# Determinar la versión de Snort activo que se ejecuta en Firepower Threat Defence (FTD)

## Contenido



## Introducción

Este documento describe los pasos para confirmar la versión de snort activa que ejecuta Cisco Firepower Threat Defense (FTD) cuando se gestiona mediante Cisco Firepower Device Manager (FDM), Cisco Firepower Management Center (FMC) o Cisco Defense Orchestrator (CDO).

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cisco Firepower Management Center (FMC)
- Cisco Firepower Threat Defence (FTD)
- Administrador de dispositivos Cisco Firepower (FDM)
- Cisco Defense Orchestrator (CDO)

### Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

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

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Antecedentes

SNORT® Intrusion Prevention System ha lanzado oficialmente Snort 3, una actualización completa que incluye mejoras y nuevas funciones que mejoran el rendimiento, un procesamiento más rápido, una escalabilidad mejorada para la red y una gama de más de 200 complementos para que los usuarios puedan crear una configuración personalizada para su red.

Las ventajas de Snort 3 incluyen, entre otras:

- Rendimiento mejorado
- Inspección SMBv2 mejorada
- Nuevas funciones de detección de scripts
- Inspección HTTP/2
- Grupos de reglas personalizados
- Sintaxis que facilita la escritura de reglas de intrusión personalizadas
- Motivos por los que se "habría descartado" en línea producen eventos de intrusión
- No se reinicia Snort cuando se implementan cambios en VDB, políticas SSL, detectores de aplicaciones personalizadas, orígenes de identidad de portal cautivo y detección de identidad de servidor TLS
- Mantenimiento mejorado gracias a los datos de telemetría específicos de Snort 3 enviados a Cisco Success Network y a los mejores registros de solución de problemas

La compatibilidad con Snort 3.0 se introdujo para Cisco Firepower Threat Defense (FTD) 6.7.0, justo cuando el FTD se gestiona a través de Cisco Firepower Device Manager (FDM).

---

**Nota**: para las nuevas implementaciones de FTD 6.7.0 administradas por FDM, Snort 3.0 es el motor de inspección predeterminado. Si actualiza el FTD a 6.7 desde una versión anterior, Snort 2.0 seguirá siendo el motor de inspección activo, pero podrá cambiar a Snort 3.0.

---

**Nota**: Para esta versión, Snort 3.0 no admite routers virtuales, reglas de control de acceso basadas en tiempo ni el descifrado de conexiones TLS 1.1 o inferiores. Active Snort 3.0 sólo si no necesita estas funciones.

---

A continuación, la versión 7.0 de Firepower introdujo la compatibilidad con Snort 3.0 para los dispositivos Firepower Threat Defense administrados por Cisco FDM y por Cisco Firepower Management Center (FMC).

---

**Nota**: para las nuevas implementaciones de FTD 7.0, Snort 3 es ahora el motor de inspección predeterminado. Las implementaciones actualizadas siguen utilizando Snort 2, pero puede cambiar en cualquier momento.

---

**Precaución**: puede cambiar libremente entre Snort 2.0 y 3.0, de modo que puede revertir el cambio si es necesario. El tráfico se interrumpe cada vez que cambia de versión.

---

**Precaución**: antes de cambiar a Snort 3, se recomienda encarecidamente que lea y entienda la Guía de

---

configuración de Firepower Management Center Snort 3. Preste especial atención a las limitaciones de las funciones y a las instrucciones de migración. Aunque la actualización a Snort 3 está diseñada para tener un impacto mínimo, las funciones no se asignan exactamente. El plan y la preparación antes de la actualización pueden ayudarle a asegurarse de que el tráfico se maneje como se esperaba.

# Determinar la versión de Snort activo que se ejecuta en FTD

## Interfaz de línea de comandos (CLI) de FTD

Para determinar la versión de snort activa que se ejecuta en un FTD, inicie sesión en la CLI de FTD y ejecute el comando **show snort3 status**:

**Ejemplo 1:** Cuando no se muestra ningún resultado, el FTD ejecuta Snort 2.

```
<#root>

>

show snort3 status

>
```

**Ejemplo 2:** Cuando el resultado muestra **"Snort 2 actualmente en ejecución"**, el FTD ejecuta Snort 2.

```
<#root>

>

show snort3 status

Currently running Snort 2
```

**Ejemplo 3:** Cuando el resultado muestra **"Snort 3 actualmente en ejecución"**, el FTD ejecuta Snort 3.

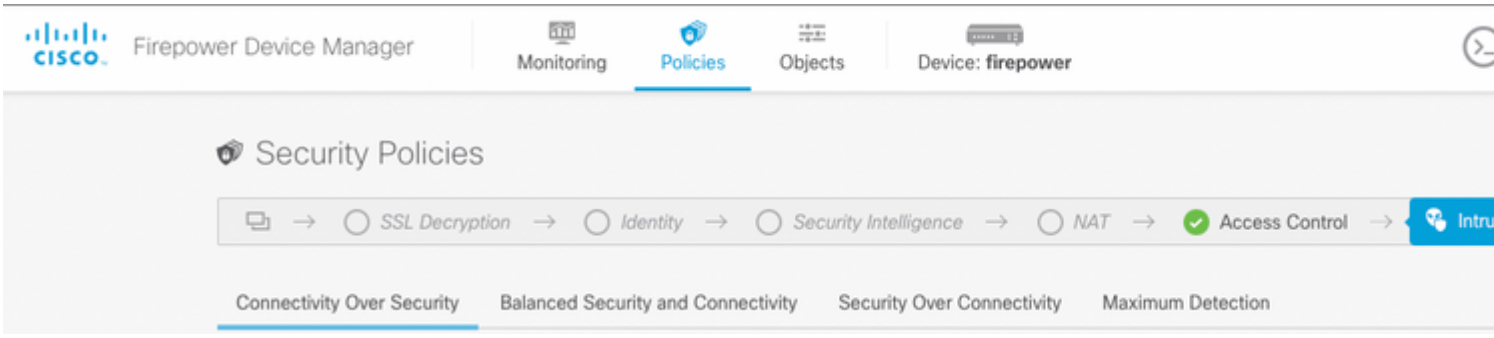
```
<#root>

>

show snort3 status

Currently running Snort 3
```

## FTD gestionado por Cisco FDM

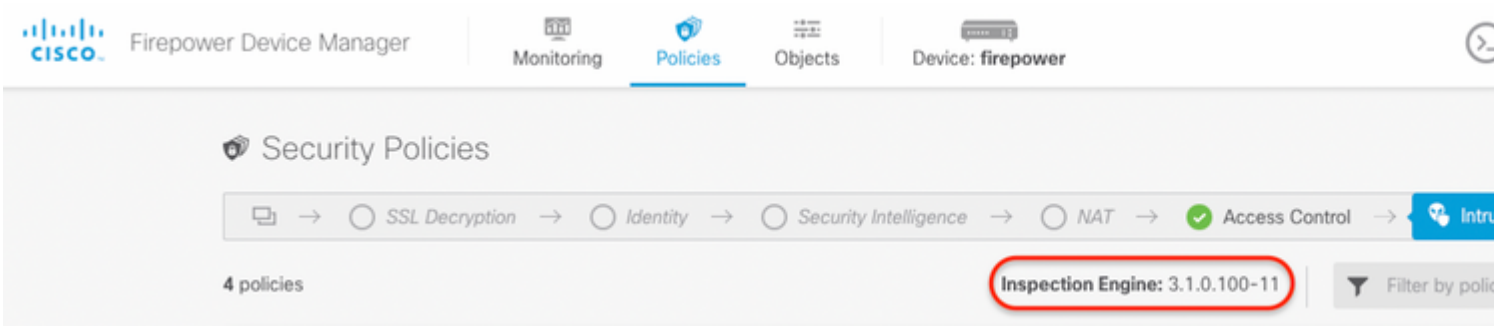
Para determinar la versión de snort activa que se ejecuta en un FTD administrado por Cisco FDM, continúe con los siguientes pasos:

1. Inicie sesión en Cisco FTD a través de la interfaz web de FDM.
2. En el menú principal, seleccione **Policies**.
3. A continuación, seleccione la ficha **Intrusión**.
4. Busque la sección **Versión de Snort** o **Motor de inspección** para confirmar la versión de Snort activa en el FTD.

**Ejemplo 1:** el FTD ejecuta la versión 2 de snort.




**Ejemplo 2:** El FTD ejecuta la versión 3 de snort.

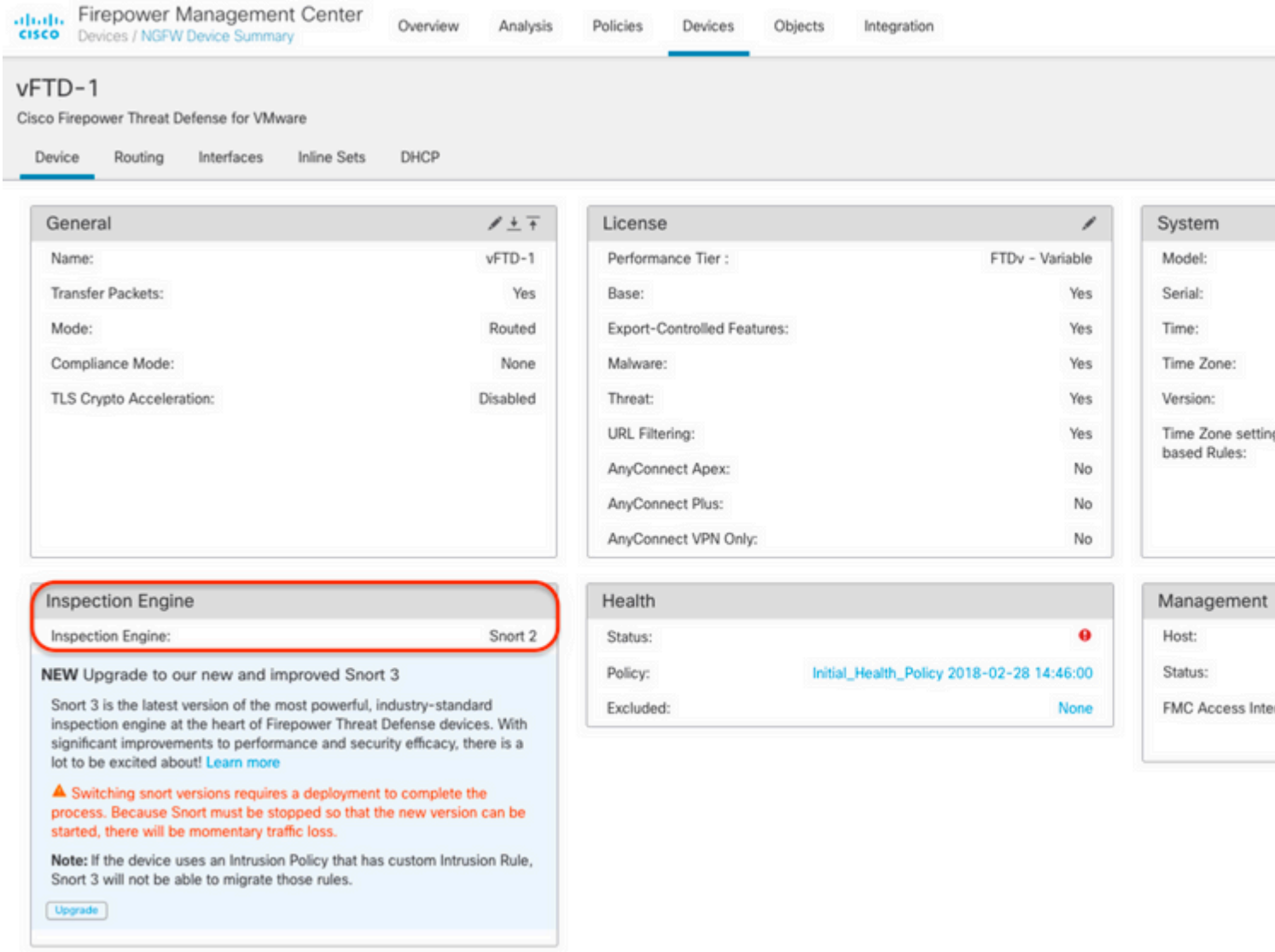



## FTD gestionado por el Cisco FMC

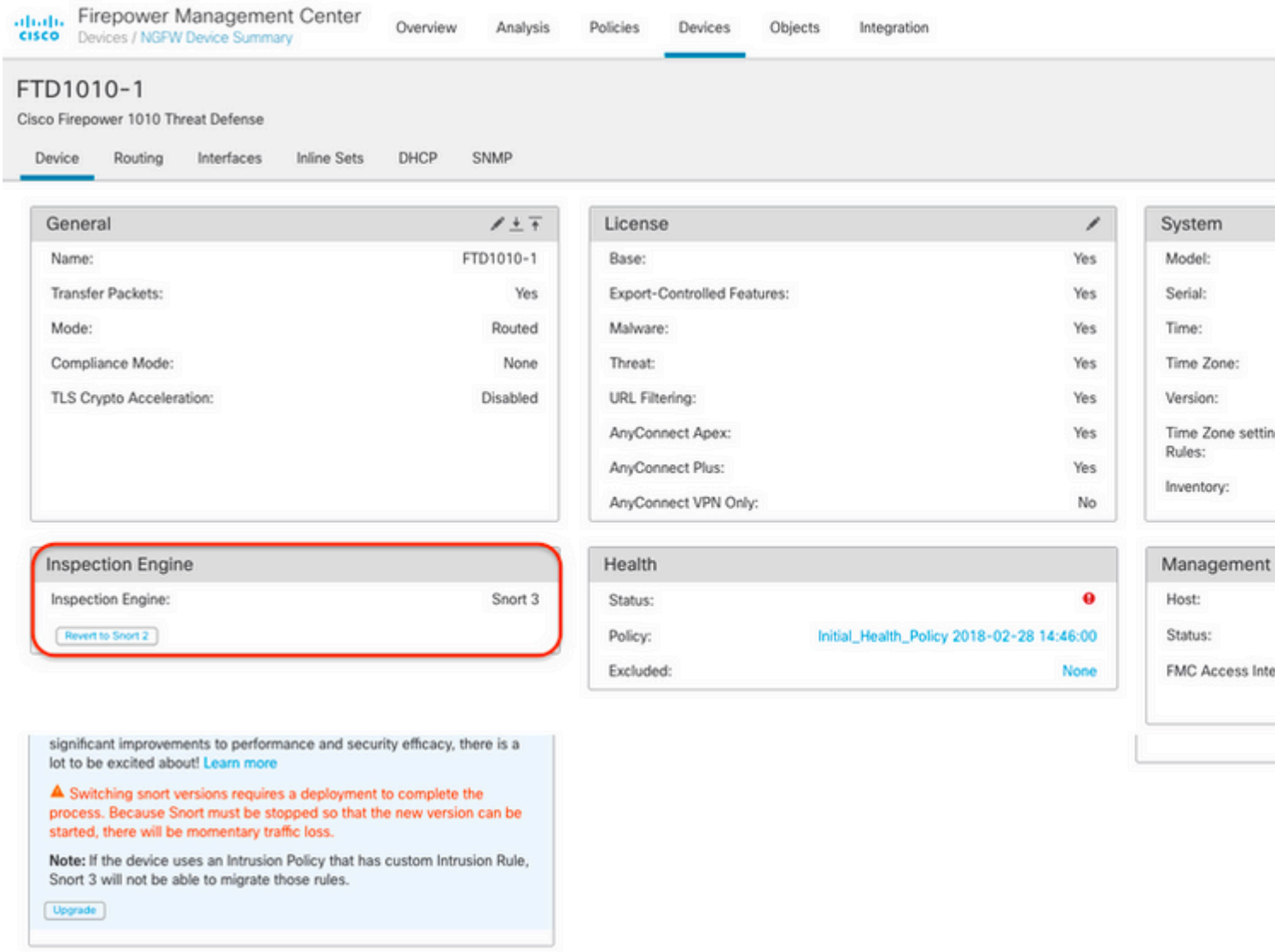
Para determinar la versión de snort activa que se ejecuta en un FTD gestionado por Cisco FMC, continúe con los siguientes pasos:

1. Inicie sesión en la interfaz web de Cisco FMC.
2. En el menú **Devices**, seleccione **Device Management**.
3. A continuación, seleccione el dispositivo FTD adecuado.
4. Haga clic en el icono **Edit** pencil.
5. Seleccione la pestaña **Device** y busque la sección **Inspection Engine** para confirmar la versión de snort que está activa en el FTD:

**Ejemplo 1:** el FTD ejecuta la versión 2 de snort.




**Ejemplo 2:** El FTD ejecuta la versión 3 de snort.

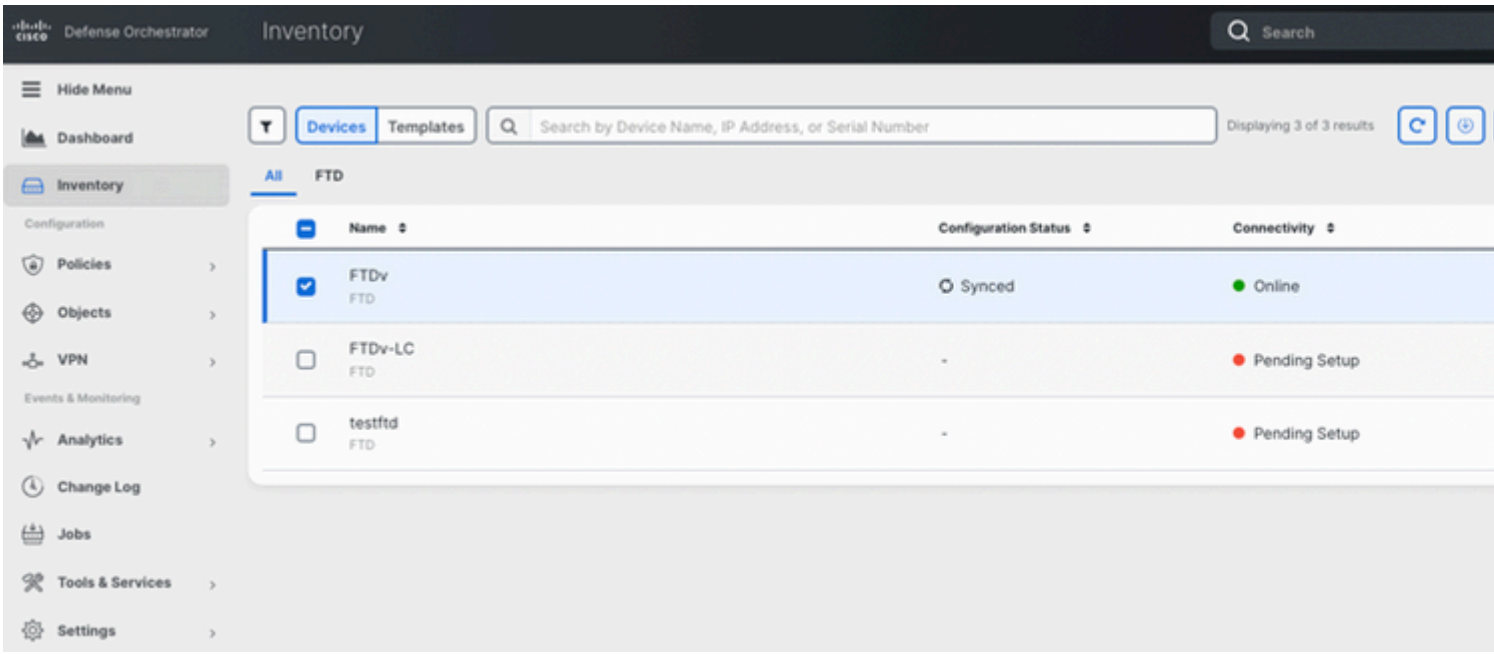



## FTD gestionado por el CDO de Cisco

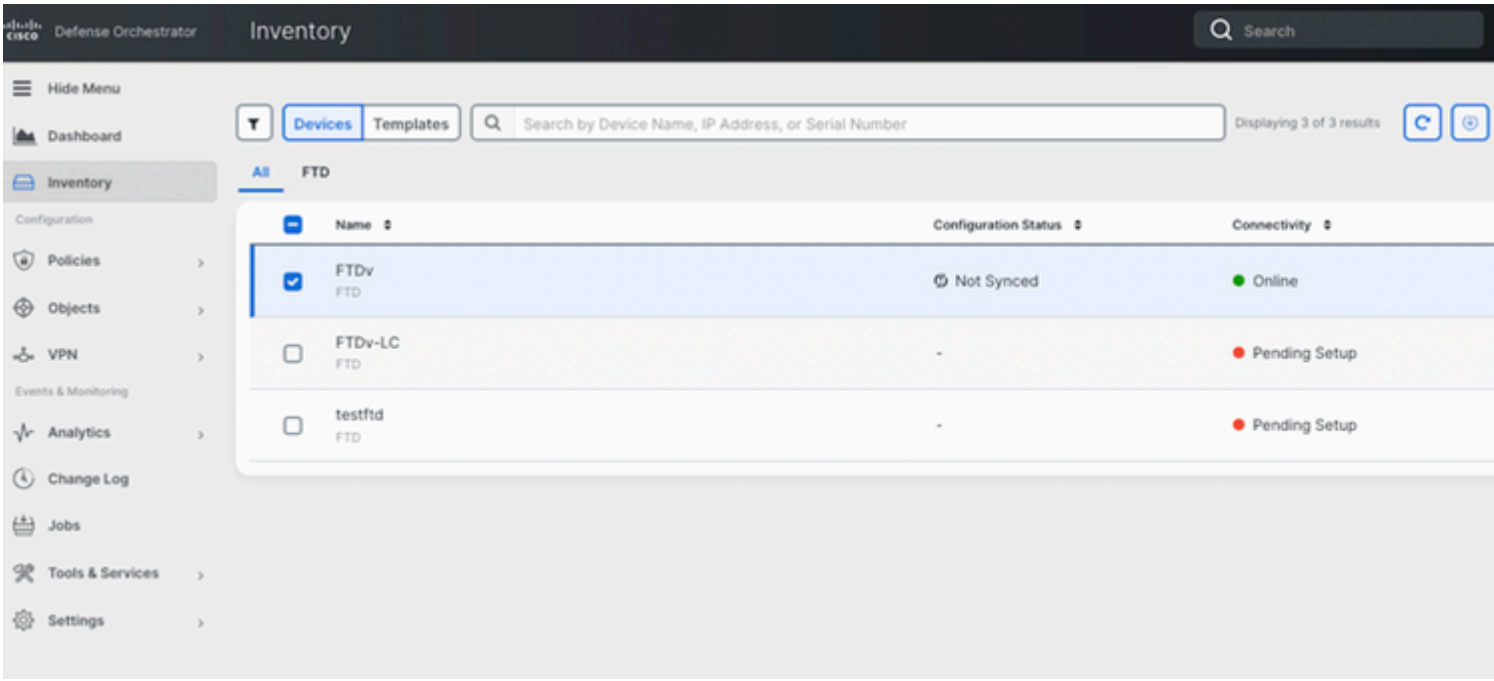
Para determinar la versión de snort activa que se ejecuta en un FTD gestionado por Cisco Defense Orchestrator, continúe con los siguientes pasos:

1. Inicie sesión en la interfaz web de Cisco Defense Orchestrator.
2. En el menú **Inventory**, seleccione el dispositivo FTD adecuado.
3. En la sección **Detalles del dispositivo**, busque **Versión de Snort**:

**Ejemplo 1:** el FTD ejecuta la versión 2 de snort.




**Ejemplo 2:** El FTD ejecuta la versión 3 de snort.




# Información Relacionada

- Notas de la versión de Cisco Firepower, versión 6.7.0
- Notas de la versión de Cisco Firepower, versión 7.0
- Sitio web de Snort 3
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).