

Session Border Controls are touted by some as the answer to securing VoIP and Unified Messaging Applications. However, SBC's were not originally designed as security gateways, at least not to provide the level of security needed to safely add public IP links to VoIP networks. This application note reviews the limitations of SBCs and suggests alternatives.

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 the 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 a Session Border Controller (SBC) does not provide the ideal solution for securing most SIP networks, particularly when security is needed at a network perimeter.

Session Border Controllers

The term Session Border Controller (SBC) has been applied to a wide range of product types. Originally, SBCs were designed to provide peering connectivity between different carriers. In this role SBCs are called on to relay VoIP traffic between two relatively well controlled networks, albeit networks under the control and management of different organisations.

The task of linking two carrier networks is radically different from the problem that most enterprises are facing; providing perimeter security to enable VoIP and Unified Messaging services to be extended to home workers and roaming users and to allow the connection of SIP Trunks. These services require links to public IP networks, a much less ordered environment than carrier backbones.

Most SBCs are focused almost exclusively on providing peering connectivity for VoIP with very little support for the value added applications that protocols like SIP are delivering. SIP was designed to deliver new applications such as presence and Instant Messaging and to drive the closer integration with data networks. The fact that SBCs focus on VoIP leaves them less able to secure these newer applications.

The SBC's carrier heritage also means that they include features that are of little value to an enterprise or service provider wanting to secure SIP based VoIP and Unified Messaging. These features include support for multiple VoIP protocols, protocol conversion and codec conversion (transcoding). Supporting these features requires large and expensive hardware placing the entry level cost of an SBC at between \$25K and \$100K.

Unified Messaging Security

The challenge faced by enterprises and service providers alike is to provide perimeter security for VoIP and other SIP based applications. This requirement is driven by the need to provide a consistent service to all users regardless of their location. Just as users expect easy access to web and email so they expect the same level of service from VoIP and Unified Messaging. One of the key benefits of Unified Messaging is its ability to integrate all forms of business communication, this aim cannot be realised without effective security controls.

Unified Messaging applications face threats at many levels:

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. SBCs do not include the security controls needed to address all of these threats. The level of security offered is product dependent, but as a category SBCs are less effective than

standard firewalls at addressing IP Network level threats, provide little if any protection against content level threats and offer only partial protection against application level threats.

The Risk

SBCs were designed to operate in the relatively controlled environment of carrier backbone networks; they are less well suited to public IP networks. Most SBCs lack the features needed to protect VoIP calls against unauthorised monitoring, to block a range of application level DoS attacks and to provide the policy and content controls needed to other messaging applications. A system not fully protected against these threats is at risk of an attack that at best can cause serious disruption and at worst can lead to a complete service failure.

UM Labs

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 is designed to address the complete set of threats faced by VoIP and UM applications. The focus on providing perimeter security controls means that a UM Labs Gateway delivers a more effective security solution than an SBC and can omit many of the more complex features that have no direct security function. This means that UM Labs can deliver a much more cost effective solution to the problem of securing SIP based VoIP and Unified Messaging than any SBC.

Feature	UM Labs	Session Border Controller
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	✓✓	✓
Policy and content controls for other SIP based applications	✓✓	✗
Far-End NAT Traversal	✓✓	✓✓
Local NAT	✓✓	✓✓
IP Level Security	✓✓	✓
Entry Level Cost (approximate)	\$2K	\$25K +

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