Talos 연결 상태 문제 해결

목차

소개

이 문서에서는 Secure Firewall FMC 및 FDM에서 TALOS 연결 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco FMC(Secure Firewall Management Center)
- Cisco FDM(Secure Firewall Device Manager)

- Cisco FTD(Secure Firewall Threat Defense)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

FMC 버전 7.6.0 또는 7.7.0
FDM 버전 7.6.0 또는 7.7.0
FTD 버전 7.6.0 또는 7.7.0

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

배경 정보

Cisco FMC(Secure Firewall Management Center)는 클라이언트측 인증서를 사용하여 Cisco Talos 위협 인텔리전스 서비스와의 보안 연결을 설정합니다. FMC에서 URL 평판 데이터베이스(URLDB), LSP(Lightweight Security Packages) 및 기타 보완 데이터를 비롯한 중요 업데이트를 성공적으로 다운로드하려면 이 인증이 필요합니다.

정상 작동 조건에서 이 인증서는 소프트웨어 설치 중에 미리 프로비저닝되며 만료 날짜가 가까워지면 자동으로 갱신되도록 설계되었습니다. 그러나 특정 버전의 Cisco 보안 방화벽 FMC 소프트웨어의 알려진 문제로 인해 2025년 3월 30일 이후 자동 갱신 프로세스가 성공적으로 완료되지 못합니다. 이 경우 FMC에서 Talos를 인증할 수 없으므로 연결이 실패하고 업데이트된 위협 인텔리전스를 검색할 수 없습니다.

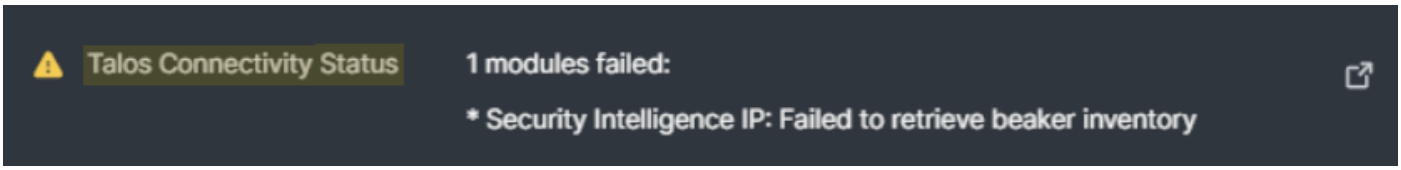
인증서 상태 확인

FMC GUI

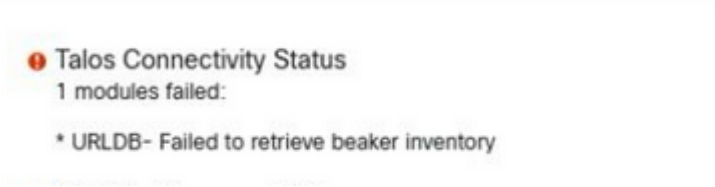
클라이언트 측 인증서가 갱신되지 않을 경우 Cisco FMC는 상태 알림을 트리거하여 Cisco Talos와의 통신 중단을 관리자에게 알립니다. System > Health로 이동하고 Talos Connectivity Status 섹션을 검토하여 이러한 알림을 모니터링할 수 있습니다.

인증서 만료 문제로 인해 시스템이 영향을 받는 경우 일반적으로 다음 오류 메시지 중 하나가 표시됩니다.

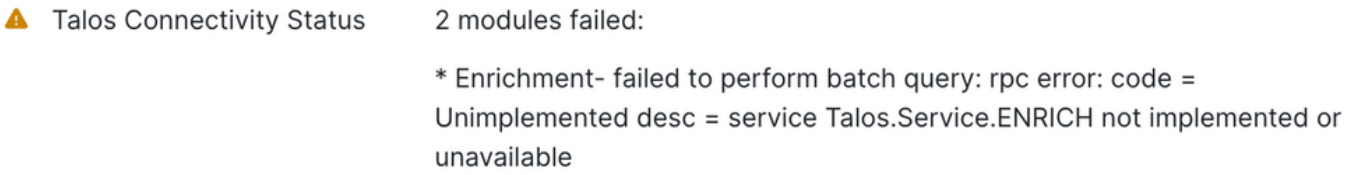
- "LSP - 비커 인벤토리를 검색하지 못했습니다":



- "URLDB - 비커 인벤토리를 검색하지 못했습니다.":



- "보강 - 일괄 쿼리를 수행하지 못했습니다.":



FMC CLI

FMC 어플라이언스가 이 문제의 영향을 받는지 확인하려면 expert 모드에 액세스하여 명령을 실행하여 클라이언트측 인증서의 현재 만료일을 확인합니다.

<#root>

```
expert
sudo su
//type the 'FMC CLI admin password'
```

sudo openssl x509 --in /var/sf/beaker3/securefirewall-dev-prod-01_prod.pem --text

명령 출력에서 유효성 섹션을 찾습니다. Not After 필드는 인증서의 현재 만료 날짜를 나타냅니다. 이 날짜가 이미 지났거나 다가오는 경우, 갱신 프로세스가 실패하고 수동 서비스 재시작이 인증서 갱신을 시작하는 데 필요합니다.

예:

<#root>

```
> expert
>sudo su
//type the 'FMC CLI admin password'
openssl x509 --in /var/sf/beaker3/securefirewall-dev-prod-01_prod.pem --text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 46240369 (0x2c19271)
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = US, ST = California, L = San Jose, O = Cisco Systems Inc., OU = Security, CN = Keym
```

Validity

```
Not Before: Jan 30 22:32:39 2024 GMT
```

Not After :

```
 Mar 30 22:32:39 2025 GMT
        Subject: CN = SFW76EVAL-prod-01, C = US, ST = California, L = San Jose, O = Cisco, OU = Securit
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
```

문제 해결

1. 시나리오 식별

소프트웨어 버전	연결된 버그 ID	주요 원인
7.6.0 또는 7.7.0	Cisco 버그 ID CSCwo63951	인증서 만료/연결 실패
7.6.1+ 또는 7.7.10+	Cisco 버그 ID CSCwr23982	등록/라이센싱 컨피그레이션(예: air-gapped)

2. 버전 7.6.0 및 7.7.0의 문제 해결

증상

앞서 언급한 상태 알림 외에도 다음과 같은 동작이 관찰됩니다.

- FDM 작업 관리자 오류: "Snort 3 클라우드 업데이트 실패: 업데이트 서버 또는 연결 시간 초과에서 응답이 없습니다."

- 로그 항목: /ngfw/var/log/messages 오류: 터널(UUID)에 연결하지 못했습니다. 오류: 연결되지 않았습니다.

- 상태: UI에서 업데이트 정체: URL Filtering Preferences(URL 필터링 기본 설정) 화면에 "Not updated yet(아직 업데이트되지 않음)"이 표시됩니다.

임시 해결 방법

서비스를 즉시 복원하려면 Expert Mode를 통해 필요한 프로세스를 다시 시작합니다.

1단계. CLI에 액세스하고 expert 모드로 들어갑니다.

2단계. 다음 명령을 실행합니다.

```
expert
sudo su
//type the 'FMC CLI admin password'
pmtool restartbyid talosAgent
pmtool restartbyid beaker3
```

참고: 이 해결 방법은 5일 동안만 유효한 인증서를 트리거합니다. 영구 수정이 적용될 때까지 5일마다 이 프로세스를 반복해야 합니다.

영구적 해결

이 문제를 영구적으로 해결하려면 다음 조건을 충족해야 합니다.

1단계. 연결 확인: 어플라이언스에 https://api-sse.cisco.com에 대한 아웃바운드 액세스 권한이 있는지 확인합니다. 이렇게 하려면 FMC CLI에 액세스하여 expert 모드로 들어간 다음 명령을 실행합니다.

1.1단계. DNS 확인 테스트:

<#root>

```
expert
sudo su
```

```
//type the 'FMC CLI admin password'

nslookup api-sse.cisco.com
```

1.2단계. TCP 포트 액세스 테스트:

<#root>

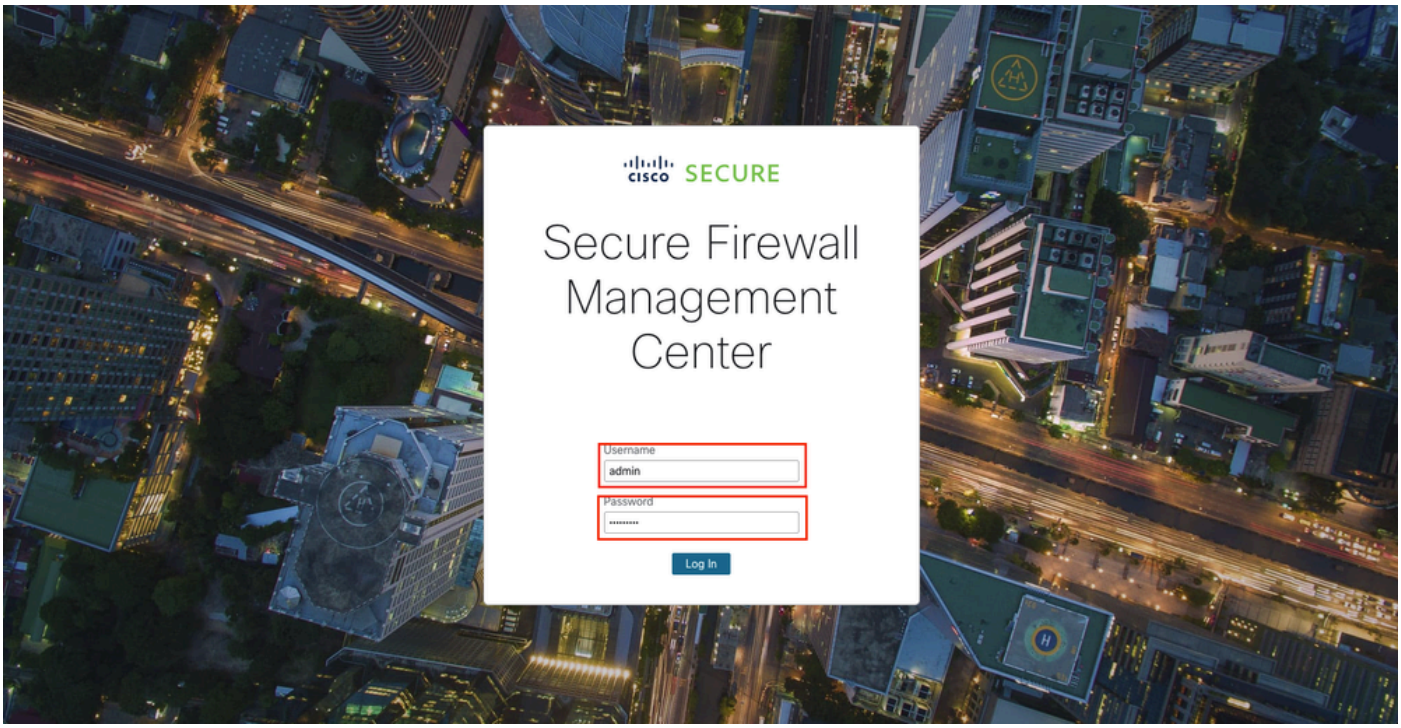
```
 expert
sudo su
//type the 'FMC CLI admin password'

telnet api-sse.cisco.com 443
```

참고: 모든 업스트림 방화벽, 프록시 또는 보안 디바이스를 통해 https://api-sse.cisco.com에 대한 아웃바운드 HTTPS(TCP 443) 액세스가 허용되는지 확인합니다.

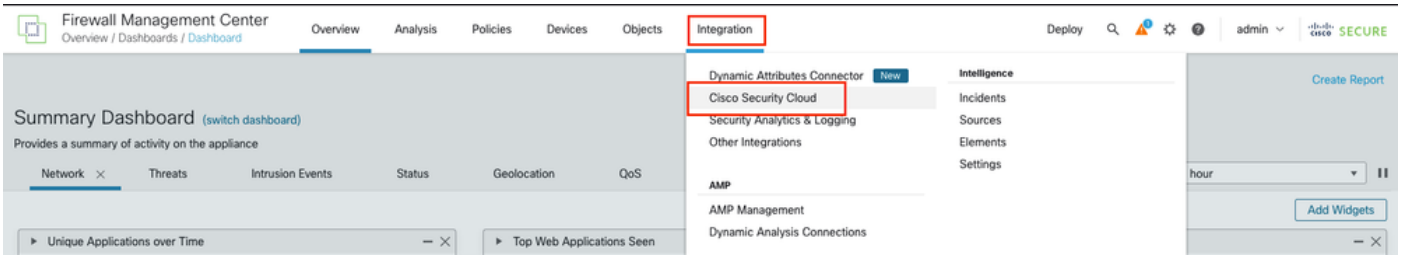
2단계. 텔레메트리 활성화: SSEConnector가 새 인증서를 받을 수 있도록 CSN(Customer Success Network) 텔레메트리를 활성화했는지 확인합니다. FMC에서 CSN을 활성화하는 절차는 다음과 같습니다.

2.1단계. 웹 브라우저를 열고 FMC URL로 이동하여 FMC GUI에 로그인합니다(예: https://<FMC_IP_or_Hostname>). 사용자 이름과 비밀번호를 입력하여

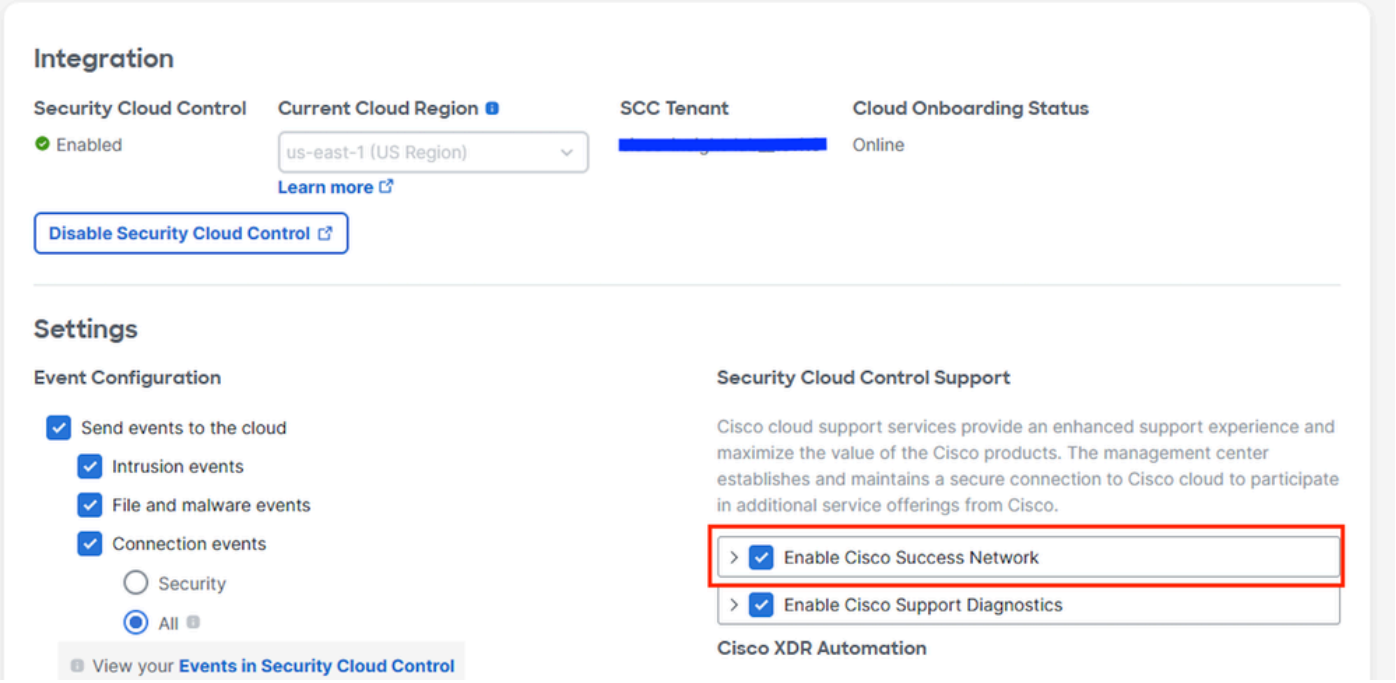
FMC GUI 인터페이스.



2.2단계. Cisco Success Network Settings(Cisco Success Network 설정)로 이동합니다. 주 메뉴에서 Integration > Cisco Security Cloud를 선택합니다.



2.3단계. Cisco Success Network(Cisco 성공 네트워크)라는 레이블이 지정된 옵션을 찾아 활성화합니다. 이를 위해 Enable Cisco Success Network to activate the telemetry(Cisco Success Network 활성화) 확인란을 선택합니다.



3단계. 업데이트 설치: GeoDB 2025-04-03-094 또는 VDB 406 이상 설치 그러면 새 365일 인증서 설치가 트리거됩니다.

참고: 고가용성(HA). HA 쌍에서는 SSEConnector 프로세스가 스탠바이 유닛에서 실행되지 않습니다. 스탠바이 FMC를 업데이트하려면 스탠바이가 액티브 상태가 되도록 역할 스위치를 수행한 다음 필요한 VDB 또는 GeoDB 업데이트를 설치합니다.

---

3. 버전 7.6.1 이상 및 7.7.10 이상 문제 해결

이 문제는 일반적으로 평가판 라이센스, SSM 온프레미스, PLR 또는 SLR을 사용하는 환경과 같이 표준 Cisco Security Cloud(CSC) 등록이 없는 환경에서 발생합니다.

영향을 받는 기능

- 자동/수동 LSP(Lightweight Security Package) 업데이트
- URL 필터링 데이터베이스 콘텐츠 업데이트 및 클라우드 조회.
- 연결 이벤트의 Talos 보완

권장 작업

1. 표준환경 Integration(통합) > Cisco Security Cloud(Cisco 보안 클라우드)를 통해 FMC를 등록합니다. 등록하면 30분 이내에 자동으로 새 인증서 다운로드가 트리거됩니다.

2. 수동 업데이트 자동 업데이트가 실패할 경우 software.cisco.com에서 최신 LSP를 수동으로 다운로드하여 FMC에 직접 설치합니다.

3. 에어갭이 있는 환경 네트워크에 인터넷 액세스가 없는 경우 Talos Connectivity Status 상태 모듈은 관련이 없게 됩니다. 이 시나리오에서는 적용된 상태 정책 내에서 이 특정 모듈을 비활성화합니다.

관련 정보

- 추가 지원이 필요한 경우 Cisco Technical Assistance Center(TAC)에 문의하십시오. 유효한 지원 계약이 필요합니다. Cisco Worldwide Support 연락처

- Cisco 지원 및 다운로드: Cisco 기술 지원 및 다운로드

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.