Konfigurieren von VRF-orientiertem Syslog auf FTD

Inhalt

Einleitung

In diesem Dokument werden die Konfigurationsschritte für ein VRF-fähiges Syslog auf FTD beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Syslog
- Firepower Threat Defense (FTD)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-

Versionen:

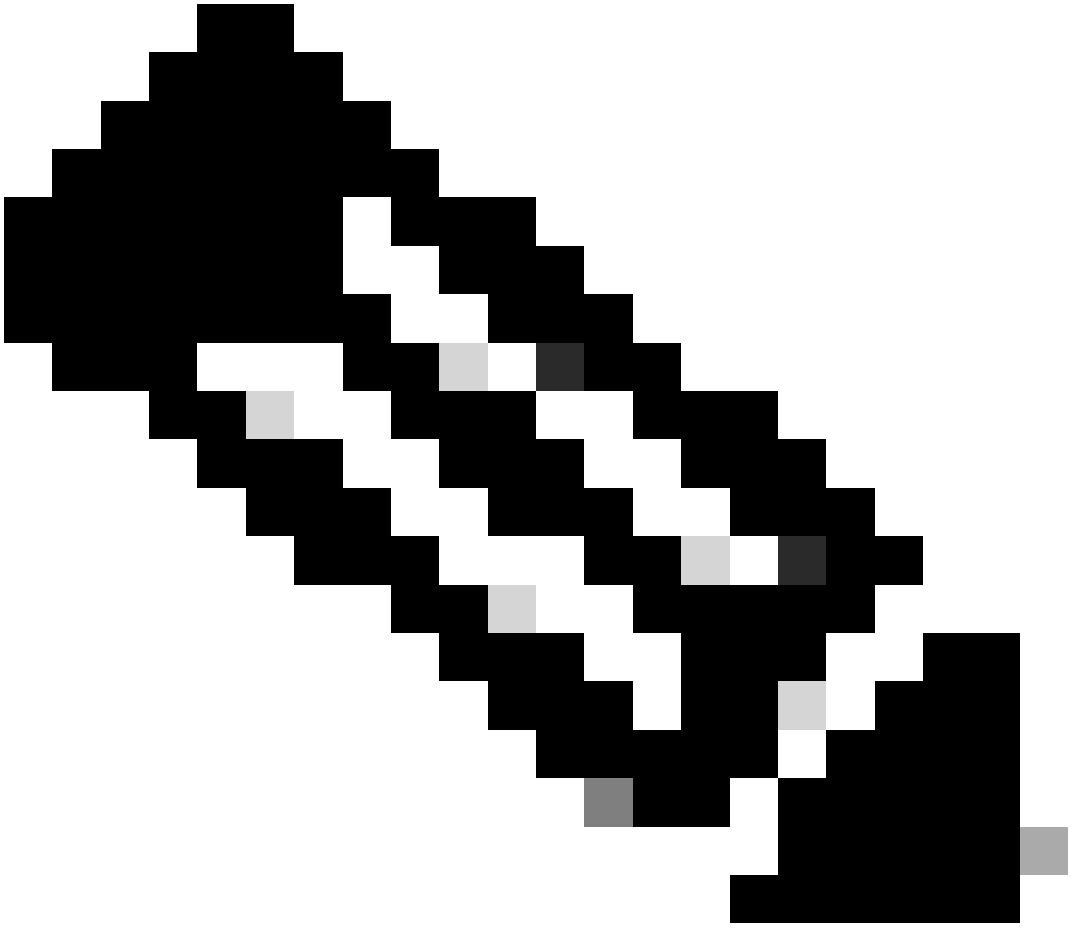
- Secure Firewall Management Center (FMCv) v7.4.2
- Secure Firewall Threat Defense Virtual (FTDv) v7.4.2

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Software- und Hardware-Mindestanforderungen

- Anwendung und Mindestversion: Sichere Firewall 7.4.1
- Unterstützte verwaltete Plattformen und Versionen: Alle unterstützen FTD 7.4.1
- Manager:
  1) FMC permanent + FMC REST API
  2) über die Cloud bereitgestelltes FMC
  3) FDM + REST API

Unterstützung von Snort3, Multi-Instance/Context und HA/Clustering

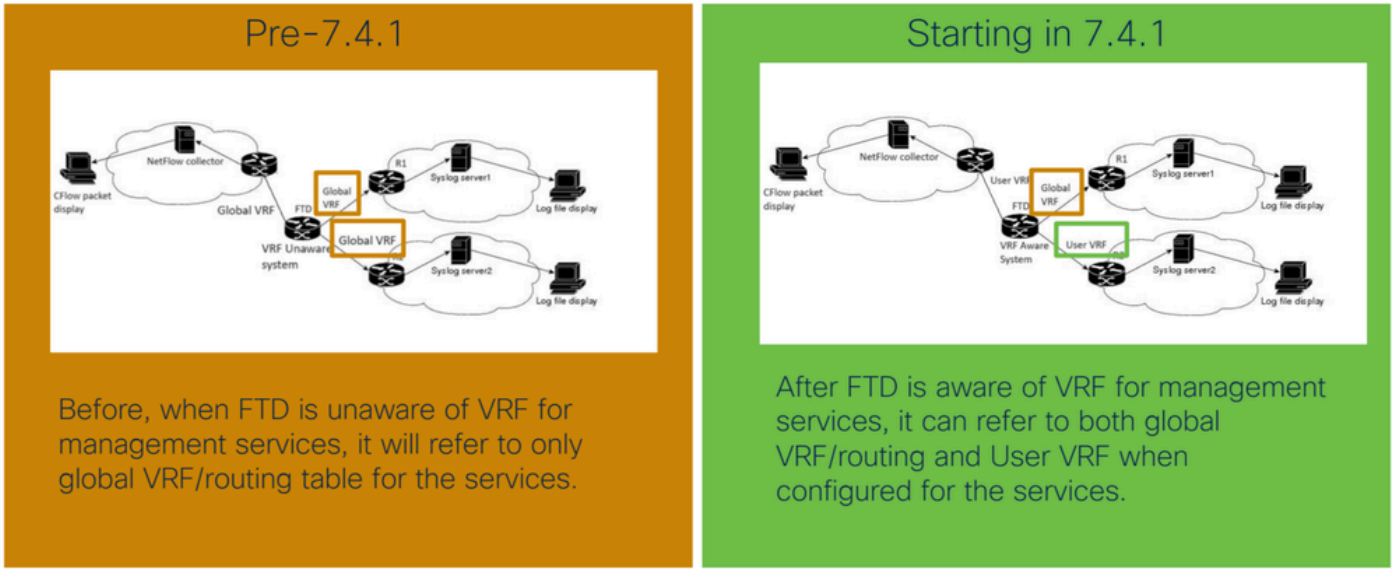


Anmerkung: Kompatibel mit IPv4- und IPv6-Syslog-Servern. IPv6 wird auf dem Syslog-FTP-Server noch nicht unterstützt.

- Unterstützt durch Multi-Instance.
- Unterstützt durch HA-Geräte
- Wird auf geclusterten Geräten unterstützt.

Konfigurieren

Netzwerkdiagramm



Vergleich von Netzwerkdiagrammen zwischen Pre und Post 7.4.

Konfigurationen

Virtual Routing and Forwarding (VRF) ist eine Technologie, die in Netzwerken eingesetzt wird, um das Nebeneinanderbestehen mehrerer Instanzen einer Routing-Tabelle innerhalb eines Routers zu ermöglichen und eine Netzwerkisolierung zwischen verschiedenen virtuellen Netzwerken zu ermöglichen. Jede VRF-Instanz ist unabhängig von anderen Instanzen. Der Datenverkehr zwischen den Instanzen wird getrennt gehalten. Multi-VRF ist eine Funktion, mit der Service Provider mehrere VPNs und Services unterstützen können, auch wenn sich ihre IP-Adressen überschneiden. Mithilfe von Eingangsschnittstellen werden Routen für verschiedene Dienste festgelegt und virtuelle Tabellen für die Paketweiterleitung erstellt, indem jeder VRF-Instanz Layer-3-Schnittstellen zugewiesen werden. Management-Services (Syslog, NetFlow) verwenden standardmäßig globales VRF. Benutzer möchten die Benutzer-VRF für Management-Services sowie die globale VRF-Instanz verwenden, da nicht alle Upload-Ziele über die globale VRF-Instanz erreichbar sind.

In diesem Dokument sind Global + Benutzer-VRF = Multi-VRF

Aktivieren Sie Syslog für Benutzer-VRF.

- Syslog kann den FTP-Service in einem Multi-VRF-Kontext verwenden.

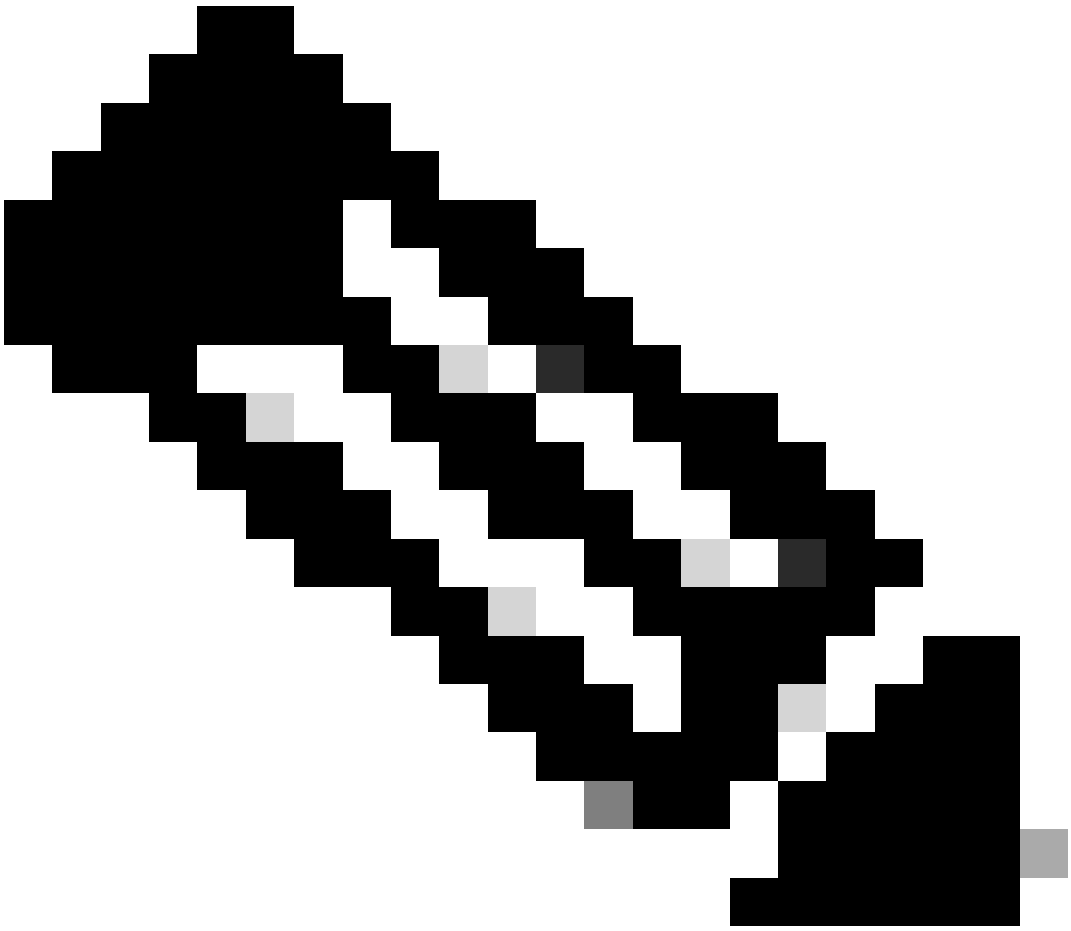
So funktioniert es

Wenn die Schnittstelle mit Benutzer-VRF konfiguriert ist, wird die Route in der VRF-Routing-Domäne statt in der globalen Standard-Routing-Domäne gesucht.

- Es werden zwei Arten von Serverkonfigurationen unterstützt:

1. Senden Sie Protokollmeldungen an Syslog-Server, um den Netzwerkverkehr zu überwachen und Fehler zu beheben.
2. Senden des Protokollpufferinhalts als Textdatei an einen FTP-Server

- Syslog sendet die Protokolle an die entsprechenden UDP-/TCP-Server innerhalb dieser VRF-Instanz.
- Bei Buffer-Wrap-Syslogs werden die Protokolle an den konfigurierten FTP-Server innerhalb dieser VRF-Instanz gesendet.

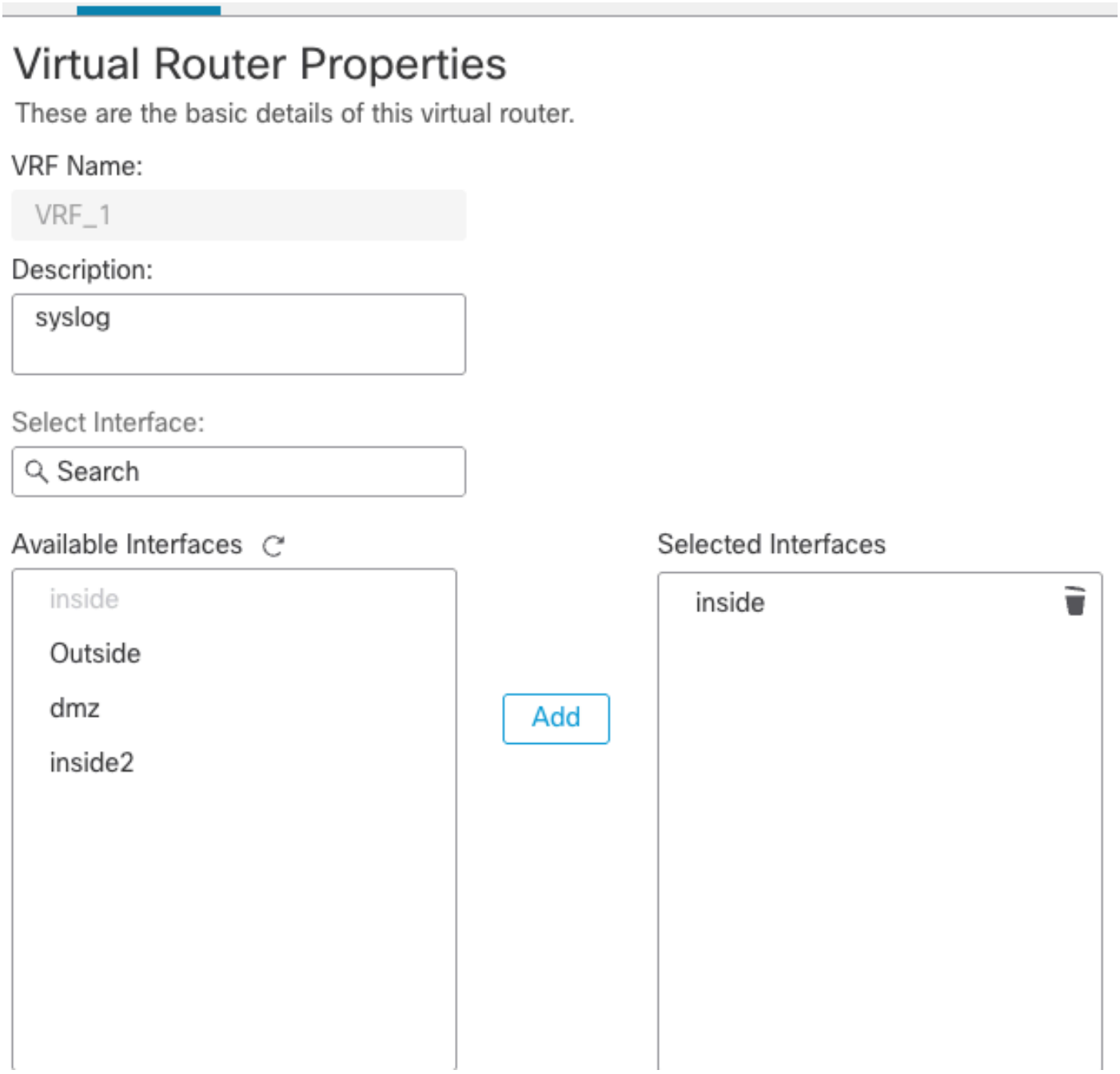


Anmerkung: Syslog- und FTP-Server können Teil verschiedener VRFs sein.

Virtuellen Router konfigurieren

Schritt 1: Erstellen eines VRF

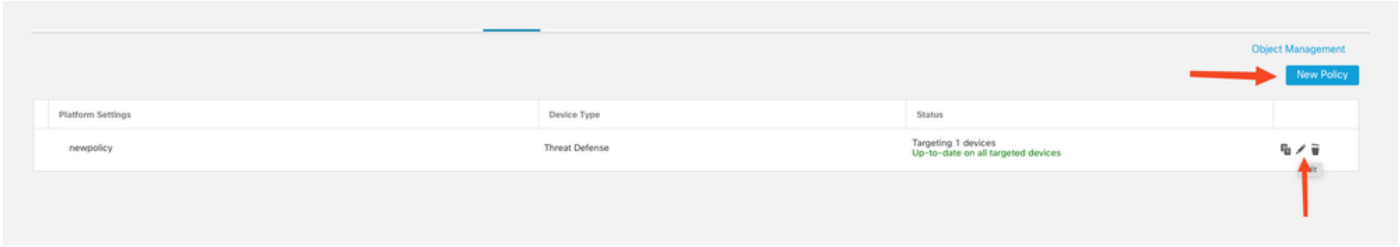
- Melden Sie sich bei FMC an, und navigieren Sie zu Device > Device Management (Gerät > Geräteverwaltung).
- Wählen Sie das Gerät aus, und klicken Sie auf das Bleistiftsymbol, um es zu bearbeiten.
- Navigieren Sie zu Routing > Virtuellen Router verwalten > Virtuellen Router hinzufügen.
- Geben Sie den Namen unter VRF-Name ein.
- Wählen Sie die Schnittstelle aus, und klicken Sie auf Hinzufügen und Speichern.



Hinzufügen einer Schnittstelle zu VRF

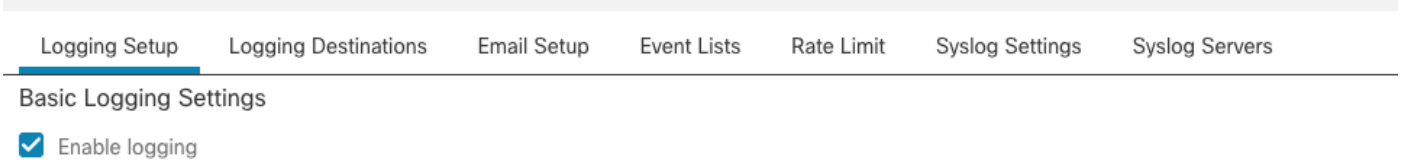
Schritt 2: Konfigurieren Sie die Protokollierungseinstellungen.

- Navigieren Sie zu Geräte > Plattformeinstellungen.
- Erstellen Sie eine neue Richtlinie, oder bearbeiten Sie das Bleistiftsymbol für die vorhandene Richtlinie.



Erstellen der Plattformeinstellungen

- Wählen Sie Logging Setup und Enable logging aus.

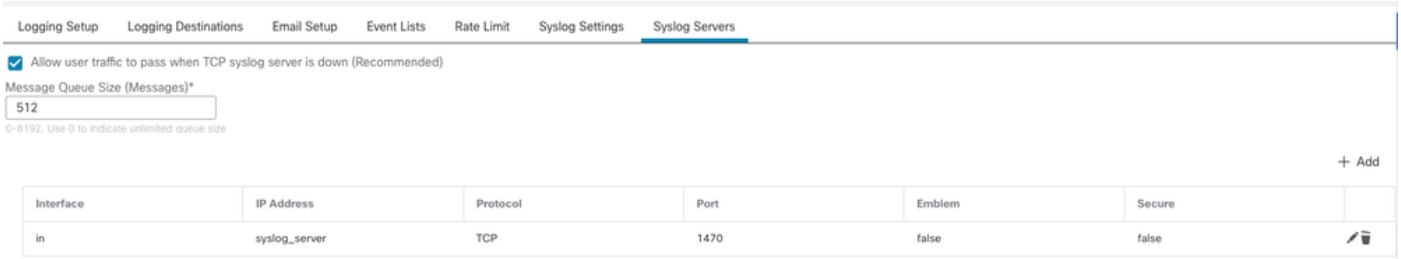


Protokollierung aktivieren

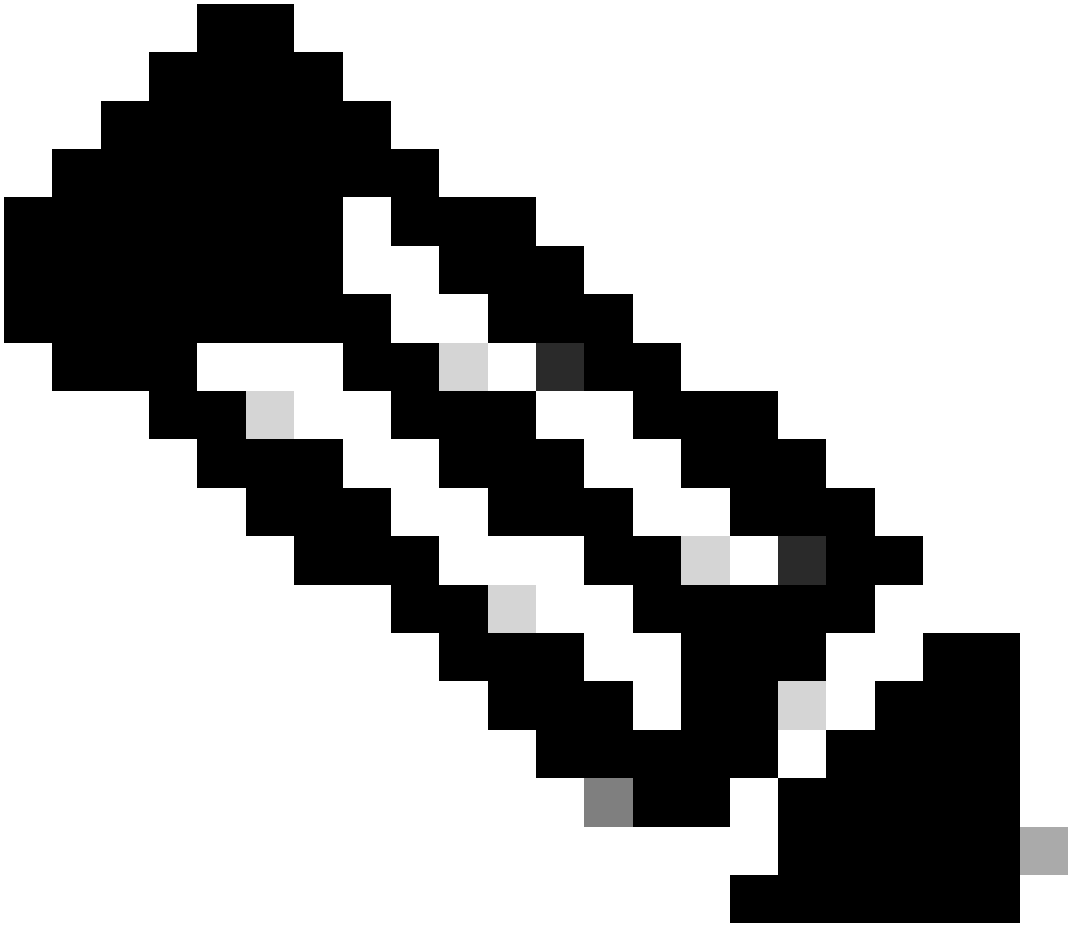
- Wählen Sie Protokollziel aus, und klicken Sie auf Hinzufügen.
- Legen Sie das Protokollziel als Syslog-Server fest.

Ziel als Syslog-Server protokollieren

- Wählen Sie Syslog-Server > Hinzufügen aus.



Hinzufügen eines Syslog-Servers mit VRF-fähiger Schnittstelle



Anmerkung: Die interne Schnittstelle ist Teil der Sicherheitszone in.

- Die im Befehl logging host konfigurierte Schnittstelle ist jetzt VRF-kompatibel.
- Klicken Sie auf Speichern.

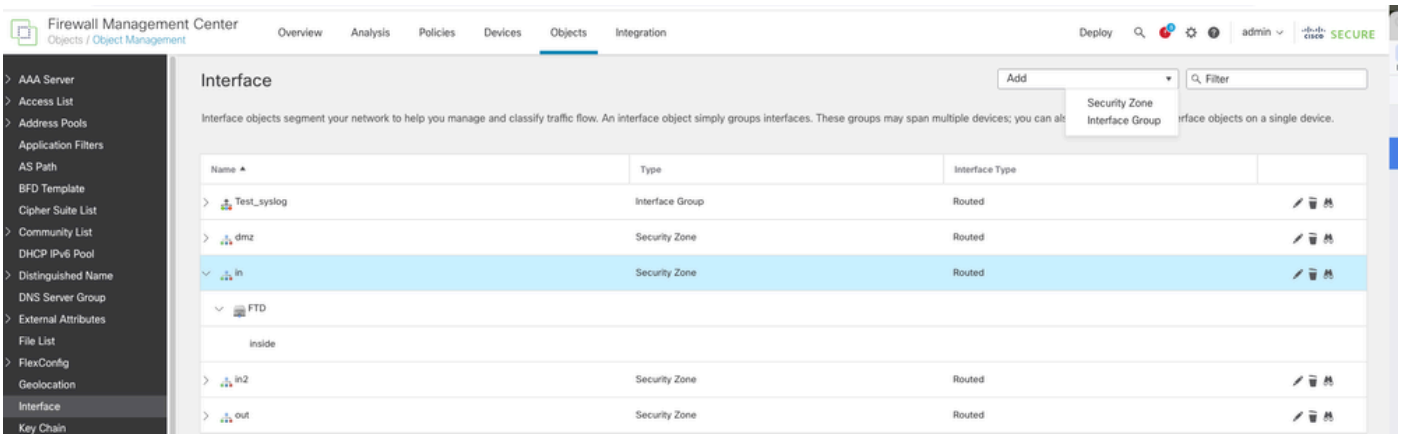
Voraussetzungen für FTP-Server-Konfiguration in FMC

- Verwenden Sie Interface Group Object (Schnittstellengruppenobjekt).
- Das Schnittstellengruppenobjekt kann sowohl eine Benutzer- als auch eine globale VRF-Instanz aufweisen.

Konfiguration

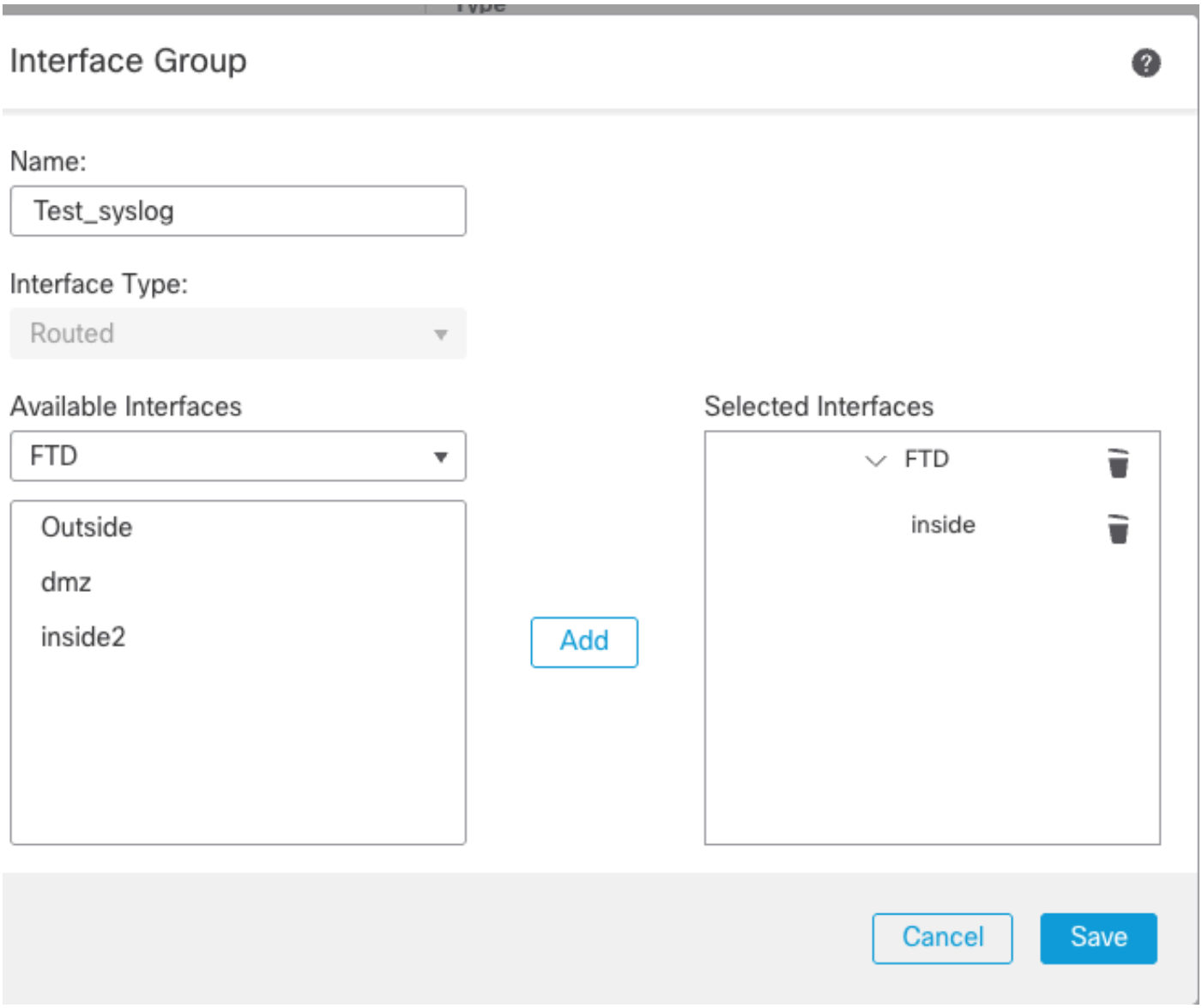
Schritt 1:

- Navigieren Sie zu Object > Object Management > Interface > Add > Interface Group.



Hinzufügen einer Schnittstellengruppe

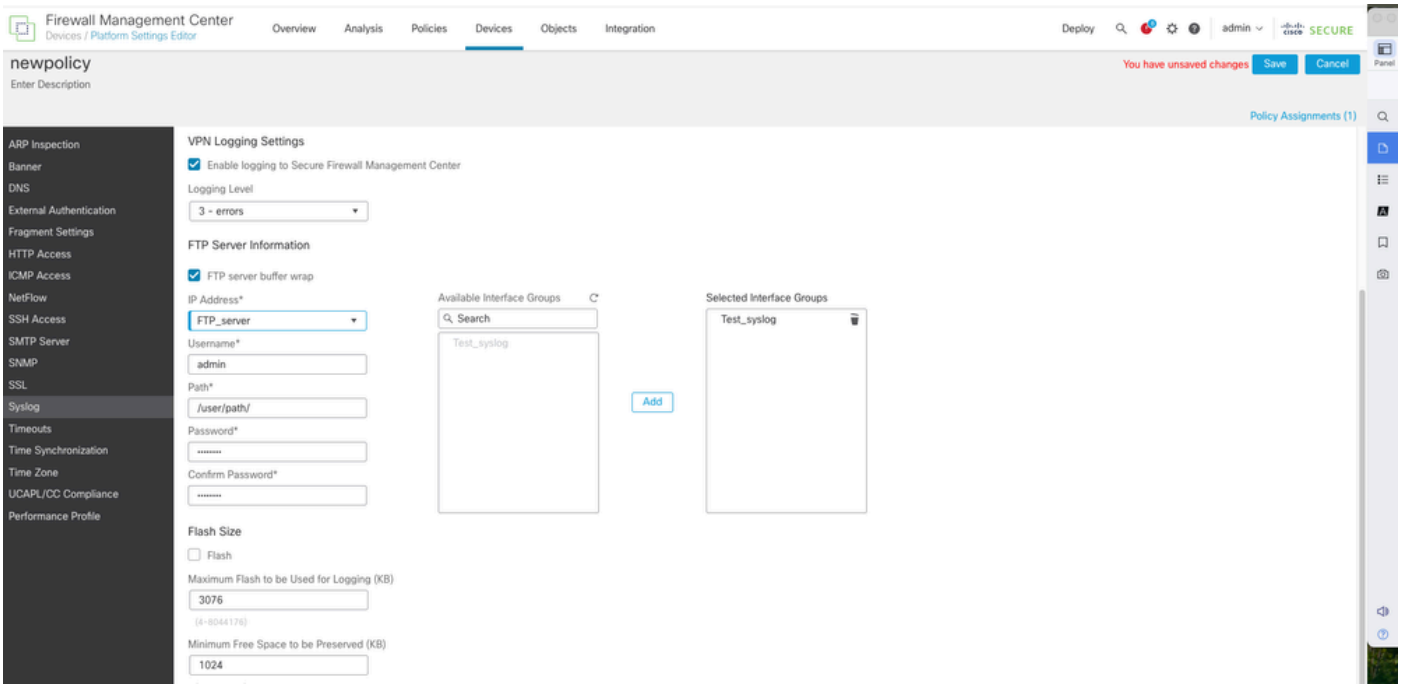
- Wählen Sie das Gerät aus dem Dropdown-Menü aus, und fügen Sie die VRF-Schnittstelle hinzu.



Hinzufügen einer VRF-fähigen Schnittstelle

Schritt 2:

- Navigieren Sie zu Devices > Platform Settings > Syslog > Logging Setup. Aktivieren Sie FTP Server Buffer Wrap.
- Klicken Sie auf Speichern.



Aktivieren von FTP-Servern mit VRF-fähiger Schnittstelle

Überprüfung

vor 7.4.1

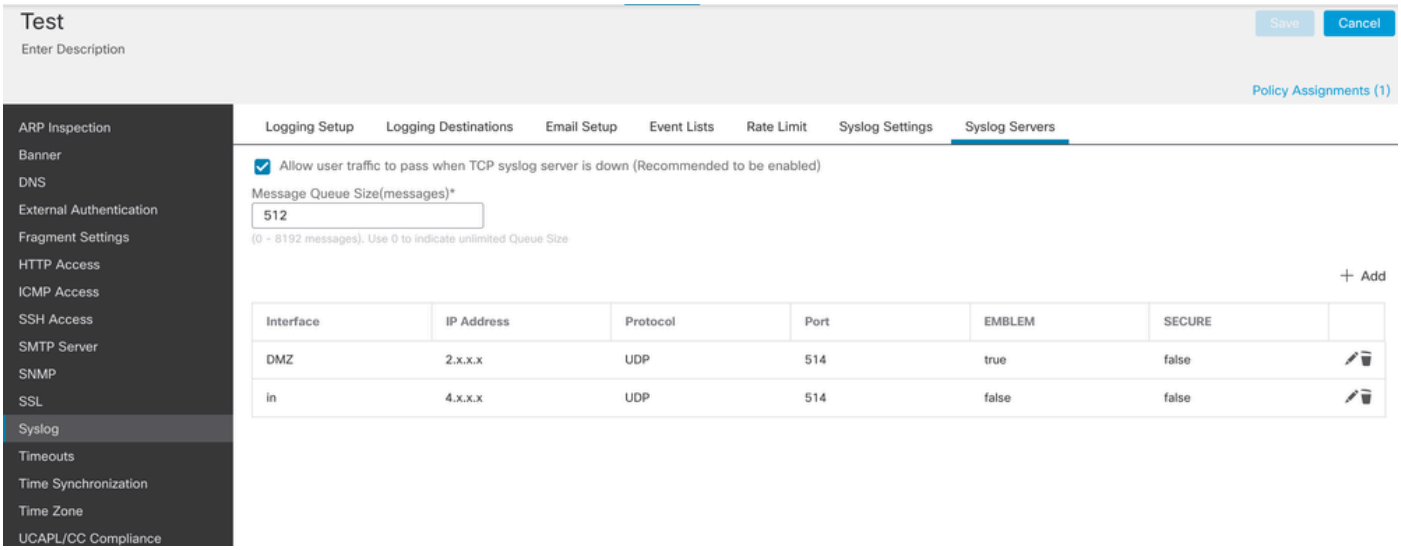
In diesem Test lauten FTD und FMC 7.0.5.

FTD wird mit VRF konfiguriert, und die DMZ-Schnittstelle wurde der VRF-Instanz zugewiesen.

Die DMZ-Schnittstelle wird mit einem Syslog-Server als Protokollierungshost konfiguriert.

Darüber hinaus wird die interne Schnittstelle mit den Syslog-Einstellungen konfiguriert.

Die interne Schnittstelle ist Teil von Global VRF.

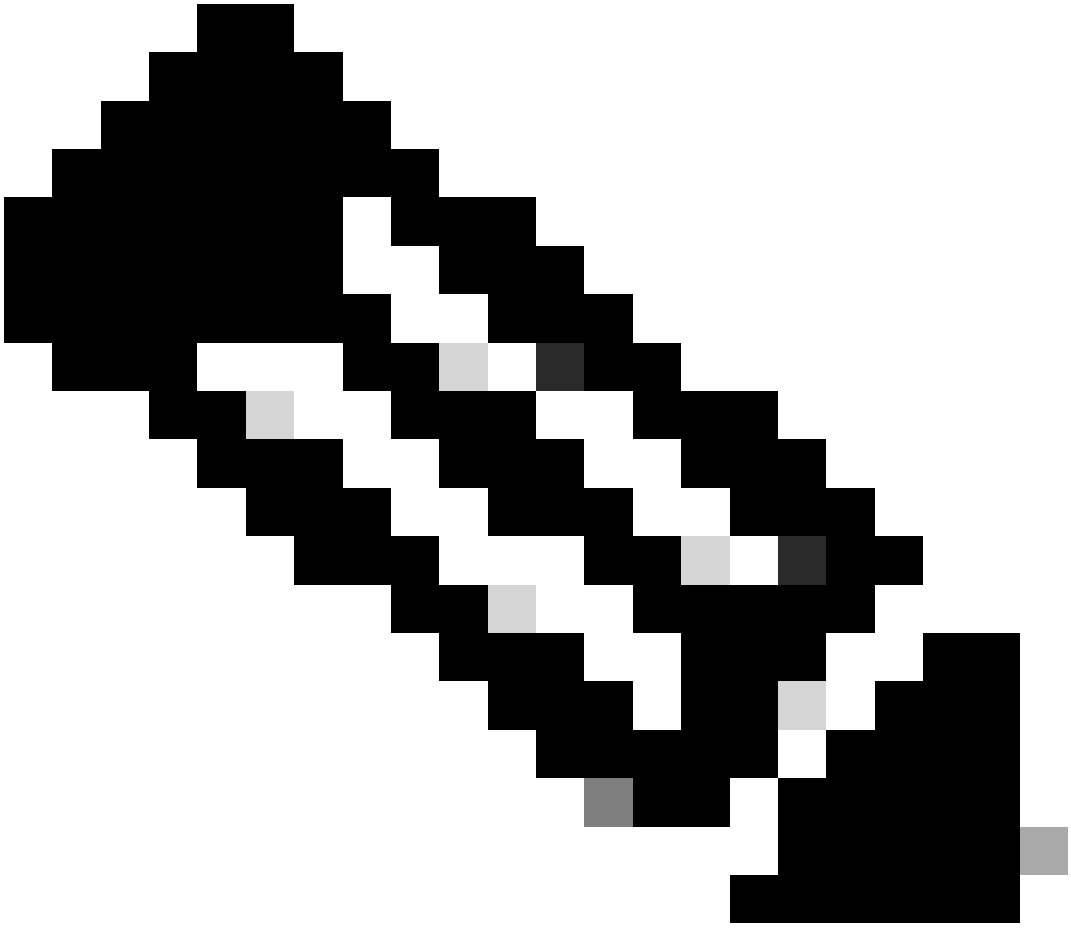


Syslog-Servereinstellung auf 7.0.5 FMC

CLI-Überprüfung

```
> 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
```



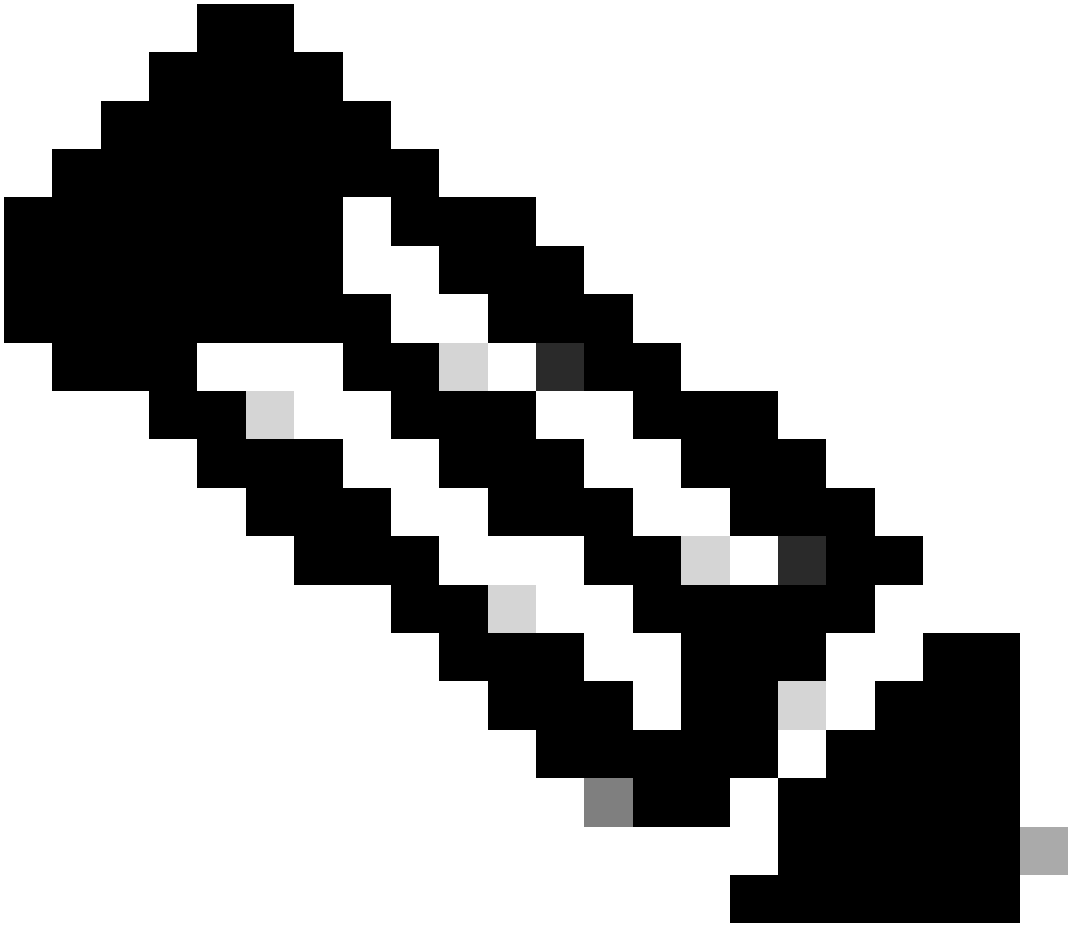
Anmerkung: Der Syslog-Server mit dem Ziel 2.x.x.x ist in den Protokolleinstellungen für die FTD-CLI nicht verfügbar. Dies ist Teil von Benutzer-VRF.
Der Syslog-Server mit dem Ziel 4.x.x.x steht über die Protokollierungseinstellung für die FTD-CLI zur Verfügung. Dies ist Teil von Global VRF.

Nach 7.4.1

CLI-Überprüfung

```
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
```



Anmerkung: Der Syslog-Server-Host 192.x.x.x verwendet die VRF-kompatible interne Schnittstelle.

FTP-Serververifizierung

vor 7.4.1

- Auf FMC haben die FTP-Servereinstellungen keine Option zur Auswahl der zu verwendenden Schnittstelle. Es ist nur die IP-Adresse der Syslog-Serveroption verfügbar.

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.