Configure VRF Aware Syslog on FTD

Contents

Introduction

This document describes the configuration steps for VRF aware syslog on FTD.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Syslog
- Firepower Threat Defense (FTD)

Components Used

The information in this document is based on these software and hardware versions:

- Secure Firewall Management Center (FMCv) v7.4.2
- Secure Firewall Threat Defense Virtual (FTDv) v7.4.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Minimum Software and Hardware Platforms

- Application and Minimum version: Secure Firewall 7.4.1
- Supported Managed Platforms and version: All which support FTD 7.4.1
- Managers:
  1) FMC on-perm + FMC REST API
  2) cloud-delivered FMC
  3) FDM + REST API

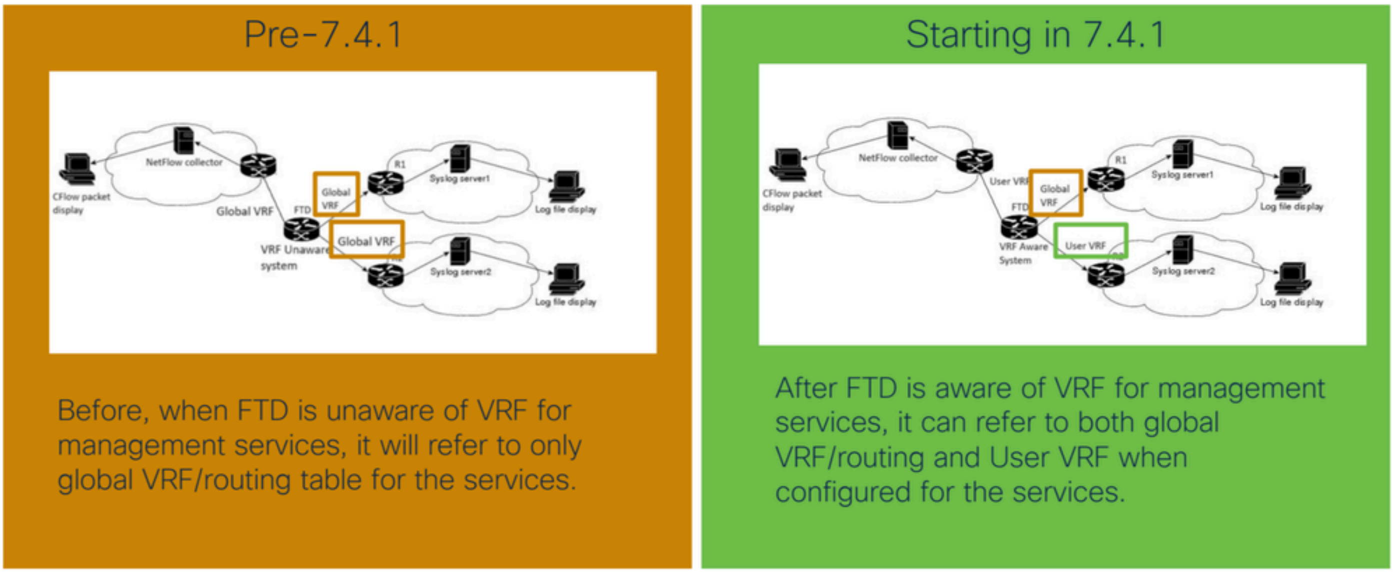
Snort3, Multi-Instance/Context and HA/Clustering Support

Note: Works with both IPv4 and IPv6 syslog servers. IPv6 is not supported yet in Syslog ftp server.

- Supported with Multi-instance.
- Supported with HA'd devices.
- Supported on Clustered Devices.

Configure

Network Diagram



Pre-7.4.1

Before, when FTD is unaware of VRF for management services, it will refer to only global VRF/routing table for the services.

Starting in 7.4.1

After FTD is aware of VRF for management services, it can refer to both global VRF/routing and User VRF when configured for the services.

Network Diagram Comparison between Pre and Post 7.4.

Configurations

Virtual Routing and Forwarding (VRF) is a technology used in networking to allow multiple instances of a routing table to coexist within the same router, providing network isolation between different virtual networks. Each VRF instance is independent of others, and traffic between them is kept separate. Multi-VRF is a feature that enables service providers to support multiple VPNs and services, even if their IP addresses overlap. It uses input interfaces to designate routes for various services and create virtual packet-forwarding tables by assigning Layer 3 interfaces to each VRF. Management services (Syslog, NetFlow) use Global VRF as default. Users want to use User VRF for Management services as well as the Global VRF because not all upload destinations are reachable via Global VRF.

In this document, Global + User VRF = Multi-VRF

Enable Syslog for User VRF.

- Syslog can use ftp service in a multi-VRF context.

How it Works

When interface is configured with User VRF, route lookup occurs in VRF routing domain, instead of default global routing domain.

- Two types of server configurations are supported:

1. Send logging messages to Syslog servers to monitor and troubleshoot the network traffic.
2. Send the log buffer content to an FTP server as a text file

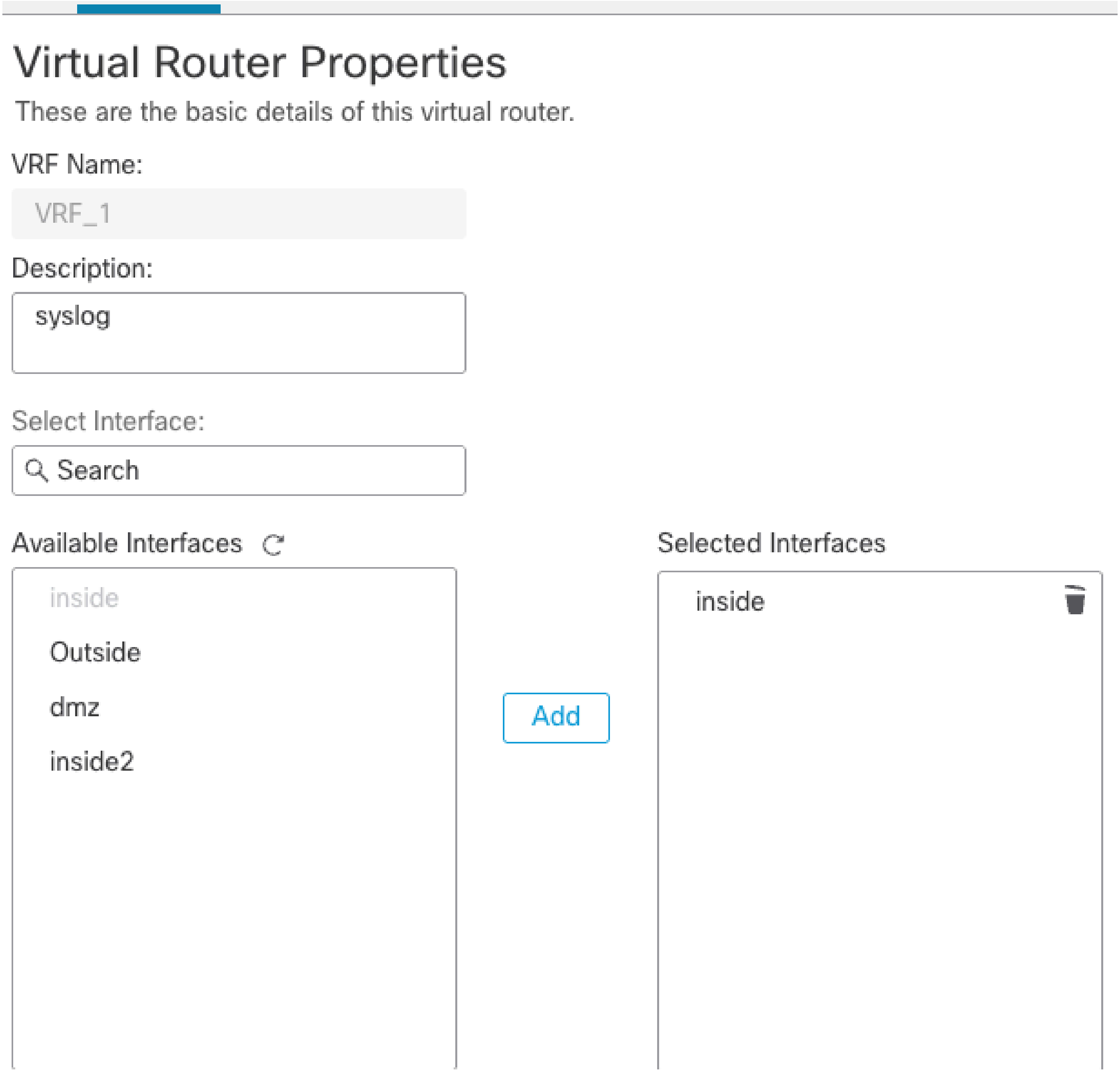
- Syslog emits the logs to the respective UDP/TCP servers within that VRF.
- For buffer wrap syslogs, the logs are sent to configured FTP server within that VRF.

Note: Syslog server and FTP server can be part of different VRFs.

Configure Virtual Router

Step 1. Create a VRF

- Log in to **FMC** and navigate to **Device > Device Management**.
- Select the **Device** and click the **Pencil** icon to edit it.
- Navigate to **Routing> Manage Virtual Router > Add Virtual Router**.
- Enter the **name** in **VRF Name**.
- Select the **interface** and click **Add** and **Save**.



Virtual Router Properties

These are the basic details of this virtual router.

VRF Name: VRF_1

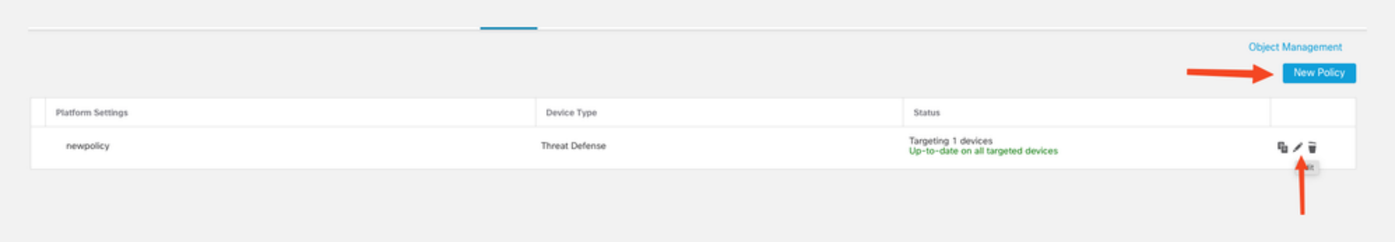
Description: syslog

Select Interface:

Adding Interface to VRF

Step 2. Configure the logging set-up.

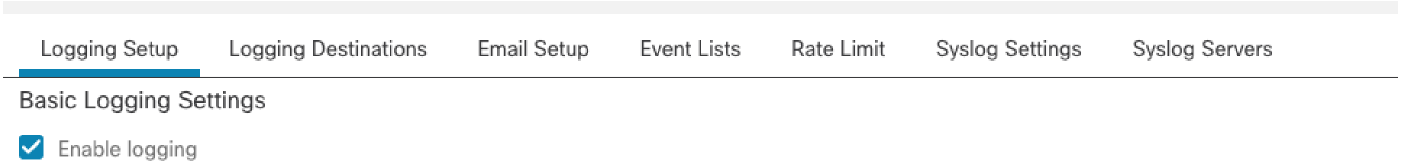
- Navigate to **Devices** > **Platform Settings**.
- Create a **New Policy** or edit the **Pencil** icon on existing policy.



Platform Settings	Device Type	Status
newpolicy	Threat Defense	Targeting 1 devices Up-to-date on all targeted devices

Creating the Platform Settings

- Select **Logging Setup** and **Enable logging**.

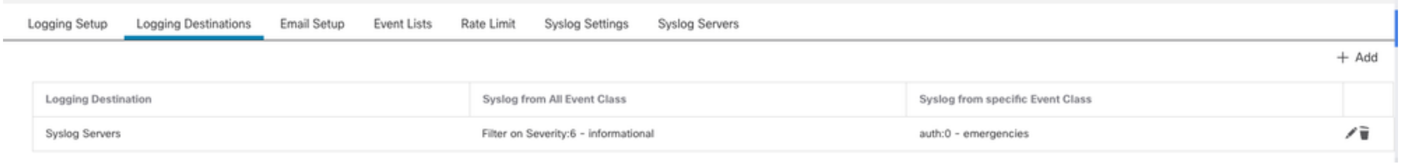


Basic Logging Settings

☑ Enable logging

Enable Logging

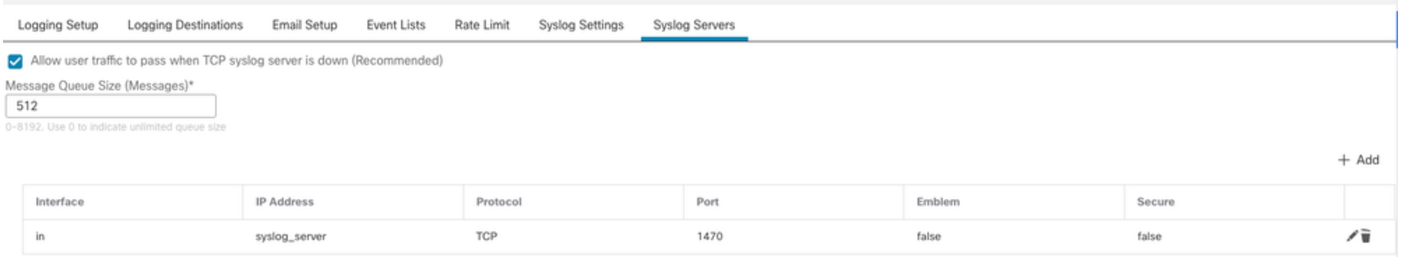
- Select **Logging Destination** and click **Add**.
- Set the **Logging Destination** as **Syslog servers**.



Logging Destination	Syslog from All Event Class	Syslog from specific Event Class
Syslog Servers	Filter on Severity:6 - informational	auth:0 - emergencies

Logging Destination as Syslog Servers

- Select **Syslog Servers** > **Add**.



☑ Allow user traffic to pass when TCP syslog server is down (Recommended)

Message Queue Size (Messages)*

512

0-8192. Use 0 to indicate unlimited queue size

Interface	IP Address	Protocol	Port	Emblem	Secure
in	syslog_server	TCP	1470	false	false

Adding Syslog Server with VRF Aware Interface

Note: Inside interface is part of Security-zone in.

- The interface configured in logging host command is now VRF aware.
- Click **Save**.

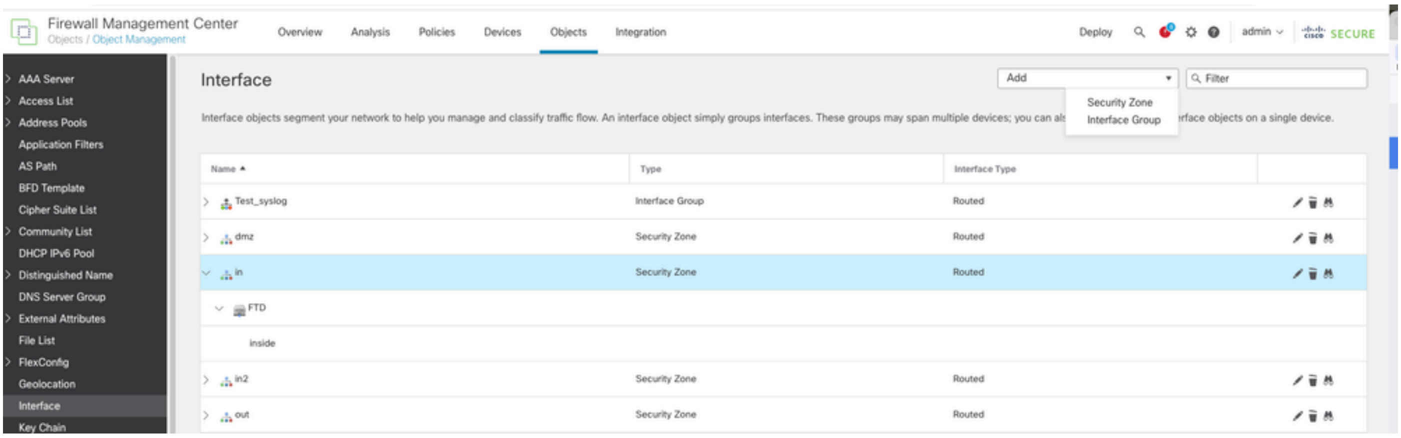
Prerequisites for FTP Server Configuration in FMC

- Use **Interface Group Object**.
- Interface Group Object can have both User and Global VRF.

Configuration

Step 1.

- Navigate to **Object > Object Management > Interface > Add > Interface Group**.



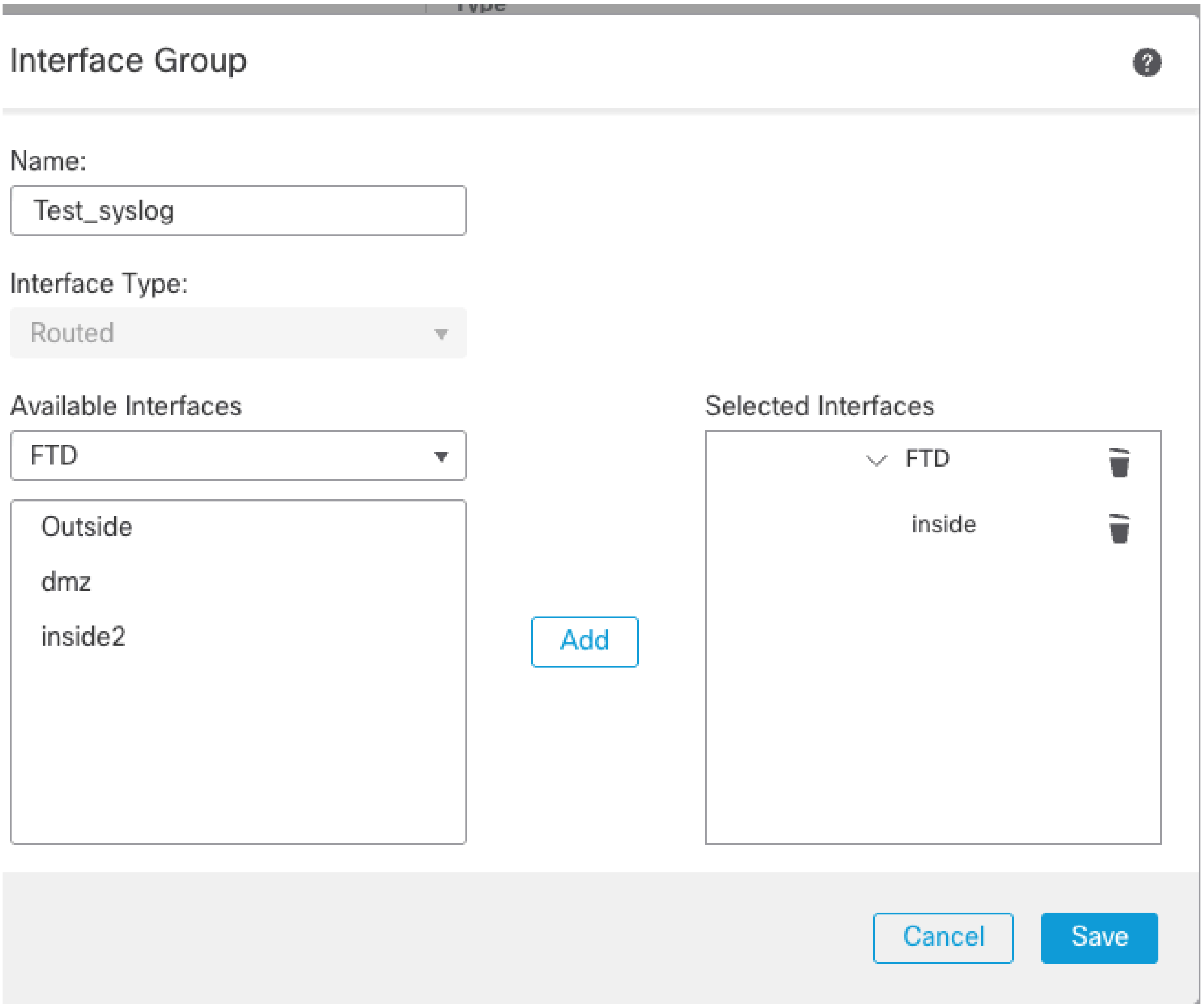
Interface

Interface objects segment your network to help you manage and classify traffic flow. An interface object simply groups interfaces. These groups may span multiple devices; you can als rface objects on a single device.

Name ▲	Type	Interface Type
Test_syslog	Interface Group	Routed
dmz	Security Zone	Routed
in	Security Zone	Routed
FTD		
inside		
in2	Security Zone	Routed
out	Security Zone	Routed

Adding Interface Group

- Select the **Device** from drop down and **Add** the VRF **Interface**.



Interface Group

Name: Test_syslog

Interface Type: Routed

Available Interfaces: FTD

Outside
dmz
inside2

Selected Interfaces

FTD
inside

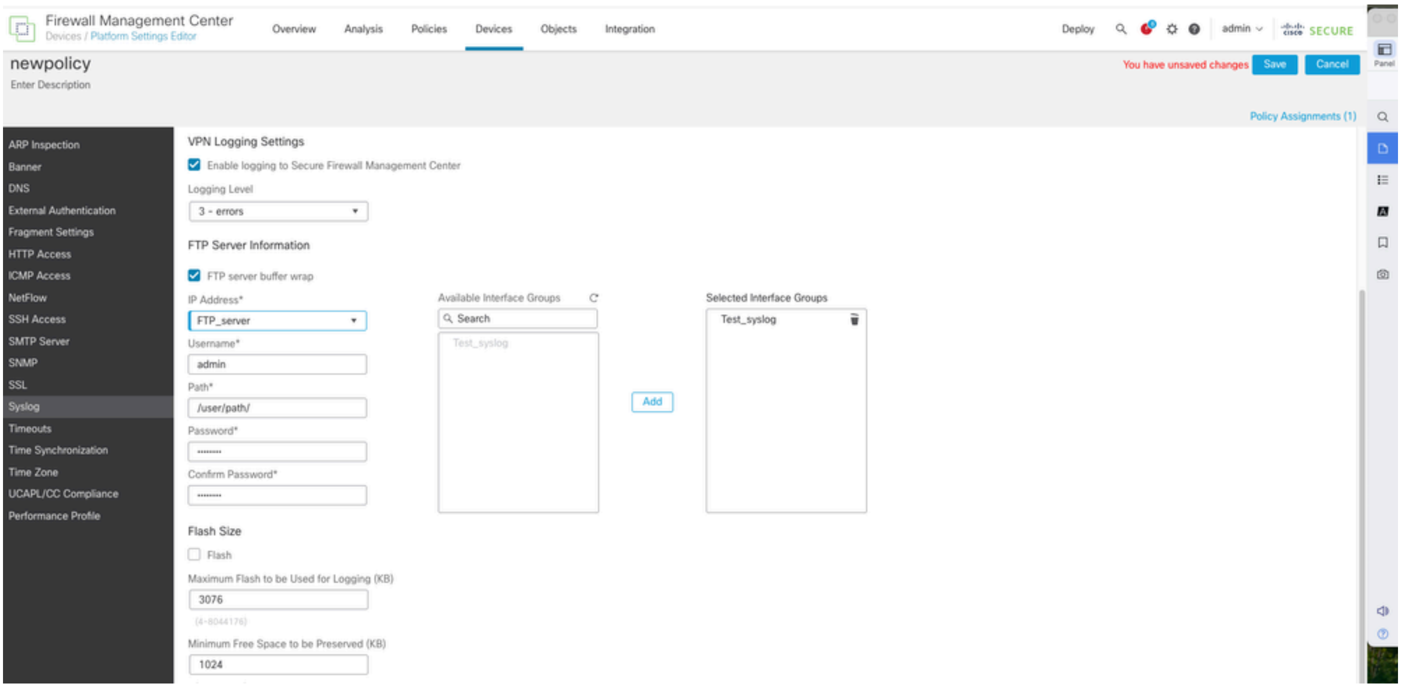
Adding VRF Aware Interface

Step 2.

- Navigate to **Devices > Platform Settings > Syslog > Logging Setup**. Enable **FTP server buffer**

wrap.

- Click **Save**.



VPN Logging Settings

☑ Enable logging to Secure Firewall Management Center

Logging Level: 3 - errors

FTP Server Information

☑ FTP server buffer wrap

IP Address*: FTP_server

Username*: admin

Path*: /user/path/

Password*: ********

Confirm Password*: ********

Available Interface Groups: Test_syslog

Selected Interface Groups: Test_syslog

Flash Size

□ Flash

Maximum Flash to be Used for Logging (KB): 3076

(4-8044176)

Minimum Free Space to be Preserved (KB): 1024

Enable FTP Server with VRF Aware Interface

Verify

Pre 7.4.1

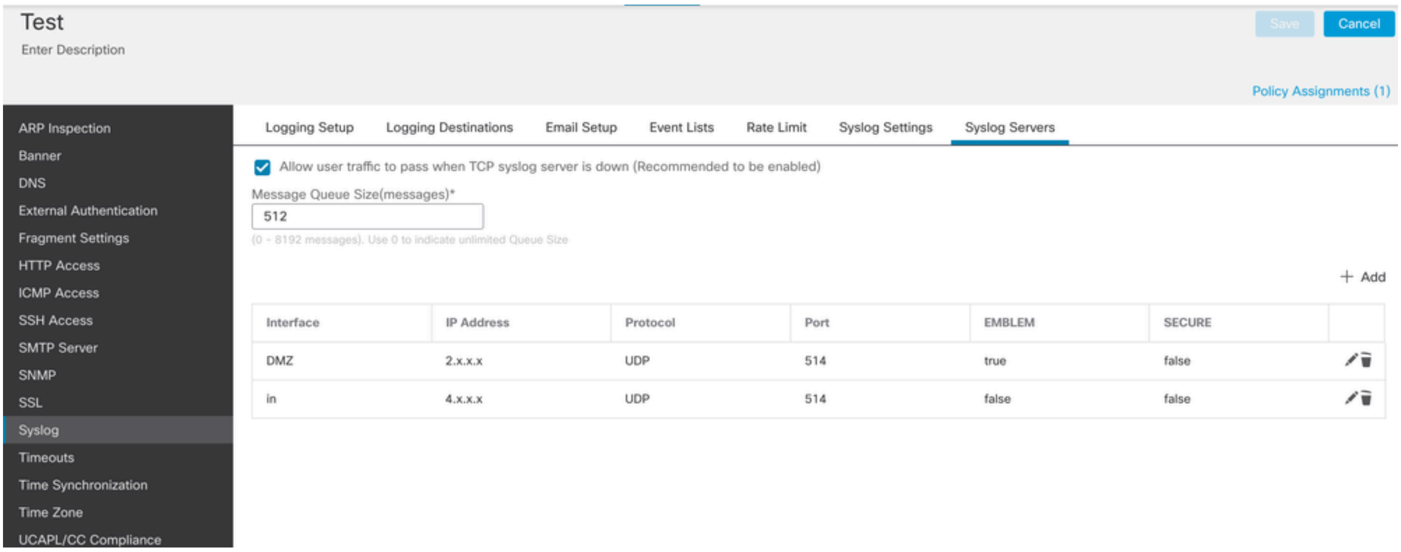
In this test, the FTD and FMC is 7.0.5.

FTD is configured with VRF and dmz interface has been assigned to VRF.

The dmz interface is configured with syslog server logging host.

Additionally inside interface is configured with syslog setting.

The inside interface is part of Global VRF.



☑ Allow user traffic to pass when TCP syslog server is down (Recommended to be enabled)

Message Queue Size(messages)*: 512

(0 - 8192 messages). Use 0 to indicate unlimited Queue Size

Interface	IP Address	Protocol	Port	EMBLEM	SECURE
DMZ	2.x.x.x	UDP	514	true	false
in	4.x.x.x	UDP	514	false	false

Syslog Server Setting on 7.0.5 FMC

CLI Verification

```
> 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: Syslog server with destination 2.x.x.x is not available on logging setting for FTD CLI. This is part of User VRF.
Syslog server with destination 4.x.x.x is available on logging setting for FTD CLI. This is part of Global VRF.

Post 7.4.1

CLI Verification

```
ftd1# show vrf

Name                             VRF ID     Description      Interfaces
VRF_1                            1          syslog           inside
```

```
td1# show logging
Syslog logging: enabled
```

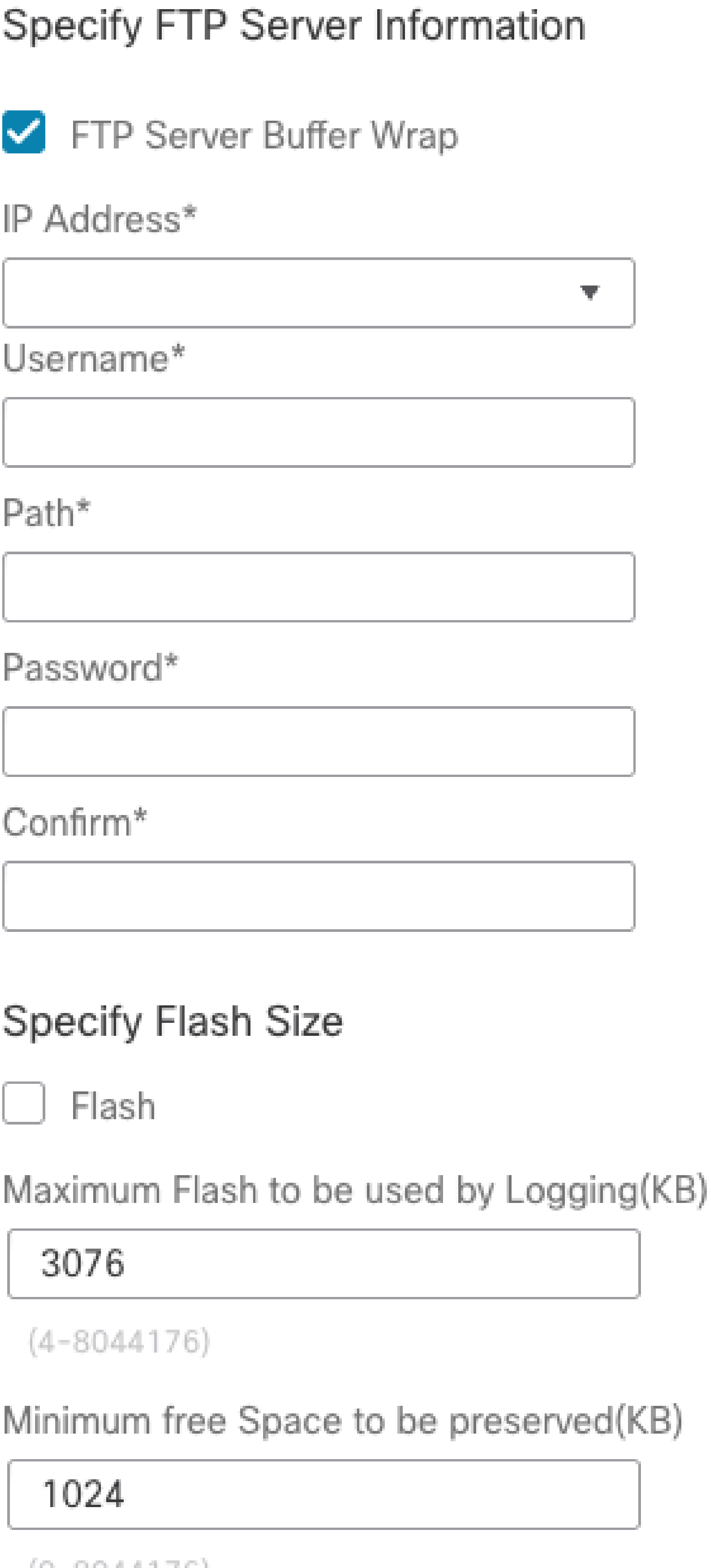
```
Facility: 20
Timestamp logging: disabled
Hide Username logging: enabled
Standby logging: disabled
Debug-trace logging: disabled
Console logging: disabled
Monitor logging: disabled
Buffer logging: disabled
Trap logging: level informational, class auth, facility 20, 19284 messages logged
    Logging 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: Syslog server host 192.x.x.x is using the VRF aware inside interface.

FTP Server Verification

Pre 7.4.1

- On FMC, FTP server setting does not have the option to select Interface to use. Only IP address of the syslog server option is available.



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

(0-8044176)