

Standard firewalls are an imperfect solution to the challenge of securing VoIP applications. They do not address the complete set of threats that face VoIP networks and complicate the task of installing and operating VoIP applications. This application note examines the problem.

Voice over IP (VoIP) applications and related Unified Messaging applications are complex. This complexity is evident in both the range of services provided and in type of security threats that face these applications. The Session Initiation Protocol (SIP) is widely used for VoIP, Video, Instant messaging and other Unified Messaging applications. This application note looks at some of the implications of this complexity and specifically why this means that relying on a standard firewall to secure SIP based VoIP not only fails to fully protect the VoIP application but risks compromising other applications.

The need for good IP level security controls is generally well understood and most firewall vendors produce products that do an effective job at securing standard applications such as Web and email. Unfortunately, VoIP is not a standard application and general purpose firewalls are not the best solution for providing VoIP Security.

To understand the reasons for this we must look at the range of threats that face VoIP systems. These threats fall into three main groups.

1. IP Network level threats, the same threats faced by Web, email and other standard IP applications.
2. Application and protocol level threats, including call disruption attacks and denial of service attacks. These attacks can seriously impact the delivered service quality or even trigger a complete service failure.
3. Content level threats, including unauthorised call monitoring, call flooding and nuisance calls.

Other threats such as toll fraud fall into both application and content groups.

Firewalls are effective at addressing IP network level threats. However, because they are general purpose devices, and in many cases are based on a design that pre-dates VoIP, they are unable to examine the contents of VoIP messages. This means that a general purpose firewall simply cannot secure a VoIP system against application and content level threats.

To compound the problem, SIP and other protocols that drive VoIP do not fit well into the firewall security model. All firewalls implement Network Address Translation (NAT). This is done partly for security and partly to provide the necessary translation between private LAN network addresses and public Internet addresses. NAT changes the source and/or destination address of a packet as it passes through the firewall. A problem arises when the protocol packets include embedded network addresses. General purpose firewalls do not examine packet contents and so cannot translate these embedded addresses. In VoIP packets the embedded addresses define the end-points of a call, without these the call will not work.

This means that not only do general purpose firewalls fall short in protecting a VoIP system from application, protocol and content threats, but the NAT transformations they apply to VoIP messages actually break the protocols. VoIP system designers have to go to great lengths to work around these problems. There is a real risk that these problems force the firewall into a configuration where the level of security it provides for both voice and data applications is compromised. This risk is magnified whenever a VoIP connection has to pass through more than one firewall or NAT gateway, for example when a home worker make a call via a DSL router and through the corporate firewall to the IP-PBX. When a VoIP connection has to pass through a second NAT gateway some of the work-arounds used to address the NAT challenges. This problem, the problem of "Far-end NAT traversal", is well known.

SIP Aware Firewalls

Many firewall vendors advertise their products as “SIP Aware”. Strictly speaking, the term SIP Aware should be applied only to products that implement the SIP to a level where they can examine the message contents and map any embedded IP addresses to match the NAT transformations applied to the messages source and destination network addresses. In practice “SIP Aware” has come to mean any Firewall that can pass SIP traffic. As we have seen this includes virtually all firewalls.

A fully SIP Aware firewall does address some of the difficulties of managing NAT and far-end NAT traversal but still fails to address the SIP specific application, protocol and content level threats. This leaves the VoIP system open to a range of threats including authorised call monitoring and a range of call disruption and Denial of Service (DoS).

The Risk

Any VoIP or other Unified Messaging application relying entirely on a standard firewall or even a SIP Aware firewall is unprotected against a set of application, protocol and content threats that can compromise the confidentiality and integrity of any information exchanged, including anything discussed during a phone conversation. The system is also open to a range of DoS attacks that at best can cause serious disruption and at worst can lead to a complete service failure. In addition, the complexity of the underlying protocols means that there is a real risk that in configuring the firewall to handle VoIP, the firewall’s security is compromised to a point that other applications are at risk.

UM Labs SIP Security Controllers

UM Labs have developed a range of SIP Security Gateways that are designed to provide comprehensive security for all SIP based VoIP and Unified Messaging applications. The UM Labs gateways are available in a range of capacities including an entry-level product designed to secure connections to SIP trunks, roaming users and home workers while larger systems are designed for enterprise and service provider use. Each of the products address all of the threats that face VoIP networks, including IP network level threats and the higher level security issues that neither SIP Aware or standard firewalls are not designed to handle.

Feature	UM Labs	SIP Aware Firewalls
Protects against call eavesdropping	✓✓	✗
Protects against nuisance calls and call flooding	✓✓	✗
Protects against call disruption attacks	✓✓	✗
Protects against SIP level DoS attacks	✓✓	✗
Enables VoIP without compromising other applications	✓✓	✓
Far-End NAT Traversal	✓✓	✓✓
Local NAT	✓✓	✓✓
IP Level Security	✓✓	✓

About UM Labs UM Labs Ltd. was founded in 2008 by security software pioneers dedicated to the promotion of secure global standards for unified communications. The company has an extensive support organization and partner network, with offices in the following locations:

United Kingdom

Heathrow Blvd 4
280 Bath Road
West Drayton
UB7 0DQ
UK
Phone: +44 20 3021 3200

Website: um-labs.com

USA

5586 Main St, Suite 206
Williamsville
NY 14221
USA
Phone: 716 568-4931

Email: info@um-labs.com

Canada

366 Adelaide St, Suite 301
Toronto, ON
M5V 1R9
Canada
Phone: 416 598-7537

VoIP: sip:info@um-labs.com