

Avaya Solution & Interoperability Test Lab

Application Notes for Configuring a SonicWALL VPN with an Avaya IP Telephony Infrastructure - Issue 1.0

Abstract

These Application Notes describe the steps for configuring SonicWALL's VPN to support an Avaya IP Telephony infrastructure consisting of a Main site with Avaya Communication Manager, and two branch sites. During compliance testing, H.323 telephone calls traversing the VPN tunnel were successfully established and maintained while competing non-VoIP traffic queued according to bandwidth reservation defined in the SonicWALL devices. In addition, non-VoIP network traffic using Network Address Translation (NAT) outside of the VPN tunnel was successfully demonstrated. 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

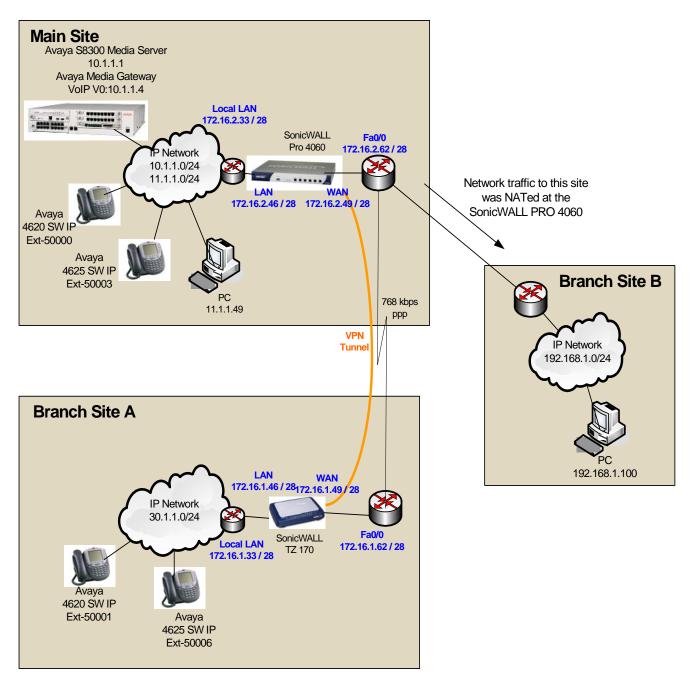
These Application Notes describe a compliance-tested solution comprised of Avaya Communication Manager, Avaya IP Telephones, and SonicWALL Unified Threat Management (UTM) devices. The SonicWALL UTM devices tested were the SonicWALL PRO 4060 and TZ 170.

The sample configuration simulates an enterprise with a Main Site, Branch Site A, and Branch Site B. The Main Site and Branch Site A are connected via a 768Kbps PPP WAN link. An Avaya S8300 Media Server at the Main Site is responsible for supporting Avaya IP telephones at the Main Site and Branch Site A. A SonicWALL UTM device is installed at these two sites between the WAN router and the local IP networks. Although the SonicWALL UTM device is capable of functioning as a firewall, that was not the focus of the compliance testing. A single VPN tunnel was established between the SonicWALL PRO 4060 at the Main Site and the TZ 170 at the Branch Site A. The SonicWALL UTM devices were configured to automatically recognize RTP traffic flow negotiated by the H.323 protocol and provide guaranteed bandwidth for the call. Guaranteed bandwidth for two simultaneous Avaya VoIP telephone calls was configured in the SonicWALL UTM devices.

Branch Site B simulated a PC only user site with no Avaya VoIP requirement. This site was used to demonstrate and verify that SonicWALL Network Address Translation does not interfere with Avaya VoIP traffic traversing the VPN tunnel between the Main Site and Branch Site A.

1.1. Configuration

Figure 1 illustrates the configuration used in these Application Notes. All Avaya IP telephones are registered with Avaya Communication Manager in the Main Site. A 768K PPP link simulating a WAN link connects the Main Site and Branch Site A while the SonicWALL UTM establishes the VPN tunnel over this link. A separate 10Mbps link simulating a WAN link connects the Main Site and Branch Site B. All data traffic destined to Branch Site B is NAT to the SonicWALL PRO 4060 WAN interface IP address.





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

2. Equipment and Software Validated

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

Equipment	Software/Firmware
Avaya S8300 Media Server with G700 Media	Avaya Communication Manager 3.0.1
Gateway	(R0.13x.00.0.346.0)
Avaya 4620SW IP Telephones (H.323)	2.2.3
Avaya 4625SW IP Telephones (H.323)	2.5
SonicWALL Pro4060	SonicOS Enhanced 3.2.0.0-20e
SonicWALL TZ170	SonicOS Enhanced 3.2.0.0-20e

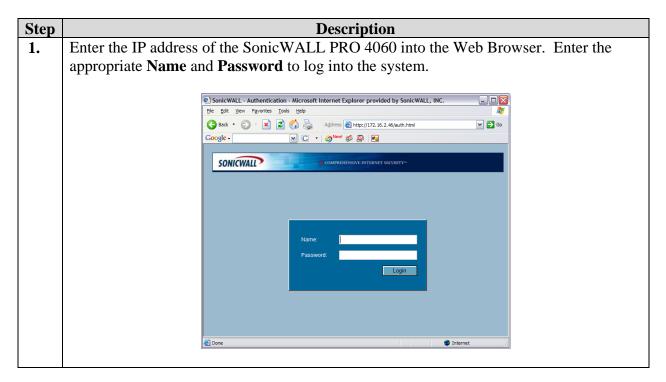
3. SonicWALL Unified Threat Management

The SonicWALL Unified Threat Management (UTM) devices SonicWALL PRO 4060 and TZ 170, were used to establish a VPN tunnel between the Main Site and Branch site A and provide Network Address Translation between the Main Site and Branch Site B. The following steps outline the configuration for SonicWALL Unified Threat Management devices and the VPN tunnel.

The steps in this section depict the screen displays for the SonicWALL PRO 4060 at the Main Site. Repeat these steps for the SonicWALL TZ 170 at Branch Site A with the appropriate IP address information.

3.1. General SonicWALL UTM Configuration

This section presents the SonicWALL VPN tunnel configuration.

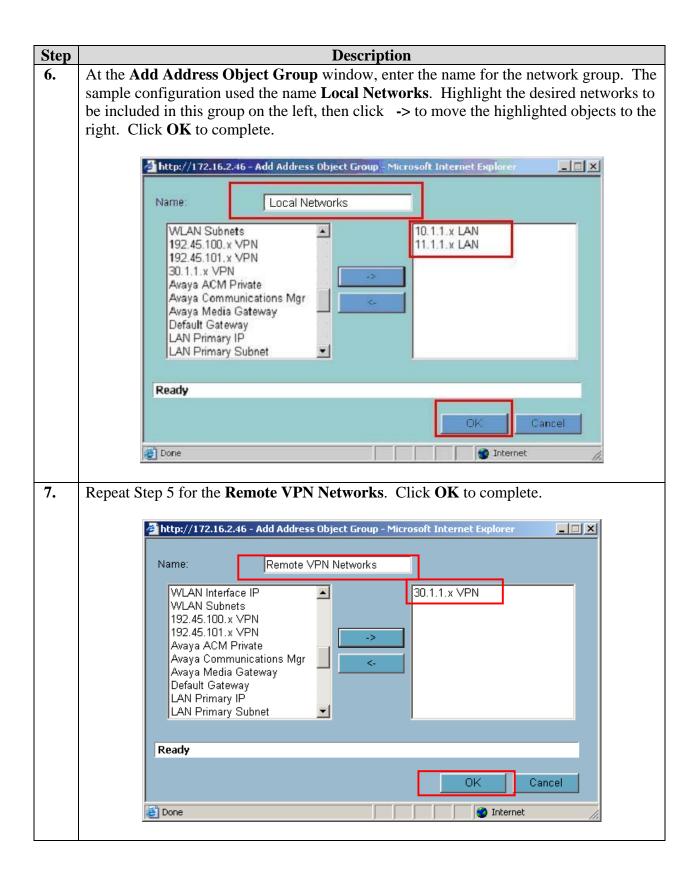


Description The System>Status screen is displayed after successfully logging on. Click on the												
Network tab on	twork tab on the left to expand it.											
	T											
	SonicWALL - Administration for 0006B1029C38 - Microsoft Internet Explorer provided by SonicWALL, INC.											
<u>File E</u> dit <u>V</u> iew F <u>a</u> vori	Ele Edit View Favorites Iools Help											
🕞 Back 🝷 💮 🕤	🔹 😰 🏠 🍓 🛛 A <u>d</u> a	dress 🕘 http://172.16.2.46/main.html				💌 🔁 G						
Google -	▼ G • Ø	New! 🎲 🔊 🛛										
SONICWALL	COMPR	EHENSIVE INTERNET SECURITY~										
System	1											
🕿 Status	System > Status				Wizards	?						
Licenses												
Administration												
Certificates	System Messages • WARNING: A rule ex	tists allowing HTTP/HTTPS management from	the WAN. This is a potential v	ulnerability. Choo	ose a good password	_						
💼 Time	The password hasn		ale walk mie ie u potential v	amorability, chot	soo a good password.							
🖿 Schedules		ied a DNS server address; some functions wil	Il not operate properly.									
💼 Settings												
💼 Diagnostics												
💼 Restart	System Information Model:	PRO 4060	Security Services	Status								
	Serial Number:	0006B1029C38	Service Name	<u>Status</u>		2						
	Authentication Code		Nodes/Users		Unlimited Nodes							
	Firmware Version:	SonicOS Enhanced 3.2.0.0-20e	VPN	Licensed								
	ROM Version:	SonicROM 3.1.0.11	Global VPN Client		- 1010 Licenses (0 in use)							
	CPU (10s average):	0.00% - 2.0GHz Intel Processor	CFS (Content Filter)	Licensed								
	Total Memory:	256MB RAM, 64MB Flash	Network Anti-Virus	Licensed								
	System Time:	01/12/2006 07:39:38	Gateway Anti-Virus	Licensed								
	Up Time:	0 Days 01:22:55	Anti-Spyware	Licensed								
Network	Current Connections		Intrusion Prevention	Licensed								
SonicPoint	Last Modified By:	10.1.1.205:X0 01/12/2006 07:31:02	E-Mail Filter	Licensed								
P			ViewPoint	Licensed								
Firewall	Registration Code:	ABSK7EL8										
Firewall VoIP		ABSK7EL8	Network Interfaces									
Firewall VoIP VPN	Latest Alerts		Namo	IP Address	Link Status	>						
Firewall VoIP VPN Users	Latest Alerts Date/Time	Message		IP Address 172.16.2.46	<u>Link Status</u> 100 Mbps full-duplex	Ð						
Firewall VoIP VPN Users Hardware Failover	Latest Alerts Date/Time 01/12/2006 07:25:23	Message IPSec Replay Detected	Name			Ð						
Firewall VoIP VPN Users Hardware Failover Security Services	Latest Alerts Date/Time 01/12/2006 07:25:23 01/12/2006 07:24:16	Message IPSec Replay Delected IPSec Replay Detected	X0 (LAN)	172.16.2.46 172.16.2.49	100 Mbps full-duplex	Đ						
Firewall VoIP VFN Users Hardware Failover Security Services Log	Latest Alerts Date/Time 01/12/2006 07:25:23 01/12/2006 07:24:16 01/12/2006 07:23:15	Message IPSec Replay Detected IPSec Replay Detected IPSec Replay Detected	Name Image: State of the	172.16.2.46 172.16.2.49 0.0.0.0	100 Mbps full-duplex 100 Mbps full-duplex	2						
Firewall VoIP VFN Users Hardware Failover Security Services Log Wizards	Latest Alerts Date/Time 01/12/2006 07:25:23 01/12/2006 07:24:16 01/12/2006 07:23:15 01/12/2006 07:23:05	Message IPSec Replay Detected IPSec Replay Detected IPSec Replay Detected IPSec Replay Detected	Name X0 (LAN) X1 (WAN) X2 (Unassigned)	172.16.2.46 172.16.2.49 0.0.0.0 0.0.0.0	100 Mbps full-duplex 100 Mbps full-duplex No link	Đ						
Firewall VoIP VPN Users Hardware Failover Security Services Log Wizards Help	Latest Alerts Date/Time 01/12/2006 07:25:23 01/12/2006 07:24:16 01/12/2006 07:23:15	Message IPSec Replay Detected IPSec Replay Detected IPSec Replay Detected IPSec Replay Detected	Name X0 (LAN) X1 (WAN) X2 (Unassigned) X3 (Unassigned)	172.16.2.46 172.16.2.49 0.0.0.0 0.0.0.0 0.0.0.0	100 Mbps full-duplex 100 Mbps full-duplex No link No link	Đ						
Firewall VoIP VFN Users Hardware Failover Security Services Log Wizards Help Logout	Latest Alerts Date/Time 01/12/2006 07:25:23 01/12/2006 07:24:16 01/12/2006 07:23:15 01/12/2006 07:20:05 01/12/2006 07:18:55	Message IPSec Replay Detected IPSec Replay Detected IPSec Replay Detected IPSec Replay Detected	Name State X0 (LAN) State X1 (WAN) State X2 (Unassigned) State X3 (Unassigned) State X4 (Unassigned)	172.16.2.46 172.16.2.49 0.0.0.0 0.0.0.0 0.0.0.0	100 Mbps full-duplex 100 Mbps full-duplex No link No link No link	Đ						
Firewall VoIP VPN Users Hardware Fallover Security Services Log Wizards Help Logout	Latest Alerts Date/Time 01/12/2006 07:25:23 01/12/2006 07:24:16 01/12/2006 07:23:15 01/12/2006 07:23:05	Message IPSec Replay Detected IPSec Replay Detected IPSec Replay Detected IPSec Replay Detected	Name State X0 (LAN) State X1 (WAN) State X2 (Unassigned) State X3 (Unassigned) State X4 (Unassigned)	172.16.2.46 172.16.2.49 0.0.0.0 0.0.0.0 0.0.0.0	100 Mbps full-duplex 100 Mbps full-duplex No link No link No link	Đ						

p		Desc	ription							
	Under the expanded N	etwork tab on the lef	t, select Address	s Obje	ects.	Click the A				
	button in the Address	Objects panel to disp	olay the Add Ad	dress	Obje	ects pop-up				
	window.				v					
	SonicWALL - Administration for 0006B1029C38 - Microsoft Internet Explorer Image: Constraint of Constraints Eile Edit View Favorites Iools Help SonicWALL - Administration for 0006B1029C38 - Microsoft Internet Explorer Image: Constraint of Constraints Image:									
	Address http://172.16.2.46	/main.html			-	🔁 Go 🛛 Links 📆 🔹				
	SONICWALL	COMPREHENSIVE INTERN	NET SECURITY**							
	System	View Style: O All Address Objects	Custom Address Objects	Default A	ddress O	bjects				
	interfaces	📕 🗉 # Name	Address Detail	Туре	Zone	Configure				
	🖿 WAN Failover & LB	1 Remote VPN Networks		Group		۵ 😚				
	💼 Zones	🗖 🛨 2 Local Neworks		Group		8 B 🔰				
	🕿 Address Objects	Add Group Delete				Delete All				
	Routing									
	 NAT Policies ARP DHCP Server 	Address Objects		Items 1	to 9 ((of9) KI < ▷ KI				
	💼 IP Helper	🔲 # Name	Address Detail	Type	Zone	Configure				
	Web Proxy Dynamic DNS	🗖 1 10.1.1.x LAN	10.1.1.0/255.255.255.0	Network	LAN	80				
		2 LAN Router	172.16.2.33/255.255.255.255	Host	LAN	80 B				
	SonicPoint	🗖 3 11.1.1.x LAN	11.1.1.0/255.255.255.0	Network	LAN	80 🕅				
	Firewall	🗖 4 30.1.1.xVPN	30.1.1.0/255.255.255.0	Network	VPN	806				
	VoIP	□ 5 192.45.101.x VPN	192.45.101.0/255.255.255.0	Network	VPN	80 6				
	Users	6 192.45.100.x VPN	192.45.100.0/255.255.255.0	Network	VPN	8				
	Hardware Failover	🗖 7 Avaya Communications Mgr	10.1.1.1/255.255.255.255	Host	LAN	80 6				
	Security Services	🗖 8 Avaya Media Gateway	10.1.1.4/255.255.255.255	Host	LAN	80				
	Log Wizards	9 Avaya ACM Private	10.1.1.1/255.255.255.255	Host	LAN	8				
	Help	Add Delete			I	Delete All				
	Logout									
	Status: Ready									
	e				🥑 Ir	nternet				

Step]	Description	n	
4.	Define all the IP netwo after entering the infor configuration that need follows:	mation. There a	re three IP	networks and t	wo hosts in the sample
	Name:	Zone Assignment	Туре	Network	Netmask
	10.1.1.x	LAN	Network	10.1.1.0	255.255.255.0
	10.1.1.x 11.1.1.x	LAN	Network		255.255.255.0
	30.1.1.x	VPN	Network		255.255.255.0
	LAN Router	LAN	Host		
	Avaya	LAN	Host		N/A
	Media				
	Repeat step 3 and 4 un			nosts above are	defined.
		Name:	10.1.1.x		
		Zone Assignment:	LAN	~	
		Туре:	Network	~	
		Network:	10.1.1.0		
		Netmask:	255.255.255.0	1	
		Ready	ОК	Cancel	
		Cone Done	9 I	nternet 🥂	

Step	Description												
5.	Define the group where the Address Objects belong. In the sample configuration, the												
	were two groups. The Local Networks was composed of all the locally connected IP												
	networks, and the Remote VPN Networks was composed of all the IP networks on t												
	other end of the VPN		was composed o	1 411 0	10 11	neevoon							
		tunnen.											
	Click Add Group to display the Add Address Object Group pop-up windows.												
	Click Add Group to display the Add Address Object Group pop-up windows.												
	SonicWALL - Administration for 000681029C38 - Microsoft Internet Explorer												
	File Edit View Favorites		net Explorer										
	G Back - 🕞 - 🗙	🗿 🚮 🔎 Search 🔶 Favorites	🚱 🖂 - 🤮 💽 - 🗖	1 🛍 👌	8								
	Address 🕘 http://172.16.2.4	5/main.html		, 1		🗲 Go 🛛 Links 🍳	1						
	SONICWALL	COMPREHENSIVE INTER	NET CECHDITVIN										
		COMPREMENSIVE INTER											
	System Network	View Style: C All Address Objects	Custom Address Objects	Default A	ddress O	bjects							
	interfaces	🔲 🗉 # Name	Address Detail	Туре	Zone	Configure							
	🖿 WAN Failover & LB	□ 1 Remote VPN Networks		Group		6 🎸							
	💼 Zones 💼 DNS	🗖 🗉 2 Local Neworks		Group		6 🞸							
	Address Objects	Add Group Delete				Delete All							
	💼 Routing												
	NAT Policies ARP	Address Objects		Items 1	to 9 (i	of 9) 🕅 🔍 🕨 🕅							
	DHCP Server			-	-	0.5							
	💼 IP Helper 💼 Web Proxy	■ # Name	Address Detail	Type	Zone	Configure							
	💼 Dynamic DNS		10.1.1.0/255.255.255.0	Network									
		2 LAN Router	172.16.2.33/255.255.255.255		LAN	80 B N A							
	SonicPoint	□ 3 11.1.1.x LAN	11.1.1.0/255.255.255.0	Network		80 10 No							
	Firewall	4 30.1.1.x VPN	30.1.1.0/255.255.255.0	Network		80 B N A							
	VPN	5 192.45.101.x VPN	192.45.101.0/255.255.255.0	Network		80 B							
	Users	6 192.45.100.x VPN	192.45.100.0/255.255.255.0	Network		80							
	Hardware Failover Security Services	7 Avaya Communications Mgr		Host	LAN	80 B							
	Log	🗖 8 Avaya Media Gateway	10.1.1.4/255.255.255.255	Host	LAN	806							
	Wizards	🔲 9 Avaya ACM Private	10.1.1.1/255.255.255.255	Host	LAN	80 6							
	Help	Add Delete				Delete All							
	Logout												
	Status: Ready												
	10 A				🔮 Ir	iternet	11.						



Description										
Define the routing configuration of the SonicWALL PRO 4060 by clicking on Rou										
under the Network tab on the left. Click Add under the Route Policies panel to di										
the Add Route Policy pop-up windows.										
	🛃 SonicWALL - Adminis	stration for 0006B1029C38 - N	icrosoft Internet Explo	rer provi	ded by SonicWALL	., INC.				_ □ 🛛
	Eile Edit View Favorite									//
		 ▲ ddress ▲ ▲ ddress ▲ ▲ C ✓ Ø^{New!} % 	http://172.16.2.46/main.h	tml						🚩 🄁 Go
	SONICWALL		E INTERNET SECURITY**							
	System	11								
	Network	Network > Routing								?
	Interfaces WAN Failover & LB	Route Advertisemen								
	💼 Zones 💼 DNS	Routing Mode: Simple RIF	Advertisement 💌							
	 Address Objects Routing 	Interface (Zone)			Status			Config	jure	
	MAT Policies	X0 (LAN) X1 (WAN)			Disabled Disabled			& &		
	DHCP Server	X2 (N/A)			Disabled			8		
	IP Helper Web Proxy	X3 (N/A)			Disabled			8		
1	💼 Dynamic DNS	X4 (N/A) X5 (N/A)			Disabled Disabled			- 89 - 89		
										=
		Route Policies						Ite	ems 1 to	o6 (of 6) KI ⊲ ▷ KI
		View Style: All Policies	Ocustom Policies	efault Poli	des					
	SonicPoint	# Source	Destination	Servio	e Gateway	Interfa	ce Metri	c Priori	ty Comme	ent Configure
	Firewall VoIP	🗆 1 Any	255.255.255.255/32	Any	0.0.0.0	X0	20	1	Ø	¥ 6
	VPN	2 Any	Default Gateway	Any	0.0.0.0	X1	20	2	9	8
	Users Hardware Failover	3 Any 4 Any	LAN Primary Subnet WAN Primary Subnet	Any Any	0.0.0.0	X0 X1	20 20	3	9	
	Security Services	5 WAN Primary Subne		Any	Default Gateway		20	4 5	9	¥8
	Wizards	6 Anv	0.0.0/0	Any	172.16.2.62	X1	20	6	ø	۵ 🐨
	Help Logout	Add De	ete							Delete All
	Status: Ready									
	é									Internet
_	~									
De	fine a route po	olicy as shown	:							
		v source destin							rvice	use <i>LAN</i>
Ro	uter gateway	reachable fron	n interface	X0	with a m	etric	of 1 .	•		
Lo	cal Networks	and LAN Rou	<i>ter</i> were de	efine	d in ster	5 6 ai	nd 4 a	abov	e res	pectively.
					1					
		(e) http	://172.16.2.46 - A	id Route	Policy - Micros	(a) (
			General							
			oute Policy Setti	nge						
		R								
			sace Any		100					
		9. D		worka	2 P					
		9 0 9 0	inter Any Internation Local Ne Internation Any Internation LAN Rec	25.3500	2					
		a D a tr	surce Any estimation Local Ne intos Any	25.3500	×					
		9. 0. 0. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1.	sarce Any refination Local Ne mice Any Reway LAN Rec enface X0	25.3500	2		I			
		a 5 4 9 1 1 1 1 0	seco Any rotration Local Ne revoc Any Revoy LAN Rou Reflace X0 afric 1	flør	×					
		a 5 4 9 1 1 1 1 0	seco Any estimation: Local Ne nece Any tervay LAN Ro, entrace X0 abit: 1 chastie route when t	flør	i v v v	ed				
			sece Any estimation Local Ne nece Any steway LAN Ro. entrace X0 able: 1 chastle route when 1 ady	flør	×					

3.2. Configure the VPN tunnel for the SonicWALL UTM devices

Step			Descr	ription			
1.	Begin configuration	on of the VI	PN tunnel by cl	icking on Set	tings unde	er the VI	N tab on the
	left. Click Add ur	nder the VP	N policies pan	el to display t	he Securit	y Policy	y pop-up
	window.						
	SonicWALL - Administration	n for 0006B1029C38 -	Microsoft Internet Explorer p	rovided by SonicWALL, INC.			_ 🗆 🛛
	<u>File E</u> dit <u>V</u> iew F <u>a</u> vorites <u>T</u> or	ols <u>H</u> elp					N
	G Back 🔹 🕥 🔹 😫		http://172.16.2.46/main.html				💌 🔁 Go
	Google -	⊻ G ▼ Ø ^{New!}	1				
	SONICWALL	COMPREHENS	SIVE INTERNET SECURITY**				
	System Network			1/011	Dellas Missad	Anata	
	SonicPoint	VPN > Settings		VPN	Policy Wizard	Apply	Cancel ?
	Firewall V VoIP	PN Global Settings	5				
	VPN	Enable VPN					
	Settings	Unique Firewall Identifier:	0006B1029C38	_			
	Advanced	PN Policies				Items 1 to 3 (of 3) 比 ◁ ▷ 比
	L2TP Server	# Name	Gateway	Destinations Crypt	o Suite	Enable	Configure
		1 WAN GroupVPN			DES HMAC SHA1 (IKE)		888
		2 WLAN GroupVPN		ESP 30	DES HMAC SHA1 (IKE)		8 B 6 C
		3 Avaya DevConnec	172.16.1.49	30.1.1.1 - 30.1.1.255 ESP 30	DES HMAC SHA1 (IKE)		808
		Add	elete				Delete All
	s s	Site To Site Policies: 1 Pol	licies Defined, 1 Policies Enabled	, 3000 Maximum Policies Allow	ed		
	G	GroupVPN Policies: 2 Poli	cies Defined, 0 Policies Enabled,	20 Maximum Policies Allowed			
	C	urrently Active VP	N Tunnels			Items 1 to 2 (of 2) 🕅 🗸 🗅 🕅
	Users	# Name	Local	Remote	Gateway		
	Hardware Failover	1 Avaya DevCo	nnect 11.1.1.1 - 11.1.1.255	30.1.1.1 - 30.1.1.255	172.16.1.49	Renegotiate	illi ⇔
	Security Services	2 Avaya DevCo	nnect 10.1.1.1 - 10.1.1.255	30.1.1.1 - 30.1.1.255	172.16.1.49	Renegotiate	illi ⇔
	Wizards						
	Help 2 Logout	2 Currently Active VPN Tun	nels				
	Status: The configuration ha	s been updated.					
	<u>é</u>					🔮 Ir	iternet
	<u>.</u>						

Step		Description
2.	•	Policy pop-up window, enter the following
	information for the VPN tunnel.	
	-	ect (a descriptive name for the VPN tunnel)
	IPsec Primary Gateway Name of	
	<i>1/2.10.1.49</i> (the 1 interface)	IP address of the remote SonicWALL's WAN
	IPsec Secondary Gateway Name	e or Address:
	0.0.0.0	
	Shared Secret: 1234 (a secret stri	ring that will be entered into both SonicWALL devices)
	Click on the Network tab after ent	tering the above information.
	http://172.16.2.46 - VPN Policy -	- Microsoft Internet Explorer provided by SonicWALL, INC. 📃 🗖 🔀
	General Network Pro	roposals Advanced
	Security Policy	
	Authentication Method:	IKE using Preshared Secret
	Name:	Avaya DevConnect
	IPsec Primary Gateway Name or Add IPsec Secondary Gateway Name or A	
	IKE Authentication	
	Shared Secret	
	Confirm Shared Secret	•••• Mask Shared Secret
	Local IKE ID:	IP Address
	Peer IKE ID:	IP Address
	Ready	
		OK Cancel Help
	🖉 Done	🔹 🔹 Internet

Step		Description
3.	Under the Network tab. select Local	Networks and Remote VPN Networks as defined
	in Section 3.1 step 6 and 7 respective	
	🐔 http://172.16.2.46 - VPN Policy - N	Nicrosoft Internet Explorer provided by SonicWALL, INC. 🛛 🗔 🗆 🔯
	General Network Prop	osals Advanced
	Local Networks	
	Choose local network from list	Local Networks
		es using DHCP through this VPN Tunnel
	O Any address 🔎	
	Destination Networks	
	O Use this VPN Tunnel as default ro	ute for all internet traffic
		dresses using DHCP through this VPN Tunnel
	Choose destination network from	list Remote VPN Networks
	Ready	
	Ready	
		OK Cancel Help
	8	Internet 🔮
4.	All the fields in the Proposal tab we	ere left at the default value in the sample
	configuration. Click on the Advanc	ed tab to continue.
	@ http://172.16.2.46 - VPN Policy - I	Microsoft Internet Explorer provided by SonicWALL, INC. 🛛 🖃 🔀
	General Network Pro	posals Advanced
	IKE (Phase 1) Proposal	
	Exchange:	Main Mode
	DH Group:	Group 2
	Encryption:	3DES V
	Authentication:	SHA1
	Life Time (seconds):	28800
	Ipsec (Phase 2) Proposal	
	Protocol:	ESP
	Encryption:	3DES V
	Authentication:	SHA1
	Enable Perfect Forward Secrecy	
	DH Group:	Group 2
	Life Time (seconds):	28800
	Ready	
		OK Cancel Help
	e	🥥 Internet

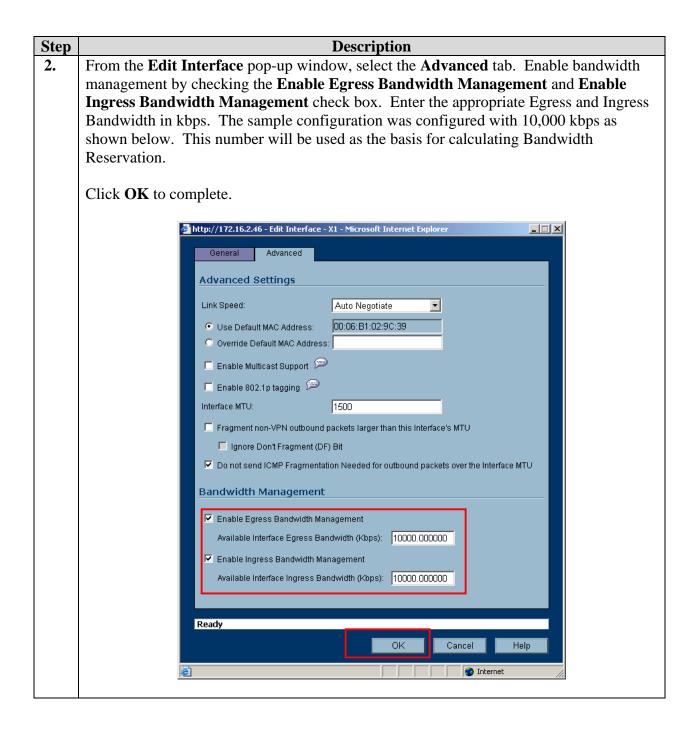
Solution & Interoperability Test Lab Application Notes ©2006 Avaya Inc. All Rights Reserved.

Step	Description
5.	Under the Advanced tab, Enable Keep Alive by clicking the check box on the left.
	Click OK to complete.
	1
	🐔 http://172.16.2.46 - VPN Policy - Microsoft Internet Explorer provided by SonicWALL, INC. 📃 🗆 🔀
	General Network Proposals Advanced
	General Ivelwork Proposals Advanced
	Advanced Settings
	Enable Keep Alive
	Suppress automatic Access Rules creation for VPN Policy
	Require authentication of VPN clients by XAUTH
	User group for XAUTH users:Select a user group
	Enable Windows Networking (NetBIOS) Broadcast
	Enable Multicast
	Apply NAT Policies
	Translated Local Network:Select Translated Local Network-
	Translated Remote Network:Select Translated Remote Network-
	Management via this SA: HTTP HTTPS
	User login via this SA:
	Default LAN Gateway (optional): 0.0.0.0
	VPN Policy bound to: Zone WAN 💌
	Ready
	OK Cancel Help
	Internet
I	

3.3. Configure the Firewall Access Rules and Bandwidth Reservation for the SonicWALL VPN Tunnel.

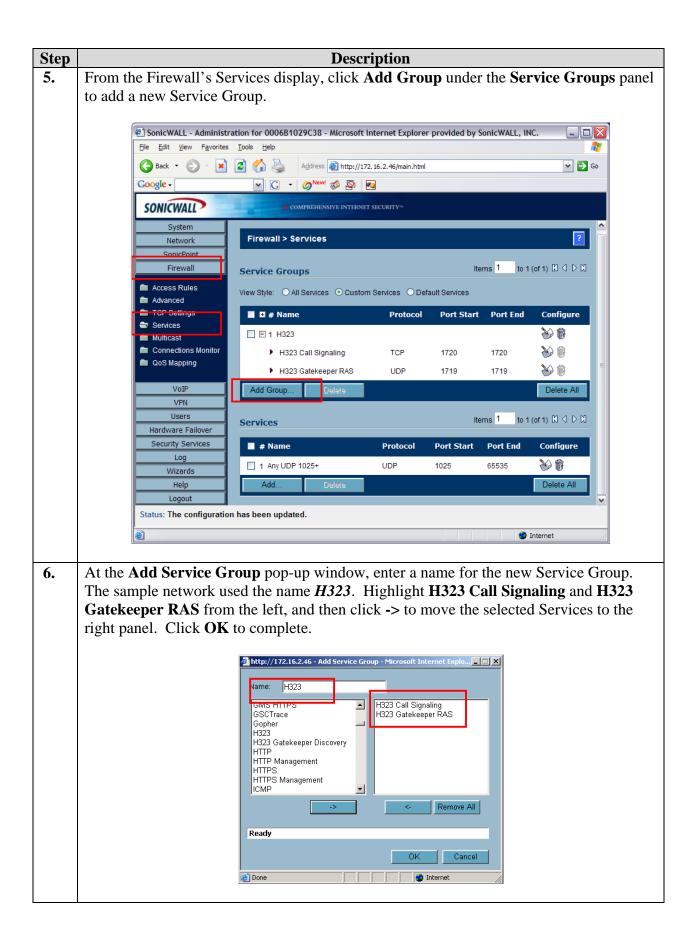
This section defines the necessary Firewall Access Rules and Bandwidth Reservation for VoIP traffic for the VPN Tunnel.

Step												
1.	Begin by defining	the Ban	dwidth fo	or the V	VAN	interfa	ice by	y selecti	ng Int	terfaces u	ınder	
	the Network tab on the left. Click on the \bigotimes icon on the right for the WAN Zone											
	under the Interface					10011 0		119110 10			10	
		Setting	s punei.									
	🏄 SonicWALL - Administrati	on for 0006B10	29C38 - Microsoft	t Internet Ex	olorer					_		
	File Edit View Favorites Iools Help											
	🕞 Back - 🕤 - 🖹 🙆 🏠 🔎 Search 👷 Favorites 🤪 🔗 - 🍃 🔯 - 🗍 🎇 🦄											
	Address 🛃 http://172.16.2.46	/main.html							•	🔁 Go 🛛 Links	1	
	SONICWALL		COMPREHENSIVE	INTERNET SEC	URITY							
	Cystem											
	Network	Networ	k > Interfaces				Setu	ıp Wizard	Clea	r Statistics ?		
	🕿 Interfaces											
	💼 WAN Failover & LB	Interface	e Settings									
	💼 Zones 💼 DNS	🗖 Name	Zone			Mask IP A	_		Comm			
	Address Objects	E X0	LAN			255.240 Stati		100 Mbps ful				
	Routing	E X1	WAN			255.240 Stati		100 Mbps ful	l-duplex De	efault WAN 🔬		
	NAT Policies ARP	E X2	Unassigne	d 0.0.0.0	0.0.0	.0 N/A	(No link				
	DHCP Server	E X3	Unassigne	d 0.0.0.0	0.0.0	.0 N/A	۱.	No link		8		
	💼 IP Helper	E ×4	Unassigne	d 0.0.0.0	0.0.0	.0 N/A	1	No link		8		
	🛍 Web Proxy	⊡ ×5	Unassigne	d 0.0.0.0	0.0.0	.0 N/A	k.	No link		8		
		Add Inte	rface									
	SonicPoint											
	Firewall	Interface	e Traffic Stati	stics							-	
	VoIP	Interface T	raffic Statistics								_	
	VPN	Traffic Stat		<u>x(</u>		<u>X1</u>	<u>X2</u>	<u>X3</u>	<u>X4</u>	<u>×5</u>		
	Users	Rx Unicast			6145	486757 0	0 0	0	0	0		
	Hardware Failover Security Services	Rx Bytes:	ast Packets:	54 48	4 9766161	355059269		0	0	0		
	Log	Tx Unicast	Packets:		1433	300627	0	0	0	0		
	Wizards	Tx Broadca	ast Packets:	3		4307	0	0	0	0		
	Help	Tx Bytes:		24	9513674	265103080	0	0	0	0		
	Logout											
	Status: Ready											
	e) Internet	11.	



<u>Step</u> 3.	*									
		wall services by selectin								
	left. Click on Add u	under Services panel to	display the	e Add Sei	rvice po	op-up winde	ow.			
							_			
		tration for 0006B1029C38 - Microsoft	nternet Explore	r provided by S	onicWALL, II					
	<u>File Edit View Favorite</u>									
	🕒 Back 🔹 🐑 🐇 🗶] 💈 🏠 🖕 A <u>d</u> dress 🖉 http://17	2.16.2.46/main.html			💌 🄁 🛛	Go			
	Google -	💌 G 🔹 🧭 🕬 🔛	4							
	SONICWALL	COMPREHENSIVE INTERNE	r security™							
	System				_	_				
	Network	Firewall > Services				?				
	Firewall			Ito	ms 1 to 1	1 (of 1) [X]				
		Service Groups		ne						
	Access Rules	View Style: O All Services O Custom Services O Default Services								
	TOP Settings	📕 🗄 # Name	Protocol	Port Start	Port End	Configure				
	Services	🗌 🗉 1 H323				80 B				
	Connections Monitor	H323 Call Signaling	TCP	1720	1720	X) 🕅				
	🛍 QoS Mapping	H323 Gatekeeper RAS	UDP	1719	1719	N n	≡			
	VoIP	Add Group Delete				Delete All				
	VPN									
	Users	Services		Ite	ms 1 to f	1 (of 1) 🕅 🖣 🖯 🕅				
	Hardware Failover Security Services	# Name	Protocol	Port Start	Port End	Configure				
	Log									
	Wizards	1 Any UDP 1025+	UDP	1025	65535	<u> </u>				
	Help Logout	Add Delete				Delete All				
	Status: The configurati	on has been updated.								
		en nac soon apaatoa.								
	۲					Internet	:			

Step		Description			
4.	Enter the following information for the new Firewall service.				
	Name: Protocol: Port Range:	Any UDP 1025+ (a descriptive name for the Firewall service) UDP(17) 1025 - 65535			
	This rule is desi H.323.	gned to filter out all UDP traffic that has not been negotiated using the			
	Click OK after entering all the information.				
		🎒 http://172.16.2.46 - Add Service - Microsoft Internet Exp 💶 🗵			
		Name: Any UDP 1025+			
		Protocol: UDP(17)			
		Port Range: 1025 _ 65535			
		Sub Type: None 💌			
		Beath			
		Ready			
		OK Cancel			
		🖉 Done			



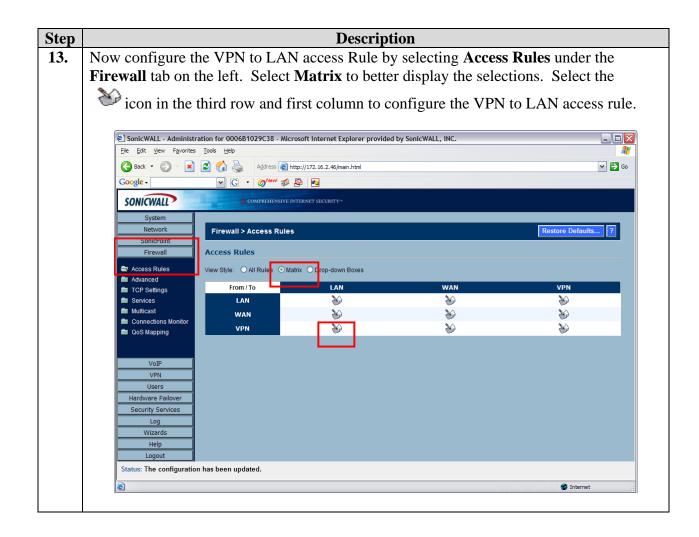
Step			Descript	tion						
7.	Select Access Rules under the Firewall tab on the left to configure the Firewall's rules. Select Matrix to better display all the selections. There are two sides of the firewall that									
need to be configured. One is LAN to VPN and the other is VPN to LAN. Sel										
		$\overset{\circ}{\sim}$ icon in the first row and third column to configure the LAN to VPN Access rule.								
	🖤 icon in the f	irst row and thi	rd column to c	onfigure the LAN	to VPN Access rule.					
	SonicWALL - Administra	ation for 0006B1029C38 - Micro	osoft Internet Explorer provideo	d by SonicWALL, INC.						
	<u>File Edit View Favorites</u>									
	G Back 👻 🕥 🕤 😫		p://172.16.2.46/main.html		💌 🛃 Go					
	Google -	🖌 🖸 🖌 🎯 New! 🚿 🗄	P 2							
	SONICWALL	COMPREHENSIVE IN	TERNET SECURITY**							
	System	_								
	Network	Firewall > Access Rules			Restore Defaults ?					
	Firewall	Access Rules								
	🚔 Access Rules	View Style: 🔿 All Rules 💿 Mat	rix OC rop-down Boxes							
	Advanced TCP Settings	From / To	LAN	WAN	VPN					
	Services	LAN	8	2	8					
	Multicast	WAN	2	2	N					
	Cos Mapping	VPN	8	8	8					
	VoIP									
	Users									
	Hardware Failover									
	Security Services									
	Log Wizards									
	Help									
	Logout	have been used at a d								
	Status: The configuration	n nas been updated.								
	<u>é</u>				🔮 Internet 🥂					

				Descript	ion					
Cli	ck on Add un	der the I	Firewall > A	ccess Rul	es > LA	N >	VPI	V pan	el to	add a ne
	ess Rule.							1		
	SonicWALL - Administ	tration for 0006B	1029C38 - Microsoft Intern	et Explorer provided	by SonicWALL, II	NC.				_ 0
	<u>File Edit View Favorite</u>	es <u>T</u> ools <u>H</u> elp								
	G Back 🝷 🕥 🕤 🗙) 💈 🏠 🎍	Address 🚵 http://172.16.2.	46/main.html						💌 🄁 🗸
	Google -	▼ G	• Ø ^{New!} 🚳 🗟 🔤							
	SONICWALL		COMPREHENSIVE INTERNET SECUR	UTY ^{as}						
	System									
	Network	Firewall >	Access Rules > LAN > Vi	PN 🚺	Public Server Wi	zard	Clear	Statistics	Restore	Defaults ?
	SonicPoint Firewall							Items	1 to 5	j(of5) [X] <] ▷ [X]
	🚔 Access Rules		es (LAN > VPN)					items	10 0	
	Advanced	View Style: O	All Rules Matrix Drop-	down Boxes						
	TCP Settings Services	🔳 # Priori	ity Source	Destination	Service	Action	Users	Comment	Enable	e Configure
	Multicast	□ 1 1 🕄	Local Neworks	Remote VPN Networks	H323	Allow	All	7	V	11 🏷 🖗
	QoS Mapping	🗆 2 2 ÎÎ	Avaya Media Gateway	Remote VPN Networks	Any UDP 1025+	Discard	All		V	11 🏷 🕅
		33	WAN RemoteAccess Networks	Any	Any	Allow	All	ø		11 📎 🖗
	VoIP VPN	4 4	WLAN RemoteAccess Networks	Any	Any	Allow	All	9		۲
	Users Hardware Failover	55	Local Neworks	Remote VPN Networks	Any	Allow	All	@ _`	~	۱ 🎸 🛍
	Security Services	Add	Delete						Res	tore Defaults
	Log Wizards									
	Help									
	Logout									
	Status: The configurati	on has been upd	ated.							
	۲								0	Internet

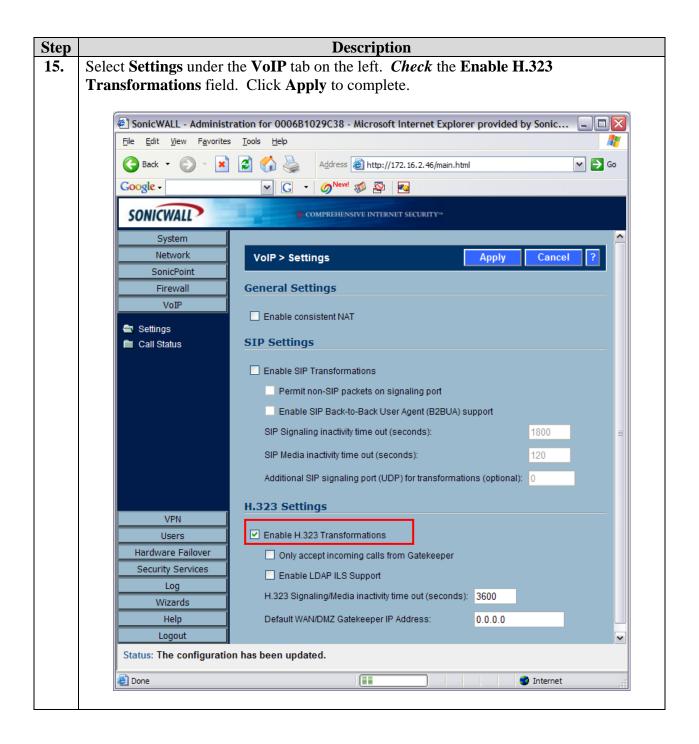
Step		Description
9.	Under the Gen information:	eral tab of the Add Rules pop-up window, enter the following
	Action: Service: Source: Destination:	<i>Allow</i> radio button selected <i>H323</i> (defined in section 3.3 step 6) <i>Local Networks</i> (defined in section 3.1 step 6) <i>Remote VPN Networks</i> (defined in section 3.1 step 7)
	Click on the B	andwidth tab to continue.
		Settings Action: Caneral Advanced Oo8 Bandwidth Settings Action: Callow Deny Discard From Zone: LAN Service: H323 Source: Local Networks Destination: Remote VPN Networks Users Allowed: All Schedule: Always on
		Comment Enable Logging Allow Fragmented Packets Ready OK Cancel Help Thernet

Step	n	escription
10.		h and priority are defined for the Outbound and
10.	Inbound traffic.	in and priority are defined for the Outbound and
	The H323 Access Rule in the sample ne	twork has defined the following:
	Outbound Bandwidth Management	_
	Guaranteed Bandwidth (%):	5
	Maximum Bandwidth (%):	10
	Bandwidth Priority:	0 highest
	Inbound Bandwidth Management	
	Guaranteed Bandwidth (%):	5
	Maximum Bandwidth (%):	10
	Bandwidth Priority:	0 highest
	After entering all the information, click	OK to complete.
		1
	Note: The percentage is based on the W. Step 2, not the bandwidth of the VPN tu	AN interface bandwidth defined in Section 3.3 nnel.
	http://172.16.2.46 - Add Rule - Microsoft	Internet Explorer
	General Advanced Qo	S Bandwidth
	Bandwidth Management	
	🔽 Enable Outbound Bandwidth Manag	gement ('allow' rules only)
	Guaranteed Bandwidth (%):	5
	Maximum Bandwidth (%):	10
	Bandwidth Priority:	0 highest 💌
	🔽 Enable Inbound Bandwidth Manage	ment ('allow' rules only)
	Guaranteed Bandwidth (%):	5
	Maximum Bandwidth (%):	10
	Bandwidth Priority:	0 highest 💌
	Ready	
		OK Cancel Help
	ē	📄 📄 🔯 Internet

	Description			
Click Add again from the Firewall > Access Rule > LAN > VPN menu in Section 3.3				
-	nother access rule.			
Under the Gen information:	eral tab of the Access Rules pop-up window, enter the following			
Action: Service: Source: Destination:	Discard radio button selected Any UDP 1025 + (defined in section 3.3 step 2) 10.1.1.x LAN (defined in section 3.1 step 4) Remote VPN Networks (defined in section 3.1 step 7)			
This rule disca	rds RTP traffic that has not been negotiated using H.323.			
Click on the O	K tab to complete.			
	🖉 http://172.16.2.46 - Add Rule - Microsoft Internet Explorer			
	General Advanced QoS Bandwidth			
	Settings			
	Action: C Allow C Der			
	From Zone:			
	To Zone: VPN			
	Service: Any UDP 1025+			
	Source: 10.1.1.x LAN			
	Destination: Remote VPN Networks			
	Schedule: Always on			
	Comment:			
	C Enable Logging			
	Allow Fragmented Packets			
	Ready			
	OK Cancel Help			
	Done			
After entering	the "H323" and "Any UDP 1025 +" access rules, make sure the rules			
order is as disp	played in Step 8 of this section. The "H323" must be before the "Any			
	Access Rule. If necessary, use the ¹¹ icon to move the selected rule up or			
down to obtain	the appropriate order.			
	Step 6 to add a Under the Gen information: Action: Service: Source: Destination: This rule disca Click on the O			



Step	Description
14.	Repeat Steps 8-13 in this Section to configure the same Access Rules for the VPN to LAN direction. Note: Make sure in Step 9 the Source is <i>Remote VPN Networks</i> and the Destination is
	Avaya Media Gateway as shown below.
	🚰 http://172.16.2.46 - Add Rule - Microsoft Internet Explorer
	General Advanced QoS Bandwidth Settings
	Action: C Allow C Dem Discard
	Service: Any UDP 1025+ Source: Remote VPN Networks
	Destination: Avaya Media Gateway Image: Comparison of the second se
	Comment:
	 ✓ Enable Logging ✓ Allow Fragmented Packets
	Ready
	OK Cancel Help
	Internet



4. Interoperability Compliance Testing

The interoperability compliance testing focused on assessing the ability of the SonicWALL PRO 4060 and TZ170 to establish a VPN tunnel that would support an infrastructure consisting of Avaya Communication Manager, and Avaya 46xx IP telephones while providing guaranteed bandwidth management for Avaya VoIP traffic.

4.1. General Test Approach

The general test approach was to verify that the Avaya IP telephones could successfully place and receive calls through the network as shown in **Figure 1** while competing with simulated non-VoIP low priority traffic. In addition, network traffic to Branch Site B was Network Address Translated to that of the IP address of the SonicWALL PRO 4060 WAN interface.

The main objectives were to verify:

- SonicWALL UTM devices can automatically allow RTP traffic streams based on H.323 signaling.
- Calls between telephones at the different locations were successfully completed and maintained with good voice quality.
- Multiple telephone calls between sites could be completed as per the desired bandwidth configured in the SonicWALL UTM devices.
- Non-VoIP traffic did not encroach upon the bandwidth reserved for the voice application.
- The solution supports G.711 and G.729 codecs.
- The solution supports DTMF.
- Preservation of Layer-3 DiffServ information.
- Network Address Translation (NAT) was implemented between the Main Site and Branch Site B.

4.2. Test Results

The objectives were successfully verified during compliance testing. Multiple telephone calls were successfully placed and received as per the bandwidth policy defined by the SonicWall UTM devices during varying levels of simulated competing traffic. Voice quality was good throughout testing regardless of traffic flow. DTMF was verified via access to the Meet-me Conference configured the Avaya Communication Manager.

5. Verification Steps

The following steps may be used to verify the configuration:

- Make sure all the SonicWALL UTM devices interfaces are reachable.
- Place and receive call from the Avaya telephones.
- From the SonicWALL UTM devices, verify the status of the VPN Link.
- From the SonicWALL UTM devices, verify the Access Rules are configured correctly by placing the mouse pointer over the bar chart icon in Step 8 Section 3.3. A pop-up window will display the packet count and byte processed by the Access Rule.

6. Support

For technical support on the SonicWALL UTM, contact SonicWALL, Inc. at http://www.sonicwall.com/support/contact.html

North America 1-888-777-1476

7. Conclusion

These Application Notes have described the administration steps required to configure the SonicWALL UTM devices to interoperate with and prioritize WAN bandwidth for Avaya IP H.323 phone traffic. During compliance testing, H.323 phone calls traversing the WAN link were successfully established and maintained while sharing the link with non-VoIP traffic.

8. Additional References

- [1] Administrator Guide for Avaya Communication Manager, Doc # 03-300509, Issue 1, June 2005
- [2] Avaya Communication Manager Advanced Administration Quick Reference, Doc # 03-300364, Issue 2, June 2005 Release 3.0
- [3] SonicOS Enhanced 3.0 Administrator's Guide

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

Product documentation for SonicWALL products may be found at http://www.sonicwall.com

©2006 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by [®] and [™] 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.