Uitgangen van Rebranding-apparaten naar Cisco Secure Firewall begrijpen

Inhoud

Inleiding

Dit document beschrijft inzicht in de uitvoer van het Rebranding-apparaat naar Cisco Secure Firewall.

Voorwaarden

Achtergrondinformatie

- De weergegeven apparaatnamen komen nu overeen met andere branding materialen
- Dit zorgt voor een sterker merk en een meer eenvoudige gebruikerservaring
- Geen functionele gevolgen voor platforms; alleen de tekst is gewijzigd.
- Oudere FTD-hardwareplatforms (FPR1010/11XX, FPR41XX, FPR93XX) maken nog steeds gebruik van FirePOWER-branding
- Sommige systeemfouten en componentnamen kunnen nog steeds vuurkracht gebruiken

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Next Gen Firewall(NGFW)-portfolio

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Firepower Management Center (FMC) versie 7.6.0

- Firepower Device Manager (FDM) versie 7.6.0
- All Virtual Firepower Threat Defence (FTD) versie 7.6.0
- Cisco Secure-firewall 31XX.42XX

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Functiebeschrijving

Hoe het werkt:

- Volledige modelnamen en korte modelnamen voor CSF31XX, CSF42XX, Firewall Threat Defence (FTD) Virtual, en alle platforms van Firewall Management Center (FMC) bevatten Cisco Secure Firewall-branding.
- De CSF31X FDM-software is nu SFDM, Secure Firewall Device Manager.
- Deze optie heeft geen functionele componenten.
- Er zijn geen configuratieopties voor deze functie.

Upgraden:

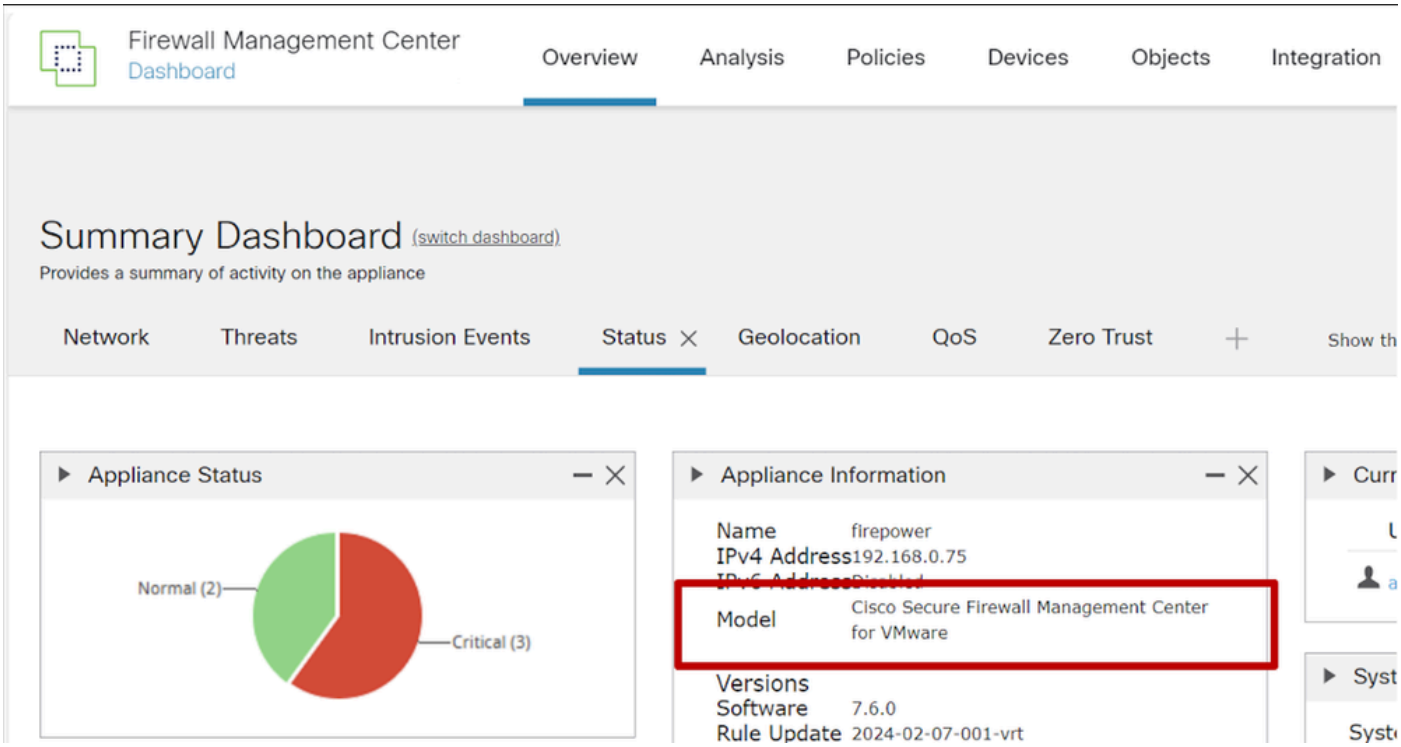
- Wanneer u een upgrade uitvoert naar Secure Firewall 7.6, worden alle relevante CLI's en GUI's bijgewerkt om de huidige branding weer te geven.
- Geen problemen tijdens upgrade voor geregistreerde apparaten
    - Als Firewall Threat Defence (FTD) is bijgewerkt, werkt Firewall Management Center (FMC) zijn GUI bij met de huidige merknaam.
    - Als Firewall Management Center (FMC) is bijgewerkt, herstellen alle geregistreerde apparaten de connectiviteit na de upgrade zoals verwacht.

Configureren

Firewall Management Center - voorbeelden

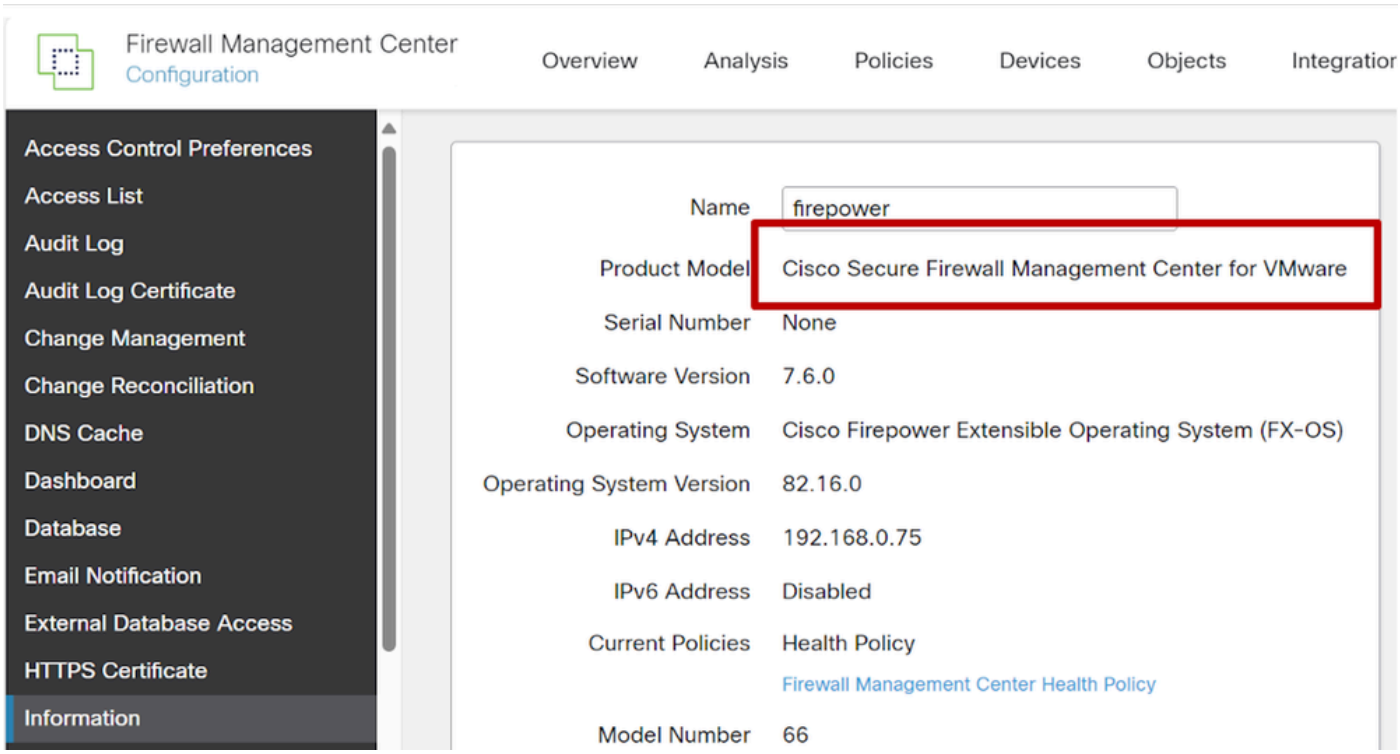
Samenvattingsstatus:

- Bij de modelnaam Management Center is de Cisco-branding al gestart.



Configuratiegegevens:

- Bij de modelnaam Management Center is de Cisco-branding al gestart.



CLI-uitvoer:

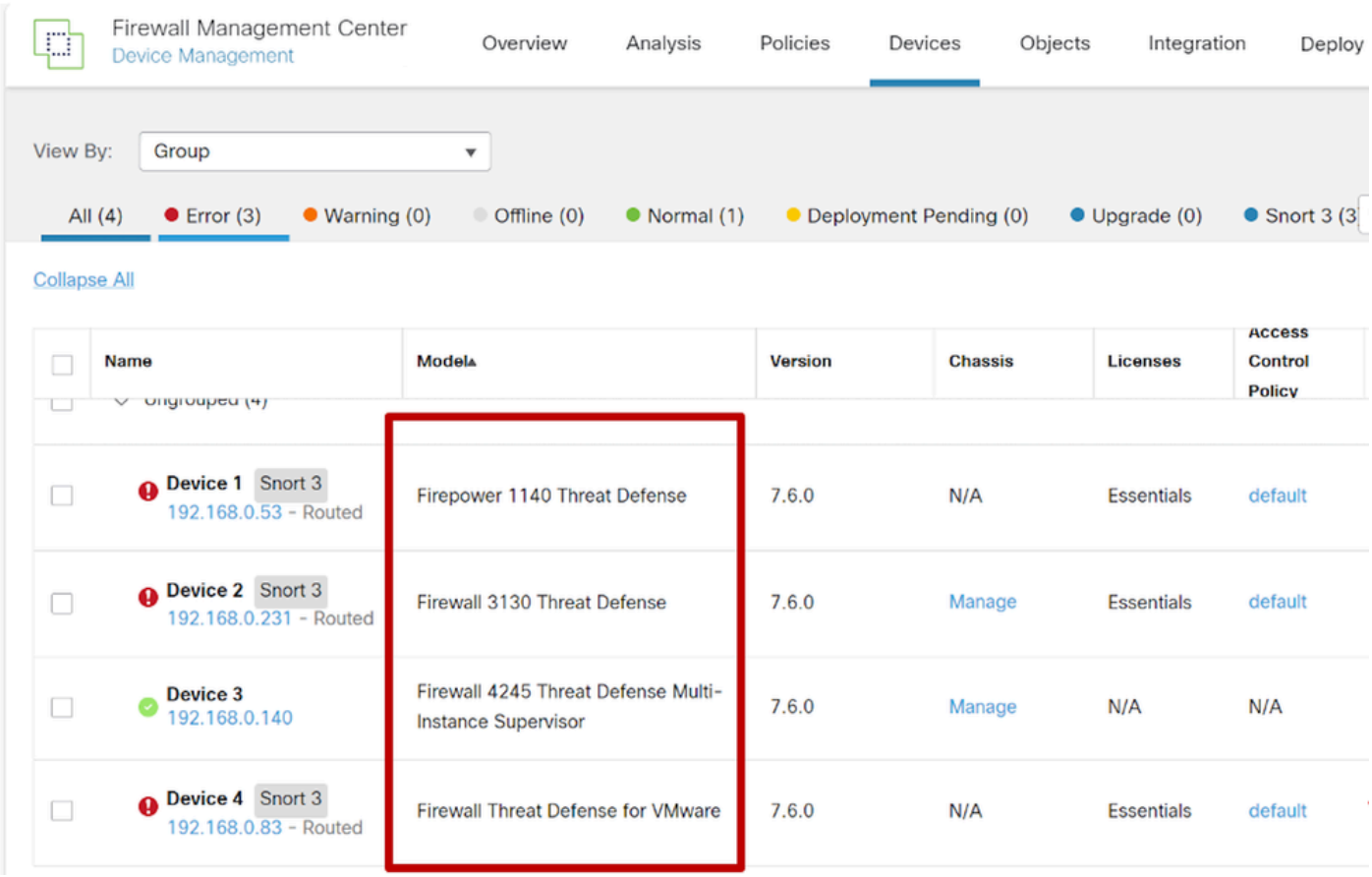
- De volledige modelnaam wordt weergegeven met het merk Cisco Secure Firewall.

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
```

Apparaatbeheer:

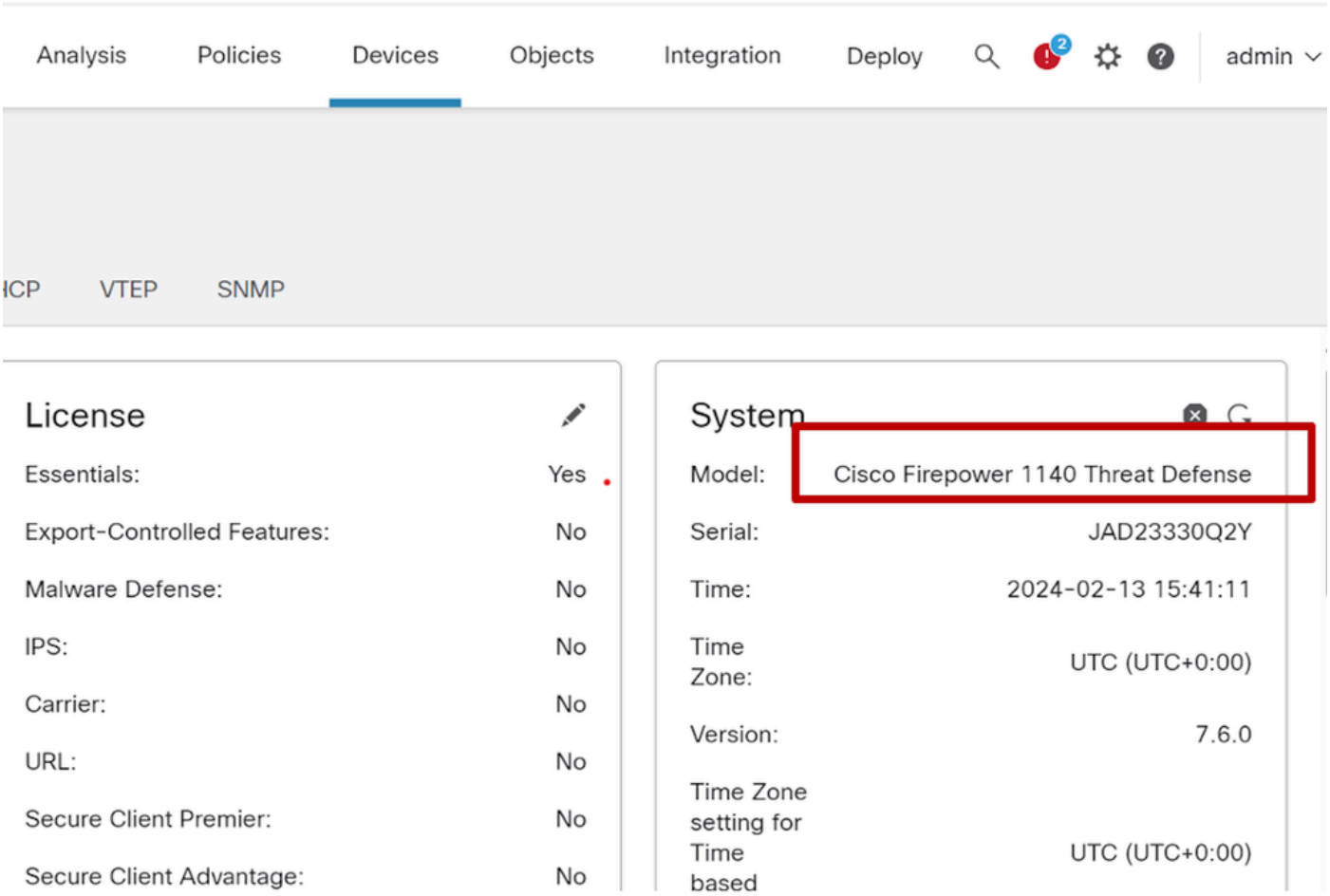
- Beheerde apparaten tonen verkorte modelnamen.
- Zowel Firepower (hier FPR1140) als Secure Firewall Devices (hier, 3130, 4215 en FTD op VMware) kunnen samen worden weergegeven.



Voorbeeld van FirePOWER-apparaten

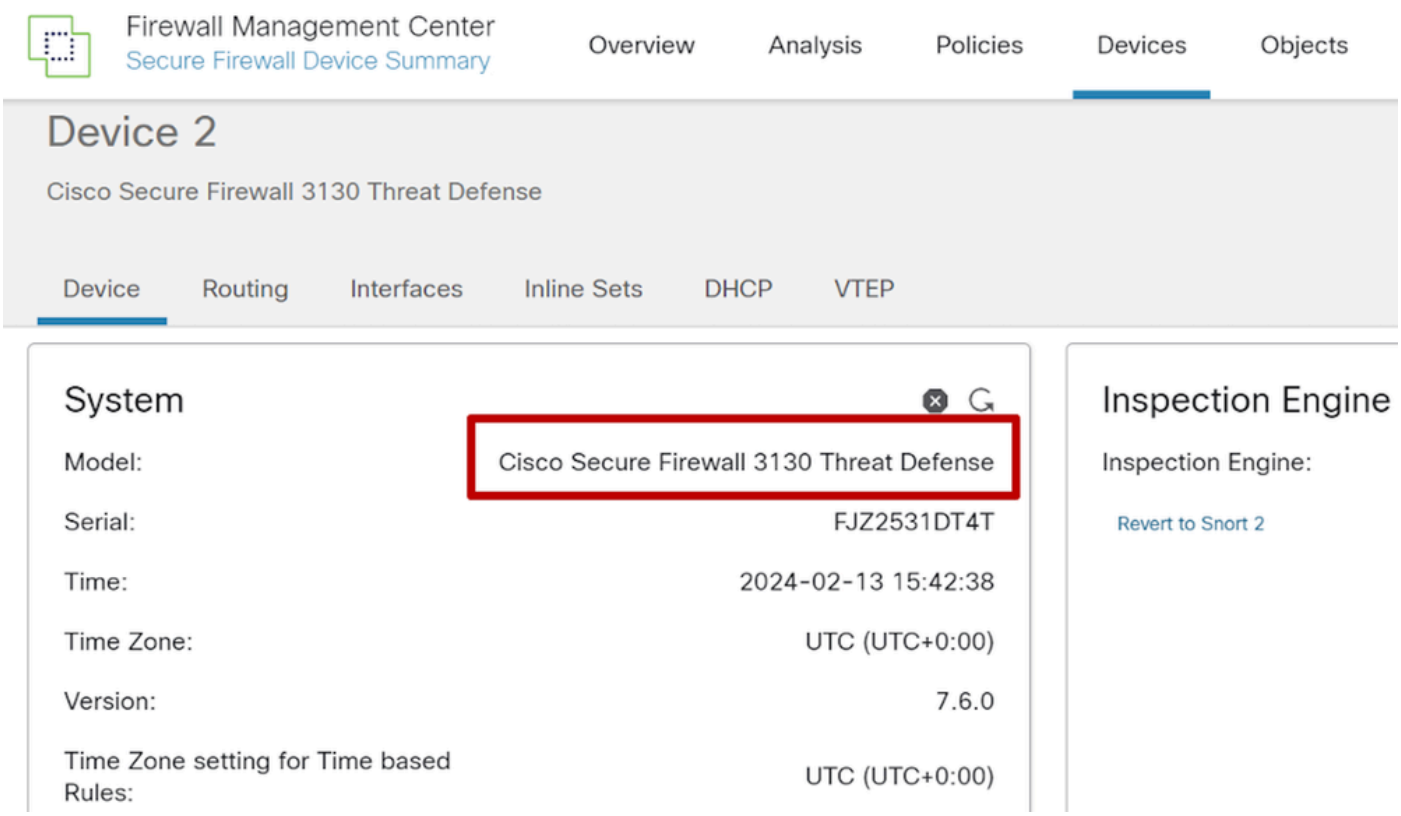
Samenvatting status:

- De volledige modelnaam wordt in de informatie van het apparatensysteem getoond
- FP 11XX wordt weergegeven als FirePOWER



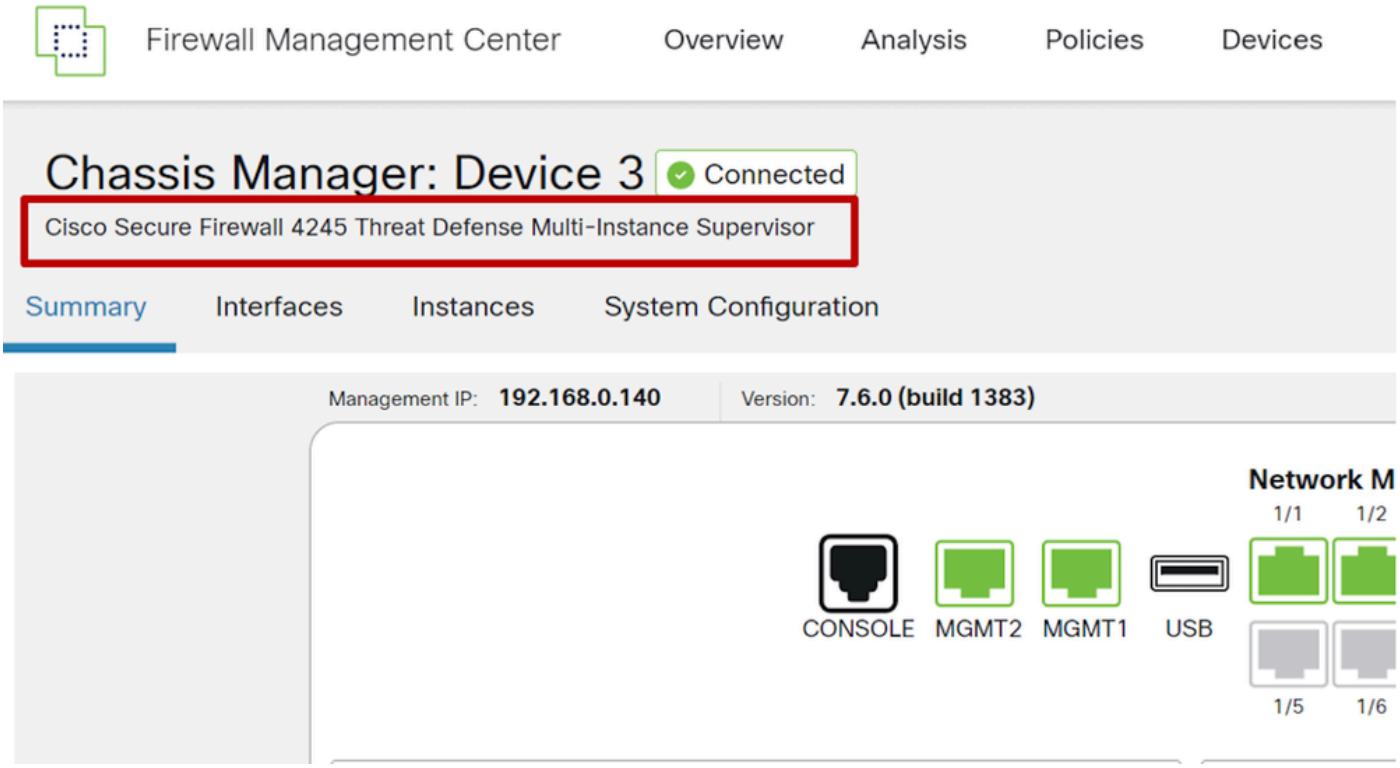
Systeemgegevens voor Secure Firewall Device:

- De volledige modelnaam wordt in de informatie van het apparatensysteem getoond.
- CSF31XX wordt weergegeven als Cisco Secure Firewall.



Chassis Manager voor 3100/4200 in multi-instantie modus:

- De volledige modelnaam wordt in de informatie van het apparatensysteem getoond.
- Het CSF42XX-chassis wordt weergegeven als Cisco Secure Firewall.



Configuratie-standaardwaarden voor Firewall Threat Defense:

- Systeem hostname standaard is nog steeds vuurkracht,

- We hielden vuurkracht, omdat dit niet direct verwijst naar het loopplatform.
- Dit kan eenvoudig door de gebruiker worden gewijzigd.

Wilt u IPv4 configureren? (j/n) [y]:

Wilt u IPv6 configureren? (j/n) [y]: n

IPv4 via DHCP of handmatig configureren? (DHCP/handleiding) [handmatig]:

Voer een IPv4-adres in voor de beheerinterface [192.168.0.190]: 192.168.0.231

Voer een IPv4-netmasker in voor de beheerinterface [25.255.255.0]:

Voer de IPv4-standaardgateway in voor de beheerinterface [data-interfaces]: 192.168.0.254

Voer een volledig gekwalificeerde hostnaam in voor dit systeem [firepower]:

Voer een komma-gescheiden lijst in van DNS-servers of 'geen' [x.x.x.x]:

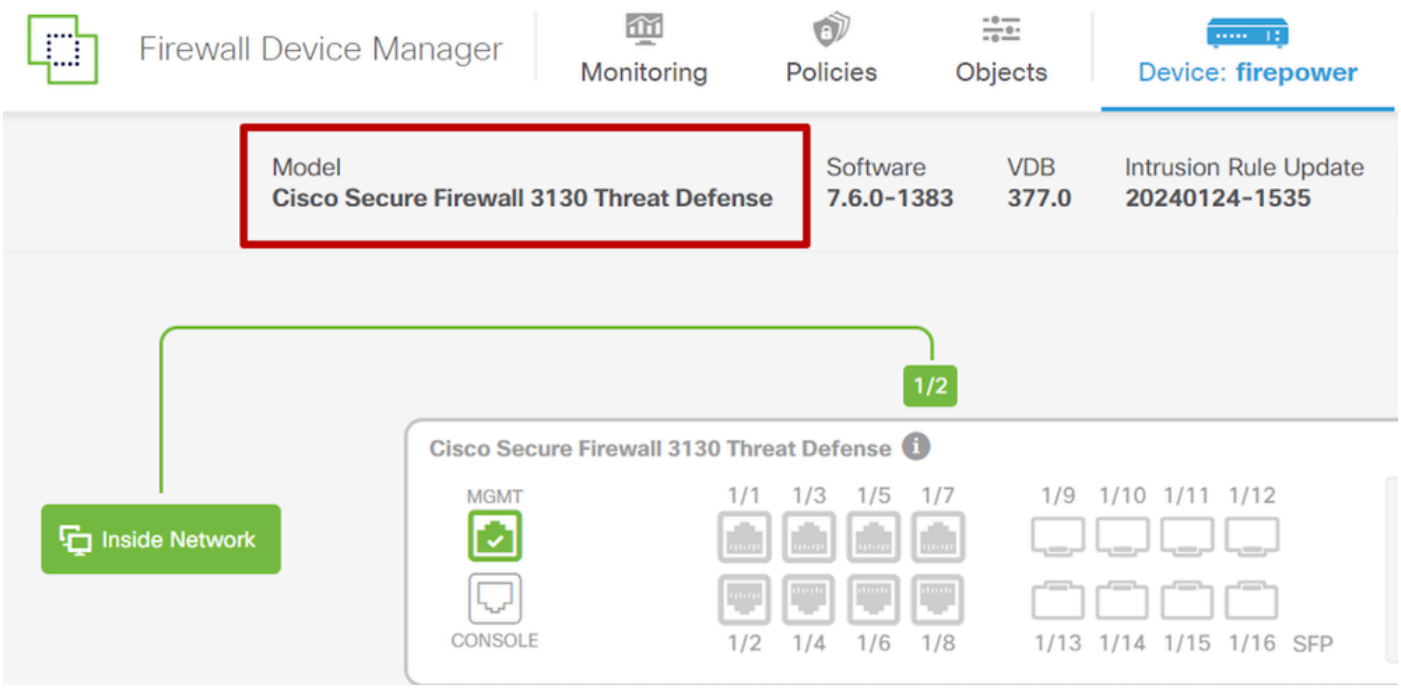
Voer een door komma's gescheiden lijst in van zoekdomeinen of 'geen' []:

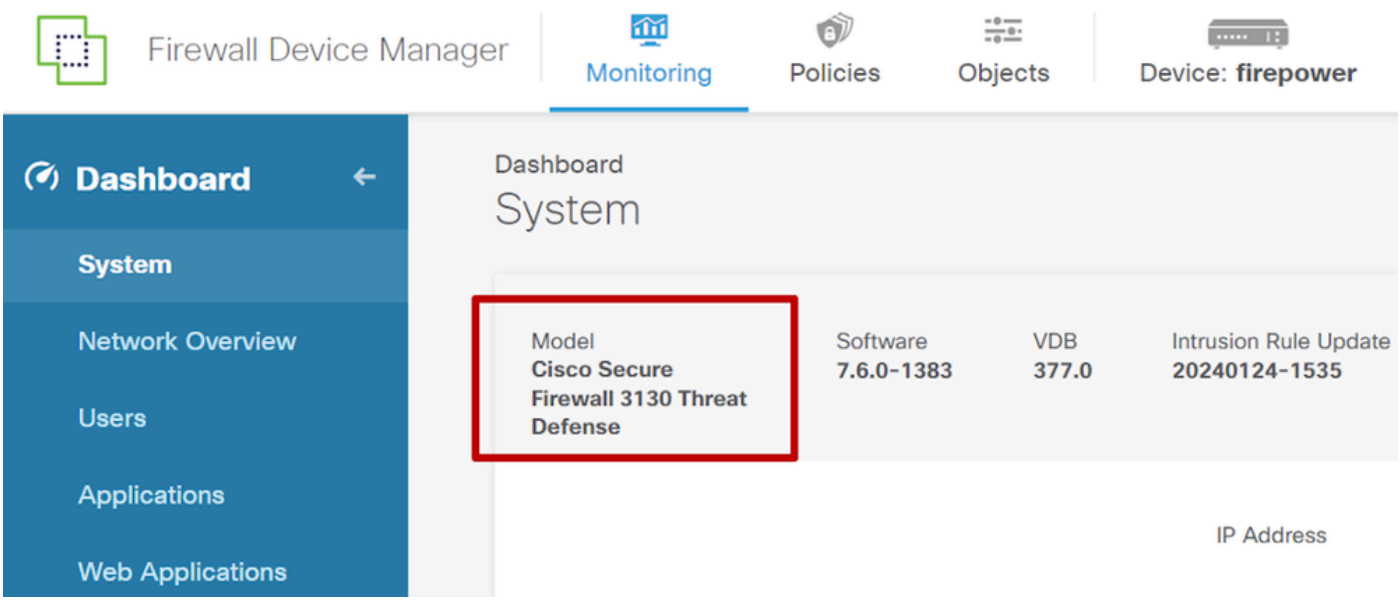
Als uw netwerkinformatie is gewijzigd, moet u opnieuw verbinding maken.

Voorbeelden van Firewall Device Manager

Samenvattingsstatus:

- De belangrijkste apparatenpagina toont volledige modelnaam met het Veilige Brandmerken van de Firewall.





CLI-uitvoer van Firewall Threat Defence:

- De volledige modelnaam wordt weergegeven met de naam Secure Firewall.
- Dit wordt ook getoond op SSH logins.
- Andere CLI-uitvoer, zoals showversie, gebruikt Secure Firewall in plaats van Firepower.

Het apparaat lokaal beheren? (ja/neen) [ja]:

De firewallmodus voor routing configureren.

Informatie over beleidsimplementatie bijwerken

- apparaatconfiguratie toevoegen

Succesvol uitgevoerde eerste configuratie stappen voor Secure Firewall Device Manager voor Secure Firewall Threat Defence.

> versie tonen

----------[vuurkracht]----------

Model : Cisco Secure Firewall 3130 Threat Defence (80) versie 7.6.0 (Build 13)

UUID : 123ab4d5-e6a-11bb-cc7-f888d99f000d

VDB-versie : 377

Firewall Device Manager System Monitor:

- Het dashboard van de systeemcontrole gebruikt ook correcte modelnaam.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.