Avaya Solution & Interoperability Test Lab

Application Notes for Configuring an Multi-Site VoIP Solution using Check Point VPN-1 Power/UTM NGX R65.2.100 with an Avaya Aura™ Telephony Infrastructure in a Converged VoIP and Data Network - Issue 1.1

Abstract

These Application Notes describe the steps for configuring Multi-Site VoIP Solution using Check Point's VPN-1 Power/UTM NGX R65.2.100 with an Avaya Aura™ Telephony Infrastructure in a Converged VoIP and Data Network consisting of a Corporate Headquarters with three remote sites.

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

1. Introduction

These Application Notes describe the configuration of a Multi-Site Avaya/Check Point VoIP solution using Check Point's VPN-1 Power/UTM NGX R65.2.100 consisting of the Check Point NGX R65.4 SmartCenter, Check Point NGX R65.4 SmartConsole and Check Point NGX R65.2.100 Gateways with an Avaya Aura™ Telephony Infrastructure consisting of Avaya Aura™ Communication Manager, Avaya Aura™ SIP Enablement Services, Avaya Modular Messaging, Avaya Aura™ Communication Manager Messaging and Avaya IP Telephones in a converged Voice over IP and Data Network.

The configurations discussed in these Application Notes describe what ports have to be opened on the main office and at the remote site firewalls to provide contact center services.

A firewall is a security system that acts as a protective boundary between private and public IP networks. It filters incoming traffic while allowing the systems behind the firewall to communicate with the outside world.

Check Point NGX R65.2.100 Firewall is a VoIP aware gateway offering comprehensive security for Enterprises, Telecom networks, and Service Provider VoIP environments.
The NGX R65.2.100 version of Check Point's security product VPN-1 Power/UTM, provides the highest levels of security, connectivity, and Quality of Service (QoS), by using Check Point's stateful inspection engine to analyze the VoIP traffic.

1.1. Interoperability Compliance Testing

Compliance testing emphasis was placed on validating that VoIP traffic and voice features, e.g., voicemail, conferencing, worked properly while traversing the network through the Check Point VPN-1 Power/UTM NGX R65.2.100 firewalls.

Note: ALG with NAT was not compliance tested.

The telephony features verified to operate correctly included:

- Attended/Unattended transfer
- Conference call add/drop/participation
- Multiple call appearances
- Caller ID operation
- Call forwarding
- Call Park,/Call pick-up
- Bridged call appearances
- Voicemail using Communication Manager Messaging and Avaya Modular Messaging
- Message Waiting Indicator (MWI)
- Hold/Return from hold
- Direct IP Media (Shuffling)
- G.711 and G.729 codecs

Serviceability testing:

- Serviceability testing was conducted to verify the ability of the Avaya/Check Point solution to recover from adverse conditions, such as power cycling network devices and disconnecting cables between the LAN interfaces. In all cases, the ability to recover after the network normalized was verified.

1.2. Support

For technical support on Check Point products, consult the support pages at http://www.checkpoint.com

2. Reference Configuration

The configuration in **Figure 1** shows a converged VoIP and data network with multiple remote sites. For compliance testing, a centralized corporate DHCP server was used. To better manage the different traffic types, the voice and data traffic were separated onto different VLANs.

2.1. Corporate Headquarters

The Corporate Headquarters consisted of one Check Point NGX R65.4 SmartCenter, one Check Point NGX R65.4 SmartConsole, one Check Point NGX R65.2.100 Gateway, one Communication Manager running on an Avaya S8300 Server with an Avaya G450 Media Gateway, Communication Manager running on an Avaya S8500 Server, one SIP Enablement Services, Avaya Modular Messaging, Avaya Aura™ Communication Manager Messaging, one Avaya 2410 Digital Telephone, one Avaya 9640 IP Telephone running Avaya one-X Deskphone Edition on VLAN Voice1 (H.323), one Avaya 9630 IP Telephone running Avaya one-X Deskphone SIP on VLAN Voice1 and one Corporate DHCP/File server. The Corporate Headquarters provided a DHCP/File server for assigning IP network parameters and to download settings to the Avaya IP telephones.

2.2. Remote Site A

Remote Site A consisted of one Check Point NGX R65.2.100 Gateway, one Avaya 9650 IP Telephone running Avaya one-X Deskphone Edition (H.323), one Avaya 9620 IP Telephone running Avaya one-X Deskphone SIP, and a PC on data network. The Avaya H.323 IP telephone register to the headquarters Communication Manager and the Avaya SIP IP telephone register to the headquarters SIP Enablement Services.

2.3. Remote Site B

Remote Site B consisted of one Check Point NGX R65.2.100 Gateway, one Avaya G650 Media Gateway, and two Avaya Analog Telephones. The Remote Site B Avaya G650 Media Gateway registers via the Avaya proprietary CCMS protocol, to the headquarters Avaya S8500 Server. While the Avaya Analog Telephones are directly connected to the Remote Site B Avaya G650 Media gateway, they are administered on the headquarters Avaya S8500 Server running Communication Manager.

2.4. Remote Site C

Remote Site C consisted of one Check Point NGX R65.2.100 Gateway, one Avaya G700 Media Gateway, and two Avaya 2410 Digital Telephones. The Remote Site C Avaya G700 Media Gateway registers via H.248, to the headquarters Communication Manager running on the Avaya S8300 Server. While the Avaya 2410 Digital Telephones are directly connected to the Remote Site C Avaya Media gateway, they are administered on the headquarters Communication Manager.

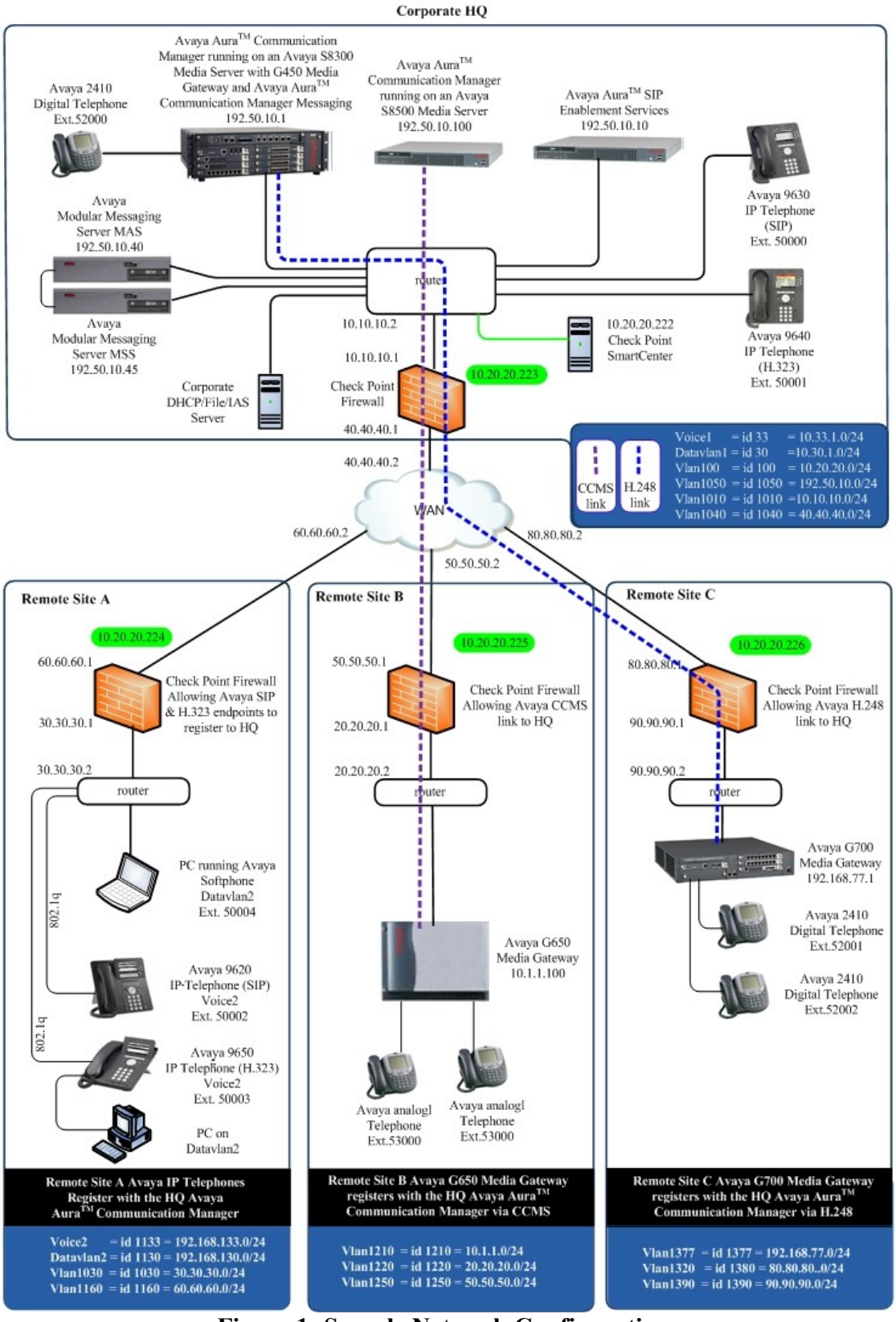


Figure 1: Sample Network Configuration

3. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya Products	
HQ Avaya PBX 1	
Avaya S8300 Server running Avaya Aura™ Communication Manager	Avaya Aura™ Communication Manager 5.2
Avaya G450 Media Gateway (Corporate Site) MGP MM712 DCP Media Module Avaya Aura™ Communication Manager Messaging	 28.22.0 HW9 5.2
HQ Avaya SIP Enablement Services	
Avaya Aura™ SIP Enabled Services Server	5.2 SP2
HQ Avaya Messaging (Voice Mail) Products	
Avaya Modular Messaging - Messaging Application Server (MAS)	5.0
Avaya Modular Messaging - Message Storage Server (MSS)	5.0
Avaya Aura™ Communication Manager Messaging	5.2
HQ Avaya PBX 2	
Avaya S8500 Server (CCMS) to site B	Avaya Aura™ Communication Manager 5.2
Site B Avaya PBX Products	
Avaya G650 Media Gateway (CCMS) TN799DP (C-LAN) TN2602AP (MEDPRO) TN2312BP (IPSI)	 HW01, FW026 HW02, FW007 HW15, FW030
Site C Avaya PBX Products	
Avaya G700 Media Gateway MGP MM712 DCP Media Module	 26.31.0 HW05 / FW08
Avaya Telephony Sets	
Avaya 9600 Series IP Telephones	Avaya one-X Deskphone Edition 3.0.1
Avaya 9600 Series IP Telephones	Avaya one-X Deskphone SIP 2.4
Avaya 2410 Digital Telephone	5.0
Check Point Products	
Check Point NGX R65.4 SmartCenter	R65.4
Check Point NGX R65.4 SmartConsole	R65.4
Check Point NGX R65.2.100 Gateway	R65.2.100
MS Products	
Microsoft Windows 2003 Server	File/DHCP Service

4. Configure QoS on Communication Manager

There were two Communication Manager used in **Figure 1**. This section describes the steps required for Communication Manager to support the configuration shown in **Figure 1**. The following pages provide instructions on how to administer the required configuration parameters. The assumption is that the appropriate license and authentication files have been installed on the servers and that login and password credentials are available. It is assumed that the reader has a basic understanding of the administration of Communication Manager and has access to the System Administration Terminal (SAT) screen. For detailed information on the installation, maintenance, and configuration of Communication Manager, please consult references in **Section 9, [1]** through **[3].**

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

In order to achieve prioritization of VoIP traffic, the VoIP traffic must be classified. The Avaya Aura™ Telephony Infrastructures supports both 802.1p and DiffServ.

The DiffServ and 802.1p/Q values configured in the ip-network-reagion will be downloaded to the Avaya H.323 IP Telephones via Communication Manager. Avaya SIP IP Telephones will get QoS settings by downloading the 46xxsettings file from the HTTP server (not shown in this document). For more information on QoS settings please refer to **Section 9, [1]** through **[3]**.

4.1. Configure the ip-network-region for the Avaya IP Telephones

The Differentiated Services Code Point (DSCP) value of 46 will be used for both Per-Hop Behavior (PHB) values. DSCP 46 represents the traffic class of premium and the traffic type voice. Set the **Call Control PHB Value** to **46** and the **Audio PHB Value** to **46**. **Call Control 802.1p Priority** and **Audio 802.1p Priority** are set to **6**.

1. From the SAT, use the **change ip-network-region 1** command to change the DIFFSERV/TOS PARAMETERS and 802.1P/Q PARAMETERS settings. Change the following:

- **Call Control PHB Value** set to **46**
- **Audio PHB Value** set to **46**
- **Call Control 802.1p** set to **6**
- **Audio 802.1p priority** set to **6**

```
change ip-network-region 1                                    Page   1 of  19
                             IP NETWORK REGION
  Region: 1
Location:         Authoritative Domain: dev4.com
    Name:
MEDIA PARAMETERS                Intra-region IP-IP Direct Audio: yes
      Codec Set: 1              Inter-region IP-IP Direct Audio: yes
   UDP Port Min: 2048                     IP Audio Hairpinning? y
   UDP Port Max: 3027
DIFFSERV/TOS PARAMETERS                 RTCP Reporting Enabled? y
 Call Control PHB Value: 46      RTCP MONITOR SERVER PARAMETERS
        Audio PHB Value: 46       Use Default Server Parameters? y
        Video PHB Value: 26
802.1P/Q PARAMETERS
 Call Control 802.1p Priority: 6
        Audio 802.1p Priority: 6
        Video 802.1p Priority: 5      AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS                                      RSVP Enabled? n
  H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
   Keep-Alive Interval (sec): 5
            Keep-Alive Count: 5
```

5. Configure Check Point

A firewall policy is a set of rules and protections that determines what types of connections are or are not allowed across a firewall. Firewall security policies were configured on the main office SmartCenter that centrally manages all sites. All the Gateways were configures to allow legal and wanted types of traffic to and from sites and to block any traffic, which was illegal or unexpected. The enterprise server platforms at the main office and remote sites were assigned IP Addresses within the same IP Address domain. Network Address Translation (NAT) was NOT tested.

Check Point NGX R65.2.100 Firewall is a VoIP aware gateway offering comprehensive security, connectivity and QoS, by using Check Point's stateful inspection engine to analyze the VoIP traffic. The firewall dynamically opens the ports for media (audio/video) for SIP and H.323 protocols.

In addition, the default set of VoIP protections in Check Point SmartDefense was enforced during the tests to have full RFC enforcement and security protection against Denial of Service (DoS) attacks.

5.1 SmartDashboard Rule Base Configuration

The following configuration describes the ports that had to be opened to provide services to all sites and corporate HQ. The Check Point SmartDashBoard application was used to configure the firewall rules on R65.4 SmartCenter that centrally manages all R65.2.100 gateways in HQ and remote sites. Please refer to the Check Point Firewall-1 **[8]** and SmartCenter **[9]** documentation for more information on how to create and deploy the firewall policy rules specified in **Table 2**. It is assumed that the reader has a basic understanding of the administration of Check Point Gateways and SmartConsole.

The following table summarizes the rules that had to be configured on for all the Check Point Gateways in order to allow all the legal and wanted traffic from and to the all the Remote Sites.
Abbreviations

Corporate HQ:

- MAS - Avaya Modular Messaging Server MAS
- MSS - Avaya Modular Messaging Server MSS
- AACM - Communication Manager running on an Avaya S8300 Server with an Avaya G450 Media Gateway
- SES - SIP Enablement Services
- h323.HQ – network containing H.323 endpoints, for example: Avaya 9640 IP Telephone running Avaya one-X Deskphone Edition on VLAN Voice1 (H.323)
- sip.HQ - one Avaya 9630 IP Telephone running Avaya one-X Deskphone SIP
- DHCP - Corporate DHCP/File server.

Remote Site A:

- h323.A - Avaya 9650 IP Telephone running Avaya one-X Deskphone Edition (H.323)
- sip.A - Avaya 9620 IP Telephone running Avaya one-X Deskphone SIP

Remote Site B:

- MG_B - Avaya G650 Media Gateway

Remote Site C:

- MG_C - Avaya G700 Media Gateway

Rule	Rule Name	Service	Port(s)	From	To	Notes
		ports needed to be opened (example ports)				
1.	DHCP	bootp	UDP 67	- All the Remote Sites - Corporate HQ	- All the Remote Sites - Corporate HQ	
2.	SIP	sip sip-tcp	UDP 5060 TCP 5060	- MAS - MSS - AACM - SES - sip.HQ - sip.A	- MAS - MSS - AACM - SES - sip.HQ - sip.A	- These should be opened for the networks containing SIP endpoints or servers in both sites

3.	H.323	H323 H323_ras	TCP 1720 UDP 1719	- MAS - MSS - AACM - h323.HQ - h323.A	- MAS - MSS - AACM - h323.HQ - h323.A	- These should be opened for the networks containing H.323 endpoints or servers in both sites - In order to allow H.323 phones registration on all the GWs inspecting H.323 traffic, set "fw ctl set int h323_gk_init_tcp_conn 1" permanently.
4.	H.248 traffic	H.248	TCP 2944 TCP 2945 TCP 1039	- AACM - MG_B	- AACM - MG_B	H.248 signaling channel between media server and media gateway.
5.	H.248 RTP	RTP(udp-high-ports)	UDP 1024-65535	- MG_C	Any Site	UDP high ports are opened in order to allow RTP traffic for H.248 protocol. Since H.248 is not inspected, data ports are not opened dynamically and have to be opened statically. *
6.	H.248 RTP	RTP(udp-high-ports)	UDP 1024-65535	Any Site	- MG_C	See previous.
7.	CCMS traffic between Remote Site B and Corporate HQ	CCMS	TCP 5010 TCP 5011 TCP 5012 TCP 1956	- AACM - MG_B	- AACM - MG_B	**CCMS** is an **Avaya** proprietary protocol for **port** network control.

Table 2: All Sites Firewall Ports

* UDP high ports are opened in this case **only** in order to allow media connections opened by H.248 protocol. It is a bad practice to open UDP high ports for inspected protocols (sip, h323, etc.), since those media protocol connections are opened dynamically.

5.1 Additional H.323 Configuration on R65.2.100 gateways

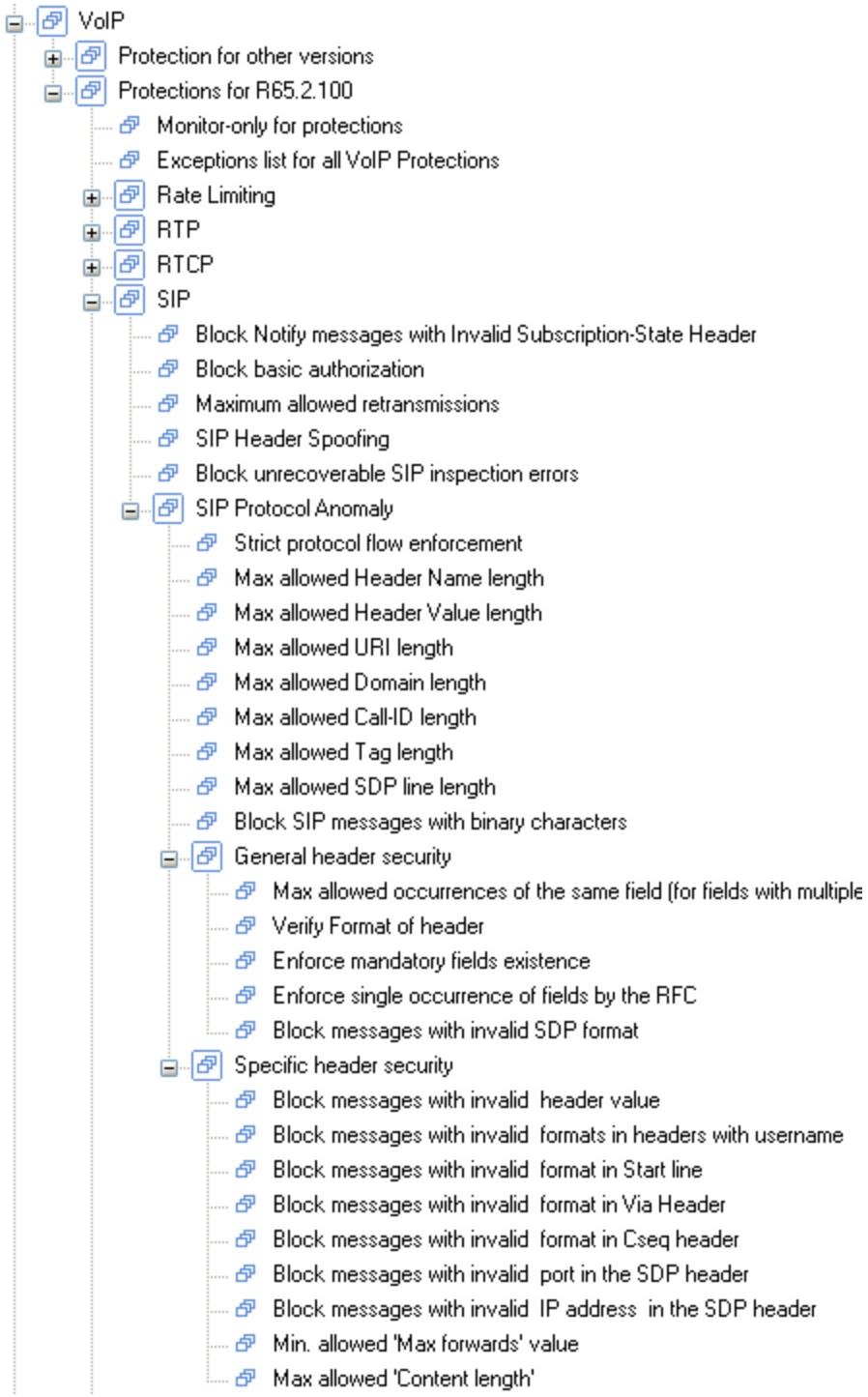
In order to allow H.323 phones registration on all the R65.2.100 gateways inspecting H.323 traffic, set the global parameter h323_gk_init_tcp_conn by running the following command on the gateways "**fw ctl set int h323_gk_init_tcp_conn 1**".

For more information on how to set the global firewall parameter, refer to **Section 9, [10]**.

The endpoint normally initiates the H.323 (H.225) TCP connection to the Gatekeeper or server. In scenarios where the Gatekeeper initiates the TCP connection to the Endpoint, the global parameter "h323_gk_init_tcp_conn" should be set to 1.
Note that when running Communication Manager, the TTS (Time to service) feature is enabled by default. When TTS is enabled, the Gatekeeper initiates the TCP connection to the endpoint, and so the "h323_gk_init_tcp_conn" parameter must be set.

5.2 SmartDefense configuration in SmartDashboard

The default set of VoIP protections in Check Point SmartDefense was enforced during the tests to have full RFC enforcement and security protection against DoS attacks.



For Compliance testing the following protections were configured differently:

- **SmartDefense-> Application Intelligence-> VoIP-> Protections for R65.2.100-> SIP-> SIP Protocol Anomaly -> Specific header security -> Block messages with invalid format In Start line**
    - When H.323 phone is bridging, Communication Manager running on an Avaya S8300 Server with an Avaya G450 Media Gateway sends a "SIP/2.0 181" response without the third part in the start-line. The message is dropped by firewall rule "**Block messages with invalid format In Start line**". In order to allow this message to pass, Communication Manager running on an Avaya S8300 Server with an Avaya G450 Media Gateway or relevant endpoint should be added to the exception list of the above protection.

- **SmartDefense-> Application Intelligence-> VoIP-> Protections for R65.2.100-> SIP-> SIP Protocol Anomaly -> Strict protocol flow enforcement**
    - When a '484 Address Incomplete' message is sent out of order by Avaya Modular Messaging Server, it is being dropped by the firewall rule "**Strict protocol flow enforcement**" protection. In order to allow this packet through, the Avaya Modular Messaging Server or relevant endpoint should be added to the exception list of the above protection.

6 General Test Approach and Test Results

6.1 Test Approach

All feature functionality test cases were performed manually. The general test approach entailed verifying the following list traversing the network through the Check Point VPN-1 Power/UTM NGX R65.2.100 firewalls:

- LAN/WAN connectivity between all locations.
- Registration of Avaya H.323 and SIP IP telephones in Remote Site A with Corporate HQ Communication Manager (H.323) and SIP Enablement Services (SIP).
- H.248 Registration of the Avaya G700 Gateway in Remote Site C with Corporate HQ Communication Manager.
- Verification of the DHCP relay configuration.
- Inter-office calls using G.711 mu-law & G.729 codecs.
- Verifying that DSCP and 802.1p Priority QoS values are not altered by the Check Point VPN-1 Power/UTM NGX R65.2.100 solution.
- Verifying that Avaya Modular Messaging voicemail and MWI work properly.
- Verifying that Communication Manager Messaging voicemail and MWI work properly.
- Retrieving Voicemail messages from Remote locations.
- Features Tested:
    - Attended/Unattended transfer
    - Conference call add/drop/participation
    - Multiple call appearances
    - Caller ID operation
    - Call forwarding
    - Call Park,/Call pick-up
    - Bridged call appearances
    - Voicemail using Communication Manager Messaging & Avaya Modular Messaging
    - Message Waiting Indicator (MWI)
    - Hold/Return from hold
    - Direct IP Media (Shuffling)
    - G.711 and G.729 codecs

6.2 Test Results

All feature functionality, serviceability, and performance test cases passed. VoIP traffic and voice features worked properly while traversing the network through the Check Point VPN-1 Power/UTM NGX R65.2.100 firewalls.

7 Verification Steps

While the Check Point VPN-1 Power/UTM NGX R65.2.100 firewalls are in place, the general verification steps include:

- Verifying the DHCP relay through the network is functioning by confirming that the Avaya IP telephones receive their IP addresses from the DHCP server.
- Check that the Avaya H.323 IP telephones have successfully registered with Communication Manager using the **list registered-station** command.
- Check that the Avaya SIP IP telephones have successfully registered with SIP Enablement Services by listng the Registered Users on the Administrative GUI.
- Place internal and external calls between the digital telephone and IP telephones at each site.

8 Conclusion

These Application Notes describe the configuration steps for integrating Check Point VPN-1 Power/UTM NGX R65.2.100 with an Avaya t Aura™ telephony infrastructure. All feature functionality, serviceability, and performance test cases passed. VoIP traffic and voice features worked properly while traversing the network through the Check Point VPN-1 Power/UTM NGX R65.2.100 firewalls.

9 Additional References

The documents referenced below were used for additional support and configuration information.

The following Avaya product documentation can be found at http://support.avaya.com.

[1] *Administering Avaya Aura™ Communication Manager,* May 2009, Issue 5.0, Document Number 03-300509.

[2] *Administering Avaya Aura™ SIP Enablement Services*, May 2009, Issue 2.1, Document 03-602508.

[3] *Avaya Aura™ SIP Enablement Services (SES) Implementation Guide*, May 2009, Issue 6, Document 16-300140.

[4] *Avaya one-X Deskphone Edition for 9600 Series IP Telephones Administrator Guide Release 3.0,* Document Number 16-300698.

[5] *Avaya one-X Deskphone SIP for 9600 Series IP Telephones Administrator Guide, Release 2.0,* Document Number 16-601944.

[6] *Modular Messaging, Release 5.0 with the Avaya MSS Messaging Application Server (MAS) Administration Guide,* January 2009.

[7] *Avaya Aura™ Communication Manager Messaging Installation and Initial Configuration, Release 5.2*, May 2009, Issue 1, Document Number 03-603353.

Related Product documentation for Check Point products are:

[8] *NGX R65.4 and R65.2.100 Release Notes*
http://downloads.checkpoint.com/dc/download.htm?ID=8758

[9] *VOIP NGX R65.2.100 Administration Guide*
http://downloads.checkpoint.com/dc/download.htm?ID=8690

[10] Global firewall parameter
https://supportcenter.checkpoint.com/supportcenter/portal?eventSubmit_doGoviewsolutiondetails=&sI solutionid=sk26202

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