Firepower Threat Defense 인증서 기반 인증

FTD 인증서 기반 인증 요구 사항 및 사전 요건

모델 지원

FTD

지원되는 도메인

모든

사용자 역할

관리자

Network Admin(네트워크 관리자)

Firepower Threat Defense VPN 인증서 가이드라인 및 제한 사항

- 인증서 등록 개체이 연결된 후 디바이스에 설치되면 인증서 등록 프로세스가 즉시 시작됩니다. 이 프로세스는 자체 서명 및 SCEP 등록 유형의 경우 자동으로 진행되므로, 관리자의 추가 작업이 필요하지 않습니다. 수동 인증서 등록 및 PKCS12 파일 가져오기의 경우 관리자의 추가 작업이 필요합니다.
- 인증서 등록이 완료되면 디바이스에 인증서 등록 개체와 이름이 동일한 트러스트 포인트가 존재하게 됩니다. 이 트러스트 포인트를 VPN 인증 방법의 컨피그레이션에서 사용하십시오.
- FTD 사용자 인터페이스에 선택 사항이 표시되지만 현재는 ECDSA가 아닌 RSA 키만 지원합니다.
- FTD VPN이 클러스터링된 환경에서 지원되지 않으므로 PKI도 클러스터링 환경에서 지원되지 않습니다.
- FTD 디바이스는 Microsoft CA 서비스, Cisco Adaptive Security Appliance 및 Cisco IOS Router에서 제공하는 CA 서비스를 사용한 인증서 등록을 지원합니다.
- FTD 디바이스는 CA(Certificate Authority)로 구성할 수 없습니다.

인증서 관리 도메인 및 디바이스에 대한 지침

- Firepower Threat Defense 디바이스는 Microsoft CA 서비스, Cisco Adaptive Security Appliance 및 Cisco IOS Router에서 제공하는 CA 서비스를 지원하고 이들을 사용해 인증합니다.
- 인증서 등록은 하위 또는 상위 도메인에서 수행할 수 있습니다.
- 상위 도메인에서 등록이 완료되면 동일한 도메인에 인증서 등록 개체가 포함되어야 합니다. 디바이스의 트러스트 포인트가 하위 도메인에 오버라이드된 경우, 오버라이드된 값이 디바이스에 구축됩니다.
- 리프 도메인의 디바이스에 인증서 등록이 완료되면 상위 도메인 및 다른 하위 도메인에서는 보이지 않습니다.
- 리프 도메인을 삭제하면 포함된 디바이스의 인증서 등록을 제거할 필요가 없습니다.
- 디바이스에 한 도메인의 인증서가 등록되면 다른 도메인에는 등록이 허용되지 않습니다. 하지만 다른 도메인에서 인증서를 볼 수 있습니다.
- 디바이스가 한 도메인에서 다른 도메인으로 이동하는 경우, 또는 도메인이 아닌 곳에서 도메인으로 이동하는 경우 해당 디바이스의 인증서 등록을 제거하고 새 도메인에 재구성되어야 합니다. 디바이스에서 등록을 제거하면 알림을 받게 됩니다.

FTDVPN 인증서 매핑

디지털 인증서의 소개는 PKI 인프라 및 디지털 인증서을 참조하십시오.

관리되는 디바이스에서 인증서를 가져오고 등록하는 데 사용되는 개체에 대한 설명은 인증서 등록 개체을 참조하십시오.

프로시저

단계 **1** **Devices(**디바이스**)** > **Certificates(**인증서**)**을(를) 선택합니다.

이 화면에 나열된 각 디바이스에 대해 다음 열을 볼 수 있습니다.

- **Name(**이름**)** - 이미 관련된 트러스트 포인트가 있는 디바이스를 나열합니다. 연결된 트러스트 포인트 목록을 보려면 디바이스를 확장합니다.
- **Enrollment Type(**등록 유형**)** - 트러스트 포인트에 사용된 등록 유형을 표시합니다.
- **Status(**상태**)** - **CA** 인증서 및 **ID** 인증서의 상태를 제공합니다. 인증서 내용이 사용 가능일 때 돋보기를 클릭하여 볼 수 있습니다.

  CA 인증서 정보를 볼 때 CA 인증서를 발급한 모든 인증 기관의 계층 구조를 볼 수 있습니다.

  등록이 실패한 경우 오류 메시지를 보려면 상태를 클릭합니다.
- 추가 열은 **CA** 인증서 및 **ID** 인증서의 상태를 제공합니다. 인증서 내용의 각 열이 사용 가능일 때 돋보기를 클릭하여 볼 수 있습니다.

  이 열의 값은 등록 유형에 따라 다르며 등록 프로세스 동안 변경됩니다. CA 인증서는 사용 가능, 사용 불가, 해당 없음 상태가 될 수 있습니다. ID 인증서는 새로 고침 동안 사용 가능, 보류, 사용 가능 및 보류 상태가 될 수 있습니다.
- 추가 열에는 다음 작업을 수행하는 아이콘이 나열됩니다.
  - **Export Certificate(**인증서 내보내기**)** - 인증서의 복사본을 내보내고 다운로드하려면 클릭합니다. PKCS12(전체 인증서 체인) 또는 PEM(ID 인증서 전용) 형식을 내보내도록 선택할 수 있습니다.

    나중에 파일을 가져오려면 PKCS12 인증서 형식을 내보내려면 암호를 제공해야 합니다.
  - **Re-enroll certificate(**인증서 다시 등록**)** - 기존 인증서를 다시 등록합니다.
  - **Refresh certificate status(**인증서 상태 새로 고침**)** - 인증서를 새로 고쳐 Firepower Threat Defense 디바이스 인증서 상태를 Firepower Management Center와 동기화합니다.
  - **Delete certificate(**인증서 삭제**)** - 트러스트 포인트에 대한 모든 연결된 인증서를 삭제합니다.

단계 **2** **(+)** 선택 > 새 인증서 추가를 선택하여 디바이스에 등록 개체를 연결하고 설치합니다. 등록 유형에 따릅니다.

참고 인증서 등록 개체이 연결된 후 디바이스에 설치되면 인증서 등록 프로세스가 즉시 시작됩니다. 이 프로세스는 자체 서명 및 SCEP 등록 유형의 경우 자동으로 진행되므로, 관리자의 추가 작업이 필요하지 않습니다. 수동 인증서 등록 및 PKCS12 파일 가져오기의 경우 관리자의 추가 작업이 필요합니다.

관련 항목

자체 서명 등록을 사용한 인증서 설치 , 4 페이지
SCEP 등록을 사용한 인증서 설치, 5 페이지
수동 등록을 사용한 인증서 설치, 6 페이지
PKCS12 파일을 가져오는 방법으로 인증서 설치, 7 페이지

자체 서명 등록을 사용한 인증서 설치

프로시저

단계 **1** **Devices(**디바이스**) > Certificates(**인증서**)** 화면에서 **Add(**추가**) > Add New Certificate(**새 인증서 추가**)**를 선택하고 **Add New Certificate(**새 인증서 추가**)** 대화 상자를 엽니다.

단계 **2** 드롭다운 목록에서 **Device(**디바이스**)**를 엽니다.

단계 **3** 다음 방법 중 하나로 인증서 등록 개체를 이 디바이스와 연결합니다.

- 드롭다운 목록에서 적절한 유형의 인증서 등록 개체를 선택합니다.
- **(+)**를 클릭하고 새 인증서 등록 개체를 추가하려면 인증서 등록 개체 추가을 참조하십시오.

단계 **4** 설치를 누르면 자체 서명된 자동 등록 프로세스가 시작됩니다.

자체 서명된 등록 유형의 트러스트 포인트의 경우 관리되는 디바이스가 자체 CA로 작동하여 자체 ID를 생성하는 CA 인증서가 필요하지 않으므로 **CA** 인증서 상태는 항상 `NotApplicable` 상태입니다.

디바이스가 자체 서명된 ID 인증서를 생성하면 **ID** 인증서는 InProgress에서 Available 상태로 변경됩니다.

단계 **5** 이 장치에 대해 생성된 자체 서명된 ID 인증서를 보려면 돋보기를 클릭합니다.

다음에 수행할 작업

인증서 등록이 완료되면 디바이스에 인증서 등록 개체와 이름이 동일한 트러스트 포인트가 존재하게 됩니다. 이 트러스트 포인트를 VPN 인증 방법의 컨피그레이션에서 사용하십시오.

SCEP 등록을 사용한 인증서 설치

시작하기 전에

참고 SCEP 등록을 사용할 경우 매니지드 디바이스와 CA 서버 간에 직접 연결이 설정됩니다. 등록 프로세스를 시작하기 전에 디바이스가 CA 서버에 연결되었는지 확인하십시오.

프로시저

단계 **1** 설치를 누르면 자동 등록 프로세스가 시작됩니다.

단계 **2** **Devices(**디바이스**) > Certificates(**인증서**)** 화면에서 **Add(**추가**) > Add New Certificate(**새 인증서 추가**)**를 선택하고 **Add New Certificate(**새 인증서 추가**)** 대화 상자를 엽니다.

단계 **3** 드롭다운 목록에서 **Device(**디바이스**)**를 엽니다.

단계 **4** 다음 방법 중 하나로 인증서 등록 개체를 이 디바이스와 연결합니다.

- 드롭다운 목록에서 적절한 유형의 인증서 등록 개체를 선택합니다.
- **(+)**를 클릭하고 새 인증서 등록 개체를 추가하려면 인증서 등록 개체 추가을 참조하십시오.

단계 **5** 설치를 누르면 자동 등록 프로세스가 시작됩니다.

SCEP 등록 유형 트러스트 포인트의 경우 CA 서버에서 CA 인증서를 가져와 디바이스에 설치하므로 **CA** 인증서 상태가 InProgress에서 Available로 전환됩니다.

ID 인증서는 디바이스가 특정 CA에서 SCEP를 사용해 ID 인증서를 가져오므로 `InProgress`에서 `Available` 상태로 변경됩니다.

참고 몇 가지 오류 메시지 때문에 SCEP 인증서 등록이 실패할 수 있습니다. 예를 들면 다음과 같습니다.

```
Error:
crypto ca authenticate scep1 nointeractive:[error]:ERROR:receiving Certificate
Authority certificate: status = FAIL, cert length = 0
Possible
```

이런 상황을 해결하기 위한 몇 가지 권장 사항입니다.

- FTD에서 SCEP 서버의 연결성을 확인하십시오 - SCEP 서버에 경로가 추가됩니다.
- SCEP 서버가 hostname/FQDN을 참조하면 FlexConfig 개체를 사용해 DNS 서버를 구성합니다.
- SCEP 서버와 FTD 디바이스가 동일한 NTP 서버 구성으로 실시간으로 동기화되도록 합니다.

단계 **6** 이 장치에 생성되고 설치된 ID 인증서를 보려면 돋보기를 클릭합니다.

다음에 수행할 작업

인증서 등록이 완료되면 디바이스에 인증서 등록 개체와 이름이 동일한 트러스트 포인트가 존재하게 됩니다. 이 트러스트 포인트를 VPN 인증 방법의 컨피그레이션에서 사용하십시오.

수동 등록을 사용한 인증서 설치

프로시저

단계 **1** 등록 프로세스를 시작 하려면 설치 를 누릅니다.

단계 **2** **Devices(**디바이스**) > Certificates(**인증서**)** 화면에서 **Add(**추가**) > Add New Certificate(**새 인증서 추가**)**를 선택하고 **Add New Certificate(**새 인증서 추가**)** 대화 상자를 엽니다.

단계 **3** 드롭다운 목록에서 **Device(**디바이스**)**를 엽니다.

단계 **4** 다음 방법 중 하나로 인증서 등록 개체를 이 디바이스와 연결합니다.

- 드롭다운 목록에서 적절한 유형의 인증서 등록 개체를 선택합니다.
- **(+)**를 클릭하고 새 인증서 등록 개체를 추가하려면 인증서 등록 개체 추가을 참조하십시오.

단계 **5** 가져오기를 누르면 수동 등록 프로세스를 시작합니다.

Firepower Management Center가 (등록 개체가 제공한) CA 인증서를 관리되는 디바이스에 설치하고 CA 서버를 인증하며 관리되는 디바이스에 트러스트 포인트를 생성하므로 **CA** 인증서 상태는 `InProgress`에서 `Available` 상태로 전환됩니다.

ID 인증서 상태가 CSR 생성 및 ID 인증서 가져오기가 보류 중이라는 경고 메시지를 보여줄 수 있습니다.

단계 **6** ID 인증서를 가져오기 위해 PKI CA 서버에서 적절한 작업을 실행합니다.

a) CSR을 보고 복사하려면 **Identity Certificate(ID** 인증서**)** 경고를 클릭합니다.

b) CRS을 사용해 ID 인증서를 가져오기 위해 PKI CA 서버에서 적절한 작업을 실행합니다.

이러한 작업은 Firepower Management Center 또는 관리되는 디바이스와는 완전히 별개입니다. 완료되면 관리되는 디바이스에 대한 ID 인증서가 생성됩니다. 복사 또는 파일에 저장할 수 있습니다.

c) 수동 프로세스를 완료하려면 가져온 ID 인증서를 관리되는 디바이스에 설치합니다.

Firepower Management Center 대화 상자로 돌아가 ID 인증서를 필드에 붙여 넣습니다. 또는 검색을 선택하여 ID 인증서 파일을 선택합니다.

단계 **7** ID 인증서를 가져오려면 가져오기를 선택합니다.

가져오기가 완료되면 ID 인증서 상태는 `Available`이 됩니다.

단계 8 장치에 대한 ID 인증서를 보려면 돋보기를 클릭합니다.

다음에 수행할 작업

인증서 등록이 완료되면 디바이스에 인증서 등록 개체와 이름이 동일한 트러스트 포인트가 존재하게 됩니다. 이 트러스트 포인트를 VPN 인증 방법의 컨피그레이션에서 사용하십시오.

PKCS12 파일을 가져오는 방법으로 인증서 설치

프로시저

단계 1 장치 > 인증서 화면에서 **PKCS12** 파일 가져오기 대화 상자를 열려면 + 추가 > **PKCS12** 파일 가져오기를 클릭합니다.

단계 2 디바이스 드롭다운 목록에서 사전 구성된 관리되는 디바이스를 선택합니다.

단계 3 **PKCS12**인증서 등록 유형을 지정합니다.

단계 4 PKCS#12 인증서 파일을 찾아서 선택하려면 검색을 선택합니다.

단계 5 암호 해독을 위해 암호 문구 값을 입력합니다.

단계 6 추가를 누릅니다.

파일 가져오기의 경우 CA 인증서 및 ID 인증서 상태는 PKCS12 파일이 디바이스에 설치됨에 따라 `In Progress`(진행 중)에서 `Available`(사용 가능)으로 전환됩니다.

단계 7 사용 가능 상태에서 장치에 대한 ID 인증서를 보려면 돋보기를 클릭합니다.

다음에 수행할 작업

관리되는 디바이스의 인증서(트러스트 포인트)는 PKCS#12 파일과 동일합니다. VPN 인증 설정에서 이 인증서를 사용합니다.

FTD VPN 인증서 문제 해결

인증서 등록 환경의 차이로 인해 문제가 발생했는지 여부는 Firepower Threat Defense VPN 인증서 가이드라인 및 제한 사항, 2 페이지을 참조하십시오. 다음을 확인합니다.

- 디바이스에서 CA 서버에 대한 경로가 있는지 확인합니다.

  CA 서버의 호스트 이름이 등록 개체에 지정된 경우 Flex Config를 사용해 서버에 적절히 연결하는 DNS를 구성합니다. CA 서버의 IP 주소를 사용해도 됩니다.

- Microsoft 2012 CA 서버를 사용하는 경우 관리되는 디바이스에서 기본 IPsec 템플릿을 허용하지 않으므로 변경해야 합니다.

작업 템플릿을 구성하려면 MS CA 설명서를 참조하여 다음 단계를 따르십시오.

1. IPsec(오프라인 요청) 템플릿을 복제합니다.
2. **Extensions(**확장**) > Application policies(**애플리케이션 정책**)**에서 *IP security IKE intermediate(IP* 보안 *IKE* 중급*)* 대신 *IP security end system(IP* 보안 최종 시스템*)*을 선택합니다.
3. 권한 및 템플릿 이름을 설정합니다.
4. 새 템플릿을 추가하고 새 템플릿 이름을 반영하기 위해 레지스트리 설정을 변경합니다.

Firepower Threat Defense 인증서 기반 인증 히스토리

기능	버전	세부 사항
수동 등록 기능 향상	6.7	이제 ID 인증서 없이 CA 인증서만 생성할 수 있습니다. CA 인증서 없이 CSR을 생성하고 CA에서 ID 인증서를 가져올 수도 있습니다.
PKCS CA 체인	6.7	인증서를 발급하는 인증 기관(CA)의 체인을 보고 관리할 수 있습니다. 인증서 복사본을 내보낼 수도 있습니다.