Relatório Técnico

Conferência pela Web: Aproveite todo o potencial da colaboração segura e em tempo real

Este documento aborda informações de segurança do Cisco WebEx Meeting Center, Cisco WebEx Training Center, Cisco WebEx Support Center e Cisco WebEx Event Center.

Introdução

As soluções on-line Cisco WebEx® permitem que os funcionários globais e as equipes virtuais se reúnam e colaborem em tempo real como se estivessem trabalhando na mesma sala. A colaboração on-line pode melhorar a colaboração presencial tradicional fazendo com que o tempo e os custos de viagem, e até mesmo a sala de conferência, não sejam um problema. Empresas, instituições e agências governamentais em todo o mundo confiam nas soluções Cisco WebEx® para simplificar os processos empresariais e melhorar os resultados das equipes de vendas, marketing, treinamento, gerenciamento de projeto e suporte.

A segurança é uma grande preocupação para todas essas empresas e agências. A colaboração on-line deve oferecer vários níveis de segurança, desde o agendamento de reuniões à autenticação de participantes até o compartilhamento de documentos.

A Cisco faz da segurança a prioridade no projeto, na implantação e na manutenção da rede, da plataforma e dos aplicativos. Você pode incorporar as soluções WebEx® em seus processos empresariais com confiança, mesmo com os requisitos de segurança mais rigorosos.

Compreender os recursos de segurança dos aplicativos on-line do Cisco WebEx e da infraestrutura de comunicação subjacente, a Cisco WebEx Cloud, é uma parte importante de sua decisão de investimento.

A infraestrutura Cisco WebEx Cloud

Cisco WebEx Meetings é uma solução de software como serviço (SaaS) oferecida pela Cisco WebEx Cloud, uma plataforma altamente segura de fornecimento de serviços com desempenho, integração, flexibilidade, escalabilidade e disponibilidade líderes do setor. A Cisco WebEx Cloud oferece a facilidade de implantação e a disponibilização de aplicativos para reduzir o custo total de propriedade, enquanto torna possível um maior nível de segurança empresarial.

Arquitetura alternada

A Cisco implementa uma rede de alternância de alta velocidade, especializada e distribuída globalmente. Os dados da sessão de reunião que se originam no computador do apresentador e que chegam aos computadores dos convidados são alternados e nunca armazenados de maneira contínua pela Cisco WebEx Cloud.[1]

[1] Quando o usuário permite a gravação na rede (NBR), a reunião é registrada e armazenada. Além da NBR, o WebEx também armazena dados do perfil e arquivos do usuário.

Data centers

A Cisco WebEx Cloud é uma infraestrutura de comunicação desenvolvida especificamente para comunicações pela Web em tempo real. As sessões WebEx usam equipamentos de switching localizados em data centers em todo o mundo. Esses data centers são estrategicamente colocados perto dos principais pontos de acesso à Internet e usam fibra óptica de alta banda larga dedicada para rotear o tráfego em todo o mundo. A Cisco opera a infraestrutura completa dentro da Cisco WebEx Cloud. Os dados nos Estados Unidos permanecem na região dos Estados Unidos, e os dados na Europa permanecem na Europa.

Além disso, a Cisco opera os locais de ponto de presença (PoP) que facilitam conexões backbone, emparelhamento de Internet, backup de site global e tecnologias de cache usadas para melhorar o desempenho e a disponibilidade para o usuário final. A Cisco está disponível 24 horas por dia, 7 dias por semana, para suporte logístico, operacional, de segurança e de mudanças de gerenciamento.

Visão geral da experiência de reunião altamente segura do WebEx

A experiência de reunião do WebEx inclui:

- Configuração do local da reunião
- Opções de segurança para agendamento
- Opções para iniciar e participar de uma reunião WebEx
- Tecnologias de criptografia
- Segurança de camada de transporte
- Compatibilidade de firewall
- Privacidade de dados da reunião
- Segurança da reunião
- Login único
- Certificações de terceiros (auditorias independentes validam a segurança do Cisco WebEx)

Os termos “reuniões WebEx” e “sessões de reuniões Cisco WebEx” referem-se à audioconferência integrada, conferência por voz pela Internet e videoconferência única ou com vários pontos usadas em todos os produtos on-line do Cisco WebEx. Esses produtos incluem:

- Cisco WebEx Meeting Center
- Cisco WebEx Training Center
- Cisco WebEx Event Center
- O Cisco WebEx Support Center (inclusive o Cisco WebEx Remote Support e o Cisco WebEx Remote Access)

A menos que exista outra especificação, os recursos de segurança descritos neste documento pertencem aos aplicativos WebEx mencionados acima.

Funções do WebEx Meeting

Os quatro papéis em uma reunião WebEx são organizador, organizador alternativo, apresentador e convidado. As seções a seguir descrevem os privilégios de segurança de cada função.

Host

O organizador agenda e inicia uma reunião WebEx. O organizador controla a experiência da reunião. Do ponto de vista da segurança, o organizador pode conceder privilégios de apresentador aos convidados. O organizador também pode bloquear a reunião e remover convidados.

Organizador alternativo

O organizador designa um organizador alternativo, que pode iniciar uma reunião agendada no WebEx no lugar do organizador. Do ponto de vista da segurança, o organizador alternativo tem os mesmos privilégios do organizador.

Apresentador

Um apresentador compartilha apresentações, aplicativos específicos ou a sua área de trabalho. O apresentador controla as ferramentas de anotação. Do ponto de vista da segurança, o apresentador pode conceder e revogar o controle remoto nos aplicativos compartilhados e na área de trabalho para convidados específicos.

Convidado

Um convidado não tem responsabilidade com a segurança ou privilégios.

Módulo de administração do site do WebEx

O módulo de administração do site do WebEx permite que os administradores autorizados gerenciem e reforcem políticas de segurança para privilégios de organizador e apresentador a cada reunião. Por exemplo, você pode personalizar as configurações de sessão para desativar a capacidade de um apresentador de compartilhar aplicativos ou transferir arquivos por site ou por usuário.

O modelo de administração do site do WebEx gerencia essas funções relacionadas à segurança:

Gerenciamento de contas

- Bloquear uma conta após um número configurável de tentativas de login
- Liberar automaticamente uma conta bloqueada após um período especificado
- Desativar contas após um período de inatividade definido

Ações de conta de usuário específicas

- Exigir que um usuário altere a senha no próximo login
- Bloquear ou desbloquear uma conta de usuário
- Ativar ou desativar uma conta de usuário

Criação de conta

- Requer texto de segurança para novas solicitações de conta
- Requer uma confirmação por e-mail para novas contas
- Permite autorregistro (login) para novas contas
- Configura regras de autorregistro para novas contas

Senhas da conta

Reforça critérios fortes para a senha da conta, incluindo:

- Combinação de letras minúsculas e maiúsculas
- Tamanho mínimo

- Número mínimo de caracteres numéricos
- Número mínimo de caracteres alfabéticos
- Número mínimo de caracteres especiais
- Nenhum caractere a ser repetido três vezes ou mais
- Nenhuma reutilização de um número específico de senhas anteriores
- Nenhum texto dinâmico (nome do site, nome do organizador, nome de usuário)
- Nenhuma senha de uma lista configurável (por exemplo, “senha")
- Período mínimo antes da alteração de senha
- Alteração da senha da conta do organizador em um cronograma configurável
- Alteração da senha da conta para todos os usuários no próximo login

Salas de reunião pessoal

As salas de reunião pessoais são acessíveis através de um URL e uma senha personalizados. Nessas salas, o organizador pode listar reuniões agendadas e em andamento, iniciar e entrar em reuniões e compartilhar arquivos com os convidados da reunião. Os administradores podem definir recursos relacionados à segurança para salas de reuniões pessoais, inclusive:

- Opções para compartilhar arquivos na sala de reunião pessoal
- Requisitos de senha para arquivos na sala de reunião pessoal

Outros recursos de segurança permitidos por meio da administração do site do WebEx

- O organizador ou os convidados podem escolher armazenar seus nomes e endereços de e-mail para tornar a organização ou a participação em novas reuniões mais algo mais fácil.
- Os organizadores atribuem as gravações para outros organizadores.
- O acesso do local pode ser restrito e exigir a autenticação de todos os organizadores e o acesso dos convidados. Pode ser necessário autenticar-se para acessar as informações do local, como reuniões listadas, bem como para obter acesso a reuniões no site.
- As regras para senhas fortes podem ser aplicadas ao WebEx Access Anywhere.
- É possível não listar todas as reuniões.
- A aprovação de solicitação da opção “Esqueceu a senha?” pode ser necessária.
- Talvez seja necessário redefinir as senhas da conta em vez de reinseri-las em nome de um usuário.

Opções de segurança para agendar reuniões WebEx

- Os organizadores individuais podem ter a capacidade de especificar a segurança de acesso à reunião (nos parâmetros configurados no nível de administração do site que não pode ser substituído).
- Uma reunião pode não estar listada para que não seja exibida no calendário visível.
- Os convidados podem ter permissão para participar de reuniões antes que o organizador entre.
- Os convidados podem acessar o áudio antes que o organizador entre.
- Apenas os convidados com uma conta no site do WebEx podem participar.
- As informações de teleconferência podem ser exibidas em reuniões.

- As reuniões poderão ser encerradas automaticamente em um horário configurável se apenas um convidado permanecer.
- Pode-se exigir que os convidados digitem o endereço de e-mail para participar de reuniões

Reuniões listadas ou não listadas

Os organizadores podem optar por listar uma reunião no calendário de reuniões público em um site do WebEx personalizado. Ou podem agendar a reunião como não listada, de modo que ela nunca apareça em um calendário de reunião. Reuniões não listadas exigem que o organizador informe explicitamente aos convidados sobre a existência da reunião, enviando um link para convidados que usam o processo de convite por e-mail ou pedindo que o convidado insira o número da reunião fornecido na página Participar da reunião.

Reuniões internas ou externas

Os organizadores podem restringir os convidados de reuniões aqueles com uma conta ou um site WebEx personalizado, conforme verificado pela capacidade de fazer login no site para participar da reunião.

Senhas da reunião

Um organizador pode definir uma senha de reunião e, em seguida, escolher incluir ou excluir a senha no e-mail de convite da reunião.

Inscrição

- O organizador pode restringir o acesso à reunião com o recurso de registro. O organizador gera uma “lista de controle de acesso” permitindo apenas os convidados que se inscreveram e foram aprovados explicitamente pelo organizador.
- As reuniões podem ser protegidas com o bloqueio da reutilização de IDs de registro no WebEx Training Center e no WebEx Event Center. Qualquer convidado que tentar reutilizar uma ID de registro que já está em uso será impedido de participar da reunião. Isso evita o compartilhamento de IDs entre vários convidados.
- Além disso, o organizador mantém a segurança da reunião ao restringir e expulsar participantes.

Qualquer combinação dessas opções de agendamento pode ser ajustada para oferecer suporte para suas políticas de segurança.

Iniciar e participar de uma reunião WebEx

Uma reunião WebEx começa após a autenticação da ID de usuário e senha do organizador pelo site do WebEx personalizado. O organizador tem o controle inicial da reunião e é o apresentador inicial. O organizador pode conceder ou revogar permissões de organizador ou apresentador para qualquer convidado, expulsar convidados selecionados ou encerrar a sessão a qualquer momento.

O organizador pode apontar um organizador alternativo para iniciar e gerenciar a reunião caso o organizador não consiga participar ou perca a conexão com a reunião. Isso mantém as reuniões mais seguras ao eliminar a possibilidade de que a função do organizador seja atribuída a um convidado inesperado ou não autorizado.

Você pode configurar seu site do WebEx personalizado para permitir que os convidados acessem a reunião, inclusive a parte de áudio, antes do organizador e para limitar os recursos disponíveis para convidados recentes para bate-papo e áudio.

Quando um convidado entra em uma reunião do WebEx pela primeira vez, o software do cliente WebEx é automaticamente baixado e instalado no computador do convidado. O software do cliente WebEx tem um

certificado emitido pela VeriSign. Em reuniões subsequentes, o aplicativo WebEx baixa e instala somente os arquivos que contêm alterações ou atualizações. Os convidados podem usar a função Desinstalar fornecida pelo sistema operacional do computador para remover facilmente os arquivos do WebEx.

Tecnologias de criptografia

As reuniões WebEx são projetadas para disponibilizar conteúdo de mídia em tempo real de maneira segura para cada convidado de uma sessão. Quando o Apresentador compartilha um documento ou apresentação, eles são codificados pelo Universal Communications Format (UCF), uma tecnologia da Cisco® , que otimiza os dados para compartilhamento. O aplicativo de reunião do WebEx em dispositivos móveis como iPad, iPhone e BlackBerry usam mecanismos de criptografia semelhantes ao PC client.

As reuniões WebEx proporcionam estes mecanismos de criptografia:

- Para reuniões WebEx em PCs e dispositivos móveis, os dados são transportados do cliente para a Cisco WebEx Cloud usando o Secure Sockets Layer (SSL) de 128 bits.
- A criptografia de ponta a ponta (E2E) é uma opção fornecida com o Cisco WebEx Meeting Center. Esse método criptografa todo o conteúdo da reunião, de ponta a ponta, entre os participantes da reunião que usam o Padrão avançado de criptografia (AES) com uma chave de 256 bits gerada aleatoriamente no computador do organizador e distribuída para os convidados com um mecanismo público baseado em chave. Diferentemente da criptografia SSL que é encerrada pela Cisco WebEx Cloud, a criptografia E2E criptografa todos os conteúdos das reuniões dentro da infraestrutura Cisco WebEx Cloud. Os dados de conteúdo da reunião com texto claro são apresentados somente na memória do computador dos participantes.[2]
- Se um usuário selecionar a opção "Lembrar de mim", a ID de login e a senha desse usuário das reuniões do WebEx salvas em PCs e dispositivos móveis serão criptografadas usando o AES de 128 bits.

Os administradores e organizadores podem selecionar a criptografia E2E usando a opção “Tipo de reunião”. A solução E2E oferece maior segurança do que o AES sozinho (embora a criptografia E2E também use AES para criptografia payload), pois a chave é conhecida apenas pelo organizador e os convidados.

Cada conexão do cliente de reunião WebEx para a WebEx Cloud é autenticada com um token de criptografia para que apenas usuários legítimos possam participar de uma reunião específica.

Segurança da camada de transporte

Além das proteções de camada de aplicativo, todos os dados da reunião são transportados usando o SSL de 128 bits. Em vez de usar a porta de firewall 80 (usada para tráfego HTTP padrão da Internet) para passar através do firewall, o SSL usa a porta de firewall 443 (usada para tráfego HTTP).

Os convidados da reunião WebEx se conectam à Cisco WebEx Cloud usando uma conexão lógica nas camadas de aplicativo/apresentação/sessão. Não há conexão de ponta a ponta entre os computadores dos convidados.

Compatibilidade de firewall

O aplicativo de reunião do WebEx se comunica com a Cisco WebEx Cloud para estabelecer uma conexão confiável e altamente segura usando HTTPS (porta 443). Como resultado, seus firewalls não precisam ser especialmente configurados para habilitar reuniões WebEx.

---

[2] Observe que o NBR não está disponível quando a criptografia E2E está habilitada. Esta opção estará disponível somente para WebEx Meeting Center.

Privacidade de dados da reunião

Todo o conteúdo das reuniões WebEx (bate-papo, áudio, vídeo, área de trabalho ou compartilhamento de documentos) são temporários (existem apenas durante a reunião). O conteúdo da reunião não é armazenado na nuvem da Cisco ou em um computador de um convidado. A Cisco mantém apenas dois tipos de informações da reunião. Eles incluem:

- **Registros detalhados de eventos (EDRs):** A Cisco usa EDRs para cobrança e relatórios. Você pode revisar as informações detalhadas do evento em seu site do WebEx personalizado ao fazer login usando sua ID de organizador. Após a autenticação, você também pode baixar esses dados no site do WebEx ou acessá-los através de APIs do WebEx. Os EDRs contêm informações básicas sobre a reunião, inclusive quem (nome de usuário e e-mail) participa de qual reunião (ID da reunião) e quando (horário de entrada e saída).
- **Arquivos de gravação na rede (NBR):** Se o organizador escolher gravar uma sessão de reunião do WebEx, a gravação será armazenada na Cisco WebEx Cloud e poderá ser acessada na área de Minhas Gravações no seu site WebEx personalizado. O arquivo será criado apenas se o organizador permitir o NBR durante a reunião ou escolher uma opção do site para gravar todas as reuniões. Os NBRs podem ser acessados por meio de links de URL. Cada link contém um token imprevisível. O organizador tem total controle de acesso a um arquivo de NBR, inclusive a capacidade para apagá-lo, compartilhá-lo ou adicionar uma senha para protegê-lo. A função de NBR é opcional e pode ser desativada pelo administrador.

Login único

A Cisco oferece suporte para autenticação unificada para login único (SSO) usando a Linguagem de Aumento da Segurança da Declaração (SAML) 1.1 e 2.0 e os protocolos WS-Federation 1.0. O suporte para SAML 1.1 está sendo descontinuado. O uso da autenticação unificada requer o upload de um certificado X.509 de chave pública para seu site do WebEx personalizado. Você poderá gerar asserções SAML que contenham atributos de usuário e assinar digitalmente as asserções com a chave privada correspondente. O WebEx valida a assinatura de asserção SAML com base no certificado de chave pública pré-carregado antes de autenticar o usuário.

Relatório de empresas terceirizadas

Além de seus procedimentos internos rigorosos, o WebEx Office of Security envolve várias empresas terceirizadas independentes para conduzir auditorias rigorosas com base em políticas, procedimentos e aplicativos internos da Cisco. Essas auditorias são criadas para validar os requisitos de segurança de missão crítica para aplicativos comerciais e do governo.

Avaliação de segurança de empresas terceirizadas

A Cisco usa fornecedores externos para realizar testes de violação contínuos e avançados e avaliações de serviço. Como parte do comprometimento, as empresas terceirizadas executam as seguintes avaliações de segurança:

- Identificar o aplicativo e/ou as vulnerabilidades de serviço mais importantes e propor soluções
- Recomendar áreas gerais para o aprimoramento de arquitetura
- Identificar erros de codificação e dar orientação para melhorias na prática de codificação
- Trabalhar diretamente com a equipe de engenharia do WebEx para explicar descobertas e dar orientação para o trabalho de correção

Certificação de Porto Seguro

Em março de 2012, a Cisco recebeu a certificação de Porto Seguro referente aos dados de clientes e parceiros (a certificação de Porto Seguro referente a dados de funcionários foi recebida em 2011). Esse certificação serve como um componente adicional para o programa de conformidade de privacidade abrangente da Cisco e, embora não seja exigido pelo governo, a empresa reconhece o valor que os clientes dão a esta certificação.

A Diretiva de Proteção de Dados da UE proíbe a transferência de dados pessoais de cidadãos europeus para nações fora da União Europeia que não atendem ao padrão de “adequação” da UE para proteção de privacidade. O Departamento de Comércio dos EUA, de acordo com a Comissão Europeia, desenvolveu uma Estrutura de Porto Seguro que permite que as empresas dos EUA atendam às diretrizes, seguindo um conjunto de princípios de privacidade da certificação Porto Seguro. As empresas certificam a conformidade com esses princípios no site do Departamento de Comércio dos EUA. A estrutura foi aprovada pela UE em 2000, e as empresas que cumprem os princípios têm a garantia de que a UE considerará suas práticas de proteção de privacidade para cidadãos da UE “adequadas”.

SSAE16

A PricewaterhouseCoopers realiza uma auditoria anual de Demonstrações de Padrões para Contratos de Certificação No.16 (SSAE16) de acordo com os padrões estabelecidos pelo Instituto Americano de Contadores Públicos Certificados. Para mais informações sobre o SSAE16, consulte: http://www.ssae16.com.

ISO 27001 e 27002

A Cisco recebeu o ISO 27001 pelo WebEx Services em outubro de 2012. O certificado é renovado a cada três anos com uma auditoria externa intermediária anual. O ISO 27001 é um padrão de segurança de informações publicado pela Organização Internacional de Normatização (ISO) que fornece recomendações de práticas recomendadas para criar um sistema de gerenciamento de segurança de informações (ISMS). Um ISMS é uma estrutura de políticas e procedimentos que inclui todos os controles legais, administrativos, físicos e técnicos que envolvem os processos de gerenciamento de riscos de informações de uma empresa. De acordo com sua documentação, o ISO 27001 foi desenvolvido para “oferecer um modelo para configurar, implementar, operar, monitorar, analisar, manter e aprimorar um sistema de gerenciamento de segurança da informação”. Consulte este link para obter mais informações sobre o ISO 27001 e o 27002: http://www.27000.org/.

Para mais informações:

Para obter mais informações sobre as soluções Cisco WebEx, visite www.cisco.com/web/BR/produtos/webex/index.html ou entre em contato com seu representante de vendas.

Sede – Américas
Cisco Systems, Inc.
San Jose, CA

Sede – Ásia-Pacífico
Cisco Systems (USA) Pte. Ltd.
Cingapura

Sede – Europa
Cisco Systems International BV Amsterdam,
Holanda

A Cisco possui mais de 200 escritórios em todo o mundo. Os endereços, números de telefone e fax estão disponíveis no site da Cisco: **www.cisco.com/go/offices**.

Impresso nos EUA C11-709579-01 04/14