

Time Sensitive Information!

These Configuration Changes Must Be Applied Ten Days Prior to Absolute VOICE Cut-Over

SonicWall 6.5 OS Router Configuration For Absolute VOICE Cloud Telephony Deployment Document Version 4.0

January 30th, 2018

www.callabsolute.com



Table of Contents

- 1. Introduction
- 2. Checklist
- 3. Basic Configuration
- 4. Traffic Shaping QoS Configuration
- 5. SSL Action Control
- 6. Security Exclusions IPS/Content Filtering

Read Me!

- 1. These changes must be applied before client implements their Absolute VOICE hosted telephony solution.
- 2. If you are <u>experienced</u> with business class firewalls and routers, please have your IT staff/contractor perform these changes for you.
- 3. Please read this entire document before attempting to make any changes.
- 4. If you have questions about this document, you can call 800-955-6703 to schedule an appointment with one of our firewall support specialists. We will attempt schedule your appointment within 24- 48 hours of your call to us so please allow adequate time.
- 5. After changes are completed please let your client or Absolute VOICE Customer Support specialist know.
- 6. Once completed, an Absolute VOICE technician will be requesting access or a collaborative web session to verify settings prior to customer cut over.

Introduction

This document is for IT administrators and illustrates configuration changes required on SonicWall firewall & router appliances to support Absolute VOICE's cloud communications telecommunications platform. This document assumes a basic network deployment consisting of one internal LAN network containing the IP phones and one WAN network connected to the Internet. While we strongly recommend a dedicated network for VoIP traffic, the instructions below can be used for a "converged" network whereby both VoIP and non-VoIP traffic share one physical WAN network. With basic modifications (such as adding access rules for additional interfaces); this configuration can be extrapolated for other network layouts. The screenshots below may vary slightly from what is displayed while configuring the device depending on model (i.e. NSA vs. Pro) and SonicOS Enhanced software version. Setting values not mentioned may be left at default or changed as required for specific purposes.



Please call Absolute VOICE Customer Support at 800-955-6703 if you need any further information. Firewall changes can be in depth and you will need to schedule time with one of our specialists if you need assistance.

Screenshots and instructions are based on TZ 300 running SonicOS Enhanced 6.5.0.2-8.

We recommend loading the latest SonicOS (firmware).



Screen Shot #:	Configuration:	Completed:
1	System \rightarrow Status	
2	Network \rightarrow Interfaces	
3	Network \rightarrow WAN Interface \rightarrow Advanced \rightarrow Bandwidth Management	
4	VoIP → Settings	
5	Firewall Settings → BWM	
6	Firewall Settings → SSL Control	
7	Objects \rightarrow Service Objects \rightarrow Expanded Abs VoIP Group	
8	Objects → Address Objects (Abs Subnet)	
9	Firewall \rightarrow Access Rules \rightarrow LAN to WAN Overview	
10	Firewall>Access Rules>Edit One Absolute VOICE Rule>Advanced Tab	
11	Firewall → Access Rules → Edit One Absolute VOICE Rule>Ethernet BWM Tab	
12	Firewall \rightarrow Access Rules \rightarrow WAN to LAN	
13	Security Services \rightarrow Content Filter \rightarrow CFS Exclusion List	
14	Security Services $ ightarrow$ Intrusion Prevention $ ightarrow$ Exclusion List	



Manage \rightarrow VoIP \rightarrow Settings

Connectivity	•		
VPN	General Settings		
SSL VPN			
Wireless	Enable consistent NAT		
3G/4G/Modem			
- CALC	SIP Settings		
Policies		197 N - 202 N	10000
Objects	Use global control to enable SIP Transformations Use firewall Ru	ile-based control to enable	e SIP Transform
	Enable SIP Transformations		
System Setup	Enable Transformations on TCP connections		
Appliance	Perform transformations for TCP/UDP port(s) in Service Object:	SIP	T
Users	Permit non-SIP packets on signaling port *		
High Availability	Enable SIP Back-to-Back User Agent (B2BUA) support		
WAN Acceleration	SIP Signaling inactivity time out (seconds): *	3600	
VOIP	SIP Media inactivity time out (seconds):	120	
Security Configuration	Additional SIP signaling port (UDP) for transformations (optional):	0	
Firewall Settings	Enable SIP endpoint registration anomaly tracking		
Security Services	Registration tracking interval (seconds):	300	
Decryption Services Anti-spam	Failed registration threshold:	5	
	Endpoint block interval (seconds):	3600	
Logs & Reporting	analysine successing factoringly.	here	
Appflow Settings			
Log Settings	H.323 Settings		

- Check "Enable consistent NAT"
- Uncheck " Enable SIP Transformations
- Click "Accept to Save"

Abs Vutevoice Manage -> Firewall Settings -> Bandwidth Management

and the second second	internet orrer seconds			
Policies	Priority	Enable	Guaranteed	Maximum\Burst
Rules	0 Realtime	8	15 %	100 %
Objects	1 Highest		0 %	100 %
System Setur	2 High	0	0 %	0 %
Appliance	3 Medium High		0 %	100 %
Users	4 Medium	2	0 %	100 %
Network High Availability	5 Medium Low		0 %	100 %
WAN Acceleration	6 Low	8	0 %	0 %
VOIP	7 Lowest	Ð	0 %	100 %
Security Configuration		Total:	15	15
Firewall Settings Advanced Settings	_			
Bandwidth Management				
Flood Protection				

- Set the "Bandwidth Management Type" to "Global"
- Check "Enable" for the priority "0 Realtime"
- "Realtime" "Guaranteed" percentage set to 10%
 - Adjust higher depending on the amount of bandwidth and phones.
- "Realtime" "Maximum\Burst" percentage set to 100%
- Disable all other Priorities by unchecking the "Enable" check box, except "Realtime".
- Set the "Medium" priority to 0% for "Guaranteed" percentage.

Note: Please ensure that all other Priorities are disabled.

Note: The "<u>Medium" queue</u> cannot be disabled but we need to set the "Guaranteed" percentage to <u>0%.</u>



- Click the "Add" button under "<u>Services Objects</u>" tab to create the Absolute VOICE service ports:
 Create the following Services:
 - AbsRTPext
 - Protocol:
 - Protocol: UDP
 Dort stort: 1000
 - Port start: 16000
 - Port end: 16999
 - AbsRTPint
 - Protocol: UDP
 - Port start: 11780
 - Port end: 11800
 - AbsSIP9000
 - Protocol: UDP
 - Port start: 9000
 - Port end: 9000
- Click the "Service Groups" tab and click the "Add" button to create a Service Object:
 - Name the object: AbsVoIPGrp
 - Add the following services:
 - SIP
 - AbsSIP9000
 - AbsRTPext
 - AbsRTPint

See below and following page for screen shots.

Connectivity VPN	* Service	Okjests Service	e Groups				λ.N			Mode: Config
SSL VPN Access Points Wireless	⊕ Ad	t 🕞 Delete 🔹	Search	Vew All Types • C						
36/46/Hodem	• 11	Name Otris TOF (Jesus	n Relability (Protocol 109	Port Start 25%	Port End 2518	Class Default	Comments	Configure
Pulicies	0.12	Cera UDP			ND4	1604	1604	Default	ø	20
Rales Objecta	0.0	OwRTPExt			UDP	16000	16999	Custum	17	08
Hatch Objects	E 24	OwATFlat			UCP	11790	11800	Custon	ø	@8
Action Objects Address Objects	8 15	DexSIP9000			UD#	8000	9000	Custom	ø	28
Sandere Oligiecha	1.11	cu-seenie			NOP	24032	24032	Default	9	(20)







Objects → Address Objects

• Click on the Add button below the "Address Objects"

🕀 Add	⊖ Delete ▼ Search	Show IPv4 & IPv6 -
	Name	Details
1	Default Active WAN IP	10.203.28.196/255.255.255.255
2	Default Gateway	0.0.0/255.255.255.255

- Click the "Add" button under Address Objects section to create the Absolute VOICE subnet object:
 - Create the following Services:
 - Absolute VOICE Servers
 - Zone Assignment: WAN
 - Type: Network
 - IP Address: 184.178.213.0
 - Netmask: 255.255.255.0

Add	d Address Object - Google Chrome 🕒 🗖 🗙
A Not secure htt	ps://192.168.1.1/addNetObjDlg.html?objTypes=159
Sonic	Network Security Appliance
Name:	Absolute VOICE Servers
Zone Assignment:	WAN
Type:	Network 🔻
Network:	184.178.213.0
Netmask/Prefix Length:	255.255.255.0
Ready	
	OK CANCEL



Rules \rightarrow **Access Rules** (Create LAN to WAN Rule for Abs Ports)

Click on "Add..." to bring up a dialog for adding a new firewall access rule. This rule will setup the priority and timers for the SIP/RTP ports.

e	Add Rule - Google	Chrome 📃 🗖
A Not secure	https://192.168.1.1/addRuleDlg.html?ob	Types=15935
SONICW	ALL Network Security Appliance	5
General	Advanced QoS BWM Geolf	
Action:	Allow Deny Discard	
From :	LAN	
To :	WAN	
Source Port	Any	•
Service:	AbsVoIPGRP	i
Source:	Any	
Destination:	Any	
Users Included:	All	these users will be allowed if not ex
Users Excluded:	None	these users will be denied.
Schedule:	Always on	
Comment	Abs VoIP Traffic	
IP Version:	● IPv4 ◎ IPv6	
Enable L	ogging Enable	e Botnet Filter
Allow Fra	gmented Packets	e SIP Transformation
Enable fi	ow reporting Enable	e H.323 Transformation
- Cashie a	and an address	

- Check "Allow" for "Action"
- "From Zone" set to LAN
- "To Zone" set to WAN
- "Service" set to CrexVoIPGrp
- "Source" set to Any
- "Destination" set to Any
- "Users Allowed" set to All
- "Schedule" set to Always on
- "Comment" set to Abs VoIP Traffic
- Check "Enable Logging"
- Check "Allow Fragmented Packets"
- Click on the "Advanced" tab (continued on next page)



Add Rule - Google C	hrome	
Not sequre https://192.168.1.1/addRuleDlg.html?obj	lypes=1	5935#
SONIC WALL Network Security Appliance		
General Advanced QoS BWM GeolP		
TCP Connection Inactivity Timeout (minutes):	15	
UDP Connection Inactivity Timeout (seconds):	80	
Number of connections allowed (% of maximum connections)	100	
Enable connection limit for each Source IP Address	128	Threshold
Enable connection limit for each Destination IP Address	128	Threshold
Create a reflexive rule		
Disable DPI		

- "UDP Connection Inactivity Timeout (seconds)" set to 80
- Click on the "QoS" tab

CCD Marking C	ettings
DSCP Marking S	ettings
DSCP Marking Action:	Preserve 👻
Note: DSCP values in p	packets will remain unaltered.
Note: DSCP values in p	packets will remain unaltered.
Note: DSCP values in p	packets will remain unaltered.
Note: DSCP values in p 302.1p Marking	packets will remain unaltered. Settings
Note: DSCP values in p 802.1p Marking	packets will remain unaltered. Settings
Note: DSCP values in p 302.1p Marking 802.1p Marking Action:	packets will remain unaltered. Settings None

- "DSCP Marking Action" set to Preserve
- Click on the "Ethernet BWM" tab (continued on next page)



Not secure https://192.168.1.1/	addRuleDlg.html?objTypes=15
General Advanced QoS	BWM GeoIP
Enable Egress Bandwidth Mana Bandwidth Priority:	gement ('allow' rules only) 0 Realtime
Enable Ingress Bandwidth Mana Bandwidth Priority:	agement ('allow' rules only) 0 Realtime
Note: BWM Type: Global; To change	go to Firewall Settings > BWM

- Check "Enable Outbound Bandwidth Management ('allow' rules only)"
 Bandwidth Priority set to "0 Realtime"
- Check "Enable Inbound Bandwidth Management ('allow' rules only)"
 Bandwidth Priority set to "0 Realtime"
- Click "Add" to add the rule set



Click on "Add..." to bring up a dialog for adding a new firewall access rule.

Advanced QoS BWH GeolP Action: Allow Deny Discard From: LAN To: WAN Van WAN Source Port: Any Source: Any Source: Any Destination: AbsServers Included: All Users None Excluded: None Schedule: Always on Comment: AbsServers Traffic IP Version: IPv4 IP Version: IPv4 Included: IPv6	100	ALL Heriork Security Appli	ance	52
Action: Allow Deny Discard From: LAN To: WAN Source Port: Any Service: Any Destination: AbsServers Users Included: All Users Excluded: None Excluded: None Excluded: All Users Excluded: None Excluded:these users will be allowed if n Users Excluded:these users will be denied. Schedule: Always on Comment: AbsServers Traffic IP Version: IPV4 IPv6 Enable Logging Enable Botnet Filter	General	Advanced QoS BWM	GeolP	
From : LAN To : WAN Source Port: Any Service: Any Source: Any Source: Any Destination: AbsServers Users All Included: None Excluded: None Schedule: Always on Comment: AbsServers Traffic IP Version: IPv4 IPv6 Enable Botnet Filter 	Action:	Allow O Deny O Discard		
To: WAN Source Port: Any Service: Any Source: Any Destination: AbsServers Users All Included: All Users None Excluded: None Schedule: Always on Comment: AbsServers Traffic IP Version: IPv6 Enable Botnet Filter 	From :	LAN	٠	
Source Port: Any Service: Any Source: Any Destination: AbsServers Users All these users will be allowed if n Users None these users will be denied. Schedule: Always on Comment: AbsServers Traffic IP Version: IP V4 IPV6 Enable Logging Enable Botnet Filter	To :	WAN	۲	
Service: Any Source: Any Destination: AbsServers Included: All Users All Included: None Excluded: None Schedule: Always on Comment: AbsServers Traffic IP Version: ● IPv6 ● Inpu6	Source Port:	Any	•	•
Source: Any Destination: AbsServers Users All Included: All Users None Excluded: None Schedule: Always on AbsServers Traffic IP Version: ● IPv4 IP Version: ● IPv6 Enable Logging ■ Enable Botnet Filter	Service:	Any	۲	
Destination: AbsServers Users All Included: All Users None Excluded: None Schedule: Always on Comment: AbsServers Traffic IP Version: ● IPv6 ✓ Enable Logging	Source:	Any	۲	
Users All these users will be allowed if in Users Excluded: None these users will be denied. Schedule: Always on Comment: AbsServers Traffic IP Version: IP Version: IP Version: IP Version: IP Logging Enable Botnet Filter	Destination:	AbsServers	•	
Users Excluded: None these users will be denied. Schedule: Always on Comment: AbsServers Traffic IP Version: IP V4 IPv6 Enable Logging Enable Botnet Filter	Users Included:	All	٣	these users will be allowed if not ex
Schedule: Always on Comment: AbsServers Traffic IP Version: IP V4 IPv6 Enable Logging Enable Botnet Filter	Users Excluded:	None	*	these users will be denied.
Comment: AbsServers Traffic IP Version: IP V4 IPv6 Enable Logging Enable Botnet Filter	Schedule:	Always on	۲	
IP Version: IPv4 IPv6 IPv6 Inv6 Enable Logging Enable Botnet Filter	Comment:	AbsServers Traffic		
Enable Logging Enable Botnet Filter	IP Version:	● IPv4 ◎ IPv6		
	Enable L	ogging	Enable	Botnet Filter
Allow Fragmented Packets Enable SIP Transformation	Allow Fra	gmented Packets	Enable	SIP Transformation

- Check "Allow" for "Action"
- "From Zone" set to LAN
- "To Zone" set to WAN
- "Service" set to Any
- "Source" set to Any
- "Destination" set to CrexServers
- "Users Allowed" set to All
- "Schedule" set to Always on
- "Comment" set to Abs Traffic
- Check "Enable Logging"
- Check "Allow Fragmented Packets"
- Click on the "Advanced" tab (continued on next page)



Add Rule - Google C	hrome	
Not sequre https://192.168.1.1/addRuleDlg.html?obj	lypes=1	5935#
SONIC WALL Network Security Appliance		
General Advanced QoS BWM GeolP		
TCP Connection Inactivity Timeout (minutes):	15	
UDP Connection Inactivity Timeout (seconds):	80	
Number of connections allowed (% of maximum connections)	100	
Enable connection limit for each Source IP Address	128	Threshold
Enable connection limit for each Destination IP Address	128	Threshold
Create a reflexive rule		
Disable DPI		

- "UDP Connection Inactivity Timeout (seconds)" set to 80
- Click on the "QoS" tab

CCD Marking C	ottings
DSCP Marking S	lettings
DSCP Marking Action:	Preserve 💌
Note: DSCP values in p	packets will remain unaltered.
Note: DSCP values in p	packets will remain unaltered.
Note: DSCP values in p	packets will remain unaltered.
Note: DSCP values in p 302.1p Marking	packets will remain unaltered. Settings
Note: DSCP values in p 802.1p Marking	packets will remain unaltered. Settings
Note: DSCP values in p 302.1p Marking 802.1p Marking Action:	packets will remain unaltered. Settings None

- "DSCP Marking Action" set to Preserve
- Click on the "Ethernet BWM" tab (continued on next page)



Add Rule - Google Chrome /addRuleDlg.html?objTypes=15
Security Appliance
BWM GeolP
agement ('allow' rules only) 0 Realtime
agement ('allow' rules only)
0 Realtime 🔻
e go to Firewall Settings > BWM

- Check "Enable Outbound Bandwidth Management ('allow' rules only)" o Bandwidth Priority set to "0 Realtime" •
- Check "Enable Inbound Bandwidth Management ('allow' rules only)" o Bandwidth Priority set to "0 Realtime" •



Prioritize the new Absolute VOICE access rules: Firewall ->

Access Rules

- Sort the Matrix via LAN → WAN
- Select the Priority up/down arrows to set the Absolute VOICE SIP, RTP and IP's (if created) as the top priority.

474 55, 479		⊕ Að	1 6	Delete •	Search	6	IPv4 & IPv6	Vara All Types •	¢ ₽• 1	X O P	om LAN • T	WAN - III
Access Points Wireless				fram	74	Priority	Searce	Destination	Service	Action	Users Incl.	Uners Fact
3G/4G/Hodem	х.	0.1	я	LAN	WAN	1.88	âty	Any	CrevialPGra	Abe	48	Nove
and the second se		0.2	14	LAN	wate .	z 88	Any	Absolute VOICE Servers	any	Alter	48	Nord
Rules		0.1	H	LAN	10446	a 88	Any	Any	Any	Allen		fore
Access Fales		0.4	14	LAN .	was	+ 88	Any	Any .	My	Alter	.4	Nove



Firewall -> Access Rules (Create WAN to LAN Rule for Inbound Abs Subnet)

Click on "Add..." to bring up a dialog for adding a new firewall access rule. This rule will setup the priority and timers for the SIP/RTPports.

	Add Rule - Google Chro	me 💶 🕻
Not secure	https://192.168.1.1/addRuleDlg.html?objType	s=15935
SONICW	Network Security Appliance	R
General	Advanced QoS BWM GeoIP	
Action:	Allow O Deny O Discard	
From :	LAN ·	
To :	WAN •	
Source Port	Any	
Service:	Any	
Source:	AbsServers	
Destination:	Any	
Users Included:	All •	these users will be allowed if not ex
Users Excluded	None *	these users will be denied.
Schedule:	Always on 🔻	
Comment	Inbound Absolute VOICE Server Traffic	
IP Version:	IPv4 IPv6	
Enable L	ogging Enable Botn	et Filter
Allow Fra	gmented Packets Enable SIP	Transformation
Enable fi	ow reporting Enable H.32	3 Transformation
Cashie a	adiat manitas	

- Check "Allow" for "Action"
- "From Zone" set to WAN
- "To Zone" set to LAN
- "Service" set to Any
- "Source" set to "Absolute VOICE Servers"
- "Destination" set to Any
- "Users Allowed" set to All
- "Schedule" set to Always on
- "Comment" set to "Inbound Absolute VOICE Server Traffic
- Check "Enable Logging"
- Check "Allow Fragmented Packets"
- Click on the "Advanced" tab (continued on next page)



DNICWALL	Network Security	Appliance			
General Advance	ed QoS BW	GeolP			
TCP Connection Inact	ivity Timeout (minutes)	t.	15		
UDP Connection Inact	ivity Timeout (seconds):	80		
Number of connection	s allowed (% of maxim	um connections):	100		
Enable connection	limit for each Source	IP Address	128	Threshold	
Enable connection	limit for each Destina	tion IP Address	128	Threshold	
Create a reflexive	rule				
Disable DPI					
For traffic from an una	uthenticated user:				
Don't redirect u	inauthenticated users t	to log in			

- "UDP Connection Inactivity Timeout (seconds)" set to 80
- Click on the "QoS" tab
 - Settings remain default

DSCP Marking Se	ettings	
DSCP Marking Action:	Preserve	•
Note: DSCP values in r	ackete will remain unaltered	
Note. Door values in p	ackets will remain unaltered.	
Note: Door values in p	ackets will remain unaltered.	
Note: Door values in p	ackets win remain unaitereu.	
302.1p Marking	Settings	
802.1p Marking	Settings	
802.1p Marking Action:	Settings	×

- "DSCP Marking Action" set to Preserve
- Click on the "Ethernet BWM" tab (continued on next page)



ot secure https://192.168.1.1/addRuleDlg.html?objTypes=15935 NICULE Network Security Appliance General Advanced QoS BWM GeolP Bandwidth Management Enable Egress Bandwidth Management ('allow' rules only) Bandwidth Priority: 0 Realtime	A	dd Rule - Google Chrome
Metwork Security Appliance General Advanced QoS BWH GeolP Bandwidth Management GeolP GeolP GeolP Bandwidth Management O Realtime Image: Comparison of the security	Not secure https://192.168.1.1/a	ddRuleDlg.html?objTypes=15935#
General Advanced QoS BWH GeolP Bandwidth Management GeolP GeolP Enable Egress Bandwidth Management ('allow' rules only) Bandwidth Priority: 0 Realtime Enable Ingress Bandwidth Management ('allow' rules only) Bandwidth Priority: 0 Realtime	DNICWALL Network Se	ecurity Appliance
 Enable Egress Bandwidth Management ("allow' rules only) Bandwidth Priority: 0 Realtime Enable Ingress Bandwidth Management ('allow' rules only) Bandwidth Priority: 0 Realtime 	General Advanced QoS Bandwidth Management	BWM GeoIP
Bandwidth Priority: 0 Realtime Enable Ingress Bandwidth Management ('allow' rules only) Bandwidth Priority: 0 Realtime	Enable Egress Bandwidth Manag	gement ('allow' rules only)
 Enable Ingress Bandwidth Management ('allow' rules only) Bandwidth Priority: 0 Realtime 	Bandwidth Priority:	0 Realtime
Bandwidth Priority: 0 Realtime •	Enable Ingress Bandwidth Manag	gement ('allow' rules only)
	Bandwidth Priority:	0 Realtime
lote: BWM Type: Global; To change go to Firewall Settings > BWM	Note: BWM Type: Global; To change g	go to Firewall Settings > BWM

- Check "Enable Outbound Bandwidth Management ('allow' rules only)"
 Bandwidth Priority set to "0 Realtime"
- Check "Enable Inbound Bandwidth Management ('allow' rules only)"
 Bandwidth Priority set to "0 Realtime"
- Click Add to save the Rule



Instructions for configuring the SonicWall to prioritize the voice traffic and shape other traffic for optimal performance. You must have already completed the basic configuration above for the traffic shaping to work properly.

Determine the Upload and Download Speeds

With a computer behind the router point your browser to <u>http://www.speedtest.net</u> and then click Begin Test.

Once the test is completed you should be provided with both an Upload (also referred to as Egress and Outbound Bandwidth) and Download (also referred to as Ingress and Inbound Bandwidth) speed. Record this as you will need it in the next step for configuring traffic shaping.

For DSL and cable connections you may want to lower the results by 5% or more to allow for varying line conditions.



Locate the WAN interface and click configure for interface configuration.

Under the interface configuration click on the "Advanced" tab.

← → C ▲ Not secure	https://192.168.1.1	/main.html	Edit Interface	- X1 - Google Chrome	- 0
🖽 Apps 😁 Error 🍉 TLG Re	set For Slow 🛷 E	aseus Home Page	A Not secure https://192.168.1.1/editin	terface_1.html#	
SONICWALL	Network Security App	liance MON	SONICWALL Network Securit	y Appliance	
Updates Licenses	Interface Se	ettings	Expert Mode Settings		9
Firmware & Backups	* Name	Zone	use nouced mode - Add real Policy to previ	fint outpound/indourie translation	
Restart	X0	LAN	NAT Policy outbound/inbound interface:	(and	
	×1*	WAN	Interface MTU:	1500	
Connectivity	22	Unassigned	Fragment non-VPN outbound packets large	r than this Interface's MTU	
VPN			Ignore Don't Fragment (DF) Bit		
SSL VPN	₩0	WLAN	Do not send ICHP Pragmentation Needed f	or outbound packets over the Interface	нти
Wireless	W0:V20	WLAN			
3G/4G/Hodem	Add Interface:	-Select Interface	Bandwidth Management		
Policies			244 BC34 CT		
Rules			🖉 Enable Egress Bandwidth Management		
Objects	Interface	Traffic Statist	Available Interface Egress Bandwidth (Kbs	s); 150000	
System Setup	Name	Rx Unicest Par	😤 Enable Ingress Bandwidth Management		
Appliance	×D	25,598,302	Available Interface Ingress Bandwidth (Kb	ps)c 150000	
Users	X1	48,230,179	Note: BWM Type: Global; To change go to Fine	wall Settings > BWH	
Network	X2	0	Ready		
Interfaces	W0	3,232,970			
PortShield Groups Pailover & Load Balancing Zones DNS DNS Provy	W0:V20	2,845,205	1	OK	HELP

- Check "Enable Egress Bandwidth Management"
 - "Available Interface Egress Bandwidth (Kbps)" set to the upload speed you got from your speed test in Kbps.
- Check "Enable Ingress Bandwidth Management"
 - "Available Interface Ingress Bandwidth (Kbps)" set to the download speed you got from your speed test in Kbps.
- <u>Note:</u> The picture above is showing 150mbps upload and 150mbps download. <u>Please enter</u> <u>the correct upload and download speed of your internet connection</u> otherwise it will throttle your network speeds.



SSL Action Control (Firewall Settings→SSL Control)



- Change the radio button for SSL Action.
 - o Click on "Log the event"
 - Click Accept to save
- Note: This setting may affect application requests being blocked from Absolute VOICE servers for services such as Hot Desking, etc...



Security Services → Content Filter

System Setup Appliance Users	Enable Local CFS Server Primary Local CFS Server:	P	second(s)
 Network High Availability WAN Acceleration 	Secondary Local CFS Server:		
VOIP Security Configuration	CFS Exclusion		
 Firewall Settings Security Services Base Setup 	Excluded Address:	Absolute VOICE Servers	•
Content Filter Client AV Enforcement Client CE Enforcement	CFS Policies		

- Click on "Enabled CFS Exclusion List"
- In the drop down select the "Absolute VOICE Servers" network object created earlier
 0 184.178.213.0/24
- Click Accept to save



Security Service Exclusions – Intrusion Prevention (IPS)

Security Services → Intrusion Prevention

If this feature is licensed and enabled.



- Click on the "Configure IPS Settings" button
- Click on check box for "Enable IPS Exclusion List"
- Click the radio button and select the "Absolute VOICE Servers" network object
- Click OK
- Click Accept to Save



Version	Reason for Change	Date
1.0 Draft	Initial Draft Document	September 6, 2012
2.0 Draft	Updated SIP settings and addition of Absolute VOICE Server Addresses	May 1, 2013
3.0 Draft	Updated BWM settings and grouping of ports to simplify configuration	May 22, 2014
3.2	Sonicwall Version Update	April 21 st , 2015
3.3	Added SSL Action Update	January 16 th , 2016
3.4	Updated BWM Notated WAN interface Ingress/Egress Security Exclusions – IPS/Content	April 4 th , 2016
3.5	WAN – LAN Rule added. Checklist added	March 16 th , 2017
4.0	Document updated for 6.5+ firmware	January 20 th , 2018