



Setting Up a SonicWALL for VoIP

G12 Communications

Includes Instructions for Traffic Prioritization



Setting up a SonicWALL for VoIP

Includes Instructions for Traffic Prioritization

Overview

This document provides instructions and guidance on how to configure a SonicWALL appliance for VoIP services from carriers that use standards-based UDP SIP.

Background

Most hosted VoIP solutions require consistent and low ping times, along with 60-90Kbps per concurrent phone call. Internet connections that are heavily utilized will experience call quality degradation and an overall poor experience with hosted voice.






Included are instructions for traffic prioritization. This uses features within the SonicWALL firewall to appropriately prioritize VoIP related traffic above all other Internet traffic to help ensure a positive experience.

Note – this is not QoS (Quality of Service). QoS can only be set if the network is owned end-to-end, or if the ISP has QoS tagging enabled on the connection (typically for MPLS networks, and is usually charged as an add-on fee.)

Procedure

- 1) Collect information about the Internet connection. Some of this information may be necessary if there is an issue with the connection itself or
 - a. Who is the provider (ISP)?
 - b. How is your ISP handing off the connection? Is it a cable modem, a T-1 router, a DSL modem, etc.?
 - c. Is there anything else connected to the ISP's device?
 - d. How fast is the connection?
 - i. For this, we will need to know the actual speeds of the Internet connection. This can be most closely estimated by running at least two speed tests from three speed test servers (six total tests). Some speed test sites include:
 1. <http://speedtest.comcast.net>
 2. <http://www.speedtest.net>
 3. <http://myspeed.visualware.com>
 - ii. Ensure the testing device (laptop/desktop/server) is connected directly to the firewall via a wired connection. Do not use wireless connection.
 - iii. Run the test during off-peak times, or when Internet usage is low.
 - iv. Document the upload and download speeds of each test.
 - v. Remove the highest and lowest speed test result. Upload and download
 - vi. Calculate the average of the remaining download speed tests and document the calculated speed. Calculate the average of the upload speed tests separately and document the calculated speed. These numbers will be the starting point for connection tuning later on.
- 2) Log into the SonicWall.
- 3) Click on the System node, then click Status.
 - a. Confirm the firmware version is SonicOS Enhanced 5.9 or greater. If the version is older than 5.9, it is recommended that the firmware on the device is upgraded.
- 4) Click on the VoIP node, then click Settings.
 - a. Confirm that "Enable Consistent NAT" is selected.
 - b. If the client is using a hosted PBX service, confirm that "Enable SIP Transformations" is **not enabled**.
 - c. If the client is using SIP trunking, confirm that "Enable SIP Transformations" is enabled.
 - d. Click Accept if any settings were changed.

5) Click on the Network node, then click Interfaces.

Interface Settings								View IP Version: <input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6 
Name	Zone	Group	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
X0	LAN		192.168.1.1	255.255.255.0	Static	1 Gbps Full Duplex	Default LAN	
X1	WAN	Default LB Group	192.168.1.254	255.255.255.248	Static	100 Mbps Full Duplex	Default WAN	
X2	LAN		192.168.1.3	255.255.255.0	Static	No link		
X3	Guest		192.168.1.4	255.255.255.0	Static	No link		

Add Interface:

- Click the Configure link on the WAN Interface, then click the advanced tab.
- Scroll down to the Bandwidth Management section and select the checkboxes for “Enable Interface Egress Bandwidth...” and “Enable Interface Ingress Bandwidth...”
- Set the Ingress value to the average download speed calculated in step 1D.
 - Convert Mbps to Kbps by multiplying by 1024.
 - $9.2 \text{ Mbps} \times 1024 = 9420 \text{ kbps}$
- Set the Egress value to the average upload speed calculated in step 1D.
- Click OK.



6) Click on the Firewall Settings Node, then select BWM. Select the option for Advanced, then click Accept.

7) Click on the Firewall Node, then select Bandwidth Objects.

- Create a new Bandwidth Object – call it VoIP-Outbound
 - Set Guaranteed to the minimum number of current calls you’d like to have x 90Kbps
 - For a minimum of 10 concurrent calls: $10 \times 90 \text{ Kbps} = 900 \text{ Kbps}$
 - This minimum should be no more than $\frac{1}{2}$ of the connection upload speed.
 - Set Maximum bandwidth to the lesser of: total number of phones x 90kbps or the 90% of the maximum upload speed of the Internet connection.
 - Set traffic priority to “0 Real-time”
 - Set Violation Action to Delay
 - Optionally, set a comment.

vi. Click OK.

SonicWALL Network Security Appliance

General Elemental

Bandwidth Object Settings

Name: VoIP-Outbound

Guaranteed Bandwidth: 300 kbps

Maximum Bandwidth: 4500 kbps

Traffic Priority: 0 Realtime

Violation Action: Delay

Comment: Outbound VoIP Priority Rule

Ready

OK Cancel Help

b. Create a second new Bandwidth Object – Call it VoIP-Inbound. Duplicate the settings from VoIP-Outbound.

8) For Hosted PBX: Click on the Firewall Node, then click Access rules.

- a. Select the From LAN to WAN link. Add a new Rule.
 - i. On the General Tab, set the following settings:
 1. From LAN
 2. To: WAN
 3. Source Port: Any
 4. Service: VOIP
 5. Source: Any
 6. Destination: Any
 7. Users Included: All
 8. Optional – set a comment.

SonicWALL Network Security Appliance

General Advanced GeoS BWM

Settings

Action: ☒ Allow ☐ Deny ☐ Discard

From: LAN

To: WAN

Source Port: Any

Service: VOIP

Source: Any

Destination: Any

Users Included: All ... these users will be allowed if not excluded

Users Excluded: None ... these users will be denied

Schedule: Always on

Comment: VoIP Traffic Priority Rule

☒ Enable Logging ☒ Enable Geo-IP Filter

☒ Allow Fragmented Packets ☒ Enable Botnet Filter

☐ Enable Flow reporting

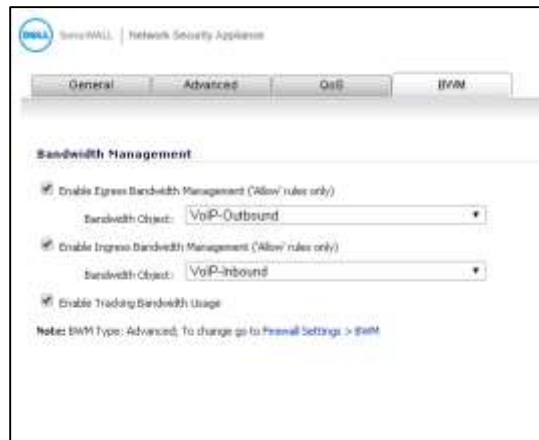
☐ Enable packet monitor

☐ Enable Management


ii. Click on the BWM tab

1. Select the checkbox for enable Egress Bandwidth Management. Click the drop-down and select VoIP-Outbound

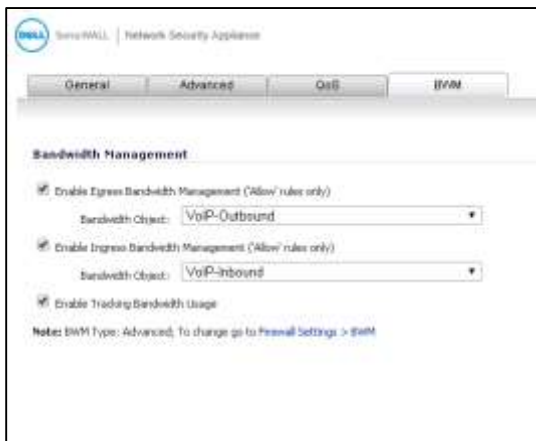
2. Select the checkbox for Enable Ingress Bandwidth Management. Click the drop-down and select VoIP-Inbound
3. Optional: Select the checkbox for Enable Tracking Bandwidth Usage



iii. Click Add.

b. Make sure the new rule is #1 in the list. Click the Change Priority Button  and set the priority to 1.

- 9) For SIP Trunking: Use the server wizard to port forward VoIP traffic to your SIP endpoint. Edit the newly added firewall rules to include the following bandwidth management settings on the BWM tab:



a.

- 10) Export the current configuration to back up these new settings.