Configurar o VRF Aware Syslog no FTD

Contents

Introdução

Este documento descreve as etapas de configuração para o syslog sensível a VRF no FTD.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Syslog
- Firepower Threat Defense (FTD)

Componentes Utilizados

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

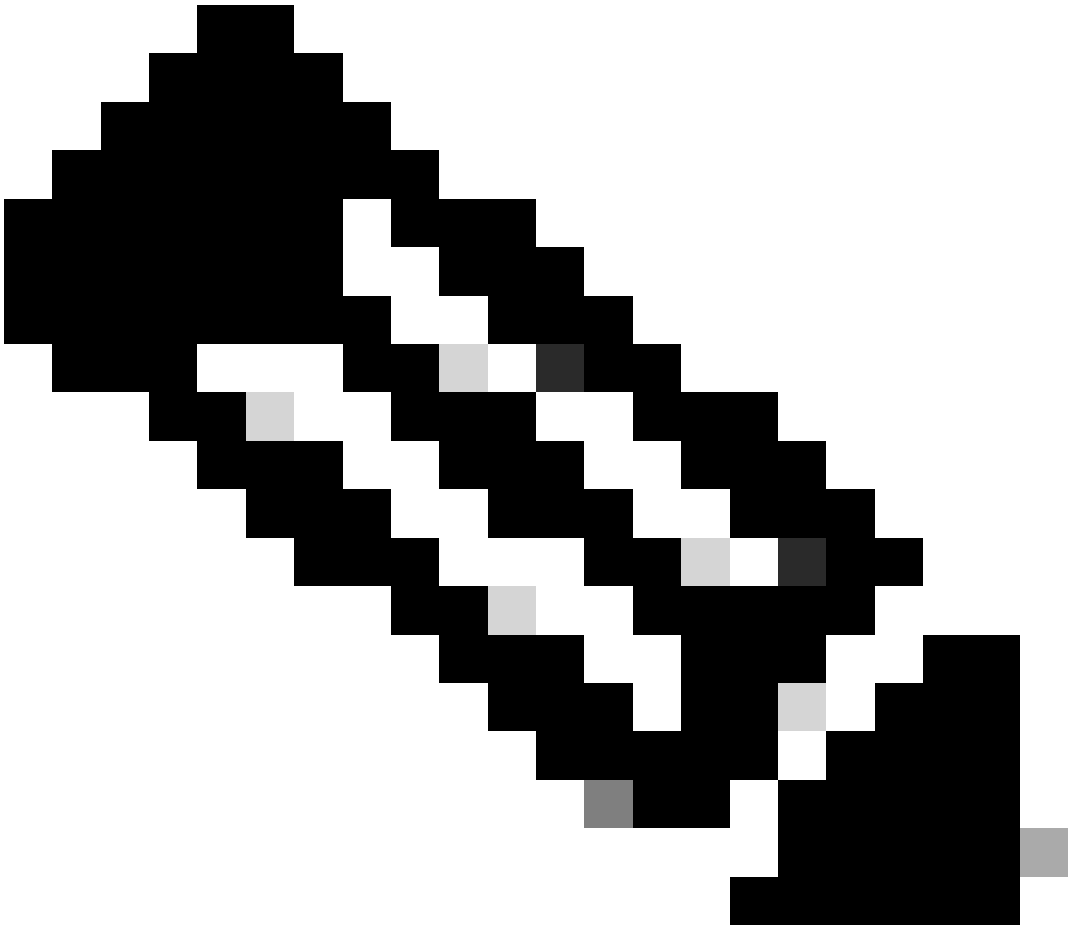
- Centro de gerenciamento seguro de firewall (FMCv) v7.4.2
- FTDvv (Threat Defense Virtual) de firewall seguro v7.4.2

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.

Plataformas mínimas de software e hardware

- Aplicativo e versão mínima: Secure Firewall 7.4.1
- Plataformas gerenciadas suportadas e versão: Todos que suportam o FTD 7.4.1
- Gerentes:
  1) FMC no local + FMC REST API
  2) FMC fornecido em nuvem
  3) FDM + REST API

Suporte a Snort3, várias instâncias/contexto e HA/clustering



Note: Funciona com os servidores syslog IPv4 e IPv6. IPv6 ainda não é suportado no

---

servidor Syslog ftp.

- Suportado com Várias Instâncias.
- Compatível com dispositivos de alta disponibilidade.
- Suportado em dispositivos em cluster.

Configurar

Diagrama de Rede

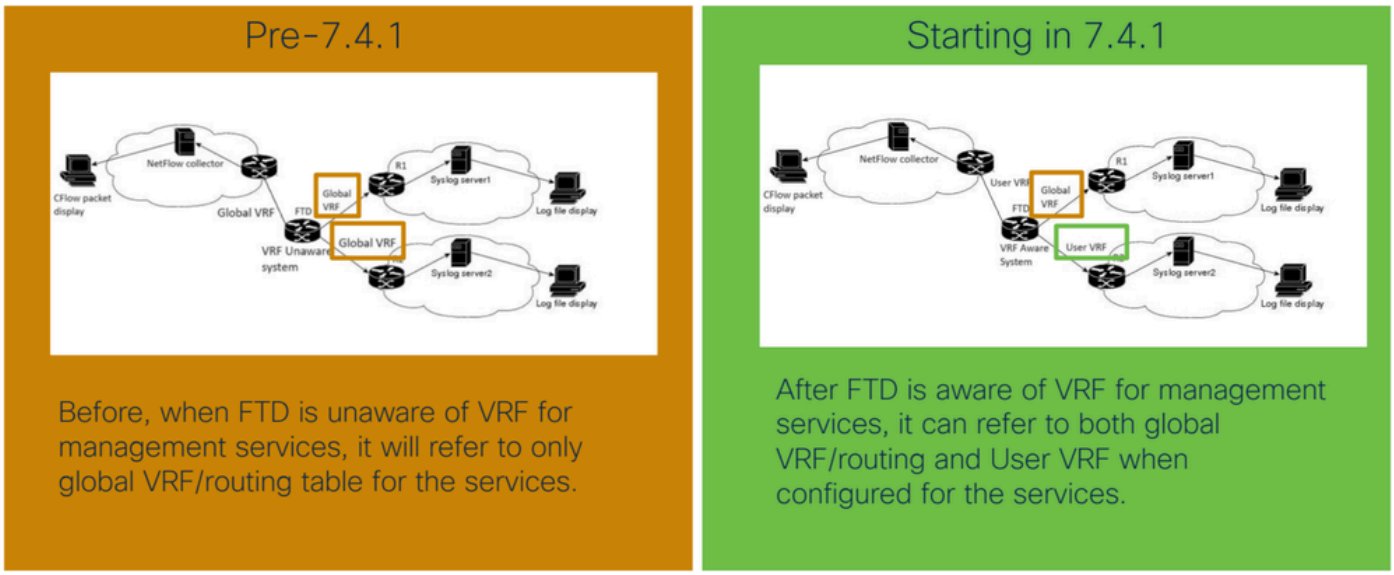


Diagrama de rede Comparação entre Pré e Pós 7.4.

Configurações

O Virtual Routing and Forwarding (VRF) é uma tecnologia usada em redes para permitir que várias instâncias de uma tabela de roteamento coexistam dentro do mesmo roteador, fornecendo isolamento de rede entre diferentes redes virtuais. Cada instância do VRF é independente das outras e o tráfego entre elas é mantido separado. O Multi-VRF é um recurso que permite que os provedores de serviços suportem várias VPNs e serviços, mesmo que seus endereços IP se sobreponham. Ele usa interfaces de entrada para designar rotas para vários serviços e criar tabelas virtuais de encaminhamento de pacotes atribuindo interfaces de Camada 3 a cada VRF. Os serviços de gerenciamento (Syslog, NetFlow) usam o VRF global como padrão. Os usuários desejam usar o VRF de usuário para serviços de gerenciamento, bem como o VRF global, pois nem todos os destinos de carregamento podem ser acessados por meio do VRF global.

Neste documento, Global + User VRF = Multi-VRF

Ative o Syslog para o VRF do usuário.

- O Syslog pode usar o serviço ftp em um contexto multi-VRF.

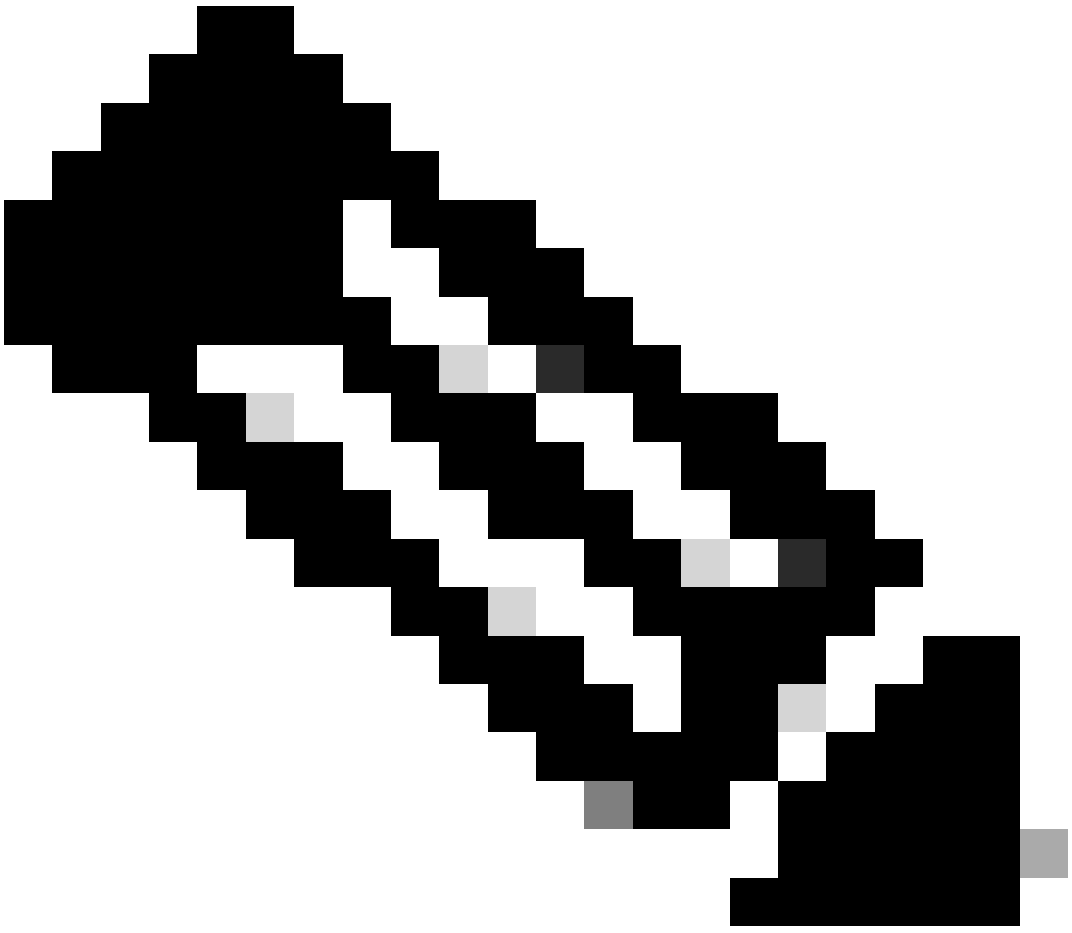
Como funciona

Quando a interface é configurada com o VRF de usuário, a pesquisa de rota ocorre no domínio de roteamento VRF, em vez do domínio de roteamento global padrão.

- Há suporte para dois tipos de configurações de servidor:

1. Envie mensagens de registro aos servidores Syslog para monitorar e solucionar problemas de tráfego de rede.
2. Enviar o conteúdo do buffer de log para um servidor FTP como um arquivo de texto

- O Syslog emite os logs para os respectivos servidores UDP/TCP dentro desse VRF.
- Para syslogs de encapsulamento de buffer, os logs são enviados para o servidor FTP configurado dentro desse VRF.

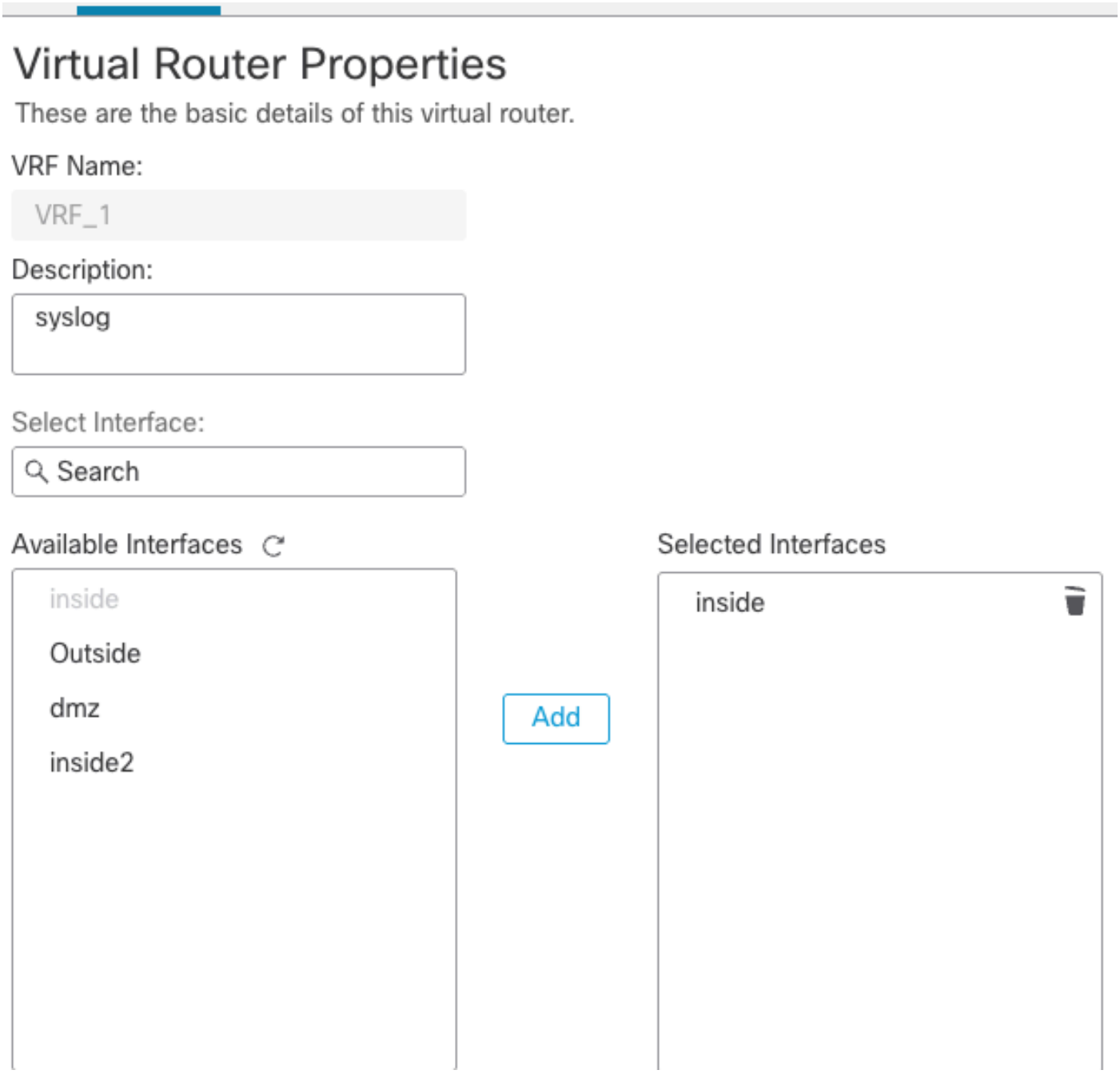


Note: O servidor Syslog e o servidor FTP podem fazer parte de VRFs diferentes.

Configurar Roteador Virtual

Etapa 1. Criar um VRF

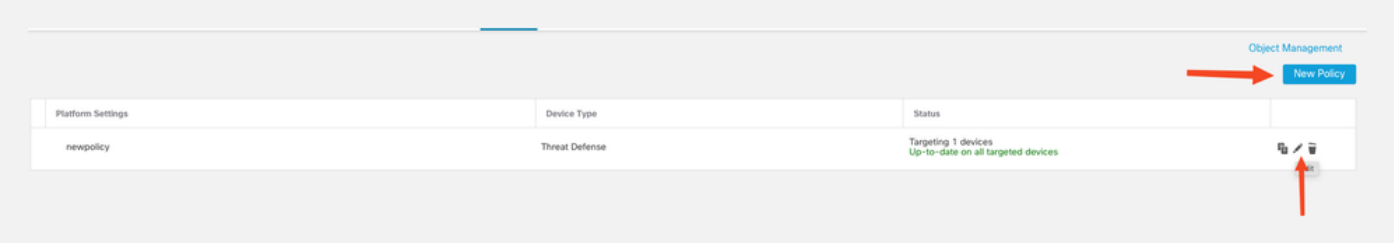
- Faça login no FMC e navegue até Device > Device Management.
- Selecione o dispositivo e clique no ícone do lápis para editá-lo.
- Navegue até Routing> Manage Virtual Router > Add Virtual Router.
- Insira o nome em VRF Name.
- Selecione a interface e clique em Adicionar e Salvar.



Adicionando interface ao VRF

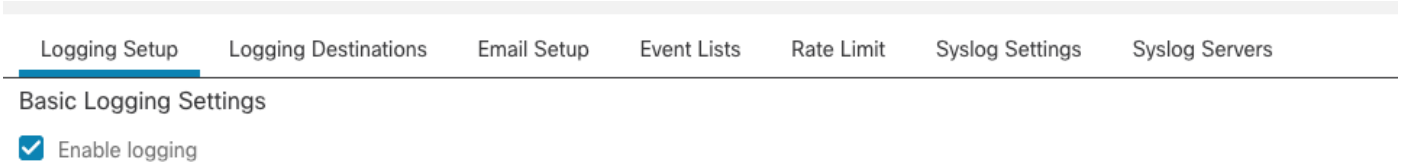
Etapa 2. Configurar a configuração do registro.

- Navegue até Devices > Platform Settings.
- Crie uma Nova Diretiva ou edite o ícone Lápis na diretiva existente.



Criando as configurações da plataforma

- Selecione Configuração de registro e Ativar registro.

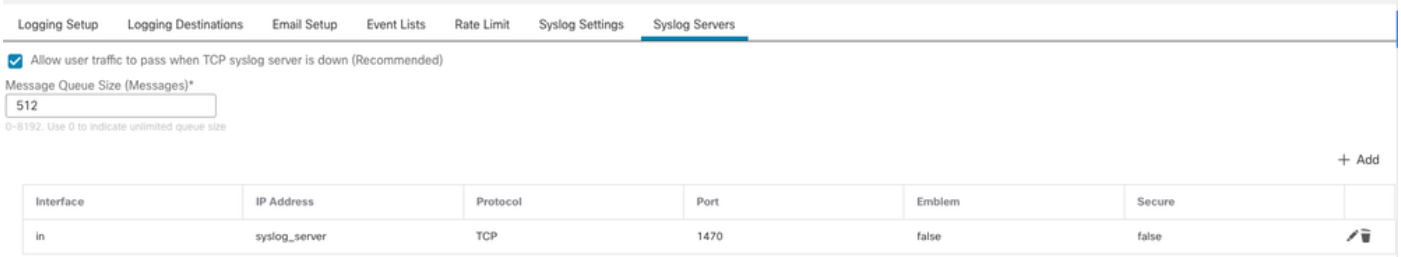


Habilita o registro em log

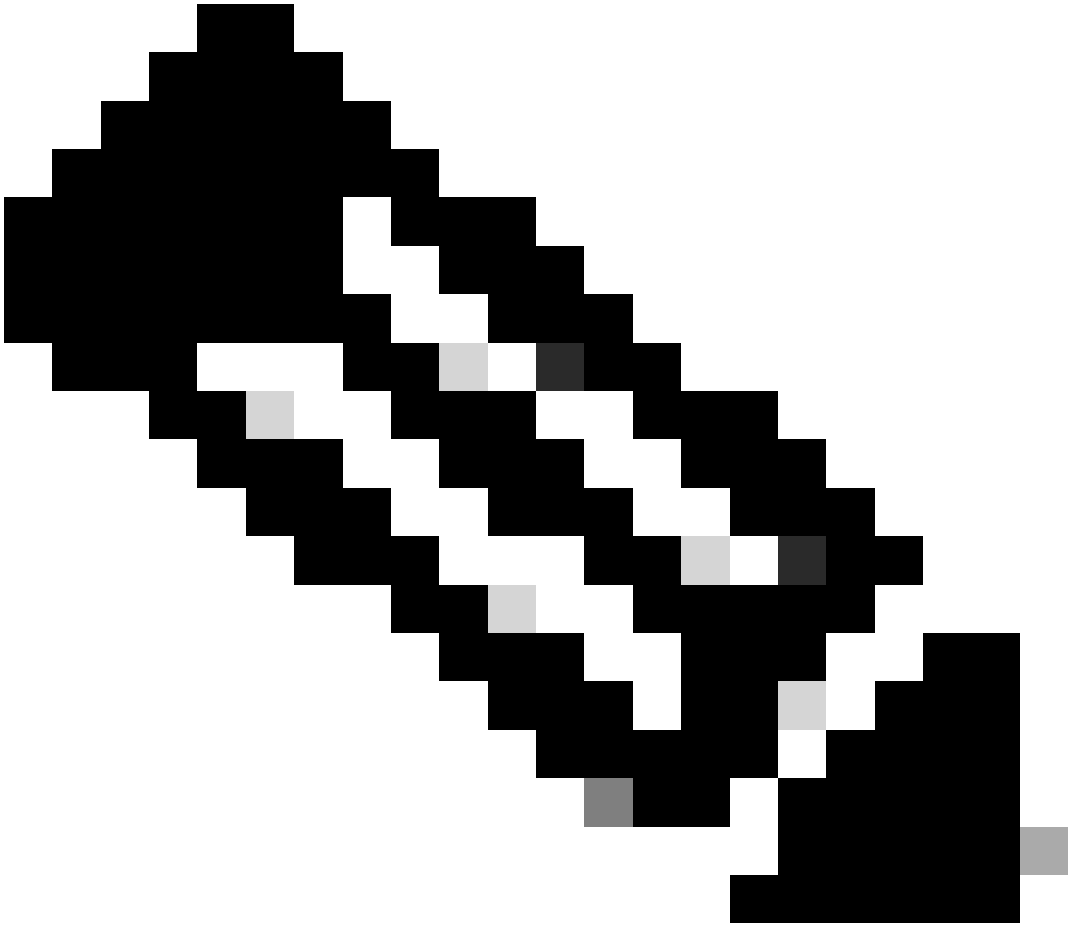
- Selecione Logging Destination e clique em Add.
- Defina Logging Destination como servidores Syslog.

Registrando o destino como servidores Syslog

- Selecione Syslog Servers > Add.



Adicionando Servidor Syslog com Interface VRF



Note: A interface interna faz parte da zona de segurança no.

- A interface configurada no comando logging host agora reconhece VRF.
- Click Save.

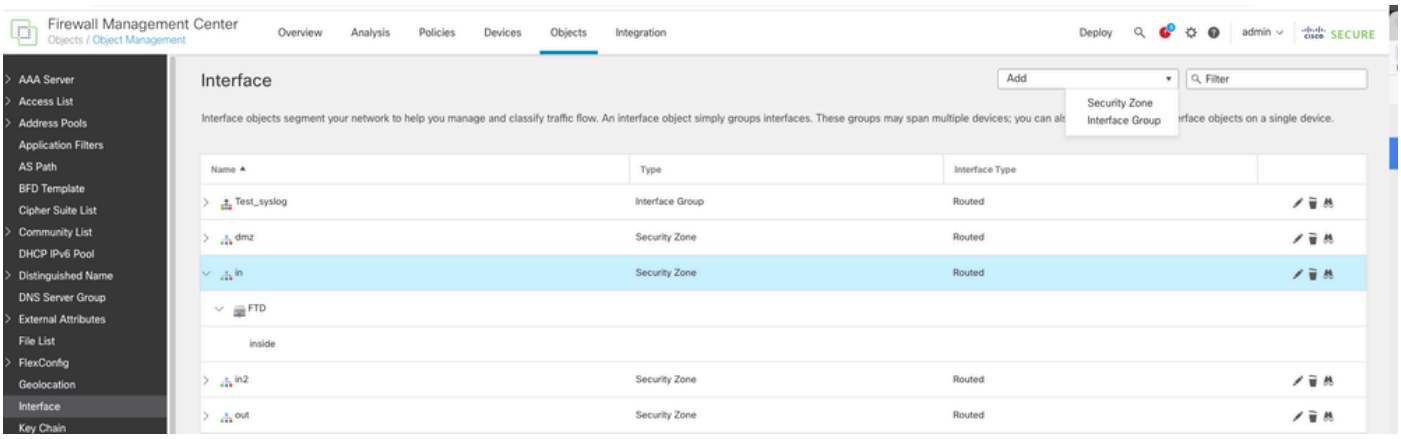
Pré-requisitos para a configuração do servidor FTP no FMC

- Use Interface Group Object.
- O objeto de grupo de interface pode ter VRF global e de usuário.

Configuração

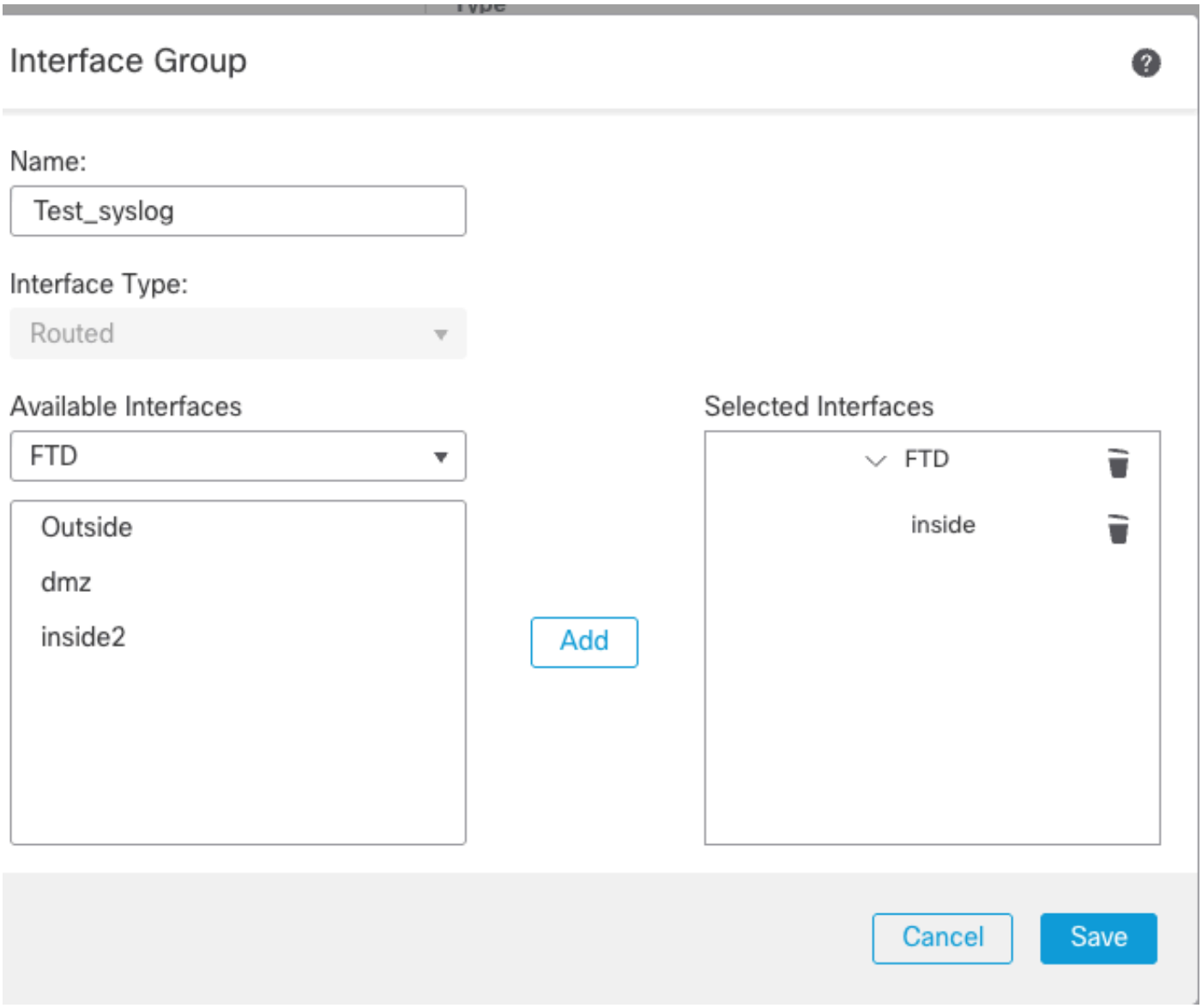
Etapa 1.

- Navegue até Object > Object Management > Interface > Add > Interface Group.



Adicionando grupo de interface

- Selecione o Dispositivo no menu suspenso e Adicione o VRF Interface.



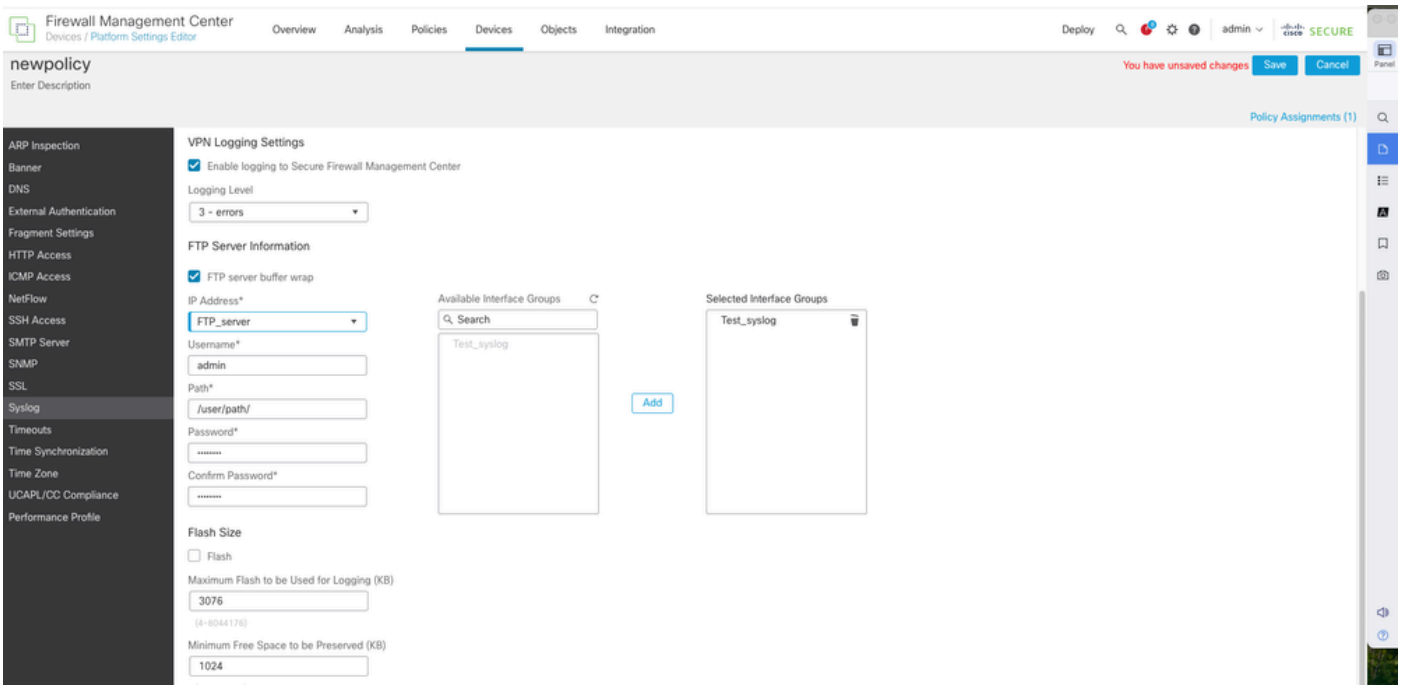
Adicionando interface VRF

Etapa 2.

- Navegue até Devices > Platform Settings > Syslog > Logging Setup. Habilite o

encapsulamento de buffer do servidor FTP.

- Click Save.



Ative o servidor FTP com interface sensível a VRF

Verificar

Antes do 7.4.1

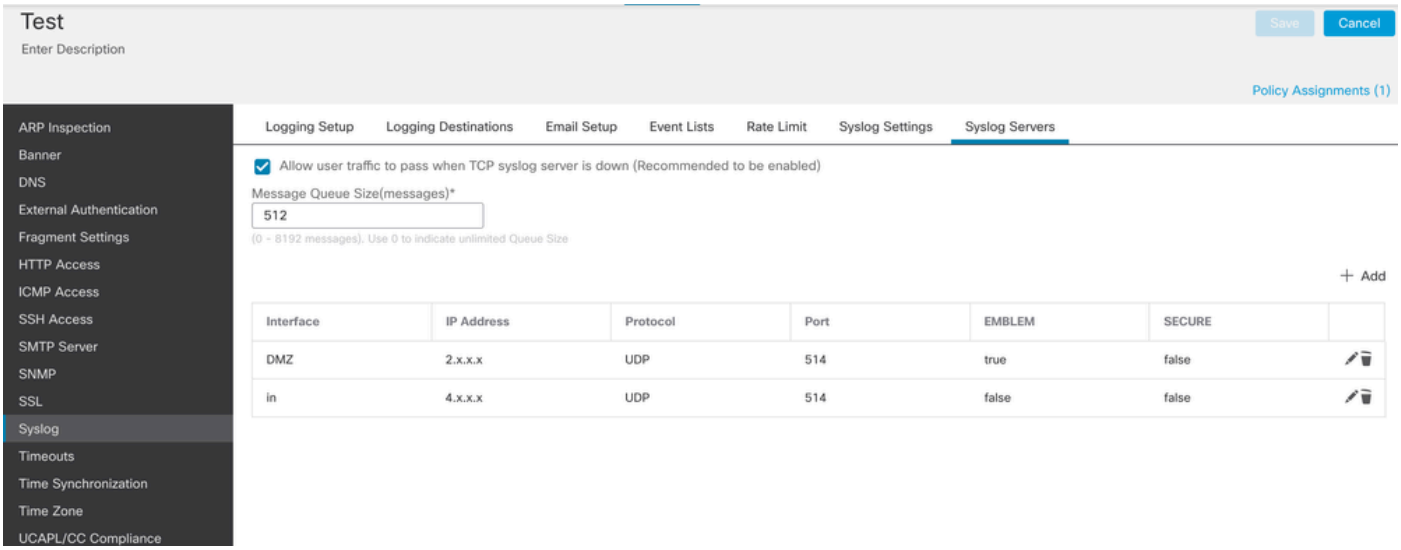
Neste teste, o FTD e o FMC são 7.0.5.

O FTD é configurado com VRF e a interface dmz foi atribuída ao VRF.

A interface dmz é configurada com o host de registro do servidor syslog.

Além disso, a interface interna é configurada com a configuração de syslog.

A interface interna faz parte do Global VRF.

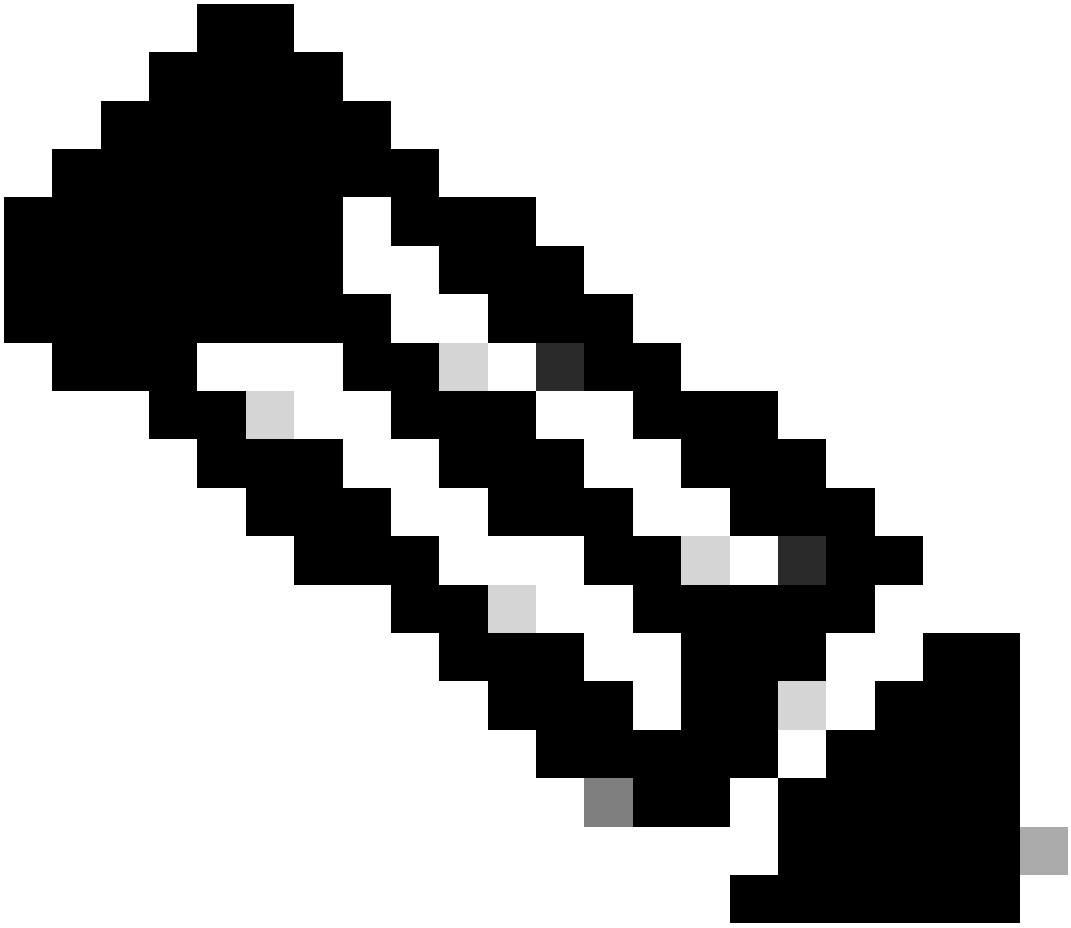


Configuração do Servidor Syslog no FMC 7.0.5

Verificação da 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
```



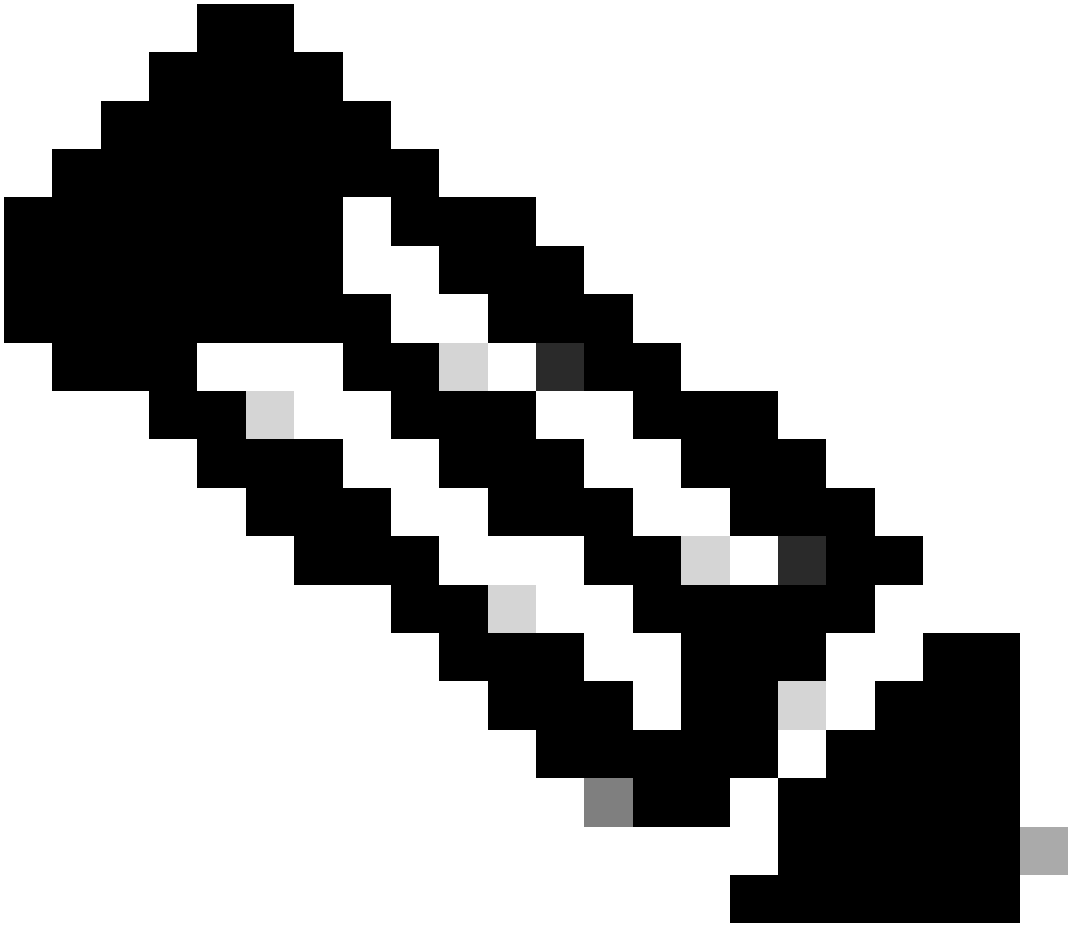
Note: O Servidor syslog com destino 2.x.x.x não está disponível na configuração de registro para CLI FTD. Isso faz parte do VRF do usuário.
O Servidor syslog com destino 4.x.x.x está disponível na configuração de registro para CLI FTD. Isso faz parte do VRF global.

Postagem 7.4.1

Verificação da 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
```



Note: O host do servidor de syslog 192.x.x.x está usando a interface interna sensível a VRF.

Verificação do servidor FTP

Antes do 7.4.1

- No FMC, a configuração do servidor FTP não tem a opção de selecionar a interface a ser usada. Somente o endereço IP da opção de Servidor syslog está disponível.

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

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.