Configuring VoIP for SonicOS Enhanced

Document Scope

This solutions document describes how to deploy and manage SonicWALL's integrated VoIP security features to enable the secure deployment of VoIP communications in a variety of network environments.

This document contains the following sections:

VoIP Overview

This section provides an overview of VoIP. It contains the following sections:

What is VoIP?

Voice over IP (VoIP) is an umbrella term for a set of technologies that allow voice traffic to be carried over Internet Protocol (IP) networks. VoIP transfers the voice streams of audio calls into data packets as opposed to traditional, analog circuit-switched voice communications used by the public switched telephone network (PSTN).

VoIP is the major driving force behind the convergence of networking and telecommunications by combining voice telephony and data into a single integrated IP network system. VoIP is all about saving cost for companies through eliminating costly redundant infrastructures and telecommunication usage charges while also delivering enhanced management features and calling services features.

VoIP Security

Companies implementing VoIP technologies in an effort to cut communication costs and extend corporate voice services to a distributed workforce face security risks associated with the convergence of voice and data networks. VoIP security and network integrity are an essential part of any VoIP deployment.

The same security threats that plague data networks today are inherited by VoIP but the addition of VoIP as an application on the network makes those threats even more dangerous. By adding VoIP components to your network, you're also adding new security requirements.

VoIP encompasses a number of complex standards that leave the door open for bugs and vulnerabilities within the software implementation. The same types of bugs and vulnerabilities that hamper every operating system and application available today also apply to VoIP equipment. Many of today's VoIP call servers and gateway devices are built on vulnerable Windows and Linux operating systems.

Firewall Requirements for VoIP

VoIP is more complicated than standard TCP/UDP-based applications. Because of the complexities of VoIP signaling and protocols, as well as inconsistencies that are introduced when a firewall modifies source address and source port information with Network Address Translation (NAT), it is difficult for VoIP to effectively traverse a standard firewall. Here are a few of the reasons why.

- **VoIP operates using two separate protocols** - A signaling protocol (between the client and VoIP Server) and a media protocol (between the clients). Port/IP address pairs used by the media protocols (RTP/RTCP) for each session are negotiated dynamically by the signaling protocols. Firewalls need to dynamically track and maintain this information, securely opening selected ports for the sessions and closing them at the appropriate time.
- **Multiple media ports are dynamically negotiated through the signaling session** - negotiations of the media ports are contained in the payload of the signaling protocols (IP address and port information). Firewalls need to perform deep packet inspection on each packet to acquire the information and dynamically maintain the sessions, thus demanding extra firewall processing.
- **Source and destination IP addresses are embedded within the VoIP signaling packets** - A firewall supporting NAT translates IP addresses and ports at the IP header level for packets. Fully symmetric NAT firewalls adjust their NAT bindings frequently, and may arbitrarily close the pinholes that allow inbound packets to pass into the network they protect, eliminating the service provider's ability to send inbound calls to the customer. To effectively support VoIP it is necessary for a NAT firewall to perform deep packet inspection and transformation of embedded IP addresses and port information as the packets traverse the firewall.
- **Firewalls need to process the signaling protocol suites consisting of different message formats used by different VoIP systems** - Just because two vendors use the same protocol suite does not necessarily mean they will interoperate.

To overcome many of the hurdles introduced by the complexities of VoIP and NAT, vendors are offering Session Border Controllers (SBCs). An SBC sits on the Internet side of a firewall and attempts to control the border of a VoIP network by terminating and re-originating all VoIP media and signalling traffic. In essence, SBCs act as a proxy for VoIP traffic for non-VoIP enabled firewalls. SonicWALL security appliances are VoIP enabled firewalls that eliminate the need for an SBC on your network.

VoIP Protocols

VoIP technologies are built on two primary protocols, H.323 and SIP.

H.323

H.323 is a standard developed by the International Telecommunications Union (ITU). It’s a comprehensive suite of protocols for voice, video, and data communications between computers, terminals, network devices, and network services. H.323 is designed to enable users to make point-to-point multimedia phone calls over connectionless packet-switching networks such as private IP networks and the Internet. H.323 is widely supported by manufacturers of video conferencing equipment, VoIP equipment and Internet telephony software and devices.

H.323 uses a combination of TCP and UDP for signaling and ASN.1 for message encoding. H.323v1 was released in 1996 and H.323v5 was released in 2003. As the older standard, H.323 was embraced by many early VoIP players.

An H.323 network consists of four different types of entities:

- **Terminals** - Client end points for multimedia communications. An example would be an H.323 enabled Internet phone or PC.
- **Gatekeepers** - Performs services for call setup and tear down, and registering H.323 terminals for communications. Includes:
  - Address translation.
  - Registration, admission control, and status (RAS).
  - Internet Locator Service (ILS) also falls into this category (although it is not part of H.323). ILS uses LDAP (Lightweight Directory Access Protocol) rather than H.323 messages.
- **Multipoint control units (MCUs)** - Conference control and data distribution for multipoint communications between terminals.
- **Gateways** - Interoperation between H.323 networks and other communications services, such as the circuit-switched Packet Switched Telephone Network (PSTN).

SIP

The Session Initiation Protocol (SIP) standard was developed by the Internet Engineering Task Force (IETF). RFC 2543 was released in March 1999. RFC 3261 was released in June 2002. SIP is a signaling protocol for initiating, managing and terminating sessions. SIP supports ‘presence’ and mobility and can run over User Datagram Protocol (UDP) and Transmission Control Protocol (TCP).

Using SIP, a VoIP client can initiate and terminate call sessions, invite members into a conferencing session, and perform other telephony tasks. SIP also enables Private Branch Exchanges (PBXs), VoIP gateways, and other communications devices to communicate in standardized collaboration. SIP was also designed to avoid the heavy overhead of H.323.

A SIP network is composed of the following logical entities:

- **User Agent (UA)** - Initiates, receives and terminates calls.
- **Proxy Server** - Acts on behalf of UA in forwarding or responding to requests. A Proxy Server can fork requests to multiple servers. A back-to-back user agent (B2BUA) is a type of Proxy Server that treats each leg of a call passing through it as two distinct SIP call sessions: one between it and the calling phone and the other between it and the called phone. Other Proxy Servers treat all legs of the same call as a single SIP call session.

- **Redirect Server** - Responds to request but does not forward requests.
- **Registration Server** - Handles UA authentication and registration.

SonicWALL’s VoIP Capabilities

The following sections describe SonicWALL’s integrated VoIP service:

- “VoIP Security” on page 4
- “VoIP Network” on page 5
- “VoIP Network Interoperability” on page 5
- “Supported VoIP Protocols” on page 7

VoIP Security

- **Application-layer protection for VoIP protocols** - Full protection from application-level VoIP exploits through SonicWALL Intrusion Prevention Service (IPS). IPS integrates a configurable, high performance scanning engine with a dynamically updated and provisioned database of attack and vulnerability signatures to protect networks against sophisticated Trojans and polymorphic threats. SonicWALL extends its IPS signature database with a family of VoIP-specific signatures designed to prevent malicious traffic from reaching protected VoIP phones and servers. Signature granularity allows SonicWALL IPS to detect and prevent attacks based on a global, attack group, or per-signature basis to provide maximum flexibility and control false positives.
- **DoS and DDoS attack protection** - Prevention of DoS and DDoS attacks, such as the SYN Flood, Ping of Death, and LAND (IP) attack, which are designed to disable a network or service.
  - Validating packet sequence for VoIP signaling packets using TCP to disallow out of sequence and retransmitted packets beyond window.
  - Using randomized TCP sequence numbers (generated by a cryptographic random number generator during connection setup) and validating the flow of data within each TCP session to prevent replay and data insertion attacks.
  - Ensures that attackers cannot overwhelm a server by attempting to open many TCP/IP connections (which are never fully established-usually due to a spoofed source address) by using SYN Flood protection.
- **Encrypted VoIP Device Support** - SonicWALL supports VoIP devices capable of using encryption to protect the media exchange within a VoIP conversation or secure VoIP devices that do not support encrypted media using IPSec VPNs to protect VoIP calls.
- **Stateful monitoring** - Stateful monitoring ensures that packets, even though appearing valid in themselves, are appropriate for the current state of their associated VoIP connection.
- **Traffic legitimacy** - Stateful inspection of every VoIP signaling and media packet traversing the firewall ensures all traffic is legitimate. Packets that exploit implementation flaws, causing effects such as buffer overflows in the target device, are the weapons of choice for many attackers. SonicWALL security appliances detect and discard malformed and invalid packets before they reach their intended target.

VoIP Network

Note SonicWALL's Secure Wireless Solution includes the network enablers to extend secure VoIP communications over wireless networks. Refer to the *SonicWALL Secure Wireless Network Integrated Solutions Guide* available on the SonicWALL documentation site http://www.sonicwall.com/support /documentation.html for complete information.

- **Bandwidth Management (BWM) and Quality-of-Service (QoS)** - Bandwidth management (both ingress and egress) can be used to ensure that bandwidth remains available for time-sensitive VoIP traffic. BWM is integrated into SonicWALL Quality of Service (QoS) features (on SonicOS Enhanced) to provide predictability that is vital for certain types of applications.
- **High availability** - High availability is provided by SonicOS hardware failover, which ensures reliable, continuous connectivity in the event of a system failure.
- **VoIP over Wireless LAN (WLAN)** - SonicWALL extends complete VoIP security to attached wireless networks with its Distributed Wireless Solution. All of the security features provided to VoIP devices attached to a wired network behind a SonicWALL are also provided to VoIP devices using a wireless network.
- **WAN redundancy and load balancing** - WAN redundancy and load balancing allows for an interface to act as a secondary or backup WAN port. The secondary WAN port can also be used in a more dynamic load balancing, active/active setup, where outbound traffic flows are divided between the primary and secondary WAN ports for increased throughput.

VoIP Network Interoperability

- **Comprehensive monitoring and reporting** - For all supported VoIP protocols, SonicOS offers extensive monitoring and troubleshooting tools:
  - Dynamic live reporting of active VoIP calls, indicating the caller and called parties, and bandwidth used.
  - Audit logs of all VoIP calls, indicating caller and called parties, call duration, and total bandwidth used. Logging of abnormal packets seen (such as a bad response) with details of the parties involved and condition seen.
  - Detailed syslog reports and ViewPoint reports for VoIP signaling and media streams. SonicWALL ViewPoint is a Web-based graphical reporting tool that provides detailed and comprehensive reports of your security and network activities based on syslog data streams received from the firewall. Reports can be generated about virtually any aspect of firewall activity, including individual user or group usage patterns and events on specific firewalls or groups of firewalls, types and times of attacks, resource consumption and constraints, etc.
- **Configurable inactivity timeouts for signaling and media** - In order to ensure that dropped VoIP connections do not stay open indefinitely, SonicOS monitors the usage of signaling and media streams associated with a VoIP session. Streams that are idle for more than the configured timeout are shut down to prevent potential security holes.
- **Full syntax validation of all VoIP signaling packets** - Received signaling packets are fully parsed within SonicOS to ensure they comply with the syntax defined within their associated standard. By performing syntax validation, the firewall can ensure that malformed packets are not permitted to pass through and adversely affect their intended target.

- **Plug-and-protect support for VoIP devices** - With SonicOS, VoIP device adds, changes, and removals are handled automatically, ensuring that no VoIP device is left unprotected. Using advanced monitoring and tracking technology, a VoIP device is automatically protected as soon as it is plugged into the network behind a SonicWALL security appliance.
- **SonicOS allows the administrator to control incoming calls** - By requiring that all incoming calls are authorized and authenticated by the H.323 Gatekeeper or SIP Proxy, SonicOS can block unauthorized and spam calls. This allows the administrator to be sure that the VoIP network is being used only for those calls authorized by the company.
- **Support for dynamic setup and tracking of media streams** - SonicOS tracks each VoIP call from the first signaling packet requesting a call setup, to the point where the call ends. Only based on the successful call progress are additional ports opened (for additional signaling and media exchange) between the calling and called party.

  Media ports that are negotiated as part of the call setup are dynamically assigned by the firewall. Subsequent calls, even between the same parties, will use different ports, thwarting an attacker who may be monitoring specific ports. Required media ports are only opened when the call is fully connected, and are shut down upon call termination. Traffic that tries to use the ports outside of the call is dropped, providing added protection to the VoIP devices behind the firewall.
- **Validation of headers for all media packets** - SonicOS examines and monitors the headers within media packets to allow detection and discarding of out-of-sequence and retransmitted packets (beyond window). Also, by ensuring that a valid header exists, invalid media packets are detected and discarded. By tracking the media streams as well as the signaling, SonicWALL provides protection for the entire VoIP session.

Supported VoIP Protocols

SonicWALL security appliances support transformations for the following protocols.

H.323

SonicOS provides the following support for H.323:

- VoIP devices running all versions of H.323 (currently 1 through to 5) are supported
- Microsoft's LDAP-based Internet Locator Service (ILS)
- Discovery of the Gatekeeper by LAN H.323 terminals using multicast
- Stateful monitoring and processing of Gatekeeper registration, admission, and status (RAS) messages
- Support for H.323 terminals that use encryption for the media streams
- DHCP Option 150. The SonicWALL DHCP Server can be configured to return the address of a VoIP specific TFTP server to DHCP clients
- In addition to H.323 support, SonicOS supports VoIP devices using the following additional ITU standards:
    - T.120 for application sharing, electronic white-boarding, file exchange, and chat
    - H.239 to allow multiple channels for delivering audio, video and data
    - H.281 for Far End Camera Control (FECC)

SIP

SonicOS provides the following support for SIP:

- Base SIP standard (both RFC 2543 and RFC 3261)
- SIP INFO method (RFC 2976)
- Reliability of provisional responses in SIP (RFC 3262)
- SIP specific event notification (RFC 3265)
- SIP UPDATE method (RFC 3311)
- DHCP option for SIP servers (RFC 3361)
- SIP extension for instant messaging (RFC 3428)
- SIP REFER method (RFC 3515)
- Extension to SIP for symmetric response routing (RFC 3581)

SonicWALL VoIP Vendor Interoperability

The following is a partial list of devices from leading manufacturers with which SonicWALL VoIP interoperates.

H.323	SIP
Soft-phones: Microsoft NetMeeting OpenPhone SJLabs SJ Phone **Telephones/VideoPhones:** Cisco 7905 D-Link DV 1000 PolyCom VS-FX Sony PCS-1 Sony PCS-11 **Gatekeepers:** Cisco IOS OpenH323 Gatekeeper **Gateway:** Cisco VG200	**Soft-phones:** Apple iChat Microsoft MSN Messenger Nortel Multimedia PC Client PingTel Instant Xpressa Siemens SCS Client SJLabs SJPhone XTen X-Lite Ubiquity SIP User Agent **Telephones/ATAs:** Cisco 7905 Cisco 7960 Cisco ATA 186 Grandstream BudgetOne 100 Mitel 5055 Packet8 ATA PingTel Xpressa PolyCom SoundPoint IP 500 Pulver Innovations WiSIP **SIP Proxies/Services:** Cisco SIP Proxy Server Brekeke Software OnDo SIP Proxy Packet8 Siemens SCS SIP Proxy Vonage

CODECs

SonicOS supports media streams from any CODEC - Media streams carry audio and video signals that have been processed by a hardware/software CODEC (COder/DECoder) within the VoIP device. CODECs use coding and compression techniques to reduce the amount of data required to represent audio/video signals. Some examples of CODECs are:

- H.264, H.263, and H.261 for video
- MPEG4, G.711, G.722, G.723, G.728, G.729 for audio

VoIP Protocols that SonicOS Does Not Perform Deep Packet Inspection on

SonicWALL security appliances running SonicOS Enhanced do not currently support deep packet inspection for the following protocols; therefore, these protocols should only be used in non-NAT environments.

- Proprietary extensions to H.323 or SIP
- MGCP
- Megaco/H.248
- Cisco Skinny Client Control Protocol (SCCP)
- IP-QSIG
- Proprietary protocols (Mitel's MiNET, 3Com NBX, etc.)

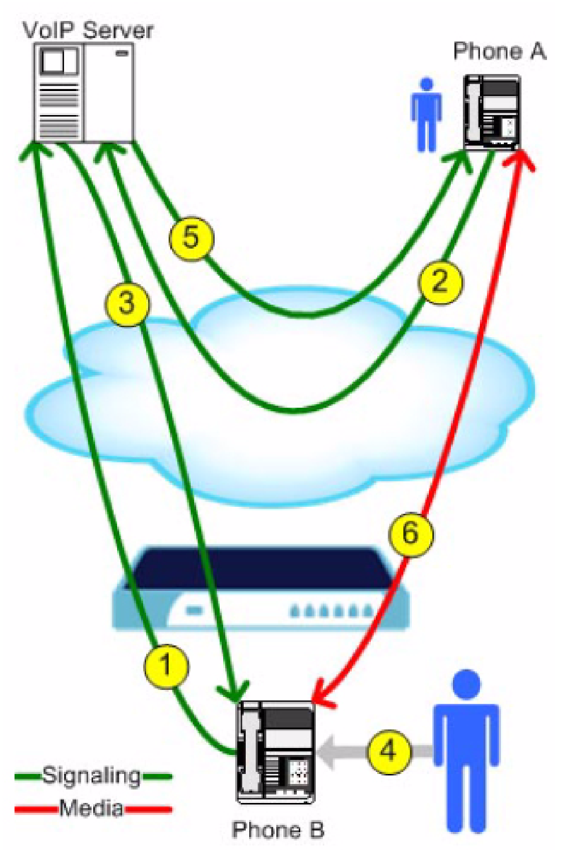
How SonicOS Handles VoIP Calls

SonicOS provides an efficient and secure solution for all VoIP call scenarios. The following are examples of how SonicOS handles VoIP call flows.

Incoming Calls

Figure 1 shows the sequence of events that occur during an incoming VoIP call.

Figure 1 Incoming VoIP Call Flow



The following describes the sequence of events shown in Figure 1.

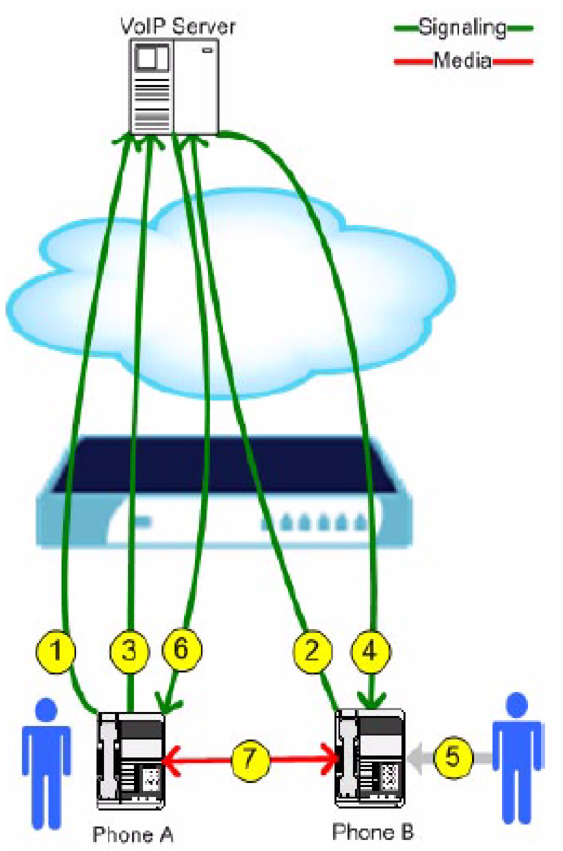
1. **Phone B registers with VoIP server -** The SonicWALL security appliance builds a database of the accessible IP phones behind it by monitoring the outgoing VoIP registration requests. SonicOS translates between phone B's private IP address and the firewall's public IP address used in registration messages. The VoIP server is unaware that phone B is behind a firewall and has a private IP address—it associates phone B with the firewall's public IP address.
2. **Phone A initiates a call to phone B -** Phone A initiates a call to phone B using a phone number or alias. When sending this information to the VoIP server, it also provides details about the media types and formats it can support as well as the corresponding IP addresses and ports.
3. **VoIP Server validates the call request and sends the request to phone B**. The VoIP server sends the call request to the firewall's public IP address. When it reaches the firewall, SonicOS validates the source and content of the request. The firewall then determines phone B's private IP address.

4. **Phone B rings and is answered**. When phone B is answered, it returns information to the VoIP server for the media types and formats it supports as well as the corresponding IP addresses and ports. SonicOS translates this private IP information to use the firewall's public IP address for messages to the VoIP server.
5. **VoIP server returns phone B media IP information to phone A**. Phone A now has enough information to begin exchanging media with Phone B. Phone A does not know that Phone B is behind a firewall, as it was given the public address of the firewall by the VoIP Server.
6. **Phone A and phone B exchange audio/video/data through the VoIP server**. Using the internal database, SonicOS ensures that media comes from only Phone A and is only using the specific media streams permitted by Phone B.

Local Calls

Figure 2 shows the sequence of events that occur during a local VoIP call.

Figure 2 Local VoIP Call Flow



The following describes the sequence of events shown in Figure 2.

1. **Phone A registers with the VoIP server** - The SonicWALL security appliance adds Phone A to its database of accessible IP phones by monitoring the outgoing VoIP registration request. SonicOS translates between Phone A's private IP address and the firewall's public IP address. The VoIP server is unaware that Phone A is behind a firewall.

2. **Phone B registers with the VoIP server** - The SonicWALL security appliance adds Phone B to its database. The SonicWALL associates the same public IP address for both phones, but it assigns different port numbers for each phone.
3. **Phone A initiates a call to phone B by sending a request to the VoIP server -** Even though they are behind the same firewall, phone A does not know Phone B's IP address. Phone A initiates a call to phone B using a phone number or alias.
4. **VoIP Server validates the call request and sends the request to phone B -** The VoIP server sends the call request to the firewall's public IP address.The firewall then determines phone B's private IP address.
5. **Phone B rings and is answered** - When phone B is answered, the firewall translate its private IP information to use the firewall's public IP address for messages to the VoIP server.
6. **VoIP Server returns phone B media IP information to phone A -** Both the called and calling party information within the messages are translated by SonicOS back to the private addresses and ports for phone A and phone B.
7. **Phone A and phone B directly exchange audio/video/data -** The SonicWALL security appliance routes traffic directly between the two phones over the LAN. Directly connecting the two phones reduces the bandwidth requirements for transmitting data to the VoIP server and eliminates the need for the SonicWALL security appliance to perform address translation.

Configuring SonicWALL VoIP Features

Configuring the SonicWALL security appliance for VoIP deployments builds on your basic network configuration in the SonicWALL management interface. This document assumes the SonicWALL security appliance is configured for your network environment.

Supported Interfaces

VoIP devices are supported on the following SonicOS Enhanced Zones:

- Trusted zones (LAN, VPN)
- Untrusted zones (WAN)
- Public zones (DMZ)
- Wireless zones (WLAN)

Supported Platforms

SonicWALL security appliances running SonicOS Standard 3.0 (or higher) and SonicOS Enhanced 3.0 (or higher) support SonicWALL's integrated VoIP features. SonicWALL security appliances with SonicOS Enhanced include additional features including call monitoring, reporting functionality, and QoS support (e.g., inbound bandwidth management). All SonicWALL TZ 170 Series and SonicWALL PRO Series security appliances running SonicOS Enhanced feature the same comprehensive level of VoIP security described in this document. These SonicWALL security appliances include:

SonicWALL TZ 170 Series	SonicWALL PRO Series
SonicWALL TZ 170	SonicWALL PRO 1260
SonicWALL TZ 170 SP	SonicWALL PRO 2040
SonicWALL TZ 170 Wireless	SonicWALL PRO 3060
SonicWALL TZ 170 SP Wireless	SonicWALL PRO 4060
	SonicWALL PRO 5060

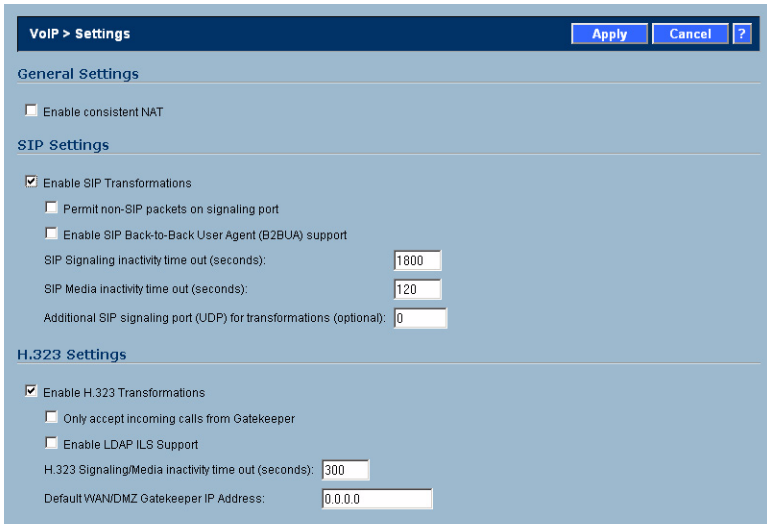
Configuration Tasks

- "General VoIP Configuration" on page 14
  - "Configuring Consistent Network Address Translation (NAT)" on page 14
  - "Configuring SIP Settings" on page 15
  - "Configuring H.323 Transformations" on page 16
- "Configuring BWM and QoS" on page 17
  - "Bandwidth Management" on page 17
  - "Quality of Service" on page 17
  - "Configuring Bandwidth on the WAN Interface" on page 18
  - "Configuring VoIP Access Rules" on page 19
  - "Using the Public Server Wizard" on page 21

- “Configuring VoIP Logging” on page 24
- “Configuring SonicWALL IPS” on page 24

General VoIP Configuration

SonicOS Enhanced includes the VoIP configuration settings on the **VoIP** > **Settings** page. This page is divided into three configuration settings sections: **General Settings**, **SIP Settings**, and **H.323 Settings**.



VoIP > Settings

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): 0

H.323 Settings

☑ Enable H.323 Transformations

□ Only accept incoming calls from Gatekeeper

□ Enable LDAP ILS Support

H.323 Signaling/Media inactivity time out (seconds): 300

Default WAN/DMZ Gatekeeper IP Address: 0.0.0.0

Configuring Consistent Network Address Translation (NAT)

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.

For example, NAT could translate the private (LAN) IP address and port pairs, 192.116.168.10/50650 and 192.116.168.20/50655 into public (WAN) IP/port pairs as follows:

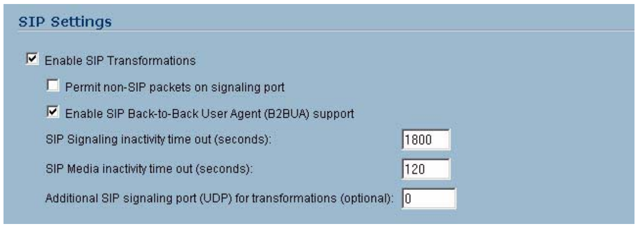
Private IP/Port	Translated Public IP/Port
192.116.168.10/50650	64.41.140.167/40004
192.116.168.20/50655	64.41.140.167/40745

With Consistent NAT enabled, all subsequent requests from either host 192.116.168.10 or 192.116.168.20 using the same ports illustrated in the previous result in using the same translated address and port pairs. Without Consistent NAT, the port and possibly the IP address change with every request.

To enable Consistent NAT, select the **Enable Consistent NAT** setting and click **Apply**. This checkbox is disabled by default.

Note Enabling Consistent NAT causes a slight decrease in overall security, because of the increased predictability of the address and port pairs. Most UDP-based applications are compatible with traditional NAT. Therefore, do not enable Consistent NAT unless your network uses applications that require it.

Configuring SIP Settings



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): 0

By default, SIP clients use their private IP address in the SIP Session Definition Protocol (SDP) messages that are sent to the SIP proxy. If your SIP proxy is located on the public (WAN) side of the SonicWALL security appliance and SIP clients are on the private (LAN) side behind the firewall, the SDP messages are not translated and the SIP proxy cannot reach the SIP clients.

Selecting **Enable SIP Transformations** transforms SIP messages between LAN (trusted) and WAN/DMZ (untrusted). You need to check this setting when you want the SonicWALL security appliance to do the SIP transformation. If your SIP proxy is located on the public (WAN) side of the SonicWALL and SIP clients are on the LAN side, the SIP clients by default embed/use their private IP address in the SIP/Session Definition Protocol (SDP) messages that are sent to the SIP proxy, hence these messages are not changed and the SIP proxy does not know how to get back to the client behind the SonicWALL. Selecting **Enable SIP Transformations** enables the SonicWALL to go through each SIP message and change the private IP address and assigned port. **Enable SIP Transformation** also controls and opens up the RTP/RTCP ports that need to be opened for the SIP session calls to happen. NAT translates Layer 3 addresses but not the Layer 7 SIP/SDP addresses, which is why you need to select Enable SIP Transformations to transform the SIP messages.

Tip In general, you should check the **Enable SIP Transformations** box unless there is another NAT traversal solution that requires this feature to be turned off. SIP Transformations works in bi-directional mode, meaning messages are transformed going from LAN to WAN and vice versa.

Selecting **Permit non-SIP packets on signaling port** enables applications such as Apple iChat and MSN Messenger, which use the SIP signaling port for additional proprietary messages. Enabling this checkbox may open your network to malicious attacks caused by malformed or invalid SIP traffic. This checkbox is disabled by default.

(Available in SonicOS Enhanced 3.2) The **Enable SIP Back-to-Back User Agent (B2BUA) support** setting should be enabled when the SonicWALL security appliance can see both legs of a voice call (for example, when a phone on the LAN calls another phone on the LAN). This setting should only be enabled when the SIP Proxy Server is being used as a B2BUA.

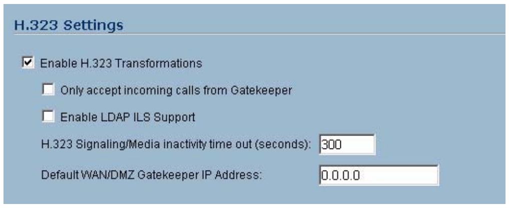
Tip If there is not the possibility of the SonicWALL security appliance seeing both legs of voice calls (for example, when calls will only be made to and received from phones on the WAN), the **Enable SIP Back-to-Back User Agent (B2BUA) support** setting should be disabled to avoid unnecessary CPU usage.

SIP Signaling inactivity time out (seconds) and **SIP Media inactivity time out (seconds)** define the amount of time a call can be idle (no traffic exchanged) before the SonicWALL security appliance denying further traffic. A call goes idle when placed on hold. The default time value for **SIP Signaling inactivity time out** is 1800 seconds (30 minutes). The default time value for **SIP Media inactivity time out** is 120 seconds (2 minutes).

The **Additional SIP signaling port (UDP) for transformations** setting allows you to specify a non-standard UDP port used to carry SIP signaling traffic. Normally, SIP signaling traffic is carried on UDP port 5060. However, a number of commercial VOIP services use different ports, such as 1560. Using this setting, the security appliance performs SIP transformation on these non-standard ports.

Tip Vonage's VoIP service uses UDP port 5061.

Configuring H.323 Transformations



H.323 Settings

☑ Enable H.323 Transformations

□ Only accept incoming calls from Gatekeeper

□ Enable LDAP ILS Support

H.323 Signaling/Media inactivity time out (seconds): 300

Default WAN/DMZ Gatekeeper IP Address: 0.0.0.0

Select **Enable H.323 Transformation** in the **H.323 Settings** section and click **Apply** to allow stateful H.323 protocol-aware packet content inspection and modification by the SonicWALL security appliance. The SonicWALL security appliance performs any dynamic IP address and transport port mapping within the H.323 packets, which is necessary for communication between H.323 parties in trusted and untrusted networks/zones. Disable the **Enable H.323 Transformation** to bypass the H.323 specific processing performed by the SonicWALL security appliance.

Select **Only accept incoming calls from Gatekeeper** to ensure all incoming calls go through the Gatekeeper for authentication. The Gatekeeper will refuse calls that fail authentication (SonicOS Enhanced).

Select **Enable LDAP ILS Support** to enable Microsoft NetMeeting users to locate and connect to users for conferencing and collaboration over the Internet (SonicOS Enhanced).

The **H.323 Signaling/Media inactivity time out (seconds)** field specifies the amount of time a call can be idle before the SonicWALL security appliance denying further traffic. A call goes idle when placed on hold. The default time value for **H.323 Signaling/Media inactivity time out** is 300 seconds (5 minutes).

The **Default WAN/DMZ Gatekeeper IP Address** field has a default value of 0.0.0.0. Enter the default H.323 Gatekeeper IP address in this field to allow LAN-based H.323 devices to discover the Gatekeeper using the multicast address 224.0.1.41. If you do not enter an IP address, multicast discovery messages from LAN-based H.323 devices will go through the configured multicast handling (SonicOS Enhanced).

Configuring BWM and QoS

One of the greatest challenges for VoIP is ensuring high speech quality over an IP network. IP was designed primarily for asynchronous data traffic, which can tolerate delay. VoIP, however, is very sensitive to delay and packet loss. Managing access and prioritizing traffic are important requirements for ensuring high-quality, real-time VoIP communications.

SonicWALL's integrated Bandwidth Management (BWM) and Quality of Service (QoS) features provide the tools for managing the reliability and quality of your VoIP communications.

Bandwidth Management

SonicOS offers an integrated traffic shaping mechanism through its Egress (outbound) and Ingress (inbound) management interfaces. Outbound BWM can be applied to traffic sourced from Trusted and Public Zones (such as LAN and DMZ) destined to Untrusted and Encrypted Zones (such as WAN and VPN). Inbound bandwidth management can be applied to traffic sourced from Untrusted and Encrypted Zones destined to Trusted and Public Zones.

Enabling bandwidth management allows you to assign guaranteed and maximum bandwidth to services and prioritize traffic on all WAN zones. Using access rules, bandwidth management can be enabled on a per-interface basis. Packets belonging to a bandwidth management enabled policy will be queued in the corresponding priority queue before being sent on the bandwidth management-enabled WAN interface. Access rules using bandwidth management have a higher priority than access rules not using bandwidth management. Access rules without bandwidth management are given lowest priority.

Quality of Service

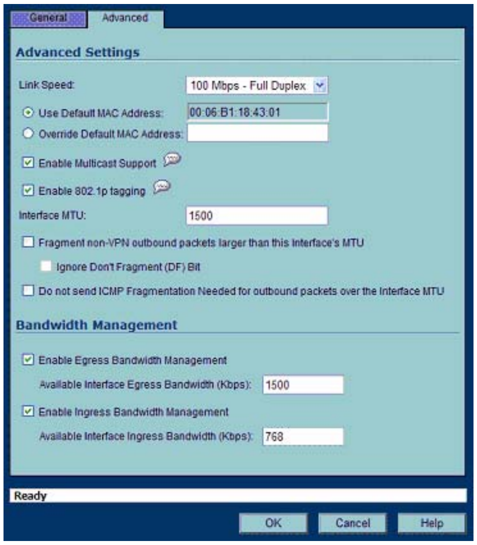
QoS encompasses a number of methods intended to provide predictable network behavior and performance. Network predictability is vital to VoIP and other mission critical applications. No amount of bandwidth can provide this sort of predictability, because any amount of bandwidth will ultimately be used to its capacity at some point in a network. Only QoS, when configured and implemented correctly, can properly manage traffic, and guarantee the desired levels of network service.

SonicOS Enhanced includes QoS features that adds the ability to recognize, map, modify and generate the industry-standard 802.1p and Differentiated Services Code Points (DSCP) Class of Service (CoS) designators.

Note Refer to the Configuring QoS and BWM Feature Module for complete BWM and QoS configuration instructions. Available on the SonicWALL Web site <www.sonicwall.com/support/documentation.html>

Configuring Bandwidth on the WAN Interface

BWM configurations begin by enabling BWM on the relevant WAN interface, and specifying the interface's available bandwidth in Kbps. This is performed from the **Network > Interfaces** page by selecting the **Configure** icon for the WAN interface, and navigating to the **Advanced** tab:



Advanced Settings

Link Speed: 100 Mbps - Full Duplex

● Use Default MAC Address: 00:06:B1:18:43:01

○ Override Default MAC Address:

☑ Enable Multicast Support

☑ Enable 802.1p tagging

Interface MTU: 1500

□ Fragment non-VPN outbound packets larger than this Interface's MTU

□ Ignore Don't Fragment (DF) Bit

□ Do not send ICMP Fragmentation Needed for outbound packets over the Interface MTU

Bandwidth Management

☑ Enable Egress Bandwidth Management

Available Interface Egress Bandwidth (Kbps): 1500

☑ Enable Ingress Bandwidth Management

Available Interface Ingress Bandwidth (Kbps): 768

Ready

Egress and Ingress BWM can be enabled jointly or separately on WAN interfaces. Different bandwidth values may be entered for outbound and inbound bandwidth to support asymmetric links. Link rates up to 100,000 Kbps (100Mbit) may be declared on Fast Ethernet interface, while Gigabit Ethernet interfaces will support link rates up to 1,000,000 (Gigabit). The bandwidth specified should reflect the actual bandwidth available for the link. Oversubscribing the link (i.e. declaring a value greater than the available bandwidth) is not recommended.

Once one or both BWM settings are enabled on the WAN interface and the available bandwidth has been declared, a **Bandwidth** tab will appear on Access Rules. See the following "Configuring VoIP Access Rules" section for more information.

To configure Bandwidth Management on the SonicWALL security appliance:

Step 1 Select **Network > Interfaces**.

Step 2 Click the Edit icon in the Configure column in the **WAN** (**X1**) line of the Interfaces table. The **Edit Interface** window is displayed.

Step 3 Click the **Advanced** tab.

Step 4 Check **Enable Egress** (Outbound) **Bandwidth Management** and enter the total available WAN bandwidth in the **Available Interface Egress Bandwidth Management** field.

Step 5 Check **Enable Ingress** (Inbound) **Bandwidth Management** and enter the total available WAN bandwidth in the **Available Interface Ingress Bandwidth Management** field.

Step 6 Click **OK**.

Configuring VoIP Access Rules

By default, the SonicWALL security appliance's stateful packet inspection allows all communication from the LAN to the Internet and blocks all traffic to the LAN from the Internet. Additional network access rules can be defined to extend or override the default access rules.

If you are defining VoIP access for client to use a VoIP service provider from the WAN, you configure network access rules between source and destination interface or zones to enable clients behind the firewall to send and receive VoIP calls.

If your SIP Proxy or H.323 Gateway is located behind the firewall, you can use the SonicWALL **Public Server Wizard** to automatically configure access rules.

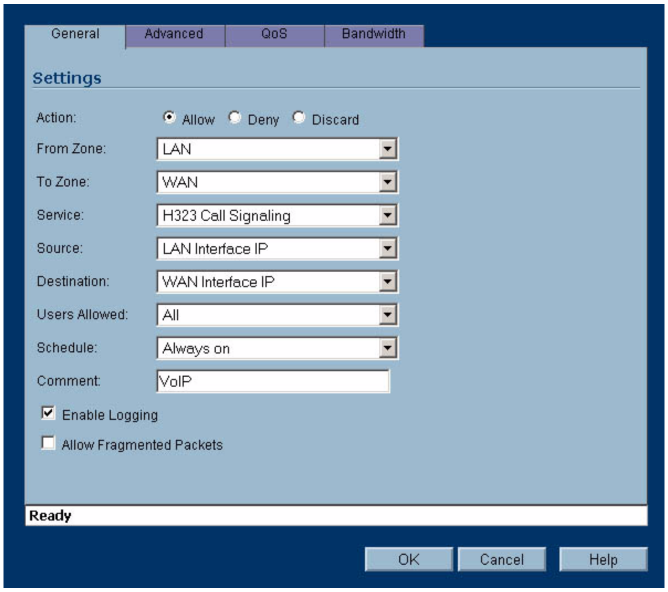
Tip Although custom rules can be created that allow inbound IP traffic, the SonicWALL security appliance does not disable protection from Denial of Service attacks, such as the SYN Flood and Ping of Death attacks.

To add access rules for VoIP traffic on the SonicWALL security appliance running SonicOS Enhanced:

Note You must select Bandwidth Management on the **Network** > **Interfaces** page for the **WAN** interface before you can configure bandwidth management for network access rules.

Step 1 Go to the **Firewall** > **Access Rules** page, and under **View Style** click **All Rules**.

Step 2 Click **Add** at the bottom of the **Access Rules** table. The **Add Rule** window is displayed.



Settings

Action: ● Allow ○ Deny ○ Discard

From Zone: LAN

To Zone: WAN

Service: H323 Call Signaling

Source: LAN Interface IP

Destination: WAN Interface IP

Users Allowed: All

Schedule: Always on

Comment: VoIP

☑ Enable Logging

☐ Allow Fragmented Packets

Ready

Step 3 In the **General** tab, select **Allow** from the **Action** list to permit traffic.

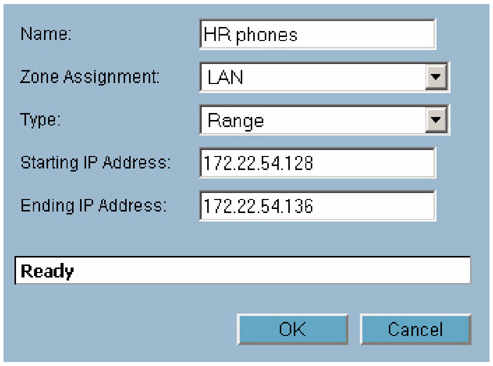
Step 4 Select the from and to zones from the **From Zone** and **To Zone** menus.

Step 5 Select the service or group of services affected by the access rule from the **Service** list.

- For H.323, select one of the following or select **Create New Group** and add the following services to the group:

  - **H.323 Call Signaling**
  - **H.323 Gatekeeper Discovery**
  - **H.323 Gatekeeper RAS**
- For SIP, select **SIP**

Step 6 Select the source of the traffic affected by the access rule from the **Source** list. Selecting **Create New Network** displays the **Add Address Object** window.



Name: HR phones

Zone Assignment: LAN

Type: Range

Starting IP Address: 172.22.54.128

Ending IP Address: 172.22.54.136

Ready

Step 7 If you want to define the source IP addresses that are affected by the access rule, such as restricting certain users from accessing the Internet, select **Range** in the **Type:** pulldown menu. The enter the lowest and highest IP addresses in the range in the **Starting IP Address:** and **Ending IP Address** fields.

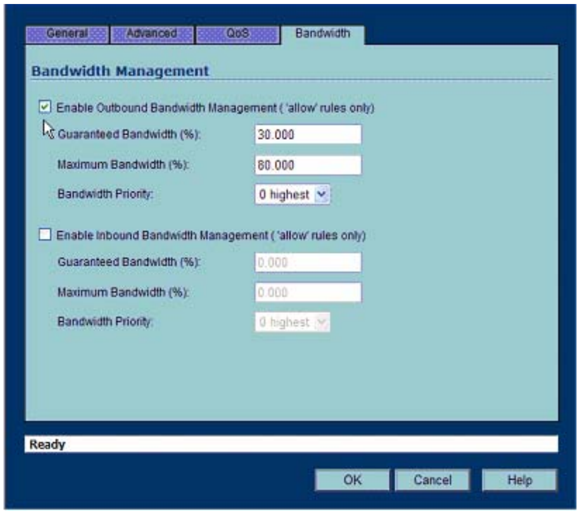
Step 8 Select the destination of the traffic affected by the access rule from the **Destination** list. Selecting **Create New Network** displays the **Add Address Object** window.

Step 9 From the **Users Allowed** menu, add the user or user group affected by the access rule.

Step 10 Select a schedule from the **Schedule** menu if you want to allow VoIP access only during specified times. The default schedule is **Always on**. You can specify schedule objects on the **System > Schedules** page.

Step 11 Enter any comments to help identify the access rule in the **Comments** field.

Step 12 Click the **Bandwidth** tab.



Bandwidth Management

☑ Enable Outbound Bandwidth Management ('allow' rules only)

Guaranteed Bandwidth (%): 30.000

Maximum Bandwidth (%): 80.000

Bandwidth Priority: 0 highest

☐ Enable Inbound Bandwidth Management ('allow' rules only)

Guaranteed Bandwidth (%): 0.000

Maximum Bandwidth (%): 0.000

Bandwidth Priority: 0 highest

Ready

Step 13 Select **Bandwidth Management**, and enter the **Guaranteed Bandwidth** in Kbps.

Step 14 Enter the maximum amount of bandwidth available to the Rule at any time in the **Maximum Bandwidth** field.

Step 15 Assign a priority from 0 (highest) to 7 (lowest) in the **Bandwidth Priority** list. For higher VoIP call quality, ensure VoIP traffic receives HIGH priority.

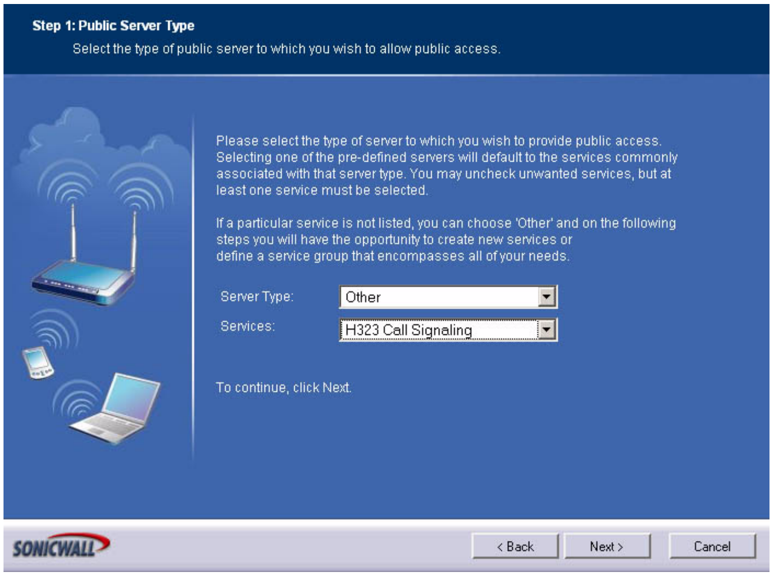
Tip Rules using Bandwidth Management take priority over rules without bandwidth management.

Using the Public Server Wizard

The SonicWALL **Public Server Wizard** provides an easy method for configuring firewall access rules for a SIP Proxy or H.323 Gatekeeper running on your network behind the firewall. Using this wizard performs all the configuration settings you need for VoIP clients to access your VoIP servers.

Step 1 Click **Wizards** on the SonicOS navigation bar.

Step 2 Select **Public Server Wizard** and click **Next**.



Step 1: Public Server Type

Select the type of public server to which you wish to allow public access.

Please select the type of server to which you wish to provide public access. Selecting one of the pre-defined servers will default to the services commonly associated with that server type. You may uncheck unwanted services, but at least one service must be selected.

If a particular service is not listed, you can choose 'Other' and on the following steps you will have the opportunity to create new services or define a service group that encompasses all of your needs.

Server Type: Other

Services: H323 Call Signaling

To continue, click Next.

Step 3 Select **Other** from the **Server Type** list.

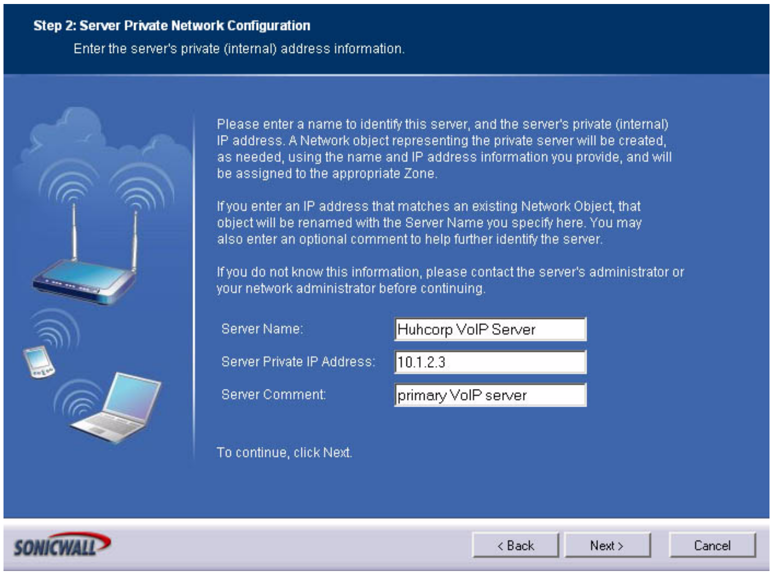
Select **SIP** from the **Services** menu if you're configuring network access for a SIP proxy server from the WAN.

Select **Gatekeeper RAS** if you're configuring network access for a H.323 Gatekeeper from the WAN.

Select **H.323 Call Signaling** for enabling Point-to-Point VoIP calls from the WAN to the LAN.

Click **Next**

Note SonicWALL recommends NOT selecting **VoIP** from the **Services** menu. Selecting this option opens up more TCP/UDP ports than is required, potentially opening up unnecessary security vulnerabilities.



Step 2: Server Private Network Configuration

Enter the server's private (internal) address information.

Please enter a name to identify this server, and the server's private (internal) IP address. A Network object representing the private server will be created, as needed, using the name and IP address information you provide, and will be assigned to the appropriate Zone.

If you enter an IP address that matches an existing Network Object, that object will be renamed with the Server Name you specify here. You may also enter an optional comment to help further identify the server.

If you do not know this information, please contact the server's administrator or your network administrator before continuing.

Server Name: Huhcorp VoIP Server

Server Private IP Address: 10.1.2.3

Server Comment: primary VoIP server

To continue, click Next.

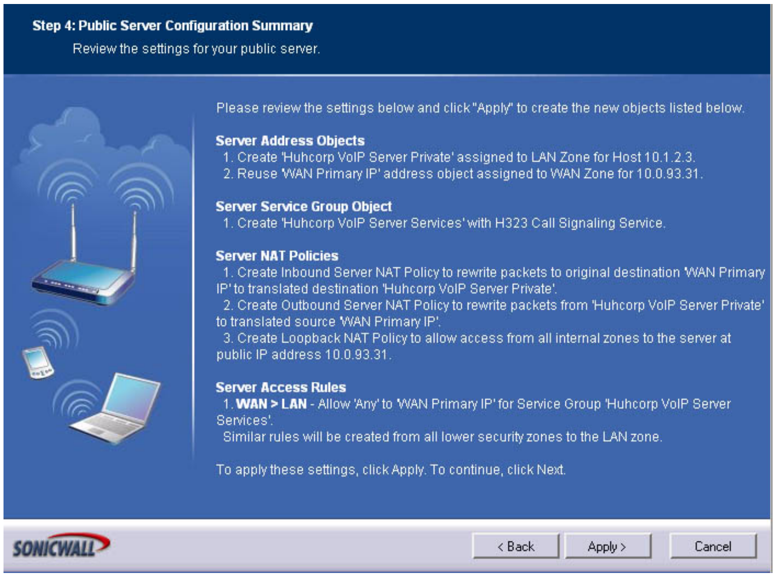
Step 4 Enter the name of the server in the **Server Name** field.

Step 5 Enter the private IP address of the server. Specify an IP address in the range of addresses assigned to the zone where the server is located. The Public Server Wizard will automatically assign the server to the zone in which its IP address belongs. You can enter optional descriptive text in the Server Comment field.

Step 6 Click **Next**.

Step 7 Enter the public IP address of the server. The default is the WAN public IP address. If you enter a different IP, the Public Server Wizard will create an address object for that IP address and bind the address object to the WAN zone.

Step 8 Click **Next**.



Step 4: Public Server Configuration Summary

Review the settings for your public server.

Please review the settings below and click "Apply" to create the new objects listed below.

Server Address Objects

1. Create 'Huhcorp VoIP Server Private' assigned to LAN Zone for Host 10.1.2.3.
2. Reuse 'WAN Primary IP' address object assigned to WAN Zone for 10.0.93.31.

Server Service Group Object

1. Create 'Huhcorp VoIP Server Services' with H323 Call Signaling Service.

Server NAT Policies

1. Create Inbound Server NAT Policy to rewrite packets to original destination 'WAN Primary IP' to translated destination 'Huhcorp VoIP Server Private'.
2. Create Outbound Server NAT Policy to rewrite packets from 'Huhcorp VoIP Server Private' to translated source 'WAN Primary IP'.
3. Create Loopback NAT Policy to allow access from all internal zones to the server at public IP address 10.0.93.31.

Server Access Rules

1. **WAN > LAN** - Allow 'Any' to 'WAN Primary IP' for Service Group 'Huhcorp VoIP Server Services'.

Similar rules will be created from all lower security zones to the LAN zone.

To apply these settings, click Apply. To continue, click Next.

Step 9 The Summary page displays a summary of all the configuration you have performed in the wizard. It should show:

- **Server Address Objects** - The wizard creates the address object for the new server. Because the IP address of the server added in the example is in the IP address range assigned to the LAN zone, the wizard binds the address object to the LAN zone.
- **Server Service Group Object** - The wizard creates a service group object for the services used by the new server.
- **Server NAT Policies** - The wizard creates a NAT policy to translate the destination addresses of all incoming packets with one of the services in the new service group and addressed to the WAN address to the address of the new server. The wizard also creates a Loopback NAT policy
- **Server Access Rules** - The wizard creates an access policy allowing all traffic to the WAN Primary IP for the new service.

Step 10 Click **Apply** in the Public Server Configuration Summary page to complete the wizard and apply the configuration to your SonicWALL.

Tip The new IP address used to access the new server, both internally and externally, is displayed in the **URL** field of the **Congratulations** window.

Step 11 Click **Close** to close the wizard.

Configuring VoIP Logging

You can enable the logging of VoIP events in the SonicWALL security appliance log in the **Log** > **Categories** page. Log entries are displayed on the **Log** > **View** page. To enable logging:

Step 1 Select **Log** > **Categories**.

Step 2 Select **Expanded Categories** from the **View Style** menu in the **Log Categories** section.

Step 3 Locate the **VoIP** (**VOIP H.323/RAS, H.323/H.225, H.323/H.245 activity**) entry in the table.

Step 4 Select **Log** to enable the display of VoIP log events in on the **Log** > **View** page.

Step 5 Select **Alerts** to enable the sending of alerts for the category.

Step 6 Select **Syslog** to enable the capture of the log events into the SonicWALL security appliance Syslog.

Step 7 Click **Apply**.

Configuring SonicWALL IPS

SonicWALL Intrusion Prevention Service (IPS) provides full protection from application-level VoIP exploits. SonicWALL extends its IPS signature database with a family of VoIP-specific signatures designed to prevent malicious traffic from reaching protected VoIP phones and servers. Signature granularity allows SonicWALL IPS to detect and prevent attacks based on a global, attack group, or per-signature basis to provide maximum flexibility and control false positives. SonicWALL IPS can also be configured to block Skype VoIP traffic.

If you do not have SonicWALL IPS activated on your SonicWALL, you must purchase the SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service from a SonicWALL reseller or through your mySonicWALL.com account. If SonicWALL Intrusion Prevention Service is not activated on your SonicWALL security appliance, the **Security Services** > **Intrusion Prevention** page indicates an upgrade is required and includes a link to activate your subscription.

Activating the SonicWALL IPS FREE TRIAL

To activate a SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention Service license or try a FREE TRIAL, you need a mySonicWALL.com account and your SonicWALL security appliance must be registered at mySonicWALL.com. Creating a mySonicWALL.com account is fast, simple, and FREE. Simply complete an online registration form from your SonicWALL security appliance management interface. Registering your SonicWALL security appliance is a simple procedure done directly from the management interface.

To try a FREE TRIAL of SonicWALL IPS:

Step 1 Click the FREE TRIAL link. The **www.mySonicWALL.com** **Login** page is displayed.

Step 2 Enter your mySonicWALL.com account username and password in the User Name and Password fields, then click Submit. The **System** > **Licenses** page is displayed. If your SonicWALL is already connected to your mySonicWALL.com account, the **System** > **Licenses** page appears after you click the FREE TRIAL link.

Step 3 Click **FREE TRIAL** in the **Manage Service** column in the **Manage Services Online** table. Your SonicWALL IPS trial subscription is activated on your SonicWALL.

Configuring SonicWALL IPS

After activating SonicWALL IPS, the **Security Services** > **Intrusion Prevention** page displays the configuration settings for managing the service on your SonicWALL security appliance.

Note Refer to the *SonicWALL Intrusion Prevention Service Administrator's Guide* on the SonicWALL Web site http://www.sonicwall.com/support /documentation.html for complete product documentation.

VoIP Deployment Scenarios

SonicWALL security appliances can be deployed VoIP devices can be deployed in a variety of network configurations. This section describes the following deployment scenarios:

- Generic Deployment Scenario
- Deployment Scenario 1: Point-to-Point VoIP Service
- Deployment Scenario 2: Public VoIP Service
- Deployment Scenario 3: Trusted VoIP Service

Generic Deployment Scenario

All three of the follow deployment scenarios begin with the following basic configuration procedure:

Step 1 Enable bandwidth management on the WAN interface on **Network** > **Interfaces**.

Step 2 Configure SIP or H.323 transformations and inactivity settings on **VoIP** > **Settings**.

Step 3 Configure Firewall Access Rules on **Firewall** > **Access Rules**. An access rule is configured to enable two-way communications from the WAN to the LAN and the LAN to the WAN. For network access rules, create a WAN to LAN access rule to enable incoming calls from the WAN to the LAN. Select H.323 Call Signaling or SIP as the service.

Step 4 Configure the DHCP Server on the **Network** > **DHCP Server** page with static private IP address assignments to VoIP clients.

Step 5 Enable SonicWALL Intrusion Prevention Service to provided application-layer protection for VoIP communications on the **Security Services** > **Intrusion Prevention** page.

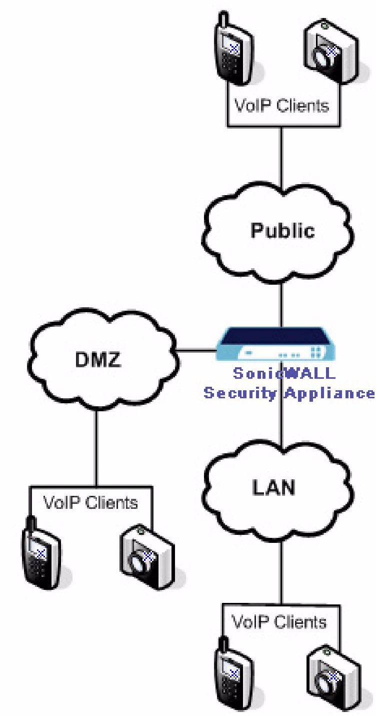
Step 6 Connect VoIP Clients to network.

Deployment Scenario 1: Point-to-Point VoIP Service

The point-to-point VoiP service deployment is common for remote locations or small office environments that use a VoIP end point device connected to the network behind the firewall to receive calls directly from the WAN. The VoIP end point device on the Internet connects to VoIP client devices on the LAN behind the firewall using the SonicWALL security appliance's Public IP address.

Figure 5 shows a point-to-point VoIP service topology.

Figure 3 Point-to-Point VoIP Service Topology.

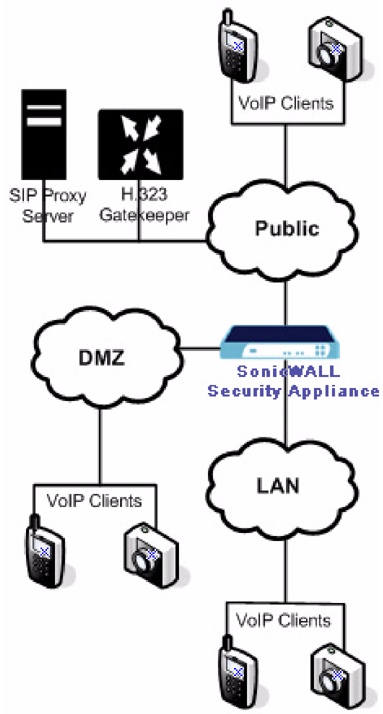


This deployment does not require a VoIP server. The Public IP address of the SonicWALL security appliance is used as the main VoIP number for hosts on the network. This requires a static Public IP address or the use of a Dynamic DNS service to make the public address available to callers from the WAN. Incoming call requests are routed through the SonicWALL security appliance using NAT, DHCP Server, and network access rules.

Deployment Scenario 2: Public VoIP Service

The Public VoIP Service deployment uses a VoIP service provider, which maintains the VoIP server (either a SIP Proxy Server or H.323 Gatekeeper). The SonicWALL security appliance public IP address provides the connection from the SIP Proxy Server or H.323 Gatekeeper operated by the VoIP service provider. Figure 5 shows a public VoIP service topology.

Figure 4 Public VoIP Service Topology.

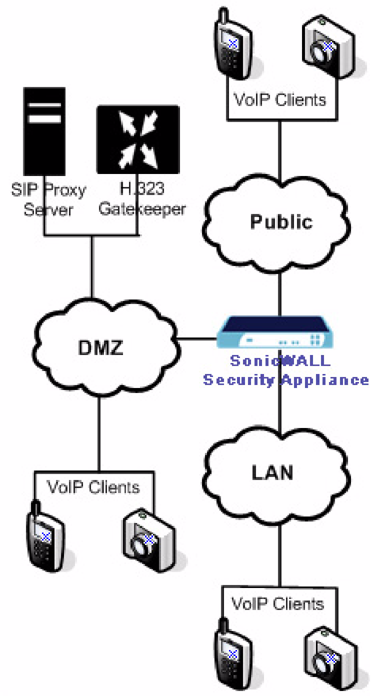


For VoIP clients that register with a server from the WAN, the SonicWALL security appliance automatically manages NAT policies and access rules. The SonicWALL security appliance performs stateful monitoring of registration and permits incoming calls for clients while they remain registered. No configuration of clients is required.

Deployment Scenario 3: Trusted VoIP Service

The organization deploys its own VoIP server on a DMZ or LAN to provide in-house VoIP services that are accessible to VoIP clients on the Internet or from local network users behind the security gateway. Figure 5 shows a trusted VoIP service topology.

Figure 5 Trusted VoIP Service Topology.



For VoIP clients that register with a server on the DMZ or LAN, the SonicWALL security appliance automatically manages NAT policies and access rules. The SonicWALL security appliance performs stateful monitoring of registration and permits incoming calls for clients while they remain registered. No configuration on the VoIP clients is required.

To make a server on the LAN accessible to clients on the WAN:

Step 1 Define a Host address object with the zone and IP address of the server.

Step 2 Define a NAT policy, mapping traffic coming to the SonicWALL security appliance’s public (WAN) IP address and VoIP service (SIP or H.323 Gatekeeper (RAS) to server.

Step 3 Define access rules allowing VoIP service to pass through the firewall.

Glossary

Consistent NAT – This SonicWALL VoIP feature ensures predictable re-use of the same translated IP address and UDP port pair for internal (LAN) address and port pairs.

Session Initiation Protocol (SIP) – A Internet Engineering Task Force (IETF) standard protocol for initiating an interactive user session that involves multimedia elements such as video, voice, chat, and gaming. SIP is a request-response protocol, dealing with requests from clients and responses from servers. It works on the Application Layer and can establish multimedia sessions or Internet telephony calls, and modify, or terminate them.

H.323 – A standard approved by the International Telecommunications Union (ITU) to promote compatibility in videoconference transmissions over IP networks. It provides a standard for interoperability in audio, video and data communications as well as VoIP because it addresses call control and management for both point-to-point and multipoint conferences as well as gateway administration of media traffic, bandwidth and user participation.

Bandwidth Management (BWM) – Refers to any of a variety of algorithms or methods used to shape traffic or police traffic. Shaping often refers to the management of ourbound traffic, while policing often refers to the management of inbound traffic. There are many different methods of bandwidth management, including various queuing and discarding techniques, each with their own design strengths. SonicWALL employes a Token Based Class Based Queuing method for inbound and outbound BWM, as well as a discard mechanism for certain types of inbound traffic. Important terminologies used within SonicWALL's BWM implementation include:

- **Inbound (Ingress or IBWM) –** The ability to shape the rate at which traffic enters a particular interface. For TCP traffic, actual shaping can occur where the rate of ingress flow can be adjusted by delaying egress acknowledgements (ACKs) causing the sender to slow its rate. For UDP traffic, a discard mechanism is used since UDP has no native feedback controls.
- **Outbound (Egress or OBWM) –** Conditioning the rate at which traffic is sent out an interface. OUtbound BWM uses a credit (or token) based queuing system with 8 priority rings to service different types of traffic, as classified by Access Rules.
- **Guaranteed Bandwidth –** A declared percentage of the total available bandwidth on an interface which will always be granted to a certain class of traffic. Applicable to both inbound and outbound BWM. The total Guaranteed Bandwidth across all BWM rules cannot exceed 100% of total available bandwidth.
- **Maximum Bandwidth –** A declared percentage of the total available bandwidth on an interface defining the maximum bandwidth to be allowed to a certain class of traffic. Applicable to both inbound and outbound BWM. Used as a throttling mechanism.
- **Priority –** An additional dimension used in the classification of traffic. SonicOS uses 8 priority rings (0=highest, 7 = lowest) to comprise the queue structure used for BWM. Queues are services in the order of their priority ring.

Document Version History

Version Number	Date	Notes
1.0	2/6/2006	This document was created.