Recommended QoS Configuration Settings for SONICWALL TZ Series

Contents

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 TZ Series.

Additional routers that have been tested and recommended are shown on the Recommended Routers page of the RingCentral website.

Supported Browsers

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 enables 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 SONICWALL TZ Series.
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). A MOS score of 4 is good.

Configure your router

SONICWALL TZ Series QoS configuration

Brand: SONICWALL
Model: TZ270
Hardware version: 20405
Firmware version: SonicOS 7.0.1-5018

To review the SONICWALL TZ Series guide that covers configuring QoS in the Equipment operating system click here.

Ports and Firewalls Settings for RingCentral VoIP Service

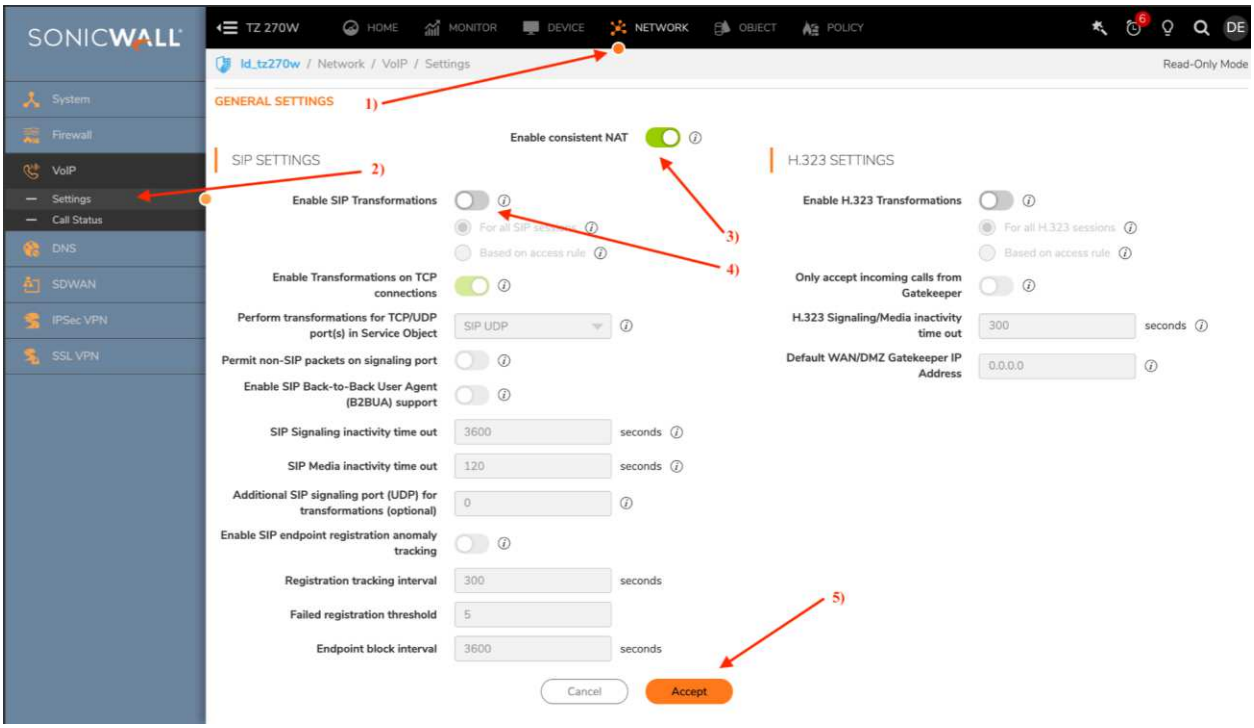
Please see RingCentral Ports and Firewalls reference link for the required TCP/UDP ports that need to be opened for RingCentral devices to work. Categories are:

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

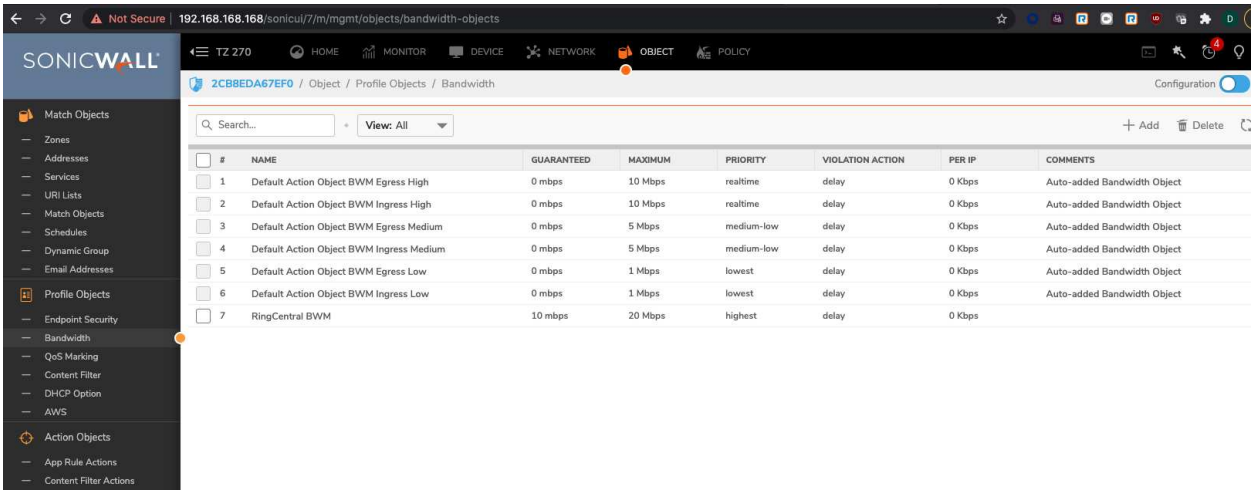
Also, see information on Port Triggering on the referenced page.

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

2. At the top of the page select Network. On the left side of the page, expand VoIP/Settings. Check the Enable consistent NAT box and turn off Enable SIP Transformations. Select Accept to save the changes. (See the graphic on the next page)

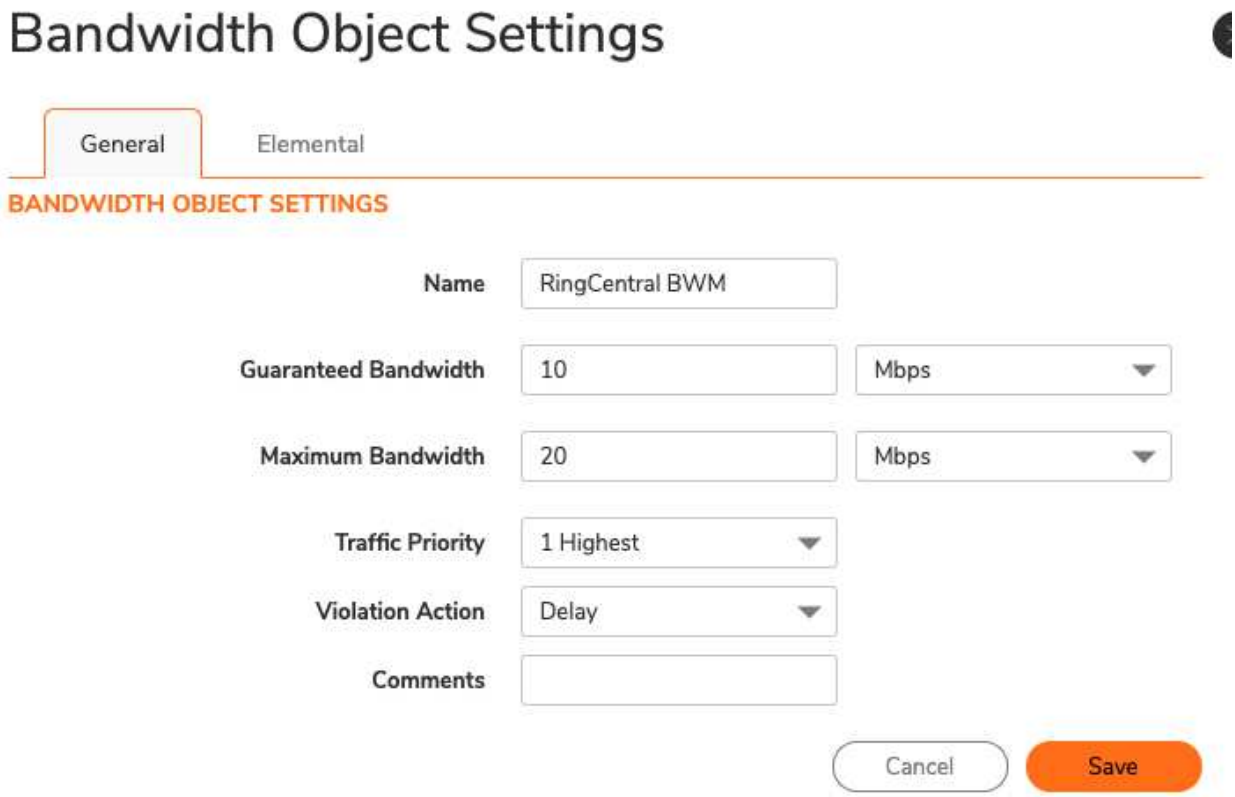


3. Select the Objects tab on the top. Navigate to Profile Objects/Bandwidth on the left side of the screen.

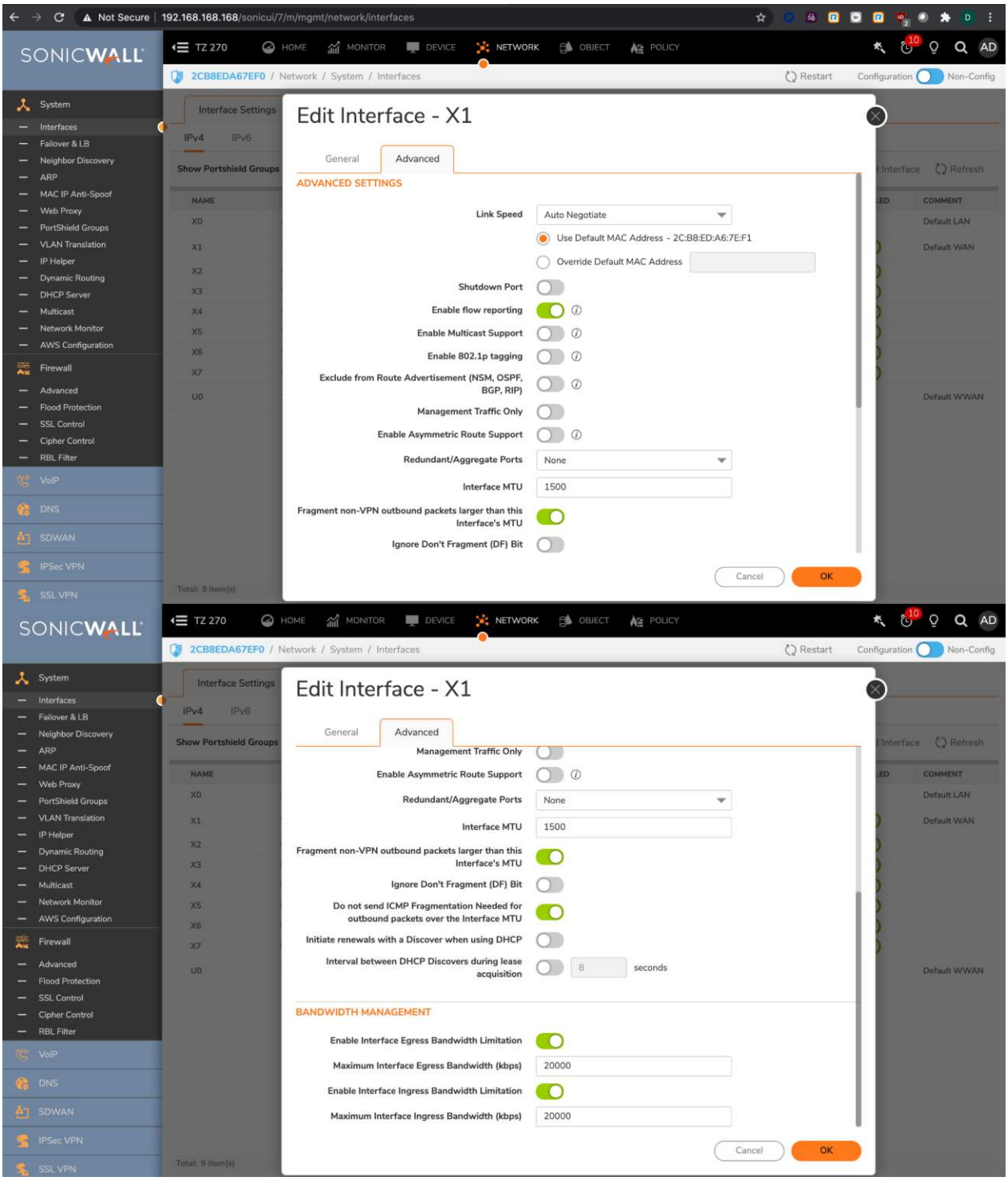


3A. Hit the +Add and give the object a name.
3B. Set the Guaranteed Bandwidth to 10 Mbps
3C. Set the Maximum Bandwidth to 20 Mbps

3D. Set the Traffic Priority to 1 Highest
3E. Set the Violation Action to Delay
3F. Hit Save to accept the changes

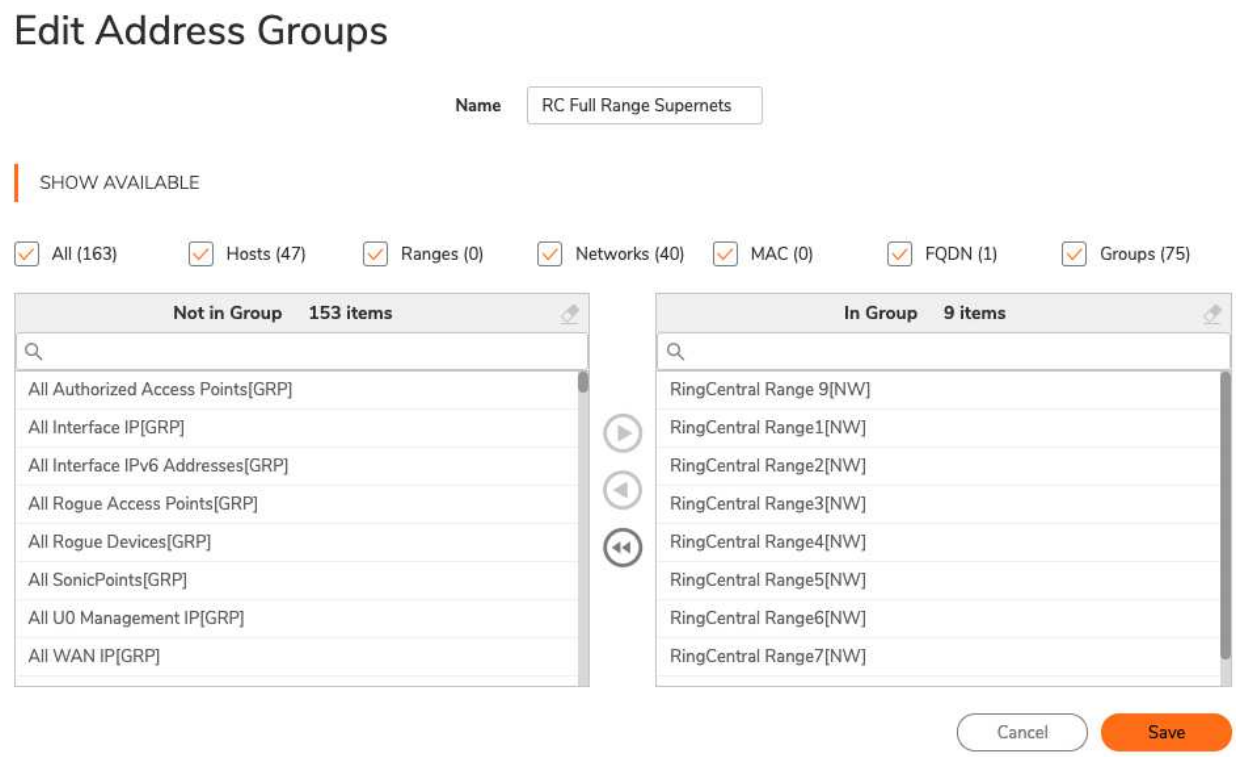


5. Select the Network tab on top.
5A. Navigate to System/Interfaces on the left.
5B.Edit the X1 interface and select the Advanced tab
5C. Set the Link Speed to Auto Negotiate (UNLESS there's a need to set it to something specific)
5D. Under Bandwidth Management check Enable Egress;
5F. Set Interface Egress Bandwidth to match the available bandwidth;
5G. Check Enable Ingress;
5H. Set Interface Ingress Bandwidth to match the available bandwidth.
5I. Click OK to save changes/settings.



6. Select the Object tab on the top;
6A. Navigate to Match Objects/Addresses on the left;
6B. Hit the +Add
6C. Set the Zone Assignment to WAN
6D. Set the Type to Network

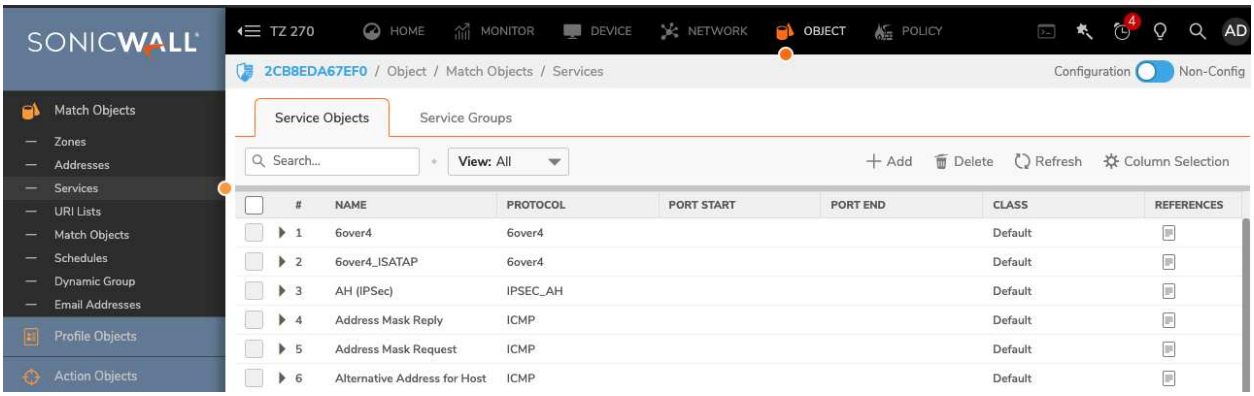
6E. Add the IP Address for one of the supernets (found below.)
screenshot below.
6F. Hit the Save button to commit the changes



Once added you can expand the group and it should look like this:

37	RC Full Range Supernets	-	Group	ipv4	-	Custom
	RingCentral Range1	80.81.128.0/255.255.240.0	network	ipv4	WAN	Custom
	RingCentral Range2	103.44.68.0/255.255.255.0	network	ipv4	WAN	Custom
	RingCentral Range3	104.245.56.0/255.255.248.0	network	ipv4	WAN	Custom
	RingCentral Range4	185.23.248.0/255.255.252.0	network	ipv4	WAN	Custom
	RingCentral Range5	192.209.24.0/255.255.248.0	network	ipv4	WAN	Custom
	RingCentral Range6	199.68.212.0/255.255.252.0	network	ipv4	WAN	Custom
	RingCentral Range8	199.255.120.0/255.255.252.0	network	ipv4	WAN	Custom
	RingCentral Range7	208.87.40.0/255.255.252.0	network	ipv4	WAN	Custom
	RingCentral Range 9	66.81.240.0/255.255.240.0	network	ipv4	WAN	Custom

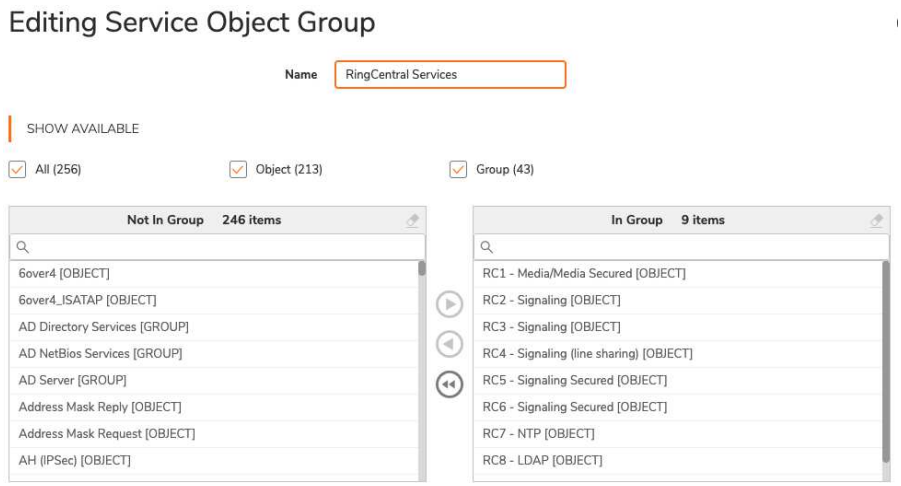
7. Select the Object tab on the top;
7A. Navigate to Match Objects/Services
7B. Under Services click the +Add option.
7C. Add the following services to support the RingCentral Desk Phone



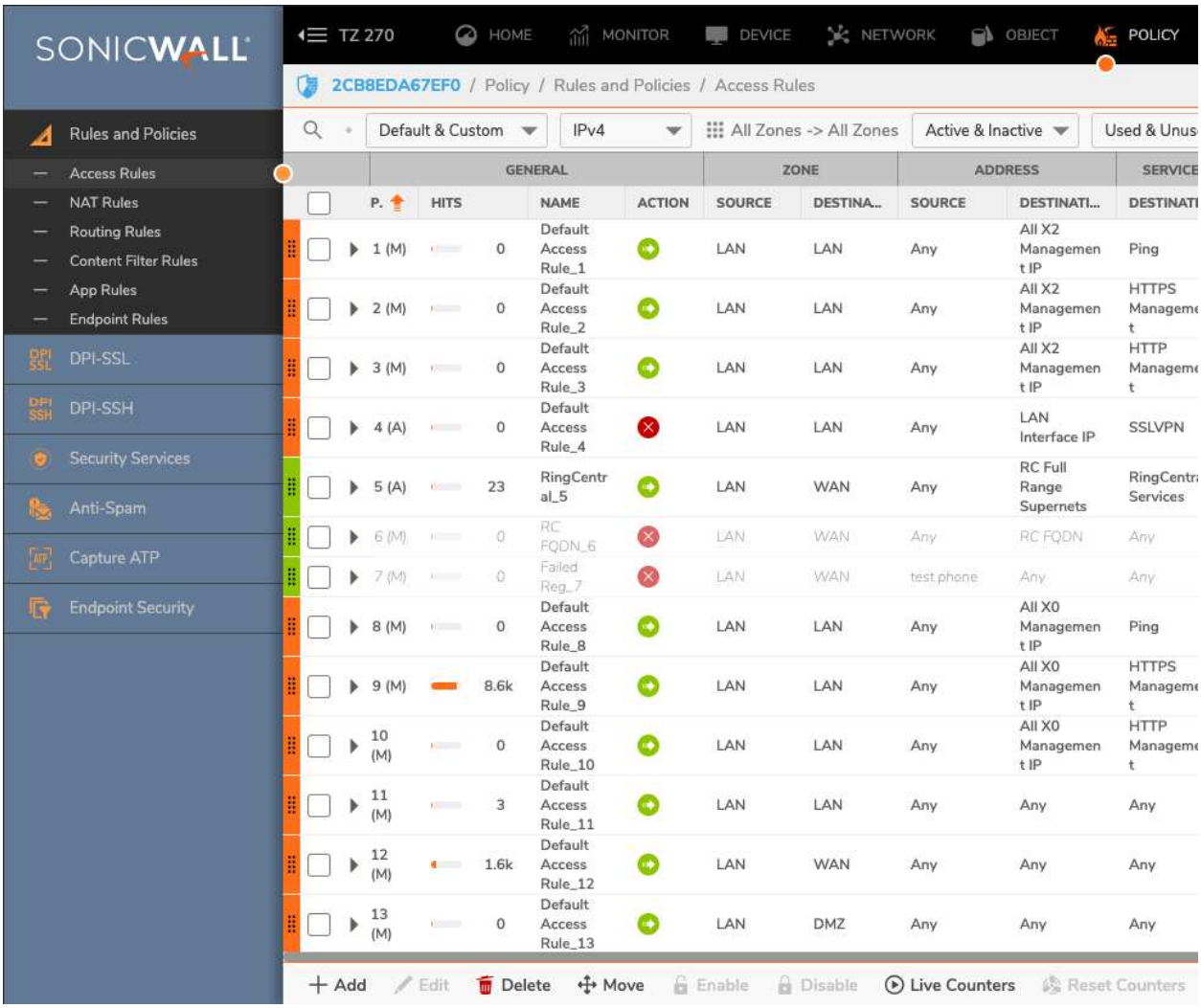
1. RC1: UDP 20000 - 64999 – Media/Media Secured
2. RC2: UDP 5090 – Signaling
3. RC3: TCP 5090 – Signaling
4. RC4: TCP 5099 – Signaling (when line sharing is used)
5. RC5: TCP 5096 – Signaling Secured
6. RC6: TCP 5098 – Signaling Secured
7. RC7: UDP - 123 – Network Time Service
8. RC8: TCP 636 – LDAP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

Other types of endpoints require the addition of Services according to Tables B.2 through B.9, here

8. Select the Service Groups tab and hit the +Add button
8A. Name the Service Group RingCentral Services
8B. Move the RingCentral Service Objects from the left window to the right as shown in the below screenshot.
8C. Hit the save button to create the Service Object Group

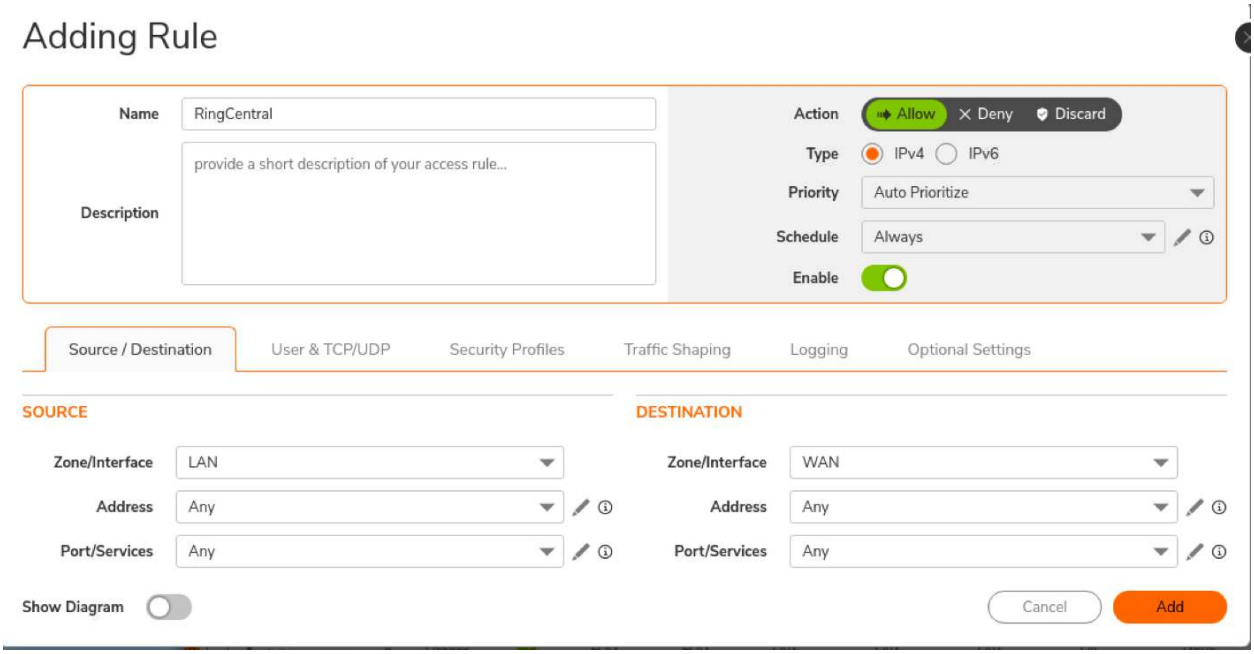


9. Select Policy at the top of the page and Access Rules on the left.
9A. At the bottom of the screen select the + Add button
9B. Name the Rule RingCentral
9C. Select the Source/Destination tab
9D. Set the Source Zone/Interface to LAN
9E. Set the Destination Zone/Interface to WAN

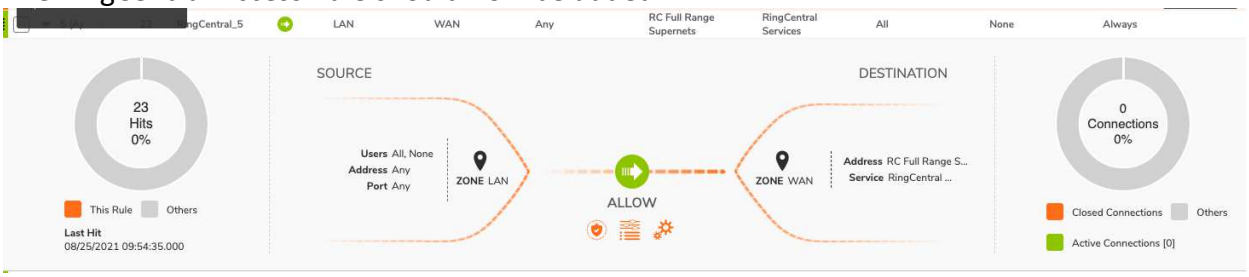


10. Create a new rule for LAN to WAN, as seen below.

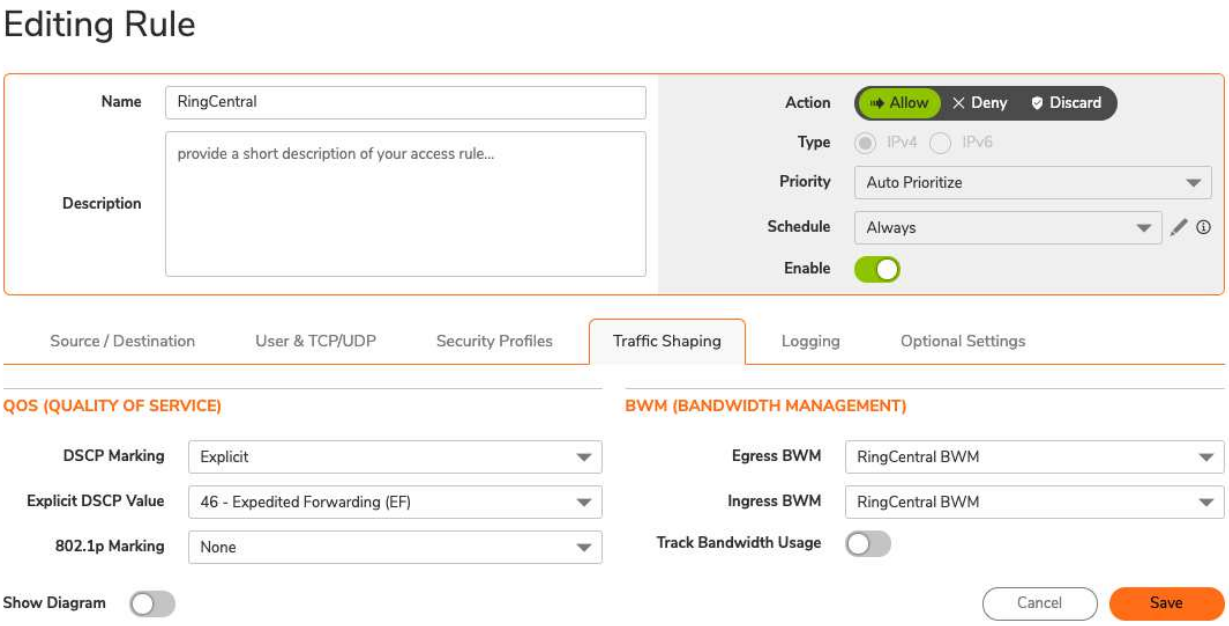
10A. Select Add for both and select the drop-down menus as indicated in the screenshots.



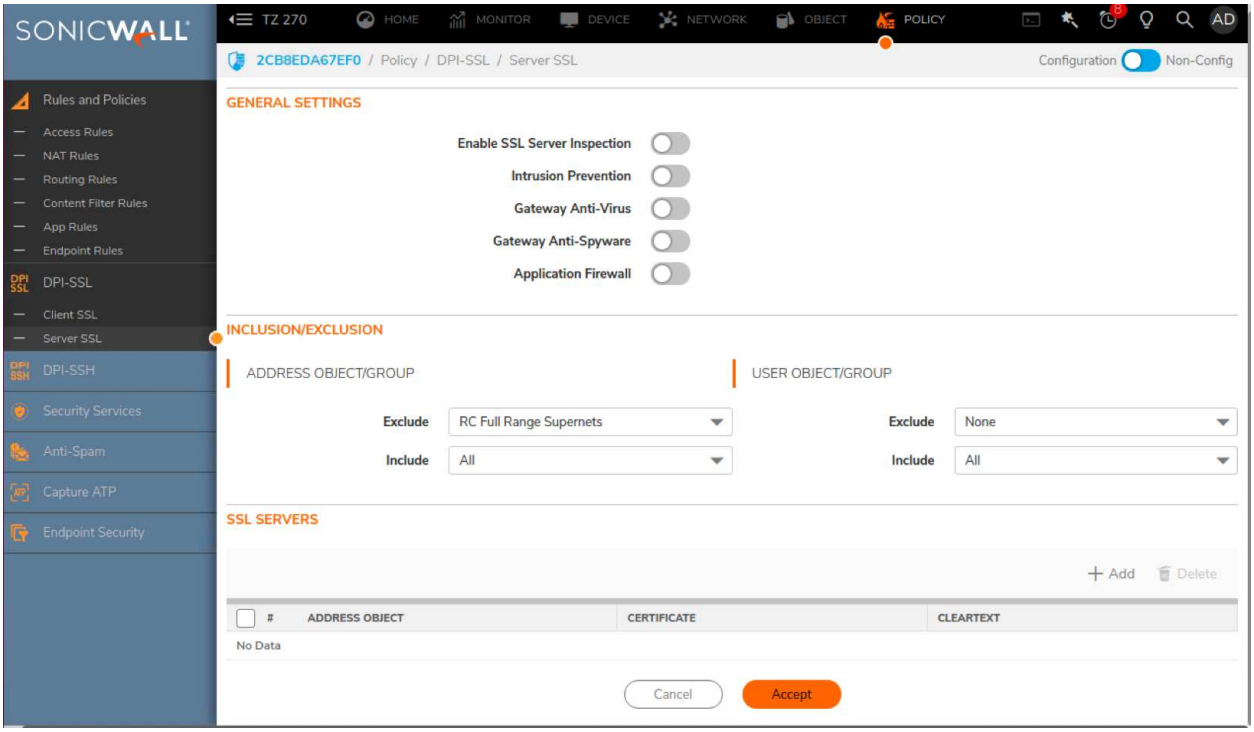
The RingCentral Access Rule should now be added.



10B. Click edit on the LAN to WAN setting and go to the Traffic Shaping tab.
10C. Set DSCP Marking to Explicit and Explicit DSCP Value to 46 (EF).
10D. Select the RingCentral Bandwidth management rule built-in SECTION 3.



11. Select Policy at the top of the screen
11A. On the left expand DPI-SSL/Server SSL
11B. Under the Inclusion/Exclusion section Exclude the RC Supernets under the Address Object/Group
11C. Hit Accept to commit the changes



Congratulations. You have finished configuring your SONICWALL TZ series 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.