Configurar a versão 1.0 do Transport Layer Security no ESA e CES

Contents

Introdução

Este documento descreve como habilitar o Transport Layer Security versão 1.0 (TLSv1.0) nas alocações do Cisco Email Security Appliance (ESA) e do Cisco Cloud Email Security (CES).

Como você pode ativar o TLSv1.0 no Cisco ESA e CES?

Observação: as alocações do Cisco CES provisionadas têm o TLSv1.0 desabilitado por padrão de acordo com os requisitos de segurança devido aos impactos de vulnerabilidade no protocolo TLSv1.0. Isso inclui a sequência de codificação para remover todo o uso do conjunto de codificação compartilhada SSLv3.

Cuidado: Os métodos e as cifras SSL/TLS são definidos com base nas políticas e preferências de segurança específicas da sua empresa. Para obter informações de terceiros com relação a cifras, consulte o documento Segurança/TLS do lado do servidor Mozilla para obter configurações de servidor recomendadas e informações detalhadas.

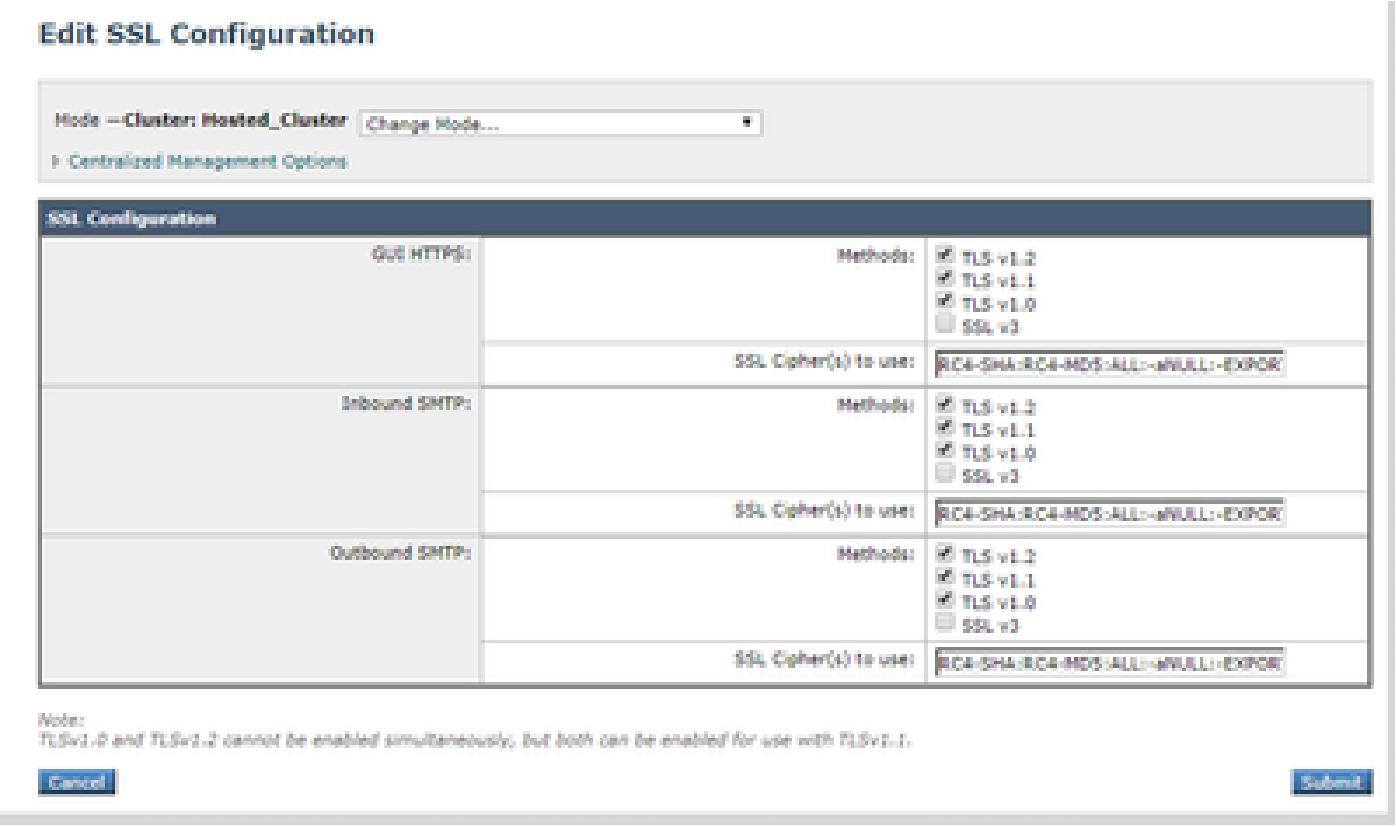
Para habilitar o TLSv1.0 no Cisco ESA ou CES, você pode fazer isso na Interface gráfica do usuário (GUI) ou na interface de linha de comando (CLI).

Observação: para obter acesso ao CES na CLI, revise: Acessando a interface de linha de comando (CLI) da solução Cloud Email Security (CES)

Interface gráfica do usuário

1. Faça login na GUI.
2. Navegue até System Administration > SSL Configuration.
3. Selecione Edit Settings.

4. Marque a caixa TLSv1.0. É importante observar que o TLSv1.2 e o não podem ser ativados em conjunto com o TLSv1.0, a menos que o protocolo de Bridging TLSv1.1 também esteja ativado, como mostrado na imagem:



Interface da linha de comando

1. Execute o comando sslconfig.
2. Execute o comando GUI ou INBOUND ou OUTBOUND, dependendo do item para o qual você deseja habilitar o TLSv1.0:

```
<#root>

(Cluster Hosted_Cluster)>

sslconfig


sslconfig settings:

GUI HTTPS method: tlsv1_2


GUI HTTPS ciphers:
RC4-SHA
RC4-MD5
ALL
-aNULL
-EXPORT

Inbound SMTP method: tlsv1_2
```

```
Inbound SMTP ciphers:
RC4-SHA
RC4-MD5
ALL
-aNULL
-EXPORT

Outbound SMTP method: tlsv1_2


Outbound SMTP ciphers:
RC4-SHA
RC4-MD5
ALL
-aNULL
-EXPORT

Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
- CLUSTERSET - Set how ssl settings are configured in a cluster.
- CLUSTERSHOW - Display how ssl settings are configured in a cluster.

[]> INBOUND



Enter the inbound SMTP ssl method you want to use.

1. TLS v1.0



2. TLS v1.1



3. TLS v1.2


4. SSL v2
5. SSL v3

[3]> 1-3



Enter the inbound SMTP ssl cipher you want to use.
[RC4-SHA:RC4-MD5:ALL:-aNULL:-EXPORT]>
```

Cifras

As alocações de ESAs e CES podem ser configuradas com conjuntos de cifras estritos. É importante garantir que as cifras SSLv3 não sejam bloqueadas quando você ativar o protocolo TLSv1.0. A falha em permitir pacotes de cifras SSLv3 resulta em falhas de negociação de TLS ou fechamentos de conexão TLS abruptos.

Exemplo de cifra:

<#root>

```
HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!DES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA:!ADH:!IDEA:!3D
```

!SSLv3:!TLSv1

```
:-aNULL:-EXPORT:-IDEA
```

Essa string de cifra impede que o ESA/CES permita a negociação em cifras SSLv3 conforme indicado em !SSLv3:, isso significa que quando o protocolo é solicitado no handshake, o handshake SSL falha, pois não há cifras compartilhadas disponíveis para negociação.

Para garantir que a cadeia de caracteres de cifra de exemplo funcione com TLSv1.0, ela precisa ser modificada para remover !SSLv3:!TLSv1: visto na cadeia de caracteres de cifra substituída:

```
HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!DES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA:!ADH:!IDEA:!3D
```

Observação: você pode verificar os conjuntos de cifras compartilhados no handshake SSL na CLI do ESA/CES com o comando VERIFY.

Possíveis erros registrados em mail_logs/Message Tracking, mas não limitados a:

```
Sun Feb 23 10:07:07 2020 Info: DCID 1407038 TLS failed: (336032784, 'error:14077410:SSL routines:SSL23_
Sun Feb 23 10:38:56 2020 Info: DCID 1407763 TLS failed: (336032002, 'error:14077102:SSL routines:SSL23_
```

Informações Relacionadas

- Alterar os métodos e as cifras usados com SSL/TLS no ESA
- Detalhes da Força da Cifra SSL
- Guia de configuração abrangente para TLS no ESA
- 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.