



SonicWALL SonicOS Enhanced Sample Configuration

While many differing network configurations are possible, this document assumes a basic environment with one internal LAN network, containing the IP phones and one WAN network connected to the Internet. While we strongly recommend a dedicated network for VoIP traffic, the instructions below can be used for a “converged” network whereby both VoIP and non-VoIP traffic share one physical WAN network. With basic modification (such as adding access rules for additional interfaces), this configuration can be extrapolated for other network layouts.

The screenshots below may vary slightly from what is displayed while configuring the device, depending on model (i.e. NSA vs. Pro) and SonicOS Enhanced software version. Setting values not mentioned may be left at default or changed as required for specific purposes.

For more detailed information, please refer to the SonicWALL document entitled [“Configuring VoIP for SonicOS Enhanced”](#), available on the SonicWALL website.

Please refer to the WorldSmart hardware list to confirm the SonicOS Enhanced version in-use is supported.



- Configure Bandwidth on the WAN interface (Network->Interfaces->WAN->Configure->Advanced):
 - Fragment non-VPN outbound packets larger than this Interface's MTU: checked/on
 - Ignore Don't Fragment (DF) bit: not checked/off
 - Do not send ICMP Fragmentation Needed for outbound packets of the Interface MTU: not checked/off
 - Enable Egress Bandwidth Management: checked/on
 - Available Interface Egress Bandwidth (Kbps): <as appropriate>
 - Enable Ingress Bandwidth Management: checked/on
 - Available Interface Ingress Bandwidth (Kbps): <as appropriate>

The screenshot displays the configuration page for a WAN interface, divided into two tabs: "General" and "Advanced". The "Advanced" tab is selected, showing the following settings:

Advanced Settings

- Link Speed: Auto Negotiate (dropdown menu)
- Use Default MAC Address: (selected) with value 00:06:B1:0 :A :0
- Override Default MAC Address: (not selected)
- Enable Multicast Support: (not selected)
- Enable 802.1p tagging: (not selected)
- Interface MTU: 1500 (text input)
- Fragment non-VPN outbound packets larger than this Interface's MTU: (checked)
- Ignore Don't Fragment (DF) Bit: (not checked)
- Do not send ICMP Fragmentation Needed for outbound packets over the Interface MTU: (not checked)

Bandwidth Management

- Enable Egress Bandwidth Management: (checked)
 - Available Interface Egress Bandwidth (Kbps): 384.000000 (text input)
- Enable Ingress Bandwidth Management: (checked)
 - Available Interface Ingress Bandwidth (Kbps): 384.000000 (text input)



- General VoIP Settings (VoIP->Settings):
 - Enabled consistent NAT: checked/on
 - Enable SIP Transformations: checked/on
 - Permit non-SIP packets on signaling port: not checked/off
 - Enabled SIP Back-to-Back User Agent (B2BUA) support: not checked/off
 - SIP Signaling inactivity time out (seconds): 3600
 - SIP Media inactivity time out (seconds): 240
 - Additional SIP signaling port (UDP) for transformations (optional): 0

A screenshot of a web-based configuration interface for VoIP settings. The page has a dark blue header with the text "VoIP > Settings". Below the header, there are two main sections: "General Settings" and "SIP Settings". In the "General Settings" section, there is a checkbox labeled "Enable consistent NAT" which is checked. In the "SIP Settings" section, there are three checkboxes: "Enable SIP Transformations" (checked), "Permit non-SIP packets on signaling port" (unchecked), and "Enable SIP Back-to-Back User Agent (B2BUA) support" (unchecked). Below these checkboxes are three input fields: "SIP Signaling inactivity time out (seconds):" with the value "3600", "SIP Media inactivity time out (seconds):" with the value "240", and "Additional SIP signaling port (UDP) for transformations (optional):" with the value "0".

Note: By enabling “SIP Transformations”, RTP streams are bound to the SIP control channel. Bandwidth management policies for the ‘SIP’ service will also apply to RTP/RTCP traffic that is dynamically negotiated.



For access rules, be sure to add a rule in both directions for the networks/interfaces that the VoIP traffic should traverse (i.e. WAN->LAN and LAN->WAN) with otherwise identical values. In a simple network with one WAN network and one LAN network, two rules would be added, one for each direction of traffic flow.

- VoIP Access Rules (Firewall->Access Rules->Add->General) :
 - Action: Allow
 - From Zone: <As appropriate, i.e. WAN>
 - To Zone: <As appropriate, i.e. LAN>
 - Service: SIP
 - Source: Any
 - Destination: Any
 - Users Allowed: All
 - Schedule: Always on
 - Comment: SIP Traffic
 - Enabled Logging: (optional)
 - Allow Fragmented Packets: checked/on

A screenshot of the "Settings" dialog box for adding a VoIP Access Rule. The dialog has four tabs: "General", "Advanced", "QoS", and "Ethernet BWM", with "General" selected. The "Settings" section contains the following fields:

- Action: Radio buttons for "Allow" (selected), "Deny", and "Discard".
- From Zone: Dropdown menu set to "WAN".
- To Zone: Dropdown menu set to "LAN".
- Service: Dropdown menu set to "SIP".
- Source: Dropdown menu set to "Any".
- Destination: Dropdown menu set to "Any".
- Users Allowed: Dropdown menu set to "All".
- Schedule: Dropdown menu set to "Always on".
- Comment: Text input field containing "SIP traffic".
- Enable Logging: Checked checkbox.
- Allow Fragmented Packets: Checked checkbox.

At the bottom, there is a status bar showing "Ready" and three buttons: "OK", "Cancel", and "Help".



- Advanced:
 - TCP Connection Inactivity Timeout (seconds): 15
 - UDP Connection Inactivity Timeout (seconds): 180
 - Number of connections allowed (% of maximum connections): 100

A screenshot of a software configuration window titled "Advanced Settings". The window has a dark blue header bar with four tabs: "General", "Advanced", "QoS", and "Ethernet BWM". The "Advanced" tab is selected. The main area is light blue and contains three settings, each with a text label and a numeric input field:

- "TCP Connection Inactivity Timeout (minutes):" with a value of "15".
- "UDP Connection Inactivity Timeout (seconds):" with a value of "180".
- "Number of connections allowed (% of maximum connections):" with a value of "100".

At the bottom left, there is a status bar that says "Ready". At the bottom right, there are three buttons: "OK", "Cancel", and "Help".



- Ethernet BWM:
 - Enable Outbound Bandwidth Management ('allow' rules only): checked/on
 - Guaranteed Bandwidth: 50.000 %
 - Maximum Bandwidth: 90.000 %
 - Bandwidth Priority: 0 highest
 - Enable Inbound Bandwidth Management ('allow' rules only): checked/on
 - Guaranteed Bandwidth: 50.000 %
 - Maximum Bandwidth: 90.000 %
 - Bandwidth Priority: 0 highest
 - Enable Tracking Bandwidth Usage: (optional)

A screenshot of a software configuration window titled "Ethernet BWM". The window has a dark blue header with four tabs: "General", "Advanced", "QoS", and "Ethernet BWM". The "Ethernet BWM" tab is selected. Below the tabs, the title "Ethernet Bandwidth Management" is displayed. The configuration area contains three sections, each with a checked checkbox and a label: "Enable Outbound Bandwidth Management ('allow' rules only)", "Enable Inbound Bandwidth Management ('allow' rules only)", and "Enable Tracking Bandwidth Usage". Each of the first two sections has three sub-parameters: "Guaranteed Bandwidth" (set to 50.000 %), "Maximum Bandwidth" (set to 90.000 %), and "Bandwidth Priority" (set to 0 highest). At the bottom of the window, there is a status bar showing "Ready" and three buttons: "OK", "Cancel", and "Help".