配置在Cisco ESA和CES的传输层安全版本1.0

目录

简介

本文描述如何启用在Cisco电子邮件安全工具(ESA)和Cisco Cloud电子邮件安全(CES)分配的传输层安全版本1.0 (TLSv1.0)。

如何能启用在Cisco ESA和CES的TLSv1.0 ？

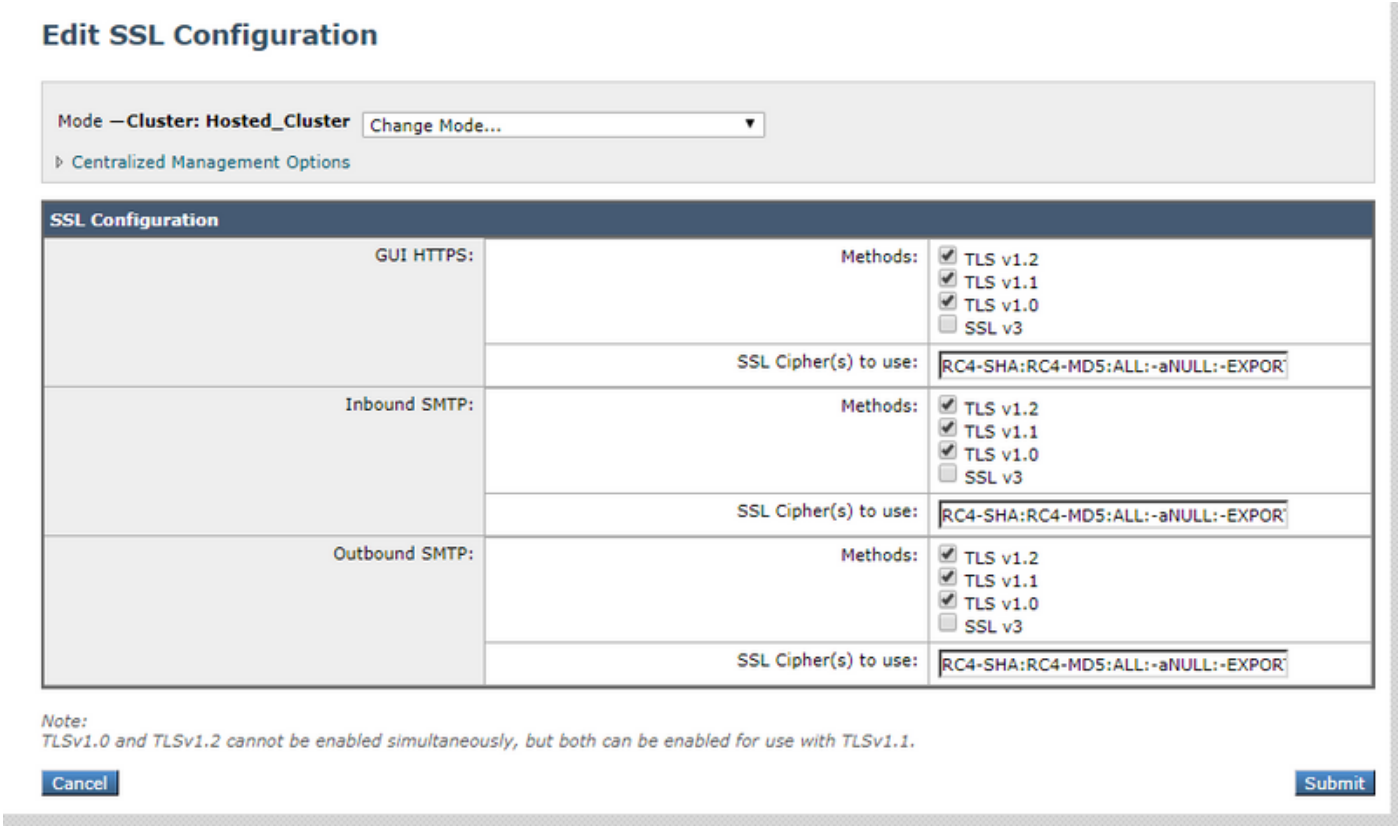
> **Note**:设置的默认情况下Cisco CES分配有根据安全需求禁用的TLSv1.0由于在TLSv1.0协议的漏洞影响。这包括密码器字符串删除SSLv3共享的密码器套件的各种用法。
>
> **警告：**根据您的公司特定安全策略和首选和密码器集合的SSL/TLS方法。 关于密码器的第三方信息，参考安全/服务器端TLS Mozilla文档推荐的服务器配置和详细信息。

为了启用在您的Cisco ESA或CES的TLSv1.0，您能从图形用户界面(GUI)或命令行界面(CLI)如此执行。

> **Note**:为了获得对您的CES的访问在CLI请查看： **访问您的Cloud电子邮件安全(CES)解决方案命令行界面(CLI)**

图形用户界面

1. 登录GUI。
2. 导航对**系统管理> SSL配置**。
3. 选择**编辑设置**。
4. 检查**TLSv1.0**方框。请注意TLSv1.2，并且不可能与TLSv1.0一道启用如镜像所显示，除非桥接协议TLSv1.1也启用：



命令行界面

1. 运行命令**sslconfig**。
2. 运行命令**GUI**或**入站**或**出站**根据哪个项目的您要启用TLSv1.0 ：

```
(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]>
```

密码器

当您启用TLSv1.0协议时， ESAs和CES分配可以配置与严格密码器套件，它是重要保证SSLv3密码器没有阻塞。疏忽允许SSLv3密码器套件导致TLS协商失败或突然的TLS连接关闭。

示例密码器字符串：

```
HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!DES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA:!ADH:!I
DEA:!3DES:!SSLv2:!SSLv3:!TLSv1:-aNULL:-EXPORT:-IDEA
```

此密码器字符串从允许在SSLv3密码器的协商终止ESA/CES如指示**! SSLv3** ：这含义，当协议在握手时请求， SSL握手发生故障，尽管没有共享密码器可用为协商。

为了保证与TLSv1.0的示例密码器字符串功能，需要修改它删除**! SSLv3:!TLSv1** ： 看到在被替换的密码器字符串：

```
HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!DES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA:!ADH:!I
DEA:!3DES:!SSLv2:-aNULL:-EXPORT:-IDEA
```

> **Note**:您能验证在ESA/CES CLI的SSL握手共享的密码器套件用**verify命令**。

可能的错误登陆mail_logs/消息跟踪，但是没限制对：

```
Sun Feb 23 10:07:07 2020 Info: DCID 1407038 TLS failed: (336032784, 'error:14077410:SSL
routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure')
Sun Feb 23 10:38:56 2020 Info: DCID 1407763 TLS failed: (336032002, 'error:14077102:SSL
routines:SSL23_GET_SERVER_HELLO:unsupported protocol')
```

相关信息

- 修改方法和密码器与在ESA的SSL/TLS一起使用
- SSL加密优点详细信息
- TLS的全面的设置指南在ESA
- 技术支持和文档 - Cisco Systems