

Configuración de una programación de actualización de base de datos regular para VDB en FDM

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Configuraciones](#)

[Verificación](#)

[Resolución de problemas](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar una programación de actualización de base de datos regular para la regla o VDB en FDM.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Administrador de dispositivos Firepower
- Base de datos de vulnerabilidad (VDB)

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- FDM 7.0

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

La base de datos de vulnerabilidades de Cisco (VDB) es una base de datos de vulnerabilidades conocidas para hosts susceptibles, así como huellas digitales para sistemas operativos, clientes y aplicaciones.

El sistema de firewall correlaciona las huellas dactilares con las vulnerabilidades para ayudarle a determinar si un host concreto aumenta el riesgo de que se ponga en peligro la red. Cisco Talos Intelligence Group (Talos) publica actualizaciones periódicas de la VDB.

Se recomienda habilitar el programador automático durante el proceso de incorporación para comprobar y aplicar regularmente las actualizaciones de la base de datos de seguridad. Esto garantiza que el dispositivo esté actualizado.

Configurar

Configuraciones

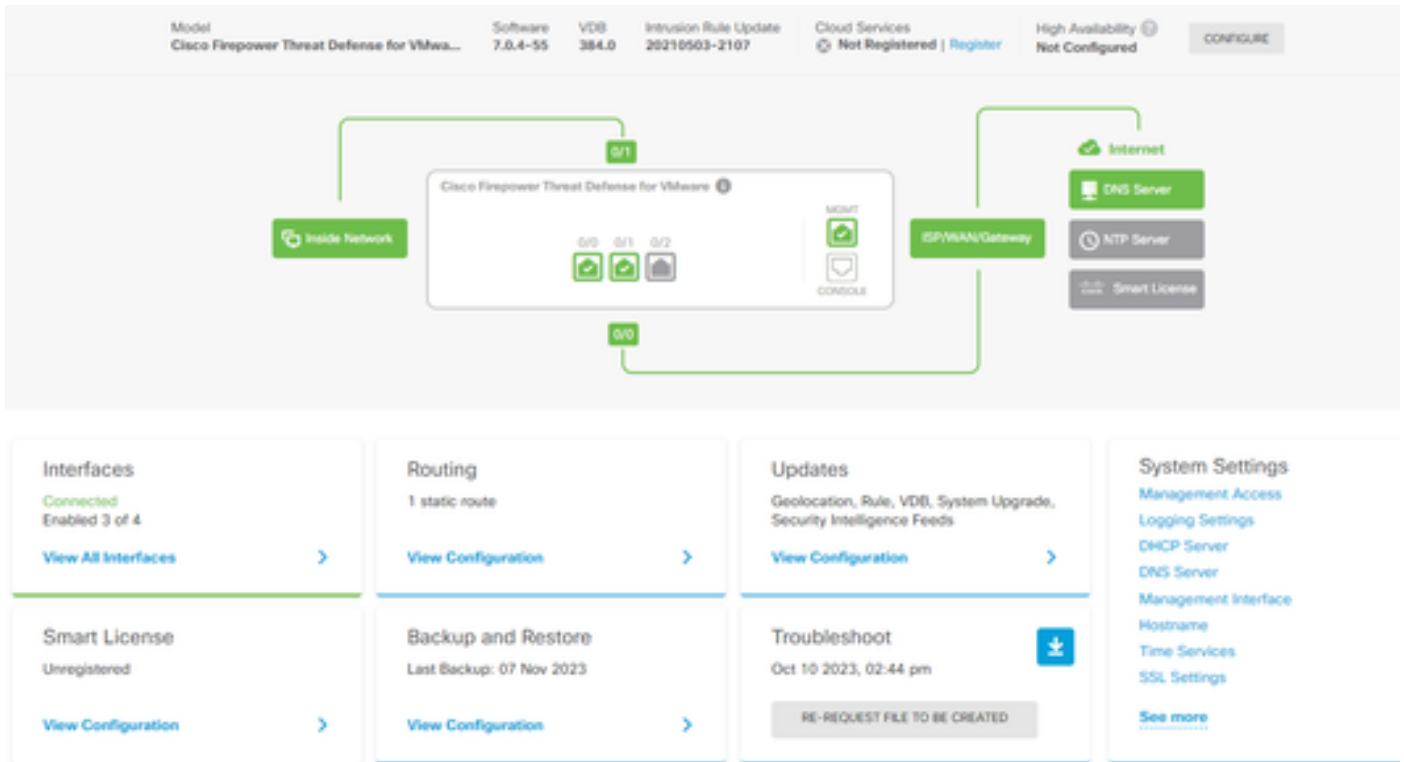
1. Inicie sesión en Firepower Device Manager



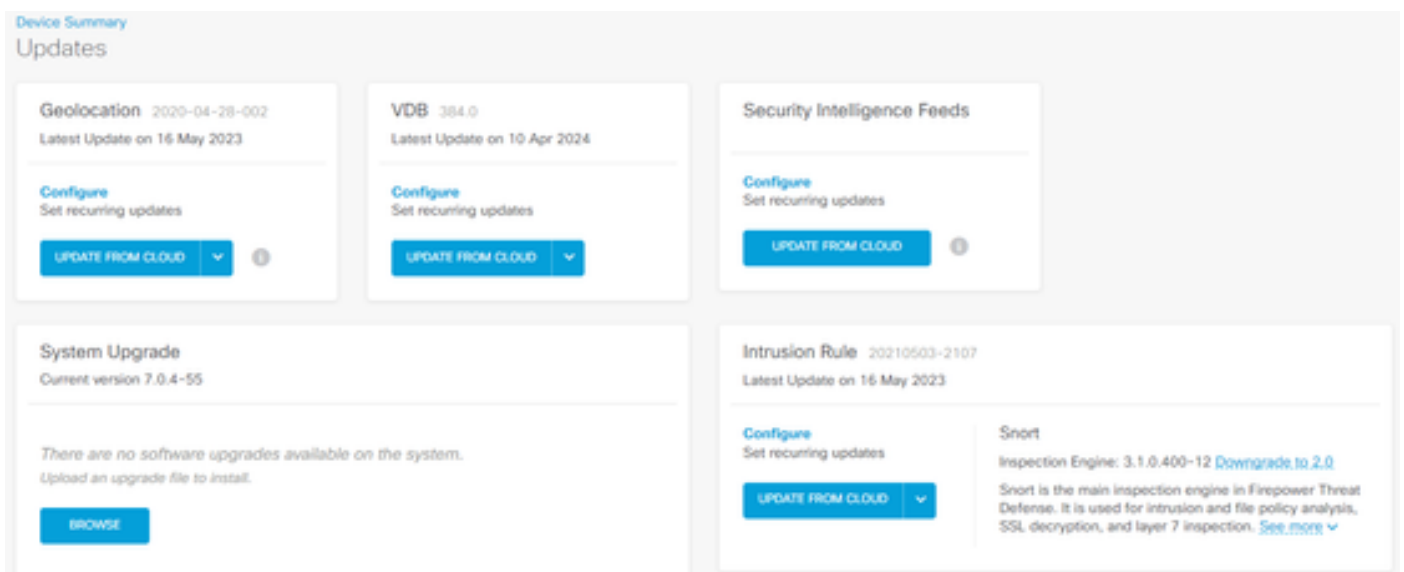
Firepower Device Manager

LOG IN

2. En la pantalla **Dispositivos**, navegue hasta **Actualizaciones > Ver configuración**.



3. En la pantalla Updates, navegue hasta VDB > Configure.



4. En la pantalla Establecer actualizaciones periódicas, cambie la configuración predeterminada según sus necesidades y haga clic en Guardar.

Set recurring updates ✕

Frequency

Weekly ▾

Days of Week

Sundays ✕ ▾ at 11 ▾ : 00 ▾

Time (UTC-05:00)
America/Mexico_City

Automatically deploy the update.
(**Note:** The deployment will also deploy all pending configuration changes.)

DELETE CANCEL SAVE

Verificación

En la pantalla Updates, en la sección VDB, se refleja la opción de actualización recurrente seleccionada.

Device Summary

Updates

✔ **Schedule for VDB updates has been created**

Geolocation 2020-04-28-002

Latest Update on 16 May 2023

Configure

Set recurring updates

UPDATE FROM CLOUD



VDB 384.0

Latest Update on 10 Apr 2024



Weekly

on Sundays at 11:00 AM [Edit](#)

(UTC-05:00) America/Mexico_City

UPDATE FROM CLOUD



Resolución de problemas

En caso de que la actualización automática de VDB no funcione como se espera, puede revertir la VDB.

Pasos:

SSH a la CLI del dispositivo de administración (bandeja de entrada FMC, FDM o SFR)

Cambie al modo experto y root, y establezca la variable de rollback:

```
<#root>
```

```
expert
```

```
sudo su
```

```
export ROLLBACK_VDB=1
```

Valide que el paquete de VDB al que pretende realizar la actualización se encuentre en el dispositivo en `/var/sf/updates` e instálelo:

```
<#root>
```

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

Siga los registros de instalación de vdb normales en la ubicación correspondiente en /var/log/sf/vdb-*

Una vez finalizada la instalación de VDB, implemente la política en los dispositivos.

En FTD CLI, para verificar el historial de las instalaciones de VDB, una forma es verificar el contenido de estos directorios:

```
root@firepower:/ngfw/var/cisco/deploy/pkg/var/cisco/packages#ls -al
total 72912
drwxr-xr-x 5 root root 130 Sep 1 08:49 .
drwxr-xr-x 4 root root 34 Ago 16 14:40 ..
drwxr-xr-x 3 root root 18 Aug 16 14:40 exporter-7.2.4-169
-rw-r-r— 1 root root 2371661 Jul 27 15:34 exporter-7.2.4-169.tgz
drwxr-xr-x 3 root root 21 ago 16 14:40vdb-368
-rw-r-r— 1 root root 36374219 Jul 27 15:34 vdb-368.tgz
drwxr-xr-x 3 root root 21 Sep 1 08:49vdb-369
-rw-r-r— 1 root root 35908455 Sep 1 08:48 vdb-369.tgz
```

Información Relacionada

[Actualizar bases de datos del sistema](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).