

# Déterminer la version active de Snort exécutée sur Firepower Threat Defense (FTD)

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Déterminez la version active du sniffeur qui s'exécute sur le FTD](#)

[Interface de ligne de commande \(CLI\) FTD](#)

[FTD géré par Cisco FDM](#)

[FTD géré par Cisco FMC](#)

[FTD géré par Cisco CDO](#)

[Informations connexes](#)

---

## Introduction

Ce document décrit les étapes à suivre pour confirmer la version active de snort qu'un pare-feu Cisco Firepower Threat Defense (FTD) exécute lorsqu'il est géré par Cisco Firepower Device Manager (FDM), Cisco Firepower Management Center (FMC) ou Cisco Defense Orchestrator (CDO).

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Firepower Management Center (FMC)
- Cisco Firepower Threat Defense (FTD)
- Gestionnaire de périphériques Cisco Firepower (FDM)
- Cisco Defense Orchestrator (CDO)

### Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Firepower Threat Defense (FTD) v6.7.0 et 7.0.0
- Cisco Firepower Management Center (FMC) v6.7.0 et 7.0.0

- Cisco Defense Orchestrator (CDO)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Informations générales


Le système de prévention des intrusions SNORT® a officiellement lancé Snort 3, une mise à niveau complète qui propose des améliorations et de nouvelles fonctionnalités qui améliorent les performances, un traitement plus rapide, une évolutivité améliorée pour votre réseau, et une gamme de plus de 200 plugins afin que les utilisateurs puissent créer une configuration personnalisée pour leur réseau.

Les avantages de Snort 3 incluent, sans s'y limiter :


- Performances améliorées
- Inspection SMBv2 améliorée
- Nouvelles fonctionnalités de détection de script
- Inspection HTTP/2
- Groupes de règles personnalisés
- Syntaxe facilitant l'écriture de règles d'intrusion personnalisées
- Les raisons de « aurait abandonné » en ligne entraînent des événements d'intrusion
- No Snort redémarre lorsque des modifications sont déployées sur la VDB, les stratégies SSL, les détecteurs d'applications personnalisés, les sources d'identité de portail captif et la découverte d'identité de serveur TLS
- Facilité de maintenance améliorée grâce aux données télémétriques spécifiques à Snort 3 envoyées à Cisco Success Network et à de meilleurs journaux de dépannage

La prise en charge de Snort 3.0 a été introduite pour la version 6.7.0 de Cisco Firepower Threat Defense (FTD), juste au moment où le FTD est géré via Cisco Firepower Device Manager (FDM).

---

 Remarque : pour les nouveaux déploiements FTD 6.7.0 gérés par FDM, Snort 3.0 est le moteur d'inspection par défaut. Si vous mettez à niveau le FTD vers 6.7 à partir d'une version plus ancienne, alors Snort 2.0 reste le moteur d'inspection actif, mais vous pouvez passer à Snort 3.0.

---

 Remarque : pour cette version, Snort 3.0 ne prend pas en charge les routeurs virtuels, les règles de contrôle d'accès basées sur le temps ou le déchiffrement des connexions TLS 1.1 ou inférieures. Activez Snort 3.0 uniquement si vous n'avez pas besoin de ces

---


---

 fonctionnalités.


---

Ensuite, la version 7.0 de Firepower a introduit la prise en charge de Snort 3.0 pour les périphériques Firepower Threat Defense gérés à la fois par Cisco FDM et par Cisco Firepower Management Center (FMC).


---

 Remarque : pour les nouveaux déploiements FTD 7.0, Snort 3 est désormais le moteur d'inspection par défaut. Les déploiements mis à niveau continuent d'utiliser Snort 2, mais vous pouvez basculer à tout moment.

---

 Attention : vous pouvez basculer librement entre Snort 2.0 et 3.0, afin de pouvoir revenir à vos modifications si nécessaire. Le trafic est interrompu chaque fois que vous changez de version.

---

 Attention : avant de passer à Snort 3, il est vivement recommandé de lire et de comprendre le [Guide de configuration de Snort 3 de Firepower Management Center](#). Soyez particulièrement attentif aux limitations des fonctionnalités et aux instructions de migration. Bien que la mise à niveau vers Snort 3 soit conçue pour un impact minimal, les fonctionnalités ne correspondent pas exactement. Le plan et la préparation avant la mise à niveau peuvent vous aider à vous assurer que le trafic est traité comme prévu.

---

## Déterminez la version active du sniffeur qui s'exécute sur le FTD

### Interface de ligne de commande (CLI) FTD

Afin de déterminer la version de snort active qui s'exécute sur un FTD, connectez-vous à l'ILC FTD et exécutez la commande `show snort3 status` :

Exemple 1 : Lorsqu'aucune sortie n'est affichée, le FTD exécute Snort 2.

```
<#root>
>
show snort3 status
>
```

Exemple 2 : Lorsque la sortie affiche "Actuellement en cours d'exécution de Snort 2", le FTD exécute Snort 2.

```
<#root>
```

>

```
show snort3 status
```

Currently running Snort 2

Exemple 3 : Lorsque la sortie affiche "Actuellement en cours d'exécution de Snort 3", alors le FTD exécute Snort 3.

```
<#root>
```

>

```
show snort3 status
```

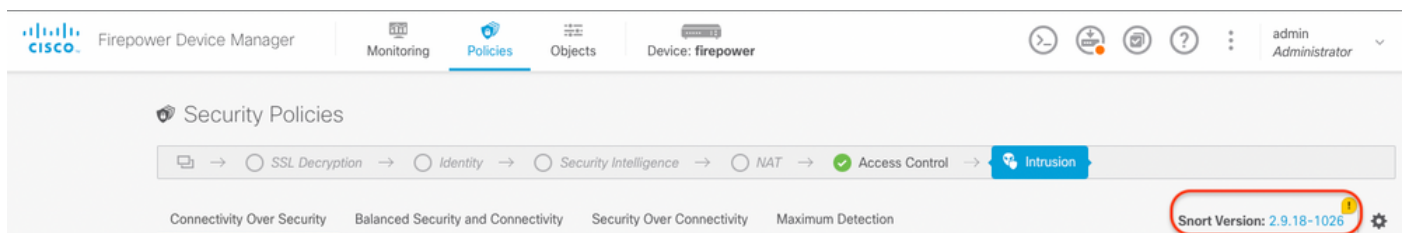
Currently running Snort 3

## FTD géré par Cisco FDM

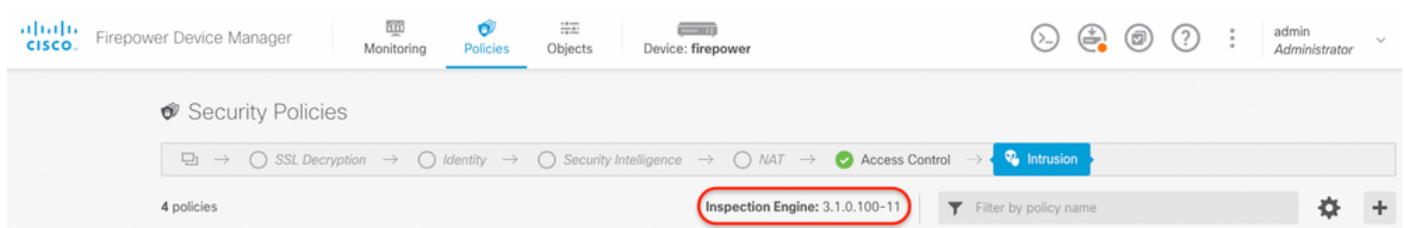
Afin de déterminer la version active de snort qui s'exécute sur un FTD qui est géré par Cisco FDM, passez aux étapes suivantes :

1. Connectez-vous au FTD Cisco via l'interface Web de FDM.
2. Dans le menu principal, sélectionnez Politiques.
3. Sélectionnez ensuite l'onglet Intrusion.
4. Recherchez la section Snort Version ou Inspection Engine pour confirmer la version de Snort qui est active dans le FTD.

Exemple 1 : Le FTD exécute snort version 2.



Exemple 2 : Le FTD exécute snort version 3.



## FTD géré par le Cisco FMC

Afin de déterminer la version active de snort qui s'exécute sur un FTD qui est géré par Cisco FMC, passez aux étapes suivantes :

1. Connectez-vous à l'interface Web de Cisco FMC.
2. Dans le menu Périphériques, sélectionnez Gestion des périphériques.
3. Sélectionnez ensuite le périphérique FTD approprié.
4. Cliquez sur l'icône Modifier le crayon.
5. Sélectionnez l'onglet Device et recherchez la section Inspection Engine pour confirmer la version de snort qui est active dans le FTD :

Exemple 1 : Le FTD exécute snort version 2.

The screenshot displays the Cisco Firepower Management Center interface for a device named vFTD-1. The 'Inspection Engine' section is highlighted with a red box, showing the active version as Snort 2. A 'NEW Upgrade' notification is visible, encouraging an upgrade to Snort 3. The notification text reads: 'NEW Upgrade to our new and improved Snort 3. Snort 3 is the latest version of the most powerful, industry-standard inspection engine at the heart of Firepower Threat Defense devices. With significant improvements to performance and security efficacy, there is a lot to be excited about! [Learn more](#). ⚠️ Switching snort versions requires a deployment to complete the process. Because Snort must be stopped so that the new version can be started, there will be momentary traffic loss. Note: If the device uses an Intrusion Policy that has custom Intrusion Rule, Snort 3 will not be able to migrate those rules. [Upgrade](#)'.

General	License	System
Name: vFTD-1	Performance Tier: FTDv - Variable	Model: Cisco Firepower Threat Defense for VMware
Transfer Packets: Yes	Base: Yes	Serial: [REDACTED]
Mode: Routed	Export-Controlled Features: Yes	Time: 2023-04-20 00:57:11
Compliance Mode: None	Malware: Yes	Time Zone: UTC (UTC+0:00)
TLS Crypto Acceleration: Disabled	Threat: Yes	Version: 7.0.4
	URL Filtering: Yes	Time Zone setting for Time based Rules: UTC (UTC+0:00)
	AnyConnect Apex: No	
	AnyConnect Plus: No	
	AnyConnect VPN Only: No	

Health	Management
Status: [REDACTED]	Host: [REDACTED]
Policy: Initial_Health_Policy 2018-02-28 14:46:00	Status: [REDACTED]
Excluded: None	FMC Access Interface: Management Interface

Exemple 2 : Le FTD exécute snort version 3.

Firepower Management Center  
Devices / NGFW Device Summary

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin

### FTD1010-1

Cisco Firepower 1010 Threat Defense

Device Routing Interfaces Inline Sets DHCP SNMP

#### General

Name: FTD1010-1

Transfer Packets: Yes

Mode: Routed

Compliance Mode: None

TLS Crypto Acceleration: Disabled

#### License

Base: Yes

Export-Controlled Features: Yes

Malware: Yes

Threat: Yes

URL Filtering: Yes

AnyConnect Apex: Yes

AnyConnect Plus: Yes

AnyConnect VPN Only: No

#### System

Model: Cisco Firepower 1010 Threat Defense

Serial: [REDACTED]

Time: 2023-04-20 01:44:01

Time Zone: UTC (UTC+0:00)

Version: 7.0.4

Time Zone setting for Time based Rules: (UTC-05:00) America/New\_York

Inventory: [View](#)

#### Inspection Engine

Inspection Engine: Snort 3

[Revert to Snort 2](#)

significant improvements to performance and security efficacy, there is a lot to be excited about! [Learn more](#)

⚠️ Switching snort versions requires a deployment to complete the process. Because Snort must be stopped so that the new version can be started, there will be momentary traffic loss.

Note: If the device uses an Intrusion Policy that has custom Intrusion Rule, Snort 3 will not be able to migrate those rules.

[Upgrade](#)

#### Health

Status: ●

Policy: Initial\_Health\_Policy 2018-02-28 14:46:00

Excluded: None

#### Management

Host: [REDACTED]

Status: ●

FMC Access Interface: [Management Interface](#)

## FTD géré par le Cisco CDO

Afin de déterminer la version active de snort qui s'exécute sur un FTD qui est géré par Cisco Defense Orchestrator, passez aux étapes suivantes :

1. Connectez-vous à l'interface Web de Cisco Defense Orchestrator.
2. Dans le menu Inventaire, sélectionnez le périphérique FTD approprié.
3. Dans la section Device Details, recherchez Snort Version :

Exemple 1 : Le FTD exécute snort version 2.

Defense Orchestrator Inventory

Search

Hide Menu Dashboard Inventory Policies Objects VPN Analytics Change Log Jobs Tools & Services Settings

Devices Templates Search by Device Name, IP Address, or Serial Number

Name	Configuration Status	Connectivity
<input checked="" type="checkbox"/> FTDv FTD	Synced	Online
<input type="checkbox"/> FTDv-LC FTD	-	Pending Setup
<input type="checkbox"/> testftd FTD	-	Pending Setup

#### FTDV

Device Details

Location: n/a

Model: Cisco Firepower Threat Defense for Azure

Serial: [REDACTED]

Version: 7.2.0

Onboarding Method: Registration Key

**Snort Version: 2.9.21-102**

Synced: Your device's configuration is up-to-date.

Device Actions: [Check for Changes](#), [Manage Licenses](#), [Workflows](#), [Remove](#)

Exemple 2 : Le FTD exécute snort version 3.

The screenshot shows the Cisco Defense Orchestrator (DO) interface. The main window displays the 'Inventory' section for 'FTD' devices. A table lists three devices: 'FTDv' (FTD, Not Synced, Online), 'FTDv-LC' (FTD, -, Pending Setup), and 'testftd' (FTD, -, Pending Setup). The 'FTDv' device is selected, and its details are shown on the right. The 'Device Details' section includes: Location (n/a), Model (Cisco Firepower Threat Defense for Azure), Serial (redacted), Version (7.2.0), Onboarding Method (Registration Key), and Snort Version (3.1215-126, highlighted with a red circle). Below this, a 'Not Synced' message states: 'The configuration has been modified in FMC. Synchronize your device's configuration by deploying the changes from FMC Deployment page'. The 'Device Actions' section includes: Check for Changes, Manage Licenses, Workflows, and Remove.

Name	Configuration Status	Connectivity
FTDv FTD	Not Synced	Online
FTDv-LC FTD	-	Pending Setup
testftd FTD	-	Pending Setup

**Device Details for FTDv**

- Location: n/a
- Model: Cisco Firepower Threat Defense for Azure
- Serial: [Redacted]
- Version: 7.2.0
- Onboarding Method: Registration Key
- Snort Version: 3.1215-126

**Not Synced**  
The configuration has been modified in FMC. Synchronize your device's configuration by deploying the changes from FMC Deployment page

**Device Actions**

- Check for Changes
- Manage Licenses
- Workflows
- Remove

## Informations connexes

- [Notes de version de Cisco Firepower, version 6.7.0](#)
- [Notes de version de Cisco Firepower, version 7.0](#)
- [Site Web de Snort 3](#)
- [Assistance et documentation techniques - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.