Des solutions de réunion en ligne pour une collaboration en temps réel, efficace et sécurisée

Ce livre blanc présente en détail les fonctionnalités de sécurité dont sont dotés Cisco WebEx Meeting Center, Cisco WebEx Training Center, Cisco WebEx Support Center et Cisco WebEx Event Center.

Introduction

Les solutions Cisco WebEx® rendent possibles les échanges et la collaboration en temps réel d'employés et d'équipes géographiquement dispersés comme s'ils se trouvaient dans la même pièce. La collaboration en ligne améliore la qualité des échanges en face à face et élimine les problématiques liées aux délais de trajet et aux coûts des déplacements, et même les difficultés relatives aux salles de réunion. Dans le monde entier, les entreprises, les institutions et les organismes publics utilisent les solutions Cisco WebEx® pour simplifier les processus et améliorer la performance des équipes dédiées à la vente, au marketing, à la formation, à la gestion de projet et à l'assistance.

Pour l'ensemble de ces entreprises et organismes, la sécurité est une question essentielle. La sécurité doit être assurée à plusieurs niveaux : depuis la programmation des réunions jusqu'à l'identification des participants en passant par le partage de documents.

Cisco fait de la sécurité la première des priorités et intègre cette exigence lors de la conception, du déploiement et de la maintenance de son réseau, de sa plate-forme et de ses applications. Vous pouvez intégrer les solutions WebEx® à vos processus, même avec les contraintes de sécurité les plus strictes.

Avant de vous décider à investir, il est important de bien comprendre les fonctionnalités de sécurité dont sont dotées les applications Cisco WebEx et l'infrastructure de communication sous-jacente, le cloud Cisco WebEx.

Le cloud Cisco WebEx

Solution SaaS (logiciel en tant que service) hébergée dans le cloud Cisco WebEx, WebEx Meetings est une plate-forme de prestation de services hautement sécurisée offrant des performances de pointe, une intégration flexible, une évolutivité et une sécurité supérieures. Le cloud Cisco WebEx garantit une facilité de déploiement et de distribution des applications qui permet de diminuer le coût total d'acquisition, tout en assurant le plus haut niveau de sécurité pour l'entreprise.

Une architecture commutée

Cisco dispose d'un réseau dédié de commutateurs haut débit répartis à travers le monde. Les données qui partent de l'ordinateur de l'animateur d'une réunion et arrivent sur les ordinateurs des participants sont commutées via le cloud Cisco WebEx, sans jamais être stockées.[1]

[1] Ce n'est que lorsque la réunion est enregistrée que les données sont stockées. Outre l'enregistrement, WebEx conserve les données du profil d'utilisateur et les fichiers de l'utilisateur.

Les data centers

Le cloud Cisco WebEx est une infrastructure de communication conçue spécialement pour les communications en ligne en temps réel. Les réunions sont possibles grâce à un équipement de commutation situé dans plusieurs data centers répartis à travers le monde. Les data centers sont placés stratégiquement près des principaux points d'accès Internet et utilisent des fibres dédiées à haut débit pour router le trafic dans le monde. Cisco gère l'ensemble de l'infrastructure au sein du cloud Cisco WebEx. Les données qui se trouvent aux États-Unis restent en Amérique du Nord et les données utilisées en Europe demeurent dans l'espace européen.

Par ailleurs, Cisco gère des lieux de points de présence (PoP) qui facilitent les connexions stables, le peering des liaisons Internet, la sauvegarde globale du site et les technologies de mise en cache utilisées pour optimiser la performance et la disponibilité pour l'utilisateur final. Le personnel Cisco, disponible 24 heures sur 24, 7 jours sur 7, assure une assistance pour la sécurité, le fonctionnement des solutions et les demandes de changement.

La réunion WebEx, une expérience ultrasécurisée

WebEx Meetings offre de nombreuses fonctionnalités pour :

- Configurer le site de la réunion
- Sécuriser au moment de la programmation
- Démarrer et rejoindre une réunion
- Tirer parti des technologies de chiffrement
- Sécuriser la couche de transport
- Assurer une compatibilité avec les pare-feu
- Garantir la confidentialité des données liées à la réunion
- Sécuriser la réunion
- Utiliser le processus d'authentification unique (SSO)
- Bénéficier des accréditations d'instances indépendantes (les audits réalisés confirment la solidité du système de sécurité de Cisco WebEx)

Les termes « Réunion WebEx » et « Session Cisco WebEx » évoquent les réunions avec audio intégré, les audioconférences en ligne et les vidéoconférences simple ou multipoint qu'il est possible de réaliser grâce aux produits Cisco WebEx. Cisco WebEx se décline en quatre solutions :

- Cisco WebEx Meeting Center
- Cisco WebEx Training Center
- Cisco WebEx Event Center
- Cisco WebEx Support Center (Cisco WebEx Remote Support et Cisco WebEx Remote Access)

Sauf indication contraire, les fonctionnalités de sécurité décrites dans ce document s'appliquent à toutes les applications WebEx mentionnées ci-dessus.

WebEx Meetings, les différents rôles

Il y en a quatre : organisateur, organisateur suppléant, animateur ou participant. Les sections suivantes décrivent les privilèges en terme de sécurité dévolus à l'utilisateur en fonction de son rôle.

L'organisateur

L'organisateur programme et lance la réunion. Il veille à son bon déroulement. L'organisateur peut accorder les privilèges d'animateur aux participants. Il peut également verrouiller la réunion et expulser des participants.

L'organisateur suppléant

L'organisateur nomme un suppléant qui peut démarrer une réunion programmée à la place de l'organisateur. Le suppléant et l'organisateur disposent de privilèges identiques.

L'animateur

L'animateur partage des présentations, des applications spécifiques ou un ordinateur dans son intégralité. Il contrôle les outils d'annotation. L'animateur peut permettre à chaque participant de contrôler à distance les applications et les ordinateurs partagés, comme il peut en reprendre le contrôle.

Le participant

Le participant n'a ni responsabilité, ni privilège.

Le module d'administration du site WebEx

Le module d'administration permet aux administrateurs autorisés de gérer et d'appliquer les politiques de sécurité, pour chacune des réunions et en fonction des privilèges dévolus à l'organisateur et à l'animateur. Ainsi, vous pouvez personnaliser les sessions et configurer de manière à empêcher l'animateur de partager des applications ou transférer des fichiers vers tel site ou utilisateur.

Le module d'administration du site WebEx gère les fonctionnalités de sécurité suivantes :

Gestion de compte

- Verrouillage de l'accès à un compte après un certain nombre déterminé de connexions ayant échoué
- Déverrouillage automatique d'un compte verrouillé après une durée déterminée
- Désactivation des comptes après une certaine période d'inactivité

Actions spécifiques concernant les comptes d'utilisateur

- Demander à ce que l'utilisateur change son mot de passe lors de sa prochaine connexion
- Verrouillage ou déverrouillage de compte
- Activation ou désactivation de compte

Création de compte

- Demander un texte de sécurité pour les demandes de nouveau compte
- Demande de confirmation des nouveaux comptes par courrier électronique
- Autoriser l'auto-enregistrement (inscription) des nouveaux comptes
- Configurer les règles d'auto-enregistrement des nouveaux comptes

Mots de passe permettant l'accès aux comptes

Renforcement des critères de sécurité pour les mots de passe dont les suivants :

- Casse mixte
- Longueur minimale
- Nombre minimal de caractères numériques
- Nombre minimal de caractères alphabétiques

- Nombre minimal de caractères spéciaux
- Pas de caractère répété trois fois ou plus
- Pas de réutilisation d'un certain nombre de mots de passe antérieurs
- Pas de texte dynamique (nom de site, nom de l'organisateur, nom d'utilisateur)
- Pas de mots de passe présents sur une liste configurable (par exemple « mot de passe »).
- Délai minimal entre deux changements de mot de passe
- Changement du mot de passe par l'organisateur au bout d'une durée configurable
- Changement du mot de passe par tous les utilisateurs à l'ouverture de session suivante

Les salles de réunion personnelles

Les salles de réunion personnelles sont accessibles via une URL et un mot de passe personnalisés. Dans cette salle, l'organisateur peut lister les réunions planifiées et en cours, démarrer et rejoindre les réunions et partager des fichiers avec les participants à la réunion. Les administrateurs peuvent définir des fonctions de sécurité pour les salles de réunion personnelles, notamment les suivantes :

- Options pour le partage de fichiers dans la salle de réunion personnelle
- Règles relatives aux mots de passe pour les fichiers dans la salle de réunion personnelle

Autres fonctionnalités de sécurité activées à partir de la console d'administration du site WebEx

- L'organisateur ou les participants peuvent choisir d'enregistrer leur nom et leur adresse e-mail pour faciliter l'organisation ou la participation à d'autres réunions.
- Les organisateurs peuvent réassigner des enregistrements à d'autres organisateurs.
- Il est possible de limiter l'accès au site en exigeant l'authentification de l'organisateur et de tous les participants. L'identification peut être obligatoire pour accéder à toute information sur le site (les réunions listées, par exemple) ainsi que pour obtenir l'accès aux réunions sur le site.
- Des règles de mot de passe fort sont applicables à WebEx Access Anywhere.
- Toutes les réunions peuvent être retirées de la liste.
- Une requête d'approbation ou « Mot de passe oublié » peut être nécessaire.
- Il est possible d'exiger la réinitialisation des mots de passe des comptes au nom d'un utilisateur.

Options de sécurité pour planifier les réunions WebEx

- Les organisateurs ont la possibilité d'imposer des règles de sécurité pour l'accès aux réunions (lesquelles restent dans le cadre des paramètres définis au niveau de l'administration du site et qu'il est impossible de contourner).
- Une réunion peut être retirée de la liste ; elle n'apparaîtra pas sur le calendrier visible.
- Les participants peuvent être autorisés à rejoindre la réunion avant l'organisateur.
- Les participants peuvent prendre part à la réunion en audio avant l'arrivée de l'organisateur.
- Seuls les participants avec un compte sur le site WebEx sont autorisés à rejoindre la réunion.
- Les informations relatives à la téléconférence peuvent apparaître dans les réunions.
- Les réunions peuvent se terminer automatiquement au bout d'une durée configurable s'il ne reste plus qu'un seul participant.
- Les participants sont éventuellement invités à saisir leur adresse e-mail lorsqu'ils rejoignent la réunion.

Réunions listées ou non

Les organisateurs peuvent choisir de lister une réunion dans le calendrier public des réunions sur un site personnalisé WebEx. Ils peuvent aussi planifier une réunion non listée ; elle n'apparaîtra jamais sur le calendrier des réunions. Les réunions non listées nécessitent que l'organisateur informe les participants explicitement de l'existence de la réunion, soit en leur envoyant un lien, dans une invitation envoyée par e-mail, soit en leur demandant d'entrer le numéro de la réunion donnée sur la page Rejoindre la réunion.

Réunions internes ou externes

Les organisateurs peuvent limiter l'accès des participants à la réunion aux personnes disposant d'un compte sur un site personnalisé WebEx, auquel ils pourront se connecter pour rejoindre la réunion.

Mots de passe pour pouvoir accéder à une réunion

Un organisateur peut définir un mot de passe pour la réunion, puis choisir d'envoyer ou non ce mot de passe dans un e-mail d'invitation.

Inscription

- L'organisateur peut limiter l'accès à la réunion à l'aide de la fonction d'inscription. L'organisateur crée une « Liste de contrôle d'accès » : seuls les invités s'étant inscrits au préalable et ayant été explicitement approuvés par l'organisateur pourront participer à la réunion.
- Il est possible de sécuriser les réunions en bloquant la réutilisation des identifiants d'inscription dans WebEx Training Center et WebEx Event Center. Toute personne essayant de réutiliser un identifiant déjà utilisé sera interdit d'accès à la réunion. Cela empêche l'échange d'identifiants entre entre participants.
- De plus, un organisateur peut maintenir la sécurité d'une réunion en en limitant l'accès et en expulsant des participants.

N'importe quelle combinaison de ces options peut être ajustée pour être adaptée à vos règles en matière de sécurité.

Démarrer et rejoindre une réunion

La réunion démarre une fois que l'identifiant et le mot de passe de l'organisateur ont été identifiés sur votre site personnalisé WebEx. L'organisateur a le contrôle initial de la réunion et en est le premier animateur. L'organisateur peut permettre à n'importe quel participant de devenir organisateur ou animateur mais il peut aussi reprendre le contrôle, choisir d'expulser des participants ou de terminer la session à n'importe quel moment.

L'organisateur peut nommer un organisateur suppléant pour commencer et contrôler la réunion au cas où il serait lui-même dans l'incapacité de participer à la réunion ou s'il venait à être déconnecté. Cela élimine le risque que le rôle d'organisateur ne soit délégué à un participant non attendu ou non autorisé.

Vous pouvez configurer votre site personnalisé WebEx afin de permettre aux participants de rejoindre la réunion (partie audio incluse) avant l'organisateur et limiter les possibilités de discussion entre les participants avant le début de la réunion, que ce soit par chat ou par audio.

Lorsqu'une personne rejoint une réunion WebEx pour la première fois, le logiciel WebEx est automatiquement téléchargé et installé sur son ordinateur. Le logiciel WebEx est signé de façon numérique à l'aide d'un certificat émis par VeriSign. Lors des réunions suivantes, l'application WebEx télécharge et installe seulement les fichiers contenant des changements ou des mises à jour. Les participants peuvent utiliser la fonction « Désinstaller » du système d'exploitation de leur ordinateur pour supprimer facilement les fichiers WebEx.

Technologies de chiffrement

Les réunions WebEx sont conçues pour distribuer du contenu multimédia riche, en temps-réel et de façon sécurisée, à chacun des participants à une session WebEx. Lorsqu'un animateur partage un document ou une présentation, le fichier est encodé au moyen de la technologie UCF (Universal Communications Format), propriété de Cisco®, laquelle optimise les données pour le partage. L'application de réunion WebEx sur les appareils mobiles tels que l'iPad, l'iPhone et le BlackBerry utilise des mécanismes de chiffrement similaires à ceux du client PC.

La plate-forme de réunion WebEx utilise les mécanismes de chiffrement suivants :

- Pour les réunions WebEx sur PC ou sur appareils mobiles, les données sont transportées du client au Cisco WebEx cloud au moyen du protocole SSL 128 bits (SSL).
- Cisco WebEx Meeting Center offre une option de chiffrement de bout en bout (E2E). Cette méthode permet de crypter l'ensemble du contenu de la réunion, d'un bout à l'autre, entre les participants, au moyen de la norme de chiffrement AES (Advanced Encryption Standard) avec une clé de 256 bits générée de façon aléatoire sur l'ordinateur de l'organisateur et distribuée aux participants à l'aide d'un mécanisme basé sur une clé publique. Contrairement aux données chiffrées au moyen de SSL qui sont décryptées dans le cloud Cisco WebEx, le chiffrement E2E crypte tout le contenu des réunions au sein de l'infrastructure du cloud Cisco WebEx. Les données en texte clair sont seulement fournies à la mémoire de l'ordinateur des participants à la réunion.[2]
- Si un utilisateur sélectionne l'option « Se souvenir de moi », son identifiant et son mot de passe pour les réunions WebEx sauvegardés sur le PC ou l'appareil mobile sont cryptés au moyen du protocole AES 128 bits.

Les administrateurs de site et les organisateurs peuvent choisir le chiffrement E2E via l'option « Type de réunion ». La solution E2E offre une meilleure sécurité que le cryptage AES seul (bien qu'E2E utilise également AES pour le chiffrement des données utiles), car la clé n'est connue que de l'organisateur et des participants.

Chaque connexion entre le client WebEx et le cloud Cisco WebEx est authentifiée par un jeton cryptographique de façon à ne permettre l'accès à la réunion qu'aux utilisateurs légitimes.

Transport Layer Security (TLS)

En plus de fonctions de protection de la couche applicative, toutes les données relatives à la réunion sont acheminées au moyen du protocole SSL 128 bits. Au lieu d'utiliser le port pare-feu 80 (utilisé pour le trafic Internet HTTP standard) pour passer au travers du pare-feu, le protocole SSL utilise le port pare-feu 443 (réservé au trafic HTTPS).

Les participants à une réunion se connectent au cloud Cisco WebEx en utilisant une connexion logique au niveau de la couche d'application / de présentation / de session. Il n'y a pas de connexion de pair à pair entre les ordinateurs des participants.

Compatibilité avec les pare-feu

L'application WebEx communique avec le cloud WebEx afin d'établir une connexion fiable et hautement sécurisée via le HTTPS (port 443). De cette manière, vos pare-feu n'ont pas besoin d'être spécialement configurés pour permettre les réunions WebEx.

[2] Notez que l'enregistrement n'est possible que si le chiffrement E2E est activé. Cette option n'est disponible que pour WebEx Meeting Center.

Confidentialité des données liées à la réunion

L'ensemble du contenu d'une réunion WebEx (discussion en ligne, audio, vidéo, partage de bureau ou de document) est transitoire (c'est-à-dire qu'il n'existe que le temps de la réunion). Le contenu des réunions n'est pas stocké par défaut sur un cloud Cisco ou sur l'ordinateur du participant. Cisco ne retient que deux types d'éléments, à savoir :

- **Les données détaillées sur l'événement :** Cisco utilise ces données pour la facturation et la génération de rapports. Vous pouvez consulter ces données sur votre site WebEx personnalisé en vous connectant à l'aide de votre identifiant d'organisateur. Une fois identifié, vous pouvez aussi télécharger ces données ou y accéder via les API WebEx. Ces données renseignent sur les participants (nom d'utilisateur et adresse e-mail), sur la réunion (identifiant de la réunion) et sur les heures d'arrivée et de départ des participants.
- **L'enregistrement de la réunion :** si un organisateur choisit d'enregistrer une réunion, l'enregistrement sera stocké dans le cloud Cisco WebEx et pourra être consulté en cliquant sur Mes Enregistrements sur le site personnalisé WebEx. Le fichier sera créé seulement si un organisateur lance l'enregistrement pendant la réunion ou s'il a activé l'option d'enregistrement systématique de toutes les réunions. Les enregistrements des réunions sont accessibles via une URL. Chaque lien contient un jeton imprévisible. L'organisateur a le contrôle total sur les enregistrements et peut notamment le supprimer, le partager ou encore ajouter un mot de passe pour le protéger. La fonction d'enregistrement des réunions est facultative et peut être désactivée par l'administrateur.

Authentification unique

Cisco prend en charge l'identification fédérée pour l'authentification unique (SSO) au moyen des protocoles SAML (Security Assertion Markup Language) 1.1 et 2.0 et WS-Federation 1.0. La prise en charge du protocole SAML 1.1 est progressivement supprimée. Utiliser l'identification fédérée nécessite que vous téléchargiez un certificat de clé publique X.509 sur votre site personnalisé WebEx. Vous pouvez générer alors des assertions SAML contenant les attributs de l'utilisateur et vous signez numériquement les assertions avec la clé privée correspondante. WebEx valide la signature de l'assertion SAML par rapport au certificat de clé publique préchargé avant d'identifier l'utilisateur.

Rapports d'instances indépendantes

En plus de ses propres procédures internes rigoureuses, le bureau de la sécurité WebEx demande l'audit rigoureux de ses politiques internes, des procédures et des applications Cisco, à des instances indépendantes. Ces audits doivent valider le respect des exigences en matière de sécurité pour l'utilisation de la solution par des entreprises et des organismes publics.

Évaluation indépendante de la sécurité des données

Cisco fait appel à des prestataires indépendants pour réaliser des tests de pénétration, approfondis et continus, et une évaluation de ses services. Dans cet objectif, un prestataire indépendant procède aux évaluations suivantes :

- Identification des applications essentielles et/ou des vulnérabilités du service et proposition de solutions.
- Recommandations générales pour améliorer l'architecture.
- Identification des erreurs de programmation et conseil visant l'amélioration des pratiques de programmation.

- Travail direct avec les ingénieurs de WebEx pour expliquer les résultats et conseil visant la résolution des problèmes.

Certification Safe Harbor

En mars 2012, Cisco a obtenu la certification Safe Harbor pour les données des clients et partenaires (la certification Safe Harbor pour les données du personnel a été obtenue en 2011). Cette certification vient compléter la large palette de certifications de sécurité dont Cisco est titulaire. Elle n'est exigée par aucun organisme public ou autorité des normes, mais l'entreprise a conscience de la valeur que ses clients accordent à cette certification.

La directive de protection des données de l'Union européenne interdit le transfert des données personnelles de citoyens européens vers des nations non européennes n'assurant pas un niveau de protection « adéquat ». Le Ministère du Commerce des États-Unis, de concert avec la Commission européenne, a développé un cadre appelé Safe Harbor qui permet aux organisations américaines de se conformer à la directive en vertu des principes de confidentialité Safe Harbor. Les entreprises certifient leur conformité à ces principes sur le site web du Ministère du Commerce des États-Unis. Le cadre a été approuvé par l'Union européenne en 2000 et donne aux entreprises obéissant à ses principes l'assurance que l'Union européenne considère leurs pratiques comme des protections de confidentialité adéquates pour les citoyens européens.

SSAE16

PricewaterhouseCoopers conduit chaque année l'audit SSAE16 (Statement on Standards for Attestation Engagements No. 16, déclaration sur les normes d'attestation n° 16 conformément aux normes établies par l'American Institute of Certified Public Accountants (association professionnelle américaine des experts comptables)). Pour de plus amples informations sur le SSAE16, consultez : http://www.ssae16.com.

ISO 27001 et 27002

Cisco a été certifié ISO 27001 pour les services WebEx en octobre 2012. Cette certification est renouvelée tous les trois ans et donne lieu à un audit externe annuel. ISO 27001 est une norme de sécurité des informations publiée par l'Organisation internationale de normalisation (ISO) qui fournit les meilleures recommandations en matière de création d'un système de gestion des informations de sécurité (ISMS). Un ISMS est un ensemble de règlementations et de procédures qui inclut tous les contrôles légaux, administratifs, physiques et techniques impliqués dans les processus de gestion de la sécurité de l'information d'une organisation. Selon sa documentation, l'ISO 27001 a été développée pour « fournir un modèle afin d'établir, mettre en œuvre, faire fonctionner, surveiller, examiner, maintenir et améliorer un système de gestion de la sécurité de l'information ». Suivez ce lien pour obtenir des informations supplémentaires sur les normes ISO 27001 et ISO 27002 : http://www.27000.org/.

Informations complémentaires

Pour plus d'informations sur les solutions Cisco WebEx, visitez https://www.webex.fr/ ou contactez votre conseiller commercial.

Siège social aux États-Unis
Cisco Systems
San José, Californie

Siège social en Asie-Pacifique
Cisco Systems (USA) Pte. Ltd
Singapour

Siège social en Europe
Cisco Systems International BV Amsterdam.
Pays-Bas

Cisco compte plus de 200 agences à travers le monde. Les adresses, numéros de téléphone et numéros de fax sont répertoriés sur le site de Cisco, à l'adresse : www.cisco.com/go/offices.