FMC 및 FDM용 CA 번들의 자동 업데이트 구성

목차

소개

이 문서에서는 Secure Firewall Management Center 및 Secure Firewall Device Manager용 Cisco CA 번들의 자동 업데이트 사용에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Secure Firewall Management Center(이전의 Firepower Management Center) 및 Secure Firewall Device Manager(이전의 Firepower Device Manager)에 대한 지식
- Secure Firewall Appliance(이전의 Firepower) 지식

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 소프트웨어 버전 7.0.5 이상을 실행하는 Cisco Secure Firewall Management Center(FMC 1000, 1600, 2500, 2600, 4500, 4600 및 가상).
- 소프트웨어 버전 7.1.0-3 이상을 실행하는 Cisco Secure Firewall Management Center(FMC 1600, 2600, 4600 및 가상).

- 소프트웨어 버전 7.2.4 이상을 실행하는 Cisco Secure Firewall Management Center(FMC 1600, 2600, 4600 및 가상).
- Secure Firewall Device Manager에서 관리하는 소프트웨어 버전 7.0.5 이상을 실행하는 Cisco Secure Firewall(FPR 1000, 2100, 3100, 4100, 9300, ISA300, 가상)
- Secure Firewall Device Manager에서 관리하는 소프트웨어 버전 7.1.0-3 이상을 실행하는 Cisco Secure Firewall(FPR 1000, 2100, 3100, 4100, 9300, ISA300, 가상)
- Secure Firewall Device Manager에서 관리하는 소프트웨어 버전 7.2.4 이상을 실행하는 Cisco Secure Firewall(FPR 1000, 2100, 3100, 4100, 9300, ISA300, 가상)

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 CA 번들에 사용

Cisco Secure Firewall(이전의 Firepower) 디바이스는 인증서가 포함된 로컬 CA 번들을 사용하여 여러 Cisco 서비스(Smart Licensing, Software, VDB, SRU 및 Geolocation Updates)에 액세스합니다. 시스템은 이제 매일 시스템 정의 시간에 자동으로 Cisco에 새 CA 인증서를 쿼리합니다. 이전에는 CA 인증서를 업데이트하려면 소프트웨어를 업그레이드해야 했습니다.

메모: 이 기능은 버전 7.0.0~7.0.4, 7.1.0~7.1.0-2 또는 7.2.0~7.2.3에서 지원되지 않습니다. 지원되는 버전에서 지원되지 않는 버전으로 업그레이드할 경우 기능이 일시적으로 비활성화되고 시스템에서 Cisco에 문의하는 것을 중지합니다.

SFMC 및 SFDM에서 CA 번들에 대한 자동 업데이트 구성

CA 번들에 대한 자동 업데이트 활성화

Secure Firewall Management Center 및 Secure Firewall Device Manager에서 CA 번들에 대한 자동 업데이트를 활성화하려면

1. SSH 또는 콘솔을 사용하여 CLI를 통해 SFMC 또는 SFDM에 액세스합니다.
2. CLI에서 configure cert-update auto-update enable 명령을 실행합니다.

<#root>

```
> configure cert-update auto-update enable

Autoupdate is enabled and set for every day at 18:06 UTC
```

3. CA 번들 업데이트가 자동 업데이트를 수행할 수 있는지 테스트하려면 configure cert-update test

명령을 실행합니다.

```
<#root>

> configure cert-update test

Test succeeded, certs can safely be updated or are already up to date.
```

수동으로 CA 번들 업데이트 실행

Secure Firewall Management Center 및 Secure Firewall Device Manager에서 CA 번들에 대한 업데이트를 수동으로 실행하려면

1. SSH 또는 콘솔을 사용하여 CLI를 통해 SFMC 또는 SFDM에 액세스합니다.
2. CLI에서 configure cert-update run-now 명령을 실행합니다.

```
<#root>

> configure cert-update run-now

Certs have been replaced or was already up to date.
```

다음을 확인합니다.

CA 번들에 대한 자동 업데이트 확인

Secure Firewall Management Center 및 Secure Firewall Device Manager에서 CA 번들에 대한 자동 업데이트 컨피그레이션을 검증하려면

1. SSH 또는 콘솔을 사용하여 CLI를 통해 SFMC 또는 SFDM에 액세스합니다.
2. CLI에서 show cert-update 명령을 실행합니다.

```
<#root>

> show cert-update


Autoupdate is enabled and set for every day at 18:06 UTC
CA bundle was last modified 'Wed Jul 19 03:11:31 2023'
```

문제 해결

업데이트 오류

권장 단계:

1. 현재 DNS 컨피그레이션을 확인합니다.
2. 관리 인터페이스에 대한 인터넷 및 프록시 컨피그레이션을 확인합니다.
3. ICMP를 사용하여 tools.cisco.com에 연결하고 expert 모드에서 다음 명령을 사용하여 curl을 활성화했는지 확인합니다.

```
sudo curl -vvk  https://tools.cisco.com
```

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.