

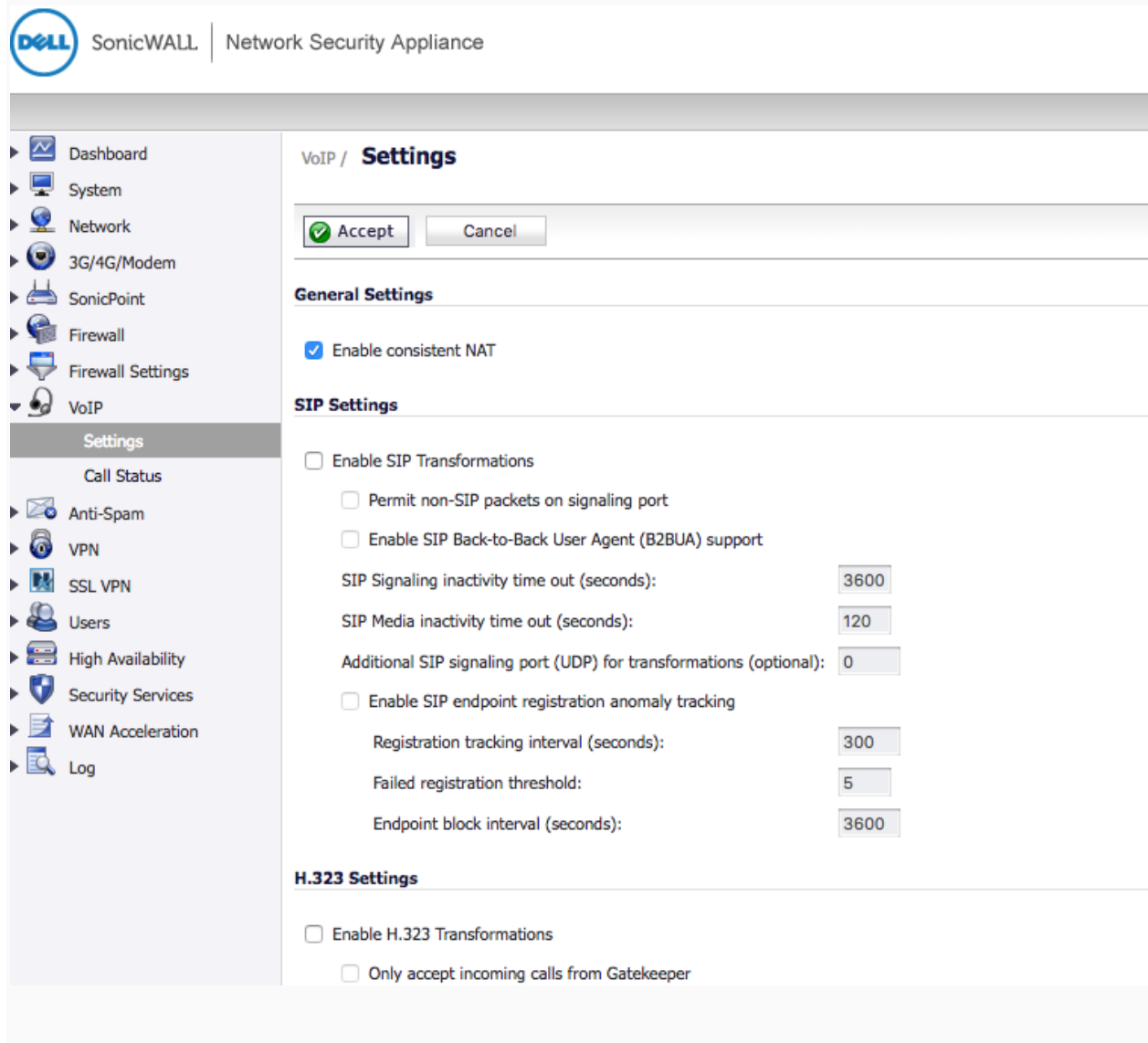
This configuration is on a Sonicwall TZ205 with 5.9.1.7-2o firmware, but should be relatively similar for all models.

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.

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. The top left features the Dell SonicWALL logo and the text 'Network Security Appliance'. A navigation sidebar on the left lists various system settings, with 'VoIP' selected and expanded to show 'Settings'. The main content area is titled 'VoIP / Settings' and includes 'Accept' and 'Cancel' buttons. Under 'General Settings', the checkbox for 'Enable consistent NAT' is checked. The 'SIP Settings' section contains several options and input fields: 'Enable SIP Transformations' (unchecked), 'Permit non-SIP packets on signaling port' (unchecked), 'Enable SIP Back-to-Back User Agent (B2BUA) support' (unchecked), 'SIP Signaling inactivity time out (seconds):' (3600), 'SIP Media inactivity time out (seconds):' (120), 'Additional SIP signaling port (UDP) for transformations (optional):' (0), 'Enable SIP endpoint registration anomaly tracking' (unchecked), 'Registration tracking interval (seconds):' (300), 'Failed registration threshold:' (5), and 'Endpoint block interval (seconds):' (3600). The 'H.323 Settings' section at the bottom has 'Enable H.323 Transformations' (unchecked) and 'Only accept incoming calls from Gatekeeper' (unchecked).

2. Enable WAN BWM (Bandwidth Management)

Ensure advanced is checked as seen below

 SonicWALL | Network Security Appliance

Dashboard
System
Network
3G/4G/Modem
SonicPoint
Firewall
Firewall Settings
Advanced
BWM
Flood Protection
Multicast
SSL Control
VoIP
Anti-Spam
VPN
SSL VPN
Users
High Availability
Security Services
WAN Acceleration
Log

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 checked="" type="checkbox"/>	30 %	100 %
3 Medium High	<input type="checkbox"/>	<input type="checkbox"/>	0 %	100 %
4 Medium	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	50 %	100 %
5 Medium Low	<input type="checkbox"/>	<input type="checkbox"/>	0 %	100 %
6 Low	<input checked="" type="checkbox"/>	<input checked="" 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

The screenshot shows the SonicWALL Network Security Appliance configuration page. The left sidebar contains navigation options like Dashboard, System, Network, and various services. The main area is titled 'Interfaces' and shows a table of interface settings. The X1 interface is highlighted, and a red arrow points to the 'Configure' icon in the 'Configure' column.

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		

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.

The screenshot shows the 'Edit Interface - X1' configuration page. The 'Advanced Settings' section includes options for Link Speed (Auto Negotiate), MAC Address (CO:EA:E4:79:09:15), and Interface MTU (1500). The 'Bandwidth Management' section has 'Enable Interface Egress Bandwidth Limitation' and 'Enable Interface Ingress Bandwidth Limitation' checked. The Egress bandwidth is set to 35000.000000 kbps and the Ingress bandwidth is set to 100000.000000 kbps. The status is 'Ready'.

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

The screenshot shows the SonicWALL configuration interface for Access Rules. The 'View Style' is set to 'Matrix'. A red arrow points from the 'LAN' column under the 'FROM' section to the 'WAN' column under the 'TO' section. The 'TO' section also includes 'VPN' and 'SSLVPN' columns.


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'. A red arrow points to the 'Add...' button below the table.

#	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 twice, one using our NJ servers FQDN of core-nj.syntelsolutions.com and the second rule will use our FL server of core-fl.syntelsolutions.com

Add Rule

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

 SonicWALL | Network Security Appliance

General Advanced QoS BWM

Settings

Action: Allow Deny Discard

From : LAN

To : WAN

Source Port: Any

Service: Any

Source: Any

Destination: --Select a network--

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

Users Excluded: None *... these users will be denied.*

Schedule: Always on

Comment:

Enable Logging

Allow Fragmented Packets

Enable packet monitor

Enable Management

Ready

Add Close Help

Add Rule

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

SonicWALL | Network Security Appliance

General Advanced QoS BWM

Settings

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

Ready

Add Close Help

Add Address Object

Not Secure | <https://192.168.75.1/addNetObj...>

SonicWALL | Network Security Appliance

Name: Syntel Solutions

Zone Assignment: WAN

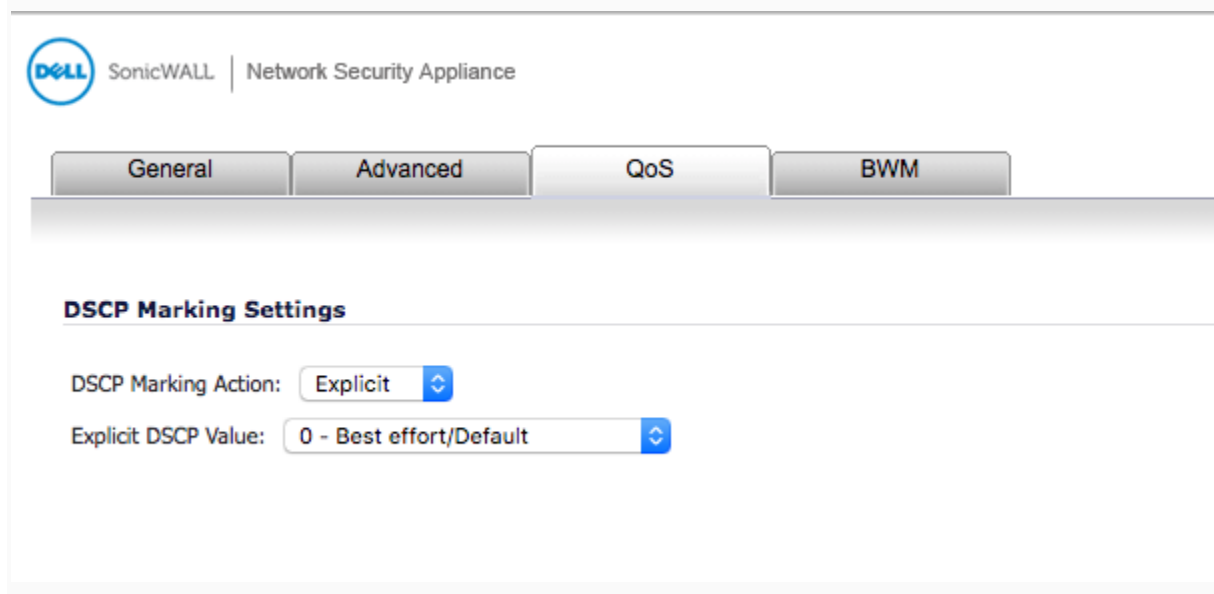
Type: FQDN

FQDN Hostname: core-nj.syntelsolutions.com

Ready

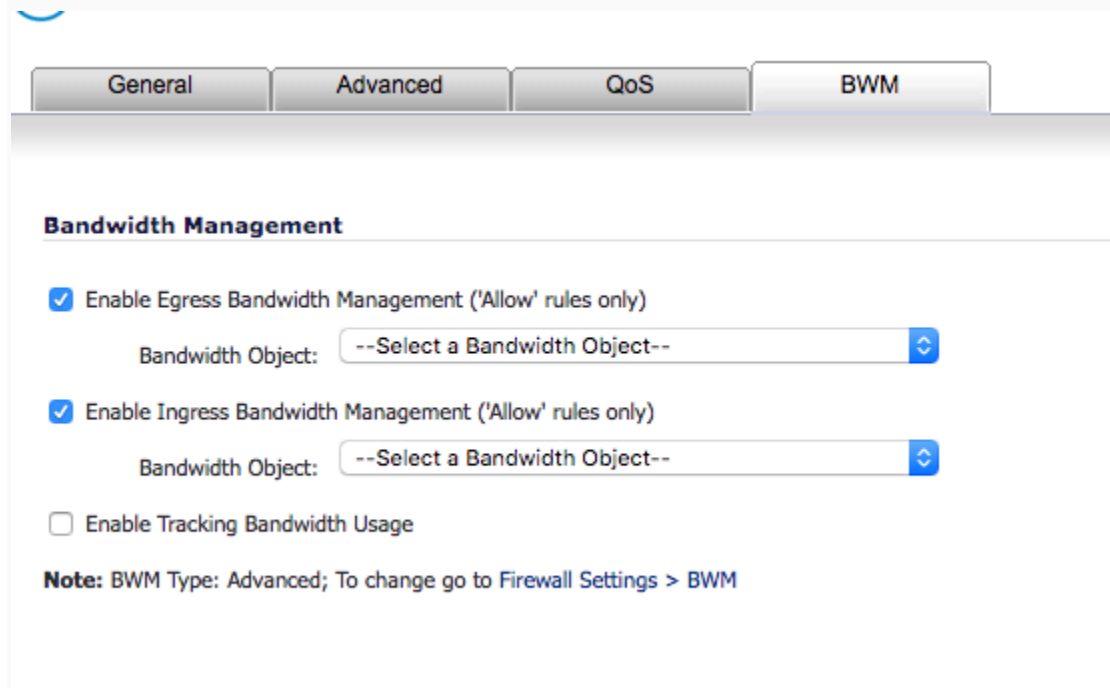
OK Cancel

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



The screenshot shows the SonicWALL Network Security Appliance interface. At the top left is the Dell logo and the text "SonicWALL | Network Security Appliance". Below this are four tabs: "General", "Advanced", "QoS", and "BWM". The "QoS" tab is selected and highlighted. Underneath the tabs is the "DSCP Marking Settings" section. It contains two dropdown menus: "DSCP Marking Action:" set to "Explicit" and "Explicit DSCP Value:" set to "0 - Best effort/Default".

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.



The screenshot shows the SonicWALL Network Security Appliance interface with the "BWM" tab selected. The section is titled "Bandwidth Management". It contains three checkboxes: "Enable Egress Bandwidth Management ('Allow' rules only)" which is checked, "Enable Ingress Bandwidth Management ('Allow' rules only)" which is checked, and "Enable Tracking Bandwidth Usage" which is unchecked. Below each checked checkbox is a "Bandwidth Object:" dropdown menu, both currently showing "--Select a Bandwidth Object--". At the bottom, there is a note: "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



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](#)

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

DELL SonicWALL | Network Security Appliance

Dashboard / System / Network / 3G/4G/Modem / SonicPoint / Firewall

Access Rules

- App Rules
- App Control Advanced
- Match Objects
- Action Objects
- Address Objects
- Service Objects
- Bandwidth Objects
- Email Addr Objects

Firewall Settings / VoIP / Anti-Spam / VPN / SSL VPN / Users

Firewall / **Access Rules**

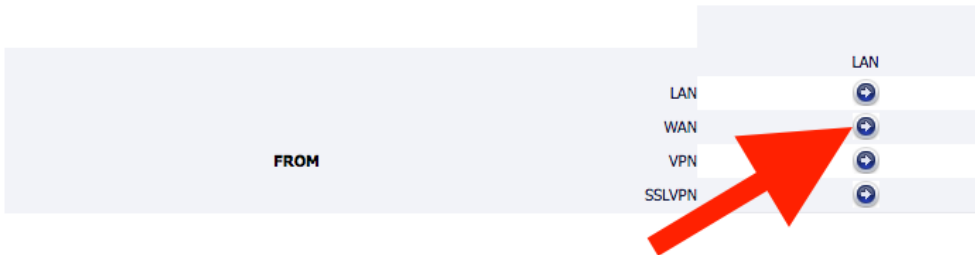
Restore Defaults...

Access Rules

View Style: All Rules | Matrix | Drop-down Boxes

FROM

- LAN
- WAN
- VPN
- SSLVPN



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

DELL SonicWALL | Network Security Appliance

Wizards | Help | Logout

Mode: Configuration

Dashboard / System / Network / 3G/4G/Modem / SonicPoint / Firewall

Access Rules

Restore Defaults...

Access Rules (WAN > LAN)

View Style: All Rules | Matrix | Drop-down Boxes

View IP Version: IPv4 Only | IPv6 Only | IP-v4 and IPv6

Items 1 to 3 (of 3)

Show Unused Zones | Hide Disabled Rules

Add... Delete

#	From	To	Priority	Source	Destination	Service	Action	Users Incl.	Users Excl.	Packet Monitor	Comment	Enable	Configure
1	WAN	>	LAN	1	Syntel FL	Any	Any	Allow	All	None		<input checked="" type="checkbox"/>	
2	WAN	>	LAN	2	Syntel NG	Any	Any	Allow	All	None		<input checked="" type="checkbox"/>	
3	WAN	>	LAN	3	Any	Any	Any	Deny	All	None		<input checked="" type="checkbox"/>	

Add... Delete

Clear Statistics | Restore Defaults

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.