



RingCentral Recommended QoS Configuration Settings for SONICWALL SOHO Router User Guide

[Home](#) » [RingCentral](#) » RingCentral Recommended QoS Configuration Settings for SONICWALL SOHO Router User Guide



Recommended QoS Configuration Settings for SONICWALL SOHO Router



Contents [[hide](#)]

- [1 Introduction](#)
- [2 Quality of Service](#)
- [3 Configure your router](#)
- [4 Ports and Firewalls Settings for RingCentral VoIP Service](#)
- [5 Documents / Resources](#)
 - [5.1 References](#)
- [6 Related Posts](#)

Introduction

RingCentral® has taken the “guesswork” out of router selection. Since we know that Quality of Service (QoS) is paramount to your business, we have carefully selected and tested a set of dependable routers suitable for supporting high quality Voice-over-IP conversations.

This document provides recommended configuration settings to ensure the highest possible QoS for voice calls on the SONICWALL® SOHO wireless router.

Additional routers that have been tested and recommended are shown on the [Recommended Routers](#) page of the RingCentral website.

Supported browsers for test

- Internet Explorer 11 or higher (Windows XP, 7, 8 or higher)
- Firefox version 36 or higher (Windows and Mac)
- Safari version 6.2 or higher (Mac)

Note:

The routers recommended here are quality hardware that we have tested internally and work reliably with our services.

However, given the constantly updated firmware and physical changes made by manufacturers and the nature of cloud-based services, RingCentral cannot control the final configuration of the hardware or your computer systems/networks, or promise that any given router will work with your system, or guarantee that our information is 100% up to date.

Quality of Service

RingCentral provides reliable, high-quality voice service. Your local network, Internet connection, and your router all contribute to overall call quality, with sufficient dedicated bandwidth to voice calls being the biggest factor. To help you manage your call quality, RingCentral offers tools to check your Internet connection speed, and instructions to configure the Quality of Service (QoS) settings of your routers.



The Quality of Service (QoS) settings on your router enable it to give priority to real time voice traffic over lower priority data traffic, such as large downloads. This document provides recommended configuration settings to ensure the highest possible QoS on the SONICWALL SOHO router. After configuring your router for optimum QoS, select port and firewall settings for mobile and softphone apps from the table [here](#).

Test your connection capacity

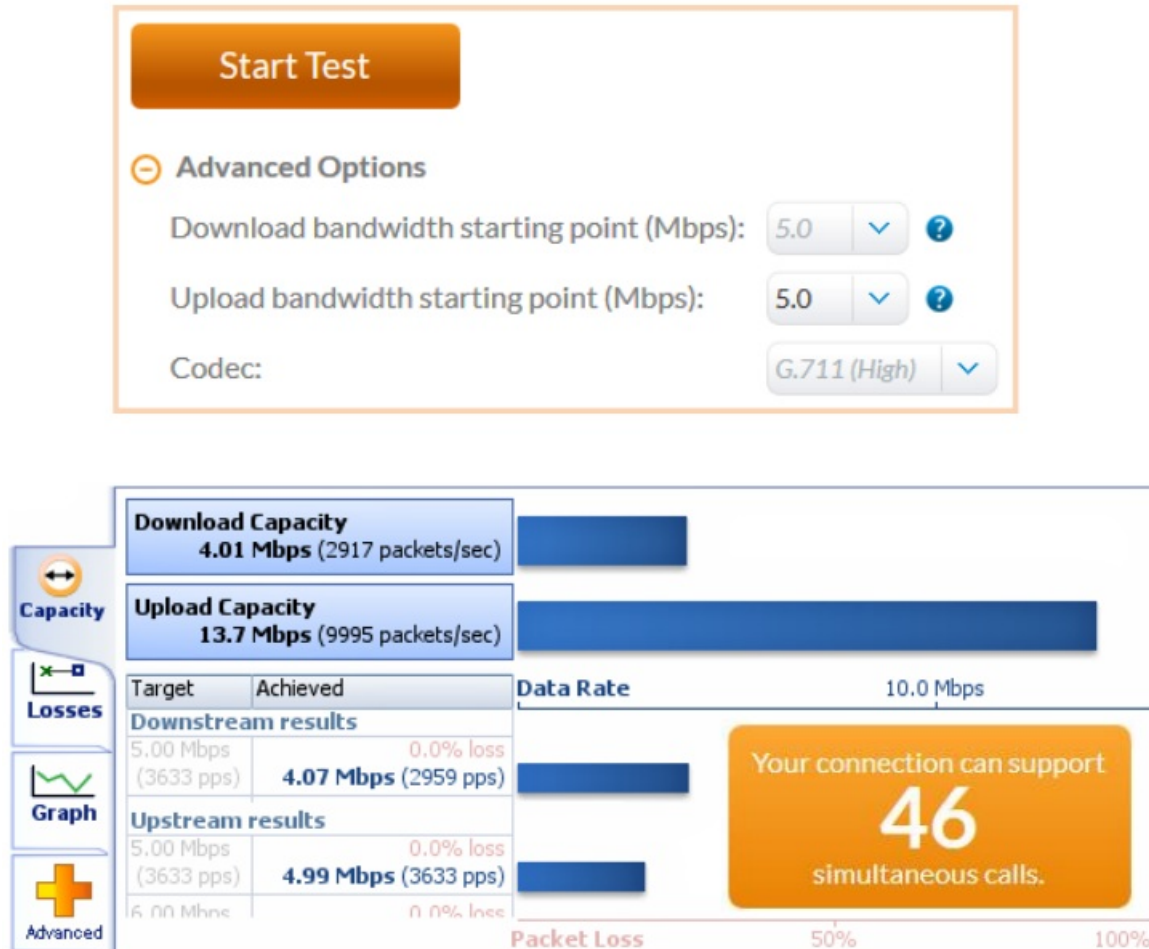
The RingCentral [Connection Capacity test](#) will help determine the maximum number of simultaneous RingCentral calls that can be supported on your broadband connection. Run this test during normal business hours when the connection is in use by other applications, including large file downloads.

The capacity test should be run using the maximum number of simultaneous call connections needed, and should use the G.711 codec selection.

Specific requirements for QoS: Bandwidth 100Kbps up and down per call; Latency (one-way) less than 150ms; Jitter not to exceed 100ms; Packet loss less than 3%.

These requirements are the foundation for ensuring your local network can support satisfactory VoIP. Failure to meet these requirements will result in poor voice quality.

When the test completes, you will see the recommended number of simultaneous calls your connection can support while maintaining good quality voice calls.



Test your connection quality

RingCentral provides a [VoIP Quality test](#) that will simulate VoIP calls between your computer and RingCentral, and provide an estimate of the voice quality you should expect when using our service. For the most accurate results, run this test at least three different times throughout a business day, and during peak usage times, while connected to the network that you plan to use for RingCentral.

A two-minute test is typically sufficient, while longer tests are useful to find intermittent problems or to simultaneously test VoIP performance along with other traffic such as file transfers or remote access. Select the maximum number of simultaneous users you expect to support, and set the test duration between 1 and 5 minutes; 2 minutes is considered sufficient in most instances.

Click jitter and packet loss on the RESULTS SUMMARY panel to view the overall quality of your expected VoIP connection.

MOS score (Mean Opinion Score) refers to a test that has been used for decades in telephony networks to obtain the human user's view of the quality of the network. The MOS is the arithmetic mean of all the individual scores, and can range from 1 (worst) to 5 (best). An MOS score of 4 is good.

Number of simultaneous calls: 45

Advanced Options

Test Duration (minutes): 2

Codec: G.711 (High)

Start Test

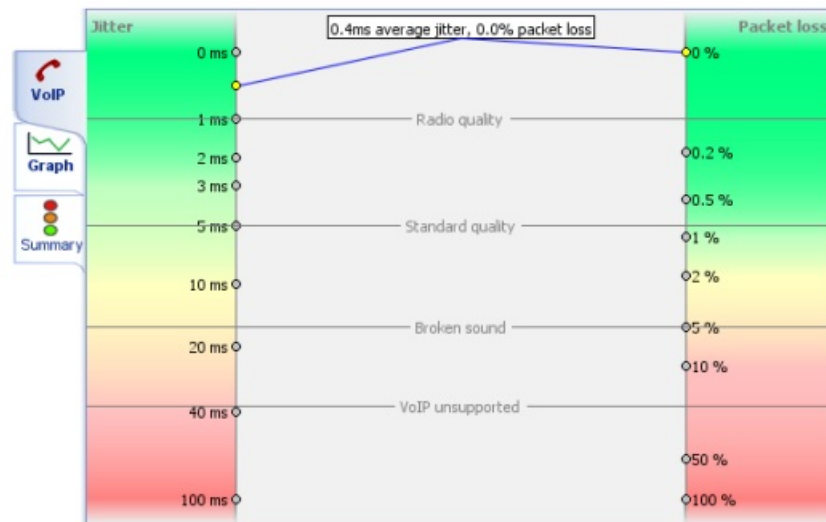
RESULTS SUMMARY

Test audit report

Your connection's **jitter** was measured as 0.4 ms, which indicates that it can produce a constant flow of data. Voice-over-IP conversations should be of good quality.

Your connection's **packet loss** was measured at 0.0%, which indicates that it is accurately transferring data. Voice-over-IP conversations should be of good quality.

Your connection's **MOS score** is estimated to be 4.2.



Configure your router

SONICWALL SOHO QoS configuration



Brand:	SONICWALL
Model:	SONICWALL SOHO
Hardware version:	12831
Firmware version:	SonicOS Enhanced 5.9.1.10-1o

To review the guide that covers configuring QoS in the SonicOS operating system click [here](#).

1. Log into the SONICWALL router with administrative permissions. The default username is admin and the default password is admin. Click OK.

2. the left side of the page, expand VoIP / Settings.

Check the Enable consistent NAT box and uncheck all other settings. Select Accept to save the changes. (See the graphic on the next page.) On the left side of the page, expand VoIP / Settings – illustrated; see instructions above.

SONICWALL | Network Security Appliance

VoIP / Settings

General Settings

☒ Enable consistent NAT

SIP Settings

☐ Enable SIP Transformations

☐ Permit non-SIP packets on signaling port

☐ Enable SIP Back-to-Back User Agent (B2BUA) support

SIP Signaling inactivity time out (seconds): 3600

SIP Media inactivity time out (seconds): 120

Additional SIP signaling port (UDP) for transformations (optional): 0

H.323 Settings

☐ Enable H.323 Transformations

☐ Only accept incoming calls from Gatekeeper

☐ Enable LDAP ILS Support

H.323 Signaling/Media inactivity time out (seconds): 300

Default WAN/DMZ Gatekeeper IP Address: 0.0.0.0

3. Go to Firewall Settings / BWM.

3A. Under Bandwidth Management Type, select Global.

3B. Under Priority, disable EVERY category, except for Medium, which is enabled by default; set Guaranteed to 50%; Maximum\Burst to 100%.

3C. Enable Realtime; set Guaranteed to 50%; Maximum\Burst to 100%.

3D. Click Accept to save changes/settings.

SONICWALL | Network Security Appliance

Firewall Settings / **BWM**

Bandwidth Management Type: ☐ WAN ☒ Global ☐ None

Priority	Enable	Guaranteed	Maximum\Burst
0 Realtime	<input checked="" type="checkbox"/>	50 %	100 %
1 Highest	<input type="checkbox"/>	0 %	100 %
2 High	<input type="checkbox"/>	0 %	0 %
3 Medium High	<input type="checkbox"/>	0 %	100 %
4 Medium	<input checked="" type="checkbox"/>	50 %	100 %
5 Medium Low	<input type="checkbox"/>	0 %	100 %
6 Low	<input type="checkbox"/>	0 %	0 %
7 Lowest	<input type="checkbox"/>	0 %	100 %
Total:		100	

Note: This priority table is used only when global bandwidth management is selected.

In global BWM mode, all traffic (by default) is marked as "medium" priority unless configured via firewall rule/app firewall rule.

4. Go to Network / Interfaces / X1 (WAN).

4A. Under the General tab, click the Configure icon (on far right).

4B. Go to Advanced tab > Link Speed: and set to Auto Negotiate (UNLESS there's a need to set it to something specific)

4C. Under Bandwidth Management check Enable Egress; set Interface Egress Bandwidth to match the available bandwidth;

check Enable Ingress; set Interface Ingress Bandwidth to match the available bandwidth.

4D. Click OK to save changes/settings.

SONICWALL | Network Security Appliance

General
Advanced

Advanced Settings

Link Speed: Auto Negotiate

☒ Use Default MAC Address: C0:EA:E4:24:9B:E9

☐ Override Default MAC Address:

☐ Enable Multicast Support

☐ Management Traffic Only

Interface MTU: 1500

☒ Fragment non-VPN outbound packets larger than this Interface's MTU

☐ Ignore Don't Fragment (DF) Bit

☐ Do not send ICMP Fragmentation Needed for outbound packets over the Interface MTU

Bandwidth Management

☒ Enable Egress Bandwidth Management

Available Interface Egress Bandwidth (Kbps): 100000.000000

☒ Enable Ingress Bandwidth Management

Available Interface Ingress Bandwidth (Kbps): 100000.000000

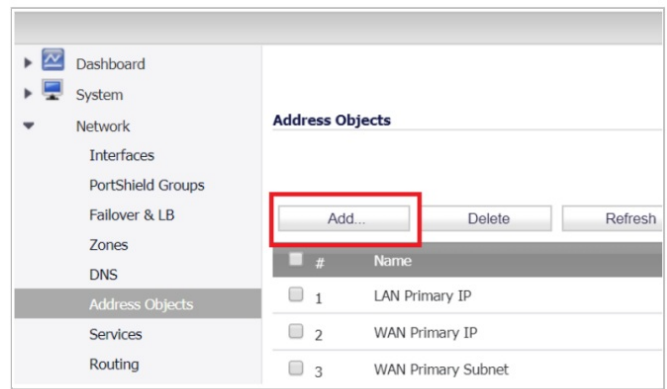
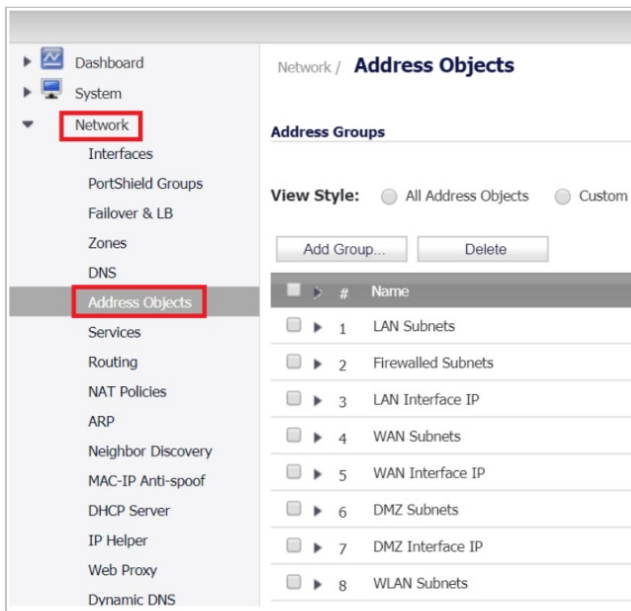
Note: BWM Type: Global; To change go to [Firewall Settings > BWM](#)

Ready

OK
Cancel
Help

5. On the left side of the page, Expand Network. Select Address Objects and create objects and subnet masks for

80.81.128.0/255.255.240.0;	103.44.68.0/255.255.255.0;	104.245.56.0/255.255.248.0;
185.23.248.0/255.255.252.0;	192.209.24.0/255.255.248;	199.68.212.0/255.255.252.0;
199.255.120.0/255.255.252.0; 208.87.40.0/255.255.252.0 as shown at bottom.		
- 5A. Scroll down and click Add to add the RCFFullRang Supernets.



5B. Create objects for the following: RingCentral Supernets.

RingCentral Supernets	
80.81.128.0/20	
103.44.68.0/22	
104.245.56.0/21	
185.23.248.0/22	
192.209.24.0/21	
199.68.212.0/22	
199.255.120.0/22	
208.87.40.0/22	

SONICWALL Network Security Appliance

Name: RCFullRange 1
Zone Assignment: WAN
Type: Network
Network: 80.81.128.0
Netmask/Prefix Length: 255.255.240.0
Ready
Add Close

SONICWALL Network Security Appliance

Name: RCFullRange 2
Zone Assignment: WAN
Type: Network
Network: 103.44.68.0
Netmask/Prefix Length: 255.255.255.0
Ready
Add Close

SONICWALL Network Security Appliance

Name: RCFullRange 3
Zone Assignment: WAN
Type: Network
Network: 104.245.56.0
Netmask/Prefix Length: 255.255.248.0
Ready
Add Close

SONICWALL Network Security Appliance

Name: RCFullRange 4
Zone Assignment: WAN
Type: Network
Network: 185.23.248.0
Netmask/Prefix Length: 255.255.252.0
Ready
Add Close

SONICWALL Network Security Appliance

Name: RCFullRange 5
Zone Assignment: WAN
Type: Network
Network: 192.209.24.0
Netmask/Prefix Length: 255.255.248.0
Ready
Add Close

SONICWALL Network Security Appliance

Name: RCFullRange 6
Zone Assignment: WAN
Type: Network
Network: 199.68.212.0
Netmask/Prefix Length: 255.255.252.0
Ready
Add Close

SONICWALL Network Security Appliance

Name: RCFullRange 7
Zone Assignment: WAN
Type: Network
Network: 199.255.120.0
Netmask/Prefix Length: 255.255.252.0
Ready
Add Close

SONICWALL Network Security Appliance

Name: RCFullRange 8
Zone Assignment: WAN
Type: Network
Network: 208.87.40.0
Netmask/Prefix Length: 255.255.252.0
Done adding Address object entry
Add Close

6. A. Once the address objects are added, add the address group from the same section of the interface, as seen below.

SONICWALL | Network Security Appliance

Name:

















LAN Primary Subnet
 Secondary Default Gateway
 U0 IP
 U0 IPv6 Link-Local Address
 U0 IPv6 Primary Static Address
 U0 IPv6 Primary Static Address
 U0 Subnet
 WAN IPv6 Link-Local Address
 WAN IPv6 Primary Static Address
 WAN IPv6 Primary Static Address

->
 <-

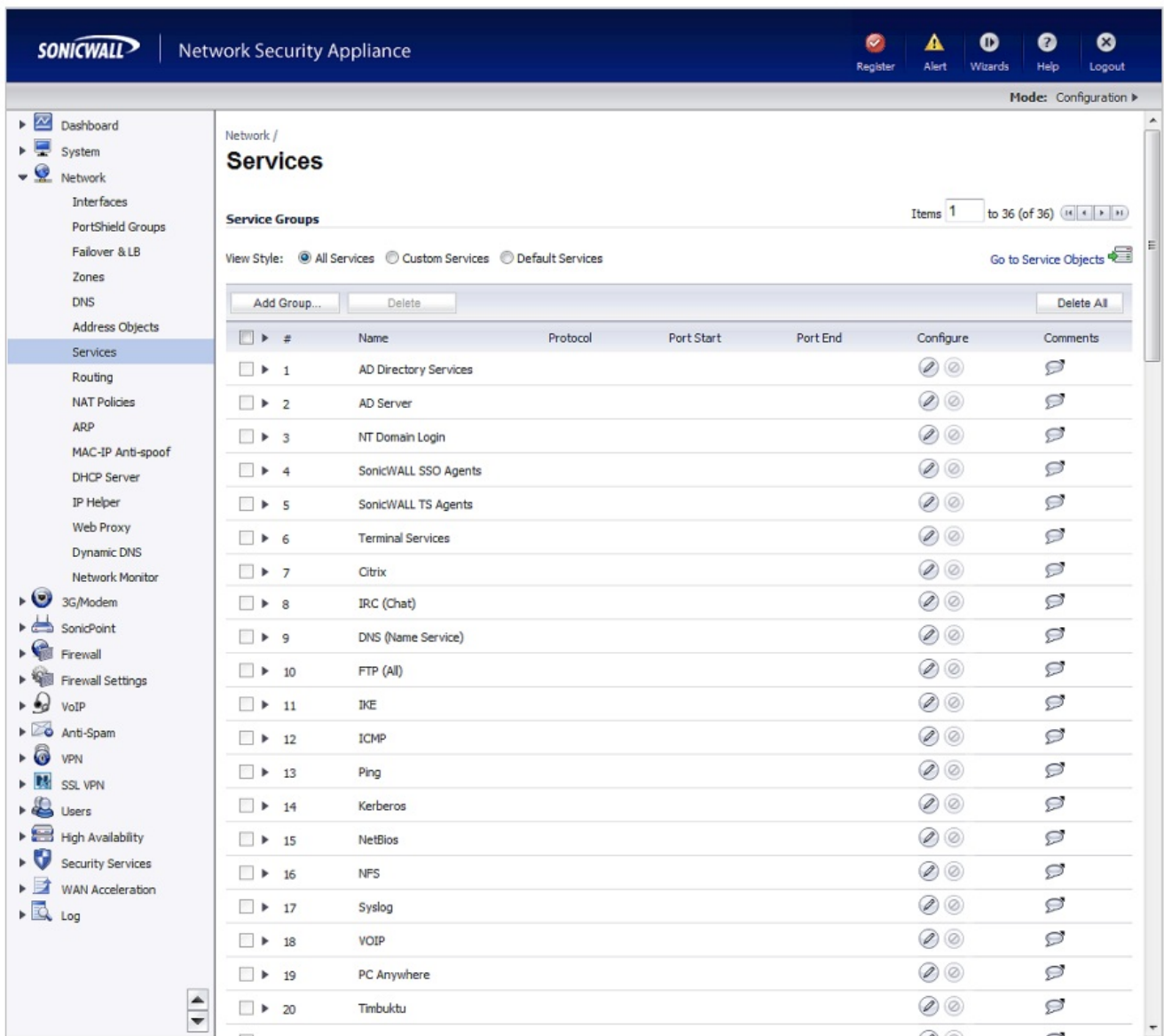
RCFullRange1
 RCFullRange2
 RCFullRange3
 RCFullRange4
 RCFullRange5
 RCFullRange6
 RCFullRange7
 RCFullRange8

Ready

6B. Click OK. Once added you can expand the group and it should look like this:

RCFullRange Group		Group		
RCFullRange1	80.81.128.0/255.255.240.0	Network	WAN	 
RCFullRange2	103.44.68.0/255.255.255.0	Network	WAN	 
RCFullRange3	104.245.56.0/255.255.248.0	Network	WAN	 
RCFullRange4	185.23.248.0/255.255.252.0	Network	WAN	 
RCFullRange5	192.209.24.0/255.255.248.0	Network	WAN	 
RCFullRange6	199.68.212.0/255.255.252.0	Network	WAN	 
RCFullRange7	199.255.120.0/255.255.252.0	Network	WAN	 
RCFullRange8	208.87.40.0/255.255.252.0	Network	WAN	 

7. A. On the left side of the page, Expand Network and select Services.

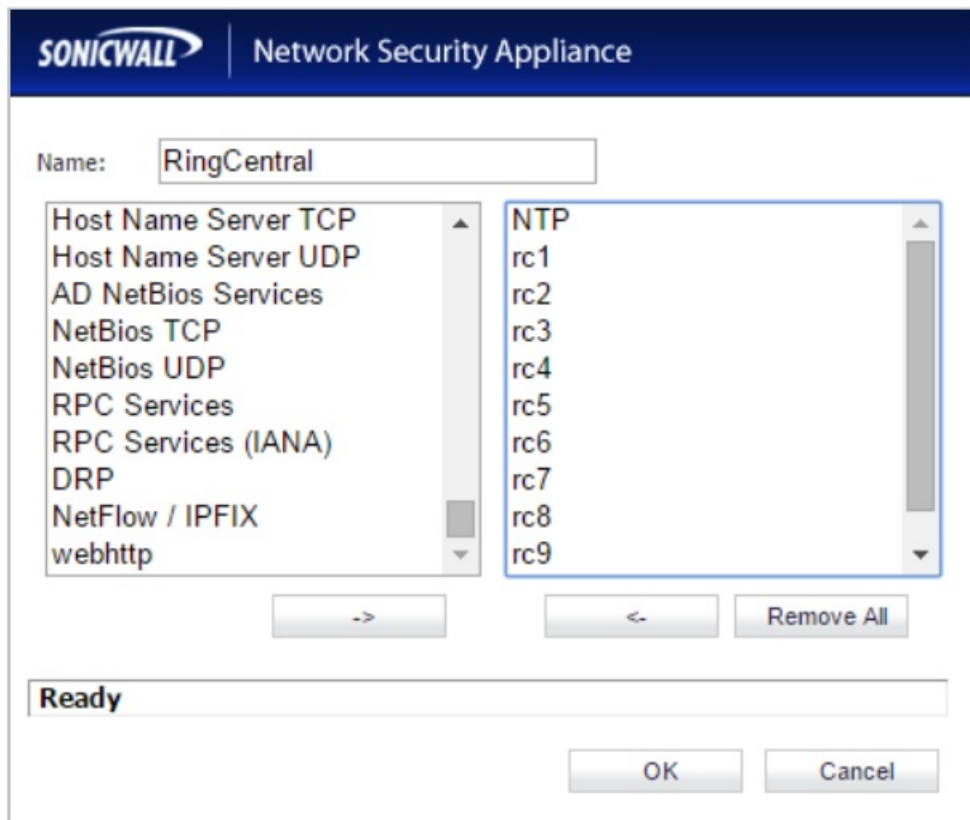


7B. Under Services click the Add option. Then add the following services to support the RingCentral Desk Phone. (See [Table B.1, here.](#))

1. RC1: UDP 20000 – 64999 – Media/Media Secured
2. RC2: UDP 5090 – Signaling
3. RC3: TCP 5090 – Signaling
4. RC4: TCP 5099 – Signaling (when line sharing is used)
5. RC5: TCP 5096 – Signaling Secured
6. RC6: TCP 5098 – Signaling Secured
7. RC7: UDP – 123 – Network Time Service
8. RC8: TCP 636 – LDAP Directory Service
9. RC9: TCP 443 – Provisioning

Other types of endpoints require addition of Services according to [Tables B.2 through B.9, here.](#)

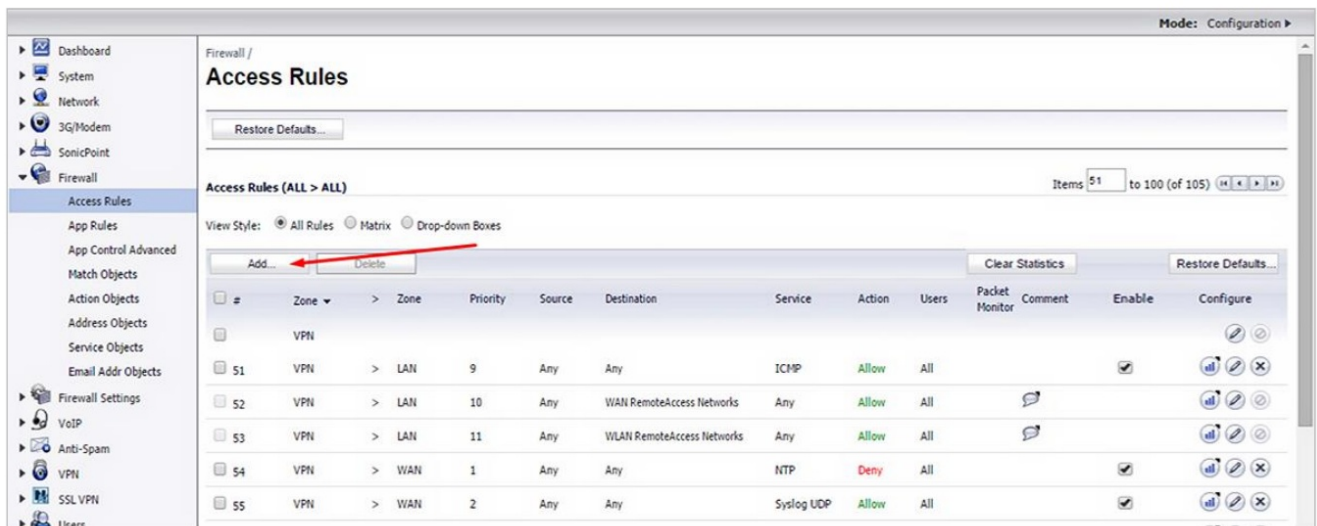
7D. Now select the Add Group option from the Service Groups section, also under the Services section. Name the group RingCentral; highlight all RingCentral Services. Use the arrows in the box to move the highlighted information from left the right.



Note:

Selections shown at left are the default profiles for the SONICWALL router before step 7B. Select OK. The RingCentral Service should now be added.

- On the left side of the page, Expand Firewall. Select Access Rules. Click the Add button.



- Create two new rules for WAN to LAN and LAN to WAN, as seen below. Select Add for both and select the drop-down menus as indicated in the screenshots.

SONICWALL Network Security Appliance

General Advanced QoS

Settings

Action: ☒ Allow ☐ Deny ☐ Discard

From : WAN

To : LAN

Source Port: Any

Service: RC Services

Source: RCFullRange Group

Destination: RCFullRange Group

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

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

Schedule: Always on

Comment:

☒ Enable Logging

☒ Allow Fragmented Packets

☐ Enable packet monitor

☐ Enable Management

SONICWALL Network Security Appliance

General Advanced QoS

Settings

Action: ☒ Allow ☐ Deny ☐ Discard

From : LAN

To : WAN

Source Port: Any

Service: RC Services

Source: Any

Destination: RCFullRange Group

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

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

Schedule: Always on

Comment:

☒ Enable Logging

☒ Allow Fragmented Packets

☐ Enable packet monitor

☐ Enable Management

10. The RingCentral Access Rule should now be added.

19	LAN	>	WAN	7	Any	RCFullRNGGrp	Any	Allow	All	<input checked="" type="checkbox"/>			
111	WAN	>	LAN	11	RCFullRNGGrp	Any	Any	Allow	All	<input checked="" type="checkbox"/>			

11. Click edit on both the LAN to WAN and WAN to LAN settings and go to the Ethernet BWM tab. Enable both the inbound and outbound bandwidth management settings and set to Realtime.

SONICWALL Network Security Appliance

General Advanced QoS Ethernet BWM

Ethernet Bandwidth Management

☒ Enable Outbound Bandwidth Management ('allow' rules only)

Bandwidth Priority: 0 Realtime

☒ Enable Inbound Bandwidth Management ('allow' rules only)

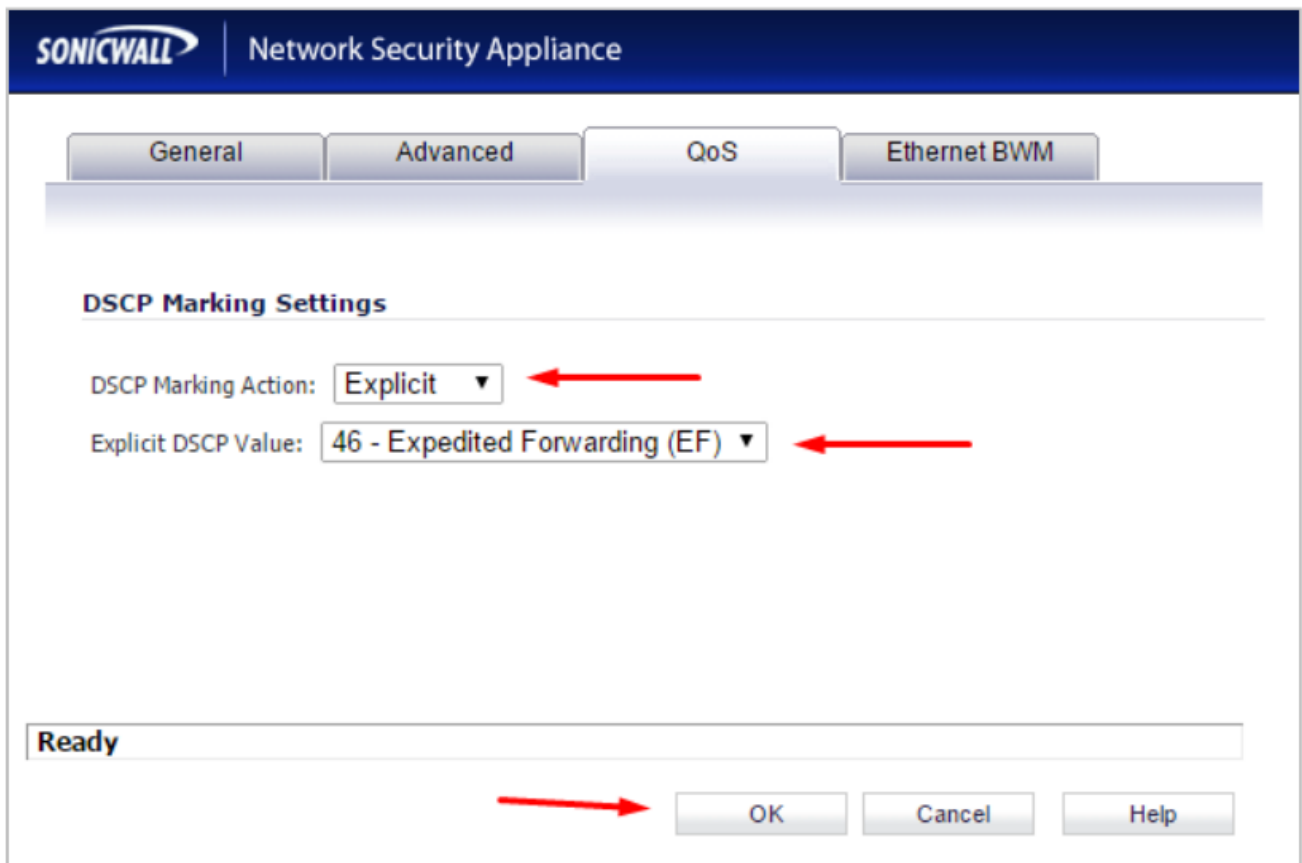
Bandwidth Priority: 0 Realtime

Note: BWM Type: Global; To change go to Firewall Settings > BWM

Ready

OK Cancel Help

12. Go to the QoS tab and set the DSCP Marking Action to Explicit and set the Explicit DSCP Value to “46” and click OK to save.



The screenshot shows the SonicWall Network Security Appliance interface. At the top, there are four tabs: General, Advanced, QoS (selected), and Ethernet BWM. Below the tabs, the 'DSCP Marking Settings' section is visible. It contains two dropdown menus: 'DSCP Marking Action' set to 'Explicit' and 'Explicit DSCP Value' set to '46 - Expedited Forwarding (EF)'. Red arrows point to these two dropdowns. At the bottom of the window, there is a status bar that says 'Ready' and three buttons: 'OK', 'Cancel', and 'Help'. A red arrow points to the 'OK' button.

Congratulations. You have finished configuring your SONICWALL SOHO firewall/ router for QoS prioritization of voice packets.

Now select the port and firewall settings for mobile and softphone apps from the table on the next page.

Ports and Firewalls Settings for RingCentral VoIP Service


Please see RingCentral [Ports and Firewalls](#) reference link for the required TCP/UDP ports that need to be opened for RingCentral devices to work. Categories are:

- Device Type
- Protocol
- Source Port—Customer Side
- Destination Port—RingCentral Side

Also see information on Port Triggering on the referenced [page](#).

©2019 RingCentral, Inc. All rights reserved. RingCentral and the RingCentral logo are registered trademarks of RingCentral, Inc. Other third-party marks and logos displayed in this document are the trademarks of their respective owners.

Documents / Resources

	<p>RingCentral Recommended QoS Configuration Settings for SONICWALL SOHO Router [pdf] User Guide</p> <p>Recommended QoS Configuration Settings for SONICWALL SOHO Router, Recommended QoS Configuration Settings, SONICWALL SOHO Router</p>
---	---

References

- [🌐 Configuring Quality of Service Mapping](#)
- [📄 Test Your Connection's Call Capacity | RingCentral](#)
- [📄 QoS Routers that Work Best with your RingCentral System](#)
- [📄 VoIP Test for Your Connection Quality | RingCentral](#)
- [📄 Network Requirements | MVP](#)
- [📄 article-v2](#)