White Paper

Unleash the Power of Highly Secure, Real-Time Collaboration

Introduction

Cisco WebEx® web conferencing solutions help accelerate business results through online collaboration. Team members can easily share information through any computer or mobile device, allowing people to collaborate any time, from anywhere, inside and outside corporate firewalls. WebEx solutions are delivered as software-as-a-service (SaaS) through the Cisco® WebEx cloud - a highly available and secure service delivery platform with unmatched performance, integration flexibility, and enterprise-grade security. However, companies still have many questions about security: from scheduling meetings to authenticating participants and sharing documents. How can Cisco guarantee that sensitive information is properly protected before, during, and after online meetings?

Cisco makes security the top priority in the design, deployment, and maintenance of its network, platform, and applications. This paper will show you how you can incorporate WebEx solutions into your business processes with confidence, even with the most rigorous security requirements. This paper focuses specifically on Cisco WebEx Meetings - the new web conferencing solution from Cisco. Understanding the security features of Cisco WebEx Meetings and the underlying communications infrastructure will help you make your investment decision with confidence.

This document primarily focuses on the security features of Cisco WebEx Meetings; in addition it discusses security elements of Cisco WebEx Event Center, Cisco WebEx Training Center, and Cisco WebEx Support Center. More information is available on security features specific to Cisco WebEx Meeting Center.

The Cisco WebEx Cloud

The Cisco WebEx meeting services are delivered through the Cisco WebEx cloud, a communications infrastructure purpose-built for real-time web communications.

Switched Architecture

Cisco WebEx cloud uses a globally distributed, dedicated network of high-speed meeting switches. Meeting session data originating from the presenter's computer and arriving at the attendees' computers is switched - never persistently stored - through the Cisco WebEx cloud.[1]

[1] When the user enables Network-based Recording (NBR), the meeting is recorded and stored. In addition to NBR, WebEx also stores user profile data.

Data Centers

WebEx Meetings sessions use switching equipment located in multiple data centers around the world. These data centers are strategically placed near major Internet access points and use dedicated high-bandwidth fiber to route traffic around the globe. Cisco owns and operates all infrastructure used within the Cisco WebEx cloud. During a meeting, the shared data is temporary switched across the region for users attending the meeting from other regions. However stored data always stays within the region - data within the United States (U.S.) stays within the U.S., and data within Europe remains in the European region even during the back-up process. For example, recordings generated on a WebEx site configured in Europe are always stored within the European Union regional data centers.

Additionally, Cisco operates network Point of Presence (iPoP) locations that facilitate backbone connections, Internet peering[2], Global Site Backup, and caching technologies used to enhance end-user performance and availability. Cisco personnel are available 24 hours a day, seven days a week for logistical security, operational, and change-management support. For more information on Cisco WebEx cloud, visit: http://www.cisco.com/en/US/solutions/ns1007/collaboration_cloud.html.

The Secure Meeting Experience

The secure WebEx meeting experience includes the following aspects:

- Meeting roles
- Admin configuration
- Security features and options for WebEx meetings
- Encryption technologies
- Transport-layer security
- Firewall compatibility
- Meeting data privacy
- Single Sign On

WebEx Meeting Roles

The following three roles are commonly used in a web meeting:

- **Host:** The host schedules and starts a WebEx meeting. The host can grant presenter privileges to attendees. The host can also lock the meeting and expel attendees.
- **Presenter:** A presenter can share presentations, specific applications, or entire desktop. The presenter controls the annotation tools. The presenter can grant and revoke remote control over the shared applications and desktop to individual attendees.
- **Attendee:** An attendee participates in a meeting and has no security responsibilities or privileges.
- **Panelist:** Cisco WebEx Event Center and Cisco WebEx Training Center have a panelist role which is similar to the presenter role. Panelists can review and answer the questions in the Q&A, or speak during the meeting along with the presenter.

[2] For details on peering policy, refer to: http://www.webex.com/peering-policy.html.

WebEx Meetings Administration Module

The WebEx Meetings administration module allows authorized administrators to manage organization-level security controls and policies.

This module helps manage the following security-related features:

Account Management

- Add, edit, activate, deactivate, import, and export user accounts
- Force user to reset account password
- Enable or disable user account self-registration
- Enable or disable automatic approval of account registration request from organization's domain (e.g. employee@company.com)
- Control if specific WebEx services enabled for all newly provisioned or self-registered users or specific users
- Configure lock-out of the user account after a number of failed attempts (typically between three and 10) to sign in
- Configure unlock of locked user accounts after a number of minutes

Resource Management

- Allow and disallow storage overflow for site or users[3]
- Enable and disable storage enforcement for each user
- Enable, configure, and disable file upload size limitation
- Block upload of specific file types (e.g. exe, zip, etc.)

Account Password Enforcement

- Minimum password length
- Minimum number of alphabetic characters
- Minimum number of numeric characters
- Minimum number of special characters
- Must include mixed case
- List of unacceptable passwords (e.g. "password", "pass", "passwd", etc.)
- Allow or disallow user's first name, last name, email address, and company name to be used as passwords
- Configure the number of previously used passwords (typically between three and eight) that cannot be used as a new password
- Require user to change password every N days
- Allow or disallow user to save account password in cookie

Other Security Options

- User login session inactivity timeout period
- Configure if URL links posted in feeds and comments are clickable or not

[3] Please note that the WebEx site storage overflow is typically negotiated as part of the Cisco contract term. Overflow is usually enabled by default.

- Configure show warning message when user clicks the links or not
- Single Sign On-related options
- Configure user profile default view settings (e.g. user profile is visible to anyone, visible only to the user's organization and network, or visible only to the user's organization)
- Allow or forbid users from changing profile view settings
- A site admin can configure the telephony dial-in or callback feature for WebEx Event Center. Alternatively, the callback feature can be disabled for the whole site, requiring all users to dial into the meeting

Policy Editor

Policy editor is provided in the WebEx Meetings administration tool. It allows the admin user to define granular access control policies for the organization, such as allowing or disabling public file sharing, allowing or forbidding external users from uploading files, etc.

Security Features and Options for WebEx Meetings

The following features help further enforce security for WebEx Meetings:

- **No public meeting list:** Meetings are listed only in the "Meetings" pages of the meeting host and invitees (for invitees who have logged into their WebEx Meetings account).
- **Include meeting password option:** The meeting organizer has an option to include a meeting password in the meeting invitation or "join meeting" email. If a password is not included, invitees will need to either log into their WebEx Meetings account or input a password manually to join the meeting.
- **Restrict access:** During a meeting, the host can choose to restrict access for certain attendees or expel participants to maintain security. Similarly, a site admin can restrict external file sharing, preventing meeting attendees from sharing files with participants who join meetings from outside the organization.

When a user starts or joins a WebEx meeting for the first time, the WebEx Meetings service automatically downloads and installs a client application to the attendee's computer. Cisco WebEx client software security certificates are digitally signed VeriSign, informing the meeting participant that the files come from Cisco. After the initial download, the WebEx client application downloads and installs only select files - containing changes or updates. Attendees can use the Uninstall function provided by their computer's operating system to easily remove WebEx files.

Encryption Technologies

WebEx Meetings provides the following encryption mechanisms:

- End-to-end (E2E) encryption option. This method encrypts all meeting content, end-to-end, between meeting participants using the AES encryption standard with a 256-bit key randomly generated on the host's computer and distributed to attendees with a public key-based mechanism. Unlike SSL, which is terminated at the cloud side, in E2E-enabled meetings all meeting content is kept in encrypted format within the Cisco WebEx cloud Infrastructure. Clear text meeting content data is only presented in meeting participants' computer memory.
- User password saved in the Cisco WebEx cloud in non-reversible salted hash format.
- If a user chooses the "Remember me" option on the login page, the user's login ID and password for WebEx Meetings saved on their computers or mobile devices are encrypted using 128-bit Advanced Encryption Standard (AES).

Hosts can select E2E using the “Meeting type” option on the scheduling page. The E2E solution provides stronger security than AES alone (though E2E also uses AES for the payload encryption), due to the fact that the key is known only to the meeting host and attendees.

Every WebEx Meetings connection must authenticate properly prior to establishing a connection with the Cisco WebEx cloud to join a meeting. The client authentication process uses a unique per-client, per-session cookie to confirm the identity of each attendee attempting to join a WebEx Meetings session. Each meeting contains a unique set of session parameters generated by the Cisco WebEx cloud. Each authenticated attendee must have access both to these session parameters and the unique session cookie to join the meeting.

Traffic for WebEx Meetings on mobile devices such as the iPad, iPhone, Android, and BlackBerry is also encrypted, however E2E meetings are not supported on mobile devices.

Transport Layer Security

In addition to the application layer safeguards, all meeting data is transported using 128-bit SSLv3. Rather than using firewall port 80 (standard HTTP Internet traffic) to pass through the firewall, SSL uses firewall port 443 (HTTPS traffic), restricting access over port 80 without affecting WebEx traffic.

WebEx Meetings attendees connect to the Cisco WebEx cloud using a logical connection at the application, presentation, or session layers. There is no peer-to-peer connection between attendees’ computers.

Firewall Compatibility

The WebEx Meetings service communicates with the Cisco WebEx cloud to establish a reliable and secure connection using HTTPS (port 443). As a result, customer firewalls do not have to be specially configured to enable WebEx Meetings.

Meeting Data Privacy

All WebEx Meetings content, including chat, audio, video, desktop, or document sharing is transient - it exists only during the meeting. Meeting content is not stored at either Cisco WebEx cloud or an attendee’s computer. Cisco retains the following types of meeting information[4]:

- **Event Detail Records (EDRs):** Cisco uses EDRs for billing and reporting. Customers may review event detail information on their customized WebEx site by logging in using their host ID. Once authenticated, customers can also download this data from the WebEx site or access it through WebEx APIs. EDRs contain basic meeting attendance information, including who (user name and email) joins what meeting (meeting ID) and when (join and leave meeting time). Such information is useful primarily for billing and reporting purposes.
- **NBR files:** If a host chooses to record a WebEx Meetings session, the recording will be stored within the Cisco WebEx cloud and can be accessed in the “Files” area on the WebEx Meetings site. Hosts can enable NBR recording at the meeting scheduling page or while the meeting is in progress. The NBR recording is protected by a cryptographic token. The host has full control of NBR recording file access, including the ability to delete the files or share it. The NBR functionality is optional and can be turned off by the administrator.

[4] Note that all retained data is stored within the same region where the WebEx site is configured. For example, European data centers do not store or back up data from the U.S.

- **User profile:** WebEx stores user profile information and settings, such as user preferences and user information (user name, email, address, and phone numbers, if provided by the user).
- **User files:** WebEx Meetings introduces a concept of Meeting Spaces - a highly secure, centralized online space for organizing and sharing all meeting-related activities and information. Meeting Spaces provide a facility for storing and sharing files. Each file has an encrypted metadata pointer which is stored in a separate database from the file itself, providing additional data security.

Single Sign On

Cisco supports federated authentication for user Single Sign On (SSO) using SAML 2.0 and WS-Fed 1.0 protocols. Using federated authentication requires customers to upload a public key X.509 certificate to their customized WebEx Meetings site. Third-party applications can then generate SAML assertions containing user attributes and digitally sign the assertions with the matching private key. WebEx validates the SAML assertion signature against the preloaded public key certificate before authenticating the user.

Third-Party Security Validation and Audits

Beyond its own stringent internal procedures, the WebEx Office of Security engages multiple independent third parties to conduct rigorous audits against Cisco internal policies, procedures, and applications. These audits are designed to validate mission-critical security requirements for both commercial and government applications.

Safe Harbor Certification

In March 2012, Cisco has successfully obtained Safe Harbor Certification for customer and partner data (Safe Harbor Certification for employee data was obtained in 2011). This serves as an additional component of Cisco's comprehensive privacy compliance program, and while not required, the company recognizes the value that customers place on this Certification.

The EU Data Protection Directive prohibits the transfer of European citizens' personal data to non-European Union (EU) nations that do not meet the EU's "adequacy" standard for privacy protection. The U.S. Department of Commerce, in concert with the European Commission, developed a "Safe Harbor Framework" that allows U.S. organization to comply with the Directive by abiding by a set of Safe Harbor Privacy Principles. Companies certify their compliance with these Principles on the U. S. Department of Commerce website. The Framework was approved by the EU in 2000 and gives companies that abide by the Principles assurance that the EU will consider their practices "adequate" privacy protections for EU citizens.

SSAE16

PricewaterhouseCoopers LLP performs an annual SSAE16 audit in accordance with standards established by the AICPA. For additional information on the SSAE16 standard please see: http://www.ssae16.com.

ISO-27001/2

Cisco designed its SSAE16 controls to resemble information security controls from ISO27002, noted in an appendix to ISO27001. ISO-27001 is an information security standard published by the International Organization of Standardization (ISO) that provides best-practice recommendations on creating an information-security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical, and technical controls involved in an organization's information risk-management processes. According to its documentation, ISO 27001 was developed to "provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an information-security management system." Refer to this link for additional information on ISO-27001/2: http://www.27000.org/.

For More Information

For more information on Cisco WebEx web conferencing, visit: http://www.cisco.com/go/webconferencing.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-711182-00 07/12