Configurare una pianificazione di aggiornamento regolare del database per VDB su FDM

Sommario

[Introduzione](#)

[Prerequisiti](#)

- [Requisiti](#)
- [Componenti usati](#)

[Premesse](#)

[Configurazione](#)

- [Configurazioni](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come configurare una pianificazione di aggiornamento regolare del database per la regola o VDB in FDM.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Firepower Device Manager
- VDB (Vulnerability Database)

Componenti usati

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

- FDM 7.0

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.

Premesse

Il Cisco Vulnerability Database (VDB) è un database di vulnerabilità note agli host vulnerabili, nonché di impronte digitali per sistemi operativi, client e applicazioni.

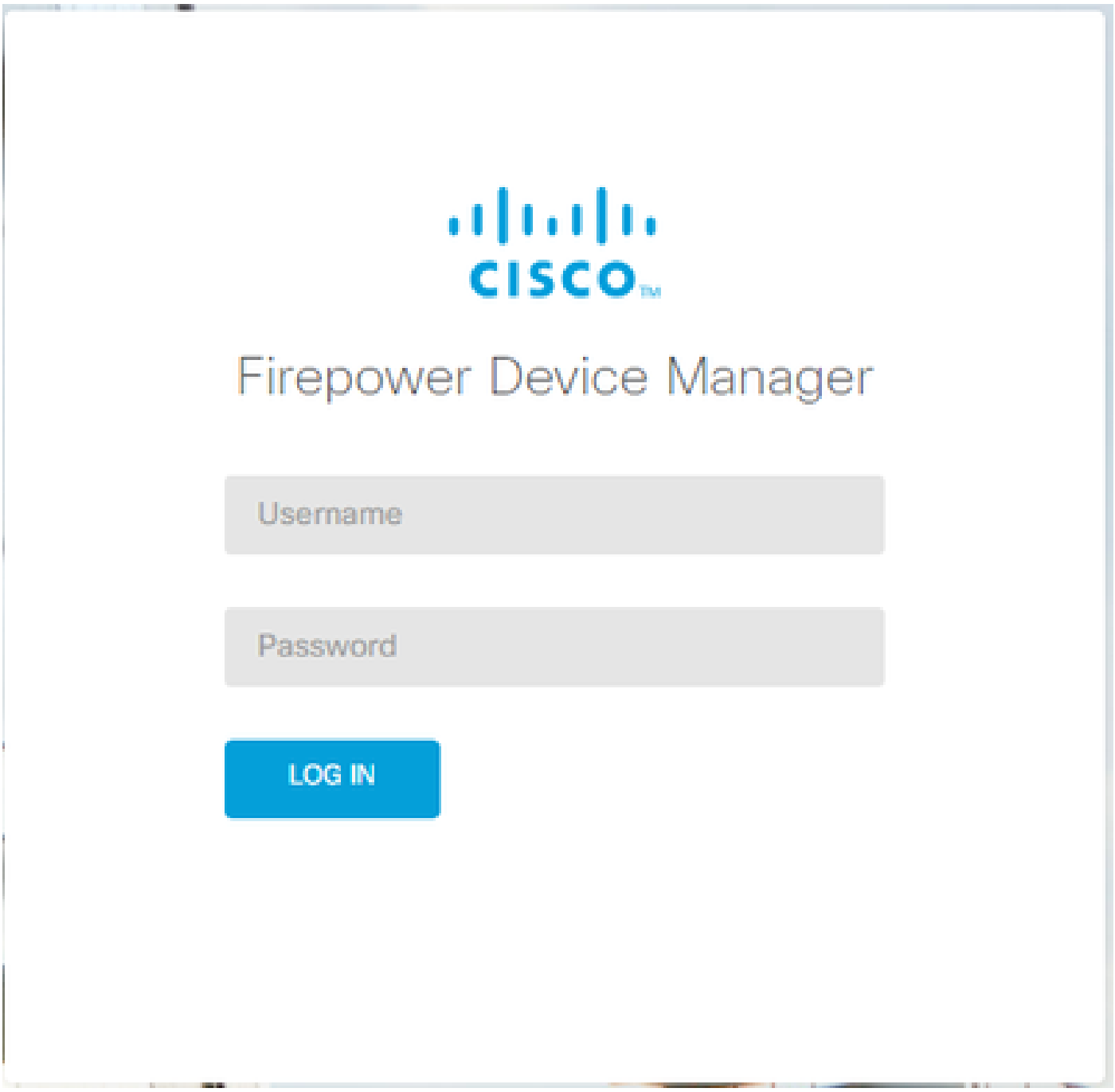
Il sistema firewall mette in correlazione le impronte digitali con le vulnerabilità per consentire di determinare se un determinato host aumenta il rischio di compromissione della rete. Il Cisco Talos Intelligence Group (Talos) aggiorna periodicamente il VDB.

È consigliabile attivare lo scheduler automatico durante il processo di caricamento per verificare regolarmente la disponibilità di aggiornamenti al database di protezione e applicarli. In questo modo il dispositivo rimane sempre aggiornato.

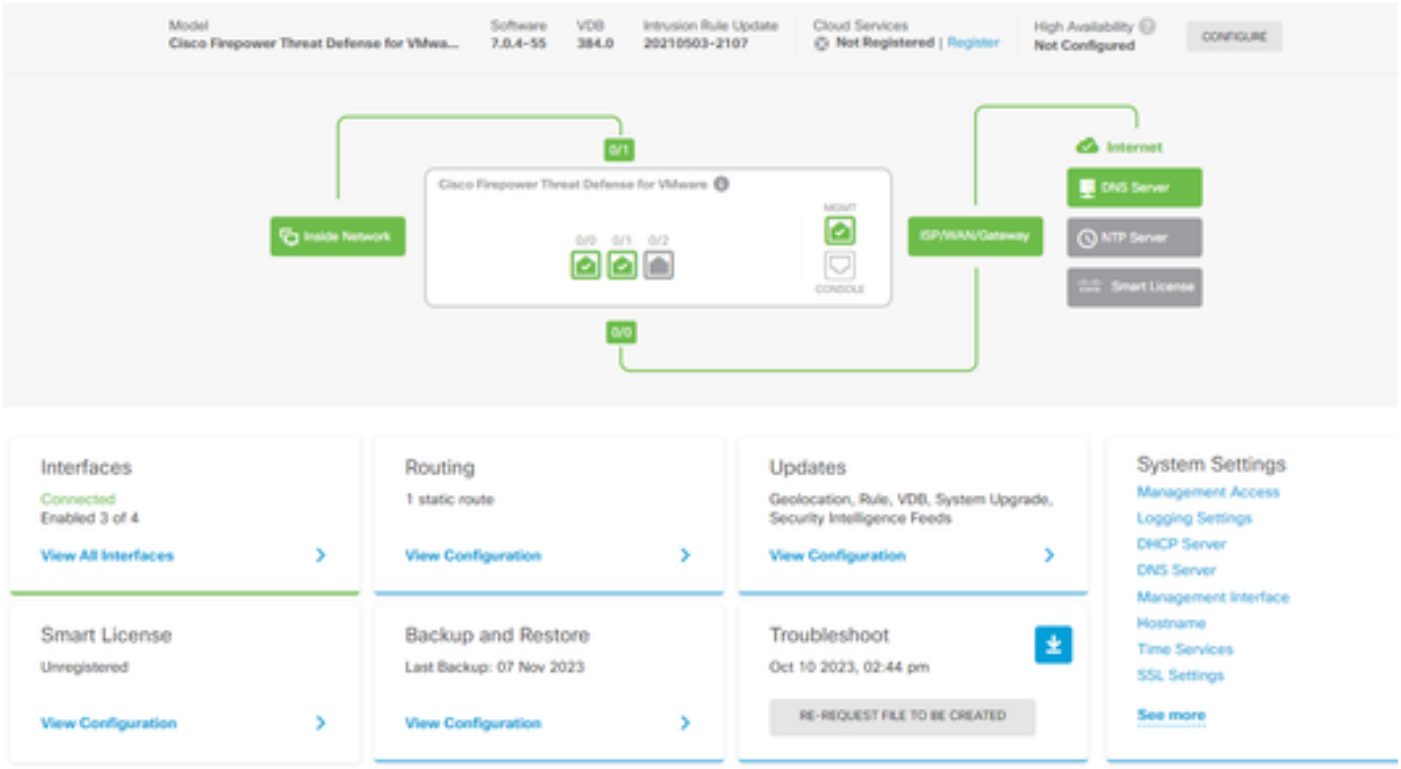
Configurazione

Configurazioni

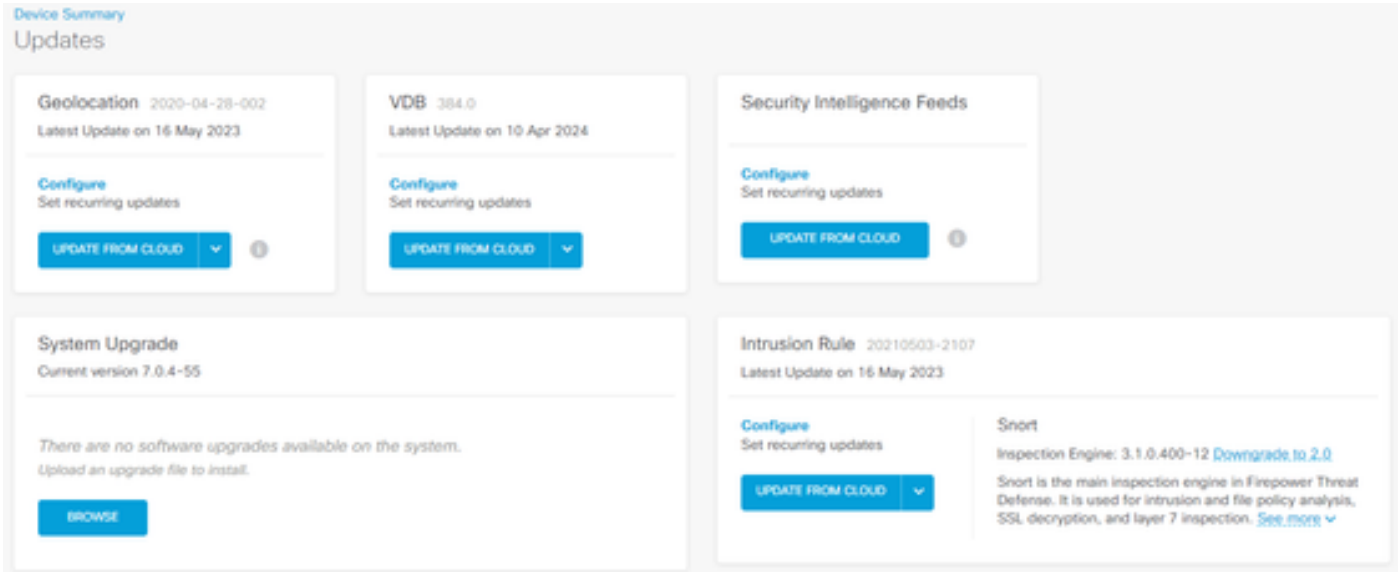
1. Accedere a Firepower Device Manager



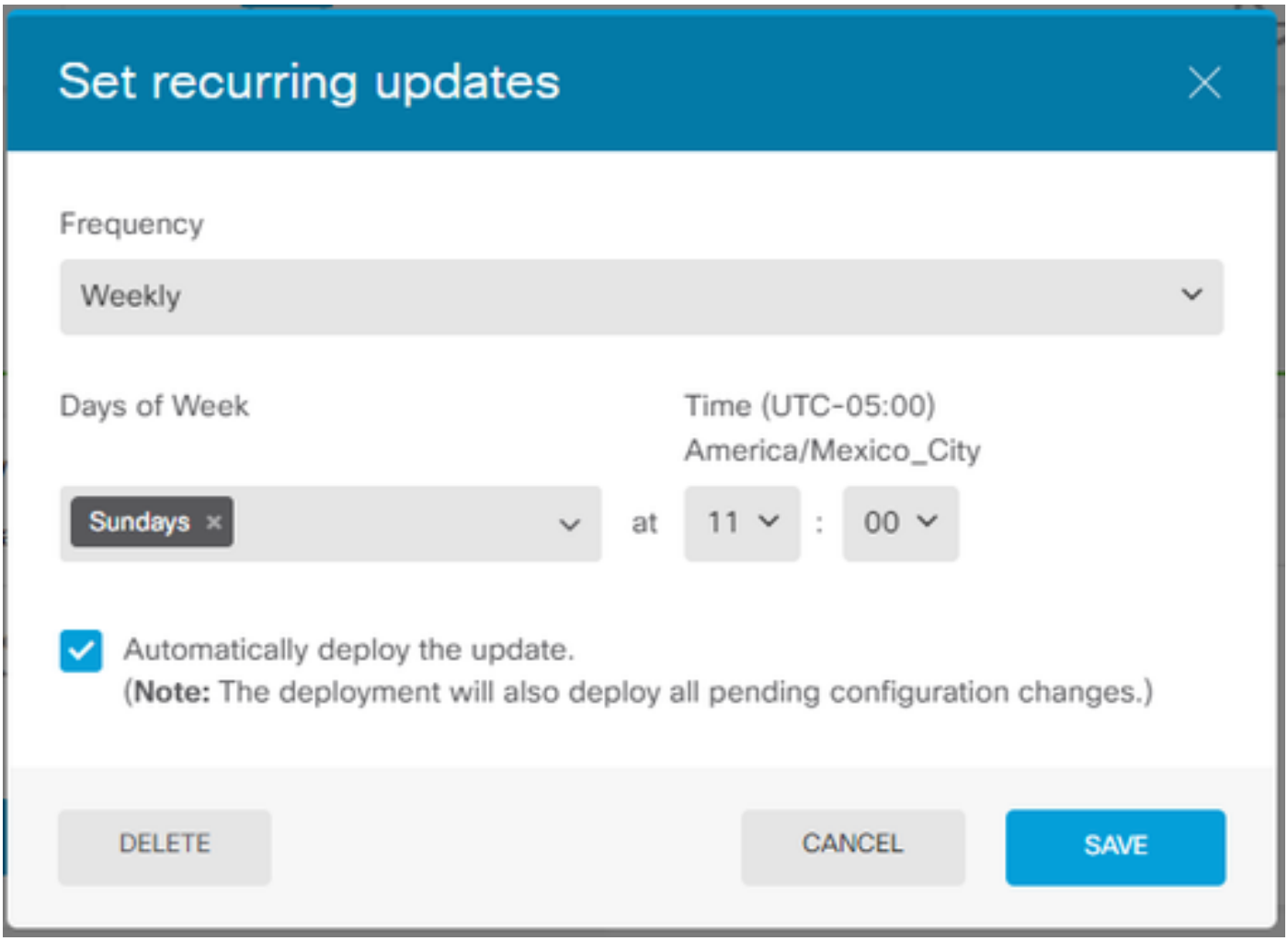
2. Nella schermata Dispositivi, selezionare Aggiornamenti > Visualizza configurazione.



3. Nella schermata Aggiornamenti, passare a VDB > Configura.

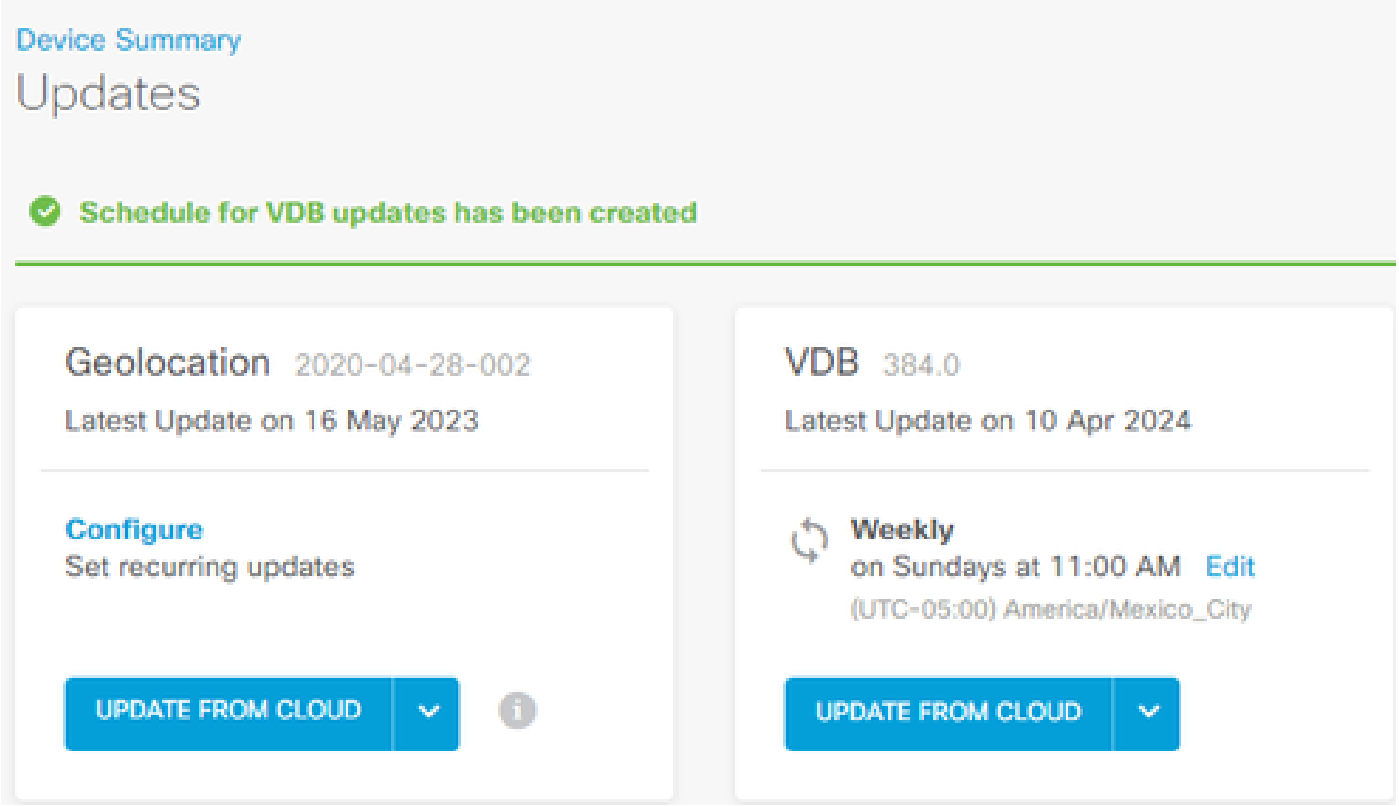


4. Nella schermata Imposta aggiornamenti ricorrenti, modificare le impostazioni predefinite in base alle proprie esigenze e fare clic su Salva.



Verifica

Nella schermata Updates, nella sezione VDB, viene riflessa l'opzione di aggiornamento ricorrente selezionata.



Risoluzione dei problemi

Se l'aggiornamento automatico di VDB non funziona come previsto, è possibile eseguire il rollback di VDB.

Passaggi:

SSH alla CLI del dispositivo di gestione (FMC, FDM o SFR nella casella di riepilogo)

Passare alla modalità Expert e alla directory principale e impostare la variabile di rollback:

<#root>

```
expert
```

```
sudo su
export ROLLBACK_VDB=1
```

Verificare che il pacchetto VDB a cui si intende effettuare il downgrade si trovi sul dispositivo in /var/sf/updates e installarlo:

<#root>

```
install_update.pl --detach /var/sf/updates/<name of desired VDB Package file>
```

Seguire i normali registri di installazione di vdb nella posizione appropriata in /var/log/sf/vdb-*

Al termine dell'installazione di VDB, distribuire il criterio ai dispositivi.

Nella CLI FTD, per controllare la cronologia delle installazioni VDB, è possibile controllare i seguenti contenuti della directory:

root@firepower:/ngfw/var/cisco/deploy/pkg/var/cisco/packages#ls -al
totale 72912
drwxr-xr-x 5 root root 130 set 108:49 .
drwxr-xr-x 4 radice 34 ago 16 14:40 ..
drwxr-xr-x 3 root root 18 ago 16 14:40 export-7.2.4-169
-rw-r—r— 1 radice 2371661 Lug 27 15:34 esportatore-7.2.4-169.tgz
drwxr-xr-x3 radice 21 ago 16 14:40vdb-368
-rw-r—r— 1 radice 36374219 lug 27 15:34 vdb-368.tgz
drwxr-xr-x 3 root root 21 set 108:49vdb-369
-rw-r—r— 1 radice 35908455 set 1 08:48 vdb-369.tgz

Informazioni correlate

Aggiornamento dei database di sistema

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).