covergence

secure SIP trunking

More and more enterprises are discovering the value of voice over IP (VoIP) and other applications based on SIP, the Session Initiation Protocol. But as they migrate to VoIP, enterprises are faced with a challenge: What's the best way to interconnect IP PBXes and other SIP systems—like Microsoft Office Live Communications Server (LCS)—between sites? How can they make the most cost-effective use of wide-area IP services and still maintain the quality of service (QoS) and network security they require? Purpose-built to provide comprehensive security and control for VoIP and other SIP applications, Eclipse™ from Covergence is the first solution that meets the challenge of secure SIP trunking.

One Clock Tower Place, Suite 200
Maynard, MA 01754

978 823 5300

www.covergence.com

The Business Imperative

Conditioned by decades of TDM-based telephony, business users expect secure, "toll-quality" service from their phone systems. At the same time, enterprise IT managers want to take advantage of in-place and cost-effective wide-area services used to interconnect company sites. But as VoIP calls traverse untrusted networks like the Internet, they are subject to attacks intended to disable, disrupt or degrade service delivery, to steal service or illegally obtain user information.

Generic solutions like virtual private networks (VPNs) provide a modicum of security, but are a poor fit for delay-sensitive VoIP and multimedia applications. Only an application-specific solution like Eclipse can create secure SIP trunks through untrusted networks without sacrificing either QoS or the cost advantage of public IP transport.

The SIP Trunking Challenge

With email or web browsing, a few seconds' delay or an occasional resend goes unnoticed. But with VoIP, a small delay or the loss of a few packets can destroy the quality of the call. Security mechanisms increase the risk of unacceptable performance by introducing delay into the packet stream, and the "stronger" the level of security, the greater the potential delay.

SIP's dual-path architecture adds to the challenge. With most applications, control traffic and data traffic share a single protocol—HTTP for web browsing, SMTP for email, etc.—and a single end-to-end network path. But with SIP applications, at least two protocols and two paths are involved—one for signaling and one for media. This dual-path design allows signaling and media capacity to scale independently, but it also creates a significant vulnerability, since no network element has a coordinated view of both traffic streams

VPNs do not distinguish between voice and data or between signaling and media. Everything is lumped together at the same priority, and as traffic levels increase, voice quality suffers. Moreover, because VPNs are not "VoIP-aware," they cannot route media flows intelligently. A VoIP call between two branch offices might be backhauled to a central site via one VPN and then forwarded to its destination via another. The call passes through three VPN devices and is encrypted and decrypted twice, consuming double the bandwidth and incurring at least twice the delay of a more direct path.

Eclipse Meets the Trunking Challenges

Designed to secure SIP services without sacrificing performance or QoS, Eclipse delivers secure, efficient trunking between IP PBXes and a variety of other SIP devices. Authentication, encryption and validation protect both signaling and media flows as they cross untrusted networks. QoS is assured by a combination of bandwidth and QoS-based call admission control; QoS mapping, monitoring and marking; and QoS-based routing. Support for standard protocols ensures that Eclipse works with any SIP-enabled PBX or application server.

Feature	Description and Benefits
Authentication and Access Control	Prevents a wide range of attacks by denying access to malicious, unauthenticated users and domains.
Signaling Encryption	Standard Transport Layer Security (TLS) encryption ensures the authenticity, confidentiality and integrity of SIP signaling streams to prevent attacks that exploit the visibility of signaling information (e.g. call hijacking attacks).
Signaling Validation	Performs syntactic and semantic validation of signaling streams to prevent service theft and attacks based on the injection of invalid signaling information (e.g. buffer overflow attacks).
Media Encryption	Encrypts media sessions (audio, video, file transfer, etc) using the Secure Real-time Transport Protocol (SRTP) to ensure the authenticity, confidentiality and integrity of real-time media information. Prevents attacks that exploit the visibility of media streams (eavesdropping, media injection attacks, etc.).
Media Validation	Prevents service theft by ensuring that all media sessions between SIP user agents are the same as the sessions that were negotiated during the session set-up.
Performance	Without sufficient processing power, VoIP security mechanisms will decrease the number of calls that a security appliance can support. Eclipse scales to support hundreds-of-thousands of VoIP sessions without sacrificing call capacity or QoS.

By creating separate logical trunks—VPNs for data, secure SIP trunks for voice—enterprises can ensure the security and performance of delay-sensitive VoIP traffic. Rather than contend for bandwidth with miscellaneous data traffic, voice flows get the high-priority treatment they require. And rather than make do with generic security, SIP signaling and media flows receive complete application-aware protection.

Because it is VoIP and SIP-aware, Eclipse supports complex full-mesh or partial-mesh trunking topologies with both least-cost and QoS-based routing (Figure 1.1). By reducing or eliminating VoIP backhaul, direct routing between endpoints improves QoS and saves money. Alternate routing increases service availability by automatically bypassing network outages.

Of course, secure SIP trunks can interconnect more than just SIP PBXes. A secure SIP trunk between Microsoft Office LCS at a branch office and a central-site SIP PBX allows branch office employees to make and receive calls using Microsoft Office Communicator. With a SIP-enabled access device as a TDM-to-VoIP gateway, a secure SIP trunk could even interconnect a TDM PBX and a SIP PBX. In all cases, Eclipse safeguards VoIP QoS and secures the connections between enterprise sites.

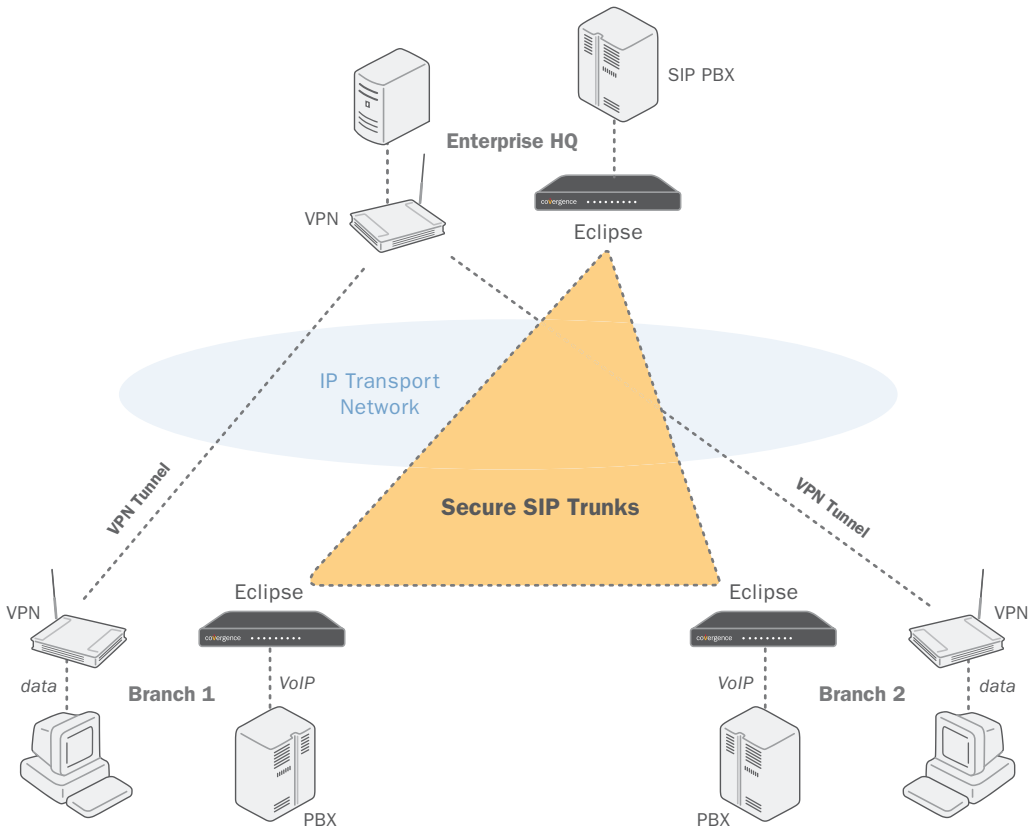

Diagram 1.1

Customer Solution:
Secure SIP Trunking Between Campuses

A large university uses a carrier's Multi-Protocol Label Switching (MPLS) service to interconnect IP PBXes on campuses in two cities. Although MPLS provides logical separation between different customers' traffic, the university wanted the added protection of site-to-site encryption. IPSec VPNs were deemed too cumbersome, so the carrier suggested an Eclipse solution. Eclipse appliances at both campuses ensure the security of SIP signaling and media traffic as it crosses the carrier backbone (Figure 1.2). The Eclipse appliances also act as firewalls and handle Network Address Translation (NAT) traversal. The Eclipse solution further protects the university's campus networks by hiding their topology from the carrier network.

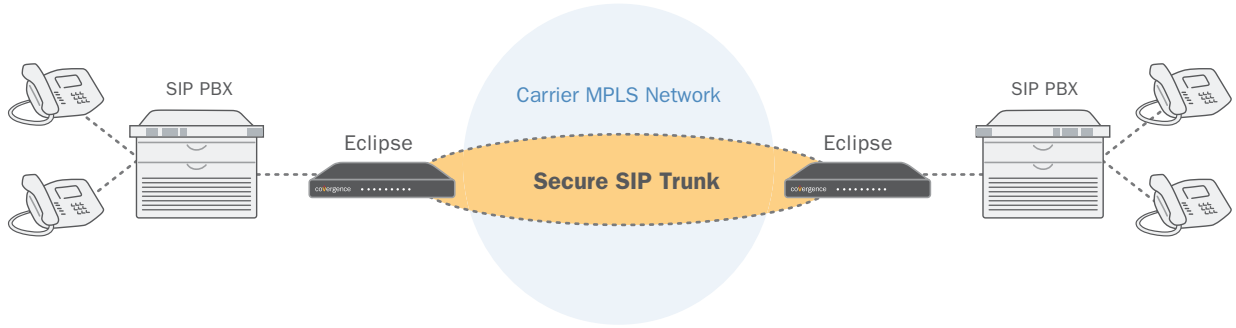

Diagram 1.2

Customer Solution:
Accelerated SIP Migration

After years of mergers and acquisitions, a global manufacturing company depends on multiple vendors' IP telephony gear to support its internal voice network. In some cases, offices are interconnected over the Internet with H.323 as the signaling protocol. In other cases, media gateways and TDM tie lines provide the inter-site links. The company wanted to rationalize its infrastructure by converting to SIP signaling throughout, but worried about the security of using SIP over untrusted networks. By deploying an Eclipse solution, the company is able to move forward with confidence (Figure 1.3). Eclipse is compatible with a variety of vendors' IP PBXes, so the company can upgrade its PBXes from H.323 and use SIP end-to-end. Eclipse provides the secure SIP trunking that the company requires to create an all-SIP environment with no reduction in security or performance.

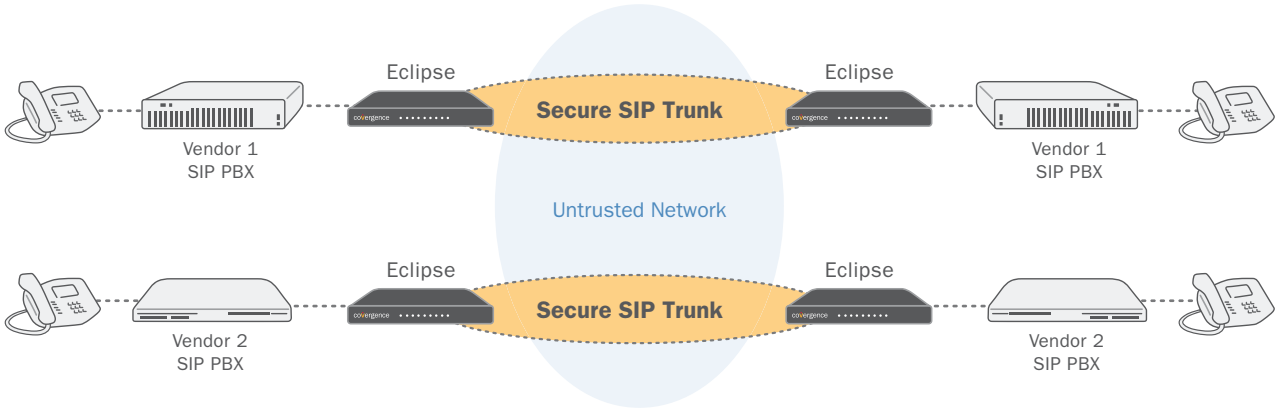

Diagram 1.3