Guia detalhado da instalação para o TLS no ESA

Índice

Introdução

Este documento descreve como criar um certificado para o uso com o Transport Layer Security (TLS), ativar o TLS de entrada e de partida, e para pesquisar defeitos edições básicas TLS em Cisco envie por correio eletrónico a ferramenta de segurança (ESA).

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

A aplicação TLS no ESA fornece a privacidade para a transmissão ponto a ponto dos email com a criptografia. Permite que um administrador importe um certificado e uma chave privada de um serviço do Certificate Authority (CA), ou usa um certificado auto-assinado.

Cisco AsyncOS para a Segurança do email apoia a extensão *STARTTLS ao* Simple Mail Transfer Protocol (SMTP) (*S TP seguro sobre o TLS*).

> Dica: Para obter mais informações sobre do TLS, refira o RFC 3207.

> Nota: Este documento descreve como instalar Certificados no conjunto em nível com o uso da característica do *gerenciamento centralizado no* ESA. Os Certificados podem ser aplicados a nível da máquina também; contudo, se a máquina nunca é removida do conjunto e adicionada então para trás, os Certificados do máquina-nível serão perdidos.

Visão geral funcional e exigências

Um administrador pôde desejar criar um certificado auto-assinado no dispositivo para qualqueras um razões:

- A fim cifrar as conversações SMTP com o outro MTAs que usam TLS (conversações de entrada e de partida)
- A fim permitir o serviço HTTPS no dispositivo para o acesso ao GUI através do HTTPS
- Para o uso como um certificado de cliente para os protocolos lightweight directory access (LDAP), se o servidor ldap exige um certificado de cliente
- A fim permitir uma comunicação segura entre o dispositivo e a enterprise manager de Rivest-Shamir-Addleman (RSA) para a proteção da perda de dados (DLP)
- A fim permitir uma comunicação segura entre o dispositivo e um dispositivo avançado da grade da ameaça da proteção do malware de Cisco (ampère)

O ESA vem PRE-configurado com um certificado da demonstração que possa ser usado a fim estabelecer conexões TLS.

> Cuidado: Quando o certificado da demonstração for suficiente para o estabelecimento de

uma conexão TLS segura, esteja ciente que não pode oferecer uma conexão passível de verificação.

Cisco recomenda que você obtém um X.509, ou a privacidade aumentou o certificado do email (PEM) de CA. Isto pôde igualmente ser referido como um certificado de *Apache*. O certificado de CA é desejável sobre o certificado auto-assinado porque um certificado auto-assinado é similar ao certificado previamente mencionado da demonstração, que não pode oferecer uma conexão passível de verificação.

> Nota: O formato do certificado PEM é definido mais no RFC 1421 com o RFC 1424. O PEM é um formato do recipiente que possa incluir somente o certificado público (como com Apache instala e arquivo de certificado de CA */etc/ssl/certs*) ou um certificate chain inteiro, para incluir a chave pública, a chave privada, e os certificados de raiz. O nome *PEM* é de um método falhado para o email seguro, mas o formato do recipiente que usou é ainda active e é uma tradução base-64 das chaves X.509 ASN.1.

Traga seu próprio certificado

A opção para importar seu próprio certificado está disponível no ESA; contudo, a exigência é que o certificado esteja no formato do *PKCS-12*. Este formato inclui a chave privada. Os administradores não têm frequentemente os Certificados que estão disponíveis neste formato. Por este motivo, Cisco recomenda que você gerencie o certificado no ESA e o tem assinado corretamente por CA.

Atualize um certificado atual

Se um certificado que já exista expirou, salte a seção de *distribuição dos certificados auto-assinados d*estes documento e re-sinal o certificado que existe.

> Dica: Refira a renovação a um certificado em um documento Cisco da ferramenta de segurança do email para mais detalhes.

Distribua certificados auto-assinados

Esta seção descreve como gerar um certificado auto-assinado e uma solicitação de assinatura de certificado (CSR), fornecer o certificado auto-assinado a CA para assinar, transferir arquivos pela rede o certificado assinado ao ESA, especificar o certificado para o uso com os serviços ESA, e suportar a configuração de ferramenta e os certificados.

Gerencia um certificado auto-assinado e um CSR

A fim criar um certificado auto-assinado através do CLI, incorpore o comando do **certconfig**.

Termine estas etapas a fim criar um certificado auto-assinado do GUI:

1. Navegue **certificado ao > Add da rede > dos Certificados do** dispositivo GUI.

2. Clique o menu suspenso do **certificado auto-assinado da criação**.

   Quando você cria o certificado, assegure-se de que o *Common Name* combine o hostname da relação de escuta, ou que combina o hostname da relação da entrega.

   A relação de *escuta* é a relação que é ligada ao ouvinte que é configurado sob a **rede > os ouvintes**.

   A relação da *entrega* é selecionada automaticamente, a menos que configurado explicitamente do CLI com o comando do **deliveryconfig**.
3. Para uma conexão de entrada passível de verificação, valide que estes três artigos combinam:

   MX Record (hostname do Domain Name System (DNS))

   Common Name

   Hostname da relação

   Nota: O hostname do sistema não afeta as conexões TLS com respeito a ser passível de verificação. O hostname do sistema é mostrado no canto superior direito do dispositivo GUI, ou da saída do comando do **sethostname** CLI.

   Cuidado: Recorde **submeter** e **comprometer** suas mudanças antes que você exporte o CSR. Se estas etapas não são terminadas, o certificado novo não estará comprometido à configuração de ferramenta, e o certificado assinado de CA não pode assinar, nem seja aplicado a, um certificado que já exista.

Forneça o certificado auto-assinado a CA

Termine estas etapas a fim submeter o certificado auto-assinado a CA para assinar:

1. Salvar o CSR a um computador local no formato PEM (**rede > Certificados > de nome > de *transferência do* certificado *solicitação de assinatura de certificado***).

2. Envie o certificado gerado a CA reconhecido para assinar.

3. Peça X.509/PEM/Apache um certificado formatado o certificado intermediário, assim como. CA gerencie então um certificado no formato PEM.

   Nota: Para uma lista de fornecedores de CA, refira o artigo de Wikipedia do Certificate Authority.

Transfira arquivos pela rede o certificado assinado ao ESA

Depois que CA retorna o certificado público confiado que está assinado por uma chave privada, você deve transferir arquivos pela rede o certificado assinado ao ESA. O certificado pode então

ser usado com um ouvinte público ou privado, um serviço da interface IP HTTPS, a interface ldap, ou todas as conexões TLS de partida aos domínios do destino.

Termine estas etapas a fim transferir arquivos pela rede o certificado assinado ao ESA:

1. Assegure-se de que o certificado público confiado que é formato recebido dos usos PEM, ou um formato que possa ser convertido ao PEM antes que você o transfira arquivos pela rede ao dispositivo. Dica: Você pode usar o OpenSSLtoolkit, um programa de software gratuito, a fim converter o formato.
2. Transfira arquivos pela rede o certificado assinado:

   Navegue à **rede > aos Certificados**.

   Clique o nome do certificado que foi enviado a CA para assinar.

   Entre no trajeto ao arquivo no volume da máquina local ou da rede.

   Nota: Quando você transfere arquivos pela rede o certificado novo, overwrites o certificado atual. Um certificado intermediário que seja relacionado ao certificado auto-assinado pode igualmente ser transferido arquivos pela rede.

   Cuidado: Recorde **submeter** e **comprometer as** mudanças depois que você transfere arquivos pela rede o certificado assinado.

Especifique o certificado para o uso com serviços ESA

Agora que o certificado é criado, assinado, e transferido arquivos pela rede ao ESA, pode ser usado para os serviços que exigem o uso do certificado.

TLS de entrada

Termine estas etapas a fim usar o certificado para os serviços de entrada TLS:

1. Navegue à **rede > aos ouvintes**.
2. Clique o nome do ouvinte.
3. Selecione o nome do certificado do menu suspenso do *certificado*.
4. Clique em Submit.
5. Repita etapas 1 a 4 como necessário para todos os ouvintes adicionais.
6. **Comprometa as** mudanças.

TLS de partida

Termine estas etapas a fim usar o certificado para os serviços de partida TLS:

1. Navegue **para enviar políticas > controles do destino**.
2. O clique **edita configurações globais… na** seção das *configurações globais*.
3. Selecione o nome do certificado do menu suspenso do *certificado*.
4. Clique em Submit.
5. **Comprometa as** mudanças.

HTTPS

Termine estas etapas a fim usar o certificado para os serviços HTTPS:

1. Navegue à **rede > às interfaces IP**.
2. Clique o nome da relação.
3. Selecione o nome do certificado do menu suspenso do *certificado HTTPS*.
4. Clique em Submit.
5. Repita etapas 1 a 4 como necessário para todas as interfaces adicionais.
6. **Comprometa as** mudanças.

LDAP

Termine estas etapas a fim usar o certificado para os LDAP:

1. Navegue à **administração do sistema > ao LDAP**.
2. O clique **edita ajustes… na** seção das *configurações globais LDAP*.
3. Selecione o nome do certificado do menu suspenso do *certificado*.
4. Clique em Submit.
5. **Comprometa as** mudanças.

Filtragem URL

Termine estas etapas a fim usar o certificado para a Filtragem URL:

1. Incorpore o comando do **websecurityconfig no** CLI.
2. Continue com os prompts de comando. Assegure-se de que você selecione **Y** quando você alcançar esta alerta:

```
Do you want to set client certificate for Cisco Web Security Services Authentication?
```

3. Selecione o número que é associado com o certificado.

4. Inscreva o **comando commit** a fim comprometer as alterações de configuração.

Suporte a configuração de ferramenta e os certificados

Assegure-se de que a configuração de ferramenta salvar neste tempo. A configuração de ferramenta contém o trabalho terminado do certificado que foi aplicado através dos processos previamente descritos.

Termine estas etapas a fim salvar o arquivo de configuração de ferramenta:

1. Navegue ao **arquivo da administração do sistema > do arquivo de configuração > da transferência ao computador local a ver ou salvar**.

2. Exporte o certificado:

   Navegue à **rede > aos Certificados**.

   Clique o **certificado de exportação**.

   Selecione o certificado para exportar.

   Dê entrada com o nome de arquivo do certificado.

   Incorpore uma senha para o arquivo certificado.

   Clique a **exportação**.

   Salvar o arquivo a um local ou a uma máquina da rede.

   Os Certificados adicionais podem ser exportados neste tempo, ou **cancelamento do** clique a fim retornar ao lugar da **rede > dos Certificados**.

   Nota: Este processo salvar o certificado no formato do PKCS-12, que cria e salvar o arquivo com proteção de senha.

Ative o TLS de entrada

A fim ativar o TLS para todas as sessões de entrada, conecte à Web GUI, escolha **políticas do correio > políticas do fluxo de correio** para o ouvinte de entrada configurado, e termine então estas etapas:

1. Escolha um ouvinte para que as políticas devem ser alteradas.

2. Clique o link para o nome da política a fim editá-la.

3. *Nos recursos de segurança* secione, escolha um dos estes *criptografia e opções de autenticação* a fim ajustar o nível do TLS que é exigido para esses ouvinte e política do fluxo de correio:

   Fora de – Quando esta opção é escolhida, o TLS não está usado.

   Preferido – Quando esta opção é escolhida, o TLS pode negociar do MTA remoto ao ESA. Contudo, se o MTA remoto não negocia (antes da recepção de uma resposta *220*), a transação de SMTP continua *na claro* (não cifrado). Nenhuma tentativa é feita a fim verificar se o certificado origina de um Certificate Authority confiado. Se um erro ocorre depois que a resposta 220 está recebida, a seguir a transação de SMTP não cai de volta ao texto claro.

   Exigido – Quando esta opção é escolhida, o TLS pode ser negociado do MTA remoto ao ESA. Nenhuma tentativa é feita a fim verificar o certificado do domínio. Se a negociação falha, nenhum email está enviado através da conexão. Se a negociação sucede, a seguir o correio está entregado através de uma sessão de criptografia.
4. Clique em Submit.

5. Clique o botão das **mudanças comprometer**. Você pode adicionar um comentário opcional neste tempo, se desejado.

6. O clique **compromete mudanças** a fim salvar as mudanças.

A política do fluxo de correio para o ouvinte é atualizada agora com os ajustes TLS que você escolheu.

Termine estas etapas a fim ativar o TLS para as sessões de entrada que chegam de um grupo seleto de domínios:

1. Conecte à Web GUI e escolha **políticas do correio > vista geral do CHAPÉU**.

2. Adicionar os remetentes ao grupo apropriado do remetente.

3. Edite os ajustes TLS da política do fluxo de correio que é associada com o grupo do remetente que você alterou na etapa precedente.

4. Clique em Submit.

5. Clique o botão das **mudanças comprometer**. Você pode adicionar um comentário opcional neste tempo, se desejado.

6. O clique **compromete mudanças** a fim salvar as mudanças.

A política do fluxo de correio para o grupo do remetente é atualizada agora com os ajustes TLS que você escolheu.

> Dica: Refira o seguinte artigo para mais informações sobre de como o ESA segura a verificação TLS: Que é o algoritmo para a verificação de certificado no ESA?

Ative o TLS de partida

A fim ativar o TLS para sessões externas, conecte à Web GUI, escolha **políticas do correio > controles do destino**, e termine então estas etapas:

1. O clique **adiciona o destino….**

2. Adicionar o domínio do destino (tal como *domain.com*).

3. *Na seção de suporte TLS*, clique o menu suspenso e escolha uma destas opções a fim permitir o tipo de TLS que deve ser configurado:

   Nenhum – Quando esta opção é escolhida, o TLS não está negociado para conexões externas da relação ao MTA para o domínio.

   Preferido – Quando esta opção é escolhida, o TLS está negociado da relação ESA ao MTA para o domínio. Contudo, se a negociação TLS falha (antes da recepção de uma resposta 220), a transação de SMTP continua *na claro* (não cifrado). Nenhuma tentativa é feita a fim verificar se o certificado origina de CA confiado. Se um erro ocorre depois que a resposta 220 está recebida, a seguir a transação de SMTP não cai de volta ao texto claro.

   Exigido – Quando esta opção é escolhida, o TLS está negociado da relação ESA ao MTA para o domínio. Nenhuma tentativa é feita a fim verificar o certificado do domínio. Se a negociação falha, nenhum email está enviado através da conexão. Se a negociação sucede, a seguir o correio está entregado através de uma sessão de criptografia.

   Preferir-verifique – Quando esta opção é escolhida, o TLS está negociado do ESA ao MTA para o domínio, e das tentativas do dispositivo verificar o certificado do domínio. Neste caso, estes três resultados são possíveis:

   O TLS é negociado e o certificado é verificado. O correio é entregado através de uma sessão de criptografia.

   O TLS é negociado, mas o certificado não é verificado. O correio é entregado através de uma sessão de criptografia.

   Nenhuma conexão TLS é feita, e o certificado não é verificado. O mensagem de Email é entregado no texto simples.**Exigir-verifique** – Quando esta opção é escolhida, o TLS está negociado do ESA ao MTA para o domínio, e a verificação do certificado do domínio é exigida. Neste caso, estes três resultados são possíveis:

   Uma conexão TLS é negociada, e o certificado é verificado. O mensagem de Email é entregado através de uma sessão de criptografia.

   Uma conexão TLS é negociada, mas o certificado não é verificado por CA confiado. O correio não é entregado.

Uma conexão TLS não é negociada, mas o correio não é entregado.

4. Faça mais as mudanças que são precisadas os *controles do destino* para o domínio do destino.

5. Clique em Submit.

6. Clique o botão das **mudanças comprometer**. Você pode adicionar um comentário opcional neste tempo, se desejado.

7. O clique **compromete mudanças** a fim salvar as mudanças.

Troubleshooting

Esta seção descreve como pesquisar defeitos edições básicas TLS no ESA.

Certificados intermediários

Você deve procurar Certificados intermediários duplicados, especialmente quando os Certificados atuais são atualizados em vez de uma criação nova do certificado. Os certificados intermediários puderam ter mudado, ou puderam impropriamente ter sido acorrentados, e o certificado pôde ter transferido arquivos pela rede Certificados intermediários múltiplos. Isto pode introduzir edições do encadeamento e da verificação do certificado.

Permita notificações para falhas exigidas da conexão TLS

Você pode configurar o ESA a fim enviar um alerta se a negociação TLS falha quando as mensagens estão entregadas a um domínio que exija uma conexão TLS. O mensagem de alerta contém o nome do domínio do destino para a negociação falhada TLS. O ESA envia o mensagem de alerta a todos os receptores que são ajustados para receber alertas de advertência do nível de seriedade para tipos do alerta do *sistema*.

> Nota: Esta é uma configuração global, assim que não pode ser ajustado em uma base do por-domínio.

Termine estas etapas a fim permitir alertas da conexão TLS:

1. Navegue **para enviar políticas > controles do destino**.

2. O clique **edita configurações globais**.

3. Verifique a **emissão um alerta quando uma conexão TLS exigida falha a** caixa de verificação.

   Dica: Você pode igualmente configurar este ajuste com o **destconfig >** comando CLI **setup**.

O ESA igualmente registra os exemplos para que o TLS é exigido para um domínio mas não poderia ser usado nos logs do correio do dispositivo. Isto ocorre quando qualqueras um circunstâncias são estadas conformes:

- O MTA remoto não apoia o ESMTP (por exemplo, não compreendeu o *comando EHLO do* ESA).
- O MTA remoto apoia o ESMTP, mas o comando *STARTTLS* não estava na lista de Ramais que anunciou em sua resposta *EHLO*.
- O MTA remoto anunciou a extensão *STARTTLS* mas respondeu com um erro quando o ESA enviou o comando *STARTTLS*.

Situe sessões de comunicação bem sucedidas TLS nos logs do correio

As conexões TLS são gravadas nos logs do correio, junto com outras ações significativas que são relacionadas às mensagens, tais como sentenças das ações do filtro, as anti-vírus e do anti-Spam, e tentativas da entrega. Se há uma conexão TLS bem sucedida, haverá uma entrada do *sucesso* TLS nos logs do correio. Igualmente, uma conexão TLS falhada produz uma entrada *falhada* TLS. Se uma mensagem não tem uma entrada associada TLS no arquivo de registro, essa mensagem não esteve entregada sobre uma conexão TLS.

> Dica: A fim compreender os logs do correio, refira o documento Cisco da determinação da disposição da mensagem ESA.

Está aqui um exemplo de uma conexão TLS bem sucedida do host remoto (recepção):

```
Wed Jul 20 19:47:40 2005 Info: New smtp ICID 282204970 interface mail.example.com
(10.2.3.4) address 10.3.4.5 reverse dns host unknown verified no
Wed Jul 20 19:47:40 2005 Info: ICID 282204970 ACCEPT SG None match SBRS None
Wed Jul 20 19:47:40 2005 Info: ICID 282204970 TLS success
Wed Jul 20 19:47:40 2005 Info: Start MID 200257070 ICID 282204970
```

Está aqui um exemplo de uma conexão TLS falhada do host remoto (recepção):

```
Tue Jun 28 19:08:49 2005 Info: New SMTP ICID 282204971 interface Management
(10.2.3.4) address 10.3.4.5 reverse dns host unknown verified no
Tue Jun 28 19:08:49 2005 Info: ICID 282204971 ACCEPT SG None match SBRS None
Tue Jun 28 19:08:49 2005 Info: ICID 282204971 TLS failed
Tue Jun 28 19:08:49 2005 Info: ICID 282204971 lost
Tue Jun 28 19:08:49 2005 Info: ICID 282204971 TLS was required but remote host did
not initiate it
Tue Jun 28 19:08:49 2005 Info: ICID 282204971 close
```

Está aqui um exemplo de uma conexão TLS bem sucedida ao host remoto (entrega):

```
Tue Jun 28 19:28:31 2005 Info: New SMTP DCID 834 interface 10.10.10.100 address
192.168.1.25 port 25
Tue Jun 28 19:28:31 2005 Info: DCID 834 TLS success protocol TLSv1 cipher
DHE-RSA-AES256-SHA
Tue Jun 28 19:28:31 2005 Info: Delivery start DCID 834 MID 1074 to RID [0]
```

Está aqui um exemplo de uma conexão TLS falhada ao host remoto (entrega):

```
Fri Jul 22 22:00:05 2005 Info: DCID 2386070 IP 10.3.4.5 TLS failed: STARTTLS
unexpected response
```

Informações Relacionadas

- Cisco envia por correio eletrónico a ferramenta de segurança - Guias do utilizador final

- Dispositivo do Gerenciamento de segurança do índice de Cisco - Guias do utilizador final
- Suporte Técnico e Documentação - Cisco Systems