

Avaya Solution & Interoperability Test Lab

Configuring a VPN Tunnel and QoS Between a Samsung UbigateTM iBG3026 Gateway and a Juniper Networks SSG 520 Gateway - Issue 1.0

Abstract

These Application Notes describe the procedures for configuring a site-to-site Virtual Private Network (VPN) tunnel between a Samsung UbigateTM iBG3026 Gateway and a Juniper Networks SSG 520 gateway with Quality of Service (QoS) to support an Avaya IP telephony infrastructure.

The Samsung iBG3026 functions as a multi-service IP switch/router. A VPN/Internet Protocol Security (IPSec) option card provides encryption and decryption of IPSec VPN tunnels for the router. With a variety of QoS features and an Ethernet module with Power-over-Ethernet ports, the Samsung iBG3026 provides the necessary infrastructure for IP telephony.

1. Introduction

These Application Notes describe the procedures for configuring a Virtual Private Network (VPN) tunnel between a Samsung UbigateTM iBG3026 gateway and a Juniper Networks SSG 520 gateway with Quality of Service (QoS) to support an Avaya IP telephony infrastructure. The Samsung iBG3026 and Juniper SSG 520 have site-to-site IPSec VPN and QoS capabilities suitable for multi-site Avaya IP telephony deployment.

2. Test Configuration

The sample network implemented for these Application Notes is shown in Figure 1. Two office locations are included – a HQ Office and a Branch Office.



Figure 1: Test Configuration

The HQ Office consists of a Juniper SSG 520 functioning as a perimeter security device and an IPSec VPN head-end. Avaya Communication Manager running on the Avaya S8500B Server, Avaya G650 Media Gateway and Avaya SIP Enablement Services are also located at the HQ Office to provide the IP telephony infrastructure for the entire enterprise. The Avaya C363T-PWR Converged Stackable Switch provides LAN connectivity to the servers and IP telephones. Voice and data are on separate Virtual LANs (VLANs).

The Branch Office consists of a Samsung iBG3026 as a branch multi-service LAN/WAN switch/router. The Avaya IP telephones and Avaya IP Softphone PC are connected directly to the Ethernet ports on the Samsung iBG3026 which are configured as a VLAN.

JC; Reviewed:	Solution & Interoperability Test Lab Application Notes	2 of 33
SPOC 6/25/2007	©2007 Avaya Inc. All Rights Reserved.	Ubigate-Juniper.doc

A site-to-site VPN tunnel between the Samsung iBG3026 Gateway and the Juniper SSG 520 Gateway connects the 2 offices over the WAN.

An Avaya C364T-PWR Converged Stackable Switch simulates the WAN by routing the IP traffic between the two offices.

To establish the IPSec VPN tunnel, two phases of negotiation are required:

- In Phase 1, the participants establish a secure channel in which to negotiate the IPSec Security Associations (SAs).
- In Phase 2, the participants negotiate the IPSec SAs for encrypting and authenticating the ensuing exchanges of user data.

In this test configuration, the following parameters are used:

Phase 1

Authentication Method: Pre-shared Key Encryption: Advanced Encryption Standard (AES) 128-bit keys Authentication: Secure Hash Algorithm-1 (SHA-1) Diffie-Hellman (DH) Group: 2

Phase 2

Encapsulation: Encapsulation Security Payload (ESP) Encryption: AES 128-bit keys Authentication: SHA-1 Perfect Forward Secrecy: DH Group 2

3. Equipment and Software Validated

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

Equipment	Software
Avaya S8500 Server	Avaya Communication Manager
	3.1.2 (R013x.01.2.632.1)
	Patch 12372
Avaya G650 Media Gateway	-
• TN2312BP IP Server Interface	HW07, FW31
• TN799DP C-LAN Interface	HW01, FW17
TN2302AP IP Media Processor	HW20, FW113
TN2602AP IP Media Processor	HW02, FW24
Avaya SIP Enablement Services	SES03.1.1-03.1.114.0
Avaya 9630 IP Telephones	R1.1 (H.323)
Avera 4610SW ID Telephones	R2.7 (H.323)
Avaya 4010S w IP Telephones	R2.2.2 (SIP)
Aveve 4621SW ID Telephones	R2.7 (H.323)
Avaya 40215 w IF Telephones	R2.2.2 (SIP)
Avaya 2420 Digital Telephone	-
Avaya 6221 Analog Telephone	-
Avaya IP Softphone	R5.2 Service Pack 1
Avaya C363T-PWR Converged Stackable Switch	4.5.14
Avaya C364T-PWR Converged Stackable Switch	4.5.14
Samsung Ubigate iBG3026	SNOS 1.0.5.9 Advanced
	DSP 1.0.2 firmware
Juniper Networks SSC 520	ScreenOS 5.4.0r3a.0
Jumper merworks SSO 320	(Firewall+VPN)

4. Configure Avaya Communication Manager, Avaya SIP Enablement Services and Avaya IP Telephones

These application notes assume that the configuration of Avaya Communication Manager, Avaya SIP Enablement Services and the Avaya IP telephones are already in place. Refer to [1] for detail instructions on the configuration on these components.

5. Configure Juniper Networks SSG 520

The configuration steps utilize the web user interface (WebUI) of the Juniper SSG 520.

5.1. Access JUNIPER SSG 520



5.2. Configure Ethernet Interfaces

The Juniper SSG 520 has four built-in Ethernet interfaces: ethernet0/0 to ethernet0/3. The following steps are used to configure ethernet0/0 to a **Trust** security zone facing the internal corporate network and ethernet0/2 to an **Untrust** security zone facing the public internet. The Samsung iBG3026 will interact with ethernet0/2 when establishing an IPSec tunnel.

5.2.1. Configure ethernet0/0

Step	Description								
1.	From the left navigati	on menu, se	elect Netwo	ork > I	nterfa	ces. 7	The Ne	etwork > In	iterfaces
	(List) screen appears.	The IP add	ress is alrea	ady por	pulated	d for e	etherne	et0/0 from t	he basic
	configuration in Secti	on 5.1 Step	1 Click E	dit for	etherr	net0/0	to co	nfigure add	itional
	parameters	on on one orep				100070		inguio uuu	monu
	parameters.								
		Network > Interfa	ces (List)					ssq520sq1	2
		List 20 v per pa	ae						
		List ALL(6)	Interfaces				ſ	New Tunnel IF	*
		Name	IP/Netmask	Zone	Туре	Link	PPPoE	Configure	
	Home	ethernet0/0	10.1.10.4/24	Trust	Layer3	Up	-	Edit	
	Configuration	ethernet0/1	0.0.0/0	DMZ	Layer3	Down	-	Edit	
	Network	ethernet0/2	0.0.0.0/0	Untrust	Layer3	Up	-	Edit	
		ethernet0/3	0.0.0.0/0	HA	Layer3	Down	-	Edit	
	Zones	serial6/0	0.0.0.0/0	Untrust	WAN	Down	-	Edit	
	DHCP	serial6/1	0.0.0/0	Untrust	WAN	Down	-	Edit	
	+ 802.1X								
	+ Routing + NSRP								
	+ PPP								



5.2.2. Configure ethernet0/2



Solution & Interoperability Test Lab Application Notes ©2007 Avaya Inc. All Rights Reserved.

Step	Description	
2.	From the ethernet	t0/2 Properties: Basic screen, configure the highlighted fields shown
	below to set up the	e ethernet0/2 interface. All remaining fields can be left as the defaults.
	Click OK to save.	In this example, it is assumed that the maximum bandwidth of the
	WAN interface is	2048 Kbps.
		1
	Ssg520sg1:Juniper-Screen	10S 5.4.0r3a.0 - Windows Internet Explorer
	Http://10.1.10.4	finswebu.html
	😪 🕸 🔤 ssg520sg1: Juniper-S	GreenOS 5.4.0r3a.0
		Network > Interfaces > Edit \$\$5205g1
		Interface: ethernet0/2 (IP/Netmask: 1.1.1.1/24) Back To Interface List
		Properties: Basic MP DIP VIP IGMP Monitor 802.1X
		Interface Name ethernet0/2 0010.dbd3.e306
	Home	As member of group none V
	+ Configuration	
	Binding	O Obtain IP using DHCP Automatic update DHCP server parameters
	Zones	O Obtain IP using PPPoE None Create new pppoe setting
	 Interfaces DHCP 	IP Address / Netmask 1.1.1.1 / 24
	802.1X F. Routing	Manage IP 0.0.0.0 0010.dbd3.e306
	NSRP PPP	
	Screening	Block Intra-Subnet Traffic
	MCast Policies	
	 VPNs Objects 	Service Options
	Addresses Senices	Management Services SNMP SSL
	+ Users	Other Services Ping Path MTU(IPv4) Ident-reset
	Schedules Group Expressions	Maximum Transfer Unit(MTU) Admin MTU 0 Bytes (Operating MTU: 1500; Default MTU: 1500)
	Certificates	DNS Proxy
	+ Reports + Wizards + Help	WebAuth IP Address 0.0.0.0 SSL Only
	- Logout	Traffic Bandwidth Egress Maximum Bandwidth 2048 Kbps
	Toggle Menu	Ingress Maximum Bandwidth 2048 Kbps
		OK Apply Cancel
	Done	

5.3. Configure Tunnel Interface

Create an un-numbered tunnel interface to set up a route-based VPN tunnel. The tunnel interface is bound to a VPN tunnel in Section 5.4.2 Step 3. An un-numbered tunnel interface uses the IP address of the interface that is assigned. In this example, the interface is ethernet0/2.

Step	Description										
1.	From the Network > I	nterfaces (L	ist) scree	en. se	lect T	Րսոո	el IF	' from	the dr	op-down]	ist
	and click New	· · · · · · · · · · · · · · · · · · ·	,	,						1	
	and enex i tew.										
	/ see520se1. Juniper S	reeo05 5.4.0r3a.0 Windows Inte	rnet Explorer						EES	2	
	(C) - (M) http://10	1. 10. 4/nswebui html				~	Fy X [ijess	[A]		
	🐨 🐼 💽 81g 520 sg 1: 3.	iper-ScreenOS 5.4.0r3a.0	200	_	_		<u>م</u> • و	a - 🖶 - Gre	age • 🌍 Tgols •	30	
		List 20 v per page	(st)					ssgozo	501 2		
	Juniper	List ALL(6) MIn	terfaces					New Tu	nnel IF 💌	_	
		Name	IP/Netmask	Zone	Туре	Link	PPPoE	Configu	re		
	Home	ethemet0/0	10.1.10.4/24	Trust	Layer3	Up		Edit			
	Configuration Network	ethemet0/1 ethemet0/2	0.0.0.0/0	Untrust	Layer3	Up		Edit			
	Binding DNS	ethemet0/3	0.0.0/0	HA	Layer3	Down		Edit			
	Lones Interfaces Disco	serial6/0	0.0.0.0/0	Untrust	WAN	Down	-	Edit			
	B02.1X										
	I NSRP	*									
	Done					1 1/10-1	Tie 😝 En	ternet	n 100% •		
2.	From the Interface: N	ew Tunnel I	nterface	scree	en, co	onfig	ure th	ne higł	nlighte	ed fields	
	shown below to create	the un-numb	ered tun	nel in	terfa	ce. Ă	ll rei	nainin	g field	ls can be l	eft
	as the defaults. Click	K to covo	erea tam						5 11010		011
	as the defaults. Click C										
	<pre>/> ssg520sg1:Juniper-ScreenOS 5.4.0r3</pre>	.0 - Windows Internet Explo	orer								
	Http://10.1.10.4/nswebui.html August 1 Au							• • × @	oogleSG	P_*	
	ssg520sg1:Juniper-ScreenOS 5.4.0	3a.0		_				<u>⊕</u> •		Page + OF Tools +	
	Interfa	ce: New Tunnel Interfac	e e						SSG Back 1	o Interface List	
		ties: Basic	e.						DUCK	o intendee List	
	SSG-520	Tunnel Interface	Name tunnel. 1	(1~	100)						
	Home	Zone	(VR) Untrust (trus	st-vr) 💙							
	Configuration Network										
	Binding	ed IP									
	Zones	IP Address / Net	0.0.0.0	/	0						
	DHCP OUR	numbered	-								
	802.1X H Routing	Inte	erface ethernet0/2	2 (trust-vr) 💙							
		Maximum Transfer Unit((MTU) Admin MT	U 1500	Bytes	(Opera	ting MTU:	1500; Defaul	lt MTU: 1500)	
	Policies MCast Policies VPNs	DNSI	Proxy 🗌								
	 Objects Addresses 	Traffic Band	width Egress	Ma	imum Band	dwidth 0		Kbps			
	Services			Guara	nteed Band	dwidth 0		Khns			
	IP Pools		Ingress	Mai	rimum Band	lwidth 0		(hns			
	Group Expressions		- ingrood	(Md)	andin baild						
	Certificates Attacks		ОК	Ар	ply (Cancel					
	Reports Wirarde										
	Done							🕡 🌍 I	internet	€ 100% ·	
							line line line				-

5.4. Configure VPN Tunnel

Create the VPN tunnel to the Samsung iBG3026 at the HQ Office.

5.4.1. Configure Phase 1 Negotiation



Step	Description
3.	Configure the highlighted fields shown below to set up the phase 1 negotiation. Click Return (not shown below) to go back to the screen in Step 2 and click OK to save.
	🖉 ssg520sg1:Juniper-ScreenOS 5.4.0r3a.0 - Windows Internet Explorer
	C C C C C C C C C C C C C C C C C C C
	SSG-520 Home • Configuration • Network • Screening Policies • MCast Policies • MCast Policies • AutoKey KKE • AutoKey Advanced • P2 Proposal <

5.4.2. Configure Phase 2 Negotiation



Step	Description
2.	Configure the highlighted fields shown below to set up the phase 2 negotiation. Click
	Advanced to access additional configuration options.
	🖉 ssg520sg1:Juniper-ScreenOS 5.4.0r3a.0 - Windows Internet Explorer
	🚱 🗸 📓 http://10.1.10.4/nswebui.html
	👷 🎄 💽 ssg520sg1:Juniper-ScreenOS 5.4.0r3a.0
l	VPNs > AutoKey IKE > Edit ssg520sg1 ?
	sc-270 sc-270 sc-270 Home Configuration Network Cscreening Policies MCast Policies MCast Policies AutoKey Advanced Manual Key 1 2TP Monitor Status Objects Reports Beports Reports Beports Beports Beports Dore VPN Name Help Logout OK Cancel Advanced % tork



5.5. Configure Routes

The sample configuration requires adding three new route entries to the Juniper SSG 520 routing table: one specifying the default route to the internet and the second and third specifying the network address range to route to the remote Branch office. Although several routing options exist in the Juniper SSG 520 platform, static routes are used for this sample configuration.

5.5.1. Configure Default Route



Solution & Interoperability Test Lab Application Notes ©2007 Avaya Inc. All Rights Reserved.

5.5.2. Configure Route to Branch Office



Solution & Interoperability Test Lab Application Notes ©2007 Avaya Inc. All Rights Reserved.

Step	Description
3.	Repeat Step 1 to configure a new route.
4.	Configure the highlighted fields shown below to configure a "null" route. A "null" route targets the same destination address as the route through the tunnel interface but the traffic is directed to the Null interface which is a logical interface that drops all traffic that is received. This prevents the Juniper SSG 520 from routing the VPN traffic to the public WAN when the VPN tunnel is down. Specify the network address for the Branch Office for IP Address/Netmask . Select Null for Interface and leave the Gateway IP Address as 0.0.0. Specify a higher cost than in Step 2 for Metric . All remaining fields can be left as the defaults. Click OK to save.
	Ssg520sg1:Juniper-ScreenOS 5.4.0r3a.0 - Windows Internet Explorer State Image: State
	SSG-520 Virtual Router Name trust-vr IP Address/Netmask 192.168.1.0 / 24
	Home • Network Binding • DNS Zones Interfaces DHCP • 802.1X © Cateway Permanent Gateway IP Address 0.0.0 Permanent Source Source Mcast Routing Perference 20 OK Cancel

5.6. Configure Addresses

Create the IP addresses for the local and remote LAN to be used in the configuration of the policies.

Step	Description				
1.	From the left navig	ation menu. s	elect Objects > Ad	ldresses > List ar	nd the Objects >
	Addresses > List s	creen annears	Click New		
	Thun cosco > List 5	ereen appears	S. CHER I W.		
					eea
	C ssg520sg1:Juniper-Screen	OS 5.4.0r3a.0 - Windows II	nternet Explorer		
	↔ ↔ 🔽	I/nswebui.html			
	ssg520sg1:Juniper-S	Chierte > Addresses		1 • 6	
		Objects > Addresses >	Elst		ssg520sg1 P
		Untrust V Filter:		PORSTILVWY-7	New
		- Inter.		LONDIOLMAL	
		Name	IP/Domain Name	Comment	Configure
	Home	Any	€ 0.0.0.0 /0	All Addr	
	Configuration	Dial-Up VPN		Dial-Up VPN Addr	
	+ Network + Screening				
	- Policies				
	+ VPNs				
	 Objects Addresses 				
	List				
				Loc	al intranet 🔍 100% 🔹 🛒
2.	Configure the highl	ighted fields	shown below to cre	eate the IP address	s subnet for the voice
	VI ΔN at the HO O	office Specify	the network addre	ess of the voice V	[AN on the local
	I AN for ID A Jan	a Nietro a als a	and sole of Trues for	Zama Clialz OV	
	LAN IOT IP Addres	ss/meumask a	ind select I rust for	Zone . Click UK	to save.
	Ssg520sg1:Juniper-ScreenOS 5.4.	0r3a.0 - Windows Internet Exp	lorer		
	G C) ▼	.html		× +,	
	Ob	jects > Addresses > Configur	ation		ssq520sq1 ?
					•
	Juniper				
	SSG-520		Address Name Trust_LAN Voice		
	Home	P Address/Domain Name	Comment		
	Network Screening		IP Address/Netmask 10.1.10.0	/ 24	
	Policies MCast Policies	C) Domain Name		
	VPNs Objects				
	- Addresses		Zone Trust 💌		
	Groups		ОК Са	ancel	
	Services				
					Sucal intranet 🔍 100% 🔹 📑
3.	Repeat Step 1 to cre	eate a new \overline{IP}	address subnet for	the data VLAN o	n the local LAN.

Step	Description
4.	Configure the highlighted fields shown below to create the IP address subnet for the data
	VLAN. Specify the network address of the data VLAN on the local LAN for IP
	Address/Netmask and select Trust for Zone. Click OK to save.
	🖉 ssg520sg1:Juniper-Screen05 5:4.0r3a.0 - Windows Internet Explorer
	Constant Provide Consta
	Weightingstatightings Configuration Ssg520sg1 Configuration Ssg520sg1 Configuration Configur
	Muniper
	Address Name Trust_LAN Data
	Home Comment Configuration IP Address/Domain Name
	Screening O IP Address/Netmask 10.1.11.0 / 24 Policies
	MCast Policies Opmain Name
	Objects Zone Trust
	Groups Summary OK Cancel
	D Services w
5	Repeat Step 1 to create a new IP address subnet for the Branch Office
5.	
6	Configure the highlighted fields shown below to create the IP address subnet for the
0.	Branch Office. Specify the network address of the Branch Office for IP
	Address/Netmask and select Untrust for Zone Click OK to save
	Thus essive the select official conc. Check of to suve.
	🖉 ssg520sg1:Juniper-ScreenOS 5.4.0r3a.0 - Windows Internet Explorer
	Coogless Pr
	🛊 🏟 🗋 ssg52dsg1:Junper-ScreenOS 5.4.013.0
	Juniper'
	SSG-520 Address Name Branch Office
	Home
	Configuration IP Address/Domain Name Network
	Screening Domain Name
	VPNs
	Addresses Zone Untrust V
	Groups Summary OK Cancel
	Cuccamparer 4,100 %

5.7. Configure Policies

Configure the policies to allow traffic between the two sites across the VPN tunnel.

Step	Description
3.	From the Policies screen, select Trust for From and Untrust for To and click New .
	🖉 ssg520sg1:Juniper-ScreenOS 5.4.0r3a.0 - Windows Internet Explorer
	CoogleSG
	🛊 🏟 🖸 ssg520sg1:Juniper-ScreenOS 5.4.0r3a.0
	Policies (From Frust to Unitrust) ssg52Usg1 ?
	From Trust V Go New
	SSG-520 From Trust To Untrust, total policy: 1 TD Source Destination Service Action Ontions Configure Enable Move
	Home Configuration 1 Trust_LAN Voice Branch Office ANY
	Network Screening
	- Policies
	Done
4	Configure the highlighted fields shown below to create a policy allowing data traffic from
т.	the Juniper SSC 520 to the Branch Office Someung iBC2026 Click OK to save
	the Juliper SSO 520 to the Branch Office Samsung 1005020. Click OK to save.
	72 ssg520sg1;Juniper-Screen05 5,4;0r3a,0 - Windows Internet Explorer
	Policies (From Trust To Untrust) ssg520sg1 ?
	Juniper
	Rec Fo
	Configuration Source Address Order Addres Order Addres
	New Address
	Policies OAddress Book Entry Branch Office ▼ Multiple MCast Policies
	2 VPNs Service ANY V Multiple
	Reports Application None Vizards
	Help UWEB Filtering
	Action Permit V Deep Inspection
	Tunnel VPN None
	Modify matching bidirectional VPN policy
	Position at Top
	OK Cancel Advanced
	Done Stocal intranet 🔍 100% 👻

step	Description
5.	From the Policies screen, select Untrust for From and Trust for To and click New .
	C ssg520sg1:Juniper-Screen0S 5.4.0r3a.0 - Windows Internet Explorer
	Policies (From Trust To Untrust) ssg520sg1
	List 20 v per page Search
	From Unitust M Go New
	SSG-870 From Trust To Untrust, total policy: 2
	Home ID Source Destination Service Action Options Configure Enable Move
	Network Screening Strain Strain
	Policies MCast Policies
	Move
6.	Configure the highlighted fields shown below to create a policy allowing voice traffic
	from the Branch Office Samsung iBG3026 to the Juniper SSG 520. Click OK to save.
	Ssg520sg1:Juniper-ScreenOS 5.4.0r3a.0 - Windows Internet Explorer
	Stage S20sg1: Juniper-Screen0S 5.4.0r3a.0 - Windows Internet Explorer Image: Screen0S 5.4.0r
	C ssg520sg1:Juniper-ScreenOS 5.4.0r3a.0 - Windows Internet Explorer Image: Complex ScreenOS 5.4.0r3a.0 - Windows Internet Explorer Image: Complex ScreenOS 5.4.0r3a.0 - Windows Internet Explorer Image: Complex ScreenOS 5.4.0r3a.0 - Windows Internet Explorer Image: Complex ScreenOS 5.4.0r3a.0 - Windows Internet Explorer Image: Complex ScreenOS 5.4.0r3a.0 - Windows Internet Explorer Image: Complex ScreenOS 5.4.0r3a.0 - Windows Internet Explorer Image: Complex ScreenOS 5.4.0r3a.0 - Windows Internet Explorer
	Ssg520sg1:Juniper-ScreenOS 5.4.0r3a.0 - Windows Internet Explorer State Image: State
	✓ ssg520sg1:Juniper-ScreenOS 5.4.0r3a.0 - Windows Internet Explorer ✓ ✓ ▲ http://10.1.10.4/nswebul.html ✓ ▲ ▲ Ssg520sg1:Juniper-ScreenOS 5.4.0r3a.0 ✓ ● ■ ssg520sg1:Juniper-ScreenOS 5.4.0r3a.0
	Ssg520sg1:Juniper-ScreenOS 5.4.0r3a.0 - Windows Internet Explorer
	Image: Second Strate Screen OS 5.4.0r3a.0 - Windows Internet Explorer Image: Second Strate Screen OS 5.4.0r3a.0 - Windows Internet Explorer Image: Second Strate Screen OS 5.4.0r3a.0 - Windows Internet Explorer Image: Second Strate Screen OS 5.4.0r3a.0 - Windows Internet Explorer Image: Second Screen OS 5.4.0r3a.0 - Windows Internet Explorer Image: Second Screen OS 5.4.0r3a.0 - Windows Internet Explorer Image: Second Screen OS 5.4.0r3a.0 - Windows Internet Explorer Image: Second Screen OS 5.4.0r3a.0 - Windows Internet Explorer Image: Second Screen OS 5.4.0r3a.0 - Windows Internet Explorer Image: Second Screen OS 5.4.0r3a.0 - Windows Internet Explorer Image: Second Screen OS 5.4.0r3a.0 - Windows Internet Explorer Image: Second Screen OS 5.4.0r3a.0 - Windows Internet Explorer Image: Second Screen OS 5.4.0r3a.0 - Windows Internet Explorer Image: Second Screen OS 5.4.0r3a.0 - Windows Internet Explorer Image: Second Screen OS 5.4.0r3a.0 - Windows Internet Explorer Image: Second Screen OS 5.4.0r3a.0 - Windows Internet Explorer Image: Second Screen OS 5.4.0r3a.0 - Windows Internet Explorer Image: Second Screen OS 5.4.0r3a.0 - Windows Internet Explorer Image: Second Screen OS 5.4.0r3a.0 - Windows Internet Explorer Image: Second Screen OS 5.4.0r3a.0 - Windows Internet Explorer Image: Second Screen OS 5.4.0r3a.0 - Windows In
	Stage 200 gt 1: Juniper-Screen 05 5.4.0r3a.0 - Windows Internet Explorer Stage 200 gt 1: Juniper-Screen 05 5.4.0r3a.0 Stage 200 gt 1: Juniper-Screen 05 5.4.0r3a.0 Stage 200 gt 1: Juniper-Screen 05 5.4.0r3a.0 Policies (From Untrust To Trust) Stage 200 gt 1: Juniper-Screen 05 5.4.0r3a.0 Name (optional) From Branch Office (Voice) Stage 200 gt 1: Juniper-Screen 05 gt 1: Juniper-Screen 0
	Seg520sg1:Juniper-ScreenOS 5.4.0r3a.0 - Windows Internet Explorer Seg520sg1:Suniper-ScreenOS 5.4.0r3a.0 - Windows Internet Explorer <td< th=""></td<>
	Seg520sg1:Juniper-ScreenOS 5.4.0r3a.0 - Windows Internet Explorer Seg520sg1:Juniper-ScreenOS 5.4.0r3a.0 - Windows Internet Explorer Seg520sg1:Juniper-ScreenOS 5.4.0r3a.0 - Windows Internet Explorer Policies (From Untrust To Trust) Seg520sg1:Juniper-ScreenOS 5.4.0r3a.0 - Windows Internet Explorer Policies (From Untrust To Trust) Seg520sg1:Juniper-ScreenOS 5.4.0r3a.0 - Windows Internet Explorer Policies (From Untrust To Trust) Seg520sg1:Duniper-ScreenOS 5.4.0r3a.0 - Windows Internet Explorer Name (optional) From Branch Office (Voice) Name (optional) From Branch Office (Voice) New Address Destination Address Mathematical Address
	Seg520sg1:Juniper-ScreenOS 5.4.0r3a.0 - Windows Internet Explorer Seg520sg1:Juniper-ScreenOS 5.4.0r3a.0 - Windows Internet Explorer <td< th=""></td<>
	Seg520sg1:Juniper-ScreenOS 5.4.0r3a.0 - Windows Internet Explorer <p< th=""></p<>
	Source Address Name (optional) From Branch Office (Voice) Source Address Objects Network Screening Policies VPIs Objects VPIs Objects New Address VPIs Objects VPIs Objects VPIs Objects VPIs Objects VPIs Objects Wizards Help Locout WEB Filtering
	Ssg52Dsg1:Juniper-Screen0S 5.4.0r3a.0 - Windows Internet Explorer Image: Sige State of the state
	Ssg520sg1:Juniper-Screen0S 5.4.0r3a.0 - Windows Internet Explorer Image: Stress of the stre
	Stage 20 og 1:: Juniper: Screen() 5 5: 4: 0: 7a.0 Windows Internet Explorer Image: Screen() Image: Screen() Stage 20 og 1:: Juniper: Screen() 5 5: 4: 0: 7a.0 Windows Internet Explorer Image: Screen() Screen() Image: Screen() Screen() Policies Image: Screen() Policies Image: Screen() Policies Image: Policies
	² Sug52/bg1:Juniper-Screen05 5.4.0r3a.0 - Windows Internet Explorer ² Intp://10.1.10.4/newebu.html ² Screening Policies ² New Address ² New Address ² Objects ² New Address ² Virands ² Negle Menu
	Stop520bg1:Luniper-Screen05 5.4.0r3a.0 - Windows Internet Explorer Image: Stop520bg1:Luniper-Screen05 5.4.0r3a.0 Image: Stop520bg1:Screen05 5.4.0r3a.0 Image: Stop520bg1:Screen05 5.4.0r3a.0 Image: Stop520bg1:Screen05 5.0r4a/dress 5.0
	Step220pg1:Juniper-Screen05 5:4:07:3a:0 Windows Internet Explorer Step320g11:Amper-Screen05 5:4:07:3a:0 Policies (From Untrust To Trust) Step320g11:Amper-Screen05 5:4:07:3a:0 Policies (Prom Branch Office (Voice) Source Address New Address ONew Address Onew Address New Address Onew Address Onew Address Onew Address Policies (Prom Example Address Book Entry Trust_LAN Voice V Multiple Application None V WEB Filtering Loggut Logging (Prom Example Address Deep Inspection) Tunnel VPI None V Logging (Prom Example Address Deep Inspection) Tunnel VPI None V Logging (Prom Example Address Deep Inspection) Tunnel VPI None V Logging (Prom Example Address Deep Inspection) Tunnel VPI None V Position at Top (Prom Example Address Deep Inspection) Tunnel VPI None V Position at Top (Prom Example Address Deep Inspection) Tunnel VPI None V <
	Support Standard

Step	Description
7.	From the Policies screen, select Untrust for From and Trust for To and click New .
	🖉 ssg520sg1:Juniper-ScreenOS 5.4.0r3a.0 - Windows Internet Explorer
	Cocycles Coc
	🙀 🎶 🏠 ssg520sg1:Junper-ScreenOS 5.4.0r3a.0 😭 r 🔂 egg r 😳 Eggs r
	List 20 v per page Search
	From Untrust V Go New
	SSG-520 From Untrust To Trust, total policy: 1 ID Source Destination Service Action Options Configure Enable Move
	E Configuration 4 Branch Office Trust_LAN Voice ANY 🥝 Edit Clone Remove <table-cell> 🕬</table-cell>
	Poly Network Screening
	─ Policies ─ MCast Policies
	Move 🔮 Local intranet 😤 100% 👻 🤮
8.	Configure the highlighted fields shown below to create a policy allowing data traffic from
	the Branch Office Samsung iBG3026 to the Juniper SSG 520. Click OK to save.
	Ssg520sg1:Juniper-ScreenOS 5.4.0r3a.0 - Windows Internet Explorer
	Image: Second
	Policies (From Untrust To Trust)
	Juniper'
	SSC 220 Name (optional) From Pranch Office (Data)
	Home ONew Address /
	Configuration Source Address OAddress Book Entry Branch Office Multiple
	Screening Destination Address ONew Address // Destination Address
	MCast Policies
	Objects Application None
	Wizards
	Logout WEB Filtering
	Toggle Menu
	L2TP None V
	Logging 🗌 at Session Beginning 🗌
	Position at Top
	OK Cancel Advanced
	Move

5.8. Configure Quality of Service

Juniper Networks recommends the following ways to manage bandwidth for VoIP services using the standard traffic shaping mechanisms.

- Guarantee bandwidth for VoIP traffic The most effective way to guarantee the bandwidth for VoIP service and still allow other types of traffic on the interface is to create a policy which guarantees the minimum bandwidth necessary for the amount of VoIP traffic that is expected on the interface, and to set the priority queuing to the highest level. The advantage of this strategy is that VoIP can use additional bandwidth when available, and other types of traffic can use the bandwidth that is not guaranteed for VoIP when the bandwidth is not being used.
- Limit bandwidth for non-VoIP traffic By setting a maximum bandwidth for non-VoIP traffic, the remaining bandwidth is available to VoIP traffic. The level of priority queuing for VoIP traffic is also set to the highest level. The disadvantage of this method is that non-VoIP traffic cannot use additional bandwidth, even when the bandwidth is not being used by VoIP traffic.
- Use priority queuing and Differentiated Services Codepoint (DSCP) marking Guaranteeing bandwidth for VoIP traffic and limiting bandwidth for non-VoIP traffic both govern throughput on the Juniper SSG 520. DSCP marking enables the priority queuing settings downstream to be preserved. At the same time, received DSCP value set by the originating networking device or upstream router can be kept or changed so that the next hop router, typically the LAN or WAN edge router, can enforce QoS in its DiffServ domain. By default, for VPN configurations, the Juniper SSG 520 copies the DSCP marking from the inner header of the IP packet to the outer header, so that the next hop router can enforce the correct QoS on the encrypted traffic.

In this configuration, QoS is achieved by guaranteeing the bandwidth for VoIP traffic and setting it to the highest priority. DSCP is already marked by the Avaya S8500B Server, CLAN circuit packs, MedPro circuit packs and Avaya IP telephones and DSCP will be preserved as it passes through the VPN tunnel.

D	JESCI I	pulon											
F	from t	he left r	naviga	tion menu,	, select Pol	licies	and tł	ne Polici	es sc	reer	appe	ears.	Click
fo	or the	policy of	define	d for the V	oIP traffic	from	the J	uniper S	SG 5	20 t	the	Sam	sung
iF	BG30	26 (Poli	icy ID	3)				I I					0
	0000	-0 (1 01											
	C 55052)sal: Juniner-Sr	reenOS 5.4	0r3a () - Windows Inte	ernet Explorer								
	00	▼ http://10.	1. 10. 4/nswebui.	html	ernet Explorer				~	47 X	GoogleSG		
		ssg520sg1:Jur	niper-ScreenOS !	i.4.0r3a.0							• 🔊 • 0	🖶 - 🕞 e	age 🔹 🌍 T
			Poli	cies (From All zones	; To All zones)							ssg520s	g1
			List	20 🔺 per page									Sear
	3	Juniper	Fro	m All zones 🍟				To All zones 🝸	Go				N
		NETWORKS	-	and Hadaviet To Taxa	h hahal anlinu 2								
		SSG-520) Source	Destination	Service	Action	Options		Confid	jure	Enable	Move
	Home	uration	2	Branch Office	Trust_LAN Data	ANY			Edit	Clone	Remove	v	\$ }
	+ Netwo	ork nina	4	Branch Office	Trust_LAN Voice	ANY			Edit	Clone	Remove	V	\$
	Polici	es Delision	Fi	om Trust To Untrus	t, total policy: 2								
	+ VPNs	. Policies	п) Source	Destination	Service	Action	Options		Config	gure	Enable	Move
	E Repo	ts ts	1	Trust_LAN Data	Branch Office	ANY			<u>Edit</u>	<u>Clone</u>	Remove	v	\$ ===
	E Wiza	ds	3	Trust_LAN Voice	Branch Office	ANY			Edit	<u>Clone</u>	<u>Remove</u>	•	\$ ===
C	Done	dvanc	ed.								🖳 Local intra	net	a 100
С	Done	Advanc	ed.	OS 5,4,0r3a,0 - Window /rswebu.html	s Internet Explorer				v *+ ×		Local intra	net	€ 100 ■ ×
С	Done	nt Advance Ssg520sg1:1 GO + D M M M	ed.	OS 5,4.0r3a.0 - Window /rswebu.html creenOS 5,4.0r3a.0	s Internet Explorer				¥ 49 ×	K Googles	Cocal intrar	net Eage • ۞ Ts	100
С	Done	n Advanc Sep520sg1:: Soo - I Soo - I Soo - I	ed.	OS 5.4.0r3a.0 - Window Inswebu html greenOS 5.4.0r3a.0 Policies (From Trus	s Internet Explorer				× + ×	K Googles	Cocal intrar	net - 2896 * ()) T(5 g1	 100 100
С	Done	n Advanc © ssg520sg1:: @ @ - @ @ @ - @ @ @ .	ed.	OS 5.4.0r3a.0 - Window /swebu.html greenOS 5.4.0r3a.0 Policies (From Trus	s Internet Explorer t To Untrust)				★ 40 × 100 × 1	() Googles	ig Local intrar is is ssg520	Eage ~ (2) TS	€ 100
С	Done	t Advanc	ed. http://or.screen http://io.1.10.4 g550sg12Junger-8 http://or.a	OS 5.4.0r3a.0 - Window /rswebu.html creenOS 5.4.0r3a.0 Policies (From Trus	s Internet Explorer t To Untrust)				1	S Googles	Cocal Intra Cocal Intra Intra Intra Cocal Intra	et 299e * ()) Ts 5g1	 (*) 100 <
C	Done	n Advanc	ed. huniper. Screen http://10.1.10.4 p\$200g1:Junper-6 http://10.1.10.4 p\$200g1:Junper-6 http://10.1.10.4 http://10.4 http://1	OS 5.4.0r3a.0 - Window Irswebu.html creerOS 5.4.0r3a.0 Policies (From Trus Name (opt	s Internet Explorer t To Untrust) ional) To Branch Offi	ce (Voice)			× ++ ×	() Googles	SG SSG SSG520	et Eage - @ Tç Sg1	€ 100
C	Done	Advance	ed. huniper Screen http://10.1.10.4 g520g112nper2 s20 on	OS 5.4.0r3a.0 - Window Inswebu html greenOS 5.4.0r3a.0 Policies (From Trus Name (opt Source Ad	s Internet Explorer t To Untrust) ional) To Branch Offi O New Address O Address O Address	ce (Voice) s	LLAN Voice	↓/		K) Googles	Cocal Intra Cocal Intra Intra Cocal Intra Cocal Intra Cocal Intra Cocal Intra Cocal Intra Cocal Intra Cocal Intra Cocal Intra Cocal Intra Intra Cocal Intra Cocal Intra Cocal Intra Cocal Intra Cocal Intra Cocal Intra Cocal Intra	Eage + ◎ Ts 5g1	€ 100
C	Done	tt Advanc ssg520sg1:: * * * * * * * * * * * * * * * * * * *	ed. Intip/r.Screen http://10.1.10.4 gs20sg12JungerSc ss20 on	OS 5.4.073a.0 - Window /nswebu.html creenOS 5.4.0r3a.0 Policies (From Trus Name (opt Source Ad	s Internet Explorer i To Unitrust) ional) To Branch Offi New Addres O New Address O New Address	ce (Voice) s k Entry Trus s	LAN Voice	✓ Multiple	¥ 49 X	() Coogles	K Cocal intrar G S S S S S S S S S S S S S S S S S S	Eage - @ Ts Sg1	* 100
C	Done Park	Advanc ssp520og1: * * * * * * * * * * * * * * * * * * *	ed. uniper-Serven http://10.1.10.4 g520g11Juner-5 s20 on sies	OS 5.4.073a.0 - Window Inswebu.html creenOS 5.40r3a.0 Policies (From Trus Name (opt Source Ad Destination Ad	s Internet Explorer t To Untrust) ional) To Branch Offi Idress O New Address O New Address O New Address O Address Boo O Address Boo	ce (Voice) s k Entry Trus s s k Entry Bran	LAN Voice	✓ Multiple ✓ Multiple	× + ×	K Cooplet	کے ایک کی کہ	eace - ()) Tr Sage - ()) Tr	€ 100
C	Done Prince	Advanc ssg520og1:	ed. uniper-Screen http://10.1.10.4 g5205g132ungerSc f520 on ties KE Advanced	DS 5.4.073a.0 - Window /newebu.html reenOS 5.4.0r3a.0 Policies (From Trus Name (opt Source Ad Destination Ad Su	t To Untrust) ional) To Branch Offi New Address O New Address O Address Boo Address Boo O Address Boo Address Boo Address Boo Address Boo None	ce (Voice) s k Entry Trus s k Entry Bran	LLAN Voice ch Office	✓ Multiple / Multiple / Multiple		K Googlet	C C Ssg520	et Bage - @ Tg Sg1	(\$100)
C	Done Party Control of	Advanc Sep520eg1:	ed. uniper-Server http://10.1.10.4 g520g11Juner-5 szo on ites IKE Advanced ley Sature	OS 5.4.073a.0 - Window /rswebu.html creenOS 5.40r3a.0 Policies (From Trus Name (opt Source Ad Destination Ad Su	s Internet Explorer it To Untrust) ional) To Branch Offi Idress O New Address O Address Boo O New Address O Address Boo ervice ANY cation None WEB Filtering	ce (Voice) s k Entry Trus s s k Entry Bran	t_LAN Voice ch Office ■ ♥ Multip	<pre>// // // // // // // // // // // // //</pre>		Coogled	Se Cocal intra	eace - () Tr Sg1	€ 100
C	Done	Advanc	ed. huniper: Screen http://10.1.10.4 g5200g1:Junper - g5200g1:Junper - screen sc	OS 5.4.0r3a.0 - Window /rswebu.html creenOS 5.4.0r3a.0 Policies (From Trus Name (opt Source Ad Destination Ad Source Ad	s Internet Explorer it To Untrust) ional) To Branch Offi idress O New Address O Address Boo ervice ANY cation None WEB Filtering Action Permit v	ce (Voice) s k Entry Trus s k Entry Bran v Deep Inspe	t_LAN Voice ch Office Multip	✓ Multiple ✓ Multiple		K Googlet	SG Sg Sg S20	et Bage + ()) Tg 5g1	* 100
C	Done	Advance	ed. uniper Screen http://10.1.10.4 gs200g11/unper 2 ss20 on iles IKE Advanced ley Ratus	DS 5.4.0r3a.0 - Window Inswebuthtml creenOS 5.4.0r3a.0 Policies (From Trus Name (opt Source Ad Destination Ad Si Appli	s Internet Explorer it To Untrust) ional) To Branch Offi ONew Address O Address Boo ervice ANY cation None WEB Filtering Action Permit © Iunnel VPN None	ce (Voice) s k Entry Trus s k Entry Bran V Deep Inspe	ch Office	✓ Multiple ✓ Multiple ✓ Multiple		K] [Cocoper k · S	K C SSg520	eage + ⊚ Ts Sg1	€ 100
С	Done	Advance ssg520sg1: Ssg520sg1: Sg20 - 10 Advance Sg20 - 10 Sg20 - 10 Sg	ed. uniper-Screen http://10.1.0.4 gs0og112ungerC szo on sies kE Advanced ley katus	OS 5.4.073a.0 - Window Inswebu.html creenOS 5.4.0r3a.0 Policies (From Trus Name (opt Source Ad Destination Ad So Applia	s Internet Explorer a To Untrust) ional) To Branch Offi idress O New Addres O New Address O New Address O Address Boo ervice ANY cation None WEB Filtering MCEB Filtering MCED Filtering MCED Filtering MCED Filtering MCED Filtering MCED Filtering MCED Filtering MCED Filtering MCED Filtering MCED Filtering	ce (Voice) s k Entry Trus s k Entry Bran v Deep Insper v matching bic	LLAN Voice ch Office Ch Office	Multiple Multiple N policy		K Cooples	K 7 () · C	Eage - () Ts	€ 100
C	Done	Advance	ed. huniper-Screen http://10.110-4 g520g11/kmper-S g5	OS 5.4.0r3a.0 - Window Inswebul-html creenOS 5.4.0r3a.0 Policies (From Trus Name (opt Source Ad Destination Ad Source Ad Destination Ad Source Ad Destination Ad Source Ad Sour	s Internet Explorer it To Untrust) ional) To Branch Offin idress O Address Boo O Address Boo O Address Boo Cation None WEB Filtering Action Permit O IUMED VPN None Modify LZTP None O Regging at Session	ce (Voice) s k Entry Trus s k Entry Bran v Deep Insper v matching bio	t_LAN Voice ch Office ction irectional VF	Multiple Multiple Multiple PN policy		K Cooplet	K C ⊕ V ⊡ Ssg520	eate + () Tg 2age + () Tg 5g1	€ 100
C	Done	Advanc Advanc Spin Spin Spin Spin Home Configurati Network Screening MCast Polic Vizards Manual K Cutopers Autokey Autokey Autokey Autokey Cutopers Monar S Objects Configurati Network Spin	ed. uniper-Screen http://10.1.10.4 g5206g12JUnper-6 520 on ites KE Advanced ey ttatus	05 5.4.073a.0 - Window /newebu.html creenOS 5.4.073a.0 Policies (From Trus Name (opt Source Ad Destination Ad Ss Appli 1 1	s Internet Explorer t To Untrust) to Branch Offi O New Address O Address Boo O Address Boo O Address Boo O Address Boo C Address Boo	ce (Voice) s k Entry Trus s k Entry Bran Deep Inspe- y matching bio n Beginning [Cancel	LAN Voice ch Office Multip ction irectional VF	/ Multiple // Multiple // Multiple			C C C S S S S S S S S S S S S S S S S S	et Bage - () TS Sg1	€ 100

Step	Description								
3.	Configure the highlighted fields shown below to guarantee 512 kbps for VoIP traffic up to								
	a maximum of 1024 kbps. At the same time, VoIP traffic will be set to the highest								
	priority. Click OK to save.								
	Ssg520sg1:Juniper-ScreenOS 5.4.0r3a.0 - Windows Internet Explorer								
	Coordes Coorde								
	Policies (From Trust To Untrust) ssg520sg1								
	Juniper [°]								
	SSC-520 O Infranet-Auth O No Redirect Home O Redirect all traffic								
	Configuration Network Screening Policing Bandwidth O kbps Guaranteed Bandwidth 512 kbps								
	MCast Policies Traffic Shaping Maximum Bandwidth 1024 kbps Traffic Priority Highest priority								
	Manual Key DISCP Value DSCP Value DSCP Value DSCP Value								
	Objects Reports Counting Wizards								
	Help Alarm Threshold D Bytes/Sec KBytes/Min Alarm Threshold								
	Toggle Menur Schedule None								
	OK Return Cancel								
	Done Slocal Intranet 🔍 100% 👻								
4.	Repeat Steps 1 to 3 for Policy ID 4 to configure for the VoIP traffic from the Samsung								
	iBG3026 to the Juniper SSG 520.								

6. Configure Samsung Ubigate iBG3026 Gateway

The Samsung iBG3026 provides both browser-based and command line-based (telnet or console port access) administrative interfaces. However, since the full range of necessary configuration features is supported only via the command line interface (CLI), the steps in this section use only the CLI.

6.1. Configure Ethernet and VLAN Interfaces

Step	Description					
1.	Connect to the Samsung iBG3026 console interface via a terminal emulation program (e.g., HyperTerminal) using the serial cable provided for the console port at the back of the machine. Enter the user name (samsung) and password (see [4]) to log in. Enter configure terminal to access the configure mode.					
	<pre># # SAMSUNG ELECTRONICS CO., LTD. Login # login: samsung password:</pre>					
	SAMSUNG ELECTRONICS CO., LTD. CLI sarak2# configure terminal sarak2/configure#					
2.	Configure the Ethernet port 0/2 as an untrusted interface to connect to the public WAN.					
	<pre>sarak2/configure# interface ethernet 0/2 Configuring existing Ethernet interface sarak2/configure/interface/ethernet (0/2)# ip address 2.2.2.1/24 sarak2/configure/interface/ethernet (0/2)# crypto untrusted sarak2/configure/interface/ethernet (0/2)# exit sarak2/configure#</pre>					

Step	Description
3.	Create a VLAN for the Ethernet ports used by IP telephones, Windows server and IP Softphone PC and configure the VLAN as a trusted interface. The configuration below is shown for Ethernet ports 1/18 and 1/19. Repeat the steps as necessary to configure other Ethernet ports.
	<pre>sarak2/configure# vlan database sarak2/configure/vlan/database# vlan 101 bridge 1 name Remote sarak2/configure/vlan/database# exit sarak2/configure# interface vlan vlan1.101 sarak2/configure/interface/vlan vlan1.101# ip address 192.168.1.1 255.255.255.0 sarak2/configure/interface/vlan vlan1.101# crypto trusted sarak2/configure/interface/vlan vlan1.101# exit sarak2/configure# interface ethernet 1/18 Configuring existing Ethernet interface sarak2/configure/interface/ethernet (1/18)# switchport mode access sarak2/configure/interface/ethernet (1/18)# switchport access vlan 101 sarak2/configure/interface/ethernet (1/18)# exit sarak2/configure/interface/ethernet 1/19 Configuring existing Ethernet interface sarak2/configure# interface ethernet 1/19 Configuring existing Ethernet interface sarak2/configure/interface/ethernet (1/19)# switchport mode access sarak2/configure/interface/ethernet (1/19)# switchport access vlan 101</pre>
	<pre>sarak2/configure# sarak2/configure#</pre>
4.	Add a static route to the HQ Office.
	<pre>sarak2/configure# ip route 10.1.0.0 255.255.0.0 ethernet0/2 sarak2/configure#</pre>

6.2. Configure VPN Tunnel

Create the VPN tunnel to the Juniper SSG 520.

Step	Description						
1.	Configure VPN tunnel Phase 1 IKE negotiations to the Juniper SSG 520 at the HQ Office.						
	<pre>sarak2/configure# crypto sarak2/configure/crypto# ike policy ToHQ 1.1.1.1 sarak2/configure/crypto/ike/policy ToHQ 1.1.1.1# local-address 2.2.2.1 Default proposal created with priority1-des-shal-pre_shared-g1 Key String has to be configured by the user sarak2/configure/crypto/ike/policy ToHQ 1.1.1.1# key interop sarak2/configure/crypto/ike/policy ToHQ 1.1.1.1# mode main sarak2/configure/crypto/ike/policy ToHQ 1.1.1.1# proposal 1 sarak2/configure/crypto/ike/policy ToHQ 1.1.1.1/proposal 1# authentication-meth od pre-shared-key sarak2/configure/crypto/ike/policy ToHQ 1.1.1.1/proposal 1# dh-group group2 sarak2/configure/crypto/ike/policy ToHQ 1.1.1.1/proposal 1# encryption-algorithm aes128-cbc sarak2/configure/crypto/ike/policy ToHQ 1.1.1.1/proposal 1# exit</pre>						
	Sarak2/configure/crypto# Configure VPN tunnel Phase 2 IPSec negotiations to the Juniper SSG 520 at the HQ Office.						
	<pre>sarak2/configure/crypto# ipsec policy ToHQ 1.1.1.1 sarak2/configure/crypto/ipsec/policy ToHQ 1.1.1.1# match address 192.168.1.0 255.255.255.0 10.1.0.0 255.255.0.0 Default proposal created with priority1-esp-3des-shal-tunnel and activated. sarak2/configure/crypto/ipsec/policy ToHQ 1.1.1.1# pfs-group group2 sarak2/configure/crypto/ipsec/policy ToHQ 1.1.1.1# proposal 1 esp sarak2/configure/crypto/ipsec/policy ToHQ 1.1.1.1/proposal 1# encryption- algorithm aes128-cbc sarak2/configure/crypto/ipsec/policy ToHQ 1.1.1.1# exit sarak2/configure/crypto/ipsec/policy ToHQ 1.1.1.1# exit sarak2/configure/crypto# exit sarak2/configure/crypto# exit sarak2/configure#</pre>						

6.3. Configure Firewall Policies

Configure the policies to allow traffic between the two sites across the VPN tunnel.

Step	Description
1.	Assign the interfaces to the appropriate firewall map. By default, the Samsung iBG3026 creates two firewall maps:
	 internet – Untrusted interfaces connecting to the public WAN corp – Trusted interfaces connected to the local LAN
	The ethernet0/2 interface is assigned to the internet map while the VLAN created in Section 6.1 Step 3 is assigned to the corp map.
	<pre>sarak2/configure# firewall internet sarak2/configure/firewall internet# interface ethernet0/2 sarak2/configure/firewall internet# exit sarak2/configure# firewall corp sarak2/configure/firewall corp# interface vlan1.101 sarak2/configure/firewall corp# exit sarak2/configure#</pre>
2.	Configure firewall policies to allow IKE negotiation into the untrusted ethernet0/2 interface.
	<pre>sarak2/configure# firewall internet sarak2/configure/firewall internet# policy 1000 in self sarak2/configure/firewall internet/policy 1000 in# exit sarak2/configure/firewall internet# exit sarak2/configure#</pre>
3.	Configure firewall policies to allow transit traffic from the remote Juniper SSG 520 to the Samsung iBG3026.
	<pre>sarak2/configure# firewall corp sarak2/configure/firewall corp# policy 1000 in address 10.1.0.0 16 192.168.1.0 24 sarak2/configure/firewall corp/policy 1000 in# exit sarak2/configure/firewall corp# exit sarak2/configure#</pre>

6.4. Configure Quality of Service

Configure the Samsung iBG3026 to prioritize voice traffic across the VPN tunnel. The Samsung iBG3026 supports both software-based QoS in the operating system and hardware-based QoS enforced in the chipset. In this configuration, software-based QoS is utilized to ensure the bandwidth allocated for voice traffic is guaranteed across the VPN tunnel. The Samsung iBG3026 QoS implements Random Early Detection (RED) to address congestion and Class Based Queuing (CBQ) to address traffic policing for bandwidth management.

Step	Description								
1.	Configure CBQ on the VPN interface. A class called voip is created to classify voice								
	traffic and to assign QoS parameters for this class.								
	sarak2/configure# crypto								
	sarak2/configure/crypto# qos								
	sarak2/configure/crypto/qos# add-policy-class volp root-out								
	sarak2/configure/crypto/qos# add-policy-class default root-out								
	sarak2/configure/crypto/qos# policy-class voip								
	sarak2/configure/crypto/qos/policy-class volp# match-dscp 46								
	safakz/configure/crypto/qos/policy-class volp# cbq cf-percent 25 pi-percent 50								
	profity i								
	sarak2/configure/crypto/gos# policy-class default								
	sarak2/configure/crypto/gos/policy-class_default# match-dscp_default								
	sarak2/configure/crypto/gos/policy-class default# cbg cr-percent 50 pr-percent								
	75 priority 8								
	sarak2/configure/crypto/gos/policy-class default# exit								
	sarak2/configure/crypto/gos# enable cbq								
	sarak2/configure/crypto/gos# exit								
	sarak2/configure/crypto# exit								
	sarak2/configure#								

7. Verification Steps

The following steps can be used to verify that the configuration steps documented in these Application Notes have been done correctly.

7.1. Verify Juniper Networks SSG 520

From the left navigation menu, select **VPNs** > **Monitor Status** and the **VPN Monitor Status** screen appears. Locate the VPN (see **VPN Name**) configured in Section 5.4.2 Step 2. Verify that **SA Status** shows **Active** and **Link** shows **Up**.

		Delley ID	D	-		L. La La
VPN Name	SAID	POIICY ID	Peer Gateway IP	туре	SA Status	<u>Link</u>
HQ to Branch Office	00000001	-1/-1	2.2.2.1	AutoIKE	Active	Up

From the left navigation menu, select **Reports > System Log > Event** and the Event screen appears. The log shown below contains the IKE Phase 1 and IKE Phase 2 events logged as the VPN tunnel is being established.

Repo	rts > System Log > Eve	nt	ssg520sg1	?
List Sav	20 🔻 per page		Enter Description Search Refresh	All
	Date / Time	Level	Description	
	2007-05-12 06:14:26	crit	VPN 'HQ to Branch Office' from 2.2.2.1 is up.	
	2007-05-12 06:14:19	info	IKE<2.2.2.1> Phase 2 msg ID <e4834e7e>: Completed negotiations with SPI <e703d4c1>, tunnel ID <1>, and I <3600> seconds/<4194303> KB.</e703d4c1></e4834e7e>	lifetime
	2007-05-12 06:14:19	info	IKE<2.2.2.1> Phase 2 msg ID <e4834e7e>: Responded to the peer's first message.</e4834e7e>	
	2007-05-12 06:14:19	info	IKE<2.2.2.1>: Received initial contact notification and removed Phase 1 SAs.	
	2007-05-12 06:14:19	info	IKE<2.2.2.1> Phase 1: Completed Main mode negotiations with a <28800>-second lifetime.	
	2007-05-12 06:14:19	info	IKE<2.2.2.1>: Received initial contact notification and removed Phase 2 SAs.	
	2007-05-12 06:14:19	info	IKE<2.2.2.1>: Received a notification message for DOI <1> <24578> <initial-contact>.</initial-contact>	
	2007-05-12 06:14:19	info	IKE<2.2.2.1> Phase 1: Responder starts MAIN mode negotiations.	
	2007-05-12 06:13:25	notif	All logged events or alarms were cleared by admin root	

7.2. Verify Samsung Ubigate iBG3026

7.2.1. Verify Phase 1 Status

Enter the command **show crypto ike sa all**. Verify that the **State** of the policy shows **SA_MATURE**.

```
sarak2/configure# show crypto ike sa all

Policy Peer State Bytes Transform

ToHQ 1.1.1.1 SA_MATURE 1928 pre-g2-aes-shal

sarak2/configure#
```

7.2.2. Verify Phase 2 Status

Enter the command **show crypto ipsec sa all**. Verify that the IPSec policies for the tunnels going to and coming from the Juniper SSG 520 are created.

```
sarak2/configure# show crypto ipsec sa all

Policy Dest IP Spi Packets Transform

---- --- --- ---- ----

INTOHQ 2.2.2.1 0xdf6a8944 4113 esp-aes-shal-tunl

TOHQ 1.1.1.1 0xd903d4c1 3993 esp-aes-shal-tunl

sarak2/configure#
```

8. Conclusion

The Samsung Ubigate iBG3026 Gateway is able to interoperate with Juniper Networks SSG 520 Gateway to create a site-to-site VPN tunnel with QoS to support an Avaya IP telephony infrastructure.

9. Additional References

The following Avaya product documentation is available from <u>http://support.avaya.com</u>.

[1] Configuring the Samsung UbigateTM iBG3026 with Avaya SIP Enablement Services and Avaya Communication Manager, Issue 1.0, 12 Feb 2007

The following Samsung Ubigate iBG3026 guides are available from Samsung. Visit <u>http://www.samsungen.com</u> for company and product information.

[2] Ubigate iBG3026TM Configuration Guide
[3] Ubigate iBG3026TM Command Reference
[4] iBG3026_Installation Manual
[5] iBG3026_System Description
[6] iBG3026_Message Reference Manual

The following Juniper Networks product documentations are available from <u>http://www.juniper.net/techpubs/</u>:

- [7] Concepts & Examples ScreenOS Reference Guide; Volume 5: Virtual Private Networks, Release 5.4.0, Rev. A
- [8] Secure Services Gateway (SSG) 500 Series Hardware Installation and Configuration Guide ScreenOS Version 5.4.0

© 2007 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by \mathbb{B} and TM are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at <u>interoplabnotes@list.avaya.com</u>