

Avaya Solution and Interoperability Test Lab

How to Configure the Juniper NetScreen 5GT to Support Avaya H.323 IP Telephony – Issue 1.0

Abstract

These Application Notes describe how to configure the Juniper NetScreen 5GT to support Avaya H.323 IP Telephony. The sample configuration presented in these Application Notes illustrates how a Juniper NetScreen 5GT firewall can be configured to protect Avaya C-LANs and Media Processor boards using security policies which only allow H.323 signaling, RTP, and H.248 traffic to pass through the firewall.

1. Introduction

These Application Notes describe how to configure the Juniper NetScreen 5GT to support Avaya H.323 IP Telephony. The sample configuration presented in these Application Notes illustrates how a Juniper NetScreen 5GT firewall can be configured to protect Avaya C-LANs and Media Processor boards using security policies which only allow H.323 signaling, RTP, and H.248 traffic to pass through the firewall.

The Juniper NetScreen-5GT appliance integrates multiple security functions - Stateful and Deep Inspection firewall, IPSec VPN (Virtual Private Network), denial of service protection, anti-virus and Web filtering. The focus of these Application Notes is on using the Juniper NetScreen 5GT as an "interior firewall", within the enterprise network, to protect the Avaya C-LAN and Media Processor boards.

The Juniper NetScreen 5GT has five Ethernet interfaces. One of the five Ethernet interfaces was configured for the public or "untrust" security zone. The C-LAN and Media Processors were connected to the other four interfaces which were configured for the private or "trust" security zone.

Each security zone is assigned to its own virtual router, "untrust-vr" for the "untrust" security zone and "trust-vr" for the "trust" security zone. This allows the Juniper NetScreen 5GT device to maintain two separate routing tables and to conceal the routing information in one virtual router from the other. A static route is configured for the trust-vr virtual router to define the untrust-vr as the next hop to allow traffic to pass between the two security zones.

In the configuration tested in these Application Notes:

- The H.323 Application Layer Gateway (ALG) was disabled.
- The Juniper NetScreen 5GT firewall was configured in "route" mode so Network Address Translation (NAT) is not used.
- The security polices defined were limited to traffic flows to and from the Avaya C-LAN and Media Processor boards.

The following items were tested when the Avaya C-LAN and Media Processor boards were placed behind the Juniper NetScreen 5GT firewall:

- Ability of the Avaya IP Telephones to register successfully and place calls
- Ability of the Avaya G350 Media Gateway to register successfully
- Ability of the Avaya Enterprise Survivable Server (ESS) to register successfully and participate in calls
- Ability of the Avaya S8300 Media Server in Local Survivable Processor (LSP) mode to register successfully
- File synchronization to successfully occur between the primary Avaya S8720 Media Servers and the ESS and LSP servers
- Shuffled and non-shuffled H.323 calls
- Failover from the primary Avaya S8720 Media Servers to the ESS and LSP servers and recovery back to the primary Media Servers

SH; Reviewed:	Solution & Interoperability Test Lab Application Notes	2 of 40
SPOC 9/20/2006	© 2006 Avaya Inc. All Rights Reserved.	ns5gt-ipt.doc

Table 2 lists the ports that were opened on the Juniper NetScreen 5GT to support the configuration shown in **Figure 1**. For more information regarding these ports, refer to [1] in Section 7.

From	TCP/UDP Port	То	TCP/UDP Port	Notes
	or Protocol		or Protocol	
Any endpoint	UDP any	Any C-LAN	UDP 1719	For endpoint
				registration (RAS).
Any endpoint	TCP any	Any C-LAN	TCP 1720	For H.225 call
				signaling.
Any endpoint	UDP any	Any MedPro	UDP 2048-3327	To facilitate
			(UDP port range	RTP/RTCP audio
			on the IP	streams between
			Network Region	MedPros and
			form)	endpoints.
G700/G350/G250	TCP any	Any C-LAN	TCP 1039	For encrypted H.248
				signaling between
				the Avaya G700 or
				G350 Media
				Gateway and call
				server.
G700/G350/G250	TCP any	Any C-LAN	TCP 2945	For unencrypted
				H.248 signaling
				between the Avaya
				G700 or G350 Media
				Gateway and call
				server.
Any endpoint	ICMP any	Any C-LAN	ICMP any	For diagnostic
		and Any		purposes.
		MedPro		

Table 1 – TCP/UDP Ports

Figure 1 illustrates the configuration that was used to verify these Application Notes.

Note: The administration of the network infrastructure shown in *Figure 1* is not the focus of these Application Notes and will not be covered. Instead, the focus of these Application Notes is on configuring the Juniper NetScreen 5GT as an "interior firewall".



Figure 1 – Network Configuration Diagram

SH; Reviewed: SPOC 9/20/2006

Solution & Interoperability Test Lab Application Notes © 2006 Avaya Inc. All Rights Reserved.

4 of 40 ns5gt-ipt.doc

Equipment	IP Network/Mask	Description
S8720 Media Server – 1		
Ethernet 0	1.1.1/24	Control Network A
Ethernet 1	192.11.13.6/30	Services Port
Ethernet 2	192.11.13.13/30	Server Duplication Link
Ethernet 3	2.2.2.1/24	Control Network B
Ethernet 4	10.10.1.11/24	Corporate LAN
Active Server	10.10.1.10/24	Active server address for Corporate Network
Gateway	10.10.1.1./24	Gateway address
S8720 Media Server – 2		
Ethernet 0	1.1.1.2/24	Control Network A
Ethernet 1	192.11.13.6/30	Services Port
Ethernet 2	192.11.13.14/30	Server Duplication Link
Ethernet 3	2.2.2.2/24	Control Network B
Ethernet 4	10.10.1.12/24	Corporate LAN
Active Server	10.10.1.10/24	Active server address for Corporate Network
Gateway	10.10.1.1./24	Gateway address
IPSI – A	1.1.1.3/24	IPSI connected to Control Network A
Gateway	1.1.1.254/24	Gateway address
IPSI – B	2.2.2.3/24	IPSI connected to Control Network B
Gateway	2.2.2.254/24	Gateway address
C-LAN – A	192.168.1.15/24	C-LAN in Avaya G650 A carrier
Gateway	192.168.1.1/24	Gateway address
C-LAN – B	192.168.1.16/24	C-LAN in Avaya G650 B carrier
Gateway	192.168.1.1/24	Gateway address
MedPro – A	192.168.1.17/24	Media Processor in Avaya G650 A carrier
Gateway	192.168.1.1/24	Gateway address
MedPro – B	192.168.1.18/24	Media Processor in Avaya G650 B carrier
Gateway	192.168.1.1/24	Gateway address
ESS (S8500)	10.13.1.10/24	Enterprise Survivable Server
LSP (S8300)	10.11.1.10/24	Local Survivable Processor
G350 (GW)	10.11.1.254/24	Avaya G350 Media Gateway
G350 (WAN)	10.12.1.2	Avaya G350 WAN interface
Avaya C364T-PWR	10.10.1.1	Router interface connected to Juniper
-		NetScreen 5GT
Juniper NetScreen 5GT	10.10.1.2	Public interface address
· ·	192.168.1.1	Private interface address

Table 1 lists the IP address assignment for the equipment shown in Figure 1.

Table 2 – IP Address Assignment

2. Equipment and Software Validated

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

Equipment	Version
Avaya S8710 Media Server	3.1.1 Load 628.7 and Service Pack 11640
Avaya G650 Media Gateway	
Avaya TN2312BP IPSI	HW12 FW030
Avaya TN799DP C-LAN	HW01 FW017
Avaya TN2602AP MEDPRO	HW20 FW108
Avaya S8500 Media Server (ESS)	3.1.1 Load 628.7 and Service Pack 11640
Avaya S8300 Media Server (LSP)	3.1.1 Load 628.7 and Service Pack 11640
Avaya C364T-PWR Converged Stackable	4.5.14
Switch	
Avaya G350 Media Gateway	25.23.0
Avaya 4610SW IP Telephone	2.4
Avaya 4621SW IP Telephone	2.4
Avaya 2420 Digital Telephone	
Avaya 6408D+ Digital Telephone	
Avaya 6211 Analog Telephone	
Juniper NetScreen 5GT	5.3.0r2.0

Table 3 – Equipment and Version Validated

3. Juniper NetScreen 5GT Configuration

The following section describes the Juniper NetScreen 5GT configuration to support H.323 registration for Avaya IP telephones and Media Gateways.

3.1. Log in to the Juniper NetScreen 5GT Management Interface



Step	Description			
2.	The screen shown	n in Figure 3 will be displayed	after successful login.	
		0 17	C	
	Juniper-ScreenOS Administ	ration Tools (ns5et) - Microsoft Internet Explorer		
	<u>File Edit View Favorites Too</u>	is <u>H</u> elp		
	🔇 Back 🔹 🕥 - 💌 💈	🏠 🔎 Search 🤺 Favorites 🚱 🔗 🔜		
	Address Address Address	i.html		Go Links »
		Home		ns5gt
		Up time: 0 day 01:02:33, System time: 2006-	06-15 14:28:52 GMT Time Zone -5:00	
	(Juniner		manually	Refresh
	A PRETWORKS		Interface link status:	More
	Juniper-NS5GT	Device Information	Name Zone	Link
	Homo	Hardware Version: 1010(0)	trust Trust untrust Untrust	Up
	Configuration	Serial Number: 0064032005006233		
	+ Network	Host Name: ns5gt		
	+ Screening Policies	Operational Mode: trust-untrust	The most recent alarms:	More
	- MCast Policies		Date/Time Level Description	
	+- VPNs	System Status (Root)	No entry available.	
	+ Reports	Administrator: netscreen	T h	11
	Wizards	Current Logins: I Details	Date/Time Level Description	More
	Logout	Resources Status	2006-06-15 warn Admin user "netscree	en" logged in for
	Toggle Menu		14:28:51 "S"" Web 2006-06-15 Admin user "netscree	en" logged out for
		CPU:	14:28:24 Welli Welli 2006-06-15 Admin user "netscreen" loaged in for	
		Memory:	14:26:07 warn Web	un logged in for
		Socions:	14:09:51 Warn Web	en" logged in for
			2006-06-15 Admin user "netscree 13:52:43 warn Web	en" logged in for
		Policies:	10102110 00000	
		Start from here		
	ど Done			🔮 Internet
		Figure 3 – Juniper NetS	creen 5GT Home Page	
		8Fer 1.00%	· · · · · · · · · · · · · · · · · · ·	

3.2. Globally Disable the H.323 Application Layer Gateway

The required ports will be defined using the Juniper NetScreen 5GT security policies instead of using the H.323 Application Layer Gateway feature.

From the naviga	tion menu on the left, se	elect Configuration \rightarrow Advanced \rightarrow ALG \rightarrow	
Configure.			
Uncheck the H.323 check box to globally disable the H.323 Application Layer Gatewa			
shown in Figure	e 4. Click Apply.		
Juniper-ScreenOS Admini	stration Tools (ns5gt) - Microsoft Internet I	xplorer 🔳 🗖 🔀	
Eile Edit View Favorites I	ools <u>H</u> elp	X	
G Back 🝷 🐑 🖌 📓	🖞 🏠 🔎 Search 🤺 Favorites 🤣 🖉	3- 😓 🖂 🔔 🦓	
Address 🗃 http://10.10.1.2/nswe	bui.html Configuration > 0.dvanced > 01 C	Sector Se	
		uanăr <mark>t</mark>	
Juniper-NS5GT	Application Layer Gateway		
Home	Microsoft RPC		
 Configuration 	Sun RPC		
- Date/Time	RTSP		
Admin	SQL		
Auth Infranet Auth	MCCD		
- Port Mode			
 Advanced Troffic Shoping 	Media Inactivity Timeout	120 (10, 0550) cocorda	
E- ALG	Transaction Timpout	20 (5.50) seconds	
- Configure - SIP	Connections Limit per	Sum (S~50) seconds	
Flow	Gateway	200 (10~1000) connections per second	
+ Screening	🗌 Message Limit	1000 (50~5000) messages per second	
 Policies MCast Policies 	Allow Unknown Message		
+ VPNs + Objects		C Route	
+ Reports	H323		
+ Help	🗌 Н323		
- Logout	Gate Source Port Any		
Toggle Menu	Incoming Table Timeout	3600 (10~65535) seconds	
	Allow Unknown Message	NAT	
		L Route	
	Apply Cancel		
8.			
Cone Cone		S Internet	

3.3. Configure Security Zones

The steps in this section assigns virtual router name "trust-vr" to the "trust" or private security zone and "untrust-vr" to the "untrust" or public security zone.



Step	Description		
2.	Click Edit on the	row corresponding to "Trust" in Figure 5 to view the properties	for the
	Trust security zor	ne. Select trust-vr from the drop-down list for the Virtual Rou	ter Name as
	shown in Figure (6. Accept the other default settings. Click OK .	
	Juniper-ScreenOS Administra	ation Tools (ns5gt) - Microsoft Internet Explorer	
	Elle Edit View Favorites Tools		
	Back • S • S •	V Search X Pavorites 🚱 🔯 V 🎲 🖾 🛄 🐼	Ca linka »
		nom Network > Zones > Edit ns5g	t ?
		Back To :	<u>Zone List</u>
	Juniper°	Properties: Basic	
		Zone Name Trust	
	Juniper-WSSG1	Virtual Router Name Trust-vr Y	
	 Home ➡ Configuration 		
	Network Binding	Block Intra-Zone Traffic 🔽	
	DNS Zones	If TCP non SYN, send RESET back V	
	 Interfaces DHCP 	Asymmetric VPN	
	- PPPoE		
	Untrust Failover	OK Cancel	
	- Policies		
	+ VPNs		
	+ Objects + Reports		
	▪ Wizards ▪ Help		
	- Logout		
	Toggle Menu		
	Cone	🥥 Internet	.::
		Figure 6 – Trust Zone Properties	

Step	Description		
3.	Click Edit on the	row corresponding to "Untrust" in Figure 5 to view the	e properties for the
	Untrust security	zone. Select untrust-vr from the drop-down list for the	e Virtual Router
	Name as shown in	n Figure 7. Accept the other default settings. Click Ol	X.
	Juniper-ScreenOS Administr	ation Tools (ns5gt) - Microsoft Internet Explorer	
	Eile Edit View Favorites Tool		
	G Back • G • A Globach	V Search X Pavorites W V Search X Pavorites	
	Aguress entp://10.10.1.2/hswebu	nom Network > Zones > Edit	ns5gt ?
		Properties: Basic	<u>Back To Zone List</u>
	NETWORKS		
	Juniper-NS5GT	Zone Name Untrust	
	- Home	Virtual Router Name untrust-vr 💌	
	 Configuration Network 	Block Intra-Zone Traffic 🕑	
	Binding DNS	If TCP non SYN, send RESET back 🕑	
	Zones Interfaces	TCP/IP Reassembly for ALG	
	– DHCP – PPP₀E	Asymmetric VPN	
		OK Cancel	
	+ Screening Policies		
	- MCast Policies		
	+ Objects		
	+ Reports + Wizards		
	telp └─ Logout		
	Toggle Menu		
	E Done		🔮 Internet
		Figure 7 – Trust Zone Properties	

3.4. Configuring Interfaces

The steps in this section assign an IP address to the interfaces for the "trust" and "untrust" security zone. Each interface will operate in "route" mode and function as a separate router. A static route is configured for the trust-vr virtual router to define the untrust-vr as the next hop to allow traffic to pass between the "trust" and "untrust" security zones.

Juniper-ScreenOS A	dministration Tools (ns5	gt) - Microsoft Internet Exp	lorer						
File Edit View Favori	es Iools Help	🔶 Favorites 👩 📿		.88					
Address 🕘 http://10.10.1.	2/nswebui.html							💌 ラ Go	Links
	Network > In	terfaces (List)						ns5gt	?
	List 20 💙 p	er page							
Junipe	List ALL(4)	✓ Interfaces					New	Tunnel IF	*
			_	_			-		
Juniper-NS5GT	Name	IP/Netmask	Zone	Туре	Link	PPPoE	Co	onfigure	
Home	trust	192,168,1,1/24	Trust	Laver3	Uuwn	-	Edit		-
 Configuration Network 	untrust	10.10.1.2/24	Untrust	Laver3	Up	-	Edit		
- Binding	vlan1	0.0.0/0	VLAN	Layer3	Down	-	Edit		_
MCast Policies © Objects © Reports © Wizards © Help — Logout Toggie Wenu									



Step	Description					
3.	Click Edit on the	row corresponding to Untrust in Figure 8 to view the interface				
	configuration for the Untrust security zone. Enter the following information on the screen					
	shown in Figure 10 :					
	Zone Nam	ne: Select Untrust from the drop-down list.				
	IP Addres	s / Netmask: Enter the IP address for the Untrust interface.				
	• Interface	Mode: Select Route Mode				
	Service O	ntions : Select the desired options for this interface				
	s bervice o	prons. Select the desired options for this interface.				
	Note: The Manas	Peable and Telnet checkbox was enabled for the "untrust" interface for ease				
	of adminis	tration of the Juniper NetScreen 5GT from PCs located in the "untrust"				
	security zo	ne. These options do not have to be enabled.				
	,					
	Click OK .					
	Juniper-ScreenOS Administ	ration Tools (ns5gt) - Microsoft Internet Explorer				
	<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> oo	ils Help				
	🌀 Back 🝷 🕥 🕤 🗾 🛃	🏠 🔎 Search 👷 Favorites 🤣 🎯 - 🌺 🥅 🛄 🦓				
	Address 🕘 http://10.10.1.2/nswebu	i.html				
		Network > Interfaces > Edit ns5gt ?				
		Preparties: Pasie MIP, DIP, VIP, ICMP, Menitor				
		Propercies: Basic MIP DIP VIP IGMP Monitor				
	Juniper-NS5GT	Interface Name untrust (mac 0010.dba4.9d31)				
	Home	Zone Name Untrust				
	 ■ Configuration 	O Obtain IP using DHCP 🔲 Automatic update DHCP server parameters				
	Binding	O Obtain IP using PPPoE None V Create new pppoe setting				
		⊙ Static IP				
	- Interfaces	IP Address / Netmask 10.10.1.2 / 24 ✓ Manageable				
	- PPPoE	(mac 0010.dba4.9d31)				
	Untrust Failover	Interface Mode ONAT OROUTE				
		Block Intra-Subnet Traffic 🗌				
	— MCast Policies +⊢ VPNs	Service Options				
		Management Services V Web UI V Telnet V SSH				
	• Wizards	Other Services V Ping Path MTU(IPv4) Ident-reset				
	t- Help Logout	Maximum Transfer Unit				
	Toggle Menu	(MTU) Admin MTU 0 Bytes (Operating MTU: 1500; Default MTU: 1500)				
		DNS Proxy 🗌				
		WebAuth IP 0.0.0.0 SSL Only				
		Addiess				
		Traffic Bandwidth Egress Maximum Bandwidth O Kbps				
		Ingress Maximum Bandwidth 0 Kbps				
		OK Apply Cancel				
		🧭 Internet				
		Figure 10 – Untrust Network Interface				
		-				

Solution & Interoperability Test Lab Application Notes © 2006 Avaya Inc. All Rights Reserved.

Step	Description		
4.	Configure a static	route for the trust-vr virtual router to define the untrust-vr interface as the	e
	next hop to allow	traffic to pass between the "trust" and "untrust" security zones. From the	e
	navigation menu	on the left, select Network \rightarrow Routing \rightarrow Destination . Click New to crea	ite a
	static route for the	e Trust virtual router as shown in Figure 11. Enter the Destination Netw	'ork
	IP Address (e.g.,	10.0.0.0) and the Netmask (e.g., 8) for the "untrust" zone. Select Gatew	vay
	and select the un	rust interface from the drop-down list. Enter the Gateway IP address (e	e.g.,
	10.10.1.1) of the	next hop router and accept the other default settings. In the configuration	
	shown in Figure	1, the next hop router is the Avaya C364T-PWR connected directly to the	;
	Juniper NetScree	n 5GT. Click OK .	
	Juniper-ScreenOS Administ	ration Tools (ns5gt) - Microsoft Internet Explorer	
	Address Abtrol/10 10 1 2 Jonumbr	ibtm	
	ncp///10.10.1.2/ISWED	Network > Routing > Routing Entries > Configuration ns5gt	
	hurings NEECT	Virtual Router Name, trust-vr	
		10.0.0 /	
	 Home ➡ Configuration 	Network IP Address / Netmask	
	Network Binding		
		O Next Hop Virtual Router Name untrust-vr 💌	
	- Interfaces		
	- PPPoE	Gateway IP Address 10 10 1 1	
	 Routing Destination 	Preference 20	
	 Source Source Interface 	Metric 1	
	 MCast Routing Virtual Routers 	Permanent	
	Untrust Failover	Tag 0	
	– Policies		
	 MCast Policies VPNs 	OK Cancel	
	+ Objects + Reports		
	Wizards Help		
	Logout		
	Toggle Menu		
	Done	💼 Internet	
		Figure 11 – Static Route for trust-vr	

3.5. Create Address Book Entries

Address book entries are used to define resources referenced by security polices. Network addresses are used to specify the subnets of the Main and Branch Office. Individual IP addresses are specified for the Avaya ESS, C-LANs and Media Processors.

Step	Description	
1.	From the naviga page is displayed book entry for the following inform • Address • IP Address • Zone: Sel	tion menu on the left, select Objects → Addresses → List. The address list d. Click the New button on top right corner of page to create a new address he range of IP addresses used by equipment at the Main Office. Enter the mation on the screen shown in Figure 12 : Name: Avaya Main Office ess/Netmask : IP address and subnet mask of the Main Office network lect Untrust from the drop down list
	Click OK.	
	Juniper-ScreenOS Admini	stration Tools (ns5gt) - Microsoft Internet Explorer
	G Back - C - K	Search 🍸 Favorites 🚱 🖾 · 🎯 🔜 🔜 🦓
	Address E http://10.10.1.2/nswe	bui.html Objects > Addresses > Configuration ns5gt
	Juniper-NS5GT	Address Name Avaya Main Office
	Home	Comment
	 Configuration Network 	IP Address/Domain Name
	+ Screening Policies	IP Address/Netmask 10.10.1.0 / 24
	- MCast Policies	O Domain Name
	- Objects	Zone Untrust 🗸
	List	
	Summary	OK Cancel
	Services Users	
	 IP Pools Schedules 	
	 Group Expressions Certificates 	
	+ Reports • Wizards	
	∓-Help Logout	
	Toggie Menu	
	roggie menu	
	E Remove	🎯 Internet 🤢
		Figure 12 – Avava Main Office Address Book Entry

Step	Description				
2.	From the navigat	ion menu on the left, select Ob	ojects \rightarrow Addresses -	→ List. The ad	dress list
	page is displayed	l. Click the New button on top	right corner of page to	o create a new a	ıddress
	book entry. Ente	er the following information on	the screen shown in l	Figure 13:	
	Address N	Name: Avaya Branch Office			
	IP Addres	ss/Netmask: IP address and su	bnet mask of the Bran	hch Office netw	ork
	• Zone: Sel	ect Untrust from the drop dow	vn list		
	Click OK .				
	7			F	
	Eile Edit View Favorites To	tration loois (ns5gt) - Microsoft Internet Explorer ols <u>H</u> elp		Le contra de la co	
	😋 Back 🔹 🕥 - 💌 💋	🏠 🔎 Search 🤺 Favorites 🚱 🔗 🍓 🥽	3		
	Address 🗃 http://10.10.1.2/nsweb	ui.html		💌 🔁 Go	Links »
		Objects > Addresses > Configuration		ns5gt	2
	Juniper-NS5GT	Address Name	Avaya Branch Office		
	- Home	Comment			
	 Configuration Network 	IP Address/Domain Name			
	■ Screening Policies	 IP Address/Netmask 	10.11.1.0	/ 24	
	 MCast Policies VPNs 	O Domain Name]	
	 Objects Addresses 	Zone	Untrust		
	List Groups				
	- Summary		OK Cancel		
	Services Users				
	- IP Pools - Schedules				
	 Group Expressions Certificates 				
	Attacks F- Reports				
	+-Wizards +-Help				
	– Logout				
	Toggle Menu				
	Remove			🎯 Internet	
		Figure 13 – Avava Branch	Office Address Book	x Entry	
		gure ieivuju Drahen			

Step	Description		
3.	From the navigat	tion menu on the left, select Objects \rightarrow Addresses \rightarrow List. The add	lress list
	page is displayed	d. Click the New button on top right corner of page to create a new ad	ddress
	book entry. Ente	er the following information on the screen shown in Figure 14 :	
	Address I	Name: Avaya ESS	
	IP Addre	ss/Netmask: IP address and subnet mask of the ESS	
	• Zone: Sel	lect Untrust from the drop down list	
	Click OK.		
	Tuniner CoreanOC Administr	ntion Table (asEat) Minuscoft Tatourat Eurolaum	
	Eile Edit View Favorites	Iools Help	
	🛛 😋 Back 🔹 🕥 👻 🛃	🕽 🏠 🔎 Search 🤺 Favorites 🚱 🔗 - 😓 🔜 🛄 🎇 🦓	
	Address Address // 10.10.1.2/nswe	ebui.html 🔽 🔁 Go 🗍 Link	s **
		Objects > Addresses > Configuration ns5gt ?	
	Juniper-NS5GT	Address Name Avaya ESS	
	- Home	Comment	
	Configuration Network	IP Address/Domain Name	
	Screening Policies	© IP Address/Netmask 10.13.1.10 / 32	
	- MCast Policies	C Domain Name	
	Objects Addresses	Zone Untrust	
	- List		
	Summary	OK Cancel	
	Services Users		
	 IP Pools Schedules 		
	 Group Expressions Certificates 		
	Attacks Reports		
	• Wizards		
	Logout		
	Toggle Menu		
	Done	i internet	
		Figure 14 – Avaya ESS Address Book Entry	
L	l		

Step	Description		
4.	From the navigat	tion menu on the left, select Objects \rightarrow Addresses \rightarrow List. The addre	ss list
	page is displayed	I. Click the New button on top right corner of page to create a new add	ress
	book entry. Ente	er the following information on the screen shown in Figure 15 :	
	Address N	Name: Avaya CLAN – 1A02	
	IP Addres	ss/Netmask: IP address and subnet mask of the C-LAN in slot 1A02	
	• Zone: Sele	ect Trust from the drop down list	
	Click OK.		
	Iuniner-ScreenOS Administra	ation Tools (ns5nt) - Microsoft Internet Evoluter	त
	<u>File Edit View Favorites</u>	Iools Help	
	🛛 🌀 Back 👻 🕥 👻 🛃) 😚 🔎 Search 🤺 Favorites 🚱 🔗 - 😓 🔜 🛄 🇱 🦓	
	Address Address //10.10.1.2/nswe	ebui.html	
		Objects > Addresses > Configuration n55gt ?	
	NETWORKS		
	Juniper-NS5GT	Address Name Avaya CLAN - 1A02	
	Home	Comment	
	Configuration Network	IP Address/Domain Name	
	Screening Policies	• IP Address/Netmask 192.168.1.15 / 32	
	MCast Policies	O Domain Name	
	 Objects Addresses 	Zone Trust	
	- List		
	Summary	OK Cancel	
	Users		
	- Schedules		
	 Group Expressions Certificates 		
	Attacks Reports		
	Logout		
	Toggle Menu		
	Done	I Internet	
		Figure 15 – Avaya CLAN-1A02 Address Book Entry	
L	L		

Step	Description	
5.	From the naviga	tion menu on the left, select Objects \rightarrow Addresses \rightarrow List. The address list
	page is displayed	d. Click the New button on top right corner of page to create a new address
	book entry. Ent	er the following information on the screen shown in Figure 16:
	Address	Name: Avaya CLAN – 1B02
	IP Addre	ess/Netmask: IP address and subnet mask of the C-LAN in slot 1B02
	• Zone: Sel	lect Trust from the drop down list
	Click OK .	
	🏄 Juniper-Screen05 Administra	ation Tools (ns5gt) - Microsoft Internet Explorer
	Eile Edit View Favorites	
	Address @ http://10.10.1.2/nswe	ebui.html
		Objects > Addresses > Configuration ns5gt ?
	Juniper-NS5GT	Address Name Avaya CLAN - 1802
	Home	Comment
	Configuration Network	IP Address/Domain Name
	+ Screening - Policies	C Domain Name
	+ VPNs	
	- Addresses	Zone Trust
	- Groups	OK Cancel
	+ Services	
	- IP Pools	
	- Group Expressions	
	+ Attacks	
	+ Wizards + Help	
	Logout	
	Toggle Menu	
		Figure 16 – Avaya CLAN-1A02 Address Book Entry



Step	Description	
7.	From the navigation page is displayed. C book entry. Enter t • Address Nav • IP Address/ 1B03 • Zone: Select	n menu on the left, select Objects → Addresses → List . The address list Click the New button on top right corner of page to create a new address the following information on the screen shown in Figure 18 : me: Avaya MEDPRO – 1B03 Netmask: IP address and subnet mask of the MEDPRO located in slot Trust from the drop down list
	Click OK.	bols (ns5gt) - Microsoft Internet Explorer
		Address Name Avaya MEDPRO - 1803 Comment P Address/Domain Name Zone Trust OK Cancel
	Fi	gure 18 – Avaya MEDPRO – 1B03 Address Book Entry

3.6. Configuring Custom Service

Custom services allow for the specification of protocols that are not pre-defined on the NetScreen. Three custom services are defined in this section. The first custom service is used to support Avaya H.323 signaling. The second custom service is used to support RTP traffic. The third custom service is used to support H.248 signaling between the C-LAN and Media Gateway.



Solution & Interoperability Test Lab Application Notes © 2006 Avaya Inc. All Rights Reserved.

p	Description								
•	From the navigat	tion 1	nenu on the left, select Object	$s \rightarrow S \overline{s}$	ervice	$s \rightarrow \overline{c}$	Custor	n . T	he Custo
	Services page is	displ	ayed. Click the New button or	1 top ri	ght co	orner (of page	e to c	create a n
	custom service.	Ente	r the following information in	the scr	een sh	iown i	n Fig	ure 2	20.
			C				U		
	Service N	ame	: Avava RTP						
	Service T	imed	out: Use protocol default. Thi	is is the	e defa	ult set	ting.		
			ľ				0		
	The UDP ports s	pecif	fied are described in Table 1.	The D	estina	tion P	ort ra	nge	correspor
	the UDP port ran	ige s	pecified on the IP Network Reg	gion fo	orm in	Figur	e 30.	Clic	k OK.
	1	0				0			
	Juniper-ScreenOS Adminis	tration 1	Tools (ns5gt) - Microsoft Internet Explorer						
	File Edit View Favorites To	ools <u>H</u> elp							
	🌀 Back 🔹 🐑 🔹 🗾 🧟		🔎 Search 🤺 Favorites 🔣 😥 🌽 📕 📙 👋	\$					
	Address 🗃 http://10.10.1.2/nsweb	oui.html Obie	cts > Services > Custom ≥ Edit					✓	→Go Links »
									.a. 🖬
	NETWORKS								
	Juniper-NS5GT								
	- Home		Service Name Avaya_RTP						
	 Configuration Network 		Service Timeout Use protocol Never	default					
	Screening Delicion		O Custom	(minutes)				
	– MCast Policies	No.	Transport protocol	Sourc	ce Port	Destina	tion Port	IC	MP
	+ VPNs = Objects			Low	High	Low	High	Туре	Code
	 Addresses Services 	1	O none O TCP O UDP O ICMP O other		65535	2048	3327		
	- Predefined	2							
	- Sun RPC	4							
	- MS RPC - Groups	5							
	Users IP Pools	6	⊙ none ○ TCP ○ UDP ○ ICMP ○ other						
	- Schedules	7	⊙ none ○ TCP ○ UDP ○ ICMP ○ other						
	 Group Expressions Certificates 	8	⊙ none ○ TCP ○ UDP ○ ICMP ○ other						
	Attacks Reports								
	• Wizards		OK Can	cel					
	Logout								
	Toggle Menu								

Step	Description									
3.	From the navigati	ion mer	nu on the left, so	elect Objects	\rightarrow Se	ervice	$s \rightarrow 0$	Custon	n. Th	ne Custom
	Services page is c	lisplaye	ed. Click the N	ew button on	top ri	ght co	orner o	of page	e to c	reate a new
	custom service. I	Enter th	e following inf	ormation in th	ne scr	een sh	iown i	in Fig	are 2	1.
			-							
	Service Na	ame: A	vaya_H248							
	Service Ti	imeout:	Use protocol	default. This	is the	e defa	ult set	ting.		
			_					-		
	The TCP ports sp	ecified	are described in	n Table 1 . C	lick C)K.				
	Juniper-ScreenOS Administ	ration Tools (ns5gt) - Microsoft Internet	xplorer						
		Jis Tielh	and the Environment of the							~~
		2 hbarl		» 😪 🖂 📙 🦚						Co. Linke »
		Objects >	Services > Custom > Edit						ns5g	t ?
	A PRETWORKS									
	Juniper-NS5GT									
	Home		Service Nan	1e Avaya_H248						
	+ Configuration + Network		Service rimeo	 Use protocol de Never 	efault					
	Screening Policies			O Custom	(minutes)				
	– MCast Policies	No.	Transnort nr	atocol	Sourc	e Port	Destina	ition Port	ICM	1P
	+ VPNs − Objects	1			Low	High	Low	High	Туре	Code
	 Addresses Services 	1 O r			0	65535	2045	2045		
	- Predefined	2 O r				03335	2943	2943		
	- Sun RPC	4 () r								
	- MS RPC - Groups	5 📀 r	ione O TCP O UDP O	ICMP 🔘 other				1		
	Users IP Pools	6 💽 r	ione O TCP O UDP O	ICMP 🔿 other						
	- Schedules	7 💿 r	one 🔿 TCP 🔿 UDP 🔿	ICMP 🔾 other			Í			
	- Certificates	8 💿 r	ione O TCP O UDP O	ICMP 🔿 other						
	Attacks Reports									
	Wizards Help			OK Cance						
	Logout									
	Toggle Menu									
	ど Done								🥝 Internet	
			Figure 21 – A	Avaya H248 (Custo	m Se	rvice			
L										

3.7. Creating Security Policies

Two security policies must be created on the Juniper NetScreen 5GT to allow traffic to flow between the "trust" and the "untrust" zones. The security policy created in Section 3.7.1 allows all traffic to flow from the "trust" zone to the "untrust" zone. The security policy created in Section 3.7.2 only allows ICMP and traffic defined by the custom services in Section 3.6 to flow from the "untrust" zone.

3.7.1. Trust to Untrust Policy

Step	Description
1.	From the navigation menu on the left, select Policies . On the top of the Policies page, select
	Trust on the From drop-down list and Untrust on the To drop-down list. Click the New
	button on the top right corner of the page to create a new security policy. Enter the following
	information in the screen shown in Figure 22:
	Name: Avaya Private-to-Public
	• Source Address: See Step 2 below.
	• Destination Address : See Step 3 below.
	• Service: Select ANY from the drop-down list.
	• Application: Select None from the the drop-down list.
	• Action: Select Permit from the drop-down list.
	• Logging: Enable logging by checking the box to see events in the Juniper NetScreen
	5GT log.

Step	Description	stration Tools (m52g) - Microsoft Internet Explorer cols telp Cols telp Policies (From Trust To Untrust) Name (optional) Avaya Private-to-Public Source Address New Address Address Book Entry (Multiple) Destination Address Address Book Entry (Multiple) Multiple Service ANY WEB Filtering Application None WEB Filtering Antivirus Profile None Tunnel VPN None Core Modify matching bidirectional VPN policy Logging ✓ at Session Beginning OK Cancel Advanced	GO LINKS »
	الله المراجع ال المراجع المراجع المراجع المراجع المراجع	Figure 22 Trust to Untrust Policy	

Step	Description
2.	From the Policies (Trust to Untrust) screen in Figure 22, select Address Book Entry for the
	Source Address and click the Multiple button. Select the Address Book entries created for
	the C-LAN and MEDPRO boards from the Available Members window and move these over
	to the Selected Members window as shown in Figure 23 . Click OK .
	🗿 http://10.10.1.2 - Selection of Multiple Address Entries - Microsoft Internet Exp 🔲 🗖 🔀
	Source Address Entries (Trust)
	Negate the Following 📃
	C- Selected Members -> Avaya CLAN - 1A02 Avaya CLAN - 1B02 Avaya MEDPRO - 1A03 Avaya MEDPRO - 1B03 < C- Available Members -> 192.168.1.0 Avaya CLAN - 1A02 Avaya CLAN - 1B02 Avaya MEDPRO - 1B03 < Avaya CLAN - 1B02 Avaya MEDPRO - 1B03
	OK Cancel
	🛎 Done 🧶 Internet 🛒
	Figure 23 – Source Address Entries (Trust)

Step	Description
3.	From the Policies (Trust to Untrust) screen in Figure 22, select Address Book Entry for the
	Destination Address and click the Multiple button. Select the Address Book entries created
	for the Branch Office, ESS, and Main Office from the Available Members window and move
	these over to the Selected Members window as shown in Figure 24. Click OK to continue.
	Click OK to save the Trust to Untrust policy.
	🗿 http://10.10.1.2 - Selection of Multiple Address Entries - Microsoft Internet Exp 🗔 🗖 🔀
	Destination Address Entries (Untrust)
	Negate the Following 📃
	C- Selected Members -> Avaya Branch Office Avaya ESS Avaya Main Office < Available Members -> Avaya Branch Office Avaya ESS Avaya Main Office >> >>
	OK Cancel
	🙆 Done 🔹 Internet
	Figure 24 – Destination Address Entries (Untrust)

3.7.2. Untrust to Trust Policy

Step	Description							
1.	From the navigation menu on the left, select Policies . On the top of the Policies page, select							
	Untrust on the From drop-down list and Trust on the To drop-down list. Click the New							
	button on the top right corner of the page to create a new security policy. Enter the following							
	information in the screen shown in Figure 25:							
	Name: Avaya Public-to-Private							
	• Source Address: See Step 2 below.							
	• Destination Address : See Step 3 below.							
	• Service: See Step 4 below.							
	• Application: Select None from the drop-down list.							
	• Action: Select Permit from the drop-down list.							
	• Logging : Enable logging by checking the box to see events in the NetScreen log.							
	Click OK .							
	🗿 Juniper-ScreenOS Administration Tools (ns5gt) - Microsoft Internet Explorer							
	Ele Edit View Favorites Tools Help							
	S Back - S - X Search T Favorites 🚱 S - S - S - S - S - S - S - S - S - S							
	Address 🗿 http://10.10.1.2/nswebui.html 🗸 🌛 Go Links 🎽 Policies (From Untrust To Trust) ns5at 2							
	M Juniper*							
	Juniper-MS5GT Name (optional) Avaya Public-to-Private							
	Home Source Address /							
	Address Book Entry (Multiple)							
	Policies Destination Address Book Entry (Multiple) V Multiple							
	MCast Policies VPNs Service (Multiple) Multiple							
	Objects Application None							
	Wizards Help							
	Logout WEB Filtenng							
	Toggle Monu							
	Modify matching bidirectional VPN policy							
	L2TP None 💌							
	Logging 🗹 at Session Beginning 🗌							
	Position at Top 🗌							
	Remove							
	Figure 25 – 1 rust to Untrust Policy							

Step	Description											
2.	From the Policies (Untrust to Trust) screen in Figure 25, select Address Book Entry for the											
	Source Address and click the Multiple button. Select the Address Book entries created for											
	the Branch Office, ESS, and Main Office from the Available Members window and move											
	these over to the Selected Members window as shown in Figure 26. Click OK.											
	🗿 http://10.10.1.2 - Selection of Multiple Address Entries - Microsoft Internet Exp 🔳 🗖 🗙											
	Source Address Entries (Untrust)											
	Negate the Following 📃											
	C- Selected Members -> Avaya Branch Office Avaya ESS Avaya Main Office < Available Members -> Avaya Branch Office Avaya ESS Avaya Main Office >> >>											
	OK Cancel											
	🙆 Done 🔮 Internet											
	Figure 26 – Source Address Entries (Untrust)											

Step	Description											
3.	From the Policies (Untrust to Trust) screen in Figure 25, select Address Book Entry for the											
	Destination Address and click the Multiple button. Select the Address Book entries created											
	for the C-LAN and MEDPRO boards from the Available Members window and move these											
	over to the Selected Members window as shown in Figure 27 . Click OK .											
	🖆 http://10.10.1.2 - Selection of Multiple Address Entries - Microsoft Internet Exp 🖃 🗖 🔀											
	Destination Address Entries (Trust)											
	Negate the Following 📃											
	 Selected Members -> Avaya CLAN - 1A02 Avaya CLAN - 1B02 Avaya CLAN - 1B02 Avaya MEDPRO - 1A03 											
	Avaya MEDPRO - 1803 <											
	OK Cancel											
	🕘 Done 🔹 🔮 Internet											
	Figure 27 – Source Address Entries (Untrust)											

Step	Description										
4.	From the Policies (Untrust to Trust) screen in Figure 25, click the Multiple button for Ser Select the Custom Services created in Section 3.6 from the Available Members window a move these over to the Selected Members window as shown in Figure 28. Click OK to continue. Click OK to save the Untrust to Trust policy.										
	Service Entries										
	K- Selected Members → Avaya_H323 Avaya_RTP Avaya_H248 ICMP-ANY < K- Available Members → MGCP MS-AD MS-AD MS-EXCHANGE MS-IS VOIP Avaya_H323 Avaya_RTP Avaya_H248 GTP AOL BGP OK Cancel										
	🖉 Done 🥥 Internet 🛒										
	Figure 28 – Service Entries										

3.7.3. Summary of Security Policies to Support Avaya IP Telephony

From the Juniper NetScreen 5GT Home Page, click **Policies** to display the two security policies created in Sections 3.7.1 and 3.7.2.

🗿 Juniper-ScreenOS Administration Tools (ns5gt) - Microsoft Internet Explorer													
Elle Edit Yiew Favorites Iools Help													
🔇 Back 🔹 💿 🕤 📓 🐔 🔎 Search 🤺 Favorites 🤣 🎯 - 🌺 🔜 🛄 🦓													
Address 🗃 http://10.10.1.2/nswebui.html													
Policies (From All zones To All zones) ns5gt ?													
List 20 v per page											Search		
Juniper	From All zones V Go New										ew		
Juniper-NS5GT	Fror	n Trust To	Untrust, total p	oolicy: 1									
- Home	ID	Source	Destination	Service	Action	Options		Config	jure	Enable	Move		
Configuration Network Network Configuration Network Conficies MCast Policies VPNs Objects Reports Wizards Help Network Networ	1	Avaya CLAN - 1A02 Avaya CLAN - 1B02 Avaya MEDPRO - 1A03 Avaya MEDPRO - 1B03	Avaya Branch Office Avaya ESS Avaya Main Office	ANY	3	E	<u>Edit</u>	<u>Clone</u>	<u>Remove</u>	N	\$ 		
– Logout	From Untrust To Trust, total policy: 1												
Toggle Menu	ID	Source	Destination	Service	Action	Options		Config	jure	Enable	Move		
	2	Avaya Branch Office Avaya ESS Avaya Main Office	Avaya CLAN - 1A02 Avaya CLAN - 1B02 Avaya MEDPRO - 1A03 Avaya MEDPRO - 1B03	Avaya_H248 Avaya_H323 Avaya_RTP ICMP-ANY	Ø		Edit	Clone	Remove	য	¢ ***		
Edit										Interr	net		

Figure 29 – Service Entries

4. Avaya Communication Manager Configuration

From the System Access Terminal (SAT), enter the "**change ip-nework-region n**" command, where n represents the region number. Enter the UDP port range (minimum and maximum) under **Media Parameters** as shown in **Figure 30** for Network Region 1. This port range must match the Custom Service port range used in Step 2 of Section 3.6. The Main Office uses Network Region 1 and the Branch Office (not shown) uses Network Region 2. The same UDP port range is specified for each Network Region.

```
change ip-network-region 1
                                                                                                                                                                                                                                                      Page
                                                                                                                                                                                                                                                                                1 of
19
                                                                                                                       IP NETWORK REGION
      Region: 1
Location: 1
                                                                 Authoritative Domain:
             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? n
           UDP Port Max: 3327
DIFFSERV/TOS PARAMETERS
                                                                                                                                                            RTCP Reporting Enabled? y
   Call Control PHB Value: 46
Audio PHB Value: 46
Call Control PHB Value: 46
C
                              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? v
   Idle Traffic Interval (sec): 20
           Keep-Alive Interval (sec): 5
                                             Keep-Alive Count: 5
```

Figure 30 – IP Network Region Form

5. Verification Steps

The following steps can be performed to verify that the Juniper NetScreen 5GT can support Avaya IP Telephones, Avaya Media Gateways, Avaya Enterprise Survivable Servers, and Avaya Local Survivable Processors:

	<u>n</u>			T) (1		4 1	• • •		1.				
From the S	ystem A	Access Termi	nal (SA	T), use the	tion allows	stered-	ip-statio	ns ²² comm	and t				
	110 Juli	(2) to registe	to a C		uon anows	ine Av	aya IF T	elephones	(e.g.,				
20001, 300	01-300	02) to registe	r to a C	-LAN.									
list reg	11st registered-ip-stations												
REGISTERED IP STATIONS													
Station	Set	Product	Prod	Station	Ne	t Orig	Gate	keeper	TC				
Ext	Туре	ID	Rel	IP Addr	ess Rg	n Port	IP A	ddress	Sk				
20001	4621	IP_Phone	2.400	10.11.1	.21 2		192.	168.1.15	У				
50001	4621	IP_Phone	2.400	10.10.1	.51 1		192.	168.1.15	У				
50002	4610	IP_Phone	2.400	10.10.1	.52 1		192.	168.1.15	У				
register to a C-LAN.													
list media-gateway													
TIPC Med													
			MEDI	A-GATEWA	Y REPORT								
Num Name		Se	MEDI erial No W Ver/HN	A-GATEWA o/ W Vint	Y REPORT IP Address Cntrl IP A	/ ddr	Туре	NetRgn RecRule	Reg?				
Num Name 1 g350		St FT 0!	MEDI erial No W Ver/HV 5IS3572	A-GATEWA o/ W Vint 4296	Y REPORT IP Address Cntrl IP A 10 .11 .1	/ ddr .254	Туре g350	NetRgn RecRule 2	Reg? Y				
Num Name		Sr FV 0! 2!	MEDI: erial No W Ver/HN 5IS3572 5 .23 .0	A-GATEWA o/ W Vint 4296 0 /1	Y REPORT IP Address Cntrl IP A 10 .11 .1 192.168.1	/ ddr .254 .15	Type g350	NetRgn RecRule 2 1	Reg? Y				
Num Name		S(F) 0! 2!	MEDI, erial NG W Ver/HN 5IS35724 5.23.0	A-GATEWA o/ W Vint 4296 0 /1	Y REPORT IP Address Cntrl IP A 10 .11 .1 192.168.1	/ ddr .254 .15	Type g350	NetRgn RecRule 2 1	Reg? Y				
Num Name		Sr F1 0! 2!	MEDI; erial No W Ver/HU 5IS35724 5 .23 .0	A-GATEWA 0/ W Vint 4296 0 /1	Y REPORT IP Address Cntrl IP A 10 .11 .1 192.168.1	/ ddr .254 .15	Туре g350	NetRgn RecRule 2 1	Reg? y				

Step	Description												
3.	From the System Access Terminal (SAT), use the "status ess clusters" command to verify that												
	the Juniper NetScreen 5GT configuration allows both Cluster 1 (Primary Servers) and Cluster												
	2 (ESS Server) to register.												
	status ess clusters												
	Cluster ID 1 ESS CLUSTER INFORMATION												
	Cluster	Enabled?	Active Server	Register	ed?	Tra	nslations	Software					
	10	lilabica.	ID	Regibter	cu.	0]	puarea	VCIBION					
	1	У	1	У		22:0	0 7/4/2006	R013x.01.1.628	.7				
	2	У	3	Ŷ		22.0	0 //4/2006	RUI3X.UI.I.028	. /				
			Figu	re 33 – E	SS Cl	uste	r Informatio	n					
4.	From the Syste	em Access	Termina	al (SAT),	use th	e "li	st survivabl	e-processor" com	mand to				
	and the Avaya both servers ha	ave the sam	00-ess) ne time a	to registe and date i	r. File	e syn Fran	chronization slations Up	is working proper dated field.	ly because				
	list surviva	able-proce	ssor										
				SURVIVA	BLE PH	OCES	SSORS						
	Name	Туре	I	P Addres	5	Reg	LSP Act	Translations Updated	Net Rgn				
	g350-1sp 8500-ess	LSP ESS	1	$\begin{array}{c} 0 & .11 & .1 \\ 0 & .13 & .1 \end{array}$.10	y v	n	22:00 7/4/2006	2				
		200	-			1		22 00 ,, 1, 2000	-				
			Figu	re 34 – E	SS Cl	uste	r Informatio	n					
5.	Verify shuffle	d and non-s	huffled	calls can	be pla	iced	successfully	when a primary m	edia server				
	is active from	the Avaya	IP Telep	ohones at	both t	he N	lain and Brai	nch Offices.					
6.	Verify shuffle	d and non-s	shuffled	calls can	be pla	iced	successfully	when the ESS serv	ver is active				
	from the Avaya IP Telephones at both the Main and Branch Offices.												

6. Conclusion

These Application Notes describe how to configure the Juniper NetScreen 5GT to support Avaya H.323 IP Telephony. The sample configuration presented in these Application Notes illustrated how a Juniper NetScreen 5GT firewall can be configured to protect Avaya C-LANs and Media Processor boards using security policies which only allow H.323 signaling, RTP, and H.248 traffic to pass through the firewall.

7. Additional References

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

- [1] Avaya Application Solutions: IP Telephony Deployment Guide, Issue 4.2, February 2006, Document ID: 555-245-600.
- [2] Configuring the Juniper NetScreen Firewall Security Policies to support Avaya IP Telephony, Issue 1.0.

The following Juniper NetScreen documentation can be found at http://www.juniper.net.

[3] NetScreen Concepts & Examples, ScreenOS Reference Guide, Volume 2: Fundamentals, ScreenOS 5.0.0 P/N 093-1345-000, Rev. A.

© 2006 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by [®] and TM 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 and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at <u>interoplabnotes@list.avaya.com</u>