Criar Guia de Configuração de Certificados para TLS no ESA

Contents

Introduction

Este documento descreve como criar um certificado para uso com TLS, ativar TLS de entrada/saída e solucionar problemas no Cisco ESA.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

A implementação do TLS no ESA fornece privacidade para transmissão ponto a ponto de e-mails através de criptografia. Permite que um administrador importe um certificado e uma chave privada de um serviço de Autoridade de Certificação (CA) ou use um certificado autoassinado.

O Cisco AsyncOS para Email Security oferece suporte à extensão *STARTTLS* para o Simple Mail Transfer Protocol (SMTP) (*Secure SMTP over TLS*).

> **Dica**: para obter mais informações sobre TLS, consulte RFC 3207.

> **Observação**: este documento descreve como instalar certificados no nível de cluster com o uso do *recurso de gerenciamento centralizado* no ESA. Os certificados também podem ser aplicados no nível da máquina; no entanto, se a máquina for removida do cluster e adicionada novamente, os certificados no nível da máquina serão perdidos.

Visão geral funcional e requisitos

Um administrador deseja criar um certificado autoassinado no equipamento por qualquer um destes motivos:

- Para criptografar as conversações SMTP com outros MTAs que usam TLS (conversações de entrada e de saída).
- Para habilitar o serviço HTTPS no equipamento para acesso à GUI via HTTPS.
- Para uso como um certificado de cliente para LDAPs (Lightweight Diretory Access Protocols), se o servidor LDAP exigir um certificado de cliente.
- Para permitir a comunicação segura entre o dispositivo e o RSA (Rivest-Shamir-Addleman), use o Enterprise Manager para Proteção contra Perda de Dados (DLP).
- Para permitir a comunicação segura entre o dispositivo e um dispositivo Cisco Advanced Malware Protection (AMP) Threat Grid.

O ESA vem pré-configurado com um certificado de demonstração que pode ser usado para

estabelecer conexões TLS.

> **Cuidado**: embora o certificado de demonstração seja suficiente para o estabelecimento de uma conexão TLS segura, lembre-se de que ele não pode oferecer uma conexão verificável.

A Cisco recomenda que você obtenha um certificado X.509 ou Privacy Enhanced Email (PEM) de uma CA. Isso também é chamado de certificado *Apache*. O certificado de uma CA é desejável em relação ao certificado autoassinado porque um certificado autoassinado é semelhante ao certificado de demonstração mencionado anteriormente, que não pode oferecer uma conexão verificável.

> **Observação**: o formato do certificado PEM é definido mais detalhadamente no RFC 1421 até o RFC 1424. O PEM é um formato de contêiner que pode incluir apenas o certificado público (como em instalações Apache e arquivos de certificado CA */etc/ssl/certs*) ou uma cadeia de certificados inteira, para incluir a chave pública, a chave privada e os certificados raiz. O nome *PEM* é de um método com falha para e-mail seguro, mas o formato de contêiner que ele usou ainda está ativo e é uma conversão de base 64 das chaves X.509 ASN.1.

Traga seu próprio certificado

A opção de importar seu próprio certificado está disponível no ESA; no entanto, o requisito é que o certificado esteja no formato *PKCS#12*. Esse formato inclui a chave privada. Normalmente, os administradores não têm certificados disponíveis nesse formato. Por esse motivo, a Cisco recomenda que você gere o certificado no ESA e o assine corretamente por uma CA.

Atualizar um certificado atual

Se um certificado que já existe tiver expirado, ignore a seção *Implantação de Certificados AutoAssinados* deste documento e assine novamente o certificado que existe.

> **Dica**: consulte o documento Renovar um certificado em um dispositivo de segurança de e-mail da Cisco para obter mais detalhes.

Implantar Certificados Autoassinados

Esta seção descreve como gerar um certificado autoassinado e uma CSR (Certificate Signing Request, Solicitação de assinatura de certificado), fornecer o certificado autoassinado a uma CA para assinatura, carregar o certificado assinado para o ESA, especificar o certificado para uso com os serviços ESA e fazer backup da configuração do dispositivo e do(s) certificado(s).

Gerar um certificado autoassinado e CSR

Para criar um certificado autoassinado via CLI, insira o comando **certconfig**.

Para criar um certificado autoassinado a partir da GUI:

1. Navegue até **Network > Certificates > Add Certificate** na GUI do equipamento.

2. Clique no menu suspenso **Create Self-Signed Certificate**.

   Ao criar o certificado, certifique-se de que o *Nome Comum* corresponda ao nome de host da interface de escuta ou que corresponda ao nome de host da interface de entrega.
   A interface de *escuta* é a interface vinculada ao ouvinte configurado em **Rede > Ouvintes**.A interface de *entrega* é selecionada automaticamente, a menos que seja configurada explicitamente na CLI com o comando **deliveryconfig**.
3. Para uma conexão de entrada verificável, confirme se estes três itens correspondem:

   Registro MX (nome de host do Sistema de Nomes de Domínio (DNS))

   Nome comum

   Nome de host da interface

   Observação: o nome de host do sistema não afeta as conexões TLS no que diz respeito a ser verificável. O nome de host do sistema é mostrado no canto superior direito da GUI do equipamento ou na saída do comando CLI **sethostname**.

   Cuidado: lembre-se de **enviar** e **confirmar** suas alterações antes de exportar o CSR. Se essas etapas não forem concluídas, o novo certificado não será confirmado na configuração do equipamento e o certificado assinado da CA não poderá assinar, nem ser aplicado a, um certificado que já exista.

Fornecer o Certificado AutoAssinado a uma CA

Para enviar o certificado autoassinado a uma CA para assinatura:

1. Salve o CSR em um computador local no formato PEM **Network > Certificates > Certificate Name > Download Certificate Signing Request**.

2. Enviar o certificado gerado para uma autoridade de certificação reconhecida para assinatura.

3. Solicite um certificado formatado X.509/PEM/Apache, bem como o certificado intermediário. Em seguida, a CA gera um certificado no formato PEM.

   Observação: para obter uma lista de provedores de CA, consulte o artigo da Wikipédia sobre autoridade de certificação.

Carregar o certificado assinado para o ESA

Depois que a CA retornar o certificado público confiável que é assinado por uma chave privada, carregue o certificado assinado no ESA.

O certificado pode ser usado com um ouvinte público ou privado, um serviço HTTPS de interface IP, a interface LDAP ou todas as conexões TLS de saída para os domínios de destino.

Para carregar o certificado assinado no ESA:

1. Certifique-se de que o certificado público confiável recebido use o formato PEM ou um formato que possa ser convertido em PEM antes de carregá-lo no equipamento. **Dica**: você pode usar o OpenSSL toolkit, um programa de software gratuito, para converter o formato.
2. Carregar o certificado assinado:

   Navegue até **Rede > Certificados**.

   Clique no nome do certificado que foi enviado à CA para assinatura.

   Digite o caminho para o arquivo na máquina local ou no volume de rede.

   Observação: quando você faz upload do novo certificado, ele substitui o certificado atual. Um certificado intermediário relacionado ao certificado autoassinado também pode ser carregado.

   Cuidado: lembre-se de **enviar** e **confirmar** as alterações depois de carregar o certificado assinado.

Especificar o certificado para uso com serviços ESA

Agora que o certificado foi criado, assinado e carregado no ESA, ele pode ser usado para os serviços que exigem o uso do certificado.

TLS de entrada

Conclua estas etapas para usar o certificado para os serviços TLS de entrada:

1. Navegue até **Rede > Ouvintes**.
2. Clique no nome do listener.
3. Selecione o nome do certificado no menu suspenso *Certificate*.
4. Clique em Submit.
5. Repita as Etapas 1 a 4 conforme necessário para os ouvintes adicionais.
6. **Confirme** as alterações.

TLS de saída

Conclua estas etapas para usar o certificado para os serviços TLS de saída:

1. Navegue até **Políticas de e-mail > Controles de destino**.
2. Clique em **Edit Global Settings...** na seção *Global Settings*.
3. Selecione o nome do certificado no menu suspenso *Certificate*.
4. Clique em Submit.
5. **Confirme** as alterações.

HTTPS

Conclua estas etapas para usar o certificado para os serviços HTTPS:

1. Navegue até **Rede > Interfaces IP**.
2. Clique no nome da interface.
3. Selecione o nome do certificado no menu suspenso *HTTPS Certificate*.
4. Clique em Submit.
5. Repita as Etapas 1 a 4 conforme necessário para qualquer interface adicional.
6. **Confirme** as alterações.

LDAPs

Conclua estas etapas para usar o certificado para LDAPs:

1. Navegue até **Administração do sistema > LDAP**.
2. Clique em **Edit Settings...** na seção *LDAP Global Settings*.
3. Selecione o nome do certificado no menu suspenso *Certificate*.
4. Clique em Submit.
5. **Confirme** as alterações.

Filtragem de URL

Para usar o certificado para filtragem de URL:

1. Insira o comando **websecurityconfig** na CLI.
2. Prossiga com os prompts de comando. Certifique-se de selecionar **Y** quando chegar a este prompt:

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

3. Selecione o número associado ao certificado.

4. Insira o comando **commit** para confirmar as alterações de configuração.

Fazer backup da configuração do equipamento e dos certificados

Certifique-se de que a configuração do equipamento esteja salva neste momento. A configuração do equipamento contém o trabalho de certificado concluído que foi aplicado através dos processos descritos anteriormente.

Conclua estas etapas para salvar o arquivo de configuração do equipamento:

1. Navegue até **Administração do sistema > Arquivo de configuração > Fazer download do arquivo para o computador local para exibir ou salvar**.

2. Exportar o certificado:

   Navegue até **Rede > Certificados**.

   Clique em **Export Certificate**.

   Selecione o certificado a exportar.

   Insira o nome de arquivo do certificado.

   Insira uma senha para o arquivo de certificado.

   Clique em **Exportar**.

   Salve o arquivo em um computador local ou de rede.

   Certificados adicionais podem ser exportados neste momento ou clique em **Cancelar** para retornar ao local **Rede > Certificados**.

   Observação: esse processo salva o certificado no formato PKCS#12, que cria e salva o arquivo com proteção por senha.

Ativar TLS de entrada

Para ativar o TLS para todas as sessões de entrada, conecte-se à GUI da Web, escolha **Políticas de e-mail > Políticas de fluxo de e-mail** para o ouvinte de entrada configurado e, em seguida, conclua estas etapas:

1. Escolha um listener para o qual as políticas devem ser modificadas.

2. Clique no link do nome da política para editá-la.

3. Na seção *Recursos de segurança*, escolha uma destas opções de *Criptografia e autenticação* para definir o nível de TLS necessário para essa política de ouvinte e fluxo de e-mail:

   Apagado - Quando essa opção é escolhida, o TLS não é usado.

   Preferido - Quando essa opção é escolhida, o TLS pode negociar do MTA remoto para o ESA. No entanto, se o MTA remoto não negociar (antes do recebimento de uma resposta *220*), a transação SMTP continuará *na limpeza* (não criptografada). Não é feita nenhuma tentativa de verificar se o certificado é originário de uma autoridade de certificação confiável. Se ocorrer um erro após o recebimento da resposta 220, a transação SMTP não retornará ao texto não criptografado.

   Obrigatório - Quando essa opção é escolhida, o TLS pode ser negociado do MTA remoto para o ESA. Não é feita nenhuma tentativa de verificar o certificado do domínio. Se a negociação falhar, nenhum e-mail será enviado por meio da conexão. Se a negociação for bem-sucedida, o e-mail será entregue por meio de uma sessão criptografada.
4. Clique em Submit.

5. Clique no botão **Commit Changes**. Você pode adicionar um comentário opcional neste momento, se desejar.

6. Clique em **Commit Changes** para salvar as alterações.

A política de fluxo de e-mail para o ouvinte agora é atualizada com as configurações de TLS que você escolheu.

Conclua estes passos para ativar o TLS para sessões de entrada que chegam de um conjunto selecionado de domínios:

1. Conecte-se à GUI da Web e escolha **Políticas de e-mail > Visão geral do HAT**.

2. Adicione o IP/FQDN do(s) remetente(s) ao grupo de remetente apropriado.

3. Edite as configurações TLS da política de fluxo de email associada ao Grupo de Remetente que você modificou na etapa anterior.

4. Clique em Submit.

5. Clique no botão **Commit Changes**. Você pode adicionar um comentário opcional neste momento, se desejar.

6. Clique em **Commit Changes** para salvar as alterações.

A política de fluxo de e-mail para o grupo de remetente agora está atualizada com as configurações de TLS escolhidas.

Dica: consulte este artigo para obter mais informações sobre como o ESA lida com a

verificação TLS : Qual é o algoritmo para a verificação de certificado no ESA?

Ativar TLS de saída

Para ativar o TLS para sessões de saída, conecte-se à GUI da Web, escolha **Políticas de e-mail > Controles de destino** e conclua estas etapas:

1. Clique em **Adicionar destino...**.

2. Adicione o domínio de destino.

3. Na seção *Suporte TLS*, clique no menu suspenso e escolha uma destas opções para habilitar o tipo de TLS a ser configurado:

   Nenhum - Quando essa opção é escolhida, o TLS não é negociado para conexões de saída da interface para o MTA do domínio.

   Preferido - Quando essa opção é escolhida, o TLS é negociado na interface ESA para o(s) MTA(s) do domínio. No entanto, se a negociação TLS falhar (antes do recebimento de uma resposta 220), a transação SMTP continuará *na limpeza* (não criptografada). Não é feita nenhuma tentativa de verificar se o certificado é originado de uma CA confiável. Se ocorrer um erro após o recebimento da resposta 220, a transação SMTP não retornará ao texto não criptografado.

   Obrigatório - Quando essa opção é escolhida, o TLS é negociado da interface ESA para o(s) MTA(s) do domínio. Não é feita nenhuma tentativa de verificar o certificado do domínio. Se a negociação falhar, nenhum e-mail será enviado por meio da conexão. Se a negociação for bem-sucedida, o e-mail será entregue por meio de uma sessão criptografada.

   Preferred-Verify - Quando esta opção é escolhida, o TLS é negociado do ESA para o(s) MTA(s) para o domínio, e o dispositivo tenta verificar o certificado do domínio. Nesse caso, esses três resultados são possíveis:

   O TLS é negociado e o certificado é verificado. O e-mail é entregue por meio de uma sessão criptografada.

   O TLS é negociado, mas o certificado não é verificado. O e-mail é entregue por meio de uma sessão criptografada.

   Nenhuma conexão TLS é feita e o certificado não é verificado. A mensagem de e-mail é entregue em texto simples.**Verificação obrigatória** - Quando essa opção é escolhida, o TLS é negociado do ESA para o(s) MTA(s) do domínio, e a verificação do certificado do domínio é necessária. Nesse caso, esses três resultados são possíveis:

   Uma conexão TLS é negociada e o certificado é verificado. A mensagem de e-mail é entregue por meio de uma sessão criptografada.

Uma conexão TLS é negociada, mas o certificado não é verificado por uma CA confiável. O e-mail não foi entregue.

Uma conexão TLS não é negociada, mas o e-mail não é entregue.

4. Faça quaisquer alterações adicionais necessárias nos *controles de destino* para o domínio de destino.

5. Clique em Submit.

6. Clique no botão **Commit Changes**. Você pode adicionar um comentário opcional neste momento, se desejar.

7. Clique em **Commit Changes** para salvar as alterações.

Sintomas de configuração incorreta do certificado ESA

O TLS funciona com um certificado autoassinado; no entanto, se a verificação do TLS for exigida pelo remetente, um certificado assinado pela CA precisará ser instalado.

A verificação TLS pode falhar mesmo que um certificado assinado por uma CA tenha sido instalado no ESA.

Nesses casos, é recomendável verificar o certificado através das etapas na seção Verificar.

Verificar

Verificar TLS com um navegador da Web

Para verificar o certificado assinado pela CA, aplique o certificado ao serviço HTTPS da GUI do ESA.

Em seguida, navegue até a GUI do seu ESA no navegador da Web. Se houver avisos quando você navegar para https://youresa, é provável que o certificado esteja encadeado incorretamente, como a ausência de um certificado intermediário.

Verificar TLS com ferramentas de terceiros

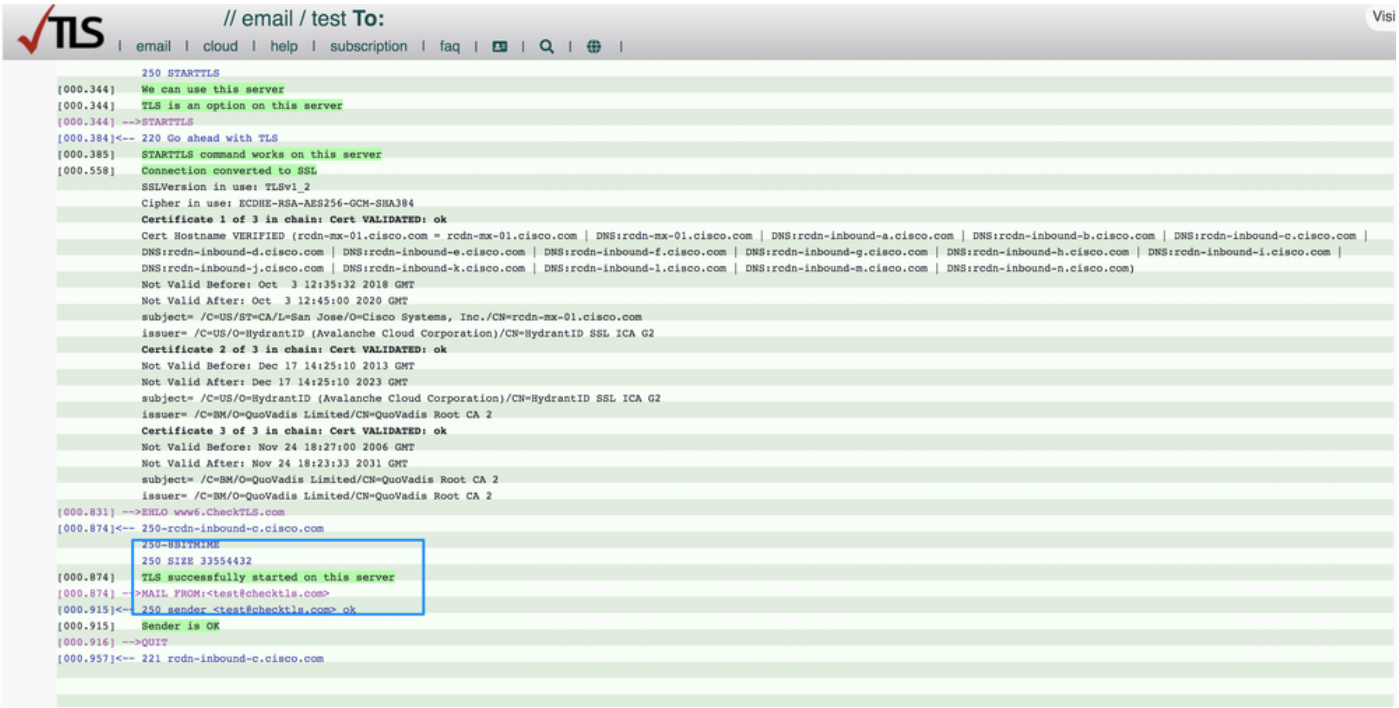
Antes do teste, certifique-se de que o certificado a ser testado seja aplicado no ouvinte em que seu equipamento recebe e-mails de entrada.

Ferramentas de terceiros, como CheckTLS.com e SSL-Tools.net podem ser usadas para verificar o encadeamento adequado do certificado.

Exemplo de saída CheckTLS.com para êxito de verificação TLS

CheckTLS Confidence Factor for "postmaster@cisco.com": 100

MX Server	Pref	Answer	Connect	HELO	TLS	Cert	Secure	From
alln-mx-01.cisco.com [173.37.147.230:25]	10	OK (41ms)	OK (422ms)	OK (50ms)	OK (48ms)	OK (450ms)	OK (58ms)	OK (41ms)
rcdn-mx-01.cisco.com [72.163.7.166:25]	20	OK (41ms)	OK (260ms)	OK (42ms)	OK (41ms)	OK (446ms)	OK (43ms)	OK (42ms)
aer-mx-01.cisco.com [173.38.212.150:25]	30	OK (80ms)	OK (484ms)	OK (81ms)	OK (79ms)	OK (548ms)	OK (80ms)	OK (81ms)
Average		100%	100%	100%	100%	100%	100%	100%



Exemplo de saída CheckTLS.com para falha de verificação de TLS

Nome de host de certificado NÃO VERIFICA (mailC.example.com != gvsvipa006.example.com)
Resolução

> **Nota:** Se um certificado autoassinado estiver em uso, o resultado esperado na coluna "Certificado OK" será "FALHA".

Se um certificado assinado por uma CA estiver em uso e a verificação TLS ainda falhar, verifique se estes itens correspondem:

- Nome comum do certificado.
- Nome do host (em GUI > Rede > Interface).
- Nome de host do registro MX: esta é a coluna Servidor MX na tabela TestReceiver.

Se um certificado assinado por uma autoridade de certificação tiver sido instalado e você vir erros, vá para a próxima seção para obter informações sobre como solucionar o problema.

Troubleshoot

Esta seção descreve como solucionar problemas básicos de TLS no ESA.

Certificados intermediários

Procure certificados intermediários duplicados, especialmente quando os certificados atuais são atualizados em vez de criar um novo certificado. O(s) certificado(s) intermediário(is) foi(ram) alterado(s) ou foi(foram) encadeado(s) incorretamente, e o certificado possivelmente carregou vários certificados intermediários. Isso pode introduzir problemas de verificação e encadeamento de certificados.

Habilitar notificações para falhas de conexão TLS necessárias

Você pode configurar o ESA para enviar um alerta se a negociação TLS falhar quando as mensagens forem entregues a um domínio que requer uma conexão TLS. A mensagem de alerta contém o nome do domínio de destino para a negociação TLS que falhou. O ESA envia a mensagem de alerta a todos os destinatários definidos para receber alertas de nível de severidade de aviso para os tipos de alerta do *sistema*.

> **Observação**: esta é uma configuração global, portanto, não pode ser definida por domínio.

Conclua estas etapas para ativar os alertas de conexão TLS:

1. Navegue até **Políticas de e-mail > Controles de destino**.
2. Clique em **Edit Global Settings**.
3. Marque a caixa de seleção **Enviar um alerta quando uma conexão TLS necessária falhar**.

   Dica: você também pode definir essa configuração com o comando CLI **destconfig > setup**.

O ESA também registra as instâncias para as quais o TLS é necessário para um domínio, mas não pode ser usado nos logs de e-mail do equipamento. Isso ocorre quando qualquer uma destas condições é atendida:

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

Localizar sessões de comunicação TLS bem-sucedidas nos logs de e-mail

As conexões TLS são registradas nos logs de e-mail, juntamente com outras ações significativas relacionadas a mensagens, como ações de filtro, vereditos de antivírus e antisspam e tentativas de entrega. Se houver uma conexão TLS bem-sucedida, haverá uma *entrada* TLS *bem-sucedida* resultante nos logs de e-mail. Da mesma forma, uma conexão TLS com falha produz uma entrada TLS *com falha*. Se uma mensagem não tiver uma entrada TLS associada no arquivo de registro, essa mensagem não foi entregue por uma conexão TLS.

> **Dica**: para compreender os logs de e-mail, consulte o documento ESA Message Disposition Determination Cisco.

Aqui está um exemplo de uma conexão TLS bem-sucedida do host remoto (recepção):

```
Tue Apr 17 00:57:53 2018 Info: New SMTP ICID 590125205 interface Data 1 (192.168.1.1) address
10.0.0.1 reverse dns host mail.example.com verified yes
Tue Apr 17 00:57:53 2018 Info: ICID 590125205 ACCEPT SG SUSPECTLIST match sbrs[-1.4:2.0] SBRS -
1.1
Tue Apr 17 00:57:54 2018 Info: ICID 590125205 TLS success protocol TLSv1 cipher DHE-RSA-AES256-
SHA
Tue Apr 17 00:57:55 2018 Info: Start MID 179701980 ICID 590125205
```

Aqui está um exemplo de falha de conexão TLS do host remoto (recepção):

```
Mon Apr 16 18:59:13 2018 Info: New SMTP ICID 590052584 interface Data 1 (192.168.1.1) address
10.0.0.1 reverse dns host mail.example.com verified yes
Mon Apr 16 18:59:13 2018 Info: ICID 590052584 ACCEPT SG UNKNOWNLIST match sbrs[2.1:10.0] SBRS
2.7
Mon Apr 16 18:59:14 2018 Info: ICID 590052584 TLS failed: (336109761, 'error:1408A0C1:SSL
routines:SSL3_GET_CLIENT_HELLO:no shared cipher')
Mon Apr 16 18:59:14 2018 Info: ICID 590052584 lost
Mon Apr 16 18:59:14 2018 Info: ICID 590052584 close
```

Aqui está um exemplo de uma conexão TLS bem-sucedida com o host remoto (entrega):

```
Tue Apr 17 00:58:02 2018 Info: New SMTP DCID 41014367 interface 192.168.1.1 address 10.0.0.1
port 25
Tue Apr 17 00:58:02 2018 Info: DCID 41014367 TLS success protocol TLSv1.2 cipher ECDHE-RSA-
AES256-GCM-SHA384
Tue Apr 17 00:58:03 2018 Info: Delivery start DCID 41014367 MID 179701982 to RID [0]
```

Aqui está um exemplo de falha de conexão TLS com o host remoto (entrega):

```
Mon Apr 16 00:01:34 2018 Info: New SMTP DCID 40986669 interface 192.168.1.1 address 10.0.0.1
port 25
Mon Apr 16 00:01:35 2018 Info: Connection Error: DCID 40986669 domain: domain IP:10.0.0.1 port:
25 details: 454-'TLS not available due to
temporary reason' interface: 192.168.1.1 reason: unexpected SMTP response
Mon Apr 16 00:01:35 2018 Info: DCID 40986669 TLS failed: STARTTLS unexpected response
```

Informações Relacionadas

- Cisco Email Security Appliance – Guias do usuário final
- Dispositivo de gerenciamento de segurança de conteúdo da Cisco - Guias do usuário final
- 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.