Bepaal de actieve snortversie die wordt uitgevoerd bij Firepower Threat Defence (FTD)

Inhoud

Inleiding

Dit document beschrijft de stappen om de actieve gescande versie te bevestigen die wordt uitgevoerd door Cisco Firepower Threat Defence (FTD) wanneer deze wordt beheerd door Cisco Firepower Device Manager (FDM), het Cisco Firepower Management Center (FMC) of de Cisco Defense Orchestrator (CDO).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Firepower Management Center (FMC)
- Cisco Firepower Threat Defence (FTD)
- Cisco Firepower Device Manager (FDM)
- Cisco Defense Orchestrator (CDO)

Gebruikte componenten

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

- Cisco Firepower Threat Defence (FTD) v6.7.0 en 7.0.0
- Cisco Firepower Management Center (FMC) v6.7.0 en 7.0.0
- Cisco Defense Orchestrator (CDO)

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.

Achtergrondinformatie

SNORT® Inbraakpreventiesysteem heeft officieel Snort 3 gelanceerd, een ingrijpende upgrade die

verbeteringen en nieuwe functies bevat die de prestaties, snellere verwerking, verbeterde schaalbaarheid voor uw netwerk verbeteren, en een reeks van meer dan 200 plugins zodat gebruikers een aangepaste set-up voor hun netwerk kunnen maken.

De voordelen van Snort 3 omvatten, maar zijn niet beperkt tot:

- Verbeterde prestaties
- Verbeterde SMBv2-inspectie
- Nieuwe mogelijkheden voor scriptdetectie
- HTTP/2-inspectie
- Aangepaste regelgroepen
- Syntaxis die aangepaste inbraakregels gemakkelijker te schrijven maakt
- Redenen voor 'zou hebben laten vallen' inline resultaten in inbraakgebeurtenissen
- Geen snelle herstart wanneer wijzigingen worden geïmplementeerd in het VDB-, SSL-beleid, aangepaste toepassingsdetectoren, bronnen van inkapseling van portal-identiteit en detectie van TLS-serveridentiteit
- Verbeterde servicemogelijkheid, dankzij korte 3-specifieke telemetriegegevens die naar Cisco Success Network zijn verzonden en betere logs voor probleemoplossing

De ondersteuning voor Snort 3.0 werd geïntroduceerd voor de 6.7.0 Cisco Firepower Threat Defence (FTD), net toen de FTD wordt beheerd via Cisco Firepower Device Manager (FDM).

Opmerking: voor nieuwe 6.7.0 FTD-implementaties die worden beheerd door FDM, is Snort 3.0 de standaard inspectie-engine. Als u de FTD van een oudere release naar 6.7 upgradt, blijft Snort 2.0 de actieve inspectie-engine, maar u kunt switches naar Snort 3.0.

Opmerking: voor deze release ondersteunt Snort 3.0 geen virtuele routers, tijdgebaseerde toegangscontroleregels of de decryptie van TLS 1.1 of lagere verbindingen. Schakel Snort 3.0 alleen in als u deze functies niet nodig hebt.

Firepower versie 7.0 introduceerde de ondersteuning Snort 3.0 voor de FirePOWER Threat Defence-apparaten die worden beheerd door zowel Cisco FDM als door het Cisco Firepower Management Center (FMC).

Opmerking: voor nieuwe 7.0 FTD-implementaties is Snuit 3 nu de standaard inspectie-engine. Upgradeimplementaties blijven Snuit 2 gebruiken, maar u kunt op elk moment switches.

Waarschuwing: u kunt vrijelijk switches tussen Snort 2.0 en 3.0, zodat u uw verandering kunt terugdraaien indien nodig. Het verkeer wordt onderbroken wanneer u versies switches.

Waarschuwing: voordat u overgaat op switch 3, wordt u ten zeerste aangeraden de configuratiehandleiding van Firepower Management Center Snort 3 te lezen en te begrijpen. Let vooral op functiebeperkingen en migratie-instructies. Hoewel de upgrade naar Snort 3 is ontworpen

---

voor minimale impact, functies niet precies in kaart te brengen. Het plan en de voorbereiding vóór de upgrade kunnen u helpen ervoor te zorgen dat het verkeer wordt verwerkt zoals verwacht.

Bepaal de actieve gescande versie die op FTD wordt uitgevoerd

FTD Command Line Interface (CLI)

Om de actieve snortversie te bepalen die op een FTD loopt, log in aan de FTD CLI en voer de opdracht **show snort3 status uit**:

Voorbeeld 1: Als er geen uitvoer wordt weergegeven, voert de FTD Snort 2 uit.

```
<#root>

>

show snort3 status


>
```

Voorbeeld 2: Wanneer de uitvoer **"Actuele uitvoering Snort 2"** toont, voert de FTD Snort 2 uit.

```
<#root>

>

show snort3 status

Currently running Snort 2
```

Voorbeeld 3: Wanneer de uitvoer **"Momenteel lopende Sort 3"** toont, voert de FTD Sort 3 uit.

```
<#root>

>

show snort3 status

Currently running Snort 3
```

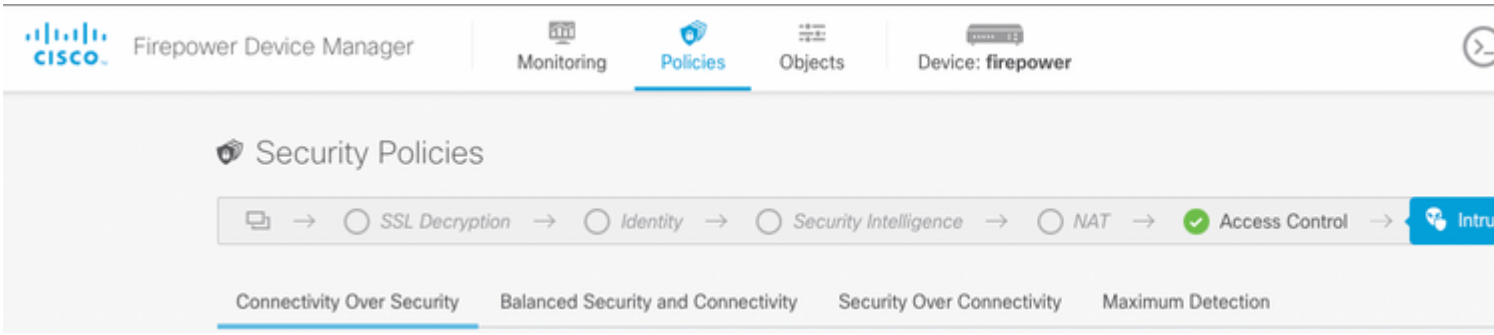
FTD beheerd door Cisco FDM

Ga verder met de volgende stappen om de actieve gescande versie te bepalen die wordt uitgevoerd op een FTD die wordt beheerd door Cisco FDM:

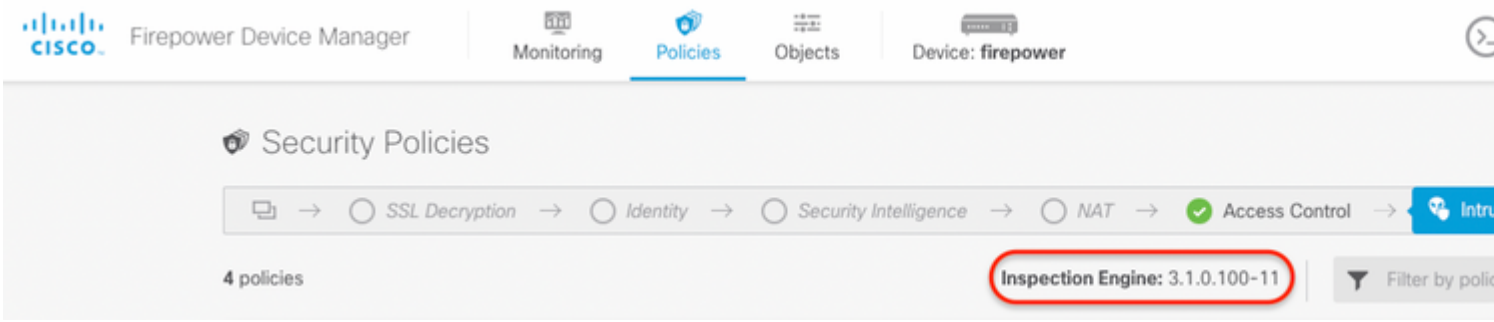
1. Log in op Cisco FTD via de FDM-webinterface.

2. Selecteer **Beleid** in het hoofdmenu.
3. Selecteer vervolgens het tabblad **Indringing**.
4. Raadpleeg het gedeelte **Snortversie** of **Inspection Engine** om te bevestigen dat de Snortversie actief is in het FTD.

Voorbeeld 1: De FTD draait snort versie 2.



Voorbeeld 2: De FTD draait snort versie 3.

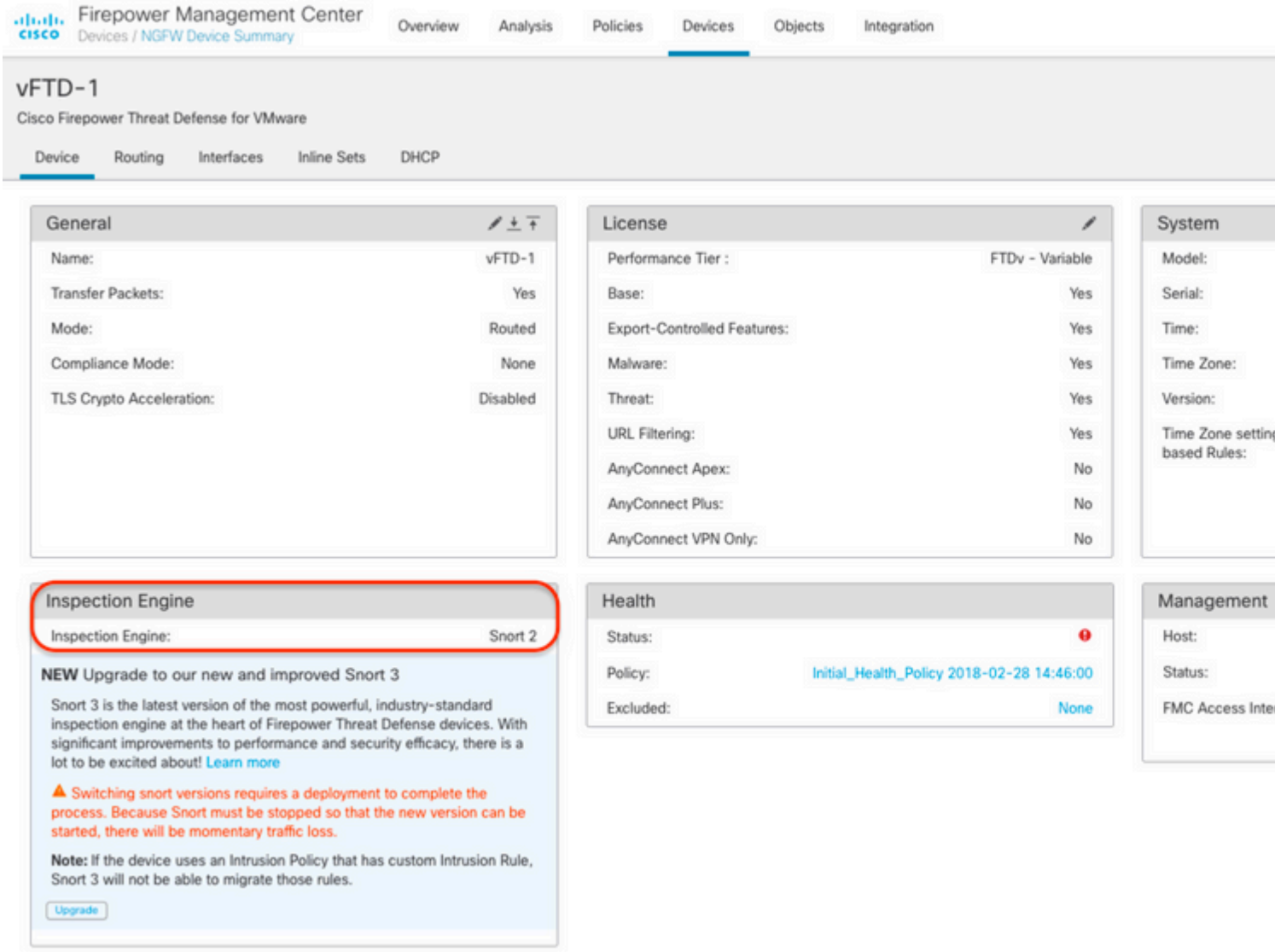


FTD beheerd door de Cisco VCC

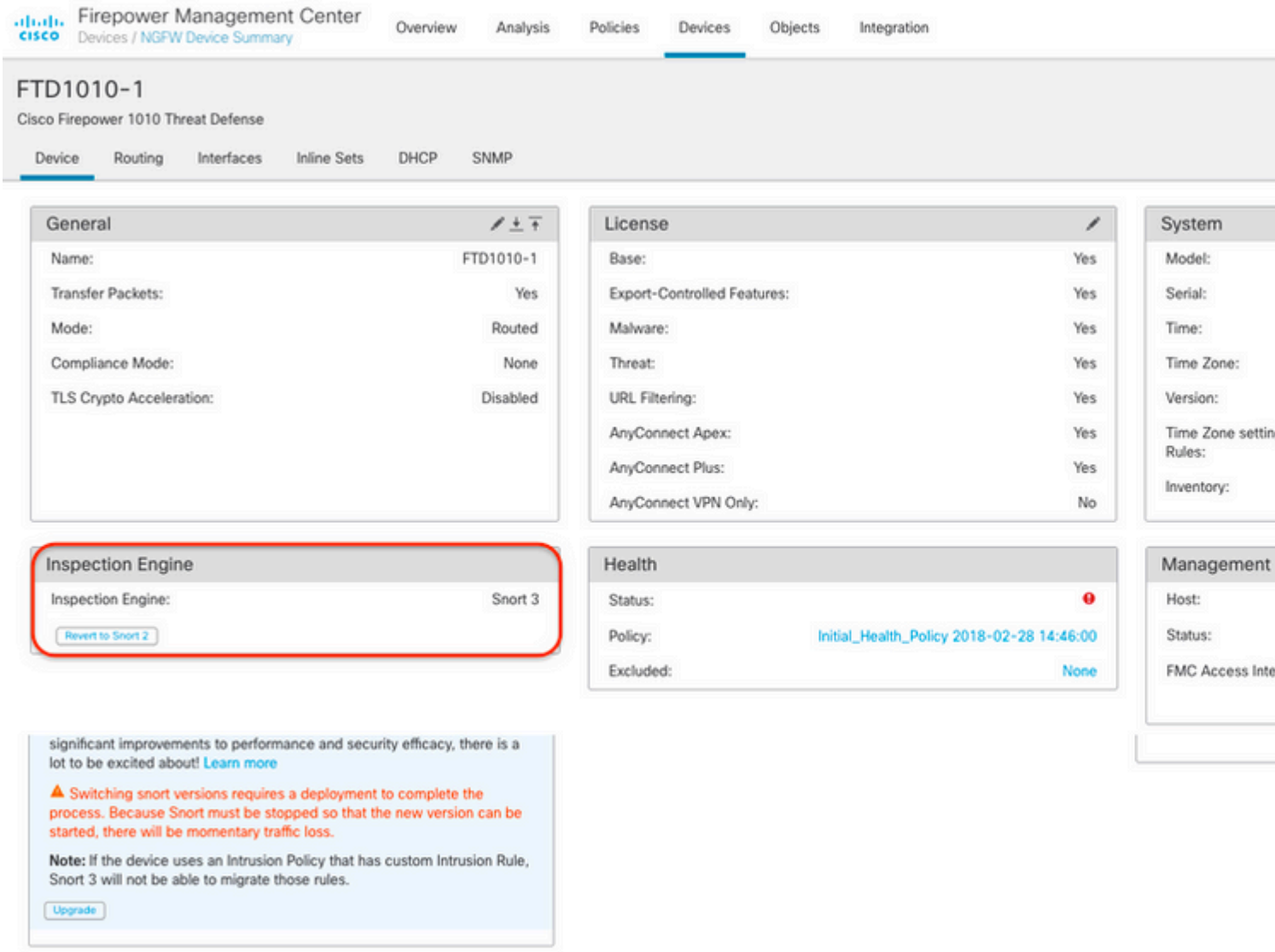
Ga verder met de volgende stappen om te bepalen welke actieve snortversie wordt uitgevoerd op een FTD die wordt beheerd door het VCC van Cisco:

1. Log in op de Cisco FMC-webinterface.
2. Selecteer in het menu **Apparaten** de optie **Apparaatbeheer**.
3. Selecteer vervolgens het juiste FTD-apparaat.
4. Klik op het pictogram potlood **bewerken**.
5. Selecteer het tabblad **Apparaat** en kijk in het gedeelte **Inspection Engine** om de gescande versie te bevestigen die in het FTD actief is:

Voorbeeld 1: De FTD draait snort versie 2.



Voorbeeld 2: De FTD draait snort versie 3.

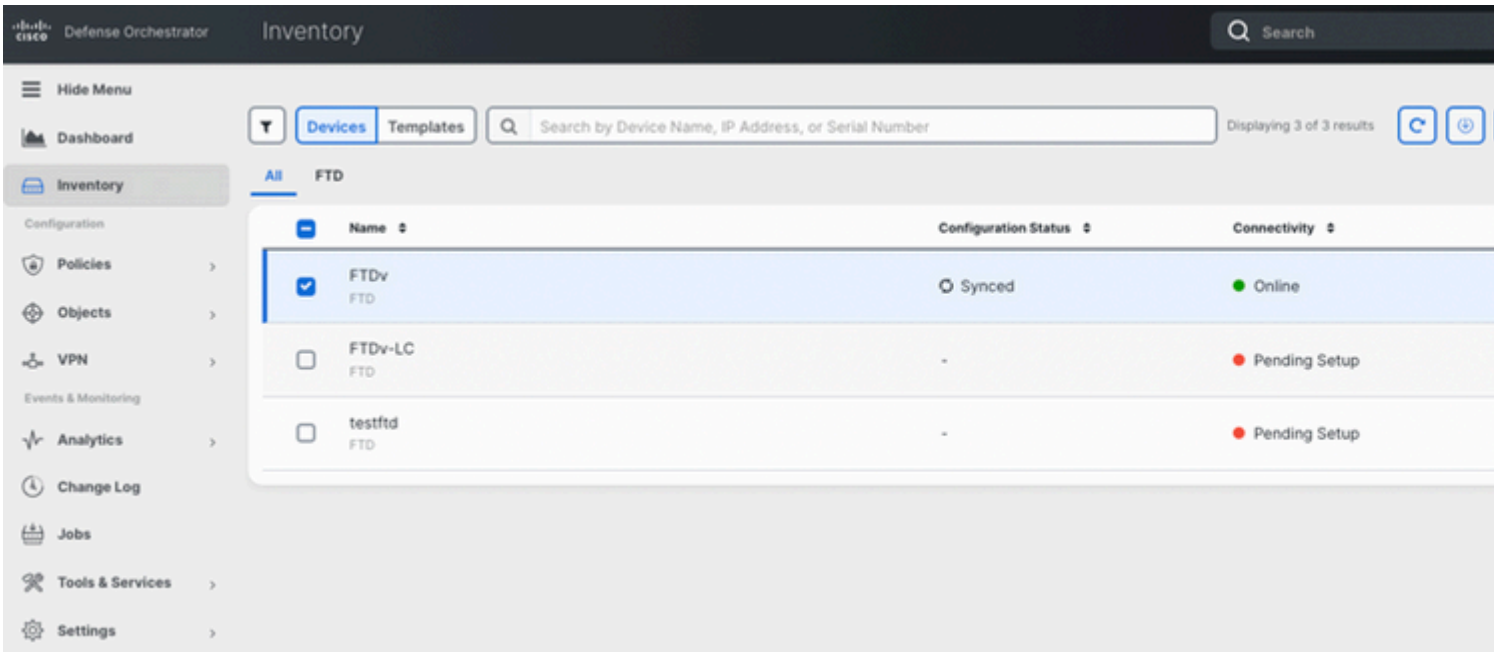


FTD beheerd door de Cisco CDO

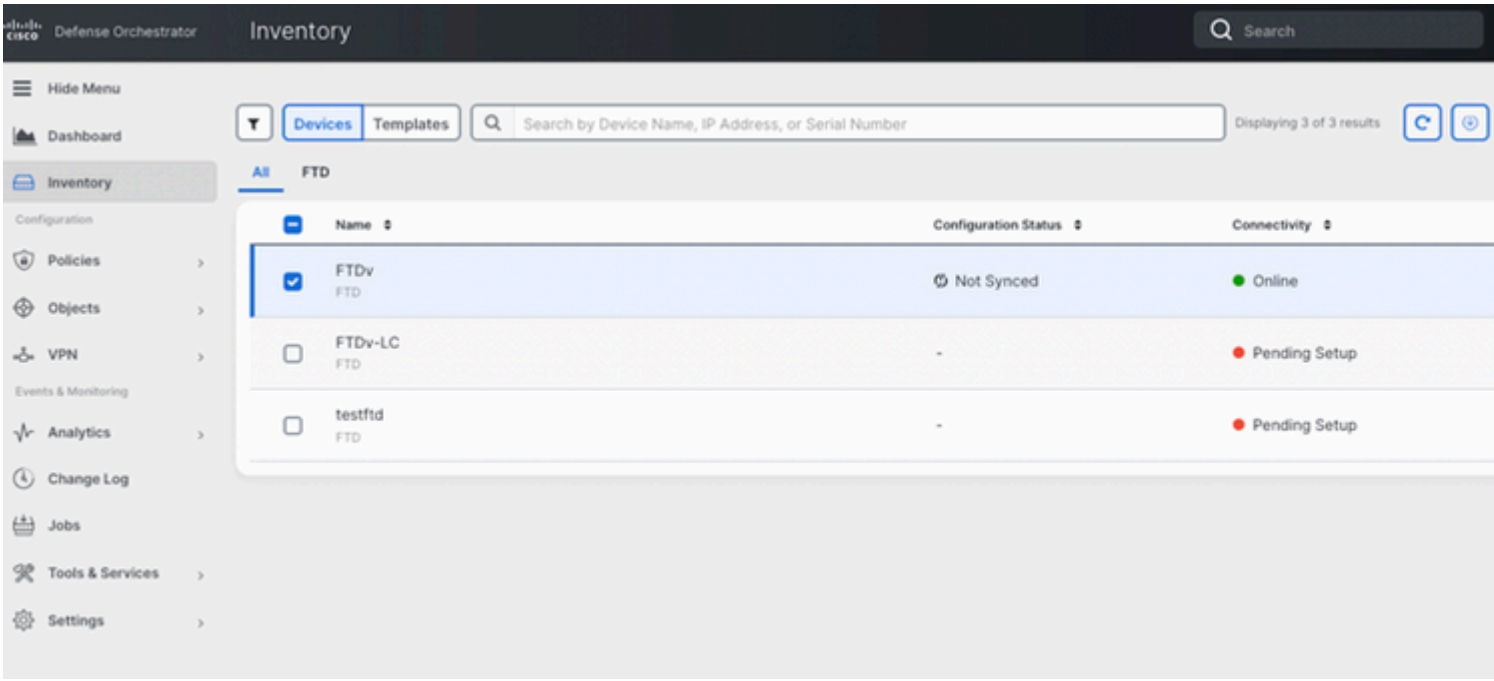
Ga verder met de volgende stappen om te bepalen welke actieve snortversie op een FTD wordt uitgevoerd die wordt beheerd door Cisco Defense Orchestrator:

1. Meld u aan bij de Cisco Defense Orchestrator-webinterface.
2. Selecteer in het menu **Inventaris** het juiste FTD-apparaat.
3. In het gedeelte **Apparaatgegevens** zoekt u naar **Snelversie**:

Voorbeeld 1: De FTD draait snort versie 2.



Voorbeeld 2: De FTD draait snort versie 3.



Gerelateerde informatie

- Cisco FirePOWER Releaseopmerkingen, versie 6.7.0
- Cisco Firepower release Notes versie 7.0
- Snort 3-website
- Technische ondersteuning en documentatie â€“ Cisco Systems

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.