Informazioni sul rebranding degli output dei dispositivi in Cisco Secure Firewall

Sommario

- Introduzione
- Prerequisiti
  - Premesse
  - Requisiti
  - Componenti usati
  - Descrizione delle funzionalità
- Configurazione
  - Esempi di Firewall Management Center
  - Esempio di dispositivi Firepower
  - Esempi di Gestione periferiche firewall

Introduzione

In questo documento viene illustrato come riassegnare i marchi di output dei dispositivi a Cisco Secure Firewall.

Prerequisiti

Premesse

- I nomi dei dispositivi visualizzati ora corrispondono ad altri materiali di branding
- In questo modo si crea un marchio più forte e un'esperienza utente più semplice
- nessun impatto funzionale su nessuna piattaforma; è stato modificato solo il testo.
- Le piattaforme hardware FTD meno recenti (FPR1010/11XX, FPR41XX, FPR93XX) utilizzano ancora il branding Firepower
- Alcuni valori predefiniti di sistema e nomi di componenti possono ancora utilizzare firepower

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Portafoglio Cisco Next Gen Firewall (NGFW)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Firepower Management Center (FMC) versione 7.6.0
- Firepower Device Manager (FDM) versione 7.6.0
- All Virtual Firepower Threat Defense (FTD) versione 7.6.0
- Cisco Secure Firewall 31XX,42XX

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Descrizione delle funzionalità

Come funziona:

- I nomi di modelli completi e brevi per le piattaforme CSF31XX, CSF42XX, Firewall Threat Defense (FTD) Virtual e tutte le piattaforme Firewall Management Center (FMC) contengono il marchio Cisco Secure Firewall.
- Il software CSF31XX FDM è ora SFDM, Secure Firewall Device Manager.
- Non esistono componenti funzionali per questa feature.
- Nessuna opzione di configurazione disponibile per questa funzionalità.

Aggiornamento:

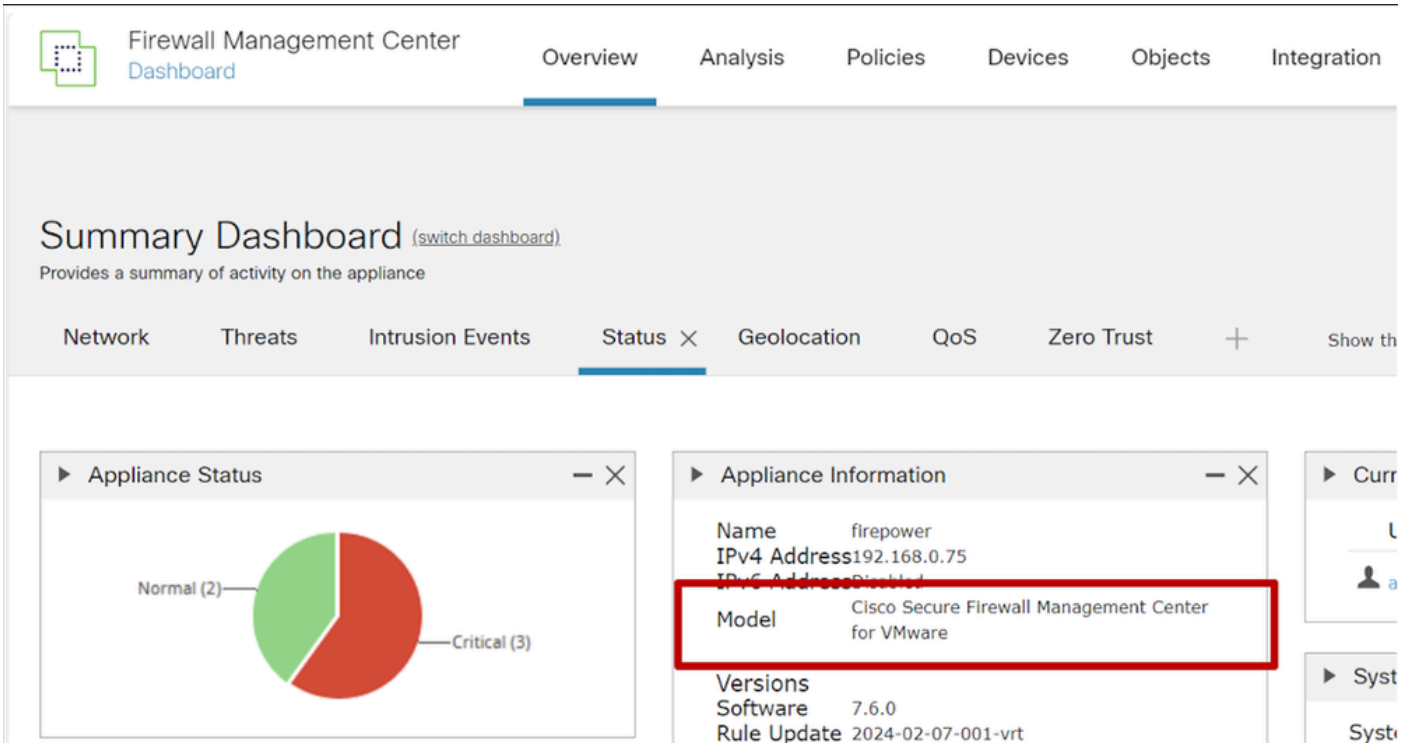
- Quando si esegue l'aggiornamento a Secure Firewall 7.6, tutte le CLI e le GUI rilevanti vengono aggiornate in base al marchio corrente.
- Nessun problema durante l'aggiornamento per i dispositivi registrati
    - Se Firewall Threat Defense (FTD) è aggiornato, Firewall Management Center (FMC) aggiorna la GUI con la personalizzazione corrente.
    - Se il Centro gestione firewall (FMC) viene aggiornato, tutti i dispositivi registrati ripristinano la connettività dopo l'aggiornamento come previsto.

Configurazione

Esempi di Firewall Management Center

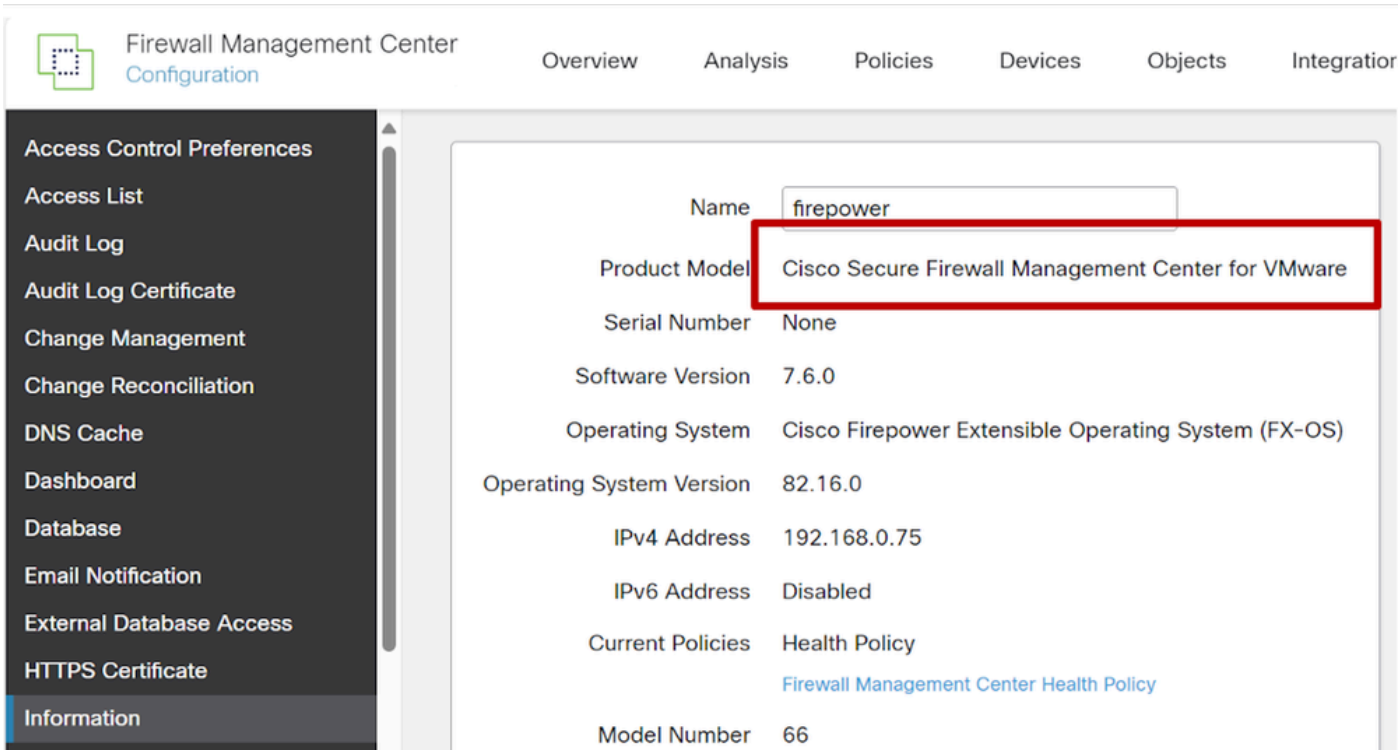
Stato riepilogo:

- Al nome del modello di Management Center è anteposto il marchio Cisco.



Informazioni di configurazione:

- Al nome del modello di Management Center è anteposto il marchio Cisco.



Output CLI:

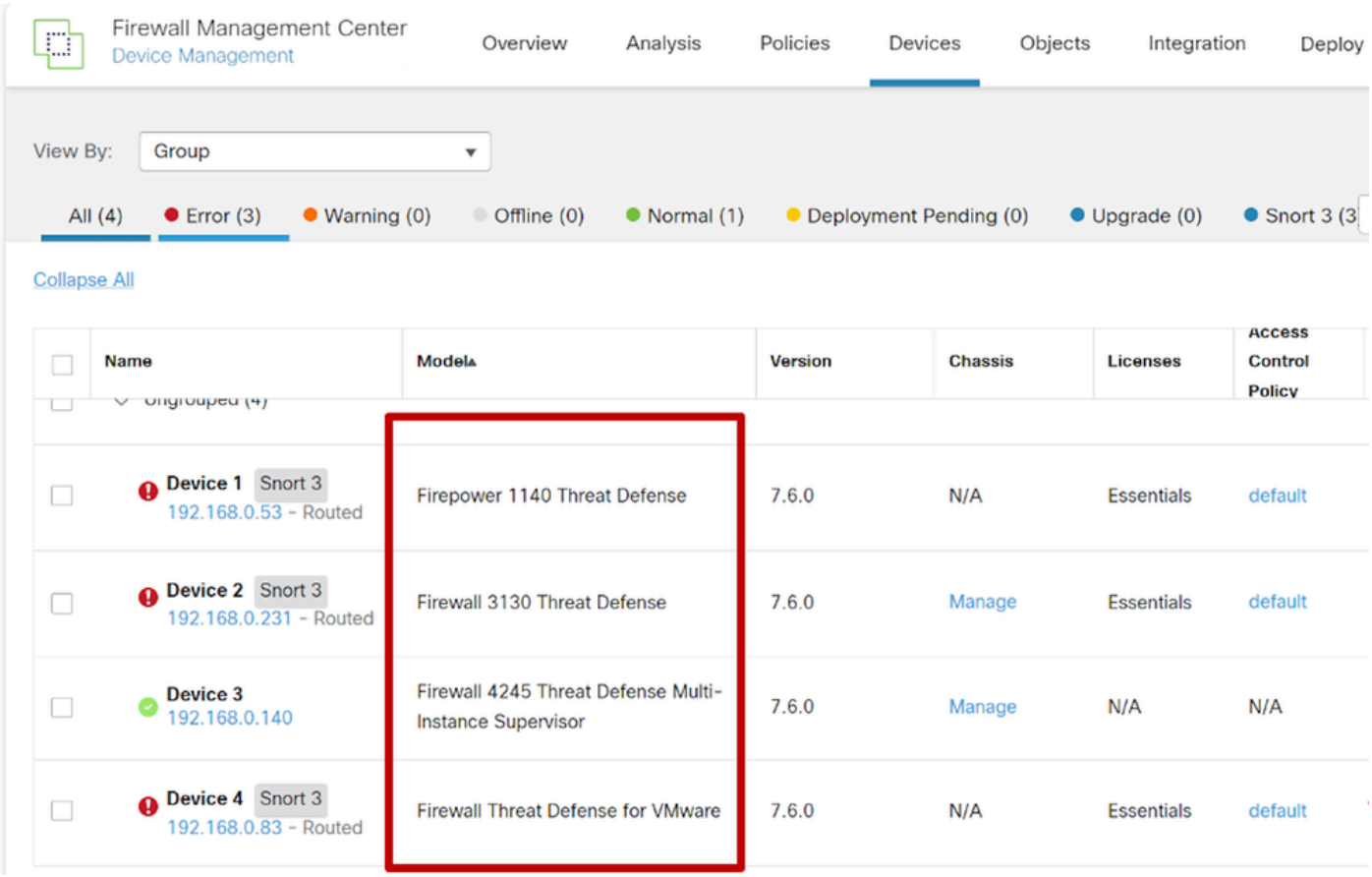
- Il nome completo del modello viene mostrato con il marchio Cisco Secure Firewall.

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
```

Gestione dispositivi:

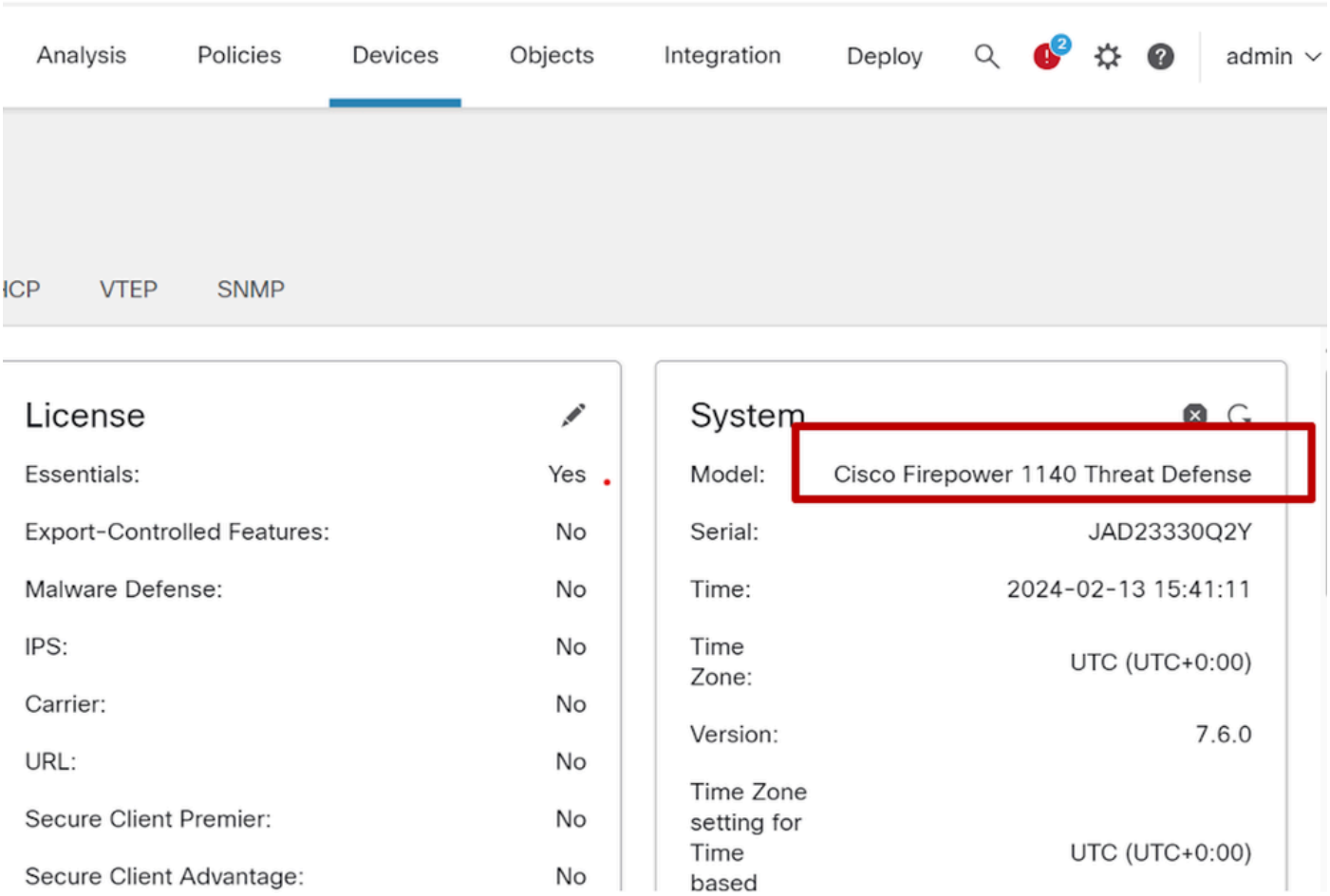
- I dispositivi gestiti mostrano nomi di modelli abbreviati.
- Firepower (FPR1140 qui) e Secure Firewall Devices (qui, 3130, 4215 e FTD su VMware) possono comparire insieme.



Esempio di dispositivi Firepower

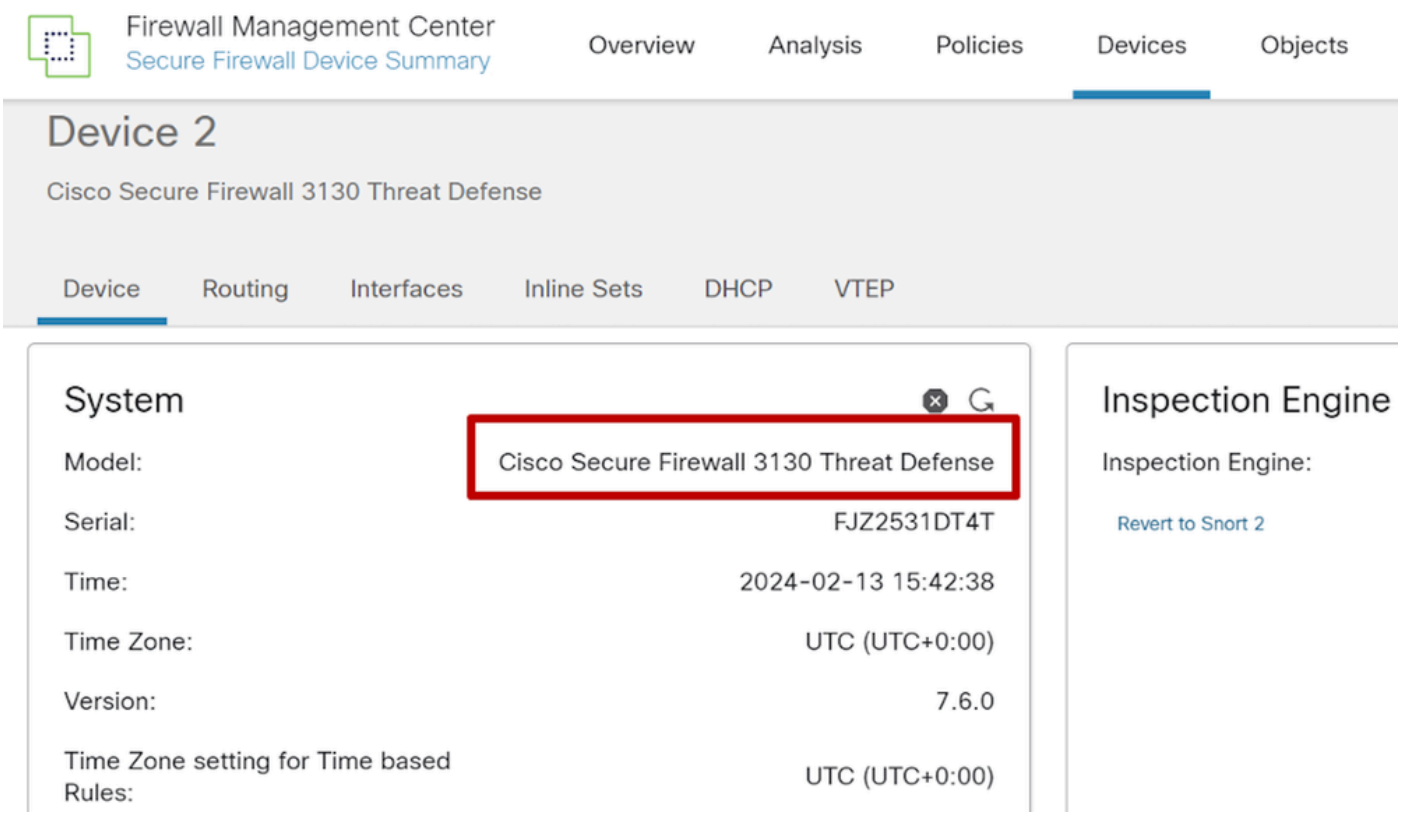
Stato riepilogo:

- Il nome completo del modello è visualizzato nelle informazioni di sistema del dispositivo
- FP 11XX viene visualizzato come Firepower



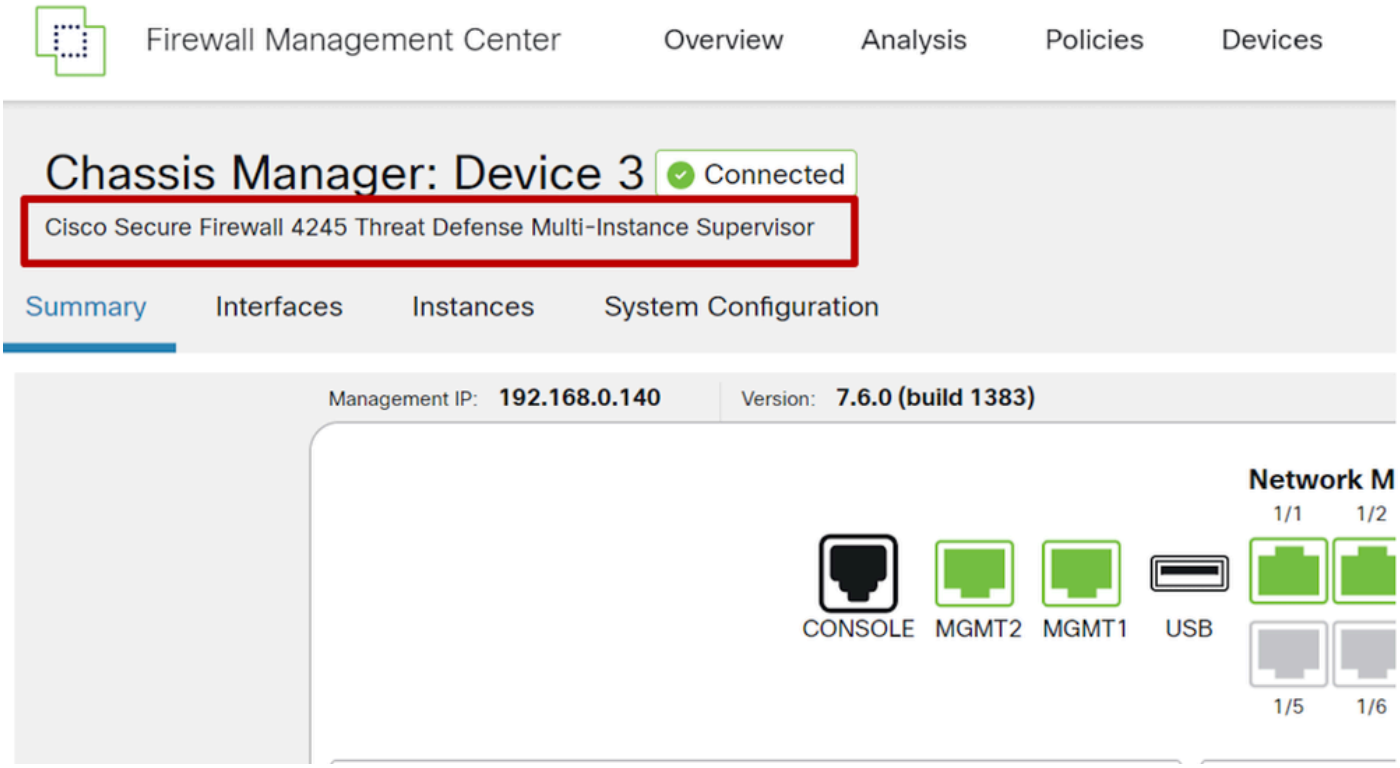
Dettagli sistema per dispositivo firewall protetto:

- Il nome completo del modello è indicato nelle informazioni di sistema del dispositivo.
- CSF31XX viene visualizzato come Cisco Secure Firewall.



Chassis Manager per 3100/4200 in modalità multi-istanza:

- Il nome completo del modello è indicato nelle informazioni di sistema del dispositivo.
- Lo chassis CSF42XX viene visualizzato come Cisco Secure Firewall.



Impostazioni predefinite di configurazione di Firewall Threat Defense:

- Il nome host di sistema predefinito è ancora firepower,

- Abbiamo mantenuto la potenza di fuoco, perché questo non fa direttamente riferimento alla piattaforma in esecuzione.
- L'utente può modificare facilmente questa impostazione.

Configurare IPv4? (s/n) [s]:

Configurare IPv6? (s/n) [s]: n

Configurare IPv4 tramite DHCP o manualmente? (dhcp/manual) [manuale]:

Immettere un indirizzo IPv4 per l'interfaccia di gestione [192.168.0.190]: 192.168.0.231

Immettere una maschera di rete IPv4 per l'interfaccia di gestione [255.255.255.0]:

Immettere il gateway predefinito IPv4 per l'interfaccia di gestione [data-interfaces]: 192.168.0.254

Immettere un nome host completo per il sistema [firepower]:

Immettere un elenco di server DNS separati da virgole o 'none' [x.x.x]:

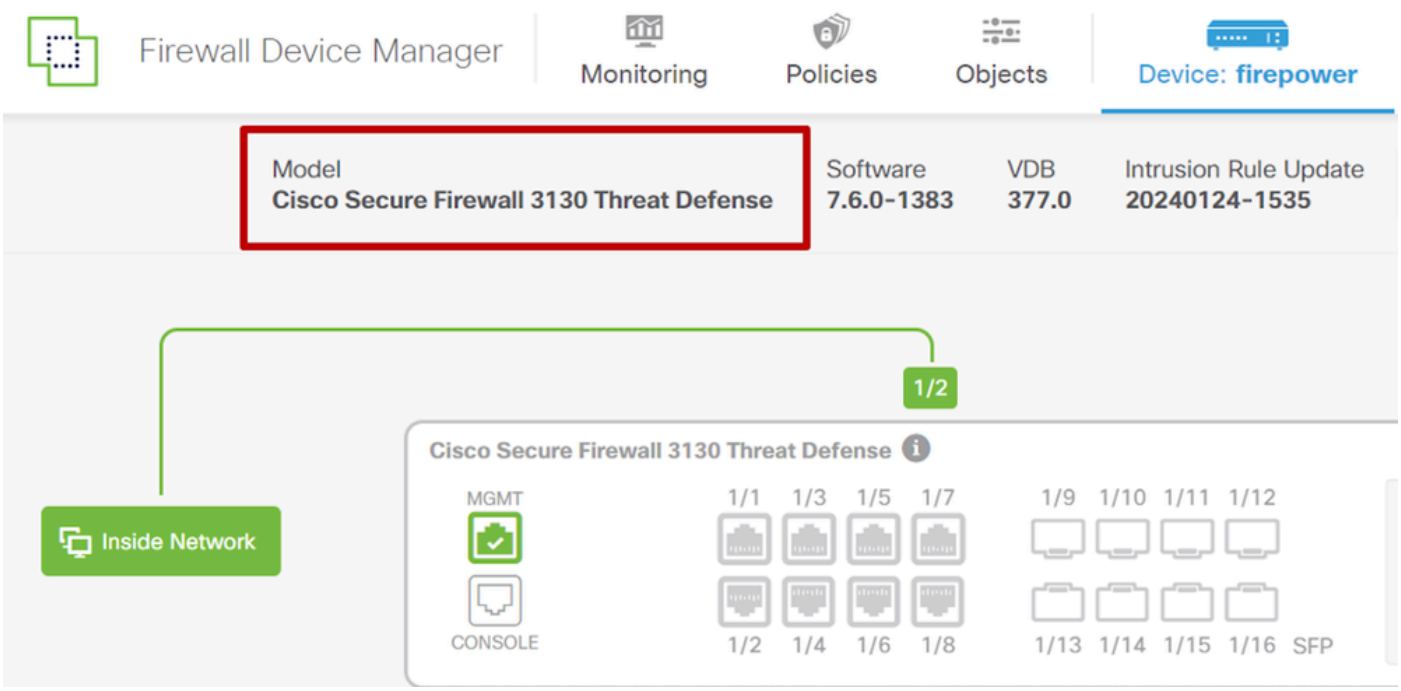
Immettere un elenco di domini di ricerca separati da virgole o 'none' []:

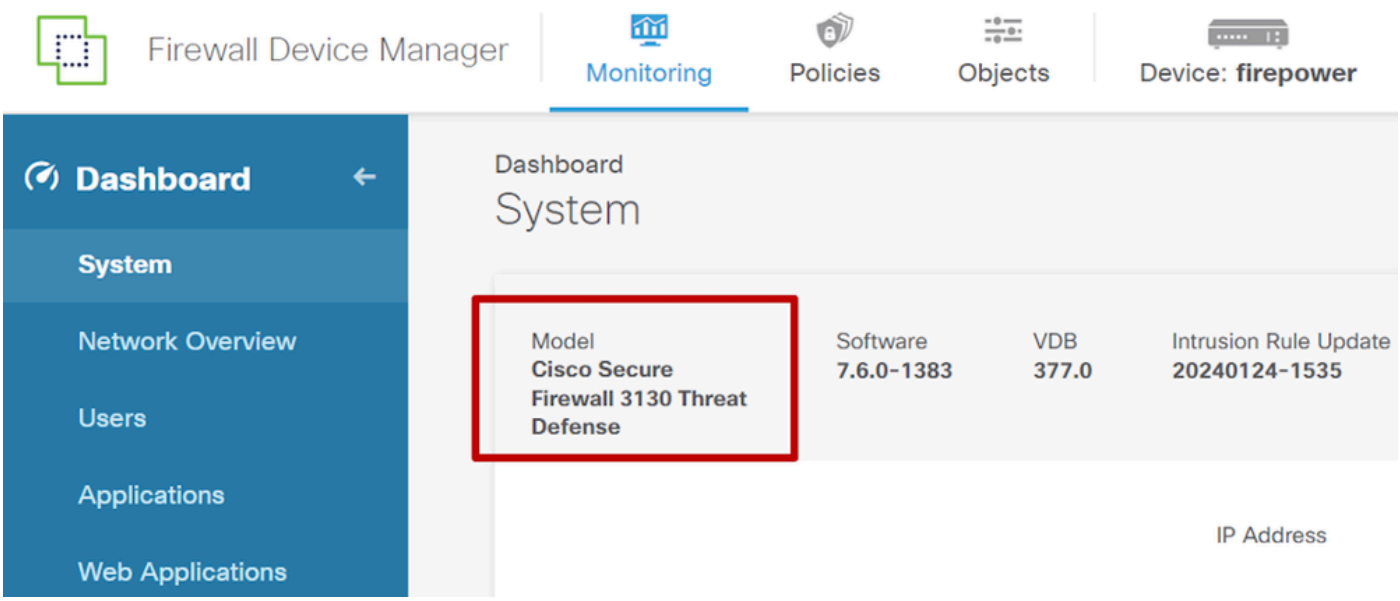
Se le informazioni di rete sono state modificate, è necessario riconnettersi.

Esempi di Gestione periferiche firewall

Stato riepilogo:

- Nella pagina del dispositivo principale viene visualizzato il nome completo del modello con il marchio Secure Firewall.





Output CLI di Firewall Threat Defense:

- Il nome completo del modello viene visualizzato con la denominazione Secure Firewall.
- Questa condizione viene mostrata anche negli accessi SSH.
- In altri output CLI, ad esempio show version, viene usato Secure Firewall invece di Firepower.

Gestire il dispositivo localmente? (sì/no) [sì]:

Configurazione della modalità firewall per il routing.

Aggiorna informazioni sulla distribuzione dei criteri

- aggiungere la configurazione del dispositivo

La procedura di configurazione iniziale per il primo avvio di Gestione periferiche firewall protette per la difesa dalle minacce del firewall è stata completata.

> show version

—[potenza di fuoco]—

Modello: Cisco Secure Firewall 3130 Threat Defense (80) versione 7.6.0 (build 13)

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

Versione VDB: 377

—

Monitor di sistema di Gestione periferiche firewall:

- Anche il dashboard di monitoraggio del sistema utilizza un nome di modello corretto.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).