

SonicWall Diagnostic Mode and GUI v7 and GUI v6

If you have trouble on the Traffic Shaping tab of an Access Policy when trying to add Bandwidth Object from BWM Dropdown Menu, you may be in GUI v7 and need to use diagnostic mode to go back to GUI v6 to make the changes. If you are NOT on firmware 7.0.1-8080-R3248 or higher you will likely need to do this but if on firmware version 7.0.1-8080-R3248 or higher you shouldn't have the problem.

The next 3 pages show how to get into the diagnostic version of the SonicWall to turn off GUI v7 and go to GUI v6 to make the changes then go back to GUI v7.

To go back into the diagnostic mode to get back to GUI v7 you type in the local or external access IP then login then change the URL from <https://ipaddress/main.html> to <https://ipaddress/diag.html> to get to the Internal Settings so you can scroll down to select making the SonicUI7 the default management again.



How can I access the internal settings of the firewall?

🕒 11/22/2021

👍 46 People found this article helpful

👁️ 195,970 Views

Description

This article describes how to access the Internal settings of SonicWALL Firewall.

 **NOTE:** SonicWall, Inc. DISCLAIMS ALL WARRANTIES AND TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL SonicWall, Inc. BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

THE FOLLOWING FEATURES AND DIAGNOSTIC ROUTINES ARE NOT SUPPORTED BY SonicWall, Inc.. SonicWall makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Resolution for SonicOS 7.X



This release includes significant user interface changes and many new features that are different from the SonicOS 6.5 and earlier firmware. The below resolution is for customers using SonicOS 7.X firmware.

1. The Diag page can be reached by typing in the LAN IP of the SonicWall in the browser, with a `IP/sonicui/7/m/mgmt/settings/diag` at the end.

 **EXAMPLE:** `192.168.168.168/sonicui/7/m/mgmt/settings/diag`

2. Click on internal settings to access the internal settings page or diag page



Resolution for SonicOS 6.5

This release includes significant user interface changes and many new features that are different from the SonicOS 6.2 and earlier firmware. The below resolution is for customers using SonicOS 6.5 firmware.

Scroll down until you see “SonicUI7 as default management GUI”. You will turn this off then scroll back up to the top and click “Accept”

The screenshot shows the SonicWall management interface for device 18B169611AF0. The page is divided into several sections:

- Time interval between inspections of the Persistent LB Table, for marking entries as idle (seconds):** 15
- Maximum reuse threshold for each entry in the Persistent LB Table, zero means unlimited:** 0
- Source IP Address to monitor (Source-Destination IP Binding to include in TSR):** 0.0.0.0
- Destination IP Address to monitor (Source-Destination IP Binding to include in TSR):** 0.0.0.0

PPPOE SETTINGS

- Allow LCP requests to PPPOE Server:
- Log LCP Echo Requests and Replies between client and server:
- Enable PPPoE End-Of-List Tag:
- Enable IPCP address option for PPPoE Unnumbered:
- PPPOE Netmask: 255.255.255.255

MANAGEMENT SETTINGS

- Turn this off** SonicUI7 as default management GUI: Switching this option off will revert to SonicUI6 for debug only. SonicUI6 is not supported for Gen7 Appliances.
- Use New License Page Format:
- Use Standby Management SA:
- Display Firewall Name in Main Management Window:
- Allow SGMS to preempt a logged in administrator:
- Show Basic Wizard after firewall is configured:
- Online Help URL: Use Default Sonicwall...
- URL:
- Add Domain/IP to Allow List of CSP header: Add

To change back to GUI v7 scroll down the Internal Settings and click on the box for “SonicUI7 as default management GUI” then click “Accept” at the bottom.

The screenshot shows the SonicWall Network Security Appliance configuration interface. The page title is "Internal Settings - to be used only at the direction of Technical Support". A warning message states: "Warning: these settings are not documented and changing settings here could prevent proper operation of the SonicWall. Only make such changes if instructed by SonicWall technical support." The "Management Settings" section contains the following options:

- Allow management via HTTP
- SonicUI7 as default management GUI
- Use Standby Management SA
- Display Firewall Name in Main Management Window
- Allow SCMS to preempt a logged in administrator
- Use JQuery Library Version 1.6.4
- Show Basic Wizard after firewall is configured
- Show Classic View Pages

Below these options, there is a field for "Online Help URL" with the value "help.sonicwall.com/help.asp". At the bottom of the page, there are "ACCEPT" and "CANCEL" buttons. A yellow callout box with the text "Check this box" points to the "SonicUI7 as default management GUI" option.



General Router Settings and Network Tools ▾



The screenshots below are from GUI v6 so if you are on GUI v7 some of them will look different and the BWM will not be in the same place. If you went into GUI v6 above feel free to go into it for the changes below too.

Configuring your Sonicwall for Kinect

This configuration is on a Sonicwall TZ205 with 5.9.1.7-2o firmware, but should be relatively similar for all models.

Note: Sonicwall's IPS service has been known to block VoIP even if you have these rules set as it confuses it for a DDoS attack. If you lower the protection level from high, it generally fixes it.

Note: The FQDNS on this doc are for APOLLO clusters. You should follow this doc and use the server addresses your site/customer is associated with:

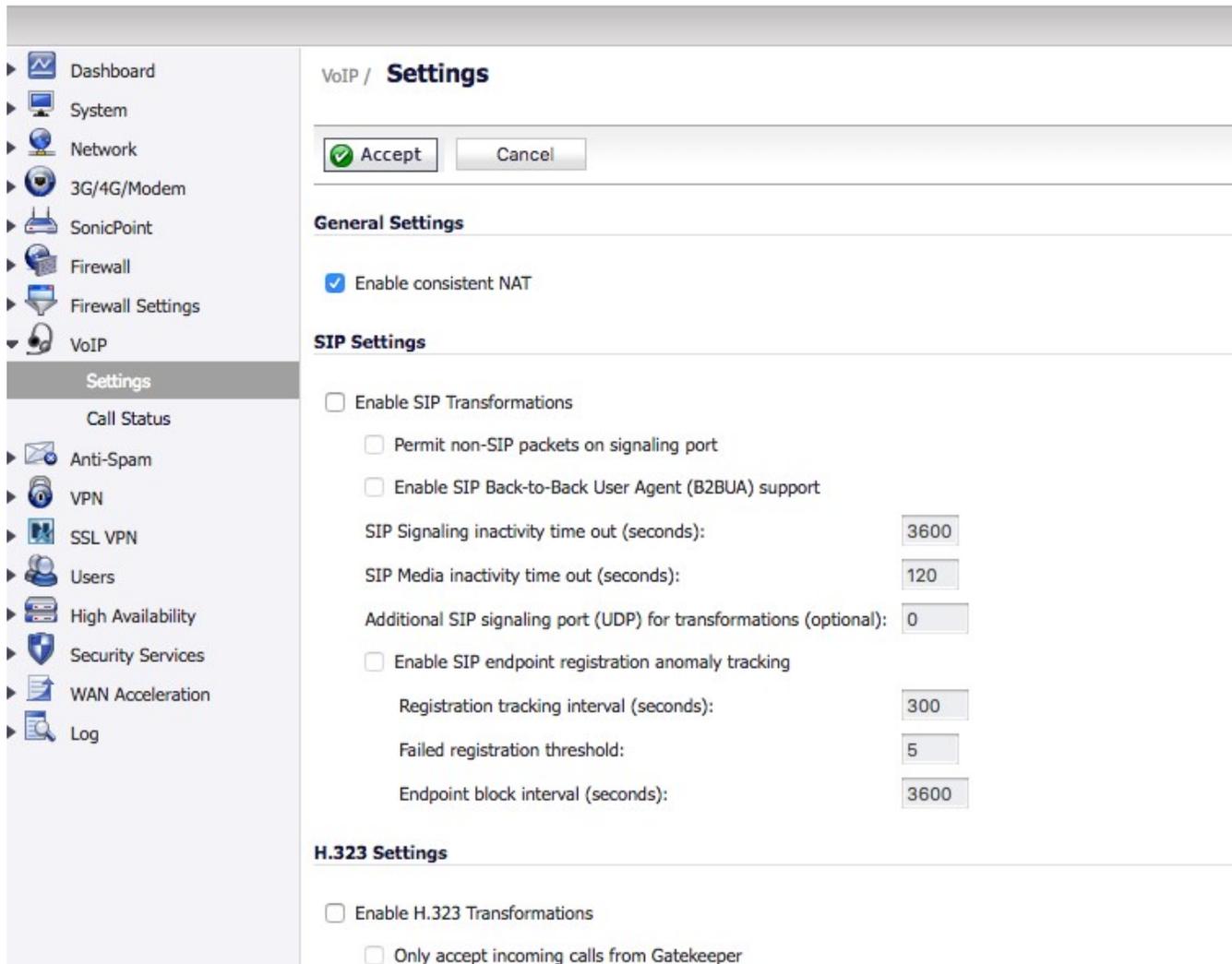
Generic Firewall Settings

We recommend the TZ series for no more than 25 phones. If you plan to expand beyond that we recommend the NSA series.

1. Consistent NAT

Ensure "Enable Consistent Nat" is checked





The screenshot shows the SonicWALL management interface for VoIP settings. On the left is a navigation menu with categories like Dashboard, System, Network, and VoIP. The 'VoIP' category is expanded to show 'Settings'. The main content area is titled 'VoIP / Settings' and features a confirmation dialog with 'Accept' and 'Cancel' buttons. Below this are three sections: 'General Settings' with a checked 'Enable consistent NAT' option; 'SIP Settings' with several unchecked options and numerical input fields for timeouts and intervals; and 'H.323 Settings' with two unchecked options.

VoIP / Settings

Accept Cancel

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):
- SIP Media inactivity time out (seconds):
- Additional SIP signaling port (UDP) for transformations (optional):
- Enable SIP endpoint registration anomaly tracking
 - Registration tracking interval (seconds):
 - Failed registration threshold:
 - Endpoint block interval (seconds):

H.323 Settings

- Enable H.323 Transformations
 - Only accept incoming calls from Gatekeeper

2. Enable WAN BWM (Bandwidth Management)

Ensure advanced is checked as seen below

Firewall Settings / **BWM**

Bandwidth Management Type: Advanced Global None

Interface BWM Settings

Priority	Enable	Guaranteed	Maximum \Burst	
0 Realtime	<input type="checkbox"/>	<input type="checkbox"/>	0 %	100 %
1 Highest	<input type="checkbox"/>	<input type="checkbox"/>	0 %	100 %
2 High	<input checked="" type="checkbox"/>	<input type="checkbox"/>	30 %	100 %
3 Medium High	<input type="checkbox"/>	<input type="checkbox"/>	0 %	100 %
4 Medium	<input checked="" type="checkbox"/>	<input type="checkbox"/>	50 %	100 %
5 Medium Low	<input type="checkbox"/>	<input type="checkbox"/>	0 %	100 %
6 Low	<input checked="" type="checkbox"/>	<input type="checkbox"/>	20 %	100 %
7 Lowest	<input type="checkbox"/>	<input type="checkbox"/>	0 %	100 %
Total:		100		

Note: This priority table is used only when global bandwidth management is selected. (When using legacy BWM, values can be set independently in Firewall Access Rules and Action Objects.)

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

3. Enable BWM on WAN

Click the configure pencil located next to your primary WAN connection

SonicWALL | Network Security Appliance Wards | Help | Logout

Mode: Configuration

Network / **Interfaces**

Interface Settings View IP Version: IPv4 IPv6

Name	Zone	Group	IP Address	Subnet Mask	IP Assignment	Status	Comment	Configure
X0	LAN		192.168.75.1	255.255.255.0	Static	1 Gbps Full Duplex	Default LAN	
X1	WAN	Default LB Group		255.255.255.248	Static	1 Gbps Full Duplex		

Add Interface: --Select Interface Type--

Display All Traffic

Interface Traffic Statistics

Name	Rx Unicast Packets	Rx Broadcast Packets	Rx Errors	Rx Bytes	Tx Unicast Packets	Tx Broadcast Packets	Tx Errors	Tx Bytes
X0	51,915	2,969	0	10,276,559	66,940	50	0	63,417,330
X1	89,260	338	0	63,219,164	67,135	45	0	10,160,534

Under the bandwidth management section, check both enable Egress and Ingress. Egress is the upload speed of your internet connection. Ingress is the download speed. Best practice is to run a speed test before setting these options.

The example below shows a 100MBPS download and 35MBPS upload speed connection.

Edit Interface - X1

Not Secure | https://192.168.75.1/editInterface_1.html#

SonicWALL | Network Security Appliance

General Advanced

Advanced Settings

Link Speed: Auto Negotiate

Use Default MAC Address: C0:EA:E4:79:09:15

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

Suppress ICMP Fragmentation Needed message generation

Bandwidth Management

Enable Interface Egress Bandwidth Limitation

Maximum Interface Egress Bandwidth (kbps): 35000.000000

Enable Interface Ingress Bandwidth Limitation

Maximum Interface Ingress Bandwidth (kbps): 100000.000000

Ready

OK Cancel Help

4. Create LAN>Wan firewall rule to allow and prioritize all traffic to both Kinect Servers

The screenshot shows the SonicWALL configuration interface for Access Rules. The 'View Style' is set to 'Matrix'. The matrix shows traffic from LAN to WAN, with a red arrow indicating the direction of traffic.

FROM	TO
LAN	WAN
WAN	VPN
VPN	SSLVPN
SSLVPN	

The screenshot shows the SonicWALL configuration interface for Access Rules in table view. The 'View Style' is set to 'Matrix' and 'View IP Version' is set to 'IPv4 Only'. Two rules are listed, and a red arrow points to the 'Add...' button.

#	From	To	Priority	Source	Destination	Service	Action	Users Incl.	Users Excl.	Packet Monitor
1	LAN	WAN	1	Any	Syntel NJ	Any	Allow	All	None	
2	LAN	WAN	2	Any	Any	Any	Allow	All	None	

You are going to create a rule that allows all traffic to our server as seen in the screen shots below. Under the destination submenu click "create new network" to add our servers. You will build this rule three times, two using our NJ servers FQDN of core2-nj.syntelsolutions.com & core-nj.syntelsolutions.com, and the third rule will use our FL server of core-fl.syntelsolutions.com

Add Rule▲ Not Secure | <https://192.168.75.1/addRuleDlg.html?objTypes=3647>



GeneralAdvancedQoSBWM

Settings

Action: Allow Deny Discard

From :

To :

Source Port:

Service:

Source:

Destination:

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

Users Excluded: ... these users will be denied.

Schedule:

Comment:

Enable Logging

Allow Fragmented Packets

Enable packet monitor

Enable Management

Ready

Add Close Help

The screenshot shows the SonicWall configuration interface. At the top, there is a browser window titled "Add Rule" with a "Not Secure" warning and the URL <https://192.168.75.1/addRuleDlg.html?objTypes=3647>. Below the browser window, the SonicWALL logo and "Network Security Appliance" are visible. The interface has four tabs: "General", "Advanced", "QoS", and "BWM". The "General" tab is selected.

Under the "Settings" section, the following options are visible:

- Action: Allow Deny Discard
- From : LAN
- To : WAN
- Source Port: Any
- Service: Any
- Source: Any
- Destination: --Select a ne...
- Users Included: All
- Users Excluded: None
- Schedule: Always on
- Comment:
- Enable Logging
- Allow Fragmented Packets
- Enable packet monitor
- Enable Management

An "Add Address Object" dialog box is open in the foreground. It has a "Not Secure" warning and the URL <https://192.168.75.1/addNetObj...>. The dialog contains the following fields:

- Name: Syntel Solutions
- Zone Assignment: WAN
- Type: FQDN
- FQDN Hostname: core-nj.syntelsolutions.com

At the bottom of the dialog, there is a "Ready" status bar and "OK" and "Cancel" buttons.

Below the dialog, there is a "Ready" status bar and "Add", "Close", and "Help" buttons.

Then under the QOS tab, change DSCP to "Explicit"

General

Advanced

QoS

BWM

DSCP Marking SettingsDSCP Marking Action: Explicit DSCP Value:

Under the BWM tab, check enable Egress and ingress, under the drop down you will create a new bandwidth object. You will use this for both inbound and outbound firewall rules as you will see later. The best rule of thumb is to guarantee about 25% of the bandwidth to the phones, and to allow 100% if needed. This way phone calls always will have priority, but not use the entire connection when not in use.



General

Advanced

QoS

BWM

Bandwidth Management Enable Egress Bandwidth Management ('Allow' rules only)Bandwidth Object: Enable Ingress Bandwidth Management ('Allow' rules only)Bandwidth Object: Enable Tracking Bandwidth Usage**Note:** BWM Type: Advanced; To change go to Firewall Settings > BWM



General

Elemental

Bandwidth Object Settings

Name:

Guaranteed Bandwidth: Mbps

Maximum Bandwidth: Mbps

Traffic Priority:

Violation Action:

Comment:

Ready

OK

Cancel

Help



General

Elemental

Bandwidth Object Settings

Name:

Guaranteed Bandwidth: Mbps

Maximum Bandwidth: Mbps

Traffic Priority:

Violation Action:

Comment:

Ready

OK

Cancel

Help



Bandwidth Management

Enable Egress Bandwidth Management ('Allow' rules only)

Bandwidth Object: 

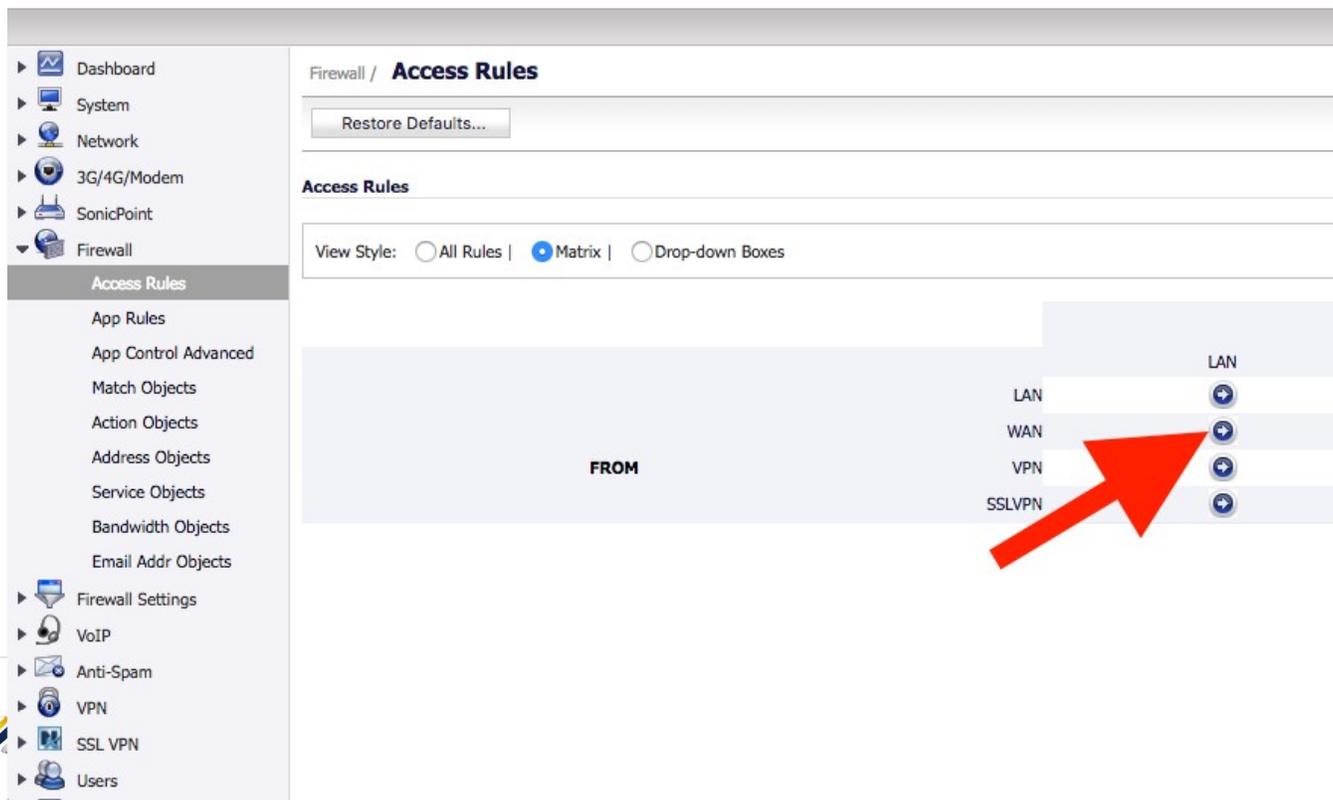
Enable Ingress Bandwidth Management ('Allow' rules only)

Bandwidth Object: 

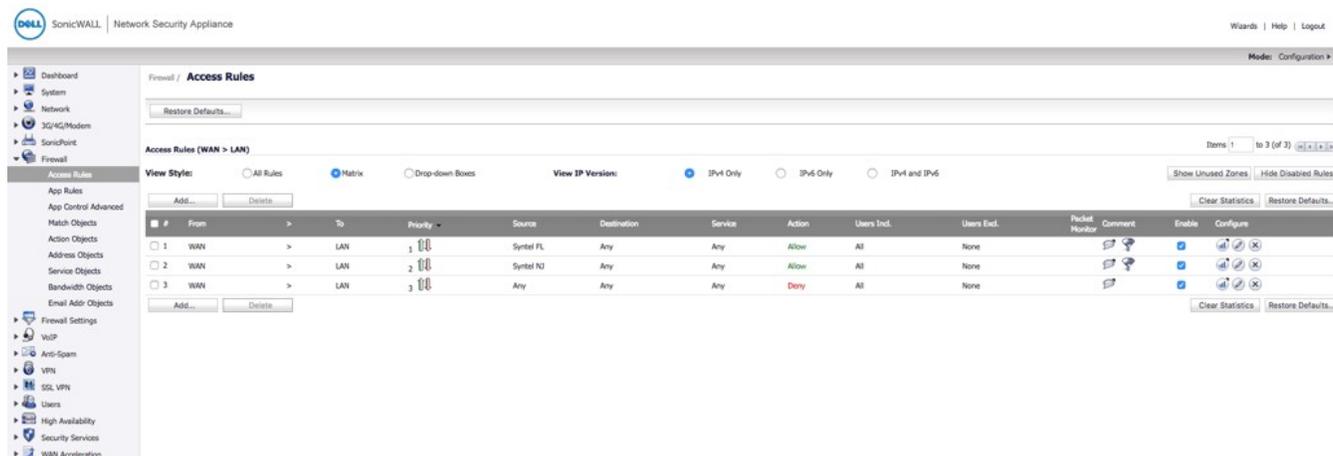
Enable Tracking Bandwidth Usage

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

5. Now we go back to access rules, to create a similar rule from WAN>LAN



Here you will build similar rules to LAN>WAN, the only difference being we will be changing the "Source" to the Kinect Servers, and the other options to "any". Therefore creating a rule saying all traffic ONLY from our servers, is allowed and prioritized.



Be sure to set the QOS and BWM tabs the same as the previous rules

Congrats! You've successfully configured your firewall for the Syntel Solutions UCaas Platform.

Download the PDF

SonicWallApolloGuide

Was this article helpful?

Related articles

[SIP ALG Detector](#)

[Check your Bandwidth Speed](#)

[Popular Overrides](#)

[Disable SIP ALG on Fortigate Firewalls](#)

[Disabling SIP ALG on Kinect Router/Modem](#)