SonicOS and SonicOSX 7 VoIP

Administration Guide

SONICWALL®

Contents

1

VoIP

NOTE: References to SonicOS/X indicate that the functionality is available in both SonicOS and SonicOSX.

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.

Topics:

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 are 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.

Security Appliance 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 Security Appliance modifies source address and source port information with Network Address Translation (NAT), it is difficult for VoIP to effectively traverse a standard Security Appliance. 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 Security Appliance processing.
- **Source and destination IP addresses are embedded within the VoIP signaling packets** - A Security Appliance supporting NAT translates IP addresses and ports at the IP header level for packets. Fully symmetric NAT Security Appliances 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 Security Appliance to perform deep packet inspection and transformation of embedded IP addresses and port information as the packets traverse the Security Appliance.
- **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 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 Security Appliance and attempts to control the border of a VoIP network by terminating and re-originating all VoIP media and signaling traffic. In essence, SBCs act as a proxy for VoIP traffic for non-VoIP enabled Security Appliances. SonicWall Security Appliances are VoIP enabled Security Appliances that eliminate the need for an SBC on your network.

ⓘ **NOTE:** VoIP is supported on all SonicWall appliances that can run SonicOS/X, as long as the VoIP application is RFC-compliant.

VoIP Protocols

VoIP technologies are built on two primary protocols: H.323 and SIP. These protocols can be applied either globally or per firewall rule.

Topics:

H.323

H.323 is a standard developed by the International Telecommunications Union (ITU). It is 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

IMPORTANT: If Wireless-Controller-Only mode has been selected for Wireless LAN Controller, VOIP is disabled.

Topics:

VoIP Security

- **Traffic legitimacy** - Stateful inspection of every VoIP signaling and media packet traversing the Security Appliance 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.
- **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.
- **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.
- **Stateful monitoring** - Stateful monitoring ensures that packets, even though appearing valid in themselves, are appropriate for the current state of their associated VoIP connection.

- **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.
- **Application-layer protection** - SonicWall delivers full protection from application-level VoIP exploits through SonicWall Intrusion Prevention Service (IPS). SonicWall IPS is built on a configurable, high performance Deep Packet Inspection engine that provides extended protection of key network services including VoIP, Windows services, and DNS. The extensible signature language used in SonicWall's Deep Packet Inspection engine also provides proactive defense against newly discovered application and protocol vulnerabilities. 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.

VoIP Network

- **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.

  NOTE: SonicWall's Secure Wireless Solution includes the network enablers to extend secure VoIP communications over wireless networks.
- **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 to provide predictability that is vital for certain types of applications.
- **WAN Redundancy and Load Balancing** - WAN redundancy and load balancing allows for an interface to act as a secondary WAN port. This secondary WAN port can be used in a simple active/passive setup, where traffic is only routed through it if the primary WAN port is down or unavailable. Load balancing can be performed by splitting the routing of traffic based on destination.
- **High Availability** - High availability is provided by SonicOS/X high availability, which ensures reliable, continuous connectivity in the event of a system failure.

VoIP Network Interoperability

- **Plug-and-protect support for VoIP devices** - With SonicOS/X, 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 Security Appliance.
- **Full syntax validation of all VoIP signaling packets** - Received signaling packets are fully parsed within SonicOS/X to ensure they comply with the syntax defined within their associated standard. By performing syntax validation, the Security Appliance can ensure that malformed packets are not permitted to pass through and adversely affect their intended target.
- **Support for dynamic setup and tracking of media streams** - SonicOS/X 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 Security Appliance. Subsequent calls, even between the same parties, uses different ports, thwarting an attacker who might 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 Security Appliance.

- **Validation of headers for all media packets** - SonicOS/X 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.
- **Configurable inactivity timeouts for signaling and media** - In order to ensure that dropped VoIP connections do not stay open indefinitely, SonicOS/X 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.
- **SonicOS/X 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/X 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.
- **Comprehensive monitoring and reporting** - For all supported VoIP protocols, SonicOS/X 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 Security Appliance. Reports can be generated about virtually any aspect of Security Appliance activity, including individual user or group usage patterns and events on specific Security Appliances or groups of Security Appliances, types and times of attacks, resource consumption and constraints.

Supported Interfaces

VoIP devices are supported on the following SonicOS/X zones:

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

Supported VoIP Protocols

Topics:

H.323

SonicOS/X 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 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/X 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/X 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

Partial list of devices with which SonicWall VoIP interoperates lists many devices from leading manufacturers with which SonicWall VoIP interoperates.

H.323	SIP
Soft-Phones: • Avaya • Microsoft NetMeeting • OpenPhone • PolyCom • SJLabs SJ Phone Telephones/VideoPhones: • Avaya • Cisco • D-Link • PolyCom • Sony Gatekeepers: • Cisco • OpenH323 Gatekeeper Gateway: Cisco	Soft-Phones: • Apple iChat • Avaya • Microsoft MSN Messenger • Nortel Multimedia PC Client • PingTel Instant Xpressa • PolyCom • Siemens SCS Client SJLabs • SJPhone • XTen X-Lite • Ubiquity SIP User Agent Telephones/ATAs: • Avaya • Cisco • Grandstream BudgetOne • Mitel • Packet8 ATA • PingTel Xpressa PolyCom • PolyCom • Pulver Innovations WiSIP • SoundPoint SIP Proxies/Services: • Cisco SIP Proxy Server • Brekeke Software OnDo SIP Proxy • Packet8 • Siemens SCS SIP Proxy • Vonage

CODECs

- **SonicOS/X 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 on which SonicOS/X Does Not Perform Deep Packet Inspection

SonicWall network Security Appliances 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.)

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.

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 is ultimately 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/X 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.

How SonicOS/X Handles VoIP Calls

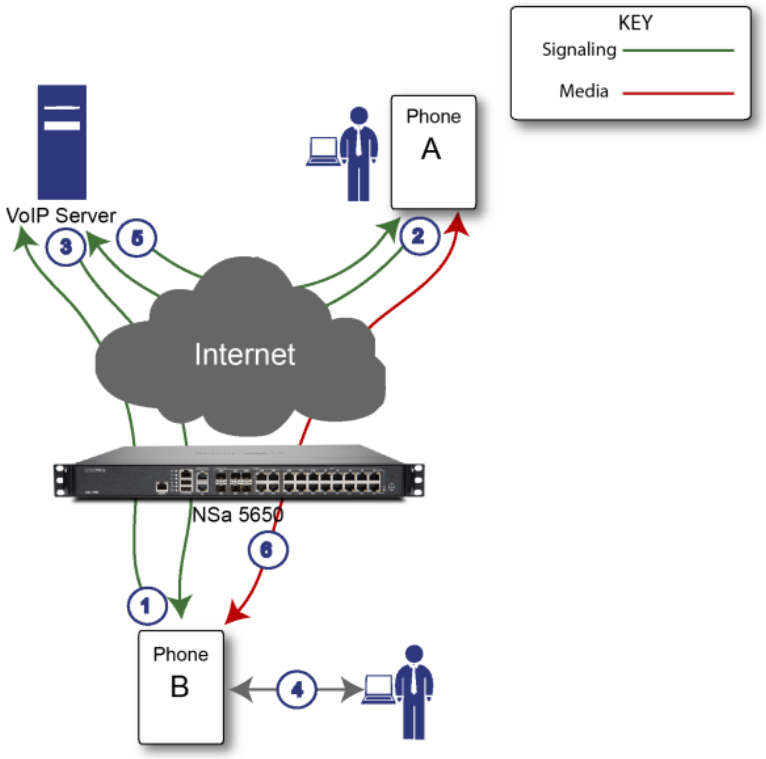
SonicOS/X provides an efficient and secure solution for all VoIP call scenarios. The following are examples of how SonicOS/X handles VoIP call flows:

- Incoming Calls
- Local Calls

Incoming Calls

Incoming Call Sequence of Events shows the sequence of events that occurs during an incoming call.

INCOMING CALL SEQUENCE OF EVENTS



The following describes the sequence of events shown in Incoming Call Sequence of Events:

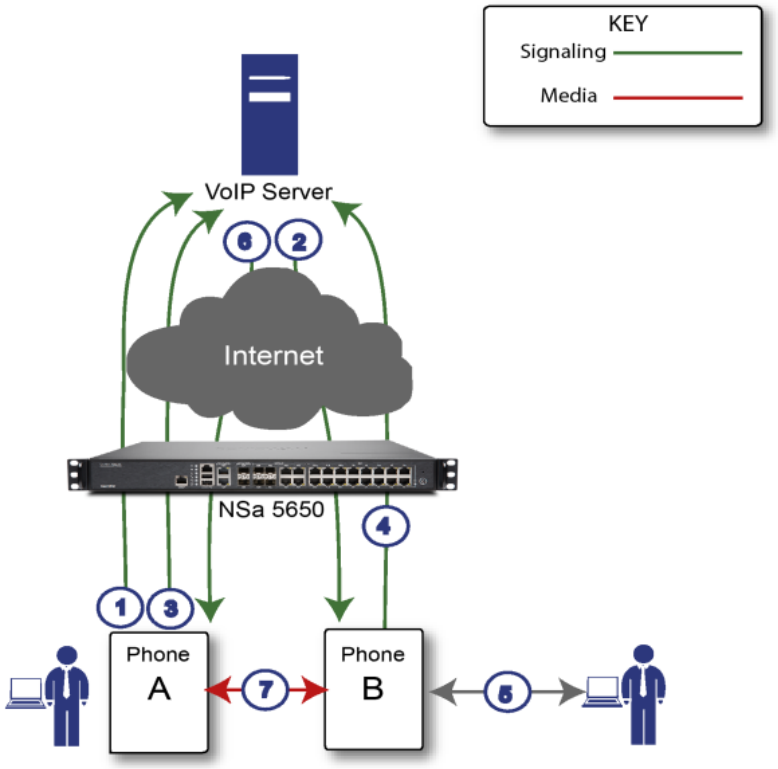
1. **Phone B registers with VoIP server** - The Security Appliance builds a database of the accessible IP phones behind it by monitoring the outgoing VoIP registration requests. SonicOS/X translates between phone B's private IP address and the Security Appliance's public IP address used in registration messages. The VoIP server is unaware that phone B is behind a Security Appliance and has a private IP address—it associates phone B with the Security Appliance'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 Security Appliance's public IP address. When it reaches the Security Appliance, SonicOS/X validates the source and content of the request. The Security Appliance 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/X translates this private IP information to use the Security Appliance'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 Security Appliance, as it was given the public address of the Security Appliance by the VoIP Server.
6. **Phone A and phone B exchange audio/video/data through the VoIP server** - Using the internal database, SonicOS/X ensures that media comes from only Phone A and is only using the specific media streams permitted by Phone B.

Local Calls

Local VoIP Call Sequence of Events shows the sequence of events that occurs during a local VoIP call.

LOCAL VOIP CALL SEQUENCE OF EVENTS



The following describes the sequence of events shown in Local VoIP Call Sequence of Events:

1. **Phones A and B register with VoIP server** - The Security Appliance builds a database of the accessible IP phones behind it by monitoring the outgoing VoIP registration requests. SonicOS/X translates between the phones' private IP addresses and the Security Appliance's public IP address. The VoIP server is unaware that the phones are behind a Security Appliance. It associates the same IP address for both phones, but different port numbers.
2. **Phone A initiates a call to phone B by sending a request to the VoIP server** - Even though they are behind the same Security Appliance, phone A does not know Phone B's IP address. Phone A initiates a call to phone B using a phone number or alias.
3. **VoIP Server validates the call request and sends the request to phone B** - The VoIP server sends the call request to the Security Appliance's public IP address. The Security Appliance then determines phone B's private IP address.

4. **Phone B rings and is answered** - When phone B is answered, the Security Appliance translate its private IP information to use the Security Appliance's public IP address for messages to the VoIP server.
5. **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/X back to the private addresses and ports for phone A and phone B.
6. **Phone A and phone B directly exchange audio/video/data** - The 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 Security Appliance to perform address translation.

2

Settings

Configuring the settings for your SonicWall network security appliance for VoIP deployments builds on your basic network configuration in the SonicWall Management Interface. This section assumes your network security appliance is configured for your network environment.

NOTE: For general information on VoIP, see VoIP.

Topics:

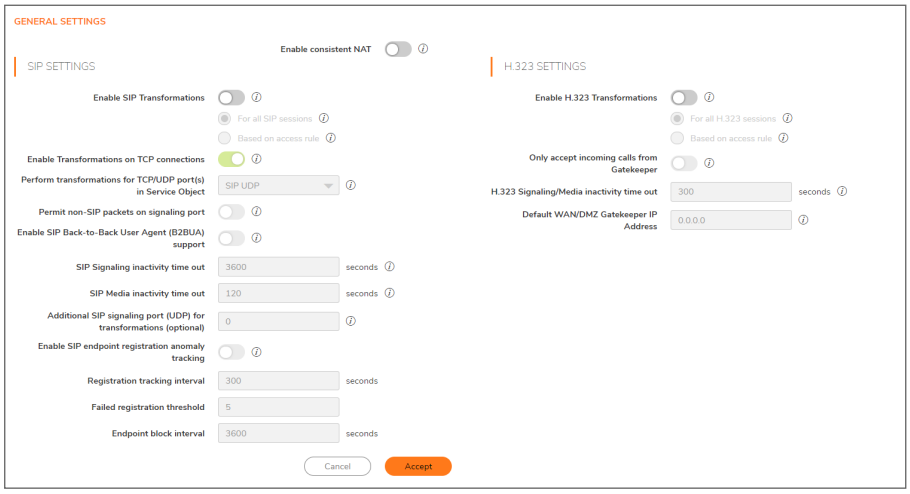
- Configuring VoIP Settings
- Configuring VoIP Logging

Configuring VoIP Settings

IMPORTANT: If Wireless-Controller-Only mode has been selected for Wireless LAN Controller, any attempt to enable SIP and/or H.323 options displays an error message in the lower right corner of the browser window.

Configure VoIP through **NETWORK | VoIP > Settings**. This page is divided into three sections:

- General Settings
- SIP Settings
- H.323 Settings



General Settings

There is one option under **General Settings: Enable Consistent 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 shown in IP address and port pairs.

IP ADDRESS AND PORT PAIRS

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 IP address and port pairs result in using the same translated address and port pairs. Without Consistent NAT, the port and possibly the IP address change with every request.

ⓘ **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.

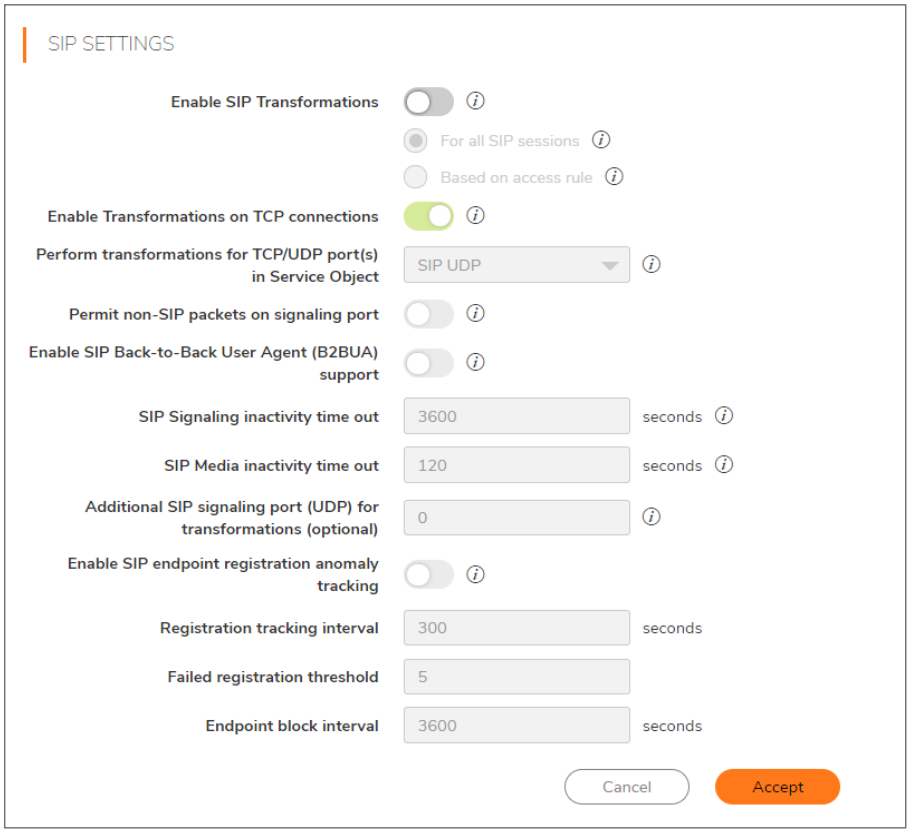
ⓘ **IMPORTANT:** For Consistent NAT to work properly, the minimum time interval between calls must be at least 200 msec.

Enabling Consistent NAT

To enable consistent NAT:

1. Select the **Enable Consistent NAT** option. This option is not selected by default.
2. Click **Accept**.

SIP Settings



By default, SIP clients use their private IP address in the SIP (Session Initiation Protocol) 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 firewall and the SIP clients are located on the private (LAN) side of the firewall, the SDP messages are not translated and the SIP proxy cannot reach the SIP clients.

Enabling SIP

To enable SIP:

1. Navigate to **NETWORK | VOIP > Settings**.
2. In the **SIP Settings** section, choose whether to enable SIP transformation globally or by firewall rule:
   - **Use global control to enable SIP Transformations**. This option is selected by default.
   - **Use firewall Rule-based control to enable SIP Transformations**. Be sure to configure a firewall rule to control SIP transformations as described in SonicOS/X Policies.
3. If you are not configuring SIP transformations, go to Step 12.
4. **Enable SIP Transformations** is not selected by default. Select this option to:
   - Transform SIP messages between LAN (trusted) and WAN/DMZ (untrusted).

     You need to check this setting when you want the Security Appliance to do the SIP transformation. If your SIP proxy is located on the public (WAN) side of the Security Appliance 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 Security Appliance.
   - Enable the Security Appliance to go through each SIP message and change the private IP address and assigned port.
   - Control and open up the RTP/RTCP ports that need to be opened for SIP session calls to happen.

NAT translates Layer 3 addresses, but not 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 select **Enable SIP Transformations** 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.

When Enable SIP Transformations is selected, the other options become available.

5. To perform SIP transformations on TCP-based SIP sessions, select **Enable SIP Transformation on TCP connections**. This option is selected by default.
6. Select a Service Object from Perform transformations to **TCP/UDP port(s) in Service Object**. The default is SIP.
7. 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. This option is not selected by default.

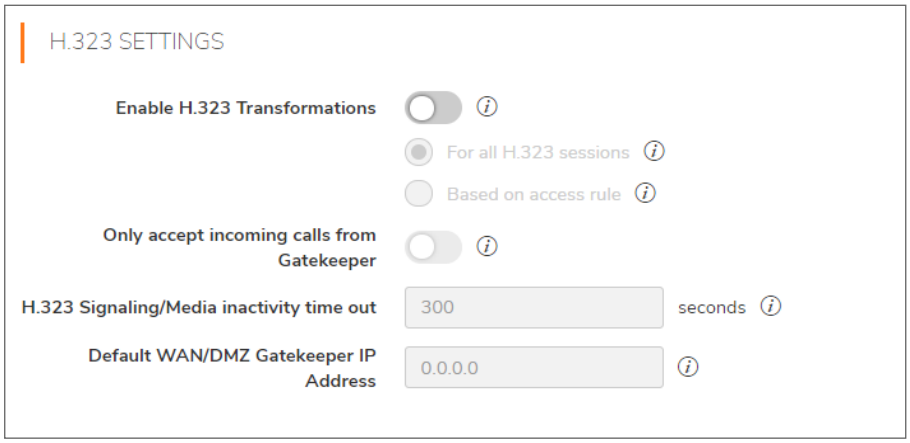
   ⓘ **IMPORTANT:** Enabling this checkbox might open your network to malicious attacks caused by malformed or invalid SIP traffic.
8. If the SIP Proxy Server is being used as a B2BUA, enable the **Enable SIP Back-to-Back User Agent (B2BUA) support** setting. This option is disabled by default and should be enabled only when the Security Appliance can see both legs of a voice call (for example, when a phone on the LAN calls another phone on the LAN).

TIP: If there is no possibility of the firewall seeing both legs of voice calls (for example, when calls are only 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.

9. Use the **SIP Signaling inactivity time out (seconds)** and **SIP Media inactivity time out (seconds)** options to define the amount of time a call can be idle (no traffic exchanged) before the firewall blocks further traffic. A call goes idle when placed on hold. Specify the maximum idle time when:
   - There is no signaling (control) message being exchanged in **SIP Signaling inactivity time out**. The minimum time is 30 seconds, the maximum time is 1000000 seconds (~1.2 days) and the default is 3600 seconds (60 minutes).
   - No media (for example, audio or video) packets are being exchanged in the SIP Media inactivity time out. The minimum time is 30 seconds, the maximum time is 3600 seconds (1 hour), and the default time is 120 seconds (2 minutes).
10. Use the **Additional SIP signaling port (UDP) for transformations** setting to specify a non-standard UDP port 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. When this setting is non zero (0 is the default; the maximum value is 65535), the Security Appliance performs SIP transformation on these non-standard ports.

    TIP: Vonage's VoIP service uses UDP port 5061.
11. To track SIP endpoint registration anomalies, select the **Enable SIP endpoint registration anomaly tracking** option. This option is not selected by default. When it is selected, these options become available:
    - **Registration tracking interval (seconds)** – Specify the interval between checking for anomalies. The default is **300** seconds (5 minutes).
    - **Failed registration threshold** – Specify the number of failed registrations before checking for anomalies. The default is **5** failures.
    - **Endpoint block interval (seconds)** – The default is **3600** (60 minutes).
12. Either:
    - Click **Accept**.
    - Go to H.323 Settings.

H.323 Settings



Configuring H.323 Settings

To configure H.323 settings:

1. Navigate to **NETWORK | VoIP > Settings | H.323 Settings**.
2. Choose whether to enable H.323 transformation globally or by firewall rule:
   - **Use global control to enable H.323 Transformations**. This option is selected by default.
   - **Use firewall Rule-based control to enable H.323 Transformations**. Be sure to configure a firewall rule to control H.323 transformations.
3. If you are not configuring H.323 transformations, go to Step 5.
4. Select **Enable H.323 Transformation** to allow stateful H.323 protocol-aware packet content inspection and modification by the firewall. This option is disabled by default. When the option is selected, the other H.323 options become active.

   The firewall 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 firewall.
5. Select **Only accept incoming calls from Gatekeeper** to ensure all incoming calls go through the Gatekeeper for authentication. The Gatekeeper refuses calls that fail authentication.
6. In the **H.323 Signaling/Media inactivity time out (seconds)** field, specify the amount of time a call can be idle before the firewall blocks further traffic. A call goes idle when placed on hold. The default time is **300** seconds (5 minutes), the minimum time is 60 seconds (1 minute), and the maximum time is 122400 seconds (34 hours).
7. 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 `225.0.1.41`. If you do not enter an IP address, multicast discovery messages from LAN-based H.323 devices go through the configured multicast handling.
8. Click **Accept**.

Topics:

Configuring Bandwidth on the WAN Interface

ⓘ **NOTE:** For information on Bandwidth Management (BWM) and configuring BWM on the WAN interface, see SonicOS/X POLICY Guide.

Configuring VoIP Access Rules

By default, stateful packet inspection on the firewall 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.

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

NOTE: You must select Bandwidth Management on **NETWORK | System > Interfaces** for the WAN interface before you can configure bandwidth management for network access rules.

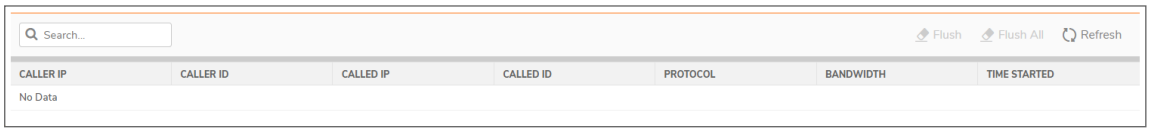
Configuring VoIP Logging

You can enable the logging of VoIP events, which are displayed on **DEVICE | Log > Settings**.

3

Call Status

The **NETWORK | VoIP > Call Status** page allows you to monitor all currently active VoIP calls. Use the **Search** feature to locate specific entries.



The VoIP Call Status table displays the following information about the active VoIP connection:

- **Caller IP** – the IP address of the device from which the call was initiated
- **Caller-ID** – the unique identifier for each initiated call
- **Called IP** – the IP address of the device on which the call was received
- **Called-ID** – the unique identifier for each received call
- **Protocol** – the type of protocol used by the call
- **Bandwidth** – the amount of bandwidth in megabits per second (Mbps) used by the call
- **Time Started** – the date and time that the call began

You can see the caller and called information as well as how long the call has been in progress and the bandwidth used. Both active H.323 and SIP calls are shown on the VoIP Call Status page.

H.323 Transformations and SIP Transformations must be enabled on the **NETWORK | VoIP > Settings** page for the corresponding calls to be shown. Only when these options are enabled does SonicOS/X inspect the VoIP payload to track call progress.

To reset the connections for all the active calls in progress, click **FLUSH ALL**. This also removes all VoIP call entries from the table.

4

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://www.sonicwall.com/support.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View and participate in the Community forum discussions at https://community.sonicwall.com/technology-and-support.
- View video tutorials
- Access https://mysonicwall.com
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit https://www.sonicwall.com/support/contact-support.

About This Document

NOTE: A NOTE icon indicates supporting information.

IMPORTANT: An IMPORTANT icon indicates supporting information.

TIP: A TIP icon indicates helpful information.

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

SonicOS and SonicOSX VoIP Administration Guide
Updated - August 2020
Software Version - 7
232-005354-00 Rev B

End User Product Agreement

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/en-us/legal/license-agreements.

Open Source Code

SonicWall Inc. is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035