

Recommended QoS Configuration Settings for SONICWALL TZ Series



Contents

- Introduction2
 - Supported Browsers for Test.....2
- Quality of Service.....3
 - Test Your Connection Capacity.....3
 - Test Your Connection Quality.....3
- Configure your router.....5
 - SONICWALL TZ Series.....5

- Ports and Firewalls Settings for RingCentral VoIP Service.....16

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

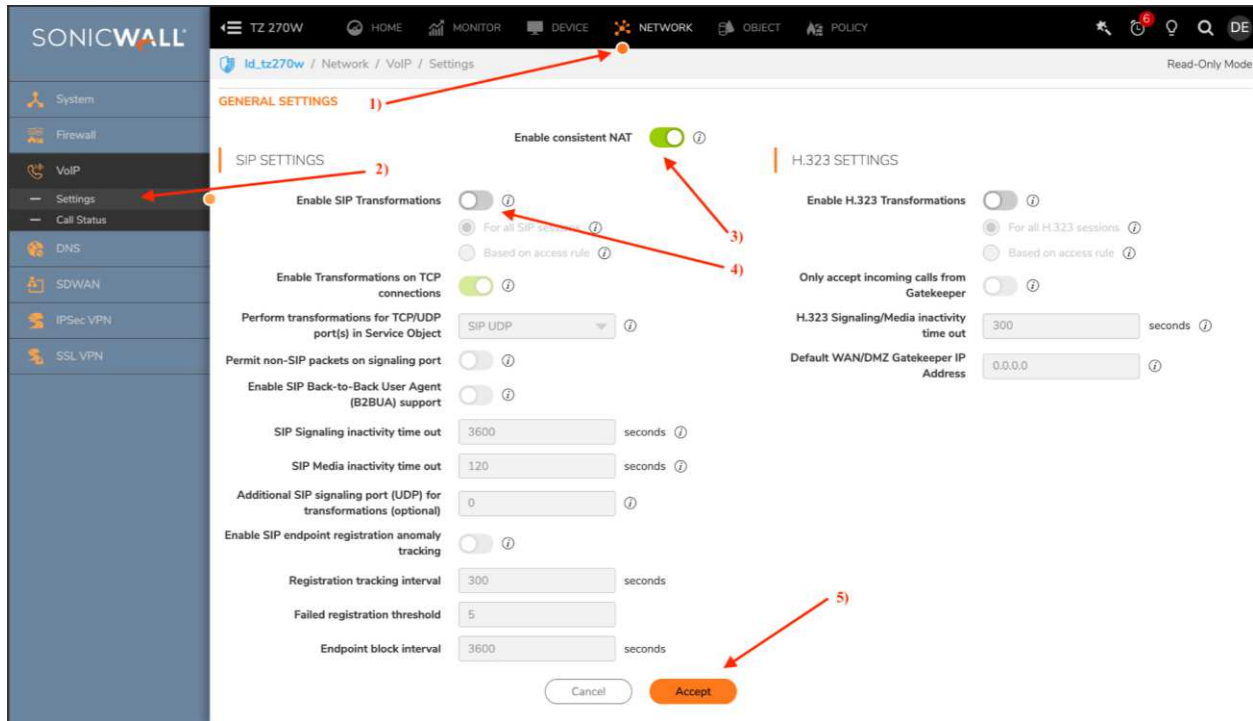
Source Port—Customer Side

Destination Port—RingCentral Side

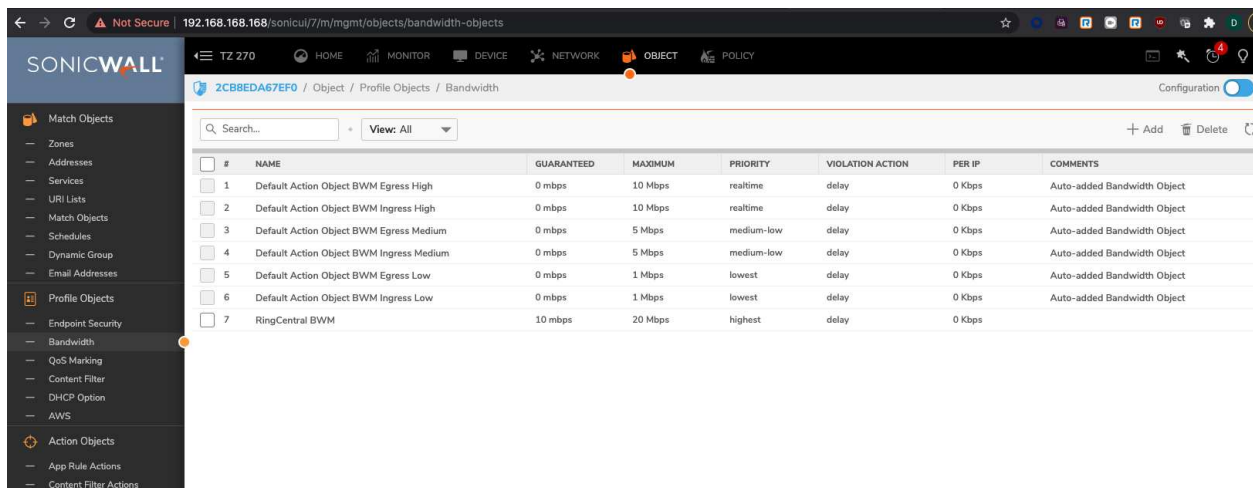
Also, see information on Port Triggering on the referenced [page](#).

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

- 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)



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



- Hit the +Add and give the object a name.
- Set the Guaranteed Bandwidth to 10 Mbps
- 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

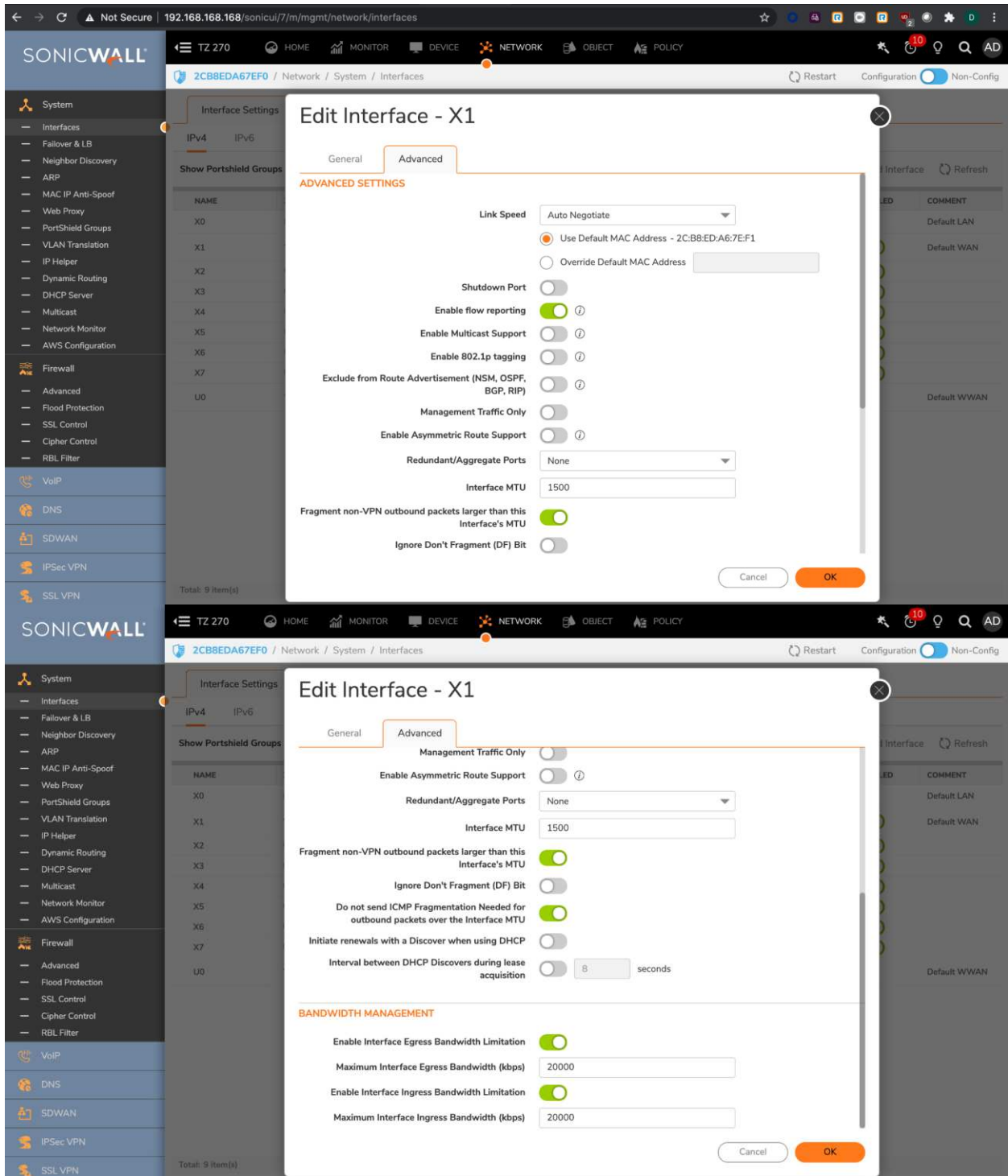
Bandwidth Object Settings

GeneralElemental

BANDWIDTH OBJECT SETTINGS

Name	<input type="text" value="RingCentral BWM"/>	
Guaranteed Bandwidth	<input type="text" value="10"/>	<input type="text" value="Mbps"/>
Maximum Bandwidth	<input type="text" value="20"/>	<input type="text" value="Mbps"/>
Traffic Priority	<input type="text" value="1 Highest"/>	
Violation Action	<input type="text" value="Delay"/>	
Comments	<input type="text"/>	

- 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

Edit Address Groups

Name

SHOW AVAILABLE

All (163)
 Hosts (47)
 Ranges (0)
 Networks (40)
 MAC (0)
 FQDN (1)
 Groups (75)

Not in Group 153 items

- All Authorized Access Points[GRP]
- All Interface IP[GRP]
- All Interface IPv6 Addresses[GRP]
- All Rogue Access Points[GRP]
- All Rogue Devices[GRP]
- All SonicPoints[GRP]
- All U0 Management IP[GRP]
- All WAN IP[GRP]

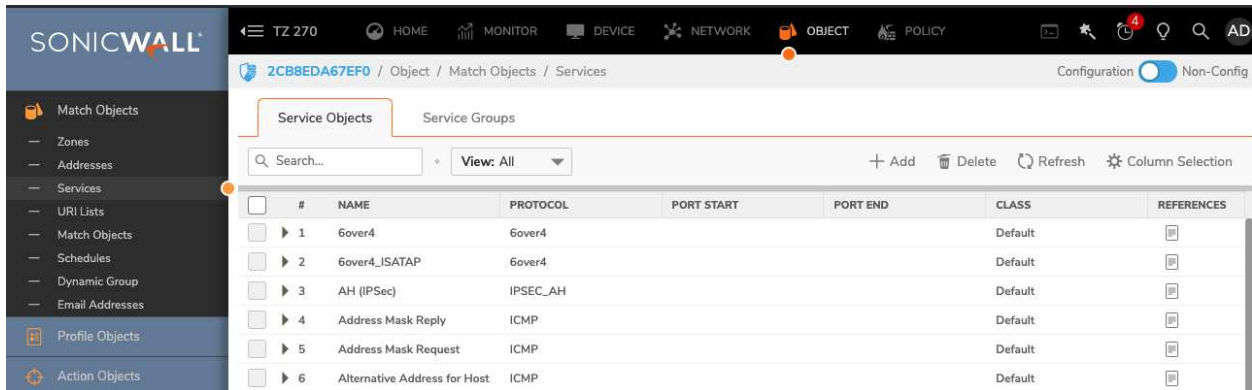
In Group 9 items

- RingCentral Range 9[NW]
- RingCentral Range1[NW]
- RingCentral Range2[NW]
- RingCentral Range3[NW]
- RingCentral Range4[NW]
- RingCentral Range5[NW]
- RingCentral Range6[NW]
- RingCentral Range7[NW]

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

<input type="checkbox"/>	▼ 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

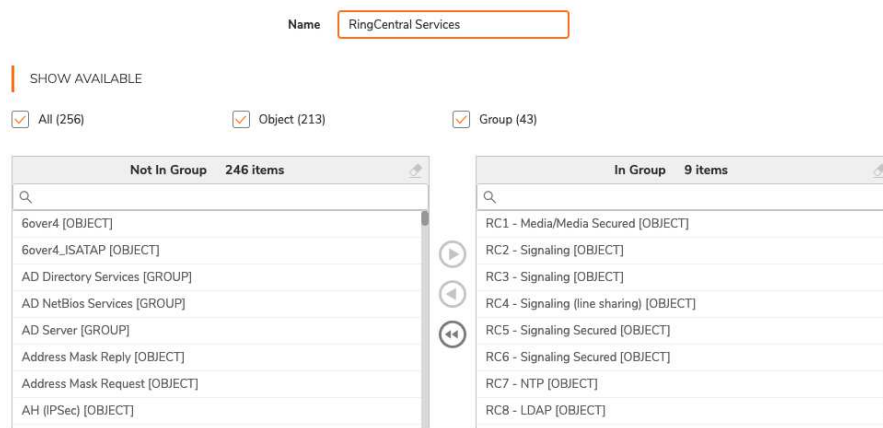


1. RC1: UDP 20000 - 64999 – Media/Media Secured
2. RC2: UDP 5090 – Signaling
3. RC3: TCP 5090 – Signaling
4. RC4: TCP 5099 – Signaling (when line sharing is used)
5. RC5: TCP 5096 – Signaling Secured
6. RC6: TCP 5098 – Signaling Secured
7. RC7: UDP - 123 – Network Time Service
8. RC8: TCP 636 – LDAP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

Editing 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

The screenshot displays the SonicWall management console interface. The top navigation bar includes 'TZ 270', 'HOME', 'MONITOR', 'DEVICE', 'NETWORK', 'OBJECT', and 'POLICY'. The breadcrumb trail shows '2CB8EDA67EF0 / Policy / Rules and Policies / Access Rules'. The left sidebar lists various rule categories, with 'Access Rules' selected. The main area shows a table of access rules with columns for 'GENERAL', 'ZONE', 'ADDRESS', and 'SERVICE'. The 'RingCentral_5' rule is highlighted in orange, indicating it is selected. Below the table, there are action buttons: '+ Add', 'Edit', 'Delete', 'Move', 'Enable', 'Disable', 'Live Counters', and 'Reset Counters'.

	GENERAL	ZONE	ADDRESS	SERVICE
	NAME	SOURCE	DESTINA...	DESTINATI...
1 (M)	Default Access Rule_1	LAN	LAN	All X2 Management IP
2 (M)	Default Access Rule_2	LAN	LAN	All X2 Management IP
3 (M)	Default Access Rule_3	LAN	LAN	All X2 Management IP
4 (A)	Default Access Rule_4	LAN	LAN	LAN Interface IP
5 (A)	RingCentral_5	LAN	WAN	RC Full Range Supernets
6 (M)	RC FQDN_6	LAN	WAN	RC FQDN
7 (M)	Failed Reg_7	LAN	WAN	test.phone
8 (M)	Default Access Rule_8	LAN	LAN	All X0 Management IP
9 (M)	Default Access Rule_9	LAN	LAN	All X0 Management IP
10 (M)	Default Access Rule_10	LAN	LAN	All X0 Management IP
11 (M)	Default Access Rule_11	LAN	LAN	Any
12 (M)	Default Access Rule_12	LAN	WAN	Any
13 (M)	Default Access Rule_13	LAN	DMZ	Any

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.

Adding Rule

The screenshot shows the 'Adding Rule' configuration page. The 'Name' field is set to 'RingCentral'. The 'Description' field contains the text 'provide a short description of your access rule...'. The 'Action' is set to 'Allow', 'Type' is 'IPv4', 'Priority' is 'Auto Prioritize', 'Schedule' is 'Always', and 'Enable' is checked. Below the main configuration, there are tabs for 'Source / Destination', 'User & TCP/UDP', 'Security Profiles', 'Traffic Shaping', 'Logging', and 'Optional Settings'. The 'Source / Destination' tab is active, showing 'SOURCE' and 'DESTINATION' settings. 'SOURCE' is set to 'Zone/Interface: LAN', 'Address: Any', and 'Port/Services: Any'. 'DESTINATION' is set to 'Zone/Interface: WAN', 'Address: Any', and 'Port/Services: Any'. There are 'Cancel' and 'Add' buttons at the bottom right.

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.

Editing Rule

Name: RingCentral

Description: provide a short description of your access rule...

Action: Allow (selected), Deny, Discard

Type: IPv4 (selected), IPv6

Priority: Auto Prioritize

Schedule: Always

Enable:

Source / Destination | User & TCP/UDP | Security Profiles | **Traffic Shaping** | Logging | Optional Settings

QOS (QUALITY OF SERVICE)

DSCP Marking: Explicit

Explicit DSCP Value: 46 - Expedited Forwarding (EF)

802.1p Marking: None

BWM (BANDWIDTH MANAGEMENT)

Egress BWM: RingCentral BWM

Ingress BWM: RingCentral BWM

Track Bandwidth Usage:

Show Diagram:

Cancel Save

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

SONICWALL

TZ 270 / Policy / DPI-SSL / Server SSL

Configuration Non-Config

GENERAL SETTINGS

Enable SSL Server Inspection

Intrusion Prevention

Gateway Anti-Virus

Gateway Anti-Spyware

Application Firewall

INCLUSION/EXCLUSION

ADDRESS OBJECT/GROUP

Exclude: RC Full Range Supernets

Include: All

USER OBJECT/GROUP

Exclude: None

Include: All

SSL SERVERS

+ Add Delete

#	ADDRESS OBJECT	CERTIFICATE	CLEARTEXT
No Data			

Cancel Accept

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](#).