Voice over IP und Netzwerksicherheit – herstellerübergreifende Lösungen mit SonicWALL Security Appliances

In diesem Whitepaper wird die Komplexität rund um den Einsatz eines sicheren VoIP-Netzwerks untersucht und anschließend die SonicWALL VoIP-Lösung vorgestellt.

INHALT

SONICWALL

Einleitung

Unternehmen, die zur Senkung ihrer Kommunikationskosten VoIP-Technologien (Voice over IP) implementieren, sollten die Sicherheitsrisiken im Zusammenhang mit einem vereinten Daten- und Sprachnetz nicht außer Acht lassen. Neben den Vorteilen durch niedrigere Telefongebühren, zentrale Verwaltung und schnelle Installation werden die kritischen Bereiche der VoIP-Sicherheit und der Netzwerkintegrität oft vernachlässigt.
In einem VoIP-Netzwerk gilt es zahlreiche Bedrohungsziele zu beachten: Die Anrufserver und ihre Betriebssysteme, die Telefone und ihre Software, ja sogar die Telefonanrufe selbst können Schwachstellen sein.

In diesem Whitepaper wird die Problematik und Komplexität rund um den Einsatz eines sicheren VoIP-Netzwerks untersucht und anschließend die gesamte SonicWALL VoIP-Lösung mit der Stateful Packet Inspection-Technologie von SonicWALL vorgestellt.

VoIP und Netzwerksicherheit – welche potentiellen Risiken bestehen?

Die bisherige Rolle der Firewall* in einem VoIP-Netzwerk ändert sich dramatisch. Bisher war die Hauptforderung dahingehend, dass sich das Gerät in das VoIP-Netzwerk integrieren lässt. VoIP benötigt unbedingt die vorhersagbare, statische Verfügbarkeit IP-basierter Ressourcen im Internet, während die Firewall mit ihrer NAT-Funktionalität (Network Address Translation) schon vom Ansatz her das VoIP-Netzwerk stört. Über Methoden und Techniken wie z.B. das „Pin-Holing“ (auch: dynamische Portfreischaltung) haben die Hersteller von Sicherheitslösungen Möglichkeiten gefunden, dennoch weitgehende Interoperabilität mit VoIP-Infrastrukturen zu ermöglichen.

Mit der zunehmenden Komplexität netzwerkbasierter Bedrohungen hat sich jedoch auch die Rolle der Firewall gewandelt: Sie muss sich nicht nur gut in die VoIP-Umgebung einfügen, sondern auch die vollständige Aktivierung und den Schutz der gesamten Infrastruktur übernehmen. Die VoIP-Umgebung eines gesamten Unternehmens, von Endbenutzergeräten wie IP-basierten Telefonen, Softphones und drahtlosen Kommunikationsgeräten bis hin zu H.323-Gatekeepern und SIP-Proxy-Servern, ist einem enormen Risiko ausgesetzt. Von einfachen DoS-Angriffen (Denial of Service), mit denen die Verfügbarkeit der IP-basierten Voice-Infrastruktur eingeschränkt werden soll, bis hin zu ausgereiften Angriffen auf die Anwendungsschicht, die auf die VoIP-Protokolle selbst abzielen, stellen die Bedrohungen eine echte Gefahr dar, die immer mehr zunimmt.

Für eine erfolgreiche VoIP-Implementierung müssen drei Schlüsselfaktoren mit einbezogen werden:

→ VoIP-Sicherheit

→ Netzwerk-Interoperabilität von VoIP und Protokollunterstützung

→ Interoperabilität mit VoIP-Anbietern

In den folgenden Abschnitten werden diese Faktoren diskutiert.

**In diesem Dokument bezeichnet „Firewall“ ein beliebiges Sicherheitsgerät zum Schutz von VoIP-Peripherie. Moderne Sicherheitsgeräte sind heute mehr als nur bloße Stateful Inspection-Firewalls; sie verwenden Deep Packet Inspection-Technologien, mit denen ihre Funktionalität beträchtlich erweitert wird.*

VoIP-Sicherheit

Das Thema VoIP-Sicherheit umfasst viele Bereiche, doch zu den wichtigsten Faktoren bei jeder Installation zählen der Zugriff, die Verfügbarkeit und die Implementierung.

Zugriff auf die Daten

VoIP-Anrufe können von Bedrohungen, wie z.B. dem Session-Hijacking und Man-in-the-Middle, angegriffen werden. Ohne die entsprechenden Sicherheitsvorkehrungen könnte ein Angreifer einen VoIP-Anruf abfangen und die Anrufparameter/-adressen ändern. Dies würde den Anruf u.a. Gefahren durch Spoofing, Identitätsdiebstahl und Anrufumleitung aussetzen.

Auch ohne das Ändern von VoIP-Paketen können Angreifer möglicherweise Telefongespräche über ein VoIP-Netzwerk abhören. Beim ungeschützten Transport von VoIP-Paketen über das Internet können Angreifer auf diese Informationen zugreifen.

Bei Verbindungen über ein herkömmlich vermitteltes Telefonnetzwerk (Public Switched Telephone Network, PSTN) müssten Telefonleitungen physikalisch unterbrochen werden, oder es müsste direkt auf die TK-Anlage zugegriffen werden, um Gespräche abzuhören. Voice-/Datennetzwerke, die in der Regel den öffentlichen Internet- und den TCP/IP-Protokollstapel verwenden, bieten nicht die gleiche Sicherheit wie Telefonleitungen. Durch den Zugriff und die Überwachung des Netzwerkverkehrs an bestimmten Stellen in der Infrastruktur (wie z.B. von/zu einem VoIP-Gateway) könnte ein Angreifer VoIP-Pakete abfangen und umstellen. Öffentlich verfügbare Tools, wie z.B. Vomit (http://vomit.xtdnet.nl/), können zur Konvertierung dieser Pakete in eine WAV-Datei verwendet werden. Der Angreifer kann das Gespräch abhören, ja sogar aufzeichnen und später erneut abspielen.

Verfügbarkeit

Ein weiterer wichtiger Punkt ist die Verfügbarkeit des VoIP-Netzwerks. Da die Verfügbarkeit von herkömmlichen Telefonleitungen mittlerweile bei 99,999 % liegt, müssten Angreifer physikalisch auf eine TK-Anlage zugreifen oder Telefonleitungen kappen, um Schaden anzurichten. Ein einfacher DoS-Angriff auf wichtige Stellen eines ungeschützten VoIP-Netzwerks würde jedoch schon genügen, um die Voice- und Datenkommunikation erheblich zu stören, möglicherweise sogar zum Erliegen zu bringen.

VoIP-Netzwerke sind besonders durch folgende DoS-Angriffe gefährdet:

Malformed Request-DoS

Hierbei handelt es sich um eine sorgfältig zusammengestellte Protokollanfrage, mit der eine bekannte Schwachstelle ausgenutzt werden kann, was zum teilweisen oder vollständigen Verlust des Dienstes führt. Mit einem solchen Angriff kann das Angriffsziel zum Absturz gebracht oder auch die Steuerung über das Angriffsziel übernommen werden.

DoS auf Medien

Die Übertragung von VoIP-Medien über RTP-Pakete (Real-Time Protocol) kann durch Angriffe gestört werden, die darauf abzielen, das Netzwerk zu überlasten oder die Fähigkeit eines Endgeräts (Telefon oder Gateway) zur Echtzeitverarbeitung des Pakets einzuschränken.

Ein Angreifer, der auf den Teil des Netzwerks zugreifen kann, in dem sich die Medien befinden, muss nur eine große Anzahl von Medien- oder QoS-Paketen (Quality of Service) einschleusen, die mit den rechtmäßigen Medienpaketen konkurrieren.

DoS durch Überlastung

Ein DoS-Angriff muss nicht unbedingt bösartige Pakete, so genannte „malformed packets“, verwenden. Allein die Überlastung des Angriffsziels mit rechtmäßigen Anfragen kann ein unzureichend ausgelegtes System schnell zum Absturz bringen.

Selbst mit einem nicht auf VoIP-Protokolle gerichteten DoS-Angriff, wie z.B. TCP SYN Flood, kann ein Gerät für einen langen Zeitraum an der Annahme von Gesprächen gehindert werden.

Schwierigkeiten bei der Implementierung

VoIP umfasst eine Vielzahl von Standards, wie z.B. das Session Initiation Protocol (SIP), H.323, das Media Gateway Control Protocol (MGCP) und H.248. Da es sich um komplexe Standards handelt, können Fehler bei der Softwareimplementierung auftreten. Bei PSTN sind Telefone einfach nur ‘unwissende Endgeräte’, da die gesamte Logik und Intelligenz in der TK-Anlage zusammenkommt. Ein Hacker hat nicht viele Möglichkeiten, den Zugriff auf ein PSTN-Netzwerk zu stören.

VoIP-Geräte sind jedoch, wie auch alle derzeit erhältlichen Betriebssysteme und Softwareanwendungen, durch die gleichen Arten von Fehlern und Schwachstellen gefährdet. Man darf nicht vergessen, dass viele der heutigen VoIP-Anrufserver und –gateways auf Windows- oder Linuxbetriebssystemen beruhen und somit auch deren Schwachstellen ausgesetzt sind. Ein Blick auf die CERT-Advisories, die für H.323 [CERT-H.323] und SIP [CERT-SIP] veröffentlicht wurden, zeigt, wie viele Schwachstellen gefunden wurden und wie viele Hersteller davon betroffen sind.

Netzwerk-Interoperabilität von VoIP und Protokollunterstützung

VoIP ist komplizierter als eine normale TCP/UDP-basierte Anwendung. Aufgrund der Komplexität der Signalisierung und der Protokolle bei VoIP sowie der Inkonsistenzen, die sich ergeben, wenn eine Firewall die Quelladress- und Quellportdaten mit NAT ändert, ist es schwierig für VoIP, eine Firewall ungehindert zu überwinden. Im Folgenden werden einige Gründe hierfür erläutert.

VoIP verwendet zwei verschiedene Protokolle: eines für die Signalisierung (zwischen dem Client und dem VoIP-Server) und eines für die Medien (zwischen den Clients). Die Port/IP-Adresspaare, die von den Medienprotokollen (RTP/RTCP) für jede Sitzung verwendet werden, werden von den Signalisierungsprotokollen dynamisch verhandelt. Firewalls müssen diese Informationen dynamisch mitverfolgen und warten und zum entsprechenden Zeitpunkt ausgewählte Ports für die Sitzungen auf sichere Weise öffnen und wieder schließen.

Mehrere Medienports werden über die Signalisierungssitzung dynamisch verhandelt; die Verhandlungen über die Medienports sind in der Nutzlast der Signalisierungsprotokolle enthalten (IP-Adress- und Portinformationen). Firewalls müssen für jedes Paket eine Deep Inspection durchführen, um diese Informationen zu erhalten und die Sitzungen dynamisch zu warten; dies erfordert zusätzliche Verarbeitungskapazitäten der Firewall.

Die Quell- und Ziel-IP-Adressen sind in die VoIP-Signalisierungspakete eingebettet. Eine Firewall mit NAT-Unterstützung übersetzt IP-Adressen und -Ports auf IP-Header-Ebene für Pakete. Schlimmer noch, vollsymmetrische NAT-Firewalls passen ihre NAT-Bindungen häufig neu an und können so zufällig die Pinholes schließen, über die eingehende Pakete in das zu schützende Netzwerk gelangen. In diesem Fall kann der Dienstanbieter keine eingehenden Anrufe an den Kunden weiterleiten.

Für die erfolgreiche Unterstützung von VoIP muss eine NAT-Firewall eine Deep Packet Inspection durchführen und eingebettete IP-Adress- und Portinformationen bei der Weiterleitung über die Firewall transformieren können.

Firewalls müssen die verschiedenen Signalisierungsprotokollfamilien verarbeiten, die aus unterschiedlichen Nachrichtenformaten bestehen, die von verschiedenen VoIP-Systemen verwendet werden. Auch wenn zwei Hersteller die gleiche Protokollfamilie verwenden, bedeutet dies nicht notwendigerweise, dass ihre Produkte interoperabel sind.

Interoperabilität mit VoIP-Anbietern

Nicht alle Hersteller von VoIP-Lösungen implementieren die auf RFCs basierenden Standard-VoIP-Protokolle auf die gleiche Weise, so dass nicht alle Lösungen kompatibel sind. Zudem implementieren einige Anbieter so genannte „standardkompatible“ proprietäre VoIP-Protokolle. Daher ist es wichtig, dass die Firewall mit so vielen VoIP-Endgeräten und -Anrufservern wie möglich interoperabel ist.

Letztendlich müssen die einzelnen Hersteller sicherstellen, dass ihre jeweiligen Geräte kompatibel sind. Gerade in diesen Bereich investiert SonicWALL viel Zeit und Aufwand. Eine Teilliste der Geräte, die mit SonicWALL interoperabel sind, ist auf Seite 19 dieses Dokuments aufgeführt.

Aktuelle Lösungen für VoIP-Sicherheit

Es gibt eine Reihe von Ansätzen zur Sicherung der VoIP-Infrastruktur. In der folgenden Tabelle sind die wichtigsten Ansätze aufgeführt.

Lösung	Vorteile	Nachteile
Keine Firewall (oder Firewall, die VoIP nicht erkennt)	Keine Auswirkungen auf IP-Voice- und Videoanwendungen	Keinerlei Netzwerksicherheit Die Endpunkte benötigen eine öffentliche IP-Adresse Die Endpunkte sind für jeden frei zugänglich
NAT-Weiterleitungslösungen, die die Firewall 'umgehen' (wie z.B. STUN [IETF-STUN])	Kein Upgrade/keine Änderung der Firewall erforderlich	Keine/eingeschränkte Netzwerksicherheit auf 'offenen' Ports; VoIP-Geräte sind noch immer ungeschützt Funktioniert nicht mit symmetrischem NAT [IETF-TURN] Funktioniert nur mit UDP und unterstützt weder H.323 noch SIP über TCP RTCP funktioniert möglicherweise nicht (wegen der engen Kopplung der RTCP-Portnummer an die RTP-Portnummer)
Session Border Controllers	Kein Upgrade/keine Änderung der Firewall erforderlich	Kurzfristige Lösung [NWFUSION-SBC] Vorrangig für Dienstanbieter entwickelt Zusätzlicher Verwaltungsaufwand Möglicherweise muss in jedem Netzwerk Client-Software installiert werden; Gefahr von Engpässen oder Instabilitäten, da die VoIP-Endpunkte den gesamten Verkehr (Signalisierung und Medien) über die Firewall leiten müssen Zentralisierte Ansätze bedeuten, dass nicht mehr das Unternehmen, sondern der Carrier für die VoIP-Sicherheit verantwortlich ist
Vollständiger VoIP-Proxy	Kein Upgrade/keine Änderung der Firewall erforderlich	Proxy ist nach wie vor gefährdet Möglicherweise ist pro VoIP-Protokoll ein Proxy erforderlich Erfordert einen Proxy hinter jeder Firewall Muss aus Hochverfügbarkeitsgründen möglicherweise paarweise installiert werden Zusätzliche Latenzzeit; führt möglicherweise zu Engpässen und Instabilitäten
SonicWALL Stateful Packet Transformation	Schützt die Signalisierung und die Medien Benutzerfreundlich durch 'Plug-and-Protect'-Technologie Keine zusätzlichen Geräte erforderlich, da vorhandene SonicWALL-Firewalls der 'aktuellen' Generation verwendet werden Unterstützt eine Vielzahl von VoIP-Protokollen Interoperabilität der VoIP-Geräte mit zahlreichen Herstellern	Werden nicht von Firewalls der vorherigen Generation unterstützt

Der SonicWALL-Ansatz

SonicWALL stellt eine Komplettlösung für VoIP bereit, die ein völlig neues Maß an Sicherheit für die VoIP-Infrastruktur, standardbasierte VoIP-Kompatibilität und Interoperabilität mit vielen weltweit führenden VoIP-Gateway- und Kommunikationsgeräten bietet.

Alle Sicherheits-Appliances von SonicWALL der Produktreihen TZ 170 und PRO (4. Generation) verfügen über das gleiche Maß an umfassender VoIP-Sicherheit, wie sie in diesem Papier beschrieben ist. Dies ist wichtig, da die Gesamtintegrität des VoIP-Netzwerks nur so gut ist wie sein schwächstes Glied. Es ist also ein Höchstmaß an Schutz erforderlich, auch für den privaten Nutzer und für persönliche Kommunikationsgeräte.

SonicWALL-Sicherheits-Appliances mit der Firmware SonicOS Standard oder Enhanced verfügen über integrierte VoIP-Funktionen. Bei SonicOS Enhanced erhält der Benutzer neben umfassenderem QoS-Support zusätzliche Funktionen zur Anrufüberwachung und Berichterstellung (z.B. Verwaltung der eingehenden Bandbreite).

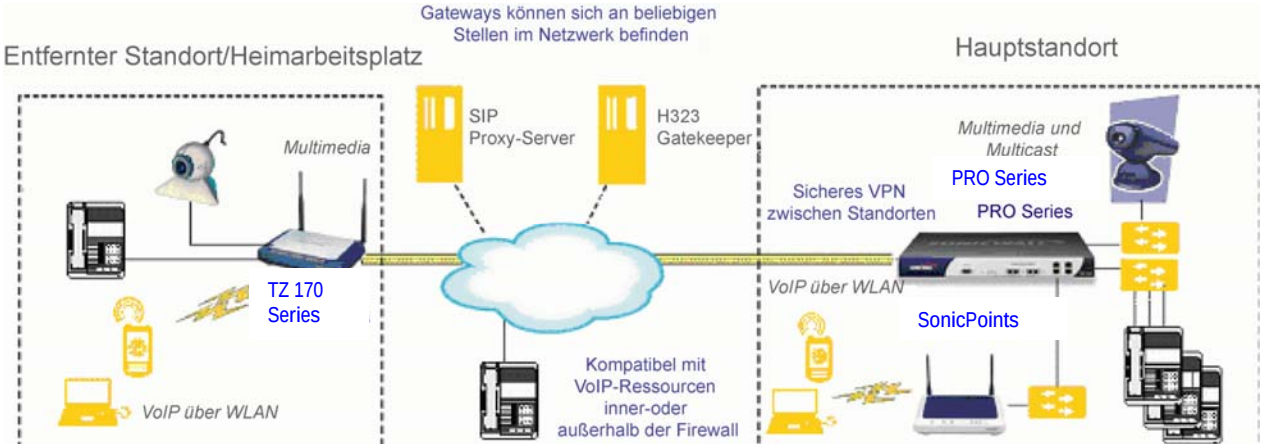


Abbildung 1
VoIP-Ansatz von SonicWALL

Die zentrale VoIP-Implementierung von SonicWALL umfasst die folgenden Funktionen, die im weiteren Verlauf dieses Papiers ausführlich beschrieben werden:

Stateful Packet Inspection und Transformation während der gesamten Dauer eines VoIP-Anrufs:

- Anrufregistrierung
- Anrufauf- und -abbau
- Medienaustausch

Sicherheit

- VoIP-Intrusion-Prevention, Virenschutz und Content-Filter
- VoIP über WLAN, mit umfassenden Funktionen zur Bedrohungsabwehr
- Erkennung und Entfernung von Malformed Packets
- Setzt 'geschlossenes' VoIP-Netzwerk durch und verhindert so nicht autorisierte Anrufe

Architektur

- Unterstützung von Streaming Media und Multicast-Anwendungen
- Beliebige Mischung von Geräten in ALLEN Bereichen (H.323- und SIP-Endpunkte, H.323-Gatekeeper, H.323-Mehrpunkt-Steuereinheit, SIP-Proxy- und -Umleitungsserver)
- Gatekeeper und Proxies können an einer beliebigen Stelle im Netzwerk platziert werden, sogar in der DMZ
- Vollsymmetrisches NAT

Umfangreiche Berichterstellung

- Anrufrückverfolgung
- Protokollierung 'abnormaler' Pakete
- Vereinfachte Fehlersuche und -behebung

SonicWALL VoIP-Sicherheit

Die leistungsstarke Deep Inspection-Technologie von SonicWALL bietet flexible Möglichkeiten für die Überprüfung und Durchsetzung des Datenverkehrs an allen Punkten in der VoIP-Infrastruktur.

VoIP-Server und -Endpunkte

Rechtmäßigkeit des Datenverkehrs

Durch die Stateful Inspection jedes einzelnen VoIP-Signalisierungs- und Medienpakets wird sichergestellt, dass der gesamte Datenverkehr, der die Firewall passiert, den Richtlinien genügt. Pakete, die Schwachstellen in der Implementierung ausnutzen und zu Problemen wie Pufferüberläufen auf dem Zielgerät führen, werden von vielen Angreifern für ihre Zwecke genutzt. SonicWALL kann bösartige und ungültige Pakete erkennen und entfernen, noch bevor sie ihr anvisiertes Ziel erreichen.

Schutz der VoIP-Protokolle auf Anwendungsebene

SonicWALL Intrusion Prevention Service (IPS) bietet vollständigen Schutz für VoIP vor Angriffen über die Anwendungsschicht. IPS kombiniert eine konfigurierbare, ultrahochperformante Scan Engine mit einer dynamisch aktualisierten und provisionierten Datenbank mit über 1.800 Angriffs- und Schwachstellensignaturen, um Netzwerke auch vor den komplexen Trojaner- und polymorphen Bedrohungen zu schützen. SonicWALL hat die IPS-Signaturdatenbank um eine Reihe VoIP-spezifischer Signaturen erweitert, mit denen bösartiger Datenverkehr von geschützten VoIP-Telefonen und –Servern abgewendet wird.

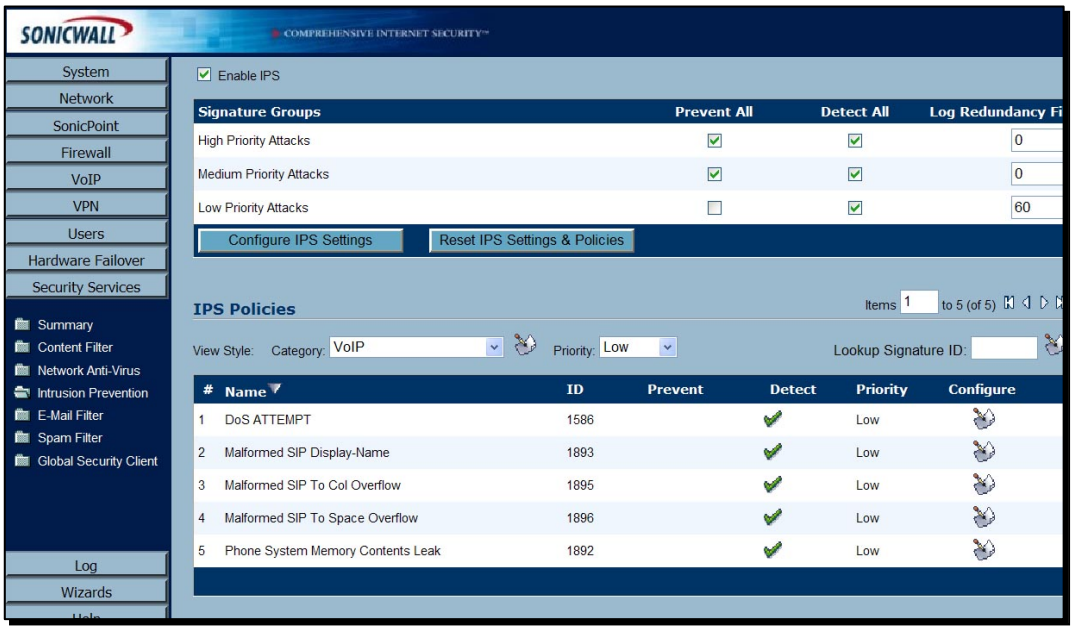


Abbildung 2
SonicWALL IPS GUI

Schutz vor DoS- und DDoS-Angriffen

Abwehr von DoS- und DDoS-Angriffen, wie z.B. SYN Flood, Ping of Death und LAND (IP) Attack, die die Deaktivierung eines Netzwerks oder Dienstes zum Ziel haben.

- Validierung der Paketsequenz für VoIP-Signalisierungspakete mittels TCP. Out of Sequence-Pakete und die erneute Paketübertragung jenseits des Zeitfensters werden nicht zugelassen.
- Durch die Verwendung zufälliger TCP-Sequenznummern (die während der Verbindungseinrichtung von einem kryptographischen Zufallszahlengenerator erstellt werden) und die Validierung des Datenflusses innerhalb jeder TCP-Sitzung werden Angriffe, die auf das erneute Abspielen und das Einfügen von Daten abzielen, verhindert.
- Der Schutz vor SYN Flood stellt sicher, dass Angreifer den Server nicht durch das Eröffnen einer Vielzahl von TCP/IP-Verbindungen überwältigen können (die aufgrund einer gespooften Quelladresse niemals vollständig etabliert werden).

Stateful Monitoring

Das Stateful Monitoring stellt sicher, dass auch augenscheinlich gültige Pakete dem aktuellen Status der zugehörigen VoIP-Verbindung entsprechen.

SonicWALL-Virenschutz

SonicWALL-Virenschutzprodukte schützen Softphone-Kunden vor virenbasierten Bedrohungen und stellen vollautomatisch sicher, dass immer mit aktuellen Virensignaturendatenbanken gearbeitet wird. Dies reduziert den Zeit- und Kostenaufwand für die Verwaltung von Virenschutzrichtlinien im gesamten Netzwerk ganz erheblich.

VoIP-Gespräche

Nahtlose Unterstützung verschlüsselter Medien

Eine Reihe von VoIP-Geräten können den Medienaustausch innerhalb eines VoIP-Gesprächs vor dem Abhören per Verschlüsselung schützen.

Starke Authentifizierung und Verschlüsselung

Die ICSA-zertifizierten IPSec-VPNs von SonicWALL für den Site-to-Site- und den Remote-Zugriff ermöglichen Remote-Benutzern, mobilen Benutzern und Zweigstellen den kostengünstigen, zuverlässigen und sicheren Remote-Zugriff auf die Netzwerkressourcen. Bei Verwendung zusammen mit einem robusten Authentifizierungsdienst bieten sie eine starke Authentifizierung der VPN-Benutzer im Internet mittels einer Public Key Infrastructure (PKI) und digitalen Zertifikaten.

Zur Sicherung von VoIP-Geräten, die keine verschlüsselten Medien unterstützen, dienen IPSec-VPNs als vollständige Lösung zum Schutz von VoIP-Anrufen.

Das VoIP-Netzwerk

VoIP über Wireless LAN (WLAN)

Mit der Distributed Wireless Solution weitet SonicWALL die vollständige VoIP-Sicherheit auch auf angeschlossene Wireless-Netzwerke aus. Ob bei Verwendung einer Appliance der Reihe TZ 170 mit integriertem 802.11-Wireless-Zugriff oder einer Appliance der Reihe PRO mit Access Points vom Typ SonicPoint 802.11a/b/g: Alle Sicherheitsfunktionen und Vorteile, die VoIP-Geräten in einem verdrahteten Netzwerk hinter einer SonicWALL zur Verfügung stehen, stehen auch VoIP-Geräten in einem Wireless-Netzwerk zur Verfügung.

Verfügbarkeit und Anrufqualität über Bandbreitenmanagement

Mit Bandbreitenmanagement für den ein- und ausgehenden Datenstrom kann die Konstanz der Bandbreite für zeitempfindlichen VoIP-Verkehr sichergestellt werden. SonicOS ermöglicht dies durch die ständige Überwachung und Verwaltung der verfügbaren Bandbreite für die Anrufe der VoIP-Geräte.

WAN-Redundanz und Lastenausgleich

WAN-Redundanz und Lastenausgleich ermöglichen den Einsatz einer Schnittstelle als sekundärer oder Sicherungs-WAN-Port. Dieser sekundäre WAN-Port kann in einem einfachen Aktiv/Passiv-Setup verwendet werden, in dem der Verkehr nur dann über den sekundären Port geleitet wird, wenn der primäre WAN-Port außer Betrieb und/oder nicht verfügbar ist. Der sekundäre WAN-Port kann auch in einem dynamischeren Aktiv/Aktiv-Setup verwendet werden, in dem der ausgehende Verkehrsfluss zur Durchsatzerhöhung zwischen dem primären und dem sekundären WAN-Port aufgeteilt wird.

Hochverfügbarkeit

Hochverfügbarkeit wird durch die Failover-Funktionen der SonicOS-Hardware bereitgestellt, die bei einem Systemausfall eine zuverlässige und kontinuierliche Verbindungsfunktionalität gewährleisten.

Netzwerk-Interoperabilität von SonicWALL VoIP

SonicOS entkapselt, entschlüsselt, validiert, transformiert, verfolgt und überwacht effizient und effektiv den gesamten VoIP-Signalisierungsverkehr, während es gleichzeitig den VoIP-Mediendatenverkehr validiert und verfolgt. Das hierdurch erreichte Niveau an Sicherheit und Benutzerfreundlichkeit ist branchenführend.

'Plug-and-Protect'-Unterstützung für VoIP-Geräte
Durch die Verwendung fortschrittlicher Überwachungs- und Trackingtechnologien ist ein VoIP-Gerät automatisch geschützt, sobald es hinter einer SonicWALL-Sicherheits-Appliance mit dem Netzwerk verbunden wird.

Bei SonicWALL ist es nicht mehr erforderlich, die Firewall in regelmäßigen Abständen neu zu konfigurieren, wie dies bei einigen anderen Herstellern der Fall ist. Mit SonicOS werden VoIP-Geräte automatisch hinzugefügt, geändert und entfernt, so dass kein VoIP-Gerät ungeschützt bleibt.

Vollständige Syntaxvalidierung aller VoIP-Signalisierungspakete
Die empfangenen Signalisierungspakete werden innerhalb von SonicOS vollständig geparst, um ihre Übereinstimmung mit der Syntax des jeweiligen Standards sicherzustellen. Durch die Syntaxvalidierung kann die Firewall sicherstellen, dass keine Malformed Packets übertragen werden, die ihr Ziel schädigen können.

Hier unterscheidet sich SonicWALL gravierend von anderen Firewall-Herstellern, die behaupten, VoIP zu unterstützen. In einigen Fällen öffnen diese Hersteller einfach Ports, ohne sich darum zu kümmern, welcher Datenverkehr darüber übertragen wird. In anderen Fällen werden nur ein paar Felder überprüft, in der Regel diejenigen, die im Zuge der NAT verändert werden; der Rest wird einfach ignoriert.

SonicWALL führt hochperformante, **vollständige** Paketvalidierungen für jedes einzelne Signalisierungspaket durch.

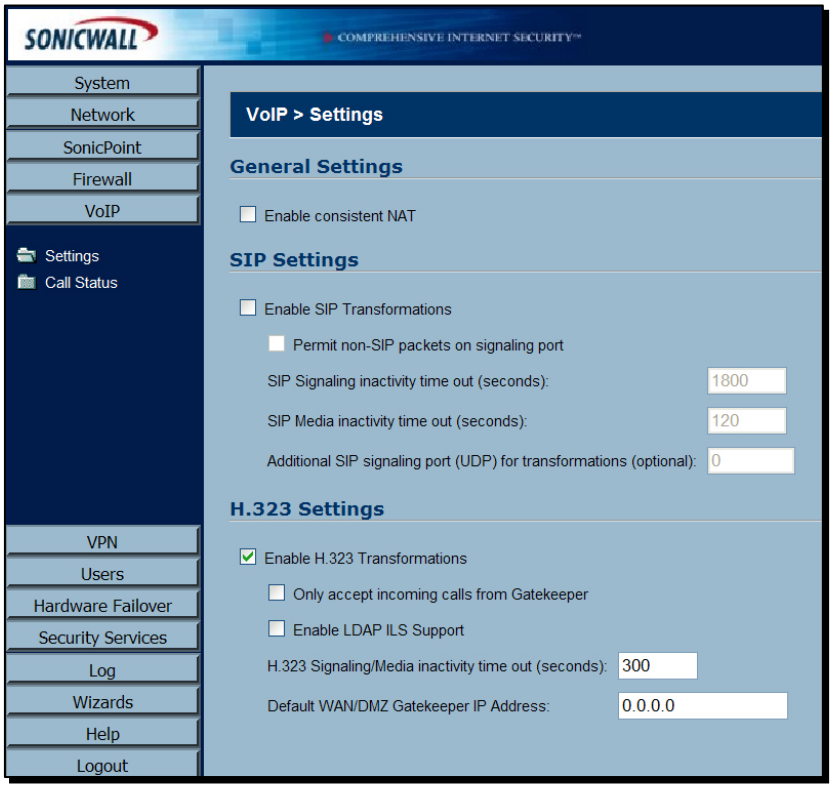


Abbildung 3
VoIP-GUI-Einstellungen

Unterstützung für das dynamische Setup und die Verfolgung von Medienströmen

SonicOS verfolgt jeden VoIP-Anruf mit; vom ersten Signalisierungspaket, das eine Anrufeinrichtung anfordert, bis zu dem Punkt, an dem der Anruf beendet wird. Nur bei erfolgreichem Anrufverlauf werden zusätzliche Ports (für den zusätzlichen Signalisierungs- und Medienaustausch) zwischen dem Anrufer und dem angerufenen Teilnehmer geöffnet.

Medienports, die als Teil der Anrufeinrichtung verhandelt werden, werden dynamisch von der Firewall zugewiesen. Nachfolgende Anrufe, auch wenn sie zwischen den gleichen Teilnehmern erfolgen, verwenden andere Ports, um Angreifer abzuwehren, die möglicherweise bestimmte Ports überwachen.

Die erforderlichen Medienports werden nur geöffnet, wenn der Anruf vollständig verbunden wurde, und bei Anrufbeendigung wieder geschlossen. Datenverkehr, der versucht, die Ports außerhalb eines Anrufs zu verwenden, wird abgewiesen; dies bietet einen zusätzlichen Schutz für die VoIP-Geräte hinter der Firewall.

Andere Hersteller von Sicherheitslösungen verwenden statische Zuweisungen für die Medienports und lassen sie in einigen Fällen geöffnet, auch wenn gerade kein Anruf aktiv ist. Mit diesem Ansatz werden die VoIP-Geräte, und mit ihnen der Rest der IP-Infrastruktur, unnötigerweise der Gefahr eines Angriffs ausgesetzt.

Validierung der Header in allen Medienpaketen

SonicOS untersucht und überwacht die Header in Medienpaketen, um Out of Sequence- und außerhalb des Zeitfensters erneut übermittelte Pakete zu erkennen und zu entfernen. Durch die Sicherstellung, dass ein gültiger Header vorhanden ist, werden zudem ungültige Medienpakete erkannt und entfernt.

Dies ist ein weiterer wichtiger Unterschied zwischen SonicWALL und anderen Herstellern von Sicherheitslösungen. Durch die Verfolgung sowohl der Medienströme als auch der Signalisierung schützt SonicWALL die gesamte VoIP-Sitzung.

Konfigurierbare Zeitüberschreitung bei Inaktivität für die Signalisierung und die Medien

Um sicherzustellen, dass abgewiesene VoIP-Verbindungen nicht unendlich lange geöffnet bleiben, überwacht SonicOS die Verwendung der Signalisierungs- und Medienströme einer VoIP-Sitzung. Ströme, die länger als das konfigurierte Zeitfenster inaktiv sind (d.h. es findet kein Paketaustausch statt), werden aus Sicherheitsgründen geschlossen.

SonicOS ermöglicht den Administratoren die Steuerung eingehender Anrufe

Durch die Forderung, dass alle eingehenden Anrufe durch den H.323-Gatekeeper oder den SIP-Proxy autorisiert und authentifiziert werden, kann SonicOS nicht autorisierte bzw. Spam-Anrufe blockieren. Dadurch kann der Administrator sicher gehen, dass das VoIP-Netzwerk nur für diejenigen Anrufe verwendet wird, die durch das Unternehmen autorisiert wurden.

SonicOS unterstützt Medienströme aus allen CODECs

Medienströme enthalten Audio- und Videosignale, die von einem Hardware-/Software-CODEC (COder/DECoder) innerhalb des VoIP-Geräts verarbeitet wurden. CODECs verwenden Kodierungs- und Kompressionstechniken, um die Datenmenge zu reduzieren, die zur Darstellung von Audio-/Videosignalen erforderlich ist.

- Einige Beispiele für CODECs sind:
  - Video: H.264, H.263 und H.261
  - Audio: MPEG4, G.711, G.722, G.723, G.728, G.729

Umfassende Überwachung und Berichterstellung

SonicOS bietet für alle unterstützten VoIP-Protokolle weit reichende Überwachungs- und Fehlerbehebungs-Tools:

- Dynamische Live-Berichterstellung aktiver VoIP-Anrufe, mit Angabe des Anrufers, des angerufenen Teilnehmers und der verwendeten Bandbreite.
- Audit-Protokolle aller VoIP-Anrufe, mit Angabe des Anrufers, des angerufenen Teilnehmers, der Anrufdauer und der insgesamt verwendeten Bandbreite. Protokollierung aufgetretener abnormaler Pakete (wie z.B. 'bad response'), mit Angaben zu den Teilnehmern und der aufgetretenen Bedingung.
- Detaillierte syslog- und ViewPoint-Berichte für VoIP-Signalisierungs- und Medienströme. SonicWALL ViewPoint ist ein webbasiertes, graphisches Tool zur Berichterstellung, das detaillierte und umfassende Berichte zu den Sicherheits- und Netzwerkaktivitäten bereitstellt und auf syslog-Datenströmen basiert, die von der Firewall empfangen werden. Berichte können zu nahezu allen Aspekten von Firewall-Aktivitäten erstellt werden, u.a. Verwendungsmuster für einzelne Benutzer bzw. Gruppen und Ereignisse auf bestimmten Firewalls oder Gruppen von Firewalls, Art und Zeitpunkt eines Angriffs, Ressourcenverbrauch und -einschränkungen usw.

SonicWALL VoIP-Protokollunterstützung

H.323

SonicOS unterstützt H.323 folgendermaßen:

VoIP-Geräte, die eine beliebige Version von H.323 (aktuell 1 bis 5) ausführen, werden unterstützt

Neben der Unterstützung für H.323 unterstützt SonicOS VoIP-Geräte, die die folgenden zusätzlichen ITU-Standards verwenden:

- T.120 für Anwendungsfreigabe, elektronisches Whiteboarding, Dateiaustausch und Chat
- H.239 für die Audio-, Video- und Datenzustellung über mehrere Kanäle
- H.281 für FECC (Far End Camera Control)

Der LDAP-basierte ILS (Internet Locator Service) von Microsoft

Auffinden des Gatekeepers durch LAN H.323-Endgeräte mithilfe von Multicast

Stateful Monitoring und –Verarbeitung der Gatekeeper-RAS- (Registrierung, Zulassung und Status) Meldungen

Unterstützung für H.323-Endgeräte, die Medienströme verschlüsseln

DHCP-Option 150. Der DHCP-Server von SonicWALL kann so konfiguriert werden, dass er die Adresse eines VoIP-spezifischen TFTP-Servers an DHCP-Clients zurückgibt

SIP

SSonicOS unterstützt Geräte, die folgende SIP Standards verwenden:

Geräte, die die folgenden Standards verwenden:

- Basis-SIP-Standard (RFC 2543 und RFC 3261)
- SIP INFO-Methode (RFC 2976)
- „Reliability of provisional responses in SIP“ (RFC 3262)
- SIP-spezifische Ereignisbenachrichtigung (RFC 3265)
- SIP UPDATE-Methode (RFC 3311)
- DHCP-Option für SIP-Server (RFC 3361)
- SIP-Erweiterung für Instant Messaging (RFC 3428)
- SIP REFER-Methode (RFC 3515)
- Erweiterung auf SIP für symmetrische Antwortweiterleitung (RFC 3581)

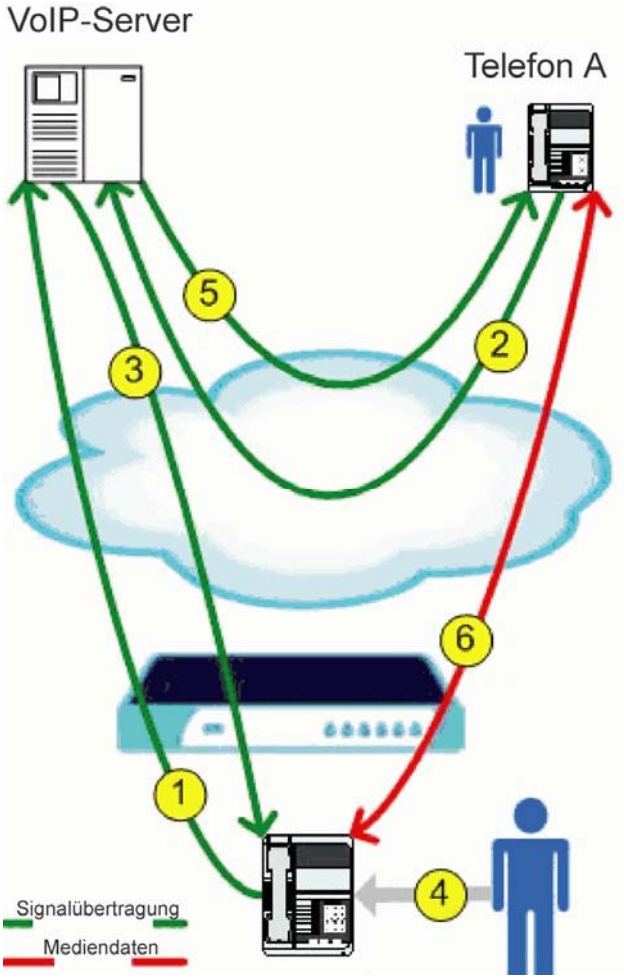
Beispiele für VoIP-Anrufverläufe

Es folgen einige Beispiele für VoIP-Anrufverläufe, die möglicherweise von anderen Lösungen nicht, oder nur unzureichend, unterstützt werden.

SonicOS stellt eine effiziente und sichere Lösung für alle VoIP-Anrufszenarien bereit.

Eingehende Anrufe

Der folgende Ablauf zeigt, wie SonicOS einen eingehenden Anruf bearbeitet:



1. Telefon B registriert sich beim VoIP-Server.

Durch die Überwachung der ausgehenden VoIP-Registrierungsanfragen kann SonicOS eine interne Datenbank der dahinter liegenden zugänglichen IP-Telefone aufbauen. SonicOS übersetzt zwischen der privaten IP-Adresse von Telefon B und der öffentlichen Firewall-Adresse innerhalb von Registrierungsnachrichten. Der VoIP-Server weiß nicht, dass sich Telefon B hinter einer Firewall befindet und über eine private IP-Adresse verfügt; er ordnet Telefon B der öffentlichen Firewall-IP-Adresse zu.

2. Etwas später initiiert Telefon A einen Anruf bei Telefon B, indem es eine Anfrage an den VoIP-Server sendet. Telefon A weiß nicht, wie es Telefon B erreichen kann, da es nur einen Alias oder eine Telefonnummer für Telefon B hat. Als Teil der Anrufanfrage stellt Telefon A dem VoIP-Server Details zu den Medienarten und –formaten bereit, die es verarbeiten kann, zusammen mit den ihnen zugeordneten IP-Adressen und Ports.

3. Der VoIP-Server validiert die Anrufanfrage und sendet sie an Telefon B.

Die eingehende Anrufanfrage wird vom VoIP-Server an die öffentliche Firewall-IP-Adresse geleitet. Wenn die Anfrage die Firewall erreicht, validiert SonicOS die Quelle und den Inhalt der Anfrage. Mit den (öffentlichen) IP-Adressinformationen in der Anfrage wird ein Lookup in der Datenbank durchgeführt, um die private Adresse zu ermitteln, an die die Anfrage gesendet werden soll.

SonicOS übersetzt zwischen der öffentlichen Firewall-Adresse und der privaten IP-Adresse von Telefon B innerhalb von Anrufanfragenachrichten.

4. Telefon B klingelt, und der Anruf wird angenommen.

Wenn der Anruf an Telefon B angenommen wird, gibt das Telefon Informationen an den VoIP-Server bezüglich der Medienarten und –formate zurück, die es verarbeiten kann, zusammen mit den ihnen zugeordneten IP-Adressen und Ports. SonicOS übersetzt diese privaten IP-Informationen, um die öffentliche Firewall-Adresse für Nachrichten zu verwenden, die zurück an den VoIP-Server gehen. Diese Medieninformationen werden außerdem von SonicOS in die interne Datenbank eingetragen.

5. Der VoIP-Server gibt die Medien-IP-Informationen von Telefon B an Telefon A zurück.

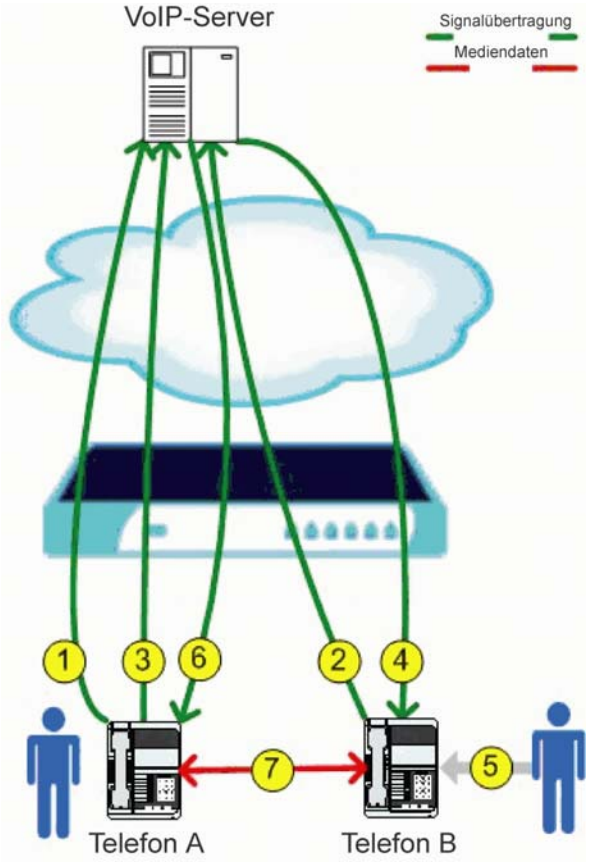
   Telefon A verfügt nun über genügend Informationen, um den Medienaustausch mit Telefon B zu beginnen. Telefon A weiß nicht, dass sich Telefon B hinter einer Firewall befindet, da es vom VoIP-Server die öffentliche Firewall-Adresse erhalten hat.

6. Telefon A und Telefon B werden verbunden und können Audio-, Video- oder Datenmedien austauschen.

   Durch die Verwendung der internen Datenbank stellt SonicOS sicher, dass nur Telefon A Medien sendet und nur die spezifischen Medienströme verwendet, die durch Telefon B zugelassen wurden.

Lokale Anrufe

Der folgende Ablauf zeigt den Anrufverlauf zwischen zwei Telefonen hinter einer SonicWALL:



1. Telefon A registriert sich beim VoIP-Server.

Telefon A wird zur internen SonicOS-Datenbank der dahinter liegenden zugänglichen IP-Telefone hinzugefügt. SonicOS übersetzt zwischen der privaten IP-Adresse von Telefon A und der öffentlichen Firewall-Adresse innerhalb von Registrierungsnachrichten. Der VoIP-Server weiß nicht, dass sich Telefon A hinter einer Firewall befindet; er ordnet Telefon A der öffentlichen Firewall-IP-Adresse zu.

2. Telefon B registriert sich beim VoIP-Server.

Auch Telefon B wird zur internen SonicOS-Datenbank der dahinter liegenden zugänglichen IP-Telefone hinzugefügt. SonicOS übersetzt zwischen der privaten IP-Adresse von Telefon B und der öffentlichen Firewall-Adresse innerhalb von Registrierungsnachrichten. Auch hier weiß der VoIP-Server nicht, dass sich Telefon B hinter einer Firewall befindet; er ordnet Telefon B der gleichen öffentlichen Firewall-IP-Adresse zu (aber auf einem anderen Port als die Adresse für Telefon A).

3. Etwas später initiiert Telefon A einen Anruf bei Telefon B, indem es eine Anfrage an den VoIP-Server sendet.

Obwohl sich beide Telefone hinter derselben Firewall befinden, weiß Telefon A nicht, wie es Telefon B erreichen kann, da es nur einen Alias oder eine Telefonnummer für Telefon B hat. Als Teil der Anrufanfrage stellt Telefon A dem VoIP-Server Details zu den Medienarten und –formaten bereit, die es verarbeiten kann, zusammen mit den ihnen zugeordneten IP-Adressen und Ports. SonicOS übersetzt diese privaten IP-Informationen, um die öffentliche Firewall-Adresse für Nachrichten zu verwenden, die zurück an den VoIP-Server gehen. Diese Medieninformationen werden außerdem von SonicOS in die interne Datenbank eingetragen.

4. Der VoIP-Server validiert die Anrufanfrage und sendet sie an Telefon B.

Die eingehende Anrufanfrage wird vom VoIP-Server an die öffentliche Firewall-IP-Adresse geleitet. Wenn die Anfrage die Firewall erreicht, validiert SonicOS die Quelle und den Inhalt der Anfrage. Mit den (öffentlichen) IP-Adressinformationen in der Anfrage wird ein Lookup in der Datenbank durchgeführt, um die private Adresse zu ermitteln, an die die Anfrage gesendet werden soll.

Da sich die Informationen zum Anrufer und den Medien auf ein Telefon (Telefon A) hinter dieser Firewall beziehen, übersetzt SonicOS sie mithilfe der internen Datenbank zurück in die privaten Adressen und Ports für Telefon A.

5. Telefon B klingelt, und der Anruf wird angenommen.

Wenn der Anruf an Telefon B angenommen wird, gibt das Telefon Informationen an den VoIP-Server bezüglich der Medienarten und –formate zurück, die es verarbeiten kann, zusammen mit den ihnen zugeordneten IP-Adressen und Ports.

SonicOS übersetzt diese privaten IP-Informationen, um die öffentliche Firewall-Adresse für Nachrichten zu verwenden, die zurück an den VoIP-Server gehen. Diese Informationen werden außerdem von SonicOS in die interne Datenbank eingetragen.

6. Der VoIP-Server gibt die Medien-IP-Informationen von Telefon B an Telefon A zurück.

Die Informationen zum Anrufer und zum angerufenen Teilnehmer in den Nachrichten werden von SonicOS zurück in die privaten Adressen und Ports für die Telefone A und B übersetzt. Telefon A verfügt nun über genügend Informationen, um direkt mit Telefon B mit dem Medienaustausch zu beginnen.

7. Telefon A und Telefon B werden verbunden und können Audio-, Video- oder Datenmedien direkt austauschen.

Durch die intelligente Mitverfolgung der gesamten Anrufeinrichtung erlaubt SonicOS die direkte Verbindung von (durch den VoIP-Server autorisierten) Anrufen zwischen den dahinter liegenden Geräten. Diese Anrufe können sich die Charakteristiken ihres lokalen Netzwerks zu Nutze machen, ohne dass der Datenverkehr unnötigerweise die Firewall verlassen muss.

Interoperabilität von SonicWALL mit anderen VoIP-Anbietern

Es folgt ein Auszug aus der Liste von Geräten führender Hersteller, mit denen SonicWALL interoperabel ist.

H.323

Softphones	
Microsoft NetMeeting	OpenPhone
SJLabs SJ Phone	
Telefone/Videophones	
Cisco 7905	D-Link DV 1000
PolyCom VS-FX	Sony PCS-1
Sony PCS-11	
Gatekeeper	
Cisco IOS	OpenH323 Gatekeeper
Gateway	
Cisco VG200	

SIP

Softphones	
Apple iChat	Microsoft MSN Messenger
Nortel Multimedia PC Client	PingTel Instant Xpressa
Siemens SCS Client	SJLabs SJPhone
XTen X-Lite	Ubiquity SIP User Agent
Telefone/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/-Dienste	
Cisco SIP Proxy Server	Brekeke Software OnDo SIP Proxy
Packet8	Siemens SCS SIP Proxy
Vonage	

Referenzen

[BCR-FORT] Business Communications Review, Stumbling Blocks On The Road To Ubiquitous VoIP (Juli 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, Februar 2004, Light Reading

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

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

[NWFUSION-SBC] Session border controllers have limited lifespan, März 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)