Beyond Interoperability: Network Security as a Voice over IP (VoIP) Enabler

This whitepaper examines the issues and complexities of deploying a secure VoIP network, then details SonicWALL's total VoIP solution.

CONTENTS

Abstract

Companies implementing Voice over IP (VoIP) technologies in an effort to cut communications costs should not overlook the security risks associated with a converged voice and data network. Tempted by the benefits of lower phone bills, centralized management and rapid deployment, the critical areas of VoIP security and network integrity are often neglected.

There are numerous threat targets to consider in a VoIP network—the call servers and their operating systems, the phones and their software, and even the phone calls themselves are vulnerable.

This whitepaper examines the issues and complexities of deploying a secure VoIP network, and then details SonicWALL's total VoIP solution, featuring SonicWALL's innovative stateful packet transformation technology.

Issues with VoIP and Network Security

The traditional role of the firewall* in a VoIP network is undergoing a radical evolution. In the past, the primary role of the firewall was simply to behave well in the VoIP environment. Where VoIP relies on predictable, static availability of IP-based resources across the Internet, the firewall's network address translation (NAT) functionality inherently breaks the VoIP network. Through 'pin-holing' and other techniques, security vendors have found ways to largely interoperate with VoIP infrastructures.

As network-based threats have become more sophisticated, however, the role of the firewall has evolved from 'behaving nicely' in a VoIP environment to fully enabling and protecting the complete infrastructure. From end-user devices such as IP-based phones, soft-phones and wireless communications devices, to infrastructure equipment such as H.323 Gatekeepers and SIP Proxy Servers, there is a tremendous amount of exposure in an organization-wide VoIP deployment. From simple denial of service (DoS) attacks aimed at limiting availability to the IP-based voice infrastructure, to full-blown application-layer attacks targeting the VoIP protocols themselves, the threats are very real…and growing.

For any successful VoIP implementation, three key factors must be considered:

- VoIP security
- VoIP network interoperability and protocol support
- VoIP vendor interoperability

The following sections describe these areas.

**For this paper, we use the word "firewall" to describe any security device that provides a perimeter security function for VoIP. In reality, modern security devices have transcended the stateful inspection firewall, and now feature deep packet inspection technologies that significantly enhance their capabilities.*

VoIP security

VoIP security encompasses many areas, but the major factors that must be considered in any deployment are Access, Availability and Implementation.

Access

VoIP calls are vulnerable to threats such as session hijacking and ‘man-in-the-middle’ attacks. Without proper safeguards, an attacker could intercept a VoIP call and modify the call parameters/addresses. This would open the call up for spoofing, identity theft, call redirection and other attacks.

Even without modifying VoIP packets, attackers may be able to eavesdrop on telephone conversations being carried over a VoIP network. If VoIP packets are traveling unprotected over the Internet, they provide attackers the opportunity to access the information they carry.

With a standard public switched telephone network (PSTN) connection, intercepting conversations requires physical access to telephone lines or access to the private branch exchange (PBX). Voice/data networks, which typically use the public Internet and the TCP/IP protocol stack, do not provide the same ‘physical wire’ security as telephone lines. By gaining access and monitoring network traffic at certain parts on a network infrastructure (such as to/from a VoIP gateway), an attacker could capture and reassemble VoIP packets. Publicly available tools such as Vomit (http://vomit.xtdnet.nl/) can be used to convert these packets into a .wav file, allowing an attacker to eavesdrop, or even record and replay conversations.

Availability

The availability of a VoIP network is also a major concern. PSTN availability has reached 99.999%—attackers would need physical access to telephone exchanges or cut phone lines to create any impact. However, a simple DoS attack aimed at key points of an unprotected VoIP network would disrupt, or worse cripple, voice and data communications.

VoIP networks are especially susceptible to DoS attacks such as:

- Malformed request DoS
  Carefully crafted protocol requests can be used to exploit a known vulnerability resulting in a partial or complete loss of service. These may be used not only to crash the target but also to gain control over it.

- DoS on media
  VoIP media is carried within Real-Time Protocol (RTP) packets, and is vulnerable to any attack that congests the network or slows the ability of an end device (phone or gateway) to process the packets in real time.

  An attacker who has access to the portion of the network where media is present simply needs to inject large numbers of media packets or high Quality of Service (QoS) packets, which will contend with the legitimate media packets.

- Load-based DoS

  A DoS attack does not necessarily need to use malformed packets to achieve its goal. Flooding a target with legitimate requests can easily overwhelm a poorly designed system.

  Even without an actual VoIP request, a DoS attack such as TCP SYN Flood can prevent a device from being able to accept calls for long periods of time.

Implementation Problems

VoIP encompasses a large number of standards – such as Session Initiation Protocol (SIP), H.323, Media Gateway Control Protocol (MGCP) and H.248. These are complex standards that leave the door open for bugs within the software implementation. With the PSTN, telephones are simply ‘dumb terminals’ – all the logic and intelligence resides within the PBX. There is not a lot that an attacker can do to disrupt access to the PSTN network.

However with VoIP, the same types of bugs and exploits that hamper every operating system and application available today also apply to VoIP equipment. Remember that many of today’s VoIP call servers and gateway devices are built on vulnerable Windows and Linux operating systems. One has to only look at the CERT advisories that have been issued for H.323 [CERT-H.323] or SIP [CERT-SIP] to see the large number of vulnerabilities that have been found and the dozens of vendors affected by them.

VoIP network interoperability and protocol support

VoIP is more complicated than a standard TCP/UDP-based application. 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 NAT, it is difficult for VoIP to effectively traverse a firewall. Here are a few of the reasons why.

- VoIP operates using two sets of protocols – signaling (between the client and VoIP Server) and media (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 deep-inspect 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. Worse still, 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 which consist of different formats of messages used by different VoIP systems. Just because two vendors use the same protocol suite does not necessarily mean they will interoperate.

VoIP vendor interoperability

Some VoIP vendors have slightly different implementations of the standard VoIP protocols based on RFCs, not all of which are compatible. Furthermore, some vendors implement “standard-compatible” proprietary VoIP protocols. Because of this, it is important for the firewall to interoperate with as wide a range of VoIP end devices and call servers as possible.

In the end, it is the responsibility of the individual vendors to ensure they are compatible with each others’ devices. SonicWALL spends a tremendous amount of time and effort in this area. A partial list of devices that SonicWALL interoperates with is listed later in this document.

Current Solutions for VoIP Security

There are many approaches for securing the VoIP infrastructure. The following table provides a summary of the major approaches.

Solution	Advantages	Disadvantages
No Firewall (or VoIP unaware firewall)	▪ Does not affect IP voice and video applications	▪ No network security at all ▪ Endpoints need public IP address ▪ Endpoints accessible by anyone
NAT Traversal solutions that 'bypass' the firewall (such as STUN [IETF-STUN])	▪ No firewall upgrade/change needed	▪ No/limited network security on 'open' ports—VoIP devices still exposed ▪ Will not work through symmetric NAT [IETF-TURN] ▪ Works only for UDP—will not support H.323 or SIP over TCP ▪ RTCP may not work (as the port number it uses is tightly-coupled to that used for RTP)
Session Border Controllers	▪ No firewall upgrade/change needed	▪ Limited-term solution [NWFUSION-SBC] ▪ Primarily designed for service providers ▪ Additional administrative overhead—another 'box' to manage ▪ May require client software to be installed on each network—becoming bottleneck/introducing jitter as VoIP endpoints must direct all traffic (signaling and media) through it ▪ Centralized approaches means carrier responsible for VoIP security—no longer under company control
Full VoIP Proxy	▪ No firewall upgrade/change needed	▪ Proxy is still exposed to attack ▪ Separate proxy may be needed for each VoIP protocol ▪ Proxy needed behind each firewall ▪ May need to deploy in pairs for high availability ▪ Adds additional latency and can become bottleneck or introduce jitter
SonicWALL Stateful Packet Transformation	▪ Protects signaling and media ▪ Ease of use—'plug and protect' technology ▪ No additional equipment required—uses existing 'current' generation SonicWALL firewalls ▪ Supports multiple VoIP protocols ▪ Multi-vendor VoIP device interoperability	▪ Not supported on previous generation firewalls

The SonicWALL Approach

SonicWALL provides a complete solution for VoIP that offers unparalleled levels of security for the VoIP infrastructure, standards-based VoIP compatibility, and interoperability with many of the world's leading VoIP gateway and communications devices.

All SonicWALL TZ 170 and PRO Series (Gen 4) security appliances feature the same comprehensive level of VoIP security as described in this paper. This is important because the overall integrity of the VoIP network is only as good as the weakest link, necessitating the highest levels of protection…even at the home office and on personal communications devices.

SonicWALL security appliances featuring either SonicOS Standard or Enhanced firmware have built-in VoIP capabilities. With SonicOS Enhanced, the user gets additional call monitoring and reporting functionality, as well as more comprehensive QoS support (e.g., inbound bandwidth management).

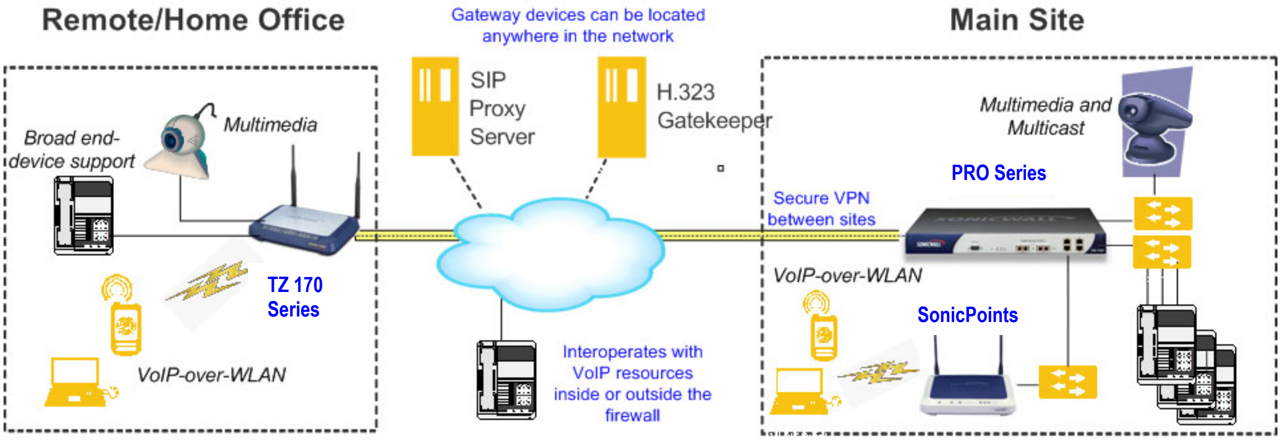


Figure 1
SonicWALL VoIP Approach

The following capabilities, which are detailed in the following sections of this paper, comprise the core of the SonicWALL VoIP implementation:

- Stateful packet inspection and transformation during the entire lifetime of a VoIP call:
    - Call registration
    - Call setup/teardown
    - Media exchange
- Security
    - VoIP intrusion prevention, anti-virus, content filtering
    - VoIP over WLAN, with full threat prevention capabilities
    - Detection and discarding malformed packets
    - Enforce 'closed' VoIP network—prevent unauthorized calls

- Architecture
  - Support for streaming media and multicast applications
  - Any mix of devices can be located in ANY zone (H.323 and SIP endpoints, H.323 gatekeeper, H.323 multipoint control unit, SIP proxy and redirect server)
  - Gatekeepers and proxies can be located anywhere in the network…even the DMZ
  - Fully symmetric NAT
- Extensive reporting
  - Call tracking
  - Logging ‘abnormal’ packets
  - Troubleshooting and debugging simplified

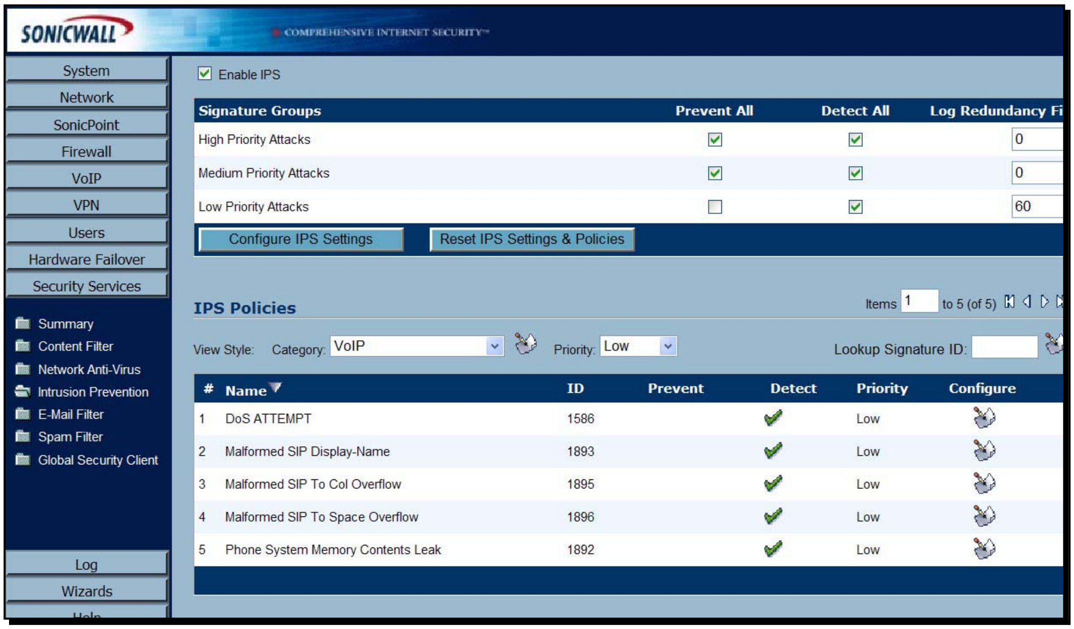
SonicWALL VoIP security

SonicWALL’s powerful deep inspection technology provides a flexible framework for inspecting and enforcing traffic at all points in the VoIP infrastructure.

VoIP Servers and Endpoints

- Traffic legitimacy
  Stateful inspection of each and 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 is able to detect and discard malformed and invalid packets before ever reaching 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, ultra-high performance scanning engine with a dynamically updated and provisioned database of over 1,800 attack and vulnerability signatures to protect networks against even the most sophisticated Trojans and polymorphic threats. SonicWALL has extended its IPS signature database with a family of VoIP-specific signatures designed to prevent malicious traffic from reaching protected VoIP phones and servers.



☑ Enable IPS

Signature Groups	Prevent All	Detect All	Log Redundancy Fi
High Priority Attacks	☑	☑	0
Medium Priority Attacks	☑	☑	0
Low Priority Attacks	□	☑	60

IPS Policies

Items 1 to 5 (of 5)

View Style: Category: VoIP Priority: Low Lookup Signature ID:

#	Name	ID	Prevent	Detect	Priority	Configure
1	DoS ATTEMPT	1586		✓	Low	
2	Malformed SIP Display-Name	1893		✓	Low	
3	Malformed SIP To Col Overflow	1895		✓	Low	
4	Malformed SIP To Space Overflow	1896		✓	Low	
5	Phone System Memory Contents Leak	1892		✓	Low	

Figure 2
SonicWALL IPS GUI

- 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.
  - Validation of the packet sequence for VoIP signaling packets using TCP. Out of sequence and retransmitted packets beyond window are disallowed.
  - 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, replay and data insertion attacks are prevented.
  - SYN Flood protection 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).
- Stateful monitoring
  Stateful monitoring ensures that packets, even though appearing valid in themselves, are appropriate for the current state of their associated VoIP connection.

- SonicWALL Anti-Virus
  SonicWALL Anti-Virus products protect soft-phone clients from virus-based threats, and auto-enforces virus definition DAT files. This dramatically reduces the time and costs associated with administering an antivirus policy throughout an entire network.

VoIP conversations

- Seamless support of encrypted media
  A number of VoIP devices are capable of using encryption to protect the media exchange within a VoIP conversation from eavesdropping and replay.
- Strong authentication and encryption

  SonicWALL's ICSA certified site-to-site and remote access IPSec VPNs provide cost-effective, reliable and secure remote access to network resources for remote users, telecommuters, and branch offices. When used in conjunction with a robust authentication service, it provides strong authentication of VPN users across the Internet using Public Key Infrastructure (PKI) and digital certificates.

  For securing VoIP devices that do not support encrypted media, IPSec VPNs provide a complete solution for ensuring the privacy of VoIP calls.

The VoIP network

- VoIP over Wireless LAN (WLAN)
  SonicWALL extends complete VoIP security to attached wireless networks with its Distributed Wireless Solution. Whether using a TZ 170 Series appliance with built-in 802.11 wireless access, or a PRO Series appliance with SonicPoint 802.11a/b/g satellite access points, all of the security features and benefits provided to VoIP devices attached to a wired network behind a SonicWALL are also provided to VoIP devices using a wireless network.
- Availability and call quality through bandwidth management
  Bandwidth management (both ingress and egress) can be used to ensure that bandwidth remains available for time-sensitive VoIP traffic. By continually monitoring and managing the bandwidth available, SonicOS can ensure that VoIP devices have available bandwidth for calls.
- WAN redundancy and load balancing
  WAN redundancy and load balancing allows for an interface to act as a secondary or back-up WAN port. This secondary WAN port can be used in a simple active/passive setup, where traffic is only routed through only if the primary WAN port is down and/or unavailable. The secondary WAN port can also be used in a more dynamic active/active setup, where outbound traffic flows are divided between the primary and secondary WAN ports for increased throughput.
- High availability
  High availability is provided by SonicOS hardware failover which ensures reliable, continuous connectivity in the event of a system failure.

SonicWALL VoIP Network Interoperability and Protocol Support

SonicWALL VoIP Network Interoperability

SonicOS efficiently and effectively decapsulates, decodes, validates, transforms as necessary, tracks and monitors all VoIP signaling traffic while at the same time validating and fast tracking VoIP media traffic to provide an industry-leading level of security and ease of use.

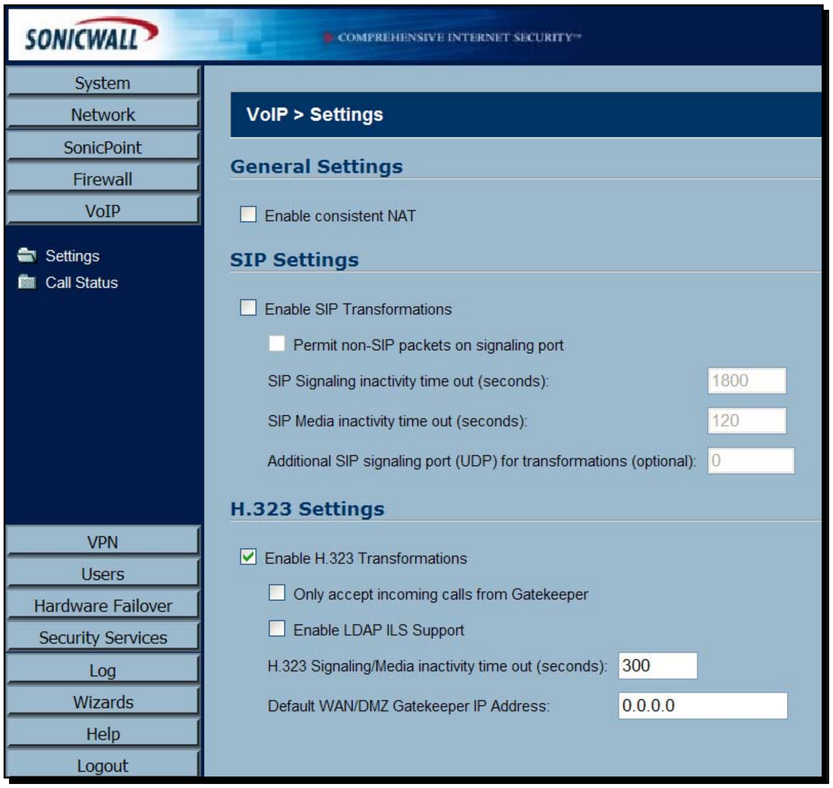
- 'Plug-and-protect' support for VoIP devices
  Using advanced monitoring and tracking technology, a VoIP device is automatically protected as soon as it is plugged into the network behind a SonicWALL security appliance.

  SonicWALL has eliminated the need for continual firewall reconfiguration, as required by some other vendors. With SonicOS, VoIP device adds, changes, and removals are handled automatically, ensuring that no VoIP device is left unprotected.

- 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.

  This is a key difference between SonicWALL and other firewall vendors who claim to support VoIP. In some cases, these vendors are simply opening up ports—without any regard for the traffic that flows through them. In other cases, a few fields are checked—primarily those that are likely to be modified as part of the NAT process and the rest simply ignored.

  SonicWALL performs high-performance **complete** packet validation for each and every signaling packet.



VoIP > Settings

General Settings

□ Enable consistent NAT

SIP Settings

□ Enable SIP Transformations

□ Permit non-SIP packets on signaling port

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

Figure 3
VoIP GUI Settings

- 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.

  Other security vendors use static mappings for the media ports and in some cases leave them open—even when not in a call. This approach unnecessarily exposes the VoIP devices to attackers, and puts the rest of the IP infrastructure at risk.

- 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.

  This is another key differentiator between SonicWALL and other security vendors. 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 monitors the usage of signaling and media streams associated with a VoIP session. Streams that are idle (i.e., no packet exchanged) for more than the configured timeout are shut down to prevent potential security holes.

- 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.

- 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

- 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.

SonicWALL VoIP Protocol Support

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
- Aside from 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)
- 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

SIP

SonicOS provides the following support for SIP:

- Devices using the following standards:
    - 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 interoperates.

H.323

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	

SIP

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	

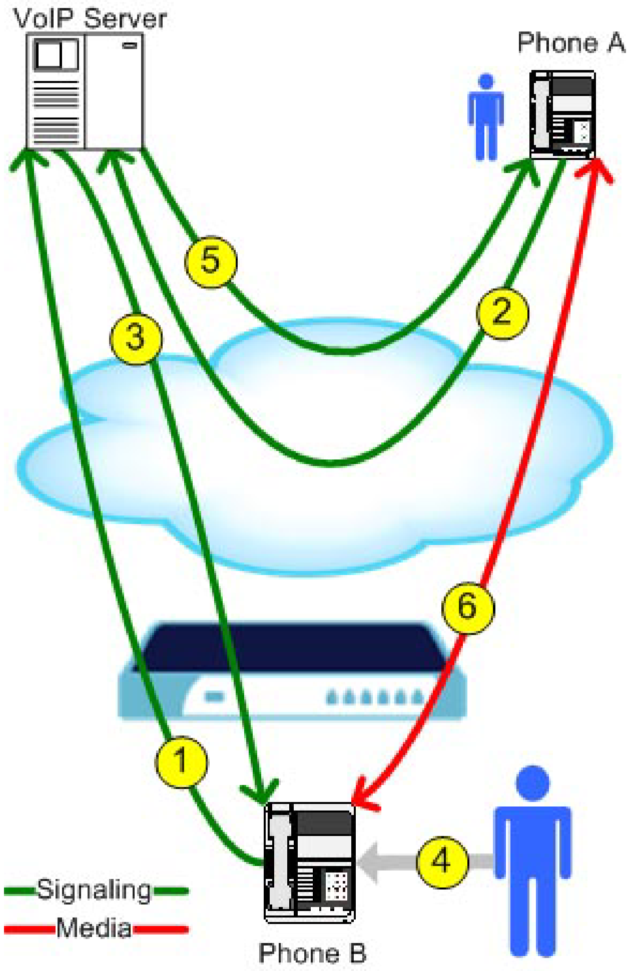
Example VoIP Call Flows

The following are some examples of VoIP call flows that other solutions may not support, or only support inefficiently.

SonicOS provides an efficient and secure solution for all VoIP call scenarios.

Incoming Calls

The following sequence illustrates how SonicOS handles an incoming call:



1. Phone B registers with VoIP Server.

By monitoring the outgoing VoIP registration requests, SonicOS is able to build an internal database of the accessible IP phones behind it. SonicOS translates between Phone B private IP address and the public firewall address within 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 public IP address.

2. Some time later, Phone A initiates a call to Phone B by sending a request to the VoIP Server. Phone A does not know how to reach Phone B—it just has an alias or phone number for Phone B. As part of the call request, Phone A provides the VoIP Server with details of the media types and formats it is able to handle, together with the associated IP addresses and ports for them.

3. VoIP Server validates the call request and sends the request to Phone B.

The incoming call request is sent to the firewall public IP address by the VoIP Server. When it reaches the firewall, SonicOS validates the source and content of the request. Based on the (public) IP address information contained within the request, a database lookup is performed to determine the private address to which to send the request.

SonicOS translates between public firewall address and Phone B private IP address within call request messages.

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 is able to handle together with the associated IP addresses and ports for them. SonicOS translates this private IP information to use the public firewall address for messages going back to the VoIP Server. This media information is also included within the internal database by SonicOS.

5. VoIP Server returns Phone B media IP information to Phone A.

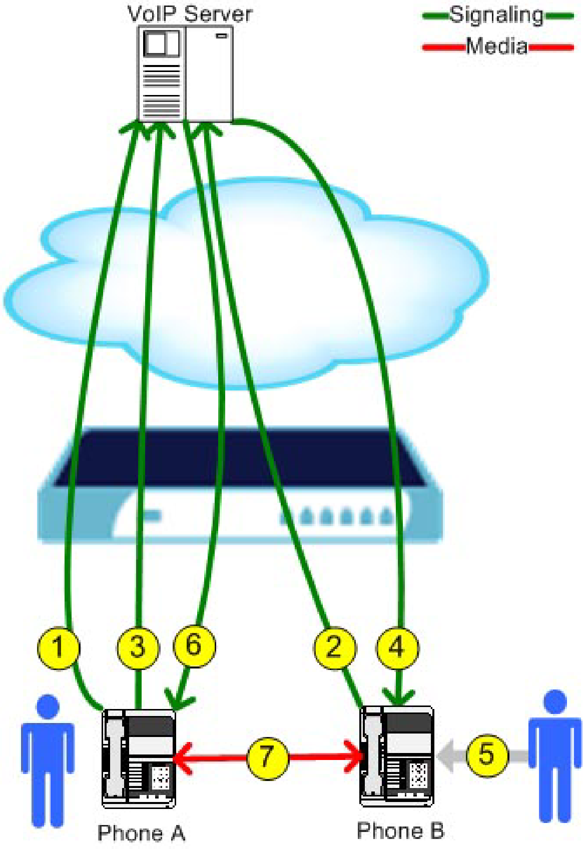
Phone A now has enough information to begin exchanging media with Phone B. Phone A does not know that Phone B is behind a firewall, as it was given the public address of the firewall by the VoIP Server.

6. Phone A and Phone B are connected and can exchange audio/video/data.

   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

The following sequence illustrates the flow for a call between two phones behind a SonicWALL:



1. Phone A registers with VoIP Server.

   Phone A is added to the SonicOS internal database of the accessible IP phones behind it. SonicOS translates between Phone A private IP address and the public firewall address within registration messages. The VoIP Server is unaware that Phone A is behind a firewall—it associates Phone A with the firewall public IP address.

2. Phone B registers with VoIP Server.

   Phone B is also added to the SonicOS internal database of the accessible IP phones behind it. SonicOS translates between Phone B private IP address and the public firewall address within registration messages. Again the VoIP Server is unaware that Phone B is behind a firewall —it also associates Phone B with the same firewall public IP address (but on a different port than that for Phone A).

3. Some time later, 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 how to reach Phone B—it just has an alias or phone number for Phone B. As part of the call request, Phone A provides the VoIP Server with details of the media types and formats it is able to handle ,together with the associated IP addresses and ports for them. SonicOS translates this private IP information to use the public firewall address for messages going back to the VoIP Server. This media information is also included within the internal database by SonicOS.

4. VoIP Server validates the call request and sends the request to Phone B.

   The incoming call request is sent to the firewall public IP address by the VoIP Server. When it reaches the firewall, SonicOS validates the source and content of the request. Based on the (public) IP address information contained within the request, a database lookup is performed to determine the private address to which to send the request.

As the calling party and media information relates to a phone (Phone A) behind this firewall, SonicOS, using the internal database, translates them back to the private addresses and ports for Phone A.

5. 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 is able to handle together with the associated IP addresses and ports for them.

SonicOS translates this private IP information to use the public firewall address for messages going back to the VoIP Server. This information is also included within the internal database by SonicOS.

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. Phone A now has enough information to begin exchanging media directly with Phone B.

7. Phone A and Phone B are connected and can directly exchange audio/video/data.

By intelligently tracking the entire call setup, SonicOS permits (VoIP Server authorized) calls between devices that are behind it to be connected directly. These calls can take advantage of their local network characteristics without the need for traffic traveling unnecessarily outside the firewall.

References

[BCR-FORT] Business Communications Review, Stumbling Blocks On The Road To Ubiquitous VoIP (July 2003).

[CERT-H323] CERT® Advisory CA-2004-01 Multiple H.323 Message. Vulnerabilities (http://www.cert.org/advisories/CA-2004-01.html)

[CERT-SIP] CERT® Advisory CA-2003-06 Multiple vulnerabilities in implementations of the Session Initiation Protocol (SIP). (http://www.cert.org/advisories/CA-2003-06.html)

[CISCO-NAT] Cisco, VoIP Traversal of NAT and Firewall (http://www.cisco.com/warp/public/788/voip/voip-nat.html)

[DISA-VOIP] Defense Information Systems Agency, Voice Over Internet Protocol (VOIP) Security Technical Implementation Guide. (http://csrc.nist.gov/pcig/STIGs/VoIP-STIG-V1R1R-4PDF.pdf)

[IETF-STUN] STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs), IETF RFC 3489.

[IETF-TURN] Traversal Using Relay NAT (TURN), IETF draft-rosenberg-midcom-turn.

[INTEL-H323] Intel, The Problems and Pitfalls of Getting H.323 Safely Through Firewalls

[LR-SESSION] Session Controllers Report Vol. 4, No. 2, February 2004, Light Reading

[NIST-VOIP] NIST Security Considerations for Voice Over IP Systems, NIST SP 800-58.

[NM-SECURING] Securing the IP Telephony Perimeter, May 2004, Network Magazine

[NWFUSION-SBC] Session border controllers have limited lifespan, March 2004, Network World Fusion.

[SYS-CISCO] The Trivial Cisco IP Phones Compromise, The Sys-Security Group.

[TMC-0603] Fortigate-400 TMC Labs (http://www.tmcnet.com/it/0603/0603Labs1.htm)

[WAIN-FWNAT] Traversing Firewalls and NATs With Voice and Video Over IP, Wainhouse Research (http://www.wainhouse.com/files/papers/WR-trans-firewall-nats.pdf)