Cisco WebEx Connect IM security:

Enterprise Instant Messaging through a commercial-grade multilayered architecture

Cisco WebEx LLC
3979 Freedom Circle,
Santa Clara, CA 95054 USA

Main: +1.408.435.7000
Sales: +1.877.509.3239

www.webex.com

Abstract

Collaboration and communication solutions empower enterprise teams to find, connect to, and work efficiently with colleagues both inside and outside the organization. To deliver an integrated solution—combining presence, enterprise-grade instant messaging, audio and video conferencing, voice over IP (VoIP), telephony, and more—without adding complexity to their existing infrastructures, IT organizations are turning to hosted collaboration solutions. Businesses demand that hosted services build in enterprise-class security, without compromising the company's privacy or weakening the protection of sensitive files and communications. Cisco WebEx™ Connect IM offers organizations the advantages of a multilayered security strategy derived from more than 10 years of experience and investments in hosted collaboration solutions.

This paper overviews the security factors that make WebEx Connect IM a robust, highly available, and secure Enterprise Instant Messaging (EIM) solution. The overview begins with a description of in-the-cloud security measures, then provides information about the measures taken to protect data in motion, authenticate users, and help IT manage policies. Specific issues and security features relating to instant messaging and shared spaces are also explained, as well as compliance and auditing practices relating to WebEx Connect IM.

Introduction

Today's IT professionals are caught in the middle of a struggle. They must balance increasingly stringent cost controls, minimize complexity, and improve manageability of the infrastructure, while still providing employees with access to the latest technology innovations.

Today, many users within organizations ranging from small businesses to global enterprise organizations use consumer IM solutions such as AOL Instant Messenger ™ (AIM), GoogleTalk™, or Yahoo! Messenger ™. While these solutions work well for consumers, they represent several risks to corporate networks and challenges to IT organizations including:

- Unencrypted IM traffic running through public networks with servers unprotected by firewalls
- Information exchanged during IM sessions that could be stored on unsecure systems
- Lack of virus scanning or spam filtering
- Spoofing and other misuse of domain names caused by consumer IM solutions do not provide professional domain names and user ID's
- The inability of IT to dictate policy or usage of consumer IM systems other than locking down the entire IM application within a network

WebEx Connect IM allows IT departments to satisfy the requirements of both corporate management and users. The hosted service delivers EIM services securely over the Internet, so organizations no longer have the burden of adding hardware infrastructure complexity and management overhead. The WebEx Software- as-a-Service (SaaS) solution makes it easy for IT to implement updates. Cisco updates the service rapidly, so users always have the most up-to-date features available.

WebEx Connect IM runs over a security framework that can be used by key collaboration applications such as instant messaging and spaces. This infrastructure, called the Cisco WebEx Collaboration Cloud, is a system of highly secure and redundant data centers located around the world. Backed by this "always secure" architecture, WebEx Connect IM is based on a multilayered security model that maximizes data security and ensures service continuity. The contributing components include:

- In-the-cloud security, to protect physical sites and introduce stringent controls over Cisco personnel that administer and manage the service
- Data-in-motion security, to safeguard message transport between WebEx Connect IM clients (user desktops, mobile users, and web clients) and the WebEx Collaboration Cloud
- Data-at-rest protection, to restrict access to user files and communications, authenticate users to determine appropriate privileges and service permissions, and to enforce collaboration policies for each enterprise

The "always secure" architecture is strengthened by compliance with industry data center standards, and regular audits provide transparency and accountability. Cisco's integrated security technologies and security-related practices provide a level of protection that often exceed the security

expectations of other enterprise-grade on-premises solutions. In fact, Cisco data centers have never been compromised while other companies often make headlines from incidents relating to data loss, lost backup tapes, or information left on public computers.

Security and the WebEx Collaboration Cloud

The WebEx Collaboration Cloud provides organizations with the Cisco advantages of persistent security, management, and integration. The strength of this hosted infrastructure stems from the multilayered security model, and offers uptime in excess of 99.99 percent.

The high-performance WebEx Collaboration Cloud is based on carrier-class information-switching architecture, and is purpose-built for real-time services through data centers that are strategically placed near major Internet access points. Dedicated, high-bandwidth fiber routes traffic around the globe. The uniquely secure, extremely scalable WebEx Collaboration Cloud serves as a highly available infrastructure, unburdened by the physical limitations of on-premise server solutions.

Security architecture

All hosted WebEx services benefit from the WebEx Collaboration Cloud security architecture (see Figure 1). The architecture encompasses the security built into the data centers' foundational layers and extends through the entire infrastructure, including management processes. Each data center element is evaluated within the overall architecture framework, and is designed to contribute to the overall security. For example, customer data is stored in file servers that do not face the network edge; data flows within the data centers are configured to minimize exposure.

For more information about the WebEx Collaboration Cloud security architecture, review the white paper: Unleashing the power of real-time collaboration: Security overview of Cisco WebEx solutions at: http://www.cisco.com/en/US/prod/collateral/ps10352/cisco_webex_security_overview.pdf

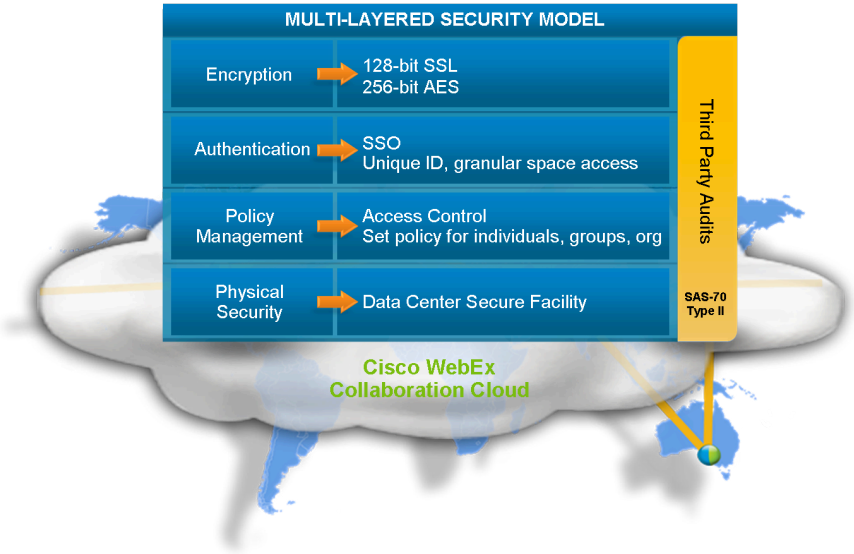

Figure 1. Cisco WebEx Multilayer Security Model

Secure XMPP connections

WebEx Connect IM utilizes Extensible Messaging and Presence Protocol (XMPP) – the Internet standard for real-time communication. XMPP standardizes a native approach for authentication and channel encryption, prevents address spoofing that can generate spam, and helps prevent the transmission of malware. The Internet Engineering Task Force (IETF) has evolved XMPP to strengthen security, and WebEx Connect IM gives users the benefits of these advancements.

In compliance with the XMPP standard, WebEx Connect IM capabilities are carried out over secure client sessions. Each session begins with the client performing service lookup using the WebEx Connect IM Domain Name System (DNS) service records. An encrypted connection is established using Transmission Control Protocol (TCP), and then the server authenticates the client. Unlike Simple Mail Transfer Protocol (SMTP) and Session Initiation Protocol (SIP), XMPP requires this authentication step. The standard client authentication for XMPP is based on the Simple Authentication and Security Layer (SASL) and the DIGEST-MD5 mechanism.

After a client has established an encrypted channel connection and has been authenticated by the server, it can then exchange presence information, messages, and request-response interactions with other users and applications. However, a WebEx Connect IM client cannot simply assert its address on the network, as with email communications. WebEx Collaboration Cloud servers prevent address forging by validating or stamping sender addresses, which helps to greatly reduce spam on the network. WebEx Connect IM servers also use native rate limiting to block denial-of-service attacks and other attempts to clog the network with large volumes of packets.

Blocking spam, viruses, and other threats

XMPP networks are characterized by a lack of spam, spam over instant messaging ("spim"), viruses, and malware. The built-in prevention of address forging makes it almost impossible for spammers to hijack addresses from which to send messages. Native rate limiting makes it more costly to run distributed botnets, since a spammer would need to establish accounts at multiple servers. It is also difficult to discover large numbers of XMPP addresses via directory harvest attacks, since XMPP servers do not divulge addresses or unknown users in response to standard requests. Users' presence information and IP addresses are only shared with authenticated entities.

Servers in the WebEx Collaboration Cloud include client-controlled white lists and blacklists to help users block communications with undesirable or risky users and groups. Since XMPP is a pure XML technology, it does not allow binary attachments, scripts, inline images, or other executable malware. Phishing attacks are possible, but the prevention of address forging has made such attacks rare. The XMPP community has also developed XMPP extensions such as spam reporting mechanisms that can be used if spam escalates.

Physical site security

Cisco operates all infrastructure used within the WebEx Collaboration Cloud. The physical security at the data centers includes hard-line perimeter devices for facilities and buildings, and employees must pass biometric access controls and possess ID badges for entry. Additional protection is provided by video surveillance.

Network-based security

WebEx Connect IM's highly secure XMPP connections and Cisco's network with built-in firewalls fortify security. Advanced intrusion detection and prevention further safeguard all network traffic. XMPP-based security and built-in Cisco protection is not limited to internal networks. Tens of thousands of Internet domains deliver XMPP services to millions of users, and since first deployed in 1999, this growing XMPP network has experienced no major security incidents.

Data at Rest

Access to data stored in the cloud can only be accomplished using WebEx Connect IM, and only after proper user authentication. Additional data protection features include:

- Administration restrictions – Only authenticated, authorized data center personnel can access specific collaboration data. Cisco uses extremely granular access controls for administration, which creates separation of duties using least-privileged, role-based access levels. All administrative accesses to WebEx Connect IM file systems and data are logged and reviewed to ensure compliance with the policies and role definitions.
- File separation – Files from different companies are stored on separate physical disks or isolated using logical unit numbers (LUNs).
- Host hardening – Cisco's host-hardening practices provide additional security for WebEx Connect IM data. Each server build is based on a minimal installation of the Linux operating system, and hardened based on guidance from Security Technical Implementation Guides (STIGs) published by the National Institute of Standards and Technology (NIST). Extraneous tools, libraries, and files have been removed to reduce the likelihood of system vulnerabilities and system misuse. As with all CSG product resources, user access is strictly limited. All systems undergo a thorough security review and acceptance validation prior to production deployment, as well as regular ongoing hardening and vulnerability assessment.
- Data removal – Since data is stored in a limited number of systems, complete removal (with no associated remnant backup data) is guaranteed at the request of the customer. Accidental deletions can be restored during a period specified by the customer.
- Restricted use – WebEx Connect IM data is never crawled or indexed for analysis.

Redundancy

Any failure of an individual server in a group initiates transparent routing of requests to other available servers within the WebEx Collaboration Cloud. Failure of an individual server is detected by the regular load-balancing check; individual servers are also monitored by the WebEx Network Operations Center.

Cisco's redundant and high-performance failsafe solutions within and between data centers contribute to the high availability of the service. Block-level replication of data across servers and data centers speeds fault and disaster recovery in the event of system failures, power outages, and other events that can affect entire sites or geographies.

Data backup and disaster recovery

WebEx Connect IM offloads the need for IT organizations to manage project data. The elimination of backup tapes alone (all backups are carried out as disk-to-disk saves) significantly decreases the risk of data loss. Service-level agreements (SLAs) include up-time guarantees and allow IT to specify the requirements and to cost-effectively provide reliable collaboration services and uninterrupted access to project data throughout the organization. Backup processes within the Cisco data centers are split into two categories: global site backups, and file backups.

Global site backups provide recovery in the event of large-scale incidents such as power outages, natural disasters, service capacity overload, or network capacity overload. The WebEx Collaboration Cloud architecture supports manual backups for scheduled maintenance and automatic real-time failover of traffic in the event of an outage or capacity issue. Tiered backups involve both online (Tier 1) and offline (Tier 2) saves, and data is stored in two geographically dispersed data centers (Mountain View, California and Denver, Colorado). Global site backups are carried out as follows:

- One snapshot is taken daily; multiple snapshots are retained on Tier 1 storage.
- One snapshot is taken daily and stored to Tier 2 storage; multiple snapshots are retained on Tier 2.
- Database and file replications are carried out to ensure data consistency. An automated sync mechanism ensures that databases and files are always synchronized. An on-demand restoration can be carried out to restore a database or file system in the event of user error or location-related issues. Even in the case of a location outage, the sync replication mechanism can be restarted and instantly synchronizes the data. Databases and files are backed up as follows:
  - Snapshots are taken daily on primary/active sites; multiple snapshots are retained on Tier 1 storage as well as on Tier 2 storage.
  - Databases are archived daily on Tier 2 storage; the number of days of retention is configured to meet customer requirements.
  - A daily backup of all databases is also created, and multiple backups stored in Tier 1 storage.

Protecting Data in Motion

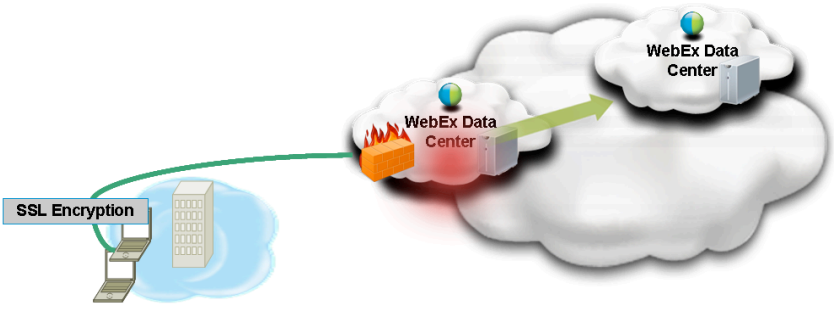

Figure 2. The Cisco WebEx Collaboration Cloud.

Data flows between WebEx Connect IM clients and the WebEx Collaboration Cloud (see Figure 2) using 128-bit encrypted Secure Socket Layer (SSL) connections. This transport layer security can also utilize 256-bit Advanced Encryption Standard (AES) protection, and sessions can be configured to be fully encrypted end to end. Conferencing and instant messaging traffic is switched, so data flows are not persistent. File transfers through the IM client are also encrypted.

Standard SSL encryption is used when communicating with non-WebEx Connect IM clients (AES encryption is not an option in these cases).

For customers who take advantage of the ability to integrate WebEx Connect IM with Cisco Unified Communications Manager, transport security for VoIP is managed by the integrated security capabilities of the Cisco Unified Communications Manager functionality.

Restricting access

Each WebEx Connect IM user has a unique access identity, including a user identity (ID) and password. To simplify access to WebEx Connect IM and other WebEx services such as WebEx Meeting Center, Cisco supports federated authentication for user Single Sign-On (SSO) using Security Assertion Markup Language (SAML) and WS-Fed protocols.

Customers retain complete ownership of user names and passwords. Administrators can manage accounts and password strength, password aging, and account deactivations. In accordance with requirements for compliance with the Sarbanes-Oxley Act (Section 404, access management), the Health Insurance Portability and Accountability Act (HIPAA), and other regulations, WebEx Connect IM has adopted strict guidelines for passwords:

- Passwords must be eight characters in length.
- Passwords must contain both upper- and lower-case letters, mixed with numbers and symbols (!, @, #, $).
- Passwords cannot be reused over the course of five password changes.
- Passwords must be changed at specified intervals.

Cross-company federations

Since WebEx Connect IM supports Security Assertion Markup Language (SAML) for user authentication. This extends authentication beyond WebEx Connect IM to other WebEx services as well as federated application domains that support CA SiteMinder™ or Microsoft® Active Directory®.

WebEx Connect IM supports native presence and IM federation with other XMPP-based clients such as GoogleTalk or Adium. WebEx Connect IM can also federate with the AIM® network, IBM® SameTime® (if the company has deployed the SameTime XMPP gateway), and Microsoft® Office Communication Server™ if the company has deployed the OCS XMPP gateway). For a list of XMPP clients, visit www.xmpp.org. While IM and presence across other IM clients are supported, other WebEx Connect IM capabilities are not – including Spaces, file transfer, audio/video conferencing and desktop sharing.

Managing policies

Policies are used to manage and enforce corporate rules governing all aspects of collaboration. IT can take advantage of granular controls to grant access to specific services and data based on roles, groups, or the needs of a particular individual. WebEx Connect IM also gives IT the ability to manage collaboration privileges and to enforce enterprise security policies.

The WebEx Connect IM organizational administration interface simplifies policy definition and management, and also gives IT the ability to selectively enable or disable WebEx Connect IM and some individual features such as external communication, file sharing or rich media such as video or audio conferencing.

For instant messaging, WebEx Connect IM utilizes a network-based policy model. Policies can be applied to the user, group, and organization levels to control the features that are available to individual users. The network-based policies enforce a system-wide identity, and policies follow users to wherever they are located, including accessing the features from outside of the company network.

For example, using WebEx Connect IM instant messaging:

- There are policies to control whether users can send instant messages to people outside of the company.
- External users must request permission to add a user to their contact list.
- Instant messaging can be protected using AES end-to-end encryption.

Supporting user-based controls

Each user also has the ability to control some collaboration parameters. For example, a user's presence information can only be followed by those people authorized by the user. IT can grant privileges based on the user's affiliations and roles in the organization.

Compliance and third-party audits

Cisco has a dedicated security department, which reports directly to the CIO of the Cisco Collaboration Software Group (CSG) and the Corporate Security Office. The combined team recommends and implements security procedures for WebEx products, services, and business operations. Team certifications include GIAC-Certified Forensic Analyst, CISSP, GIAC Certified Intrusion Analyst, ISSMP, and CISM.

Beyond its own stringent internal procedures, the WebEx Office of Security engages independent third parties to conduct rigorous audits against internal policies, procedures, and applications. These audits are designed to validate mission-critical security requirements for both commercial and government applications. Independent testing provides transparency to Cisco's customers, who always have access to audit results that demonstrate Cisco's leadership in the field of email security. Copies of audit reports can be requested from the WebEx Security Office.

ISO-27001

Cisco is actively pursuing ISO-27001 certification and has engaged Ernst & Young to assist with implementing an information security management system (ISMS) based on ISO/IEC 27001. The information security management covers all Information Assets & Information processing facilities procured and maintained by Cisco to provide Software as a Service to their customers.

Currently, PricewaterhouseCoopers (PwC) is contracted to carry out SAS-70 Type II evaluations, including auditing of Cisco facilities, and measuring progress against ISO 27001 controls. ISO-27001 is an internationally recognized information security standard published by the International Organization of Standardization (ISO) that recommends best practices for information security management. It defines requirements for corporate security policies, data management, and access control, among other things.

PwC performs an annual SAS-70 Type II audit in accordance with standards established by the American Institute of Certified Public Accountants AICPA. The controls audited against WebEx are based on ISO-27001 standards. In the opinion of PwC, WebEx services provide adequate controls as defined in this standard.

This highly respected PwC audit validates that WebEx services have been carefully evaluated compared to control objectives and control activities (including controls over information technology and security related processes) with respect to handling and processing customer data. For additional information on the SAS-70 standard please see: www.sas70.com/index2.htm.

Conclusion

WebEx Connect IM is a perfect choice for organizations that want to increase productivity by offering secure, enterprise-grade instant messaging to their employees. This SaaS-based solution, powered by the WebEx Collaboration Cloud, enables IT personnel to provide wider access to colleagues inside and outside the organization securely without the high overhead costs of in-house servers, software, firewalls, and maintenance. The combination of the WebEx security architecture, multilayered security solutions, and the WebEx Collaboration Cloud policies and practices provide enterprise-class protection for WebEx Connect IM communications and content. IT administrators can define and enforce policies that comply with corporate guidelines and goals. Cisco is committed to providing its customers with the highest level of security and performance, and has invested significant resources into the Cisco WebEx solution infrastructure to ensure optimal conditions for secure and reliable communication transmission, to and from anywhere in the world.

For More Information.
To request additional information, please contact:

Cisco WebEx LLC
3979 Freedom Circle,
Santa Clara, CA 95054 USA

Main: +1.408.435.7000
Sales: +1.877.509.3239

www.webex.com