핸드셰이크 오류 또는 인증서 검증 오류로 인한 NGFW 서비스 모듈 TLS 중단 오류

목차

소개

이 문서에서는 암호 해독 기능이 활성화된 Cisco NGFW(Next-Generation Firewall) 서비스 모듈을 통해 HTTPS 기반 웹 사이트에 대한 액세스로 특정 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- SSL(Secure Sockets Layer) 핸드셰이크 절차
- SSL 인증서

사용되는 구성 요소

이 문서의 정보는 Cisco PRSM(Prime Security Manager) 버전 9.2.1.2(52)이 포함된 Cisco NGFW 서비스 모듈을 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

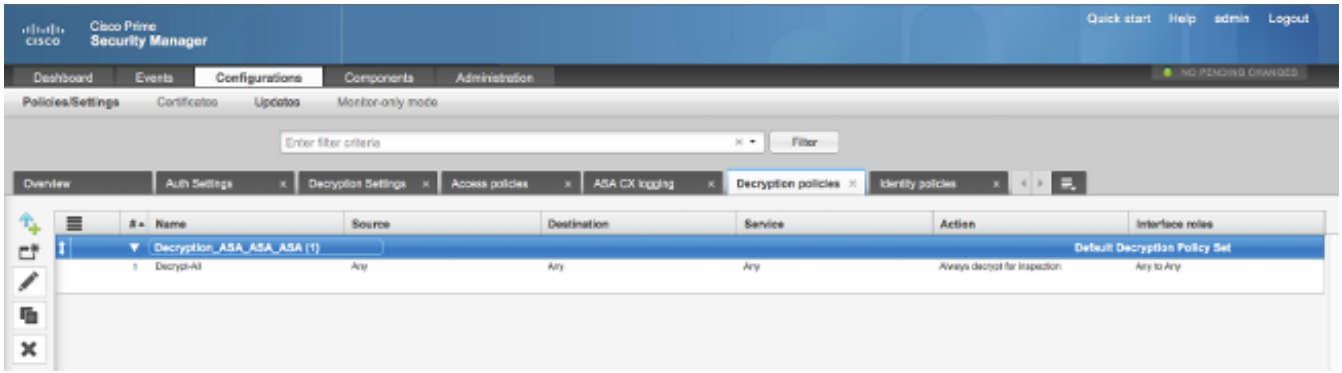
암호 해독은 NGFW 서비스 모듈에서 SSL 암호화 플로우를 해독하고(그렇지 않은 경우 암호화된 대화를 검사) 트래픽에 정책을 적용할 수 있도록 하는 기능입니다.이 기능을 구성하려면 관리자가 NGFW 모듈에서 암호 해독 인증서를 구성해야 합니다. 이 인증서는 클라이언트 액세스 HTTPS 기

반 웹 사이트에 원래 서버 인증서 대신 표시됩니다.

암호 해독이 작동하려면 NGFW 모듈이 서버에서 제공한 인증서를 신뢰해야 합니다.이 문서에서는 NGFW 서비스 모듈과 서버 간에 SSL 핸드셰이크가 실패하는 경우의 시나리오에 대해 설명합니다. 이 경우 특정 HTTPS 기반 웹 사이트가 해당 웹 사이트에 연결하려고 시도할 때 실패합니다.

이 문서에서는 PRSM이 포함된 NGFW 서비스 모듈에서 다음 정책을 정의합니다.

- **ID 정책**:정의된 ID 정책이 없습니다.
- **암호 해독 정책**:Decrypt-**All** 정책은 다음 컨피그레이션을 사용합니다.

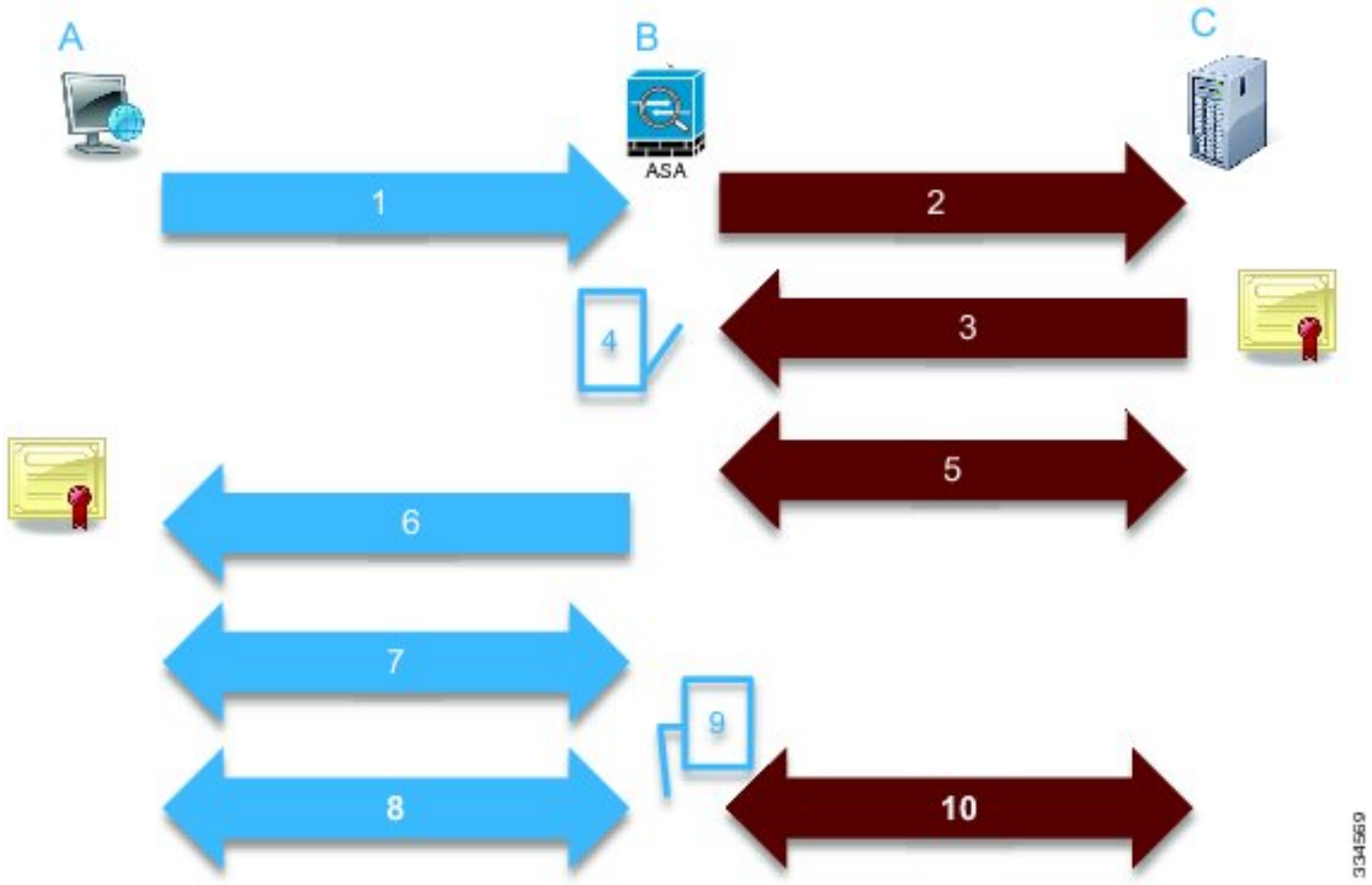


- **액세스 정책**:정의된 액세스 정책이 없습니다.
- **암호 해독 설정**:이 문서에서는 **암호 해독 인증서**가 NGFW 서비스 모듈에 구성되어 있으며 클라이언트가 이를 신뢰한다고 가정합니다.

NGFW 서비스 모듈에 암호 해독 정책이 정의되고 이전에 설명한 대로 구성된 경우 NGFW 서비스 모듈은 모듈을 통해 모든 SSL 암호화 트래픽을 가로채고 해독하려고 시도합니다.

> **참고:**이 프로세스에 대한 단계별 설명은 ASA CX 및 Cisco Prime Security Manager 9.2 사용 설명서의 Decrypted Traffic Flow 섹션에서 확인할 수 있습니다.

이 그림에서는 이벤트 시퀀스를 보여 줍니다.



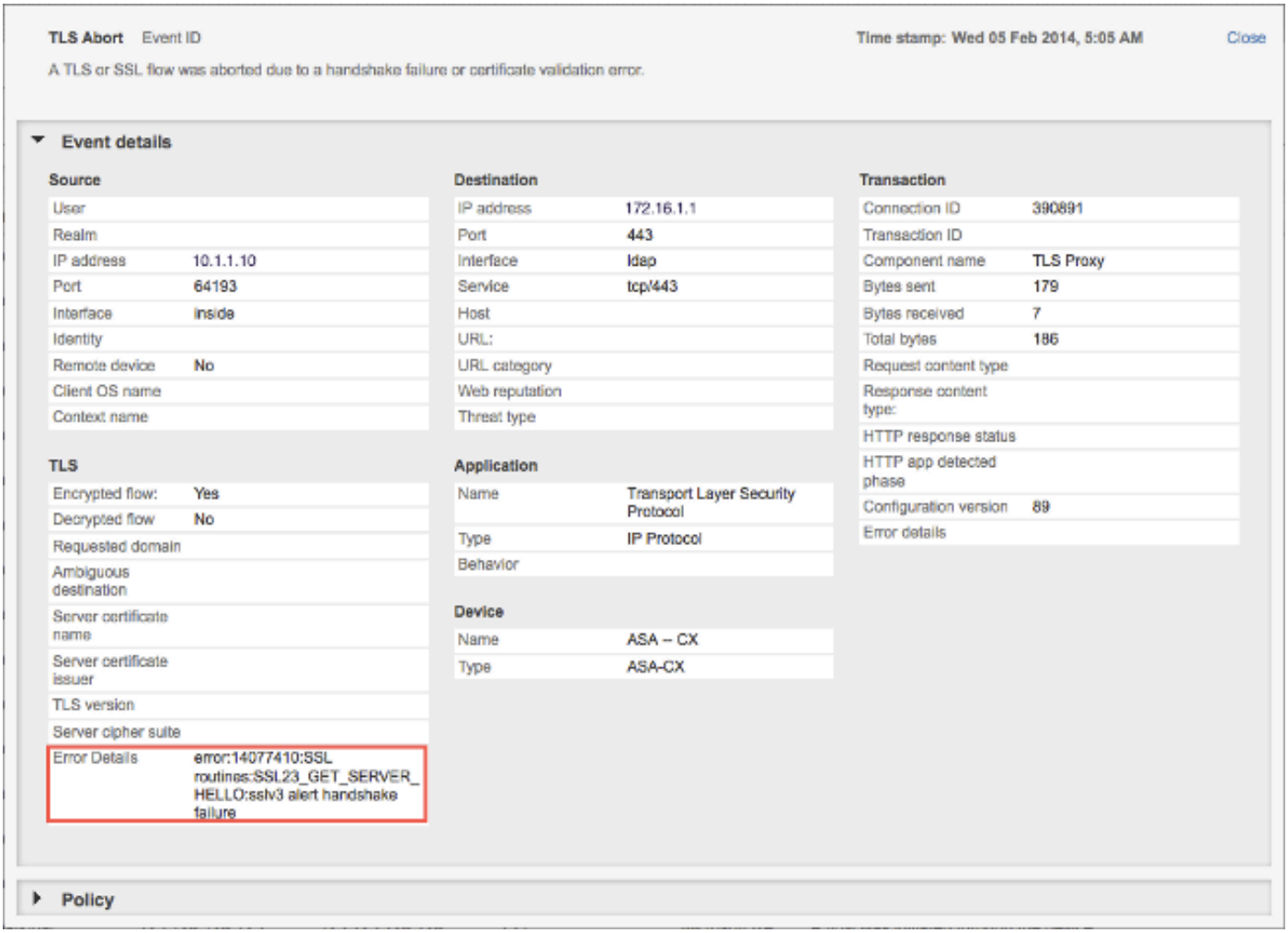
이 이미지**에서 A**는 클라이언트이고 **B는** NGFW 서비스 모듈이며 **C는** HTTPS 서버입니다.이 문서에 제공된 예제의 경우 HTTPS 기반 서버는 Cisco ASA(Adaptive Security Appliance)의 Cisco ASDM(Adaptive Security Device Manager)입니다.

이 프로세스에는 다음 두 가지 중요한 요소가 있습니다.

- 프로세스의 두 번째 단계에서 서버는 NGFW 서비스 모듈에서 제공하는 SSL 암호 그룹 중 하나를 수락해야 합니다.
- 프로세스의 네 번째 단계에서 NGFW 서비스 모듈은 서버에서 제공하는 인증서를 신뢰해야 합니다.

문제

서버가 NFGW 서비스 모듈에서 제공하는 SSL 암호를 허용할 수 없는 경우 다음과 같은 오류 메시지가 표시됩니다.



다음과 같은 오류 세부 정보(강조 표시)에 유의해야 합니다.

```
error:14077410:SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure
```

모듈 진단 아카이브에서 **/var/log/cisco/tls_proxy.log** 파일을 보면 다음 오류 메시지가 나타납니다.

```
2014-02-05 05:21:42,189 INFO  TLS_Proxy   - SSL alert message received from
 server (0x228 = "fatal : handshake failure") in Session: x2fd1f6

2014-02-05 05:21:42,189 ERROR TLS_Proxy - TLS problem (error:14077410:
 SSL routines:SSL23_GET_SERVER_HELLO:sslv3 alert handshake failure) while
 connecting to server for Session: x2fd1f6
```

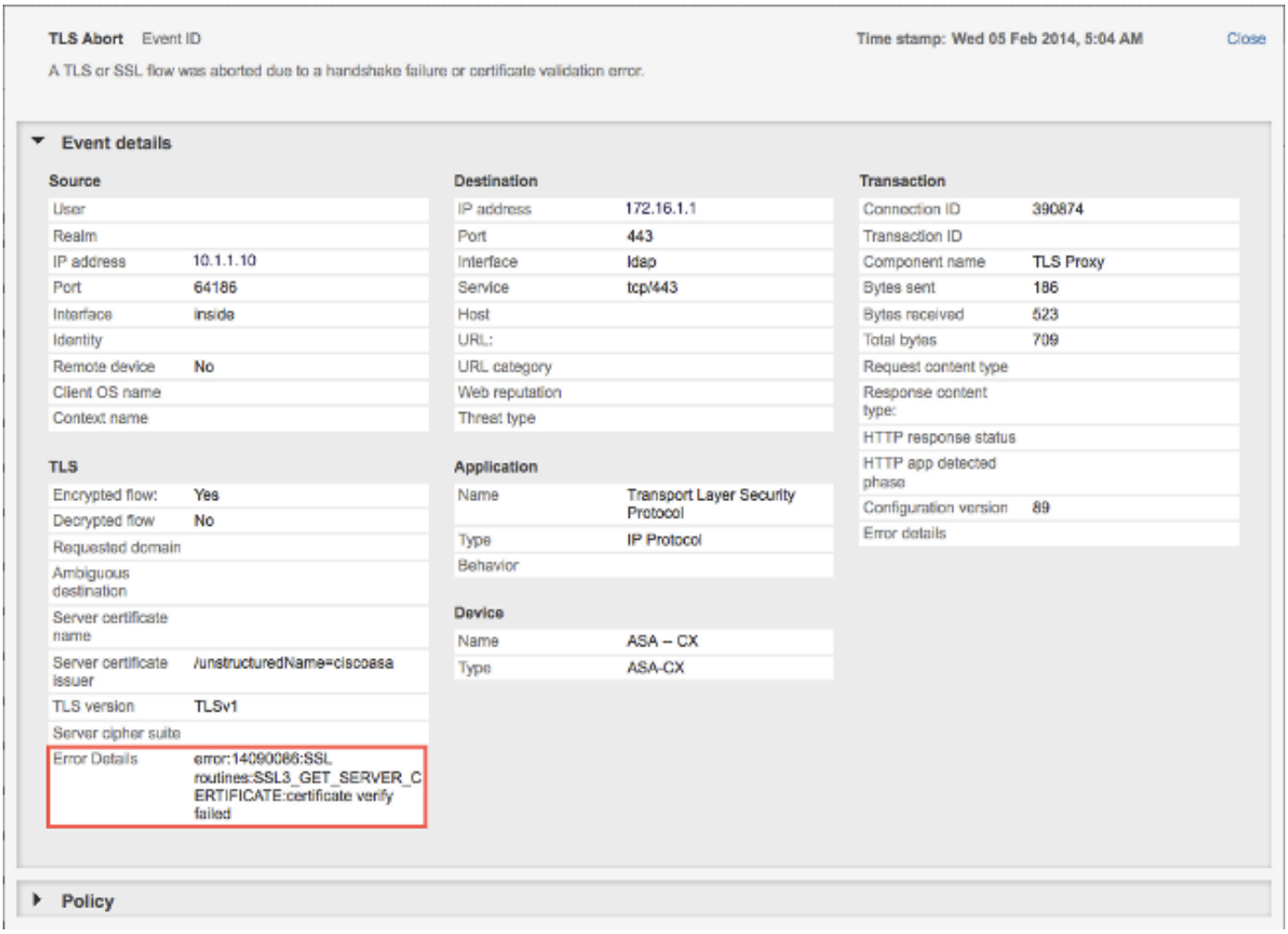
솔루션

이 문제의 가능한 원인 중 하나는 모듈에 3DES/AES(Triple Data Encryption Standard/Advanced Encryption Standard) 라이센스(종종 K9라고도 함)가 설치되어 있지 않기 때문입니다.모듈에 대한 K9 라이센스를 무료로 다운로드하여 PRSM을 통해 업로드할 수 있습니다.

3DES/AES 라이센스를 설치한 후에도 문제가 지속되면 NGFW 서비스 모듈과 서버 간의 SSL 핸드셰이크에 대한 패킷 캡처를 얻고 서버 관리자에게 문의하여 서버에서 적절한 SSL 암호를 사용하도록 설정하십시오.

문제

NGFW 서비스 모듈이 서버에서 제공하는 인증서를 신뢰하지 않으면 다음과 같은 오류 메시지가 표시됩니다.



다음과 같은 오류 세부 정보(강조 표시)에 유의해야 합니다.

```
error:14090086:SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed
```

모듈 진단 아카이브에서 **/var/log/cisco/tls_proxy.log** 파일을 보면 다음 오류 메시지가 나타납니다.

```
2014-02-05 05:22:11,505 INFO  TLS_Proxy - Certificate verification failure:
 self signed certificate (code 18, depth 0)

2014-02-05 05:22:11,505 INFO TLS_Proxy - Subject: /unstructuredName=ciscoasa

2014-02-05 05:22:11,505 INFO TLS_Proxy - Issuer: /unstructuredName=ciscoasa

2014-02-05 05:22:11,505 INFO TLS_Proxy - SSL alert message received from
 server (0x230 = "fatal : unknown CA") in Session: x148a696e

2014-02-05 05:22:11,505 ERROR TLS_Proxy - TLS problem (error:14090086:
 SSL routines:SSL3_GET_SERVER_CERTIFICATE:certificate verify failed) while
 connecting to server for Session: x148a696e
```

솔루션

모듈이 서버 SSL 인증서를 신뢰할 수 없는 경우 SSL 핸드셰이크 프로세스가 성공했는지 확인하기 위해 PRSM이 있는 모듈로 서버 인증서를 가져와야 합니다.

서버 인증서를 가져오려면 다음 단계를 완료합니다.

1. 브라우저를 통해 인증서를 다운로드하려면 서버에 액세스할 때 NGFW 서비스 모듈을 우회합니다.모듈을 우회하는 한 가지 방법은 특정 서버에 대한 트래픽을 해독하지 않는 암호 해독 정책을 생성하는 것입니다.이 비디오에서는 정책을 생성하는 방법을 보여줍니다.

   다음은 비디오에 표시되는 단계입니다.

   CX에서 PRSM에 액세스하려면 https://**<IP_ADDRESS_OF_PRSM>으로 이동하십시오**.이 예에서는 https://10.106.44.101을 **사용합니다**.

   PRSM에서 **Configurations > Policies/Settings > Decryption policies**로 이동합니다.

   화면 왼쪽 상단 모서리에 있는 아이콘을 클릭하고 목록 맨 위에 정책을 추가하려면 **Add above policy(위** 정책 추가) 옵션을 선택합니다.

   정책의 이름을 지정하고 Source(소스)를 **Any(모두)**로 유지하고 **CX 네트워크 그룹** 객체를 생성합니다.
   참고:HTTPS 기반 서버의 IP 주소를 포함해야 합니다.이 예에서는 **172.16.1.1**의 IP 주소가 사용됩니다.Action**에** 대해 Do not decrypt를 선택합니다.

   정책을 저장하고 변경 사항을 커밋합니다.
2. 다음 비디오와 같이 브라우저를 통해 서버 인증서를 다운로드하고 PRSM을 통해 NGFW 서비스 모듈에 업로드합니다.

   다음은 비디오에 표시되는 단계입니다.

   앞에서 설명한 정책이 정의되면 브라우저를 사용하여 NGFW 서비스 모듈을 통해 열리는 HTTPS 기반 서버로 이동합니다.
   참고:이 예에서 Mozilla Firefox 버전 26.0은 URL https://172.16.1.1이 있는 서버(ASA의 ASDM)로 이동하기 위해 **사용됩니다**.보안 경고가 나타나면 이를 수락하고 보안 예외를 추가합니다.

   주소 표시줄 왼쪽에 있는 작은 잠금 모양 아이콘을 클릭합니다.이 아이콘의 위치는 사용되는 브라우저와 버전에 따라 달라집니다.

   View **Certificate(인증서 보기**) 버튼**을** 클릭한 다음 서버 인증서를 선택한 후 Details(세부사항) 탭 아래에 있는 Export(내보내기) 버튼을 클릭합니다.

   원하는 위치에 개인 컴퓨터에 인증서를 저장합니다.

   PRSM에 로그인하고 Configurations(컨피그레이션) **> Certificates(인증서)로 이동합니다**.

   I want to... > Import certificate를 클릭하고 이전에 다운로드한 서버 인증서(4단계)를 선택합니

다.

변경 사항을 저장하고 커밋합니다.완료되면 NGFW 서비스 모듈은 서버에서 제공하는 인증서를 신뢰해야 합니다.

3. 1단계에서 추가된 정책을 제거합니다. 이제 NGFW 서비스 모듈이 서버와 핸드셰이크를 성공적으로 완료할 수 있습니다.

관련 정보

- ASA CX 및 Cisco Prime Security Manager 9.2 사용 설명서
- 기술 지원 및 문서 – Cisco Systems