Cisco Secure Firewall에 대한 장치 출력 브랜딩 변경 이해

목차

소개

이 문서에서는 Cisco Secure Firewall로 장치 출력을 리브랜딩하는 방법에 대한 통찰력을 설명합니다.

사전 요구 사항

배경 정보

- 표시된 장치 이름이 이제 다른 브랜딩 자료와 일치합니다.
- 이를 통해 더 강력한 브랜드와 더 편리한 사용자 환경을 만들 수 있습니다
- 모든 플랫폼에 기능적 영향 없음; 텍스트만 변경되었습니다.
- 이전 FTD 하드웨어 플랫폼(FPR1010/11XX, FPR41XX, FPR93XX)은 여전히 Firepower 브랜딩을 사용합니다
- 일부 시스템 기본값 및 구성 요소 이름에서는 여전히 firepower을 사용할 수 있습니다

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco NGFW(Next Gen Firewall) 포트폴리오

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- FMC(firepower Management Center) 버전 7.6.0

- Firepower 장치 관리자(FDM) 버전 7.6.0
- 모든 FTD(Virtual Firepower Threat Defense) 버전 7.6.0
- Cisco Secure Firewall 31XX,42XX

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.

기능 설명

운영 방식:

- CSF31XX, CSF42XX, FTD(Firewall Threat Defense) Virtual 및 모든 FMC(Firewall Management Center) 플랫폼의 전체 모델 이름 및 짧은 모델 이름에는 Cisco Secure Firewall 브랜딩이 포함되어 있습니다.
- 이제 CSF31XX FDM 소프트웨어는 SFDM, Secure Firewall Device Manager입니다.
- 이 기능에 대한 기능 구성 요소가 없습니다.
- 이 기능에 대한 컨피그레이션 옵션이 없습니다.

업그레이드:

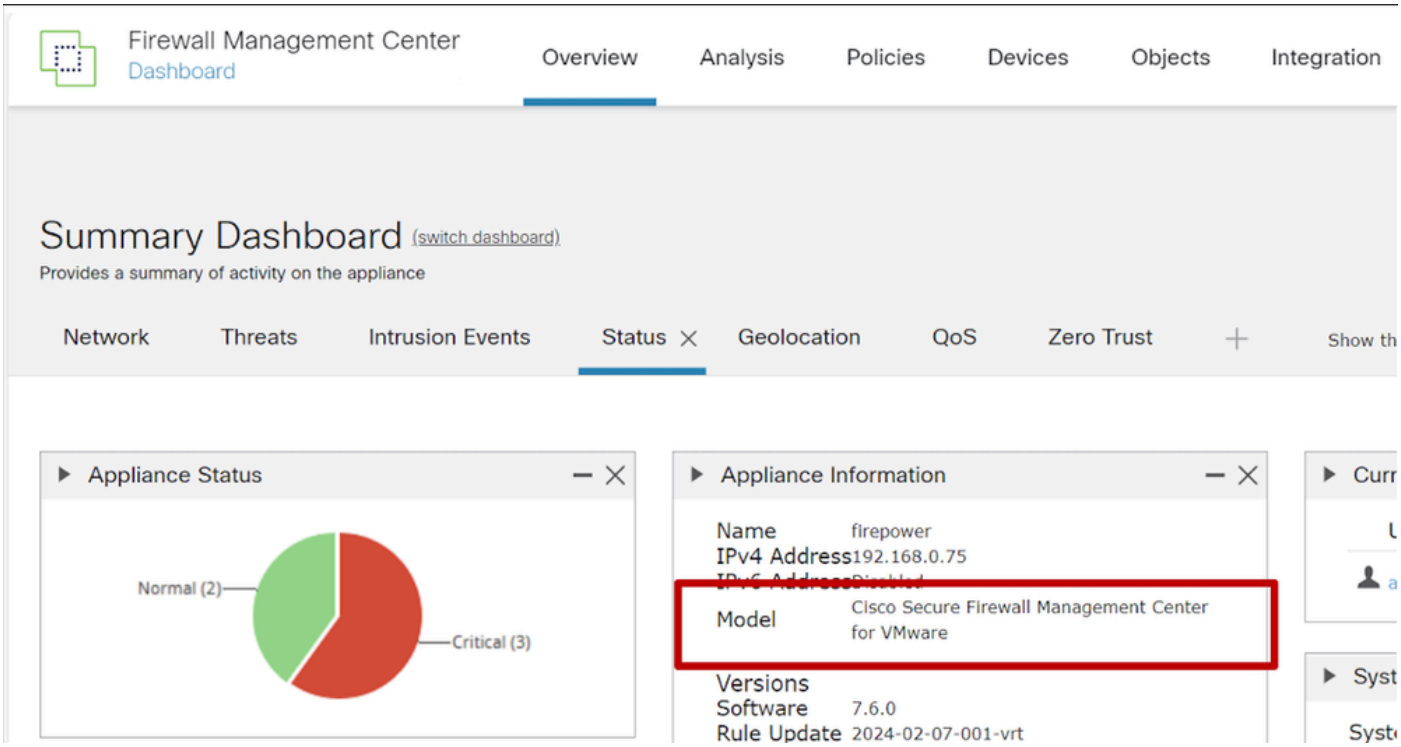
- Secure Firewall 7.6으로 업그레이드할 때 모든 관련 CLI 및 GUI가 최신 브랜딩을 반영하여 업데이트됩니다.
- 등록된 디바이스에 대한 업그레이드 중 문제 없음
  - FTD(Firewall Threat Defense)를 업그레이드하면 FMC(Firewall Management Center)에서 최신 브랜딩으로 GUI를 업데이트합니다.
  - FMC(Firewall Management Center)를 업그레이드하면 업그레이드 후 등록된 모든 디바이스가 예상대로 연결을 복원합니다.

구성

방화벽 관리 센터의 예

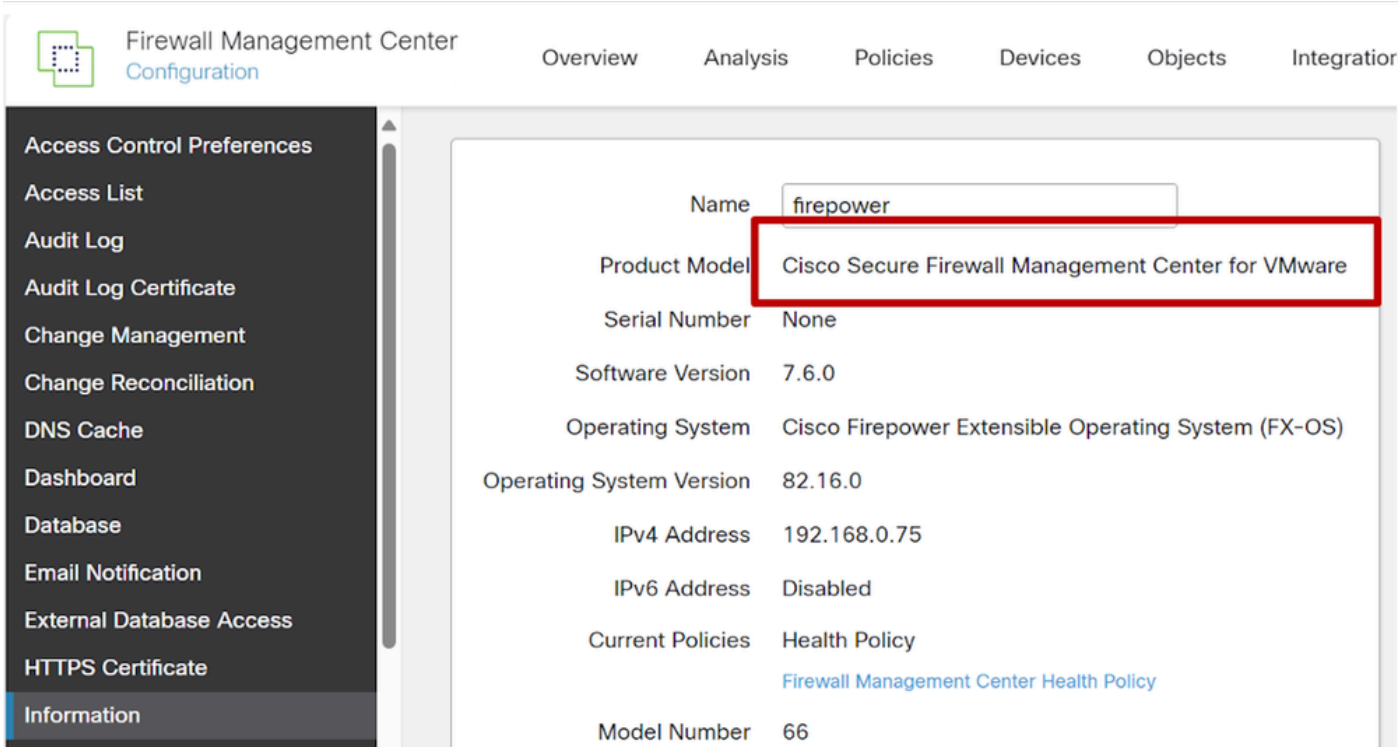
요약 상태:

- Management Center 모델 이름 앞에 Cisco 브랜딩이 추가됩니다.



구성 정보:

- Management Center 모델 이름 앞에 Cisco 브랜딩이 추가됩니다.



CLI 출력:

- 전체 모델 이름이 Cisco Secure Firewall 브랜딩과 함께 표시됩니다.

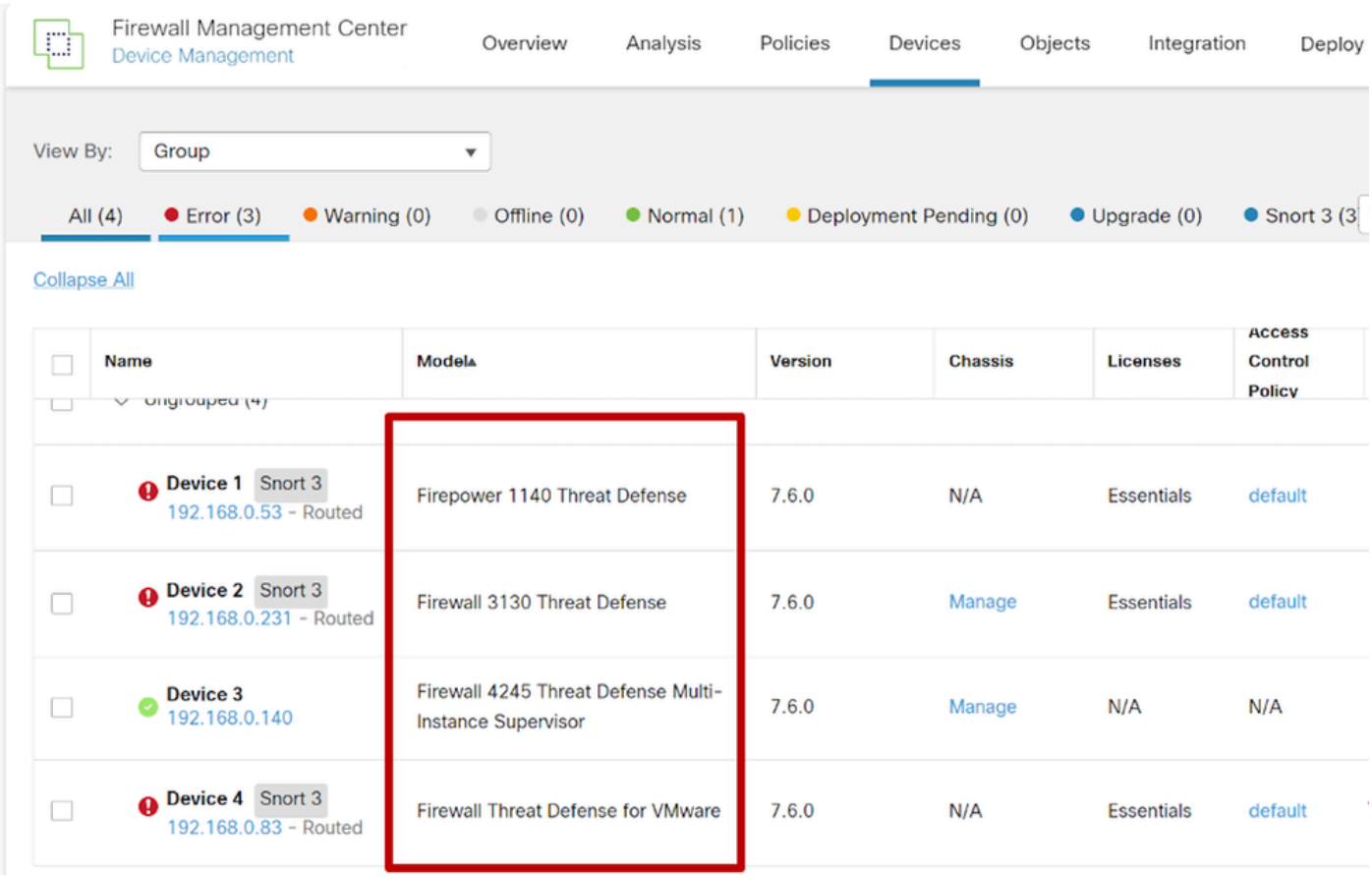
Copyright 2004-2024, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Firepower Extensible Operating System (FX-OS) v2.16.0 (build 239)
Cisco Secure Firewall Management Center for VMware v7.6.0 (build 12)

```
> show version
-----------------[ firepower ]-----------------
Model                : Cisco Secure Firewall Management Center for VMware (66)
Version 7.6.0 (Build 12)
UUID                 : c1f610d6-a0f7-11ee-9fc9-c65704d8547c
Rules update version     : 2024-02-07-001-vrt
LSP version          : lsp-rel-20240207-1539
VDB version           : 377
```

장치 관리:

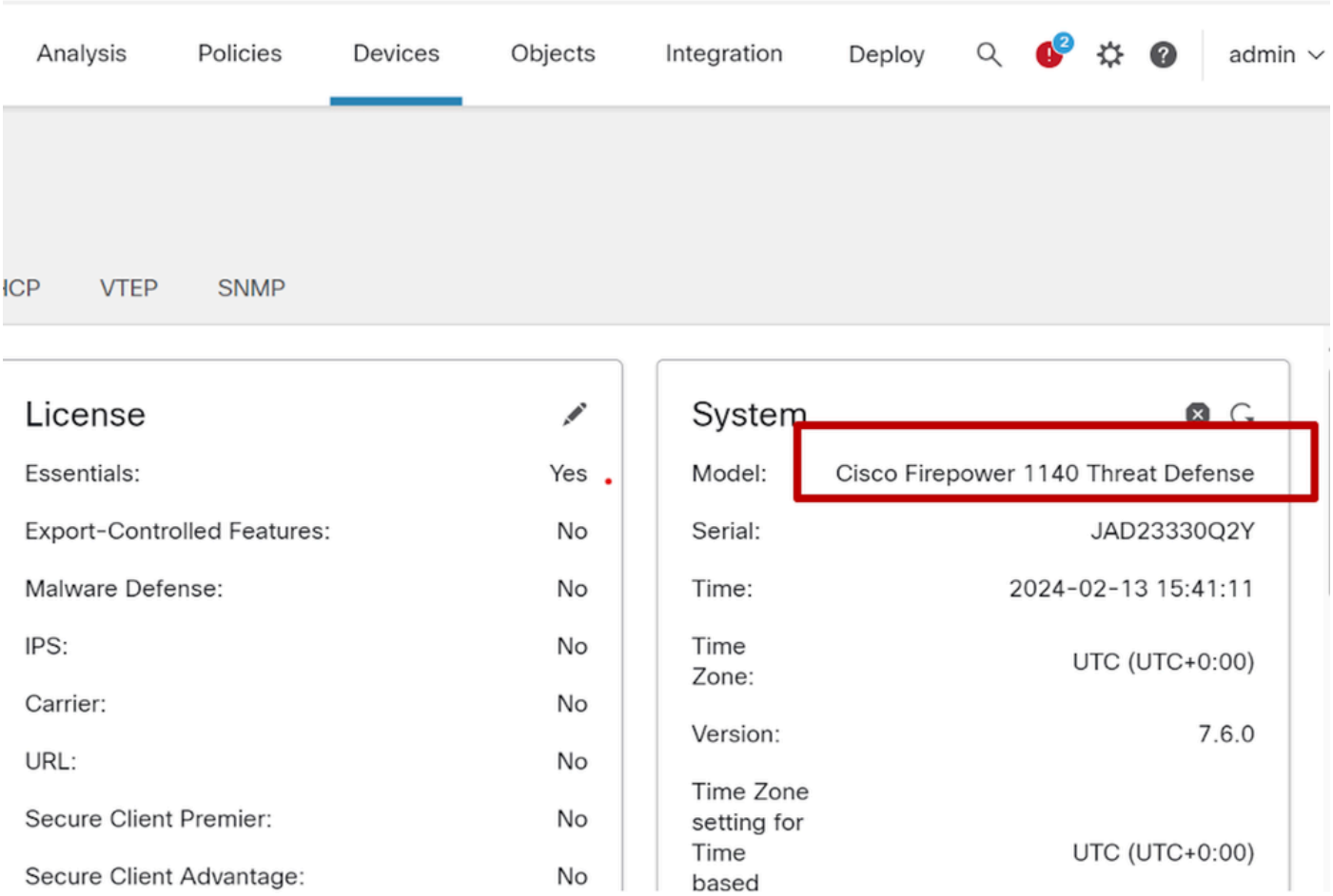
- 관리되는 디바이스는 단축된 모델 이름을 표시합니다.
- firepower(여기서는 FPR1140)와 보안 방화벽 디바이스(여기서는 3130, 4215, VMware의 FTD)가 함께 표시될 수 있습니다.



Firepower 디바이스 예

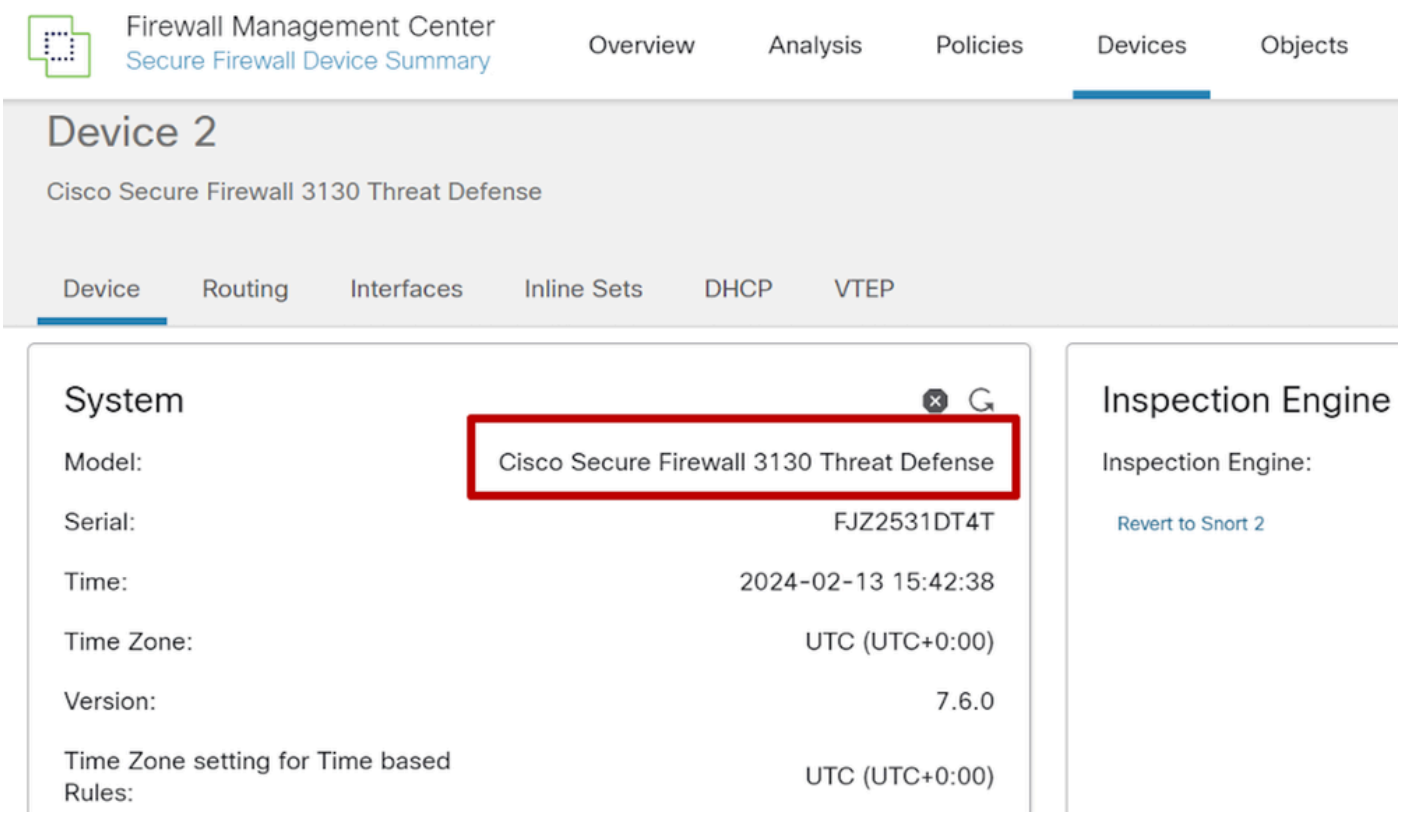
요약 상태:

- 전체 모델 이름이 디바이스 시스템 정보에 표시됨
- FP 11XX는 Firepower으로 표시됨



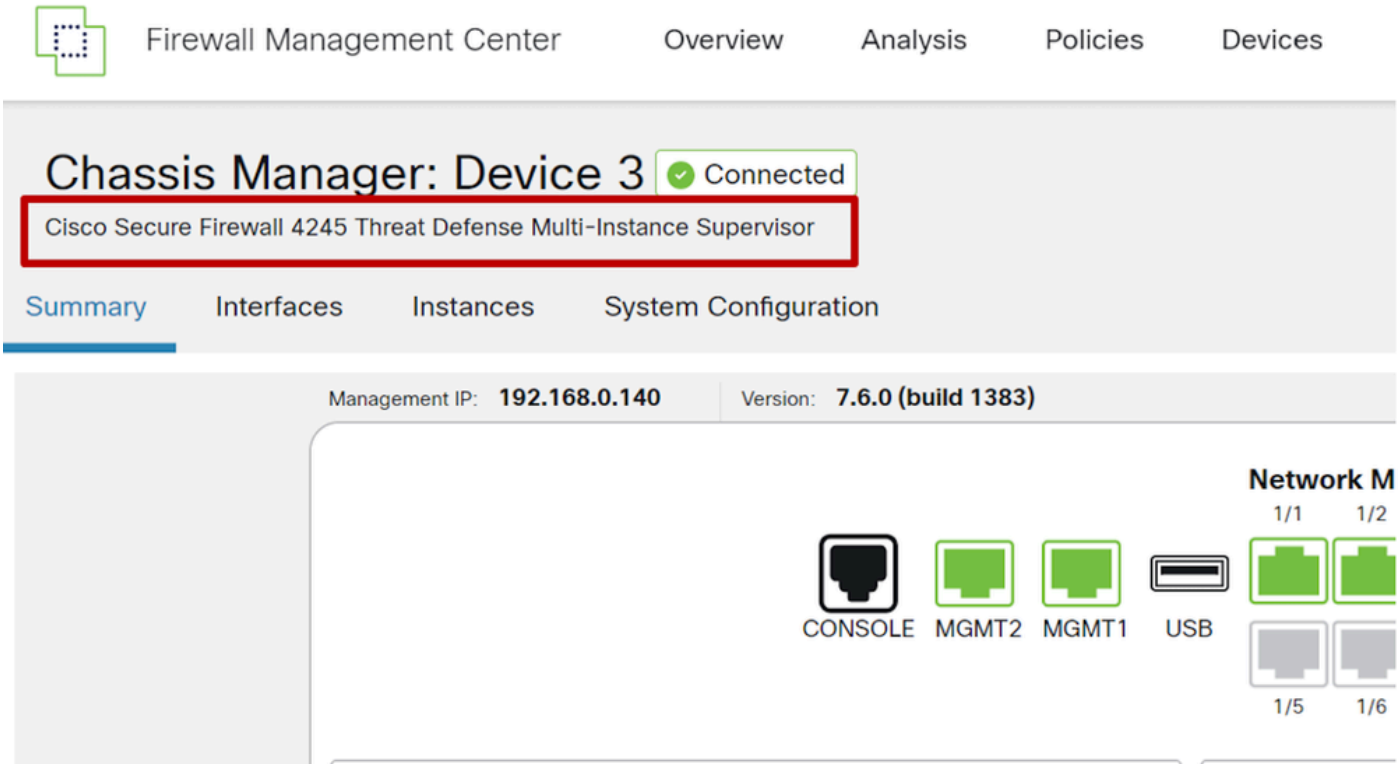
Secure Firewall Device(보안 방화벽 디바이스)에 대한 시스템 세부 정보:

- 전체 모델 이름이 디바이스 시스템 정보에 표시됩니다.
- CSF31XX는 Cisco Secure Firewall로 표시됩니다.



다중 인스턴스 모드의 3100/4200용 섀시 관리자:

- 전체 모델 이름이 디바이스 시스템 정보에 표시됩니다.
- CSF42XX 섀시는 Cisco Secure Firewall로 표시됩니다.



방화벽 위협 방어 컨피그레이션 기본값:

- 시스템 호스트 이름 기본값은 여전히 firepower,

- 실행 중인 플랫폼을 직접 참조하지 않기 때문에 firepower을 유지했습니다.
- 이는 사용자가 쉽게 변경할 수 있습니다.

IPv4를 구성하시겠습니까? (y/n) [y]:

IPv6을 구성하시겠습니까? (y/n) [y]: 네트워킹

DHCP를 통해 IPv4를 구성합니까, 아니면 수동으로 구성합니까? (dhcp/manual) [manual]:

관리 인터페이스 [192.168.0.190]의 IPv4 주소를 입력합니다. 192.168.0.231

관리 인터페이스 [255.255.255.0]에 대한 IPv4 넷마스크를 입력합니다.

관리 인터페이스 [data-interfaces]에 대한 IPv4 기본 게이트웨이를 입력합니다. 192.168.0.254

이 시스템 [firepower]에 대한 전체 호스트 이름을 입력하십시오.

쉼표로 구분된 DNS 서버 목록 또는 'none' [x.x.x.x]을 입력하십시오.

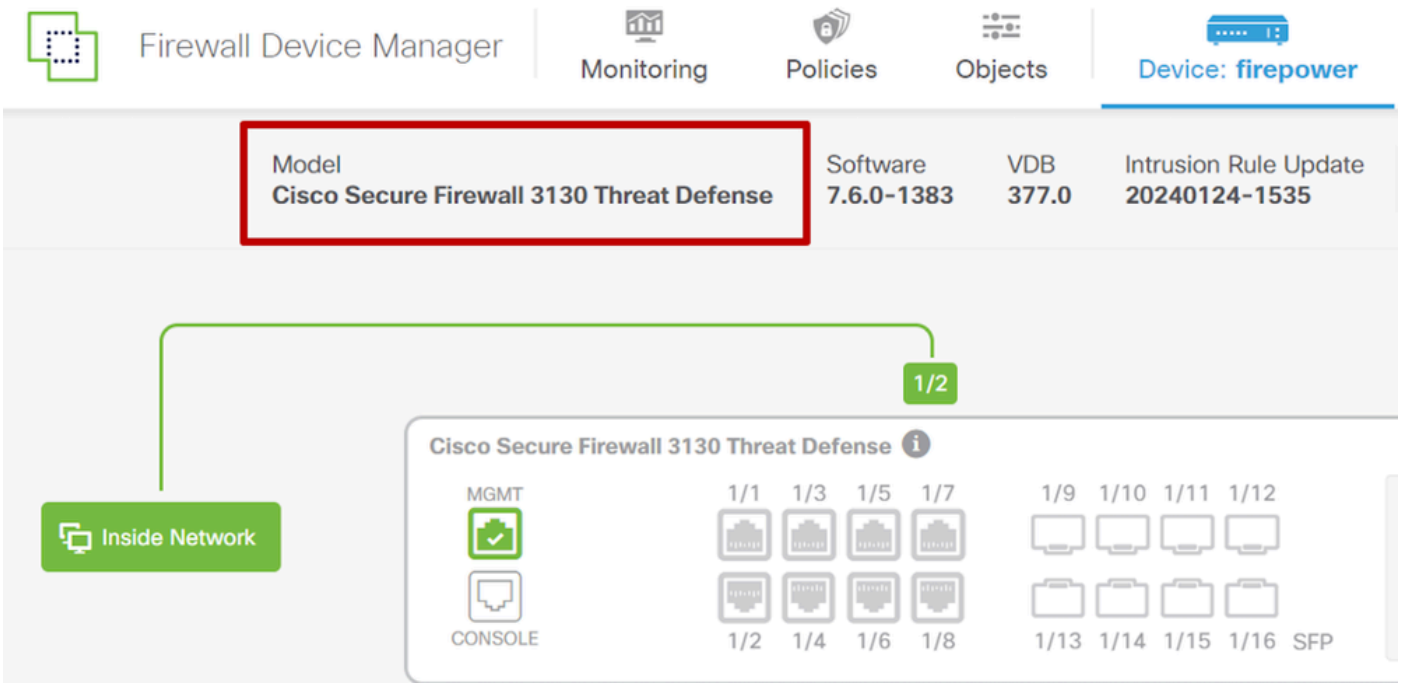
쉼표로 구분된 검색 도메인 목록 또는 'none'[]을 입력하십시오.

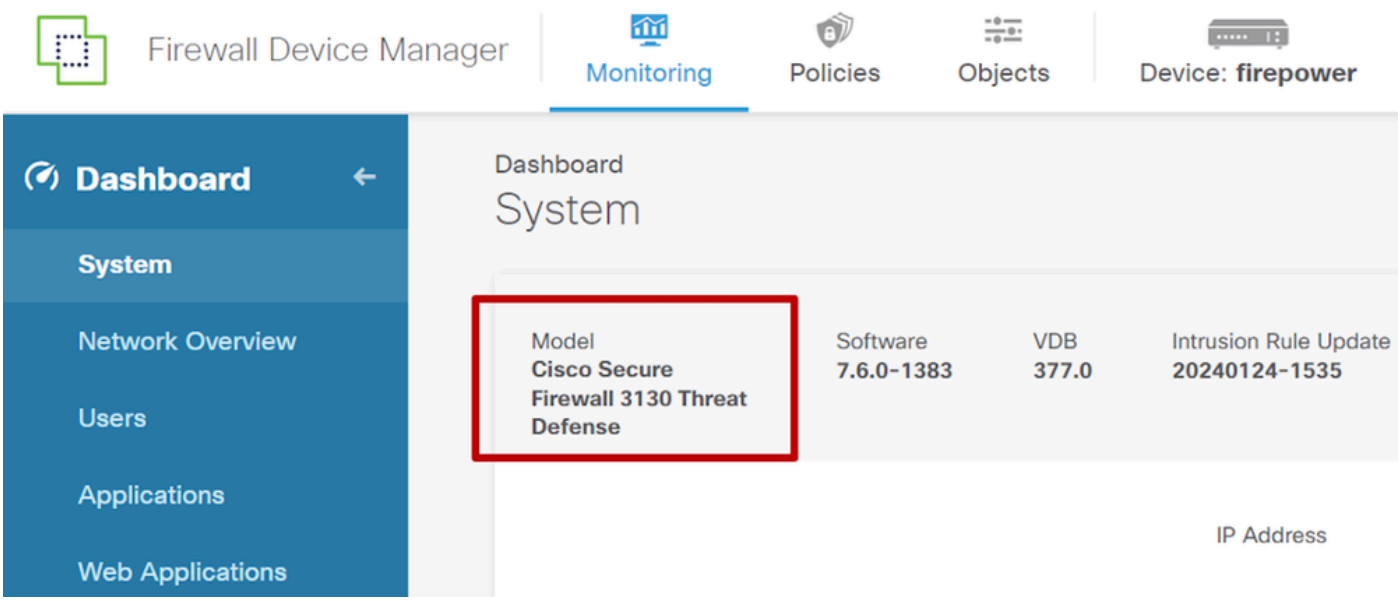
네트워킹 정보가 변경된 경우 다시 연결해야 합니다.

방화벽 장치 관리자의 예

요약 상태:

- 기본 디바이스 페이지에는 Secure Firewall 브랜딩과 함께 전체 모델 이름이 표시됩니다.





방화벽 Threat Defense CLI 출력:

- 전체 모델 이름이 Secure Firewall(보안 방화벽) 이름과 함께 표시됩니다.
- 이는 SSH 로그인에도 표시됩니다.
- show version과 같은 다른 CLI 출력에서는 Firepower 대신 Secure Firewall을 사용합니다.

디바이스를 로컬로 관리합니까? (예/아니요) [예]:

라우팅된 방화벽 모드를 구성하는 중입니다.

정책 배포 정보 업데이트

- 디바이스 컨피그레이션 추가

Secure Firewall Device Manager for Secure Firewall Threat Defense에 대해 첫 부팅 초기 컨피그레이션 단계를 성공적으로 수행했습니다.

> 버전 표시

----------[firepower]----------

모델: Cisco Secure Firewall 3130 Threat Defense(80) 버전 7.6.0(빌드 13)

UUID: 123ab4d5-e6aa-11bb-ccc7-f888d99f000d

VDB 버전: 377

방화벽 장치 관리자 시스템 모니터:

- 시스템 모니터링 대시보드에서도 올바른 모델 이름을 사용합니다.

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.