



## Vopro VoIP & QoS Configuration for SonicWALL Firewalls

1. Selecting the right SonicWALL model
2. Configuring SonicWALL enhanced OS for QoS
3. Configuring SonicWALL for Failover (Dual WAN)
4. Configuring SonicWALL to force phones to use secondary WAN (X2)

### **Selecting the right SonicWALL for your needs:**

All models are not created equally. It's optimal to have a SonicWALL that is fast enough to handle all traffic on the network. This includes computers, phones, wireless access points, etc., anything that uses it as the gateway. The differences in the models are not only related to how many ports or VPN tunnels they offer, but also the amount of RAM, CPU speed, and throughput. If your SonicWALL is too slow to handle the entire network load, your VoIP quality will suffer. Models change from time to time, so this guide isn't meant to tell you exactly which model to purchase, but rather to suggest that you consult your SonicWALL vendor when selecting the proper model for your environment. Keep in mind that if a SonicWALL is configured properly, it will be doing stateful packet inspection, anti-virus, anti-spyware, VPNs, etc, etc. It has a lot of work to do, so a faster box is going to produce better results overall. If the budget supports it, an NSA model is always a great choice, but the CURRENT higher end TZ models should work well for most. The older, white plastic TZ models generally should not be used for hosted VoIP on any network with more than 25 devices.

# Configuring SonicWALL Enhanced OS for QoS

This is a step by step guide of how to configure a SonicWALL for hosted VoIP. You should be using firmware SonicOS Enhanced 6.5 or higher. **\*NOTE\* For the SonicWALL to work properly in providing QoS for VoIP traffic, ALL network devices must go through the SonicWALL for Internet access. If you plug in something like a wireless access point into an open port on your Internet provider's gateway box, that traffic will not be managed and can throttle your bandwidth and cause the VoIP traffic to not have priority over it!**

## 1. Consistent NAT

The screenshot shows the SonicWALL management interface. The left sidebar contains navigation options: Updates, Licenses, Firmware & Backups, WXA Firmware, Restart, Connectivity, VPN, SSL VPN, Access Points, 3G/4G/Modem, Policies, Rules, Objects, System Setup, Appliance, Users, Network, SD-WAN, High Availability, WAN Acceleration, and VOIP. The main content area is titled 'General Settings' and 'SIP Settings'. Under 'General Settings', the checkbox 'Enable consistent NAT' is checked. Under 'SIP Settings', the checkbox 'Enable SIP Transformations' is unchecked, and 'Enable Transformations on TCP connections' is checked. A yellow callout box with a black border contains the following text: 'Check the box to "Enable consistent NAT". Never check any of the boxes under SIP Settings unless specifically told to by your provider. Most VoIP providers perform the SIP Transformations on their end. This will cause one way audio issues and internal calls to go to incorrect extensions, etc. etc.'

**Located under VoIP/Settings.** This should always be checked. Consistent NAT enhances standard NAT policy to provide greater compatibility with peer-to-peer applications that require a consistent IP address to connect to, such as VoIP. Consistent NAT uses an MD5 hashing method to consistently assign the same mapped public IP address and UDP Port pair to each internal private IP address and port pair. Basically, this allows the SIP server to always locate your phones behind the firewall.

## 2. UDP Default to 90

The screenshot shows the SonicWall Network Security Appliance configuration interface. The top navigation bar includes 'MONITOR', 'INVESTIGATE', 'MANAGE', and 'QUICK CONFIGURATION'. The left sidebar shows the navigation menu with 'Firewall Settings' expanded to 'Flood Protection'. The main content area is titled 'UDP Settings' and includes the following sections:

- UDP Settings:** 'Default UDP Connection Timeout (seconds):' is set to 90.
- UDP Flood Protection:** 'Enable UDP Flood Protection' is unchecked. 'UDP Flood Attack Threshold (UDP Packets / Sec):' is 1000, 'UDP Flood Attack Blocking Time (Sec):' is 2, and 'UDP Flood Attack Protected Destination List:' is 'Any'.
- UDP Traffic Statistics:** A table with the following rows: Connections Opened, Connections Closed, Total UDP Packets, Validated Packets Passed, Malformed Packets Dropped, UDP Floods In Progress, Total UDP Floods Detected, and Total UDP Flood Packets Rejected.

A yellow callout box with the text 'Nothing else on this page needs to be changed from the default settings.' is overlaid on the statistics table. A blue arrow points from the 'UDP' tab to the 'UDP Settings' section, and another blue arrow points from the '90' input field to the 'UDP Settings' section. A black arrow points from the 'Flood Protection' menu item to the main content area.

**Located under Manage/Firewall Settings/Flood Protection.** This is the number of seconds of idle time you want to allow before UDP connections time out. **This value is overridden by the UDP Connection timeout you set for individual rules.** If this value is too short, the SIP server will lose your phone's registrations and won't be able to find your phones. However, if this setting is too high, it makes your network vulnerable to hackers since UDP ports will be left open too long. You can opt to set it on the rule we are going to create, but it is easy to do it here for all newly created rules. If you are concerned about utmost security, I recommend leaving the default at 30, and just setting your VoIP firewall rule to 90.

# Configuring SonicWALL enhanced OS for QoS

In this section, you're going to create a custom service for the ports that SkySwitch uses for the streaming audio portion of phone calls, then create a Group with that newly created service, along with the built in SIP services (5060 & 5061).

## 3. Create Custom Service for RTP (2000-65000)

The screenshot shows the SonicWALL Manage interface. The top navigation bar includes 'MONITOR', 'INVESTIGATE', 'MANAGE', and 'QUICK CONFIGURATION'. The left sidebar shows a navigation tree with 'Objects' expanded to 'Service Objects'. The main content area displays the 'Service Objects' configuration page. At the top, there are tabs for 'Service Objects' and 'Service Groups', along with '+ Add', '- Delete', and a search box. Below this is a table of service objects:

#	Name	Protocol	Port Start	Port End	Class	Comments	Configure
1	DVR Media	TCP	1160	1160	Custom		
2	DVR Web	TCP	82	82	Custom		
3	VOIP RTP	UDP	2000	65000	Custom		

An arrow points to the 'VOIP RTP' service in the table.

**Located under Manage/Objects/Service Objects.** Here you will create a custom service for the RTP ports the phones use to stream audio over the Internet. Click on View Custom on the

Service Objects tab, then click +ADD.

Not secure | 10.0.20.1/addServiceObjDlg.html

SONICWALL™ Network Security Appliance

Name: VOIP RTP

Protocol: UDP(17)

Port Range: 2000 - 65000

Sub Type: None

Ready

OK CANCEL

Give the service any name you like, choose UDP as the protocol, and set the port range as shown. Ok to Save.

#### 4. Create Custom Group for RTP and SIP

SONICWALL™ Network Security Appliance MONITOR INVESTIGATE MANAGE QUICK CONFIGURATION Help | Logout

Firewall Name: COEAE474A084 Mode: Configuration

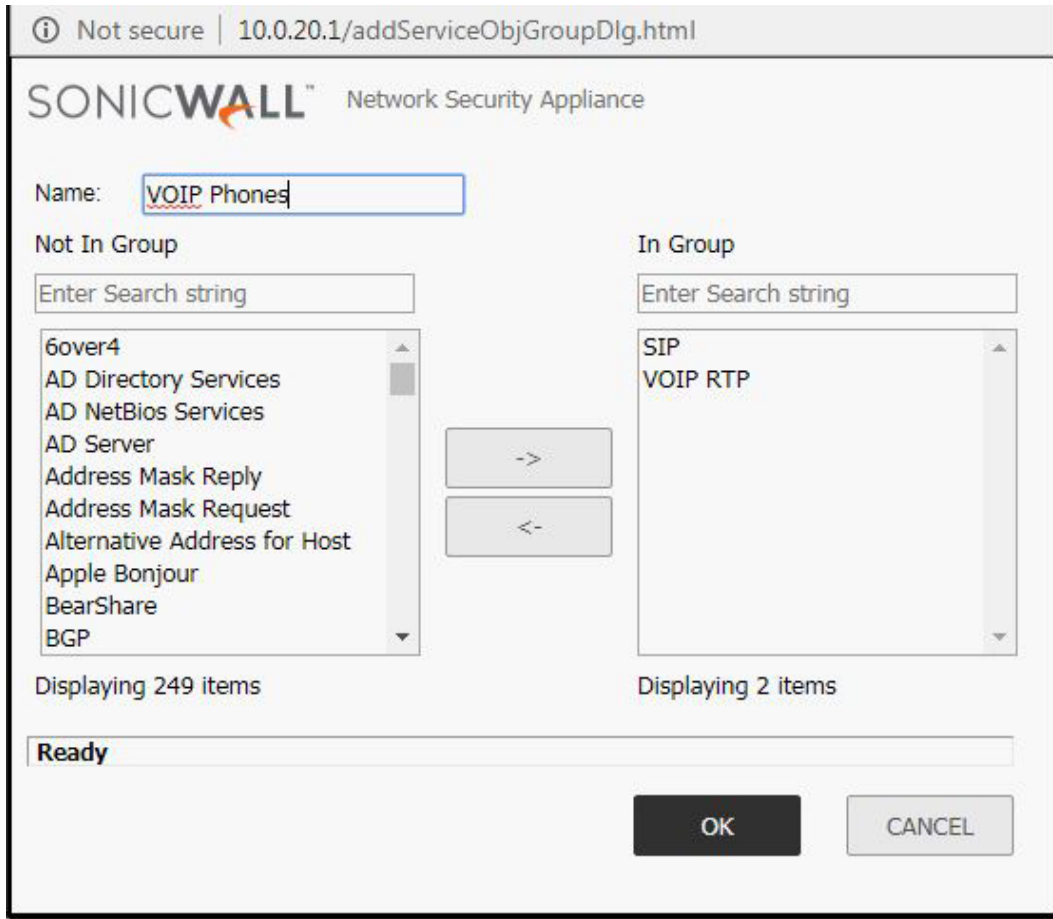
Service Objects Service Groups

+ Add - Delete Search... View Custom

#	Name	Protocol	Port Start	Port End	Class	Comments	Configure
1	DVR				Custom		
2	DVR-CAMS Services				Custom		
3	Temp Routing Group				Custom		
4	VOIP Phones				Custom		
	SIP	UDP	5060	5061	Default		
	VOIP RTP	UDP	2000	65000	Custom		

Here, you will create a group with the new RTP service you just created along with the built in SIP service that the SonicWALL already has (ports 5060 & 5061).

**Located under Manage/Service Objects/Service Groups Tab.** Click on Service Groups Tab, set View to Custom, and then click +Add



Give the group a name, then add the custom service you just created for RTP along with the SIP service that already exists. Press OK to save.

## 5. Create LAN > WAN rule for new Service

The screenshot shows the SonicWall configuration interface. The top navigation bar includes 'MANAGE' and 'QUICK CONFIGURATION'. The left sidebar shows the 'Rules' section expanded to 'Access Rules'. The main area displays a table of existing rules:

#	Name	From	To	Priority	Source	Destination	Service	Action	Users Incl.	Users Excl.	Cl.
1	v4	LAN	WAN	6 (Auto)	Any	Any	VOIP Phones	Allow	All	None	Cu
2	v4	LAN	WAN	7 (Manual)	Any	Any	Any	Allow	All	None	De
3	v6	LAN	WAN	134 (Manual)	Any	Any	Any	Allow	All	None	De

An arrow points to the 'To' column, which is set to 'WAN'.

You will now create a single rule that is going to control QoS for all VoIP phones on the network.

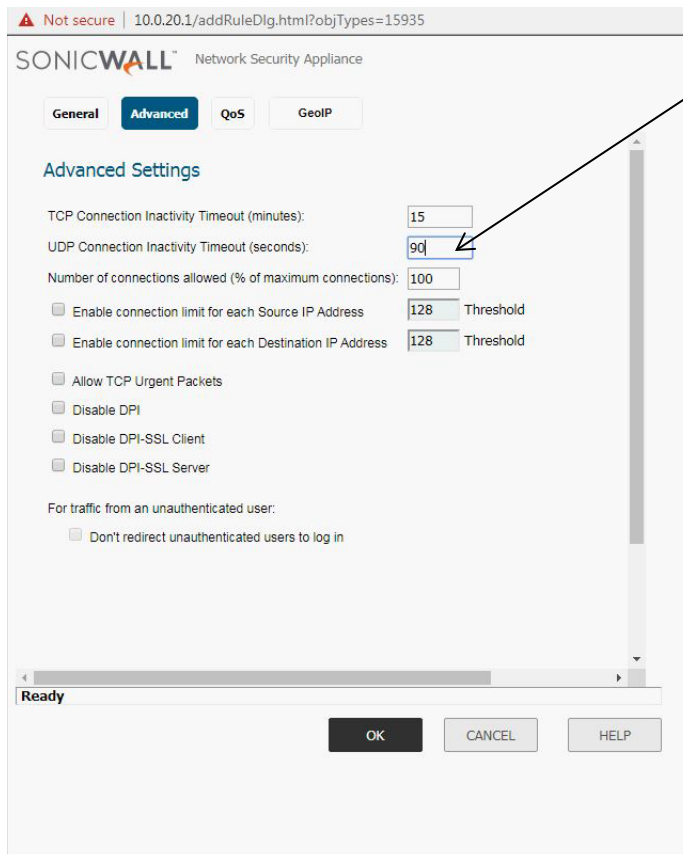
**Located under Manage/Rules/Access Rules.** Choose From LAN to WAN. You will be creating a rule from LAN to WAN. You will be configuring 3 tabs for this rule. Press +ADD

The screenshot shows the 'Add Rule' dialog box in the SonicWall configuration interface, specifically the 'QoS' tab. The settings are as follows:

- Policy Name: (empty)
- Action:  Allow  Deny  Discard
- From: LAN
- To: WAN
- Source Port: Any
- Service: VOIP Phones
- Source: Any
- Destination: Any
- Users Included: All
- Users Excluded: None
- Schedule: Always on
- Priority: Retain original priority
- Comment: QoS for Phones
- IP Version:  IPv4  IPv6

The dialog box is titled 'Ready' and has 'OK', 'CANCEL', and 'HELP' buttons at the bottom.

For Service, choose the custom group service you just created in the previous step. Source and Destination can be Any. Set a comment so you know what this rule is for.



The only setting that needs to be modified on the Advanced tab is the UDP Connection Inactivity Timeout. 90 seconds should be sufficient, but some phones might require more. Adjust accordingly. If you didn't modify the default setting, make sure you adjust this setting to 90. This will only apply to your phones, not every device on the network. This is more secure for your network.



Not secure | 10.0.20.1/addRuleDlg.html?objTypes=15935#

SONICWALL™ Network Security Appliance

General Advanced **QoS** GeolP

### DSCP Marking Settings

DSCP Marking Action:

Explicit DSCP Value:

### 802.1p Marking Settings

802.1p Marking Action:

Note: No 802.1p tagging

Ready

OK CANCEL HELP

On the QoS tab/DSCP Marking Settings:

Choose **Explicit** from the drop down for DSCP Marking Action.

Choose **46 – Expedited Forwarding** from the Explicit DSCP Value drop down.

This is the setting that tells the SonicWALL to forward VoIP packets first from the LAN to the WAN.

# Configuring SonicWALL Enhanced OS for Failover (Dual WAN)

With one of VoIP's failure points being the WAN connection, it's always a good idea to recommend having a backup WAN (Internet connection) from a different provider in case the main WAN goes down for some reason. SonicWALL's enhanced OS handles this easily if configured properly. This ensures connectivity not only for VoIP phones, but for all devices on the network needing Internet connectivity.

The screenshot shows the SonicWALL management interface. The left sidebar has 'Failover & Load Balancing' selected under the 'Network' section. The main content area is titled 'Settings' and includes the following configuration options:

- Enable Load Balancing
- Respond to Probes
- Current probe rate: < 1 per second, 0 total
- Any TCP-SYN to Port 0

Below the settings is the 'Groups' section, which contains a table of configured WAN interfaces:

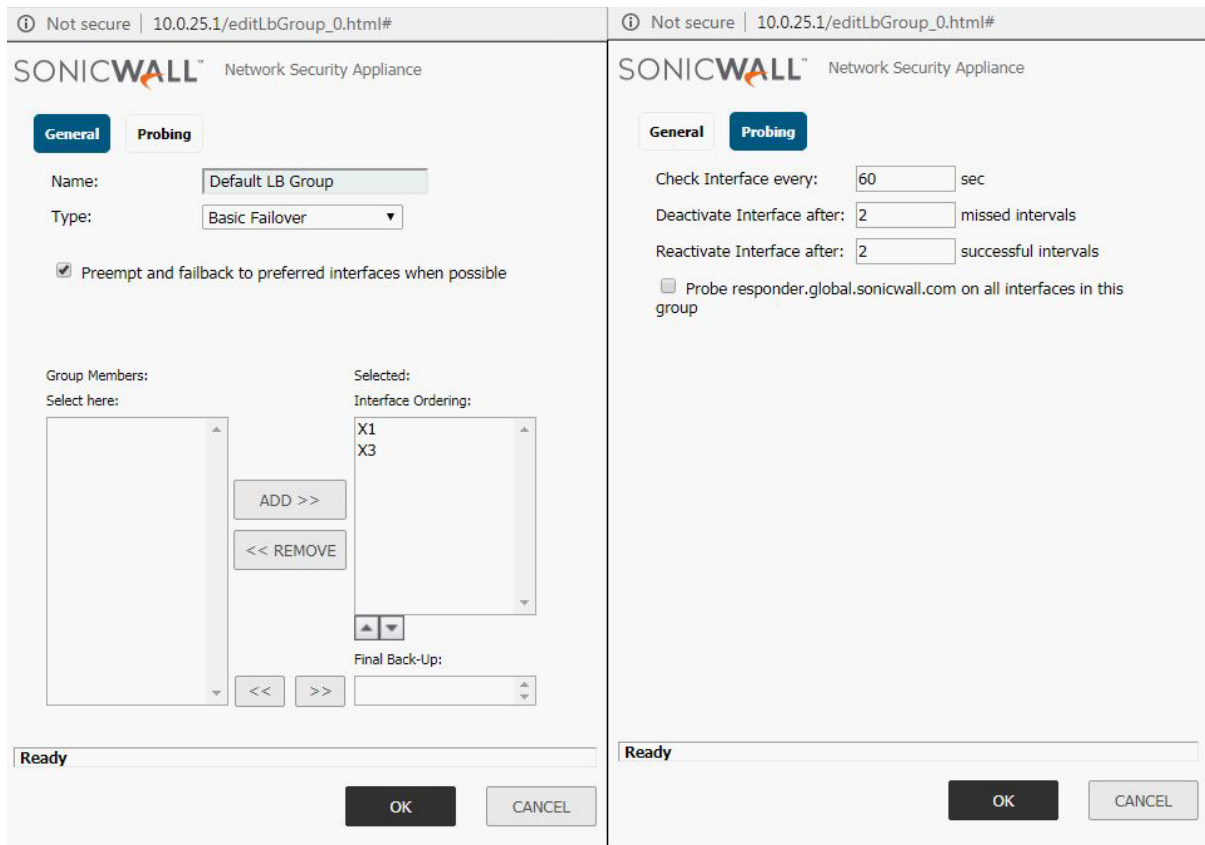
Name	Type	IP Address	Link Status	LB Status	Main Target	Alternate Target	Configure	Notes
Default LB Group	Basic Failover							
X1		99.50.204.149 (WAN)	Link Up	Available	Target Alive	Target Alive		
X3		75.80.46.130 (WAN)	Link Up	Available	Target Alive	Target Alive		

At the bottom, there is a 'Statistics' section with a dropdown menu set to 'Default LB Group' and a 'Clear' button. Below this is a table of interface statistics:

Interface	Total Connect...	New Connecti...	Current Ratio	Average Ratio	Total Unicast ...	Rx Unicast	Rx Bytes	Tx Unicast	Tx Bytes	Throughput (...)	Throughput (...)
X1	66661714	906589	98	96	1203225766567	885115278	1079458880744	478759014	123766885823	9	76
X3	40919	0	2	4	43958984908	1556040	43919039456	450127	39945452	2	18

**Located under Manage/Network/Failover & Load Balancing.** Click on the small down arrow under Groups to expand the windows. All WAN interfaces you have configured will appear there. Also, you must check the boxes "Enable Load Balancing" and "Respond to Probes". Do that first and press Accept. Now click the configure button for the Default Group.

On the General Tab, you shouldn't have to change anything if you want to use Basic Failover. That is selected under Type. The check box tells the SonicWALL to fall back to your primary WAN interface when it's up. The interface ordering should be fine if you setup your primary on X1 and your secondary on X2 or other interface (it will automatically be shown here) The probing tab is where the magic happens. First box you are telling the SonicWALL to check the WAN interfaces every X seconds. Next, you are asking it to deactivate if it misses x intervals. In this example, after 2 minutes of your primary WAN being down, the SonicWALL will automatically start routing traffic on the secondary WAN port (X2).



The Probing tab settings need to be carefully thought out. If you have a WAN connection that tends to bounce offline a lot for some reason, setting the “Check Interface” setting to a number too low will cause the SonicWALL to switch between WAN ports too often. While not a problem for web traffic, VoIP phones don’t register with their SIP server that often. Most register every 300 seconds or more. This means if you’re SonicWALL switches to the secondary WAN, the phones will be “offline” until their registration period occurs again, plus the amount of time set in the “Deactivate Interface” box. It’s recommend to use these settings to only have the SonicWALL failover if the WAN connection is really down and will be for a period of time longer than several minutes. In the example, the config is to check the WAN interfaces every 60 seconds, but only “failover” after 1 minutes of being down. Come back up after it is solid and back online for 1 minute.

Now the probes themselves need to be configured. **Click configure for each WAN interface.**

## X1 Probe Settings

- Physical Monitoring Only
- Logical/Probe Monitoring enabled

Probe succeeds when either Main Target or Alternate Target responds. ▼

	Host:	Port:
Main Target:	<input type="text" value="8.8.8.8"/>	<input type="text" value="0"/>
Alternate Target:	<input type="text" value="9.9.9.9"/>	<input type="text" value="0"/>
Default Target IP:	<input type="text" value="8.8.8.8"/>	

**Note:** An IP Address of 0.0.0.0 or a DNS resolution failure will use the Default Target IP configured.

Ready

OK

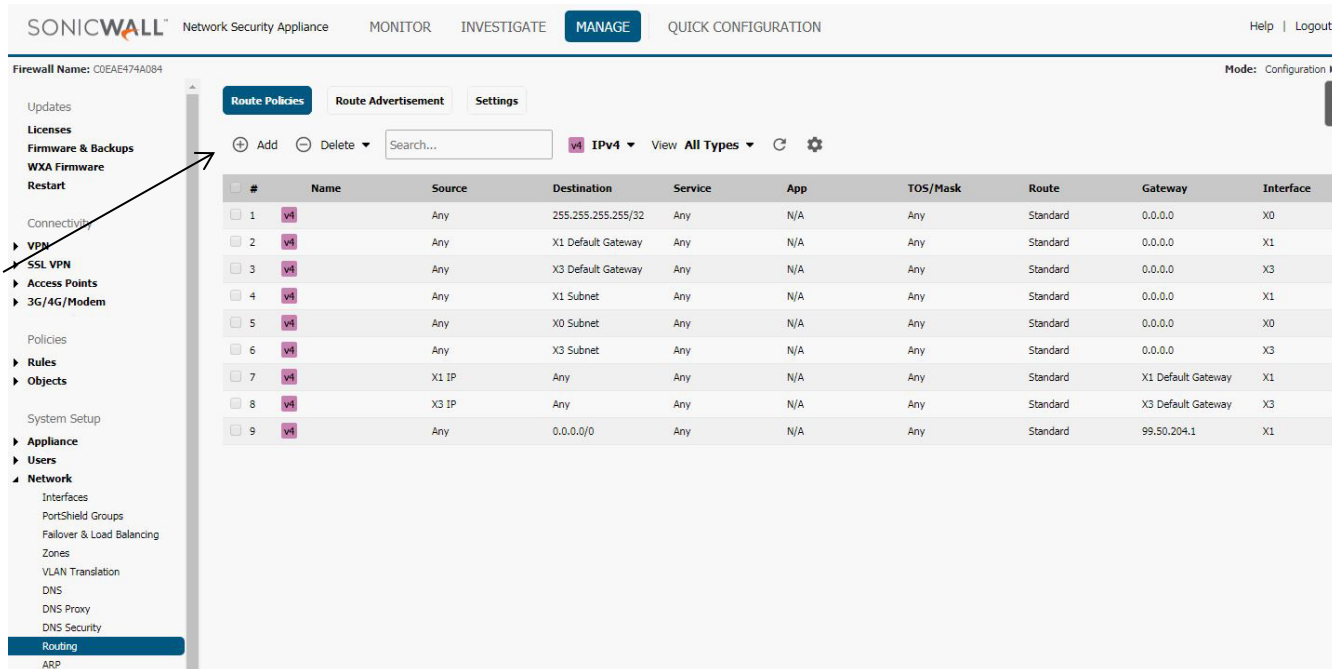
CANCEL

Select the radio button “Logical/Probe Monitoring enabled”. From the drop down, select “Probe succeeds when either Main Target or Alt Target responds. **This setting is critical!** The SonicWALL will be pinging two different targets to see if your WAN connection is up. This is the setting that instructs it to “Failover” to the secondary WAN if the probe (ping) fails. It’s strongly recommended to use Ping, and that you use host addresses from **two different** public DNS servers. This almost ensures that your probe will never be wrong about your WAN connection. For example, if you were to use the two public, Google DNS servers (8.8.8.8 and 8.8.4.4) and Google’s DNS goes down (it has), the SonicWALL would think the primary WAN is down because the ping failed. It would then be in failover mode and using the secondary WAN. Not a huge issue, but remember, the phones will be offline for 1 minute, plus the registration timeout period. So by using two different public DNS servers for your probe, the SonicWALL will only ever failover when the WAN interface is truly down. Choose Ping for both Target settings and enter your host IP addresses that will be pinged.

# Configuring SonicWALL to force phones to use secondary WAN (X2)

Here's the scenario. You have two WAN connections to two different ISP's. You have Failover on the SonicWALL in case the primary goes down. You have your QoS rule setup for VoIP phones on the network and everything is working smoothly. Suddenly, and without warning, you are told that voice calls are "choppy" and the customer is experiencing jitter. Obviously, this isn't a SonicWALL issue as you know it's worked perfectly for months. You have rebooted all phones, the LAN switch, and perhaps even the SonicWALL. Nothing locally appears to have changed and you can't find anything wrong that would suddenly be causing this. Web browsing is fine, and everything else that uses the Internet is working normally. Your first call should be to the primary WAN provider. In most cases, they will come out and test the node in your area and find an issue with overloading, or some other infrastructure issue causing major packet loss. HTTP and other protocols really don't care as the packets eventually show up, but obviously VoIP traffic can't handle this. The bad news is that it may take days or even weeks to identify and resolve the issue! You can't have VoIP phones using a connection like that for even a day. Fortunately, you have a secondary WAN connection! SonicWALL can be easily configured to route any Address object over any Gateway that you choose. This example will force all VoIP phones on the network to only use the secondary WAN connection (X2), which hopefully is operating properly. This will require some level of IP knowledge that I won't go into detail here, but it's very straightforward.

## 1. Create a Route Policy: Located under Manage/Network/Routing.



The screenshot shows the SonicWALL configuration interface. The left sidebar contains a navigation menu with categories like Updates, Licenses, Connectivity, Policies, System Setup, and Network. The 'Network' category is expanded, and 'Routing' is selected. The main content area displays the 'Route Policies' configuration page. At the top, there are tabs for 'Route Policies', 'Route Advertisement', and 'Settings'. Below the tabs, there are controls for adding, deleting, and searching policies, along with filters for 'IPv4' and 'View All Types'. A table lists the configured route policies with the following columns: #, Name, Source, Destination, Service, App, TOS/Mask, Route, Gateway, and Interface.

#	Name	Source	Destination	Service	App	TOS/Mask	Route	Gateway	Interface
1	v41	Any	255.255.255.255/32	Any	N/A	Any	Standard	0.0.0.0	X0
2	v41	Any	X1 Default Gateway	Any	N/A	Any	Standard	0.0.0.0	X1
3	v41	Any	X3 Default Gateway	Any	N/A	Any	Standard	0.0.0.0	X3
4	v41	Any	X1 Subnet	Any	N/A	Any	Standard	0.0.0.0	X1
5	v41	Any	X0 Subnet	Any	N/A	Any	Standard	0.0.0.0	X0
6	v41	Any	X3 Subnet	Any	N/A	Any	Standard	0.0.0.0	X3
7	v41	X1 IP	Any	Any	N/A	Any	Standard	X1 Default Gateway	X1
8	v41	X3 IP	Any	Any	N/A	Any	Standard	X3 Default Gateway	X3
9	v41	Any	0.0.0.0/0	Any	N/A	Any	Standard	99.50.204.1	X1

Not secure | 10.0.25.1/addPbrDlg.html

SONICWALL™ Network Security Appliance

General Advanced

### Route Policy Settings

Name: Custom route for phones

Source: Any

Destination: Any

Service
  App

Service: VOIP Phones

Standard Route
  Multi-Path Route
  SD-WAN Route

Interface: X3

Gateway: X3 Default Gateway

Metric: 1

Comment: Route phones over this \

Disable route when the interface is disconnected  
 Allow VPN path to take precedence  
 Permit Acceleration

Probe: None

Disable route when probe succeeds  
 Probe default state is UP

Ready

OK CANCEL HELP

Click Add.

Source is Any.

Destination is Any.

Service will be the Address object you just created VOIP (Phones in this example).

Interface: X3

Gateway: This is your secondary WAN (X3 Default Gateway) in this example

Metric is 1.

Comment to describe what this used for.

Check the box to "Disable route when the interface is disconnected". Think of this as backward failover. If this WAN (X3) fails, the phones will go back to using the primary WAN (X1).

You might even consider just using this WAN connection 100% of the time only for the VoIP phones as it essentially is QoS by default as it would have no other traffic to compete with (unless the primary WAN fails, then everything else on the network will use it while the primary is down), but your QoS rule would still apply and give the phones priority over everything else.