Avaya Solution & Interoperability Test Lab

Configuring Check Point ® Firewall-1® to support Avaya Contact Center Solutions - Issue 1.1

Abstract

These Application Notes explain how to configure Check Point ® Firewall-1 ® to support the Avaya Contact Center Release 3.0 solution. 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. Testing was conducted via the Developer*Connection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes explain how to configure Check Point Firewall-1 to support the Avaya Contact Center Release 3.0 solution. 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. Firewalls have one of two "stances", which is a default rule that is defined if none of the other user-defined rules apply:

- Default permit stance: permit what is not explicitly denied.
- Default deny stance: deny what is not explicitly permitted.

The "default permit stance" is more permissive; the "default deny stance" is more secure. The main office and remote site firewall configurations shown in these Application Notes used the "default deny stance".

The network architecture depicted in **Figure 1** represents the Avaya Contact Center Release 3.0 reference configuration, which is used as a reference throughout this document. The main office and remote site firewalls are circled in red. The contact center environment consists of Avaya Communication Manager on an Avaya Shared Blade Server 3000 located at the main office. The Avaya Shared Blade Server 3000 is in the Processor C-LAN (PC-LAN) mode. An Avaya S8300 Media Server configured as a Local Survivable Processor and Avaya 4600 Series IP Telephones are located at each remote site.

In Avaya Contact Center Release 3.0, the Network Address Translation (NAT) traversal support for H.323 endpoints is provided via a network based Juniper VF 3000, which is located at the main office. For all VoIP calls, Juniper VF3000 processes signaling and media relay functions. The H.323, H.248 and RTP packets flow through Juniper VF3000 only and do not pass through the main office firewall. All the IP Telephones at the remote sites are configured with Juniper VF3000 Signaling Control IP address as their default gateway. The Juniper VF 3000 registers to Avaya Communication Manager in the main office.

Avaya Interaction Center 7.0, Avaya Business Advocate 7.0, Avaya Operational Analyst and Microsoft SQL server are installed on another IBM HS20 Blade Server running VMWare in the main office. Also installed in the main office are Avaya Interactive Response, Avaya Call Management System, and Avaya Predictive Dialing System.

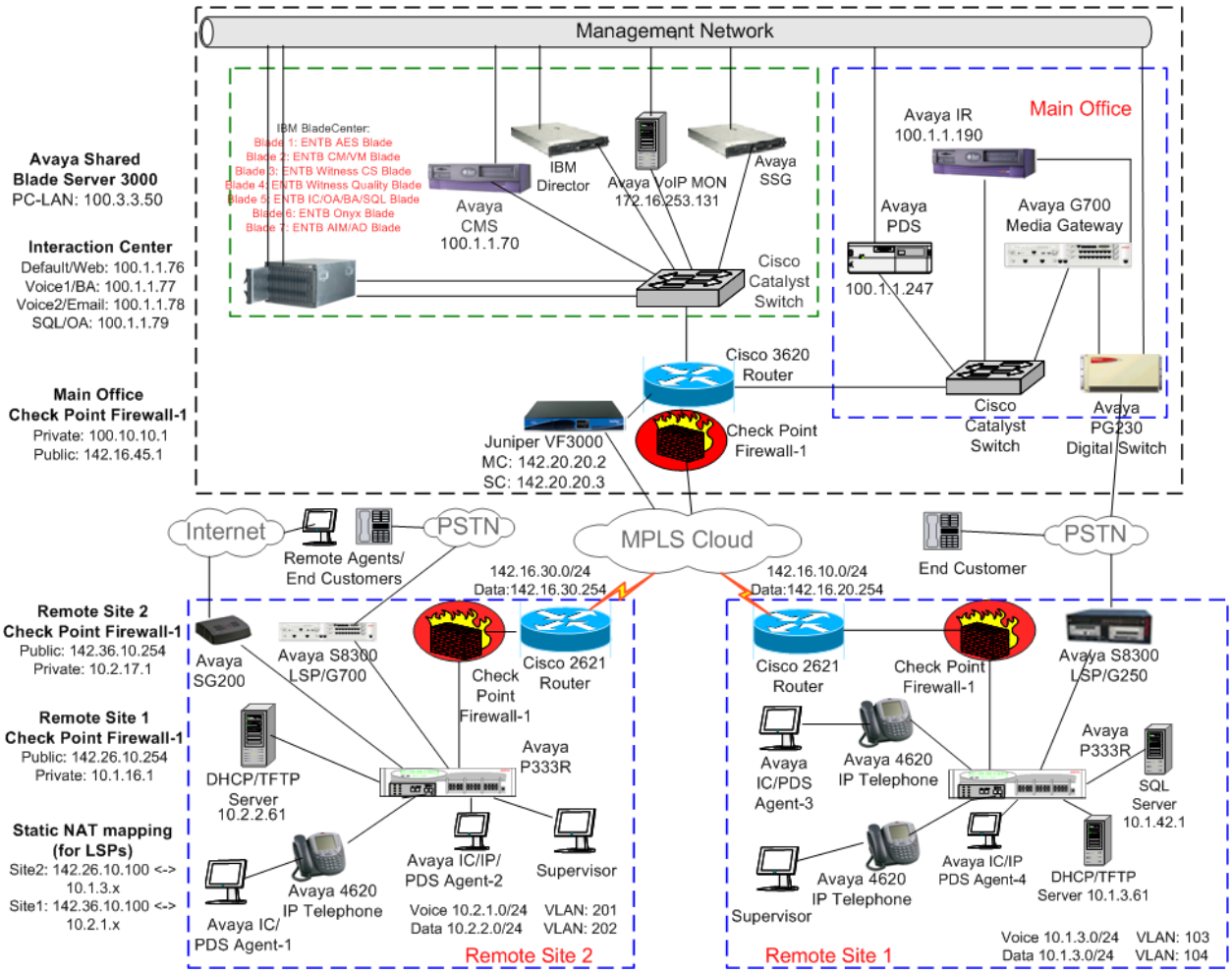

Figure 1: Avaya Contact Center R3.0 Reference Configuration

Standard firewall security policies[1] were configured on the main office and remote site Check Point Firewall-1 to provide contact center services to all the sites. Furthermore, all firewalls were configured to allow all traffic originating from the private networks to get out to the public networks. The enterprise server platforms at the main office used public "Class C" IP addresses while the remote sites used private "Class C" IP addresses.

The Check Point Firewall-1 is considered a "stateful" firewall. A "stateful" firewall is one that monitors all aspects of the communications that cross its path and inspects the source and destination addresses of each message that it handles.

[1] A firewall policy is a set of rules that determine what types of connections are or are not allowed across a firewall.

2. Hardware and Software Validated

The following hardware and software version were used for this configuration:

Equipment	Software
Avaya Shared Blade Server 3000	3.0 (R013x.00.0.344.0)
Avaya S8300 Media Servers (LSPs)	3.0
Avaya G700 Media Gateway	--
Avaya G250 Media Gateway	--
Avaya MultiVantage Application Enablement Service Server ▪ Red Hat Linux Enterprise Version 3.0 ▪ IBM HS20 Blade ▪ Processor: Intel Xeon CPU 2.4GHz ▪ Disk: 60 GB	3.0 Build 46
Avaya Interaction Center ▪ Microsoft Server 2003 ▪ IBM HS20 Blade	R7.0 Build 58
Avaya Business Advocate	R7.0
Avaya Operational Analyst	R7.0
Avaya Interactive Response (Sun Blade 150)	R1.3
Avaya Call Management System (Sun Blade 150)	R13
Avaya Predictive Dialing System (HP-UX for B2000/B2600)	R12 (SP4)
Avaya Proactive Contact Gateway (PG-230 Digital Switch)	15.2.3
Avaya Campaign Director	4 (SP4)
Avaya PDS Agent	1.0 (SP4)
Installation and Recovery Server	3.0 (Load 340.3 Patch 1501)
IBM Director V4.2 for Avaya Shared Blade Server 3000	Windows 2003 Server
IBM HS20 Blade Servers for Avaya Shared Blade Server 3000 (Model 8832LEX) ▪ Processor: Intel Xeon CPU 2.8GHz/533MHz (Dual) ▪ Disk: 40GB IDE (Dual), Memory: 4024MB ▪ Fiber-Channel Expansion Card	--
IBM Blade Center Chassis (Model 86771XX)	HW: 05
IBM Blade Center Management Module	HW: 04 / Rev: 16
IBM Blade Center 4-port GB Ethernet Switch Modules	HW: 02 / Rev: 68 (MA)
IBM Blade Center Fiber Channel Switch Modules	Rev: 07
IBM DS4300 Storage Server (SAN)	05.34.04.00
IBM FAStT Storage Manager Client	9
IBM Director (with IBM Patch IC43838)	4.20.2
VMware ESX Server (for Avaya Shared Blade Server 3000)	2.1.2
VMware ESX Server (for Avaya Interaction Center)	2.5
Check Point Firewall-1 (NG with Application Intelligence)	R55 091
Juniper VF 3000	603021
DHCP/TFTP Servers: Microsoft Windows 2000 Server	5.00.2195 (SP2)

Table 1: Equipment and Software Validated

3. Main Office Firewall Configuration

The following configuration describes the ports on the main office Check Point Firewall-1 that had to be opened to provide contact center services to the remote sites. The Check Point Smartdashboard™ application was used to configure the firewall rules. Please refer to the *Check Point Firewall-1* [1] and *SmartCenter*™ [2] documentation for more information on how to create and deploy the firewall policy rules specified in **Table 2**.

The following table summarizes the ports that were opened on the public side of the main office firewall. All traffic from the private side was allowed to traverse the firewall to the public side.

Rule	Service	Port(s)	From	To	Notes
	Avaya Interaction Center/Operational Analyst and Onyx Server Ports[2]				
1.	VESP	TCP 9001-9100	Remote Site firewall public IP address	Main Office IC servers	VESP protocol between IC servers and IC agents.
2.	PAGING	TCP 4200	Remote Site firewall public IP address	Main Office IC servers	Communication between IC agent desktop and IC web server component.
3.	IC_EMAIL	TCP 19113	Remote Site firewall public IP address	Main Office IC servers	Communication between IC agent desktop and IC email server component.
4.	IC_HTTP	TCP 9170	Remote Site firewall public IP address	Main Office IC voice servers	Communication between IC agent desktop and IC voice server components.
5.	IC_ICM	TCP 9501	Remote Site firewall public IP address	Main Office IC website	Communication between IC agent desktop and IC website.
6.	HTTPS[3]	TCP 443	Remote Site firewall public IP address	Main Office IC, OA, and Onyx servers	Communication between IC agent/supervisor desktop and IC/OA/Onyx websites.
	Avaya Business Advocate Supervisor Port				
7.	RDP	TCP 3389	Remote Site	Main Office	Terminal services port used by

[2] TCP ports (9503 (ICM), 4010 (HTTP), and 2300 (Attribute)) also need to be opened if the IC website server goes through a firewall. These ports are used for the communication between the Icweb and the IC website servers.
[3] HTTP (TCP Port 80) can alternatively be used if encrypted HTTP traffic is not required.

Rule	Service	Port(s)	From	To	Notes
			firewall public IP address	BA server	the remote site supervisor to gain access to the BA Supervisor tool[4].
	Avaya Call Management System Supervisor and Visual Vectors Application Ports				
9.	Telnet	TCP 23	Remote Site firewall public IP address	Main Office CMS	Telnet protocol used by the CMS Supervisor and CMS Visual Vector applications. These applications are used by the remote site supervisor for voice ACD reporting and call center administration.
10.	VV_SERVER	TCP 4000-4199	Remote Site firewall public IP address	Main Office CMS	Communication between CMS Visual Vectors at the remote site and the CMS server. This port range can be configured in the CMS "/opt/OrbixMT/config" file.
11.	VV_Deamon	TCP 2890	Remote Site firewall public IP address	Main Office CMS	Communication between CMS Visual Vectors at the remote site and the CMS Orbix deamon. This port can also be configured in the CMS "/opt/OrbixMT/config" file.
	SNMP Port				
12.	SNMP_TRAP	UDP 162	Remote Site firewall public IP address	Main Office VoIP Monitoring Server[5]	SNMP Traps from the Avaya S8300 LSPs and G700 Media Gateways. In the test configuration, this is the remote site firewall public IP address.
	DNS Ports				
13.	DNS_TCP	TCP 53	Remote Site firewall public IP address	Main Office DNS server	Domain Name Server download
14.	DNS_UDP	UDP 53	Remote Site	Main Office	Domain Name Server

[4] Terminal Services was used as a workaround since the BA supervisor tool could not be installed at the remote sites. The BA tool does not work across Network Address Translation (NAT).

[5] The Avaya VoIP Monitoring server was used as proxy, routing SNMP and HP OV traffic between the main office and management networks.

Rule	Service	Port(s)	From	To	Notes
			firewall public IP address	DNS server	download
	Avaya Predictive Dialing System				
15.	PDS_Agent	TCP 22700	Remote Site firewall public IP address	Main Office PDS	PDS Agent incoming traffic. This is destination port on the PDS.
16.	PDS_Director	TCP 23200 TCP 23260	Remote Site firewall public IP address	Main Office PDS	PDS Campaign Editor, PDS Campaign Analyst, Agent Blend Administer and PDS MiddleTier Configurator ports. These are destination ports on the PDS. All reporting tools in PDS use these TCP ports.
17.	PDS_SQL	TCP 1521	Remote Site firewall public IP address	Main Office PDS	PDS Campaign Monitor port used for database query.

Table 2: Avaya Contact Center R3.0 Main Office Firewall Ports

4. Remote Site Firewall Configuration

The following configuration describes the ports on the remote site Check Point Firewall-1 that had to be opened. As previously noted, the Check Point Smartdashboard application was used to configure the firewall rules. Please refer to the *Check Point Firewall-1* [1] and *SmartCenter* [2] documentation for more information on how to create and deploy the firewall policy rules specified in **Table 3**.

The following table summarizes the ports that were opened on the public side of the remote office firewalls. All traffic from the private side was allowed to traverse the firewalls to the public side.

Rule	Service	Port(s)	From	To	Notes
	Avaya Communication Manager (CM) Ports				
1.	H.248	TCP 2945	Other Remote Site firewall public IP address Juniper VF 3000 Signaling controller outside IP address	Remote Site firewall public IP address	H.248 signaling channel between media server and media gateway.
2.	RTP	UDP 2048-65535	Other Remote Site firewall public IP address Juniper VF 3000 Media Controller outside IP address	VF3000 (public IP address) & G700	UDP port range for media traffic to the G700/G250 VoIP cards and VF3000 Media Controller and other site G700/G250 VoIP cards. This port range is configurable in Communication Manager.
3.	H.323 RAS	UDP 1719	Other Remote Site firewall public IP address Juniper VF 3000 Signaling controller outside IP address	Remote Site firewall public IP address	H.323 RAS port used for G700/G250 keep-alive messages and VoIP endpoints.
4.	H.323 Signaling	TCP 1720	Other Remote Site firewall public IP address Juniper VF	Remote Site firewall public IP address	H.323 signaling port used for VoIP endpoints.

Rule	Service	Port(s)	From	To	Notes
			3000 Signaling controller outside IP address		
5.	Translation SYNC	TCP 21874	Main Office Shared Server IP address	Remote Site firewall public IP address	Used in Avaya Communication manager Release 3.x for translation synchronization.
	SNMP Port				
6.	SNMP_READ	UDP 161	Main Office VoIP Monitoring Server[6]	Remote Site S8300 LSPs (Remote Site firewall public IP address)	SNMP Reads from the Avaya Data Center Multi-Site administrators.
	MS SQL Server Port				
7.	ODBC	TCP 139	Main Office IC and IR servers	Remote Site SQL server	IC and IR SQL queries to enterprise legacy databases

Table 3: Avaya Contact Center R3.0 Remote Site Firewall Ports

[6] The Avaya VoIP Monitoring server was used as proxy, routing SNMP and HP OV traffic between the main office and management networks.

5. Verification Steps

The reference configuration depicted in these Application Notes was verified by checking that the main office and remote site firewalls were properly configured.

Step	Description
1.	**Action:** 1. Log in an ACD Agent. 2. Place a voice call from a customer to the VDN configured in Avaya Communication Manager. **Verify:** 1. Customer call terminates at the agent qualified for the call. 2. Two-way talk path exists.
2.	**Action:** 1. Log in an Avaya Interaction Center Agent. 2. Place a voice call from a customer to the VDN configured in Avaya Interaction Center. 3. Send a test email from the customer. 4. Initiate a chat session from the customer. **Verify:** 1. Customer call terminates at the Avaya IC Agent qualified for the call. 2. Customer email is routed to the correct Avaya IC Agent. 3. Customer can communicate with Avaya IC Agent on the chat channel.
3.	**Action:** 1. Place a voice call from a customer that terminates on the Avaya Interactive Response System. **Verify:** 1. The Avaya Interactive Response answers the call. 2. Two-way talk path exists.
4.	**Action:** 1. Place a voice call to a VDN assigned to an Avaya Interactive Response System station, which is mapped to a script that executes SQL database DIP. **Verify:** 1. The Avaya Interactive Response System is able to retrieve the information from the customer site SQL server.

Step	Description
5.	**Action:** 1. From the Avaya CMS Supervisor located at the enterprise site, login to the Avaya Call Management System. **Verify:** 1. The Avaya CMS Supervisor and Avaya Visual Vector can login to the server in the data center. **2.** Avaya CMS Supervisor can access the administration and reporting tools.
6.	**Action:** 1. Log in an Avaya Predictive Dialing Agent. 2. Place an outbound call from the Avaya Predictive Dialing Agent. **Verify:** 1. The call terminates at the customer. 2. Two-way talk path exists. **3.** Avaya Campaign Editor, Campaign Monitor, Campaign Analyst can access the PDS administration and reporting tools.
7.	**Action:** 1. From a remote site, "telnet" to a server located at the main office. 2. From a remote site, "ping" to a server located at the main office. **Verify:** **1.** From a remote site, the user cannot "telnet" to a server located at the main office. **2.** From a remote site, the user cannot "ping" to a server located at the main office.

6. Support

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

7. Conclusion

As illustrated in these Application Notes, Check Point Firewall-1 can be successfully configured to allow an Avaya Contact Center Release 3.0 solution to provide contact center and telephony services.

8. References

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

Related Product documentation for Check Point products are:
[1] *Check Point Firewall-1 and SmartDefense User Guide,*
http://www.checkpoint.com/support/technical/documents/docs_r55.html
[2] *Check Point SmartCenter User Guide,*
http://www.checkpoint.com/support/technical/documents/docs_r55.html

Appendix

Figure 2 shows the Main Office Check Point Firewall-1 Configuration.

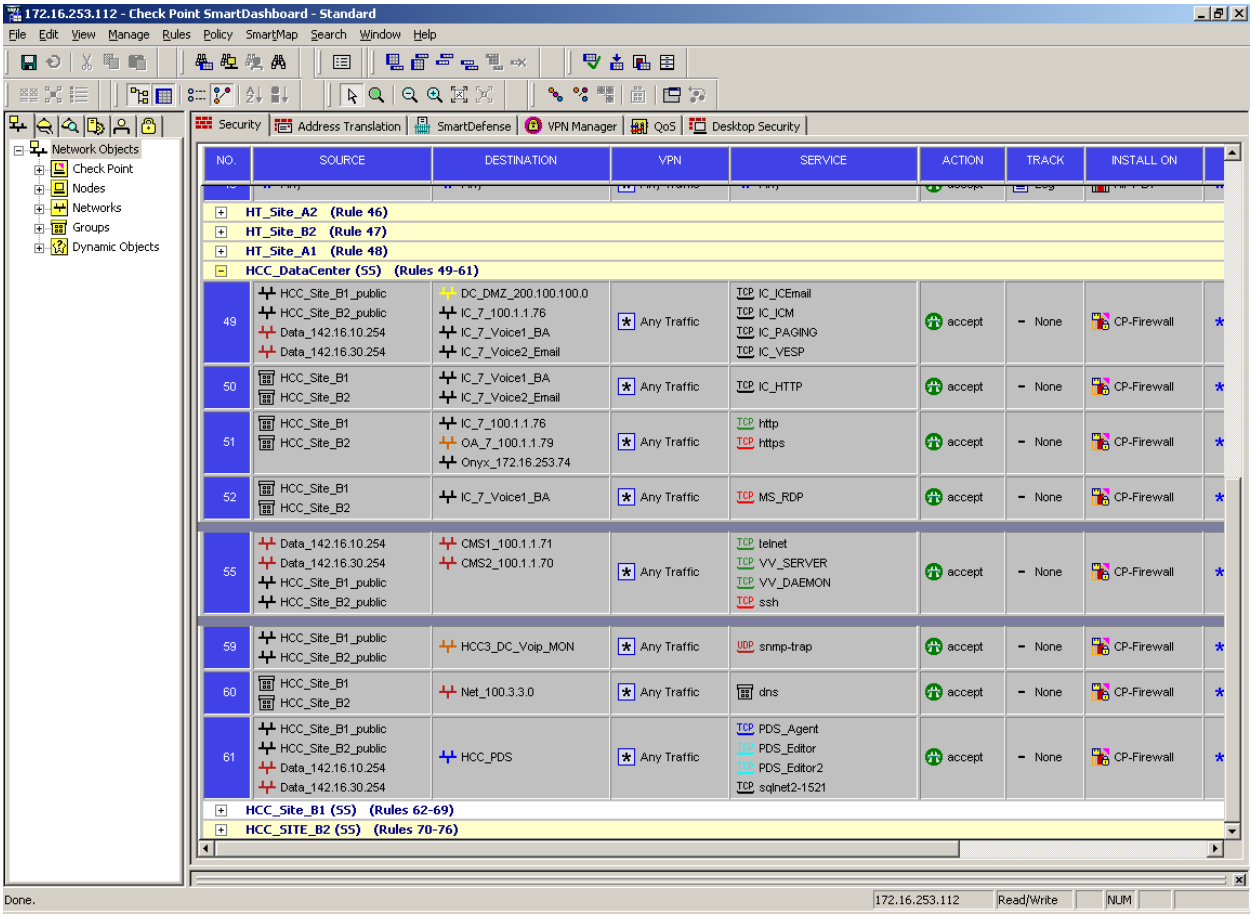

Figure 2: Main Office Check Point Firewall-1

Figure 3 shows the Remote Site 1 Check Point Firewall-1 Configuration.

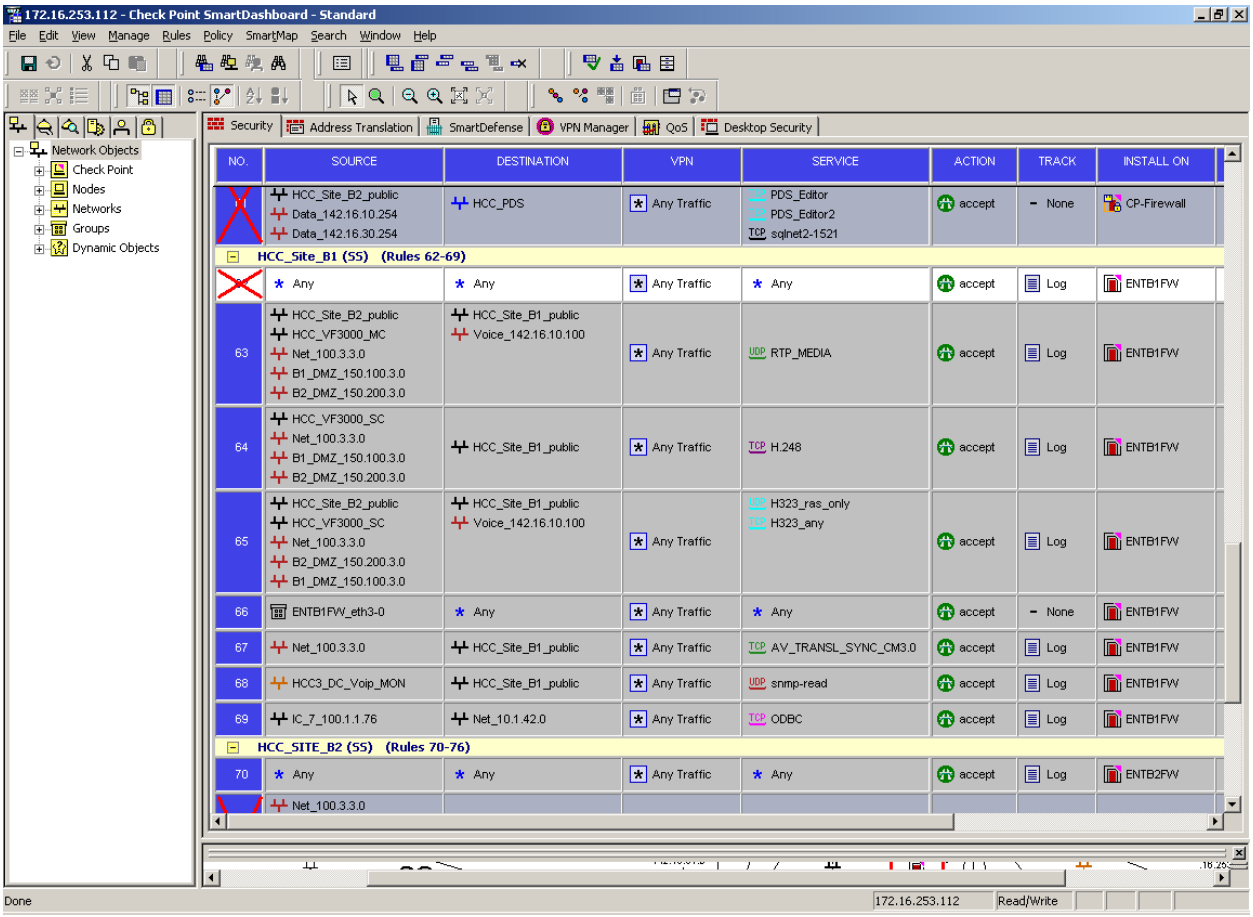

Figure 3: Remote Site 1 Check Point Firewall-1 Policy

Figure 4 shows the Remote Site 2 Check Point Firewall-1 Configuration.

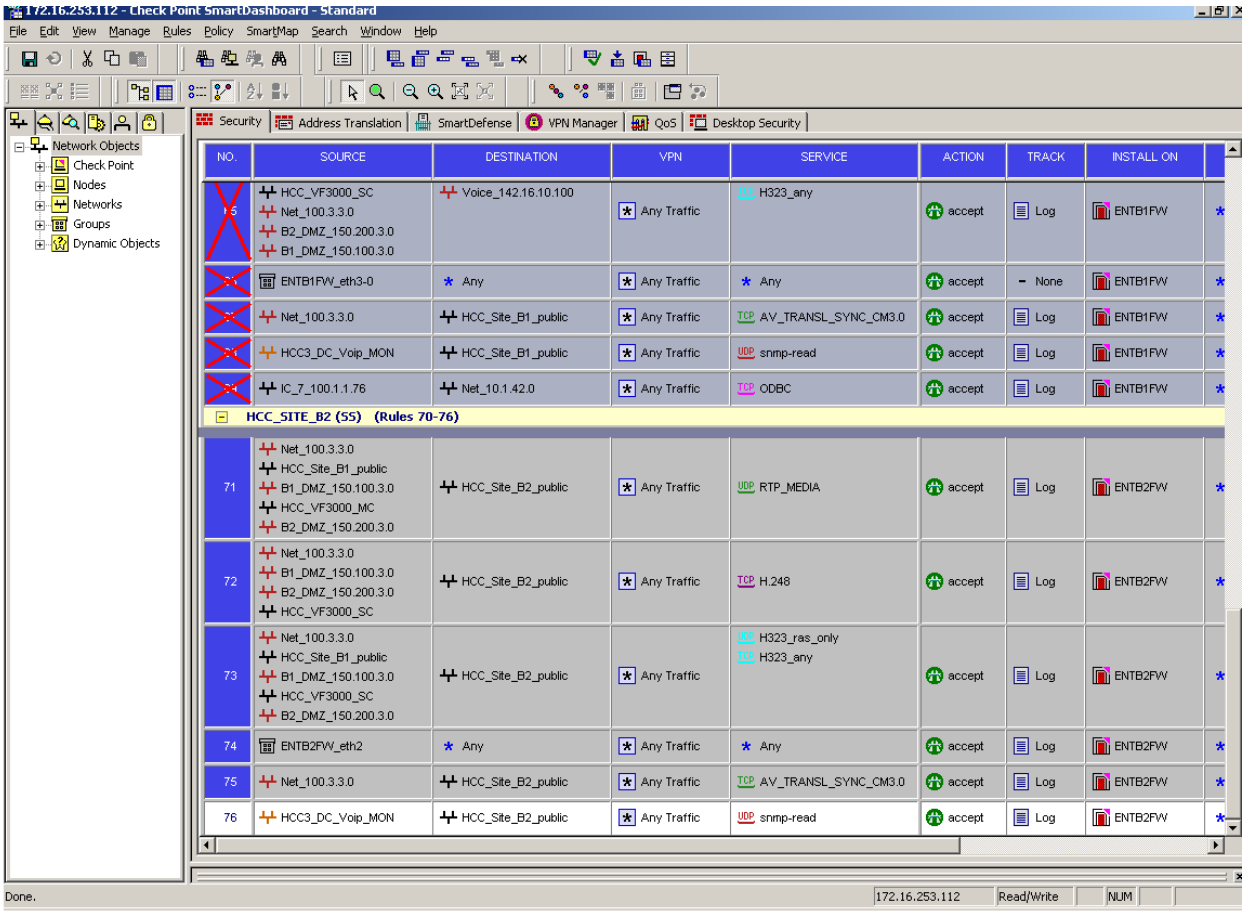

Figure 4: Remote Site 2 Check Point Firewall-1 Policy

Table 4 shows the VoIP protocols that are processed by Juniper VF3000.

Rule	Service	Port(s)	From	To	Notes
	Avaya Communication Manager (CM) Ports				
1.	H.248	TCP 2945	Remote Site G700/G250 (Firewall public IP address)	Juniper VF3000 in Data Center	H.248 signaling channel between media servers and media gateway.
2.	RTP	UDP 2048-65535	Remote Site G700/G250 (Firewall public IP address)	Juniper VF3000 in Data Center	UDP port range for media traffic to the MedPro from the G700 VoIP cards. This port range is configurable in Communication Manager.
3.	RTCP	UDP 5005	Remote Site G700/G250 (Firewall public IP address)	Juniper VF3000 in Data Center	Real-time Transfer Control Protocol to provide metrics on RTP sessions. This port is configurable in Communication Manager.
4.	H.323 RAS	UDP 1719	Remote Site G700/G250 (Firewall public IP address)	Juniper VF3000 in Data Center	H.323 RAS port used for VoIP endpoints and G700 keep-alive messages.
5.	H.323 Signaling	TCP 1720	Remote Site G700/G250 (Firewall public IP address)	Juniper VF3000 in Data Center	H.323 signaling port used for VoIP endpoints.
6.	Translation SYNC	TCP 21874	Remote Site S8300 LSPs (Firewall public IP address)	Juniper VF3000 in Data Center	Used in Avaya Communication manager Release 3.x for translation synchronization.

Table 4: VoIP Protocols that flow through Juniper VF3000

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