

Configuring VoIP for SonicOS Standard

VoIP menu

Select VoIP ⇒ Settings

1. Enable Consistent NAT
2. Disable SIP Transformations
3. Disable H.323 Transformations if not using.

SonicWALL Network Security Appliance

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): 1800
- SIP Media inactivity time out (seconds): 120
- Additional SIP signaling port (UDP) for transformations (optional): 5061
- Enable SIP endpoint registration anomaly tracking
- Registration tracking interval (seconds): 300
- Failed registration threshold: 5
- Endpoint block interval (seconds): 3600

H.323 Settings

- Enable H.323 Transformations
 - Only accept incoming calls from Gatekeeper
- H.323 Signaling/Media inactivity time out (seconds): 300
- Default WAN/DMZ Gatekeeper IP Address: 0.0.0.0

Firewall Settings menu

Select Firewall Settings ⇒ UDP Settings

- UDP connection Timeout= 300

Select Firewall Settings ⇒ Flood Protection

- Disable UDP Flood Protection



SonicWALL | Network Security Appliance

The screenshot displays the SonicWALL management console interface. On the left is a navigation menu with categories like Dashboard, System, Network, and Firewall. The 'Firewall Settings' section is expanded, showing sub-options: Advanced, BWM, Flood Protection (highlighted), Multicast, QoS Mapping, and SSL Control. The main content area is divided into several sections:

- Attack threshold (incomplete connection attempts / second):** 300
- SYN-Proxy options:**
 - All LAN/DMZ servers support the TCP SACK option
 - Limit MSS sent to WAN clients (when connections are proxied)
 - Maximum TCP MSS sent to WAN clients: 1460
 - Always log SYN packets received
- Layer 2 SYN/RST/FIN/TCP Flood Protection - MAC Blacklisting**
 - Threshold for SYN/RST/FIN/TCP flood blacklisting (Packets / Sec): 1000
 - Enable SYN/RST/FIN/TCP flood blacklisting on all interfaces
 - Never blacklist WAN machines
 - Always allow DELL SonicWALL management traffic
- UDP Settings**
 - Default UDP Connection Timeout (seconds): 300
- UDP Flood Protection**
 - Enable UDP Flood Protection
 - UDP Flood Attack Threshold (UDP Packets / Sec): 1000
 - UDP Flood Attack Blocking Time (Sec): 2
 - UDP Flood Attack Protected Destination List: Any
- ICMP Flood Protection**
 - Enable ICMP Flood Protection
 - ICMP Flood Attack Threshold (ICMP Packets / Sec): 200
 - ICMP Flood Attack Blocking Time (Sec): 2
 - ICMP Flood Attack Protected Destination List: Any
- Traffic Statistics**