Tratto da: Cisco WebEx web conferencing security White Paper 2011

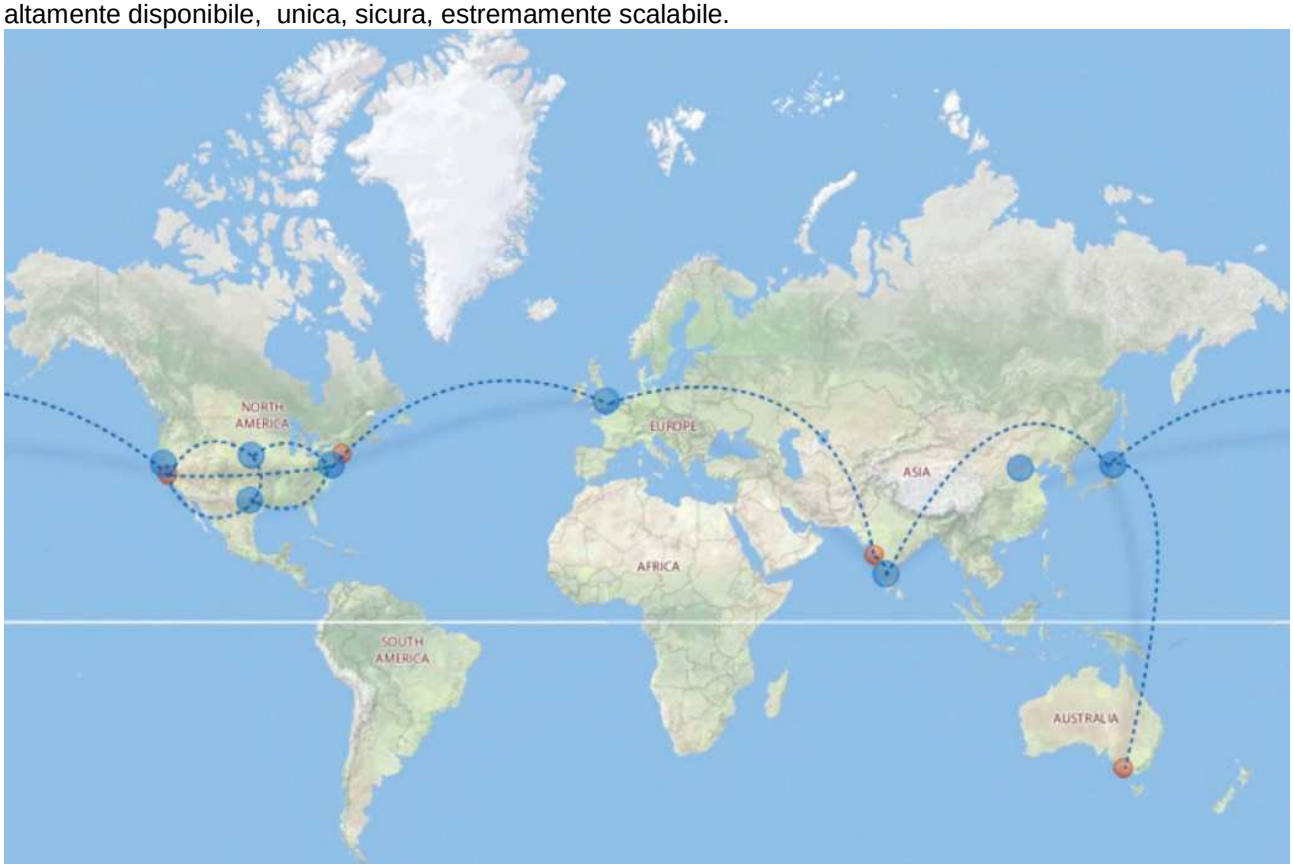
Tradotto da: Gabriella Molinelli NSC s.r.l.

L'infrastruttura di Cisco Collaboration Cloud

La Cisco Collaboration Cloud è un'infrastruttura di comunicazione realizzata con lo scopo di effettuare comunicazioni via web in tempo reale. I Data Centers sono stati localizzati in siti strategici vicino ai maggiori nodi di accesso Internet dedicati, con connessioni su fibra, banda larga, per permettere l'instradamento del traffico in tutto il mondo.

Architettura "Switched"

Cisco utilizza un sistema di switching dedicato, che opera su una rete a banda larga, unico, distribuito a livello mondiale. I dati relativi alle sessioni di Meeting originate dal computer del Presentatore, raggiungono i computer degli Ospiti in modalità "switched", diretta – non vengono mai memorizzati - attraverso la Cisco Collaboration Cloud. La Cisco Collaboration Cloud permette la realizzazione di un'infrastruttura di meeting altamente disponibile, unica, sicura, estremamente scalabile.



Data centers

Le sessioni di WebEx meeting utilizzano apparati switching situati in più Data Center situati in diverse località a livello mondiale. Cisco detiene la proprietà assoluta su tutta l'infrastruttura utilizzata dalla Cisco Collaboration Cloud. Attualmente questo network è formato da Data Center situati presso: Mountain View, CA; Thornton, CO; Richardson, TX; Ashburn, VA; London, UK; Bangalore, India; Beijing, China; e Tokyo, Japan. In più Cisco è presente in quattro iPoPs (Point of Presence - siti di presenza di rete) che facilitano le connessioni centrali di backbone, Internet peering, e tecnologie di caching utilizzate per migliorare le performance e la disponibilità del servizio presso l'utilizzatore finale. I iPoPs sono situati in San Jose, CA; New York City, NY; Mumbai, India; e Melbourne, Australia. I tecnici Cisco sono disponibili in modalità 24x7 per fornire il necessario supporto logistico di sicurezza, operatività e di change-management.

Tecnologie di crittografia.

I WebEx meetings sono progettati per fornire modalità di comunicazione in elevata sicurezza ed in tempo reale ad ogni Partecipante invitato alla sessione . Quando il Presentatore condivide un documento o una presentazione, la Universal Communications Format (UCF), una tecnologia proprietaria Cisco, codifica ed ottimizza i dati per la condivisione. L'applicazione di WebEx meeting utilizza meccanismi di crittografia anche su dispositivi mobili quali iPad, iPhone, e BlackBerry, simili a quelli utilizzati per i PC.

WebEx meeting utilizza i seguenti meccanismi di crittografia:

1. Per WebEx meetings su PC e dispositivi mobili, i dati sono trasportati dal client alla Cisco Collaboration Cloud utilizzando la funzionalità di crittografia a 128-bit Secure Socket Layer version3 (SSLv3).

2. I documenti e le presentazioni sono crittografati End-to-End utilizzando la funzionalità di crittografia a 256-bit Advanced Encryption Standard (AES) prima della trasmissione.

3. La crittografia End-to-End (E2E) è un'opzione fornita dalla versione di Cisco WebEx Meeting Center WBS26 e successive. Questo metodo crittografa tutti i contenuti del meeting, End-to-End, fra i Partecipanti, utilizzando lo standard di crittografia AES con chiave a 256-bit generata casualmente sul computer di chi ospita il meeting, e distribuita ai Partecipanti con un meccanismo basato su chiave pubblica.

4. La Public Key Infrastructure (PKI) basata su crittografia End-to-End è un'opzione disponibile dalla versione WebEx Meeting Center WBS27 e successive, con utilizzo crittografia standard a 256-bit AES. Il meccanismo richiede che il Partecipante si autentichi con certificato X.509 per iniziare o partecipare ad un meeting.

5. La password utente di login su dispositivi mobili viene crittografata utilizzando la funzionalità di crittografia 128-bit Data Encryption Standard (DES).

Gli amministratori del Sito e gli Ospiti possono selezionare sia la funzionalità di crittografia E2E o PKI utilizzando l'opzione di "Meeting type". Le funzionalità di E2E e PKI forniscono una sicurezza maggiore rispetto alla funzionalità AES da sola (le funzionalità di E2E e PKI utilizzano anche AES per la crittografia dei trasferimenti di dati relativi ai pagamenti), dato che la chiave è conosciuta solo da chi ospita i meeting e da chi vi partecipa.

Ogni connessione alla WebEx meeting richiede un'autenticazione adeguata, prima di stabilire una connessione con la Cisco Collaboration Cloud, prima di partecipare a una WebEx meeting. Il processo di autenticazione del client utilizza un coockie unico per singolo client e per singola sessione, per confermare l'identità di ogni Partecipante che richiede l'accesso ad una WebEx meeting. Ogni meeting contiene una unica sessione di parametri generati dalla Cisco Collaboration Cloud. Ogni Partecipante autenticato deve avere accesso a questi parametri di sessione e ad un'unica sessione di coockie per poter accedere al meeting con successo. (in parole semplici nel momento in cui l'utente si disconnette dal meeting per accedere nuovamente deve aprire una nuova sessione, perché i dati inseriti la prima volta non sono più validi/disponibili)

Transport layer security ("Sicurezza a livello di Trasporto")

In aggiunta alle precauzioni a livello applicativo, tutti i dati dei meeting sono trasmessi utilizzando la funzionalità di crittografia a 128-bit SSLv3. Anche se è attiva la funzionalità di firewall su porta 80 (standard HTTP Internet traffic) la crittografia SSL utilizza il firewall su port 443 (HTTPS traffic), restringendo ulteriormente l'accesso su porta 80 senza alcun effetto sul traffico WebEx.

I Partecipanti ad una WebEx meeting sono connessi alla Cisco Collaboration Cloud utilizzando una connessione logica a livelli di "application/presentation/session". Non esiste alcuna connessione "peer-to-peer" (ndr: condivisione di risorse e di servizi tra computer) tra i computer dei Partecipanti.

Compatibilità Firewall

L'applicazione di WebEx meeting comunica con la Cisco Collaboration Cloud per stabilire una connessione sicura ed affidabile utilizzando il protocollo HTTPS (porta 443) quindi i firewall non devono essere configurati in modo specifico per abilitare la WebEx meeting.

Memorizzazione dei dati Post-meeting

Nessuna informazione relativa alla sessione viene memorizzata nella Cisco Collaboration Cloud e neanche alcuna informazione relativa ai computer dei Partecipanti. Cisco memorizza solo due informazioni relative al meeting:

- Event Detail Records (EDRs) (registrazione dei dettagli del meeting): Cisco utilizza gli EDRs per scopi di fatturazione e reportistica. E' possibile verificare le informazioni di dettaglio di ogni meeting sul sito WebEx personalizzato, tramite l'accesso con il proprio ID Host. Ad autenticazione effettuata, è possibile scaricare anche i dati dal sito WebEx personalizzato o accedervi tramite la WebEx API.

- Network-based recording (NBR): se un Ospite sceglie di effettuare la registrazione di una sessione WebEx, la registrazione sarà salvata nella Cisco Collaboration Cloud e vi si potrà accedere dall'area MyRecordings del sito WebEx personalizzato. (nota: oppure sarà possibile scegliere di registrare il meeting in locale sul proprio pc)

Single Sign On

Cisco supporta l'autenticazione tramite Single Sign On (SSO) utilizzando i protocolli SAML 1.1, 2.0 e WS-Fed 1.0. Per la gestione di questa tipologia di autenticazione occorre caricare la chiave pubblica di un certificato X.509 nel proprio sito WebEx. Viene così generate una traccia SAML che contiene tutti i dati dell'utente che firma digitalmente i dati che corrispondo alla chiave privata. WebEx valida i dati SAML a fronte di una chiave pubblica certificate pre-caricata prima dell'autenticazione utente.

Terze parti - reporting

Sotto la sua diretta gestione delle procedure interne, il WebEx Office of Security ingaggia più rappresentanze di terze parti per la conduzione di rigorosi e continui controlli relativi alle policy interne, procedure, e applicazioni. Questi controlli servono a validare i requisiti critici di tutela della sicurezza sia per la parte commerciale che gestionale. Fra questi controllori ci sono diversi Information Security Partners, LLC (iSEC Partners) per la verifica dei corretti instradamenti dei dati e delle applicazioni, e PriceWaterhouseCoopers, per le verifiche su SAS-70 Type II.

ISO-27001/2

Cisco ha definito i controlli di auditing e reporting SAS70 in base agli standard internazionali ISO27002, in appendice alle ISO27001. ISO-27001 è uno standard di Best Practices relative alla corretta gestione della sicurezza informatica (ISMS - information-security management system) pubblicate dalla International Organization of Standardization (ISO). Un ISMS è un metodo di regole e procedure che definiscono tutti i controlli legali, fisici e tecnologici nell'ambito della gestione dei processi di Risk Management. In base alla documentazione di riferimento, ISO 27001 è stata definite per "fornire un modello per stabilire, implementare, effettuare, correggere, mantenere e migliora la gestione del sistema di sicurezza informatica". Per ulteriori informazione fare riferimento a: ISO-27001/2: http://www.27000.org/.

Conclusioni

La tua azienda può affidarsi a Cisco WebEx per utilizzare strumenti online di collaborazione e condivisione di attività operative, basati su un sistema altamente sicuro ed affidabile.