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

Table of Contents

Read Me!

1. These changes must be applied before client implements their Absolute VOICE hosted telephony solution.
2. If you are experienced 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.

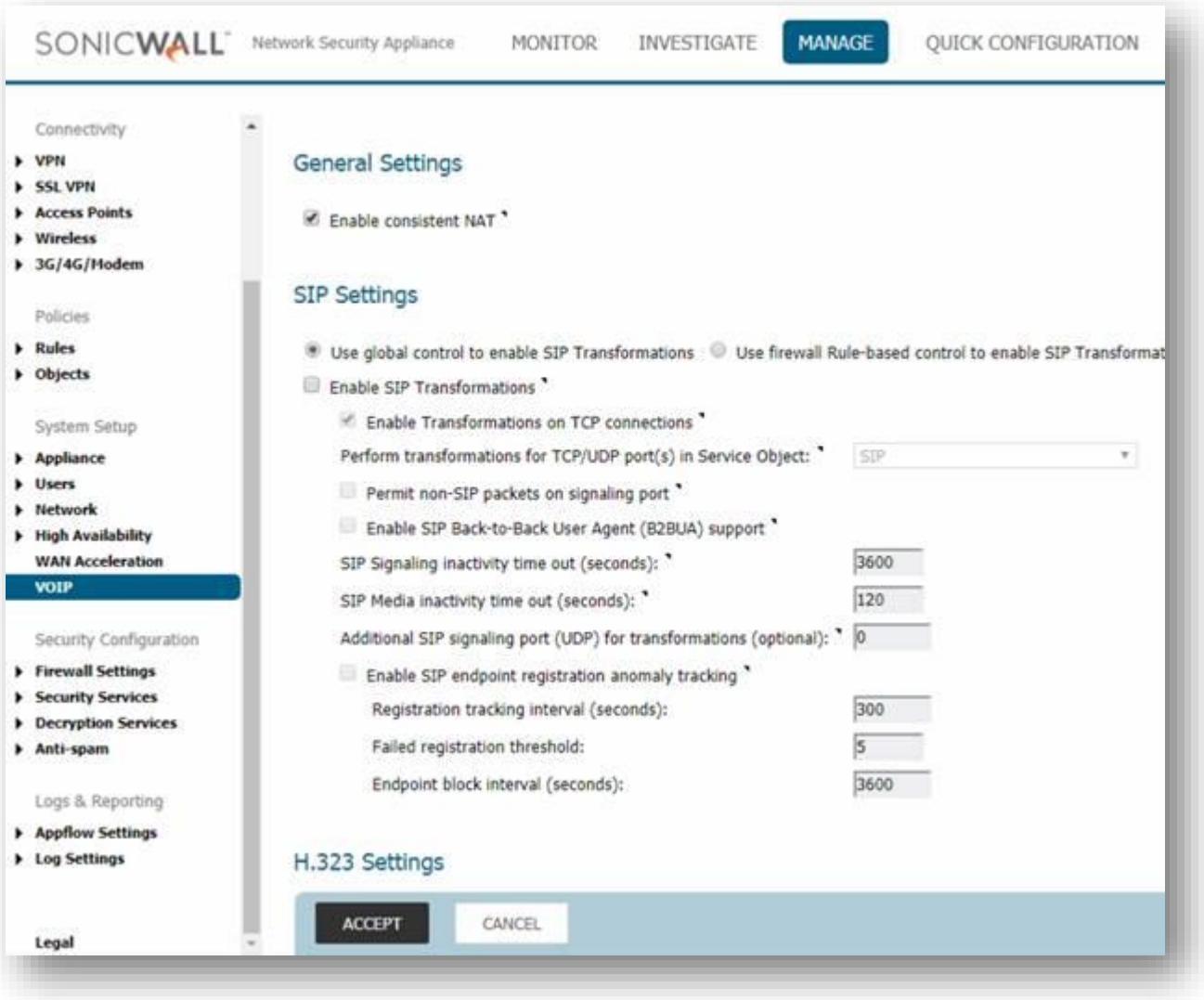
We recommend loading the latest SonicOS (firmware).

Firewall Checklist

Screen Shot #:	Configuration:	Completed:
1	System → Status	
2	Network → Interfaces	
3	Network → WAN Interface → Advanced → Bandwidth Management	
4	VoIP → Settings	
5	Firewall Settings → BWM	
6	Firewall Settings → SSL Control	
7	Objects → Service Objects → Expanded Abs VoIP Group	
8	Objects → Address Objects (Abs Subnet)	
9	Firewall → Access Rules → 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 → Access Rules → WAN to LAN	
13	Security Services → Content Filter → CFS Exclusion List	
14	Security Services → Intrusion Prevention → Exclusion List	

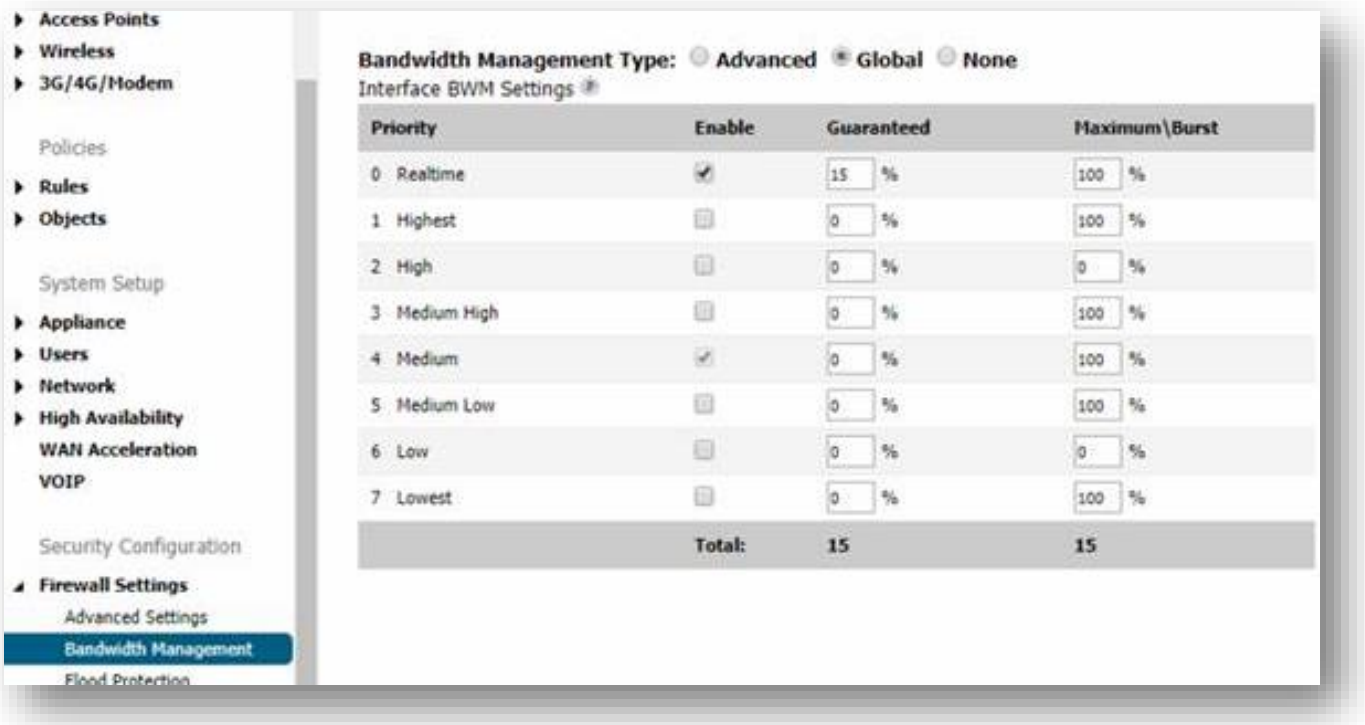
Basic Configuration

Manage → VoIP → Settings



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

Manage → Firewall Settings → Bandwidth Management



- 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.

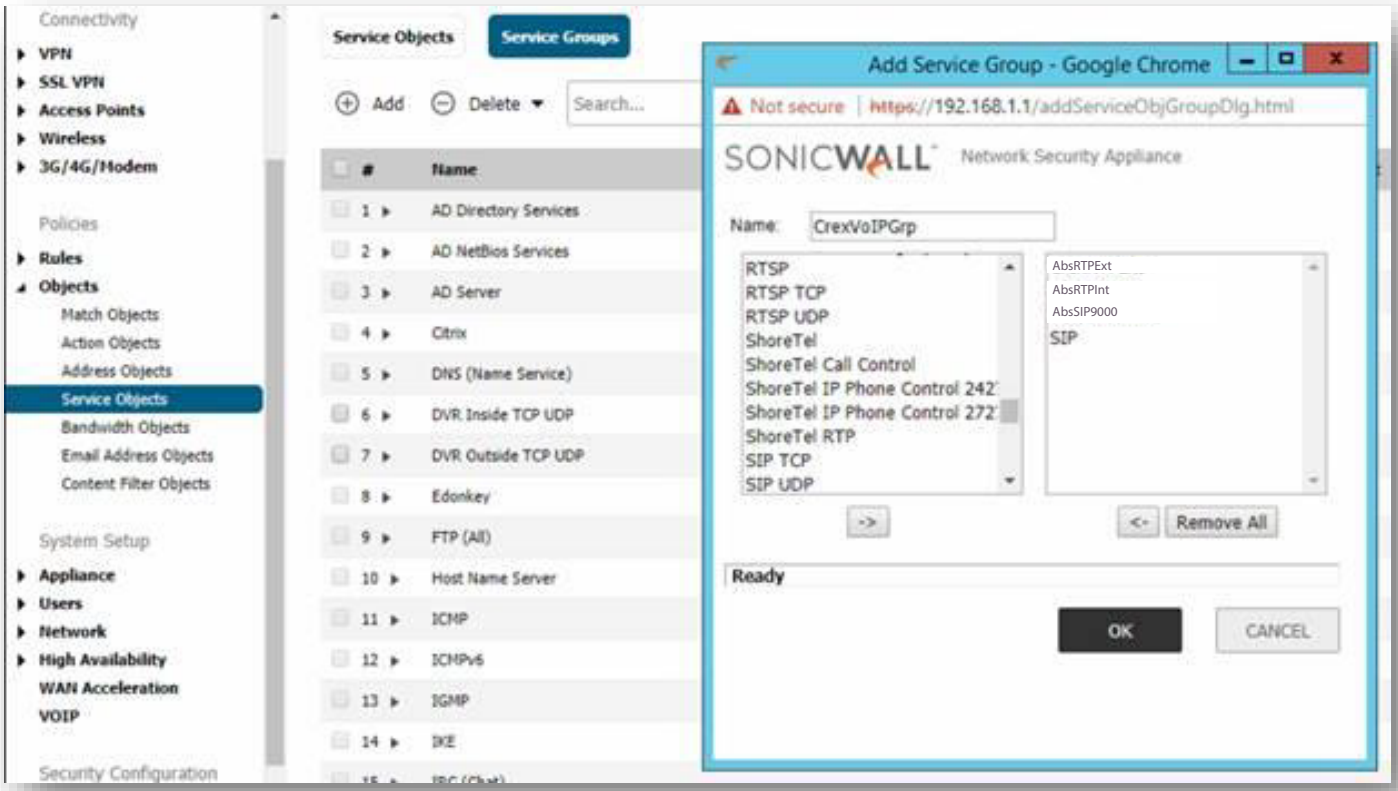
Note: Please ensure that all other Priorities are disabled.
Note: The “Medium” queue cannot be disabled but we need to set the “Guaranteed” percentage to 0%.

Manage → Objects → Service Objects

- Click the “Add” button under “Services Objects” tab to create the Absolute VOICE service ports:
  - Create the following Services:
    - AbsRTPext
      - Protocol: UDP
      - Port start: 16000
      - Port end: 16999
    - AbsRTPint
      - Protocol: UDP
      - Port start: 11780
      - Port end: 11800
    - AbsSIP9000
      - Protocol: UDP
      - Port start: 9000
      - Port end: 9000

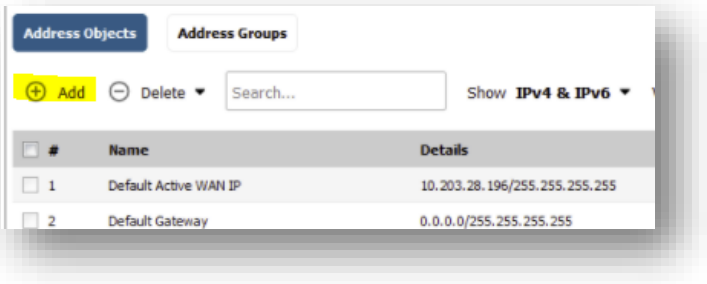
- Click the “Service Groups” tab and click the “Add” button to create a Service Object:
  - Name the object: AbsVoIPGrp
  - Add the following services:
    - SIP
    - AbsSIP9000
    - AbsRTPext
    - AbsRTPint

See below and following page for screen shots.

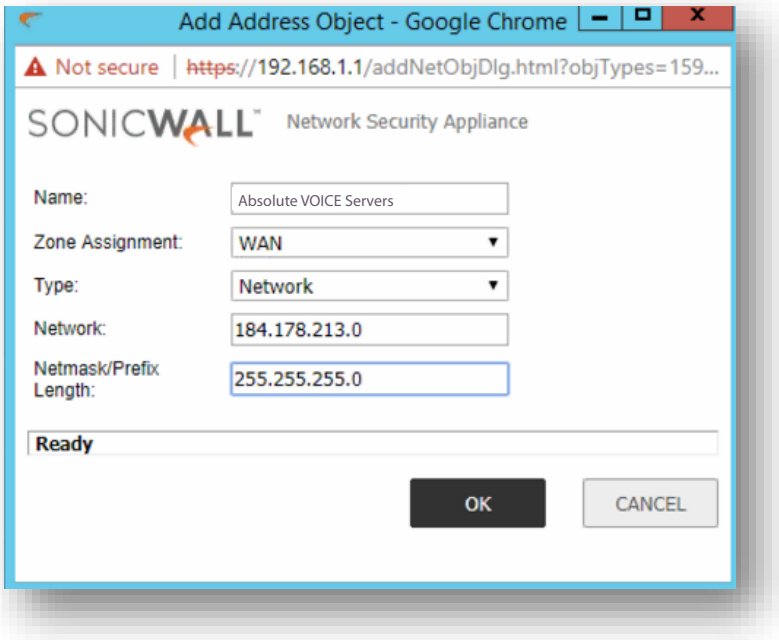

Connectivity
VPN
SSL VPN
Access Points
Wireless
3G/4G/Modem
Policies
Rules
Objects
Match Objects
Action Objects
Address Objects
Service Objects
Bandwidth Objects
Email Address Objects
Content Filter Objects
System Setup
Appliance
Users
Network
High Availability
WAN Acceleration
VOIP
Security Configuration
Service Objects
Service Groups
Add
Delete
Search...
Name
1 AD Directory Services
2 AD NetBios Services
3 AD Server
4 Citrix
5 DNS (Name Service)
6 DVR Inside TCP UDP
7 DVR Outside TCP UDP
8 Edonkey
9 FTP (All)
10 Host Name Server
11 ICMP
12 ICMPv6
13 IGMP
14 IKE
Add Service Group - Google Chrome
Not secure | https://192.168.1.1/addServiceObjGroupDlg.html
SONICWALL Network Security Appliance
Name: CrexVoIPGrp
RTSP
RTSP TCP
RTSP UDP
ShoreTel
ShoreTel Call Control
ShoreTel IP Phone Control 242
ShoreTel IP Phone Control 272
ShoreTel RTP
SIP TCP
SIP UDP
AbsRTPExt
AbsRTPInt
AbsSIP9000
SIP
->
<-
Remove All
Ready
OK
CANCEL

Objects → Address Objects

- Click on the Add button below the “Address Objects”

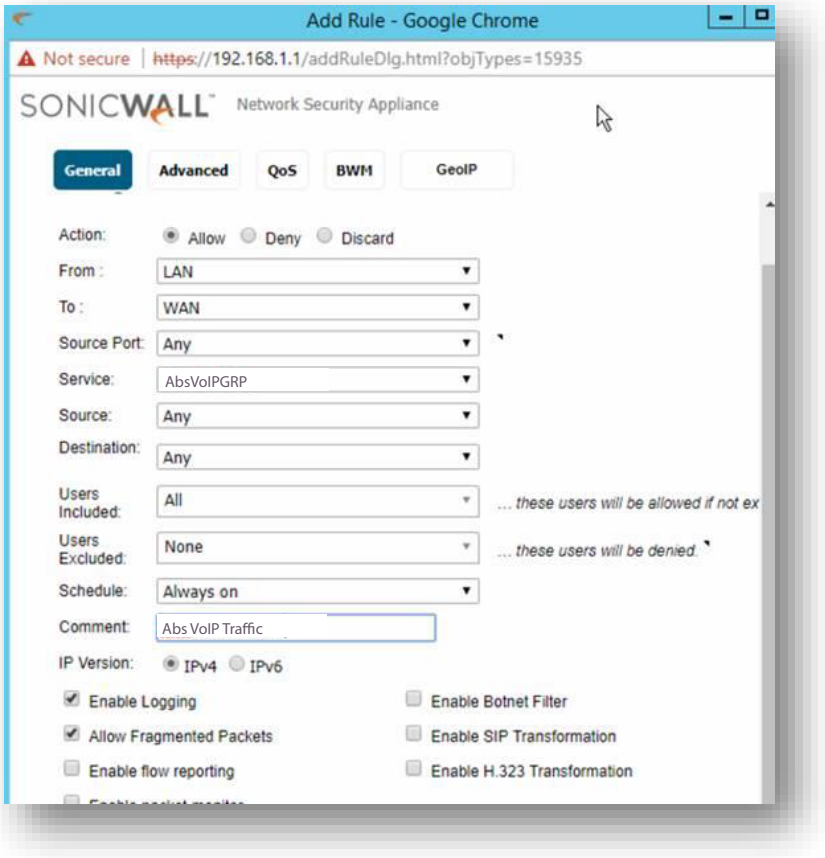


- Click the “Add” button under Address Objects section to create the Absolute VOICE subnet object:
  - Create the following Services:
    - Absolute VOICE Servers
      - Zone Assignment: WAN
      - Type: Network
      - IP Address: 184.178.213.0
      - Netmask: 255.255.255.0



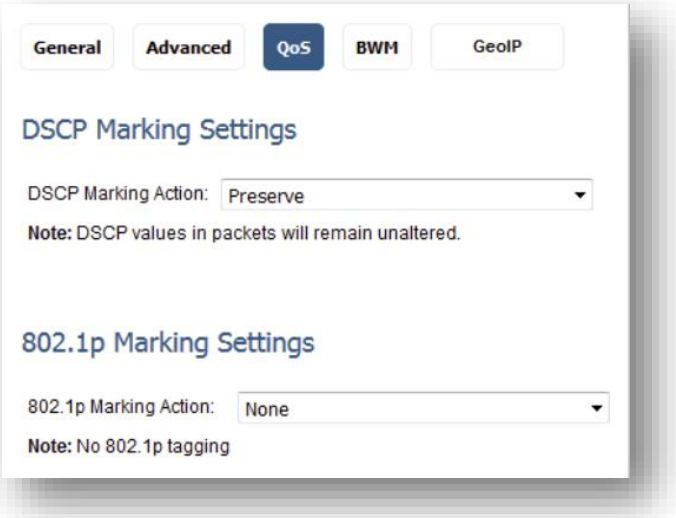
Rules → Access Rules (Create LAN to WAN Rule for Abs Ports)

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.

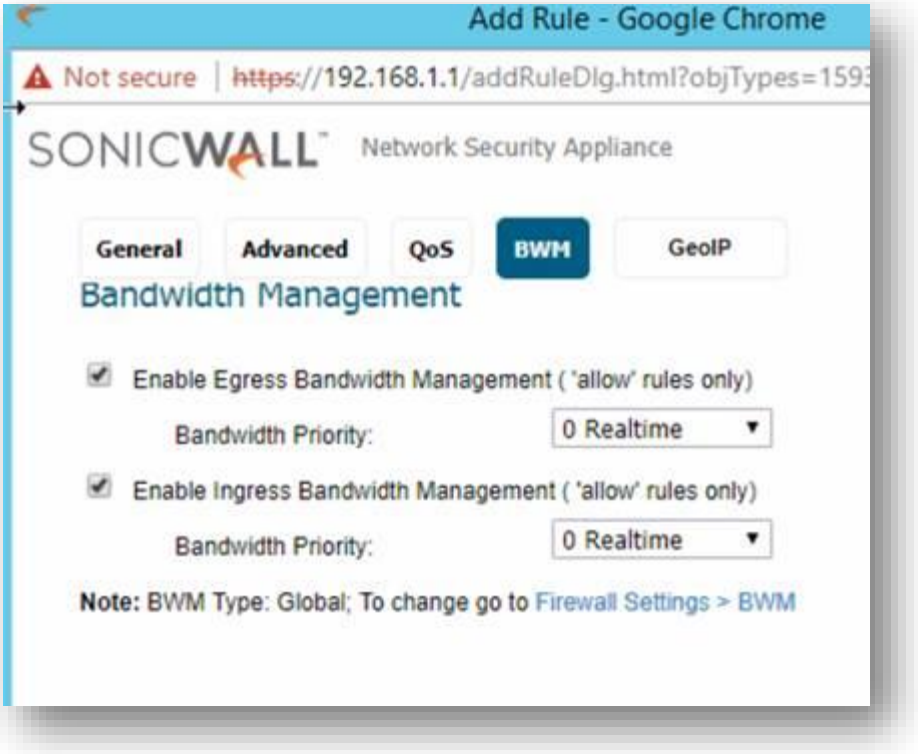


- Check “Allow” for “Action”
- “From Zone” set to LAN
- “To Zone” set to WAN
- “Service” set to CrexVoIPGrp
- “Source” set to Any
- “Destination” set to Any
- “Users Allowed” set to All
- “Schedule” set to Always on
- “Comment” set to Abs VoIP Traffic
- Check “Enable Logging”
- Check “Allow Fragmented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

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



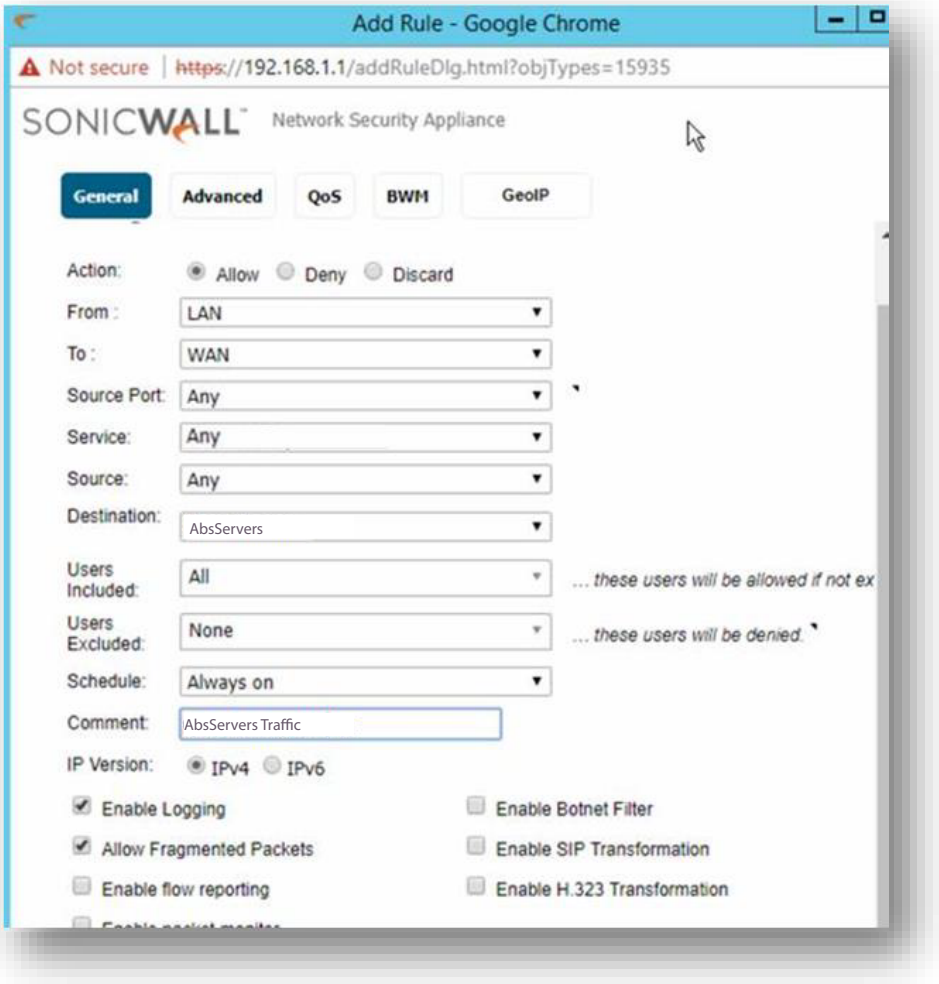
- "DSCP Marking Action" set to Preserve
- Click on the "Ethernet BWM" tab (continued on next page)



- 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

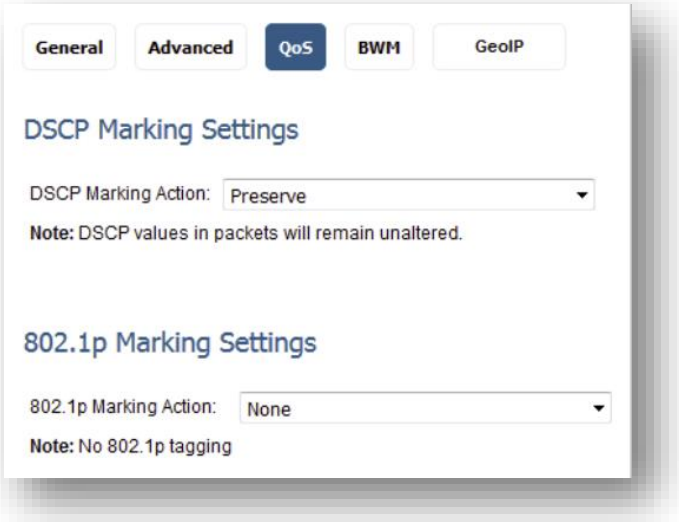
Firewall → Access Rules (Create LAN to WAN Rule for Abs IP Subnet)

Click on “Add…” to bring up a dialog for adding a new firewall access rule.

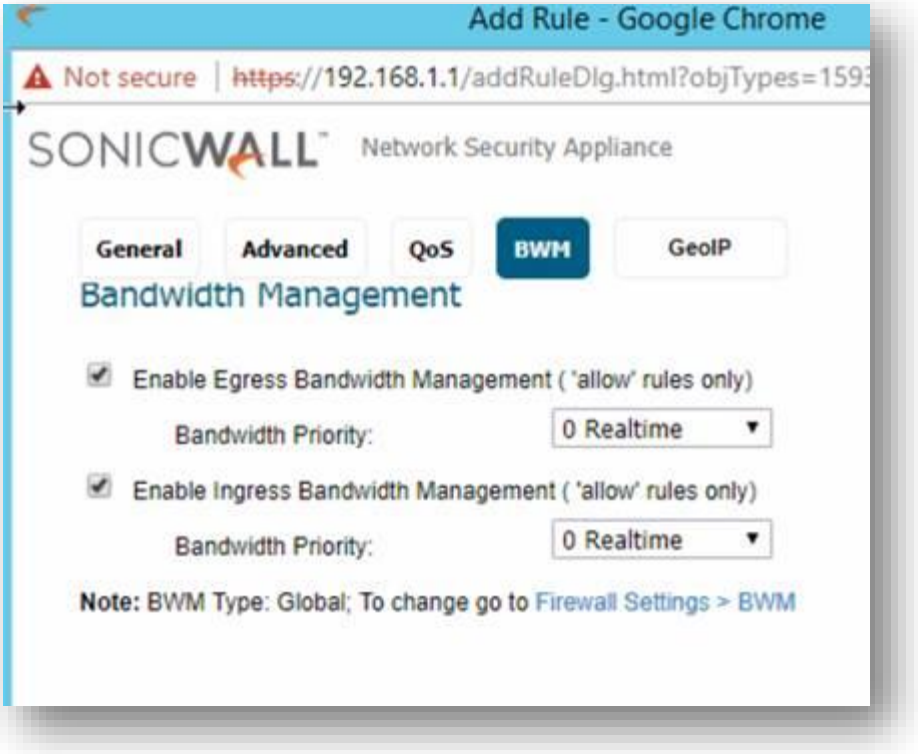


- Check “Allow” for “Action”
- “From Zone” set to LAN
- “To Zone” set to WAN
- “Service” set to Any
- “Source” set to Any
- “Destination” set to CrexServers
- “Users Allowed” set to All
- “Schedule” set to Always on
- “Comment” set to Abs Traffic
- Check “Enable Logging”
- Check “Allow Fragmented Packets”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

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



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



- 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”

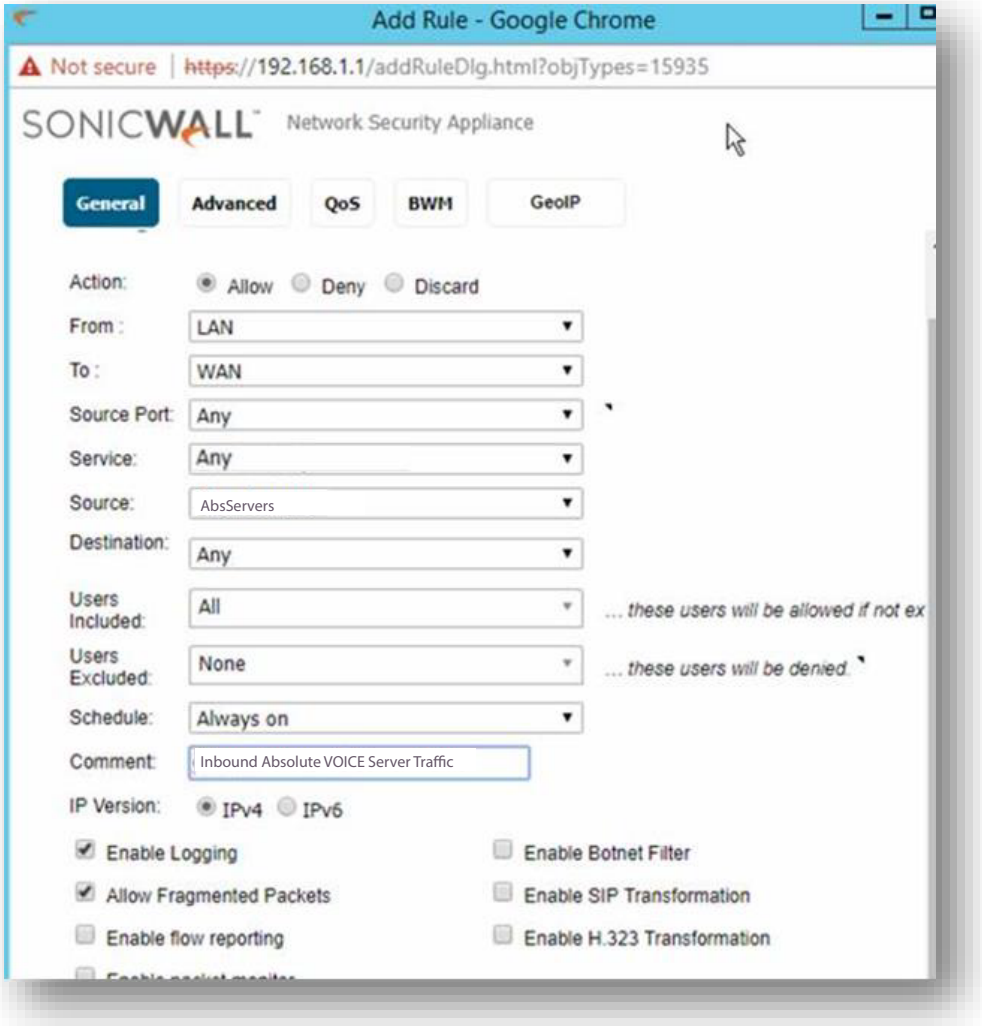
Prioritize the new Absolute VOICE access rules: Firewall ->

Access Rules

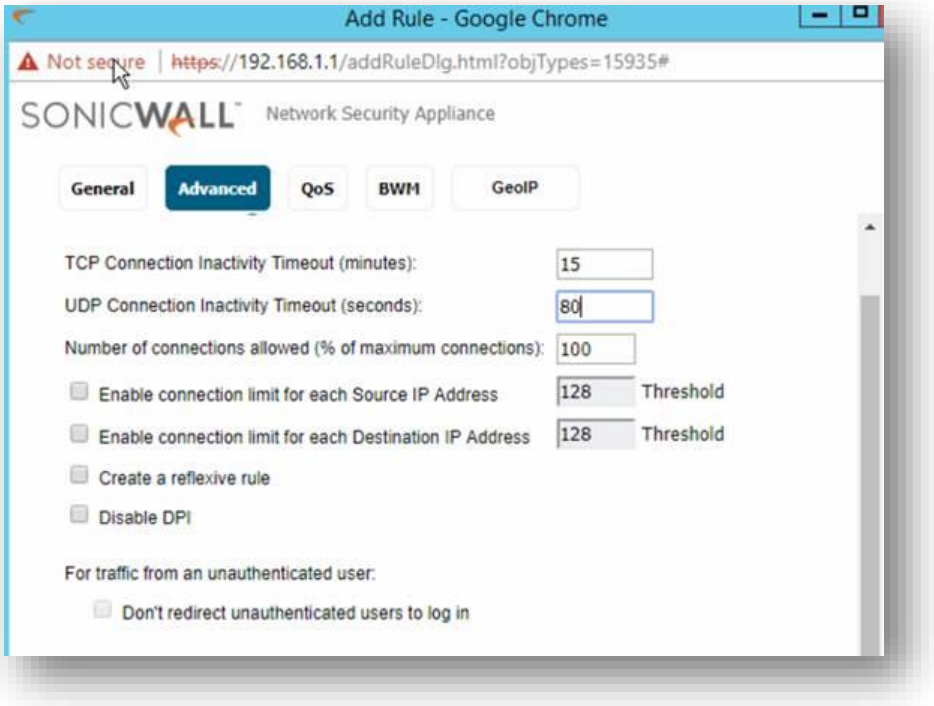
- Sort the Matrix via LAN → WAN
- Select the Priority up/down arrows to set the Absolute VOICE SIP, RTP and IP's (if created) as the top priority.

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

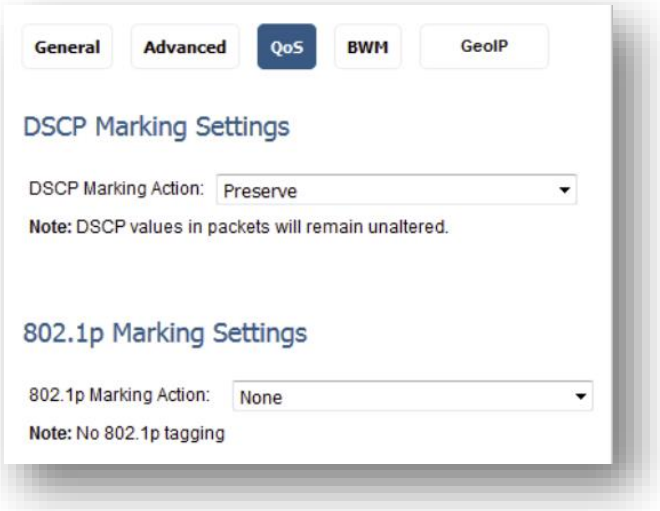
Click on “Add…” to bring up a dialog for adding a new firewall access rule.
This rule will setup the priority and timers for the SIP/RTPports.



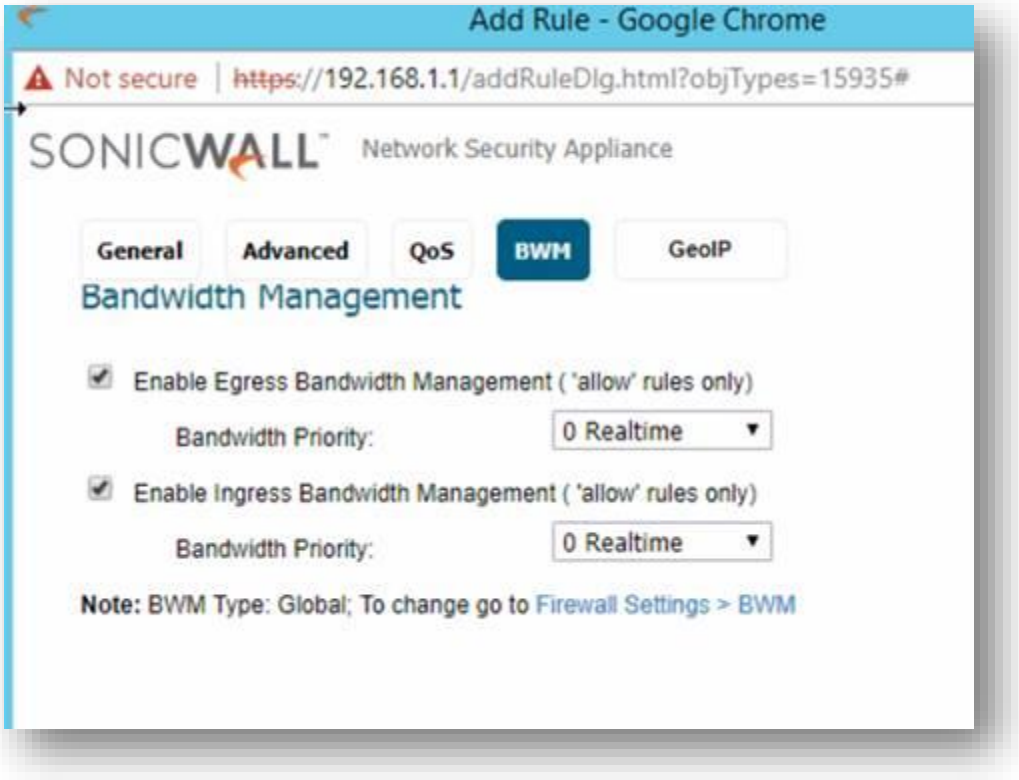
- Check “Allow” for “Action”
- “From Zone” set to WAN
- “To Zone” set to LAN
- “Service” set to Any
- “Source” set to “Absolute VOICE Servers”
- “Destination” set to Any
- “Users Allowed” set to All
- “Schedule” set to Always on
- “Comment” set to “Inbound Absolute VOICE Server Traffic
- Check “Enable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



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



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



- 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

Traffic Shaping QoS Configuration

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 http://www.speedtest.net and then click Begin Test.

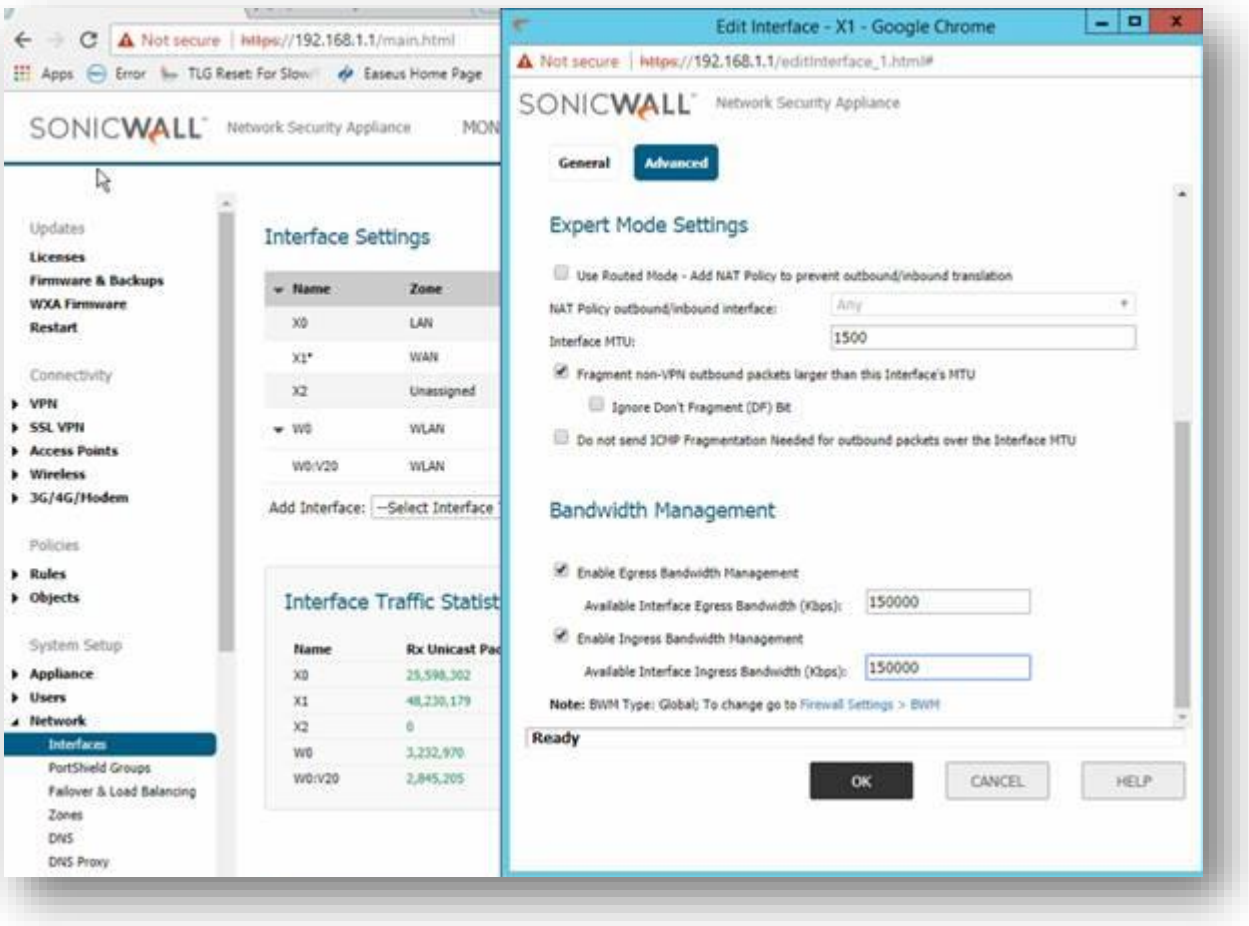
Once the test is completed you should be provided with both an Upload (also referred to as Egress and Outbound Bandwidth) and Download (also referred to as Ingress and Inbound Bandwidth) speed. Record this as you will need it in the next step for configuring traffic shaping.

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

Network → Interfaces

Locate the WAN interface and click configure for interface configuration.

Under the interface configuration click on the “Advanced” tab.

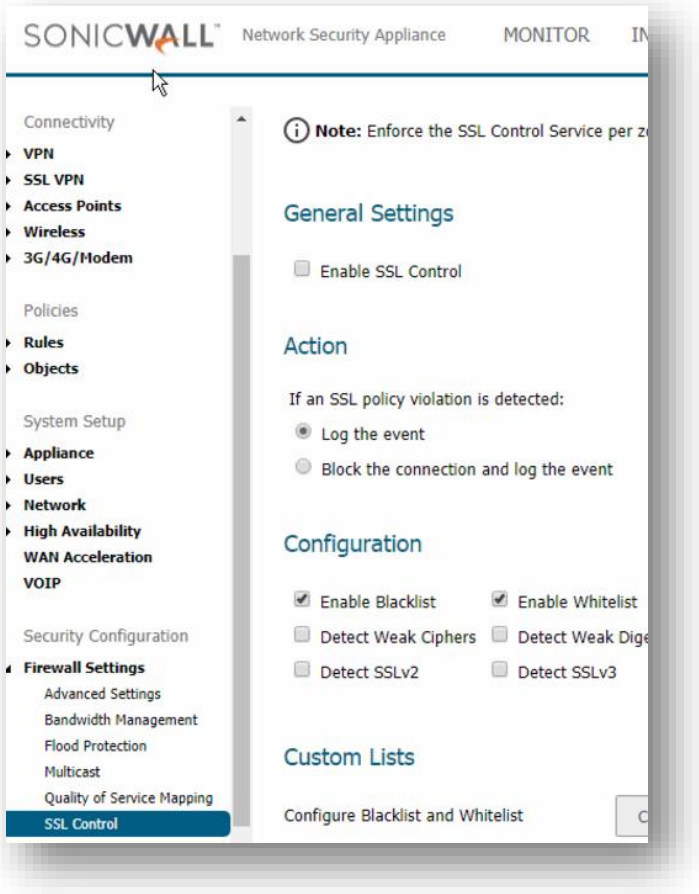


- Check “Enable Egress Bandwidth Management”
  - “Available Interface Egress Bandwidth (Kbps)” set to the upload speed you got from your speed test in Kbps.

- Check “Enable Ingress Bandwidth Management”
  - “Available Interface Ingress Bandwidth (Kbps)” set to the download speed you got from your speed test in Kbps.

- **Note: The picture above is showing 150mbps upload and 150mbps download. *Please enter the correct upload and download speed of your internet connection* otherwise it will throttle your network speeds.**

SSL Action Control (Firewall Settings→SSL Control)

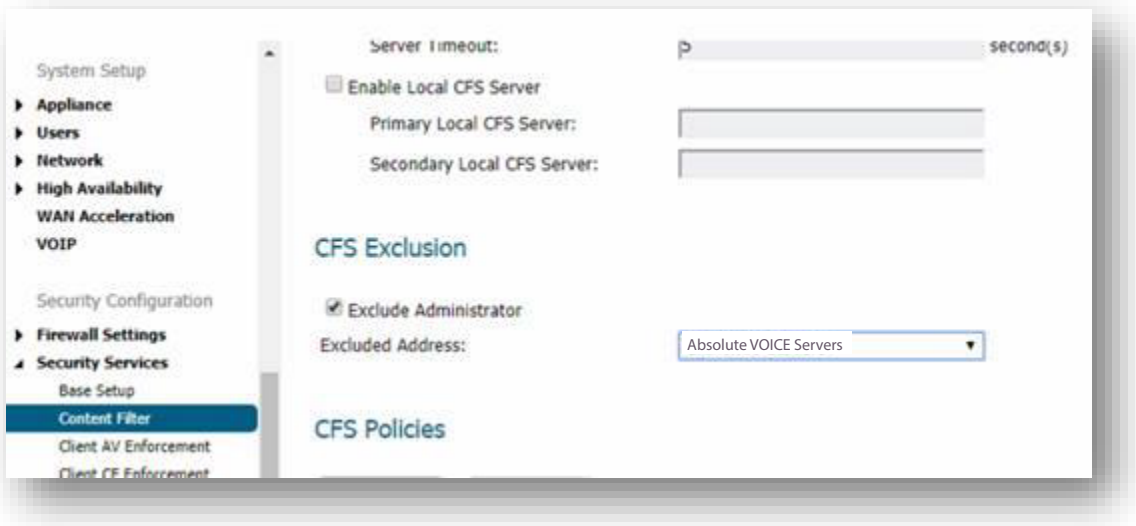


- Change the radio button for SSL Action.
  - Click on “Log the event”
  - Click Accept to save

- **Note: This setting may affect application requests being blocked from Absolute VOICE servers for services such as Hot Desking, etc…**

Security Service Exclusions – Content Filter

Security Services → Content Filter

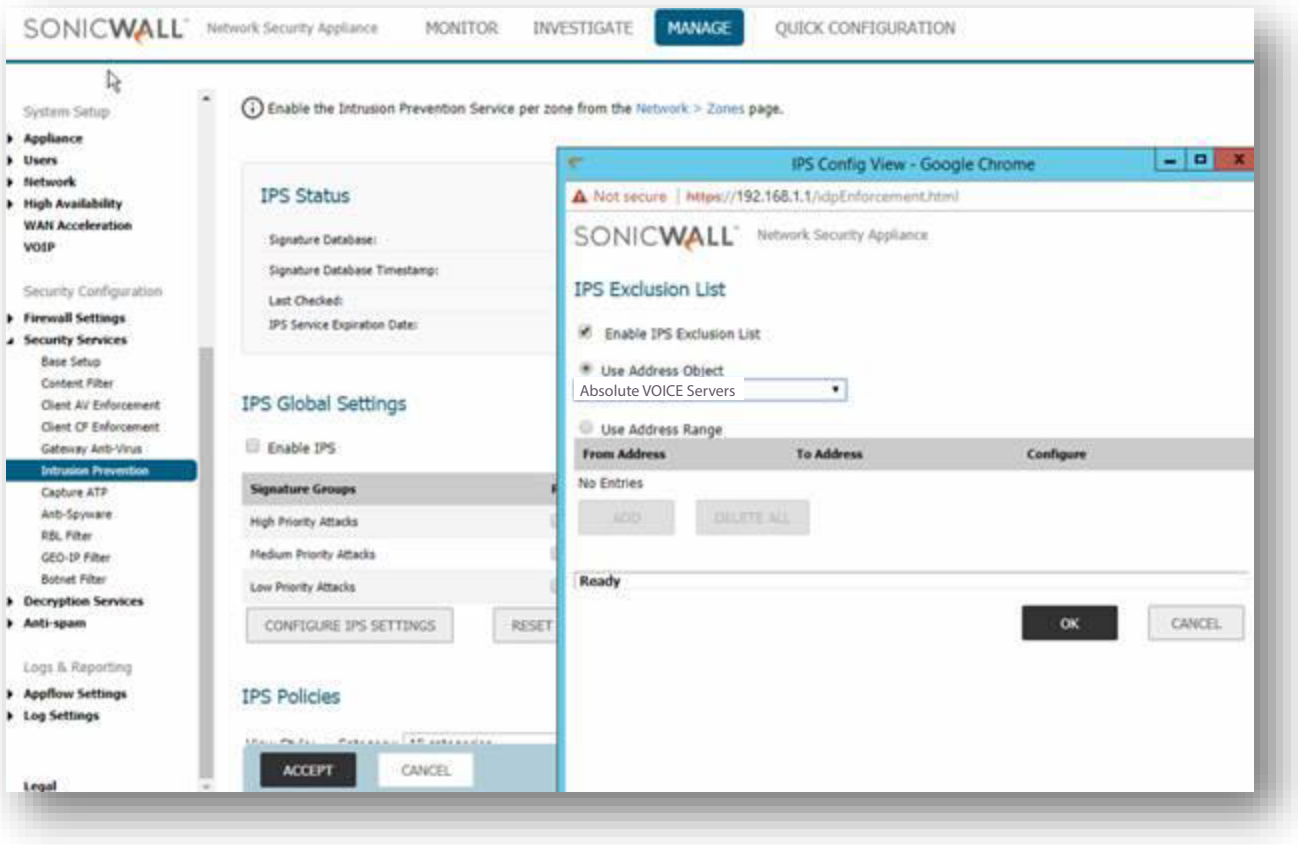


- Click on “Enabled CFS Exclusion List”
- In the drop down select the “Absolute VOICE Servers” network object created earlier
  - 184.178.213.0/24
- Click Accept to save

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

Document Revision History

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 21st, 2015
3.3	Added SSL Action Update	January 16th, 2016
3.4	Updated BWM Notated WAN interface Ingress/Egress Security Exclusions – IPS/Content	April 4th, 2016
3.5	WAN – LAN Rule added. Checklist added	March 16th, 2017
4.0	Document updated for 6.5+ firmware	January 20th, 2018