Cisco ESA 및 CES에서 Transport Layer Security 버전 1.0 구성

목차

소개

이 문서에서는 Cisco ESA(Email Security Appliance) 및 Cisco CES(Cloud Email Security) 할당에서 TLSv1.0(Transport Layer Security version 1.0)을 활성화하는 방법에 대해 설명합니다.

Cisco ESA 및 CES에서 TLSv1.0을 활성화하려면 어떻게 해야 합니까?

> **참고:**프로비저닝된 Cisco CES 할당에는 TLSv1.0 프로토콜에 대한 취약성 영향 때문에 보안 요구 사항에 따라 기본적으로 TLSv1.0이 비활성화되어 있습니다.여기에는 SSLv3 공유 암호 그룹의 모든 사용을 제거하는 암호화 문자열이 포함됩니다.

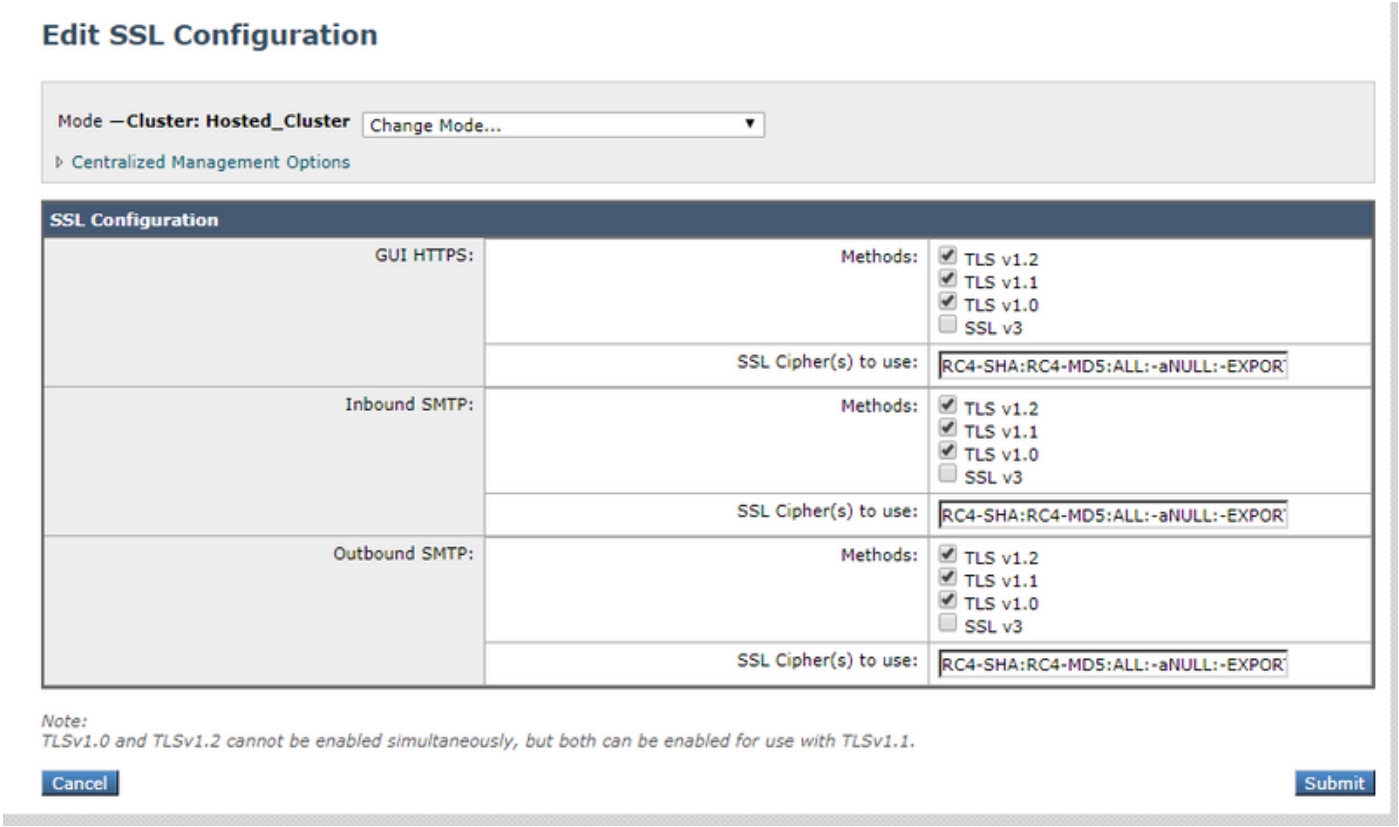
> **주의:**SSL/TLS 방법 및 암호는 회사의 특정 보안 정책 및 환경 설정에 따라 설정됩니다. 암호화에 대한 서드파티 정보는 권장 서버 구성 및 자세한 정보를 보려면 Security/Server Side TLS Mozilla 문서를 참조하십시오.

Cisco ESA 또는 CES에서 TLSv1.0을 활성화하려면 GUI(Graphical User Interface) 또는 CLI(Command Line Interface)에서 활성화할 수 있습니다.

> **참고:**CLI에서 CES에 액세스하려면 다음을 검토하십시오. Access the Command Line Interface (CLI) of Your Cloud Email Security (CES) Solution

그래픽 사용자 인터페이스

1. GUI에 로그인합니다.
2. System Administration(**시스템 관리) > SSL Configuration(SSL 컨피그레이션)으로 이동합니다**.
3. Edit **Settings를 선택합니다**.
4. TLSv**1.0** 상자를 선택합니다.이미지에 표시된 대로 브리징 프로토콜 TLSv1.1을 활성화하지 않으면 TLSv1.2를 TLSv1.0과 함께 활성화할 수 없다는 점에 유의해야 합니다.



명령줄 인터페이스

1. sslconfig 명령을 **실행합니다**.
2. TLSv1.0을 활성화할 항목에 따라 명령 **GUI** 또는 INBOUND 또**는 OUTBOUND**를 실행합니다.

```
(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]>
```

암호

ESA 및 CES 할당은 엄격한 암호 그룹으로 구성할 수 있으며, TLSv1.0 프로토콜을 활성화할 때 SSLv3 암호가 차단되지 않도록 하는 것이 중요합니다.SSLv3 암호 그룹을 허용하지 않으면 TLS 협상 실패 또는 갑작스러운 TLS 연결 닫기가 발생합니다.

샘플 암호 문자열:

```
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
```

이 암호 문자열은 ESA/CES가 SSLv3 암호에서 SSLv3 암호**에** 대한 협상을 허용하지 않도록 합니다. 즉, 핸드셰이크에서 프로토콜이 요청되면 협상에 사용할 수 있는 공유 암호가 없으므로 SSL 핸드셰이크가 실패합니다.

샘플 암호 문자열 함수가 TLSv1.0과 함께 작동하도록 하려면 교체된 암호 문자열에서 발견된 **!SSLv3:!TLSv1:**을 제거하도록 수정해야 합니다.

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

> **참고:**VERIFY 명령을 사용하여 ESA/CES CLI에서 SSL 핸드셰이크에서 공유된 암호 그룹을 확인할 수 **있습니다**.

mail_logs/Message Tracking(메일 로그/메시지 추적)에 기록될 수 있는 오류(이에 제한되지 않음):

```
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')
```

관련 정보

- [ESA에서 SSL/TLS와 함께 사용되는 방법 및 암호 변경]
- [SSL 암호 강도 세부 정보]
- [ESA에서 TLS를 위한 포괄적인 설정 가이드]
- [기술 지원 및 문서 – Cisco Systems]