
# SIP Security Controllers

## Product Overview

Document Version: V1.1
Date: October 2008

# 1. Introduction

UM Labs have developed a range of perimeter security gateways for VoIP and other applications running the Session Initiation Protocol. The products in this range are named *SIP Security Controllers* and are designed for enterprise users. The entry level product is designed as a low-cost device supporting up to 10 or 20 concurrent calls, the product line scales to a rack-mountable system that can be clustered to support up to 1,000 concurrent calls.

In addition to providing much needed security features, the UM Labs SIP Security Controller includes a number of features designed to simplify the interconnection of VoIP Networks and remote SIP users. These functions include local Network Address Translation (NAT) and the ability to handle far-end NAT traversal without the need to manage complex firewall configurations or to use additional protocols.

This overview provides a high level description of the product, presents some sample deployments and outlines the product's benefits.

# 2. Product Design

SIP based VoIP applications use a number of different protocols. These include Session Initiation Protocol (SIP) to handle signalling (call set up, call termination and related functions) and the Real-time Transport Protocol (RTP) to handle media (the voice or video stream). For VoIP calls, a third protocol, Session Description Protocol (SDP) provides an interface between SIP and RTP. SIP also handles other application such as presence and Instant Messaging. The UM Labs SIP Security controllers are designed to handle and to secure all of these protocols and applications.

UM Labs' SIP Security Controllers are designed to process all SIP and related traffic crossing a network boundary. In most cases that network boundary is the perimeter of a corporate network where the controller handles VoIP calls between the corporate PBX and other networks. These other networks may include branch offices, remote users and SIP trunk services or even calls made to and received from other users over the Internet. The SIP Security Controllers may also be used to interconnect network segments within a larger organisation or for service provider deployment where the controller will relay calls between the service provider's core systems and customer connections. The product is supplied as a range of appliances of varying capacities. Each model in the range is supplied with multiple network interfaces.

The shipped appliance includes a hardened operating system, all necessary security software and a Web interface for configuration and management. The security software implements the controls needed to protect VoIP network components, to provide control over SIP message routing and to offer a number of service enablement features aimed at simplifying VoIP network deployment.

## 2.1. Security

The SIP Security Controller implements security controls at three levels:

- IP Network level
- Protocol and Application level
- Content level

### 2.1.1. IP Network Level Security

The IP Security module is designed to protect both the SIP Security Controller and any other VoIP Network components from IP Level security threats. VoIP is an IP application and therefore faces a similar range of threats to other IP applications such as Web and email. Protecting VoIP applications from these threats is complicated by the fact that the network protocols used to drive VoIP use a wide range of network ports and cannot easily be handled with the same simple security rules that are used to protect other application such as web and email. In addition the VoIP protocols do not work well with devices that implement Network Address Translation (NAT). As virtually all firewalls, DSL routers and WiFi hotspots are NAT gateways, then configuring standard IP firewalls and VoIP devices to work together is always a challenge.

The UM Labs SIP Security Controllers solve this problem by automatically configuring the IP security module to support the configured VoIP traffic flows, while at the same time maintaining a high standard of protection against IP network level threats. The SIP Security Controller's IP security module is designed to conform to the US Government's protection profile entitled *Firewall for Medium Robustness Environments*.

### 2.1.2. Protocol and Application Security

All VoIP protocols and applications and specifically those applications using SIP are potentially susceptible to a wide range of protocol and application specific vulnerabilities. These include a number of flooding vulnerabilities and call disruption attacks. Details of these attacks are available on the UM Labs website. The consequences of these threats range from user inconvenience through service disruption to complete service failure. Standard security technologies are not able to protect against these threats because these threats are exploited by sending valid protocol requests. Any standard security gateway that is configured to permit VoIP traffic will be unable to block these malicious requests.

The UM Labs SIP Security Controllers protect against this set of security threats by tracking the status of each call, insuring that any protocol requests received are in the correct context, that they originate from a valid source and where possible these requests are authenticated. The SIP Security controller also detects and blocks flooding attacks by limiting the rate at which an individual system can send requests and by controlling the maximum request rate permitted for any single network interface.

The SIP Security Controllers provide encryption for SIP signalling. Many of the more serious call disruption threats are dependent on monitoring SIP traffic. Encrypting that traffic is an effective defence.

### 2.1.3. Content Security

Content security threats affect the media streams generated by SIP applications; the audio or video stream or perhaps an Instant Message generated by a SIP IM client. The single biggest risk is that of call hijacking, but related threats such as RTP injection, where an attacker feeds an alternate media stream to replace or disrupt an existing stream cannot be ignored.

The SIP Security Controller protects against these threats in two ways. Firstly by carefully monitoring the media streams to ensure that only valid streams previously negotiated by the signalling protocol as part of the call set up are permitted and secondly by encrypting the media streams wherever possible.

The SIP Security Controllers implement SRTP media encryption and offer two alternative key exchange options. These are RFC 4568 (SDES) and ZRTP. ZRTP is an additional cost option. For more details on the encryption services provide by the SIP Security controller, see section 2.4.

## 2.2. SIP Message Handling

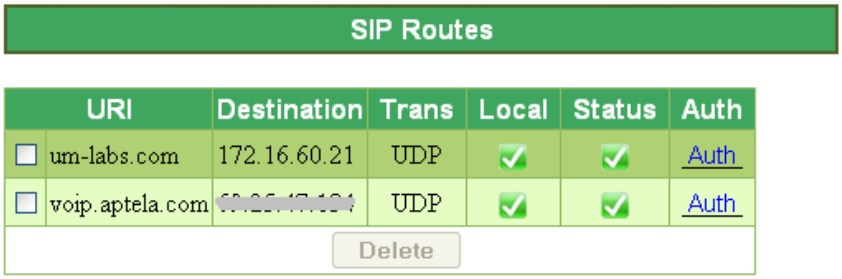
The UM Labs SIP Security Controllers process and validate all SIP messages passing between its connected networks. To enable the correct processing of these messages, the first message in each SIP transaction (setting up a call, terminating a call etc) is examined to determine the appropriate destination for that message. All subsequent messages in that transaction are then delivered along the same path according to the rules specified in the SIP standard.

The Security controller applies a standard set of routing rules to direct the calls to the appropriate destination. These rules are applied to the first message received for each new transaction, these are:

- The message is checked to see if its destination is a device that has previously *Registered* via the SIP security controller (see below); if so the message is sent to that device. This ensures that calls destined for phones and other devices on remote networks are always correctly processed with the SIP Security Controller handling the complexities of traversing NAT gateways.
- The message is checked against a static SIP routing table set up by the administrator. If a match is found the message is delivered to the indicated destination. This enables the SIP security controller to operate as the entry point for all inbound SIP messages and to ensure that those messages are correctly delivered to the PBX handling calls for a specific domain or group of users.
- Finally, if the message has not yet been delivered, the SIP Security Controller applies the standard SIP message processing rules and looks up the destination domain using a domain name server.

This routing process ensures that all messages are correctly delivered, and that the system administrator is able to exercise control over messages designated for local systems. In most cases the only configuration needed is for the administrator to identify the local domains and to define the PBX that handles calls for each of those domains. The Security Controller can handle calls from multiple domains routing each to a different PBX (see Figure 1). The destination PBX

for a specified domain may be located on a private network or may be located across the




Internet on a remote site.

Figure 1 SIP Route Control

Each domain may also be defined as a *local* domain. In this context a local domain is one under local control.

If a network includes branch office users, home workers or roaming users, then their phones should Register via the SIP Security Controller. In SIP terms the Security Controller is a *Proxy Registrar.* Registration is the process where a phone identifies itself to the PBX and provides its current network location so that the PBX can send it calls. By operating as a Proxy Registrar, the SIP Security Controller is able to keep track of each remote phone so that the routing process described operates correctly. The Security Controller is also able to detect changes in a phone's network address (a fairly common occurrence, especially if the connection is from a roaming user). While such changes may be completely valid, they may also represent a call hijack or spoofing attack. The Security Controller ensures that any detected changes are validated and where appropriate the remote device is re-authenticated.

## 2.3. Service Enablement

The SIP Security Controller's service enablement features include handling all local Network Address Translation (NAT) and managing far-end NAT traversal. These features are entirely automatic requiring no intervention from the network administrator. The Security Controller monitors each SIP message and determines when NAT needs to be applied locally and more importantly when it needs to compensate for address changes made by remote NAT devices. This avoids the need for additional configuration either on the phones connecting to the network or on the PBX. Avoiding these potentially complex configuration changes makes the task of deploying the VoIP network much simpler and reduces the risk of encountering problems during the installation and consequently reduces the overall implementation cost.

## 2.4. Encryption

One of the key functions of the SIP Security Controller is to protect calls by encrypting both the SIP signalling and the RTP media stream. The SIP Security controller follows the standards for encryption using Transport Layer Security (TLS) to protect SIP traffic and Secure RTP (SRTP) to encrypt the RTP media streams. If a connecting phone or other device supports either of these encryption protocols, then the SIP Security Controller will automatically encrypt the SIP

Signalling, the RTP Media or both. This means that if a remote user has a hardware or software phone that supports standards based encryption, the SIP Security Controller will automatically encrypt calls to and from that user. Equally, if a SIP trunk service provider is running a UM Labs SIP Security controller, or has a gateway which supports the same standards then calls to and from that service provider will be encrypted.

While SRTP is the preferred standard for RTP encryption, SRTP does not specify how the encryption keys used to protect a media stream are established. SRTP uses a new key for each media stream and then discards the key at the end of the call. This means that a voice call will use two encryption keys as voice calls have one media stream in each direction.

As two news keys must be generated for each voice call, a secure an effective key exchange mechanism is essential. The SIP Security Controller supports the two most widely implemented. These are the standard defined by RFC4568 which has the rather unwieldy name of *Session Description Protocol Security Descriptions for Media Streams* (SDES) and the more succinctly named ZRTP.

SDES, as its name suggests uses SDP which in-turn is carried by SIP to exchange SRTP encryption keys. Its effective use depends on the use of TLS to protect the SIP signalling. SDES is included as standard in the SIP Security Controller. The Controller will always offer an SDES key if the SIP signalling is running over TLS. If the remote system does not support SRTP then the call will fall back to using clear text RTP.

One of the disadvantages of SDES is that the encryption keys are visible to any intermediate SIP routing devices. This will include any SIP routers or application servers operating by a SIP Trunk provider or other telco organisation. ZRTP was designed by Phil Zimmermann, creator of PGP email encryption to overcome this problem. ZRTP is a key exchange protocol that sets up SRTP encryption keys, but uses the media stream to establish those keys. This means that the key exchange is not visible to any intermediate SIP processing device. ZRTP is available as an additional cost option on all models of the UM Labs SIP Security Controller, it is designed to provide an additional level of media security for remote uses calling into a corporate VoIP network.

## 2.5. Call Recording

There are many cases when it necessary for an organisation to record both inbound and outbound calls. This is common practice in call centres and is also a requirement in many other types of organisation where there is a regulatory requirement to record and archive all forms of external communication. The larger models of the SIP Security Controller provide call recording as an additional cost option. Recorded calls are saved as WAV files and indexed by date, caller and call recipient. If an encrypted call is received, then the call is recorded after decryption.

## 2.6. Appliance Capacity

Two models of the SIP Security Controller are currently available.

The RC-2100 is an entry level device designed for small scale networks and branch offices and can be licensed to handle up to 20 concurrent calls. The RC-2100 ships as a desktop style appliance.

The EC-4200 is the enterprise level product. It is a 1u Rack mount device which can be clustered for higher levels of throughput and resilience or used as a standalone device. The entry level EC-4200 is licensed for 50 concurrent calls, a cluster can handle up to 1,000 concurrent calls.

## 3. Deployment

As discussed in section 2, the SIP Security Controller is designed as a perimeter security appliance and is normally deployed at the network perimeter. However a number of variants on this design are possible.

The preferred deployment is to install the SIP Security Controller alongside the general purpose firewall (see Figure 2). In this configuration, the Security Controller handles all SIP traffic and related protocols (such as RTP for voice and video streams) freeing up the general purpose firewall to handle all other applications.

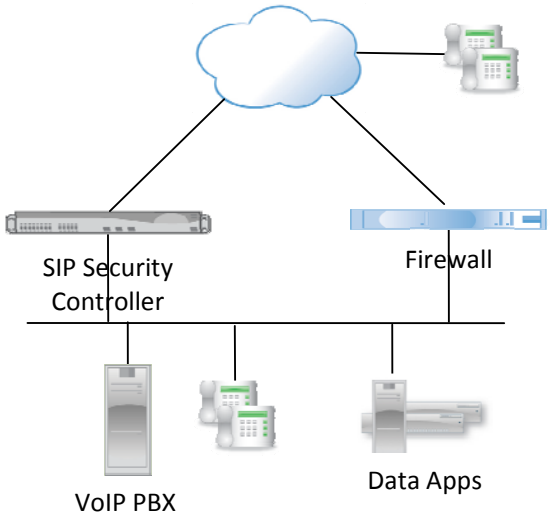



**Figure 2 Preferred Deployment**

This configuration is safe because the Security Controller includes an IP security layer that provides the IP firewall protection needed. This IP Security Layer is optimised for SIP and related protocols and dynamically adjusted so that only data streams assigned to valid calls are permitted to pass. As this optimisation depends on a detailed examination of the SIP requests that initialled a call, the SIP Security Controller is able to implement a more rigorous set of security controls than any standard firewall can achieve.

However, the security policy adopted by some organisations may prohibit this preferred deployment. In this case an alternative deployment where the SIP security controller is

connected between the firewall's DMZ and the internal network, or even configured with a single interface and connected behind the firewall (see Figure 3).

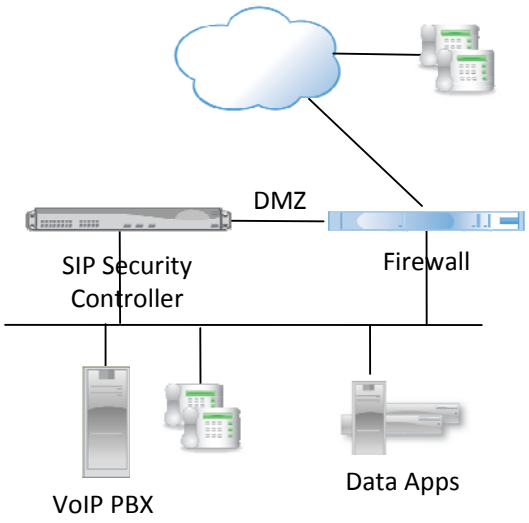



**Figure 3 Alternative Deployment**

The disadvantage of this approach is that all SIP traffic as well as all media traffic must pass through the Firewall. This means that a potentially large range of ports must be opened on the Firewall, this risks compromising the security of other network components and applications.

Either of the deployments described above can secure calls to and from SIP trunks and well as connecting remote users. In cases where a number of remote users are located in a branch office, it may be convenient to deploy a second, smaller, SIP Security controller at that location. This second system will then secure all calls to and from the branch, automatically encrypting both the SIP signalling and the RTP media between the two SIP security controllers. This means that all calls transmitted over this link will benefit from encryption regardless of the capabilities of the phones in use.

In most cases the branch office will have a NAT gateway, possibly just a DSL router. The SIP security controller will work in this configuration.

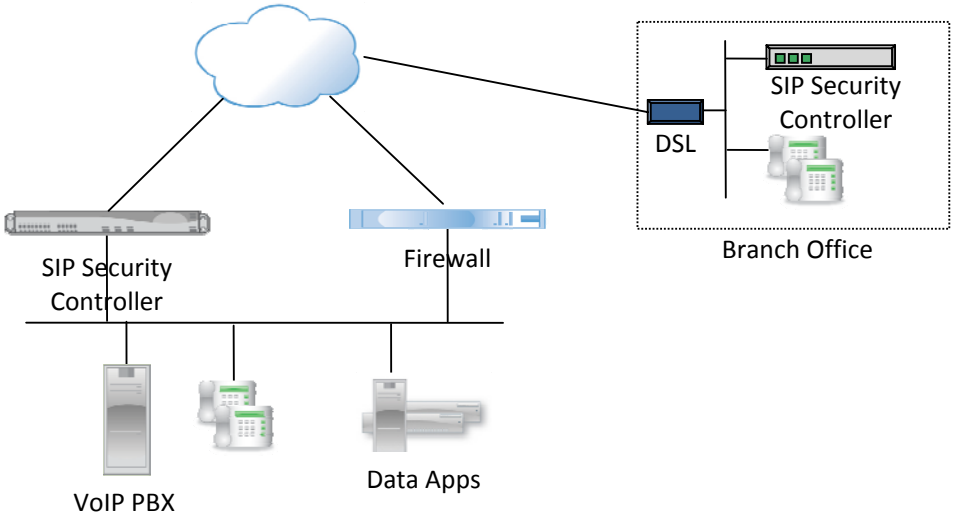



Figure 4 Branch Office Link

## 4. Management and configuration

When compared with email and web VoIP is complex. This complexity means that interconnecting VoIP systems can be complex. The SIP Security controller from UM Labs aims to reduce this complexity by making the system configuration and deployment as simple as possible.

All configuration and management operations are carried out using a simple to use Web GUI. The GUI provides context sensitive help for virtually all setting to compliment the more detailed information provided on the product manual.

In most cases the only configuration that is needed, is to assign IP addresses to one or more of the SIP Security Controller's network interfaces and to set up other network details (see Figure 5). Once this is done a SIP route should be set up as shown in Figure 1. At this stage the system is ready for use. The SIP Security Controller will automatically handle NAT and far-end NAT traversal and also automatically set up the IP level security which on a standard firewall would require significant planning and testing effort.

The Web GUI also provides more complex configuration functions such as setting up and managing encryption and viewing logs and activity reports.

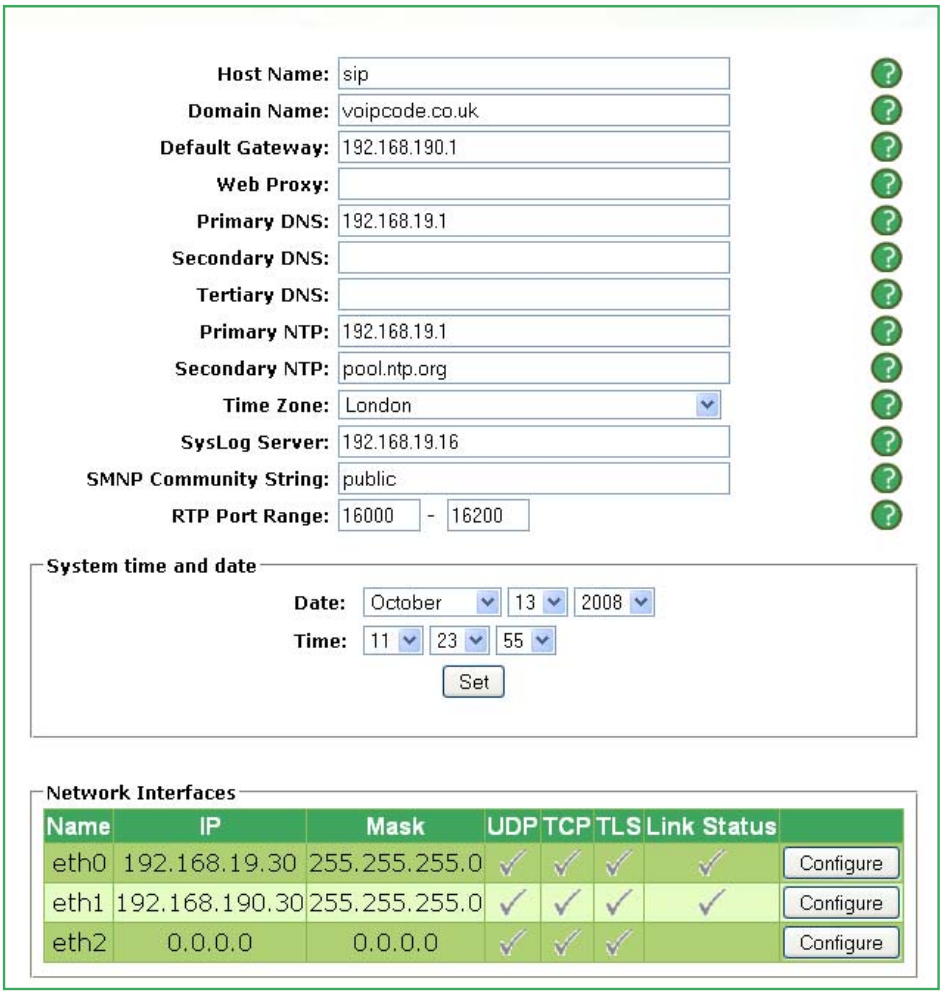



Figure 5 SIP Security Controller Network Configuration

## 5. Benefits

VoIP and related applications come with the promise of changing the way we communicate both in our business and personal lives by bringing together real-time messaging, voice, video and IM with more traditional communications applications such as email. VoIP is the foundation stone of Unified Messaging and Unified Communication.

It follows that to reach this goal, VoIP applications must reach the same level of availability, portability and geographic reach that we have come to take for granted when using email. Today virtually everyone has an email box, devices to access that mailbox are highly portable and once connected we can exchange messages globally using only an easy to remember address. Most VoIP networks have not yet reached this goal. It is still common to see a corporate VoIP network running in isolation, no external connections and not even any direct link with the corporate data network. These reasons given for this isolation include security concerns and implementation difficulties.

The SIP Security Controllers from UM Labs deliver one simple but compelling set of benefits; to enable those remote connections by protecting VoIP network components from attack and to

hide the complexities of running VoIP and other SIP based applications across network boundaries and through remote Firewalls and NAT gateways.

Even if you are not planning a full-sale Unified Communications deployment, but want to secure a SIP trunk connection or provide a VoIP service to a branch office or to remote users you still face the same set of problems.

The UM Labs SIP Security Controller offers a packaged, easy to install solution to secure and manage any remote VoIP connection and to implement that connection in a timely fashion.

For more information on the UM Labs range of SIP Security Controllers, please visit our web site or contact us.

**Web:** http://www.um-labs.com

**Email:** info@um-labs.com

**VoIP:** info@um-labs.com

**Phone:** +44 20 3021 3200