

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**

2. Interop	uction perability Testing est Description and Coverage	5
2.2. Te	est Results and Observations	5
4. Equip	ence Configuration ment and Software Validated gure Third-Party Certificates for Avaya Session Border Controller Advanced for	8
1		
5.1. In	stall Third-Party Trusted Root certificates	9
	reate a Certificate Signing Request for Avaya Session Border Controller for	11
5.3. Pr	ocess the Certificate Signing Request	13
	stall Third-Party Signed Identity Certificate	
6. Config Back Deplo	guration of Avaya Session Border Controller for Enterprise in a Back-To-Back-Toyment with Multiple Avaya Aura® Session Managers	10-
	emote Avaya Session Border Controller for Enterprise Configuration	
6.1.1.	Add Network Interfaces	
6.1.2.	Create TLS Client and Server Profile	
6.1.3.	Add Signaling Interfaces	
6.1. <i>3</i> .	Add Media Interfaces	
6.1.5.	Create Server Interworking Profile	
6.1.6.	Configure Routing	
6.1.7.	Add Server Configuration	
6.1.8.	Configure SIP Cluster Proxy	
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		
6.1.14	1	
6.1.15	L	
6.1.16		
6.2. DI	MZ 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	
6.2.5.	Create Server Interworking Profile	
6.2.6.	Configure Routing	46

	6.2.7.	Add Server Configuration	
	6.2.8.	Configure SIP Cluster Proxy	.47
	6.2.9.	Create Application, Media and Signaling Rules, End Point Policy Group, and	
	1 0	y Hiding Profile	
	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. Cor	e Avaya Session Border Controller for Enterprise Configuration	.54
	6.3.1.	Add Network Interfaces	.54
	6.3.2.	Create TLS Client and Server Profiles	
	6.3.3.	Add Signaling Interfaces	.55
	6.3.4.	Add Media Interfaces	
	6.3.5.	Create Server Interworking profile and Configure Routing	.56
	6.3.6.	Add Server Configuration	
	6.3.7.	Configure SIP Cluster proxy	.59
	6.3.8.	Create Application, Media and Signaling Rules, End Point Policy Group, and	
	Topolog	y Hiding Profile	.61
		Create Endpoint Subscriber Flow	
	6.3.10.	Create Endpoint Server Flow	
	6.3.11.	Configure Application Relay	
7.	Configu	re remote 9641 IP Deskphone	
8.	0	tion Steps	
8		ify Avaya Session Border Controller for Enterprise	
8	2. Ver	ify Avaya Aura® Session Manager	.69
9.	Conclus	ion	.70
10.	Additi	onal 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

EL; Reviewed: SPOC 2/6/2014 Solution & Interoperability Test Lab Application Notes ©2014 Avaya Inc. All Rights Reserved. 4 of 71 ASBCEb2b2b7LS.doc 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<sup>TM</sup> 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.

EL; Reviewed:	Solution & Interoperability Test Lab Application Notes	5 of 71
SPOC 2/6/2014	©2014 Avaya Inc. All Rights Reserved.	ASBCEb2b2b7LS.doc

# 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.

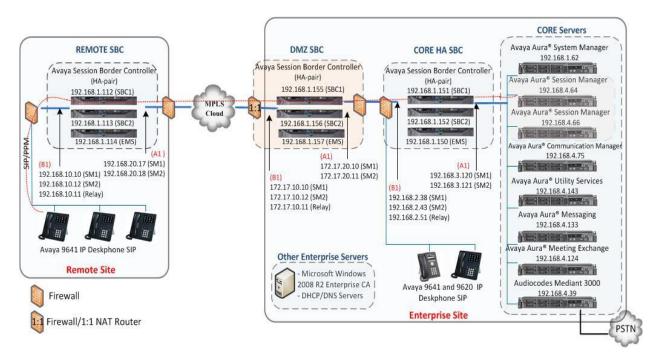
Each HA pair operates in a parallel mode configuration where both Avaya SBCE servers support the same set of VoIP interfaces. However, signaling packets are routed only to the active Avaya SBCE. The interface ports on the secondary (or stand-by) Avaya SBCE do not process any traffic. When a failover 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-toback-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	Release 6.2 FP1
R210 – II XL	Build: 6.2.0.Q64
Avaya Aura® Communication Manager	Release 6.2 FP2
running on Avaya S8800 Server	Version: 6.3.0.124.0-21000
Avaya Aura® Session Manager on Avaya	Release 6.2 FP2 (6.3.2)
S8800 Server	Build 6.3.2.0.632023
Avaya Aura® System Manager on Avaya	Release 6.2 FP2
S8800 Server	Version: 6.3.2.4.1399
Avaya Aura® Utility Services 6.3	Release 6.3.0.0.20
Virtualization Environment (VE)	Patch 6.3.0.1.20
vAppliance on Dell Poweredge R620 using	
VMWare ESXi 5.1.0	
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	Release 6.2 SP2
Server	
Avaya Meeting Exchange <sup>TM</sup> Enterprise	5.2 SP2
Edition	Bridge Patch 5.2.2.19.1
Audiocodes Mediant 3000	Release 3.0
Hewlett Packard Compaq 6000 Pro	Microsoft Windows Server 2008 R2
Microtower PC	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 <u>http://<CAserver\_IPaddress>/certsrv</u>, logging in as Active Directory domain administrator-level account and clicking on **Download a CA certificate, certificate chain, or CRL** link.

Microsoft Active Directory Certificate Services - TRIGGERCA1	Home
Welcome	
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate perform other security tasks.	
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation liview the status of a pending request.	st (CRL), or to
For more information about Active Directory Configence Songeon and Active Directory Configurate Songeon Decumentation	

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:

Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL

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

Microsoft Active Dire	ctory Certificate Services TRIGGERCA1
Download a CA	Certificate, Certificate Chain, or CRL
To trust certificates	s issued from this certification authority, install this CA certificate chain.
To download a CA	certificate, certificate chain, or CRL, select the certificate and encoding method.
CA certificate:	
Restant	
	evious [TRIGGERCA1]
Encoding method:	
	DER
Download CA cert	Base 64

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

Download CA certificate chain

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  $\rightarrow$  TLS Management  $\rightarrow$  Certificates and click the Install button.

### Session Border Controller for Enterprise

	Install Generate
Certificates	
	Installed Certificates

SIP Cluster	trigger.crt	View Delete
<ul> <li>Domain Policies</li> <li>TLS Management</li> </ul>	trigger1core.crt	View Delete
Certificates	Installed CA Certificates	
Client Profiles Server Profiles	AvayaSBCCA.crt	View Delete

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** 

	Install Certificate	
Туре	<ul> <li>Certificate</li> <li>CA Certificate</li> <li>Certificate Revocation List</li> </ul>	
Name	rootCAcert	
Certificate File	C:\Users\emmetlee\Doc	

Dashboard Administration Backup/Restore System Management Global Parameters Global Profiles **AVAYA** 

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  $\rightarrow$  TLS Management  $\rightarrow$  Certificates and click the Generate CSR button.

#### Session Border Controller for Enterprise

A	11	1	11
AI1	F	۰y	A

ashboard	Certificates	
dministration		Install Generate CS
lackup/Restore		
System Management	Certificates	
Global Parameters	Installed Cer	rtificates
Global Profiles	AvayaSBC.crt	View Delete
SIP Cluster	trigger.crt	View Delete
Domain Policies TLS Management	trigger1remote.crt	View Delete
Certificates	Installed CA C	Sertificates
Client Profiles	AvayaSBCCA.crt	View Delete
Server Profiles		

Solution & Interoperability Test Lab Application Notes ©2014 Avaya Inc. All Rights Reserved. 11 of 71 ASBCEb2b2b7LS.doc Add details for the Avaya SBCE identity certificate to be signed by the third-party or customer CA. Example responses are shown below.

Avaya

SIL

- Country US
- State/Province Name Colorado • Denver
- Locality
- Organization
- Organizational Unit
- 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. Select 2048 bits.
- Key Size • 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 for any queries on this certificate. Contact Name Contact Email address (not shown).
- **Contact Email**

Country Name	US
State/Province Name	Colorado
Locality Name	Denver
Organization Name	Avaya
Organizational Unit	SIL
Common Name	remotesbc.silstack.com
Algorithm	<ul><li>SHA1</li><li>MD5</li></ul>
Key Size (Modulus Length)	<ul><li>1024 bits</li><li>2048 bits</li></ul>
Key Usage Extension(s)	<ul> <li>Key Encipherment</li> <li>Non-Repudiation</li> <li>Digital Signature</li> </ul>
Subject Alt Name	DNS:remotesbc.silstack
Passphrase	•••••
Confirm Passphrase	•••••
Contact Name	SIL Admin

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**.

Certificate Request:	
Data:	
Version: 0 (0x0)	
Subject: C=US, ST=Colorado, L=Denver, O=Avaya, OU=SIL,	
CN=remotesbc.silstack.com	
Subject Public Key Info:	
Public Key Algorithm: rsaEncryption	
RSA Public Key: (2048 bit)	
Modulus (2048 bit):	
00:df:41:62:cc:5c:ba:15:17:91:a6:cb:dd:e8:3d:	
29:64:ef:0b:b8:0d:a0:4f:01:6b:1e:19:34:d8:a7:	
d8:2b:2a:b0:02:23:ff:85:7f:62:4d:e1:7b:37:7d:	
b1:af:e2:4a:8b:06:6f:1d:4e:9e:61:4a:b0:8a:d3:	
6c:80:0b:a9:b2:ae:8d:81:66:8e:5d:25:5b:b2:a8:	
8e:40:6c:c1:e6:07:ef:3d:09:ef:81:88:28:8d:61:	
eb:ec:0e:a1:fa:83:ce:b9:b5:c2:52:03:0a:4f:35:	
71:e9:7a:98:1b:e3:a1:7e:5f:e2:44:2e:27:ae:62:	
8b:9d:b0:92:ee:da:65:98:fd:bb:b6:13:5b:af:f4:	
c0:79:5a:63:48:f0:0a:09:02:66:e9:30:51:2a:97: 15:f2:69:4a:26:24:f5:6f:e5:5f:11:19:75:90:c6:	
15:T2:69:48:26:24:T5:6T:E5:5T:11:19:75:90:C6: 46:7b:3c:56:47:e7:d5:17:13:bd:6c:8a:3f:20:1f:	
46:/D:3C:56:4/:e/:d5:1/:13:Dd:6C:8a:3T:20:1T: 38:88:7a:cc:b0:86:67:df:25:83:41:be:7a:f2:e8:	
d8:ba:62:2c:02:a3:92:70:c1:3a:4f:43:45:42:34:	
c6:4e:dd:78:95:17:20:3c:4b:26:51:91:77:92:db:	
5f:78:16:fc:0d:64:45:54:21:dc:c5:d2:02:3e:1e:	
4b:49:3f:60:e2:c1:20:df:53:5d:74:d2:b0:07:32:	
40.45.51.00.02.01.20.01.55.50.74.02.00.07.52.	

Click on the  $\mathbf{X}$  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** 

Microsoft Active Directory Certificate Services - TRIGGERCA1	Hom
Welcome	
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify yo	ur identity to people you communicate with over the Web,

sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks. You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:

Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL

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.

	ificate Request or Renewal Request
the Saved Req	ved request to the CA, paste a base-64-encoded C uest box.
Saved Request:	
Base-64-encoded	LObxMTpRQwwc3CalEqcG4ogtv1edfTxQI85hpbMu ACsaXpHPhpmsc6ecmSPPKbF0jIWdVzbSwdPBqX9Q UZpc5IgI068=
certificate remp	WebServer-Enterprise
L Additional Attrib	· · · · · · · · · · · · · · · · · · ·

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** 

a included to your
s issued to you.
Base 64 encoded
<u>chain</u>

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.

EL; Reviewed:
SPOC 2/6/2014

**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**  $\rightarrow$  **TLS Management**  $\rightarrow$  **Certificates** (not shown). Click **Install** button. Select the following settings;

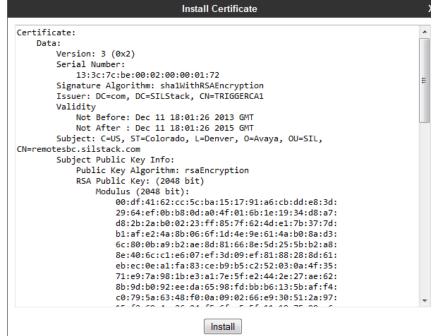
- Type Select Certificate
- Name Enter a descriptive name, e.g., **remote\_sbc**.
- Certificate File Browse to the signed **Certificate File** created in **Section 5.3**, e.g.,
- remoteSBCsigned.pem.
- Key Upload Key File
- Key File Browse to the saved private key created in Section 5.2

e.g., remotesbc.key.

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

	Install Certificate	х
Туре	<ul> <li>Certificate</li> <li>CA Certificate</li> <li>Certificate Revocation List</li> </ul>	
Name	remote_sbc	
Certificate File	C:\Users\emmetlee\Doc Browse	
Trust Chain File	Browse	
Key	<ul> <li>Use Existing Key</li> <li>Upload Key File</li> </ul>	
Key File	C:\Users\emmetlee\Doc Browse	
	Upload	

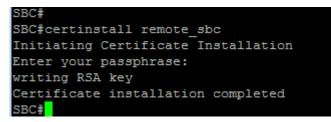
Click Install. Click Finish (not shown).



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.

EL; Reviewed:	Solution & Interoperability Test Lab Application Notes	16 of 71
SPOC 2/6/2014	©2014 Avaya Inc. All Rights Reserved.	ASBCEb2b2b7LS.doc



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 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;

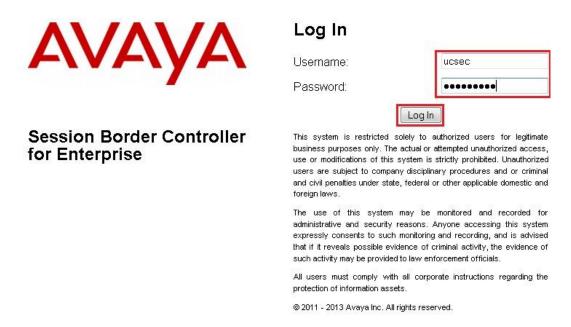
- Add network interfaces
- Create TLS profiles
- Add Signaling and Media Interfaces
- Create Server Interworking Profile
- Configure Routing
- Create Server Configuration Profile

EL; Reviewed:	
SPOC 2/6/2014	

- 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  $\rightarrow$  Device Specific Settings  $\rightarrow$  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**.

Devices	Network Configuration Inte	rface Configuration		
RemoteSBC1	Modifications or deletions of an from <u>System Management</u> .	IP address or its associated data req	uire an application restart before taking e	effect. Application restarts can be issued
	A1 Netmask 255.255.255.0	A2 Netmask	B1 Netmask 255.255.255.0	B2 Netmask
	Add			Save
	IP Address	Public IP	Gateway	Interface
	192.168.20.17		192.168.20.1	A1 Delete
	192.168.10.10		192.168.10.1	B1 Delete
	192.168.10.11		192.168.10.1	B1 Delete
	192.168.20.18		192.168.20.1	A1 Delete
	192.168.10.12		192.168.10.1	B1 Delete

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
---------	-------------	------------

	Network Configu	ration Interface Configuration		
oteSBC1		Name	Administrative S	Status
	A1		Enabled	Toggl
	A2		Disabled	Toggl
	B1		Enabled	Toggl
	B2		Disabled	Toggl
	HA Device #2			
	HA Device #2	Name	Administrative S	Status
	A1	Name	Administrative S	Status Toggi
		Name		5773 - 1
	A1	Name	Enabled	Toggl

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

- HA Link Dronagation				
HA Link Propagation				
🗹 A1	🗖 A2	✓ B1	🔲 B2	Update

#### 6.1.2. Create TLS Client and Server Profile

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

# Navigate to System Management $\rightarrow$ TLS Management $\rightarrow$ 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.

Dashboard	Client Profiles: Tr		TLS Profile
Administration	Add	Profile Name	RemoTLSclient
Backup/Restore		Certificate	remote_sbc.crt
System Management	Client Profiles	Centilicate	remote_spc.cn
Global Parameters	AvayaSBCClient		Certificate Info
Global Profiles	TriggerTLSclient	Peer Verification	Required
<ul> <li>SIP Cluster</li> <li>Domain Policies</li> <li>TLS Management Certificates</li> </ul>		Peer Certificate Authorities	AvayaSBCCA.crt Cisco_phone_CA.crt trigger1_pem rootCAcert.pem
Client Profiles Server Profiles Device Specific Settings		Peer Certificate Revocation Lists	
		Verification Depth	1
		R	enegotiation Parameters
		Renegotiation Time	0 seconds

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

	Renegotiation	Parameters
Renegotiation Time	0	seconds
Renegotiation Byte Count	0	
	Cipher Suit	e Options
Ciphers	All Null	◎ Strong ◎ Export Only Only (For Debugging) <mark>●</mark> Custom
Options	🗆 DH	ADH DMD5
Value (What's this?)	RSA	
	Fini	sh

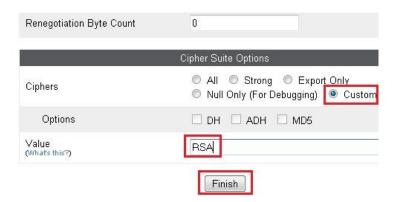
To create a TLS server profile, navigate to **System Management**  $\rightarrow$  **TLS Management**  $\rightarrow$  **Server Profiles** and click **Add**.

- 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.

Dashboard	Server Profiles: A		TLS Profile
Administration	Add	Profile Name	RemoTLSserver
Backup/Restore System Management	Server Profiles AvayaSBCServer	Certificate	remote_sbc.crt
Global Parameters			Certificate Info
<ul> <li>Global Profiles</li> </ul>	TriggerTLSserver	Peer Verification	Required 💌
<ul> <li>SIP Cluster</li> <li>Domain Policies</li> <li>TLS Management Certificates</li> </ul>	Trigger-PPM	Peer Certificate Authorities	AvayaSBCCA.crt Cisco_phone_CA.crt trigger1_pem rootCAcert.pem
Client Profiles Server Profiles Device Specific Settings		Peer Certificate Revocation Lists	
		Verification Depth	1
		R	Renegotiation Parameters
		Renegotiation Time	0 seconds

Solution & Interoperability Test Lab Application Notes ©2014 Avaya Inc. All Rights Reserved. 21 of 71 ASBCEb2b2b7LS.doc

#### 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**.

Select None.

Enter **RSA**.

Select Custom.

Enter a descriptive name, e.g., RemoPPM

down menu, e.g., remote\_sbc.crt.

Select the TLS server Identity Certificate from the drop-

- Profile Name
- Certificate
- Peer Verification
- Ciphers
- Value

Click Finish.

	TLS Profile
Profile Name	RemoPPM
Certificate	remote_sbc.crt
	Certificate Info
Peer Verification	None
Peer Certificate Authorities	AvayaSBCCA.crt Cisco_phone_CA.crt trigger1.pem rootCAcert.pem
Peer Certificate Revocation Lists	
Verification Depth	
R	enegotiation Parameters
Renegotiation Time	0 seconds

	Cipher Suite Options
Ciphers	All Strong Export Only     Null Only (For Debugging)
Options	DH ADH MD5
Value (What's this?)	RSA

### 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  $\rightarrow$  Device Specific Settings  $\rightarrow$  Signaling Interface and click on Add. Enter the following;

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

Click Finish.

Name	FromPhone-External-Sic
IP Address	192.168.10.10 💌
TCP Port Leave blank to disable	5060
UDP Port Leave blank to disable	5060
Enable Stun	
TLS Port Leave blank to disable	5061
TLS Profile	RemoTLSserver 💌
Enable Shared Control	
Shared Control Port	
	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

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

**Signaling Interface** 

#### 6.1.4. Add Media Interfaces

Browse to System Management  $\rightarrow$  Device Specific Settings  $\rightarrow$  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

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

edia Interface	and a second	fan helden offast findlig finden ander see h	in the second former	e
Aonagement.	enace will require an application restart of	fore taking effect. Application restarts can b	ie issued irom	oyster
				Ad
Name	Media IP	Port Range		
nt_Med_int_DMZ-1	192.168.20.17	35000 - 40000	Edit	Delet
External-Media-fromPhones-1	192.168.10.10	35000 - 40000	Edit	Dele
External-Media-fromPhones-2	192.168.10.12	35000 - 40000	Edit	Dele
nt Med int DMZ-2	192.168.20.18	35000 - 40000	Edit	Delet

EL; Reviewed: SPOC 2/6/2014

Solution & Interoperability Test Lab Application Notes ©2014 Avaya Inc. All Rights Reserved. 24 of 71 ASBCEb2b2b7LS.doc

#### 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).

Dashboard	Interworking Profile	es: avaya-ru		
Administration	Add			Clone
lackup/Restore	Interworking Profiles	and the second		
ystem Management		It is not recommended to edit the	defaults. Try cloning or adding a new profile instead.	
Global Parameters	cs2100	General Timers URI Man	ipulation Header Manipulation Advanced	
Global Profiles	avaya-ru			
Domain DoS	OCS-Edge-Server		General	
Fingerprint		Hold Support	NONE	
Server	E cisco-com	180 Handling	None	
Interworking	cups	181 Handling	None	
Phone Interworking	OCS-FrontEnd-Server	100 Use dias	News	

#### Session Border Controller for Enterprise

#### 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**  $\rightarrow$  **Global Profiles**  $\rightarrow$  **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**.

	Next Hop Routing
URI Group	*
Next Hop Server 1 IP, IP:Port, Domain, or Domain:Port	172.17.10.10
Next Hop Server 2 IP, IP:Port, Domain, or Domain:Port	
Routing Priority based on Next Hop Server	
Use Next Hop for In Dialog Messages	
lgnore Route Header for Messages Outside Dialog	
NAPTR	
SRV	
Outgoing Transport	◉ TLS ◎ TCP ◎ UDP
	Finish

Solution & Interoperability Test Lab Application Notes ©2014 Avaya Inc. All Rights Reserved. **AVAYA** 

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** $\rightarrow$ **Global Profiles** $\rightarrow$ **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.,

Select TLS

- 172.17.10.10
- Supported Transports
- TLS Port Enter 5061

Add Serve	er Configuration Profile - General
Server Type	Call Server 💌
IP Addresses / Supported FQDNs Separate entries with commas	172.17.10.10
Supported Transports	TCP UDP TLS
TCP Port	
UDP Port	
TLS Port	5061
	Back Next

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
  - To URISystem Manager, e.g., 22010@silstack.com.Same as From URI, e.g., 22010@silstack.com

Same as	From U	RI, e.g.,	22010@silstacl	s.com.

Enable Heartbeat	
Method	OPTIONS 💌
Frequency	60 seconds
From URI	22010@silstack.com
To URI	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** 

Add Serv	er Configuration Profile - Advanced
Enable DoS Protection	
Enable Grooming	
Interworking Profile	avaya-ru-multism 💌
TLS Client Profile	RemoTLSclient
Signaling Manipulation Script	None 💌
TLS Connection Type	🖲 SUBID 🔘 PORTID 🔘 MAPPING
	Back

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

#### Server Configuration: Server-DMZ-SM-2

General Authentication Heartbeat	Advanced
Server Type	Call Server
IP Addresses / FQDNs	172.17.10.12
Supported Transports	TLS
TLS Port	5061
	Server Type IP Addresses / FQDNs Supported Transports

#### 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).

#### Cluster Proxy: RemoteCluster

Add		
Cluster Proxies	General Primary Secondary Tertiary	
RemoteCluster		Cluster Information
	Call Server Type	Awaya
		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 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 Enter the external interface for SM1 as created in Section 6.1.3, e.g., FromPhone-External-Signaling-1

• End Point Signaling Interface

Conseel Reiman Conservation

		192.168	3 10 10					
erver Client	(Address	192.168	3.20.17					
			Edit					
vers ——								
								Add
Real Type	Port	Real IP	Real Port	Relay Mode	Rewrite URL	Server TLS Profile		
HTTPS	443	172.17.10.11	443	9 <u>-11</u> 1	1	RemoPPM	Edit	Delete
HTTPS		172.17.10.10	443				Edit	Delete
	vers Real Type HTTPS	Real Port Type Port HTTPS 443	Real Port Real IP Type Port Real IP HTTPS 443 172.17.10.11	Edit Vers Real Port Real IP Real Port HTTPS 443 172.17.10.11 443	Edit Vers Real Port Real IP Real Port Relay Mode HTTPS 443 172.17.10.11 443	Edit Vers Real Port Real IP Real Port Relay Rewrite Type Port Real IP Real Port Mode URL HTTPS 443 172.17.10.11 443	Edit Vers Real Port Real IP Real Port Relay Rewrite Server TLS Type Port Real IP Real Port Mode URL Profile HTTPS 443 172.17.10.11 443 RemoPPM	Edit         Vers         Real Type       Port       Real IP       Real Port       Relay Mode       Rewrite       Server TLS Profile         HTTPS       443       172.17.10.11       443        RemoPPM       Edit

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

• End Point Signaling Interface

Select the profile added in Section 6.1.7, e.g., Server-DMZ-SM-2 Enter the external interface for SM1 as created in Section 6.1.3, e.g., FromPhone-External-Signaling-2

General Primary Secondary Tertiary **Device Information** Device Name RemoteSBC1 Device IP 192.168.10.12 Configuration Server Client Address 192.168.20.18 Edit Delete **Configuration Servers** Add Real Relay Rewrite Server TLS Port Real IP Real Port Туре Modé Profile Туре HTTPS HTTPS 172.17.10.11 443 RemoPPM Edit Delete 443 ------PPM HTTPS ----172.17.10.12 443 Edit Delete Signaling Servers Server Configuration Profile End Point Signaling Interface Session Policy Group Server-DMZ-SM-2 FromPhone-External-Siganling-2 default Edit

#### 6.1.9. Configure Application Rules

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

Application Rules: de	əfault	
Add	Filter By Device	Clone
Application Rules	It is not recommended to edit the defaults. Try cloning or adding a new rule instead.	
default	Application Rule	

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.

	Editing	Rule:	App_RU		х
Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint	
Voice		V	200	200	
Video					]
IM					
	Mis	scella	neous		
CDR Support	0		v/ RTP v/o RTP		
RTCP Keep-Alive					
		Finis	h		

#### 6.1.10. Configure Media Rules

Navigate to System Management  $\rightarrow$  Domain Policies  $\rightarrow$  Media Rules (not shown). Click Add to create a new media rule. Enter a descriptive, e.g., avaya\_srtp. Click Next.

	Media Rule
Rule Name	avaya_srtp
	Next

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

	Media Rule
Media NAT	<ul> <li>Enforce Signaling and Media IP correlation</li> <li>Learn Media IP dynamically</li> </ul>
	Back Next

Under Audio Encryption, select **Preferred Format #1** as **SRTP\_AES\_CM\_128\_HMAC\_SHA1\_80**. Uncheck **Encrypted RTCP**. Click **Next**.

	Audio Encryption
Preferred Format #1	SRTP_AES_CM_128_HMAC_SHA1_80
Preferred Format #2	NONE
Preferred Format #3	NONE
Encrypted RTCP	
Interworking	
	Video Encryption
Preferred Format #1	RTP
Preferred Format #2	NONE
Preferred Format #3	NONE
Encrypted RTCP	$\checkmark$
Interworking	
	Miscellaneous
Capability Negotiation	
	Back

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

	Media Anomaly
Media Anomaly Detection	
Detect RTP Injection Attack	
Asymmetric RTP	
Action	Alert 💌

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  $\rightarrow$  Domain Policies  $\rightarrow$  Signaling Rules (not shown). Clone the default Signaling Rule by clicking the Clone button, while the default Signaling Rule is selected.

Signaling Rules: d		28				-
Add	Filter By Device					Clone
Signaling Rules	10 E	المراجع والعاد والمحاد		1.12.7.14		1
Signaling Rules	It is not recommend	ded to edit the defaul	ts. Try cloning or addin	g a new rule instead.		
default	General Reque		Request Headers	Response Headers	Signaling QoS	
default No-Content-Type-Ch					Signaling QoS	

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

	Clone Rule	
Rule Name	default	
Clone Name	RemoSigRule	

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

History-Info INVITE

Forbidden

**Remove Header** 

Select the values below;

- Header Name
- Method Name
- Header Criteria
- Presence Action

Click Finish.

	Add Header Control
Proprietary Request Header	
Header Name	History-Info
Method Name	INVITE
Header Criteria	<ul> <li>Forbidden</li> <li>Mandatory</li> <li>Optional</li> </ul>
Presence Action	Remove header       486       Busy Here
	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.

		Policy Group
	Group Name	avaya-b2b2b
		Next
Select the following values		
Application Rule		<b>App_RU</b> (rule created in <b>Section 6.1.9</b> )
Border Rule		default
• Media Rule		avaya_srtp (rule created in Section 6.1.1

- Security Rule ٠ Signaling Rule •
- Time of Day •

**10**) default-low **RemoSigRule** (rule created in Section 6.1.11) default

Click Finish.

	Policy Group
Application Rule	App_RU •
Border Rule	default
Media Rule	avaya_srtp 💌
Security Rule	default-low 💌
Signaling Rule	RemoSigRule 💌
Time of Day Rule	default 💌
	Back Finish

#### 6.1.13. **Create a Topology Hiding Profile**

Navigate to System Management  $\rightarrow$  Global Profiles  $\rightarrow$  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.

Topology Hiding Profile				Х
				Add Header
Header	Criteria	Replace Action	Overwrite Va	lue
Request-Line	▼ IP/Domain ▼	Overwrite	▼ silstack.com	Delete
		Back Finish		

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
То	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  $\rightarrow$  Device Specific Settings  $\rightarrow$  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**.

	Criteria
Tow Name	From-Farend-Phones-1
JRI Group	*
Jser Agent	*
Source Subnet sx: 192.188.0.1/24	*.
/ia Host Ex: domain.com, 192.168.0.1/24	<b>*</b>
Contact Host Ex: domain.com, 192.168.0.1/24	<b>*</b>
Signaling Interface	FromPhone-External-Siganling-1

Select the following values and click Finish.

• Media Interface

#### External-Media-fromPhones-1

- End Point Policy Group
- Routing Profile
- Phone Interworking Profile

Avaya-b2b2b (as configured in Section 6.1.12) To-DMZ-SM-1 (as configured in Section 6.1.6) Avaya-Ru

	Profile
Source	<ul> <li>Subscriber</li> <li>Click To Call</li> </ul>
Methods Allowed Before REGISTER	INFO MESSAGE NOTIFY OPTIONS
Media Interface	External-Media-fromPhones-1
End Point Policy Group	avaya-b2b2b
SIP Cluster Flow	
Routing Profile	To-DMZ-SM-1
	Optional Settings
Topology Hiding Profile	default 💌
Phone Interworking Profile	Avaya-Ru 💽
TLS Client Profile	None 💌
File Transfer Profile	None -
Signaling Manipulation Script	None 💌
[	Back Finish

Solution & Interoperability Test Lab Application Notes ©2014 Avaya Inc. All Rights Reserved. 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.

	Criteria
Flow Name	From-Farend-Phones-2
URI Group	*
User Agent	*
Source Subnet Ex: 192.168.0.1/24	*
Via Host Ex: domain.com, 192.168.0.1/24	*
Contact Host Ex: domain.com, 192.168.0.1/24	*
Signaling Interface	FromPhone-External-Siganling-2
	Next
	Profile
Source	<ul> <li>Subscriber</li> <li>Click To Call</li> </ul>
Methods Allowed Before REGISTI	ER INFO MESSAGE NOTIFY OPTIONS
Media Interface	External-Media-fromPhones-2
End Point Policy Group	avaya-b2b2b
SIP Cluster Flow	
Routing Profile	To-DMZ-SM-2
	Optional Settings
Topology Hiding Profile	default 💌
Phone Interworking Profile	Avaya-Ru
TLS Client Profile	None
File Transfer Profile	None 💌
Signaling Manipulation Script	None 💌
	Back Finish

Solution & Interoperability Test Lab Application Notes ©2014 Avaya Inc. All Rights Reserved.

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

Click Finish (not shown).

•

•

Flow Name	DMZ-SBC-Server-1		
Server Configuration	Server-DMZ-SM-1		
URI Group	*		
Transport	*		
Remote Subnet	*		
Received Interface	FromPhone-External-Siganling-1		
Signaling Interface	To-DMZ-Side-Internal-Siganling-1		
Media Interface	Int_Med_int_DMZ-1		
End Point Policy Group	avaya-b2b2b 💌		
Routing Profile	default		
Topology Hiding Profile	Avaya		
File Transfer Profile	None 💌		

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  $\rightarrow$  Device Specific Settings  $\rightarrow$  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**.

	Add Application Relay
	Remote Configuration
Remote Domain	silstack.com
Remote IP	172.17.10.11
Remote Port	80
Remote Transport	TCP -
	Device Configuration
Published Domain	silstack.com
Listen IP	192.168.10.11 💌
Listen Port	80
Connect IP	192.168.20.17 💌
Listen Transport	
	General Configuration
Whitelist Flows	
Use Relay Actors	

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.

vices Application Re	lay 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	ТСР	silstack.com	192.168.10.11:80	ТСР	192.168.20.1
silstack.com	172.17.10.11:5222	TCP	silstack.com	192.168.10.10:5222	тср	192.168.20.1
silstack.com	172.17.10.11:5222	TCP	silstack.com	192.168.10.12:5222	тср	192.168.20.1
silstack.com	172.17.10.11:443	TCP	silstack.com	192.168.10.11:443	ТСР	192.168.20.1
silstack.com	172.17.10.11:1023	TCP	silstack.com	192.168.10.11:1023	тср	192.168.20.1

# 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  $\rightarrow$  Device Specific Settings  $\rightarrow$ 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**.

•		data require an application restart be	tore taking effect. Application restarts o	an be
A1 Netmask 255.255.255.0 Add	A2 Netmask	B1 Netmask 255.255.255.240	B2 Netmask	Clear
IP Address	Public	: IP Ga	teway Interface	
172.17.20.10		172.17.20.1	A1 .	• Delete
172.17.10.10		172.17.10.1	B1	Delete
172.17.10.11		172.17.10.1	B1 .	• Delete
172.17.10.12		172.17.10.1	B1	Delete
172.17.20.11		172.17.20.1	A1	- Delete

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**.

Dashboard	Client Profiles: Tr		TLS Profile
Administration	Add	Profile Name	DMZTLSclient
Backup/Restore	Client Profiles	Certificate	dmz_sbc.crt
System Management <ul> <li>Global Parameters</li> </ul>	AvayaSBCClient		
<ul> <li>Global Profiles</li> </ul>	TriggerTLSclient	Peer Verification	Certificate Info
SIP Cluster		Peer ventication	Required
Domain Policies		Peer Certificate Authorities	AvayaSBCCA.crt Cisco_phone_CA.crt
TLS Management		Peer Cennicate Authonnes	trigger1 nem rootCAcert.pem
Certificates			
Client Profiles Server Profiles		Peer Certificate Revocation Lists	
<ul> <li>Device Specific Settings</li> </ul>			
		Verification Depth	1
		R	enegotiation Parameters
		Renegotiation Time	0 seconds

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

	Renegotiation Parameters	
Renegotiation Time	0 second	8
Renegotiation Byte Count	0	
	Cipher Suite Options	
Ciphers	All Strong Null Only (For Debute)	) Export Only ugging) 💿 Custom
Options	🗆 DH 🗆 ADH 🔲	MD5
Value (What's this?)	RSA	
	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.

ignaling 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  $\rightarrow$  Device Specific Settings  $\rightarrow$  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;

edia Interface		
Modifying or deleting an existing med ssued from <u>System Management</u> .	lia interface will require an applicatio	n restart before taking effect. Ap
Name	Media IP	Port Rang
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

Solution & Interoperability Test Lab Application Notes ©2014 Avaya Inc. All Rights Reserved. 45 of 71 ASBCEb2b2b7LS.doc

#### 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.

	Next Hop Routing
URI Group	*
Next Hop Server 1 IP, IP:Port, Domain, or Domain:Port	192.168.2.38
Next Hop Server 2 IP, IP:Port, Domain, or Domain:Port	
Routing Priority based on Next Hop Server	
Use Next Hop for In Dialog Messages	
lgnore Route Header for Messages Outside Dialog	
NAPTR	
SRV	
Outgoing Transport	ILS TCP OUDP
	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** $\rightarrow$ **Global Profiles** $\rightarrow$ **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).

Server Type	Call Server 🚽
IP Addresses / Supported FQDNs Separate entries with commas	192.168.2.38
Supported Transports	TCP UDP TLS
TCP Port	5060
UDP Port	5060
TLS Port	5061

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**.

Add Serv	er Configuration Profile - Advanced
Enable DoS Protection	
Enable Grooming	
Interworking Profile	avaya-ru-multism 💌
TLS Client Profile	DMZTLSclient 💌
Signaling Manipulation Script	None 💌
TLS Connection Type	🖲 SUBID 🔘 PORTID 🔘 MAPPING
	Back

#### 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).

Cluster Proxy: DMZ	Cluster	
Add		
Cluster Proxies	General Primary Secondary Tertiary	
AvayaCluster		Cluster Information
DMZCluster	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 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 <b>Section 6.2.7</b> , e.g.,
•	Endpoint Signaling Interface	Server-Core-SM-1 External interface for SM1 as created in Section
		6.2.3, e.g., FromRemote-External-Signaling-1

Device Name			DMZSB	C1			
Device IP			172.17.1	10.10			
Configuration Server Client Address		172.17.20.10					
				Edit			
Configuration S	Servers —						
Туре	Real Type	Port	Real IP	Real Port	Relay Mode	Rewrite URL	Server TLS Profile
Type HTTPS		Port 443	Real IP 192.168.2.51	Real Port 443			Profile
Туре		Port	Real IP	Real Port			
	Type HTTPS HTTPS						DMZ-PPM
HTTPS PPM ignaling Server	Type HTTPS HTTPS	443	192.168.2.51	443 443	Mode 	URL	Profile DMZ-PPM

Configure the following for the Secondary Cluster Proxy;

	Device IP	DMZ SBCE SM2 External IP Address, e.g.,
		172.17.10.12
٠	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
		<b>6.2.7</b> , e.g., <b>FromRemote-External-Signaling-2</b>

Device Name			DMZSE	C1			
Device IP		172.17.	172.17.10.12				
Configuratio	n Server Clien	t Address	172.17.	20.11			
			Edi	t Delete			
Configuration S	Servers —						
Configuration S	Servers Real Type	Port	Real IP	Real Port	Relay Mode	Rewrite URL	Server TL Profile
	Real	Port 443	Real IP 192.168.2.51	Real Port 443			Server TL Profile DMZPP1 Profile
Туре	Real Type				Mode		Profile DMZPP1
Type HTTPS	Real Type HTTPS HTTPS	443	192.168.2.51	443	Mode 	URL	Profile DMZPPM Profile

#### 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  $\rightarrow$  Device Specific Settings  $\rightarrow$  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**.

	Criteria
Flow Name	From-RemoteSBC-1
URI Group	*
User Agent	*
Source Subnet Ex: 192.168.0.1/24	*
Via Host Ex: domain.com, 192.168.0.1/24	*
Contact Host Ex: domain.com, 192.168.0.1/24	*
Signaling Interface	FromRemote-External-Signaling-1

Select the following values and click Finish.

- Media Interface
- End Point Policy Group
- Routing Profile

Select Ext\_Med\_intf\_REMO-1. Select Avaya-b2b2b. Select Route\_To\_Core-SM-1 (as configured in Section 6.2.6). Select Avaya-Ru.

• Phone Interworking Profile

8	Profile
Source	<ul> <li>Subscriber</li> <li>Click To Call</li> </ul>
Methods Allowed Before REGISTER	INFO MESSAGE NOTIFY OPTIONS ~
Media Interface	Ext_Med_intf_REMO-1
End Point Policy Group	avaya-b2b2b
SIP Cluster Flow	
Routing Profile	Route_To_Core-SM-1
	Optional Settings
Topology Hiding Profile	default
Phone Interworking Profile	Avaya-Ru
TLS Client Profile	None
File Transfer Profile	None 💌
Signaling Manipulation Script	None 💌
	Back Finish

Solution & Interoperability Test Lab Application Notes ©2014 Avaya Inc. All Rights Reserved.

#### 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  $\rightarrow$  Device Specific Settings  $\rightarrow$  End Point Flows. On the Server Flows tab and click Add (not shown). Enter the following values;

- Flow Name ٠
- Server Configuration •
- Server Configuration for SM1 as per Section 6.2.7 • Received Interface
- Signaling Interface •
- Media Interface
- FromRemote-External-Signaling-1
- **To-Core-Internal-Signaling-1** Int Med intf Core-1
- End Point Policy Group
  - As created in Section 6.2.9, avaya-b2b2b

A Descriptive Name, e.g. Core-SBC-Server-1

**Topology Hiding Profile** As created in Section 6.2.9, Avaya

#### Click Finish.

•

•

Flow Name	Core-SBC-Server-1
Server Configuration	Server-Core-SM-1
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	FromRemote-External-Signaling-1
Signaling Interface	To-Core-Internal-Signaling-1
Media Interface	Int_Media_intf_Core-1
End Point Policy Group	avaya-def-low-enc
Routing Profile	default
Topology Hiding Profile	Avaya 🔹
File Transfer Profile	None 💌
	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).

EL; Reviewed:	Solution & Interoperability Test Lab Application Notes	52 of 71
SPOC 2/6/2014	©2014 Avaya Inc. All Rights Reserved.	ASBCEb2b2b7LS.doc

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**;

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  $\rightarrow$  Device Specific Settings  $\rightarrow$ 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.

Network Configuration Int	erface Configuration		
Changes will not take effect u	ntil the interface is updated.		
A1 Netmask 255.255.255.128 Add	A2 Netmask	B1 Netmask 255.255.255.224	B2 Netmask
IP Address	Public IP	Gate	way Interface
192.168.2.38		192.168.2.33	B1 💌
192.168.3.120		192.168.3.1	A1 •
192.168.3.121		192.168.3.1	A1 💌
192.168.2.51		192.168.2.33	B1 💌
192.168.2.43		192.168.2.33	B1 💌

Solution & Interoperability Test Lab Application Notes ©2014 Avaya Inc. All Rights Reserved. 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  $\rightarrow$  TLS Management  $\rightarrow$  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  $\rightarrow$  Device Specific Settings  $\rightarrow$  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
- TCP Port
   from the network management interfaces.
  - UDP Port **5060**
  - TLS Port **5061**
  - TLS Profile
- As created in Section 6.3.2, e.g., coreTLSserver

Name	From-DMZ-External-Sigi
IP Address	192.168.2.38 💌
TCP Port Leave blank to disable	5060
UDP Port Leave blank to disable	5060
Enable Stun	
TLS Port Leave blank to disable	5061
TLS Profile	coreTLSserver 💌
Enable Shared Control	
Shared Control Port	

Solution & Interoperability Test Lab Application Notes ©2014 Avaya Inc. All Rights Reserved. 55 of 71 ASBCEb2b2b7LS.doc

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

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

## 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	192.1683.120	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  $\rightarrow$  Global Profiles  $\rightarrow$  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.

	Next Hop Routing
URI Group	*
Next Hop Server 1 IP, IP:Port, Domain, or Domain:Port	192.168.4.64
Next Hop Server 2 IP, IP:Port, Domain, or Domain:Port	
Routing Priority based on Next Hop Server	
Use Next Hop for In Dialog Messages	
Ignore Route Header for Messages Outside Dialog	
NAPTR	
SRV	
Outgoing Transport	ILS TCP OUDP
	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**.

	Next Hop Routing
URI Group	*
Next Hop Server 1 IP, IP:Port, Domain, or Domain:Port	192.168.4.66
Next Hop Server 2 IP, IP:Port, Domain, or Domain:Port	
Routing Priority based on Next Hop Server	
Use Next Hop for In Dialog Messages	
Ignore Route Header for Messages Outside Dialog	
NAPTR	
SRV	
Outgoing Transport	TLS © TCP © UDP
	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**

Server Type	Call Server 👻
IP Addresses / Supported FQDNs Separate entries with commas	192.168.4.64
Supported Transports	□ TCP □ UDP ☑ TLS
TCP Port	5060
UDP Port	5060
TLS Port	5061

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

Enter the following values and click Next.

•

To URI

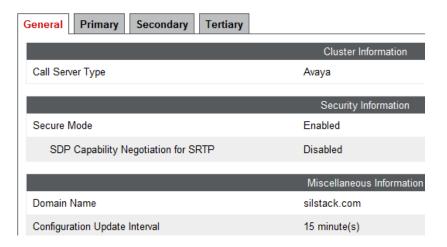
- Enable Heartbeat Check the box.
- Method Select **OPTIONS**.
- Frequency Enter **30** seconds.
- From URI SIP user
  - SIP user configured on System Manager User
    Management for heartbeat polling mechanism only, e.g.,
    22011@silstack.com. See Section 6.1.7 for more details.
    Same as From URI,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



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

Device Information			000 100				
Device Name			SBC-100	HA			
Device IP			192.168.2	2.38			
Configuration	Server Client A	ddress	192.168.3	.120			
				Edit			
			8				
Configuration Se							
onfiguration Se	ervers ———						
onfiguration Se Type	ervers Real Type	Port	Real IP	Real Port	Relay Mode	Rewrite URL	Server TL Profile
Туре	Real	Port 443	Real IP 192.168.4.143			Rewrite URL	Profile
Configuration Se Type HTTPS PPM	Real Type	10.00 V /		Real Port		Rewrite URL	core -PPN

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 <b>Section 6.3.6</b> , e.g., <b>Server-SM-2</b>
• Endpoint Signaling Interface	External interface for SM1 as created in <b>Section</b> <b>6.3.6</b> , e.g., <b>From-DMZ-External-Signaling-2</b>

#### 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**  $\rightarrow$  **Device Specific Settings**  $\rightarrow$  **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).

	Criteria
Flow Name	From-DMZ-1
URI Group	*
User Agent	*
Source Subnet Ex: 192.168.0.1/24	*
Via Host Ex: domain.com, 192.168.0.1/24	*
Contact Host Ex: domain.com, 192.168.0.1/24	*
Signaling Interface	From-DMZ-External-Signaling-1

Solution & Interoperability Test Lab Application Notes ©2014 Avaya Inc. All Rights Reserved. 61 of 71 ASBCEb2b2b7LS.doc Select the following values;

- Media Interface
- End Point Policy Group

Ext\_Med\_intf\_DMZ-1

- avaya-b2b2b Route\_To\_SM-1
- Routing Profile
- Phone Interworking Profile Avaya-Ru

Click **Finish**.

	Profile
Source	<ul> <li>Subscriber</li> <li>Click To Call</li> </ul>
Methods Allowed Before REGISTER	INFO MESSAGE NOTIFY OPTIONS
Media Interface	Ext_Med_intf_DMZ-1
End Point Policy Group	avaya-b2b2b
SIP Cluster Flow	
Routing Profile	Route_To_SM-1
	Optional Settings
Topology Hiding Profile	default 💌
Phone Interworking Profile	Avaya-Ru 💌
TLS Client Profile	None
File Transfer Profile	None 💌
Signaling Manipulation Script	None 💌
	Back

#### 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**  $\rightarrow$  **Device Specific Settings**  $\rightarrow$  **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).

•

•

Flow Name	Flow_SM
Server Configuration	Server-SM-1
URI Group	*
Transport	*
Remote Subnet	*
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	avaya-b2b2b
Routing Profile	default
Topology Hiding Profile	Avaya
File Transfer Profile	None 💌

#### 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  $\rightarrow$  Device Specific Settings  $\rightarrow$  Relay Services. Click on the Add button.

EL; Reviewed:	
SPOC 2/6/2014	

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.

pplication Rel	ay 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.	TCP	silstack.com	135.	TCP	192.168.3.121
silstack.com	135.	TCP	silstack.com	135	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	192.168.3.12

Solution & Interoperability Test Lab Application Notes ©2014 Avaya Inc. All Rights Reserved.

# 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 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.

EL; Reviewed:	Solution & Interoperability Test Lab Application Notes	
SPOC 2/6/2014	©2014 Avaya Inc. All Rights Reserved.	ASBO

```
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 \overline{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**.

# **Session Border Controller for Enterprise**

Dashboard	System Management			
Administration				
Backup/Restore System Management	Devices Updates Licensing			
Global Parameters				
<ul> <li>Global Profiles</li> <li>SIP Cluster</li> </ul>	Device Name (Serial Number)	Management IP	Version	Status
Domain Policies	EMS (IPCSEMS40004)	192.168.1.114	6.2.0.Q64	Commissioned
<ul> <li>TLS Management</li> <li>Device Specific Settings</li> </ul>	RemoteSBC1 (Secondary) (IPCS31040003)	192.168.1.112	6.2.0.Q64	Commissioned
	RemoteSBC1 (Primary)	192,168,1,113	6.2.0.Q64	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** 

EL; Reviewed:
SPOC 2/6/2014

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

	Time	Source	Destination		i antes de la		
lo.				Protocol L		and the second second second	
		172.17.10.17	172.17.10.10	TLSV1		Client	
		172.17.10.10	172.17.10.17	TLSV1	and the second se	Server	
		172.17.10.10	172.17.10.17	TLSV1		Certifi	
		172.17.10.17	172.17.10.10	TLSV1		Certifi	
		172.17.10.17	172.17.10.10	TLSV1			cate Verify
		172.17.10.10	172.17.10.17	TLSV1			Cipher Spec, Encrypted Handshake Message
		172.17.10.17	172.17.10.10	TLSV1			tion Data, Application Data
605	5 37.665227	172.17.10.10	172.17.10.17	TLSV1	654		tion Data, Application Data
						m	
		DALER OU MILE (A4)	DO DIES), II/S DA	res captured	u (940	U DILSJ	
	x cooked ca						
Inte	rnet Protoc	ol Version 4 Src.	177 17 10 10 (17				
							.10.17 (172.17.10.17)
🗄 Tran	smission Co	ontrol Protocol, Sr	c Port: sip-tls (	(5061), Dst H	Port:		.10.17 (172.17.10.17) 12432), seq: 1449, Ack: 71, Len: 1107
∃ Tran ∃ [2 R	smission Co eassembled	TCP Segments (2385	c Port: sip-tls (	(5061), Dst H	Port:		
∃ Tran ∃ [2 R ∃ Secu	smission Co eassembled re Sockets	ntrol Protocol, Sr TCP Segments (2385 Layer	c Port: sip-tls ( bytes): #508(136	(5061), Dst ( 59), #509(10)	Port:		
Tran [2 R Secu	smission Co eassembled re Sockets	TCP Segments (2385	c Port: sip-tls ( bytes): #508(136	(5061), Dst ( 59), #509(10)	Port:		
Tran [2 R Secu	smission Co eassembled re Sockets Sv1 Record	ntrol Protocol, Sr TCP Segments (2385 Layer	c Port: sip-tls ( bytes): #508(136	(5061), Dst ( 59), #509(10)	Port:		
E Tran E [2 R Secu E TL	smission Co eassembled re Sockets Sv1 Record Content Typ	ontrol Protocol, Sr TCP Segments (2385 Layer Layer: Handshake Pi	c Port: sip-tls ( bytes): #508(136	(5061), Dst ( 59), #509(10)	Port:		
E Tran E [2 R Secu E TL	smission Co eassembled re Sockets Sv1 Record Content Typ	ontrol Protocol, Sr TCP Segments (2385 Layer Layer: Handshake Pr e: Handshake (22) .5 1.0 (0x0301)	c Port: sip-tls ( bytes): #508(136	(5061), Dst ( 59), #509(10)	Port:		
E Tran E [2 R Secu ⊡ TL	smission Co eassembled re Sockets Sv1 Record Content Typ Version: TL Length: 238	ontrol Protocol, Sr TCP Segments (2385 Layer Layer: Handshake Pr e: Handshake (22) .5 1.0 (0x0301)	c Port: sip-tls ( bytes): #508(136 rotocol: Certific	(5061), Dst ( 59), #509(10)	Port:		
E Tran E [2 R Secu ⊡ TL	smission Co eassembled re Sockets Sv1 Record Content Typ Version: TL Length: 238 Handshake P	ontrol Protocol, Sr TCP Segments (2385 Layer Layer: Handshake Pr De: Handshake (22) 5 1.0 (0x0301) 30	c Port: sip-tls ( bytes): #508(136 rotocol: Certific	(5061), Dst ( 59), #509(10)	Port:		
E Tran E [2 R Secu TL	smission Co eassembled re Sockets Sv1 Record Content Typ Version: TL Length: 238 Handshake P	ontrol Protocol, Sr TCP Segments (2385 Layer Layer: Handshake Pi De: Handshake (22) 5 1.0 (0x0301) 30 Protocol: Certificate 2 Type: Certificate	c Port: sip-tls ( bytes): #508(136 rotocol: Certific	(5061), Dst ( 59), #509(10)	Port:		
E Tran E [2 R Secu ⊡ TL	smission Co eassembled re Sockets Sv1 Record Content Typ Version: TL Length: 238 Handshake P Handshake Length: 2	ontrol Protocol, Sr TCP Segments (2385 Layer Layer: Handshake Pi De: Handshake (22) 5 1.0 (0x0301) 30 Protocol: Certificate 2 Type: Certificate	c Port: sip-tls ( bytes): #508(136 rotocol: Certific	(5061), Dst ( 59), #509(10)	Port:		
Tran [2 R Secu TL	smission Co eassembled re Sockets Sv1 Record Content Typ Version: TL Length: 238 Handshake Length: 2 Certifica	ontrol Protocol, sr TCP Segments (2385 Layer Layer: Handshake Pi Pe: Handshake (22) 5 1.0 (0x0301) 80 Protocol: Certificate 2376 attes Length: 2373	c Port: sip-tls ( bytes): #508(136 rotocol: Certific	(5061), Dst ( 59), #509(10)	Port:		
Tran [2 R Secu TL	smission Co eassembled re Sockets Sv1 Record Content Typ Version: TL Length: 238 HandShake P Handshake Length: 2 Certifica ⊡ Certifica	ontrol Protocol, Sr TCP Segments (2385 Layer Layer: Handshake Pi De: Handshake (22) 5 1.0 (0x0301) 30 Protocol: Certificate 2376 a Type: Certificate 2376 ates Length: 2373 ates (2373 bytes)	c Port: sip-tls ( bytes): #508(136 rotocol: Certific	(5061), Dst ( 59), #509(10)	Port:		
Tran [2 R Secu TL	smission Co eassembled re Sockets Sv1 Record Content Typ Version: TL Length: 238 HandShake P HandShake Length: 2 Certifica Certifica	ontrol Protocol, sr TCP Segments (2385 Layer Layer: Handshake Pr be: Handshake (22) 5 1.0 (0x0301) 0 Protocol: Certificate 376 ates Length: 2373 ates (2373 bytes) icate Length; 1475	c Port: sip-tls ( bytes): #508(136 rotocol: Certific te (11)	(5061), Dst ( 99), #509(10)	Port: 16)]	12432 (	12432), seq: 1449, Ack: 71, Len: 1107
∃ Tran ∃ [2 R ∃ Secu □ TL	smission Co eassembled re Sockets Sv1 Record Content Typ Version: Ty Length: 238 HandShake P HandShake P HandShake P HandShake Certifica Certifica Certifica Certifica	ntrol Protocol, sr TCP Segments (2385 Layer Layer: Handshake Pi De: Handshake (22) .5 1.0 (0x0301) 30 Protocol: Certificate 276 ates Length: 2373 ates (2373 bytes) icate Length: 1475 icate (id-at commoni	c Port: sip-tls ( bytes): #508(136 rotocol: Certific te (11)	(5061), Dst ( 99), #509(10)	Port: 16)]	12432 (	
∃ Tran ∃ [2 R ∃ Secu □ TL	smission Co eassembled re Sockets SV1 Record Content Typ Version: TL Length: 238 Handshake Length: 23 Certifica Certifica Certific Certifi Certifi	ontrol Protocol, sr TCP Segments (2385 Layer Layer: Handshake Pr be: Handshake (22) 5 1.0 (0x0301) 0 Protocol: Certificate 376 ates Length: 2373 ates (2373 bytes) icate Length; 1475	c Port: sip-tls ( bytes): #508(136 rotocol: Certific (11) Name=coresbc.sils	(5061), Dst ; ;9), #509(10: :ate	Port: 16)] 16)] -at-or	12432 ( ganizat	12432), seq: 1449, Ack: 71, Len: 1107

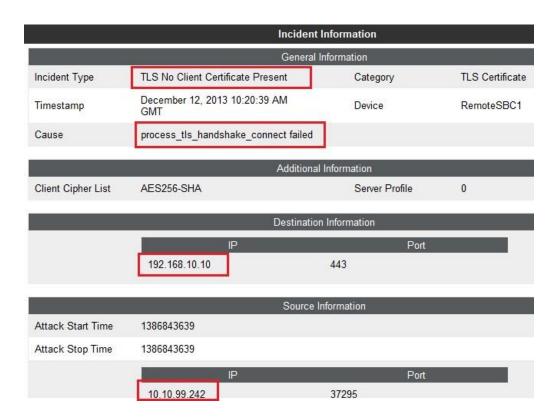
Click on the Incidents link on SBCE EMS GUI to check for errors in the SBCE logs.

	Alarms	Incidents	Statistics	Logs	Diagnostics	Users	
--	--------	-----------	------------	------	-------------	-------	--

## **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.



#### 8.2. Verify Avaya Aura® Session Manager

Log into Avaya Aura® System Manager, see **Reference [6]** for details. Navigate to **Elements** $\rightarrow$  **Session Manager**  $\rightarrow$  **System Status**  $\rightarrow$  **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**

												Custo	omize 🎙
View  Default Force Unregister AST Device Notifications: Reboot Reload  Failback As of 11:34 AM Advanced S													
Iter	ms Found	Refresh Show ALL	•							F	ilter: Disa	able, Apr	oly, Clea
	Details	Address	First Name	Last Name	Actual Location	IP Address	Remote Office	Shared Control	Simult. Devices	AST Device	Registered		
											Prim	Sec	Surv
	1	22003@silstack.com			1								
	►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)		

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

EL; Reviewed: SPOC 2/6/2014

Solution & Interoperability Test Lab Application Notes ©2014 Avaya Inc. All Rights Reserved. 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.

Interoperability 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 <u>http://support.avaya.com</u>.

[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.

#### ©2014Avaya Inc. All Rights Reserved.

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

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