Bestimmen Sie die aktive Snort-Version, die auf Firepower Threat Defense (FTD) ausgeführt wird.

Inhalt

Einleitung

In diesem Dokument werden die Schritte zur Bestätigung der aktiven Snort-Version beschrieben, die von Cisco Firepower Threat Defense (FTD) ausgeführt wird, wenn diese vom Cisco Firepower Device Manager (FDM), dem Cisco Firepower Management Center (FMC) oder dem Cisco Defense Orchestrator (CDO) verwaltet wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco FirePOWER Management Center (FMC)
- Cisco Firepower Threat Defense (FTD)
- Cisco FirePOWER-Gerätemanager (FDM)
- Cisco Defense Orchestrator (CDO)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

SNORT® Intrusion Prevention System hat Snort 3 offiziell eingeführt, ein umfassendes Upgrade, das Verbesserungen und neue Funktionen bietet, die die Leistung, die schnellere Verarbeitung, die verbesserte Skalierbarkeit für Ihr Netzwerk und eine Reihe von über 200 Plug-ins verbessern, sodass Benutzer eine benutzerdefinierte Einrichtung für ihr Netzwerk erstellen können.

Die Vorteile von Snort 3 umfassen u. a.:

- Verbesserte Leistung
- Verbesserte SMBv2-Prüfung
- Neue Funktionen zur Skripterkennung
- HTTP/2-Inspektion
- Benutzerdefinierte Regelgruppen
- Syntax, die das Schreiben benutzerdefinierter Angriffsregeln erleichtert
- Gründe dafür, dass Inline-Ergebnisse bei Angriffen verloren gegangen wären
- Kein Neustart von Snort bei Änderungen an der VDB, an SSL-Richtlinien, an benutzerdefinierten Anwendungsdetektoren, an firmeneigenen Portalidentitätsquellen und an der TLS-Serveridentitätserkennung
- Verbesserte Wartungsfreundlichkeit dank an das Cisco Success Network gesendeter Telemetriedaten speziell für Snort 3 und optimierten Fehlerbehebungsprotokollen

Die Unterstützung für Snort 3.0 wurde für Cisco Firepower Threat Defense (FTD) 6.7.0 eingeführt, sobald die FTD über den Cisco Firepower Device Manager (FDM) verwaltet wird.

Hinweis: Bei neuen FTD-Bereitstellungen mit 6.7.0, die von FDM verwaltet werden, ist Snort 3.0 die Standard-Prüfungs-Engine. Wenn Sie das FTD von einer älteren Version auf 6.7 aktualisieren, bleibt Snort 2.0 die aktive Prüfungs-Engine, aber Sie können auf Snort 3.0 umschalten.

Hinweis: In dieser Version unterstützt Snort 3.0 keine virtuellen Router, zeitbasierten Zugriffskontrollregeln oder die Entschlüsselung von TLS 1.1- oder niedrigeren Verbindungen. Aktivieren Sie Snort 3.0 nur, wenn Sie diese Funktionen nicht benötigen.

In der Firepower-Version 7.0 wurde dann die Snort 3.0-Unterstützung für die Firepower Threat Defense-Geräte eingeführt, die sowohl vom Cisco FDM als auch vom Cisco FirePOWER Management Center (FMC) verwaltet werden.

Hinweis: Bei neuen FTD-Bereitstellungen mit 7.0 ist Snort 3 jetzt die Standard-Prüfungs-Engine. Aktualisierte Bereitstellungen verwenden weiterhin Snort 2, Sie können jedoch jederzeit wechseln.

Achtung: Sie können frei zwischen Snort 2.0 und 3.0 hin- und herschalten, sodass Sie Ihre Änderung bei Bedarf rückgängig machen können. Der Datenverkehr wird bei jedem Versionswechsel unterbrochen.

Achtung: Vor dem Wechsel zu Snort 3 wird dringend empfohlen, dass Sie den Konfigurationsleitfaden zu Firepower Management Center Snort 3 lesen und verstehen. Achten Sie besonders auf Funktionsbeschränkungen und Migrationsanweisungen. Obwohl das Upgrade auf Snort 3 auf minimale Auswirkungen ausgelegt ist, lassen sich die Funktionen nicht exakt zuordnen. Mithilfe der Planung und Vorbereitung vor dem Upgrade können Sie sicherstellen, dass der Datenverkehr wie erwartet verarbeitet wird.

Bestimmen Sie die aktive Snort-Version, die auf FTD ausgeführt wird.

FTD-Befehlszeilenschnittstelle (CLI)

Um die aktive Snort-Version zu ermitteln, die auf einem FTD ausgeführt wird, melden Sie sich bei der FTD-CLI an, und führen Sie den Befehl **show snort3 status aus**:

Beispiel 1: Wenn keine Ausgabe angezeigt wird, führt die FTD Snort 2 aus.

```
<#root>

>

show snort3 status

>
```

Beispiel 2: Wenn die Ausgabe "**Momentan wird Snort 2 ausgeführt**" anzeigt, dann wird Snort 2 von der FTD ausgeführt.

```
<#root>

>

show snort3 status

Currently running Snort 2
```

Beispiel 3: Wenn die Ausgabe "**Derzeit läuft Snort 3**" anzeigt, dann führt die FTD Snort 3 aus.

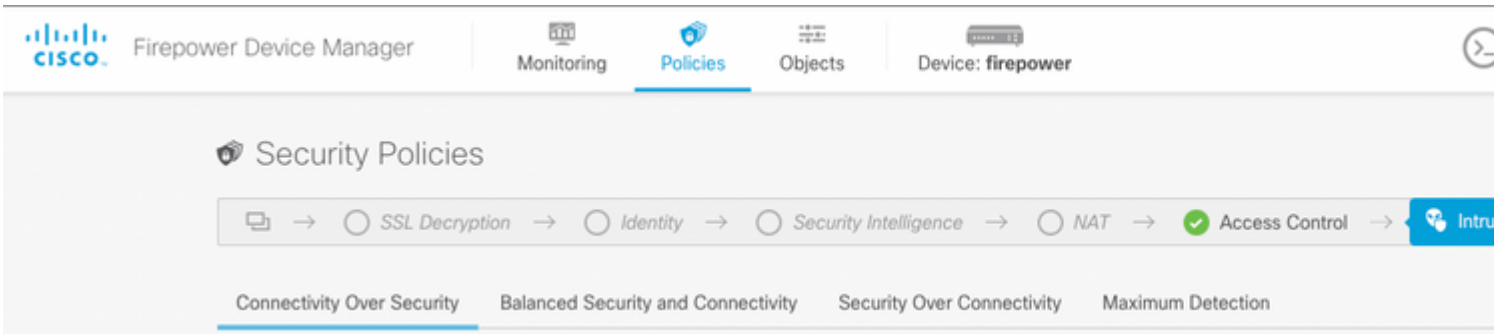
```
<#root>

>

show snort3 status

Currently running Snort 3
```

Von Cisco FDM verwaltete FTD

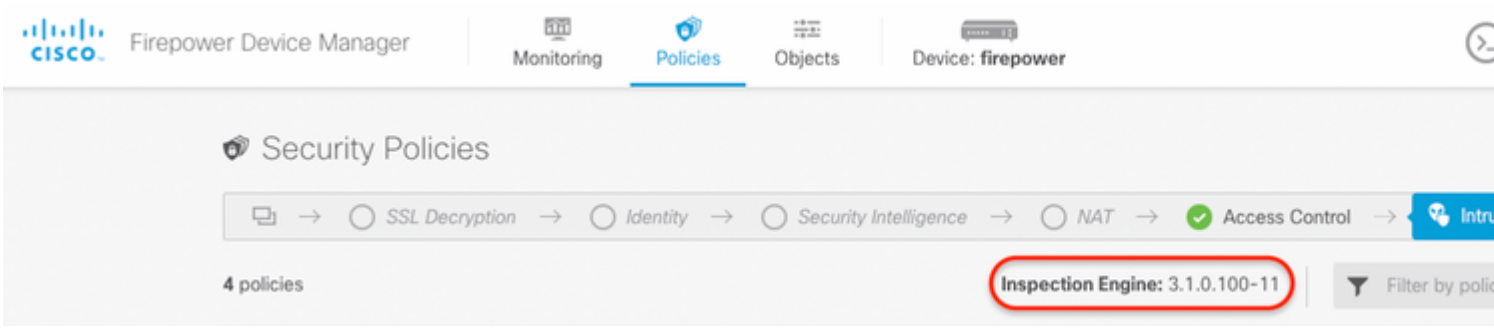
Um die aktive Snort-Version zu ermitteln, die auf einem FTD ausgeführt wird, das vom Cisco FDM verwaltet wird, gehen Sie wie folgt vor:

1. Melden Sie sich über die FDM-Webschnittstelle beim Cisco FTD an.
2. Wählen Sie im Hauptmenü die Option **Richtlinien aus**.
3. Wählen Sie dann die Registerkarte **Intrusion (Zugriff)**.
4. Suchen Sie nach der **Snort-Version** oder dem Abschnitt **Inspection Engine** (**Inspektionsmodul**), um die Snort-Version zu überprüfen, die im FTD aktiv ist.

Beispiel 1: Die FTD führt Snort Version 2 aus.



Beispiel 2: Die FTD führt Snort Version 3 aus.

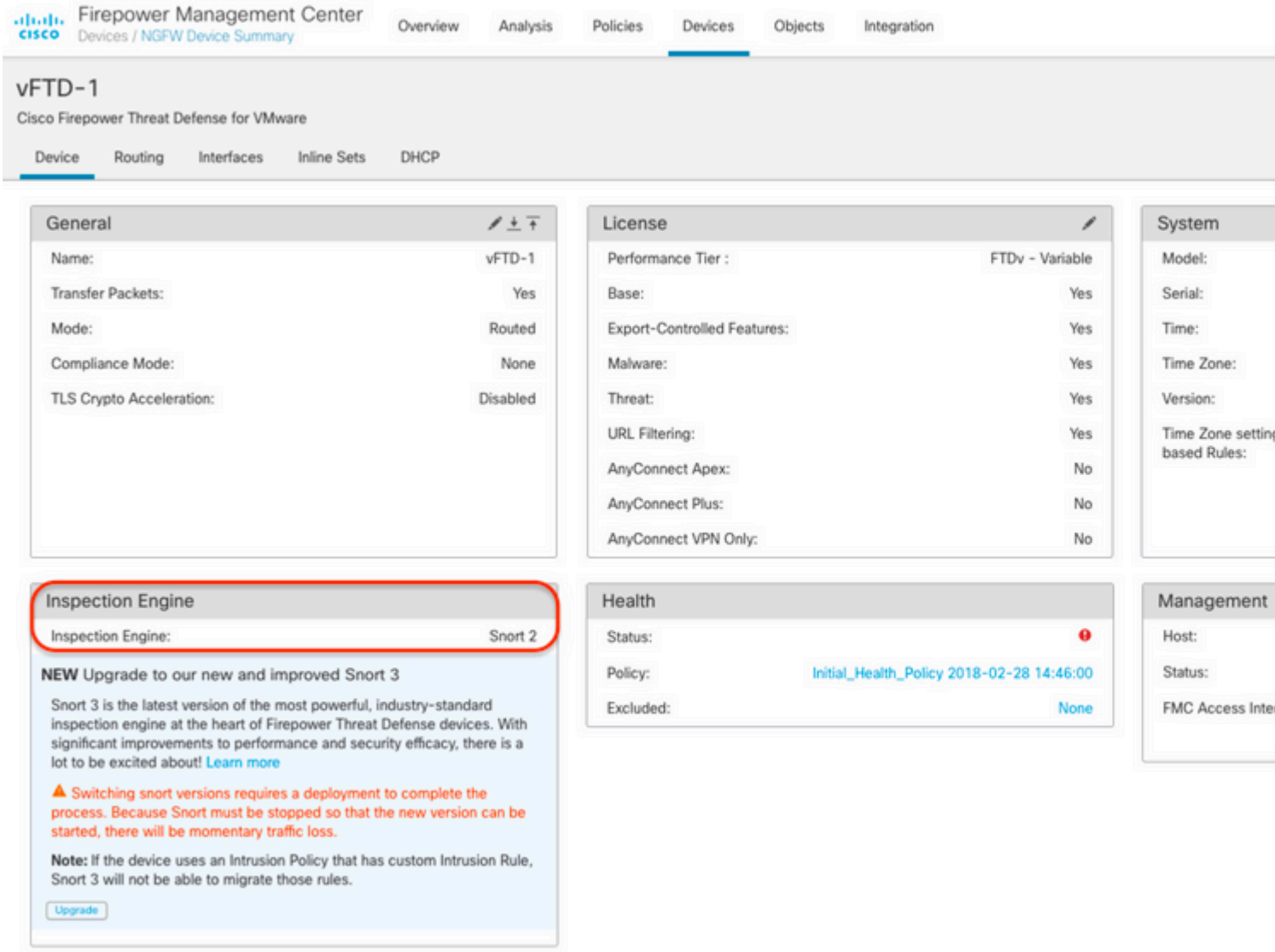


FTD verwaltet von Cisco FMC

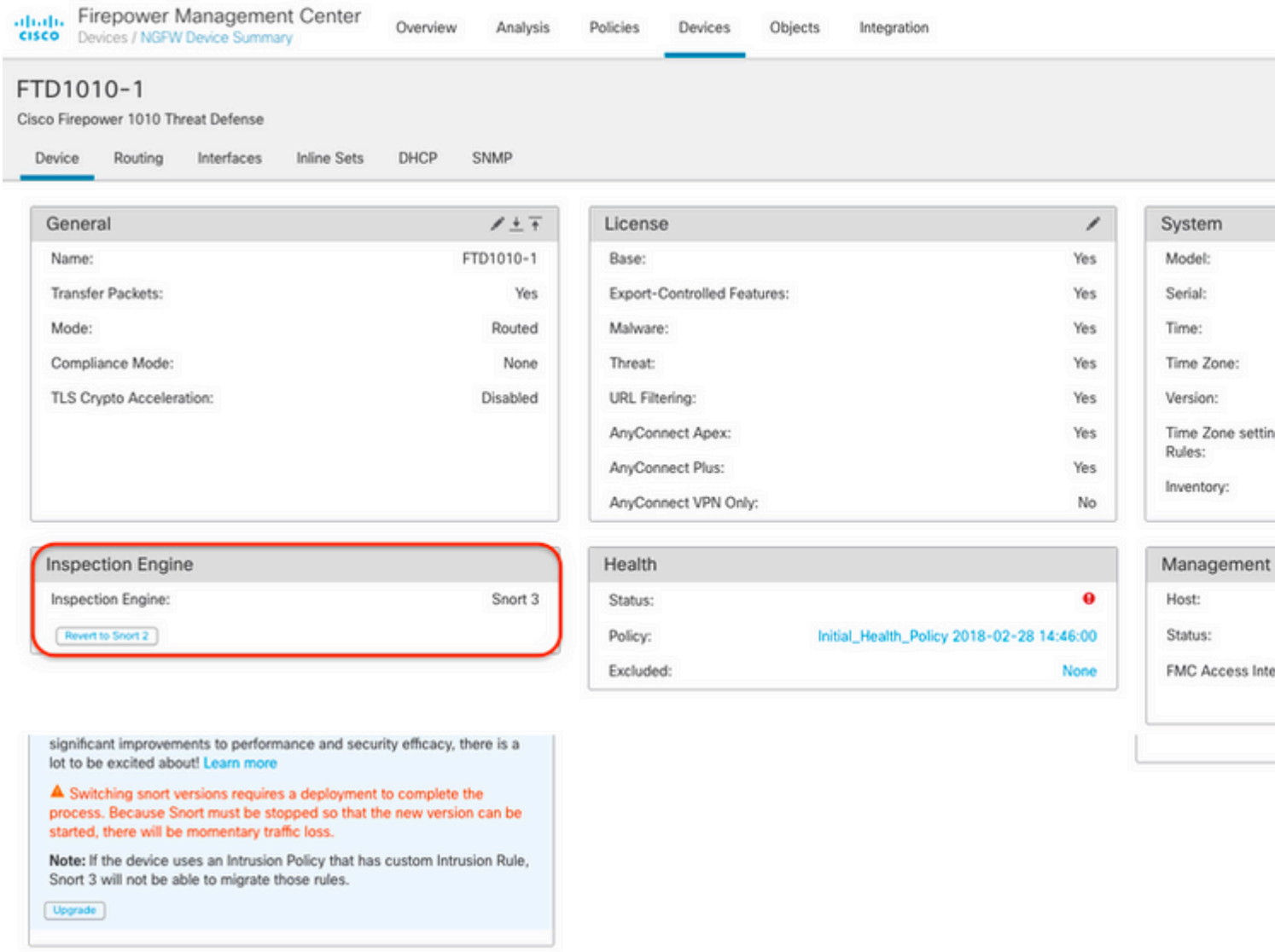
Um die aktive Snort-Version zu ermitteln, die auf einem FTD ausgeführt wird, das vom Cisco FMC verwaltet wird, gehen Sie wie folgt vor:

1. Melden Sie sich bei der Cisco FMC-Webschnittstelle an.
2. Wählen Sie im Menü **Geräte** die Option **Geräteverwaltung aus**.
3. Wählen Sie dann das entsprechende FTD-Gerät aus.
4. Klicken Sie auf das Bleistiftsymbol **bearbeiten**.
5. Wählen Sie die Registerkarte **Device (Gerät)**, und suchen Sie im Abschnitt **Inspection Engine** (**Inspektionsmodul**) nach der im FTD aktiven Snort-Version:

Beispiel 1: Die FTD führt Snort Version 2 aus.



Beispiel 2: Die FTD führt Snort Version 3 aus.

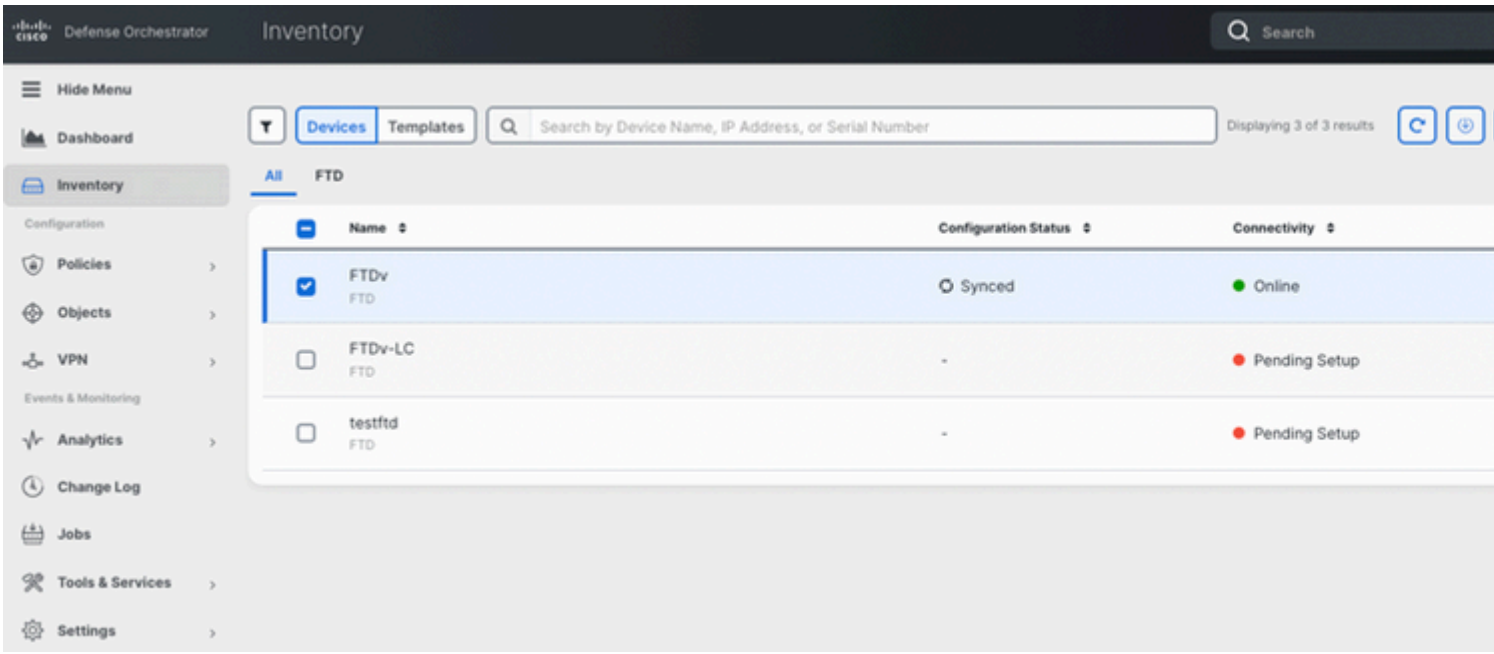


FTD verwaltet von Cisco CDO

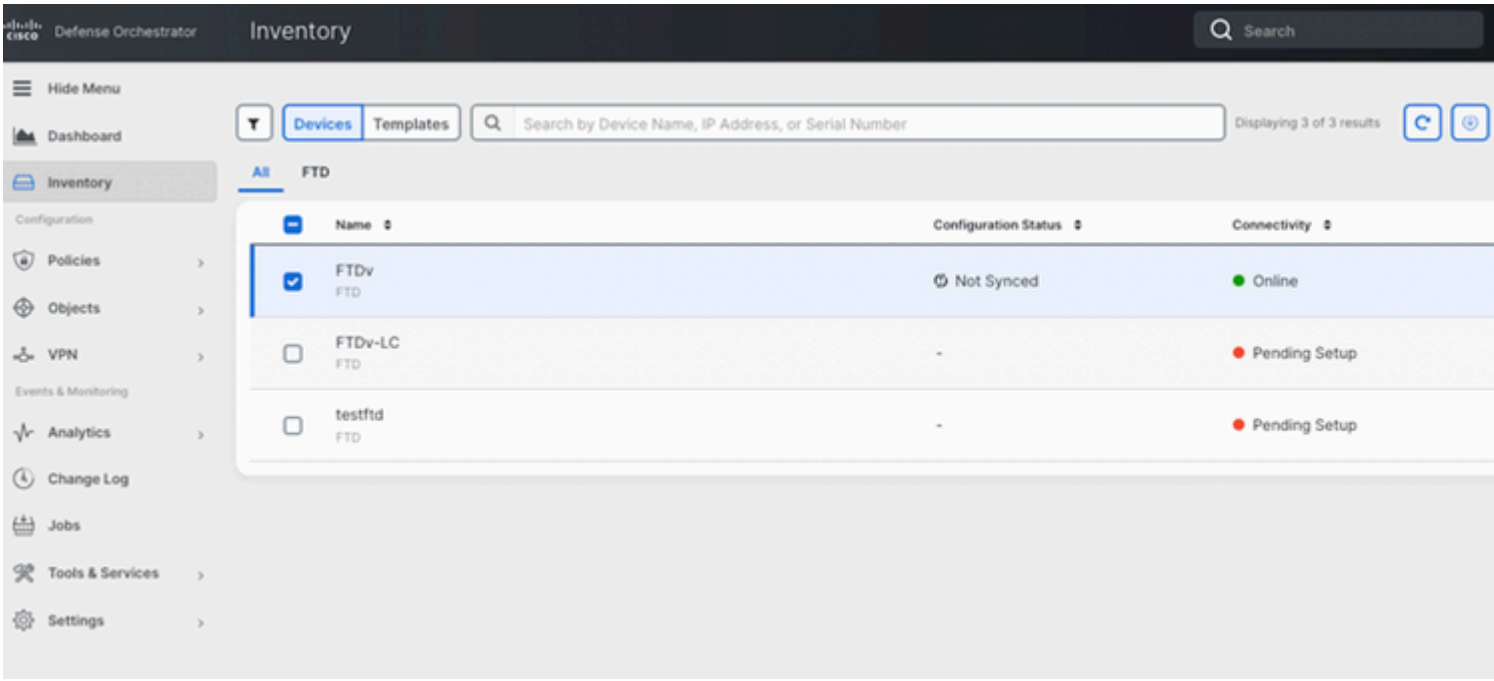
Um die aktive Snort-Version zu ermitteln, die auf einem FTD ausgeführt wird, das vom Cisco Defense Orchestrator verwaltet wird, gehen Sie wie folgt vor:

1. Melden Sie sich bei der Cisco Defense Orchestrator-Webschnittstelle an.
2. Wählen Sie im Menü **Inventory** (Bestand) das entsprechende FTD-Gerät aus.
3. Suchen Sie im Abschnitt **Device Details (Gerätedetails**) nach **Snort Version (Snort-Version)**:

Beispiel 1: Die FTD führt Snort Version 2 aus.



Beispiel 2: Die FTD führt Snort Version 3 aus.



Zugehörige Informationen

- Cisco FirePOWER - Versionshinweise, Version 6.7.0
- Cisco FirePOWER - Versionshinweise, Version 7.0
- Snort 3-Website
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.