Configuración de VRF Aware Syslog en FTD

Contenido

Introducción

Este documento describe los pasos de configuración para el syslog que reconoce VRF en FTD.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Syslog
- Firepower Threat Defense (FTD)

Componentes Utilizados

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

- Secure Firewall Management Center (FMCv) v7.4.2

- Secure Firewall Threat Defence Virtual (FTDv) v7.4.2

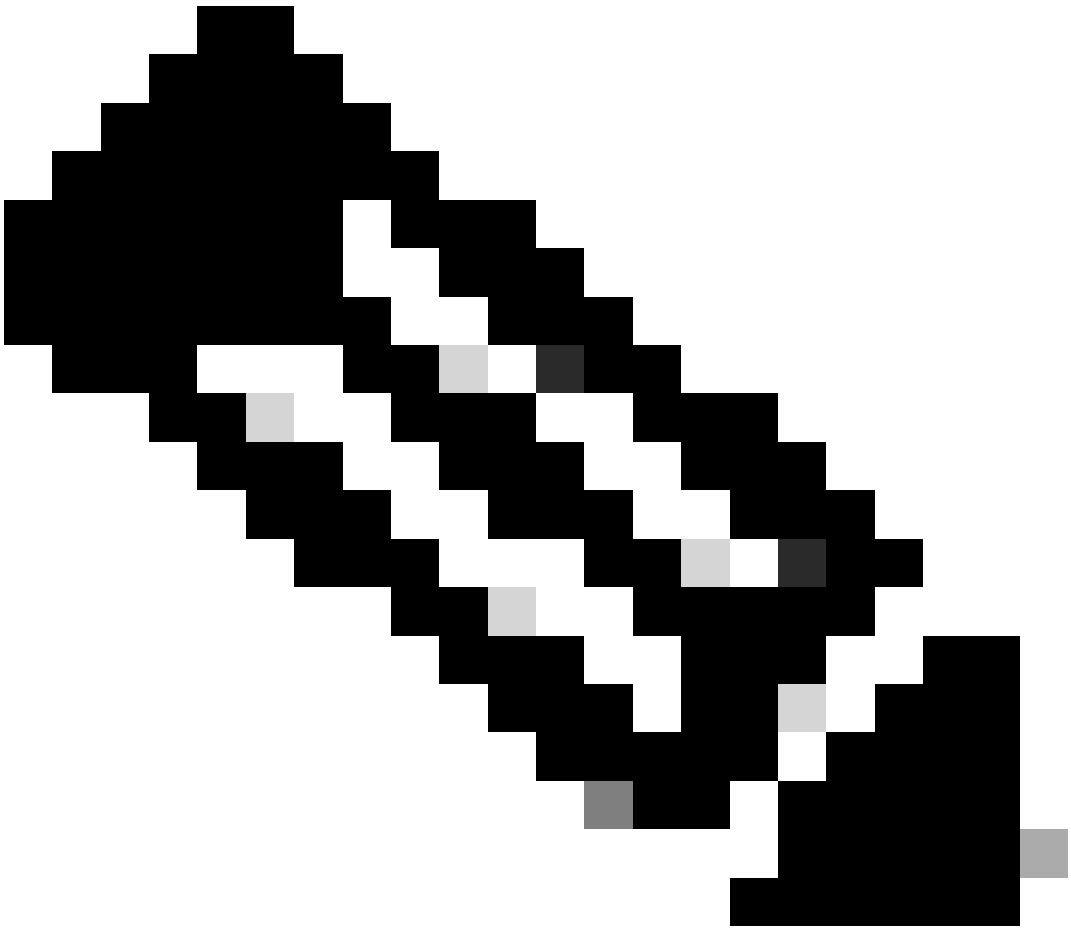
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender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

Plataformas mínimas de software y hardware

- Aplicación y versión mínima: Firewall seguro 7.4.1
- Plataformas gestionadas compatibles y versión: Todos los que admiten FTD 7.4.1
- Gerentes:
  1) FMC en funcionamiento + API REST FMC
  2) FMC en la nube
  3) FDM + API REST

Snort3, multiinstancia/contexto y compatibilidad con HA/agrupación en clústeres

---

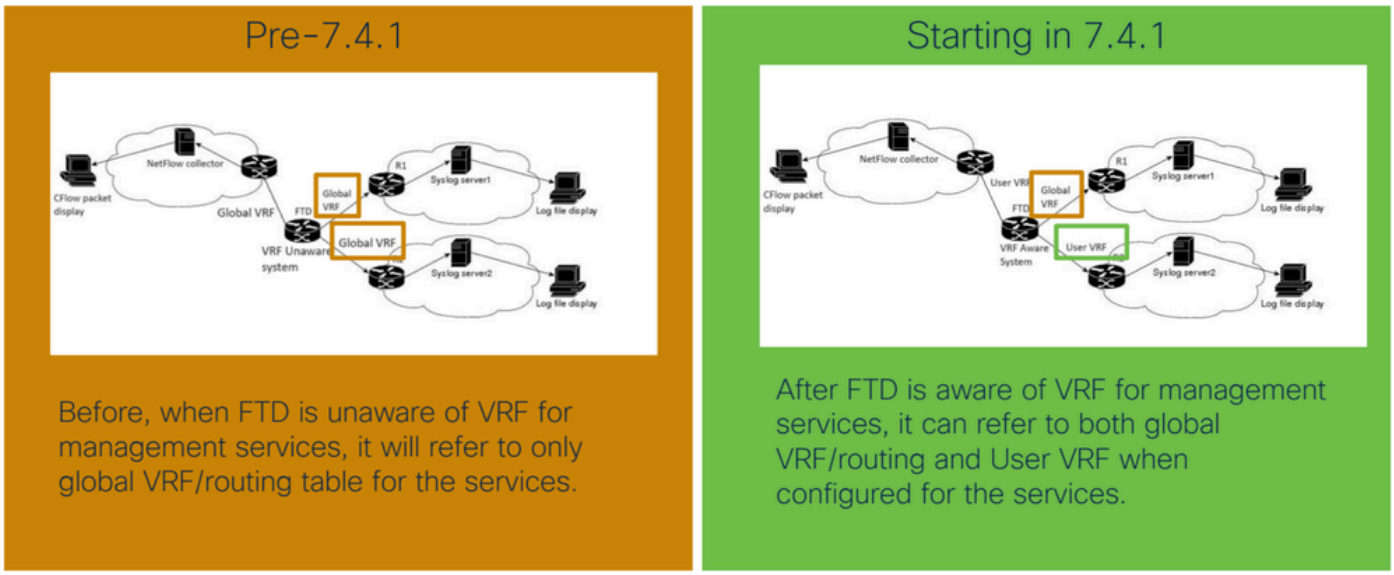


Nota: Funciona con servidores syslog tanto IPv4 como IPv6. IPv6 aún no se admite en el servidor ftp Syslog.

- Compatible con instancias múltiples.
- Compatible con dispositivos de alta disponibilidad.
- Compatible con dispositivos agrupados.

Configurar

Diagrama de la red



Comparación del diagrama de red entre Pre y Post 7.4.

Configuraciones

Virtual Routing and Forwarding (VRF) es una tecnología que se utiliza en las redes para permitir que varias instancias de una tabla de routing coexistan dentro del mismo router, lo que proporciona aislamiento de red entre diferentes redes virtuales. Cada instancia de VRF es independiente de las demás y el tráfico entre ellas se mantiene separado. Multi-VRF es una función que permite a los proveedores de servicios soportar varias VPN y servicios, incluso si sus direcciones IP se superponen. Utiliza interfaces de entrada para designar rutas para varios servicios y crear tablas de reenvío de paquetes virtuales asignando interfaces de capa 3 a cada VRF. Los servicios de gestión (Syslog, NetFlow) utilizan Global VRF de forma predeterminada. Los usuarios desean utilizar el VRF de usuario para los servicios de gestión, así como el VRF global, ya que no todos los destinos de carga son accesibles a través del VRF global.

En este documento, Global + User VRF = Multi-VRF

Habilite Syslog para el usuario VRF.

- Syslog puede utilizar el servicio ftp en un contexto multi-VRF.

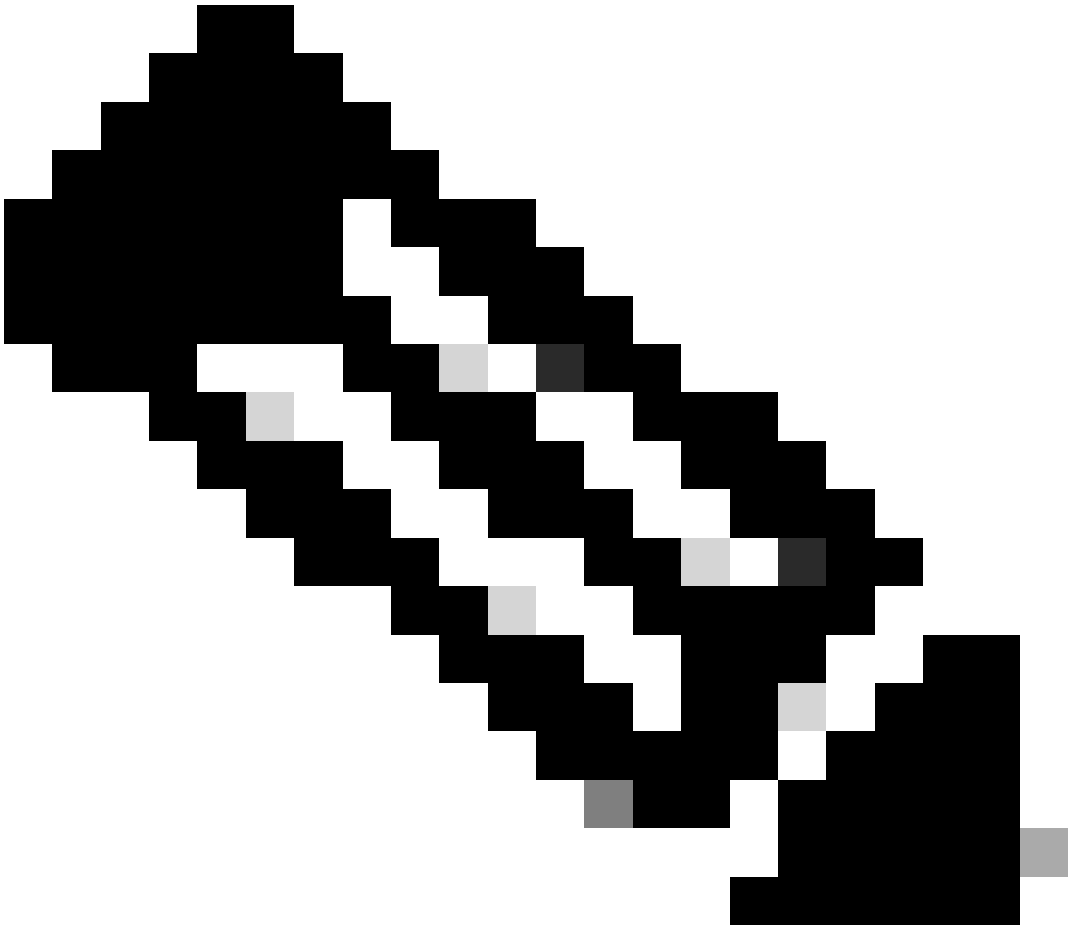
Cómo funciona

Cuando la interfaz se configura con el VRF de usuario, la búsqueda de rutas se produce en el dominio de ruteo VRF, en lugar del dominio de ruteo global predeterminado.

- Se admiten dos tipos de configuraciones de servidor:

1. Envíe mensajes de registro a los servidores Syslog para supervisar y solucionar problemas del tráfico de red.
2. Enviar el contenido del búfer de registro a un servidor FTP como archivo de texto

- Syslog emite los registros a los respectivos servidores UDP/TCP dentro de ese VRF.
- Para los syslogs de ajuste de búfer, los registros se envían al servidor FTP configurado dentro de ese VRF.

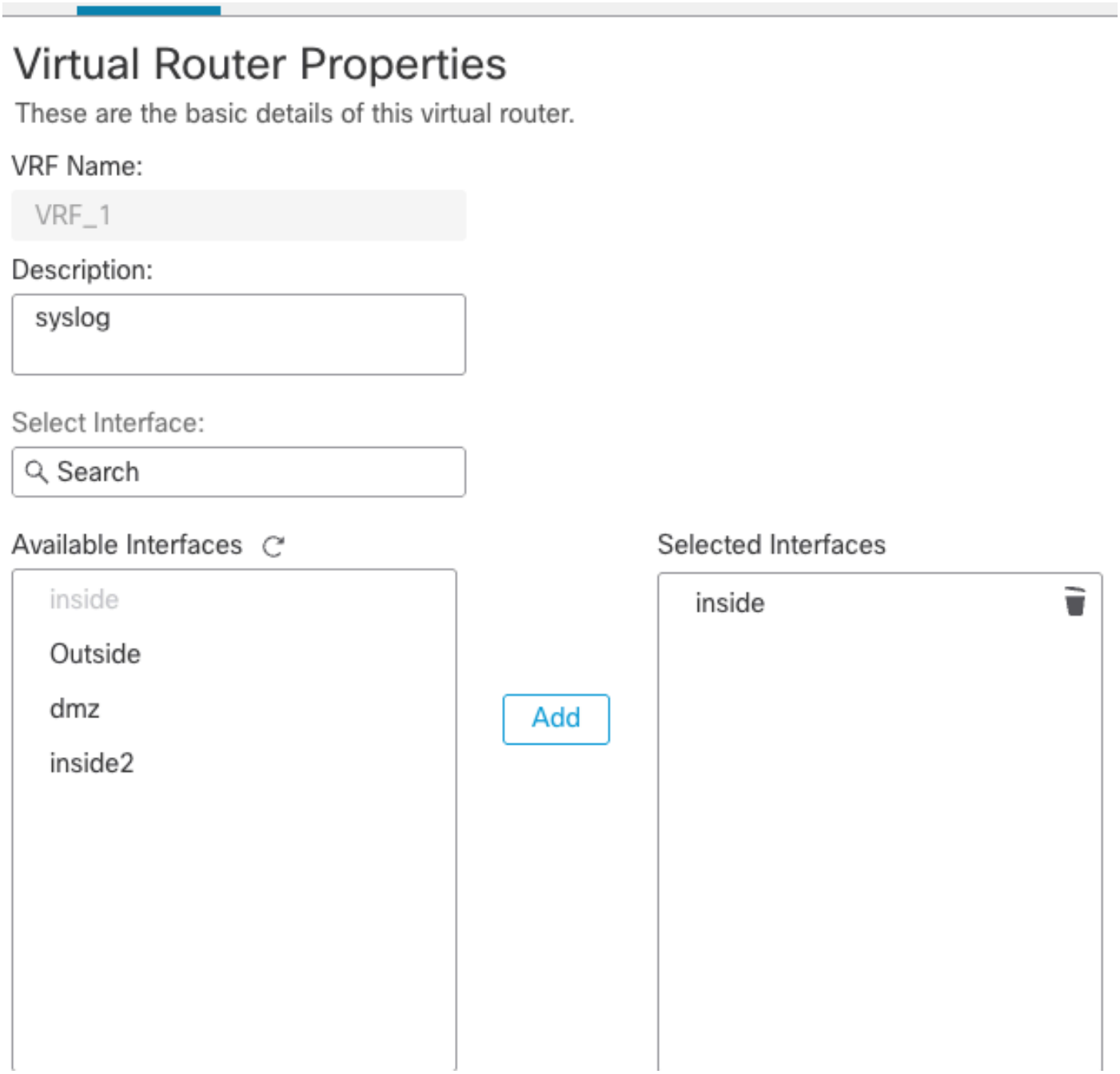


Nota: El servidor Syslog y el servidor FTP pueden formar parte de diferentes VRF.

Configuración del router virtual

Paso 1. Creación de un VRF

- Inicie sesión en FMC y navegue hasta Device > Device Management.
- Seleccione el Dispositivo y haga clic en el icono Lápiz para editarlo.
- Vaya a Routing> Manage Virtual Router > Add Virtual Router .
- Introduzca el nombre en Nombre VRF.
- Seleccione la interfaz y haga clic en Agregar y Guardar.

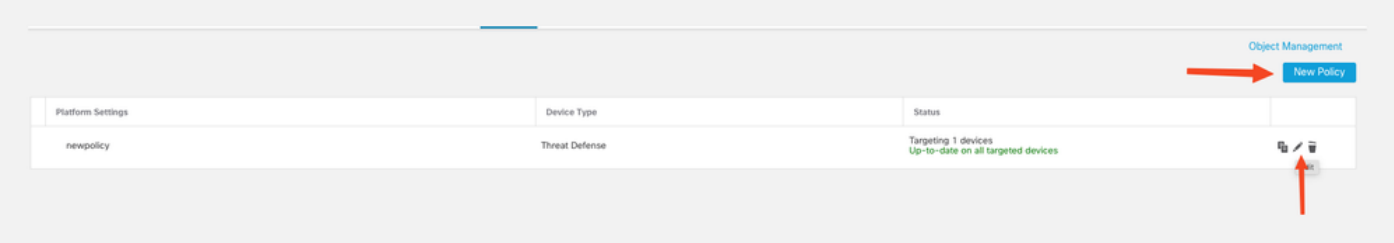


Adición de una Interfaz a VRF

Paso 2. Configure la configuración de registro.

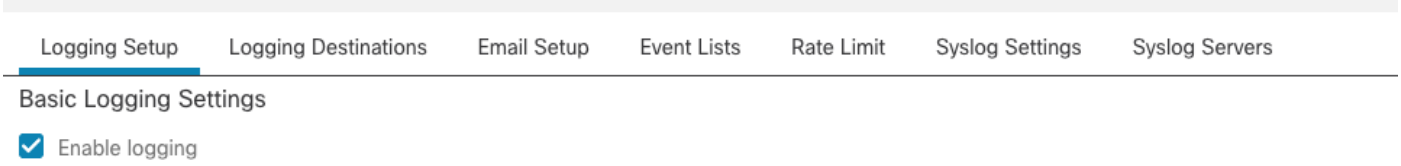
- Vaya a Devices > Platform Settings.

- Cree una nueva política o edite el icono Lápiz en una política existente.



Creación de la configuración de plataforma

- Seleccione Logging Setup y Enable logging.

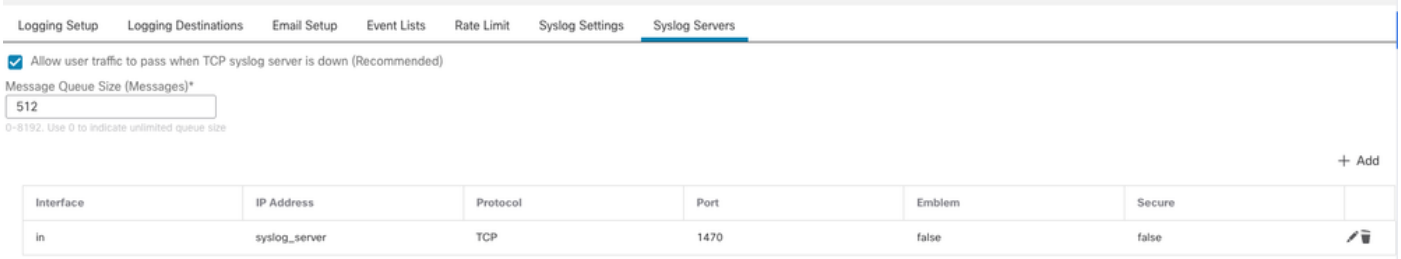


Activar registro

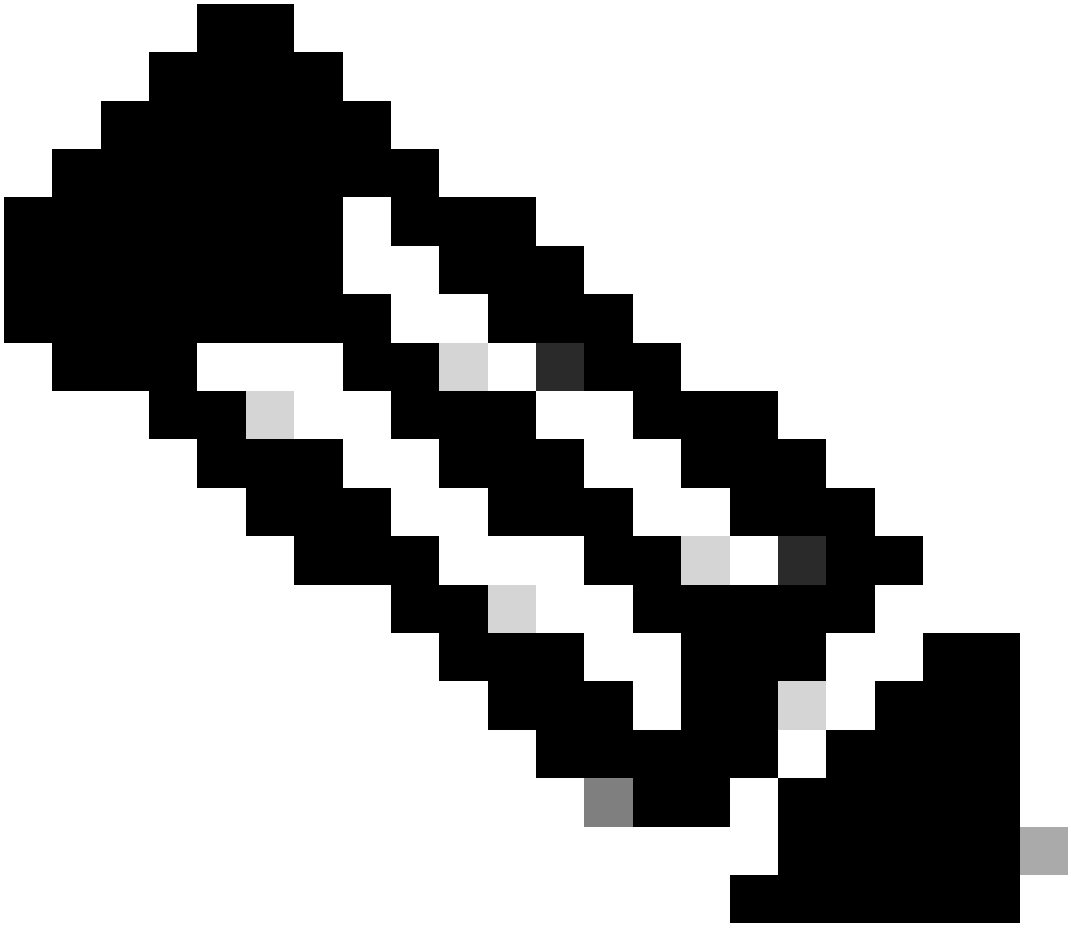
- Seleccione Logging Destination y haga clic en Add.
- Establezca el destino de registro como servidores Syslog.

Registro de Destino como Servidores Syslog

- Seleccione Syslog Servers > Add.



Adición de un servidor Syslog con interfaz VRF Aware



Nota: La interfaz interna forma parte de la zona de seguridad de.

- La interfaz configurada en el comando logging host ahora reconoce VRF.
- Click Save.

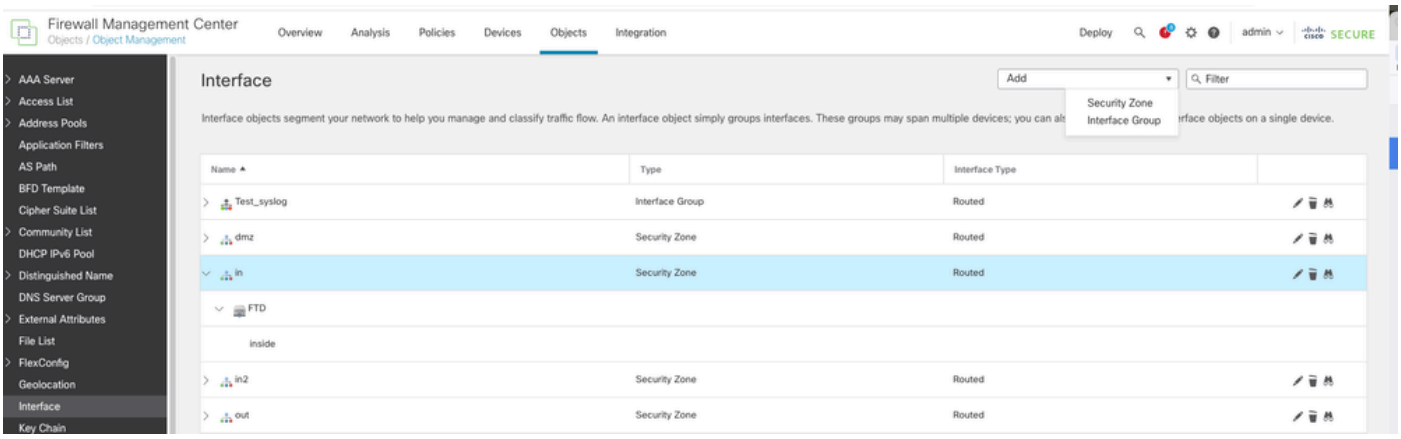
Prerrequisitos de la Configuración del Servidor FTP en FMC

- Utilice Interface Group Object.
- El objeto de grupo de interfaz puede tener tanto VRF de usuario como VRF global.

Configuración

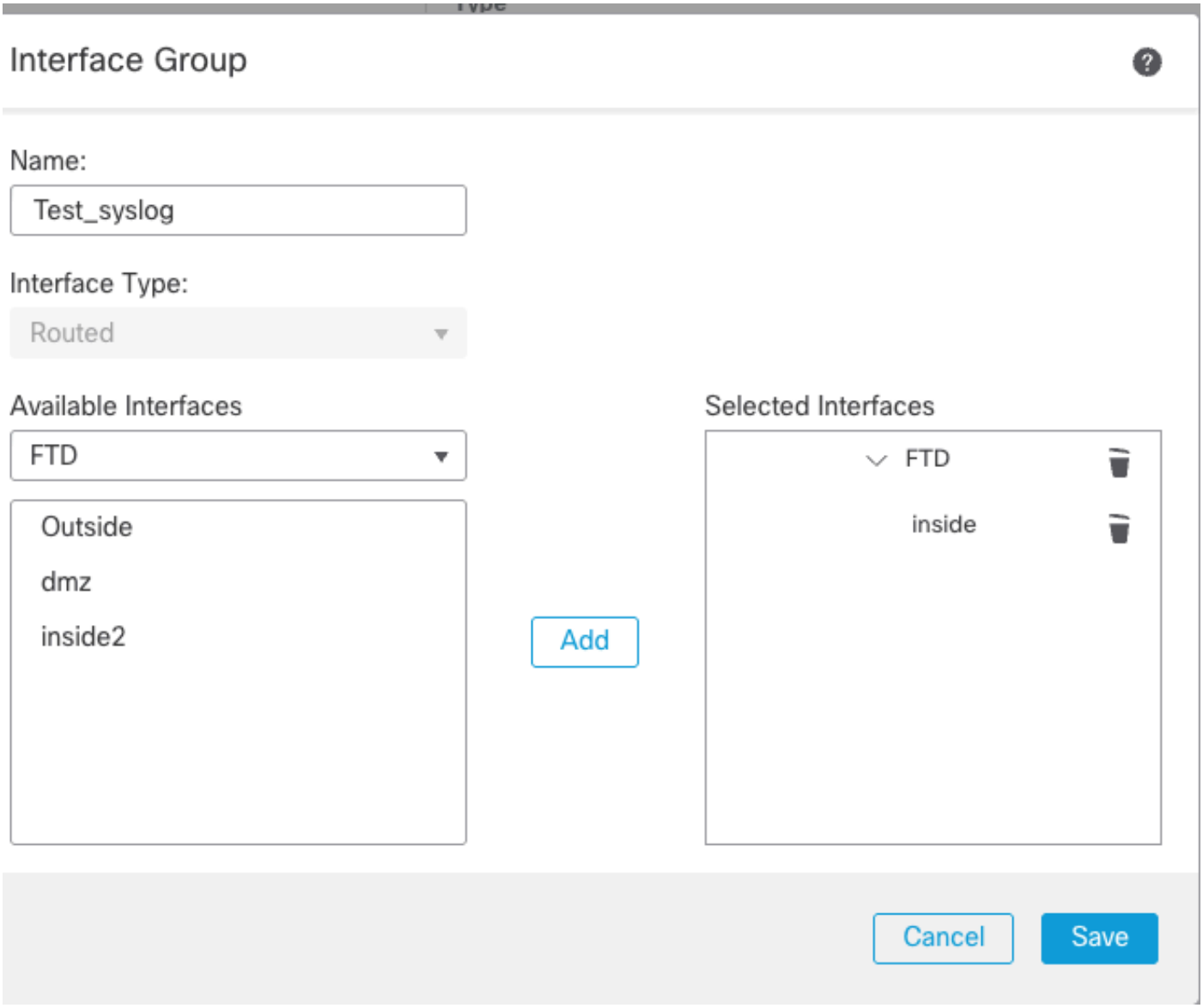
Paso 1.

- Vaya a Objeto > Administración de objetos > Interfaz > Agregar > Grupo de interfaces.



Agregando grupo de interfaces

- Seleccione el menú desplegable Device from y Add the VRF Interface.



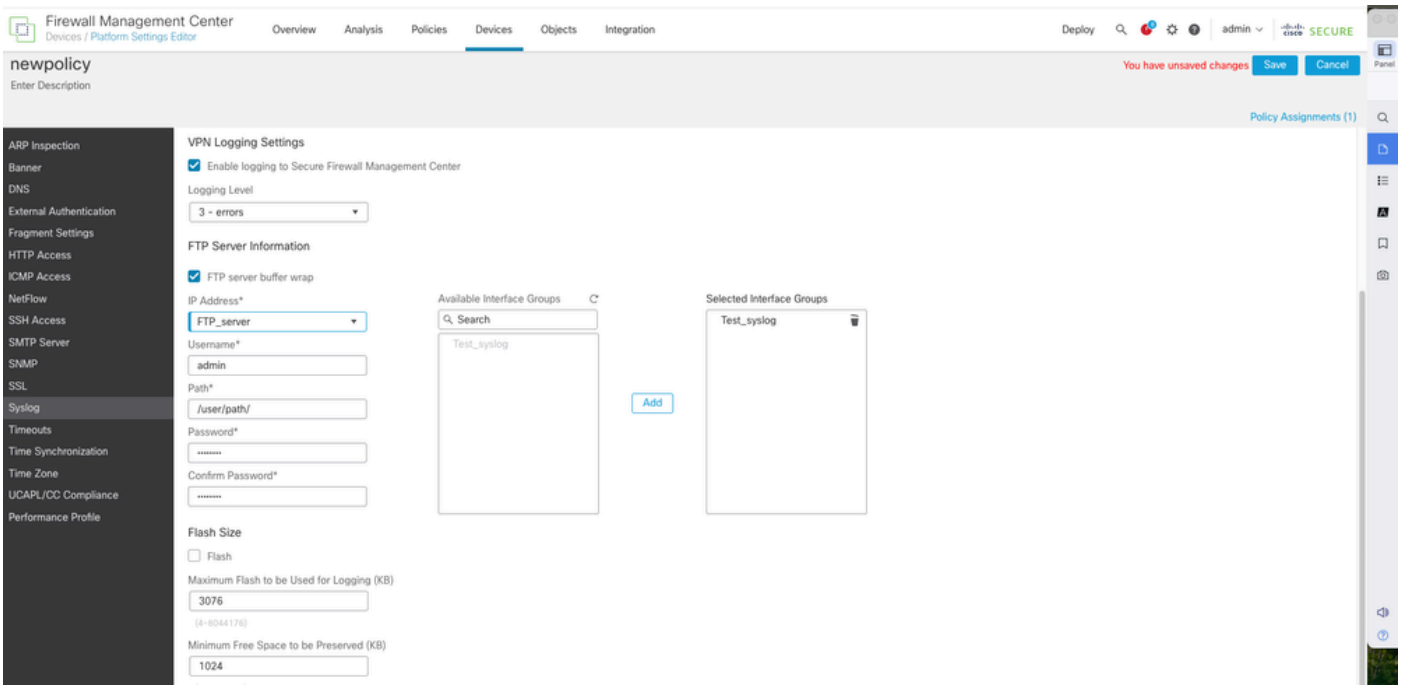
Adición de una Interfaz con Reconocimiento VRF

Paso 2.

- Navegue hasta Dispositivos > Configuración de la plataforma > Syslog > Configuración de

registro. Habilite el ajuste del búfer del servidor FTP.

- Click Save.



Habilitación del Servidor FTP con Interfaz VRF Aware

Verificación

Anterior a 7.4.1

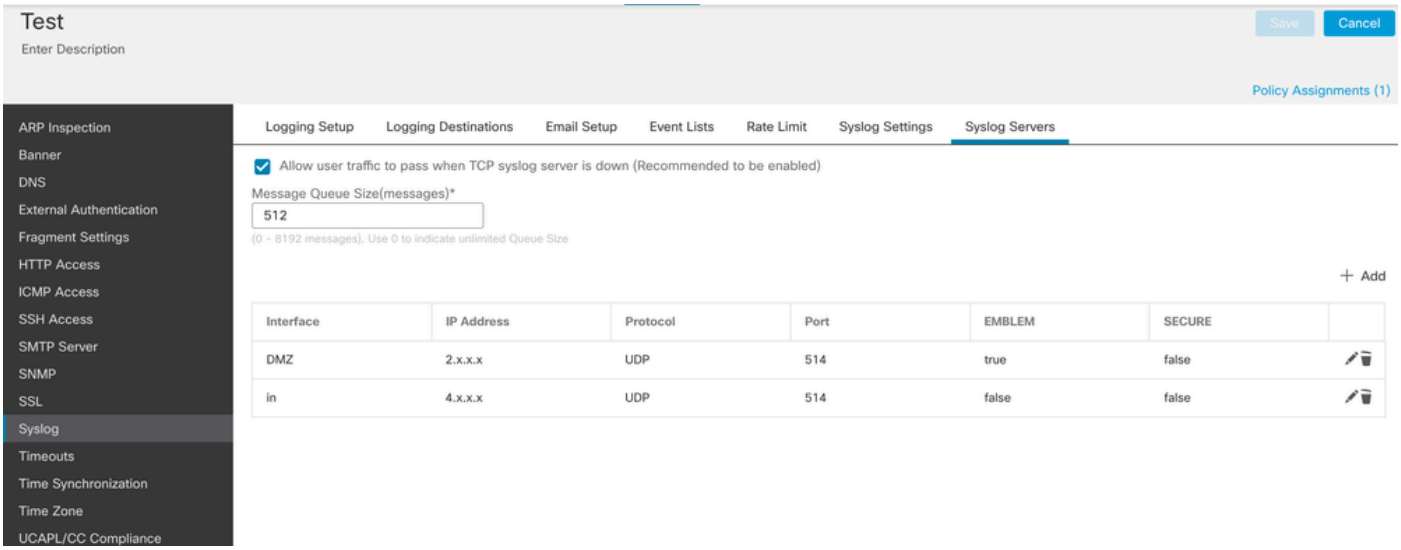
En esta prueba, el FTD y el FMC es 7.0.5.

FTD se configura con VRF y la interfaz dmz se ha asignado a VRF.

La interfaz dmz se configura con el host de registro del servidor syslog.

Además, la interfaz interna se configura con la configuración de syslog.

La interfaz interior es parte de Global VRF.

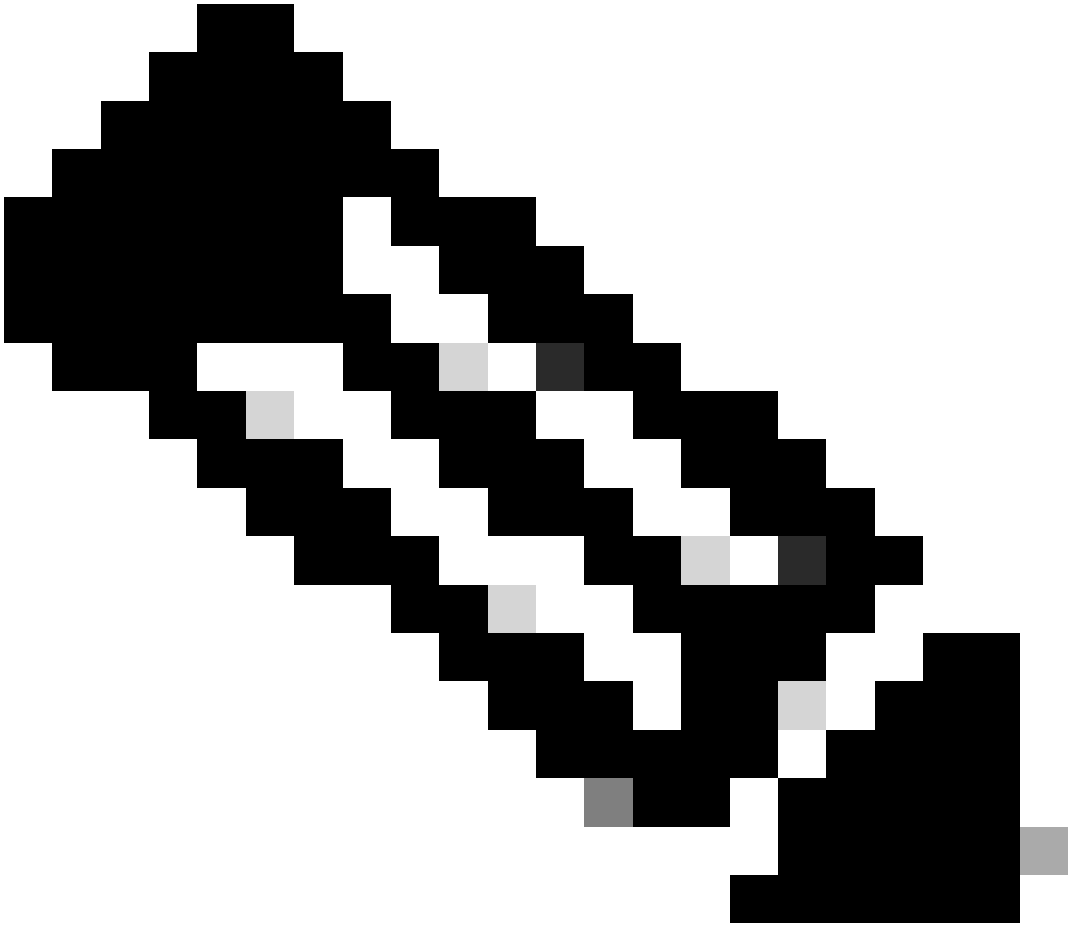


Configuración del servidor Syslog en FMC 7.0.5

Verificación de CLI

```
> show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Hide Username logging: enabled
    Standby logging: disabled
    Debug-trace logging: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: level informational, facility 20, 1193 messages logged
        Logging to inside 4.x.x.x, UDP TX:52
    Global TCP syslog stats::
        NOT_PUTABLE: 0, ALL_CHANNEL_DOWN: 0
        CHANNEL_FLAP_CNT: 0, SYSLOG_PKT_LOSS: 0
        PARTIAL_REWRITE_CNT: 0
    Permit-hostdown logging: enabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
    FMC logging: list MANAGER_VPN_EVENT_LIST, 0 messages logged
```

```
> show vrf

Name            VRF ID          Description             Interfaces
VRF-1           1                                       dmz
```



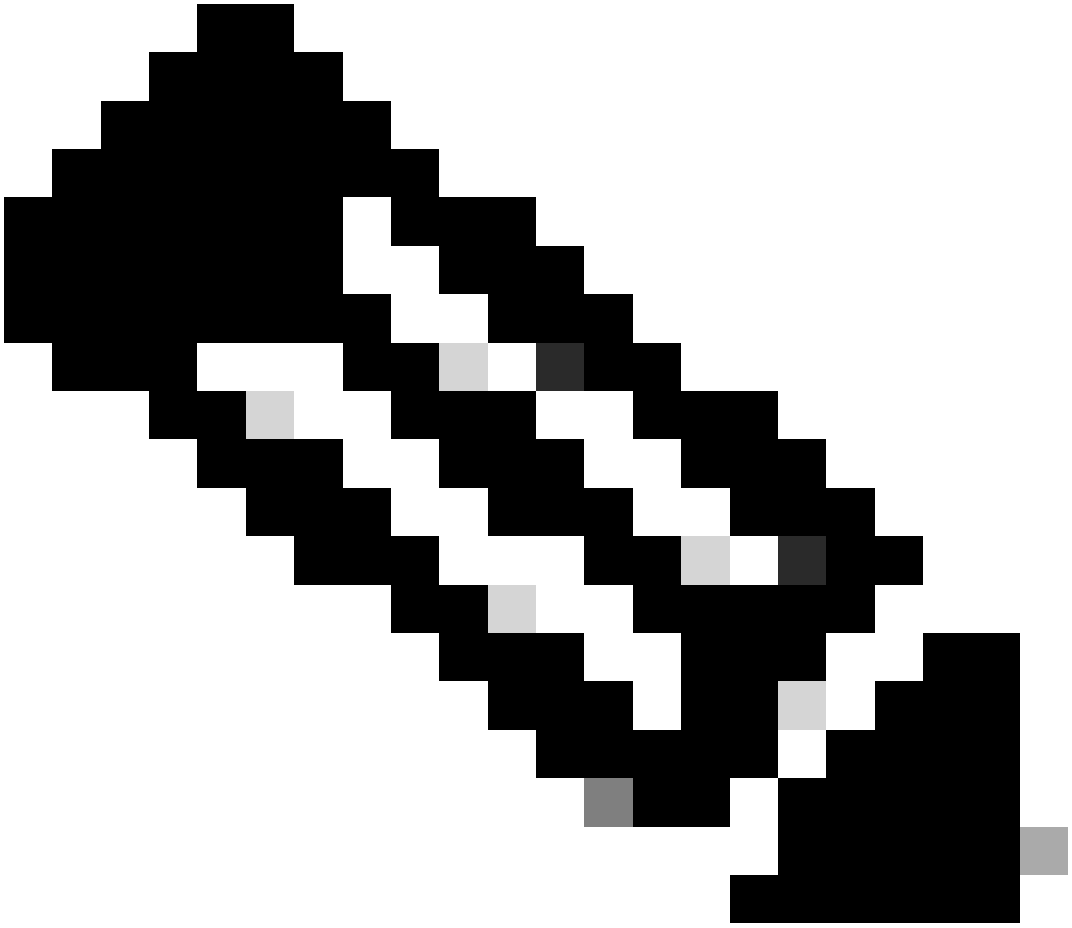
Nota: El servidor Syslog con destino 2.x.x.x no está disponible en la configuración de registro para FTD CLI. Forma parte del VRF de usuario.
El servidor Syslog con destino 4.x.x.x está disponible en la configuración de registro para FTD CLI. Esto es parte de Global VRF.

Publicación 7.4.1

Verificación de CLI

```
ftd1# show vrf

Name                            VRF ID     Description     Interfaces
VRF_1                           1          syslog          inside



td1# show logging
```

```
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Hide Username logging: enabled
    Standby logging: disabled
    Debug-trace logging: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: level informational, class auth, facility 20, 19284 messages logged
        Logging to inside 192.x.x.x tcp/1470 Not connected since Thu, 20 Mar 2025 01:53:17 UTC TX:0
            TCP SYSLOG_PKT_LOSS:0
            TCP [Channel Idx/Not Putable counts]: [0/0]
            TCP [Channel Idx/Not Putable counts]: [1/0]
            TCP [Channel Idx/Not Putable counts]: [2/0]
            TCP [Channel Idx/Not Putable counts]: [3/0]

    Global TCP syslog stats::
        NOT_PUTABLE: 0, ALL_CHANNEL_DOWN: 1584
        CHANNEL_FLAP_CNT: 1584, SYSLOG_PKT_LOSS: 0
        PARTIAL_REWRITE_CNT: 0
    Permit-hostdown logging: enabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
    FMC logging: list MANAGER_VPN_EVENT_LIST, class auth, 0 messages logged
```



Nota: El host del servidor Syslog 192.x.x.x utiliza la interfaz interna que reconoce VRF.

Verificación del servidor FTP

Anterior a 7.4.1

- En FMC, la configuración del servidor FTP no tiene la opción de seleccionar la interfaz que se va a utilizar. Sólo está disponible la dirección IP de la opción de servidor syslog.

Specify FTP Server Information

☑ FTP Server Buffer Wrap

IP Address*

Username*

Path*

Password*

Confirm*

Specify Flash Size

☐ Flash

Maximum Flash to be used by Logging(KB)

3076

(4-8044176)

Minimum free Space to be preserved(KB)

1024

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).