

Secure Email Web Manager용 TLSv1.3 구성

목차

소개

이 문서에서는 Cisco EWM(Secure Email and Web Manager)을 위한 TLS v1.3 프로토콜의 컨피그레이션에 대해 설명합니다.

사전 요구 사항

SEWM 설정 및 구성에 대한 일반적인 지식이 필요합니다.

사용되는 구성 요소

- Cisco SEWM(Secure Email Web Manager) AsyncOS 15.5.1 이상
- SSL 구성 설정.

"이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 가동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다."

개요

SEWM에는 HTTPS 관련 서비스(클래식 UI, NGUI 및 Rest API)에 대한 통신을 암호화하기 위해 통합된 TLS v1.3 프로토콜이 있습니다.

TLS v1.3 프로토콜은 업계 표준으로 만들기 위해 노력하고 있기 때문에 더욱 안전한 커뮤니케이션과 더 빠른 협상을 자랑한다.

SEWM은 SSL의 SEGWebUIor CLI 내에서 기존 SSL 컨피그레이션 방법을 사용하며 몇 가지 주목할 만한 설정을 강조 표시합니다.

- 허용되는 프로토콜을 구성할 때 사전 예방 권고
- TLS v1.3 암호는 조작할 수 없습니다.
- TLS v1.3은 GUI HTTPS에만 구성할 수 있습니다.
- TLS v1.0과 TLS v1.3 간의 TLS 프로토콜 확인란 선택 옵션은 기사 내에 자세히 나와 있는 패턴을 사용합니다.

구성

SEWM은 AsyncOS 15.5 내에서 HTTPS용 TLS v1.3 프로토콜을 통합했습니다.

HTTPS 오류를 방지하기 위해 프로토콜 설정을 선택할 때는 주의하는 것이 좋습니다.

TLS v1.3에 대한 웹 브라우저 지원은 일반적이지만 일부 환경에서는 SEWM에 액세스하기 위해 조정이 필요합니다.

TLS v1.3 프로토콜의 Cisco SEWM 구현은 SEWM 내에서 변경하거나 제외할 수 없는 3개의 기본 암호를 지원합니다.

TLS 1.3 암호:

TLS_AES_256_GCM_SHA384

TLS_CHACHA20_POLY1305_SHA256

TLS_AES_128_GCM_SHA256

WebUI에서 컨피그레이션

> System Administration > SSL Configuration으로 이동합니다.

- 15.5 AsyncOS HTTPS로 업그레이드한 후 기본 TLS 프로토콜 선택 사항에는 TLS v1.1 및 TLS v1.2만 포함됩니다.
- 나열된 두 가지 추가 서비스인 Secure LDAP Services(보안 LDAP 서비스) 및 Updater Services(업데이터 서비스)는 TLS v1.3을 지원하지 않습니다.

SSL Configuration

SSL Configuration	
Appliance Management Web User Interface:	Enable protocol versions: TLS v1.2 TLS v1.1
Secure LDAP Services:	Enable protocol versions: TLS v1.2 TLS v1.1
Updater Service:	Enable protocol versions: TLS v1.2 TLS v1.1
Peer Certificate FQDN Validation:	Used for Alert Over TLS, Updater and LDAP: Disabled
Peer Certificate X509 Validation:	Used for Alert Over TLS, Updater and LDAP: Disabled

[Edit Settings](#)


"설정 편집"을 선택하여 구성 옵션을 표시합니다.

"웹 사용자 인터페이스"에 대한 TLS 프로토콜 선택 옵션에는 TLS v1.0, TLS v1.1, TLS v1.2 및 TLS v1.3이 포함됩니다.

- AsyncOS 15.5로 업그레이드 후, 기본적으로 TLS v1.1 및 TLS v1.2 프로토콜만 선택됩니다.

SSL Configuration	
<p>Disabling SSLv3 for all services is recommended for best security. Depending on your network requirements, you may also choose to disable some versions of TLS for specific services.</p> <p>Note that the SSL/TLS service on remote servers may require that the selected TLS versions be sequential. So to avoid communications errors, always select a contiguous set of versions for each service. For example, do not enable TLS 1.0 and 1.2, while leaving TLS 1.1 disabled.</p> <p>For the peer certificate FQDN validation for LDAP, ensure that you enable LDAP server certificate validation in LDAP Global Settings.</p>	
Appliance Management Web User Interface:	<p>Changing this option will disconnect all active Web User Interface connections on Commit. You will need to log in again.</p> <p>Enable protocol versions:</p> <p><input type="checkbox"/> TLS v1.3 ←</p> <p><input checked="" type="checkbox"/> TLS v1.2</p> <p><input checked="" type="checkbox"/> TLS v1.1</p> <p><input type="checkbox"/> TLS v1.0</p>
Secure LDAP Services:	<p>Secure LDAP services include Authentication and External Authentication.</p> <p>Enable protocol versions:</p> <p><input checked="" type="checkbox"/> TLS v1.2</p> <p><input checked="" type="checkbox"/> TLS v1.1</p> <p><input type="checkbox"/> TLS v1.0</p>
Updater Service:	<p>Enable protocol versions:</p> <p><input checked="" type="checkbox"/> TLS v1.2</p> <p><input checked="" type="checkbox"/> TLS v1.1</p> <p><input type="checkbox"/> TLS v1.0</p>
Peer Certificate FQDN Validation:	<p>Used for Alert Over TLS, Updater and LDAP:</p> <p><input type="checkbox"/> Enable</p>
Peer Certificate X509 Validation:	<p>Used for Alert Over TLS, Updater and LDAP:</p> <p><input type="checkbox"/> Enable</p>


Cancel Submit

 참고: TLS1.0은 더 이상 사용되지 않으므로 기본적으로 비활성화되어 있습니다. 소유자가 TLS v1.0을 활성화하도록 선택하면 TLS v1.0을 계속 사용할 수 있습니다.

- 확인란 옵션에는 사용 가능한 프로토콜이 표시된 굵게 표시된 상자와 호환되지 않는 옵션에 대한 회색으로 표시된 상자가 표시됩니다.
- 이 그림의 샘플 옵션은 웹 사용자 인터페이스의 확인란 옵션을 보여 줍니다.

<input type="checkbox"/> TLS v1.3	<input type="checkbox"/> TLS v1.3	<input type="checkbox"/> TLS v1.3	<input type="checkbox"/> TLS v1.3
<input checked="" type="checkbox"/> TLS v1.2	<input checked="" type="checkbox"/> TLS v1.2	<input type="checkbox"/> TLS v1.2	<input type="checkbox"/> TLS v1.2
<input checked="" type="checkbox"/> TLS v1.1	<input type="checkbox"/> TLS v1.1	<input checked="" type="checkbox"/> TLS v1.1	<input type="checkbox"/> TLS v1.1
<input type="checkbox"/> TLS v1.0	<input type="checkbox"/> TLS v1.0	<input type="checkbox"/> TLS v1.0	<input type="checkbox"/> TLS v1.0

<input checked="" type="checkbox"/> TLS v1.3	<input type="checkbox"/> TLS v1.3	<input checked="" type="checkbox"/> TLS v1.3
<input checked="" type="checkbox"/> TLS v1.2	<input type="checkbox"/> TLS v1.2	<input type="checkbox"/> TLS v1.2
<input checked="" type="checkbox"/> TLS v1.1	<input type="checkbox"/> TLS v1.1	<input type="checkbox"/> TLS v1.1
<input type="checkbox"/> TLS v1.0	<input checked="" type="checkbox"/> TLS v1.0	<input type="checkbox"/> TLS v1.0

 참고: SSL 구성을 수정하면 관련 서비스가 다시 시작될 수 있습니다. 그러면 WebUI 서비스가 잠시 중단됩니다.

SSL Configuration

Attention — ⚠ Your settings have been saved. After you commit your changes, the settings of the SSL Configuration can cause all related services to restart. This leads to interruption in the services.

SSL Configuration	
Appliance Management Web User Interface:	Enable protocol versions: TLS v1.3 ←
Secure LDAP Services:	Enable protocol versions: TLS v1.2 TLS v1.1
Updater Service:	Enable protocol versions: TLS v1.2 TLS v1.1
Peer Certificate FQDN Validation:	Used for Alert Over TLS, Updater and LDAP: Disabled
Peer Certificate X509 Validation:	Used for Alert Over TLS, Updater and LDAP: Disabled

[Edit Settings](#)

CLI에서 컨피그레이션

EWM은 하나의 서비스, 즉 WebUI에서 TLS v1.3을 허용합니다.

```
sma1.example.com> sslconfig
```

최상의 보안을 위해서는 SSLv3을 비활성화하는 것이 좋습니다.

원격 서버의 SSL/TLS 서비스에서는 선택한 TLS 버전이 순차적이어야 합니다. 통신 오류를 방지하려면 항상 연속 항목을 선택하십시오.

각 서비스의 버전 집합입니다. 예를 들어, TLS 1.1을 비활성화한 상태에서 TLS 1.0 및 1.2를 활성화하지 마십시오.

수행할 작업을 선택합니다.

- 버전 - SSL/TLS 버전 활성화 또는 비활성화

- PEER_CERT_FQDN - TLS, 업데이터 및 LDAP를 통한 경고에 대해 피어 인증서 FQDN 규정 준수를 확인합니다.

- PEER_CERT_X509 - Alert Over TLS, updater and LDAP에 대한 피어 인증서 X509 준수 여부를 확인합니다.

[]> 버전

서비스에 대해 SSL/TLS 버전을 활성화하거나 비활성화합니다.

업데이터 - 업데이트 서비스

WebUI - 어플라이언스 관리 웹 사용자 인터페이스

LDAP - 보안 LDAP 서비스(인증 및 외부 인증 포함)

TLSv1.3은 업데이터 및 LDAPS에 사용할 수 없으며 WebUI만 TLSv1.3으로 구성할 수 있습니다.

서비스별로 현재 활성화된 SSL/TLS 버전: (Y: 활성화됨, N: 비활성화됨)

업데이터 WebUI LDAPS

TLSv1.0 해당 사항 없음
TLSv1.1 Y N Y
TLSv1.2 전년 대비
TLSv1.3 해당 사항 없음 해당 사항 없음

SSL/TLS 버전을 활성화/비활성화할 서비스를 선택합니다.

1. 업데이터
2. WebUI
3. LDAPS
4. 모든 서비스

[]> 2

현재 WebUI에 대해 활성화된 프로토콜은 TLSv1.2입니다.

특정 프로토콜에 대한 설정을 변경하려면 아래 옵션을 선택하십시오.

1. TLSv1.0
2. TLSv1.1
3. TLSv1.2
4. TLSv1.3

[]> 4

어플라이언스 관리 웹 사용자 인터페이스에 대한 TLSv1.3 지원을 현재 사용할 수 없습니다. 활성화 하시겠습니까? [N]> y

현재 WebUI에 대해 활성화된 프로토콜은 TLSv1.3, TLSv1.2입니다.

수행할 작업을 선택합니다.

- 버전 - SSL/TLS 버전 활성화 또는 비활성화
- PEER_CERT_FQDN - TLS, 업데이터 및 LDAP를 통한 경고에 대해 피어 인증서 FQDN 규정 준수를 확인합니다.
- PEER_CERT_X509 - Alert Over TLS, updater 및 LDAP에 대한 피어 인증서 X509 준수 여부를 확인합니다.

[]>

sma1.example.com> 커밋

경고: SSL 컨피그레이션을 변경하면 이러한 프로세스는 커밋 후 다시 시작됩니다(gui, euq_webui). 이로 인해 SMA 작업이 잠시 중단됩니다.

변경 사항을 설명하는 몇 가지 의견을 입력하십시오.

[]> tls v1.3 사용

커밋된 변경 사항: Sun 28 23:55:40 2024 EST


gui를 다시 시작하는 중...

gui 재시작됨

euq_webui 다시 시작 중...

euq_webui 다시 시작됨

잠시 기다린 후 WebUI에 액세스할 수 있는지 확인합니다.

 참고: 서비스에 대해 여러 버전의 TLS를 선택하려면 사용자가 서비스 및 프로토콜 버전을 선택한 다음 모든 설정이 수정될 때까지 서비스 및 프로토콜 선택을 한 번 더 반복해야 합니다.

다음을 확인합니다.

이 섹션에는 몇 가지 기본 테스트 시나리오와 일치하지 않는 버전 또는 구문 오류로 인해 발생하는 오류가 포함되어 있습니다.

TLSv1.3으로 구성된 EWM WebUI 또는 NGUI에 대한 웹 브라우저 세션을 열어 브라우저 기능을 확인합니다.

테스트한 모든 웹 브라우저는 TLS v1.3을 허용하도록 이미 구성되어 있습니다.

- 샘플 TLS v1.3 지원을 비활성화하도록 Firefox에서 브라우저 설정을 설정하면 어플라이언스의 ClassicUI 및 NGUI 모두에서 오류가 발생합니다.
- TLS v1.3을 테스트로 제외하도록 구성된 Firefox를 사용하는 클래식 UI.
- NGUI에서는 URL 내의 포트 번호 4431(기본값)을 제외하고 동일한 오류가 발생합니다.

Secure Connection Failed

An error occurred during a connection to dh6219-sma1.iphmx.com. Peer reports incompatible or unsupported protocol version.

Error code: SSL_ERROR_PROTOCOL_VERSION_ALERT

- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem.

This website might not support the TLS 1.2 protocol, which is the minimum version supported by Firefox.

[Learn more...](#)

It looks like your network security settings might be causing this. Do you want the default settings to be restored?

TLS v1.3 Webui 실패

- 통신을 확인하려면 TLSv1.3이 포함되도록 브라우저 설정을 확인하십시오. (이 샘플은 Firefox에서 가져온 것입니다.)

security.tls.version.fallback-limit	4	
security.tls.version.max	4	
security.tls.version.min	1	

- 잘못된 암호 값을 사용하는 샘플 openssl 명령은 다음과 같은 오류 출력을 제공합니다. 샘플 openssl 연결 테스트 실패는 잘못된 암호로 인해 발생합니다. Error with command: "-ciphersuites TLS_AES_256_GCM_SHA386"

2226823168:ERROR:1426E089:SSL 루틴:ciphersuite_cb:암호 일치 없음:ssl/ssl_ciph.c:1299:

- TLS v1.3이 비활성화될 때 ng-ui에 실행된 샘플 curl 명령은 이 오류를 생성합니다.

curl: (35) CURL_SSLVERSION_MAX가 CURL_SSLVERSION과 호환되지 않습니다.

관련 정보

- [Cisco Content Security Management Appliance - 릴리스 정보](#)
- [Cisco Content Security Management Appliance - 최종 사용자 가이드](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.