Configurer Syslog compatible VRF sur FTD

Table des matières

Introduction

Ce document décrit les étapes de configuration pour la connexion syslog compatible VRF sur FTD.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Syslog
- Firepower Threat Defense (FTD)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

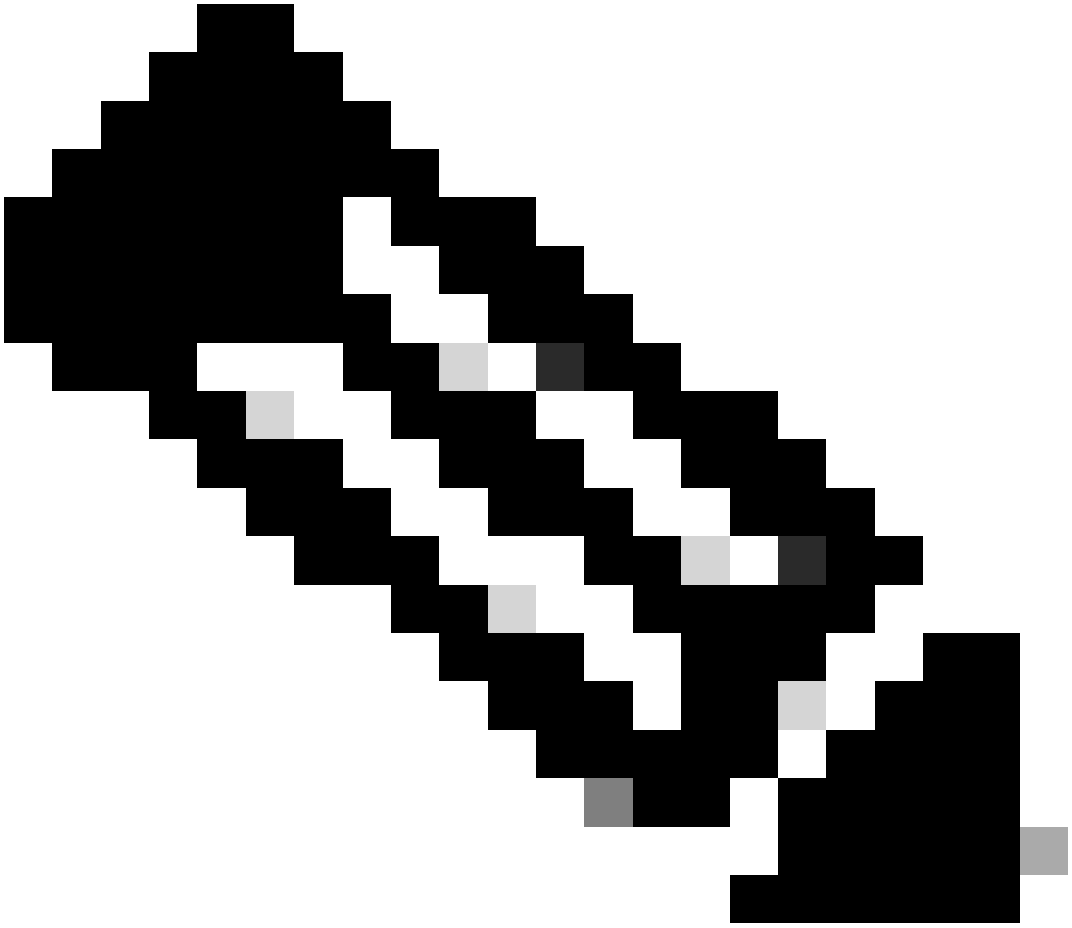
- Centre de gestion du pare-feu sécurisé (FMCv) v7.4.2
- Pare-feu sécurisé FTDv (Virtual Threat Defense) v7.4.2

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Plates-formes logicielles et matérielles minimales

- Application et version minimale : Pare-feu sécurisé 7.4.1
- Plates-formes gérées prises en charge et version : Tous ceux qui prennent en charge FTD 7.4.1
- Gestionnaires :
  1) API REST FMC on-perm + FMC
  2) FMC fourni dans le cloud
  3) FDM + API REST

Prise en charge de Snort3, Multi-Instance/Context et HA/Clustering



Remarque : Fonctionne avec les serveurs Syslog IPv4 et IPv6. IPv6 n'est pas encore pris en charge sur le serveur FTP Syslog.

- Pris en charge avec Multi-instance.
- Pris en charge avec les périphériques haute disponibilité.
- Pris en charge sur les périphériques en cluster.

Configurer

Diagramme du réseau

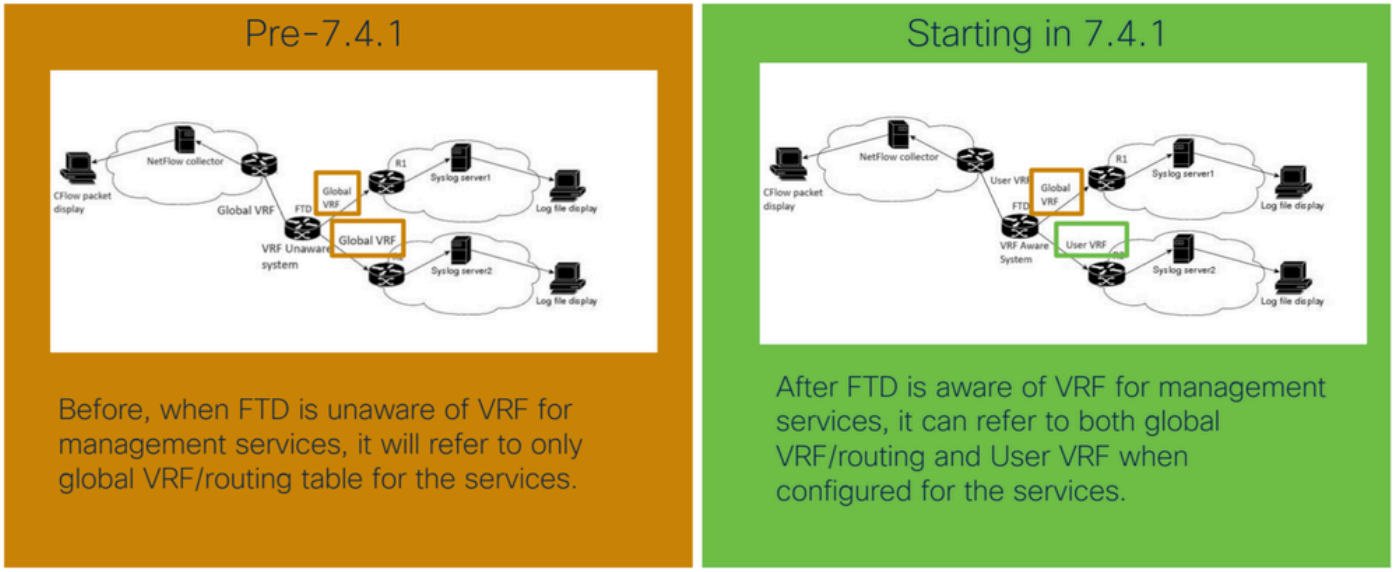


Diagramme de réseau Comparaison entre les versions antérieures et postérieures 7.4.

Configurations

La technologie VRF (Virtual Routing and Forwarding) est utilisée dans les réseaux pour permettre à plusieurs instances d'une table de routage de coexister au sein d'un même routeur, assurant ainsi l'isolation du réseau entre différents réseaux virtuels. Chaque instance VRF est indépendante des autres et le trafic entre elles est séparé. Multi-VRF est une fonctionnalité qui permet aux fournisseurs de services de prendre en charge plusieurs VPN et services, même si leurs adresses IP se chevauchent. Il utilise des interfaces d'entrée pour désigner des routes pour divers services et créer des tables virtuelles de transfert de paquets en attribuant des interfaces de couche 3 à chaque VRF. Les services de gestion (Syslog, NetFlow) utilisent le VRF global par défaut. Les utilisateurs souhaitent utiliser le VRF utilisateur pour les services de gestion ainsi que le VRF global, car toutes les destinations de téléchargement ne sont pas accessibles via le VRF global.

Dans ce document, Global + User VRF = Multi-VRF

Activez Syslog pour VRF utilisateur.

- Syslog peut utiliser le service ftp dans un contexte multi-VRF.

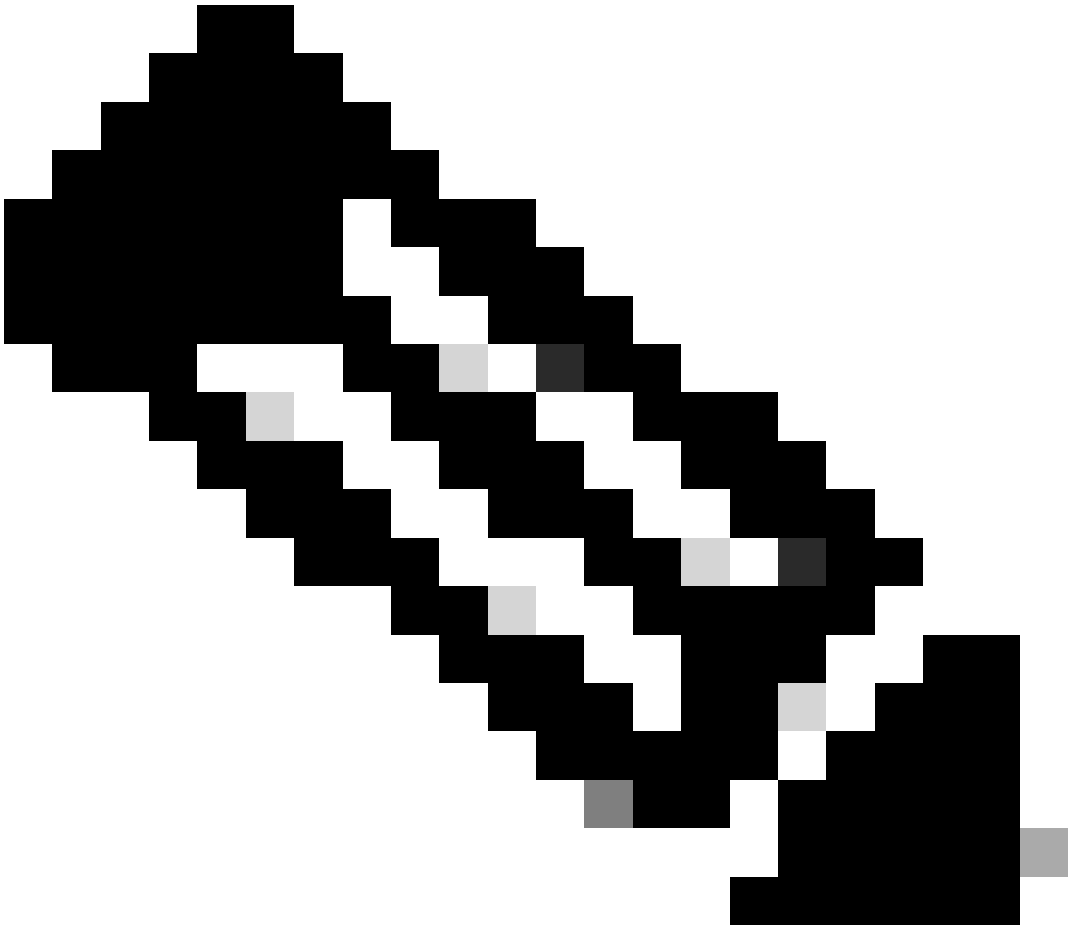
Comment ça fonctionne

Lorsque l'interface est configurée avec le VRF utilisateur, la recherche de route se produit dans le domaine de routage VRF, au lieu du domaine de routage global par défaut.

- Deux types de configuration de serveur sont pris en charge :

1. Envoyez des messages de journalisation aux serveurs Syslog pour surveiller et dépanner le trafic réseau.
2. Envoyer le contenu de la mémoire tampon du journal vers un serveur FTP sous forme de fichier texte

- Syslog envoie les journaux aux serveurs UDP/TCP respectifs au sein de ce VRF.
- Pour les syslogs de post-appel, les journaux sont envoyés au serveur FTP configuré dans ce VRF.

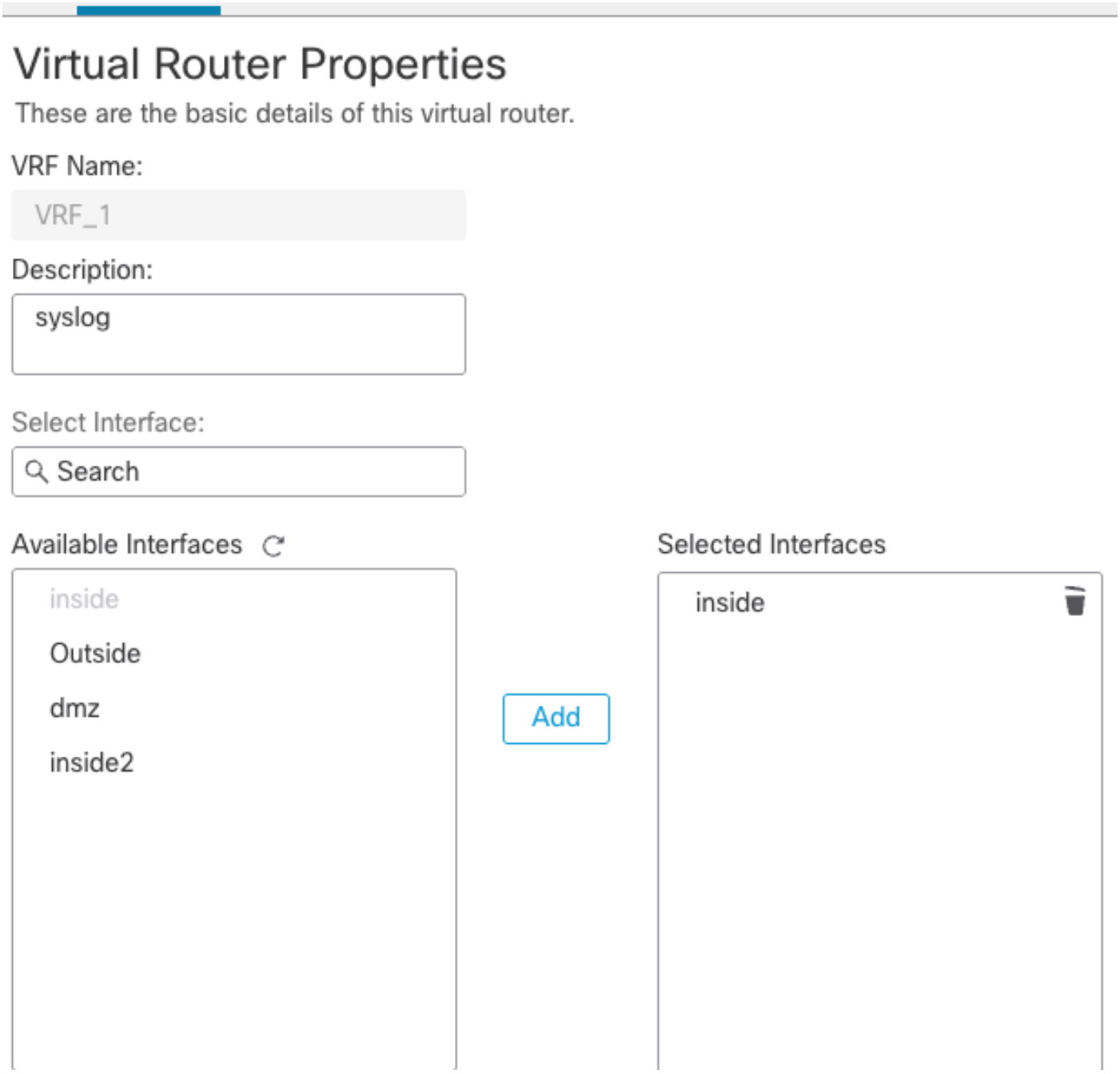


Remarque : Les serveurs Syslog et FTP peuvent faire partie de différents VRF.

Configuration du routeur virtuel

Étape 1 : création d'un VRF

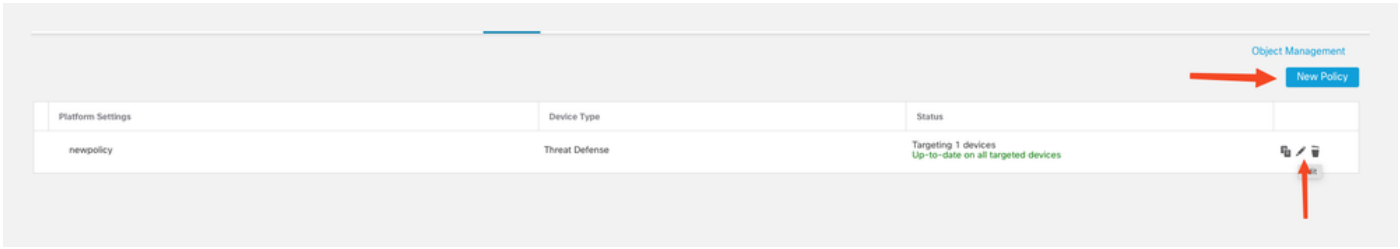
- Connectez-vous à FMC et accédez à Device > Device Management.
- Sélectionnez le Périphérique et cliquez sur l'icône Crayon pour le modifier.
- Accédez à Routing> Manage Virtual Router > Add Virtual Router.
- Entrez le nom dans Nom VRF.
- Sélectionnez l'interface et cliquez sur Add and Save.



Ajout d'une interface à VRF

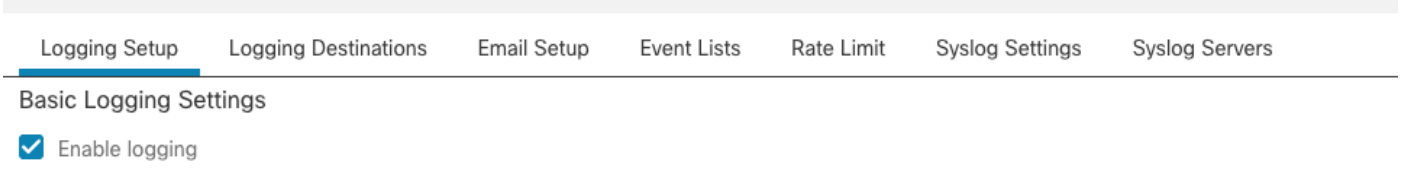
Étape 2 : configuration de la journalisation

- Accédez à Périphériques > Paramètres de la plate-forme.
- Créez une nouvelle stratégie ou modifiez l'icône Crayon sur la stratégie existante.



Création des paramètres de plate-forme

- Sélectionnez Logging Setup et Enable logging.

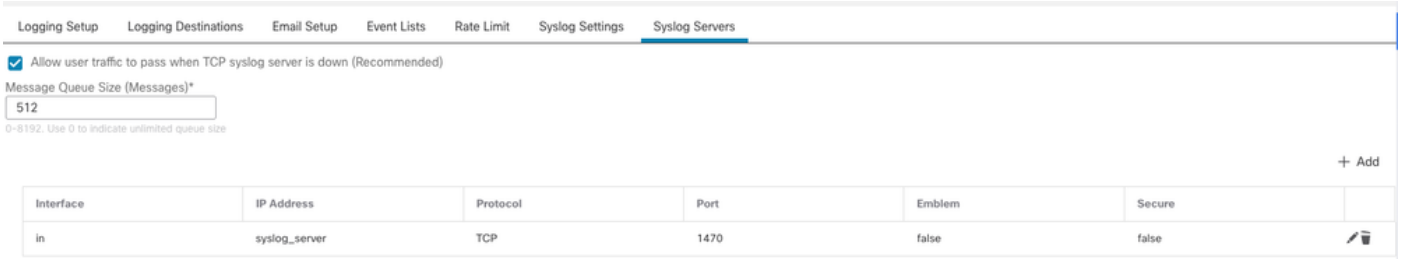


Activer la journalisation

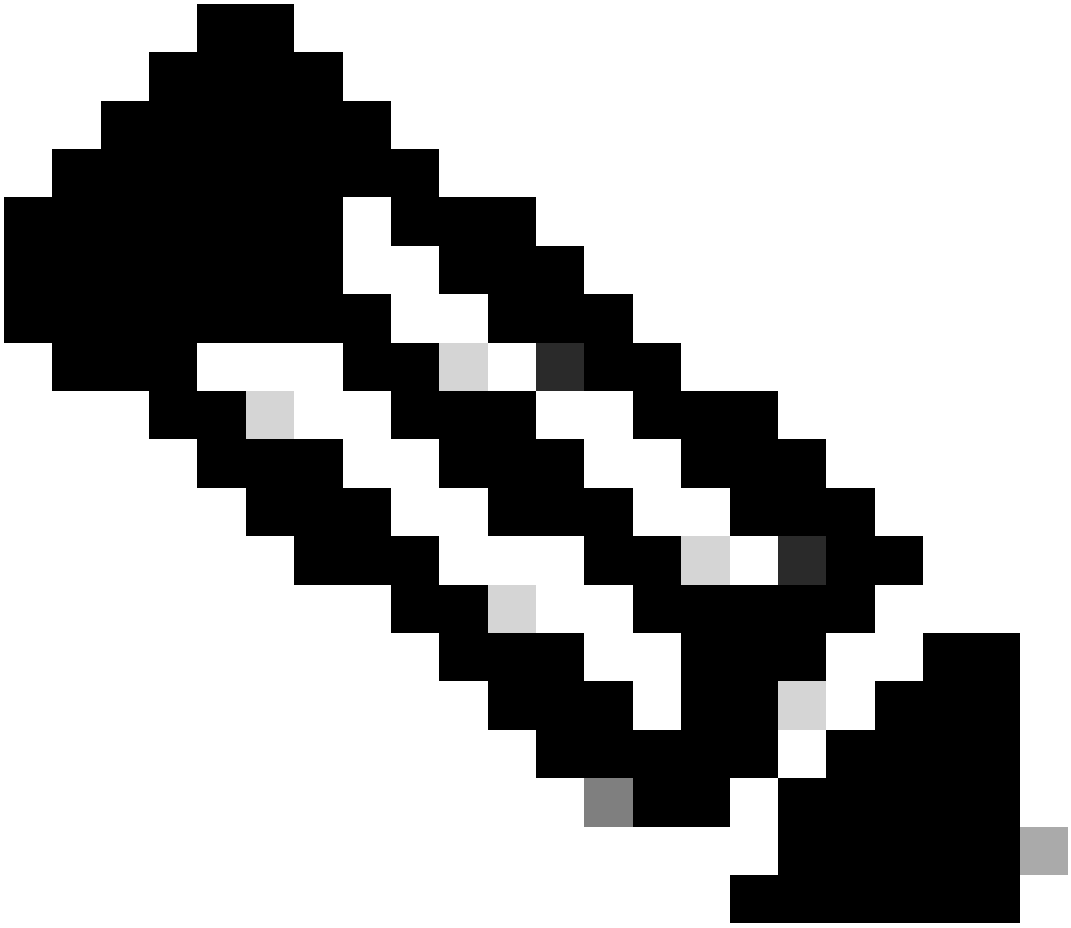
- Sélectionnez Logging Destination et cliquez sur Add.
- Définissez la destination de journalisation comme serveurs Syslog.

Consignation de la destination en tant que serveurs Syslog

- Sélectionnez Serveurs Syslog > Ajouter.



Ajout du serveur Syslog avec interface compatible VRF



Remarque : L'interface interne fait partie de la zone de sécurité dans.

- L'interface configurée dans la commande logging host est désormais compatible VRF.
- Cliquez sur Save.

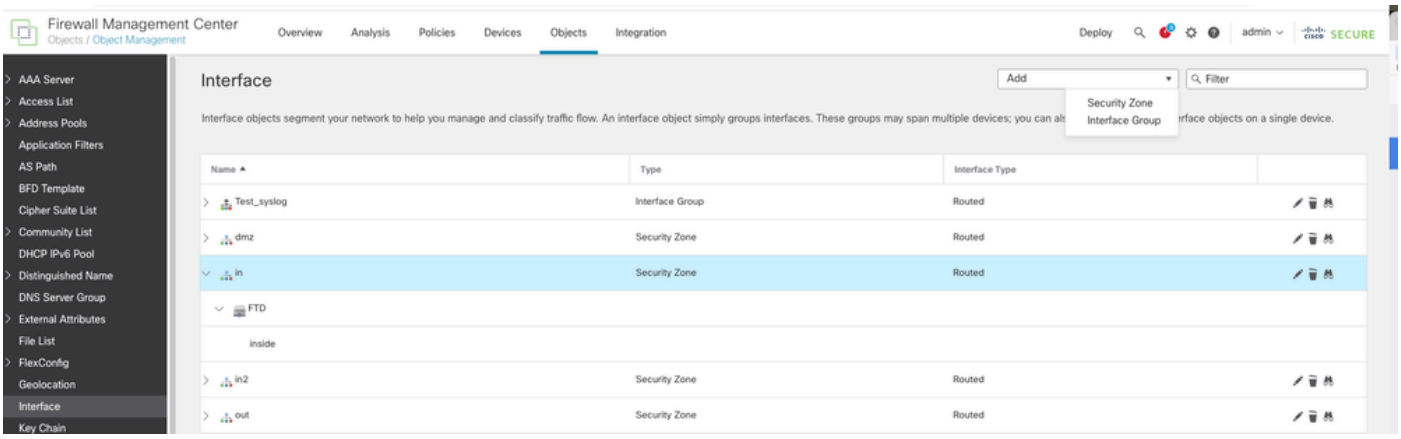
Conditions préalables à la configuration du serveur FTP dans FMC

- Utilisez Interface Group Object.
- L'objet de groupe d'interfaces peut avoir à la fois un VRF utilisateur et global.

Configuration

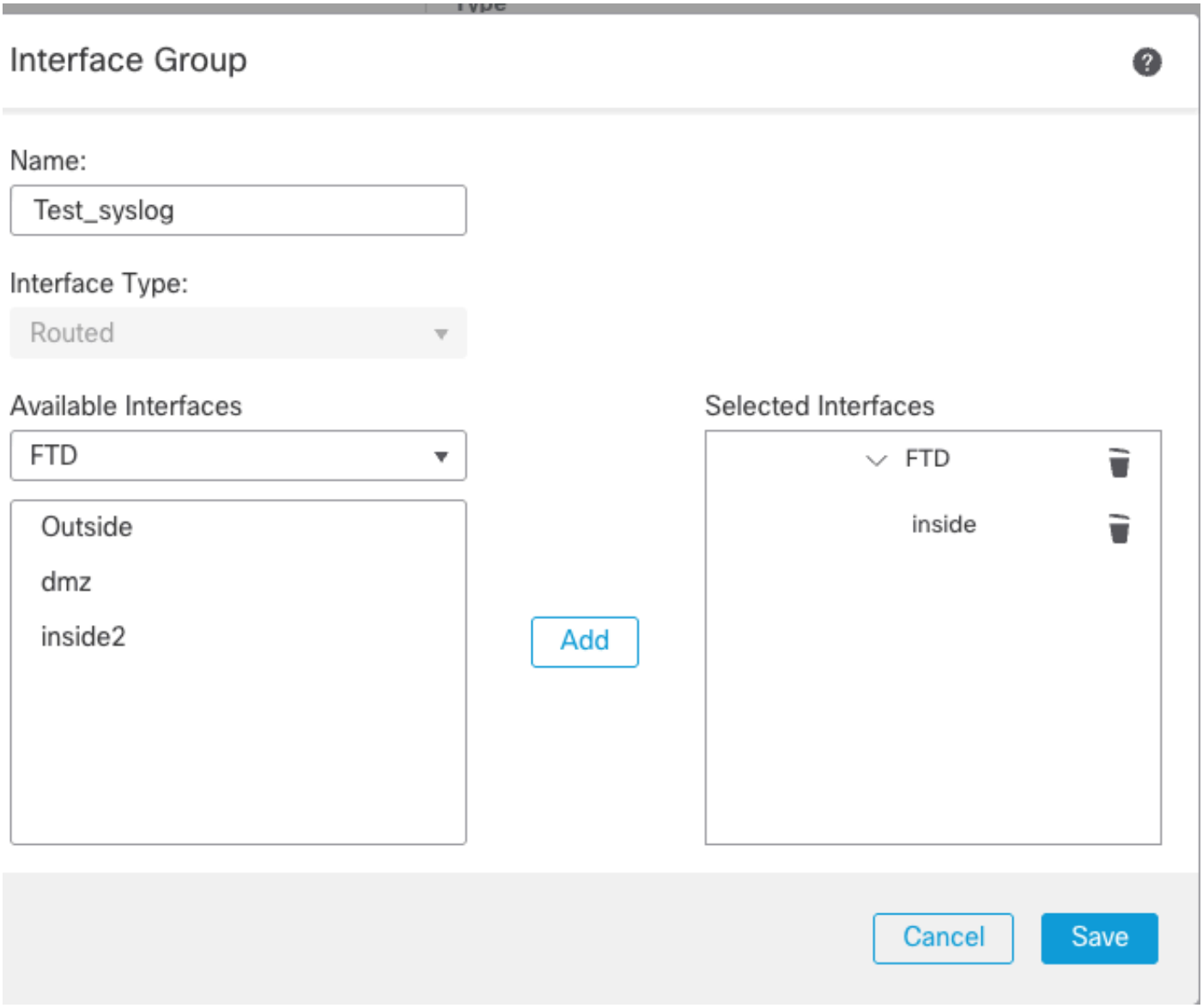
Étape 1.

- Accédez à Objet > Gestion des objets > Interface > Ajouter > Groupe d'interfaces.



Ajout du groupe d'interfaces

- Sélectionnez le périphérique dans la liste déroulante et ajoutez l'interface VRF.



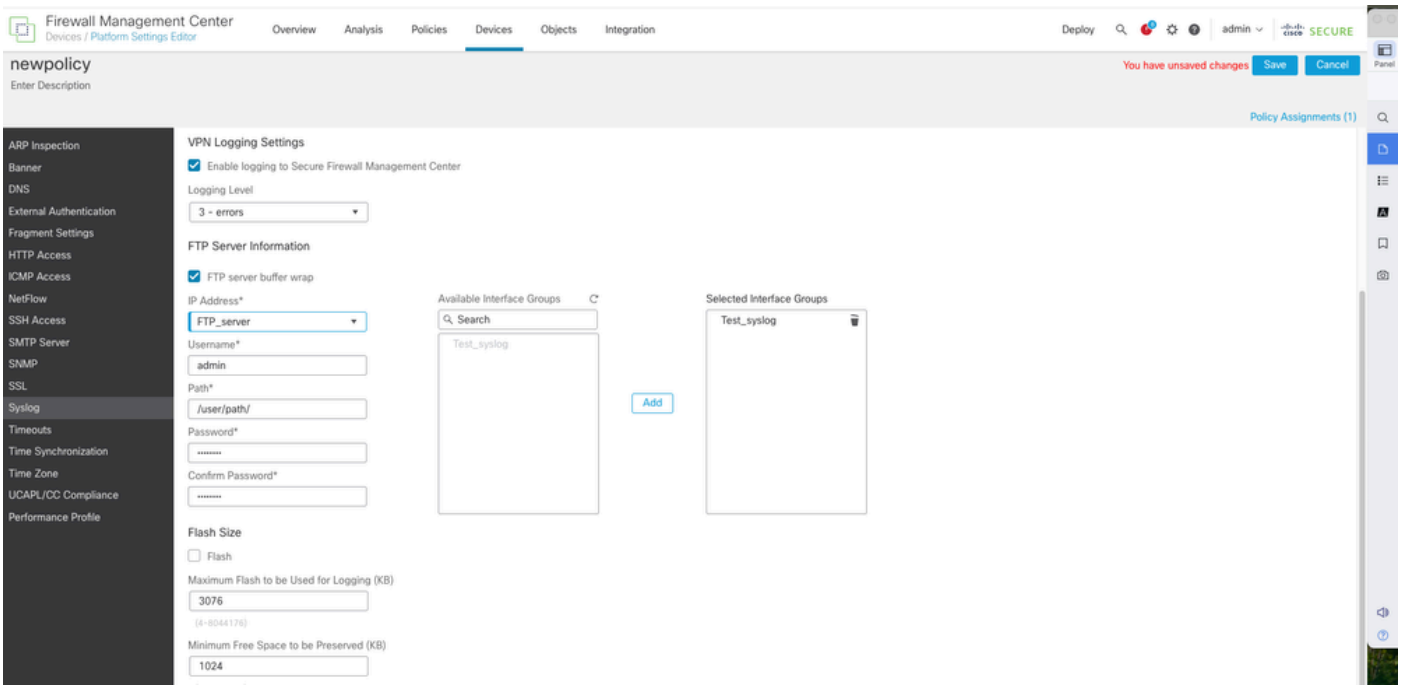
Ajout d'une interface VRF

Étape 2.

- Accédez à Devices > Platform Settings > Syslog > Logging Setup. Activez l'encapsulation de

la mémoire tampon du serveur FTP.

- Cliquez sur Save.



Activer le serveur FTP avec l'interface compatible VRF

Vérifier

Antérieure à 7.4.1

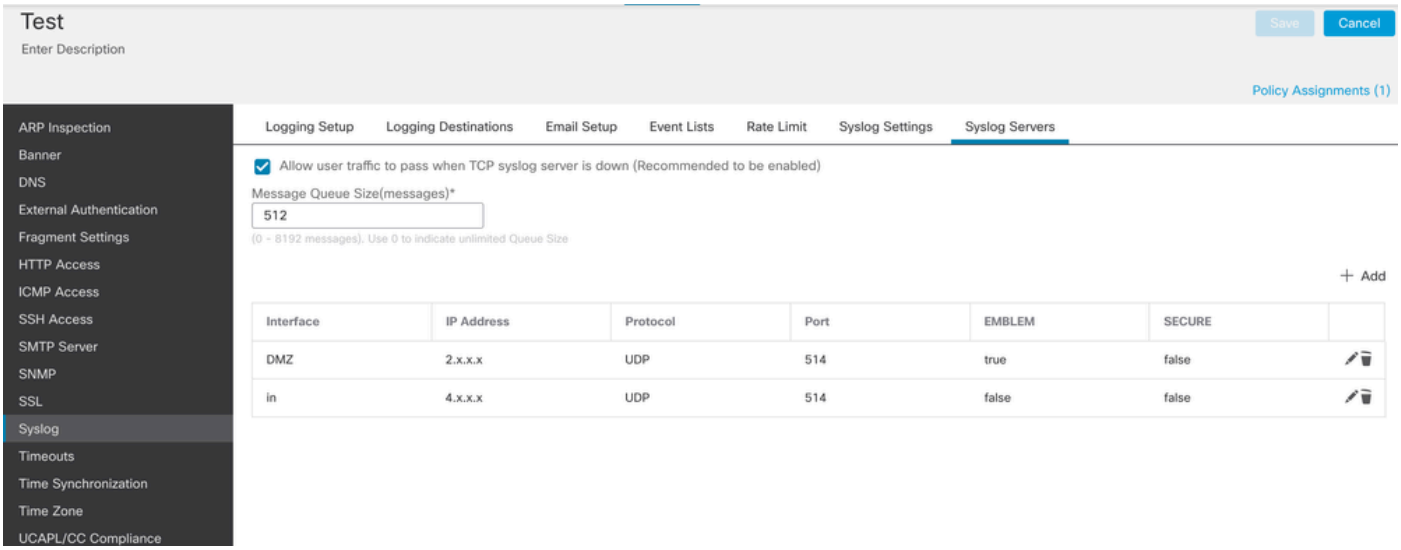
Dans cet essai, le FTD et le FMC sont 7.0.5.

FTD est configuré avec VRF et l'interface dmz a été attribuée à VRF.

L'interface dmz est configurée avec l'hôte de journalisation du serveur syslog.

En outre, l'interface interne est configurée avec le paramètre syslog.

L'interface interne fait partie du VRF global.



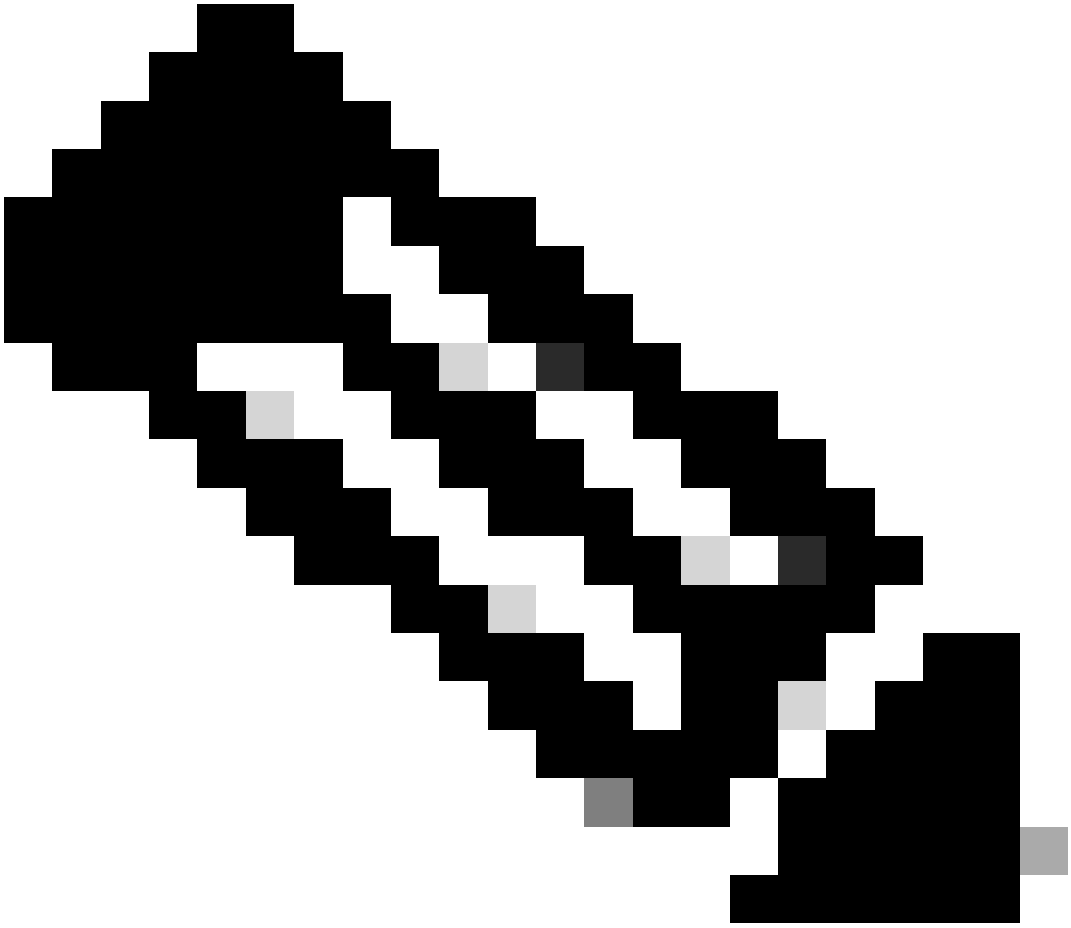
Paramètre du serveur Syslog sur 7.0.5 FMC

Vérification 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
```



Remarque : Le serveur Syslog avec la destination 2.x.x.x n'est pas disponible sur le paramètre de journalisation pour l'interface de ligne de commande FTD. Cela fait partie du VRF utilisateur.
Le serveur Syslog avec la destination 4.x.x.x est disponible sur le paramètre de journalisation pour l'interface de ligne de commande FTD. Cela fait partie du VRF mondial.

Post 7.4.1

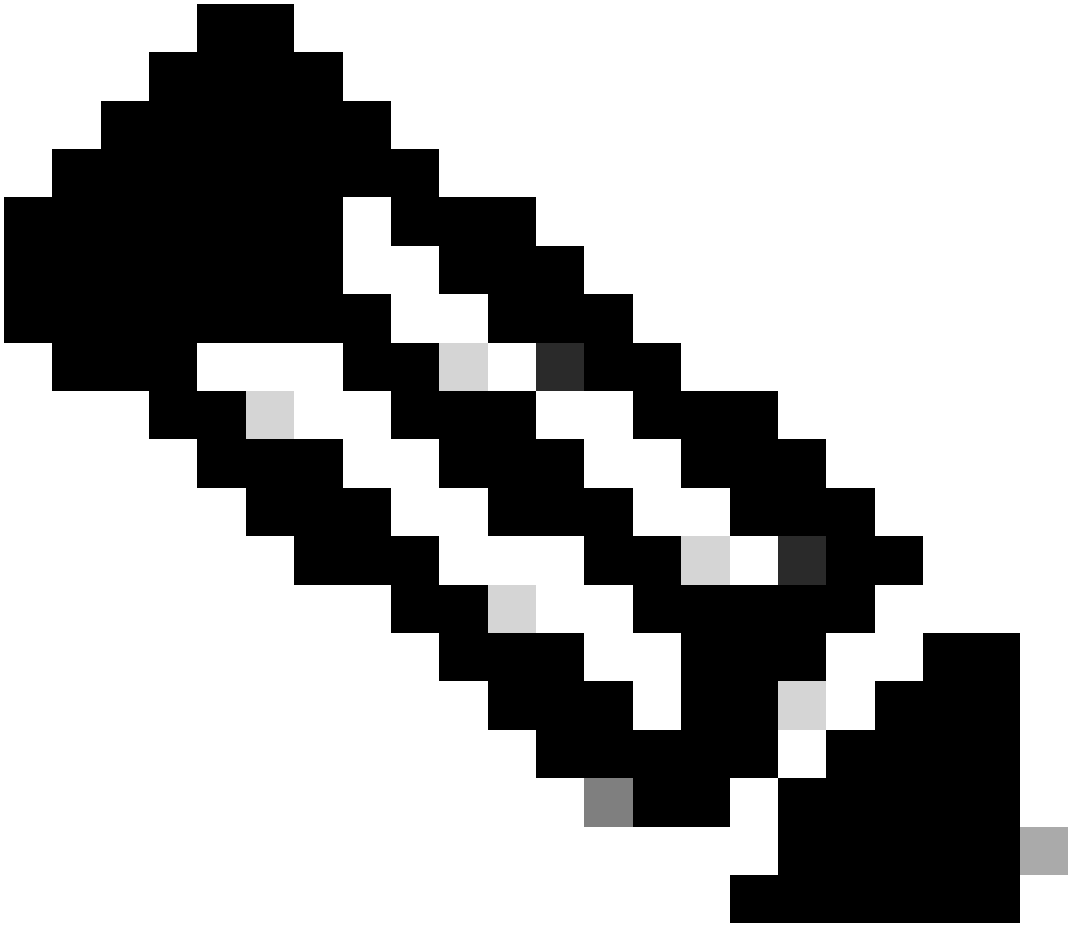
Vérification CLI

```
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
```



Remarque : L'hôte 192.x.x.x du serveur Syslog utilise l'interface interne compatible VRF.

Vérification du serveur FTP

Antérieure à 7.4.1

- Sur FMC, le paramètre du serveur FTP ne permet pas de sélectionner l'interface à utiliser. Seule l'adresse IP de l'option de serveur Syslog est disponible.

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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.