Secure Email Gateway에 대한 TLSv1.3 구성

목차

소개

이 문서에서는 Cisco SEG(Secure Email Gateway)를 위한 TLS v1.3 프로토콜의 컨피그레이션에 대해 설명합니다.

사전 요구 사항

SEG 설정 및 구성에 대한 일반적인 지식이 필요합니다.

사용되는 구성 요소

- 이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.
  - Cisco SEG(Secure Email Gateway) AsyncOS 15.5.1 이상
- SEG 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

SEG는 SMTP 및 HTTPS 관련 서비스(Classic UI, NGUI 및 Rest API)에 대한 통신을 암호화하기 위해 TLS v1.3 프로토콜을 통합했습니다.

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

SEG는 SSL의 SEG WebUI 또는 CLI 내에서 기존 SSL 컨피그레이션 방법을 사용하며 몇 가지 주목할 만한 설정을 강조 표시합니다.

- 허용되는 프로토콜을 구성할 때 사전 예방 권고
- 암호는 조작할 수 없습니다.
- TLS v1.3은 GUI HTTPS, 인바운드 메일 및 아웃바운드 메일에 대해 구성할 수 있습니다.
- TLS v1.0에서 TLS v1.3 사이의 TLS 프로토콜 확인란 선택 옵션은 기사 내에 자세히 나와 있는 패턴을 사용합니다.

구성

SEG는 AsycOS 15.5 내에서 HTTPS 및 SMTP에 대한 TLS v1.3 프로토콜을 통합합니다. HTTPS 및 이메일 전송/수신 오류를 방지하기 위해 프로토콜 설정을 선택할 때는 주의하는 것이 좋습니다.

Cisco SEG의 이전 릴리스는 TLS v1.2를 지원하는 MS O365와 같은 다른 이메일 제공업체와 함께 하이엔드에서 TLS v1.2를 지원합니다.

TLS v1.3 프로토콜의 Cisco SEG 구현은 다른 프로토콜이 허용하는 대로 SEG 암호 컨피그레이션 설정 내에서 변경하거나 제외할 수 없는 3개의 기본 암호를 지원합니다.

기존 SEG SSL 컨피그레이션 설정에서는 암호 그룹에 대한 TLS v1.0, v1.1, v1.2 조작을 계속 조작할 수 있습니다.

TLS 1.3 암호:

TLS_AES_256_GCM_SHA384

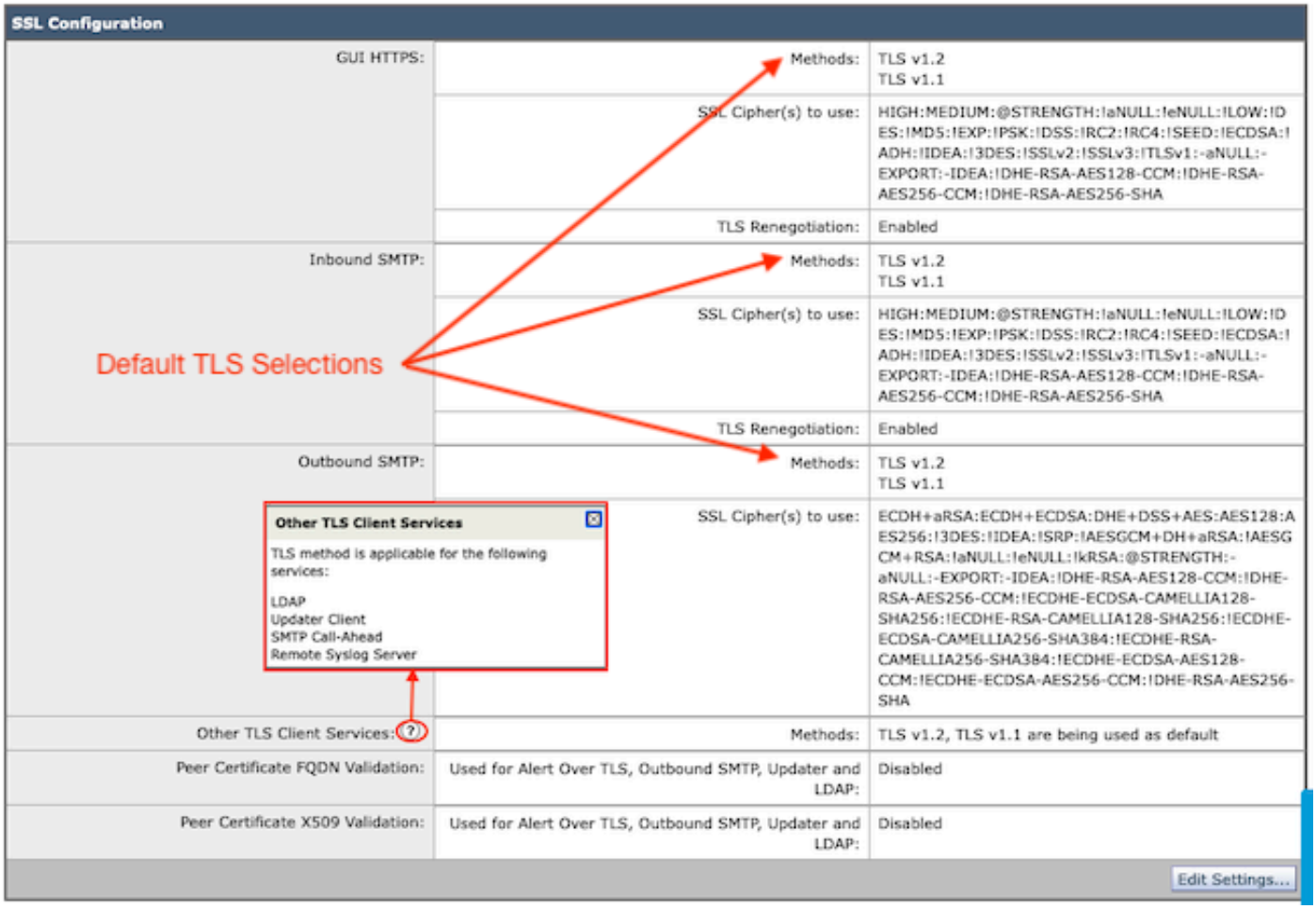
TLS_CHACHA20_POLY1305_SHA256

TLS_AES_128_GCM_SHA256

WebUI에서 컨피그레이션

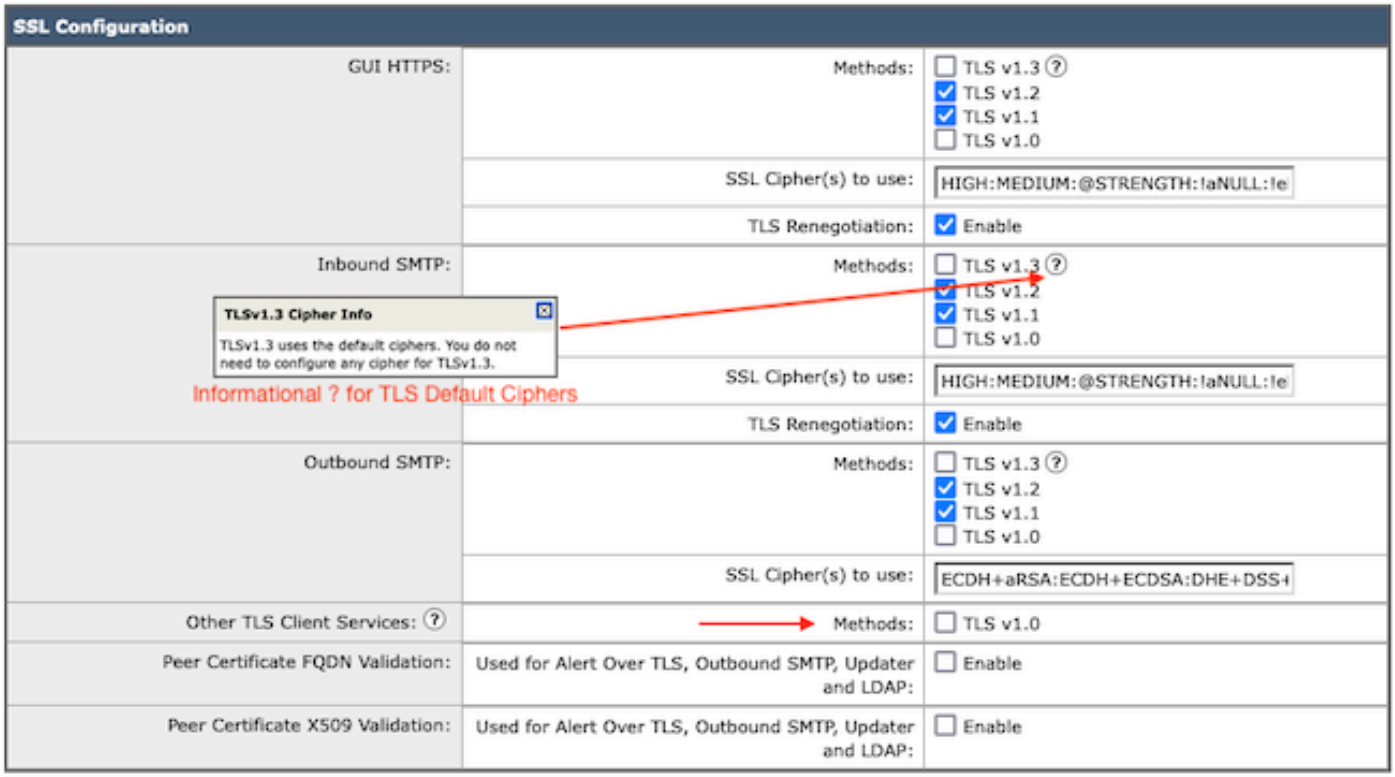
> System Administration > SSL Configuration으로 이동합니다.

- 15.5 AsyncOS로 업그레이드한 후 기본 TLS 프로토콜 선택 항목에는 TLS v1.1 및 TLS v1.2만 포함됩니다.
- "기타 TLS 클라이언트 서비스"에 대한 설정은 TLS v1.1 및 TLS v1.2를 사용하며, TLS v1.0만 사용합니다.



"설정 편집"을 선택하여 구성 옵션을 표시합니다.

- TLS v1.1 및 TLS v1.2는 다른 프로토콜을 선택하기 위해 활성 상자에 체크되어 있습니다.
- 각 TLS v1.3 옆에 있는 ?는 고정 암호 옵션의 반복입니다.
- 이제 "기타 TLS 클라이언트 서비스:"에서는 선택한 경우에만 TLS v1.0을 활용할 수 있는 옵션을 제공합니다.



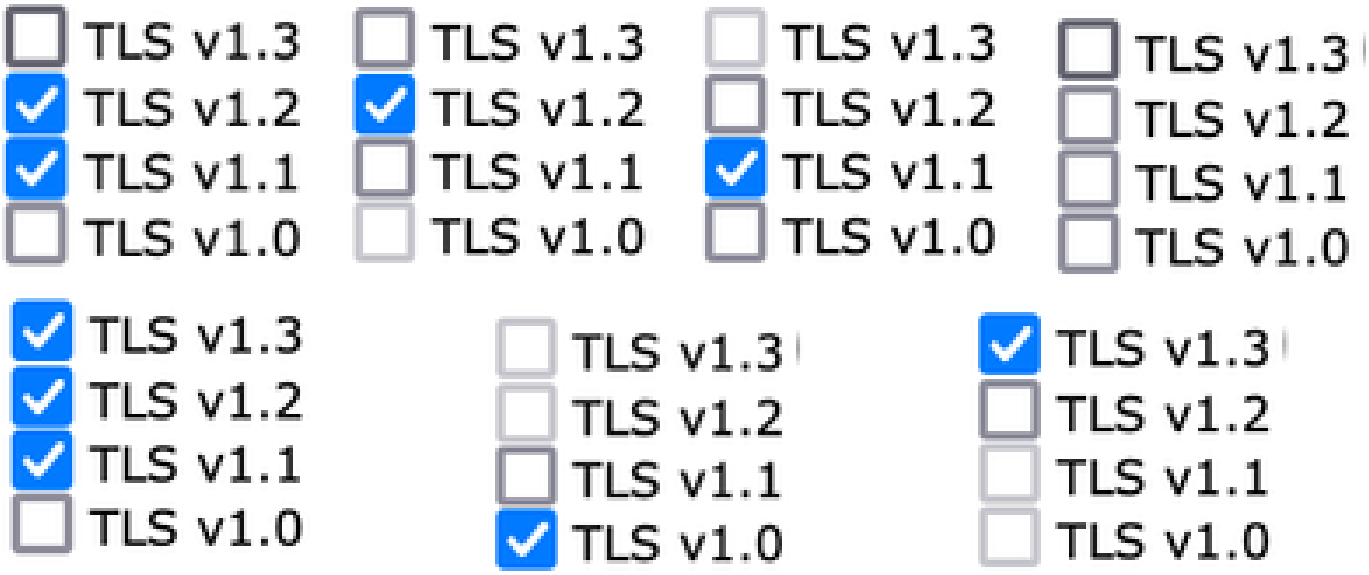
Note:
TLS protocols can be enabled only in sequence.
The configured SSL Cipher(s) do not apply to TLS 1.3. The TLS 1.3 protocol uses default ciphers.

TLS 프로토콜 선택 옵션에는 TLS v1.0, TLS v1.1, TLS v1.2, TLS v1.3이 포함됩니다.

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

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 옵션에는 확인란 옵션이 나와 있습니다.



선택한 TLS 프로토콜의 사후 커밋 샘플 보기

SSL Configuration		
GUI HTTPS:	Methods:	TLS v1.3 TLS v1.2
	SSL Cipher(s) to use:	HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!DES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA:!ADH:!IDEA:!3DES:!SSLv2:!SSLv3:!TLSv1:-aNULL:-EXPORT:-IDEA:!DHE-RSA-AES256-SHA:!DHE-RSA-AES128-CCM:!DHE-RSA-AES256-CCM
	TLS Renegotiation:	Enabled
Inbound SMTP:	Methods:	TLS v1.3 TLS v1.2 TLS v1.1 TLS v1.0
	SSL Cipher(s) to use:	HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!DES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA:!ADH:!IDEA:!3DES:!SSLv2:!SSLv3:!TLSv1:-aNULL:-EXPORT:-IDEA:!DHE-RSA-AES256-SHA:!DHE-RSA-AES128-CCM:!DHE-RSA-AES256-CCM
	TLS Renegotiation:	Enabled
Outbound SMTP:	Methods:	TLS v1.3 TLS v1.2 TLS v1.1
	SSL Cipher(s) to use:	HIGH:MEDIUM:@STRENGTH:!aNULL:!eNULL:!LOW:!DES:!MD5:!EXP:!PSK:!DSS:!RC2:!RC4:!SEED:!ECDSA:!ADH:!IDEA:!3DES:!SSLv2:!SSLv3:!TLSv1:-aNULL:-EXPORT:-IDEA:!DHE-RSA-AES256-SHA:!DHE-RSA-AES128-CCM:!DHE-RSA-AES256-CCM:!ECDHE-ECDSA-CAMELLIA128-SHA256:!ECDHE-RSA-CAMELLIA128-SHA256:!ECDHE-ECDSA-CAMELLIA256-SHA384:!ECDHE-RSA-CAMELLIA256-SHA384:!ECDHE-ECDSA-AES128-CCM:!ECDHE-ECDSA-AES256-CCM
Other TLS Client Services:	Methods:	TLS v1.2, TLS v1.1 are being used as default
Peer Certificate FQDN Validation:	Used for Alert Over TLS, Outbound SMTP, Updater and LDAP:	Disabled
Peer Certificate X509 Validation:	Used for Alert Over TLS, Outbound SMTP, Updater and LDAP:	Disabled
		Edit Settings...

참고: GUI HTTPS TLS 프로토콜을 수정하면 https 서비스 재설정으로 인해 WebUI의 연결이 잠시 끊깁니다.

CLI 구성:

SEG는 TLS v1.3 on 3 서비스를 허용합니다.

- GUI HTTPS
- 인바운드 SMTP
- 아웃바운드 SMTP

명령 > sslconfig를 실행하면 GUI HTTPS, Inbound SMTP, Outbound SMTP에 대해 현재 구성된 프로토콜 및 암호가 출력됩니다

- GUI HTTPS 방법: tlsv1_0tlsv1_1tlsv1_2tlsv1_3
- 인바운드 SMTP 방법: tlsv1_0tlsv1_1tlsv1_2tlsv1_3
- 아웃바운드 SMTP 방법: tlsv1_1tlsv1_2tlsv1_3

수행할 작업을 선택합니다.

- GUI - GUI HTTPS ssl 설정을 편집합니다.
- INBOUND - 인바운드 SMTP SSL 설정을 편집합니다.
- OUTBOUND(아웃바운드) - 아웃바운드 SMTP ssl 설정을 편집합니다.

[]> 인바운드

사용할 인바운드 SMTP SSL 방법을 입력합니다.

1. TLS v1.3
2. TLS v1.2
3. TLS v1.1
4. TLS v1.0

[2-4]> 1-3

주: SEG 선택 프로세스는 2와 같은 단일 메뉴 번호, 1-4와 같은 메뉴 번호 범위 또는 쉼표 1,2,3으로 구분된 메뉴 번호를 포함할 수 있습니다.

CLI sslconfig 후속 프롬프트는 'enter'를 누르거나 원하는 대로 설정을 수정하여 기존 값을 수락합니다.

원하는 경우 명령 > commit >> 선택 사항인 comment를 입력하고 >> "Enter"를 눌러 변경을 완료합니다.

다음을 확인합니다.

이 섹션에는 일치하지 않는 TLS 프로토콜 버전 또는 구문 오류로 인해 나타날 수 있는 몇 가지 기본 테스트 시나리오 및 오류가 포함되어 있습니다.

지원되지 않는 대상 TLS v1.3으로 인해 거부를 생성하는 SEG 발송 SMTP 협상의 샘플 로그 항목:

```
Wed Jan 17 20:41:18 2024 Info: DCID 485171 TLS deferring: (336151598, 'error:1409442E:SSL routines:ssl3
```

성공적으로 협상된 TLS v1.3을 수신하는 전송 SEG의 샘플 로그 항목:

```
Wed Jan 17 21:09:12 2024 Info: DCID 485206 TLS success protocol TLSv1.3 cipher TLS_AES_256_GCM_SHA384
```

TLS v1.3이 활성화되지 않은 수신 SEG의 샘플 로그 항목

```
Wed Jan 17 20:11:06 2024 Info: ICID 1020004 TLS failed: (337678594, 'error:14209102:SSL routines:tls_ea
```

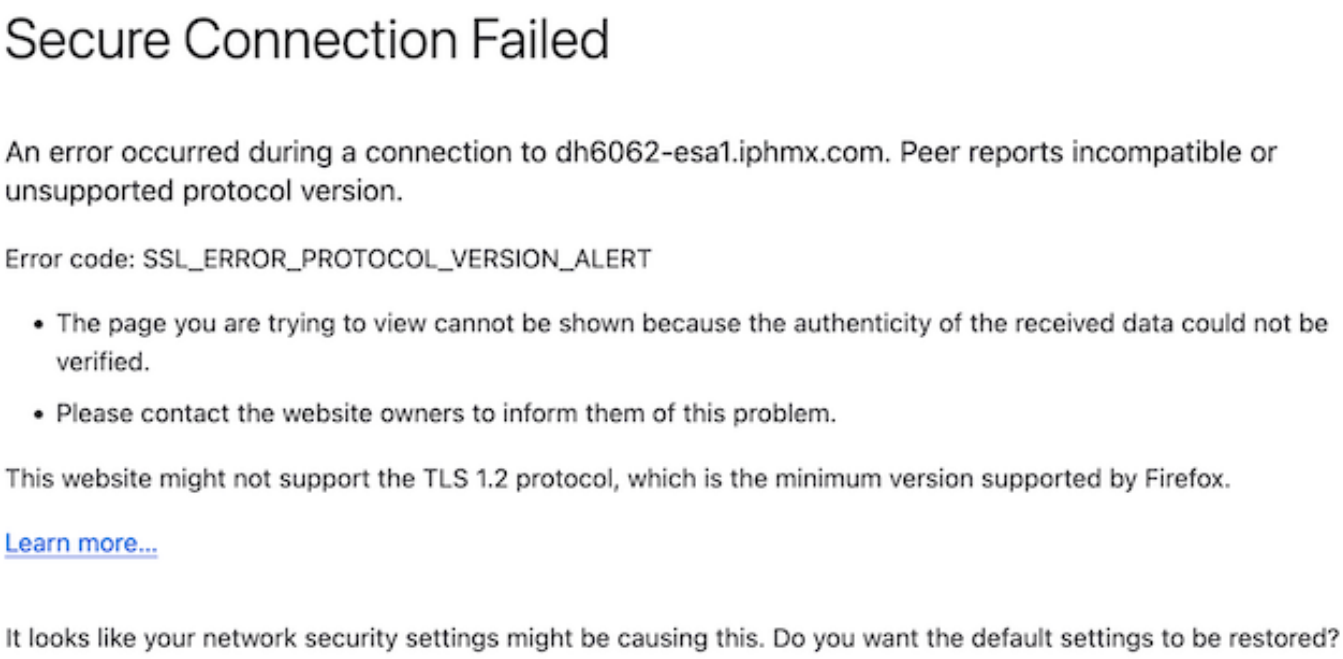
SEG 지원 TLS v1.3 수신

```
Wed Jan 17 21:09:12 2024 Info: ICID 1020089 TLS success protocol TLSv1.3 cipher TLS_AES_256_GCM_SHA384
```

브라우저 기능을 확인하려면 TLSv1.3으로 구성된 SEG WebUI 또는 NGUI에 대한 웹 브라우저 세션을 열기만 하면 됩니다.

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

- 테스트: Firefox에서 브라우저 설정을 구성하면 TLS v1.3 지원이 비활성화되어 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.



- 통신을 확인하려면 TLSv1.3이 포함되도록 브라우저 설정을 확인하십시오. (이 샘플은 Firefox에서 가져온 것이며 숫자 1-4를 사용합니다.

security.tls.version.fallback-limit	4
security.tls.version.max	4
security.tls.version.min	3

관련 정보

- Cisco Secure Email Gateway - 설정 가이드
- Cisco Secure Email Gateway 시작 페이지 - 지원 가이드
- Cisco Secure Email Gateway - 릴리스 정보

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.