# 在FTD上配置VRF感知系统日志

## 目录



## 简介

本文档介绍FTD上VRF感知系统日志的配置步骤。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- 系统日志
- Firepower Threat Defense (FTD)

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- 安全防火墙管理中心(FMCv)v7.4.2
- 安全防火墙威胁防御虚拟(FTDv)v7.4.2

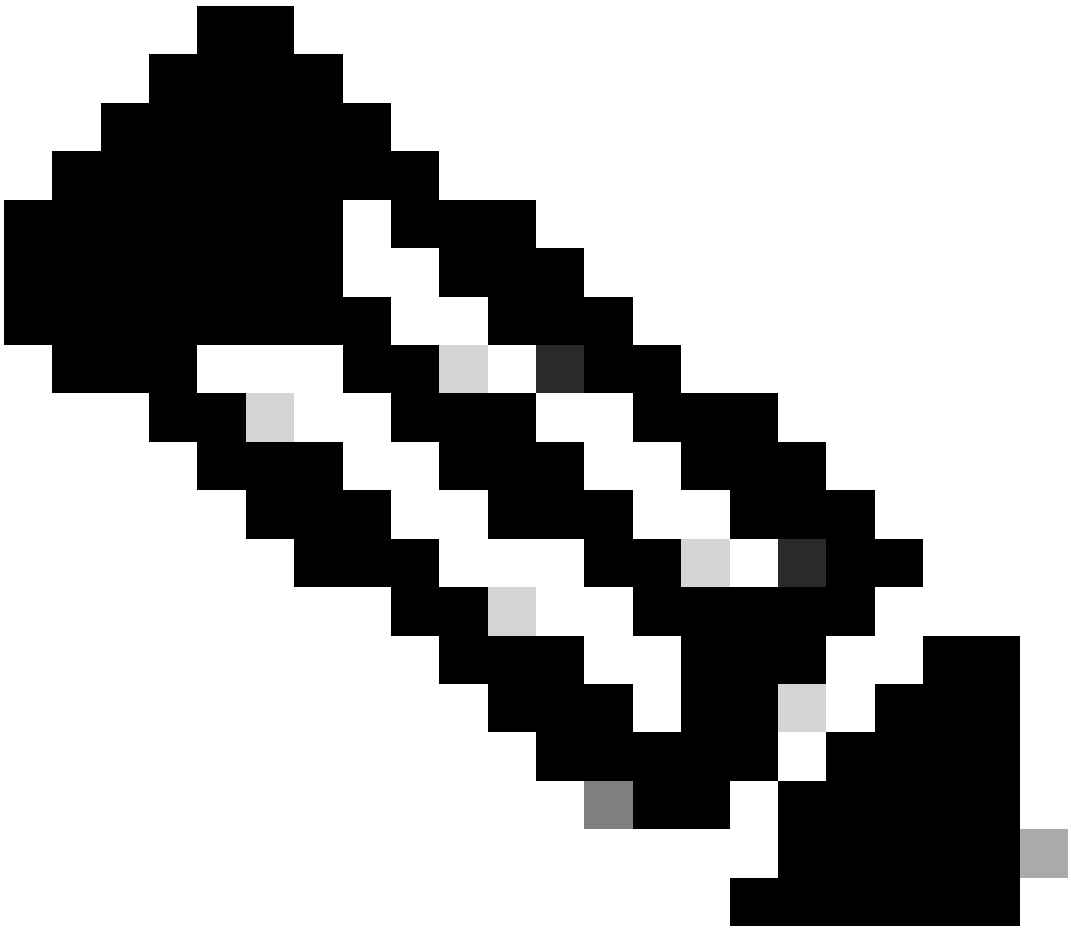
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 最低软件和硬件平台

- 应用和最低版本：安全防火墙7.4.1
- 支持的托管平台和版本：所有这些都支持FTD 7.4.1
- 经理：
  1)FMC现场+ FMC REST API
  2)云交付的FMC
  3)FDM + REST API

## Snort3、多实例/情景和HA/集群支持

---



注意：可与IPv4和IPv6系统日志服务器配合使用。系统日志ftp服务器尚不支持IPv6。

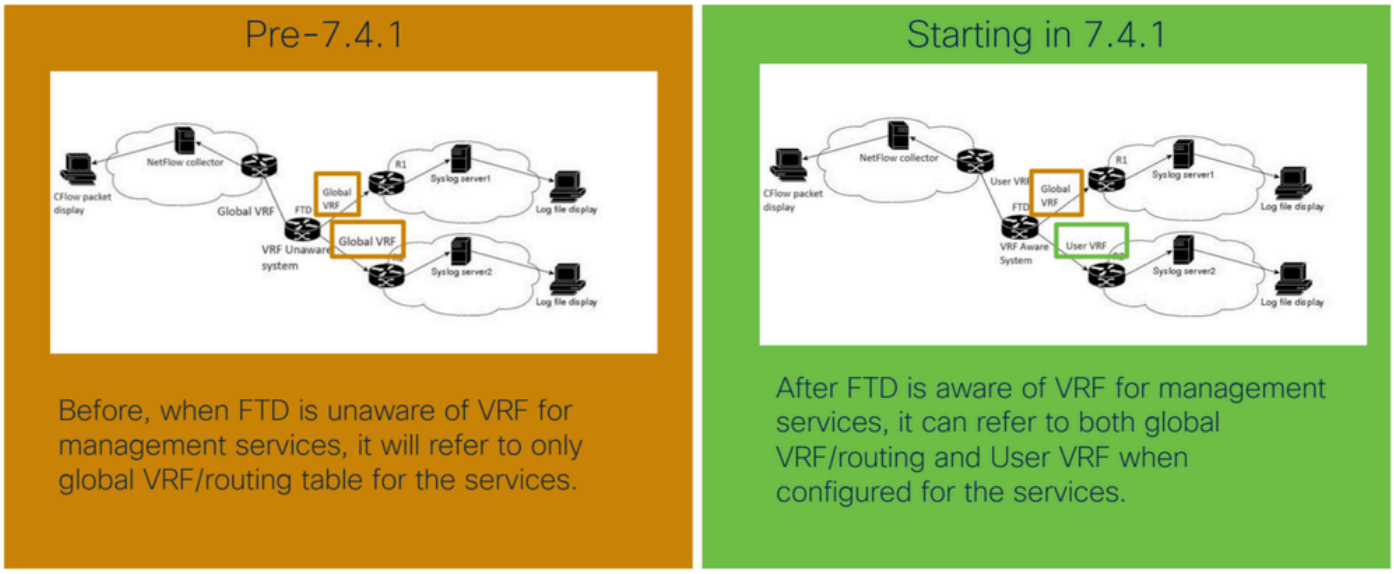
---

- 支持多实例。

- 支持HA'd设备。
- 在集群设备上受支持。

# 配置

## 网络图




7.4之前的版本与之后的版本之间的网络图比较。

## 配置

虚拟路由和转发(VRF)技术用于网络，允许路由表的多个实例在同一路由器内共存，从而在不同虚拟网络之间提供网络隔离。每个VRF实例与其他实例无关，它们之间的流量保持独立。多VRF功能使服务提供商能够支持多个VPN和服务，即使其IP地址重叠也是如此。它使用输入接口为各种服务指定路由，并通过为每个VRF分配第3层接口来创建虚拟数据包转发表。管理服务（系统日志、NetFlow）默认使用全局VRF。用户希望将用户VRF用于管理服务和全局VRF，因为并非所有上传目标均可通过全局VRF访问。

在本文档中，全局+用户VRF =多VRF

为用户VRF启用系统日志。

- 系统日志可以在多VRF环境中使用ftp服务。

## 工作原理

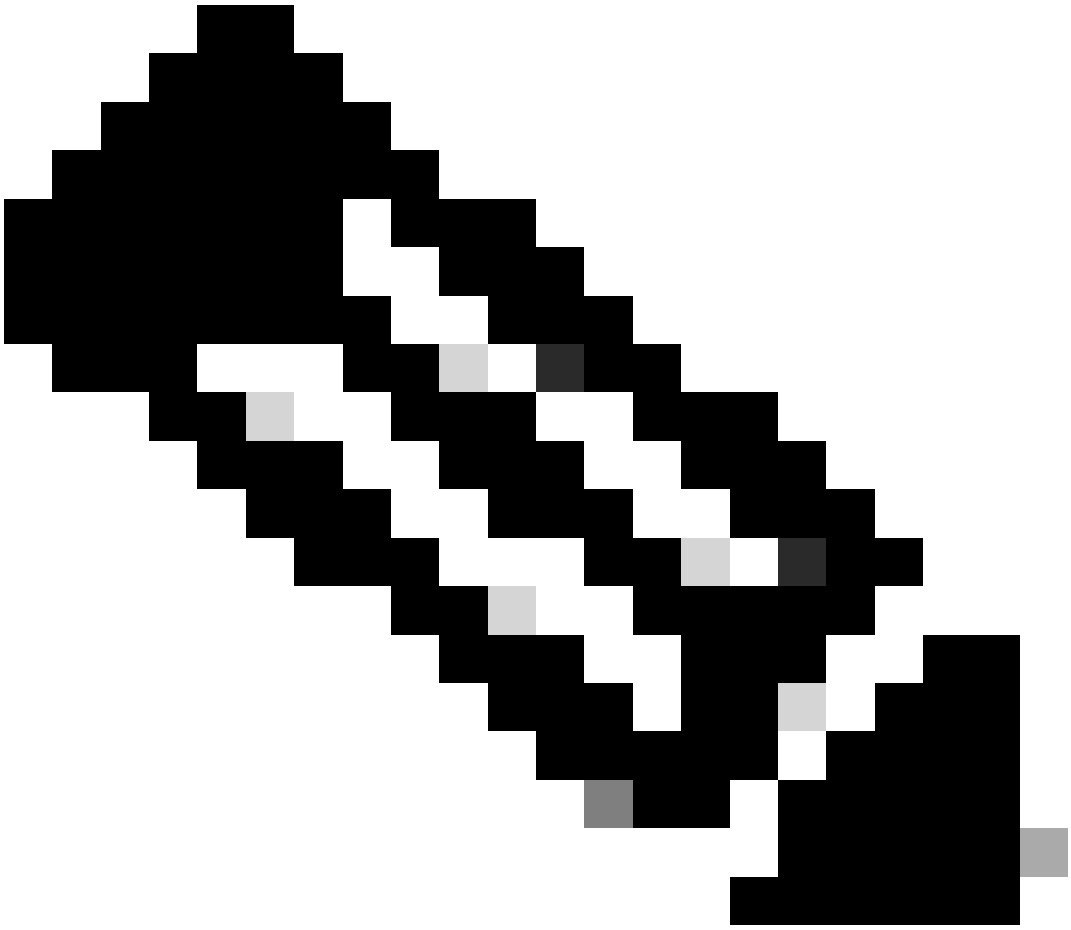
当接口配置有用户VRF时，路由查找在VRF路由域而非默认全局路由域中进行。

- 支持两种类型的服务器配置：

1. 将日志记录消息发送到系统日志服务器，以监控网络流量并对其进行故障排除。
2. 将日志缓冲区内容作为文本文件发送到FTP服务器

- 系统日志将日志发送到该VRF中各自的UDP/TCP服务器。
- 对于缓冲区封装系统日志，会将日志发送到该VRF中配置的FTP服务器。

---



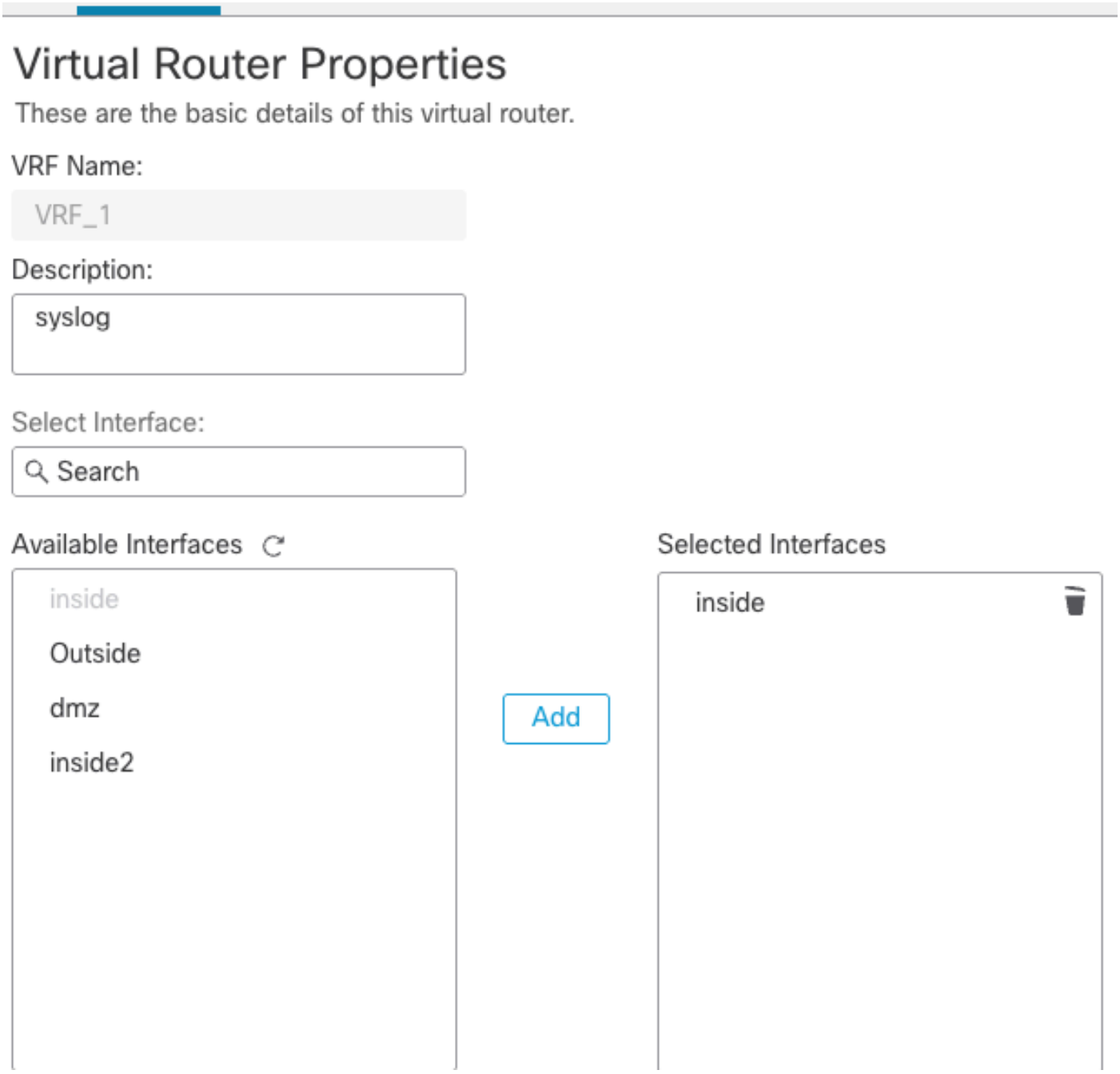
注意：系统日志服务器和FTP服务器可以是不同VRF的一部分。

---

## 配置虚拟路由器

步骤1.创建VRF

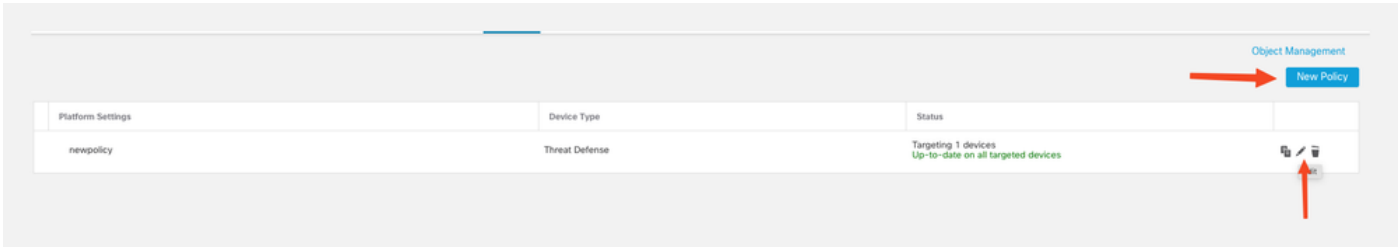
- 登录到FMC，然后导航到设备>设备管理。
- 选择Device，然后单击Pencil图标进行编辑。
- 导航到路由>管理虚拟路由器>添加虚拟路由器。
- 在VRF Name中输入名称。
- 选择接口，然后单击Add和Save。




将接口添加到VRF

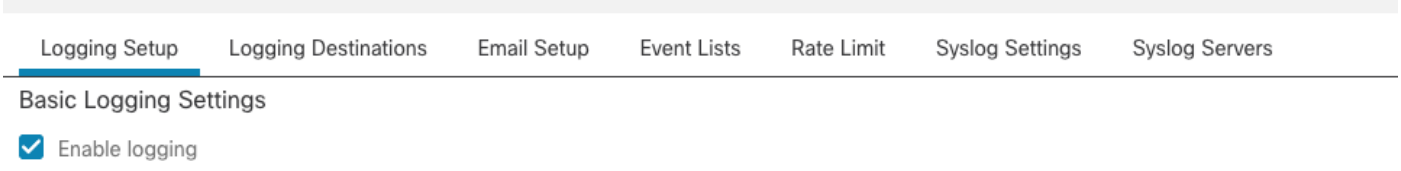
步骤2.配置日志记录设置。

- 导航到设备>平台设置。
- 创建新策略或编辑现有策略上的铅笔图标。




创建平台设置

- 选择Logging Setup和Enable logging。

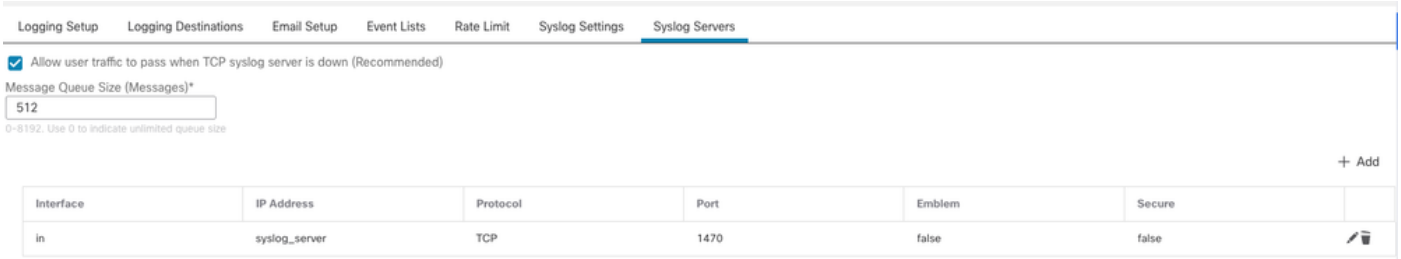



启用日志

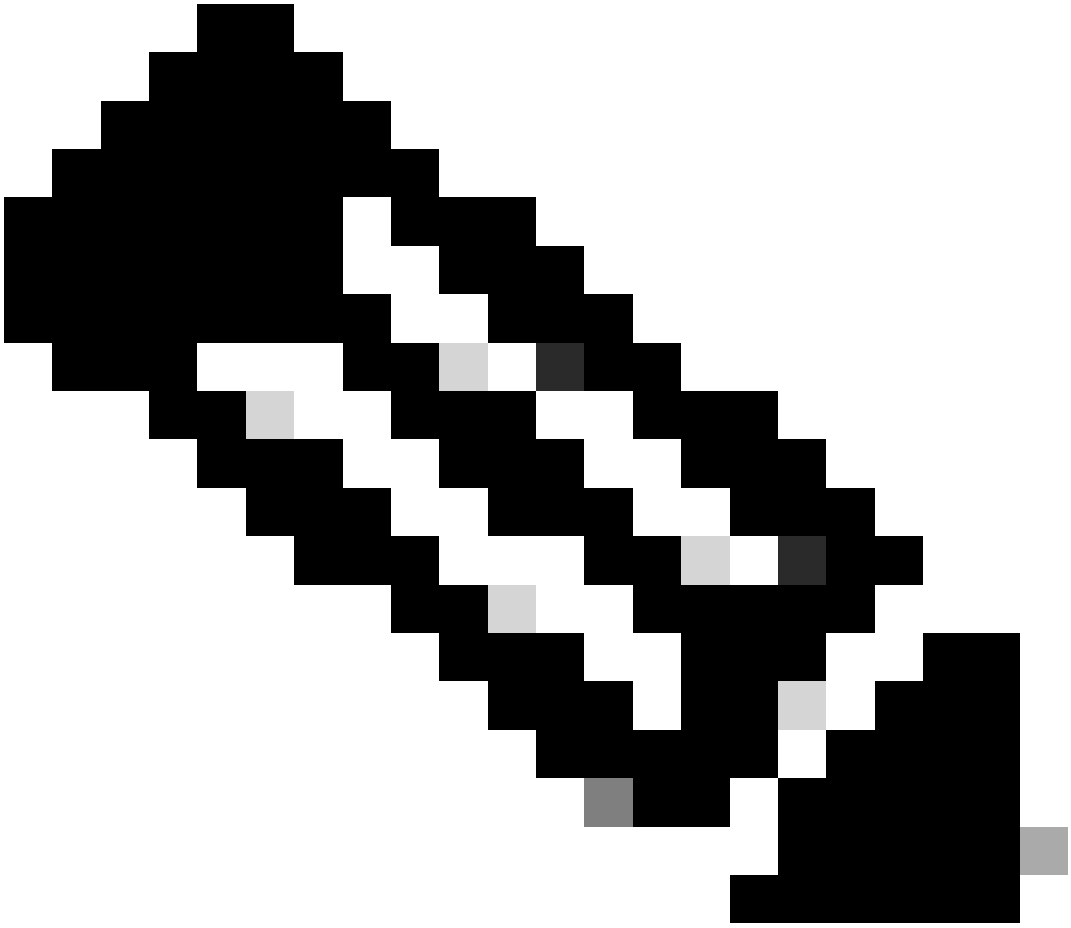
- 选择Logging Destination，然后单击Add。
- 将Logging Destination设置为系统日志服务器。


将目标记录为系统日志服务器

- 选择Syslog Servers > Add。




添加具有VRF感知接口的系统日志服务器



注意：内部接口是中的安全区域的一部分。

- logging host命令中配置的接口现在可感知VRF。
- Click Save.

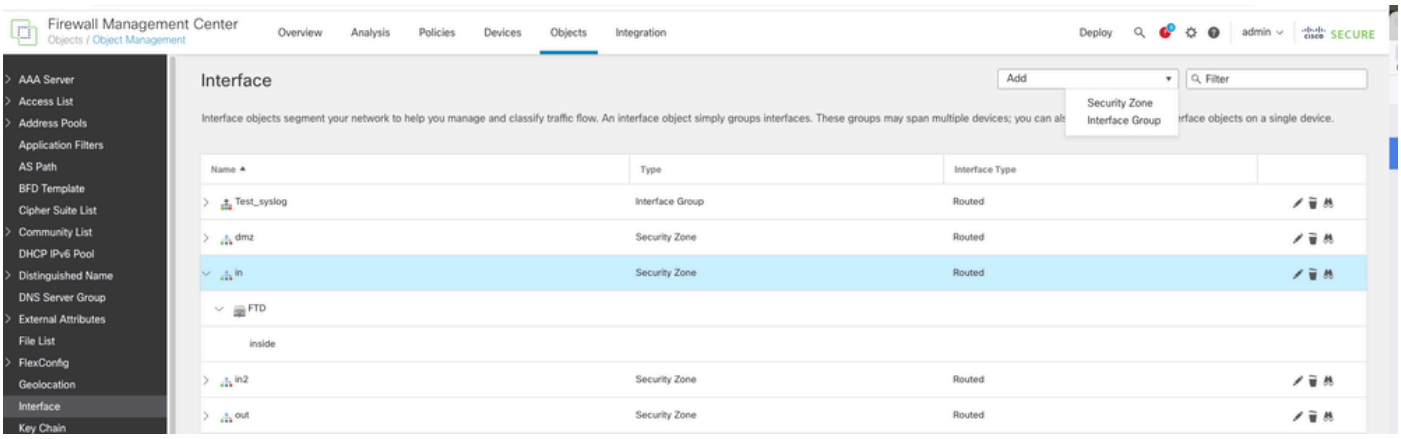
## FMC中FTP服务器配置的必备条件

- 使用接口组对象。
- 接口组对象可以同时具有用户和全局VRF。

## 配置

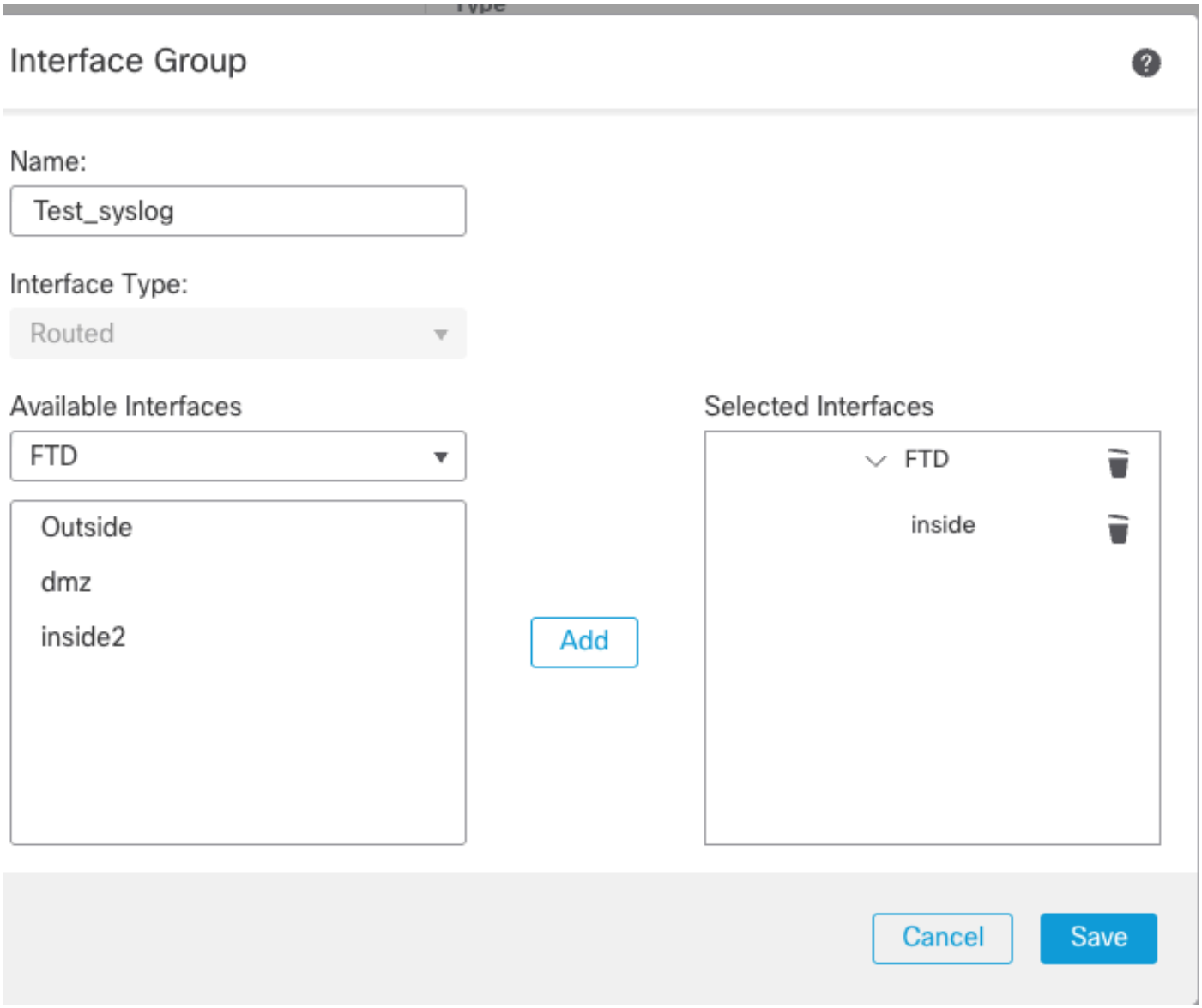
步骤1:

- 导航到对象>对象管理>接口>添加>接口组。




添加接口组

- 选择Device from下拉列表并添加VRF接口。

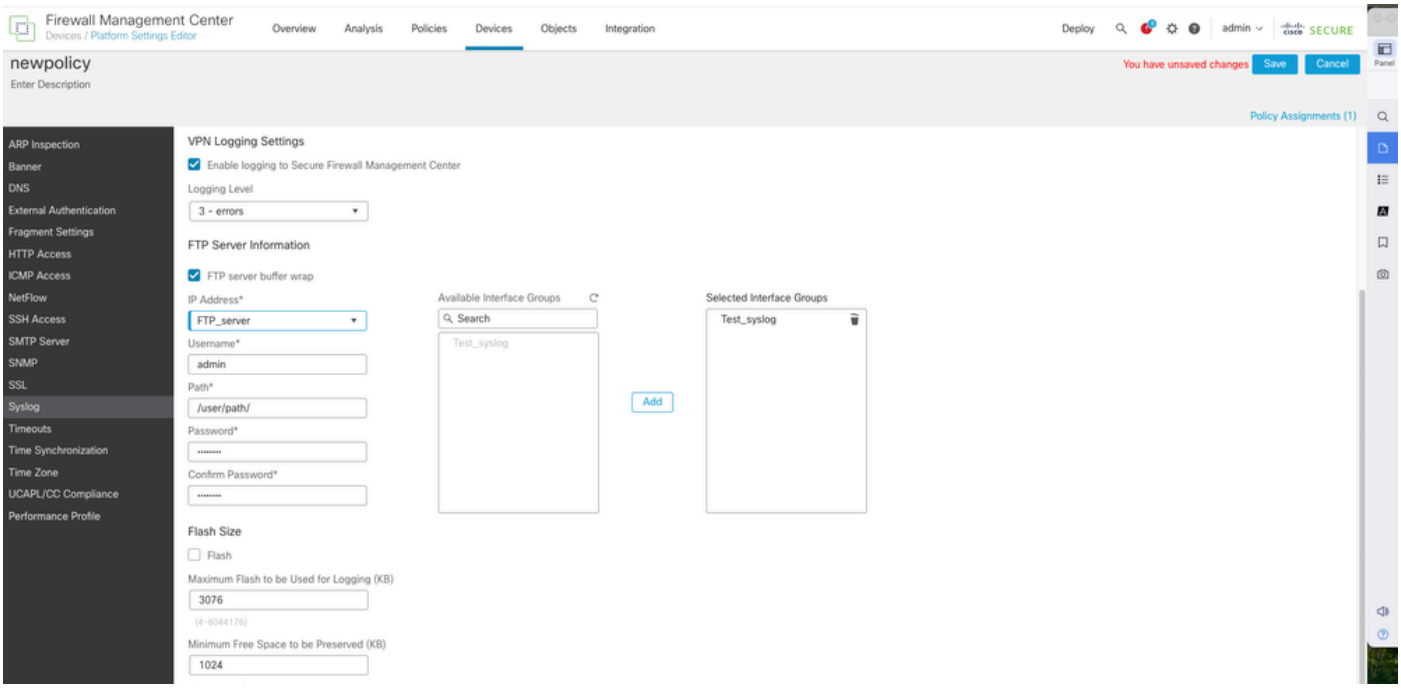



添加VRF感知接口

Step 2.

- 导航到设备>平台设置>系统日志>日志记录设置。启用FTP服务器缓冲区包。

- Click Save.




启用具有VRF感知接口的FTP服务器

# 验证

## Pre 7.4.1

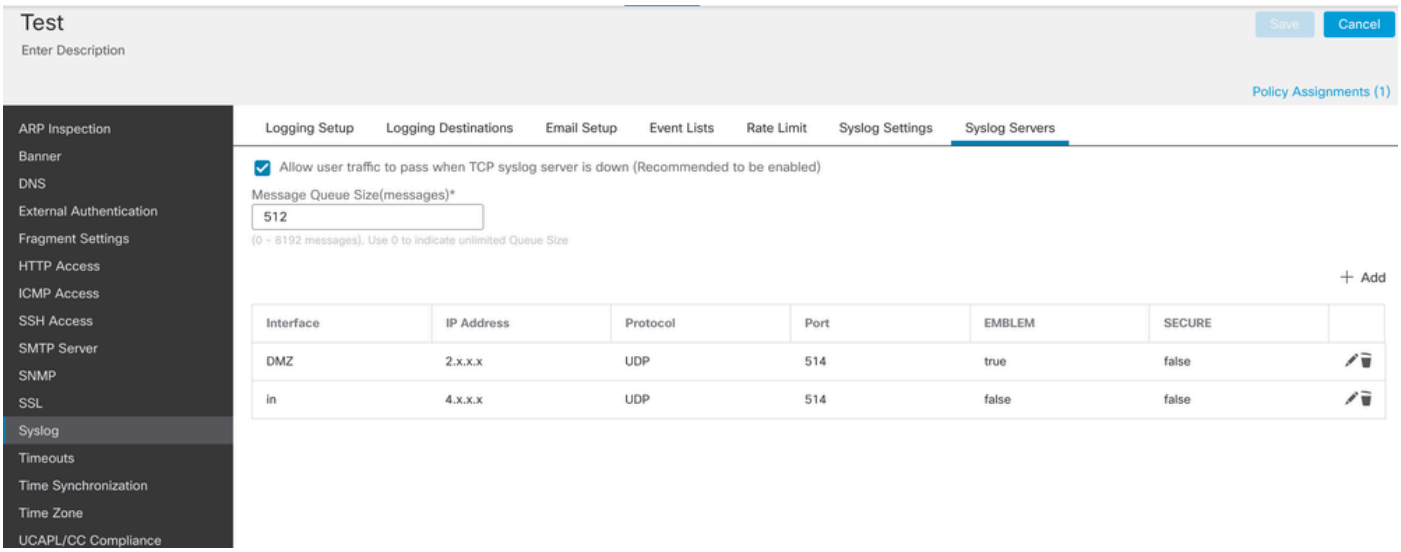
在本测试中，FTD和FMC为7.0.5。

FTD配置了VRF，并且dmz接口已分配给VRF。

使用syslog服务器日志记录主机配置dmz接口。

此外，内部接口配置了syslog设置。

内部接口是全局VRF的一部分。

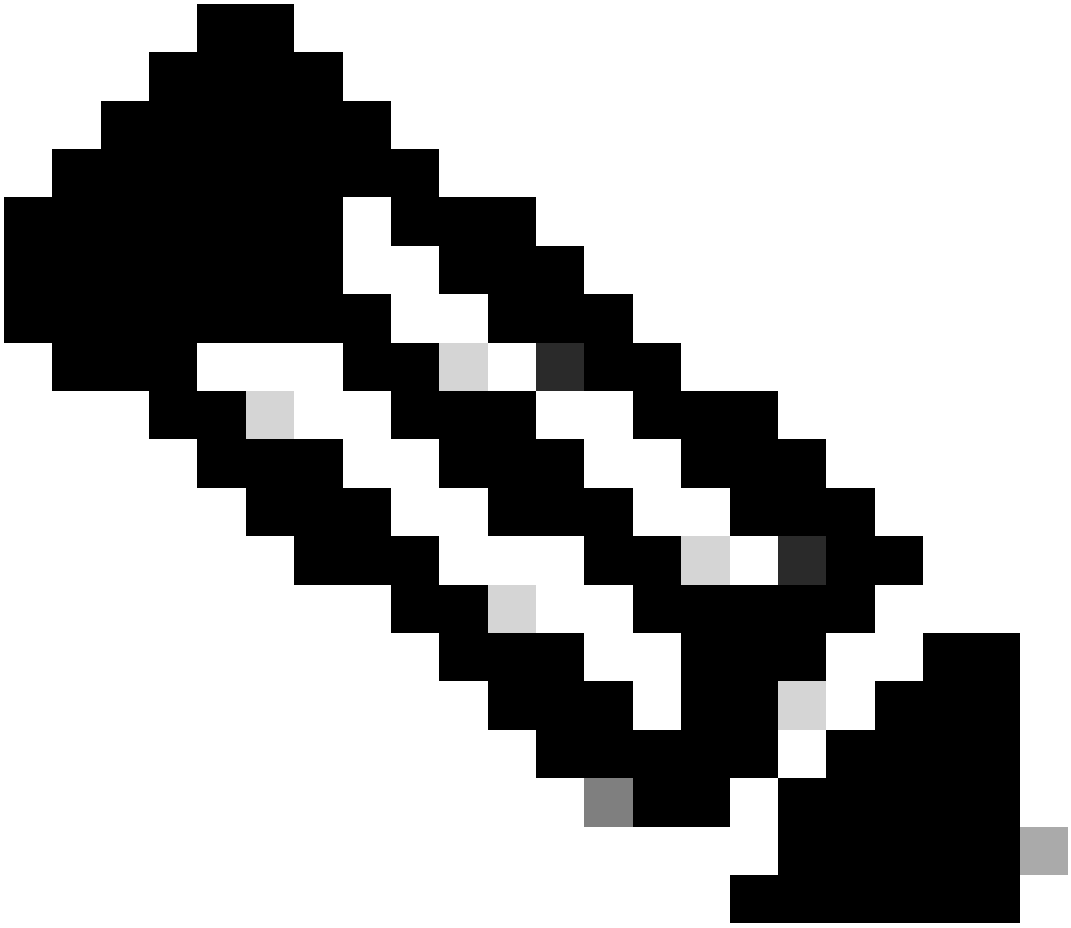


## CLI验证

```
> 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
```



注意：在FTD CLI的日志记录设置中，没有目标为2.x.x.x的系统日志服务器。这是用户VRF的一部分。
在FTD CLI的日志记录设置中，具有目标4.x.x.x的系统日志服务器可用。这是全球VRF的一部分。

## Post 7.4.1

### CLI验证

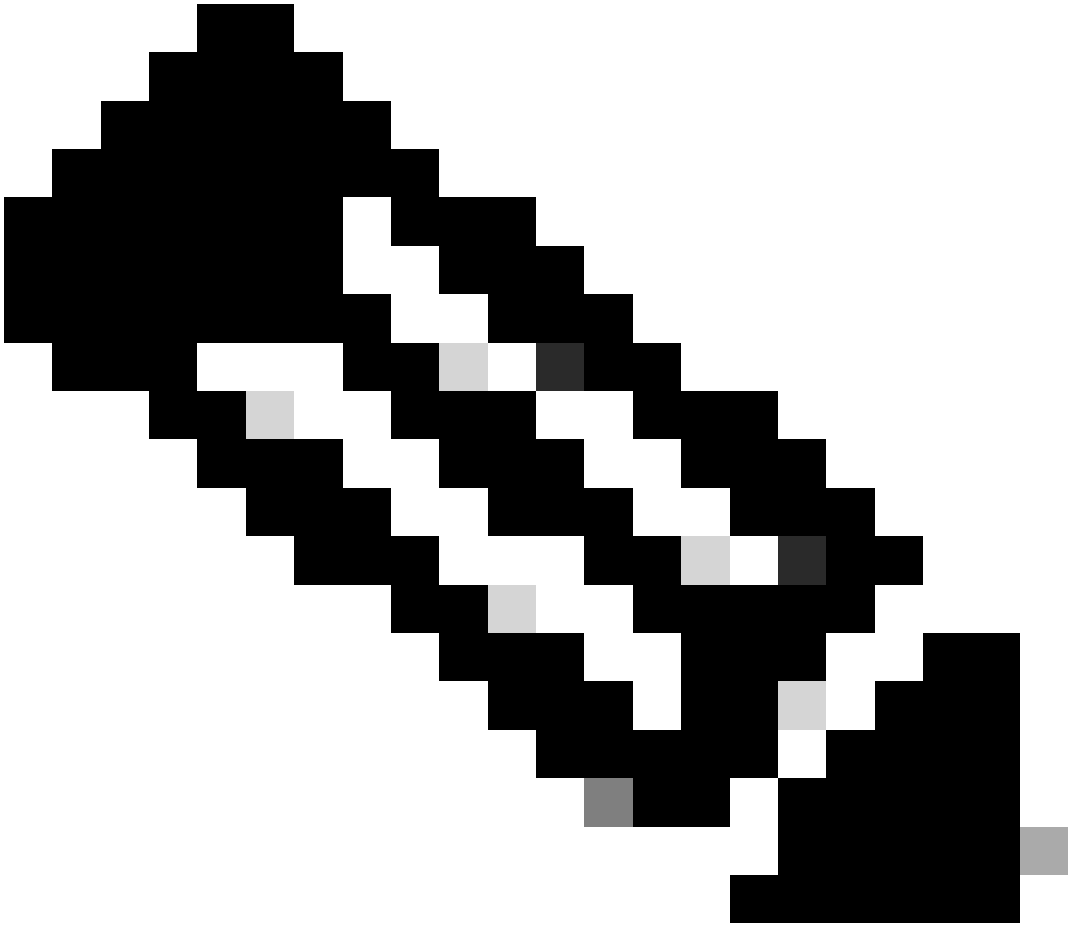
```
ftd1# show vrf

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
```



注意：Syslog服务器主机192.x.x.x使用VRF感知内部接口。

## FTP服务器验证

### Pre 7.4.1

- 在FMC上，FTP服务器设置没有用于选择要使用的接口的选项。只有syslog服务器选项的IP地址可用。

## 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

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。