Avaya Solution & Interoperability Test Lab

Configuring Remote Users with Avaya Session Border Controller Advanced for Enterprise R6.2 FP1 in a Back-To-Back-To-Back configuration with Multiple Avaya Aura® Session Managers R6.2 FP2 and Third-Party Security Certificates - Issue 1.0

Abstract

These Application Notes describe the steps to configure High Availability Avaya Aura® Session Border Controller Advanced for Enterprise 6.2 Feature Pack 1 in a back-to-back-to-back configuration to support remote Avaya 9641 SIP Deskphones. Avaya Session Border Controllers are configured to connect to multiple Avaya Aura® Session Managers. Transport Layer Security (TLS) is implemented using third-party signed certificates.

These Application Notes are intended for customers who intend to provide secure signaling by replacing default Avaya supplied certificates in a high security networked environment.

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

Table of Contents

1. Introduction 4
2. Interoperability Testing 5
   2.1. Test Description and Coverage 5
   2.2. Test Results and Observations 5
3. Reference Configuration 6
4. Equipment and Software Validated 8
5. Configure Third-Party Certificates for Avaya Session Border Controller Advanced for Enterprise 8
   5.1. Install Third-Party Trusted Root certificates 9
   5.2. Create a Certificate Signing Request for Avaya Session Border Controller for Enterprise 11
   5.3. Process the Certificate Signing Request 13
   5.4. Install Third-Party Signed Identity Certificate 15
6. Configuration of Avaya Session Border Controller for Enterprise in a Back-To-Back-To-Back Deployment with Multiple Avaya Aura® Session Managers 17
   6.1. Remote Avaya Session Border Controller for Enterprise Configuration 17
      6.1.1. Add Network Interfaces 18
      6.1.2. Create TLS Client and Server Profile 20
      6.1.3. Add Signaling Interfaces 23
      6.1.4. Add Media Interfaces 24
      6.1.5. Create Server Interworking Profile 25
      6.1.6. Configure Routing 25
      6.1.7. Add Server Configuration 26
      6.1.8. Configure SIP Cluster Proxy 29
      6.1.9. Configure Application Rules 32
      6.1.10. Configure Media Rules 32
      6.1.11. Configure Signaling Rules 34
      6.1.12. Configure Endpoint Policy Group 35
      6.1.13. Create a Topology Hiding Profile 35
      6.1.14. Create Endpoint Subscriber Flow 36
      6.1.15. Create Endpoint Server Flow 39
      6.1.16. Configure Application Relay 40
   6.2. DMZ Avaya Session Border Controller for Enterprise Configuration 42
      6.2.1. Add Network Interfaces 42
      6.2.2. Create TLS Client and Server Profile 43
      6.2.3. Add Signaling Interfaces 45
      6.2.4. Add Media Interfaces 45
      6.2.5. Create Server Interworking Profile 46
      6.2.6. Configure Routing 46

6.2.7. Add Server Configuration 46
6.2.8. Configure SIP Cluster Proxy 47
6.2.9. Create Application, Media and Signaling Rules, End Point Policy Group, and Topology Hiding Profile 50
6.2.10. Create Endpoint Subscriber Flow 50
6.2.11. Create Endpoint Server Flow 52
6.2.12. Configure Application Relay 52
6.3. Core Avaya Session Border Controller for Enterprise Configuration 54
6.3.1. Add Network Interfaces 54
6.3.2. Create TLS Client and Server Profiles 55
6.3.3. Add Signaling Interfaces 55
6.3.4. Add Media Interfaces 56
6.3.5. Create Server Interworking profile and Configure Routing 56
6.3.6. Add Server Configuration 58
6.3.7. Configure SIP Cluster proxy 59
6.3.8. Create Application, Media and Signaling Rules, End Point Policy Group, and Topology Hiding Profile 61
6.3.9. Create Endpoint Subscriber Flow 61
6.3.10. Create Endpoint Server Flow 63
6.3.11. Configure Application Relay 63
7. Configure remote 9641 IP Deskphone 65
8. Verification Steps 67
8.1. Verify Avaya Session Border Controller for Enterprise 67
8.2. Verify Avaya Aura® Session Manager 69
9. Conclusion 70
10. Additional References 70

1. Introduction

These Application Notes describe the configuration of Avaya Session Border Controller for Enterprise (SBCE) to support remote users connecting to multiple Avaya Aura® Session Managers through a back-to-back-to-back (b2b2b) configuration with third-party signed security certificates for Transport Layer Security (TLS).

Avaya Session Border Controller for Enterprise (SBCE) delivers flexibility and a high level of security to a Unified Communications network and is available in two versions; Advanced Services and Basic Services. Avaya SBCE has two main components: the Session Border Controller (SBC) and a management system called the Element Management System (EMS). The SBC and EMS components can co-reside in the same physical server or on separate servers in the case of High Availability (HA) configuration. See **Reference [3]** for details on Avaya SBCE specification. These Application Notes describe configuration of Avaya SBCE Advanced Services version in a HA configuration.

Avaya SBCE can effectively protect the enterprise network against all types of inadvertent and malicious intrusions and attacks. The Avaya SBCE two-wire-in-line topology performs border access control functionality such as Firewall/ Network Address Translation (NAT) traversal, access management and control based on user-configurable domain policies, and intrusion functionality to protect against DoS, spoofing, and stealth attacks, along with voice SPAM. High Availability support for both media and signaling ensures Avaya SBCE security functionality is provided continuously, regardless of any hardware or software failures. The signaling packets are routed only to the active (primary) Avaya SBCE, which performs all data processing. EMS replication is possible. Avaya Aura® Session Manager is deployed in an active-active configuration with endpoints registering to both Avaya Aura® Session Manager one (SM1) and Avaya Aura® Session Manager two (SM2).

Digital Certificates certify that a public key belongs to its reputed owner. To ensure greater trust, a trusted party can sign the public key and the information about its owner, creating a public-key certificate. The certificate guarantees the identity of its bearer. A trusted party that issues digital certificates is called a Certificate Authority (CA). A CA can be a third-party external service provider, e.g., VeriSign or Entrust, or belong to the same organization as the entity it serves. TLS sessions use a client-server model. Clients (i.e., devices requiring a service) contact a server and are offered an identity certificate as proof of the server's integrity. Clients verify the offered certificate by testing authenticity with a common trusted root CA certificate. If successfully authenticated; the client and server commence negotiations on an encryption scheme. If successful, transmission is secured from that point on. TLS protocol allows for servers to request a certificate from a client and authenticate it using a trusted root CA certificate. This is known as mutual authentication and is preferable to one-way authentication as it prevents unauthorized hosts obtaining services. Servers can only offer one identity certificate, but may have several trusted root CA certificates.

Non-unique, default TLS certificates, certified by Avaya, are shipped with Avaya Session Border Controller for Enterprise, Avaya Aura® Session Manager and Avaya one-X® Deskphone SIP to

provide out-of-box support for TLS sessions. For production environments, Avaya recommends replacing these default certificates with customer CA or third-party CA signed unique identity certificates. These Application Notes describe the process to replace certificates with third-party signed certificates to support remote users connecting into the enterprise network through a high-security Avaya SBCE back-to-back-to-back configuration.

Note: In the context of these Application Notes, phones connecting through the back-to-back-to-back Avaya SBCE configuration are referred to as 'remote phones', and phones connecting through a single high-availability pair of Avaya SBCEs are referred to as 'core phones'.

2. Interoperability Testing

These Application Notes describe the Avaya SBCE back-to-back-to-back configuration and third-party TLS certificate implementation. All servers and endpoints in the configuration are using third-party CA signed certificates. Once the network and configuration was complete, testing focused on normal and failover operation of remote endpoints.

2.1. Test Description and Coverage

The following test areas were covered.

- Remote phone registration and download of Personal Profile Manager (PPM) data.
- Basic calls between remote and core phones, remote and remote phones, and remote and PSTN phones.
- Call hold, transfer, conference, music-on-hold features.
- Call coverage to Avaya Aura® Messaging and Message Waiting Indicator (MWI) operations.
- Remote phones interaction with Avaya Meeting Exchange™ conference bridge.
- High Availability failover of Avaya SBCE in remote, DMZ, and core networks.
- Remote endpoints obtaining a TLS Identity certificate from CA using SCEP via Avaya SBCE relay.
- 46xxsettings file download from Avaya Aura® Utility Services via Avaya SBCE relay.
- Remote phone software upgrades from Utility Services server via Avaya SBCEs relay.

2.2. Test Results and Observations

All test cases were successful with the following observations.

- Avaya SBCE HA requires GARP support on the connected network elements.
- Session Manager SIP firewall function should be disabled for remote worker solution.
- Synchronize time/NTP across all servers, including Avaya SBCE, EMS, Session Manager, Communication Manager, Utility Server and the CA server.
- Media Capability Negotiation (Cap Neg) is not enabled for this example configuration.
- A trusted SIP entity is not configured for remote users connecting to Session Manager via Avaya Session Border Controller for Enterprise. In case both remote users and SIP trunking are required, separate set of interfaces are required for both external and internal signaling and media.
- If a Session Manager failover occurred during held call, remote users were not able to resume the held call.

3. Reference Configuration

High Availability Avaya SBCEs are deployed in a back-to-back-to-back configuration as shown in **Figure 1**. This configuration is used to support remote users in a high-security network. Avaya 9641 SIP Deskphones connect to the enterprise through a pair of HA SBCEs located at the remote site, through a second pair of HA SBCEs located at the enterprise edge in a Demilitarized Zone (DMZ) and finally, through a third pair of HA SBCEs located in the enterprise core network.

Avaya 9641 SIP and 9620 SIP Deskphones connect through a single pair of HA Avaya SBCEs located in the core network.

Each HA pair operates in a parallel mode configuration where both Avaya SBCE servers support the same set of VoIP interfaces. However, signaling packets are routed only to the active Avaya SBCE. The interface ports on the secondary (or stand-by) Avaya SBCE do not process any traffic. When a failover occurs, the standby Avaya SBCE becomes the active SBCE by advertising its MAC as the L2 address for the common IP addresses. Secure Real-Time Protocol (SRTP) is used end-to-end and media is anchored through the remote SBCE, through the DMZ SBCE and from the internal interface on Avaya SBCE located in the core network.

Administration of Avaya SBCE is provided by the Element Management System (EMS). To support End-to-End VoIP monitoring, a single EMS must be used to manage all the Avaya SBCE-HA pairs located in the core network. Separate EMS servers are required to manage Avaya SBCE-HA pairs located in remote sites and in the DMZ. To avoid conflicts between SIP and management traffic, the management interface between an EMS and an Avaya SBCE–HA pair must be on a different VLAN/subnet than VLAN/subnets used for other SBCE interfaces. To support HA failovers, Avaya SBCE requires Gratuitous Address Resolution Protocol (GARP) between connected elements. Since Avaya Aura® SIP endpoints do not support GARP, a GARP aware router/switch must be added between SIP endpoints and Avaya SBCE.

In the sample configuration, a standalone Avaya Aura® System Manager is used to administer SIP endpoints and two Avaya Aura® Session Manager elements. Session Manager operates in a replicated active-active HA redundancy mode which allows recovery of a single server failure by redistributing the Session Manager workload to other available Session Managers. Session Manager also provides simultaneous registration feature so that SIP endpoints can continue to be operational after a Session Manager failure. When a Session Manager fails or becomes unreachable, SIP endpoints establish new calls using the alternate Session Manager.

Microsoft Windows Server 2008 R2 Enterprise, deployed with Active Directory Certificate Services is used as a Certificate Authority. The CA is configured to generate certificates to use RSA public-key cryptography algorithm, 2048 bit key length and SHA1 hash algorithm. This CA can reside in the customer network or may reside at the third-party service provider data center. To establish secure connections using Third Party Certificates, all SIP endpoints are configured to use Simple Certificate Enrollment Protocol (SCEP) to request a signed certificate from the Microsoft Certificate Authority instead of using default Avaya certificates.

Avaya 9641 IP Deskphone and 9620 IP Deskphone, running Avaya one-X® Deskphone SIP software, receive their configuration settings and software from Avaya Aura® Utility Services over HTTPS. It is assumed Avaya SBCE, Session Manager and Communication Manager have been installed and configured for High Availability prior to implementing the procedures in these Application Notes. Avaya SBCE configuration shall be tailored to suit the individual customer security requirements. Firewalls are deployed across the network for additional security. Firewall configuration is outside the scope of this document. All references are in **Section 10**.

PSTN access from the core enterprise network is via Audiocodes Mediant 3000 SIP to ISDN gateway. Avaya Aura® Messaging is the voicemail server utilized by remote and core IP deskphones. These Application Notes provide an example configuration for Avaya SBCE in a back-to-back-to-back deployment with support for Session Manager failover with third-party TLS certificates.

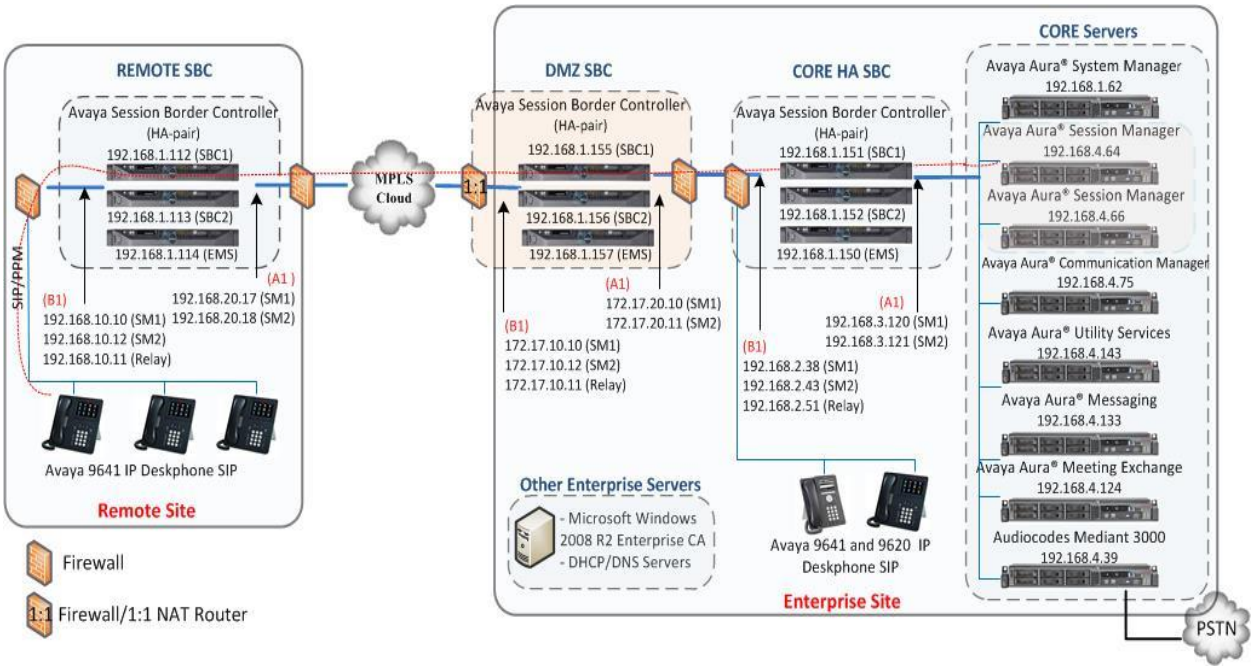


Figure 1: Remote Endpoints connecting through Avaya Session Border Controller back-to-back-to-back in a multi Avaya Aura® Session Manager TLS Network

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya Session Border Controller on Dell R210 – II XL	Release 6.2 FP1 Build: 6.2.0.Q64
Avaya Aura® Communication Manager running on Avaya S8800 Server	Release 6.2 FP2 Version: 6.3.0.124.0-21000
Avaya Aura® Session Manager on Avaya S8800 Server	Release 6.2 FP2 (6.3.2) Build 6.3.2.0.632023
Avaya Aura® System Manager on Avaya S8800 Server	Release 6.2 FP2 Version: 6.3.2.4.1399
Avaya Aura® Utility Services 6.3 Virtualization Environment (VE) vAppliance on Dell Poweredge R620 using VMWare ESXi 5.1.0	Release 6.3.0.0.20 Patch 6.3.0.1.20
Avaya 9641 IP Deskphone	Avaya one-X® Deskphone SIP Release 6.3.0 Build: 96x1-IPT-SIP-R6_3_092313
Avaya 9620 IP Deskphone	Avaya one-X® Deskphone SIP Release 2.6.11.106 Build: 2-6-11-130208
Avaya Aura® Messaging on Avaya S8800 Server	Release 6.2 SP2
Avaya Meeting Exchange™ Enterprise Edition	5.2 SP2 Bridge Patch 5.2.2.19.1
Audiocodes Mediant 3000	Release 3.0
Hewlett Packard Compaq 6000 Pro Microtower PC	Microsoft Windows Server 2008 R2 Enterprise SP1 x64 • Active Directory Certificate Services Role

5. Configure Third-Party Certificates for Avaya Session Border Controller Advanced for Enterprise

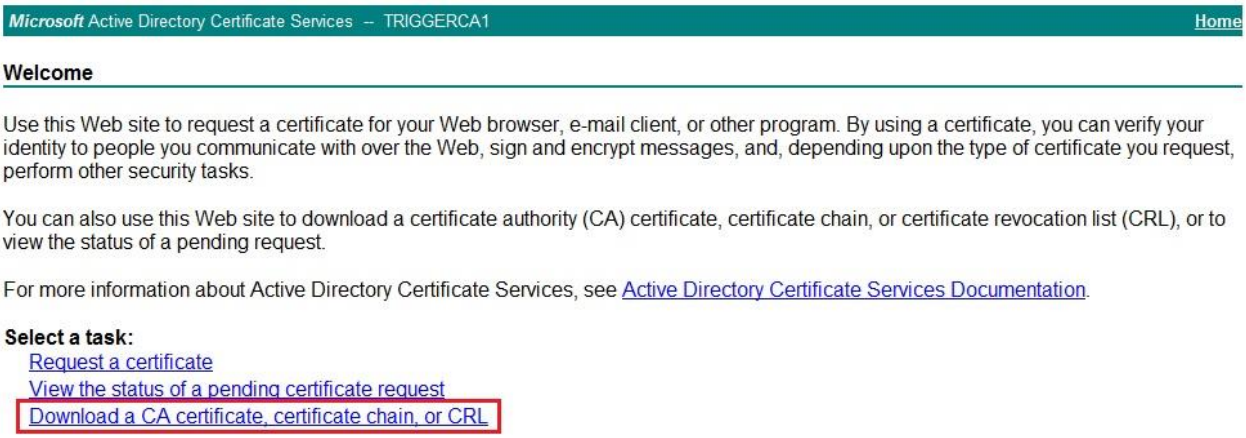
The steps required to administer third-party certificates on Avaya SBCE are;

- Install third-party trusted root CA certificate onto EMS and Avaya SBCEs.
- Create a Certificate Signing Request (CSR) for Avaya SBCE.
- Sign the CSR on the third-party CA.
- Install the signed Avaya SBCE Identity certificate.

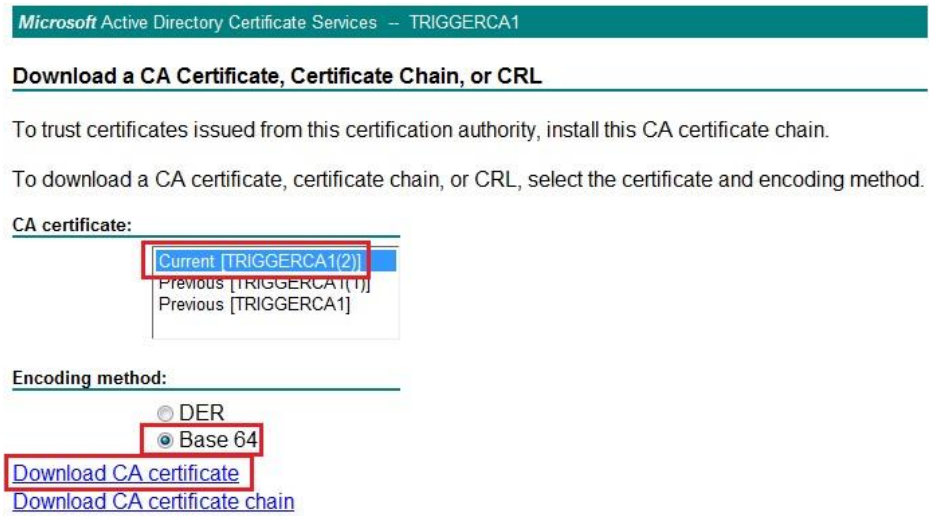
These steps are implemented on each of the remote, DMZ, and core Avaya SBCE HA pairs.

5.1. Install Third-Party Trusted Root certificates

Obtain the trusted root CA certificate from the CA administrator. For a Microsoft Windows 2008 Server CA, obtain the trusted root certificate by browsing to the CA server webpage **http://<CAserver_IPaddress>/certsrv**, logging in as Active Directory domain administrator-level account and clicking on **Download a CA certificate, certificate chain, or CRL** link.



Select the current **CA certificate** and **Base 64** encoding method. Click **Download CA certificate**.



Enter a file name (e.g., rootCAcert.pem) and save the file to the local PC.

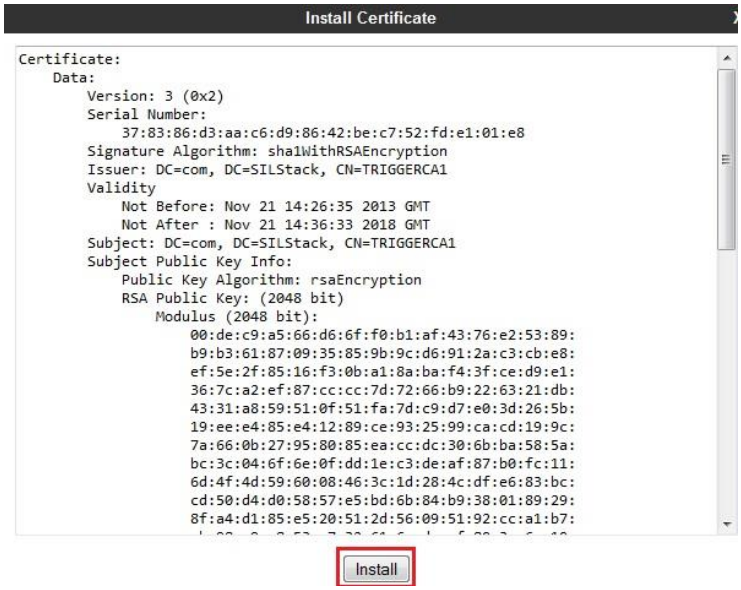
Open EMS GUI through a browser by entering **https://<SBCmanagement_IPaddress>/sbc** in the address bar, where <SBCmanagement_IPaddress> is the management IP address or Fully Qualified Domain Name (FQDN) configured during the install of the SBCE. Microsoft Internet Explorer, Mozilla Firefox and Google Chrome are supported browsers.

Enter **ucsec** for **Username** and enter appropriate **Password** (not shown).

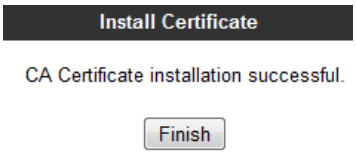
Navigate to **System Management → TLS Management → Certificates** and click the **Install** button.

Select **CA Certificate**. Enter a descriptive **Name** for the certificate and **Browse** to the trusted root CA certificate saved to the local PC. Click **Upload**

Ensure the certificate details appear correct and click **Install**.



A message appears stating the CA certificate installation is successful. Click **Finish**.

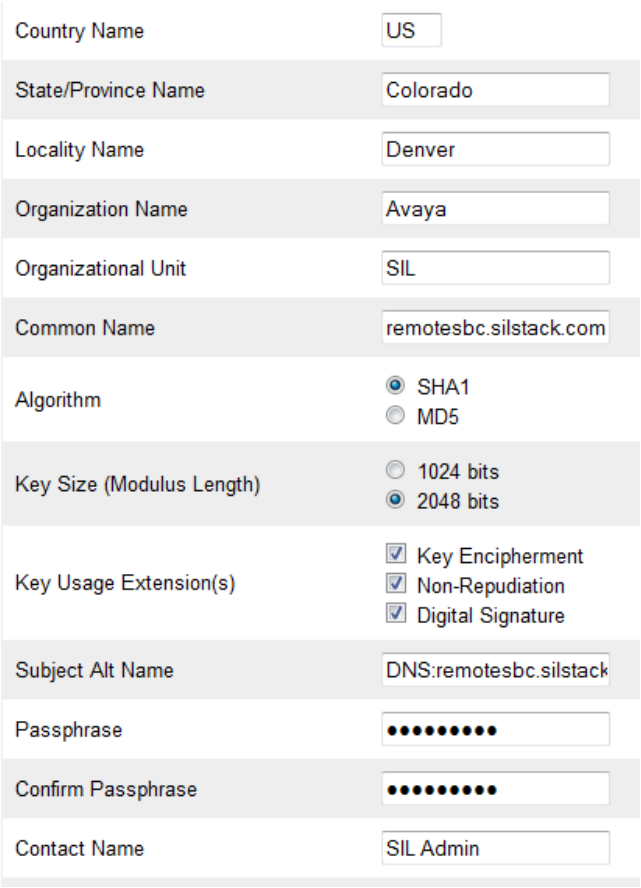


5.2. Create a Certificate Signing Request for Avaya Session Border Controller for Enterprise

To create a Certificate Signing Request for Avaya SBCE, navigate to **System Management → TLS Management → Certificates** and click the **Generate CSR** button.

Add details for the Avaya SBCE identity certificate to be signed by the third-party or customer CA. Example responses are shown below.

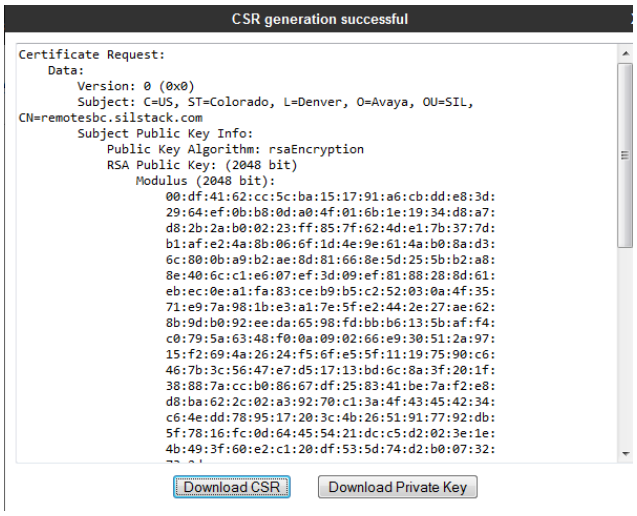
- Country **US**
- State/Province Name **Colorado**
- Locality **Denver**
- Organization **Avaya**
- Organizational Unit **SIL**
- Common Name Enter a descriptive name for the end entity covered by this identity certificate. The example uses the name of SBC HA pair and domain name, e.g., **remotesbc.silstack.com**
- Algorithm Select **SHA1**.
- Key Size Select **2048 bits**.
- Key Usage Extension(s) Check each option.
- Subject Alt Name Enter Subject Alternative Name to further identify the signed certificate. A Domain Name Server (DNS) entry or IP address can be used, e.g., **DNS: remotesbc.silstack.com** or **IP: 192.168.10.10**
- Passphrase Enter a password used when encrypting the private key.
- Contact Name Contact name for any queries on this certificate.
- Contact Email Contact Email address (not shown).



Click on **Download CSR** and save the CSR to a text file. E.g., **remoteSBC.csr**

Click **Download Private Key** and save the private key to the local PC, e.g. **remotesbc.key**.

Click on the **X** on the top right corner to close the active window.

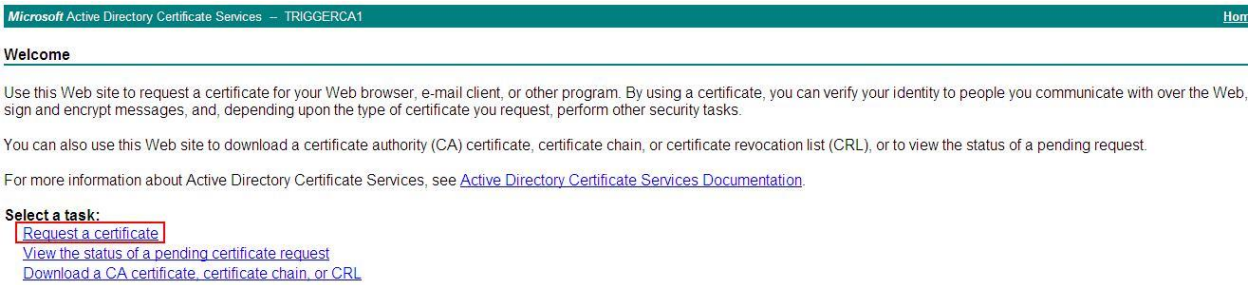


Note: SHA1 and MD5 are the only hash algorithms offered by the CSR GUI. To use SHA2 (SHA-256 or SHA-512), it is possible to use **openSSL** application on the SBCE through a command-line interface (CLI). See **Reference [7]** for details on how to use **openSSL** to create a private key and certificate signing request for SHA256/2048bit keys.

5.3. Process the Certificate Signing Request

The CSR from **Section 5.2** will be signed by CA. In this example a Microsoft Windows 2008 Server Enterprise CA is used. Using Internet Explorer, browse to the Microsoft Active Directory Certificate Services on the CA server. See **Reference [7]** for details on configuring Microsoft Windows 2008 Server as a Certificate Authority.

Enter **http://<IPaddressOfCAserver>/certsrv/**
where **<IPaddressOfCAserver>** is the IP address or FQDN of the Microsoft Windows 2008 CA. Click on **Request a certificate**



Click on **Advanced Certificate Request** (not shown). Click on **Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file** (not shown).

Paste the contents of the CSR from **Section 5.2** into the **Base-64-encoded certificate** request box, from **-----BEGIN CERTIFICATE REQUEST-----** up to and including **-----END CERTIFICATE REQUEST-----**. Use a suitable **Certificate Template** e.g., **WebServer-Enterprise**, and click **Submit**. See **Reference [7]** for details on creating certificate templates.

Select **Base64 encoded** radio button and click **Download certificate** to save file to the local PC. Save the file with **.pem** extension and a descriptive name, e.g., **remoteSBCsigned.pem**

Save the signed identity certificate file with an extension of type **crt**, e.g., **remotesbc.crt**. Avaya recommends not using any uppercase or special characters in the file name.

Note: An alternative method (to using Active Directory Certificate Services webpage) of signing the CSR utilises **certutil** command-line tool on the Windows Server 2008 CA. This method is required when a template, with a minimum support for Windows Server 2008 CA, is used. A template of this type is used when a hash algorithm of SHA-2 (SHA-256 or SHA-512) is required. An example of the command-line argument is shown below.

C:\Users\administrator.SILSTACK>certreq -submit –config "CA1.SILStack.com\CA1" -attrib "CertificateTemplate:Web-SHA256" c:/remotesbc.csr

Where;

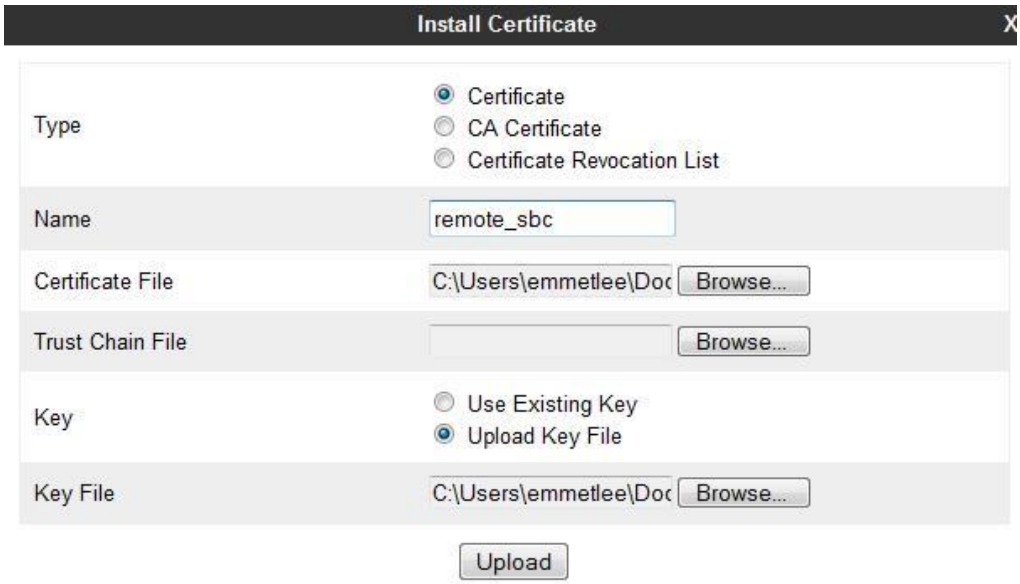
- **CA1.SILStack.com\CA1** is the name of the CA server configuration string, found by entering the command **certutil –getconfig**.
- **Web-SHA256** is the name of a template configured with sha256 hash algorithm, 2048 bit encryption, and client and server authentication.
- **c:/remotesbc.csr** is the file path to CSR.

5.4. Install Third-Party Signed Identity Certificate

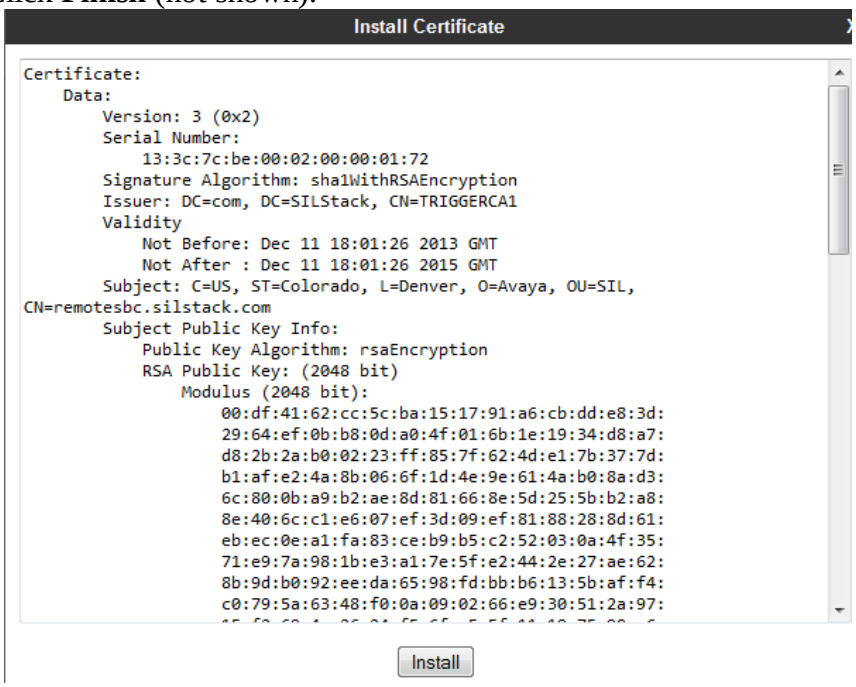
On SBCE EMS, navigate to **System Management→ TLS Management →Certificates** (not shown). Click **Install** button. Select the following settings;

- Type — Select **Certificate**
- Name — Enter a descriptive name, e.g., **remote_sbc**.
- Certificate File — Browse to the signed **Certificate File** created in **Section 5.3**, e.g., **remoteSBCsigned.pem**.
- Key — **Upload Key File**
- Key File — Browse to the saved private key created in **Section 5.2** e.g., **remotesbc.key**.

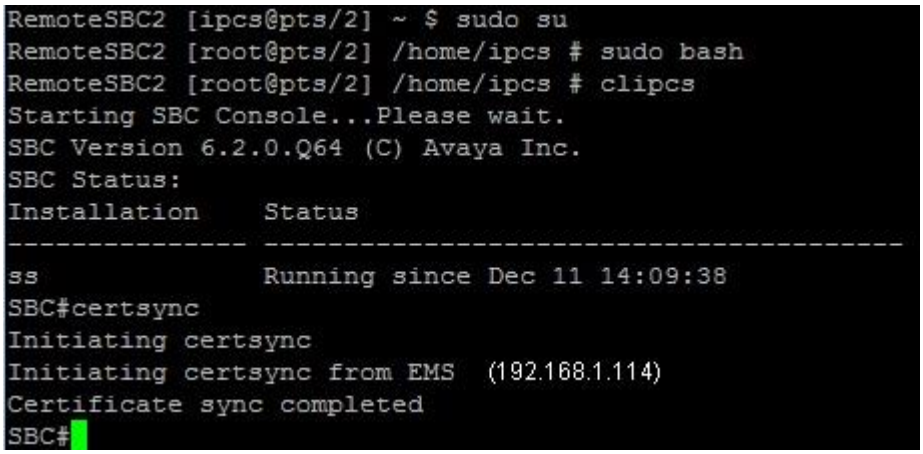
Click **Upload** to upload the certificate and private key to the EMS server.



Click **Install**. Click **Finish** (not shown).



The certificate and private key are required to be copied from the EMS server to each SBCE in the HA pair. Log into SBC1 management IP Address Command Line Interface (CLI) using an SSH client, such as PuTTY. Log in with user account **ipcs** and enter the password configured during SBCE installation. Enter the command **sudo su** to switch to root user. Enter **sudo bash**. Enter the command **clipcs** to access the SBCE console. Enter the command **certsync** to synchronize the certificates and keys from EMS to SBC1. **Certificate sync completed** is displayed for successful completion.



Issue the command **certinstall** followed by a space and the descriptive name of the certificate given when installing on EMS, e.g., **remote_sbc**. See example below. Enter the private key passphrase as configured when creating the CSR in **Section 5.2.** The text **Certificate installation completed** is shown for successful completion.

```
SBC#
SBC#certinstall remote_sbc
Initiating Certificate Installation
Enter your passphrase:
writing RSA key
Certificate installation completed
SBC#
```

Log in over CLI to the secondary SBCE in the SBCE HA-pair and repeat this process of synchronizing certificates from EMS to the SBCE. Repeat all the steps defined in **Section 5** on the DMZ SBCE and Core SBCE HA pairs.

6. Configuration of Avaya Session Border Controller for Enterprise in a Back-To-Back-To-Back Deployment with Multiple Avaya Aura® Session Managers

Install the Avaya SBCE HA pair as per **Reference [1]**. In the following sections, the IP address on the Avaya SBCE towards the remote phone is referred to as the external IP address (B1) and the IP address on Avaya SBCE towards Session Manager is referred to as the internal IP address (A1). The primary Session Manager is referred to as SM1 and the secondary Session Manager is referred to as SM2. Avaya SBCEs will have a one-to-one mapping of signaling and media interfaces. Each Avaya SBCE HA pair will have three external IP addresses and two internal IP addresses. One external and one internal IP address will be used for routing to SM1 and one external and one internal IP address will be used to route to SM2. The third external IP address is used to relay non-SIP packets, such as HTTPS traffic to a file utility server, SCEP requests to a CA, or RTCP to Prognosis server. The steps to configure Avaya SBCE in a back-to-back-to-back deployment are;

- Configure Remote Avaya SBCE HA pair.
- Configure Avaya SBCE HA pair in the Enterprise DMZ network.
- Configure Avaya SBCE HA pair in the enterprise core network.

Note: For each Avaya SBCE HA pair, ensure the management interface (IP address used to access the GUI) is not in the same subnet as the internal or external interface. High availability Avaya SBCE requires Gratuitous Address Resolution Protocol (GARP) support on the network router/switch elements.

6.1. Remote Avaya Session Border Controller for Enterprise Configuration

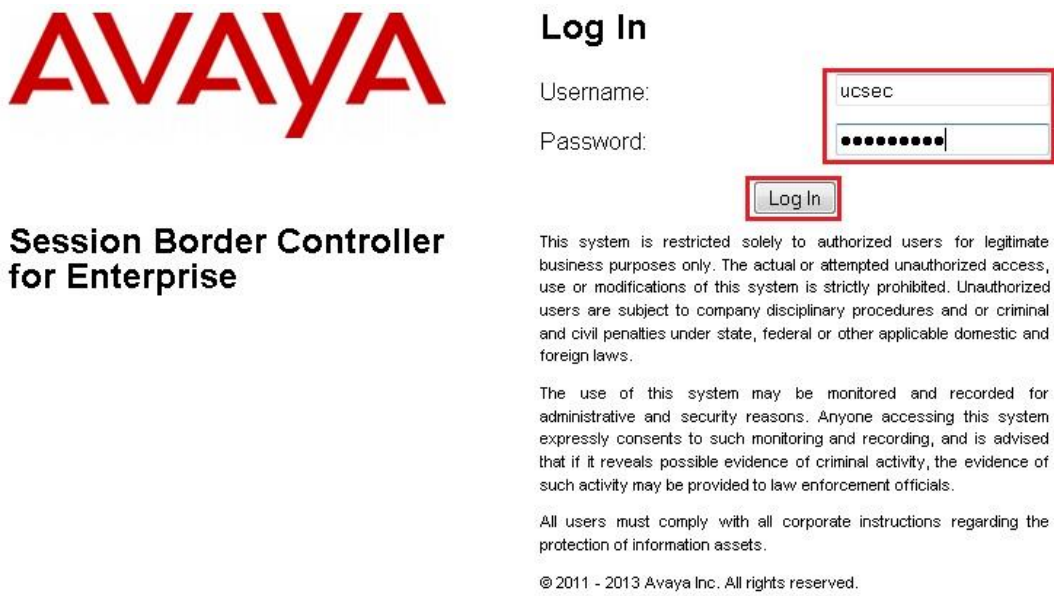
Configuration steps on the remote Avaya SBCE are;

- Add network interfaces
- Create TLS profiles
- Add Signaling and Media Interfaces
- Create Server Interworking Profile
- Configure Routing
- Create Server Configuration Profile

- Configure SIP Cluster Proxy
- Configure Application Rules
- Create Signaling Rules
- Configure Media Rules
- Configure Endpoint Policy Group
- Create Topology Hiding Profile
- Configure Endpoint Subscriber Flow
- Configure Endpoint Server flow
- Configure Application Relays

6.1.1. Add Network Interfaces

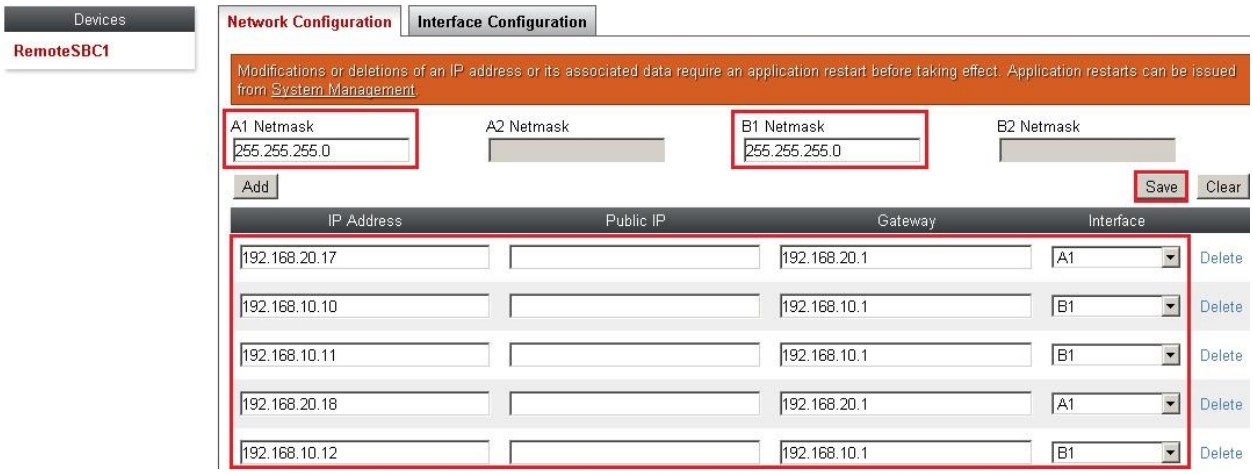
Log into remote SBCE EMS GUI as described in **Section 5.1** by browsing to the management IP address or Fully Qualified Domain Name (FQDN) of the remote EMS server. Enter **ucsec** for **Username** and enter appropriate **Password**. Click **Log In** button.



Navigate to **System Management → Device Specific Settings →Network Management** (not shown).

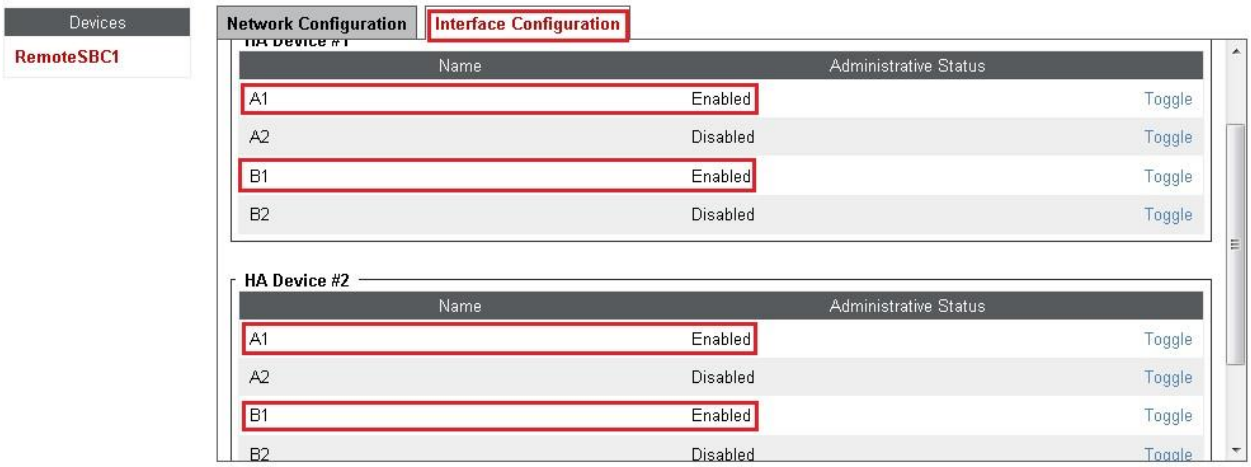
As mentioned above, two A1 (Internal) and three B1 (External) interface IP addresses are required.

On the **Network Configuration** tab; enter the subnet mask for **A1 Netmask** and **B1 Netmask**. Enter an IP address and Gateway, and select **A1** or **B1** interface from the drop-down menu as shown below. Click **Save**.



Click on the **Interface Configuration** tab and ensure one **A1** and one **B1** interface is enabled for both **HA Device #1** and **HA Device#2**. Click on the corresponding **Toggle** button to change from **Disabled** to **Enabled**.

Network Management: RemoteSBC1



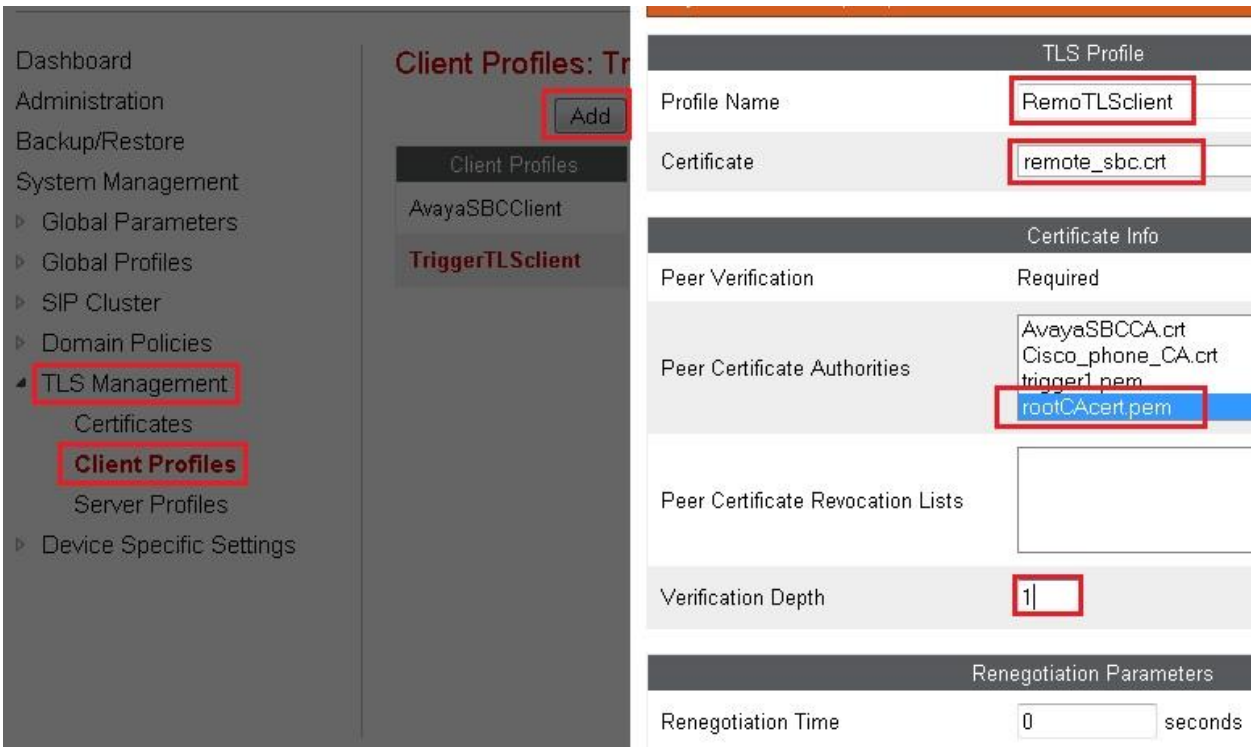
Ensure the **A1** and **B1** interfaces are selected for **HA Link Propagation**.

6.1.2. Create TLS Client and Server Profile

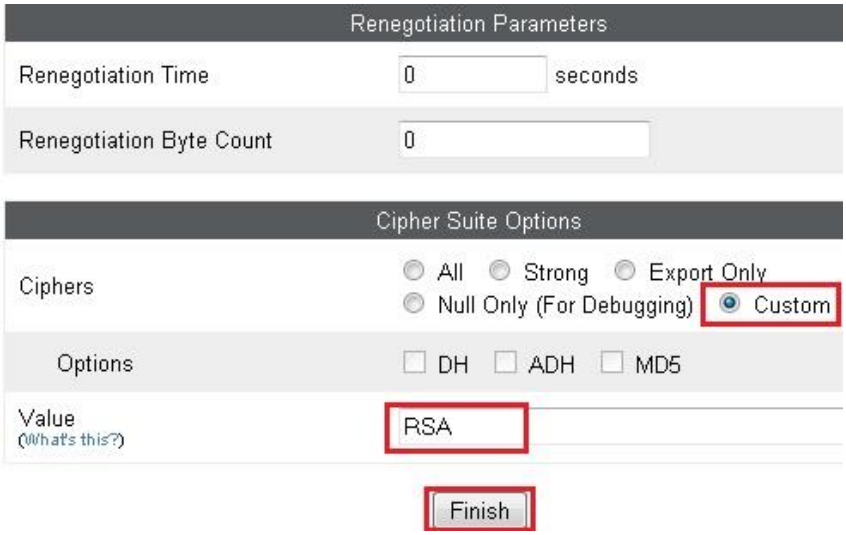
Refer to **Section 5** for installing third-party signed TLS certificates.

Navigate to **System Management → TLS Management → Client Profiles**. Click **Add** to create a new TLS client Profile. Enter the following;

- Profile Name — Enter a descriptive name, e.g., **RemoTLSclient**
- Certificate — Select Certificate created in **Section 5.3**, e.g.,**remote_sbc.crt**.
- Peer Certificate Authorities — Select the trusted root CA certificate added in **Section 5.1**, e.g., **rootCAcert.pem**.
- Verification Depth — Depth of the root CA certificate chain, e.g., **1**. If the trusted root CA is a subordinate CA, a depth of 2 or greater may be entered.

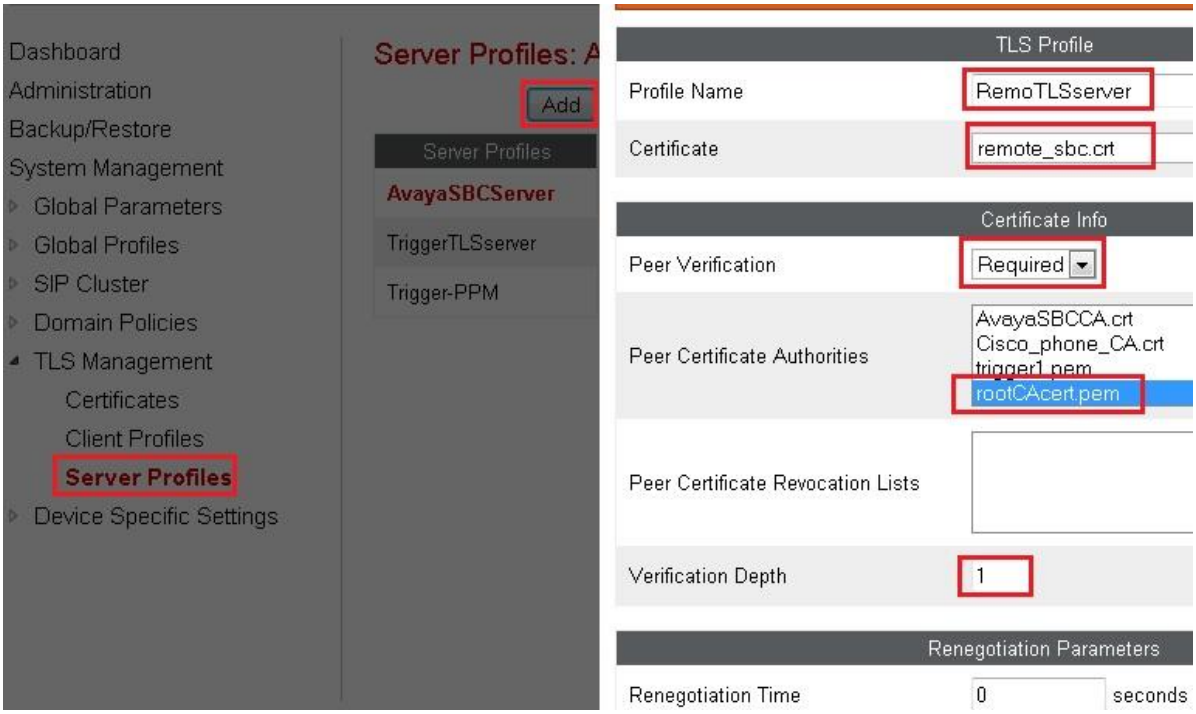


Select **Custom** option for **Ciphers** and provide a value of **RSA**. Click **Finish**.

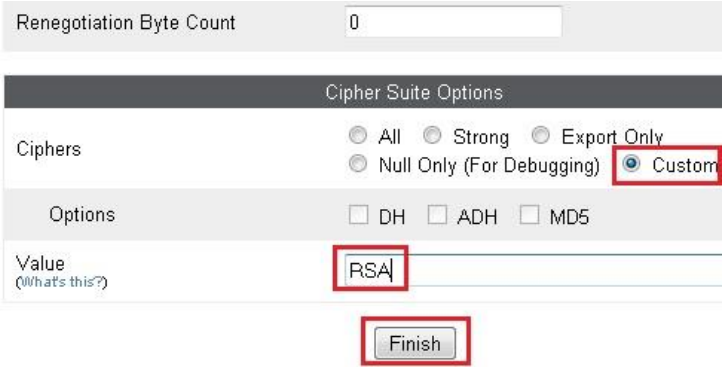


To create a TLS server profile, navigate to **System Management → TLS Management → Server Profiles** and click **Add**.

- Profile Name — Enter a descriptive name, e.g., **RemoTLSserver**
- Certificate — Select the TLS server Identity **Certificate** from the drop-down menu, e.g., **remote_sbc.crt**.
- Peer Verification — Select **Required**
- Peer Certificate Authorities — Select trusted CA root certificate, e.g., **rootCAcert.pem**.
- Verification Depth — Certificate chain depth, e.g., **1**.



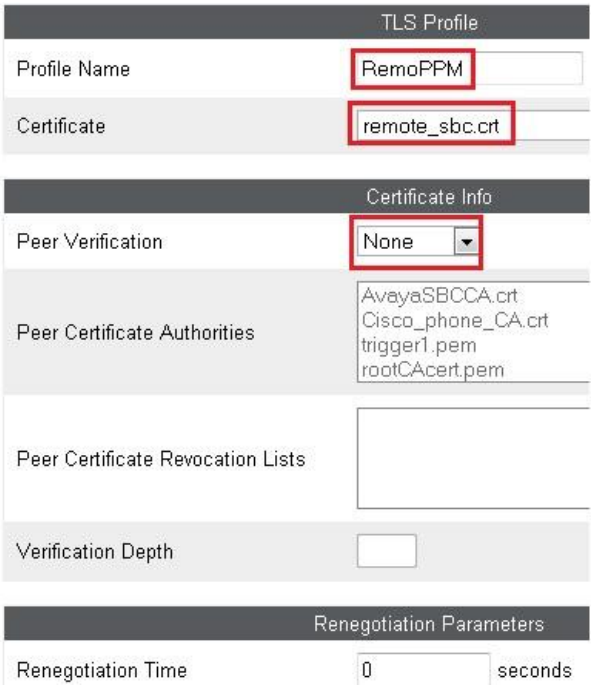
Select **Custom** for the **Cipher** suite and enter a **Value** of **RSA**. Press **Finish**.

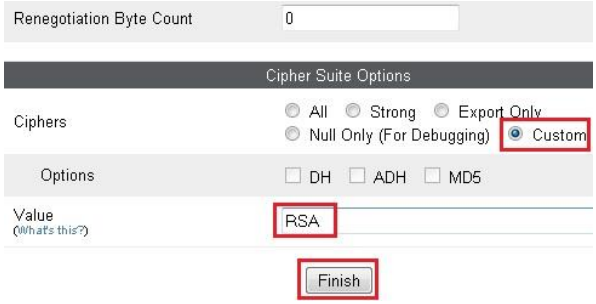


Personal Profile Manager (PPM) uses SSLv3 over HTTPS and **Peer Verification** is not supported. It is therefore necessary to create an extra TLS server profile specifically for PPM. Click **Add**.

- Profile Name — Enter a descriptive name, e.g., **RemoPPM**
- Certificate — Select the TLS server Identity **Certificate** from the drop-down menu, e.g., **remote_sbc.crt**.
- Peer Verification — Select **None**.
- Ciphers — Select **Custom**.
- Value — Enter **RSA**.

Click **Finish**.





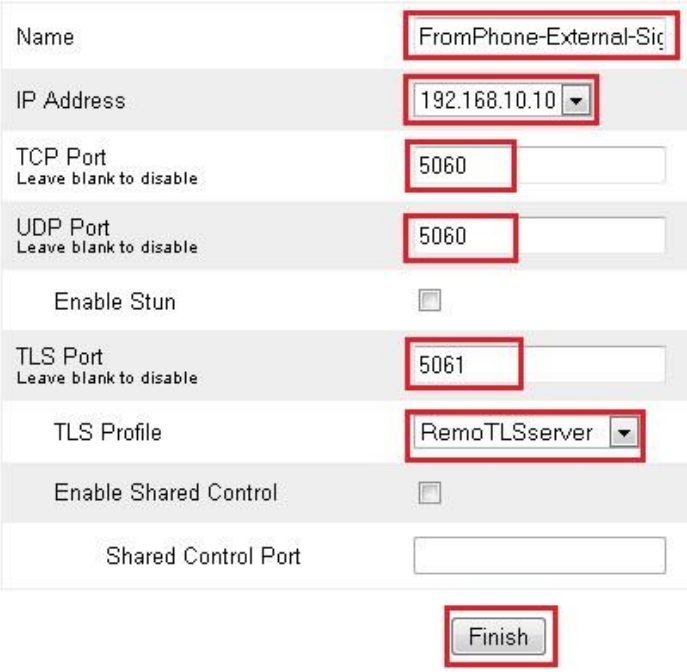
6.1.3. Add Signaling Interfaces

A signaling interface is added for both of the external and internal interfaces used for signaling.

Navigate to **System Management → Device Specific Settings →Signaling Interface** and click on **Add**. Enter the following;

- Name — Descriptive name for the interface, e.g., **FromPhone-External-Signaling-1**.
- IP Address — Select from the drop down menu. The IP address list is extracted from the network management interfaces.
- TCP Port — Enter **5060**.
- UDP Port — Enter **5060**.
- TLS Port — Enter **5061**.
- TLS Profile — Select TLS server profile created in **Section 6.1.2**, e.g., **RemoTLSserver**.

Click **Finish**.



Repeat this action for the second external interface on the remote Avaya SBCE and for both the internal interfaces on the remote SBCE as shown below

Signaling Interface

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile
FromPhone-External-Siganling-1	192.168.10.10	5060	5060	5061	RemoTLSserver
To-DMZ-Side-Internal-Siganling-1	192.168.20.17	5060	5060	5061	RemoTLSserver
FromPhone-External-Siganling-2	192.168.10.12	5060	5060	5061	RemoTLSserver
To-DMZ-Side-Internal-Siganling-2	192.168.20.18	5060	5060	5061	RemoTLSserver

6.1.4. Add Media Interfaces

Browse to **System Management→ Device Specific Settings →Media Interfaces** (not shown). Click **Add.** Enter a descriptive name for the interface. It is useful to include internal or external, and direction in which the media is flowing, in the descriptive **Name**. Select the interface **IP Address** from the drop-down menu. Modify the port range if required. Click **Finish**.

Add Media Interface

Name	Int_Med_int_DMZ-1
IP Address	192.168.20.17
Port Range	35000 - 40000

Finish

Repeat this for each of the external and internal interfaces used to carry media as shown below.

Media Interface

Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.

Add

Name	Media IP	Port Range	
Int_Med_int_DMZ-1	192.168.20.17	35000 - 40000	Edit Delete
External-Media-fromPhones-1	192.168.10.10	35000 - 40000	Edit Delete
External-Media-fromPhones-2	192.168.10.12	35000 - 40000	Edit Delete
Int_Med_int_DMZ-2	192.168.20.18	35000 - 40000	Edit Delete

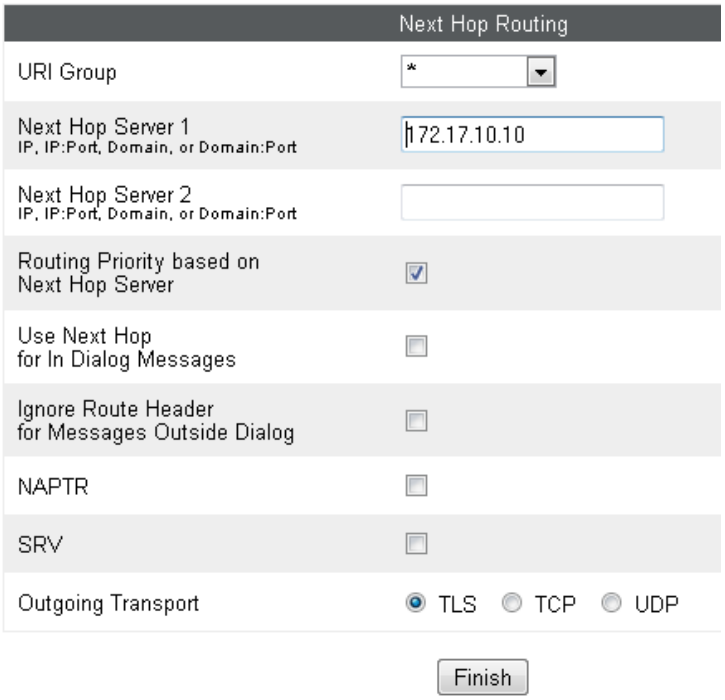
6.1.5. Create Server Interworking Profile

Navigate to **System Management→Global Profiles→Server Interworking** and click **Clone** to create a new profile from **avaya-ru** profile, e.g., **avaya-ru-multism.** Click **Finish** (not shown).

6.1.6. Configure Routing

Create two routing rules as part of a multi-Session Manager network. Rule one is for SM1 and rule two is for SM2. The next hop will be the IP address for SM1 interface on DMZ SBCE or the IP address for SM2 interface on the DMZ SBCE. Navigate to **System Management → Global Profiles → Routing**. Click **Add** (not shown).

Enter a **Profile Name** for routing rule one, e.g., **To-DMZ-SM-1**. Click **Next** (not shown). Enter SM1 IP address of DMZ for **Next Hop Server 1**, e.g., **172.17.10.10**. Select the check box for **Routing Priority based on Next Hop Server**. Select **TLS** as the Outgoing Transport protocol. Click **Finish**.



Click **Add** to create a new routing profile for SM2. **Note**: Do not click add to the right of an existing profile as this will create a second rule within the same profile.

Enter the SM2 IP address on the DMZ SBCE interface as the **Next Hop** server, e.g., **172.17.10.12**. Configure the other settings to be the same as the profile for SM1 as shown below.

View Routing Rule	
Priority	1
URI Group	*
Next Hop Server 1	172.17.10.12
Next Hop Server 2	---
Next Hop Priority	☑
NAPTR	☐
SRV	☐
Next Hop in Dialog	☐
Ignore Route Header	☐
Outgoing Transport	TLS

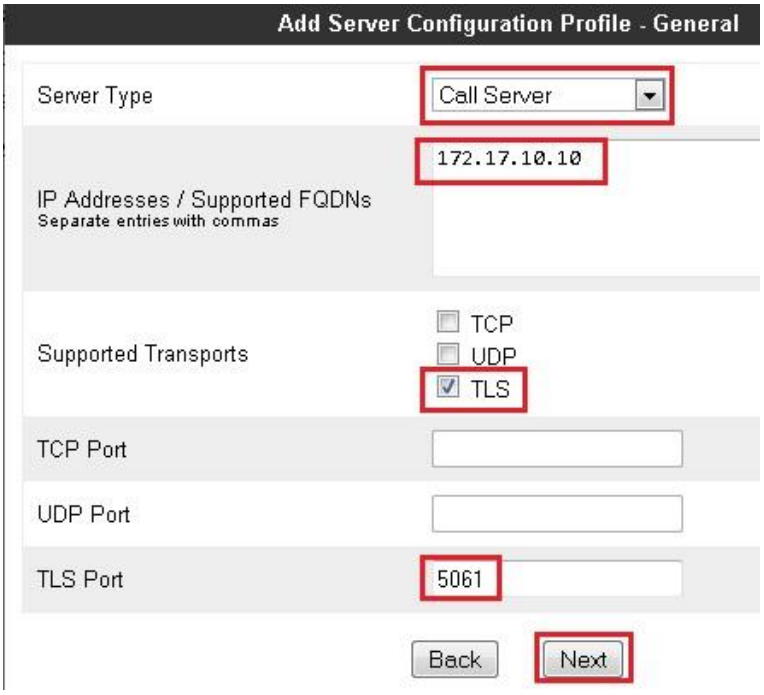
6.1.7. Add Server Configuration

Navigate to **System Management→Global Profiles→Server Configuration**. Add two server profiles; one for Session Manager One and one for Session Manager Two (failover).

The IP address is the next hop IP address on route to Session Manager. In the remote Avaya SBCE, the next hop is the DMZ SBCE. Click **Add** (not shown). Enter a descriptive server configuration profile name, e.g., **Server-DMZ-SM-1** and click **Next** (not shown).

Select the following settings and click **Next**.

- Server Type — Select **Call Server**
- IP Addresses — IP address for SM1 Interface on DMZ SBCE. E.g., **172.17.10.10**
- Supported Transports — Select **TLS**
- TLS Port — Enter **5061**

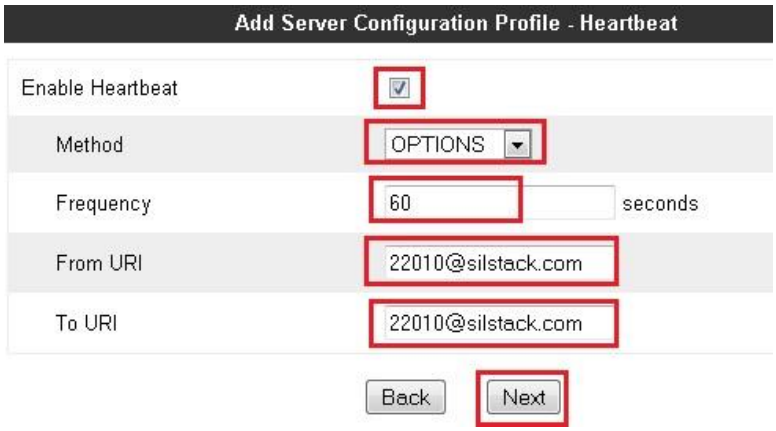


Do not enable authentication in the **Authentication** tab. Click **Next** (not shown).

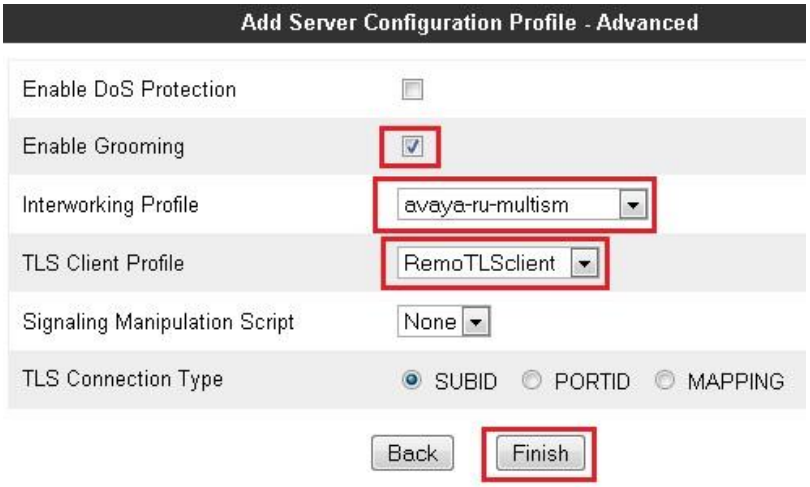
For Session Manager failover, a heartbeat is enabled using SIP OPTIONS method. Configure two SIP User accounts on System Manager User Management for this heartbeat function. It is not necessary to have any SIP endpoint logged in for these users. Heartbeat configuration is only required for the Remote and Core SBCE HA pair and not required on the DMZ SBCE HA pair.

Select the following settings and click **Next**.

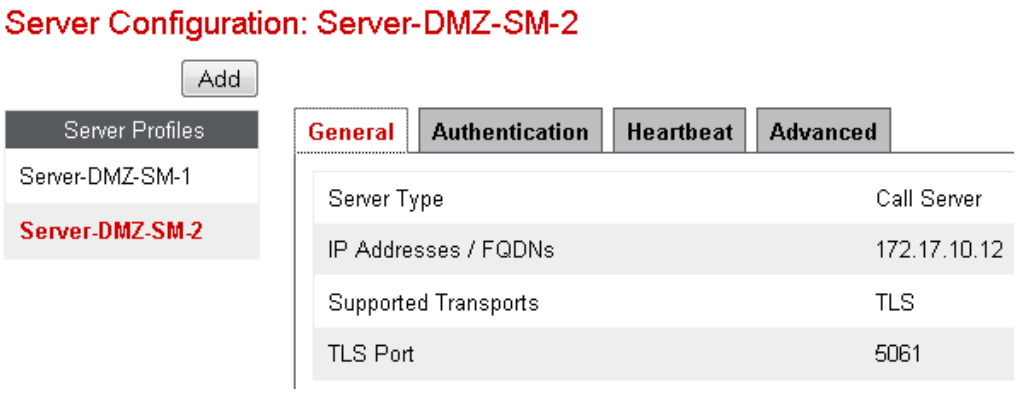
- Enable Heartbeat — Check the box
- Method — Select **OPTIONS**
- Frequency — e.g., **60** seconds.
- From URI — Enter **Login Name** defined for SIP user configured on System Manager, e.g., **22010@silstack.com**.
- To URI — Same as From URI, e.g., **22010@silstack.com**.



Select the checkbox beside **Enable Grooming**. Select the **Interworking Profile** created in **Section 6.1.5** and the **TLS Client Profile** created in **Section 6.1.2**. Click on **Finish**



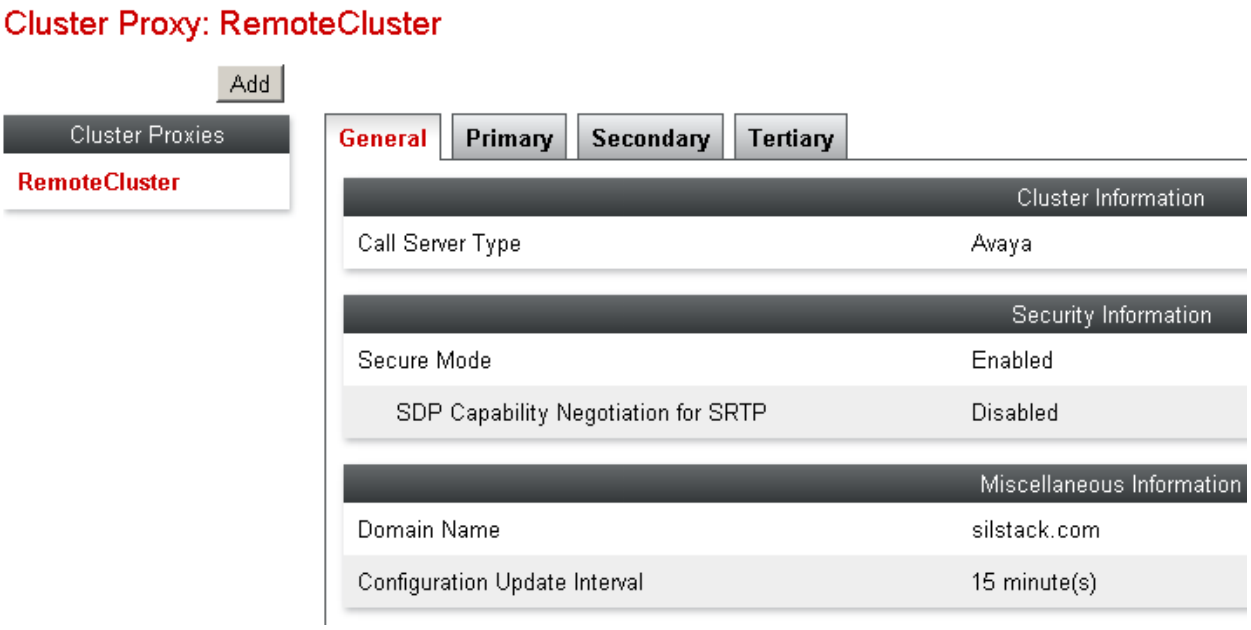
Repeat this procedure to add a Server Profile for SM2.The only change is the IP Address used as the next hop call server. Configure this as the IP address of the SM2 interface on DMZ SBCE, e.g., 172.17.10.12



6.1.8. Configure SIP Cluster Proxy

Navigate to **System Management→ SIP Cluster → Cluster Proxy** (not shown). Click **Add**.

Configure **Avaya** as the **Call Server Type**. Select the check box for **Secure Mode**. **SDP Capability Negotiation for** SRTP is disabled. Enter appropriate **Domain Name** and click **Next** (not shown).

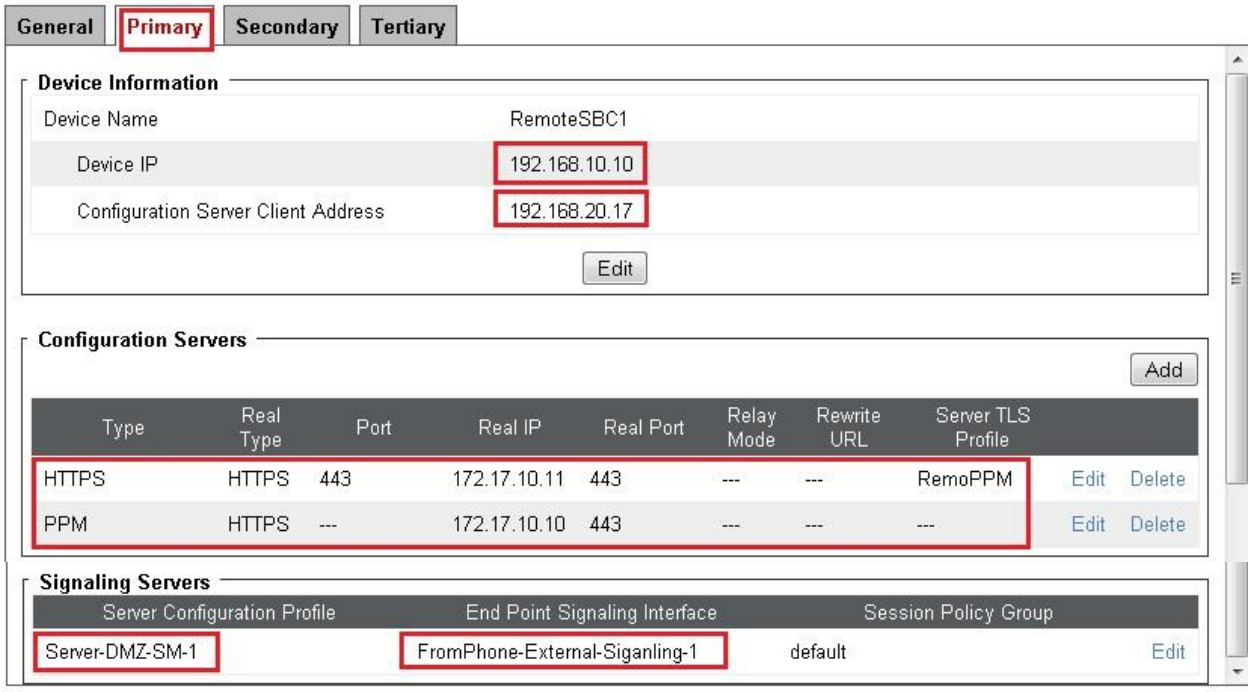


Configure the following for the Primary Cluster Proxy;

- Device IP — Remote SBCE SM1 External IP Address, e.g., 192.168.10.10
- Configuration Server Client Address — Remote SBCE SM1 Internal IP address, e.g., **192.168.20.17**

Add configuration servers for HTTPS and PPM. HTTPS is directed to the Relay IP Interface on the DMZ SBCE as configured in **Section 6.2.1**, e.g., **172.17.10.11** and will eventually route to the Utility Services file server (through SBCE b2b2b). PPM is directed to the SM1 external IP on the DMZ SBCE and will eventually route to Session Manager (through SBCE b2b2b). See the example in the screenshot below.

- Server Configuration Profile — Select the profile added in **Section 6.1.7**, e.g., **Server-DMZ-SM-1**
- End Point Signaling Interface — Enter the external interface for SM1 as created in **Section 6.1.3**, e.g., **FromPhone-External-Signaling-1**

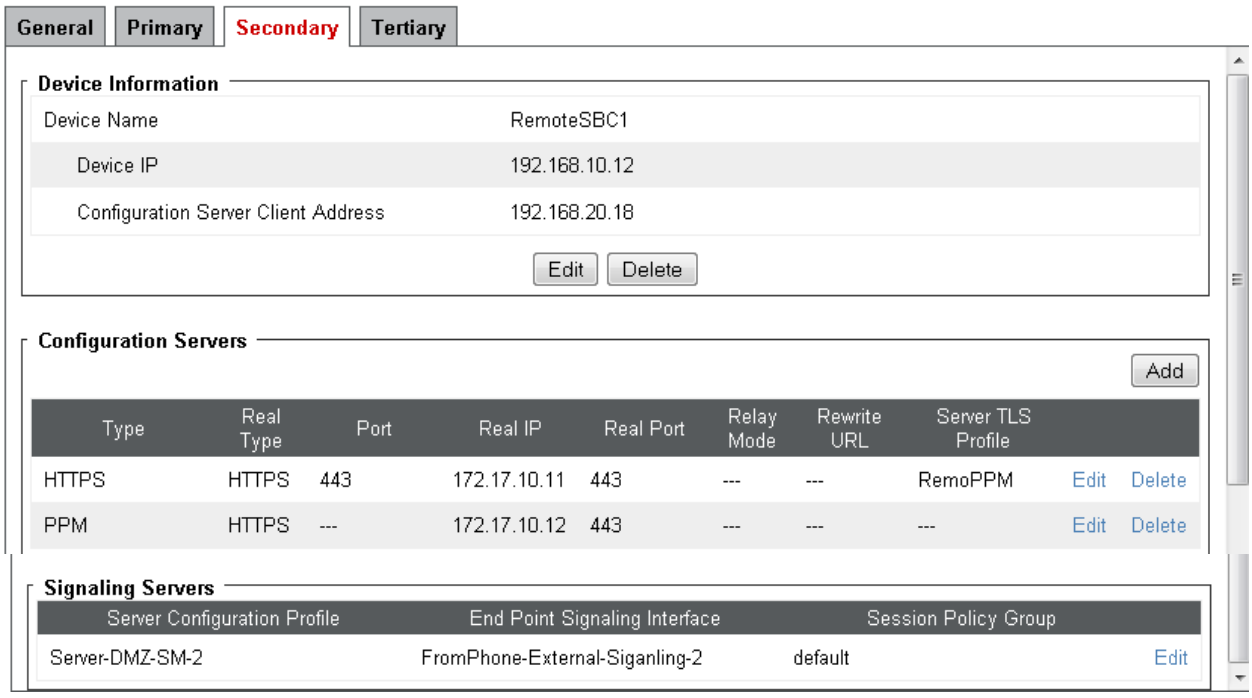


Configure the following for the Secondary Cluster Proxy;

- Device IP — Remote SBCE SM2 External IP Address, e.g., **192.168.10.12**
- Configuration Server Client Address — Remote SBCE SM2 Internal IP address, e.g., **192.168.20.18**

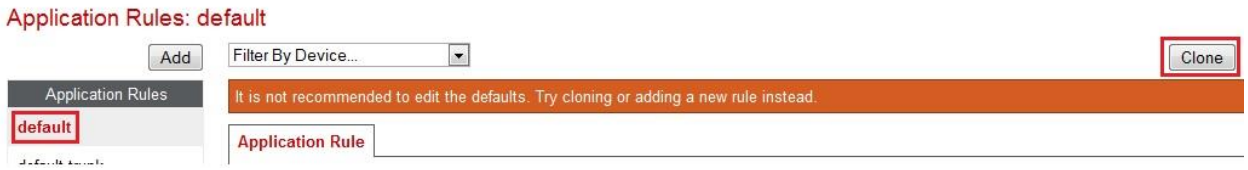
Add a configuration server for HTTPS and PPM. HTTPS port 443 will route to the Relay interface IP Address on DMZ SBCE on port 443, e.g., 172.17.10.11. PPM will route to the SM2 interface IP Address on DMZ SBCE on port 443, e.g., 172.17.10.12. See the example in the screenshot below.

- Server Configuration Profile — Select the profile added in **Section 6.1.7**, e.g., **Server-DMZ-SM-2**
- End Point Signaling Interface — Enter the external interface for SM1 as created in **Section 6.1.3**, e.g., **FromPhone-External-Signaling-2**



6.1.9. Configure Application Rules

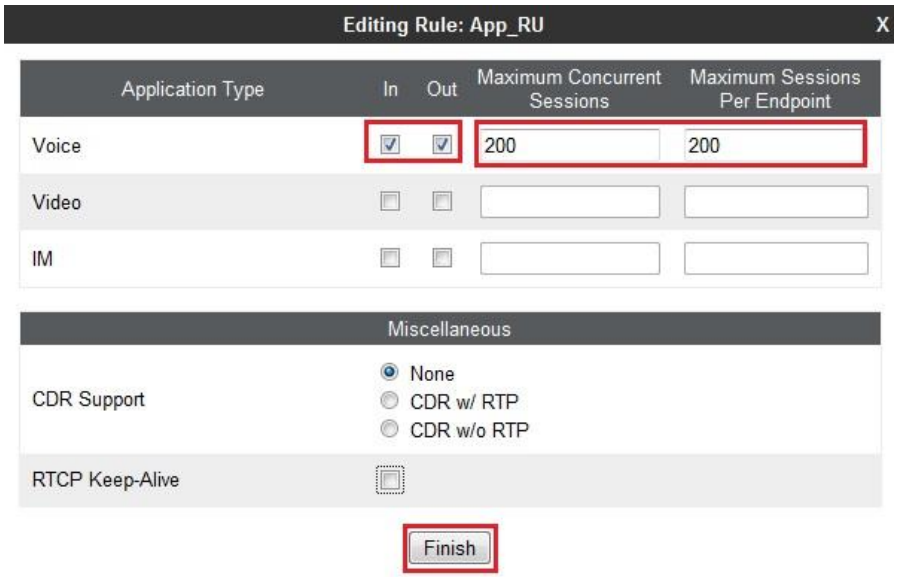
Navigate to **System Management → Domain Policies →Application Rules**. Select the **default** rule and click **Clone** to add a new application rule for remote users.



Enter a descriptive name for **Clone Name**, e.g., **App_RU**. Click **Finish** (not shown). Select the newly created application rule and click **Edit** (not shown). The example configuration uses the following values;

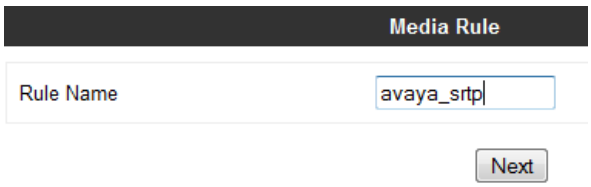
- Maximum Concurrent Sessions **200**
- Maximum Session Per Endpoint **200**

Click **Finish**.

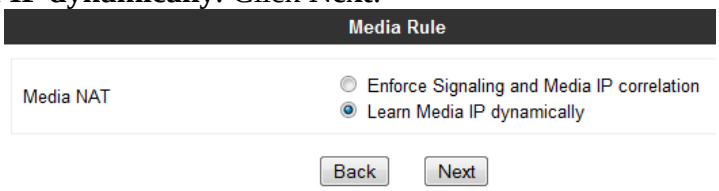


6.1.10. Configure Media Rules

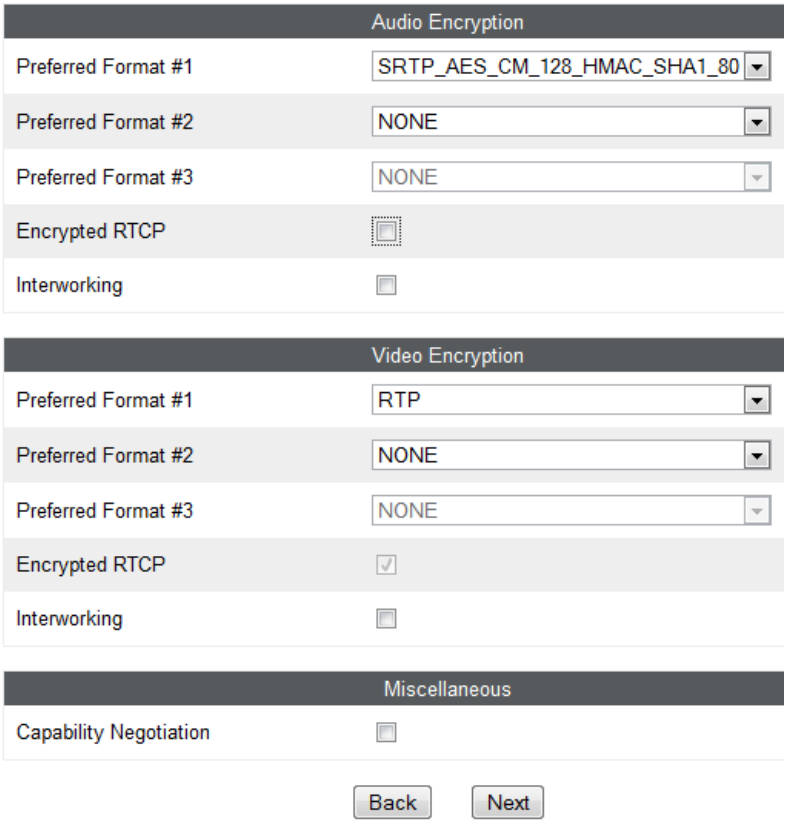
Navigate to **System Management → Domain Policies → Media Rules** (not shown). Click **Add** to create a new media rule. Enter a descriptive, e.g., **avaya_srtp**. Click **Next**.



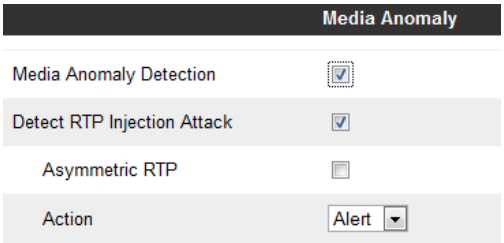
Select **Learn Media IP dynamically**. Click **Next**.



Under Audio Encryption, select **Preferred Format #1** as **SRTP_AES_CM_128_HMAC_SHA1_80**. Uncheck **Encrypted RTCP**. Click **Next**.



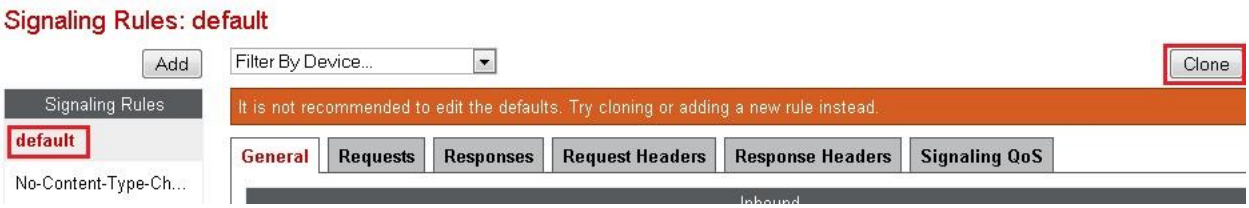
Check the box for **Media Anomaly Detection** and **Detect RTP Injection Attack** with **Alert Action**. Click **Next**.



Do not check the box for **Media Silencing** (not shown). Click **Next**. Do not check the box for **Media QoS Reporting** or for **Media QoS Marking** (not shown). Click **Finish** (not shown).

6.1.11. Configure Signaling Rules

Navigate to **System Management → Domain Policies → Signaling Rules** (not shown). Clone the default Signaling Rule by clicking the **Clone** button, while the **default** Signaling Rule is selected.



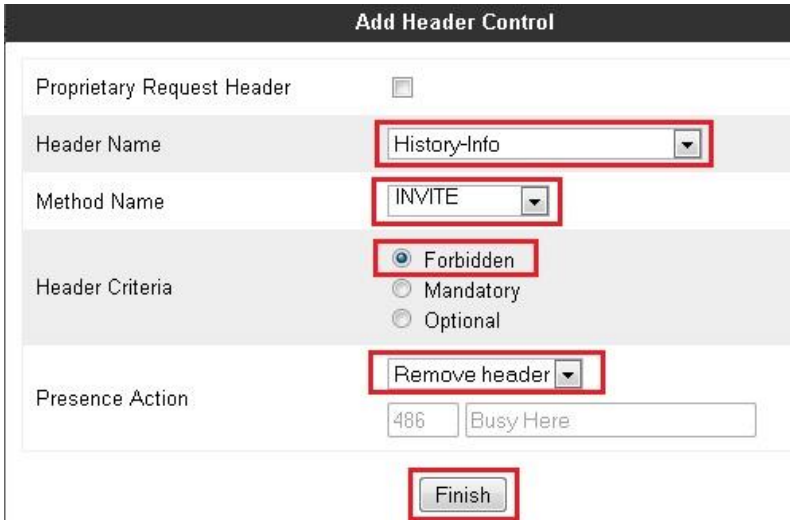
Enter a name for the cloned rule, e.g., **RemoSigRule** and click **Finish**.

Click on the **Request Headers** tab on the newly created rule. Click **Add In Header Control** (not shown).

Select the values below;

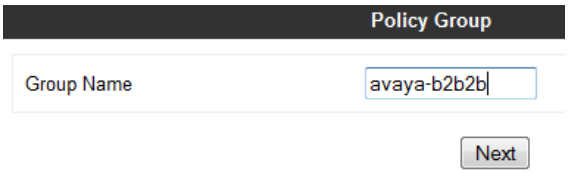
- Header Name **History-Info**
- Method Name **INVITE**
- Header Criteria **Forbidden**
- Presence Action **Remove Header**

Click **Finish**.



6.1.12. Configure Endpoint Policy Group

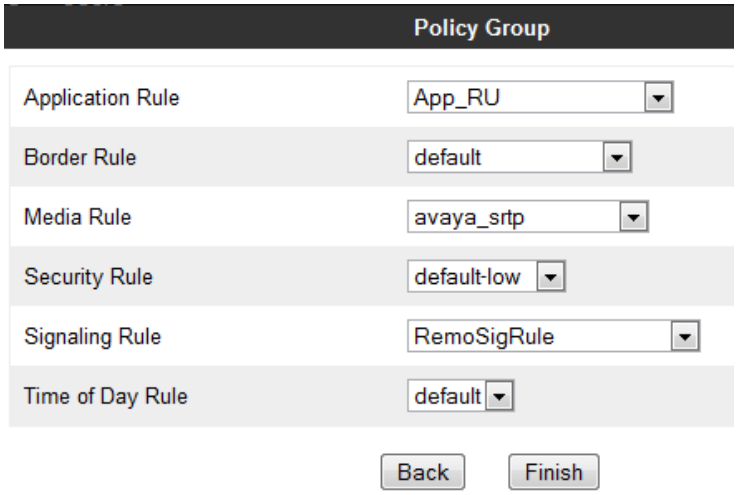
Navigate to **System Management → Domain Policies → End Point Policy Groups** (not shown). Create a new endpoint policy group by clicking **Add**. Enter a descriptive policy group name, e.g., **avaya-b2b2b**. Click **Next**.



Select the following values;

- Application Rule **App_RU** (rule created in **Section 6.1.9)**
- Border Rule **default**
- Media Rule **avaya_srtp** (rule created in **Section 6.1.10**)
- Security Rule **default-low**
- Signaling Rule **RemoSigRule** (rule created in **Section 6.1.11**)
- Time of Day **default**

Click **Finish**.



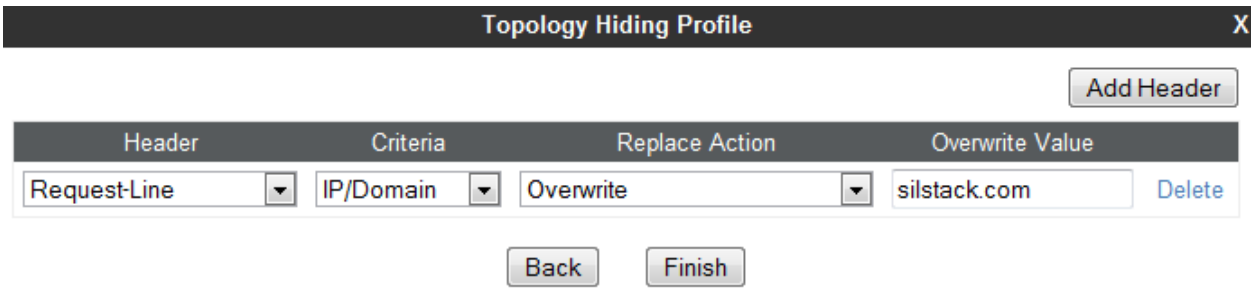
6.1.13. Create a Topology Hiding Profile

Navigate to **System Management →Global Profiles → Topology Hiding** (not shown). Click **Add** to create a new Topology Hiding Profile. Click **Next**.

Select the following values;

- Header **Request-Line**
- Criteria **IP/Domain**
- Replace Action **Overwrite**
- Overwrite Value Enter a domain name used on the network. E.g., **silstack.com**

Click **Add Header** button to add the next profile rule.



Enter criteria for **From** header as per the example below. Click **Add Header** to add a a rule for **To** header as per the example below. Click **Finish** (not shown).

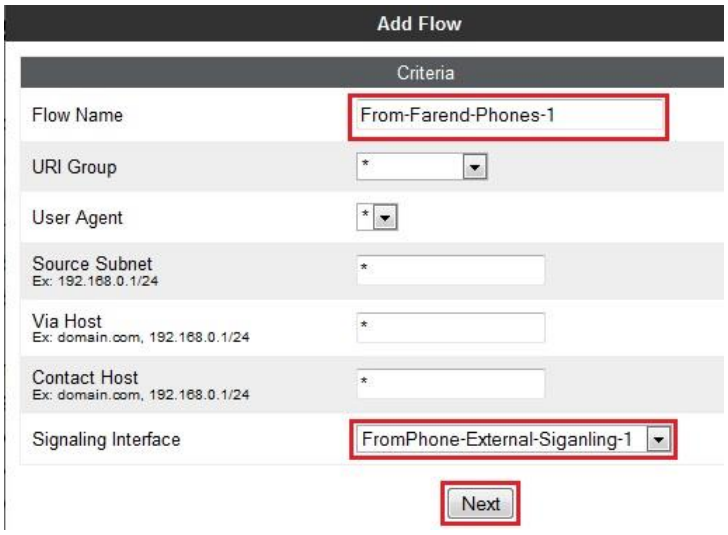
Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Overwrite	silstack.com
From	IP/Domain	Overwrite	silstack.com
To	IP/Domain	Overwrite	silstack.com

6.1.14. Create Endpoint Subscriber Flow

A subscriber flow is created for remote endpoints connecting to SM1. Navigate to **System Management → Device Specific Settings → End Point Flows** (not shown).

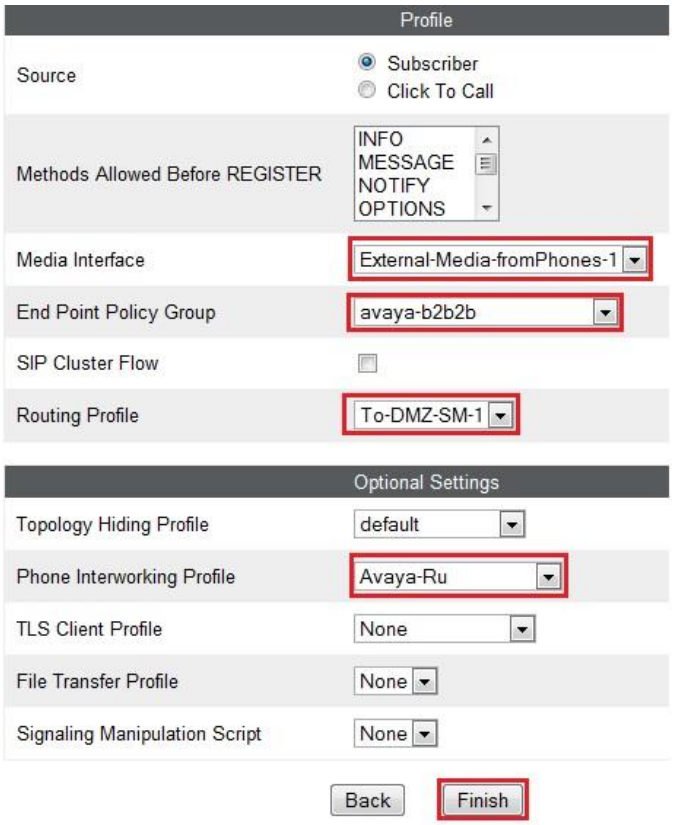
On the **Subscriber Flows** tab, click **Add** (not shown).

Enter a descriptive **Flow Name**, e.g. **From-Farend-Phones-1**. Select **Signaling Interface** for external side 1, created in **Section 6.1.3**, e.g., **FromPhone-External-Signaling-1**. Click **Next**.

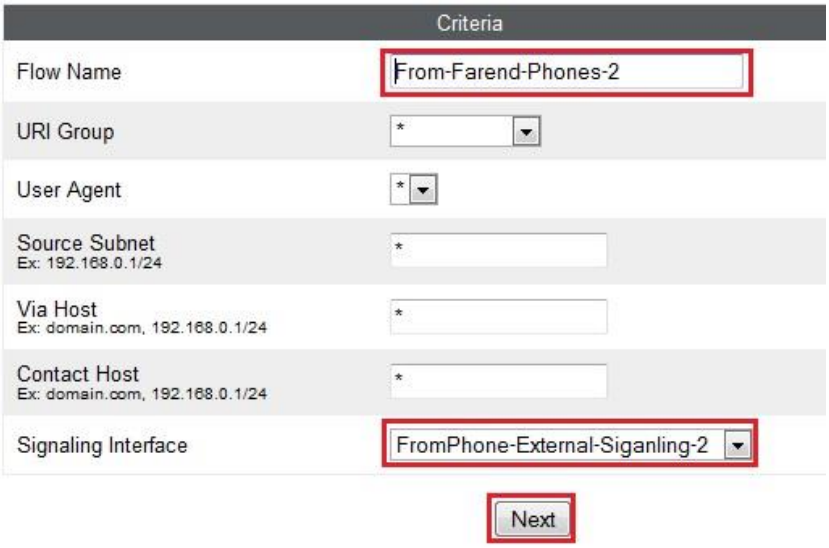


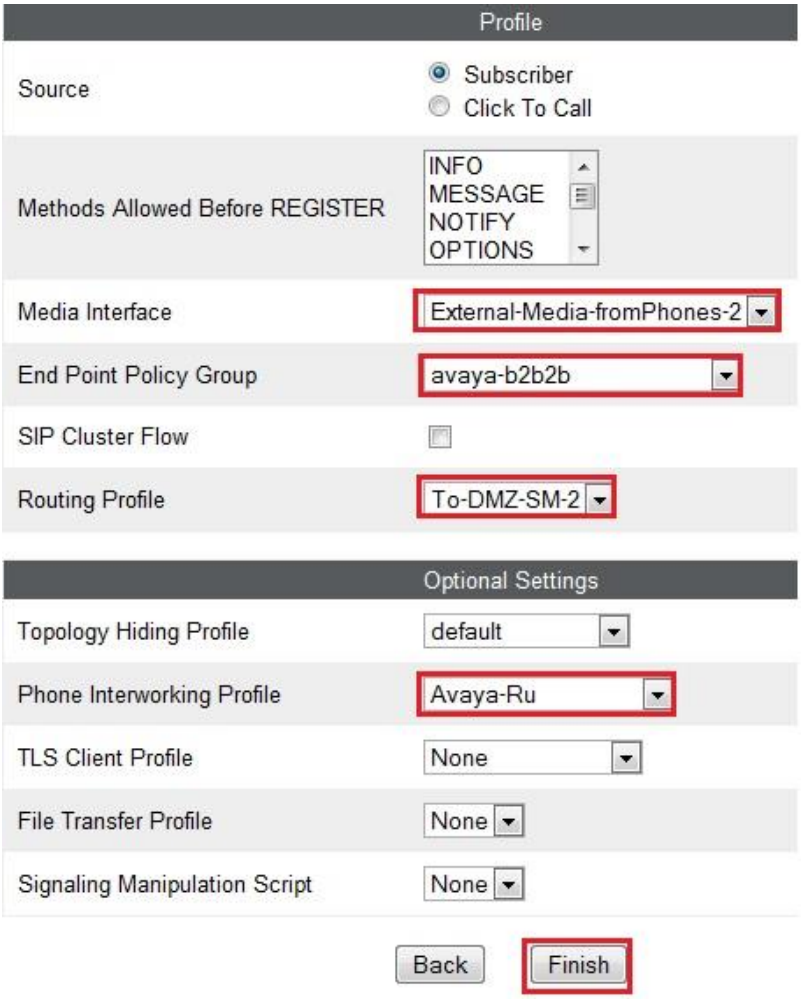
Select the following values and click **Finish**.

- Media Interface **External-Media-fromPhones-1**
- End Point Policy Group **Avaya-b2b2b** (as configured in **Section 6.1.12)**
- Routing Profile **To-DMZ-SM-1** (as configured in **Section 6.1.6**)
- Phone Interworking Profile **Avaya-Ru**



Repeat the above procedure to create a subscriber flow for remote endpoints connecting to SM2 in the event of failover. See the following screenshots for example settings.





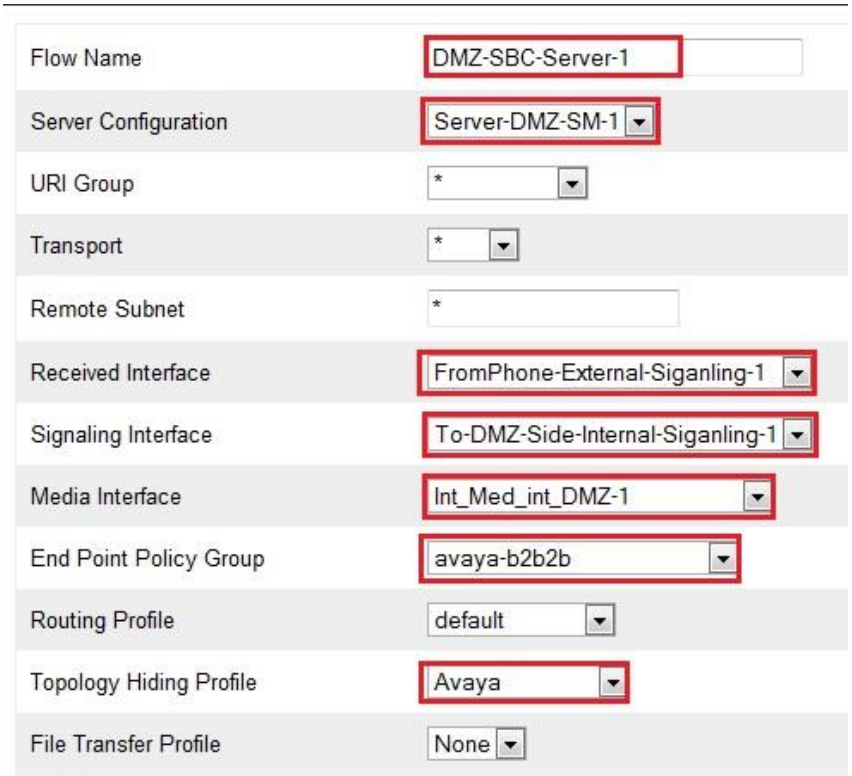
6.1.15. Create Endpoint Server Flow

A server flow is created for Avaya SBCE remote server connecting to DMZ SBCE for both SM1 and SM2.

Navigate to **System Management → Device Specific Settings → End Point Flows**. On the **Server Flows** tab (not shown), click **Add**. Enter the following values;

- Flow Name — A Descriptive Name, e.g. **DMZ-SBC-Server-1**.
- Server Configuration — Server Configuration for SM1 as per **Section 6.1.7**.
- Received Interface — **FromPhone-External-Signaling-1**.
- Signaling Interface — **To-DMZ-Side-Internal-Signaling-1**.
- Media Interface — **Int_Med_int_DMZ-1**.
- End Point Policy Group — **avaya-b2b2b** (As created in **Section 6.1.12)**.
- Topology Hiding Profile — **Avaya**, (as created in **Section 6.1.13)** .

Click **Finish** (not shown).



Repeat the above procedure for SM2 endpoint server flow as per the following screenshot. Click **Finish**.

Flow Name	DMZ-SBC-Server-2
Server Configuration	Server-DMZ-SM-2
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	FromPhone-External-Siganling-2
Signaling Interface	To-DMZ-Side-Internal-Siganling-2
Media Interface	Int_Med_int_DMZ-2
End Point Policy Group	avaya-b2b2b
Routing Profile	default
Topology Hiding Profile	Avaya
File Transfer Profile	None

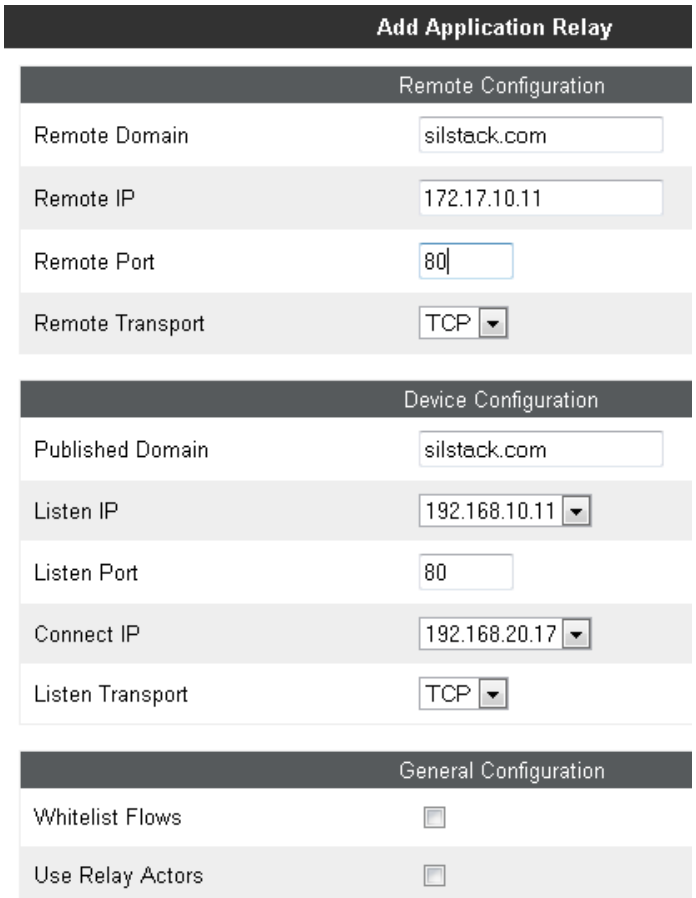
Finish

6.1.16. Configure Application Relay

The Relay on the Remote SBCE will generally relay traffic from Avaya SBCE external listening port to the relay port on the DMZ SBCE. The DMZ SBCE Relay, will in turn, forward the traffic to the relay on the Core SBC, which will relay packets to the appropriate application server. Relays can be configured for non-SIP traffic from remote phones to pass through the SBCE back-to-back-to-back network to an enterprise server on the core network. Such protocols include; HTTP, SCEP, and RTCP

Navigate to **System Management→Device Specific Settings→ Relay Services**. Click on the **Add** button (not shown).

Enter information for the listening IP address and port on the remote SBCE and the remote relay IP and port on the DMZ SBCE. The **Listen IP** is the external interface IP address used for relay. The **Connect IP** is the internal interface IP address used to connect from the Avaya SBCE to the application or next hop towards the application. The example below is for **HTTP port 80**. Click **Finish**.



.

Click **Add** button for each additional application relay. Listening port numbers on the remote SBCE external interface must be unique. There may be a requirement to route the same protocol to two different application servers in the core network. In this case a unique port is used, e.g., SCEP protocol uses HTTPS to route requests to a Certificate Authority server. The phone may also require HTTPS packets to route to the utility file server. Use listen port 443 for HTTPS relay and port 1023 to listen for SCEP requests. The remote phone is instructed via 46xxsettings file to send SCEP requests to port 1023. See **Reference [8]** for details on configuring SCEP on Avaya IP Deskphones.

The Application Relay configuration for sample network is shown below.

Devices

RemoteSBC1

Application Relay | File Transfer

Remote Domain	Remote IP:Port	Remote Transport	Published Domain	Listen IP:Port	Listen Transport	Connect IP
silstack.com	172.17.10.11:80	TCP	silstack.com	192.168.10.11:80	TCP	192.168.20.17
silstack.com	172.17.10.11:5222	TCP	silstack.com	192.168.10.10:5222	TCP	192.168.20.17
silstack.com	172.17.10.11:5222	TCP	silstack.com	192.168.10.12:5222	TCP	192.168.20.18
silstack.com	172.17.10.11:443	TCP	silstack.com	192.168.10.11:443	TCP	192.168.20.17
silstack.com	172.17.10.11:1023	TCP	silstack.com	192.168.10.11:1023	TCP	192.168.20.17

6.2. DMZ Avaya Session Border Controller for Enterprise Configuration

Configuration steps on the DMZ SBCE follow the same order as for the remote SBCE. Signaling, media rules, and routing will direct traffic incoming from the remote SBCE to the Core SBCE after applying analysis and rule changes. The steps involved are;

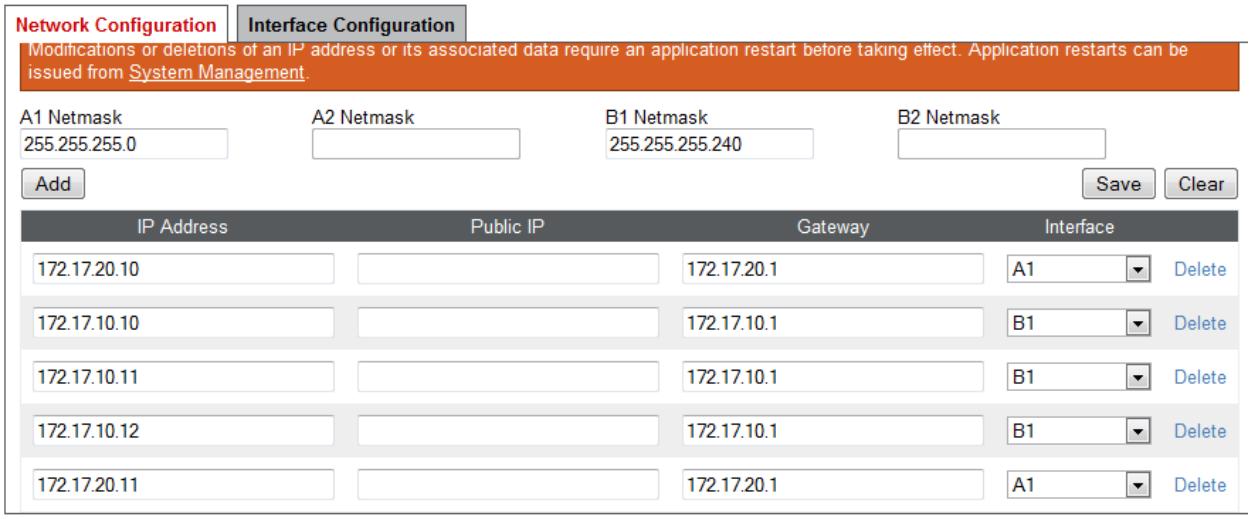
- Add network interfaces
- Create TLS profiles
- Add Signaling and Media Interfaces
- Create Server Interworking Profile
- Configure Routing
- Create Server Configuration Profile
- Configure SIP Cluster Proxy
- Create Application, Media and Signaling Rules, Endpoint Policy Group and Topology Hiding Profile.
- Configure Endpoint Subscriber Flow
- Configure Endpoint Server flow
- Configure Application Relays

6.2.1. Add Network Interfaces

Log into the DMZ SBCE EMS GUI by browsing to the management IP address or Fully Qualified Domain Name (FQDN) of the DMZ EMS server as described in **Section 6.1.1**. Enter **ucsec** for **Username** and enter appropriate **Password**. Click **Log In** button (not shown).

Navigate to **System Management → Device Specific Settings →Network Management** (not shown). As with remote SBCE, two A1 (Internal) and three B1 (External) interface IP addresses are required.

On the **Network** Configuration tab; enter the subnet mask for **A1 Netmask** and **B1 Netmask**. Enter an IP address and Gateway, and select and A1 or B1 interface from the drop-down menu as shown below. Click **Save**.



Click on the **Interface Configuration** tab and ensure one A1 and one B1 interface is enabled for both **HA Device #1** and **HA Device#2** (not shown).

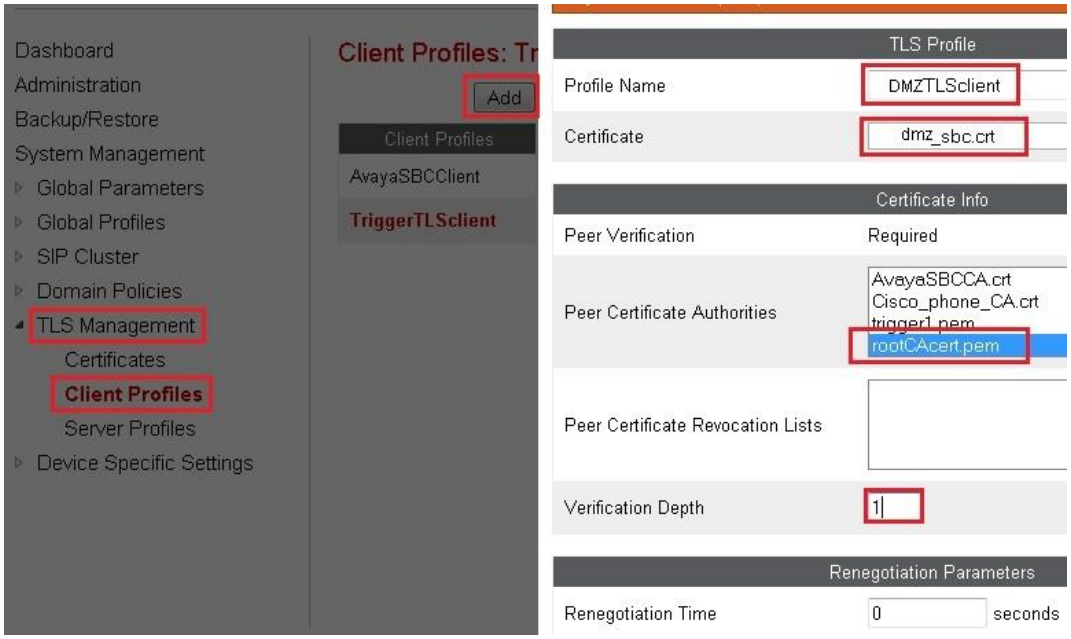
6.2.2. Create TLS Client and Server Profile

Refer to **Section 5** for installing third-party signed TLS certificates.

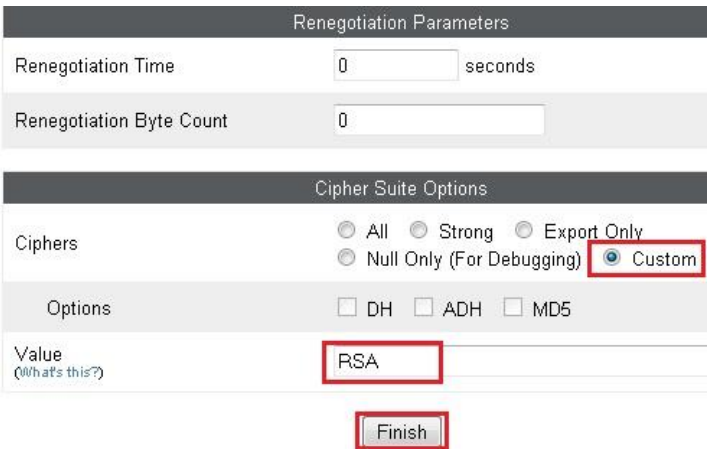
Navigate to **System Management → TLS Management → Client Profiles** (not shown).

Repeat the procedure as described in **Section 6.1.2** for DMZ SBCE.

Click **Add** to create a new TLS client Profile. Enter a **descriptive** Profile Name. Select the TLS identity **Certificate** created in **Section 5,** e.g., **dmz_sbc.crt**.Select the trusted root CA certificate added in **Section 5** as the **Peer Certificate Authorities**. Add a number for the level of **Verification Depth** on the root CA certificate chain, e.g., **1**.



Select **Custom** option for **Ciphers** and provide a value of **RSA**. Click **Finish**.



Create a TLS Server profile as per details in **Section 6.1.2** using the certificate created for DMZ. Peer verification is required for the TLS Server profile. Create a TLS Server profile to be used for PPM as per **Section 6.1.2** and again, use the signed identity certificate created for DMZ SBCE.

6.2.3. Add Signaling Interfaces

A signaling interface is added for both of the external and internal interfaces used for signaling. Navigate to **System Management → Device Specific Settings →Signaling Interface** and click on **Add** (not shown). Enter a **Name** to describe the interface, e.g., **FromRemote-External-Signaling-1**. Select an **IP Address** from the drop down menu. The IP address list is extracted from the network management interfaces. Enter a TCP, UDP and TLS Port value. Select the **TLS Profile** as the server profile created in **Section 6.2.2**, e.g., **dmzTLSserver**. Click **Finish** (not shown). The resulting output is shown below.

Signaling Interface

dmzTLSserver

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile
FromRemote-External-Signaling-1	172.17.10.10	5060	5060	5061	dmzTLSserver
To-Core-Internal-Signaling-1	172.17.20.10	5060	5060	5061	dmzTLSserver
From-Remote-External-Signaling-2	172.17.10.12	5060	5060	5061	dmzTLSserver
To-Core-Internal-Signaling-2	172.17.20.11	5060	5060	5061	dmzTLSserver

6.2.4. Add Media Interfaces

Navigate to **System Management→ Device Specific Settings →Media Interfaces** and click **Add** (not shown). Enter a descriptive name for the interface. It is useful to include internal or external, and direction in which the media is flowing, in the descriptive **Name**. Select the interface **IP Address** from the drop-down menu. Modify the port range if required. Click **Finish**. The resulting output in shown below;

Media Interface

Modifying or deleting an existing media interface will require an application restart before taking effect. Applic
issued from System Management.

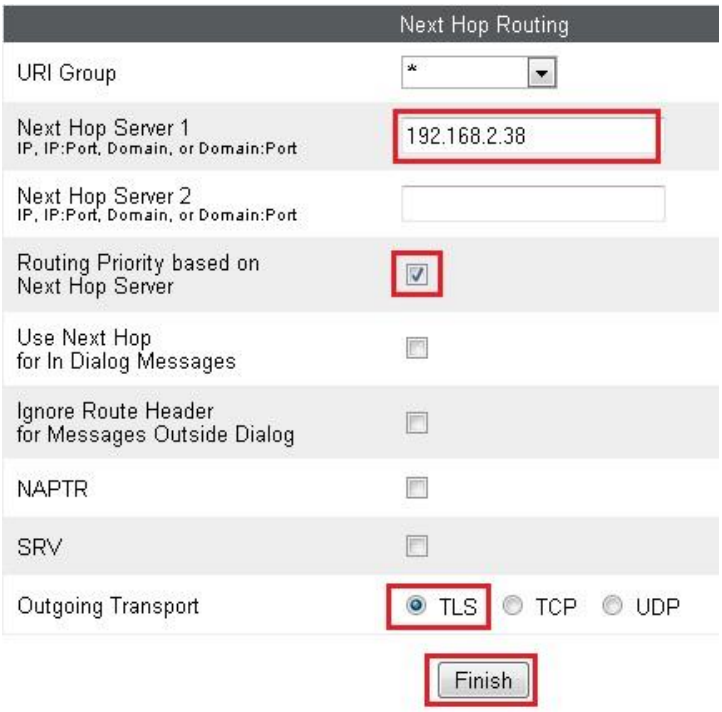
Name	Media IP	Port Range
Int_Media_intf_Core-1	172.17.20.10	35000 - 40000
Ext_Med_intf_REMO-1	172.17.10.10	35000 - 40000
Int_Media_intf_Core-2	172.17.20.11	35000 - 40000
Ext_Media_intf_REMO-2	172.17.10.12	35000 - 40000

6.2.5. Create Server Interworking Profile

Create a server interworking profile as per **Section 6.1.5**

6.2.6. Configure Routing

Create two routing rules as part of a multiple Session Manager network; first rule for SM1 and second rule for SM2. The next hop will be the external IP address for SM1 interface on Core SBCE or the external IP address for SM2 interface on the Core SBCE. Navigate to **System Management → Global Profiles → Routing**. Click **Add** (not shown)**.** Enter a **Profile Name** for routing rule one, e.g., **To-DMZ-SM-1**. Click **Next** (not shown). Enter SM1 IP address of DMZ for **Next Hop Server 1**, e.g., **192.168.2.38**. Select the check box for **Routing Priority based on Next Hop Server**. Select **TLS** as the Outgoing Transport protocol. Click **Finish**.



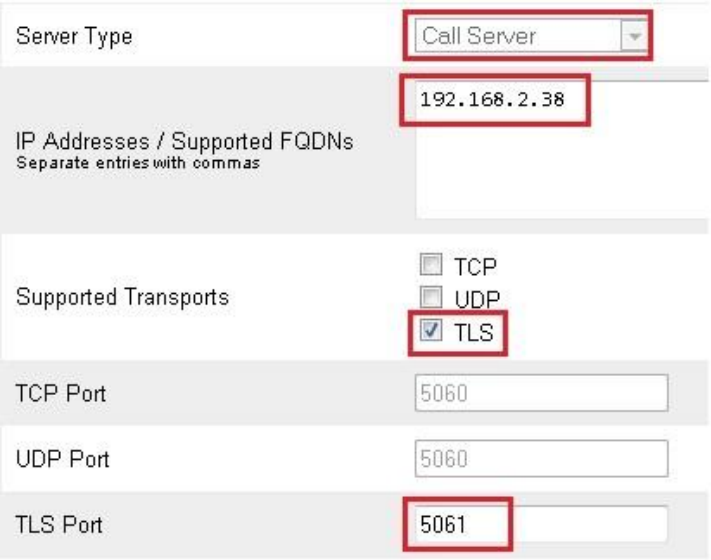
Click **Add** to create a new routing profile for SM2. Enter the external IP address for SM2 on the Core SBCE interface as the **Next Hop** server, e.g., **192.168.2.43**. Configure the other settings to be the same as the profile for SM1.

6.2.7. Add Server Configuration

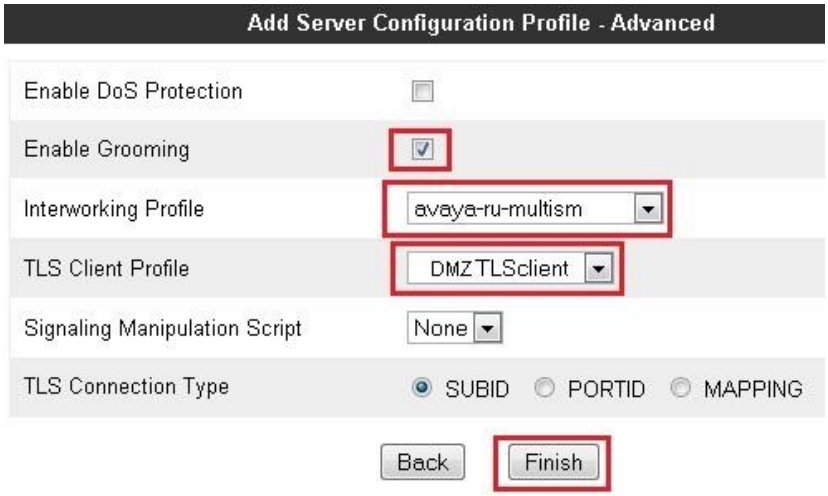
Navigate to **System Management→Global Profiles→Server Configuration**. Add two server profiles; for SM1 and SM2. The IP address is the next hop IP address on route to the Session Manager in the core. In the DMZ SBCE, the next hop is the Core SBCE. Click **Add** (not shown).

Enter a descriptive server configuration profile name, e.g., **Server-Core-SM-1** (not shown) and click **Next**.

Select **Call Server** as the **Server Type** and enter the IP address of SM1 Interface on Core SBCE. Select **TLS** as the supported transport protocol and **TLS Port 5061**. Click **Next** (not shown).



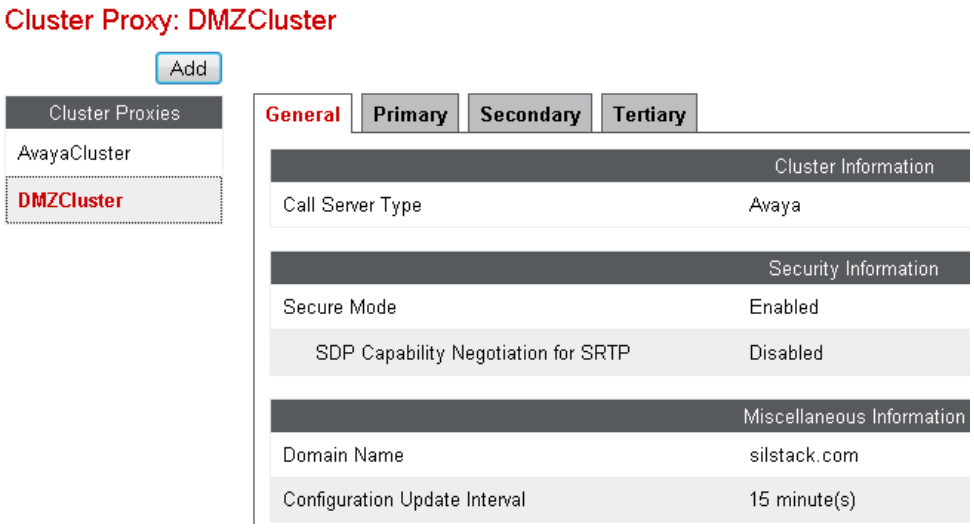
Do not enable authentication. Click **Next**. Do not enable heartbeat. Click **Next**. Select the checkbox beside **Enable Grooming**. Select the **Interworking Profile** created in **Section 6.2.5** and the **TLS Client Profile** created in **Section 6.2.2**. Click on **Finish**.



6.2.8. Configure SIP Cluster Proxy

Navigate to **System Management→ SIP Cluster → Cluster Proxy** and click **Add**.

Configure **Avaya** as the **Call Server Type**. Select the check box for **Secure Mode**. Enter a **Domain Name** and click **Next** (not shown).

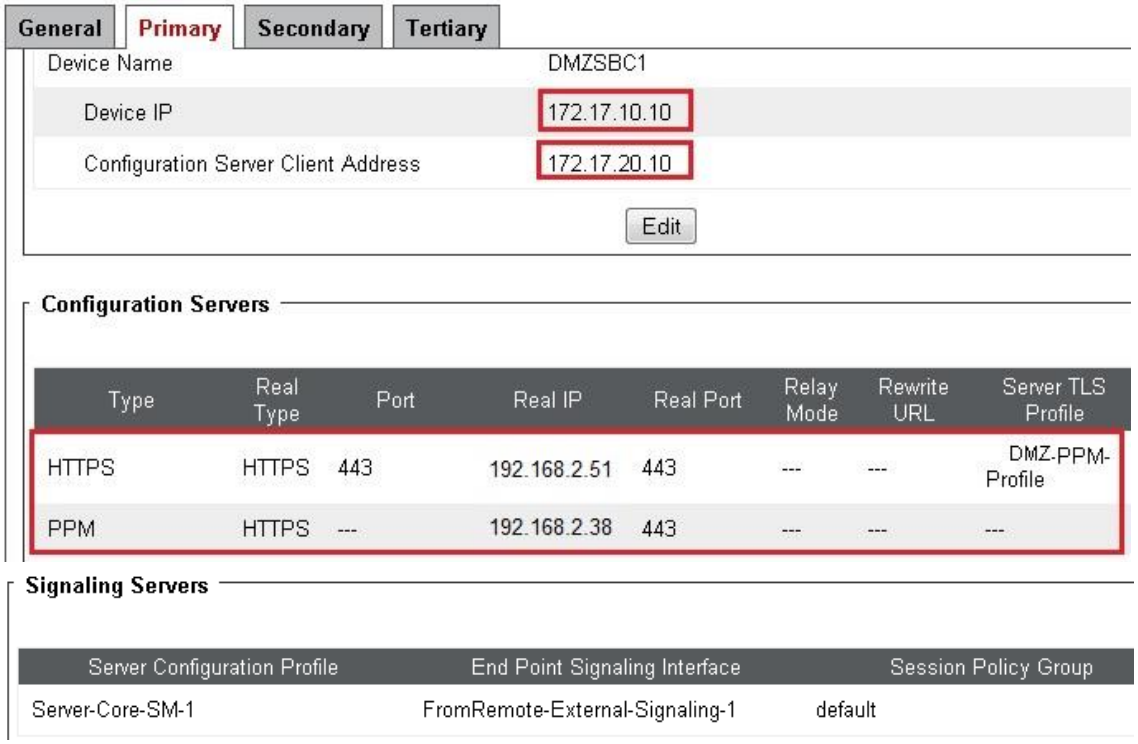


Configure the following for the Primary Cluster Proxy;

- Device IP — DMZ SBCE SM1 External IP Address, e.g., **172.17.10.10**
- Configuration Server Client Address — DMZ SBCE SM1 Internal IP address, e.g., **172.17.20.10**

Add configuration servers for HTTPS and PPM. HTTPS is directed to the Relay IP Interface on the Core SBCE as configured in **Section 6.3.1**, e.g., **192.168.2.51** and will eventually route to the Utility file server (through core Avaya SBCE). PPM is directed to the SM1 external IP on the core Avaya SBCE and will eventually route to Session Manager (through core Avaya SBCE). See the example in the screenshot below.

- Server Configuration Profile — Select the profile added in **Section 6.2.7**, e.g., **Server-Core-SM-1**
- Endpoint Signaling Interface — External interface for SM1 as created in **Section 6.2.3**, e.g., **FromRemote-External-Signaling-1**

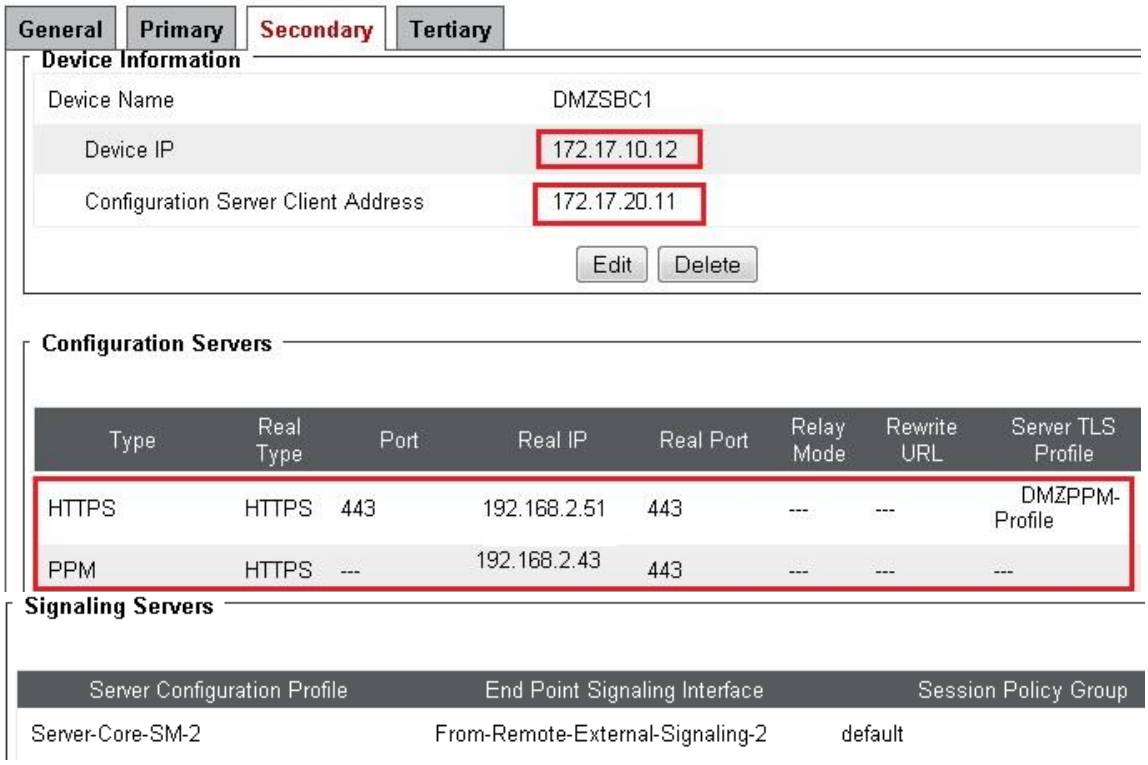


Configure the following for the Secondary Cluster Proxy;

- Device IP — DMZ SBCE SM2 External IP Address, e.g., **172.17.10.12**
- Configuration Server Client Address — DMZ SBCE SM2 Internal IP address, e.g., **172.17.20.11**

Add a configuration server for HTTPS and PPM. HTTPS port 443 will route to the Relay interface IP Address on Core SBCE on port 443, e.g., **192.168.2.51**. PPM will route to the SM2 interface IP Address on Core SBCE on port 443, e.g., **192.168.2.43**.

- Server Configuration Profile — Select the profile added in **Section 6.2.7**, e.g., **Server-Core-SM-2**
- Endpoint Signaling Interface — External interface for SM1 as created in **Section 6.2.7**, e.g., **FromRemote-External-Signaling-2**



6.2.9. Create Application, Media and Signaling Rules, End Point Policy Group, and Topology Hiding Profile

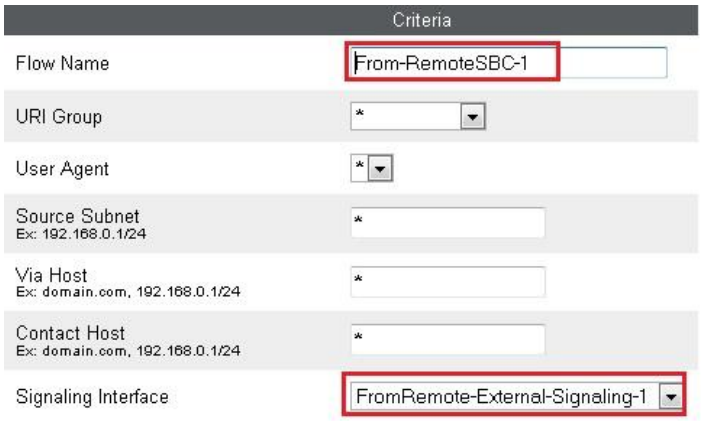
Create application rules as per **Section 6.1 9** and create media rules are per **Section 6.1.10**. Create signaling rules called **DMZSigRule** for example, as per instructions in **Section 6.1.11**. Create an endpoint policy group as per details in **Section 6.1.12**.Create a Topology Hiding Profile as per details in **Section 6.1.13**.

6.2.10. Create Endpoint Subscriber Flow

A subscriber flow is created for endpoint traffic passing through DMZ SBCE from remote SBCE en-route to Core SBCE.

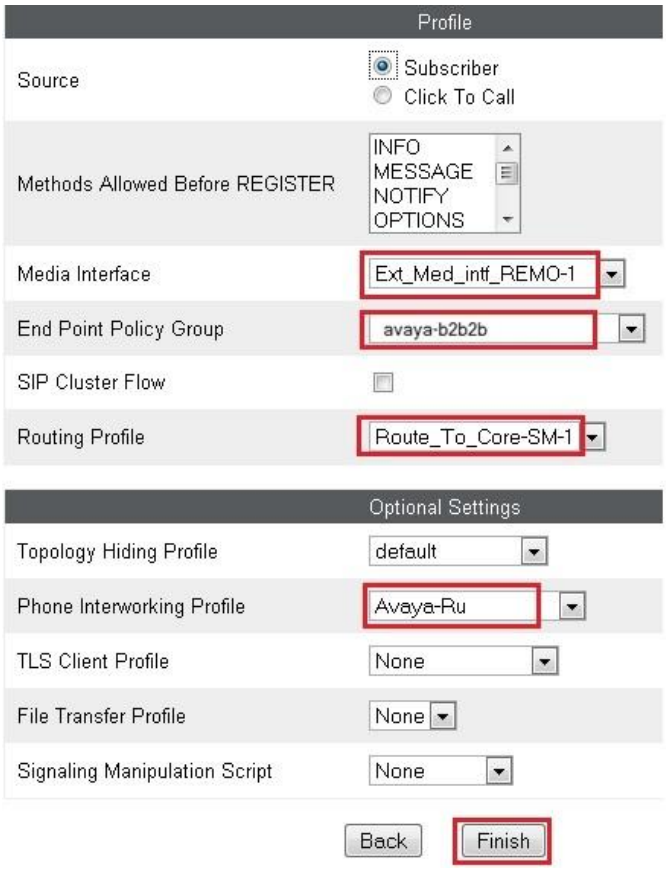
Navigate to **System Management → Device Specific Settings → End Point Flows**. On the **Subscriber Flows** tab, click **Add** (not shown).

Enter a descriptive **Flow Name**, e.g. **From-RemoteSBC-1**. Select the **Signaling Interface** for SM1 external, created in **Section 6.2.3**, e.g., **FromRemote-External-Signaling-1**. Click **Next**.



Select the following values and click **Finish**.

- Media Interface — Select **Ext_Med_intf_REMO-1**.
- End Point Policy Group — Select **Avaya-b2b2b**.
- Routing Profile — Select **Route_To_Core-SM-1** (as configured in **Section 6.2.6**).
- Phone Interworking Profile — Select **Avaya-Ru**.



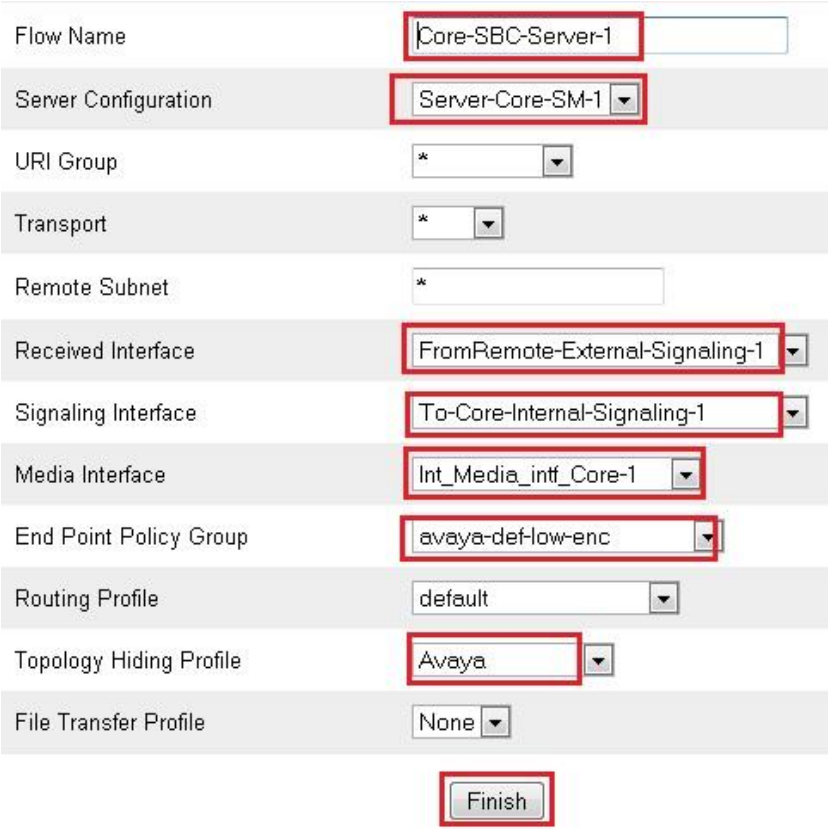
6.2.11. Create Endpoint Server Flow

A server flow is created for DMZ SBCE server connecting to Core SBCE for both SM1 and SM2.

Navigate to **System Management → Device Specific Settings → End Point Flows**. On the **Server Flows** tab and click **Add** (not shown). Enter the following values;

- Flow Name — A Descriptive Name, e.g. **Core-SBC-Server-1**
- Server Configuration — Server Configuration for SM1 as per **Section 6.2.7**
- Received Interface — **FromRemote-External-Signaling-1**
- Signaling Interface — **To-Core-Internal-Signaling-1**
- Media Interface — **Int_Med_intf_Core-1**
- End Point Policy Group — As created in **Section 6.2.9**, **avaya-b2b2b**
- Topology Hiding Profile — As created in **Section 6.2.9**, **Avaya**

Click **Finish**.



6.2.12. Configure Application Relay

The Relay on the DMZ SBCE will relay traffic from the SBCE external listening port to the relay port on the Core SBCE. The Core SBCE Relay, will in turn, forward the traffic to the appropriate application server. Navigate to **System Management→Device Specific Settings→ Relay Services** and click on the **Add** button (not shown).

Enter information for the listening IP address and port on the DMZ SBCE and the remote relay IP and port on the Core SBCE. The example below is for HTTP port 80. Click **Finish** (not shown).

Remote Configuration	
Remote Domain	silstack.com
Remote IP	192.168.2.51
Remote Port	80
Remote Transport	TCP

Device Configuration	
Published Domain	silstack.com
Listen IP	172.17.10.11
Listen Port	80
Connect IP	172.17.20.10
Listen Transport	TCP

General Configuration	
Whitelist Flows	☐
Use Relay Actors	☐

The example Application Relays configured on the DMZ SBCE are shown below and are described in more detail in **Section 6.1.16**;

Application Relay | File Transfer

Remote Domain	Remote IP:Port	Remote Transport	Published Domain	Listen IP:Port	Listen Transport	Connect IP
silstack.com	192.168.2.51:5222	TCP	silstack.com	172.17.10.10:5222	TCP	172.17.20.10
silstack.com	192.168.2.51 :5222	TCP	silstack.com	172.17.10.12:5222	TCP	172.17.20.11
silstack.com	192.168.2.51:443	TCP	silstack.com	172.17.10.11:443	TCP	172.17.20.10
silstack.com	192.168.2.51:80	TCP	silstack.com	172.17.10.11:80	TCP	172.17.20.10
silstack.com	192.168.2.51:1023	TCP	silstack.com	172.17.10.11:1023	TCP	172.17.20.10
silstack.com	192.168.2.51:5005	UDP	silstack.com	172.17.10.11:5005	UDP	172.17.20.10

6.3. Core Avaya Session Border Controller for Enterprise Configuration

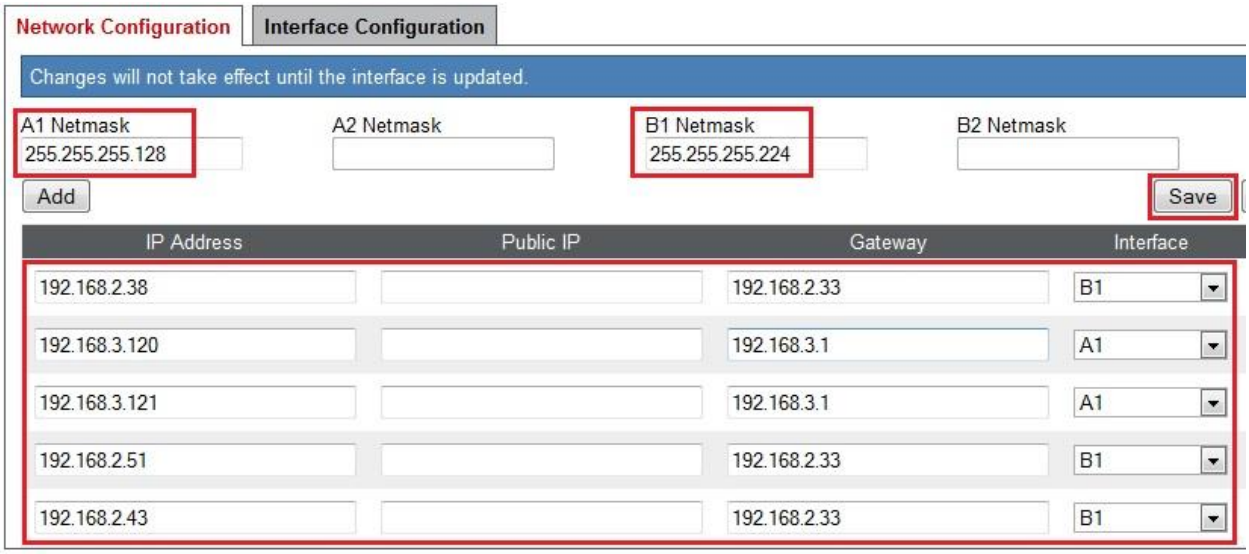
Configuration steps on the Core SBCE follow the same order as for the DMZ SBCE. Signaling, media rules, and routing will direct traffic incoming from the DMZ SBCE to the Core Session Managers, after applying analysis and rule changes. The steps involved are;

- Add network interfaces
- Create TLS profiles
- Add Signaling and Media Interfaces
- Create Server Interworking Profile and configure Routing
- Create Server Configuration Profile
- Configure SIP Cluster Proxy
- Create Application, Media and Signaling Rules, Endpoint Policy Group and Topology Hiding Profile.
- Configure Endpoint Subscriber Flow
- Configure Endpoint Server flow
- Configure Application Relays

6.3.1. Add Network Interfaces

Log into the core SBCE EMS GUI as described in **Section 6.1.1** by browsing to the management IP address or Fully Qualified Domain Name (FQDN) of the core EMS server. Enter **ucsec** for **Username** and enter appropriate **Password**. Click **Log In** button (not shown).

Navigate to **System Management → Device Specific Settings →Network Management** (not shown). As with remote and DMZ SBCE, two A1 (Internal) and three B1 (External) interface IP addresses are required. On the **Network** Configuration tab; enter the subnet mask for **A1 Netmask** and **B1 Netmask**. Enter an IP address and Gateway, and select and A1 or B1 interface from the drop-down menu as shown below. Click **Save**.



Click on the **Interface Configuration** tab and ensure one A1 and one B1 interface is enabled for both **HA Device #1** and **HA Device#2** (not shown).

6.3.2. Create TLS Client and Server Profiles

Refer to **Section 5** for installing third-party signed TLS certificates. Navigate to **System Management → TLS Management → Client Profiles**. Repeat the procedure as described in **Section 6.1.2** and **Section 6.2.2** for core SBCE. Click **Add** to create a new TLS client Profile. Enter a **descriptive** Profile Name. Select the TLS identity **Certificate** created in **Section 5,** e.g., **core_sbc.crt**. Select the trusted root CA certificate added in **Section 5** as the **Peer Certificate Authorities**. Add a number for the level of **Verification Depth** on the root CA certificate chain, e.g., **1**. Select **Custom** option for **Ciphers** and provide a value of **RSA**. Click **Finish**.

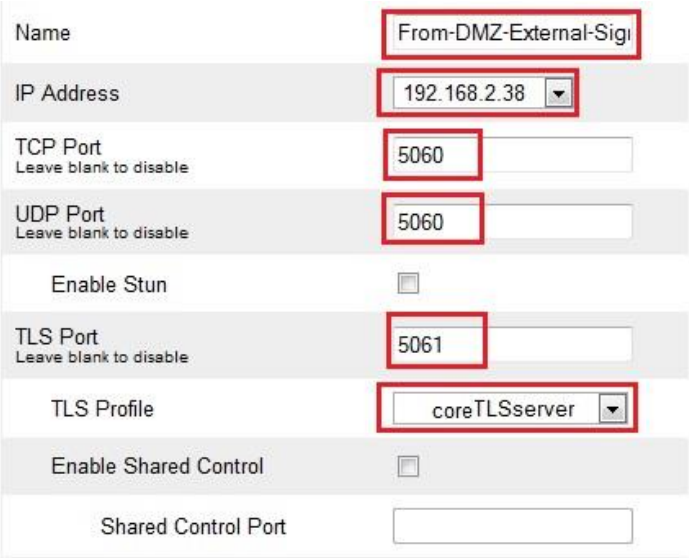
Create a TLS Server profile as per details in **Section 6.1.2** using the certificate created for core SBCE. Create a TLS Server profile to be used for PPM as per **Section 6.1.2** and again, use the signed identity certificate created for core SBCE.

6.3.3. Add Signaling Interfaces

A signaling interface is added for both of the external and internal interfaces used for signaling.

Navigate to **System Management → Device Specific Settings →Signaling Interface** and click on **Add** (not shown). Enter the following details and click **Finish** (not shown).

- Name — Enter a descriptive name, e.g., **From-DMZ-External-Signaling-1**
- IP Address — Select from the drop down menu. The IP address list is extracted from the network management interfaces.
- TCP Port — **5060**
- UDP Port — **5060**
- TLS Port — **5061**
- TLS Profile — As created in **Section 6.3.2**, e.g., **coreTLSserver**



Repeat this action to add all signaling interfaces. The resulting output is shown below.

Signaling Interface

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile
From-DMZ-External-Signaling -1	192.168.2.38	5060	5060	5061	coreTLSserver
To-ASM-Internal-Signaling-1	192.168.3.120	5060	5060	5061	coreTLSserver
From-DMZ-External-Signaling -2	192.168.2.43	5060	5060	5061	coreTLSserver
To-ASM-Internal-Signaling-2	192.168.3.121	5060	5060	5061	coreTLSserver

6.3.4. Add Media Interfaces

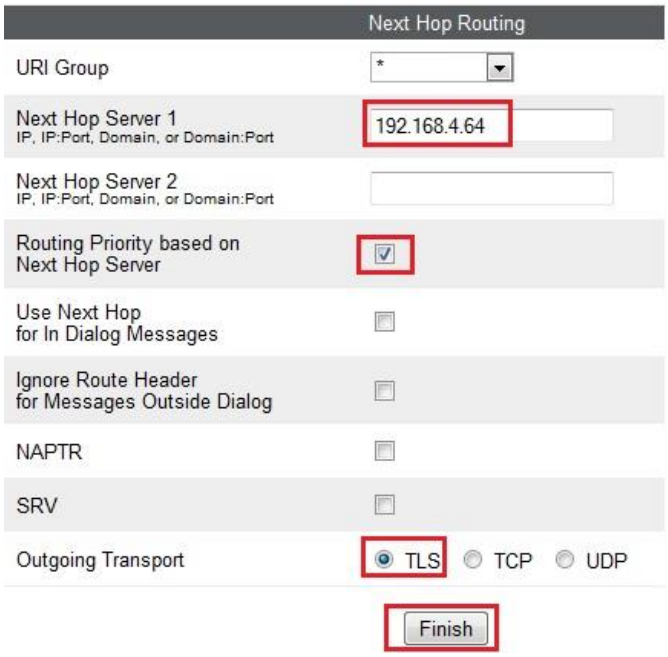
Navigate to **System Management→ Device Specific Settings →Media Interfaces**. Click **Add.**

Repeat the procedure as described in **Section 6.1.4** and **Section 6.2.4**. Enter a descriptive name for the interface. It is useful to include internal or external, and direction in which the media is flowing, in the descriptive **Name**. Select the interface **IP Address** from the drop-down menu. Modify the port range if the network requires this. Click **Finish**. The resulting output in shown below;

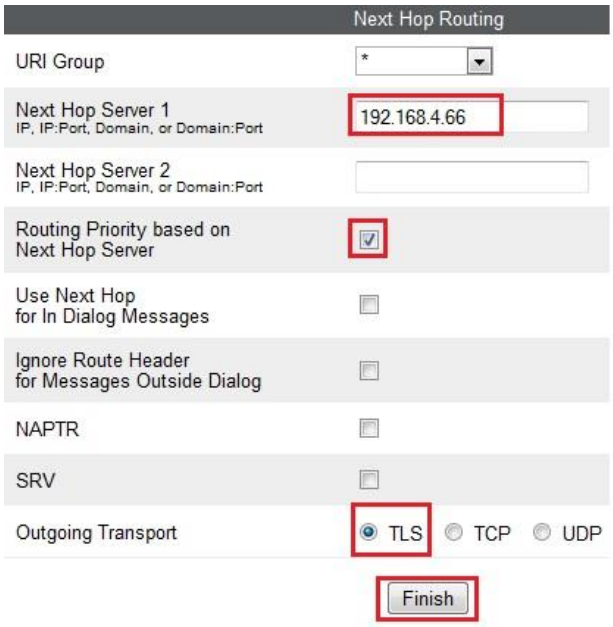
Name	Media IP	Port Range
Int_Med_intf_ASM-1	192.168..3.120	35000 - 40000
Ext_Med_intf_DMZ-1	192.168.2.38	35000 - 40000
Int_Media_intf_ASM-2	192.168.3.121	35000 - 40000
Ext_Media_intf_DMZ-2	192.168.2.43	35000 - 40000

6.3.5. Create Server Interworking profile and Configure Routing

Create a server interworking profile as per **Section 6.1.5.** Create two routing rules as part of multiple Session Manager network; first rule for SM1 and second rule for SM2. The next hop from core SBCE will be the primary Session Manager (SM1) or secondary Session Manager (SM2). Navigate to **System Management → Global Profiles → Routing**. Click **Add** (not shown)**.** Enter a **Profile Name** for routing rule one, e.g., **Route_To_SM-1**. Click **Next** (not shown). Enter IP address of primary Session Manager for **Next Hop Server 1**, e.g., **192.168.4.64**. Select the check box for **Routing Priority based on Next Hop Server**. Select **TLS** as the Outgoing Transport protocol. Click **Finish**.



Click **Add** to create a new routing profile for secondary Session Manager (SM2). Enter the secondary Session Manager (SM2) IP as the **Next Hop** server, e.g., **192.168.4.66**. Check the box for **Routing Priority based on Next Hop Server**. Select **TLS** for **Outgoing Transport** and click **Finish**.



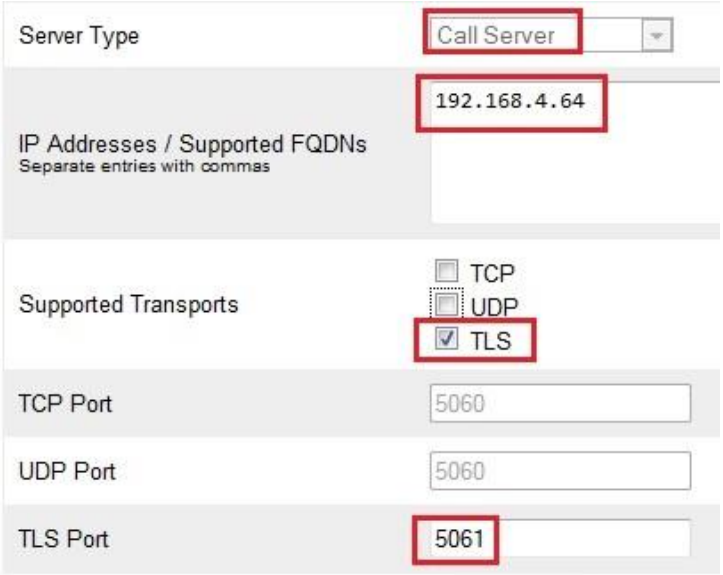
6.3.6. Add Server Configuration

Add two server profiles; for SM1 and SM2. The IP address is the next hop server, i.e., primary Session Manager (SM1) or secondary Session Manager (SM2).

Navigate to **System Management→Global Profiles→Server Configuration**. Click **Add**. Enter a descriptive server configuration profile name, e.g., **Server -SM-1** and click **Next** (not shown).

Enter the following values and click **Next** (not shown).

- Server Type **Call Server**
- IP Addresses IP address for primary Session Manager. E.g., **192.168.4.64**
- Supported transports **TLS**
- TLS Port **5061**



Do not enable authentication. Click **Next** (not shown). Click **Next** (not shown).

Enter the following values and click **Next**.

- Enable Heartbeat — Check the box.
- Method — Select **OPTIONS**.
- Frequency — Enter **30** seconds.
- From URI — SIP user configured on System Manager User Management for heartbeat polling mechanism only, e.g., **22011@silstack.com**. See **Section 6.1.7** for more details.
- To URI — Same as From URI, e.g., **22011@silstack.com**.

Enable Heartbeat	☑
Method	OPTIONS
Frequency	30 seconds
From URI	22011@silstack.com
To URI	22011@silstack.com

6.3.7. Configure SIP Cluster proxy

On the core SBC EMS; navigate to **System Management→ SIP Cluster → Cluster Proxy**. Click **Add**.

Configure **Avaya** as the **Call Server Type**. Select the check box for **Secure Mode**. Enter a **Domain Name** and click **Next** (not shown).

General | Primary | Secondary | Tertiary

Cluster Information	
Call Server Type	Avaya

Security Information	
Secure Mode	Enabled
SDP Capability Negotiation for SRTP	Disabled

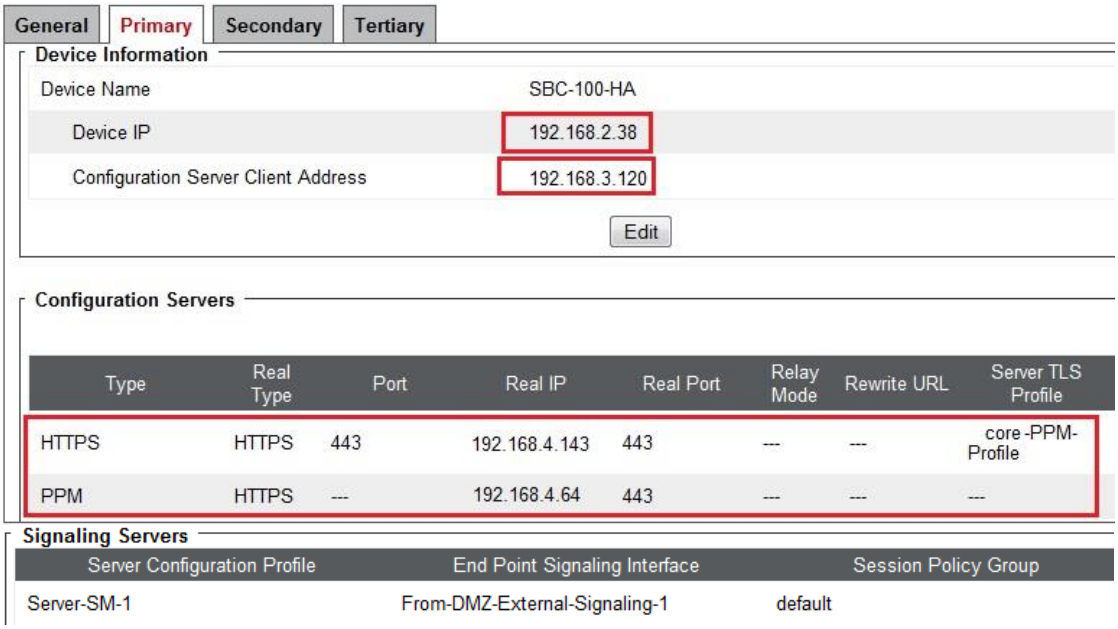
Miscellaneous Information	
Domain Name	silstack.com
Configuration Update Interval	15 minute(s)

Configure the following for the Primary Cluster Proxy;

- Device IP — Core SBCE SM1 External IP Address, e.g., **192.168.2.38**
- Configuration Server Client Address — Core SBCE SM1 Internal IP address, e.g., **192.168.3.120**

Add configuration servers for HTTPS and PPM. HTTPS is directed to the Utility Services file server IP address within the Core network, e.g., **192.168.4.143**. PPM is directed to the primary Session Manager IP, e.g., **192.168.4.64**. See the example in the screenshot below.

- Server Configuration Profile — Select the profile added in **Section 6.3.6**, e.g., **Server-SM-1**
- Endpoint Signaling Interface — External interface for SM1 as created in **Section 6.3.3**, e.g., **From-DMZ-External-Signaling-1**



Configure the following for the Secondary Cluster Proxy;

- Device IP — Core SBCE SM2 External IP Address, e.g., **192.168.2.43**
- Configuration Server Client Address — Core SBCE SM2 Internal IP address, e.g., **192.168.3.121**

Add configuration servers for HTTPS and PPM. HTTPS is directed to the Utility Services file server IP address within the Core network, e.g., **192.168.4.143**. PPM will route to secondary Session Manager on port 443, e.g., **192.168.4.66**.

- Server Configuration Profile — Select the profile added in **Section 6.3.6**, e.g., **Server-SM-2**
- Endpoint Signaling Interface — External interface for SM1 as created in **Section 6.3.6**, e.g., **From-DMZ-External-Signaling-2**

6.3.8. Create Application, Media and Signaling Rules, End Point Policy Group, and Topology Hiding Profile

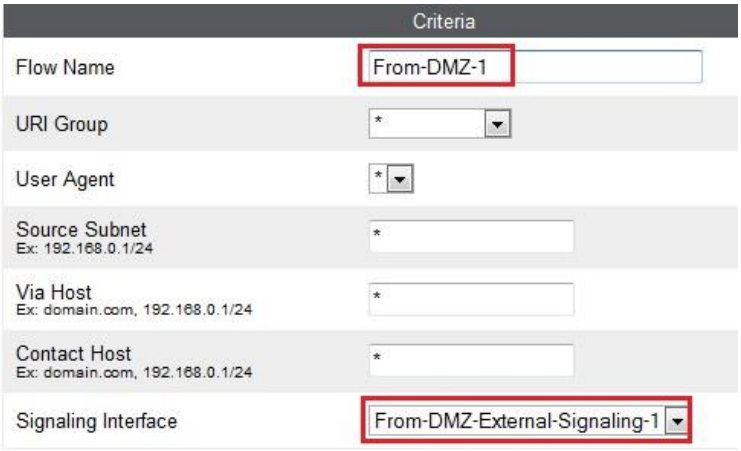
Create Application Rules as per **Section 6.1.9** and create Media Rules as per **Section 6.1.10**. Create a signaling rule called **CoreSigRule** for example, as per instructions in **Section 6.1.9**. Create an Endpoint Policy Group as per details in **Section 6.1.12**.Create a Topology Hiding Profile as per details in **Section 6.1.13**

6.3.9. Create Endpoint Subscriber Flow

A subscriber flow is created for traffic from remote endpoints passing through core SBCE to Session Manager. Navigate to **System Management → Device Specific Settings → End Point Flows**. On the **Subscriber Flows** tab, click **Add** and enter the following details;

- Flow Name — Enter a descriptive name, e.g. **From-DMZ-1**
- Signaling Interface — Select interface for SM1 external, created in **Section 6.3.3**, e.g., **From-DMZ-External-Signaling-1**

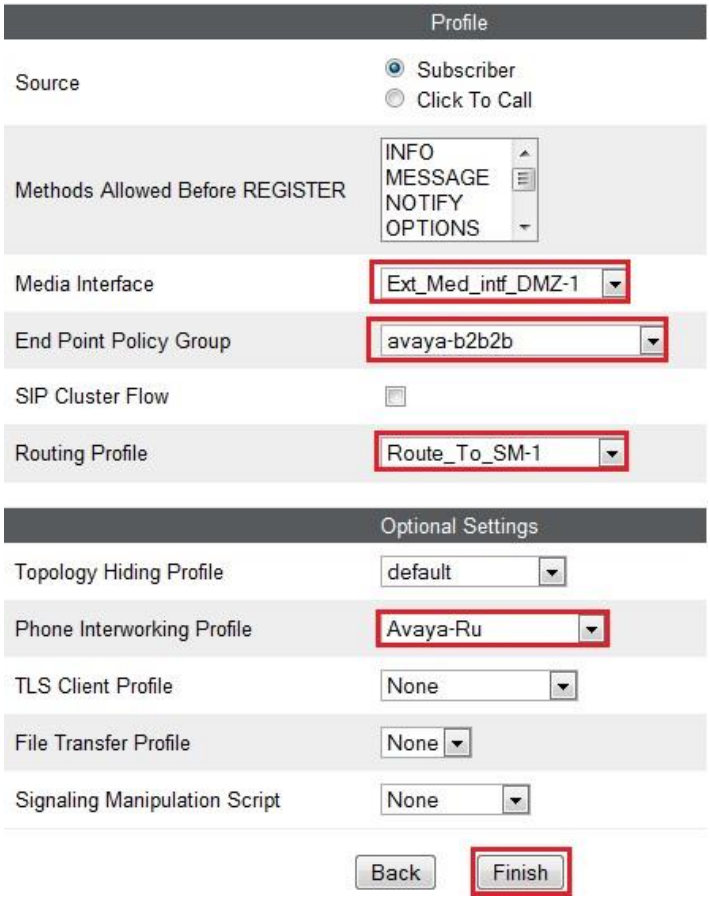
Click **Next** (not shown).



Select the following values;

- Media Interface **Ext_Med_intf_DMZ-1**
- End Point Policy Group **avaya-b2b2b**
- Routing Profile **Route_To_SM-1**
- Phone Interworking Profile **Avaya-Ru**

Click **Finish**.

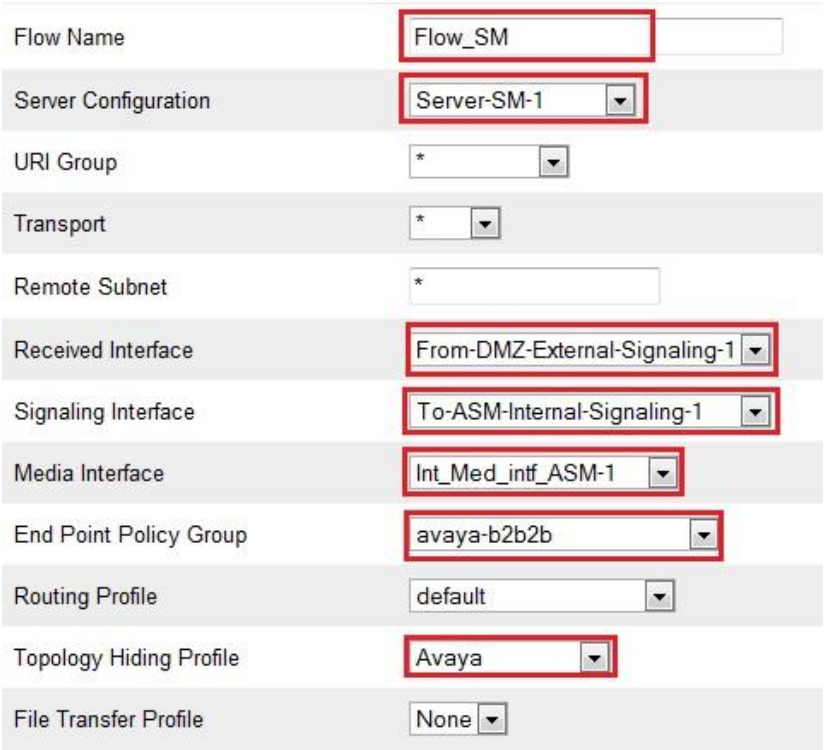


6.3.10. Create Endpoint Server Flow

A server flow is created for core SBCE server connecting to both primary and secondary Session Managers. Navigate to **System Management → Device Specific Settings → End Point Flows**. On the **Server Flows** tab, click **Add**. Enter the following values;

- Flow Name — A Descriptive Name, e.g. **Flow_SM**
- Server Configuration — Server Configuration as per **Section 6.3.6**, Server-SM-1
- Received Interface — **From-DMZ-External-Signaling-1**
- Signaling Interface — **To-ASM-Internal-Signaling-1**
- Media Interface — **Int_Med_intf_ASM-1**
- End Point Policy Group — As created in **Section 6.3.8**, **avaya-b2b2b**
- Topology Hiding Profile — As created in **Section 6.3.8**, **Avaya**

Click **Finish**(not shown).



6.3.11. Configure Application Relay

The Relay on the core SBCE will relay traffic from the SBCE external listening port to the various application servers within the core enterprise.

Navigate to **System Management→Device Specific Settings→ Relay Services**. Click on the **Add** button.

Enter information for the listening IP address and port on the core SBCE and the remote IP and port on the application server. The example below is for HTTP port 80. Click **Finish**.

Remote Configuration	
Remote Domain	silstack.com
Remote IP	192.168.4.143
Remote Port	80
Remote Transport	TCP

Device Configuration	
Published Domain	silstack.com
Listen IP	192.168.2.38
Listen Port	80
Connect IP	192.168.3.120
Listen Transport	TCP

General Configuration	
Whitelist Flows	☐
Use Relay Actors	☐

The example core SBCE relay settings are shown in the screenshot below.

Application Relay | **File Transfer**

Remote Domain	Remote IP:Port	Remote Transport	Published Domain	Listen IP:Port	Listen Transport	Connect IP
silstack.com	192.168.4.143:80	TCP	silstack.com	192.168.2.51:80	TCP	192.168.3.120
silstack.com	135[redacted]:5222	TCP	silstack.com	135.[redacted]:5222	TCP	192.168.3.121
silstack.com	135.[redacted]:5222	TCP	silstack.com	135[redacted]:5222	TCP	192.168.3.121
silstack.com	192.168.4.143:443	TCP	silstack.com	192.168.2.51:443	TCP	192.168.3.120
silstack.com	192.168.4.143:80	TCP	silstack.com	192.168.2.38:80	TCP	192.168.3.120
silstack.com	192.168.4.142:80	TCP	silstack.com	192.168.2.51:1023	TCP	192.168.3.120
silstack.com	10.129.37.7:5005	UDP	silstack.com	192.168.2.51 :5005	UDP	192.168.3.120
silstack.com	10.129.37.7:5005	UDP	silstack.com	192.168.3.120 :5005	UDP	192.168.3.121

7. Configure remote 9641 IP Deskphone

See **Reference [5]** for details on how to configure 9641 IP Deskphone SIP. This section highlights the main settings to be configured to enable remote registrations and enable SRTP. Configuration is accomplished by modifying the **46xxsettings.txt** file.

Groups are used to allow configuration settings for remote IP Deskphones and core enterprise IP Deskphones on the same 46xxsettings file. In this example, Group 300 is used for the remote site and this group number is manually entered into the phone configuration menu. For the **SIP_CONTROLLER_LIST** parameter, enter the IP addresses of the external interface (B1) on the remote SBCE as described in **Section 6.1.1**, e.g., **192.168.10.10** and **192.168.10.12**

In this example, the speakerphone on the IP deskphone is disabled for additional security, using the **SPEAKERSTAT 0** setting.

SCEP is configured to direct requests to the relay IP address (e.g., 192.168.10.11) on the external interface of the remote SBCE using the **MYCERTURL** setting. Remote SBCE relay is configured to direct the SCEP request through the SBCE back-to-back-to-back deployment and onto the SCEP service on the Windows 2008 Server Certificate Authority.

Note: port number **1023** is configured as a listening port on remote SBCE for HTTP packets to distinguish between SCEP HTTP traffic and utility file server HTTP traffic on port 80.

The CA server will assign a unique identity certificate to the phone based on the serial number of the phone, according to the **MYCERTCN** setting. See **Reference [8]** for details on SCEP configuration. Use the **TRUSTCERTS** setting to configure the third-party CA trusted root certificate to be downloaded to the phone. This trusted root certificate file rootCAcert.pem is downloaded from the utility services file server. The settings **HTTPSSRVR** and **HTTPSRVR** are configured to direct HTTP/S requests to the external relay IP address on the remote SBCE, e.g., 192.168.10.11. The relay configuration on the SBCE back-to-back-to-back deployment will direct this traffic to the Utility file server.

In this example, firewalls are used across the network with rules to allow RTP packets on a specific range of ports. The settings **RTP_PORT_LOW** and **RTP_PORT_RANGE** are used to configure the phone to use RTP ports within this range. The setting **MEDIAENCRYPTION** is enabled for SRTP.

```
##############################################################
# GROUP_300
##########  Add SET Statements for GROUP 300 below  ############
##########  Remote SBC TLS Phone SETTINGS #######

SET SIP_CONTROLLER_LIST
192.168.10.10:5061;transport=tls,192.168.10.12:5061;transport=tls
SET CONFIG_SERVER_SECURE_MODE 2
SET SIMULTANEOUS_REGISTRATIONS 2
SET ENABLE_PPM_SOURCED_SIPPROXYSRVR 0
SET HTTPSRVR 192.168.10.11
```

```
SET HTTPPORT 80
SET HTTPSSRVR 192.168.10.11
SET HTTPSPORT 443
SET SIPDOMAIN "silstack.com"
SET FAILBACK_POLICY auto
SET SIPREGPROXYPOLICY simultaneous
SET TPSLIST 192.168.10.11
SET SUBSCRIBELIST http://192.168.10.11/push/subscribe.php
SET COUNTRY "USA"
SET WAIT_FOR_REGISTRATION_TIMER 40
SET RECOVERYREGISTERWAIT 10
SET CONTROLLER_SEARCH_INTERVAL 16
SET SDPCAPNEG 0
SET ENABLE_G711U 1
SET FAST_RESPONSE_TIMEOUT 4
SET SPEAKERSTAT 0
SET MUTE_ON_REMOTE_OFF_HOOK 0
SET MYCERTURL http://192.168.10.11:1023/certsrv/mscep/mscep.dll
SET MYCERTCN $SERIALNO
SET MYCERTDN /C=US/ST=Colorado/L=Denver/O=Avaya
SET MYCERTCAID EjbSubCA
SET MYCERTKEYLEN 2048
SET TLSSRVRID 0
SET MEDIAENCRYPTION "1"
SET RTP_PORT_LOW 35000
SET RTP_PORT_RANGE 5000
SET TRUSTCERTS rootCAcert.pem
```

8. Verification Steps

This section includes instructions to verify the SBCE back-to-back-to-back deployment is successfully using third-party TLS certificates and multiple Session Manager registration is working.

8.1. Verify Avaya Session Border Controller for Enterprise

Log in to each SBCE EMS and confirm the status of HA pair. Navigate to **System Management** and ensure one SBCE is showing as **Primary** and the other is **Secondary**. Check the **Status** is displayed as **Commissioned**.

Use a packet capture trace on SBCE to verify TLS handshake is successful between the remote phone and remote SBCE, SBCE to SBCE, and between the core SBCE and Session Manager. Log into SBCE using SSH client as user **ipcs**. Issue the command **sudo su** to change to **root** user. Start a packet capture by issuing the following command;

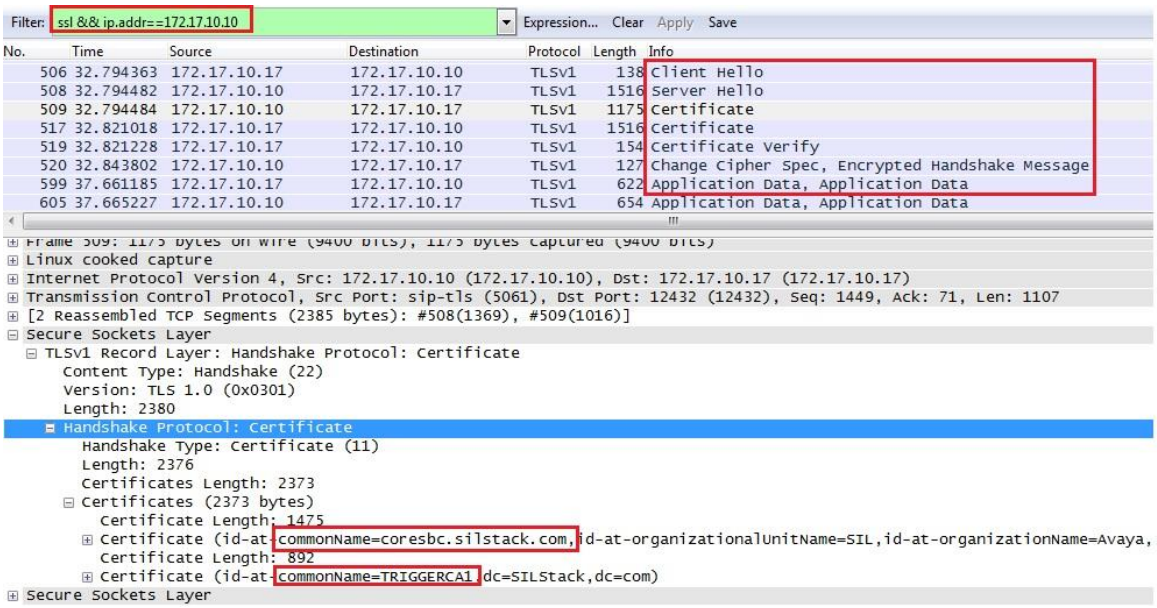
tcpdump -ni any -s -0 –w TraceFileName.pcap

where **TraceFileName.pcap** is the name of the packet capture file.
Stop the capture by using Control (Ctrl) +(and) c keys on the keyboard. Issue the following command to change ownership of the trace file from **root** to **ipcs**;

chown ipcs TraceFileName.pcap

Use a SFTP client such as WinSCP or Filezilla to connect to the SBCE as user **ipcs**. Copy the trace file from /home/ipcs directory to the local PC and open the file using a packet capture analysis tool such as Wireshark. Filter the packet capture for **SSL && ip.addr==*ipaddress***, where ***ipaddress*** is the IP address of interest. This may be the IP address of the remote phone, or far-end SBCE, or Session Manager. Check for a successful TLS handshake between the client and server. Click on the server or client sending a TLS certificate and expand the **Secure**

Sockets Layer header as shown below. Check the correct third-party signed security certificate is sent by the server or client.

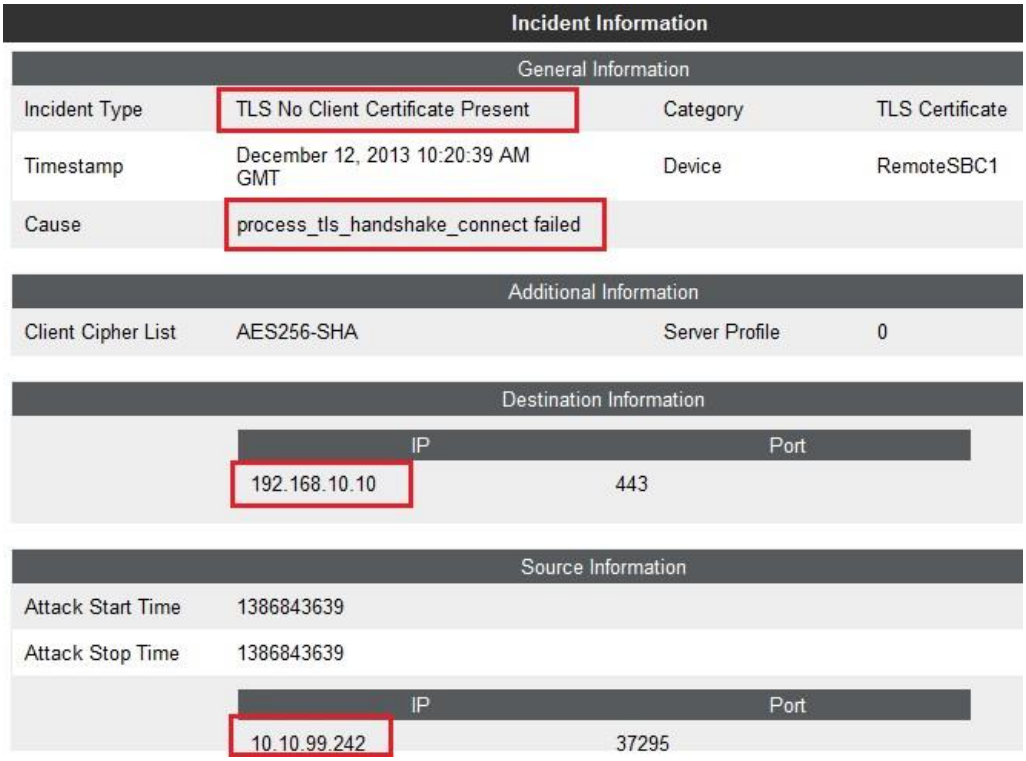


Click on the **Incidents** link on SBCE EMS GUI to check for errors in the SBCE logs.

Session Border Controller for Enterprise

Click on any error related to TLS.

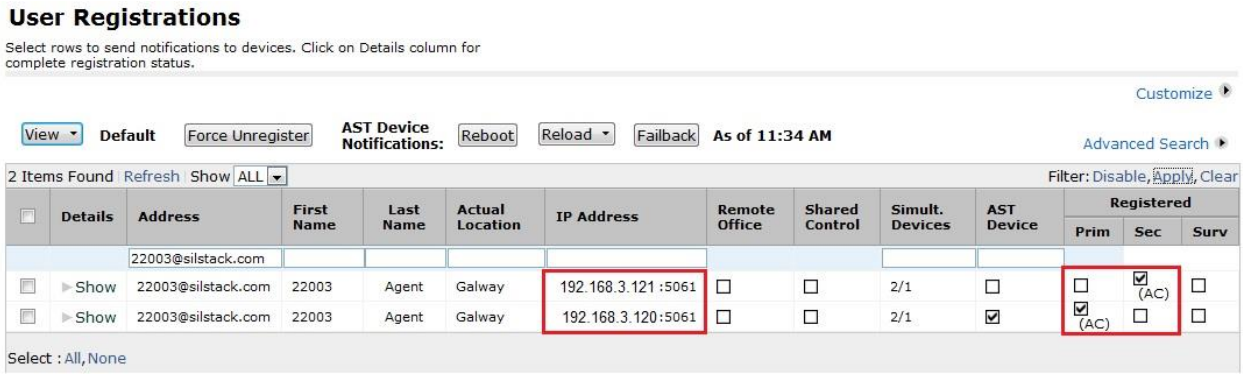
The example shown on next page illustrates when a remote phone failing to establish a TLS connection to the remote SBCE. The phone display shows **Acquiring Service** and is unable to log in. The incident details reveals there is no TLS client certificate sent by the remote phone with source IP address 10.10.99.242 and the external B1 interface IP of the remote SBCE 192.168.10.10.



Incident Information			
General Information			
Incident Type	TLS No Client Certificate Present	Category	TLS Certificate
Timestamp	December 12, 2013 10:20:39 AM GMT	Device	RemoteSBC1
Cause	process_tls_handshake_connect failed		
Additional Information			
Client Cipher List	AES256-SHA	Server Profile	0
Destination Information			
IP	192.168.10.10	Port	443
Source Information			
Attack Start Time	1386843639		
Attack Stop Time	1386843639		
IP	10.10.99.242	Port	37295

8.2. Verify Avaya Aura® Session Manager

Log into Avaya Aura® System Manager, see **Reference [6]** for details. Navigate to **Elements→ Session Manager → System Status → User Registrations**. Check the registration of remote IP Deskphone to ensure the checkbox is ticked for both primary and secondary Session Manager. The IP address of the registered endpoint will be the internal (A1) interfaces of the core SBCE.



User Registrations

Select rows to send notifications to devices. Click on Details column for complete registration status.

Customize

View | Default | Force Unregister | AST Device Notifications: | Reboot | Reload | Failback | As of 11:34 AM | Advanced Search

2 Items Found | Refresh | Show ALL | Filter: Disable, Apply, Clear

Details	Address	First Name	Last Name	Actual Location	IP Address	Remote Office	Shared Control	Simult. Devices	AST Device	Registered Prim	Registered Sec	Registered Surv
	22003@silstack.com											
Show	22003@silstack.com	22003	Agent	Galway	192.168.3.121:5061	☐	☐	2/1	☐	☐	☑ (AC)	☐
Show	22003@silstack.com	22003	Agent	Galway	192.168.3.120:5061	☐	☐	2/1	☑	☑ (AC)	☐	☐

Select : All, None

Log into Session Manager over SSH client, (e.g., PuTTY) as user **craft**.

Start the **traceSM** packet capture analysis tool using the following command;

traceSM –uni –dt

This tool can be used to monitor SIP packets from the Core SBCE to Session Manager and can also be used to verify PPM information is exchanged successfully between the remote phone and Session Manager.

9. Conclusion

These Application Notes describe a sample configuration of Avaya 9641 IP Deskphones running Avaya one-X® SIP firmware connecting from a remote site to a core enterprise network, through Avaya Session Border Controller for Enterprise R6.2 FP1 in a back-to-back-to-back deployment. Avaya Session Border Controller for Enterprise is configured for High Availability and remote Avaya 9641 IP Deskphones register to two Avaya Aura® Session Managers R6.2 FP2 using TLS with third-party signed security certificates.

Interoperabilty testing included making bi-directional calls between remote Avaya 9641 IP Deskphones and core enterprise Avaya 9641 IP Deskphones, Avaya 9620 IP Deskphones, and phones across PSTN network. Features such as call hold, transfer, conference, music-on-hold, and Message Waiting, were tested for these endpoints. Refer to **Section 2.2** for test results and observations.

10. Additional References

Avaya Product documentation relevant to these Application Notes is available at http://support.avaya.com.

.

[1] Installing Avaya Session Border Controller for Enterprise, Release 6.2, Issue 2, March 2013

[2] Administering Avaya Session Border Controller for Enterprise, Release 6.2, Issue 2, December 2013

[3] Avaya Session Border Controller for Enterprise Overview and Specification, Release 6.2, Issue 2, December 2013.

[4] Administering Avaya Aura® Session Manager, Release 6.3, Issue 3, May 2013

[5] Administering 9601/9608/9611G/ 9621G/9641G IP Deskphones SIP, Release 6.3, Issue 3, November 2013

[6] Administering Avaya Aura® System Manager, Release 6.3, Issue 2, May 2013

[7] Configuring Avaya Aura® System Manager 6.2 FP2 and Avaya Aura® Session Manager 6.2 FP2 to use Third-Party Security Certificates for Transport Layer Security

[8] Configuring Avaya Aura® Communication Manager 6.2 FP2, Avaya Aura® Utility Services 6.3, Avaya 9641 IP Deskphone and Avaya 9620 IP Deskphone to use Third-Party Security Certificates for Transport Layer Security.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com