

Cisco Secure Firewallへのデバイス出力のブランド変更について

内容

[はじめに](#)

[前提条件](#)

[背景説明](#)

[要件](#)

[使用するコンポーネント](#)

[機能説明](#)

[設定](#)

[ファイアウォール管理センターの例](#)

[Firepowerデバイスの例](#)

[ファイアウォールデバイスマネージャの例](#)

はじめに

このドキュメントでは、Cisco Secure Firewallへのデバイス出力のブランド変更に関する情報について説明します。

前提条件

背景説明

- 表示されるデバイス名が他のブランディング資料と一致するようになりました。
- これにより、ブランドが強化され、ユーザエクスペリエンスが向上します
- プラットフォームの機能への影響はなく、テキストのみが変更されています。
- 古いFTDハードウェアプラットフォーム(FPR1010/11XX、FPR41XX、FPR93XX)では、引き続きFirepowerのブランド化が使用されます
- 一部のシステムデフォルトとコンポーネント名では、引き続きfirepowerを使用できます

要件

次の項目に関する知識があることが推奨されます。

- Cisco Next Gen Firewall(NGFW)ポートフォリオ

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Firepower Management Center (FMC) バージョン 7.6.0

- Firepowerデバイスマネージャ(FDM)バージョン7.6.0
- すべての仮想Firepower Threat Defense(FTD)バージョン7.6.0
- Cisco Secure Firewall 31XX、42XX

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

機能説明

仕組み：

- CSF31XX、CSF42XX、Firewall Threat Defense(FTD)Virtual、およびすべてのFirewall Management Center(FMC)プラットフォームの完全なモデル名と短いモデル名には、Cisco Secure Firewallのブランディングが含まれています。
- CSF31XX FDMソフトウェアがSFDM Secure Firewall Device Managerになりました。
- この機能には機能コンポーネントがありません。
- この機能の設定オプションはありません。

アップグレード:

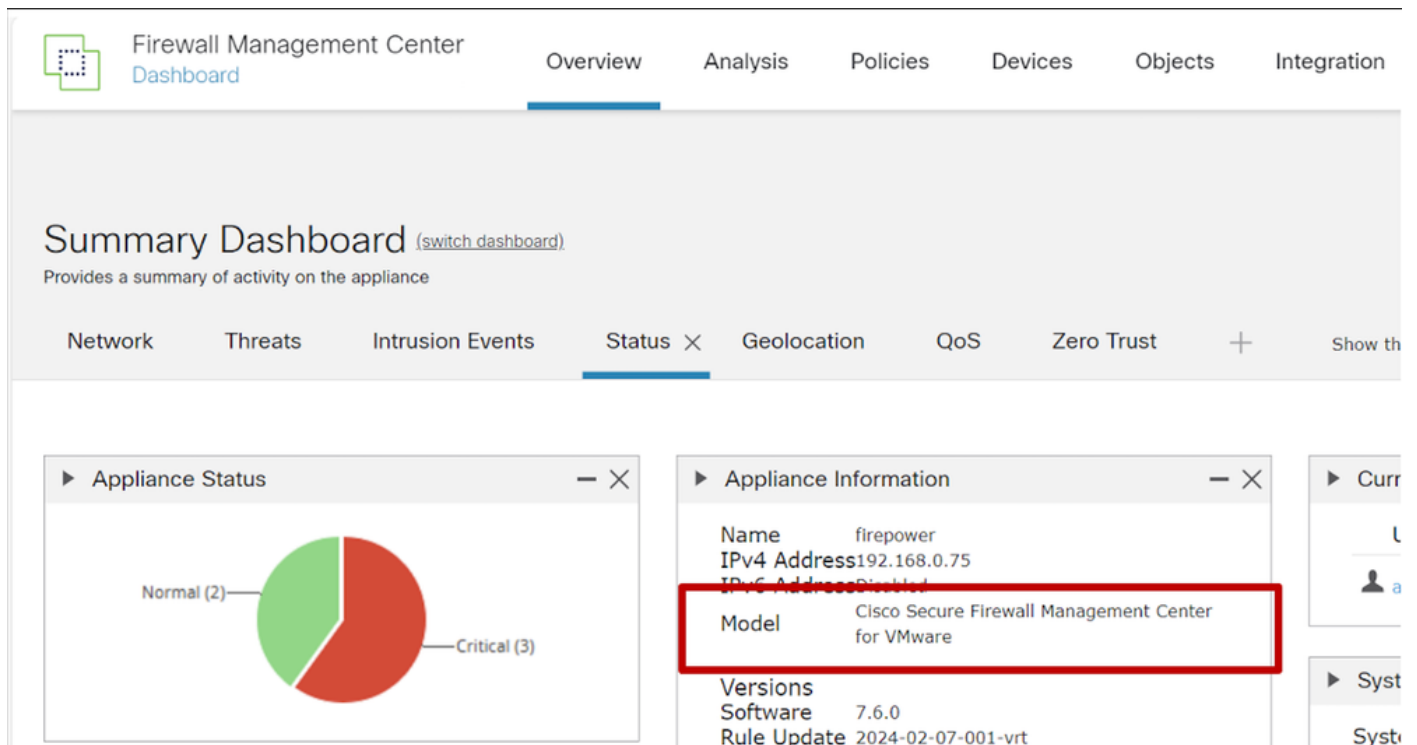
- Secure Firewall 7.6へのアップグレード時に、関連するすべてのCLIとGUIが更新され、現在のブランディングが反映されます。
- 登録デバイスのアップグレード中に問題が発生しない
 - Firewall Threat Defense(FTD)がアップグレードされると、Firewall Management Center(FMC)のGUIが最新のブランドで更新されます。
 - Firewall Management Center(FMC)がアップグレードされると、すべての登録済みデバイスはアップグレード後に期待どおりに接続を復元します。

設定

ファイアウォール管理センターの例

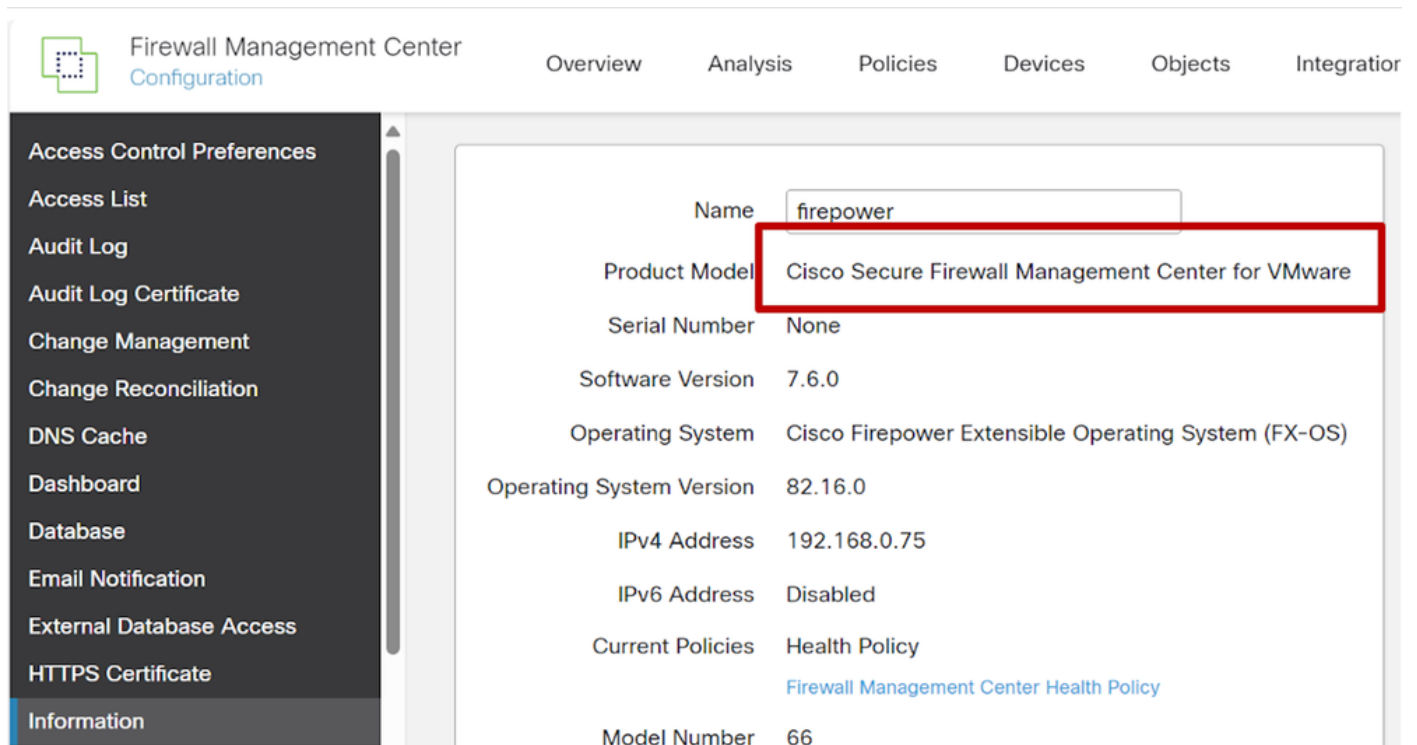
概要の状態：

- Management Centerモデル名の先頭にCiscoブランドが付加されています。



設定情報:

- Management Centerモデル名の先頭にCiscoブランドが付加されています。



CLI の出力 :

- Cisco Secure Firewallのブランディングでは、完全なモデル名が表示されます。

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
```

デバイス管理：

- ・ 管理対象デバイスのモデル名は短縮されています。
- ・ Firepower (ここではFPR1140) とセキュアファイアウォールデバイス (ここではVMware上の3130、4215、およびFTD) の両方を同時に表示できます。

Firewall Management Center
Device Management

OverviewAnalysisPoliciesDevicesObjectsIntegrationDeploy

View By: Group

All (4)Error (3)Warning (0)Offline (0)Normal (1)Deployment Pending (0)Upgrade (0)Snort 3 (3)

Collapse All

	Name	Model	Version	Chassis	Licenses	Access Control Policy
	Un grouped (4)					
	Device 1 192.168.0.53 - Routed	Firepower 1140 Threat Defense	7.6.0	N/A	Essentials	default
	Device 2 192.168.0.231 - Routed	Firewall 3130 Threat Defense	7.6.0	Manage	Essentials	default
	Device 3 192.168.0.140	Firewall 4245 Threat Defense Multi-Instance Supervisor	7.6.0	Manage	N/A	N/A
	Device 4 192.168.0.83 - Routed	Firewall Threat Defense for VMware	7.6.0	N/A	Essentials	default

Firepowerデバイスの例

概要の状態：

- 完全なモデル名がデバイスのシステム情報に表示される
- FP 11XXはFirepowerとして表示されます

The screenshot shows the Cisco Firepower Management Center (FMC) interface. The top navigation bar includes tabs for Analysis, Policies, Devices (selected), Objects, Integration, and Deploy. A search icon and a notification bell with a '2' are also present. The user 'admin' is logged in. Below the navigation bar, there are tabs for ICP, VTEP, and SNMP. The main content area is divided into two panels. The left panel, titled 'License', shows a list of license features with their status: Essentials (Yes), Export-Controlled Features (No), Malware Defense (No), IPS (No), Carrier (No), URL (No), Secure Client Premier (No), and Secure Client Advantage (No). The right panel, titled 'System', shows the device's system information. The 'Model' field is highlighted with a red box and contains the text 'Cisco Firepower 1140 Threat Defense'. Other fields include Serial (JAD23330Q2Y), Time (2024-02-13 15:41:11), Time Zone (UTC (UTC+0:00)), Version (7.6.0), and Time Zone setting for Time based (UTC (UTC+0:00)).

License	System
Essentials:	Model: Cisco Firepower 1140 Threat Defense
Export-Controlled Features:	Serial: JAD23330Q2Y
Malware Defense:	Time: 2024-02-13 15:41:11
IPS:	Time Zone: UTC (UTC+0:00)
Carrier:	Version: 7.6.0
URL:	Time Zone setting for Time based: UTC (UTC+0:00)
Secure Client Premier:	
Secure Client Advantage:	

セキュアファイアウォールデバイスのシステム詳細：

- 完全なモデル名は、デバイスのシステム情報に表示されます。
- CSF31XXはCisco Secure Firewallとして表示されます。



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](#)

マルチインスタンスモードの3100/4200用シャーシマネージャ :

- 完全なモデル名は、デバイスのシステム情報に表示されます。
- CSF42XXシャーシはCisco Secure Firewallとして表示されます。



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)



CONSOLE



MGMT2



MGMT1



USB

Network M

1/1

1/2



1/5



1/6

ファイアウォール脅威対策のデフォルト設定 :

- システムホスト名のデフォルトはfirepower、

- FirePOWERは実行中のプラットフォームを直接参照しないため、保持しました。
- これはユーザが簡単に変更できます。

IPv4を構成しますか？(y/n) [y]:

IPv6を構成しますか？(y/n) [y]: n

DHCP経由でIPv4を設定するか、手動で設定するか。(dhcp/manual) [manual]:

管理インターフェイス[192.168.0.190]のIPv4アドレスを入力してください： 192.168.0.231

管理インターフェイス[255.255.255.0]のIPv4ネットマスクを入力してください：

管理インターフェイスのIPv4デフォルトゲートウェイを入力[データインターフェイス]:192.168.0.254

このシステムの完全修飾ホスト名を入力[firepower]:

DNSサーバーのコンマ区切りの一覧を入力または'なし' [x.x.x.x]:

検索ドメインのコンマ区切りリストを入力または'なし' []:

ネットワーク情報が変更された場合は、再接続する必要があります。

ファイアウォールデバイスマネージャの例

概要の状態：

- メインデバイスページには、セキュアファイアウォールのブランド付きの完全なモデル名が表示されます。

The screenshot shows the 'Firewall Device Manager' interface. The top navigation bar includes 'Monitoring', 'Policies', 'Objects', and 'Device: firepower'. The main content area displays the configuration for a 'Cisco Secure Firewall 3130 Threat Defense' device. A red box highlights the 'Model' field, which contains 'Cisco Secure Firewall 3130 Threat Defense'. Other fields shown include 'Software' (7.6.0-1383), 'VDB' (377.0), and 'Intrusion Rule Update' (20240124-1535). Below the configuration table, there is a diagram showing the device's network interfaces. The 'MGMT' (Management) interface is highlighted with a green checkmark. The 'CONSOLE' interface is also shown. The diagram includes a green box labeled 'Inside Network' connected to the 'MGMT' interface. The device's ports are labeled 1/1 through 1/16, with 1/1 and 1/2 being the primary interfaces. A green box with '1/2' is also visible.

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

ファイアウォール脅威対策のCLI出力：

- 完全なモデル名は、セキュアファイアウォールの名前付けとともに表示されます。
- これはSSHログインでも表示されます。
- show versionなどの他のCLI出力では、Firepowerの代わりにSecure Firewallが使用されます。

デバイスをローカルで管理する(yes/no) [yes]:

ファイアウォールモードをルーテッドに設定しています。

ポリシー展開情報の更新

– デバイス構成の追加

Secure Firewall Threat Defense用のSecure Firewall Device Managerの初回ブート初期設定手順が正常に実行されました。

>バージョンの表示

-----[firepower]-----

モデル：Cisco Secure Firewall 3130 Threat Defense(80)/バージョン7.6.0 (ビルド13)

UUID:123ab4d5-e6aa-11bb-ccc7-f888d99f000d

VDBバージョン：377

Firewall Device Managerシステムモニタ：

- システム監視ダッシュボードでも、正しいモデル名が使用されます。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。