FTDでのVRF対応syslogの設定

内容

はじめに

このドキュメントでは、FTDでのVRF対応syslogの設定手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Syslog
- Firepower Threat Defense（FTD）

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

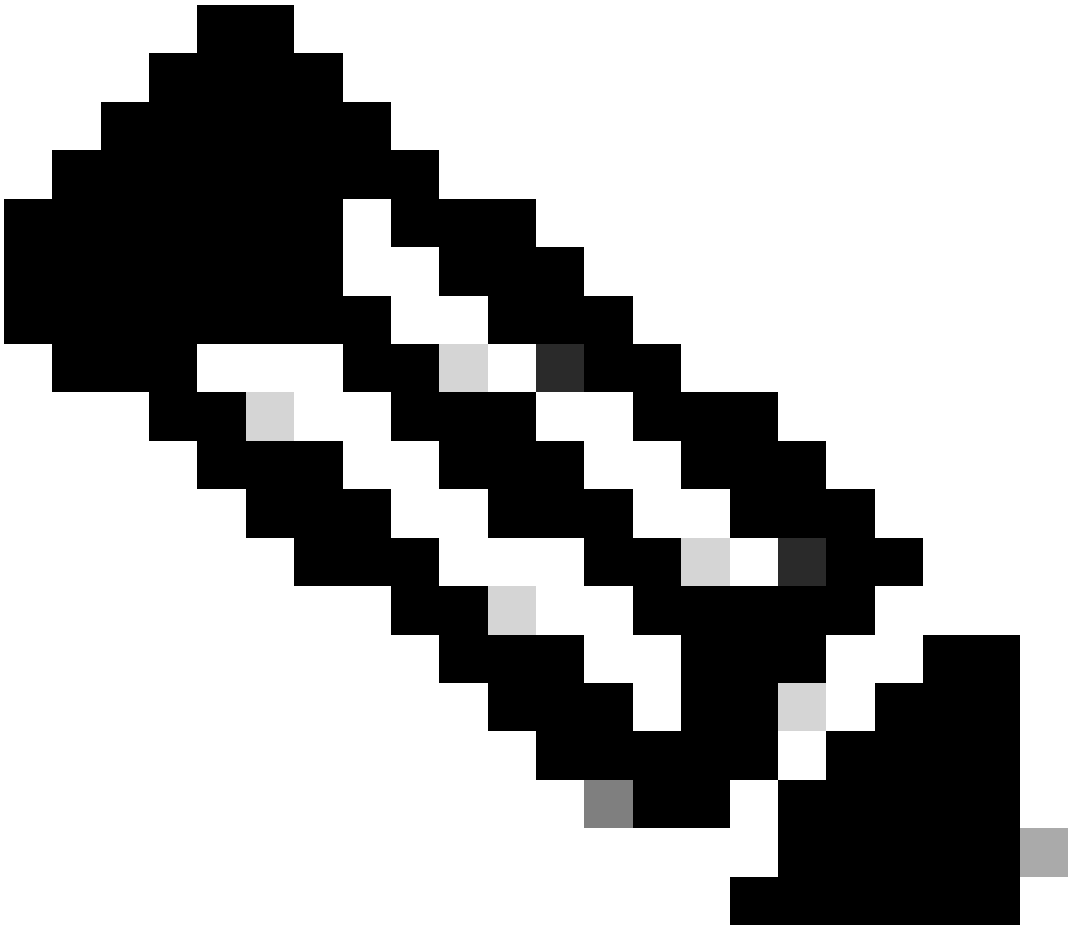
- セキュアファイアウォール管理センター(FMCv)v7.4.2
- セキュアファイアウォール脅威対策仮想(FTDv)v7.4.2

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

最低限のソフトウェアおよびハードウェアプラットフォーム

- アプリケーションおよび最小バージョン：セキュアファイアウォール7.4.1
- サポートされているマネージドプラットフォームとバージョン：FTD 7.4.1をサポートしているすべて
- マネージャ:
  1)FMCオンパーマ+ FMC REST API
  2)クラウド配信のFMC
  3) FDM + REST API

Snort3、マルチインスタンス/コンテキスト、およびHA/クラスタリングのサポート

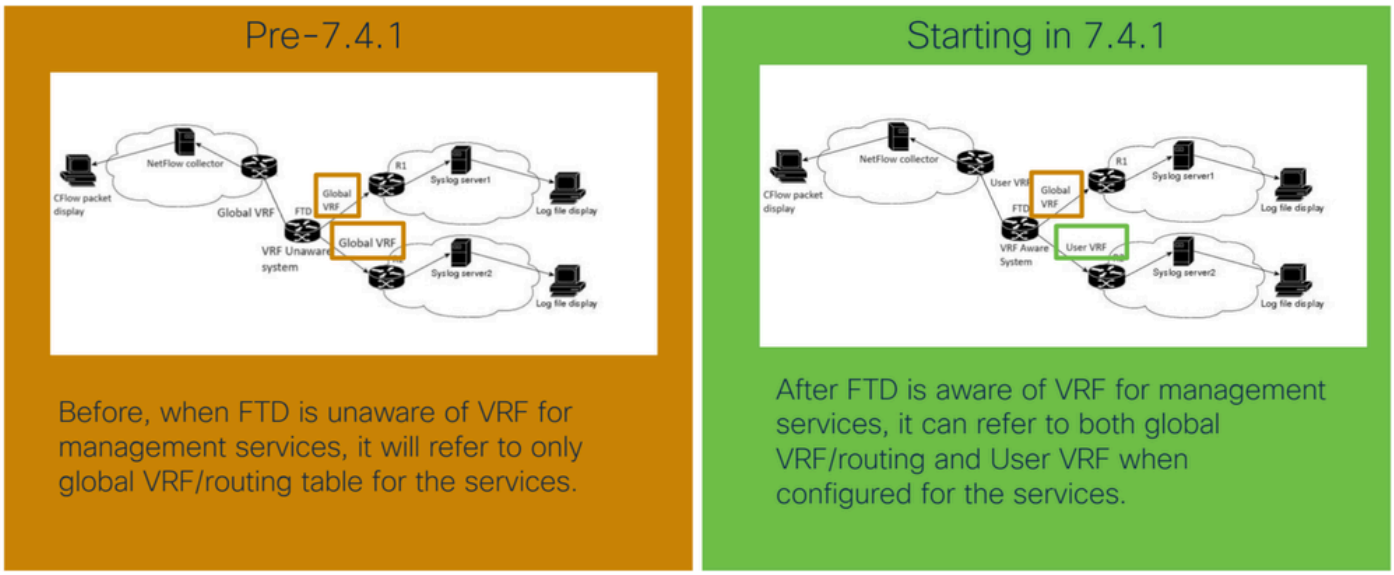


注:IPv4とIPv6の両方のsyslogサーバで動作します。IPv6は、Syslog ftpサーバではまだサポートされていません。

- マルチインスタンスでサポート
- HA対応デバイスでサポート
- クラスタ化されたデバイスでサポート

設定

ネットワーク図



7.4より前と後のネットワーク図比較。

コンフィギュレーション

Virtual Routing and Forwarding(VRF)は、ネットワークで使用されるテクノロジーです。VRFを使用すると、ルーティングテーブルの複数のインスタンスを同じルータ内に共存させることができ、異なる仮想ネットワーク間でネットワークを分離できます。各VRFインスタンスは相互に独立しており、インスタンス間のトラフィックは分離されています。マルチVRFは、IPアドレスが重複していても、サービスプロバイダーが複数のVPNとサービスをサポートできるようにする機能です。入力インターフェイスを使用してさまざまなサービスのルートを指定し、各VRFにレイヤ3インターフェイスを割り当てることで仮想パケット転送テーブルを作成します。管理サービス(Syslog、NetFlow)は、デフォルトとしてグローバルVRFを使用します。すべてのアップロード先にグローバルVRF経由で到達できるわけではないため、ユーザはグローバルVRFだけでなく、管理サービスにもユーザVRFを使用したいと考えています。

このドキュメントでは、グローバル+ユーザVRF =マルチVRFです。

ユーザVRFのsyslogを有効にします。

- SyslogはマルチVRFコンテキストでftpサービスを使用できます。

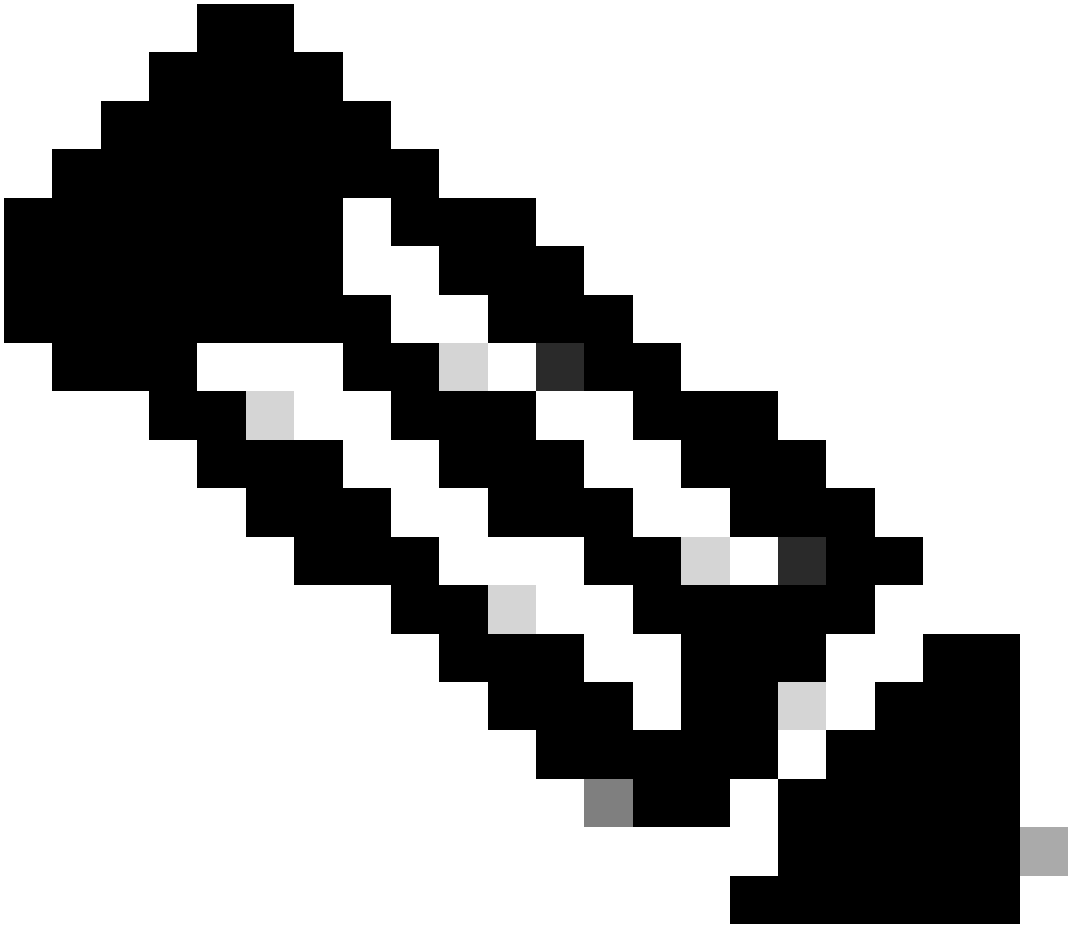
仕組み

インターフェイスにユーザVRFが設定されている場合、ルートルックアップは、デフォルトのグローバルルーティングドメインではなく、VRFルーティングドメインで発生します。

- 次の2種類のサーバ設定がサポートされています。

1. ロギングメッセージをSyslogサーバに送信して、ネットワークトラフィックの監視とトラブルシューティングを行います。
2. ログバッファの内容をテキストファイルとしてFTPサーバに送信する

- syslogは、そのVRF内の各UDP/TCPサーバにログを送信します。
- バッファラップsyslogの場合、ログはそのVRF内に設定されたFTPサーバに送信されます。

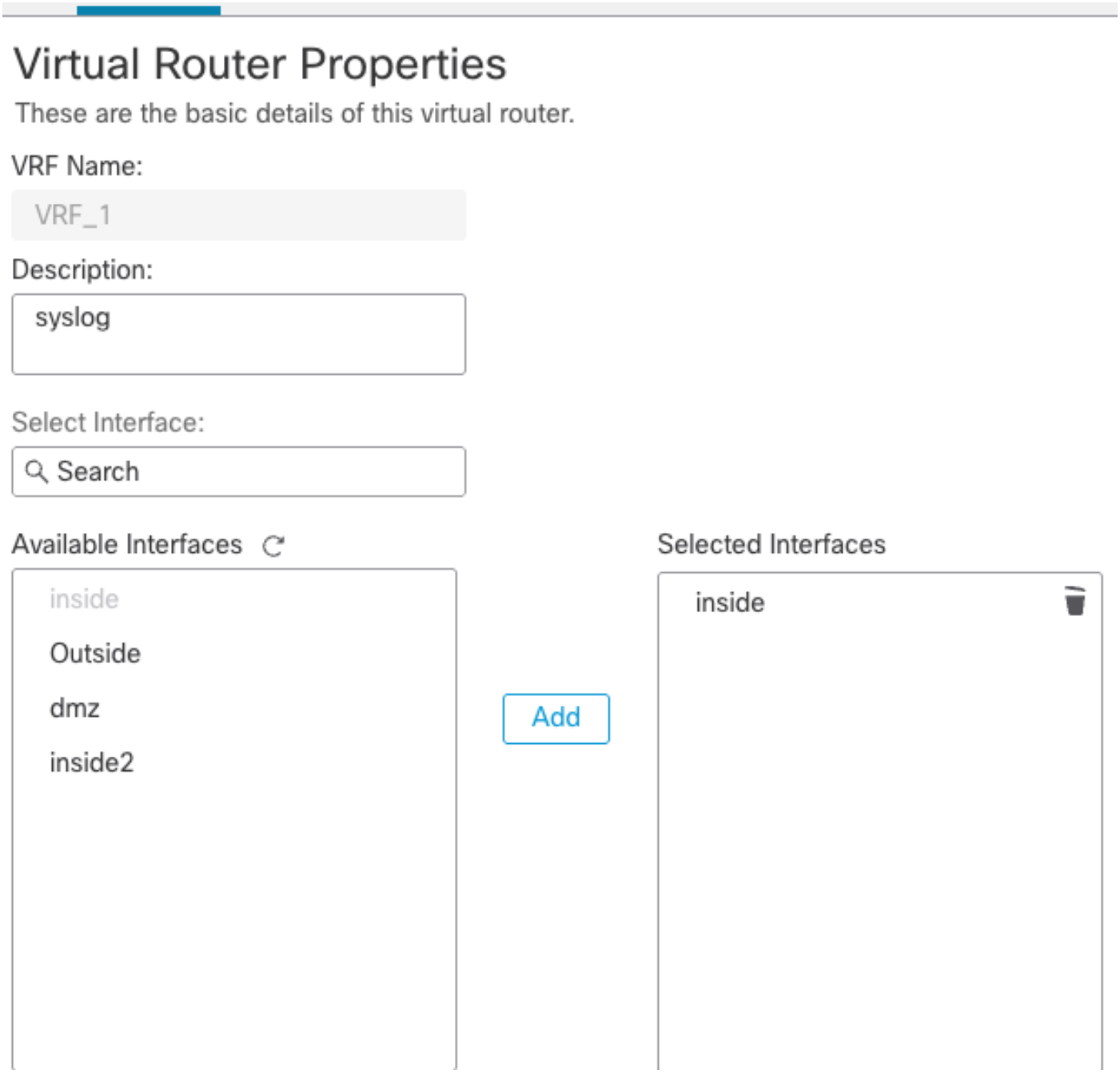


注:SyslogサーバとFTPサーバは、異なるVRFに属することができます。

仮想ルータの設定

ステップ 1： VRFの作成

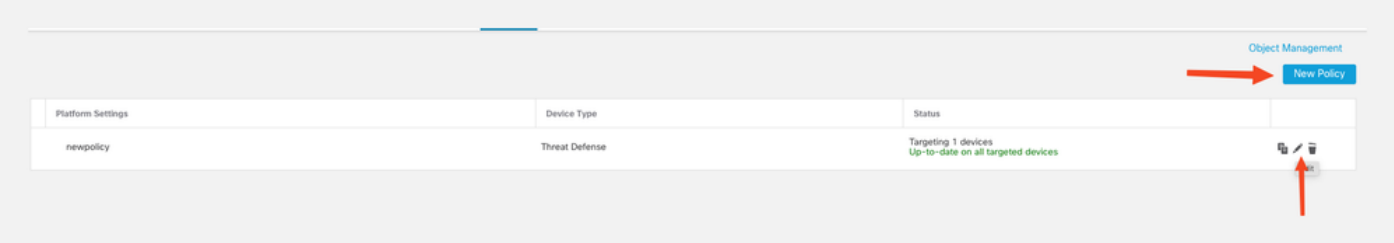
- FMCにログインし、Device > Device Managementに移動します。
- デバイスを選択し、鉛筆アイコンをクリックして編集します。
- Routing> Manage Virtual Router > Add Virtual Routerの順に移動します。
- VRF Nameに名前を入力します。
- interfaceを選択し、AddとSaveをクリックします。



VRFへのインターフェイスの追加

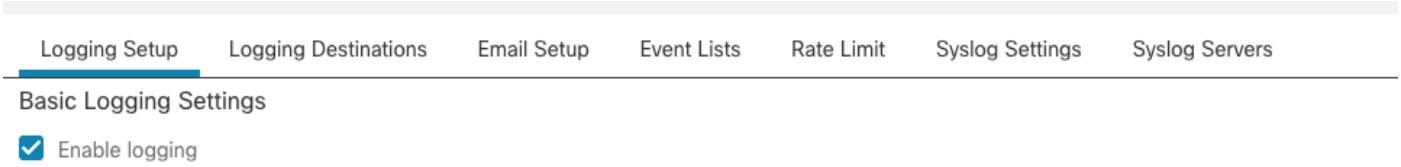
ステップ 2：ロギングセットアップを設定します。

- Devices > Platform Settingsの順に移動します。
- 新しいポリシーを作成するか、既存のポリシーの鉛筆アイコンを編集します。



プラットフォーム設定の作成

- Logging Setupを選択し、Enable loggingを選択します。

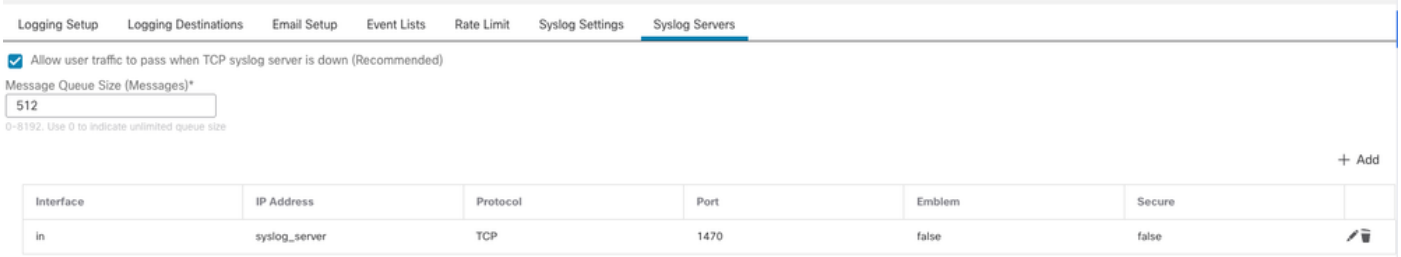


Enable Logging

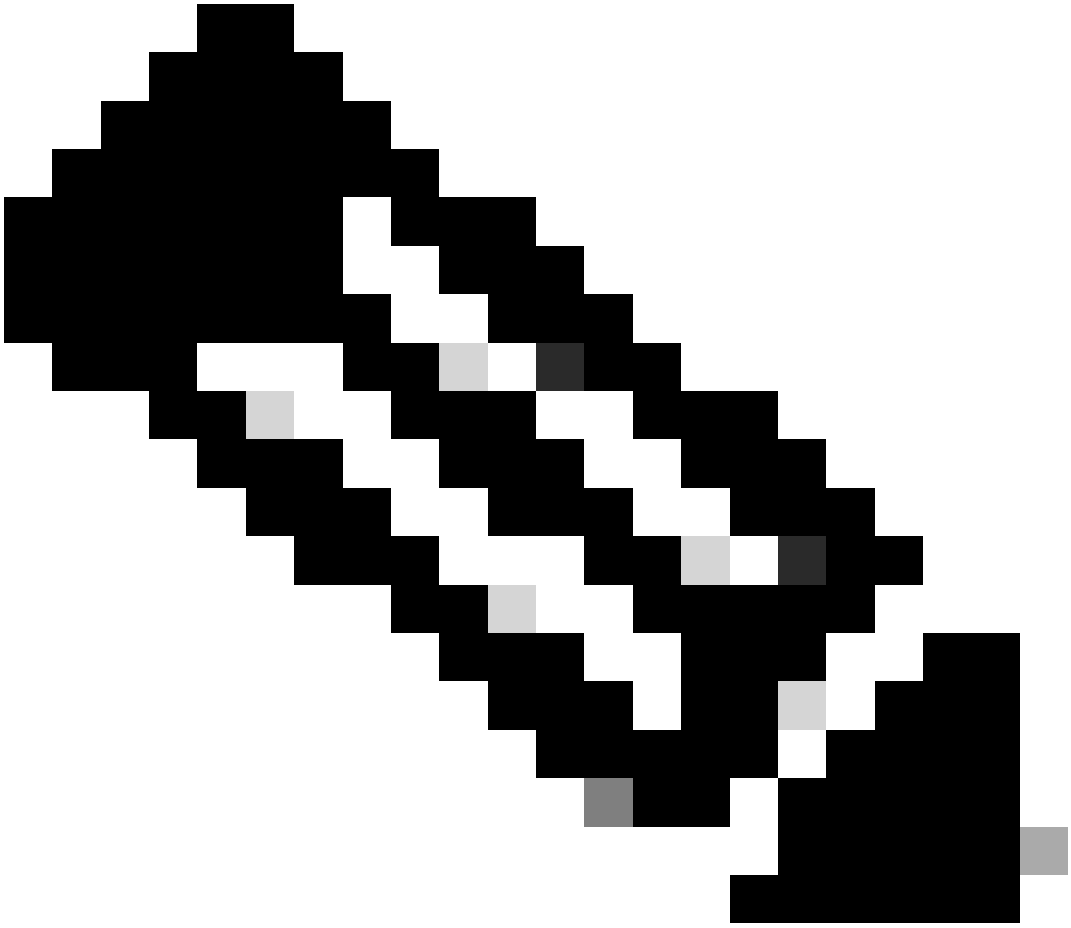
- Logging Destination を選択し、Addをクリックします。
- syslogサーバとしてロギング先を設定します。

syslogサーバとしてのロギング宛先

- Syslog Servers > Addの順に選択します。



VRF対応インターフェイスを使用したsyslogサーバの追加



注：内部インターフェイスは、のセキュリティゾーンの一部です。

- logging hostコマンドで設定されたインターフェイスはVRF対応になりました。
- [Save] をクリックします。

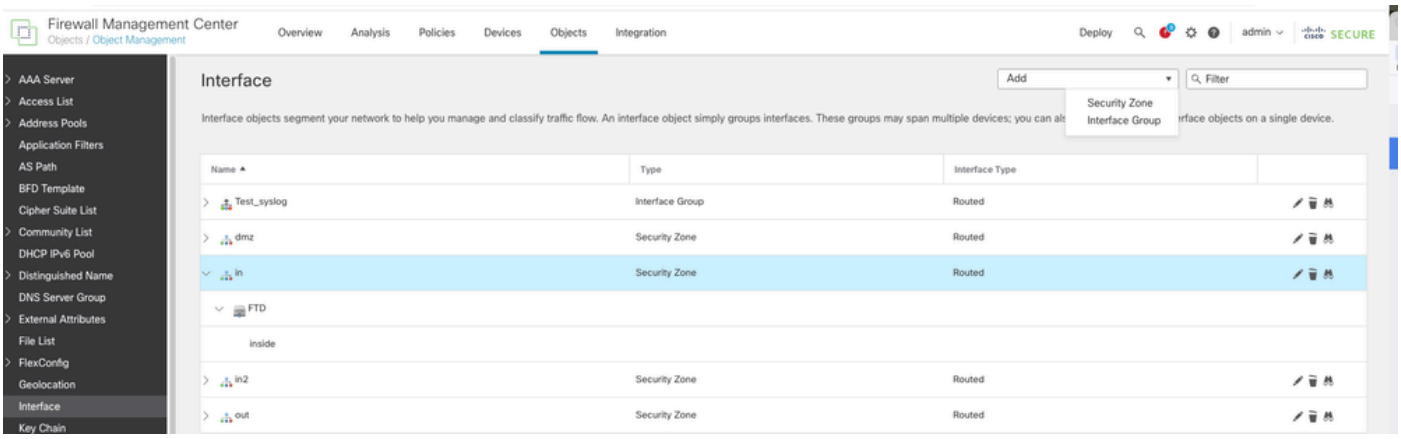
FMCでのFTPサーバ設定の前提条件

- インターフェイスグループオブジェクトを使用します。
- インターフェイスグループオブジェクトは、ユーザとグローバルの両方のVRFを持つことができます。

コンフィギュレーション

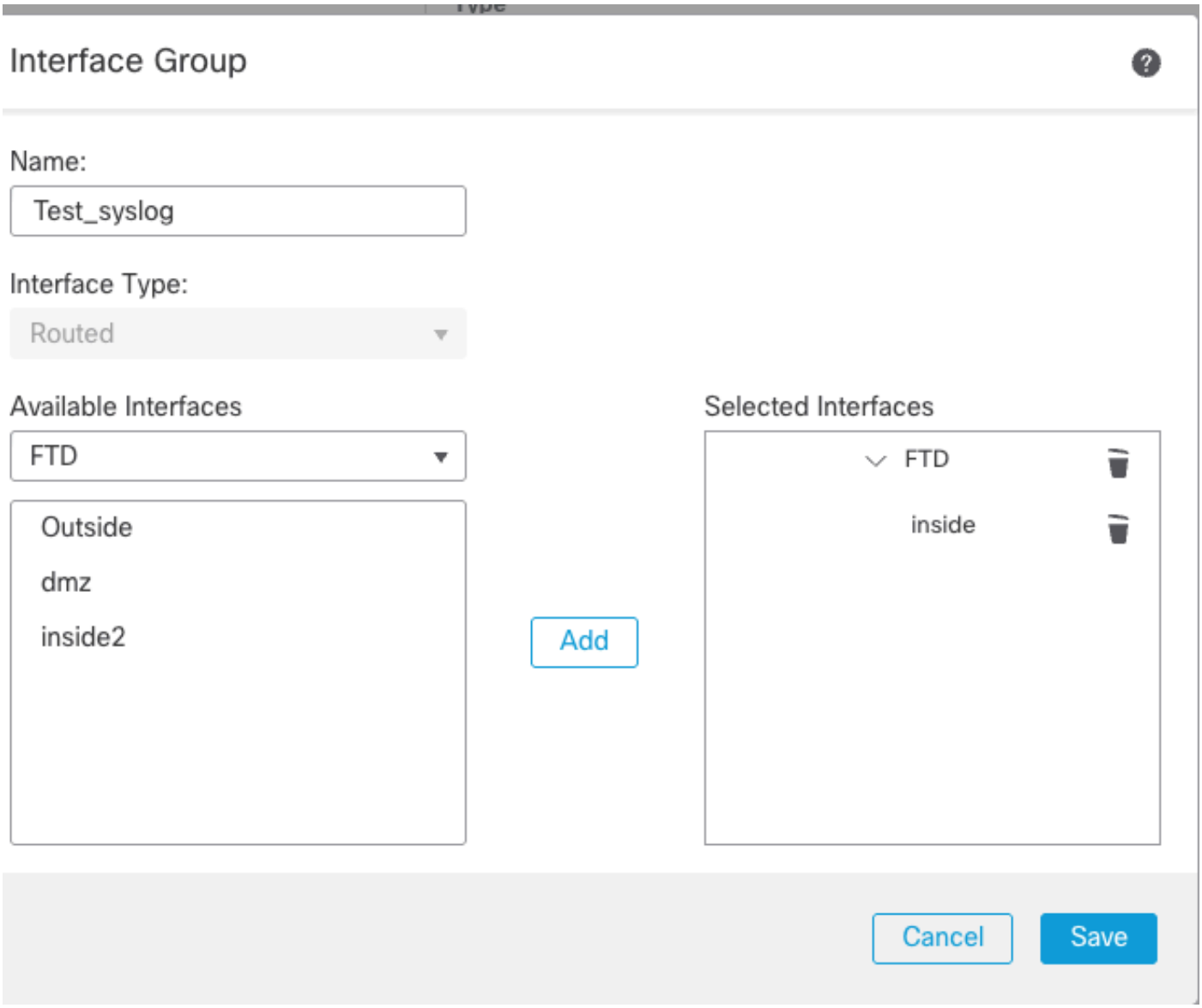
ステップ 1：

- Object > Object Management > Interface > Add > Interface Groupの順に移動します。



インターフェイスグループの追加

- Deviceをドロップダウンから選択し、VRF Interfaceを追加します。



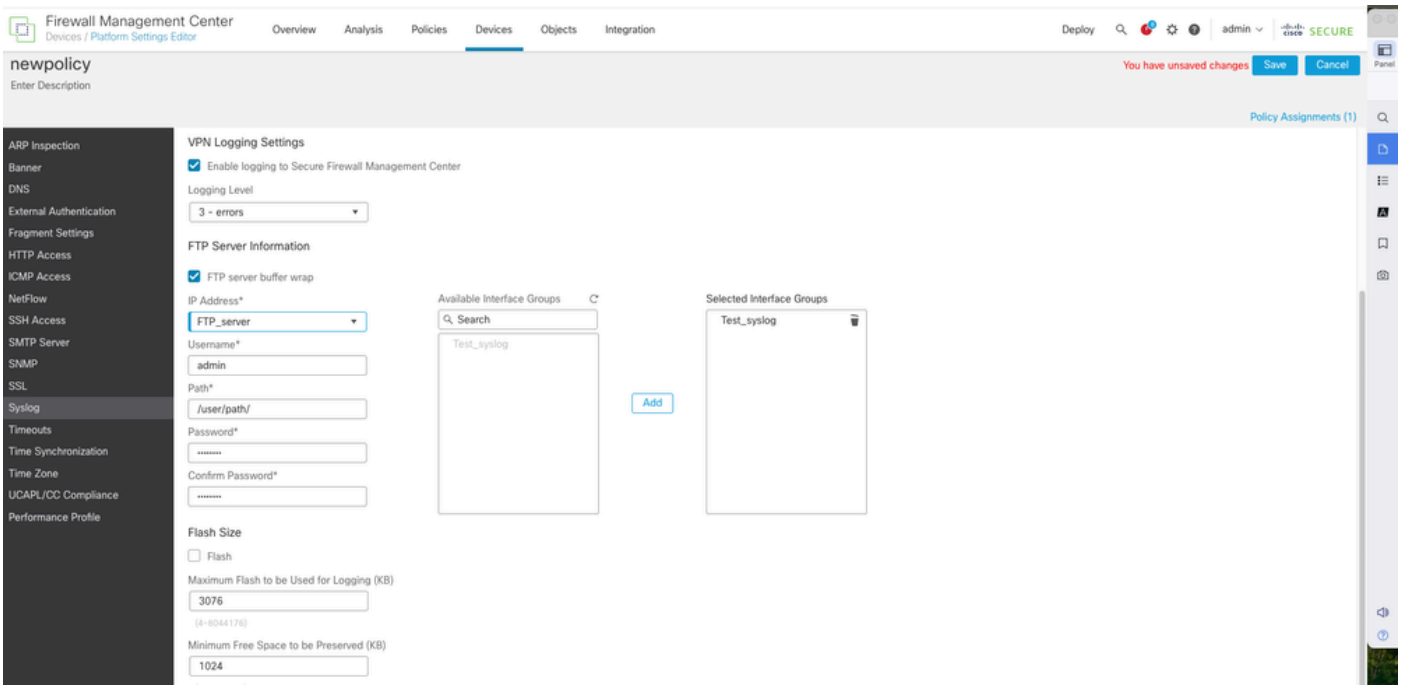
VRF対応インターフェイスの追加

ステップ 2 :

- Devices > Platform Settings > Syslog > Logging Setupの順に選択します。 FTPサーバのバ

ッファラップを有効にする。

- [Save] をクリックします。



VRF対応インターフェイスを使用したFTPサーバの有効化

確認

7.4.1よりも前

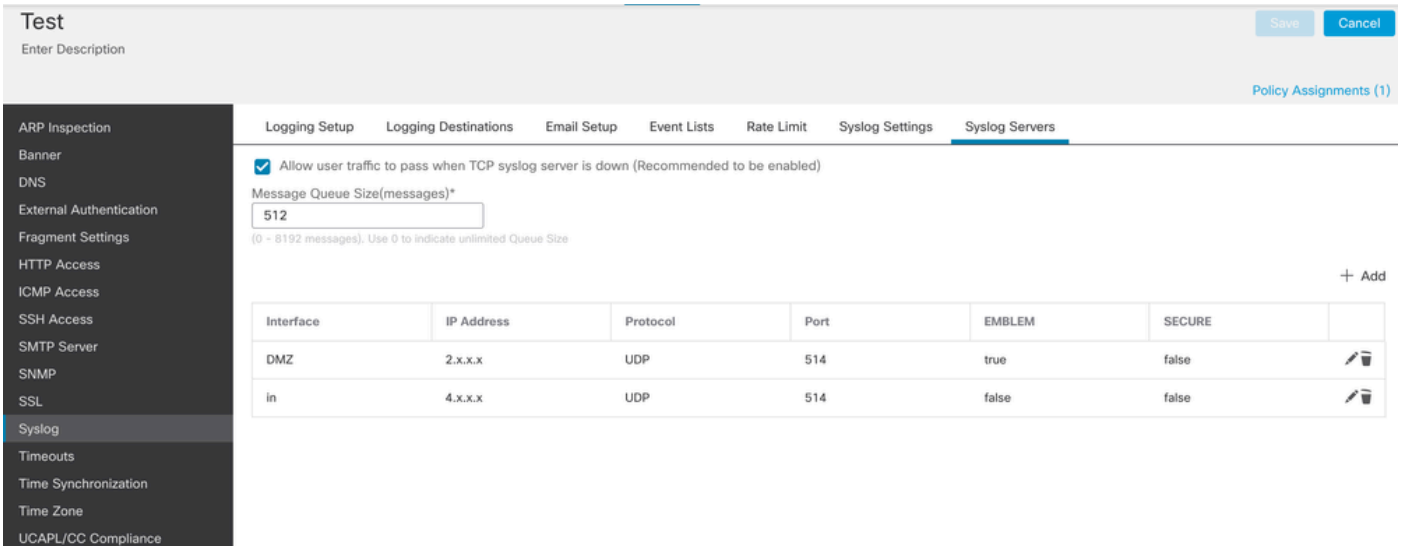
このテストでは、FTDとFMCは7.0.5です。

FTDはVRFで設定され、dmzインターフェイスはVRFに割り当てられています。

dmzインターフェイスは、syslogサーバロギングホストで設定されます。

さらに、内部インターフェイスにはsyslog設定が設定されています。

内部インターフェイスは、グローバルVRFの一部です。

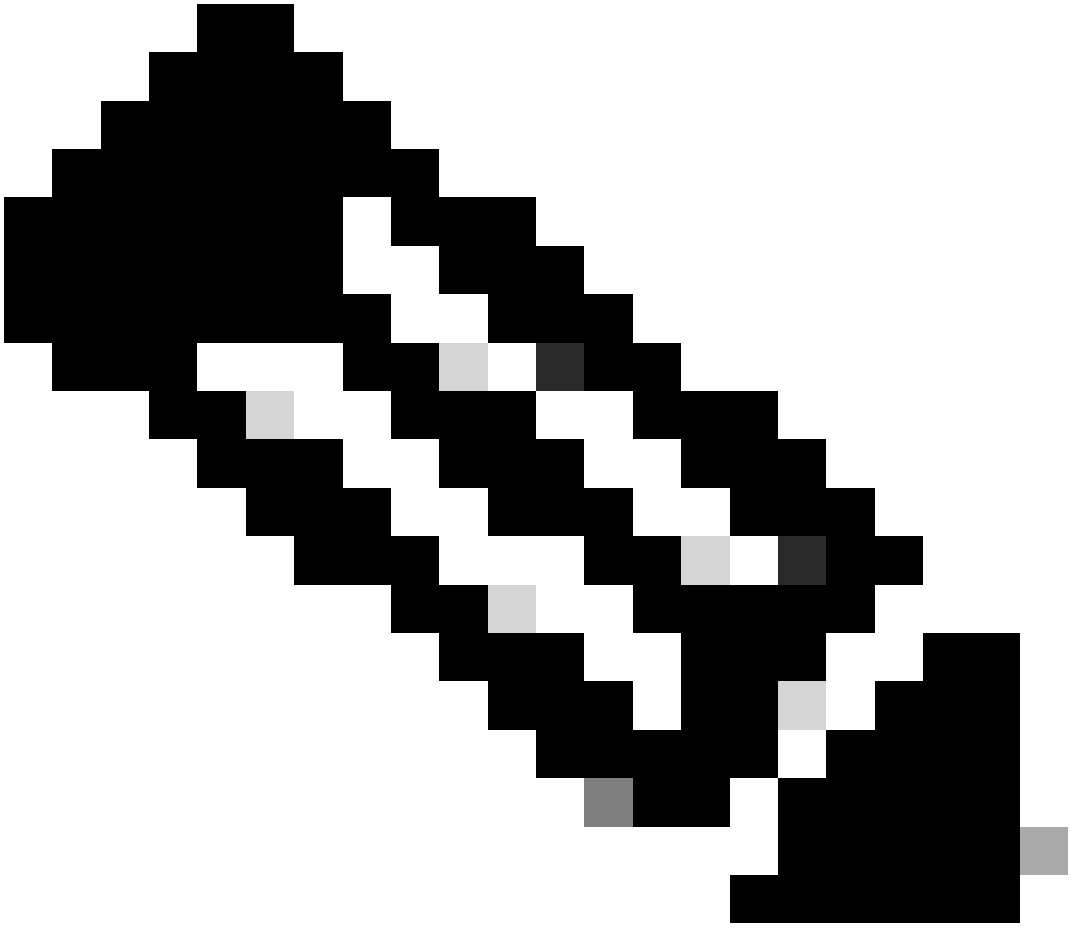


7.0.5 FMCでのsyslogサーバの設定

CLI を使用した確認

```
> 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
```



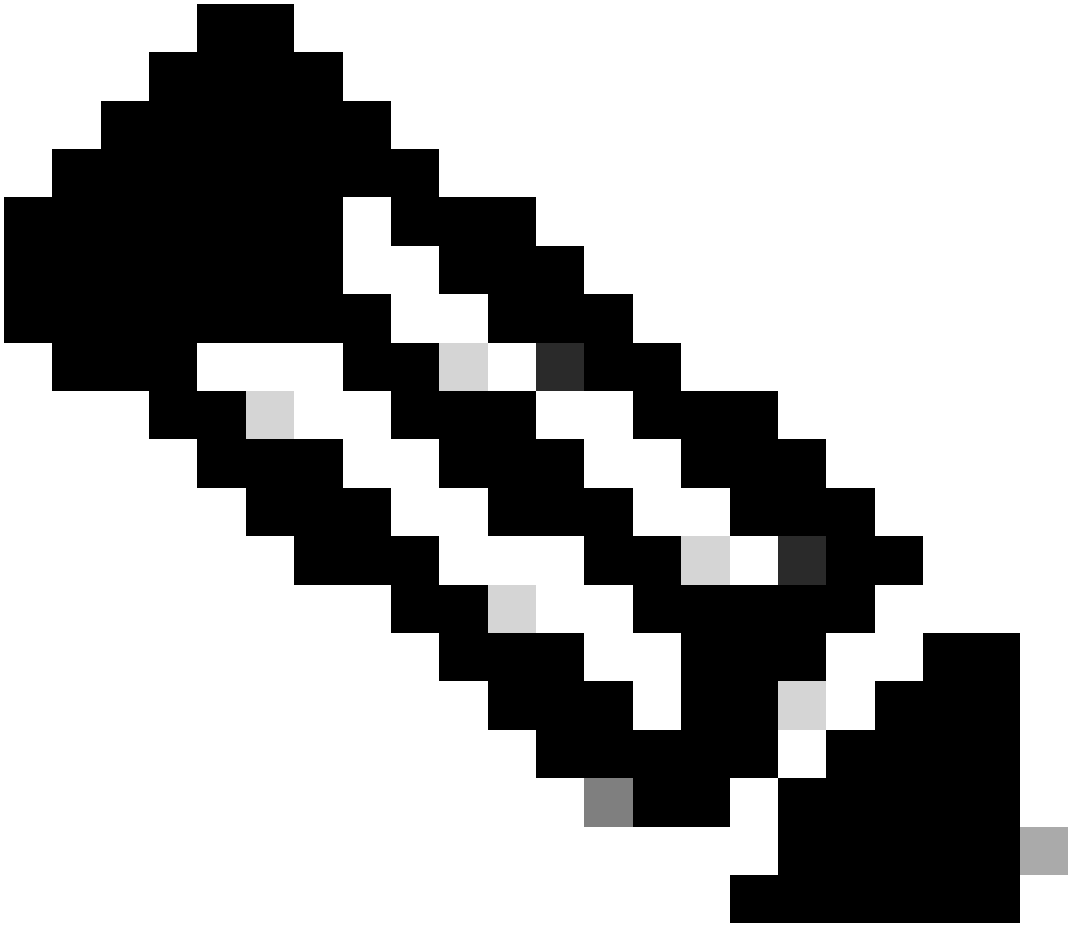
注：宛先2.x.x.xのsyslogサーバは、FTD CLIのロギング設定では使用できません。これはユーザVRFの一部です。
宛先4.x.x.xのsyslogサーバは、FTD CLIのロギング設定で使用できます。これはグローバルVRFの一部です。

7.4.1以降

CLI を使用した確認

```
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:syslogサーバホスト192.x.x.xはVRF対応の内部インターフェイスを使用しています。

FTPサーバの検証

7.4.1よりも前

- FMCでは、FTPサーバの設定に、使用するインターフェイスを選択するオプションはありません。syslogサーバオプションのIPアドレスだけが使用可能です。

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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。