RC-2100
SIP Security Controller for Trunks and Remote Connections

The range of SIP Security controllers from UM Labs is designed to deliver cost effective and easy to use Security for VoIP and other Unified Messaging Applications. Each product in the range combines strong Firewall grade security with application and content specific controls to address the complete range of VoIP and UM Security Threats.

Product Features

Security Protection, Control and Service Enablement for remote users and SIP trunks

Protection:

Against VoIP/SIP security threats

- SIP /RTP DoS attacks
- Spoofing
- Media Anomalies
- Malformed SIP messages
- wire tapping

Against IP-level security threats

- Stateful IP Firewall
- Dynamic pin-holing for RTP streams

Control:

Operating System

- Firewall Grade security
- Optimised for VoIP service delivery

Service Enablement:

NAT Traversal

- Local NAT
- Far-End NAT traversal (*without* the complexity of STUN)

Confidentiality

- SIP-over-TLS, up to 256 bit AES
- SRTP with SDES key exchange
- SRTP with ZRTP key exchange (additional license required)
- SRTP gateway with termination
- SRTP pass-through
- HTTP digest authentication for all qualifying SIP requests

The Challenge

Unified Messaging encompasses a wide range of applications from VoIP and Video Conferencing through email and IM to Presence based applications which allow users to signal their availability and ensure that calls and messages are routed in the most effective way.

While each of these applications runs on an IP Network, their security requirements are very different. Security controls for VoIP and Video conferencing must recognise the real-time nature of these applications and guard against call flooding and unauthorised call monitoring while the security requirements for Instant Messaging are closer to those for email and must include content filtering and Spam prevention.

The range and complexity of VoIP and UM applications means that securing these applications needs more than a general purpose Firewall. While general purpose Firewalls have a role to play they cannot protect VoIP and UM applications from full set of security threats that these applications face.

Effective security for VoIP and UM means combining strong Firewall security controls with application and content specific security. The range of security gateways from UM Labs is designed to deliver cost effective VoIP and UM security for all types of network.

The Business Requirement

One of the key benefits of VoIP and UM applications is their ability to integrate Voice Telephony and Video Conferencing with other messaging applications and to extend that integrated service to all parts of an organisation. VoIP services can be extended to beyond the perimeter of an organisation's network, to provide links to branch offices and remote workers, to enable SIP trunks to be used as an alternative to a standard phone line, or even to allow direct calls to other Internet users.

Realising these benefits and gaining the maximum return on investment generates two requirements. Firstly, full integration of Voice and Data networks. Secondly, changing existing security controls to permit VoIP traffic to pass through the network perimeter, extending the service to both branch offices and remote users and allowing connections to SIP trunks.

These requirements are incompatible with the design and implementation of many VoIP systems where voice are data run on separated networks and the perimeter firewall does not permit VoIP traffic.

The Solution

The RC-2100 from UM Labs Ltd is designed as a cost effective SIP security gateway combining the full set of security controls needed to enable remote SIP connections for VoIP, Video Conferencing, SIP based Instant Messaging and Presence based applications. The RC-2100 provides the security needed to safely enable the integration of voice and data networks.

Management

- Secure and intuitive Web GUI
- Remote Syslog
- Streamlined software upgrade process

Specification

- Three 10/100 Fast Ethernet ports (RJ-45)
- One RS-232 console port
- No moving parts, fan-less
- Green Appliance
- Hardware watchdog
- Hardware random number source
- Handles 10 or more concurrent calls

Compliance

Hardware

- RoHS
- WEE

Software

- RFC 3261
- RFC 3711
- RFC 4568
- RFC 2617

Licensing & Availability

- Up to 20 connections (registered remote users or SIP trunk lines)
- License upgradeable

Contact

UM Labs Ltd
Heathrow Blvd 4
280 Bath Road
West Drayton
UB7 0DQ
UK

Email: info@um-labs.com
VoIP: sip:info@um-labs.com

Revision 1.3 August 2008

The RC-2100 combines Firewall grade network security with SIP application and content controls and provides gateway and pass through encryption for both call set-up and media traffic. These controls are supplemented with authentication services for both signalling (SIP) and media (RTP) ensuring complete privacy and confidentiality for all remote connections.

The RC-2100 hardware is designed for silent operation and low power consumption allowing installation in any environment. The system include a hardware watchdog to ensure continuous operation and a hardware random number source which is used to generate high quality encryption keys for both signalling and media encryption.

Benefits

- Cost effective, comprehensive security for remote users and SIP trunks.
- Full integration of IP Firewall controls with SIP application security, controls, encryption services and authentication of sensitive operations, simplifying configuration, reducing deployment time and avoiding costly integration effort.
- Runs as a dedicated VoIP application level gateway and firewall, avoiding corporate firewall configuration changes which could weaken the security of other applications
- Full standards compliance, ensuring interoperability with any standards based VoIP Phone or PBX
- Local Network Address Translation (NAT) and Far-end NAT traversal support, enabling service provision to remote users connecting via 3rd party firewalls and other NAT gateways without the need for additional protocol support

Deployment

The RC-2100's strong IP Firewall security layer enables the product to be deployed in parallel with a general purpose Firewall. This preferred configuration provides a secure dedicated channel for VoIP traffic, safeguarding call quality and avoiding security compromising configuration changes to the existing Firewall.

The RC-2100 also includes the additional feature need to enable an alternative deployment; connected to the DMZ of an existing Firewall.