Recommended QoS Configuration Settings for Dell SonicWALL SOHO Router

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 Dell® SonicWALL® SOHO router.

Additional routers tested and recommended are the Fortinet® FortiGate® 30D, and the AdTran® NetVanta® 3448. Recommended settings to optimize QoS for VoIP calls for these routers are presented in separate documents.

AdTran NetVanta 3448

Fortinet FortiGate 30D

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 Dell 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

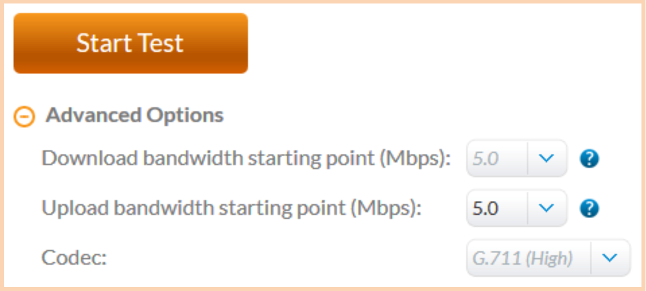
The RingCentral Connection Capacity test will help determine the maximum number of simultaneous RingCentral calls that can be supported on your broadband connection. Run this test during normal business hours when the connection is in use by other applications, including large file downloads.

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.

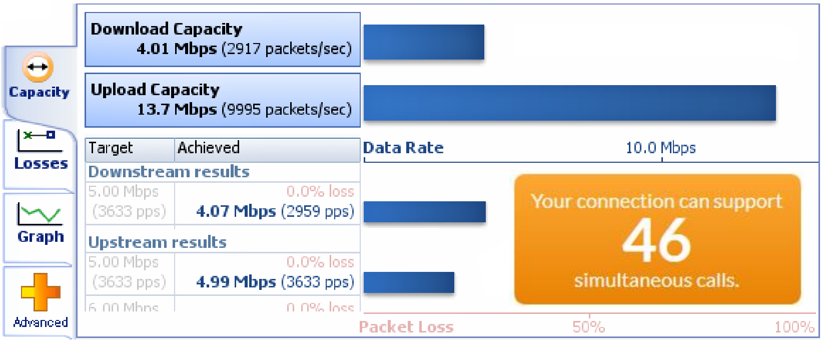


⊖ Advanced Options

Download bandwidth starting point (Mbps): 5.0

Upload bandwidth starting point (Mbps): 5.0

Codec: G.711 (High)



Download Capacity
4.01 Mbps (2917 packets/sec)

Upload Capacity
13.7 Mbps (9995 packets/sec)

Target	Achieved
Downstream results	
5.00 Mbps (3633 pps)	0.0% loss **4.07 Mbps** (2959 pps)
Upstream results	
5.00 Mbps (3633 pps)	0.0% loss **4.99 Mbps** (3633 pps)
6.00 Mbps	0.0% loss

Your connection can support 46 simultaneous calls.

Test your connection quality

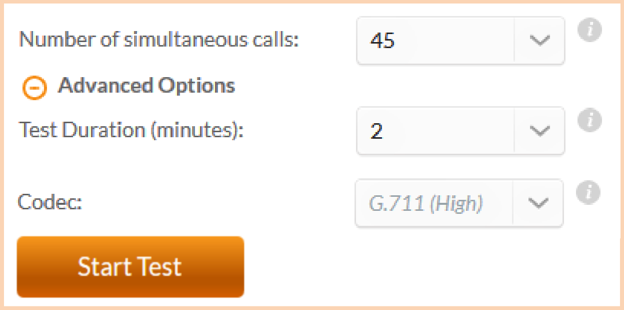
RingCentral provides a VoIP Quality test that will simulate VoIP calls between your computer and RingCentral, and provide an estimate of the voice quality you should expect when using our service. For the most accurate results, run this test *at least* three different times throughout a business day, 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.

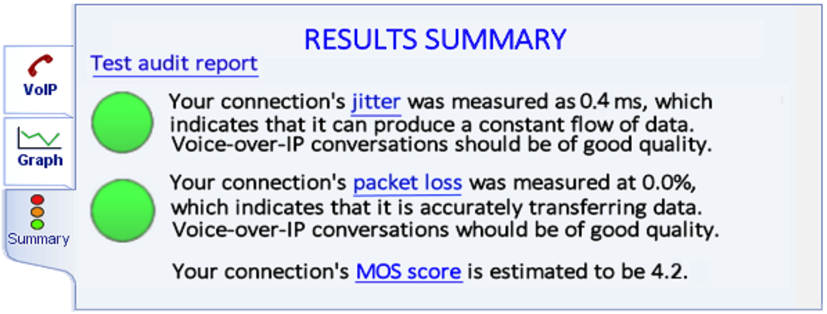


Number of simultaneous calls: 45

Advanced Options

Test Duration (minutes): 2

Codec: G.711 (High)



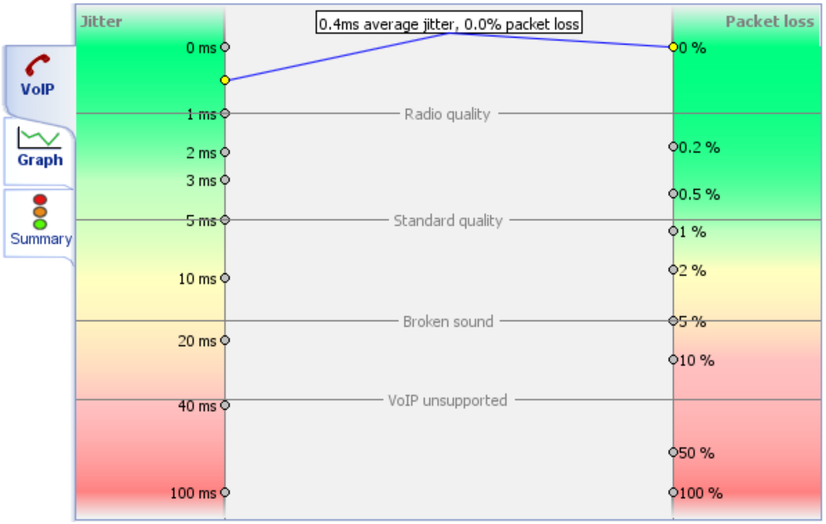
RESULTS SUMMARY

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 whould be of good quality.

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



Configure your router

Dell SonicWALL SOHO QoS configuration

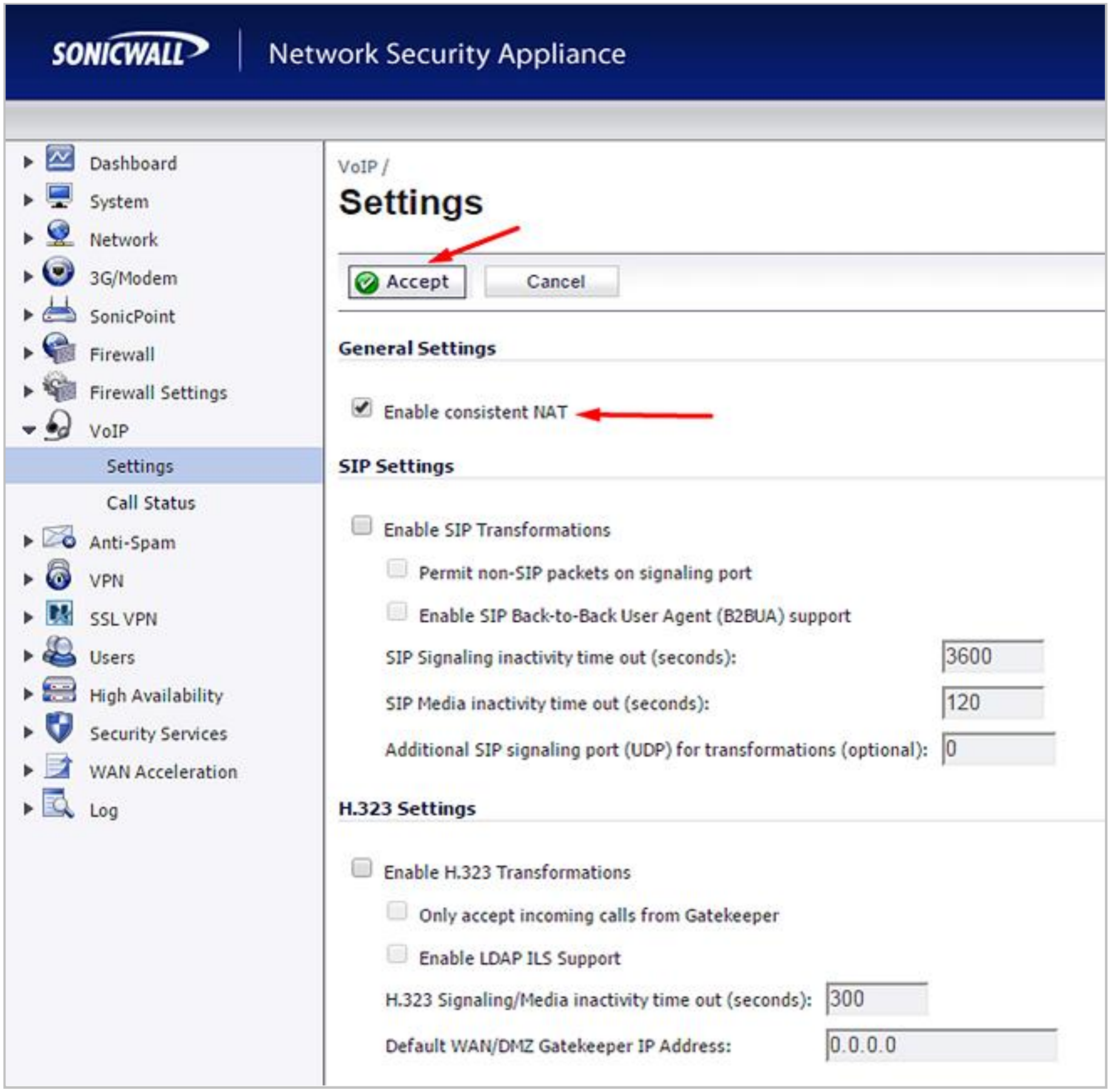
Brand:	Dell
Model:	SonicWALL SOHO
Hardware version:	12831
Firmware version:	SonicOS Enhanced 5.9.1.3-4o

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. On 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.)

2. On the left side of the page, expand **VoIP / Settings –** illustrated; *see instructions above.*



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

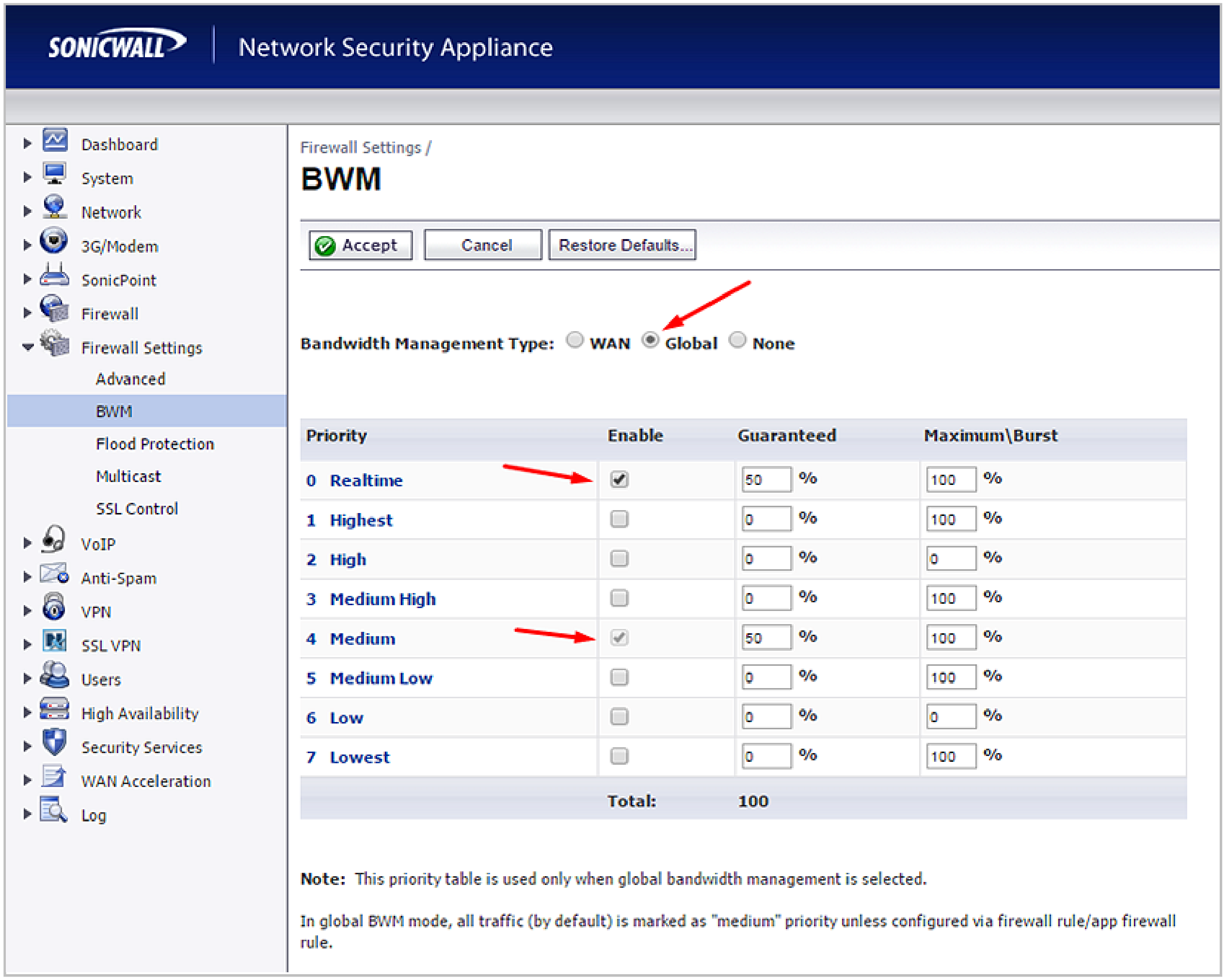
3. Go to **Firewall Settings / BWM**.

3A. Under **Bandwidth Management Type**, select **Global**.

3B. Under **Priority**, disable EVERY category, except for **Medium**, which is enabled by default; set **Maximum** to 30%; **Burst** to 50%.

3C. Enable **Realtime**; set **Maximum** to 70%; **Burst** to 100%.

3D. Click **Accept** to save changes/settings.



Firewall Settings /

BWM

Bandwidth Management Type: ○ WAN ● Global ○ None

Priority	Enable	Guaranteed	Maximum\Burst
0 Realtime	☑	50 %	100 %
1 Highest	☐	0 %	100 %
2 High	☐	0 %	0 %
3 Medium High	☐	0 %	100 %
4 Medium	☑	50 %	100 %
5 Medium Low	☐	0 %	100 %
6 Low	☐	0 %	0 %
7 Lowest	☐	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.

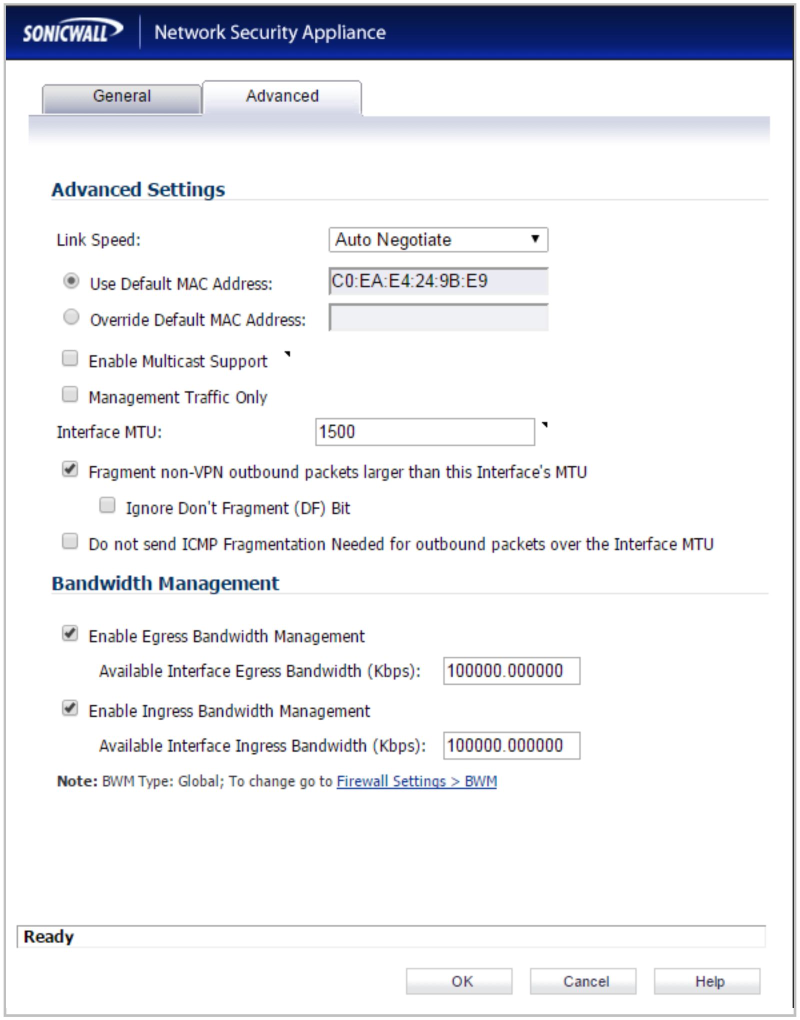
4. Go to **Network / Interfaces / X1 (WAN)**.

   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.



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

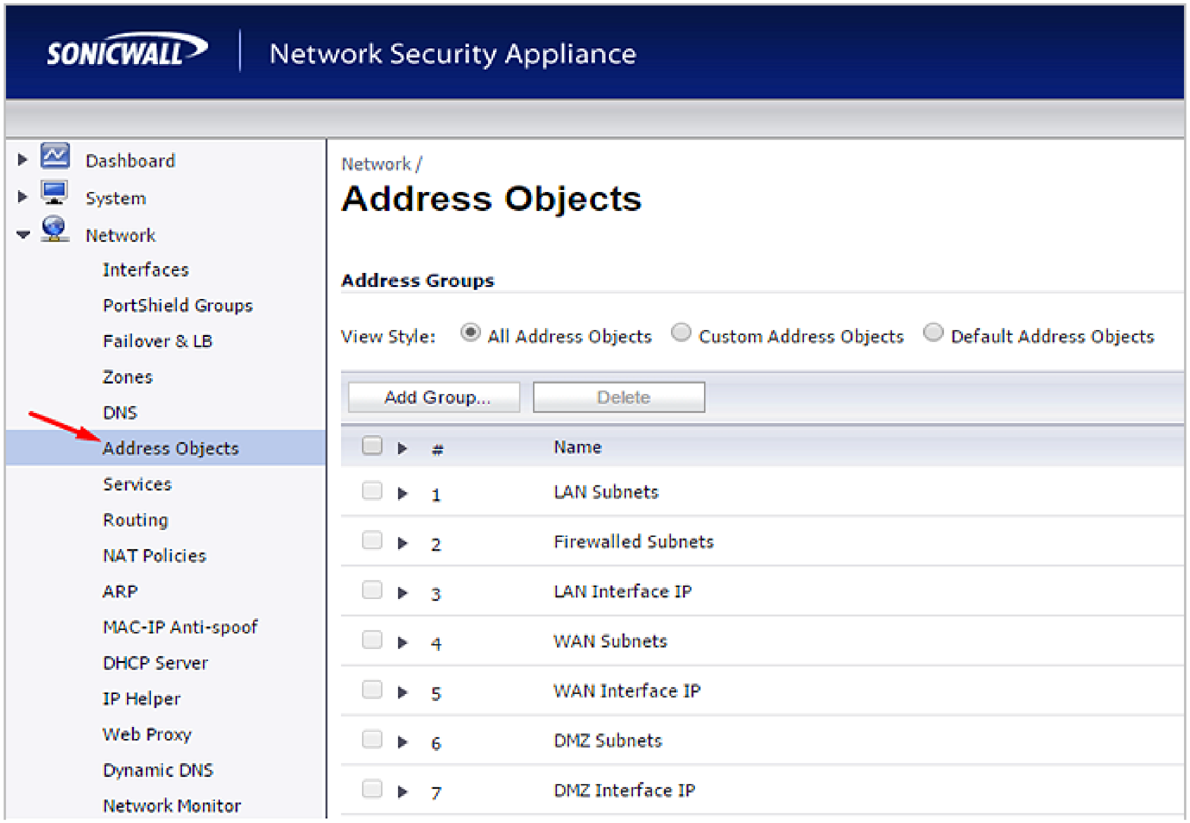
☑ Enable Ingress Bandwidth Management

Available Interface Ingress Bandwidth (Kbps): 100000.000000

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

Ready

5. On the left side of the page, **Expand Network.** Select **Address Objects** and create objects for both 199.255.120.0 and 199.68.212.0 with subnet masks of 255.255.252.0, as seen at right.



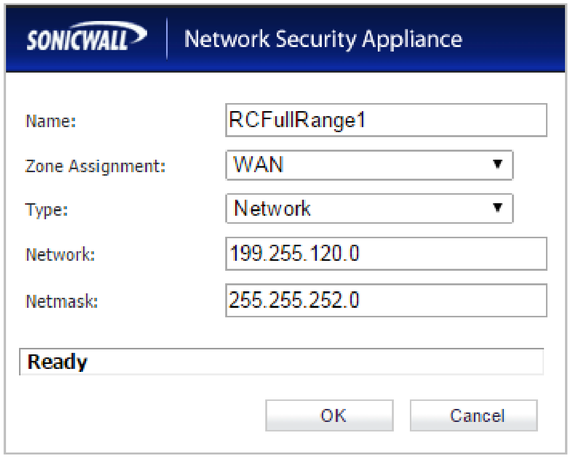
Network /

Address Objects

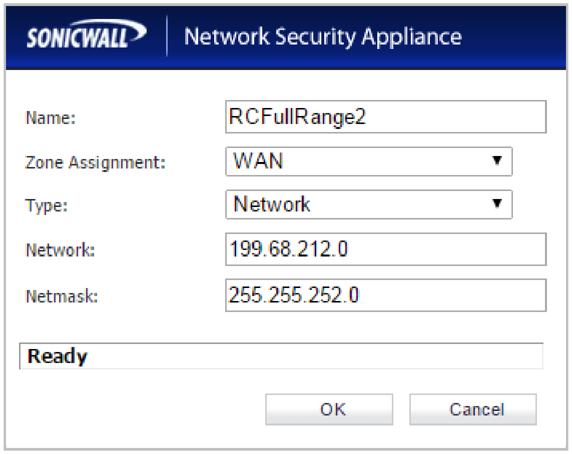
Address Groups

View Style: ● All Address Objects ○ Custom Address Objects ○ Default Address Objects

#	Name
1	LAN Subnets
2	Firewalled Subnets
3	LAN Interface IP
4	WAN Subnets
5	WAN Interface IP
6	DMZ Subnets
7	DMZ Interface IP

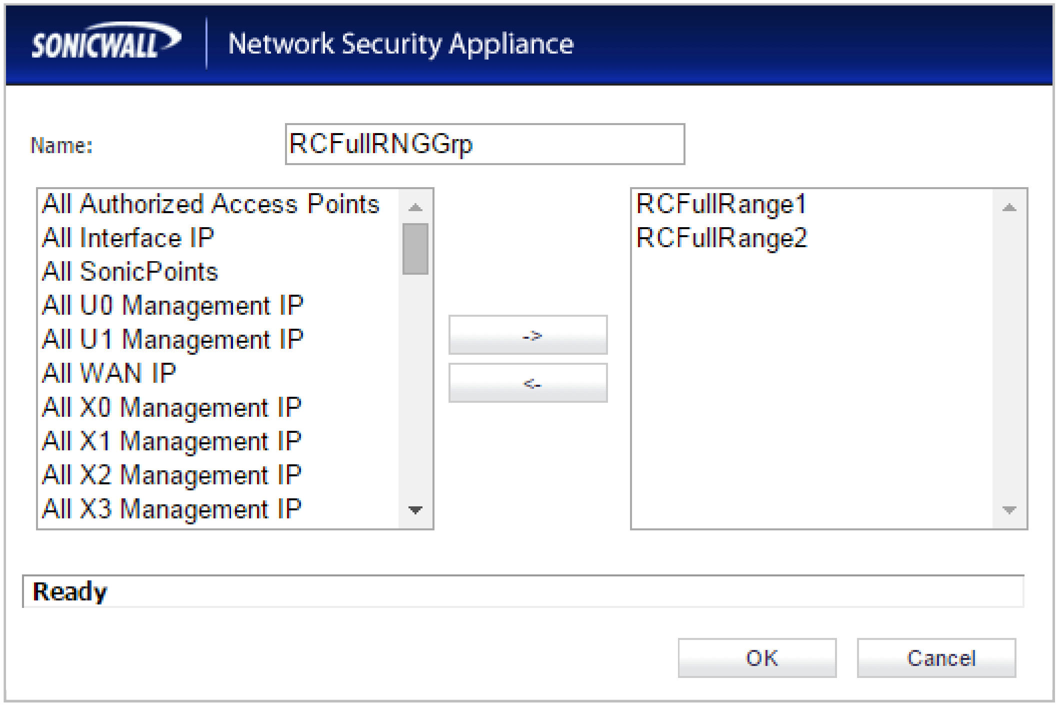


Name:	RCFullRange1
Zone Assignment:	WAN
Type:	Network
Network:	199.255.120.0
Netmask:	255.255.252.0



Name:	RCFullRange2
Zone Assignment:	WAN
Type:	Network
Network:	199.68.212.0
Netmask:	255.255.252.0

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



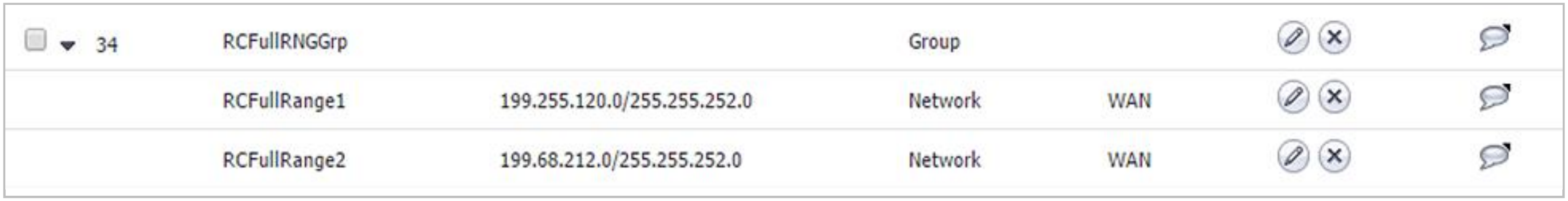
Name: RCFullRNGGrp

All Authorized Access Points
All Interface IP
All SonicPoints
All U0 Management IP
All U1 Management IP
All WAN IP
All X0 Management IP
All X1 Management IP
All X2 Management IP
All X3 Management IP

RCFullRange1
RCFullRange2

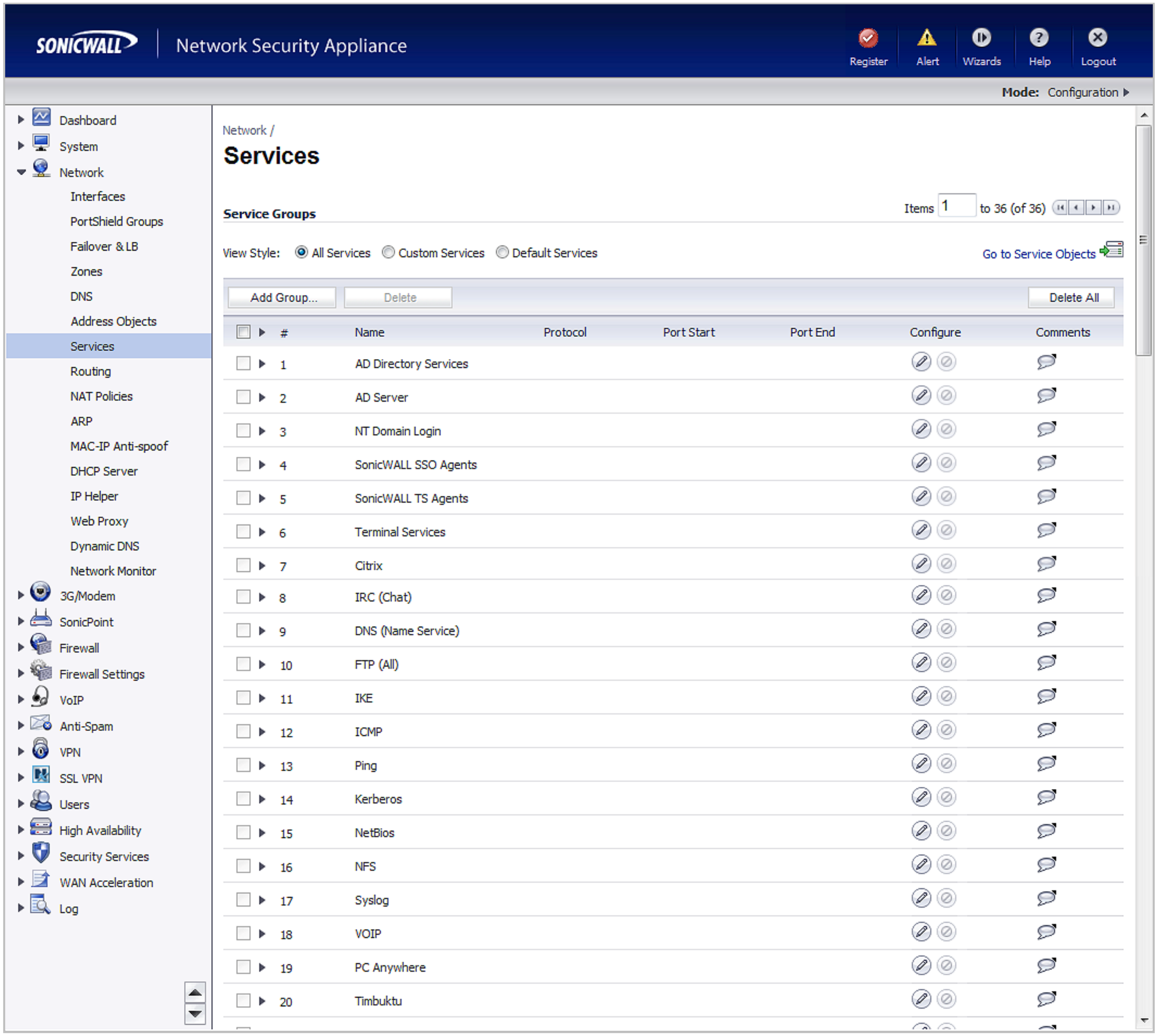
Ready

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



□ ▾ 34	RCFullRNGGrp		Group		
	RCFullRange1	199.255.120.0/255.255.252.0	Network	WAN	
	RCFullRange2	199.68.212.0/255.255.252.0	Network	WAN	

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



Network /

Services

Service Groups

Items 1 to 36 (of 36)

View Style: ● All Services ○ Custom Services ○ Default Services

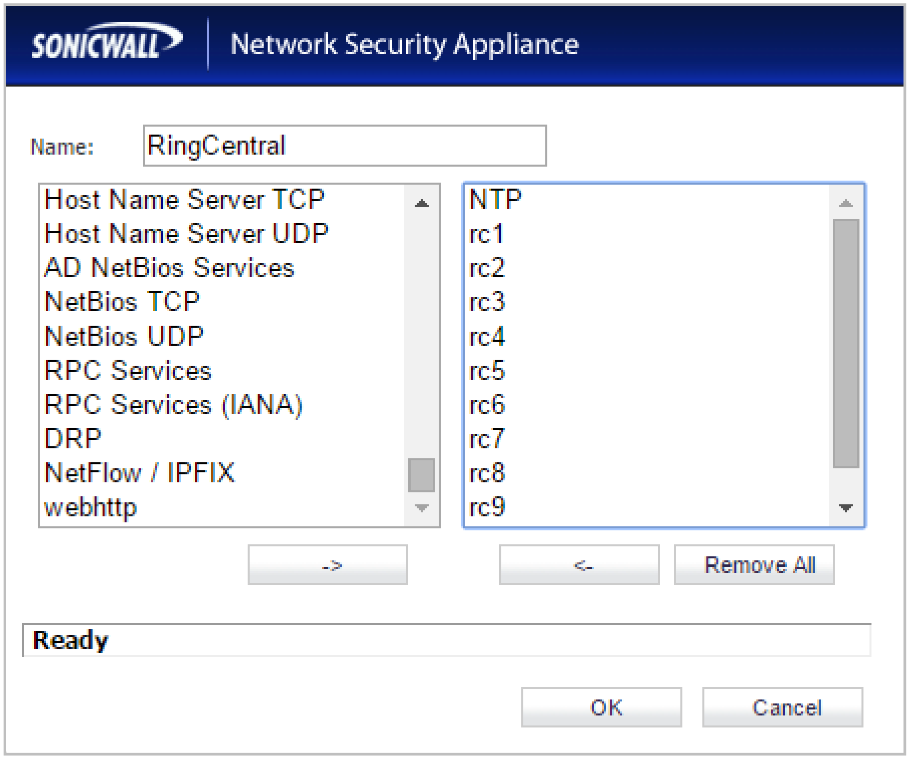
#	Name	Protocol	Port Start	Port End	Configure	Comments
1	AD Directory Services					
2	AD Server					
3	NT Domain Login					
4	SonicWALL SSO Agents					
5	SonicWALL TS Agents					
6	Terminal Services					
7	Citrix					
8	IRC (Chat)					
9	DNS (Name Service)					
10	FTP (All)					
11	IKE					
12	ICMP					
13	Ping					
14	Kerberos					
15	NetBios					
16	NFS					
17	Syslog					
18	VOIP					
19	PC Anywhere					
20	Timbuktu					

7B. Under **Services** click the add option. Then add five services, RC1 through RC5.

1. RC1: UDP 1000 – 65535
2. RC2: TCP 5060 – 6000
3. RC3: TCP 80 – 80
4. RC4: TCP 443 – 443
5. RC5: UDP 123 – 123

Note: Select applicable TCP/UDP port ranges, as needed, for your mobile and softphone apps from this table.

7D. Now select the **Add Group** option from the **Service Groups** section, also under the **Services** section. Name the group **RingCentral**; highlight **RC1** through **RC5**. Use the arrows in the box to move the highlighted information from left the right.



Name: RingCentral

Host Name Server TCP
Host Name Server UDP
AD NetBios Services
NetBios TCP
NetBios UDP
RPC Services
RPC Services (IANA)
DRP
NetFlow / IPFIX
webhttp

NTP
rc1
rc2
rc3
rc4
rc5
rc6
rc7
rc8
rc9

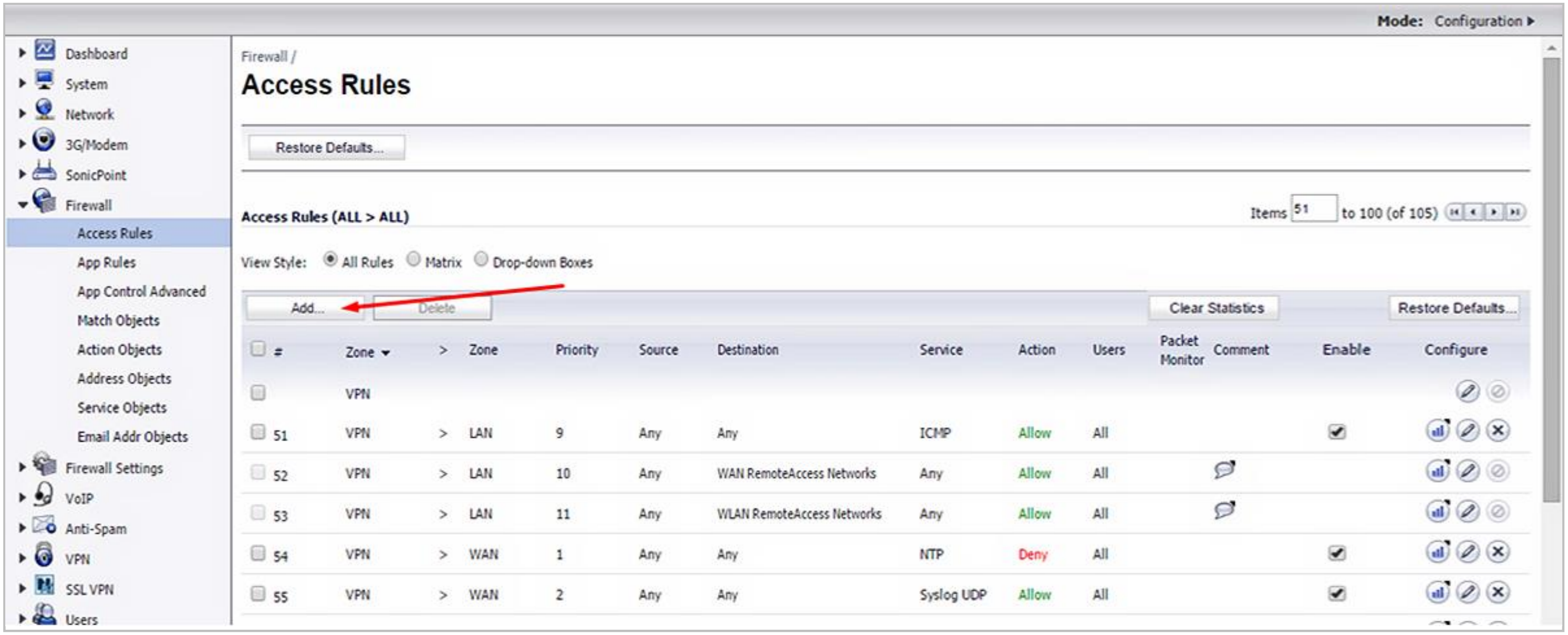
Ready

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.

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



Access Rules

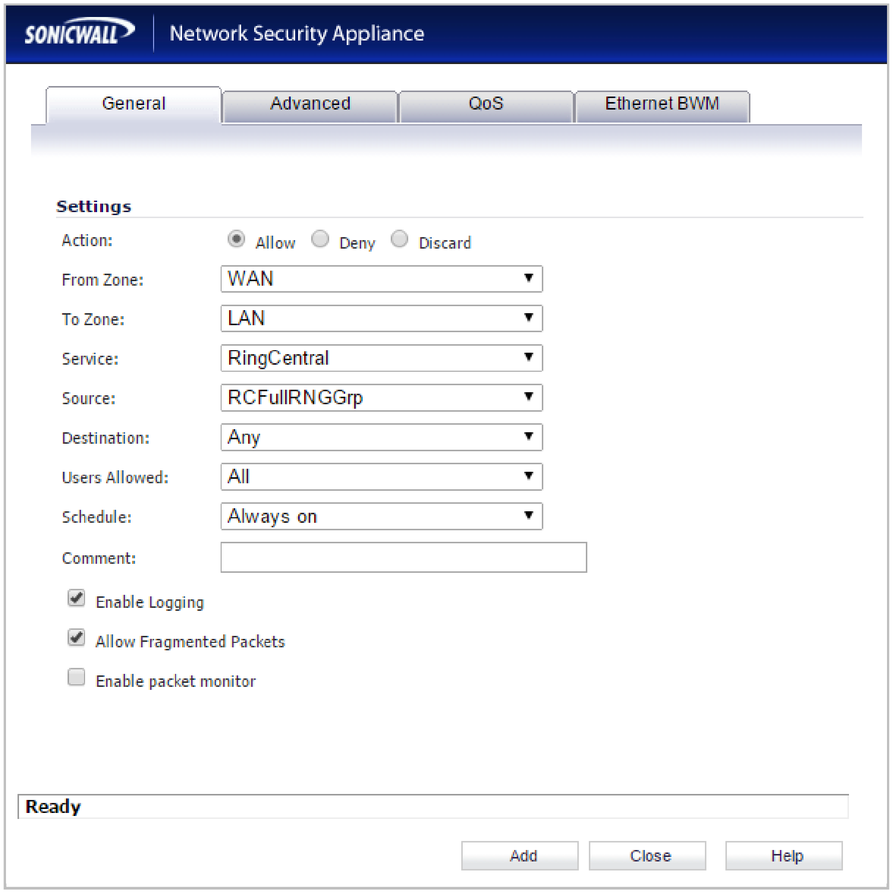
Access Rules (ALL > ALL)

Items 51 to 100 (of 105)

View Style: ● All Rules ○ Matrix ○ Drop-down Boxes

□ #	Zone	>	Zone	Priority	Source	Destination	Service	Action	Users	Packet Monitor	Comment	Enable	Configure
□	VPN												
□ 51	VPN	>	LAN	9	Any	Any	ICMP	Allow	All			☑	
□ 52	VPN	>	LAN	10	Any	WAN RemoteAccess Networks	Any	Allow	All		💬		
□ 53	VPN	>	LAN	11	Any	WLAN RemoteAccess Networks	Any	Allow	All		💬		
□ 54	VPN	>	WAN	1	Any	Any	NTP	Deny	All			☑	
□ 55	VPN	>	WAN	2	Any	Any	Syslog UDP	Allow	All			☑	

9. Create two new rules for WAN to LAN and LAN to WAN, as seen below. Select **Add** for both.



Settings

Action: ● Allow ○ Deny ○ Discard

From Zone: WAN

To Zone: LAN

Service: RingCentral

Source: RCFullRNGGrp

Destination: Any

Users Allowed: All

Schedule: Always on

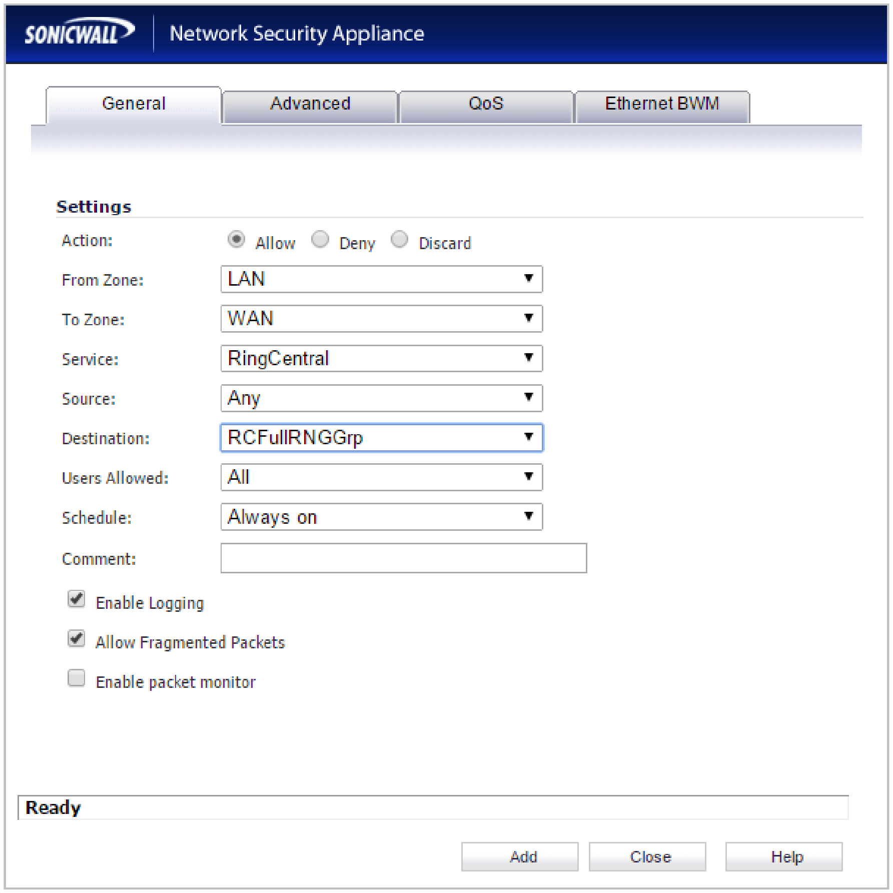
Comment:

☑ Enable Logging

☑ Allow Fragmented Packets

☐ Enable packet monitor

Ready



Settings

Action: ● Allow ○ Deny ○ Discard

From Zone: LAN

To Zone: WAN

Service: RingCentral

Source: Any

Destination: RCFullRNGGrp

Users Allowed: All

Schedule: Always on

Comment:

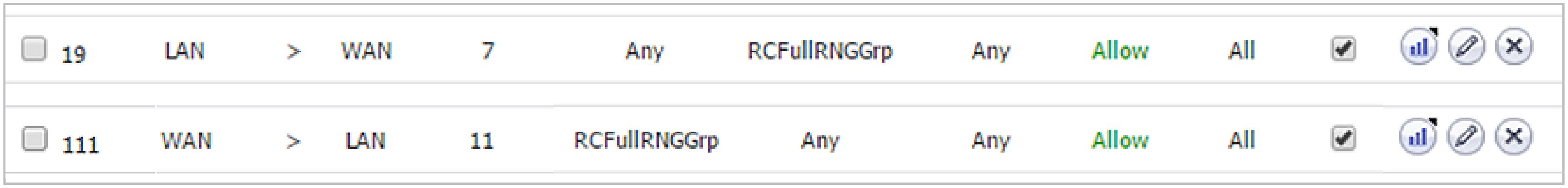
☑ Enable Logging

☑ Allow Fragmented Packets

☐ Enable packet monitor

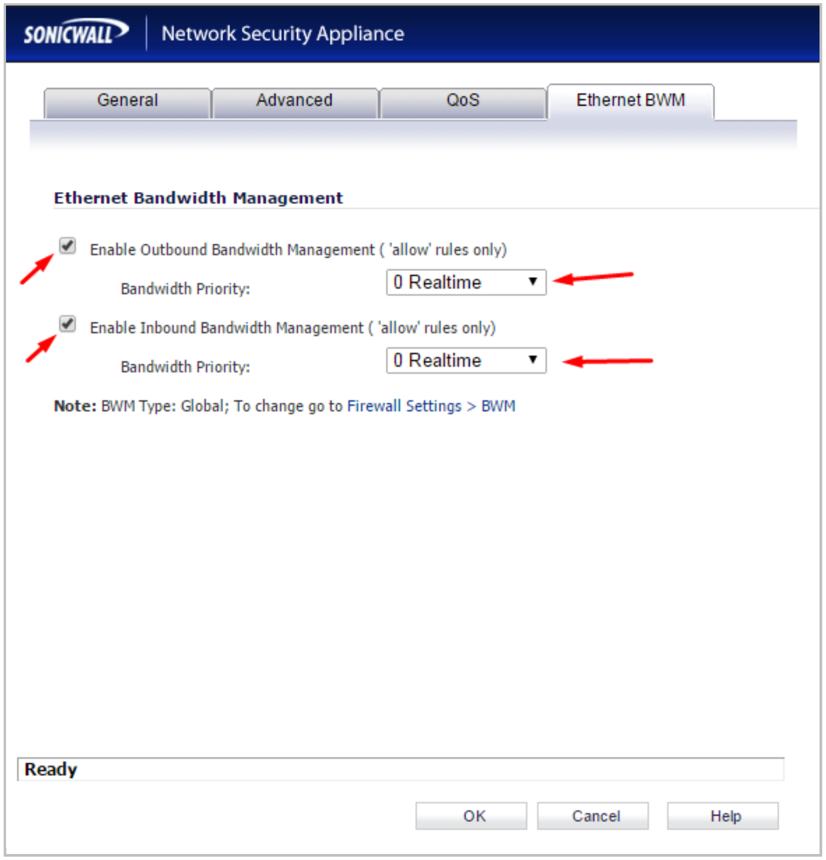
Ready

10. The RingCentral Access Rule should now be added.



□	19	LAN	>	WAN	7	Any	RCFullRNGGrp	Any	Allow	All	☑	
□	111	WAN	>	LAN	11	RCFullRNGGrp	Any	Any	Allow	All	☑	

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**.



Ethernet Bandwidth Management

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

Bandwidth Priority: 0 Realtime

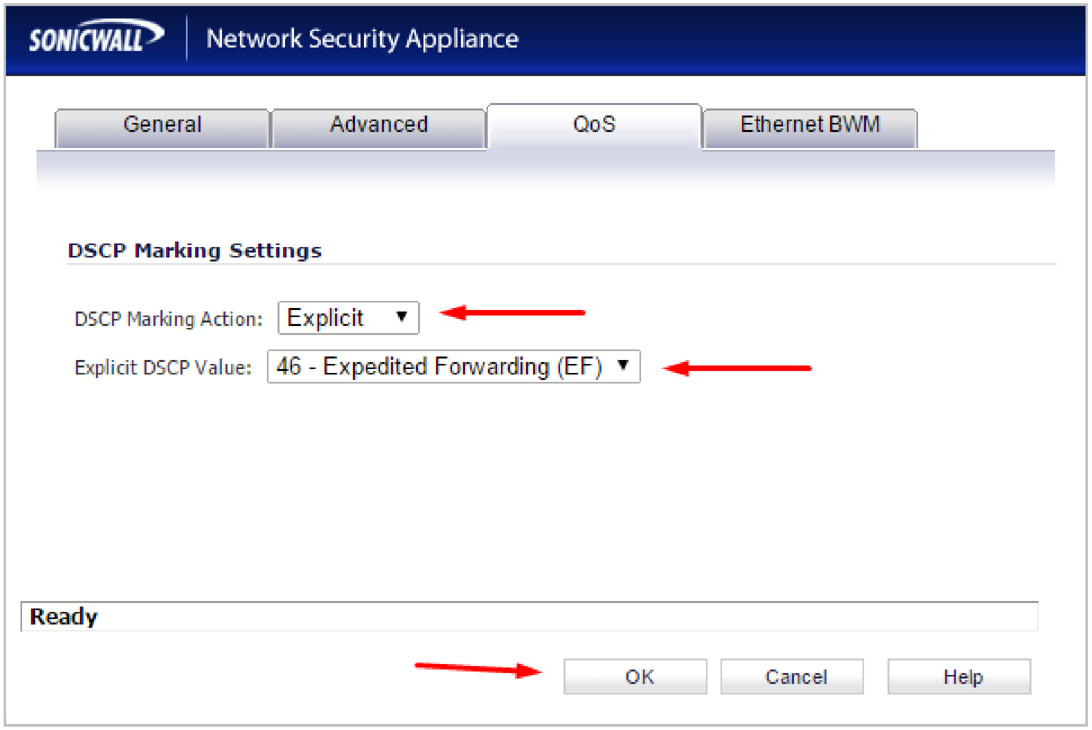
☑ Enable Inbound Bandwidth Management ('allow' rules only)

Bandwidth Priority: 0 Realtime

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

Ready

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.



DSCP Marking Settings

DSCP Marking Action: Explicit

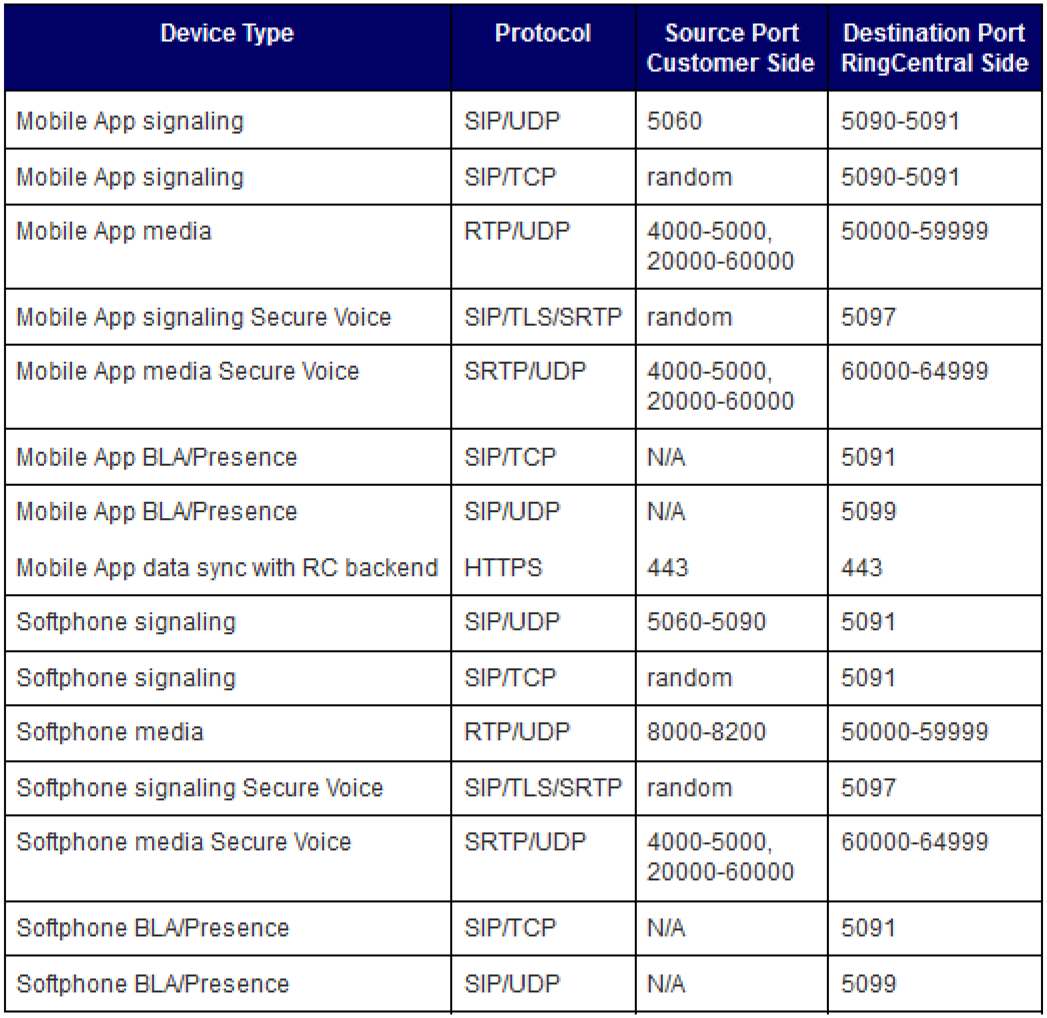
Explicit DSCP Value: 46 - Expedited Forwarding (EF)

Ready

Congratulations. You have finished configuring your Dell 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.

Port and firewall settings for mobile and softphone apps



Device Type	Protocol	Source Port Customer Side	Destination Port RingCentral Side
Mobile App signaling	SIP/UDP	5060	5090-5091
Mobile App signaling	SIP/TCP	random	5090-5091
Mobile App media	RTP/UDP	4000-5000, 20000-60000	50000-59999
Mobile App signaling Secure Voice	SIP/TLS/SRTP	random	5097
Mobile App media Secure Voice	SRTP/UDP	4000-5000, 20000-60000	60000-64999
Mobile App BLA/Presence	SIP/TCP	N/A	5091
Mobile App BLA/Presence	SIP/UDP	N/A	5099
Mobile App data sync with RC backend	HTTPS	443	443
Softphone signaling	SIP/UDP	5060-5090	5091
Softphone signaling	SIP/TCP	random	5091
Softphone media	RTP/UDP	8000-8200	50000-59999
Softphone signaling Secure Voice	SIP/TLS/SRTP	random	5097
Softphone media Secure Voice	SRTP/UDP	4000-5000, 20000-60000	60000-64999
Softphone BLA/Presence	SIP/TCP	N/A	5091
Softphone BLA/Presence	SIP/UDP	N/A	5099