

Entender a renomeação de saídas de dispositivos para o Cisco Secure Firewall

Contents

[Introdução](#)

[Pré-requisitos](#)

[Informações de Apoio](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Descrição do recurso](#)

[Configurar](#)

[Exemplos do Centro de gerenciamento de firewall](#)

[Exemplo de dispositivos Firepower](#)

[Exemplos do gerenciador de dispositivos de firewall](#)

Introdução

Este documento descreve insights sobre Renomeação de Saídas de Dispositivos para o Cisco Secure Firewall.

Pré-requisitos

Informações de Apoio

- Os nomes de dispositivos exibidos agora correspondem a outros materiais de marca
- Isso cria uma marca mais forte e uma experiência de usuário mais direta
- Sem impacto funcional em nenhuma plataforma; somente o texto foi alterado.
- Plataformas de hardware FTD mais antigas (FPR1010/11XX, FPR41XX, FPR93XX) ainda usam a marca Firepower
- Alguns padrões do sistema e nomes de componentes ainda podem usar o firepower

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Portfólio do firewall de próxima geração (NGFW) da Cisco

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Firepower Management Center(FMC) versão 7.6.0

- Firepower Device Manager (FDM) versão 7.6.0
- All Virtual Firepower Threat Defense(FTD) versão 7.6.0
- Firewall seguro da Cisco 31XX,42XX

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Descrição do recurso

Como funciona:

- Os nomes completos de modelos e os nomes curtos de modelos para CSF31XX, CSF42XX, Firewall Threat Defense (FTD) Virtual e todas as plataformas Firewall Management Center (FMC) contêm a marca Cisco Secure Firewall.
- O software CSF31XX FDM agora é o SFDM, Secure Firewall Device Manager.
- Não há componentes funcionais para este recurso.
- Não há opções de configuração para este recurso.

Atualizando:

- Ao atualizar para o Secure Firewall 7.6, todas as CLIs e GUIs relevantes foram atualizadas para refletir a marca atual.
- Nenhum problema durante a atualização para dispositivos registrados
 - Se o Firewall Threat Defense (FTD) for atualizado, o Firewall Management Center (FMC) atualizará sua GUI com a marca atual.
 - Se o Firewall Management Center (FMC) for atualizado, todos os dispositivos registrados restaurarão a conectividade após a atualização, conforme esperado.

Configurar

Exemplos do Centro de gerenciamento de firewall

Status do resumo:

- O nome do modelo do Management Center tem a marca Cisco anexada.

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

Status	Count
Normal	2
Critical	3

► 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

► Curr

U

a

► Syst

Syst

Informações de configuração:

- O nome do modelo do Management Center tem a marca Cisco anexada.

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

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

[Firewall Management Center Health Policy](#)

Model Number 66

Saída CLI:

- O nome completo do modelo é mostrado com a marca 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

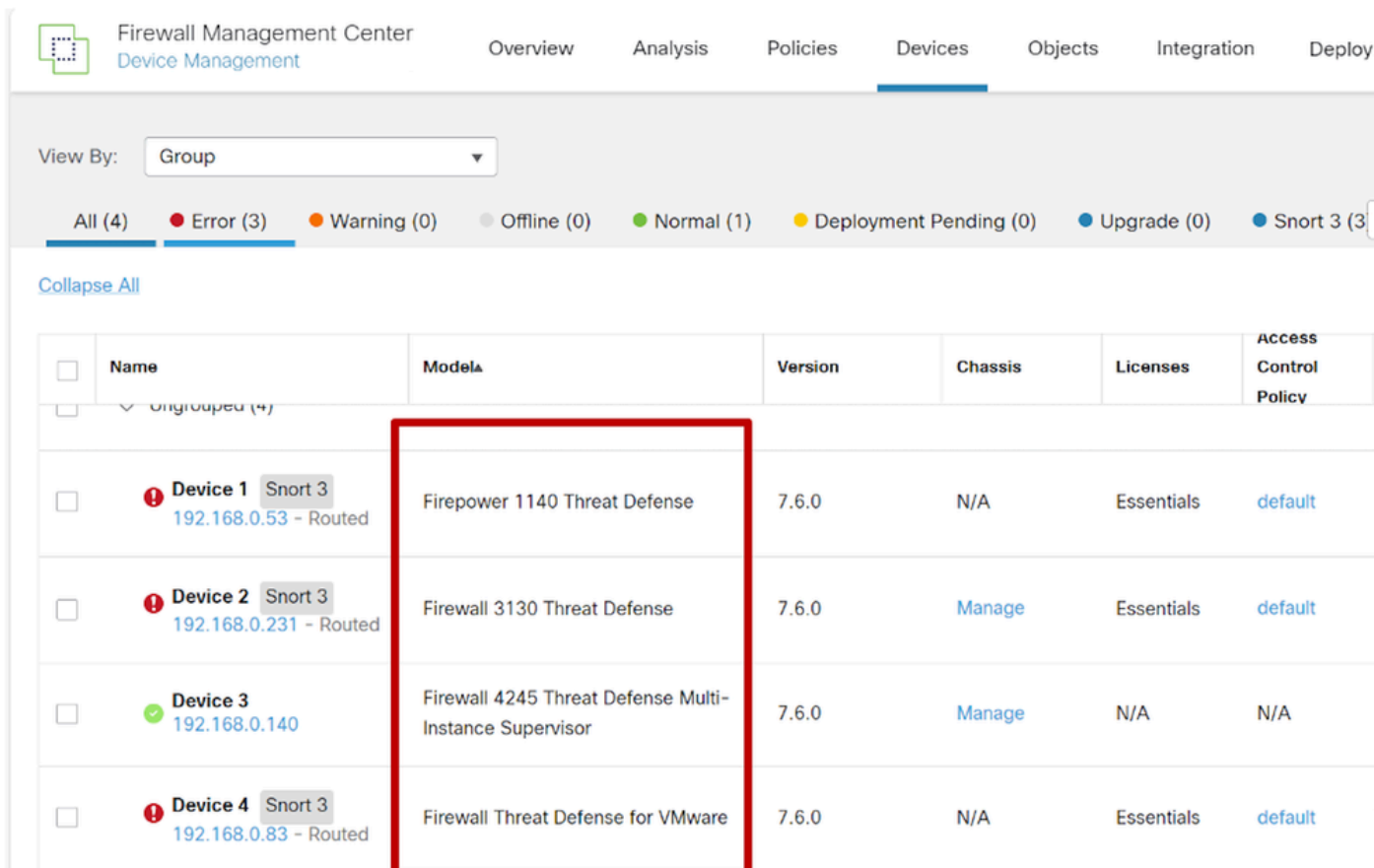
Rules update version : 2024-02-07-001-vrt

LSP version : lsp-rel-20240207-1539

VDB version : 377

Gerenciamento de dispositivos:

- Os dispositivos gerenciados mostram nomes de modelo abreviados.
- Os dispositivos Firepower (FPR1140 aqui) e Secure Firewall (3130, 4215 e FTD no VMware) podem aparecer juntos.



Firewall Management Center
Device Management

Overview Analysis Policies **Devices** Objects Integration Deploy

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
<input type="checkbox"/>	Ungrouped (4)					
<input type="checkbox"/>	Device 1 Snort 3 192.168.0.53 - Routed	Firepower 1140 Threat Defense	7.6.0	N/A	Essentials	default
<input type="checkbox"/>	Device 2 Snort 3 192.168.0.231 - 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 Snort 3 192.168.0.83 - Routed	Firewall Threat Defense for VMware	7.6.0	N/A	Essentials	default

Exemplo de dispositivos Firepower

Status do resumo:

- O nome completo do modelo é mostrado nas informações do sistema do dispositivo
- FP 11XX é mostrado como Firepower

The screenshot shows the Cisco Firepower Management Center interface. The top navigation bar includes 'Analysis', 'Policies', 'Devices', 'Objects', 'Integration', and 'Deploy'. The 'Devices' tab is active. 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)

Detalhes do sistema para o dispositivo de firewall seguro:

- O nome completo do modelo é mostrado nas informações do sistema do dispositivo.
- CSF31XX é mostrado como 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](#)

Gerenciador de chassi para 3100 / 4200 no modo de várias instâncias:

- O nome completo do modelo é mostrado nas informações do sistema do dispositivo.
- O chassi CSF42XX é mostrado como 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)



Padrões de configuração do Firewall Threat Defense:

- O nome de host padrão do sistema ainda é firepower,

- Mantivemos o poder de fogo, porque isso não faz referência direta à plataforma em execução.
- Isso pode ser facilmente alterado pelo usuário.

Deseja configurar o IPv4? (s/n) [s]:

Deseja configurar o IPv6? (s/n) [s]: n

Configurar o IPv4 via DHCP ou manualmente? (dhcp/manual) [manual]

Insira um endereço IPv4 para a interface de gerenciamento [192.168.0.190]: 192.168.0.231

Insira uma máscara de rede IPv4 para a interface de gerenciamento [255.255.255.0]:

Insira o gateway padrão IPv4 para a interface de gerenciamento [interfaces de dados]:
192.168.0.254

Digite um nome de host totalmente qualificado para este sistema [firepower]:

Insira uma lista separada por vírgulas de servidores DNS ou 'nenhum' [x.x.x.x]:

Insira uma lista separada por vírgulas dos domínios de pesquisa ou 'nenhum' []:

Se as informações de sua rede foram alteradas, será necessário reconectar.

Exemplos do gerenciador de dispositivos de firewall

Status do resumo:

- A página do dispositivo principal mostra o nome completo do modelo com a marca Secure Firewall.

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 summary for the device:

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

Below the summary, a network diagram shows the device connected to an 'Inside Network'. The device configuration details include:

- MGMT:
- CONSOLE:
- Interfaces: 1/1, 1/2, 1/3, 1/4, 1/5, 1/6, 1/7, 1/8, 1/9, 1/10, 1/11, 1/12, 1/13, 1/14, 1/15, 1/16, 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

Saída da CLI do Firewall Threat Defense:

- O nome completo do modelo é mostrado com a nomeação do Firewall Seguro.
- Isso também é mostrado nos logons SSH.
- Outra saída CLI, como show version, usa o Secure Firewall em vez do Firepower.

Gerenciar o dispositivo localmente? (sim/não) [sim]:

Configurando o modo de firewall para roteado.

Atualizar informações de implantação da política

- adicionar configuração de dispositivo

Êxito ao executar as etapas de configuração inicial da primeira inicialização do Gerenciador de dispositivos do firewall seguro para defesa contra ameaças do firewall seguro.

> show version

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

Modelo: Cisco Secure Firewall 3130 Threat Defense (80) Versão 7.6.0 (Build 13)

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

Versão do VDB: 377

Monitor de sistema do Gerenciador de dispositivos de firewall:

- O painel de monitoramento do sistema também usa o nome do modelo correto.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.