

Avaya Solution & Interoperability Test Lab

Configuring Point-to-Point Protocol between Juniper Networks Secure Services Gateway SSG520 and M7i Router to Support an H.323 trunk – Issue 1.0

Abstract

These Application Notes describe the steps for configuring Juniper Networks Secure Services Gateway SSG520 and M7i routers for a Point-to-Point Protocol (PPP) connection to support an Avaya IP Telephony infrastructure consisting of Avaya Communication Manager and Avaya IP Telephones. Security policies will be used to allow Avaya Voice over Internet Protocol (VoIP) to traverse the PPP connection and to perform traffic shaping to maintain the Quality of Service needed for VoIP traffic. Information in these Application Notes has been obtained through Developer*Connection* compliance testing and additional technical discussions. Testing was conducted via the Developer*Connection* Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

The Juniper Network Secure Services Gateway SSG520 is a security appliance that can provide a mix of security and LAN/WAN connectivity in a regional and branch office deployment. These Application Notes illustrate a sample network consisting of a Main and Branch site connected together via a Point-to-Point Protocol connection through the use of the M7i router and SSG520 respectively. Each site contains an Avaya Media Server, Avaya Media Gateway, and Avaya IP Telephones. An H.323 IP trunk was configured between the two Avaya Communication Manager servers.

From a security perspective, all network traffic internal to the Branch site is considered to be "Trusted" and all traffic coming in from the WAN interface "Untrusted". Traffic policies were configured in the SSG520 to permit only traffic necessary to support Avaya VoIP calls between the two sites. Quality of Service (QoS) on the SSG520 was achieved through the use of traffic shaping associated with each security policy. For managing QoS in the Juniper Network M7i router, DiffServ Code Point (DSCP) examination and bandwidth reservation were used to prioritize VoIP traffic.

The SSG520 also serves as the Dynamic Host Configuration Protocol (DHCP) server for the Branch site supporting option 176.

For the configuration tested in these Application Notes:

- The H.323 Application Layer Gateway (ALG) was disabled.
- The Juniper SSG520 was configured in "route" mode and Network Address Translation (NAT) was not used.
- The security polices defined were limited to traffic flows required by Avaya VoIP traffic only.

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 Networks SSG520 and M7i router to support Avaya VoIP traffic.

Table-1 below outlines the protocol type and port information used by the Avaya VoIP traffic.

From	TCP/UDP Port	То	TCP/UDP Port	Notes
	or Protocol		or Protocol	
Avaya Media	TCP any	Any C-LAN	TCP 1720	For H.225 call
Server				signaling.
Any endpoint	UDP any	Any endpoint	UDP 2048-3029	For RTP/RTCP audio
			(UDP port range	streams between
			on the IP	MedPros and
			Network Region	endpoints.
			form in Section 5	
			Step 8)	
Any endpoint	ICMP any	Any C-LAN	ICMP any	For diagnostic
		and Any		purposes.
		MedPro		

Table 1 – TCP/UDP Ports

2. Configuration

Figure 1 illustrates the configuration used in these Application Notes. All Avaya IP Telephones with an extension in the range of 2xxxx are registered with Avaya Communication Manager at the Main site and all Avaya IP Telephones with an extension in the range of 4xxxx are registered with Avaya Communication Manager at the Branch Site. An H.323 trunk, configured between the two Avaya Communication Manager servers, carries calls between the two sites. IP addresses for Avaya IP Telephones in the Main site are statically administered and the IP addresses for the Avaya IP Telephones in the Branch site are dynamically allocated by the SSG520.





3. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8300 Media Server with G250-	Avaya Communication Manager R3.1.2
DS1 Media Gateway	(R013x.01.2.632.1)
Avaya S8500 Media Server	Avaya Communication Manager R3.1.2
	(R013x.01.2.632.1)
Avaya G650 Media Gateway	-
TN2312BP IPSI	HW03 FW 22
TN799DP C-LAN	HW01 FW 16
TN2302AP IP MedPro	HW18 FW 108
Analog telephone	N/A
Avaya 4602SW IP Telephone (H.323)	R2.3 – Application (a02d01b2_3.bin)
Avaya 4610SW IP Telephone (H.323)	R2.6 – Application (a10d01b2_6.bin)
Avaya IP Softphone	R5.24.8
Juniper Networks SS520	Screen OS 5.4r1
Juniper Networks M7i router	JUNOS 7.6R2.6

4. Configure Juniper Networks equipment

This section describes the configuration for Juniper Networks SSG520 and M7i routers shown in **Figure 1**.

4.1. Configure the Juniper Networks SSG520

This section shows the necessary steps in configuring the SSG520 as shown in the **Figure 1**. The following steps use the web browser interface offered by the SSG520.

4.1.1. Logging into SSG520 and general setup

Step	Description
1.	Enter the IP address of the SSG520 into a web browser to access the web interface of the
	SSG520. Enter the appropriate Admin Name and Password at the log in screen then click
	Login to gain access into the SSG520.
	Cile Edite View Experience Teals Hele
	G Back + O + K 2 G - Search Favorites 🚱 🔄 + G K 4
	Address 🙋 https://172.16.254.132/index.html
	Admin Name: netscreen
	Password:
	Remember my name and password
	Login
	STANDER FRANKER
	📓 Done
	<u>, </u>



Step	Description
3.	Disable the Application Layer Gateway (ALG) functionality by selecting Configuration → Advanced → ALG → Configure from the navigation menu on the left and uncheck the H323 check box on the right screen. Click Apply to complete.
	Address 🗃 https://172.16.254.132/nswebui.html 💌 🄁 Go 🛛 Links 🆏 🗸
	Configuration > Advanced > ALG > Basic SSG520 ?
	Bosic MGCP H323 SIP SCCP Application Local intranet Date/Time Image: Singe Other Auth Infranet Auth Advanced Traffic Shaping Apply Cancel
	SSG-520 ▲ Home ✓ Configuration ✓ Date/Time ✓ Update ✓ Admin ✓ Admin ✓ Admin ✓ Advanced ✓ Traffic Shaping ✓ Advanced ✓ Microsoft RPC ✓ Advanced ✓ NGCP ✓ Apply Cancel

4.1.2. Configuring PPP profile and interfaces

File Edit View Favorites	Tools Help	oft Inter	net explorer				09928	<u>.</u>
🕒 Back - 🕥 - 💌 😰	🔥 🔎 Sea	rdh 📩	Favorites 🚱 🔗	• 😓 🛛	9 - 🛄 🕯	12 - 35		
Address (2) https://172.16.254.1	32/nswebui.html					3	3 🔁	Go Links
	Network >	PPP (List)				S	SG520
\$\$G-520	ppp Profile	Auth	Netmask	Static- IP	Passive	Interface Bound	Co	nfigure
Home Configuration Network	test Multi- link	None None	255.255.255.240 255.255.255.252	Yes Yes	No No	mli	Edit Edit	Remove Remove
Dinding Dis Zones Interfaces DHCP B02 1X Routing NSRP PPP PPP Profile PPPoE Profile PPPoE Profile Poincipg						-	,	

PPP Profile Static IP	ppp Checked	
Netmask	255.255.255.240 (This needs to match the mask used Area Link as shown in Step 6).	in the W
55G520:Juniper-ScreenO	5.4.0r1.0 - Microsoft Internet Explorer	
Ele Edit View Favorites	Iook Help	
G Back 🔹 🕑 🕤 💌	🛿 🏠 🔎 Search 🎌 Favorites 🚱 😒 🌭 🔯 🖌 🛄 🎎 🦓	
Address 🙋 https://172.16.25	132/navebui.html	Go Links
	Authentication CHAP PAP (PAP + CHAP = Any,	No
 Home Tonfiguration Notwork 	Authentication selection = None)	
- Binding	Netmask 255.255.255.240	
– Zones – Interfaces	Passive: Don't challenge peer	
- DHCP - 802.1X	Local Name	
Routing NSRP	Password	
- PPP Profile	OK Capcel	

	or no - merosore	Internet capiorer						
<u>File Edit View Favorites Io</u>	ols <u>H</u> elp							
🌀 Back 🔹 🕥 - 💌 🙎 🕯	🏠 🔎 Search	📩 Favorites 🧭	😞 • چ	•		1 🚳		
Address (2) https://172.16.254.132	Inswebui.html					-	- 🔁 G	io L
	Network > In	nterfaces (List)					SS	G520
	List 20 💌 p	er page						
2 Juninor	List ALL(9)	Interfaces				New	Tun	nel IF
E ZJUIIIPEI								
	Name	IP/Netmask	Zone	Туре	Link	PPPoE	Cor	nfigu
	ethernet0/0	172.16.254.132/24	Trust	Layer3	Up	-	Edit	
- Home	ethernet0/1	172.28.40.1/24	Trust	Layer3	Up	-	Edit	
- Network	ethernet0/2	0.0.0/0	Untrust	Layer3	Up	-	<u>Edit</u>	
- Binding	ethemet0/3	0.0.0/0	HA	Layer3	Down	-	Edit	
- Zones	serial1/0	192.168.3.30/28	Untrust	WAN	Down	-	Edit	
- Interfaces	serial1/1	0.0.0.0/0	Untrust	WAN	Up	-	Edit	
€-802.1X	serial2/0	0.0.0/0	Trust	WAN	Down	-	Edit	
Routing	serial2/1	0.0.0/0	Trust	WAN	Down	-	Edit	
I I NSRP		0.0.0.0	CT AN	Lover2	Down	_	Edit	



SSG520:Juniper-Screen0	S 5.4.0r1.0 - Microsoft	Internet Explorer						
Ele Edit View Favorites	Iools Help		<u> </u>			4	<u></u>	
🌀 Back 🔻 🐑 👻 📩	🚨 🏠 🎾 Search	🎌 Favorites 🥳	🛛 · 🦾	· 2		1 🐴	_	
Address 1 https://172.16.25	4.132/nswebui.html						- 🔁	Go
	Network > In	terfaces (List)					S	SG52
\mathcal{C}	List 20 💌 p	er page						
(A) luninor	List ALL(9)	Interfaces				New	Tu	nnell
A 2 DUTTIPET								
	Name	IP/Netmask	Zone	Туре	Link	PPPoE	Co	nfig
	ethernet0/0	172.16.254.132/24	Trust	Layer3	Up	-	Edit	
- Home	ethernet0/1	172.28.40.1/24	Trust	Layer3	Up	-	Edit	
- Network	ethemet0/2	0.0.0.0/0	Untrust	Laver3	Up	-	Edit	
Binding	ethemet0/3	0.0.0/0	HA	Laver3	Down	-	Edit	
- Zones	serial1/0	192.168.3.30/28	Untrust	WAN	Down	-	Edit	-
- Interfaces	serial1/1	0.0.0.0/0	Untrust	WAN	Un	-	Edit	-
- DHCP	serial2/0	0.0.0/0	Trust	WAN	Down	-	Edit	
Routing	serial2/0	0.0.0.0/0	Truct	WAN	Down		Edit	
NSRP	Selidi2/1	0.0.0.0/0	TTUSC	VVAN	Down		Edit	-
E PPP	vian1	0.0.0.0/0	VLAN	Layer3	Down	-	Eait	



4.1.3. Configuring DHCP Server services

Ele Edit View Favorit	es <u>T</u> ools	Heb		
G Back + 🕤 + 🗵	2 🏠	Search 🌟 Favorites 🧐 🍰 🖡	🍃 🖸 - 🔜 🕻	3 3
Address 🔕 https://172.16.	254.132/nsw	rebui.html		<u>ד</u> <u>ו</u> יים <u>ו</u>
	N	etwork > DHCP (List)		SSG52
330 520		ethernet0/0(172.16.254.132/24)	None	Edit
- Home		ethemet0/1(172.28.40.1/24)	Relay	Edit
- Network		ethernet0/2(0.0.0.0/0)	None	Edit
 Binding DNS 		vlan1(0.0.0/0)	None	Edit
	5353			

2.	From the Network > to continue.	> DHCP > Edit screen, enter the following information then click Apply
	DHCP Server Gateway Netmask Click on Addresses	Checked 172.28.40.1 (IP address of the default gateway) 255.255.255.0 to configure the DHCP IP address range. DNS, WINS, and other DHCP
	options can be configured in the comp	gured by clicking on Advanced Options . These advanced options were bliance test.
	SSG520:Juniper-ScreenD	S 5.4.0r1.0 - Microsoft Internet Explorer
	Elle Edit View Favorites	
	🌀 Back 🝷 🕥 🛃 📘	😂 🏠 🔎 Search 🌟 Favorites 🚱 🔗 🌭 🔯 🕣 🛄 🎇 🖄
	Address 🛃 https://172.16.25	4.132/nswebui.html 💌 🔁 Go 🛛 Links 🧌 🔻
		Network > DHCP > Edit SSG520 ?
	SSG-520 - Home - Configuration - Network - Binding - DNS - Zones - Interfaces - DHCP - 602.1X - Routing - NSRP - PPP - Screening - Policies - MCast Policies - MCast Policies - MCast Policies - Wizards - Wizards - Help - Logout	 None DHCP Client DHCP Relay Agent DHCP Server Server Mode (Auto (Probing) (Enable) Disable Lease (Unlimited Lease (Unlimited) hours (minutes Update Upstream DHCP Client on Interface Any (From Upstream DHCP Client on Interface Any (From Upstream DHCP Client on Interface Any (From Interface) None None From Option66 From Input (0.0.0)
	E Done	Cancel



Dynamic	Checked
IP Address Start	172.28 40 100 (start of the DHCP IP address range)
IP Address End	172 28 40 199 (end of the DHCP IP address range)
II Mullos Linu	172.20.40.177 (chu of the Difer if address funge)
SSG520:Juniper-Screen(5 5.4.0r1.0 - Microsoft Internet Explorer
Ele Edit View Favorites	Iools Help
🕒 Back 🝷 💮 - 💌	💈 🏠 🔎 Search 🤺 Favorites 🚱 🙈 - 🍡 🔯 - 🧾 🎇 🦓
Address https://172.16.25	4.132/nswebul.html
	Network > DHCP > DHCP Server Address Edit \$\$\$6520
	Interface: ethernet0/1 (IP/Netmask: 172.28.40.1/24)
Juniper	
C ARTWORKS	
SSG-520	
- Home	
Configuration Network	IP Address Start 172.28.40.100
- Binding	IP Address End 172.28.40.199
DNS	
- Zones	
- DHCP	C Reserved
	IP Address 0.0.0.0
Routing	Ethernet Address 0000 0000 0000
NSRP	
+ Screening	Example Ethernet Address: ABCD.1234.8EUE
- Policies	
- MCast Policies	OK Cancel
VPNs	

SSG520:Juniper-ScreenOS 5.4.0	r1.0 - Microsoft Internet Explorer	
Ele Edit View Favorites Iool	: Helb	
🌀 Back 🔹 🕥 🔹 😫 🔮	🏠 🔎 Search 🤺 Favorites 🚱 🍰 🎍 🔯 - 🛄 鑬 🦓 👘	
Address a https://172.16.254.132/n	swebui.html	🔁 Go
N	etwork > DHCP Server > Custom Options > ethernet0/1 (List)	SSC
	B	ack To
(A) luninor		
	Code Type Value Config	ure
	No entry available	
- Home		
- Network		
Binding		
DNS Zones		
- Interfaces		
- DHCP		

	1
Code	176
Туре	String
Value	MCIADD=172.28.40.5,MCPORT=1719
Note: 172.28. and 1719 is th Avaya Comm	40.5 is the IP address of the Avaya Media Server located at the Branch site in default port number used by the Avaya IP Telephones to register to the nunication Manager.
🦉 55G520:Junipe	er-ScreenOS 5.4.0r1.0 - Microsoft Internet Explorer
<u>File E</u> dit <u>V</u> iew	Favorites Tools Help
G Back + 🕤) 👻 💈 🏠 🔎 Search 🤺 Favorites 🤣 🍰 🍡 🔜 🛄 🎎 🖄
Address 🥘 https:	://172.16.254.132/nswebui.html
	Network > DHCP > Server Custom Option SSG520
Jur	Interface: ethernet0/1 (IP/Netmask: 172.28.40.1/24)
SSG-	Code 176 Type String Value
Homo	
Tiome	
+- Configuratio	
 Configuration Network Binding 	OK
Configuration Configuration Network Binding DNS	OK Cancel

4.1.4. Configuring Address objects and Custom Services

1. Create address book entries by selecting **Objects** \rightarrow **Addresses** from the navigation menu on the left. Click on the **New** button to create a new address book entry.



Addres	ss Name	IP Address	Netmask	Zone
Main Networ	k	172.28.10.0	24	Untrust
Main-CLAN		172.28.10.7	32	Untrust
Branch Netw	ork	172.28.40.0	24	Trust
Branch-Medi	a Svr	172.28.40.5	32	Trust
SSG520:Juniper-Screen05 S	.4.0r1.0 - Microsoft Intern	et Explorer		
Elle Edit View Favorites	Toola Helb			
😋 Back 🝷 🕥 🕤 💌 💈] 🏠 🔎 Search 👷	Favorites 🚱 🔗 🍹 🚱 -	🔜 🗱 🤹	
Address 🔊 https://172.16.254.1	32/nswebui.html			💌 🔁 GO
	Objects > Addres	ses > Configuration		SSG520
\$\$G-520		Address Name Main Ne	twork	
Home		Comment		
Configuration	IP Address/Do	main Name		
 Network Screening 	I r	© IP 172.28	10.0	1
		Address/Netmask 24		
Policies		C Domain Name		
Policies MCast Policies VPNs		Definant Warne		
Policies MCast Policies VPNs Objects Addresses				
Policies MCast Policies VPNs Objects Addresses List		Zone Untrust		
Policies MCast Policies VPNs Objects Addresses List Groups Summary		Zone Untrust	.	
Policies MCast Policies VPNs Objects Addresses List Groups Summary Services			Cancel	



Back Image: Construct of the second seco	<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites	<u>T</u> ools <u>H</u> elp				
Address Hetps://172.16.254.132/nswebui.html Image: Sige Services > Custom SSG520 Configuration List 20 Per page Image: Signaling Transport Protocol and Parameters Timeout (min) Configure Home Avaya- Signaling TCP src port: 0- 65535, dst port: 30 30 Edit Remove Network Screening UDP src port: 0- 65535, dst port: 1 1 Edit In Use	🌍 Back 🝷 🕥 🖌 🗾 💈	🖞 🏠 🔎 Search	- 🔶 Favorites 🛛 🔗	• 🎍 🔜 🛛	_ 1	1 🕉
Objects > Services > Custom SSG520 List 20 per page SSG-520 Name Transport Protocol and Parameters Timeout (min) Configure Name Transport Protocol and Parameters Configure Home Avaya- Signaling TCP src port: 0- 65535, dst port: 1720-1720 30 Edit Remove Network Screening UDP src port: 0- 65535, dst port: 1 Edit In Use	Address 🙆 https://172.16.254.:	132/nswebui.html		-] 🔁	Go Links
List 20 per page List 20 per page SSG-520 Name Transport Protocol and Parameters Timeout (min) Configure Home Avaya- Signaling TCP src port: 0- 65535, dst port: 1 30 Edit Remove Network VDP src port: 0- 65535, dst port: 1 1 Edit In Use Model UDP src port: 0- 65535, dst port: 1 1 Edit In Use		Objects > Ser	vices > Custom		S	SG520
SSG-520 Name Transport Protocol and Parameters Timeout (min) Configure Home Avaya- Signaling TCP src port: 0- 65535, dst port: 30 Edit Remove Network Screening UDP src port: 0- 65535, dst port: 1 30 Edit Remove Avaya-RTP ODP src port: 0- 65535, dst port: 1 1 Edit In Use		List 20 🔽 pe	er page			
SSG-520 Name Transport Protocol and Parameters Timeout (min) Configure Home Avaya- Signaling TCP src port: 0- 65535, dst port: 1720-1720 30 Edit Remove Network Screening UDP src port: 0- 65535, dst port: 1 30 Edit Remove Avaya-RTP 65535, dst port: 1 1 Edit In Use						
SSG-520 Name Transport Protocol and Parameters Timeout (min) Configure Home Avaya- Signaling TCP src port: 0- 65535, dst port: 130 30 Edit Remove Network Screening UDP src port: 0- 65535, dst port: 1 30 Edit Remove Avaya-RTP ODP src port: 0- 65535, dst port: 1 1 Edit In Use						_
Home Avaya- TCP src port: 0- 30 Edit Remove • Configuration Signaling 1720-1720 30 Edit Remove • Network • Screening UDP src port: 0- 65535, dst port: 1 Edit Remove • Olicies • Avaya-RTP 65535, dst port: 0- 1 Edit In Use		Name	Transport Protocol and Parameters	Timeout (min)	Co	nfigure
+ Screening - Policies MCast Policies - MCast Policies - UDP src port: 0- 65535, dst port: 1 Edit In Use	 Home Configuration Network 	Avaya- Signaling	TCP src port: O- 65535, dst port: 1720-1720	30	<u>Edit</u>	Remov
2048-3029	+ Screening - Policies - MCast Policies	Avaya-RTP	UDP src port: O- 65535, dst port: 2048-3029	1	<u>Edit</u>	In Use

N		eout	Avaya-S Use pro	Signaling tocol defa	ult				
1	l o.]	Franspo	rt protocol	Source]	Port	Dest	inatio	n Por	t
				Low	High	Low		High	
2		Т	ЪСР	0 6	55535	1720		1720	
Address	6.254.132/ns	webui.html	☆ Favorites	• 🎍 🖻 📙	8			Ţ	Go SSG520
SSG-520 Home Configuration Network			Service Nam Service Timeou	e Avaya-Signalin t Ose protoco O Never O Custom	g ol default (minute: Sour	5) ce Port	Destina	ation Port	ICM
- Policies		No.	Transport prot	:ocol	Low	High	Low	High	Туре
- WCast Foncies		1 C none	• TCP • UDP • I	CMP O other	0	65535	1720	1720	
+ VPNs		2 🖲 none	O TCP O UDP O IO	CMP O other					
 VPNs Objects Addresses 		3 📀 none	O TOP O UDP O IO	CMP 🗢 other 📃					
 VPNs Objects Addresses Services 				-					
 VPNs Objects Addresses Services Predefined Custom 		4 📀 none	O TOP O UDP O IO	CMP 🔍 other			· · ·		
VPNs Objects Addresses Services Predefined Custom Sun RPC		4 • none 5 • none	C TCP C UDP C IC	CMP C other					
VPNs Objects Addresses Services Predefined Custom Sun RPC MS RPC Groups		4 © none 5 © none 6 © none	 TCP UDP TCP UDP ICP UDP ICP ICP UDP ICP 	CMP C other					
 VPNs Objects Addresses Services Predefined Custom Sun RPC MS RPC Groups Users 		4 • none 5 • none 6 • none 7 • none	C TCP C UDP C IC C TCP C UDP C IC C TCP C UDP C IC	CMP C other					
VPNs Objects Addresses Services Predefined Custom Sun RPC Groups Users IP Pools Schmading		 e none none none none none none none 	C TCP C UDP C Id	CMP C other CMP C other CMP C other CMP C other CMP C other					
 VPNs Objects Addresses Services Services Sun RPC MS RPC Groups Users IP Pools Schedulco Group Expression 	ins	4 • none 5 • none 6 • none 7 • none 8 • none	C TCP C UDP C Id C TCP C UDP C Id	CMP C other CMP C other CMP C other CMP C other CMP C other					

Service	Name Avaya-	RTP					
Service	Timeout Use pro	otocol defa	ult				
	-	-					
N	o. Transport protocol	Source	Port	Destir	nation Pol	rt	
	LIDD		High	Low	High		
1	UDP	0	65535	2048	3029		
Ele Edit Yew Favorites	s Iools Help S 😚 🔎 Search 👷 Pavonites 🚱 🖉 54.132/nswebul.html	3• 😓 🖬 • [11 18			• 🔁 60	
Ele Edt Yew Fyvorites Back + K + Address https://172.16.25 SSG-629 Home	s Tools Help St. 132/nswebu.html Objects > Services > Custom > Ed Service Nam Service Timeo	it it Avaya-RTP it O Use proto C Never	Decol default			SS 0520	
Ele Edit yew Fayorites Back - · · · · · · · · · · · · · · · · · ·	s Tools Help St.132(nswebu:.html Objects > Services > Custom > Ed Service Nan Service Timeo	it ne Avaya-RTP nut @ Use proto C Never C Custom [Cool default	rre Port	Destination I	SSC520	
Ele Edt Yew Fyvortes Back +	s Tools Help St.132/nswebu.html Objects > Services > Custom > Ed Service Nan Service Timeo No. Transport pro	It It Avaya-RTP It Out © Use proto O Never C Custom [otocol	Decol default (minute Sou Low	rce Port High	Destination F Low Hig	SSC520 SSC520 Port IC gh Type	
Ele Ed yew Fyvortes Back + · · · · · · · · · · · · · · · · · ·	s Tools Help St.132(nswebu:.html Objects > Services > Custom > Ed Service Nam Service Timeo No. Transport pro 1 C none C TCP G UDP C	iit ne Avaya-RTP nut © Use proto © Never © Custom [otocol ICMP © other [Decol default (minute Sou Low 0	rce Port High 65535	Destination F Low Hig 2048 3029	2 ort 10 gh Type	
Ele Edt Yow Fgyortes Back + • • • • • Address Inteps://172.16.25 Address Inteps://172.16.25 	s Tools Help St. 132/nswebu.html Objects > Services > Custom > Ed Service Nan Service Timeo No. Transport pro 1 ∩ none ∩ TCP ← UDP ∩ 2 ← none ⊂ TCP ← UDP ∩	It It It Avaya-RTP It Ouse proto Ouse proto Ous	Cool default (minute Sou Dow 0	is) rce Port High 65535	Destination F Low Hit 2048 3029	Port IC gh Type	
Ele Edt yew Fayortes Dack + O + M Address M https://172.16.25 SSG-629 Home Configuration Network Screening Policies MCast Policies VPNs Objects Addresses Services	s Tools Help St.132/nswebu.html Objects > Services > Custom > Ed Service Nam Service Timeo No. Transport pro 1 C none C TCP C UDP C 2 € none C TCP C UDP C	It It It It It It It It It It	Decol default (minute Sou Low 0	is) rce Port High 65535	Destination F Low Hig 2048 3029	Port IC gh Type	
Ele Edt yew Fayorites Deck +	s Tools Help St.132/nswebu.html Objects > Services > Custom > Ed Service Nam Service Timeo No. Transport pro 1 C none C TCP C UDP C 2 € none C TCP C UDP C 3 € none C TCP C UDP C	III III III III III III III III	Decol default (minute Sou Low 0	is) rce Port High 65535	Destination F Low Hig 2048 2029	Port IC gh Type	
Ele Edt gew Fayorites Back +	s Tools Help Service Name Service Name S	it it it it it it it it it it	Decol default (minute Sou Low 0	rce Port High 65535	Destination F Low Hig 2048 3020	Port IC gh Type	
Ele Edt yew Fayorites Deck +	s Tools Help Service Name Service Name Service Name Service Timeo No. Transport pro 1 ∩ none ∩ TCP ∩ UDP ∩ 2 ∩ none ∩ TCP ∩ UDP ∩ 3 ∩ none ∩ TCP ∩ UDP ∩ 3 ∩ none ∩ TCP ∩ UDP ∩ 5 ∩ none ∩ TCP ∩ UDP ∩	it it it it it it it it it it	Decol default (minute Sou Lov 0	rce Port High 65535	Destination F Low Hig 2048 3029	2 ort 10 gh Type	
Ele Edt yew Fayantes Deck + C + K Address Inteps://172.16.25 Address Inteps://172.16.25 Formation State Formation State Home Configuration Network Configuration Network Configuration Network Configuration Network Configuration Network Configuration Network Configuration Network Configuration Network Configuration Network Configuration Policies MCast Policies Coljects Addresses Services Predefined Custom Sun RPC MC RPC Coups Users	s Tools Help Search ☆ Pavonites @ (S4.132)nswebu.html Objects > Services > Custom > Ed Service Nam Service Timeo No. Transport pro 1 ∩ none ∩ TCP ∩ UDP ∩ 2 ∩ none ∩ TCP ∩ UDP ∩ 3 ∩ none ∩ TCP ∩ UDP ∩ 3 ∩ none ∩ TCP ∩ UDP ∩ 5 ∩ none ∩ TCP ∩ UDP ∩	it it it it it it it it it it	Decol default (minute Sou Low 0	rce Port High 65535	Destination F Low Hig 2048 3029	2 ort 10 gh Type	
Ele Edt yew Fayantes Deck + C + K Address Matps://172.16.25 Address Matps://172.16.25 Home Configuration Network Configuration Network Configuration Network Configuration Network Configuration Network Configuration Network Configuration Network Configuration Network Configuration Network Configuration Network Configuration Network Configuration Network Configuration Network Configuration Network Configuration Network Configuration Network Configuration Network Configuration Configuration Network Network	s Tools Help Search ☆ Pavonites @ (S4.132)nswebu.html Objects > Services > Custom > Ed Service Nam Service Timeo No. Transport pro 1 C none C TCP C UDP C 2 C none C TCP C UDP C 3 C none C TCP C UDP C 3 C none C TCP C UDP C 5 C none C TCP C UDP C	It It It It It It It It It It	Decol default (minute Sou Low 0	rce Port High 65535	Destination F Low Hig 2048 3029	2 ort IC gh Type J	

4.1.5. Configuring security policies and traffic shaping

The purpose of the security policies is to permit only trusted traffic and filter out unwanted traffic. In additional, the policy allows for management of Quality of Service through traffic shaping.

Solution of the second intervent between the second intervent i				a security poincy	III UIK	o nu					
Image: section Image	🖉 55G520:Juniper-ScreenO5 5.4.0r	1.0 -	Microsoft Internet Explorer								
Address	File Edit View Favorites Tools	He	اله Search 🔶 Favorites 📿) 😞 . 📐 🗔 🗖 🕅 🚿	2						
Delicities (From Untrust To Trust) screen, enter the following information. Clic Advanced to continue. Name (optional) Avaya call signaling Optional Come (Continue)	Address Address Address	webu	i.html								Go Lini
Itsl (2) Image: Second particular		Pol	licies (From All zones To A	ll zones)						SSG5	20
Nume Image: Control of the second		Lis	t 20 per page								Searc
Survey is a service Action Options Configure End Configuration From Unitrust To Trust, lotal policy: 6 Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Description Descrestrest Description		Fro	om Alizones 🗾		To	All zones	<u> </u>				N
Henne D Source Destination Service Action Options Configure End 0 Rescenting 0 Main-CLAN Branch-Media Svr Signaling 0 Edd Clone Beauxa F 0 Main-CLAN Branch-Media Svr Stripping 0 Edd Clone Beauxa F 0 Main-Vetwork Branch Network Branch Network Stripping 0 Edd Clone Beauxa F 0 Address Any Any Any Edd Clone Beauxa F 17 172.28.10.10/32 172.28.40.0/255.255.255.0 D Edd Clone Beauxa F 18 172.28.10.10/32 172.28.40.0/255.255.255.0 D Edd Clone Beauxa F 19 Potended Sun PPC Grapping Pinon Form True Potended Any Edd Clone Beauxa F 19 Potended Sun PPC Grapping Pinon Edd Clone Beauxa F		Fror	n Untrust To Trust, total p	policy: 6	,	,					,
6 Main-CLAN Branch-Mada Sur Avaya- Philo Avaya- Philo Avaya- Philo Edd. Clanz Remove F Policies Philo Avaya- Philo Avaya- Philo Avaya- Philo Avaya- Philo Edd. Clanz Remove F Policies Philo Avaya- Philo Avaya- Philo Avaya- Philo Edd. Clanz Remove F Policies Philo Avaya- Philo Avaya- Philo Edd. Clanz Remove F Philo Avaya- Philo Avaya- Philo Edd. Clanz Remove F Philo Avaya- Philo Avaya- Philo Edd. Clanz Remove F Philo Avaya- Philo Avaya- Philo Philo Edd. Clanz Remove F Philo Avaya- Philo Avaya- Philo Philo Edd. Clanz Remove F Philo Branch-Metwork Main-CLAN Philo Philo Edd. Clanz Remove F Philo Branch-Metwork Main-CLAN Philo Edd. Clanz Remove F Philo Branch-Network Main-CLAN	- Home	ID	Source	Destination	Service	Action	Options		Configu	ure	Enable
Image: Second Source Image: Source Image: Second Source Image: Source <	+- Configuration +- Network +- Screening	6	Main-CLAN	Branch-Media Svr	Avaya- Signaling PING			Edit	<u>Clone</u>	<u>Remove</u>	v
• Write • Main Network Branch Network • Claim • Claim • Edit Claim	– Policies – MCast Policies	8	Main Network	Branch Network	Avaya- RTP	Ø		<u>Edit</u>	<u>Clone</u>	<u>Remove</u>	
Addresses Addresses Image: Comparison of the second o	+ VPNs − Objects	4	Main Network	Branch Network	ECHO PING			<u>Edit</u>	<u>Clone</u>	<u>Remove</u>	
Image: Second	+ Addresses - Services	1	Any	Any	ANY	Ø		Edit	Clone	<u>Remove</u>	
Under the colspan="2">Under the colspan="2" of	Custom	17	172.28.10.100/32	172.28.40.0/255.255.255.0	DHCP- Relay	Ø		<u>Edit</u>	Clone	<u>Remove</u>	
Outputs Prom Trust To Untrust, total policy: 7 Destination Service Action Options Configure Fore Option Surce Destination Service Action Options Configure Fore Attacks Prom Trust To Untrust, total policy: 7 Prom Trust To Untrust To Network Aryaya Sector Fore Configure Fore Attacks Prom Trust To Untrust To Network Aryaya Attacks Advance Prom Trust To Trust) Destination Advance Prom Trust To Trust) Sereen, enter the following information. Clice Advanced to continue. Name (optional) Avaya call signaling Source Address Ad	- MS RPC	15	172.28.10.151/32	172.28.40.151/32	ANY	Ø		Edit	Clone	<u>Remove</u>	
ID Source Destination Service Action Options Configure End Group Expressions Group Expressions 5 Branch-Media Svr Main-CLAN Avaya- Signaling 0 Edit Clone Remove F P Attacks Proofs Branch-Media Svr Main-CLAN Avaya- Signaling 0 Edit Clone Remove F P Attacks Proof Branch-Network Main-CLAN Avaya- Signaling 0 Edit Clone Remove F Is growthis Proofs Branch Network 172:28:10.100/32 PHCP- Prelay 0 Edit Clone Remove F Is growthis 172:28:10.100/32 PHCP- Prelay 0 Edit Clone Remove F Is growthis 172:28:10.100/32 172:28:10.151/32 ANY 0 Edit Clone Remove F Is growthis Interpretain Interpretain Select Any ANY 0 Edit Clone Remove F Int the Policies (From Untrust To Trust) Screen, enter the following i		Fror	n Trust To Untrust, total p	policy: 7							
Group Expressions 5 Branch-Media Svr Main-CLAN Signaling Edit Clone Remove F Attacks Parach Main-Network Main Network Parach Parach F	- IP Pools - Schedules	ID	Source	Destination	Service	Action	Options		Configu	ure	Enable
Reports Any Main Network Any Edit Clone Remove Edit Clone Remove In the Policies (From Untrust To Trust) screen, enter the following information. Clice Advanced to continue. Name (optional) Avaya call signaling Source Address Address Book Entry (click on dropdown menu) Select Main-CLAN From the pop-up menu and click << to move them to the Selected Members field on the left, and click OK to continue.	 Group Expressions Certificates Attacks 	5	Branch-Media Svr	Main-CLAN	Signaling PING			Edit	<u>Clone</u>	<u>Remove</u>	ম
In the Policies (From Untrust To Trust) screen, enter the following information. Click Advanced to continue. Name (optional) Avaya call signaling Source Address Address Book Entry (click on dropdown menu) Select Main-CLAN From the pop-up menu and click << to move them to the selected Members field on the left, and click OK to continu		7	Branch Network	Main Network	RTP			Edit	<u>Clone</u>	<u>Remove</u>	9
Image New	Logout	16	Branch Network	172.28.10.100/32	DHCP- Relay	Ø		<u>Edit</u>	<u>Clone</u>	<u>Remove</u>	
Image:	Toggle Menu	з	Any	Any	ANY			<u>Edit</u>	<u>Clone</u>	<u>Remove</u>	
Image: Continue of the second seco		18	172.28.40.151/32	172.28.10.151/32	ANY			Edit	<u>Clone</u>	<u>Remove</u>	
In the Policies (From Untrust To Trust) screen, enter the following information. Click Advanced to continue. Name (optional) Avaya call signaling Source Address Address Book Entry (click on dropdown menu) Select Main-CLAN From the pop-up menu and click << to move them to the	Fdit			·						No Loca	aliptrapet
In the Policies (From Untrust To Trust) screen, enter the following information. Click Advanced to continue. Name (optional) Avaya call signaling Source Address Address Book Entry (click on dropdown menu) Select Main-CLAN From the pop-up menu and click << to move them to the							J			19200	arintranet
Advanced to continue.Name (optional)Avaya call signalingSource AddressAddress Book Entry (click on dropdown menu)SelectMain-CLANFrom the pop-up menu and click << to move them to the Selected Members field on the left, and click OK to continSource AddressAddress Book Entry (click on dropdown menu)SelectBranch-Media SvrFrom the pop-up menu and click << to move them to the	In the Policies (F	'n	m Untrust To	Trust) screen, e	enter f	he fol	lowing in	for	matio	on (Tlick
Name (optional)Avaya call signalingSource AddressAddress Book Entry (click on dropdown menu)SelectMain-CLANFrom the pop-up menu and click << to move them to the Selected Members field on the left, and click OK to continSource AddressAddress Book Entry (click on dropdown menu)SelectBranch-Media SvrFrom the pop-up menu and click << to move them to the		tir				101	10 11 11 11 11	1011			JIICI
Name (optional)Avaya call signalingSource AddressAddress Book Entry (click on dropdown menu)SelectMain-CLANFrom the pop-up menu and click << to move them to the Selected Members field on the left, and click OK to continSource AddressAddress Book Entry (click on dropdown menu) SelectSelectBranch-Media Svr From the pop-up menu and click << to move them to the	Advanced to con	un	iue.								
Nume (optional)Arbity can signatingSource AddressAddress Book Entry (click on dropdown menu)SelectMain-CLANFrom the pop-up menu and click << to move them to the Selected Members field on the left, and click OK to continSource AddressAddress Book Entry (click on dropdown menu) SelectSelectBranch-Media Svr From the pop-up menu and click << to move them to the	Advanced to con										
Source AddressAddress Book Entry (click of dropdown menu)SelectMain-CLANFrom the pop-up menu and click << to move them to the Selected Members field on the left, and click OK to continSource AddressAddress Book Entry (click on dropdown menu) SelectSelectBranch-Media Svr From the pop-up menu and click << to move them to the	Advanced to con		Avav	a call signaling							
Source AddressFrom the pop-up menu and click << to move them to the Selected Members field on the left, and click OK to contin Address Book Entry (click on dropdown menu) Select Branch-Media Svr From the pop-up menu and click << to move them to the											
Source AddressAddress Book Entry (click on dropdown menu) SelectSelect Branch-Media Svr From the pop-up menu and click << to move them to the	Advanced to con Name (optional) Source Address		Avaya Addre Selec	a call signaling ess Book Entry (Main CLA	click	on dr	opdown i	mer	nu)		
Source AddressAddress Book Entry (click on dropdown menu) SelectSelectBranch-Media Svr From the pop-up menu and click << to move them to the	Advanced to con Name (optional) Source Address		Avaya Addre Selec Erom	a call signaling ess Book Entry (t Main-CLA	click	on dr	opdown i	mer	nu)	to th	
Source Address Address Book Entry (click on dropdown menu) Select Branch-Media Svr From the pop-up menu and click << to move them to the	Advanced to con Name (optional) Source Address		Avaya Addre Selec From	a call signaling ess Book Entry (t Main-CLA the pop-up menu tod Mombora fiel	click N 1 and	on dr	opdown i << to mov	mer ve tl	hem	to th	e
From the pop-up menu and click << to move them to the	Advanced to con Name (optional) Source Address		Avaya Addre Selec From Selec	a call signaling ess Book Entry (t Main-CLA the pop-up menu ted Members fiel	click N 1 and 0 d on t	on dr click · the lef	opdown i << to mov it, and clic	mer ve tl ck C	nu) hem)K to	to th o cor	e ntinu
From the pop-up menu and click << to move them to the	Advanced to con Name (optional) Source Address Source Address		Avaya Addra Selec From Selec Addra	a call signaling ess Book Entry (t Main-CLA the pop-up menu ted Members fiel ess Book Entry (click N a and d on t click	on dr click · the lef on dr	opdown i << to mov it, and clic opdown i	mer ve tl ck () mer	nu) hem DK to nu)	to th o cor	e ntinu
	Advanced to con Name (optional) Source Address Source Address		Avaya Addre Selec From Selec Addre Selec	a call signaling ess Book Entry (t Main-CLA the pop-up menu ted Members fiel ess Book Entry (t Branch-Me	click N 1 and 1 d on t click edia S	on dr click the lef on dr	opdown i << to mov it, and clic opdown i	mer ve tl ck () mer	nu) hem DK to nu)	to th o cor	e ntinu
	rce Address		Avaya Addre Selec From Selec Addre Selec From Selec	a call signaling ess Book Entry (t Main-CLA the pop-up menu ted Members fiel ess Book Entry (t Branch-Ma the pop-up menu ted Members fiel	click N a and d on t click edia S a and d on t	on dr click (the lef on dr Svr click (the lef	opdown i << to mov it, and clic opdown i << to mov it, and clic	mer ve tl ck C mer ve tl ck C	nu) hem DK to nu) hem DK to	to th o cor to th o cor	e ntinuo e ntinuo

٦

	<i>PING</i> From the pop-up menu and click << to move them to	o the
Action	Selected Members field on the left, and click OK to a <i>Permit</i>	continu
55G520:Juniper-Screen05 5	4.0r1.0 - Microsoft Internet Explorer	-1
<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites	ools Help	
🕒 Back 👻 🕥 👻 🗾	🏠 🔎 Search 🧙 Favorites 🚱 🔗 🌭 🕞 📙 🏭 🦓	
Address 🕘 https://172.16.254.13	2/nswebui.html	io Links (
	Policies (From Untrust To Trust) SSG	520
Home Configuration Network Screening Policies MCast Policies VPNs Objects Reports Wizards Help Logout Teggie Menu	Name (optional) Avaya call signaling Source Address New Address Address Book Entry Main-CLAN Multiple Oestination Address New Address Book Entry Branch-Media Svr Multiple Address Book Entry Branch-Media Svr Multiple Application None WEB Filtering Action Tunnel VPN	ble
	Modify matching bidirectional VPN policy L2TP None Logging at Session Beginning OK Cancel Advanced	
e	Local ir	ntranet
The fallensing 1		

	a	Selection of Multiple Service Entries - Microsoft Internet Explorer	
		Service Entries	
		C-Selected Members → Avaya-Signaling PING (<- Available Members → MGCP MS-AD MS-EXCHANGE MS	
3.	The following P relevant configu Traffic Shaping Guaranteed Ba	olicies (From Untrust To Trust) screen has been abbreviated to ration only. Enter the following information and click OK to compare the second sec	to display omplete.
	Maximum Ban Traffic Priority	dwidth10 kbps2nd priority	
	SSCS20:Juniper-Screen	nDS 5.4.0r1.0 - Microsoft Internet Explorer	
	3 Back • 🕥 • 💌	📓 🕎 🔎 Search 👷 Favorites 🕢 🍰 🖏 🖄 - 🛄 🎇 🖏	
	Agdress an https://172.16.	254.132(nswebui.html Zin Policies (From Untrust To Trust) Si	SG520 ?
	Junipe	r	
	SSG-520 - Home - Configuration - Network - Screening - Policies - MCast Policies - VPNs - Objects - Reports - Reports - Wizards - Help - Logout Teggie Menu	Policing Bandwidth 0 kbps Guaranteed Bandwidth 5 kbps Maximum Bandwidth 10 kbps Traffic Shaping Image: Composition of the state of	
	ð	OK Return Cancel	ocal intranet
1	1		

Name (optional	Avava Media	
Source Address	Main network (select from the drop down box)	
Destination Ad	ress Branch network (select from the drop down box)	
Service	Avaya-RTP (select from the drop down box)	
Action	Permit	
556520:Juniper-Scree	35 5.4.0r1.0 - Microsoft Internet Explorer	_0,
Elle Edit View Favori	s Iools Help	- 🦓
😋 Back + 🕥 - 💌	😰 🏠 🔎 Search 👷 Favorites 🤣 🗟 - 🌭 🔯 - 🛄 鑬 🖄	
Address a https://172.16.	54.132/nowebul.html 💽 🔂 Go 🛛 Lin	ks 📆
	Policies (From Untrust To Trust) SSG520	?
 Configuration Network Screening Policies MCast Policies VPNs Objects Reports Wizards 	C Address Book Entry Main Network V Multiple Destination Address C New Address C Address Book Entry Bronch Network C Address Book Entry Bronch Network C Address Pook Entry	
D. Help Logout Toggie Manu	WEB Filtering Action Permit ▼ Deep Inspection Tunnel VPN None ▼ Modify matching bidirectional VPN policy L2TP None ▼ Logging □ at Session Beginning □	
	OK Cancel Advanced	



6.	Repeat Step 1 to 3 to configu Trust from the From drop of the New button to begin. Use To Untrust). See Step 2 for	ure the security policies from the Trust to Untrust zone. Select down menu and Untrust from the To drop down menu and click se the following parameter to configure the Policies (From Trust r screen display information.
	Name (optional) Source Address Destination Address Service	Avaya call signaling Branch network (select from the drop down box) Main network (select from the drop down box) click on Multiple Select Avaya-Signaling PING
	Action	From the pop-up menu and click << to move them to the Selected Members field on the left, and click OK to continue. <i>Permit</i>
	Use the following traffic sha	aping parameter. See Step 3 for screen display information.
	Traffic Shaping Guaranteed Bandwidth Maximum Bandwidth Traffic Priority Action	checked 5 kbps 10 kbps 2nd priority Permit
7.	Repeat Step 1, 4 and 5 to conserve Select Trust from the From click the New button to begin Trust To Untrust). See Step	nfigure the security policies from the Trust to Untrust zone. I drop down menu and Untrust from the To drop down menu and in. Use the following parameter to configure the Policies (From ep 4 for screen display information.
	Name (optional) Source Address Destination Address Service Action	Avaya Media Branch network (select from the drop down box) Main network (select from the drop down box) Avaya-RTP (select from the drop down box) Permit
	Use the following traffic sha	aping parameter. See Step 5 for screen display information.
	Traffic Shaping Guaranteed Bandwidth Maximum Bandwidth Traffic Priority	checked 700 kbps 1000 kbps 2nd priority
	The Guaranteed and Maxim simultaneous phone calls the was for testing purpose only	um Bandwidth parameter should be based on the number of e link needs to support. The bandwidth chosen in this sample





4.2. Configure the Juniper Networks M7i router

This section shows the necessary steps in configuring the M7i router as shown in the **Figure 1**. The following steps use the Command Line Interface (CLI) offered by the router.

Step	Description
9.	Connect to the M7i. Log in using the appropriate Login ID and Password.
	login:
	Password:
	A prompt similar to the following will appear after successful log in.
	interop@M7I>
10.	Enter configuration mode by typing edit at the prompt.
	interop@M7I> <i>edit</i>
	interop@M7I#

Step	Description
11.	Configure the code-point-aliases and classifier for Avaya VoIP traffic.
	 The alias helps identify the binary DSCP setting by giving it a name. The sample network uses the name "avaya-rtp" to denote DSCP binary value 101110 for media traffic. This is equivalent to the decimal Audio PHB Value of 46 set in Avaya Communication Manager for RTP Media in Section 5, Step 8. The sample network uses the name "avaya-sig" to denote DSCP binary value 100010 for signaling traffic. This is equivalent to the decimal Call Control PHB Value of 34 set in Avaya Communication Manager for signaling in Section 5, Step 8.
	interop@M7I# edit class-of-service code-point-aliases interop@M7I# set dscp avaya-rtp 101110 interop@M7I# set dscp avaya-sig 100010 interop@M7I# exit
	 Define a classifier called "Avaya-voip". The classifier "Avaya-voip" defines the forwarding characteristic of the router based on traffic types. The network is configured to use expedited-forwarding with low loss-priority for "avaya-rtp", and assured-forwarding with low loss-priority for "avaya-sig".
	<pre>interop@M7I# edit class-of-service classifiers interop@M7I# edit dscp avaya-voip interop@M7I# set forwarding-class expedited-forwarding loss-priority</pre>

```
Step
                                       Description
12.
     Configure the scheduler to specify how much bandwidth to allocate for each type of
     traffic queue.
            The sample configuration defines scheduler-maps "voip" and assigns a name
         •
            for each of the 4 queue types.
      interop@M7I# edit class-of-service scheduler-maps
      interop@M7I# edit voip
      interop@M7I# set forwarding-class best-effort scheduler be-sched
     interop@M7I# set forwarding-class expedited-forwarding scheduler ef-
                    sched
      interop@M7I# set forwarding-class assured-forwarding scheduler af-sched
      interop@M7I# set forwarding-class network-control scheduler nc-sched
      interop@M7I# exit
     interop@M7I# exit
            Use the scheduler to define the percentage of bandwidth allocation to each traffic
            queue type. The bandwidth allocation used in these Application Notes is for
            testing only, actual percentage allocation should be based on the maximum
            number of simultaneous calls and codec used.
     interop@M7I# edit class-of-service schedulers
      interop@M7I# edit be-sched
     interop@M7I# set transmit-rate percent 10
     interop@M7I# set buffer-size percent 10
     interop@M7I# set priority low
     interop@M7I# exit
      interop@M7I# edit ef-sched
      interop@M7I# set transmit-rate percent 80
      interop@M7I# set buffer-size percent 80
      interop@M7I# set priority high
     interop@M7I# exit
     interop@M7I# edit af-sched
     interop@M7I# set transmit-rate percent 5
     interop@M7I# set buffer-size percent 5
      interop@M7I# set priority high
      interop@M7I# exit
      interop@M7I# edit nc-sched
      interop@M7I# set transmit-rate percent 5
      interop@M7I# set buffer-size percent 5
     interop@M7I# set priority high
     interop@M7I# exit
13.
     Configure the queue assignment for each traffic type. This is only for the M7i router.
     interop@M7I# edit class-of-service forwarding-classes
     interop@M7I# set queue 0 best-effort
     interop@M7I# set queue 1 expedited-forwarding
     interop@M7I# set queue 2 assured-forwarding
     interop@M7I# set queue 3 network-control
     interop@M7I# exit
```

Step	Description		
14.	Assign the scheduler-map to each interface.		
	 Configure each interface with scheduler-map "voip" using the classifier defined above. interop@M7I# edit class-of-service interfaces fe-0/0/2 interop@M7I# set unit 0 scheduler-map voip 		
	interop@M7I# exit		
	interop@M7I# edit class-of-service interfaces t1-0/3/0		
	interop@M7I# set unit 0 scheduler-map voip		
	interop@M7I# exit		
15.	Configure the Ethernet and T1 interfaces.		
	• Configure the Ethernot interface to use the scheduler		
	Configure the Ethernet Interface to use the scheduler.		
	• Assign an IP address to the interface.		
	<pre>interop@M7I# edit int fe-0/0/2 interop@M7I# set per-unit-scheduler interop@M7I# set unit 0 family inet address 172.28.10.253/24 interop@M7I# evit</pre>		
	Interopem/i# exit		
	• Configure the T1 interface to use the scheduler.		
	• Configure the T1 interface timing, encapsulation, and timeslots.		
	• Configure the clocking to be internal because the two routers are connected		
	back-to-back with each other. The default clocking is external.		
	• Assign an IP address to the interface.		
	interop@M7I# edit int t1-0/3/0		
	interop@M7I# set per-unit-scheduler		
	interop@M7I# set clocking internal		
	interop@M7I# set t1-options timeslots 1-24		
	interop@M7I# set unit 0 family inet address 192.168.3.17/28		
	interop@M/1# exit		
16.	Configure the routing options for the router. The sample configuration uses static routes.		
	interop@M7i# edit routing-options static interop@M7i# route 172.28.40.0/24 next-hop 192.168.3.30 interop@M7i # exit		
17.	Save the changes.		
	interop@M7i # <i>commit</i>		

5. Configure Avaya Communication Manager

This section shows the necessary steps in configuring Avaya Communication Manager. For detailed information on the installation, maintenance, and configuration of Avaya Communication Manager, please consult reference [1], [2], [3], and [4]. The following steps describe the configuration of Avaya Communication Manager at the Main site. Repeat these steps at the Avaya Communication Manager at the Branch site unless otherwise noted.

Step		Description		
1.	Add a new station for an Avaya IP Telephone using the add station command. Make sure the following fields are configured.			
	•	Extension:	22022	(Extension number for the Avaya Telephone)
	•	Туре:	4610	(Avaya Telephone type used for this extension)
	•	Port:	IP	(Type of connection for the Avaya Telephone)
	•	Security Code:	123456	(Security code used by the Avaya Telephone to register with Avaya Communication Manager)
	•	Direct IP-IP Audio Connections:	у	(Enable Shuffling)

The screen below shows station extension 22022. Repeat this step for each station.

add station 22022	Pag	ge 1 of 4
	STATION	
Extension: 22022	Lock Messages? n	BCC: 0
Type: 4610	Security Code: 123456	TN: 1
Port: IP	Coverage Path 1:	COR: 1
Name: Room 18	Coverage Path 2:	COS: 1
	Hunt-to Station:	
STATION OPTIONS		
Loss Group: 19	Personalized Ringing Patt	tern: 1
-	Message Lamp	Ext: 22022
Speakerphone: 2-	Mute Button Enal	bled? y
Display Language: er	ish	-
Survivable GK Node Name:		
Survivable COR: ir	rnal Media Complex	Ext:
Survivable Trunk Dest? v	IP SoftPl	hone? n
	Customizable La	bels? y

Step	Description			
	change station	22022	Page 2 of 4	
			STATION	
	FEATURE OPTIONS			
	LWC	Reception: spe	Auto Select Any Idle Appearance? n	
	LWC A	ctivation? y	Coverage Msg Retrieval? y	
	LWC Log Exter	nal Calls? n	Auto Answer: none	
	CD	R Privacy? n	Data Restriction? n	
	Redirect Not	ification? y	Idle Appearance Preference? n	
	Per Button Rin	g Control? n	Bridged Idle Line Preference? n	
	Bridged Call	Alerting? y	Restrict Last Appearance? y	
	Active Statio	n Ringing: single	Conf/Trans on Primary Appearance? n	
			EMU Login Allowed? n	
	Н.320 С	onversion? n	Per Station CPN - Send Calling Number?	
	Service	Link Mode: as-needed		
	Multim	edia Mode: enhanced		
	MWI Served	User Type:	Display Client Redirection? n	
	A	UDIX Name:	Select Last Used Appearance? n	
			Coverage After Forwarding? s	
			Direct IP-IP Audio Connections? y	
	Emergency Loca	tion Ext: 22022	Always Use? n IP Audio Hairpinning? y	
2.	Add the S8300 M	edia Server IP addre	ess located at the Branch Site into the Avava	
	Communication N	lanager using the cr	ange node-names ip command. The screen	
	below shows the e	entry for the Branch	Site as Branch-ACM with IP address of	
	172 28 40 5	j		
	1/2.20.40.5.			
	change node-nam	es ip	Page 1 of 1	
		т	P NODE NAMES	
	Name	TP Address	Name IP Address	
	Branch-ACM	172.28.40.5	Hame II Hadrebb	
	clan	172 28 10 7		
	default		· · ·	
	modero	172 20 10 0		
	medpro	172.20 .10 .0	· · ·	
	Procr	1/2.20 .10 .5	· · ·	
		• • •	· · ·	
			· · ·	
		• • •	· · ·	

Step	Description			
3.	Configure a signaling group for the H.323 trunk between the Avaya Communication			
	Manager at the Main and Branch Site. Make sure the following fields are configured.			
	~ ~	1		
	• Group Type:	h.323	(Signaling type used)	
	• Trunk Group for Channel	Selection:	(This value needs to be completed after Step 4 below has been completed)	
	• Near-end Node Name:	clan	(This is the clan name defined in Step 2)	
	• Near-end Listen Port:	1720	(Default port number for H.323 signaling)	
	• Far-end Node Name:	Branch-	ACM (Node name for Branch Site system defined in Step 2)	
	• Far-end Listen Port:	1720	(Default port number for H.323 signaling)	
	• Far-end Network Region:	1	(Region 1 was used throughout this	
			sample configuration)	
	display signaling-group 1	GNALING GROUP	Page 1 of 5	
	Group Number: 1 Grou	p Type: h.323	3	
	Remote	Office? n	Max number of NCA TSC: 0	
	тр	SBS? n Video? n	Max number of CA TSC: 0 Trunk Group for NCA TSC:	
	Trunk Group for Channel Sel	ection: 1	fram broup for her foc.	
Supplementary Service Protocol: a T303 Timer(sec): 10		Network Call Transfer? n		
	Near-end Node Name: clan Far-end Node Name: Branch-ACM Near-end Listen Port: 1720 Far-end Listen Port: 1720 Far-end Network Perion: 1 Far-end Network Perion: 1			
	LRQ Required? n	Calls	Share IP Signaling Connection? n	
	RRQ Required? n Media Encryption? v	B	vpass If IP Threshold Exceeded? n	
		-1	H.235 Annex H Required? n	
	DTMF over IP: out-of-band	l I	Direct IP-IP Audio Connections? y	
			Interworking Message: PROGress	
		DCP/Ar	nalog Bearer Capability: 3.1kHz	

Step	Description			
4.	Configure an H.323 trunk group. Use the add trunk-group command to create a new			
	trunk group.			
	• Group Type: isdn • TAC: 101 (User essigned)			
	• IAC: 101 (User assigned) • Carrier Medium: H 323 (Type of trunk)			
	Member Assignment Method: auto			
	• Signaling Group: 1 (Signaling group number created in			
	Step 3)			
	• Number of Members: 5 (Number of members for this trunk			
	group)			
	• Service Type: tie			
	add trunk-group 1 Page 1 of 21			
	TRUNK GROUP			
	Group Number: 1 Group Type: isdn CDR Reports: y			
	Direction: two-way Outgoing Display? n Carrier Medium: H.323			
	Dial Access? n Busy Threshold: 255 Night Service: Queue Length: 0			
	Service Type: tie Auth Code? n Member Assignment Method: auto			
	Signaling Group: 1 Number of Members: 5			
5.	Configure the dial plan to route calls to the Branch Site. Use the change dialplan			
	analysis command to configure calls to extension range 4xxxx. The following shows any 5 digit number starting with 4 uses the "aar" Call Type ARS/AAR Dialing without			
	FAC was enabled in the sample configuration. The "display system-parameters			
	customer-options" command can be used to verify if this option is enabled.			
	change dialplan analysis Page 1 of 12 DIAL PLAN ANALYSIS TABLE			
	Percent Full: 1			
	Dialed Total Call Dialed Total Call Dialed Total Call			
	1 3 dac			
	2 5 ext 221 5 aar			
	3 5 aar 4 5 aar			
	5 5 ext			
	9 3 Iac			
1				

Step	Description			
	display system-parameters customer-options Page 3 of 10			
	OPTIONAL FEATURES			
	Abbreviated Dialing Enhanced List? n Audible Message Waiting? n Access Security Gateway (ASG)? n Authorization Codes? n Analog Trunk Incoming Call ID? n Backup Cluster Automatic Takeover? n A/D Grp/Sys List Dialing Start at 01? n CAS Branch? n Answer Supervision by Call Classifier? n CAS Main? n ARS? y Change COR by FAC? n ARS/AAR Partitioning? y Computer Telephony Adjunct Links? n ARS/AAR Partition? y Cvg Of Calls Redirected Off-net? n ASAI Link Core Capabilities? n DCS (Basic)? n ASAI Link Plus Capabilities? n DCS Call Coverage? n Async. Transfer Mode (ATM) PNC? n DCS with Rerouting? n ATM WAN Spare Processor? n Digital Loss Plan Modification? n ATMS? n DS1 MSP? n			
	Attendant Vectoring? n DS1 Echo Cancellation? n			
6.	Configure AAR to use the appropriate route pattern using the change aar analysis			
	command. The following shows that when a 5 digits number starting with A is dialed			
	Desets Dettern 1 is seed.			
	Route Pattern I is used.			
	change aar analysis 4 Page 1 of 2			
	Percent Full: 1			
	Dialed Total Route Call Node ANI String Min Max Pattern Type Num Read			
	4 5 5 1 aar n			
	5 7 7 999 aar n			
7	Configure the Route Pattern using the change route-nattern command. The following			
<i>'</i> •	shows calls using route pattern 1 are routed to trunk group 1 configured in Stap 4. Set			
	shows cans using foule-patient 1 are fouled to trunk group 1 configured in Step 4. Set			
	FRL to 0.			
	along a set to a 1 of 0			
	change route-pattern 1 Page 1 or 3			
	Change route-pattern I Page I or 3 Pattern Number: 1 Pattern Name: SCCAN? n Secure SIP? n			
	Change Foute-pattern I Page I of 3 Pattern Number: 1 Pattern Name: SCCAN? n Secure SIP? n Grp FRL NPA Pfx Hop Toll No. Inserted DCS/ IXC			
	Change Foute-pattern 1 Page I of 3 Pattern Number: 1 Pattern Name: SCCAN? n Secure SIP? n Grp FRL NPA Pfx Hop Toll No. Inserted DCS/ IXC No Mrk Lmt List Del Digits QSIG			
	Change Foute-pattern 1 Page 1 of 3 Pattern Number: 1 Pattern Name: SCCAN? n Secure SIP? n Grp FRL NPA Pfx Hop Toll No. Inserted DCS/ IXC No Mrk Lmt List Del Digits QSIG Dgts Intw			
	Change Foute-pattern 1 Page 1 of 3 Pattern Number: 1 Pattern Name: SCCAN? n Secure SIP? n Grp FRL NPA Pfx Hop Toll No. Inserted DCS/ IXC No Mrk Lmt List Del Digits QSIG Dgts Intw 1: 1 0 n 2: n user			
	Change Foute-pattern 1 Page 1 of Pattern Number: 1 Pattern Name: SCCAN? n Secure SIP? n Grp FRL NPA Pfx Hop Toll No. Inserted DCS/ IXC No Mrk Lmt List Del Digits QSIG Dgts Intw 1: 1 0 n 2: n user 3: n user			
	Change Foute-pattern 1 Page 1 of 3 Pattern Number: 1 Pattern Name: SCCAN? n Secure SIP? n Grp FRL NPA Pfx Hop Toll No. Inserted DCS/ IXC No Mrk Lmt List Del Digits QSIG Dgts Intw 1: 1 0 n 3: n user			

Step	Description					
8.	Configure the IP network region using the change ip-network-region command. Note					
	the values for UDP Port Min, UDP Port Max, Call Control PHB Value and Audio					
	PHB Value. These values are needed to configure the security policy in the SSG520.					
	The IP NETWORK REGION form also specifies which Codec Set will be used.					
	-					
	change ip-network-region 1 Page 1 of 19					
	Region: 1					
	Location: Authoritative Domain:					
	MEDIA PARAMETERS Intra-region IP-IP Direct Audio: yes					
	Codec Set: 1 Inter-region IP-IP Direct Audio: yes					
	UDP Port Max: 3029					
	DIFFSERV/TOS PARAMETERS RTCP Reporting Enabled? y					
	Audio PHB Value: 46 Use Default Server Parameters? y					
	Video PHB Value: 26					
	Call Control 802.1p Priority: 6					
	Audio 802.1p Priority: 6 Video 802.1p Priority: 5 AUDIO RESOURCE RESERVATION DARAMETERS					
	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					
9.	Configure the appropriate Audio Codec using the change ip-codec command. The					
	following shows ip-codec-set 1 using either G.729B. G.711 codec was also verified					
	during compliance testing.					
	change ip-codec-set 1 Page 1 of 2					
	IP Codec Set					
	Codec Set: 1					
	Audio Silence Frames Packet					
	Codec Suppression Per Pkt Size(ms)					
	2:					
	3:					
	5:					
	6:					
	Media Engrantion					
	1: none					
	2:					

Step	Description			
10.	Save the configuration using the save translation command.			
	save translation SAVE TRANSLATION			
	Command Completion Status	Error Code		
	Success	0		
11.	Repeat Steps 1-10 in this section for Avaya Communication Manager a to complete the configuration. Make sure the appropriate IP address in entered when configuring the Branch Site. At the Branch site, the "nea Avaya S8300 Media Server and the "far end" is the C-LAN at the Main	It the Branch Site Iformation is Ir end" is the In site.		

6. Interoperability Compliance Testing

The interoperability compliance testing focused on assessing the ability of the Juniper Networks routers in supporting an Avaya IP Telephony infrastructure consisting of Avaya Communication Manager and Avaya IP Telephones. A data traffic generator and a voice traffic generator were used to simulate background traffic and additional voice traffic in a typical network environment.

6.1. General Test Approach

Quality of Service was verified by injecting simulated data traffic into the network using a traffic generator while calls were being established and maintained using the Avaya IP Telephones. The Juniper Networks SSG520 was configured to perform as a DHCP Server to test DHCP option 176 used by the Avaya IP Telephones. DTMF detection was tested using the Meet-me conference configured in the S8300 Media Server.

The objectives were to verify the Juniper Networks SSG520 supports the following:

- QoS (Quality of Service) for VoIP traffic through traffic shaping.
- Point-to-Point Protocol
- DHCP Server support for Option 176
- Basic calling (e.g. call, transfer, conference, DTMF detection)

6.2. Test Results

The Juniper Networks SSG520 successfully achieved all objectives. Quality of Service for VoIP traffic was maintained throughout the testing in the presence of competing simulated traffic. The Avaya IP Telephones successfully received appropriate IP addresses from the SSG520 router via DHCP and registered with the correct server.

7. Verification Steps

The following steps may be used to verify the configuration:

- Place inter-site calls between the Avaya IP Telephones.
- Use the "show interface queue" command on the Juniper router to verify that VoIP traffic is being prioritized correctly.
- Use the "show class-of-service forwarding-table" command on the Juniper routers to verify that the appropriate bandwidth is being assigned on the interfaces.

8. Conclusion

These Application Notes described the administration steps required to configure Juniper Networks Secure Services Gateway SSG520 and M7i routers to support Avaya Communication Manager and Avaya IP Telephones.

9. Support

For technical support on the Juniper Networks product, contact Juniper Networks JTAC at (888) 314-JTAC, or refer to <u>http://www.juniper.net</u>.

10. Additional References

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

- [1] Administrator Guide for Avaya Communication Manager, Doc # 03-300509, Issue 2.1, May 2006
- [2] Avaya Communication Manager Advanced Administration Quick Reference, Doc # 03-300364, Issue 2, June 2005
- [3] Administration for Network Connectivity for Avaya Communication Manager, Doc # 555-233-504, Issue 11, February 2006
- [4] Avaya IP Telephony Implementation Guide, May 1, 2006

Product documentation for Juniper Networks products may be found at http://www.Juniper.net

- [5] CLI User Guide (JUNOS Internet Software for J-series, M-series, and T-series Routing Platform) Release 7.6, Part Number 530-015682-01, Revision 1
- [6] JUNOS Internet Software for J-series, M-series, and T-series Routing Platforms, Class of Service Configuration Guide Release 7.6, Part Number 530-015688-01, Revision 1
- [7] JUNOS Internet Software for J-series, M-series, and T-series Routing Platforms, Network Interfaces Configuration Guide Release 7.6, Part Number 530-015687-01, Revision 1
- [8] JUNOS Internet Software for J-series, M-series, and T-series Routing Platforms, Services Interfaces Configuration Guide Release 7.6, Part Number 530-015687-01, Revision 1
- [9] *Concepts & Examples ScreenOS Reference Guide*, Part Number 530-015768-01, Release 5.4.0, 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 name and filename, located in the lower right corner, directly to the Avaya Developer*Connection* Program at devconnect@avaya.com.