

GoToMeeting

Outils de conférence Web Citrix Online : livre blanc sur la sécurité

Citrix Online offre des mesures de sécurité renforcée de bout en bout qui préviennent à la fois les attaques passives et actives visant la confidentialité, l'intégrité et la disponibilité des données lors de l'utilisation de GoToMeeting, GoToWebinar ou GoToTraining.

www.gotomeeting.fr

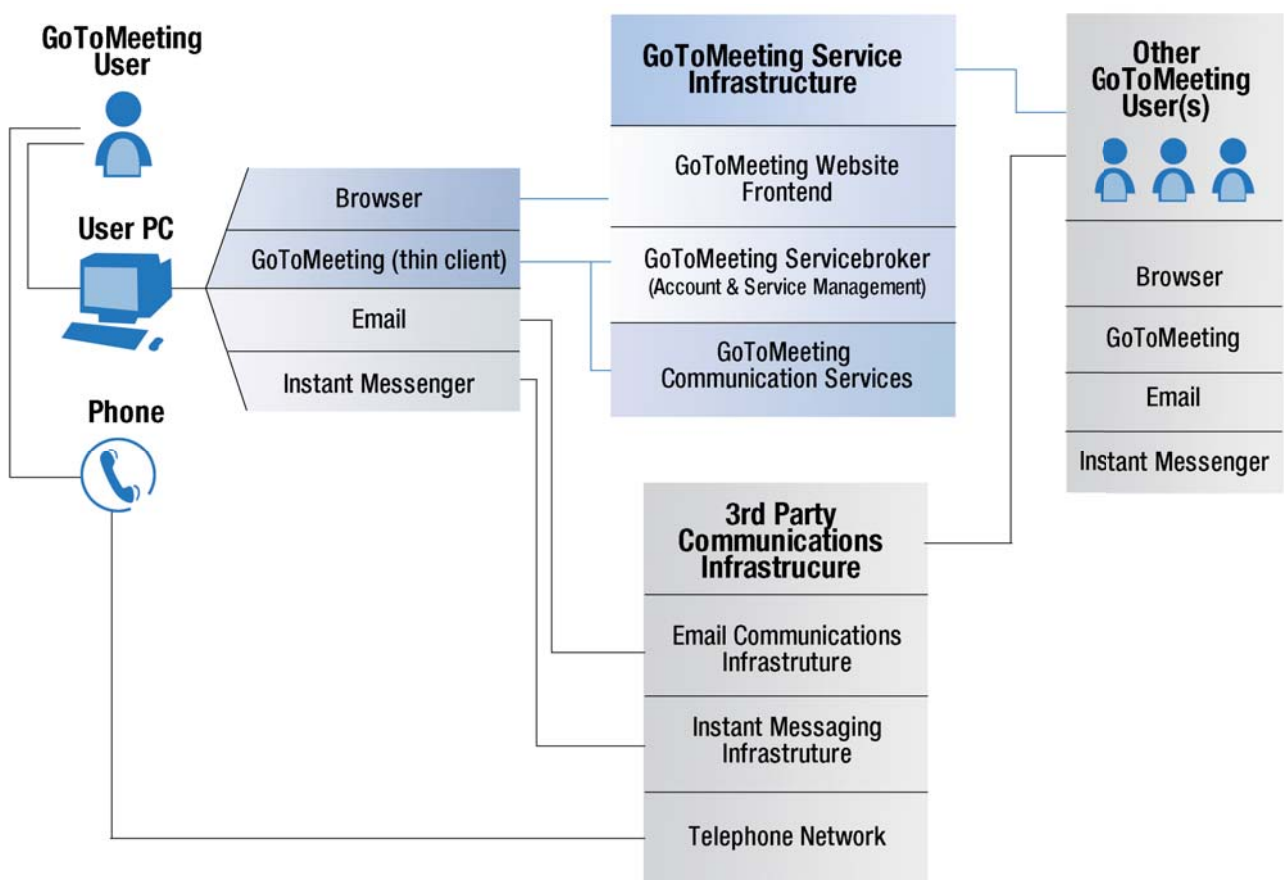
Sommaire

Résumé.....	3
Besoins des entreprises en matière de collaboration sécurisée	4
Fonctions de sécurité par rôle.....	5
Privilèges de l'organisateur.....	5
Privilèges du présentateur.....	6
Privilèges du participant.....	6
Fonctions d'authentification de compte et de session.....	7
Connexion au compte via le site Web.....	7
Divulcation des informations relatives à la session.....	7
Authentification des participants.....	7
Sécurité du site d'administration.....	8
Fonctions de sécurité des communications.....	9
Confidentialité et intégrité des communications.....	9
Sécurité de la couche TCP.....	9
Sécurité par couches multicast.....	10
Compatibilité avec les proxy et les pare-feu.....	10
Sécurité de la voix.....	11
Fonctions de sécurité du système d'extrémité.....	11
Logiciel d'extrémité signé.....	11
Mise en œuvre du sous-système cryptographique.....	12
Fonctions de sécurité de l'infrastructure hébergée.....	12
Infrastructure fiable et évolutive.....	12
Sécurité physique.....	12
Sécurité réseau.....	13
Respect de la vie privée des clients.....	13
Conclusion.....	13
Annexe : conformité aux normes de sécurité.....	13

Résumé

Les outils GoToMeeting™, GoToWebinar™ et GoToTraining™ sont les solutions de conférence Web les plus sûres du marché. Chaque solution allie une cryptographie normalisée avec chiffrement de bout en bout, une infrastructure de service hébergé à haute disponibilité et une interface intuitive, afin de garantir une confidentialité, une intégrité et une disponibilité optimales.

Ce document offre une description technique des fonctions de sécurité intégrées à GoToMeeting, GoToWebinar et GoToTraining. Il s'adresse aux techniciens et spécialistes de la sécurité responsables de la sécurité du réseau de leur entreprise et de la confidentialité et l'intégrité de ses communications.



GoToMeeting, GoToWebinar et GoToTraining sont des outils de conférence Web qui permettent à plusieurs utilisateurs PC et Mac d'interagir via le partage d'écran, le contrôle de la souris et du clavier à distance, la communication textuelle et d'autres fonctions. GoToMeeting est la solution idéale pour les présentations commerciales et les réunions de travail en ligne. Conçu pour les publics plus nombreux, GoToWebinar convient tout à fait aux présentations marketing et aux événements impliquant l'ensemble de l'entreprise. Enfin, GoToTraining offre des fonctions spécialement adaptées aux formations en ligne, telles que l'accès aux tests et aux supports de formation en ligne, ainsi qu'à un catalogue des formations hébergé.

Ces produits sont des services hébergés fournis via un navigateur Web, un client exécutable à télécharger et un réseau de serveurs de communication multicast administré par Citrix Online. Les sessions sont planifiées, tenues et modérées à l'aide du site Web Citrix Online et du logiciel client. Afin de faciliter leur utilisation et offrir la meilleure expérience possible, GoToMeeting, GoToWebinar et GoToTraining intègrent automatiquement les fonctions de conférence téléphonique et de VoIP.

Besoins des entreprises en matière de collaboration sécurisée

Grâce à des outils de collaboration en ligne intuitifs tels que GoToMeeting, GoToWebinar et GoToTraining, les entreprises sont en mesure d'accroître leur productivité en communiquant et en interagissant de manière plus efficace avec leurs collaborateurs, leurs partenaires et leurs clients. Mais l'intégration des fonctions de sécurité varie grandement d'un outil à l'autre. De plus, il est essentiel de comprendre les enjeux de la collaboration en ligne en matière de sécurité et de respecter certaines consignes.

Avant d'utiliser une solution de conférence Web, il est important de prendre en compte les menaces et risques éventuels encourus par l'entreprise. Il est d'usage de se pencher sur les besoins suivants en matière de sécurité avant l'adoption d'une solution de conférence Web :

- Prévenir toute utilisation non autorisée du service et de ses fonctions de sorte que seuls les utilisateurs légitimes et les participants puissent planifier une session en ligne et y assister ;
- Éviter de compromettre certaines ressources de l'entreprise (notamment les ordinateurs client et les réseaux privés auxquels ils sont connectés) ;
- Protéger la confidentialité et l'intégrité des communications confidentielles (partage d'écran, messages textuelles, e-mails et conversations) ;
- S'assurer de la disponibilité et de la fiabilité du service afin d'éviter toute interruption ou blocage des communications de l'entreprise ;
- Intégrer de façon transparente la solution avec les autres mesures de sécurité du réseau et des ordinateurs afin que les services de conférence tirent parti de la protection actuelle de l'organisation (au lieu de lui nuire).

Nous avons veillé à respecter ces exigences en matière de sécurité tout au long du développement de nos outils de conférence Web. L'intégration de fonctions de sécurité faciles à utiliser et à administrer permet à GoToMeeting, GoToWebinar et GoToTraining d'offrir une collaboration en ligne efficace et sans risque pour l'entreprise.

Fonctions de sécurité par rôle

Afin de permettre aux détenteurs de compte d'appliquer les règles d'accès de l'entreprise en ce qui concerne l'utilisation du service et de ses fonctions, GoToMeeting, GoToWebinar et GoToTraining attribuent à chaque utilisateur un rôle défini par l'application.

- L'organisateur peut planifier des réunions, des webinaires et des sessions de formation. L'organisateur configure chaque session, invite les participants, ouvre et clôt la session, et désigne le présentateur ;
- Les participants peuvent prendre part aux sessions. Les participants peuvent voir l'écran du présentateur, discuter avec les autres participants et afficher la liste des participants ;
- Le présentateur est un participant qui peut partager son écran avec les autres participants. Le présentateur détermine également quels utilisateurs peuvent contrôler la souris et le clavier de son ordinateur ;
- Les administrateurs internes sont des employés de Citrix Online autorisés à gérer les services et les comptes GoToMeeting, GoToWebinar et GoToTraining ;
- Les administrateurs externes font partie du personnel du client autorisé à gérer les comptes de plusieurs utilisateurs. Les administrateurs externes peuvent configurer les fonctions associées à un compte, désigner les organisateurs et utiliser différents outils de création de rapports.

Les interfaces utilisateur de GoToMeeting, GoToWebinar et GoToTraining offrent des commandes et des indicateurs d'état intuitifs qui favorisent la productivité et la sécurité des sessions en ligne.

Les commandes et les privilèges auxquels chaque utilisateur a accès dépendent de son rôle : organisateur, présentateur actuel ou simple participant.

Privilèges de l'organisateur

L'organisateur est aux commandes de la session ; il peut accorder et retirer différents privilèges aux autres participants.

Privilèges propres à l'organisateur :

- Il peut inviter les participants, avant ou pendant la session, afin que seuls les participants autorisés puissent se joindre à la session ;
- Il peut consulter la liste des participants, ainsi que leurs rôles et privilèges, afin de connaître les participants ;
- Il peut ouvrir et clore la session, ce qui évite toute interruption involontaire ou malveillante de la session ;
- Il peut désigner tout participant comme présentateur actuel, décidant à tout moment de l'écran à partager pendant la session ;
- Il peut bloquer la fonction de conversation pour un ou plusieurs participants et permettre les conversations au moment approprié ;
- Il peut déconnecter certains participants ;

- Il peut déléguer son rôle d'organisateur à un autre participant afin que la session puisse se poursuivre s'il doit la quitter avant son terme (une fois un autre participant désigné comme organisateur, il n'est plus possible d'annuler ce choix).

Privilèges du présentateur

Le présentateur est le participant qui partage son écran avec les autres participants. Au cours d'une session, un seul participant à la fois peut endosser le rôle de présentateur. Commandes disponibles au présentateur :

- Il peut activer, désactiver ou mettre en pause le partage d'écran, ce qui permet d'éviter d'afficher des données confidentielles se trouvant sur l'ordinateur de l'intervenant (lorsqu'il parcourt un fichier, par exemple) ;
- Il peut accorder/retirer la commande de la souris et du clavier à tout participant, ce qui facilite la communication via l'interaction avec l'ordinateur ;
- Il peut désigner un autre présentateur parmi les participants, ce qui contribue au dynamisme, à la fluidité et à la flexibilité du déroulement de la session.

Lorsque le présentateur partage son écran, un indicateur « En service » s'affiche sur son panneau de commande. Pour partager son écran, le présentateur doit cliquer sur le bouton Afficher mon écran du panneau de commande. Ces fonctions permettent au présentateur de savoir à tout moment s'il partage ou non son écran, et ainsi d'éviter que des informations soient partagées par inadvertance.

Privilèges du participant

L'utilisateur endossant le rôle de simple participant dispose des privilèges suivants :

- Il peut se joindre à une session lorsqu'il y est invité (même si celle-ci est déjà en cours) ;
- Il peut voir l'écran du présentateur, à moins que ce dernier ait mis en pause ou désactivé le partage d'écran ;
- Il peut recevoir le contrôle à distance de la souris et du clavier du présentateur (les privilèges de contrôle à distance sont automatiquement révoqués lorsque le rôle de présentateur est attribué à un autre participant) ;
- Il peut envoyer des messages à tous les participants ou à un participant donné via la fenêtre de conversation ou chat (l'organisateur peut cependant désactiver la fonction de conversation pour un ou plusieurs participants) ;
- Il peut quitter la session à tout moment.

L'attribution des droits et privilèges en fonction d'un rôle donne lieu à des sessions plus flexibles, ce qui facilite une interaction plus dynamique entre les participants, sans perte de contrôle ni de visibilité. Les organisateurs peuvent ajouter des participants ou désigner un autre présentateur pendant la session, en toute simplicité. Les présentateurs conservent donc une maîtrise totale de leur ordinateur, et les organisateurs disposent de tous les outils nécessaires pour gérer efficacement la session.

Fonctions d'authentification de compte et de session

L'authentification de chaque utilisateur permet d'identifier chaque individu avant de lui accorder l'accès à la session. Afin de garantir l'identité de chaque organisateur, présentateur et participant, GoToMeeting, GoToWebinar et GoToTraining disposent de fonctions d'authentification de compte et de session très performantes.

Connexion au compte via le site Web

Pour accéder à un compte utilisateur via le site Web GoToMeeting, GoToWebinar ou GoToTraining, il est nécessaire de saisir une adresse e-mail valide et le mot de passe du compte utilisateur correspondant. À titre de protection, tous les mots de passe doivent contenir au moins huit caractères (dont au moins une lettre et un chiffre). Un certain nombre d'échecs de connexion consécutifs entraîne le verrouillage temporaire du compte sur le site Web, afin de contrer toute tentative de piratage du mot de passe. Les mots de passe stockés dans la base de données du service sont chiffrés et contrôlés à l'aide d'un vérificateur sécurisé extrêmement résistant aux attaques par dictionnaire hors ligne.

Divulcation des informations relatives à la session

Contrairement à certaines solutions proposées par nos concurrents, les informations relatives aux sessions GoToMeeting, GoToWebinar et GoToTraining planifiées ne sont disponibles qu'à l'organisateur et aux participants invités. Dans la mesure où la description d'une session n'est disponible qu'une fois les utilisateurs authentifiés, et uniquement à ceux qui sont autorisés à la consulter, les informations potentiellement confidentielles, comme l'objet de la session, le nom de l'organisateur ou l'heure de la session, ne sont à aucun moment accessibles aux pirates, aux surfeurs curieux ou à vos concurrents.

Authentification des participants

Étant donné que la plupart des entreprises organisent des sessions dont l'accès est restreint, il ne suffit pas de permettre à tout utilisateur associé à un compte GoToMeeting, GoToWebinar ou GoToTraining donné d'accéder aux descriptions ou de participer aux sessions. L'autorisation de se connecter à une session dépend d'un identifiant de session unique et d'un mot de passe (facultatif).

Lorsqu'une session est programmée, un identifiant de session unique de neuf chiffres, créé par le gestionnaire de services GoToMeeting, GoToWebinar ou GoToTraining à l'aide d'un générateur de nombre pseudo-aléatoire, est communiqué à l'organisateur. L'identifiant de session est ensuite communiqué à tous les participants par e-mail, messagerie instantanée, téléphone ou un autre moyen de communication.

Pour rejoindre la session, chaque participant doit présenter l'identifiant de session au gestionnaire de services, en cliquant sur une URL contenant l'identifiant ou en le saisissant manuellement dans un formulaire affiché par le client GoToMeeting, GoToWebinar ou GoToTraining (téléchargé au préalable).

Si l'identifiant de session présenté est valide, le gestionnaire de services renvoie au client GoToMeeting, GoToWebinar ou GoToTraining des identifiants uniques pour cette session. Le participant ne voit pas ces identifiants, car c'est le logiciel qui les utilise pour se connecter à un ou plusieurs serveurs de communication. Ces identifiants comprennent un identifiant de session 64 bits, un identifiant de rôle (court) et un jeton de

rôle 64 bits (facultatif). Ils permettent d'identifier la session et d'authentifier en toute transparence l'utilisateur en tant qu'organisateur ou participant. Toutes les communications sensibles sont effectuées via des connexions SSL sécurisées, afin d'éviter la divulgation des identifiants de la session.

De plus, les participants doivent être authentifiés de bout en bout avec l'organisateur de la session. Ce système utilise une valeur aléatoire secrète générée par le gestionnaire de services et un mot de passe facultatif choisi par l'organisateur, qui le communique aux participants. Pour prévenir au mieux tout accès non autorisé et préserver l'aspect confidentiel de la session, Citrix Online recommande fortement d'utiliser un mot de passe.

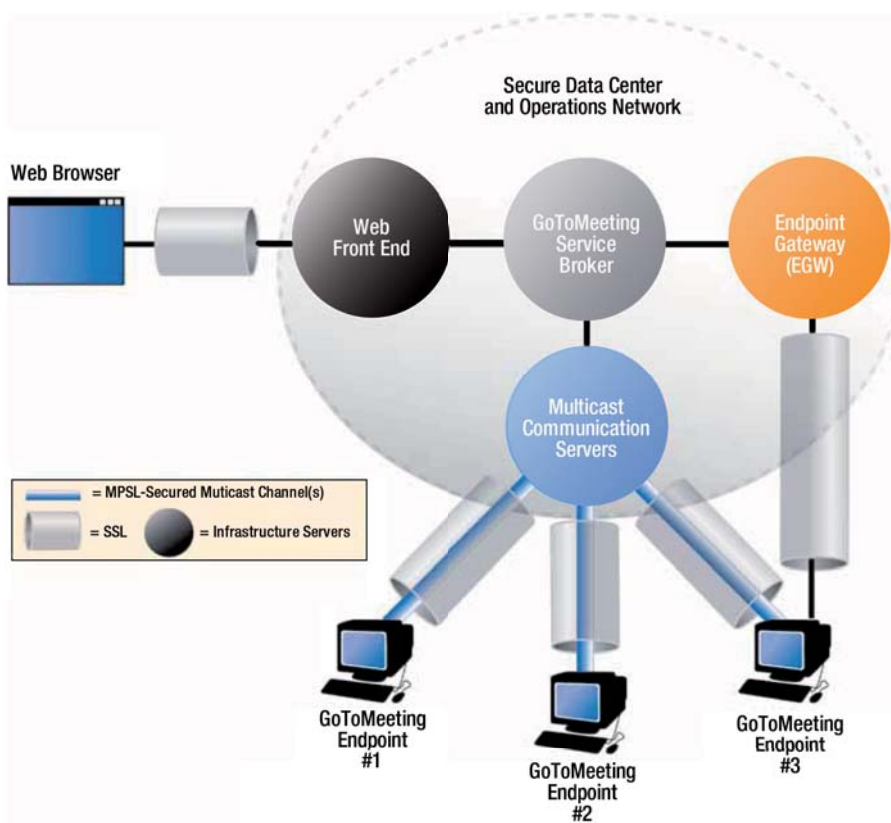
Notez que le mot de passe facultatif n'est à aucun moment communiqué à Citrix Online. Il s'agit d'une protection supplémentaire contre tout accès d'un tiers non autorisé, y compris du personnel de Citrix Online.

Une authentification de bout en bout est effectuée à l'aide du protocole SRP (Secure Remote Password). SRP est un protocole d'authentification et d'échange de clé robuste et éprouvé, qui utilise un mot de passe sécurisé. SRP résiste à une grande variété d'attaques, y compris l'écoute passive et le cassage actif de mot de passe. (Pour en savoir plus sur SRP, visitez le site Web <http://srp.stanford.edu>.)

En authentifiant les participants à deux niveaux, GoToMeeting, GoToWebinar et GoToTraining veillent à ce que seuls les participants autorisés rejoignent la session à laquelle ils ont été invités et à ce que chaque utilisateur se voie attribuer les privilèges correspondant à son rôle.

Sécurité du site d'administration

Comme toutes les connexions au site Web GoToMeeting, GoToWebinar ou GoToTraining, les connexions au portail d'administration sont protégées à l'aide du protocole SSL/TLS. Les fonctions administratives sont protégées à l'aide de mots de passe forts, de la consignation de l'activité de connexion, d'audits réguliers et d'un éventail de commandes de sécurité réseau et physiques internes.



Fonctions de sécurité des communications

La communication entre les participants d'une session GoToMeeting, GoToWebinar ou GoToTraining se fait par le biais d'une pile réseau multicast qui vient se superposer à la pile TCP/IP conventionnelle sur chaque PC utilisateur. Ce réseau est formé à partir d'un ensemble de serveurs de communication multicast (MCS) Citrix Online. Cette architecture de communication est résumée dans le schéma ci-dessous.

Les participants (extrémités de la session) communiquent avec les serveurs et passerelles de l'infrastructure Citrix Online à l'aide de connexions TCP/IP sortantes sur les ports 8200, 443 et 80. GoToMeeting, GoToWebinar et GoToTraining étant des services Web hébergés, les participants peuvent se trouver n'importe où sur Internet, qu'ils se connectent à partir d'un bureau distant, à domicile, dans un centre d'affaires ou via le réseau d'une autre société. Les services GoToMeeting, GoToWebinar et GoToTraining sont accessibles en tout lieu et à tout moment, fournissant une connectivité et une flexibilité maximales. Cependant, pour protéger la confidentialité et l'intégrité des communications commerciales privées, ces outils comprennent également des fonctions de sécurité renforcée.

Confidentialité et intégrité des communications

GoToMeeting, GoToWebinar et GoToTraining offrent des mesures de sécurité renforcée de bout en bout qui préviennent à la fois les attaques passives et actives visant la confidentialité, l'intégrité et la disponibilité. Toutes les connexions sont cryptées de bout en bout et accessibles uniquement aux participants de session autorisés.

Les données de partage d'écran, les données de contrôle de la souris et du clavier et les informations de conversation textuelle ne sont jamais exposées sous forme non cryptée pendant leur passage sur les serveurs de communication Citrix Online ou pendant leur transmission sur des réseaux publics ou privés.

Des contrôles de sécurité de communication basés sur un cryptage renforcé sont mis en œuvre à deux niveaux : la « couche TCP » et la « couche de sécurité des paquets multicast » (MPSL).

Sécurité de la couche TCP

Des protocoles SSL (Secure Sockets Layer) et TLS (Transport Layer Security) de norme IETF sont utilisés pour protéger toutes les communications entre les extrémités. Pour offrir une protection maximale contre l'écoute clandestine, l'altération des données et les attaques par rejeu, la seule suite de chiffrement SSL prise en charge pour les connexions TCP non-Web est la clé RSA de 1 024 bits avec les algorithmes HMAC-SHA1 et AES-CBC de 128 bits. Toutefois, pour assurer une compatibilité avec un maximum de navigateurs Web et de bureaux utilisateur, les sites Web GoToMeeting, GoToWebinar et GoToTraining prennent en charge les connexions entrantes utilisant les suites de chiffrement SSL les plus répandues.

Dans leur propre intérêt, Citrix Online recommande aux utilisateurs de configurer leur navigateur afin qu'il utilise un cryptage renforcé par défaut dès que possible et de toujours installer les derniers correctifs de sécurité disponibles pour leur navigateur et leur système d'exploitation.

Lorsque des connexions SSL/TLS sont établies avec le site Web et entre les composants GoToMeeting, GoToWebinar et GoToTraining, les serveurs Citrix Online s'authentifient auprès des clients à l'aide de certificats de clé publique VeriSign/Thawte. Pour une protection renforcée contre les

attaques d'infrastructure, une authentification mutuelle basée sur certificat est mise en œuvre pour toutes les liaisons entre serveurs (MCS à MCS, MCS au Gestionnaire, par exemple). Ces mesures d'authentification renforcées empêchent les éventuels fraudeurs de faire passer leur machine pour un serveur d'infrastructure ou de s'immiscer dans des sessions.

Sécurité par couches multicast

Outre la sécurité déjà offerte par les protocoles SSL/TLS, des fonctions de protection supplémentaires viennent sécuriser de bout en bout les données de paquets multicast. Tout particulièrement, les données de session multicast sont protégées par un cryptage de bout en bout et des mécanismes d'intégrité qui empêchent quiconque ayant accès à nos serveurs de communication (que cette personne soit bien intentionnée ou non) d'écouter clandestinement une session ou de manipuler les données sans être repéré. Seuls nos produits offrent un tel niveau de confidentialité et d'intégrité en matière de communications. Les communications d'entreprise ne sont jamais visibles par des tiers, qu'il s'agisse d'un utilisateur n'ayant pas été invité à une session donnée ou de Citrix Online elle-même.

La clé MPSSL est mise en œuvre sur la base d'un accord de clé authentifié SRP-6 basé sur une clé publique utilisant un module de 1 024 bits pour établir une clé de cryptage principale. Cette clé de cryptage principale est ensuite utilisée pour distribuer la clé symétrique de groupe à l'aide de l'algorithme d'enveloppe de clé AES-CTR 128 bits (reportez-vous à la page Web <http://srp.stanford.edu/design.html>). Tous les composants de la clé sont créés à l'aide d'un générateur de nombres pseudo-aléatoires compatible FIPS alimenté à l'aide de données d'entropie recueillies sur la machine hôte à partir de différentes sources pendant l'exécution. Ces méthodes d'échange et de génération de clé dynamiques et robustes offrent une protection renforcée contre le décryptage des clés.

MPSSL renforce la protection des données de paquets multicast contre l'écoute clandestine en utilisant un cryptage AES de 128 bits en mode compteur. Les données de texte brut sont en général comprimées avant cryptage à l'aide de techniques propriétaires hautes performances pour optimiser la bande passante. L'intégrité des données est protégée en incluant une valeur de contrôle d'intégrité générée avec l'algorithme HMAC-SHA-1. GoToMeeting, GoToWebinar et GoToTraining utilisent des mesures cryptographiques renforcées qui sont conformes aux normes industrielles ; les clients ont ainsi la garantie que les données de session multicast sont protégées contre toute divulgation non autorisée ou toute modification non détectée.

De plus, ces fonctions de sécurité essentielles n'entraînent pas de coûts supplémentaires, de dégradation des performances ni de difficultés d'utilisation. Les données du client sont protégées par des mesures de sécurité normalisées et hautes performances à chaque session.

Compatibilité avec les proxy et les pare-feu

À l'instar des autres produits Citrix Online, GoToMeeting, GoToWebinar et GoToTraining présentent une logique de gestion des connexions et de détection des proxy intégrée qui permet d'automatiser l'installation des logiciels, d'éviter les (re)configurations de réseau complexes et de maximiser la productivité des utilisateurs. Les pare-feu et les proxy déjà présents sur votre réseau n'ont généralement pas besoin d'être reconfigurés pour permettre l'utilisation de nos outils de conférence Web.

Au démarrage du logiciel d'extrémité GoToMeeting, GoToWebinar ou GoToTraining, l'application tente de contacter le Gestionnaire de services via la passerelle d'extrémité (EGW) en initiant une ou plusieurs connexions TCP sortantes protégées par SSL sur les ports 8200, 443 et/ou 80. La première connexion qui répond est utilisée, les autres sont abandonnées. Cette connexion servira de base à toutes les participations aux sessions ultérieures en permettant la communication entre les serveurs hébergés et le bureau de l'utilisateur.

Lorsque l'utilisateur essaie de se connecter à une session, le logiciel d'extrémité établit une ou plusieurs connexions supplémentaires aux serveurs de communication Citrix Online en utilisant là encore les connexions TCP protégées par SSL aux ports 8200, 443 et/ou 80. Ces connexions acheminent les données durant une session active.

Pour les tâches d'optimisation de la connectivité, le logiciel d'extrémité initie également une ou plusieurs connexions TCP de courte durée sur les ports 8200, 443 ou 80 qui ne sont pas protégées par SSL. Ces « sondes » réseau n'acheminent aucune information sensible ou exploitable et ne présentent donc aucun risque en ce qui concerne la divulgation d'informations secrètes.

Puisqu'ils ajustent automatiquement les conditions du réseau local en utilisant des connexions sortantes uniquement et en sélectionnant un port déjà ouvert sur la majorité des pare-feu et proxy, GoToMeeting, GoToWebinar et GoToTraining offrent un degré élevé de compatibilité avec les mesures de sécurité réseau existantes. Contrairement à d'autres produits, nos outils n'exigent pas des entreprises qu'elles désactivent les protections existantes pour permettre de tenir des conférences Web. Ces fonctions optimisent la compatibilité et la sécurité réseau globale.

Sécurité de la voix

Citrix Online offre des fonctions de conférence audio intégrées pour les sessions GoToMeeting, GoToWebinar et GoToTraining, via le réseau téléphonique ainsi qu'à l'aide du protocole VoIP. Le réseau téléphonique préserve d'emblée la confidentialité et l'intégrité des communications vocales. Afin de garantir la confidentialité et l'intégrité des connexions VoIP entre les systèmes d'extrémité et les serveurs de voix, nous utilisons un SRTP avec protocole AES-128-HMAC-SHA1 sur UDP et TLS-RSA-1024-AES-128-HMAC-SHA1 sur TCP.

Fonctions de sécurité du système d'extrémité

Le logiciel de conférence Web doit être compatible avec une grande variété d'environnements de bureau tout en créant une extrémité sûre sur le bureau de chaque utilisateur. GoToMeeting, GoToWebinar et GoToTraining répondent à ces exigences en utilisant des exécutables disponibles sur Internet qui emploient des mesures cryptographiques renforcées.

Logiciel d'extrémité signé

Notre logiciel d'extrémité client est un exécutable Win32 qui est téléchargé sur l'ordinateur des utilisateurs. Une applet Java signée numériquement contrôle le téléchargement et vérifie l'intégrité du logiciel d'extrémité GoToMeeting, GoToWebinar ou GoToTraining à partir des serveurs Citrix Online. Cela évite que l'utilisateur installe par inadvertance un cheval de Troie ou un autre logiciel malveillant imitant notre application.

Le logiciel d'extrémité est composé de plusieurs exécutables Win32 et de bibliothèques reliées de manière dynamique. Lors du développement et

du déploiement, Citrix Online applique des procédures strictes de gestion de la configuration et de contrôle de la qualité pour assurer la sécurité du logiciel. Le logiciel d'extrémité n'expose aucune interface réseau disponible en externe et ne peut pas être utilisé par des logiciels malveillants ou des virus pour exploiter ou infecter les systèmes distants. Ainsi, les différents bureaux connectés à une session ne peuvent pas être infectés par un hôte compromis utilisé par un autre participant.

Mise en œuvre du sous-système cryptographique

L'ensemble des fonctions cryptographiques et des protocoles de sécurité utilisés par le logiciel d'extrémité client GoToMeeting, GoToWebinar ou GoToTraining est mis en œuvre à l'aide des bibliothèques de pointe Certicom Security Builder® Crypto™ et Certicom Security Builder® SSL™, gage de tranquillité d'esprit et de hautes performances.

L'utilisation des bibliothèques cryptographiques est limitée aux applications d'extrémité GoToMeeting, GoToWebinar et GoToTraining ; les API externes ne sont pas accessibles aux autres logiciels exécutés sur ce bureau. Tous les algorithmes d'intégrité et de cryptage, la taille de clé et les autres paramètres de cryptographie sont codés de manière statique lors de la compilation de l'application. Aucun paramètre cryptographique n'est configurable par l'utilisateur final. Par conséquent, les utilisateurs ne peuvent pas affecter notre sécurité suite à une erreur de configuration accidentelle ou intentionnelle. Les entreprises qui utilisent GoToMeeting, GoToWebinar ou GoToTraining ont la garantie que toutes les extrémités connectées bénéficient du même niveau de sécurité de conférence Web, quel que soit le propriétaire ou l'utilisateur du bureau.

Fonctions de sécurité de l'infrastructure hébergée

Citrix Online distribue GoToMeeting, GoToWebinar et GoToTraining en utilisant un modèle de prestation de services d'application (ASP) conçu spécifiquement pour assurer un fonctionnement robuste et sûr tout en s'intégrant de manière transparente à l'infrastructure réseau et de sécurité existante de l'entreprise.

Infrastructure fiable et évolutive

L'architecture de service de Citrix Online a été conçue pour offrir des performances, une fiabilité et une évolutivité optimales. Les solutions GoToMeeting, GoToWebinar et GoToTraining sont pilotées par des serveurs et des équipements réseau de grande capacité et conformes aux normes industrielles qui sont équipés des tout derniers correctifs de sécurité disponibles. Des routeurs et des commutateurs redondants sont intégrés dans l'architecture pour éliminer tout point de défaillance. Des systèmes de sauvegarde et des serveurs en grappe aident à assurer un flux transparent des processus d'application, même en cas de charge importante ou d'erreur système. Pour des performances optimales, le Gestionnaire GoToMeeting, GoToWebinar ou GoToTraining répartit la charge des sessions client/serveur entre des serveurs de communication dispersés géographiquement.

Sécurité physique

Tous les serveurs Web, d'application, de communication et de base de données Citrix Online sont hébergés dans des centres de données sécurisés et colocalisés. L'accès physique aux serveurs est très restreint et contrôlé en permanence. Tous les sites disposent de contrôles de l'environnement et de l'alimentation redondants.

Sécurité réseau

Citrix Online utilise des contrôles d'accès basé sur VPN, routeur et pare-feu pour protéger ses réseaux de service privé et ses serveurs dorsaux. La sécurité de l'infrastructure est constamment contrôlée et des tests de vulnérabilité sont régulièrement effectués par l'équipe interne et par des vérificateurs indépendants.

Respect de la vie privée des clients

Parce que garder la confiance de nos clients est une priorité, Citrix Online s'engage à respecter leur vie privée. Vous trouverez un lien vers la politique de confidentialité actuelle sur le site <http://www.gotomeeting.fr/fec>.

Conclusion

Grâce à GoToMeeting, GoToWebinar et GoToTraining, il devient un jeu d'enfant d'organiser des réunions, de présenter des informations et des produits en ligne, et d'améliorer la communication au sein de l'entreprise. Leurs fonctions et interface sécurisées et intuitives font de ces outils les solutions de conférence Web les plus efficaces du marché.

En arrière-plan, l'architecture de service hébergée de Citrix Online prend en charge de manière transparente la collaboration multipoint en fournissant un environnement sûr et fiable. Comme le montre ce document, GoToMeeting, GoToWebinar et GoToTraining offrent flexibilité et simplicité d'utilisation sans compromettre l'intégrité, la confidentialité ni le contrôle administratif des communications professionnelles et des équipements informatiques.

Annexe : conformité aux normes de sécurité

GoToMeeting, GoToWebinar et GoToTraining sont compatibles avec les normes industrielles et des États-Unis suivantes en matière d'algorithmes cryptographiques et de protocoles de sécurité :

- Protocole TLS/SSL, version 1.0 IETF RFC 2246
- Norme AES (Advanced Encryption Standard), FIPS 197
- Suites de chiffrement AES pour TLS, IETF RFC 3268
- RSA, PKCS n°1
- SHA-1, FIPS 180-1
- HMAC-SHA-1, IETF RFC 2104
- MD5, IETF RFC 1321
- Génération de nombres pseudo-aléatoires, ANSI X9.62 et FIPS 140-2

Citrix Online

Citrix Online, division « Online Services » de Citrix Systems, Inc. (NASDAQ:CTXS) met à disposition des solutions sûres et conviviales en vue de la collaboration en ligne mondiale. Qu'il s'agisse de GoToMyPC™ pour l'accès et le travail sur des sites à distance, GoToAssist™ pour l'assistance aux clients, GoToMeeting™ pour les réunions en ligne ou GoToWebinar™ pour les séminaires Web, les clients – plus de 35.000 entreprises et des centaines de milliers de particuliers – optimisent facilement et efficacement leur distribution, leurs formations et leur service grâce aux produits GoTo.

Essayez GoToMeeting :

Contactez le service des ventes
Tél. 0800 919 211
Tester gratuitement GoToMeeting
<http://www.gotomeeting.fr>



Citrix Online Division

7414 Hollister Avenue
Goleta, CA 93117
U.S.A.
Tél. +1 805 690 6400
info@citrixonline.com

Contact pour la presse :
pr@citrixonline.com
T +1 805 690 2969

Citrix Online Europe

Proche Orient & Afrique
Citrix Online UK Ltd
Chalfont Park House
Chalfont Park, Gerrards Cross
Bucks SL9 0DZ
Royaume-Uni
Tél. +44 (0) 800 011 2120
europe@citrixonline.com

Citrix Online Asia Pacific

Level 3, 1 Julius Ave
Riverside Corporate Park
North Ryde NSW 2113
Australie
Tél. +61 2 8870 0870
asiapac@citrixonline.com

Informations relatives à Citrix Online

Les solutions de Citrix Online permettent aux gens de travailler en tout lieu. Nos produits comprennent le système d'assistance à distance GoToAssist®, GoToManage™ pour la gestion IT, GoToMeeting® pour les réunions en ligne, GoToMyPC® pour l'accès à distance, GoToTraining™ pour les formations interactives en ligne et enfin GoToWebinar® pour des événements importants via le Web.

©2011 Citrix Online, LLC. Tous droits réservés. Citrix® est une marque déposée de Citrix Systems, Inc. aux Etats-Unis et dans d'autres pays. GoToAssist®, GoToManage®, GoToMeeting®, GoToMyPC®, GoToTraining® et GoToWebinar™ sont des marques ou des marques déposées de Citrix Systems, LLC, aux Etats-Unis et dans d'autres pays. Toutes les autres marques ™ et marques déposées sont la propriété de leur propriétaire respectif.