

# Comprendre le changement de marque des périphériques vers Cisco Secure Firewall

## Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Informations générales](#)

[Exigences](#)

[Composants utilisés](#)

[Description de la fonctionnalité](#)

[Configurer](#)

[Exemples de Firewall Management Center](#)

[Exemple de périphériques Firepower](#)

[Exemples de Firewall Device Manager](#)

---

## Introduction

Ce document décrit les informations relatives au changement de marque des périphériques vers Cisco Secure Firewall.

## Conditions préalables

### Informations générales

- Les noms des périphériques affichés correspondent désormais à d'autres supports de marque
- Cela crée une marque plus forte et une expérience utilisateur plus simple
- Aucun impact fonctionnel sur les plates-formes ; seul le texte a changé.
- Les anciennes plates-formes matérielles FTD (FPR1010/11XX, FPR41XX, FPR93XX) utilisent toujours la marque Firepower
- Certains paramètres système par défaut et noms de composants peuvent toujours utiliser firepower

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Gamme de pare-feu de nouvelle génération Cisco (NGFW)

### Composants utilisés

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

- Firepower Management Center (FMC) version 7.6.0
- Firepower Device Manager (FDM) version 7.6.0
- Toutes les fonctionnalités Virtual Firepower Threat Defense (FTD) version 7.6.0
- Pare-feu sécurisé Cisco 31XX,42XX

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.

## Description de la fonctionnalité

Comment ça fonctionne:

- Les noms de modèles complets et courts pour les plates-formes CSF31XX, CSF42XX, Firewall Threat Defense (FTD) Virtual et toutes les plates-formes Firewall Management Center (FMC) portent la marque Cisco Secure Firewall.
- Le logiciel CSF31XX FDM est désormais SFDM, Secure Firewall Device Manager.
- Cette fonction ne comporte aucun composant fonctionnel.
- Il n'existe aucune option de configuration pour cette fonctionnalité.

Mise à niveau :

- Lors de la mise à niveau vers Secure Firewall 7.6, toutes les interfaces CLI et GUI pertinentes ont été mises à jour pour refléter la marque actuelle.
- Aucun problème lors de la mise à niveau des périphériques enregistrés
  - Si Firewall Threat Defense (FTD) est mis à niveau, Firewall Management Center (FMC) met à jour son interface utilisateur graphique avec la marque actuelle.
  - Si Firewall Management Center (FMC) est mis à niveau, tous les périphériques enregistrés restaurent la connectivité après la mise à niveau comme prévu.

## Configurer

### Exemples de Firewall Management Center

État récapitulatif :

- Le nom du modèle Management Center est précédé de la marque Cisco.

Firewall Management Center Dashboard

Overview Analysis Policies Devices Objects Integration

## Summary Dashboard [\(switch dashboard\)](#)

Provides a summary of activity on the appliance

Network Threats Intrusion Events Status X Geolocation QoS Zero Trust + Show th

▶ Appliance Status

▶ Appliance Information

Name	firepower
IPv4 Address	192.168.0.75
IPv6 Address	Disabled
Model	Cisco Secure Firewall Management Center for VMware
Versions	
Software	7.6.0
Rule Update	2024-02-07-001-vrt

Informations de configuration :

- Le nom du modèle Management Center est précédé de la marque Cisco.

Firewall Management Center Configuration

Overview Analysis Policies Devices Objects Integration

Access Control Preferences

Access List

Audit Log

Audit Log Certificate

Change Management

Change Reconciliation

DNS Cache

Dashboard

Database

Email Notification

External Database Access

HTTPS Certificate

Information

Name	firepower
Product Model	Cisco Secure Firewall Management Center for VMware
Serial Number	None
Software Version	7.6.0
Operating System	Cisco Firepower Extensible Operating System (FX-OS)
Operating System Version	82.16.0
IPv4 Address	192.168.0.75
IPv6 Address	Disabled
Current Policies	Health Policy
	<a href="#">Firewall Management Center Health Policy</a>
Model Number	66

Sortie CLI :

- Le nom complet du modèle est indiqué avec la marque Cisco Secure Firewall.

Copyright 2004-2024, Cisco and/or its affiliates. All rights reserved.  
Cisco is a registered trademark of Cisco Systems, Inc.  
All other trademarks are property of their respective owners.

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

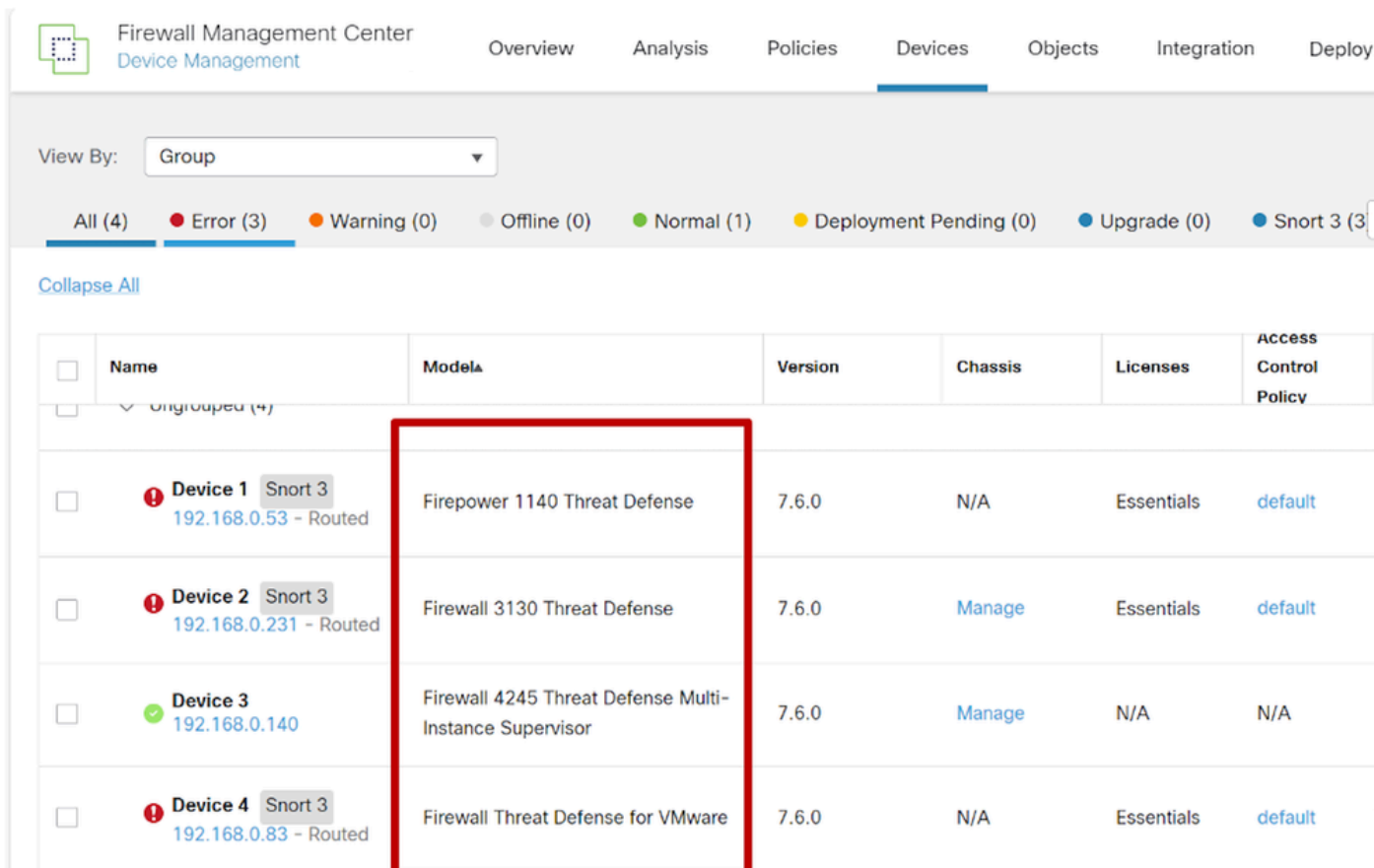
**Rules update version** : 2024-02-07-001-vrt

**LSP version** : lsp-rel-20240207-1539

**VDB version** : 377

Gestion des périphériques :

- Les périphériques gérés affichent des noms de modèle raccourcis.
- Firepower (ici FPR1140) et Secure Firewall Devices (ici, 3130, 4215 et FTD sur VMware) peuvent apparaître ensemble.



	Name	Model	Version	Chassis	Licenses	Access Control Policy
<input type="checkbox"/>	Device 1 <small>Snort 3</small> 192.168.0.53 - Routed	Firepower 1140 Threat Defense	7.6.0	N/A	Essentials	default
<input type="checkbox"/>	Device 2 <small>Snort 3</small> 192.168.0.231 - Routed	Firewall 3130 Threat Defense	7.6.0	Manage	Essentials	default
<input type="checkbox"/>	Device 3 192.168.0.140	Firewall 4245 Threat Defense Multi-Instance Supervisor	7.6.0	Manage	N/A	N/A
<input type="checkbox"/>	Device 4 <small>Snort 3</small> 192.168.0.83 - Routed	Firewall Threat Defense for VMware	7.6.0	N/A	Essentials	default

## Exemple de périphériques Firepower

État récapitulatif :

- Le nom complet du modèle est affiché dans les informations système du périphérique
- Le modèle FP 11XX est représenté par Firepower

The screenshot shows the Cisco Firepower management interface. The top navigation bar includes 'Analysis', 'Policies', 'Devices', 'Objects', 'Integration', and 'Deploy'. The 'Devices' tab is selected. Below the navigation bar, there are tabs for 'ICP', 'VTEP', and 'SNMP'. The main content area is divided into two panels. The left panel is titled 'License' and contains a table of license-related settings. The right panel is titled 'System' and contains system information. The 'Model' field in the 'System' panel is highlighted with a red box, showing 'Cisco Firepower 1140 Threat Defense'.

License	
Essentials:	Yes
Export-Controlled Features:	No
Malware Defense:	No
IPS:	No
Carrier:	No
URL:	No
Secure Client Premier:	No
Secure Client Advantage:	No

System	
Model:	Cisco Firepower 1140 Threat Defense
Serial:	JAD23330Q2Y
Time:	2024-02-13 15:41:11
Time Zone:	UTC (UTC+0:00)
Version:	7.6.0
Time Zone setting for Time based	UTC (UTC+0:00)

Détails du système du périphérique pare-feu sécurisé :

- Le nom complet du modèle est affiché dans les informations système du périphérique.
- CSF31XX est représenté sous le nom de Cisco Secure Firewall.



## Device 2

Cisco Secure Firewall 3130 Threat Defense

Device

Routing

Interfaces

Inline Sets

DHCP

VTEP

### System

Model:	Cisco Secure Firewall 3130 Threat Defense
Serial:	FJZ2531DT4T
Time:	2024-02-13 15:42:38
Time Zone:	UTC (UTC+0:00)
Version:	7.6.0
Time Zone setting for Time based Rules:	UTC (UTC+0:00)

### Inspection Engine

Inspection Engine:  
[Revert to Snort 2](#)

Gestionnaire de châssis pour 3100 / 4200 en mode multi-instance :

- Le nom complet du modèle est affiché dans les informations système du périphérique.
- Le châssis CSF42XX est représenté sous le nom de Cisco Secure Firewall.



## Chassis Manager: Device 3 Connected

Cisco Secure Firewall 4245 Threat Defense Multi-Instance Supervisor

Summary

Interfaces

Instances

System Configuration

Management IP: 192.168.0.140

Version: 7.6.0 (build 1383)



Paramètres par défaut de la configuration Firewall Threat Defense :

- Le nom d'hôte système par défaut est toujours firepower,

- Nous avons gardé la puissance de feu, car cela ne fait pas directement référence à la plateforme en cours d'exécution.
- L'utilisateur peut facilement modifier ce paramètre.

Voulez-vous configurer IPv4 ? (o/n) [o] :

Voulez-vous configurer IPv6 ? (o/n) [o] : n

Configurer IPv4 via DHCP ou manuellement ? (dhcp/manual) [manuel] :

Entrez une adresse IPv4 pour l'interface de gestion [192.168.0.190] : 192.168.0.231

Entrez un masque de réseau IPv4 pour l'interface de gestion [255.255.255.0] :

Entrez la passerelle par défaut IPv4 pour l'interface de gestion [interfaces-données] :  
192.168.0.254

Entrez un nom d'hôte complet pour ce système [firepower] :

Entrez une liste de serveurs DNS séparés par des virgules ou « aucun » [x.x.x.x] :

Entrez une liste de domaines de recherche séparés par des virgules ou « aucun » [] :

Si vos informations réseau ont changé, vous devez vous reconnecter.

## Exemples de Firewall Device Manager

État récapitulatif :

- La page principale du périphérique affiche le nom complet du modèle avec la marque Secure Firewall.

The screenshot shows the Firewall Device Manager interface. At the top, there is a navigation bar with icons for Monitoring, Policies, Objects, and Device: firepower. Below the navigation bar, the device model is displayed as 'Cisco Secure Firewall 3130 Threat Defense' in a red-bordered box. To the right of the model name, the software version is '7.6.0-1383', the VDB is '377.0', and the intrusion rule update is '20240124-1535'. Below this information, a network diagram shows the 'Inside Network' connected to the device's 'MGMT' and 'CONSOLE' ports. The device's ports are labeled 1/1 through 1/16 and SFP.



Dashboard System

Model Cisco Secure Firewall 3130 Threat Defense	Software 7.6.0-1383	VDB 377.0	Intrusion Rule Update 20240124-1535
--	------------------------	--------------	--

IP Address

Résultat de la CLI Firewall Threat Defense :

- Le nom complet du modèle est affiché avec le nom Secure Firewall.
- Ceci est également indiqué sur les connexions SSH.
- D'autres résultats de l'interface de ligne de commande, tels que show version, utilisent Secure Firewall au lieu de Firepower.

Gérer le périphérique localement ? (oui/non) [oui] :

Configuration du mode pare-feu en mode routé.

Mettre à jour les informations de déploiement

- ajouter une configuration de périphérique

Étapes de configuration initiale du premier démarrage pour Secure Firewall Device Manager for Secure Firewall Threat Defense.

> afficher la version

-----[ puissance de feu ]-----

Modèle : Cisco Secure Firewall 3130 Threat Defense (80) Version 7.6.0 (Build 13)

UUID : 123ab4d5-e6aa-11bb-ccc7-f88d99f000d

Version VDB : 377

Moniteur système du Gestionnaire de périphériques de pare-feu :

- Le tableau de bord de surveillance du système utilise également le nom de modèle correct.



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.