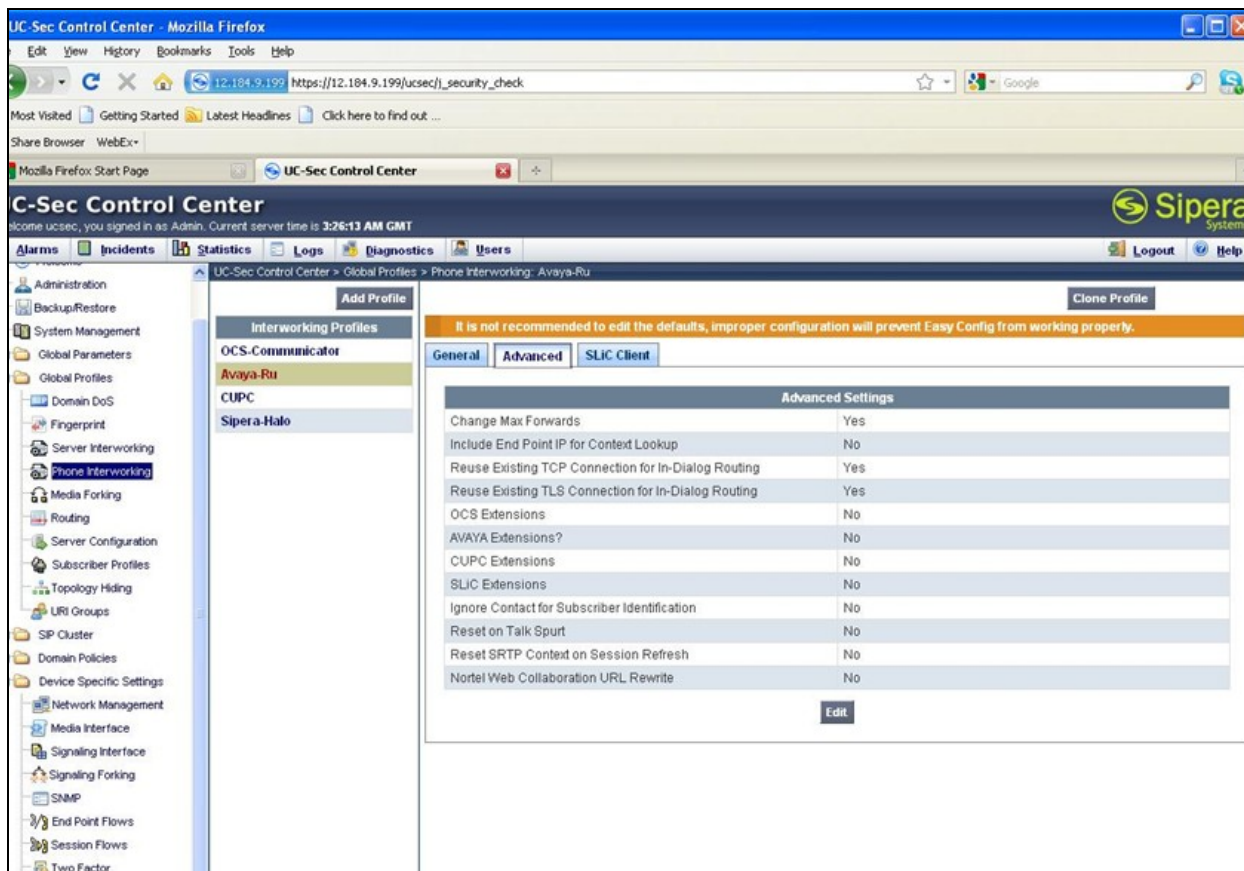


Step 11: Phone- Interworking Profile

Phone Interworking profile defines how the interoperability with a Call Server provides features applicable to phones. This profile is used in End Point Subscriber Flow configuration (**Step 15**).

To define the **Phone- Interworking Profile**, navigate to **UC-Sec Control Center → Global Profiles → Phone Interworking**

In the example below, four profiles are shown in the middle pane. Only the profile named **Avaya-Ru** was used for the compliance testing. In this profile, **Reuse Existing TCP Connection for In-Dialog Routing** and **Reuse Existing TLS Connection for In-Dialog Routing** were set to **Yes** to enable Avaya phones with TCP and TLS support at the remote side for reliable connection (TCP) and connection optimization (TLS). Click “Edit” and check the above two parameters, select **Finish** to continue (not shown).

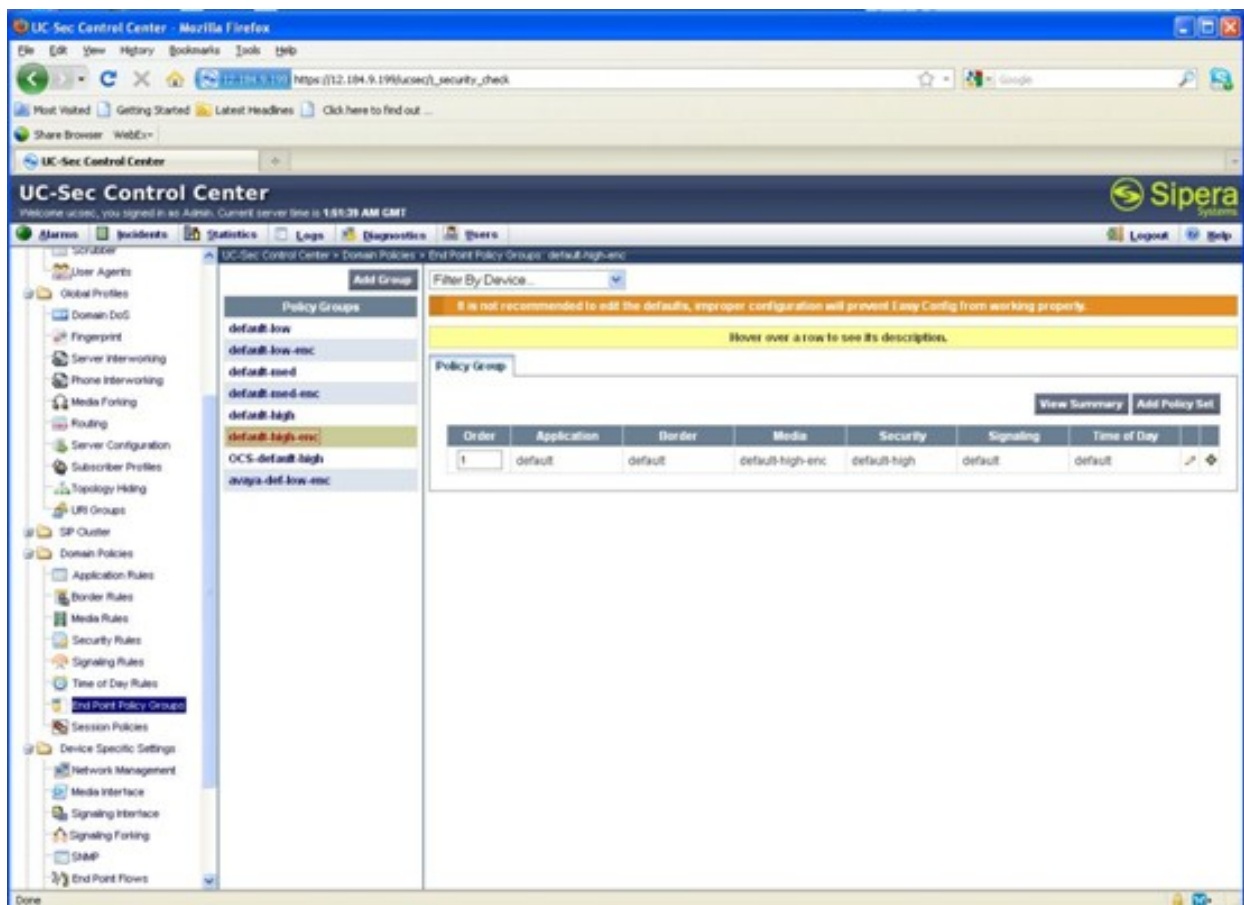


Step 12: End Point Policy Groups

An end point policy group defines a set of rules that may be applied to different aspects of the data traffic. For the compliance test, the end point policy group was used to specify if (and how) the media stream should be encrypted and the security level.

To define a new policy group, navigate to **UC-Sec Control Center → Domain Policies → End Point Policy Groups**. Select the **Add Group** button in the middle pane to enter and submit the information.

For the compliance test, only the **default-high-enc** and **default-low** groups were used. Policy group **default-high-enc** defines the use of encrypted media (SRTP). Policy group **default-low** defines the use of unencrypted media (RTP, if SRTP is not needed). The details on the media can be obtained by clicking the Media link in the Policy Group displays shown below. These policy groups will be used in the server and subscriber flows defined in the following steps (Steps 14-15).



The screenshot shows the UC-Sec Control Center web interface in a Mozilla Firefox browser. The page title is "UC-Sec Control Center" and the URL is "https://12.194.9.196/ucsec/_security_check". The interface is divided into a sidebar on the left and a main content area on the right. The sidebar contains a tree view of navigation options, including "Domain Policies" and "End Point Policy Groups". The main content area displays the "End Point Policy Groups" configuration page. It includes a "Filter By Device" dropdown, a list of policy groups, and a detailed view of the "default-high-enc" group. The detailed view shows a table with columns for Order, Application, Border, Media, Security, Signaling, and Time of Day. The table contains one row for the "default-high-enc" group.

Order	Application	Border	Media	Security	Signaling	Time of Day
1	default	default	default-high-enc	default-high	default	default

Step 13: End Point Policy Groups – Continued

Click the **default-low** policy group from the middle panel, the details of this policy group will be shown in the right panel. Policy group **default-low** defines the use of unencrypted media (RTP).

The screenshot shows the UC-Sec Control Center web interface in a Mozilla Firefox browser. The interface has a left sidebar with a tree view of navigation options. The main content area is divided into a middle panel and a right panel. The middle panel lists several policy groups, with 'default-low' selected. The right panel displays the details for the 'default-low' policy group, including a table with columns for Order, Application, Border, Media, Security, Signaling, and Time of Day.

UC-Sec Control Center - Mozilla Firefox

https://12.184.9.199/ucsec/it_security_check

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 7:40:59 AM GMT

Navigation: Home, Incidents, Statistics, Logs, Diagnostics, Users

Left Sidebar:

- UC-Sec Control Center
 - Welcome
 - Administration
 - Backup/Restore
 - System Management
 - Global Parameters
 - Global Profiles
 - SP Cluster
 - Domain Policies
 - Application Rules
 - Border Rules
 - Media Rules
 - Security Rules
 - Signaling Rules
 - Time of Day Rules
 - End Point Policy Groups**
 - Session Policies
 - Device Specific Settings
 - Network Management
 - Media Interface
 - Signaling Interface
 - Signaling Parking
 - SNMP
 - End Point Flows
 - Session Flows
 - Two Factor
 - Refer Services

Middle Panel: Policy Groups

- default-low
- default-low-enc
- default-med
- default-med-enc
- default-high
- default-high-enc
- OCS-default-high
- avaya-def-low-enc

Right Panel: Policy Group details for 'default-low'

Filter By Device: [v]

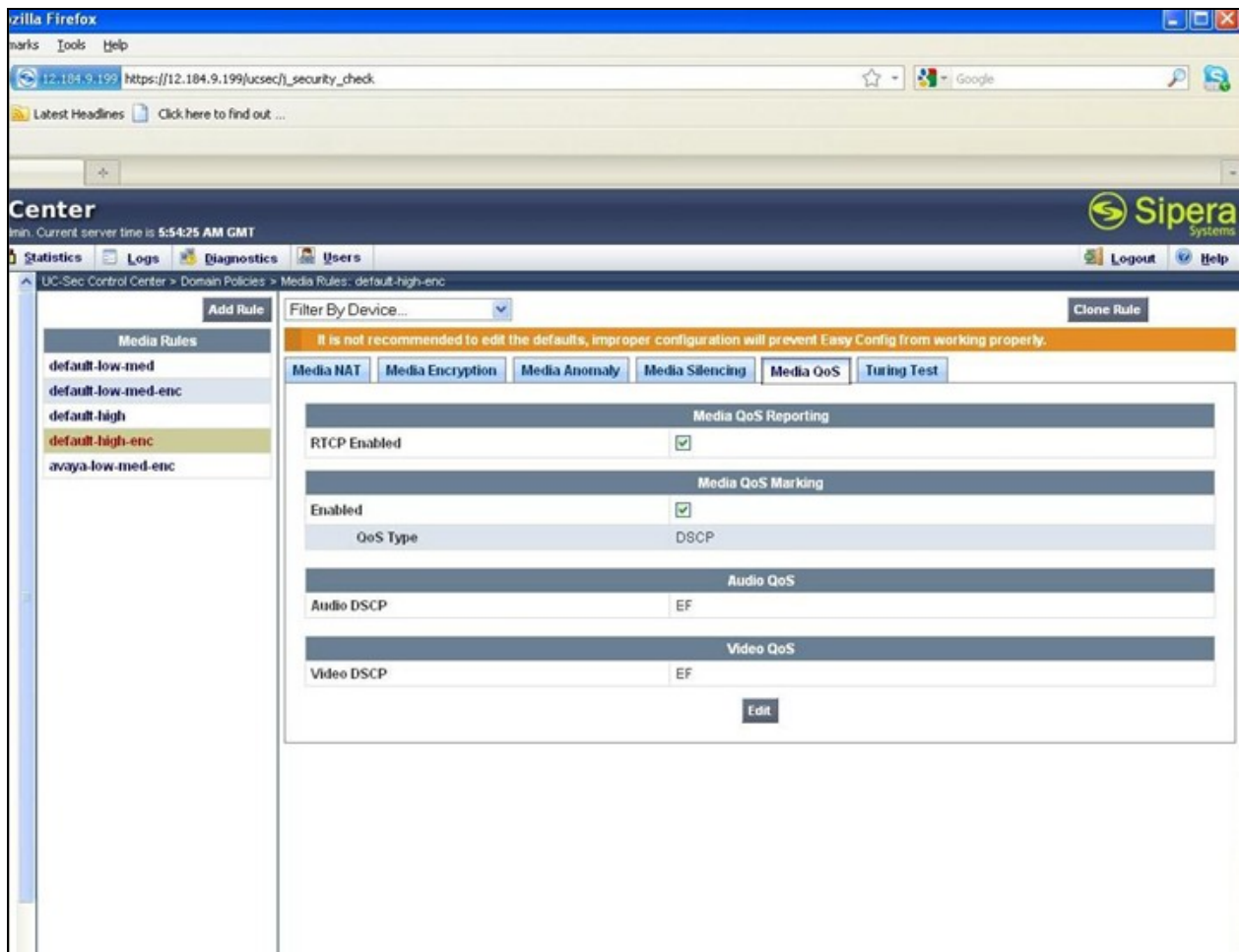
It is not recommended to edit the defaults, improper configuration will prevent Easy Config from working properly.

Hover over a row to see its description.

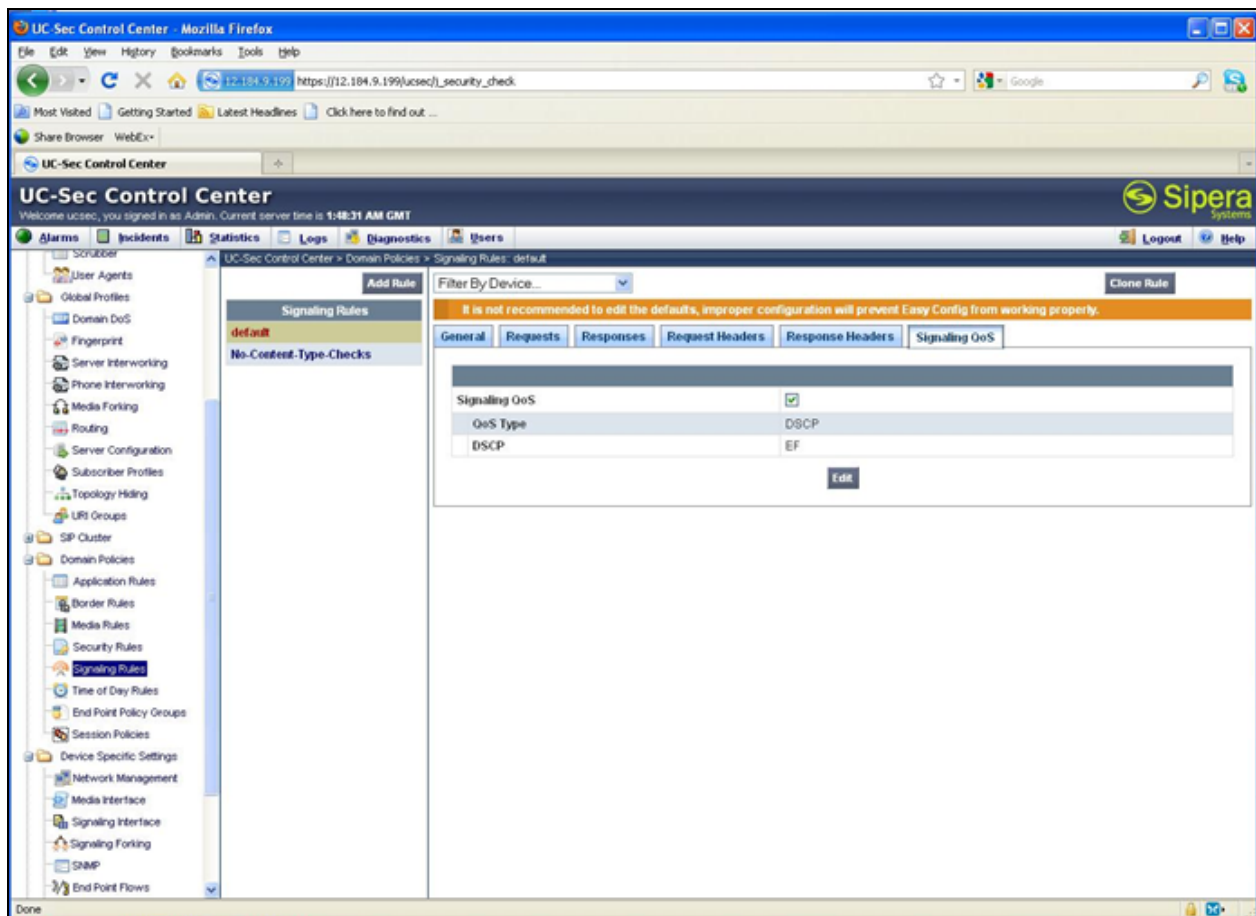
View Summary Add Policy Set

Order	Application	Border	Media	Security	Signaling	Time of Day
1	default	default	default-low-med	default-low	default	default

For compliance testing, media QoS was enabled. To enable media QoS, navigate to **UC-Sec Control Center → Domain Policies → Media Rules → default-high-enc**. Select **Media QoS** from the right panel. Click **Edit** and check the checkboxes under the title **Media QoS Reporting** and “**Media QoS Marking**”. Choose **DSCP**, and use default value (i.e. **EF**). Select **Finish** to continue (not shown).



For compliance testing, Signaling QoS was enabled. To enable signaling QoS, navigate to **UC-Sec Control Center** → **Domain Policies** → **Signaling Rules** → **default**, select **Signaling QoS** from the right pane. Select **Edit** and check the **Signaling QoS** checkbox. Change the **QoS Type** to **DSCP**, set the Value as default (i.e. **EF**). Select **Finish** to continue (not shown).

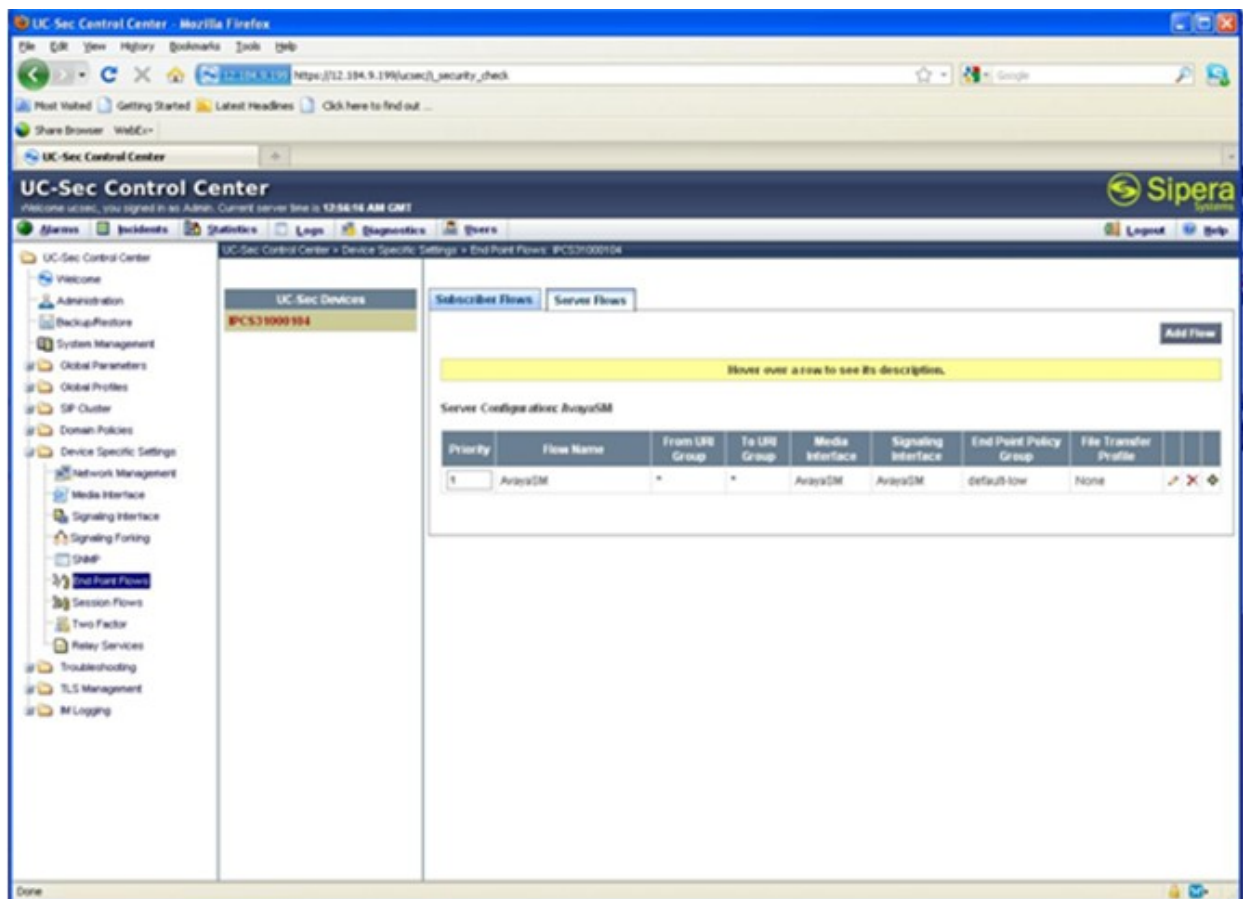


Step 14: Server Flow

Many of the previous steps have defined policies that will be applied to traffic if it is present. The server flow defines what traffic is actually allowed between the UC-Sec and the specified server, as well as which interfaces and media encryption will be used.

To define a new server flow, navigate to **UC-Sec Control Center → Device Specific Settings → Endpoint Flows**. Select the **Server Flows** tab. Select the **Add Flow** button in the right pane to enter and submit the new information.

The example below shows one server flow used for the compliance test. It specifies that all traffic to or from any URI Group will be allowed to the server named **AvayaSM** (Session Manager 6.0). Media traffic will use **Media Interface – AvayaSM (Step 6)** and signaling traffic will use **Signaling Interface – AvayaSM (Step 5)**. The **Endpoint Policy Group** named **default-low** (Step 13) will be applied to this traffic which specifies that the media is unencrypted.



Step 15: Subscriber Flows

A subscriber flow defines what traffic is allowed between the UC-Sec and the specified endpoints in much the same way the server flow defines the traffic allowed between the UC-Sec and the server.

To define a new subscriber flow, navigate to **UC-Sec Control Center → Device Specific Settings → Endpoint Flows**. Select the **Subscriber Flows** tab. Select the **Add Flow** button in the right pane to enter and submit the new information.

Three subscriber flows were created for the compliance test. If the traffic does not match the first flow, then the next flow in the list will be tested until a match is found. The detailed matching criteria are shown in **Step 17**. The **Endpoint Policy Group** named **default-high-enc** (**Step 13**) will be applied to this traffic which specifies that the media is encrypted. The second flow will match all traffic from the remote Avaya IP Telephones. Again the **Endpoint Policy Group** named **default-high-enc** (**Step 13**) will be applied to this traffic which specifies that the media is also encrypted. To see the complete details of a flow, click the monitor icon associated with the flow of interest in the right pane.

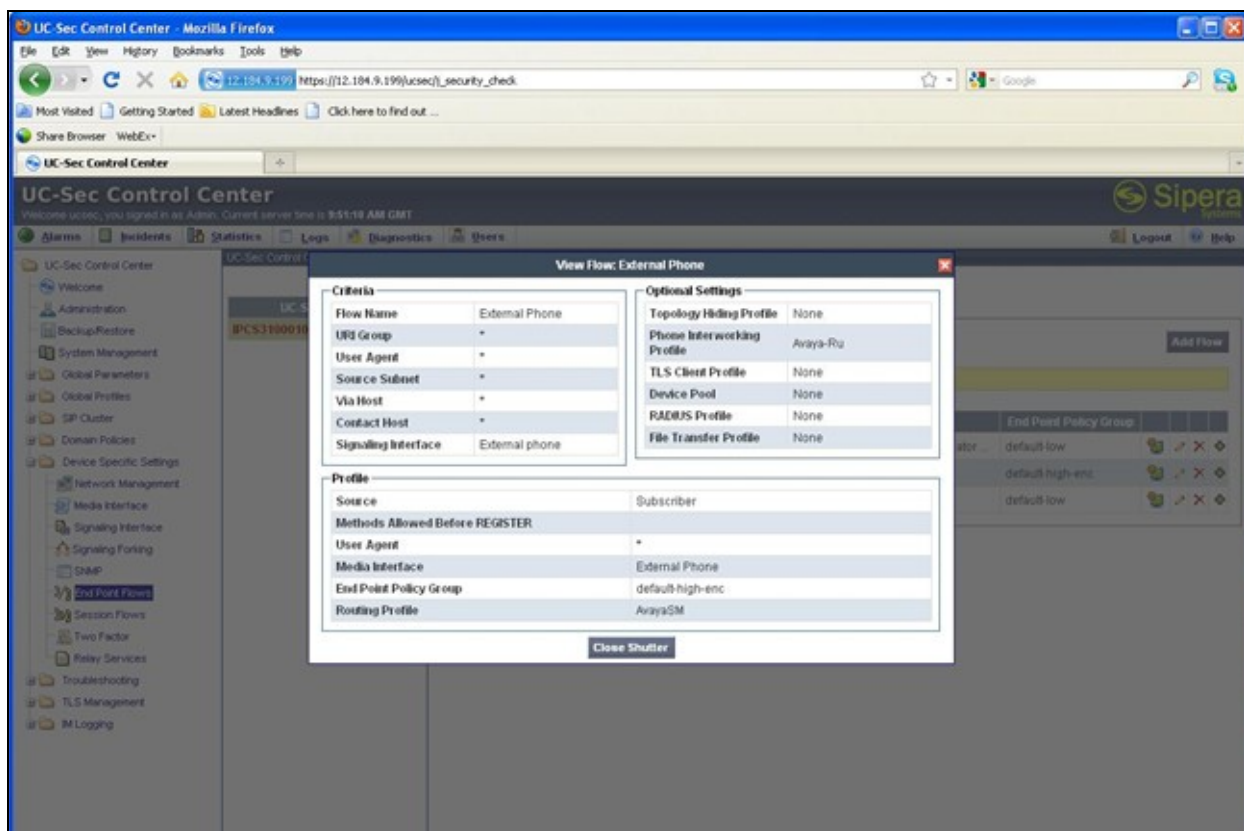
The screenshot shows the UC-Sec Control Center web interface in a Mozilla Firefox browser. The address bar shows the URL https://12.184.9.175/ucsecj_security_check. The page title is "UC-Sec Control Center". The navigation menu on the left includes: Welcome, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, SIP Cluster, Domain Policies, Device Specific Settings (selected), Network Management, Media Interface, Signaling Interface, Signaling Forking, SNMP, End Point Flows (selected), Session Flows, Two Factor, Relay Services, Troubleshooting, TLS Management, and IM Logging. The main content area is titled "UC-Sec Control Center > Device Specific Settings > End Point Flows: IPCS31000154". It has two tabs: "Subscriber Flows" (selected) and "Server Flows". Below the tabs are buttons for "Update Order" and "Add Flow". A yellow banner says "Hover over a row to see its description." Below this is a table with the following data:

Priority	Flow Name	URI Group	Source Subnet	User Agent	End Point Policy Group			
1	avaya-soft-phone	*	*	Avaya one-X Deskphone	default-high-enc			
2	External Phone	*	*	*	default-high-enc			

Step 16: Subscriber Flow – Details

The example below shows the details of the second flow, **External Phone**, in the list in **Step 15**. Select the **Monitor** icon, (not shown), for the second flow. Unlike the server flow, parameters such as **Topology Hiding Profile** and **Routing Profile** are defined within the subscriber flow itself. For the server traffic, these parameters were not defined in the flow but were defined in the server configuration.

This flow will match traffic from the remote Avaya 9600 Series IP Telephones since the **Signaling Interface** field is set to **External Phone** (Step 5) in the **Criteria** section. Media traffic will use **Media Interface – External Phone** (Step 6). The **End Point Policy Group** used is **default-high-enc** (Step 13). The **Phone Interworking Profile** used is **Avaya-Ru** (Step 11). The **Routing Profile** used is **AvayaSM** (Step 17).

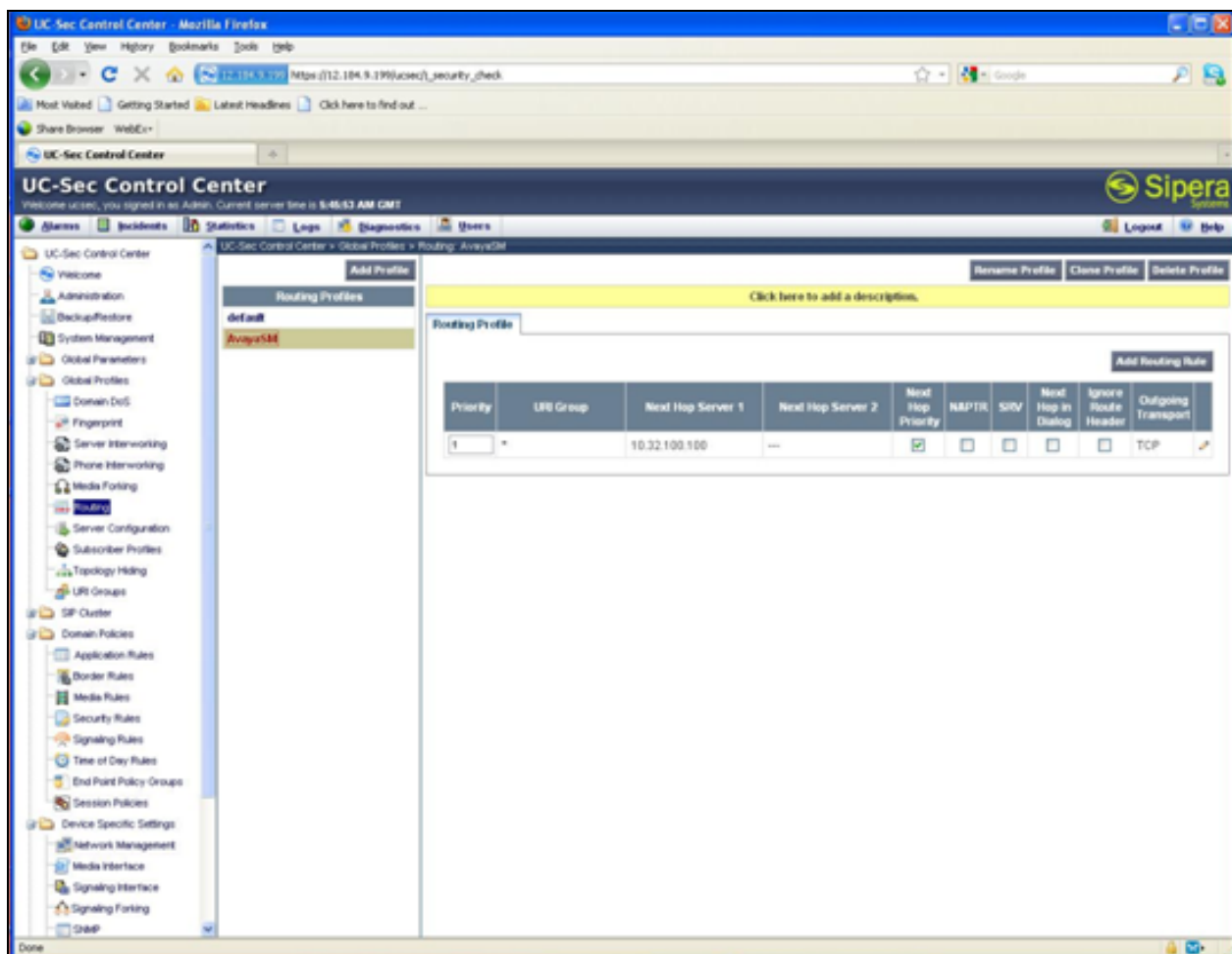


Step 17: Subscriber – Routing Profile

A routing profile defines how a call is to be routed. In this case, the routing profile is applied to calls from the subscriber to UC-Sec.

To define a new routing profile, navigate to **UC-Sec Control Center → Global Profiles → Routing**. Select the **Add Profile** button in the middle pane to enter and submit the new information.

The example below shows the routing profile named **AvayaSM** used by all the subscriber flows defined in **Steps 15-16**. It shows that all traffic (**URI Group = ***) using this profile will be routed to IP address 10.32.100.100 (Session Manager 6.0) as the next hop as defined in the **Next Hop Server 1** field.



Step 18: SIP Clusters

As part of the compliance test, SIP clusters were used to define how HTTP/HTTPS traffic will be routed for different groups of endpoints. For compliance test, HTTPS was used. Example shows configuration for both HTTP/HTTPS.

To define a new cluster, navigate to **UC-Sec Control Center → SIP Cluster**. Select the **Add Cluster** button in the middle pane to enter and submit the new information.

The cluster used for the compliance test is shown in the middle pane. By highlighting a profile in the middle pane, its details are shown in the right pane. The example below shows the cluster named **AvayaCluster**. It defines that HTTP/HTTPS traffic from the **Device IP 10.40.1.20** will be routed out the **Configuration Server Client Address 10.32.100.43** to the internal HTTP server address **10.32.100.100** as specified in the **Real IP** field. This enables the remote Avaya IP Telephones to get their configuration data via the UC-Sec.

The screenshot displays the UC-Sec Control Center web interface in a Mozilla Firefox browser. The interface is divided into three main panes. The left pane shows a navigation tree with categories like Administration, System Management, Global Profiles, and SIP Clusters. The middle pane, titled 'SIP Clusters', lists 'AvayaCluster' and has an 'Add Cluster' button. The right pane shows the configuration details for 'AvayaCluster' under the 'General' tab. It includes sections for 'Device Information', 'Configuration Servers', and 'Signaling Servers'.

Device Information

Device Name	IPCS31000104
Device IP	10.40.1.20
Configuration Server Client Address	10.32.100.43

Configuration Servers

Type	Port	Real IP	Real Port	Relay?	Rewrite URL?	Server TLS Profile
HTTPS	443	10.32.100.100	443	---	---	Mtpo-b1
HTTP Proxy	800	10.32.100.250	80	No	No	---
HTTP Server	80	10.32.100.250	80	No	---	---

Signaling Servers

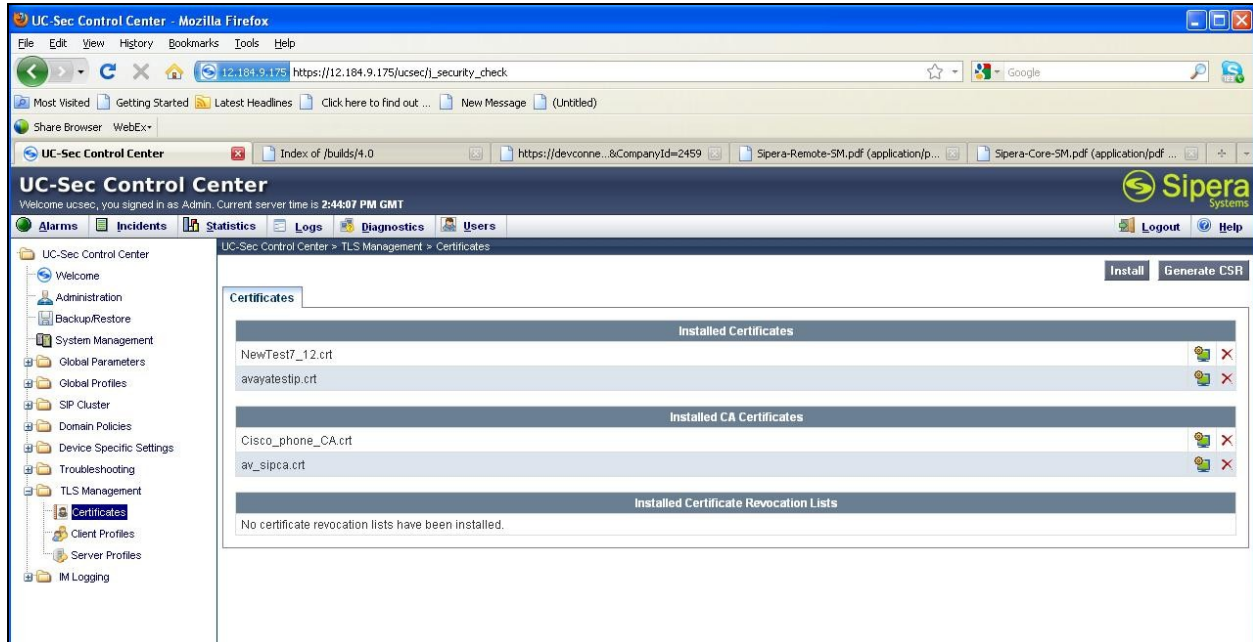
Server Configuration Profile	End Point Signaling Interface	Session Policy Group
AvayaSM	External phone	default

Step 19: TLS Certificate

A TLS certificate is used for establishing TLS connection between Avaya phones/clients and Sipera UC-Sec. Below are the two certificates that were used for TLS authentication:

1. Using a third party certificate, configure the TRUSTCERTS option in Avaya 46xxsettings file to include this certificate. Upload its corresponding root CA (Certificate Authority) certificate to the http/https server (For details how to configure TRUSTCERTS and upload the corresponding root CA certificate to http/https server, please reference to **Section 10, [1]** through **[3]**).
2. Using a root CA certificate from Avaya Aura® Session Manager. (Obtain the CA certificate from Avaya) and install it on the Sipera UC-Sec

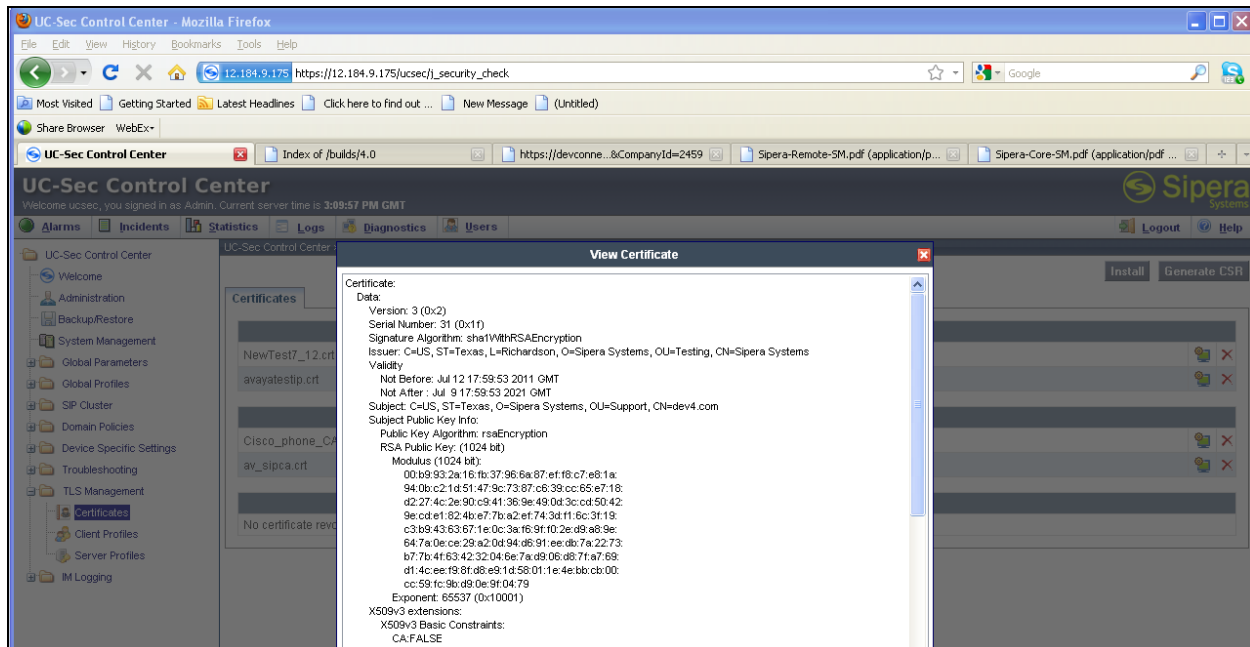
To look at the details of the certificate, navigate to **UC-Sec Control Center → TLS management → Certificates**. The example below shows the two TLS certificates named *NewTest7_12.crt* and *avayatestip.crt*. *NewTest7_12.crt* is the one used for setting up TLS for signaling message between the Avaya phones and the Sipera UC-Sec. (*avayatestip.crt*, on the other hand, is used to set up the HTTPS connection between the Avaya phones to the Sipera UC-Sec, used in step 18). The CA certificate, *av_sipca.crt*, is the one extracted from Session Manager and is used to authenticate the certificate provided from the phones.



Step 20: TLS Certificate – Continued

Press the **View** button to show details of the certificate.

The example below is for *NewTest7_12.crt*. This certificate was generated at Sipera, and its corresponding root CA certificate (*sipera-ca.crt*) is uploaded to the Avaya http/https server, so that the Avaya phone will download this root CA certificate during the Session Manager PPM process and use it to authenticate this server certificate.



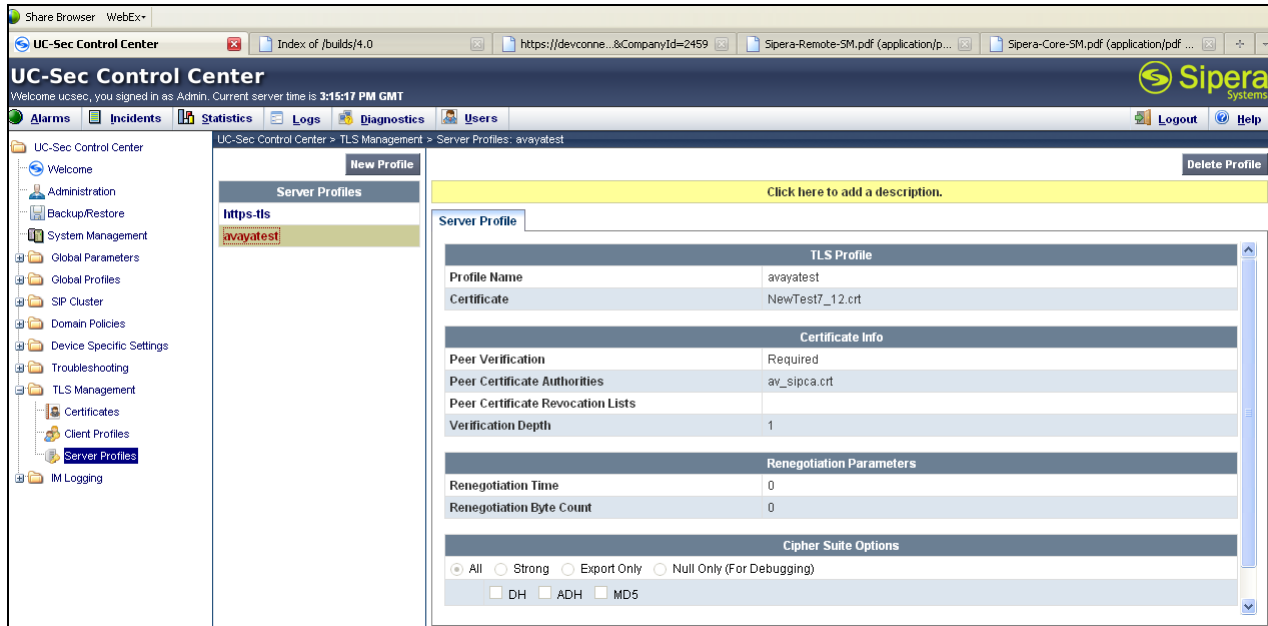
To install a 3rd party certificate, click the **Install** button (not shown). Then choose the certificate file and key file stored in the desktop and click the **Upload** button (not shown). This will allow the certificate to upload to EMS. Additional commands must be run to download these certificates to the Sipera UC-Sec. Please refer to UC-Sec Administration Guide [10].

After installing the certificate, navigate to **UC-Sec Control Center → TLS management → Server Profiles**, and select **New Profile**. Include the certificate (*NewTest7_12.crt*) and root CA certificate (*sipera-ca.crt*) that has been installed, and select **Finish**. Use this certificate server profile in the appropriate signaling interface (for TLS).

Also install another certificate and TLS server profile using the above steps. Then navigate to **UC-Sec Control Center → SIP Cluster → Cluster Proxy → <name of the SIP cluster> → Primary**, and under the **Configuration Servers**, add the HTTPS server, and include this new TLS server profile. This is used for HTTPS connection (**step 18**).

Step 21: TLS Certificate – Continued

As mentioned in above step, a certificate server profile needs to be created to include the above certificates, as show below.

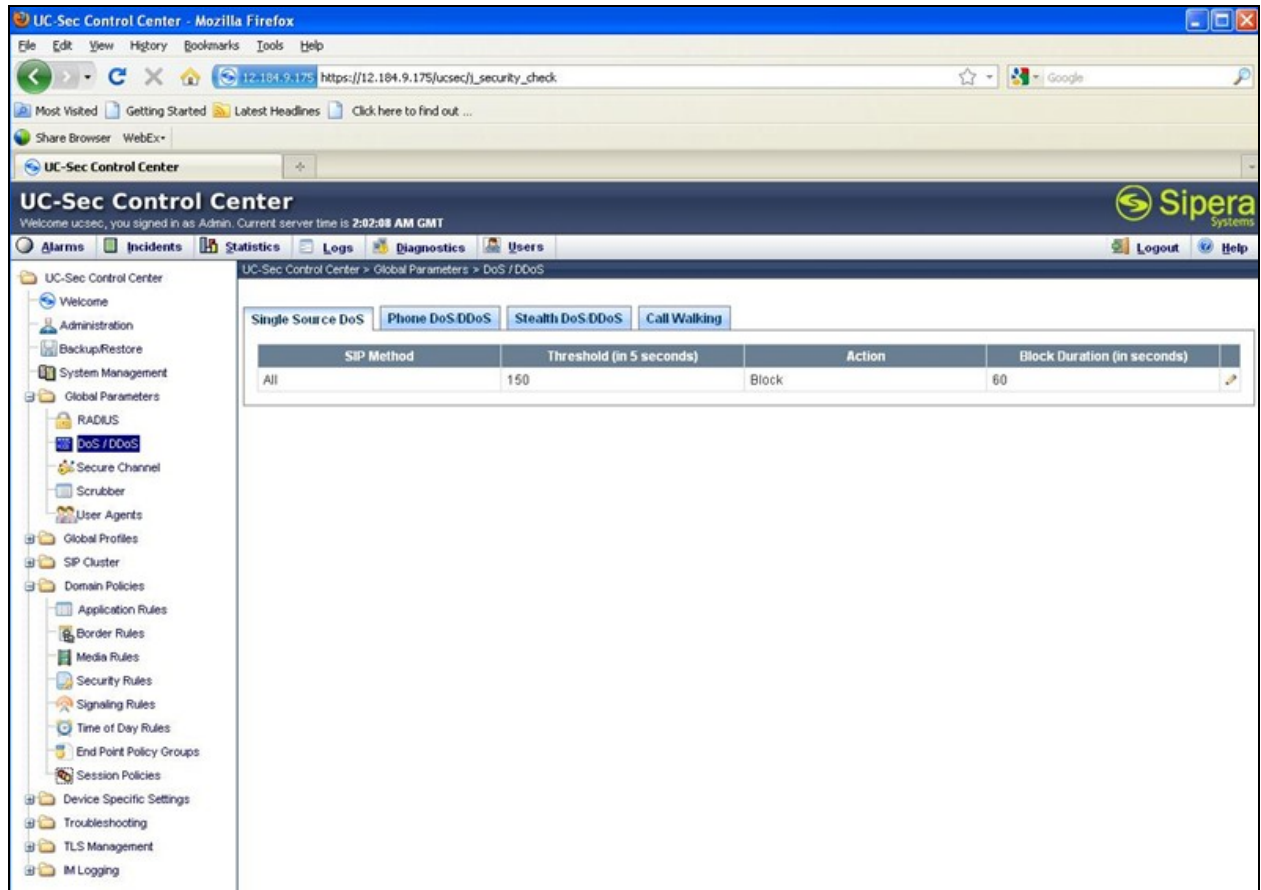


This server profile contains the server certificate *NewTest7_12.crt*, as well as the root CA certificate *av-sipca.crt*. Together they will be used to setup a TLS connection between Avaya phones and UC-Sec with mutual authentication.

This certificate server profile should be incorporated into signaling interface, as in **Step 5**.

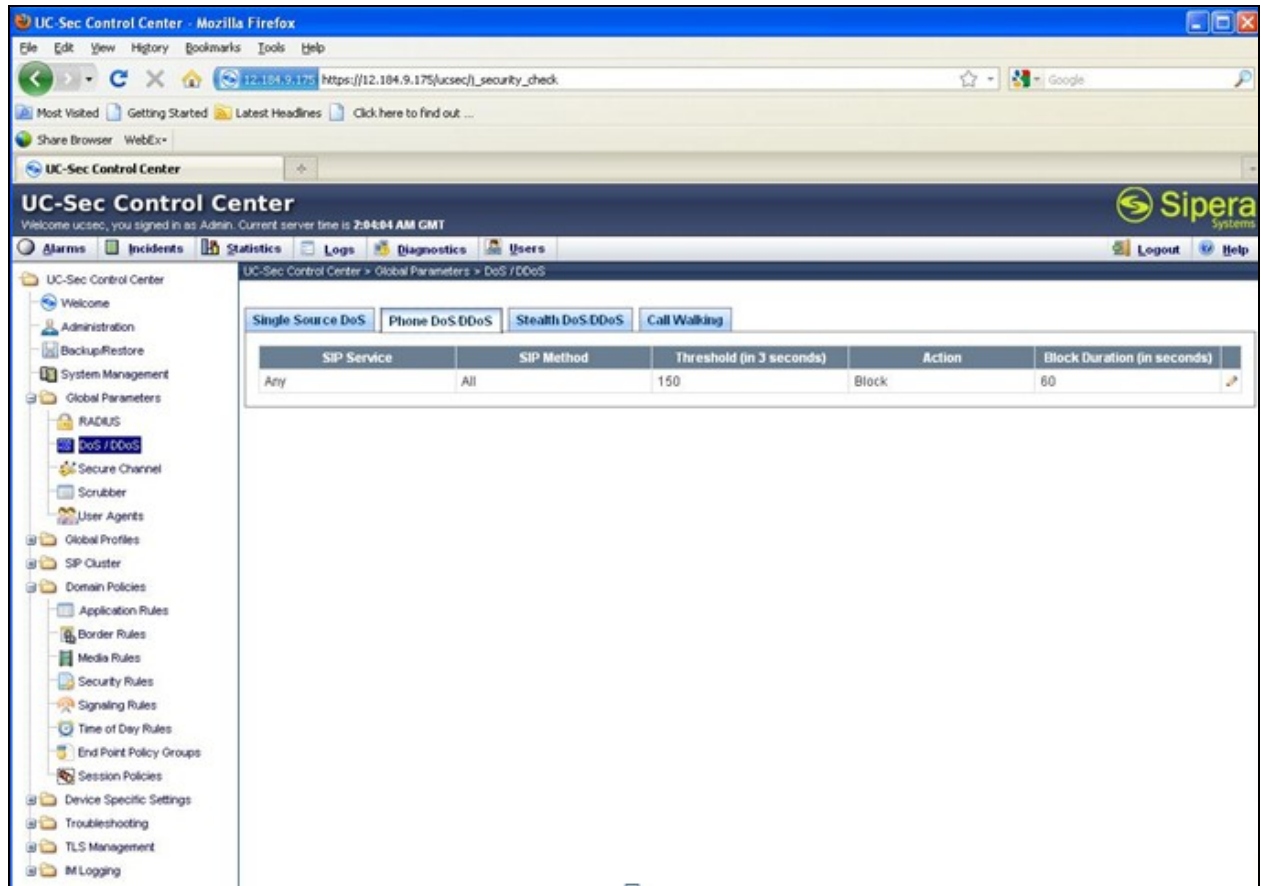
Step 22: Configure the four different DoS in GUI

Navigate to **UC-Sec Control Center → Global Parameters → DoS/DDoS → Single Source DoS**. Select the **Edit** icon. Change the **Threshold (in 5 seconds)** and **Action** to desired values (in this example, **Threshold (in 5 seconds)** is set to **150** and **Action** is **Block**). Select **Finish** (not shown). Select **Phone DoS/DDoS** to continue.



Step 23: Configure the four different DoS in GUI (continued)

Select the **Edit** icon. Change the **Threshold (in 3 seconds)**, **Action** and **Block Duration (in seconds)** to desired values (in this example, **Threshold (in 3 seconds)** is set to **150**, **Action** is **Block**, and **Block Duration** is **60**). Select **Finish** (not shown). Select **Stealth DoS/DDoS** to continue.



Step 24: Configure the four different DoS in GUI (continued)

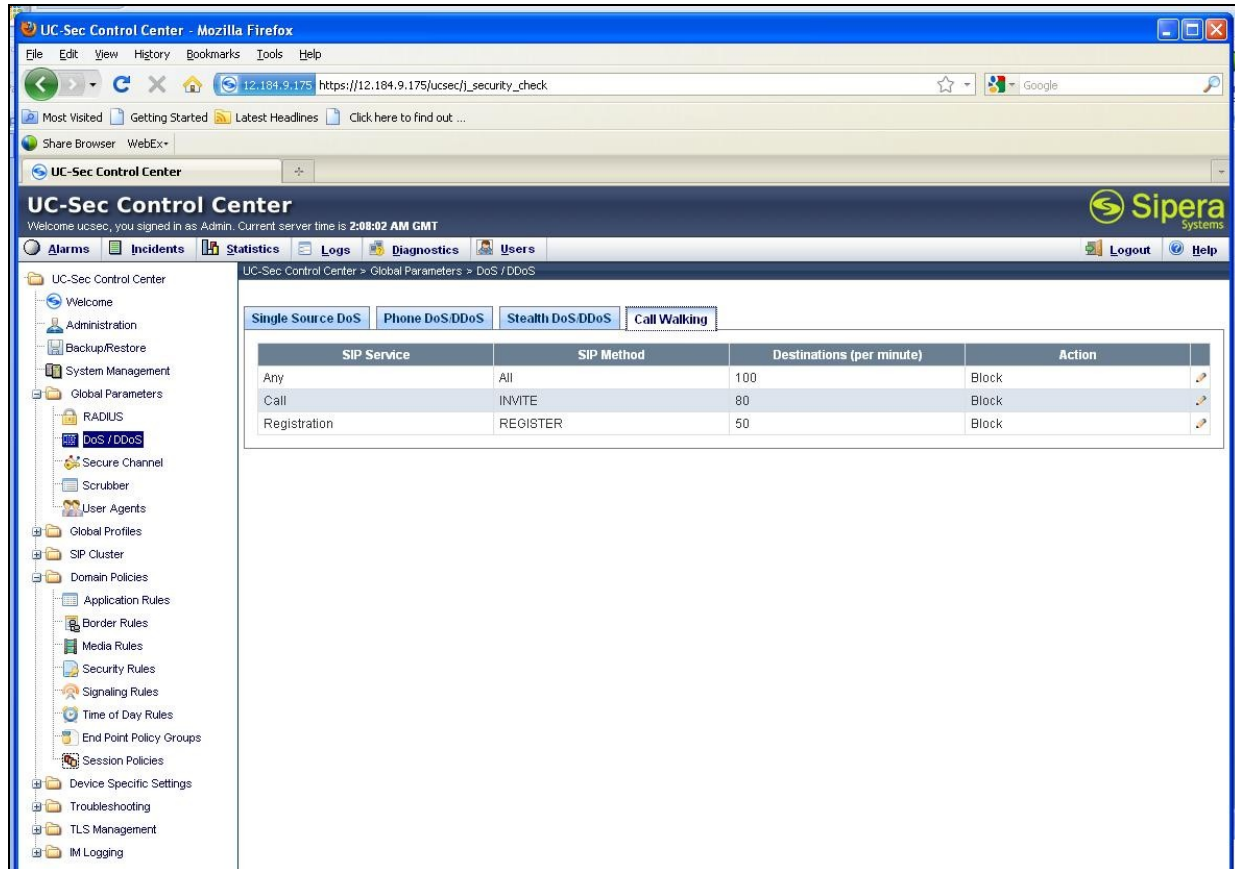
Select the **Edit** icon. Change the **Average Inter-Call Duration Threshold**, **Consecutive Average Inter-Call Duration Threshold Violations**, and **Action** to desired values (in this example, **Average Inter-Call Duration Threshold** is set to 10, **Consecutive Average Inter-Call Duration Threshold Violations** is set to 100, and the **Action** is set to **Block**). Select **Finish** (not shown). Select **Call Walking** to continue.

The screenshot shows the UC-Sec Control Center web interface in a Mozilla Firefox browser. The browser address bar shows the URL `https://12.184.9.175/ucsec/_security_check`. The interface includes a navigation menu on the left with categories like Administration, System Management, Global Parameters, and Domain Policies. The main content area displays the 'Global Parameters > DoS / DDoS' configuration page. The 'Call Walking' tab is selected, showing a table with four rows of configuration data for different timeslots.

Timeslot	SIP Service	SIP Method	Average Inter-Call Duration Threshold (in seconds)	Consecutive Average Inter-Call Duration Threshold Violations	Action	Block Duration (in seconds)
Morning (0600 - 1159)	Call	INVITE	10	100	Block	10
Afternoon (1200 - 1759)	Call	INVITE	10	100	Block	10
Evening (1800 - 2359)	Call	INVITE	10	100	Block	10
Night (0000 - 0559)	Call	INVITE	10	100	Block	10

Step 25: Configure the four different DoS in GUI (continued)

Select the **Edit** icon. Change the **Destinations (per minute)** and **Action** to desired values for each SIP service. (in this example, **Destinations (per minute)** is set to **100** for **Any**, **80** for **Call** and **50** for **Registration**, and **Action** is **Block**).



The screenshot shows the UC-Sec Control Center web interface in a Mozilla Firefox browser. The browser address bar shows the URL `https://12.184.9.175/ucsec/_security_check`. The interface has a navigation menu on the left with categories like Administration, System Management, Global Parameters, and Domain Policies. The 'DoS/DDoS' option is selected under Global Parameters. The main content area displays the 'DoS/DDoS' configuration page with tabs for 'Single Source DoS', 'Phone DoS/DDoS', 'Stealth DoS/DDoS', and 'Call Walking'. The 'Single Source DoS' tab is active, showing a table with the following data:

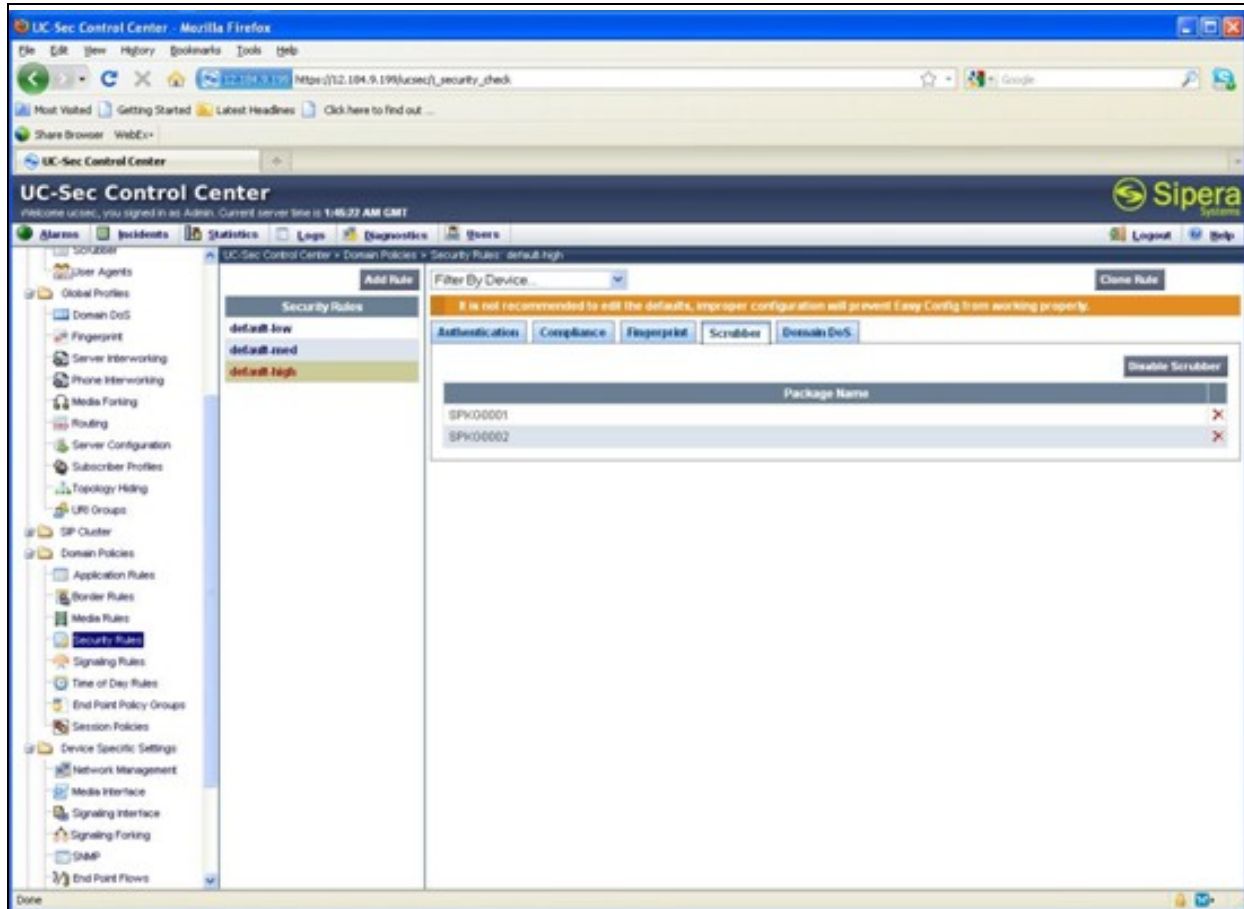
SIP Service	SIP Method	Destinations (per minute)	Action
Any	All	100	Block
Call	INVITE	80	Block
Registration	REGISTER	50	Block

Step 26: Security Feature - Scrubber

Below is the screen verifying that the scrubber is turned on. Navigate to **UC-Sec Control Center → Global Parameters → Scrubber → Packages**.

This screen is an example of how to configure scrubber feature.

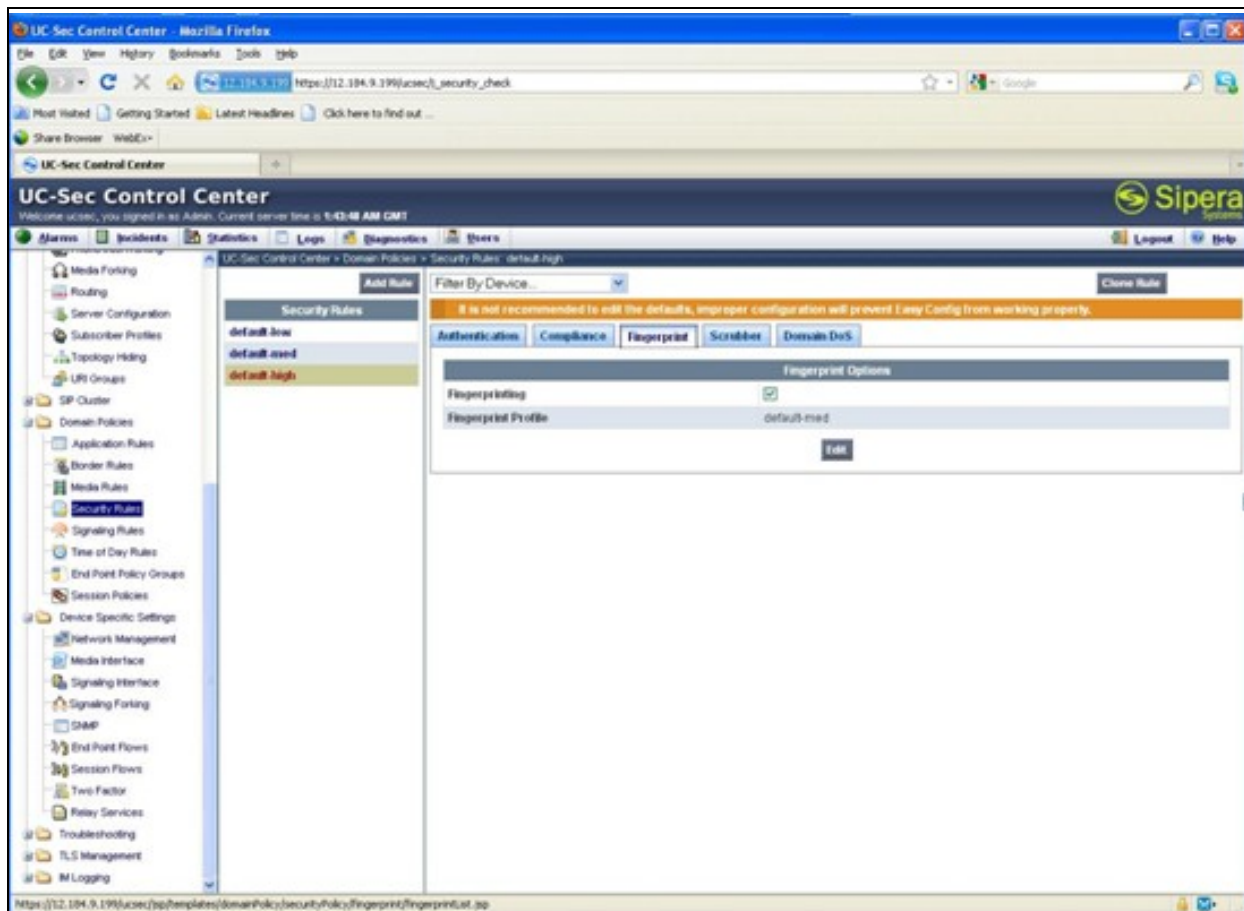
For detail information on the configuration of scrubber, please refer to UC-Sec administration guide [10], or contact Sipera Customer Support.



Step 27: Security Feature - Fingerprinting

Navigate to **UC-Sec Control Center** → **Domain Policies** → **Security Rules**, choose the appropriate security rule, and click on the **Fingerprint** tab. Select **Edit**, check the checkbox for **Fingerprinting**, and choose the appropriate fingerprint Profile. Click **Finish** (not shown).

For detailed information on the configuration of finger printing, please refer to UC-Sec administration guide [10], or contact Sipera Customer Support.



8. Verification Steps

The following steps may be used to verify the configuration:

- From the Communication Manager SAT, use the **status signaling-group** command to verify that the SIP signaling group is in-service.
- From the Communication Manager SAT, use the **status trunk-group** command to verify that the SIP trunk group is in-service.
- From the Avaya Aura® System Manager web administration interface, verify that all remote endpoints are registered with Avaya Aura® Session Manager using the private IP address of Sipera UC-Sec. To view, navigate to **Elements → Session Manager → System Status → User Registrations**.
- Verify that calls can be placed between a remote user without NAT and SIP and non-SIP endpoints at the main site.
- Verify that calls can be placed between a remote user with NAT and SIP and non-SIP endpoints at the main site.
- Verify that calls can be placed between a remote user without NAT and PSTN phones.
- Verify that calls can be placed between a remote user with NAT and PSTN phones.
- Verify that calls can be placed between remote users with and without NAT.
- From the Communication Manager SAT, use the **list trace tac** command to verify that the calls between remote users and endpoints at the main site are routed through the configured SIP trunks.

9. Conclusion

The Sipera Systems UC-Sec Secure Access Proxy passed compliance testing. These Application Notes describe the procedures required to configure the Sipera Systems UC-Sec Appliance to interoperate with Avaya Aura® Session Manager and Avaya Aura® Communication Manager to support Remote Users with and without NAT Traversal as shown in **Figure 1**.

10. Additional References

This section references the Avaya and Sipera documentation relevant to these Application Notes.

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

- [1] *Installing and Configuring Avaya Aura® Session Manager, Doc ID 03-603473 Release 6.*
- [2] *Administering Avaya Aura® Session Manager, Doc ID 03-603324, Release 6.0, June 2010*
- [3] *Installing and Configuring Avaya Aura® Communication Manager, Doc ID 03-603558, Release 6.0 June, 2010*
- [4] *Avaya one-X Deskphone Edition for 9600 Series IP Telephones Administrator Guide Release 3.1, Document Number 16-300698.*
- [5] *Modular Messaging Admin Guide Release 5.2 with Avaya MSS*
- [6] *Avaya Aura® Communication Manager Messaging Installation and Initial Configuration.*
- [7] *Avaya one-X Deskphone Edition for 9600 Series IP Telephones Administrator Guide Release 3.1, Document Number 16-300698.*
- [8] *Avaya one-X Deskphone SIP for 9600 Series IP Telephones Administrator Guide, Release 2.6, Document Number 16-601944.*

Product documentation for UC-Sec can be obtained from Sipera. Contact Sipera using the contact link at <http://www.sipera.com>.

- [9] *UC-Sec Install Guide (102-5224-400v1.01).*
- [10] *UC-Sec Administration Guide (010-5423-400v106).*

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

©2011 Avaya Inc. All Rights Reserved.

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

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.