Configurar certificado de descriptografia no aplicativo da Web seguro

Contents

- Introdução
- Pré-requisitos
  - Requisitos
  - Componentes Utilizados
- Descriptografia HTTPS
- Configurar certificado de descriptografia em SWA
  - Carregar um Certificado e uma Chave Raiz
  - Gerar um certificado e uma chave para o proxy HTTPS
- Importar certificado
  - Importar certificado de proxy de upstream para SWA
  - Importar certificado SWA para outro SWA
  - Importar certificado SWA no cliente Windows
  - Importar certificado SWA no cliente Mac
  - Importar certificado SWA no Ubuntu/Debian
  - Importar certificado SWA no CentOS 6
  - Importar certificado SWA no CentOS 5
  - Importar certificado SWA no Mozilla Firefox
  - Importar certificado SWA no Google Chrome
  - Importar certificado SWA no Microsoft Edge/Internet Explorer
  - Importar certificado SWA no Safari
  - Importar certificado SWA da política de grupo para clientes
- Conteúdo relacionado

Introdução

Este documento descreve as etapas para configurar certificados de criptografia HTTPS em clientes de dispositivos da Web seguros (SWA) e de proxy.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Acesso administrativo ao SWA
- Acesso à interface gráfica do usuário (GUI) do SWA

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Descriptografia HTTPS

A descriptografia HTTPS (Hypertext Transfer Protocol Secure) do SWA usa certificados raiz e arquivos de chave privada que você carrega no equipamento para criptografar o tráfego. Os arquivos de certificado raiz e de chave privada que você carregar no equipamento devem estar no formato PEM.



Note: O formato DER não é suportado.

Você também pode carregar um certificado intermediário que uma autoridade de certificação raiz assinou. Quando o SWA cria um certificado que representa o certificado do servidor, ele envia o certificado carregado junto com o certificado mimetizado para o aplicativo cliente. Dessa forma, enquanto o certificado intermediário for assinado por uma CA (Certificate Authority, Autoridade de Certificação) raiz na qual o aplicativo cliente confia, o aplicativo confiará no certificado de servidor simulado.

Configurar certificado de descriptografia em SWA

O SWA pode usar um certificado existente e uma chave privada para descriptografia HTTPS. No entanto, pode haver confusão sobre o tipo de certificado que deve ser usado, pois nem todos os certificados x.509 funcionam.

Há dois tipos principais de certificados: Certificados do Servidor e Certificados Raiz. Todos os certificados x.509 contêm um campo Restrições Básicas, que identifica o tipo de certificado:

- Tipo de Requerente=Entidade Final - Certificado do Servidor
- Tipo de Requerente=CA - Certificado Raiz

Carregar um Certificado e uma Chave Raiz

Etapa 1. Na GUI, navegue até Security Services e escolha HTTPS Proxy.
Etapa 2. Clique em Edit Settings.
Etapa 3. Clique em Usar certificado e chave carregados.
Etapa 4. Clique em Browse no campo Certificate para navegar para o arquivo de certificado armazenado na máquina local.



Note: Se o arquivo que você carregar contiver vários certificados ou chaves, o Web Proxy usará o primeiro certificado ou chave no arquivo.

Etapa 5. Clique em Procurar no campo Chave para navegar até o arquivo de chave privada.



Note: O comprimento da chave deve ser de 512, 1024 ou 2048 bits.

Etapa 6. Selecione Key is Encrypted se a chave estiver criptografada.
Etapa 7. Clique em Upload Files para transferir os arquivos de certificado e chave para o Secure Web Appliance. As informações do certificado carregado são exibidas na página Editar configurações de proxy HTTPS.
Etapa 8. (Opcional) Clique em Download Certificate para transferir para os aplicativos cliente na rede.

Etapa 9. Enviar e confirmar as alterações.

Gerar um certificado e uma chave para o proxy HTTPS

Etapa 1. Na GUI, navegue até Security Services e escolha HTTPS Proxy.
Etapa 2. Clique em Edit Settings.
Etapa 3. Escolha Usar certificado e chave gerados.
Etapa 4. Clique em Gerar novo certificado e chave.
Etapa 5. Na caixa de diálogo Gerar certificado e chave, digite as informações para exibi-lo no certificado raiz. Você pode digitar qualquer caractere ASCII, exceto a barra (/) no campo Nome comum.
Etapa 6. Clique em Gerar.
Etapa 7. As informações do certificado gerado são exibidas na página Editar configurações de proxy HTTPS.
Etapa 8. (Opcional) Clique em Download Certificate, para poder transferi-lo para os aplicativos clientes na rede.
Etapa 9. (Opcional) Clique no link Download Certificate Signing Request, para poder enviar a Certificate Signing Request (CSR) a uma CA.
Etapa 10. (Opcional) Carregue o certificado assinado para o Secure Web Appliance depois de recebê-lo da CA. Você pode fazer isso a qualquer momento depois de gerar o certificado no equipamento.
Etapa 11. Enviar e Confirmar alterações.

Importar certificado

Importar certificado de proxy de upstream para SWA

Se SWA estiver configurado para usar um proxy de upstream e o proxy de upstream estiver configurado para descriptografia HTTPS, você deverá importar o certificado de criptografia de proxy de upstream para SWA. Você pode gerenciar a lista de certificados confiáveis, adicionar certificados a ela e remover certificados dela com funcionalidade.

Etapa 1. Na GUI, selecione Network e selecione Certificate Management.
Etapa 2. Clique em Gerenciar certificados raiz confiáveis na página Gerenciamento de certificados.
Etapa 3. Para adicionar um certificado raiz confiável personalizado com autoridade de assinatura, e não na lista reconhecida pela Cisco, clique em Import e envie o arquivo de certificado.

Etapa 4. Enviar e confirmar as alterações.

Importar certificado SWA para outro SWA

Se você carregou o certificado e a chave HTTPS em um SWA para o proxy HTTPS e os arquivos

originais estiverem acessíveis, poderá importá-los para outro SWA do arquivo de configuração.

Etapa 1. Na GUI de ambos os SWAs, escolha System Administration e clique em Configuration File.

Etapa 2. Clique em Download file no computador local para exibir ou salvar.

Etapa 3. Escolha Criptografar senhas nos arquivos de configuração.

Etapa 4. (Opcional) Escolha Usar um nome de arquivo definido pelo usuário e adicione o nome desejado ao Arquivo de configuração.

Etapa 5. Clique em Submit na Configuração Atual para fazer download do arquivo de configuração .xml.

Etapa 6. Abra arquivos baixados com editores de texto ou editores XML.

Etapa 7. Copie essas marcas do SWA com o certificado, copie todos os dados dentro das marcas e substitua-as no arquivo de configuração do outro SWA:

```
<prox_config_signing_cert_name>....</prox_config_signing_cert_name>
<prox_config_uploaded_cert_name>....</prox_config_uploaded_cert_name>
<prox_config_uploaded_cert>....</prox_config_uploaded_key>
<prox_config_uploaded_key>....</prox_config_uploaded_key>
```

Etapa 8. Salve as alterações no arquivo .xml do SWA de destino.

Etapa 9. Para importar o arquivo de configuração .xml editado de volta para o SWA de destino, na GUI, escolha Administração do sistema e clique em Arquivo de configuração.

Etapa 10. Na seção Carregar configuração, clique em Carregar um arquivo de configuração do computador local.

Etapa 11. Clique em Escolher arquivo e escolha o arquivo de configuração .xml editado.

Etapa 12. Clique em Load para importar o novo arquivo de configuração com o certificado e a chave.

Etapa 13. Confirmar as alterações se o sistema solicitar.

Importar certificado SWA no cliente Windows

Para importar o certificado SWA HTTPS Proxy como confiável em computadores cliente com o sistema operacional Microsoft Windows, revise estas etapas:

Etapa 1. Clique em Iniciar na barra de tarefas e digite Gerenciar certificados do computador.
Etapa 2. Na página Certificates-Local Computer, expanda Trusted Root Certification e clique com o botão direito do mouse na pasta Certificates.
Etapa 3. Clique em All Tasks e escolha Import.
Etapa 4. Na página Assistente de importação de certificado, clique em Avançar.
Etapa 5. Para importar o arquivo de certificado SWA, clique em Browse e escolha o certificado baixado do SWA.



Tip: Para fazer o download do certificado SWA, consulte a Etapa 8 da seção Upload a Root Certificate and Key ou Generating a Certificate and Key for the HTTPS Proxy.

Etapa 6. Clique em Colocar todos os certificados na caixa de seleção a seguir.
Etapa 7. Selecione Trusted Root Certification Authorities e clique em Next.
Etapa 8. Clique em Finish.

Como alternativa, você pode executar esse comando para importar o certificado para Autoridades de Certificação Raiz Confiáveis.

```
certutil -addstore -f "ROOT" <Path to SWA Certificate/CertificateName.crt>
```



Note: Você deve substituir <Caminho para SWA Certificate/CertificateName.crt> pelo caminho do certificado e nome do arquivo baixados no momento.

Importar certificado SWA no cliente Mac

Etapa 1. Baixe o certificado do proxy HTTPS do SWA para o cliente Mac OS.
Etapa 2. Renomeie a extensão de arquivo como .crt.
Etapa 3. Execute este comando para importar o certificado como um certificado confiável:

```
sudo security add-trusted-cert -d -r trustRoot -k /Library/Keychains/System.keychain <Path to SWA Certi
```

Note: Você deve substituí-lo pelo caminho do certificado e nome do arquivo baixados no momento.

Importar certificado SWA no Ubuntu/Debian

Etapa 1. Baixe o certificado do proxy HTTPS do SWA.
Etapa 2. Abra o arquivo de certificado no editor de texto e copie todo o conteúdo.
Etapa 3. Crie um novo arquivo em /usr/local/share/ca-certificates/ com uma extensão .crt as.
Etapa 4. Edite o arquivo com o editor de texto desejado e cole o texto copiado no novo arquivo e salve.
Etapa 5. Execute este comando para atualizar os certificados no sistema operacional.

```
sudo update-ca-certificates
```

Tip: Se você tiver o certificado armazenado localmente no cliente, poderá copiar o certificado para /usr/local/share/ca-certificates/ e executar sudo update-ca-certificates.

Note: Em algumas versões, você deve instalar o pacote ca-certificates com este comando: sudo apt-get install -y ca-certificates.

Importar certificado SWA no CentOS 6

Etapa 1. Baixe o certificado do proxy HTTPS do SWA.
Etapa 2. Abra o arquivo de certificado no editor de texto e copie todo o conteúdo dentro do arquivo.
Etapa 3. Crie um novo arquivo em /etc/pki/ca-trust/source/anchors/ com uma extensão .crt.
Etapa 4. Edite o arquivo com o editor de texto desejado e o texto copiado anteriormente no novo arquivo e salve-o.
Etapa 5. Instale o pacote ca-certificates:

```
yum install ca-certificates
```

Etapa 6. Execute este comando para atualizar os certificados no sistema operacional:

```
update-ca-trust extract
```

Tip: Se você tiver o certificado armazenado localmente no cliente, poderá copiar o certificado para /etc/pki/ca-trust/source/anchors/ e executar a extração update-ca-trust depois de instalar o ca-certificates.

Importar certificado SWA no CentOS 5

Etapa 1. Baixe o certificado do proxy HTTPS do SWA.
Etapa 2. Abra o arquivo de certificado no editor de texto e copie todo o conteúdo dentro do arquivo.
Etapa 3. Crie um novo arquivo na pasta atual com uma extensão .crt (por exemplo, SWA.crt).
Etapa 4. Edite o /etc/pki/tls/certs/ca-bundle.crt com o editor de texto desejado, cole o texto copiado no final do arquivo e salve.

Tip: Se você tiver o certificado armazenado localmente no cliente (neste exemplo, o nome do arquivo é SWA.crt), você poderá anexar o certificado com este comando: cat SWA.crt >>/etc/pki/tls/certs/ca-bundle.crt.

Importar certificado SWA no Mozilla Firefox

Etapa 1. Faça o download do certificado de proxy HTTPS do SWA.
Etapa 2. Renomeie a extensão de arquivo como .crt.
Etapa 3. Abra o Firefox e clique no Menu (três barras no canto superior direito).
Etapa 4. Selecione Settings (em algumas versões, ele é Options).
Etapa 5. Clique em Privacy & Security no menu à esquerda e vá até Certificates.
Etapa 6. Clique em Exibir certificados.
Etapa 7. Clique na guia Autoridades e depois em Importar.
Etapa 8. Escolha o arquivo de certificado e clique em Abrir.
Etapa 9. Clique em OK.

Importar certificado SWA no Google Chrome

Etapa 1. Faça o download do certificado de proxy HTTPS do SWA.
Etapa 2. Renomeie a extensão de arquivo como .crt.
Etapa 3. Abra o Google Chrome e clique em Personalizar e controlar o Google Chrome (três pontos no canto superior direito).
Etapa 4. Selecione Settings.
Etapa 5. Clique em Privacy and Security no menu à esquerda.
Etapa 6. Selecione Security.
Etapa 7. Role até Gerenciar certificados e clique no botão à direita.
Etapa 8. Selecione a guia Autoridades de certificação raiz confiáveis e clique em Importar.
Etapa 9. Escolha o arquivo de certificado e clique em Abrir.
Etapa 10. Clique em OK.

Note: Se você instalar o certificado SWA no sistema operacional, o Google Chrome confia nesse certificado e não há necessidade de importar o certificado separadamente para o seu navegador.

Importar certificado SWA no Microsoft Edge/Internet Explorer

O Microsoft Edge e o Internet Explorer (IE) usam certificados do sistema operacional. Se você instalar o certificado SWA no sistema operacional, não há necessidade de importar o certificado separadamente para o seu navegador.

Importar certificado SWA no Safari

Etapa 1. Baixe o certificado do proxy HTTPS do SWA.
Etapa 2. Renomeie a extensão de arquivo como .crt.
Etapa 3. No Launchpad, selecione Keychain Access.
Etapa 4. No menu File, clique em Add Keychain.
Etapa 5. Escolha o arquivo do certificado SWA e clique em Adicionar.
Etapa 6. Selecione Security.
Etapa 7. Role até Gerenciar certificados e clique no botão à direita.
Etapa 8. Selecione a guia Autoridades de certificação raiz confiáveis e clique em Importar.
Etapa 9. Escolha o arquivo de certificado e clique em Abrir.
Etapa 10. Clique em OK.

Importar certificado SWA da política de grupo para clientes

Para distribuir certificados para computadores clientes pela Diretiva de Grupo do Ative Diretory,

use estas etapas:

Etapa 1. Baixe o certificado do proxy HTTPS do SWA.
Etapa 2. Renomeie a extensão de arquivo como .crt.
Etapa 3. Copie o arquivo de certificado para o controlador de domínio.
Etapa 4. No controlador de domínio, clique em Iniciar e abra o snap-in Gerenciamento de Diretiva de Grupo.
Etapa 5. Localize o GPO (Objeto de Política de Grupo) desejado ou crie um novo GPO para conter o certificado SWA a ser importado para o cliente.
Etapa 6. Clique com o botão direito do mouse em GPO e clique em Editar.
Etapa 7. No menu à esquerda, navegue até Computer Configuration > Policies > Windows Settings > Security Settings > Políticas de chave pública.
Etapa 8. Clique com o botão direito do mouse em Trusted Root Certification Authorities e clique em Import.
Etapa 9. Clique em Avançar na página Bem-vindo ao Assistente para Importação de Certificados.
Etapa 10. Escolha o arquivo de certificado SWA para importar e clique em Avançar.
Etapa 11. Clique em Place all certificates in the following store e, em seguida, clique em Next.
Etapa 12. Verifique se as informações fornecidas estão corretas e clique em Finish.



Note: Em algumas condições, você deve reiniciar o cliente ou executar gpupdate /force para aplicar as alterações na máquina cliente do Ative Diretory.

Conteúdo relacionado

- Guia do usuário do AsyncOS 14.5 para Cisco Secure Web Appliance - GD (General Deployment, implantação geral)
- Distribuir Certificados para Computadores Cliente Usando a Diretiva de Grupo | Aprendizado da Microsoft
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.