

VRF-bewuste systeemmodule op FTD configureren

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Minimale software- en hardwareplatforms](#)

[Ondersteuning van Snort3, multi-instantie/context en HA/clustering](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[Hoe het werkt](#)

[Virtuele router configureren](#)

[Voorwaarden voor FTP-serverconfiguratie in VCC](#)

[Configuratie](#)

[Verifiëren](#)

[Vooraf 7.4.1](#)

[Post 7.4.1](#)

[Verificatie van FTP-server](#)

[Vooraf 7.4.1](#)

[Post 7.4.1](#)

Inleiding

Dit document beschrijft de configuratie stappen voor VRF-bewuste syslog op FTD.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Syslog
- Firepower Threat Defense (FTD)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

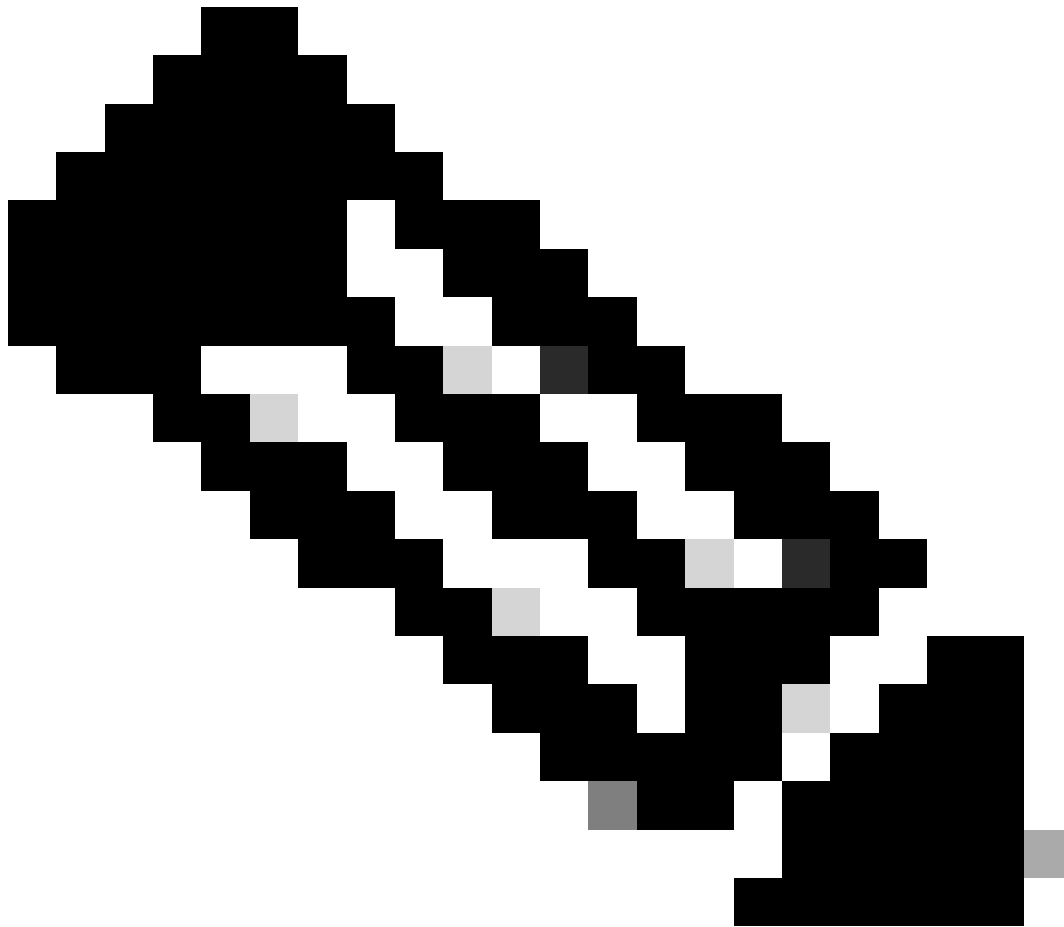
- Secure Firewall Management Center (FMCv) v7.4.2
- Secure Firewall Threat Defense Virtual (FTDv) v7.4.2

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Minimale software- en hardwareplatforms

- Toepassing en Minimale versie: Secure-firewall 7.4.1
- Ondersteunde beheerde platforms en versie: Alle ter ondersteuning van FTD 7.4.1
- Managers:
 - 1) VCC on-perm + FMC REST API
 - 2) FMC in de cloud
 - 3) FDM + REST API

Ondersteuning van Snort3, multi-instantie/context en HA/clustering



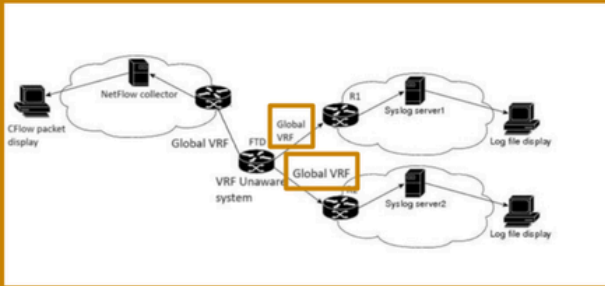
Opmerking: Werkt met zowel IPv4- als IPv6-syslog-servers. IPv6 wordt nog niet ondersteund op Syslog FTP-server.

-
- Ondersteund met multi-instantie.
 - Ondersteund met HA'd-apparaten.
 - Ondersteund op geclusterde apparaten.

Configureren

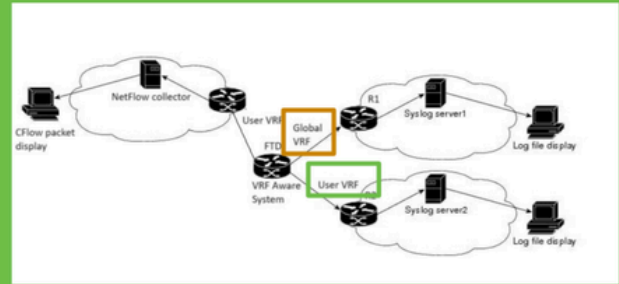
Netwerkdigram

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.

Vergelijking van netwerkdigrammen tussen Pre en Post 7.4.

Configuraties

Virtual Routing and Forwarding (VRF) is een technologie die in netwerken wordt gebruikt om meerdere instanties van een routingstabel naast elkaar te laten bestaan binnen dezelfde router, zodat netwerkisolatie tussen verschillende virtuele netwerken mogelijk is. Elke VRF-instantie is onafhankelijk van anderen en verkeer tussen hen wordt gescheiden gehouden. Multi-VRF is een functie die serviceproviders in staat stelt om meerdere VPN's en services te ondersteunen, zelfs als hun IP-adressen elkaar overlappen. Het gebruikt inputinterfaces om routes voor diverse diensten aan te wijzen en virtuele pakket-doorsturen lijsten te creëren door Layer 3 interfaces aan elke VRF toe te wijzen. Beheerservices (Syslog, NetFlow) gebruiken standaard wereldwijde VRF. Gebruikers willen gebruikers VRF gebruiken voor beheerservices en de wereldwijde VRF omdat niet alle uploadbestemmingen bereikbaar zijn via Global VRF.

In dit document is Global + User VRF = Multi-VRF

Schakel Syslog in voor Gebruiker VRF.

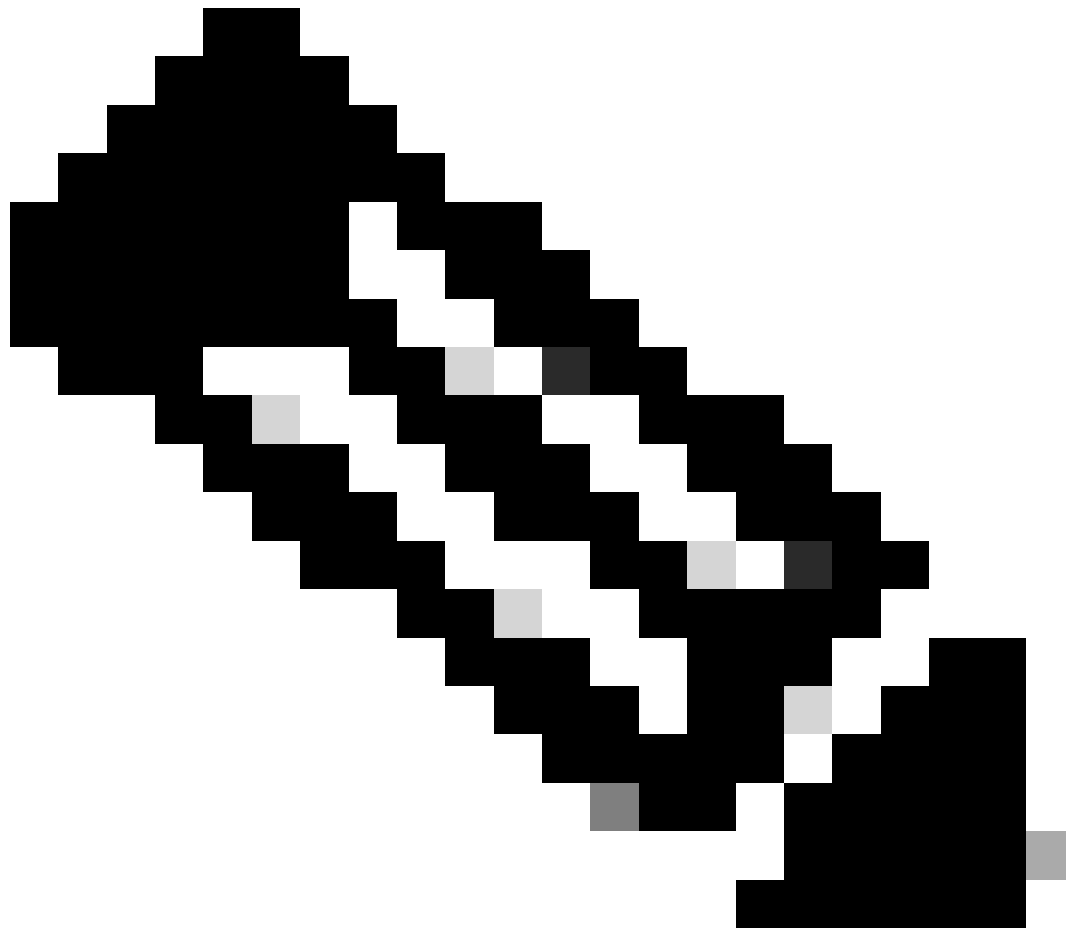
- Syslog kan ftp service gebruiken in een multi-VRF context.

Hoe het werkt

Wanneer de interface met Gebruiker VRF wordt gevormd, komt de routerraadpleging in VRF routeringsdomein voor, in plaats van standaard globaal routeringsdomein.

- Er worden twee typen serverconfiguraties ondersteund:
 1. Verzend logberichten naar Syslog servers om het netwerkverkeer te controleren en problemen op te lossen.
 2. Verzend de inhoud van de logbuffer naar een FTP-server als tekstbestand
- Syslog zendt de logbestanden uit naar de respectieve UDP/TCP-servers binnen die VRF.
- Voor bufferomloopsystemen worden de logs naar de geconfigureerde FTP-server verzonden

binnen die VRF.



Opmerking: Syslog server en FTP server kunnen deel uitmaken van verschillende VRF.

Virtuele router configureren

Stap 1. Maak een VRF

- Log in op FMC en navigeer naar apparaat > Apparaatbeheer.
- Selecteer het apparaat en klik op het pictogram Potlood om het te bewerken.
- Navigeren naar Routing> Virtuele router beheren > Virtuele router toevoegen.
- Voer de naam in bij VRF-naam.
- Selecteer de interface en klik op Toevoegen en Opslaan.

Virtual Router Properties

These are the basic details of this virtual router.

VRF Name:

VRF_1

Description:

syslog

Select Interface:

Search

Available Interfaces 

inside

Outside

dmz

inside2

Add

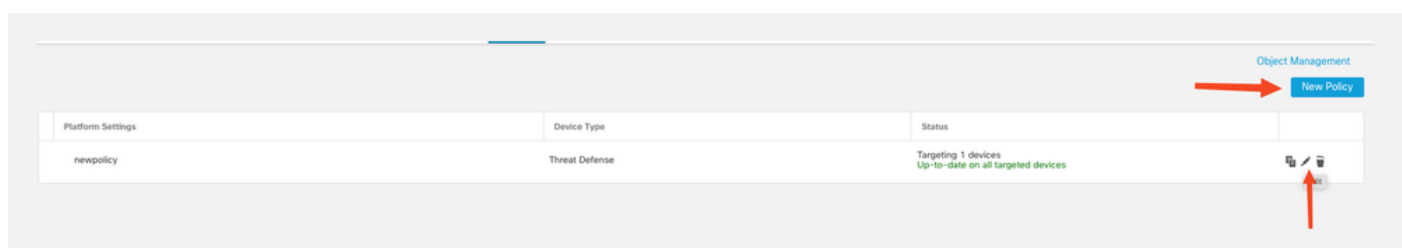
Selected Interfaces

inside 

Interface toevoegen aan VRF

Stap 2. Configureer de vastlegging.

- Navigeer naar Apparaten > Platform-instellingen.
- Maak een nieuw beleid of bewerk het potlood pictogram op bestaand beleid.



The screenshot shows a table with the following columns: Platform Settings, Device Type, and Status. The first row contains the text 'newpolicy', 'Threat Defense', and 'Targeting 1 devices Up-to-date on all targeted devices'. In the top right corner, there is a 'New Policy' button. In the bottom right corner, there is a 'New Policy' button and a 'New Policy' button.

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

De platforminstellingen maken

- Selecteer Logging Setup en Logboekregistratie inschakelen.

Logging Setup
Logging Destinations
Email Setup
Event Lists
Rate Limit
Syslog Settings
Syslog Servers

Basic Logging Settings

☒ Enable logging

Vastlegging inschakelen

- Selecteer Bestemming vastlegging en klik op Toevoegen.
- Stel de logbestemming in als Syslog-servers.

Logging Setup
Logging Destinations
Email Setup
Event Lists
Rate Limit
Syslog Settings
Syslog Servers

+ Add

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

Logboekbestemming als systeemsservers

- Selecteer Syslogservers > Toevoegen.

Logging Setup
Logging Destinations
Email Setup
Event Lists
Rate Limit
Syslog Settings
Syslog Servers

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

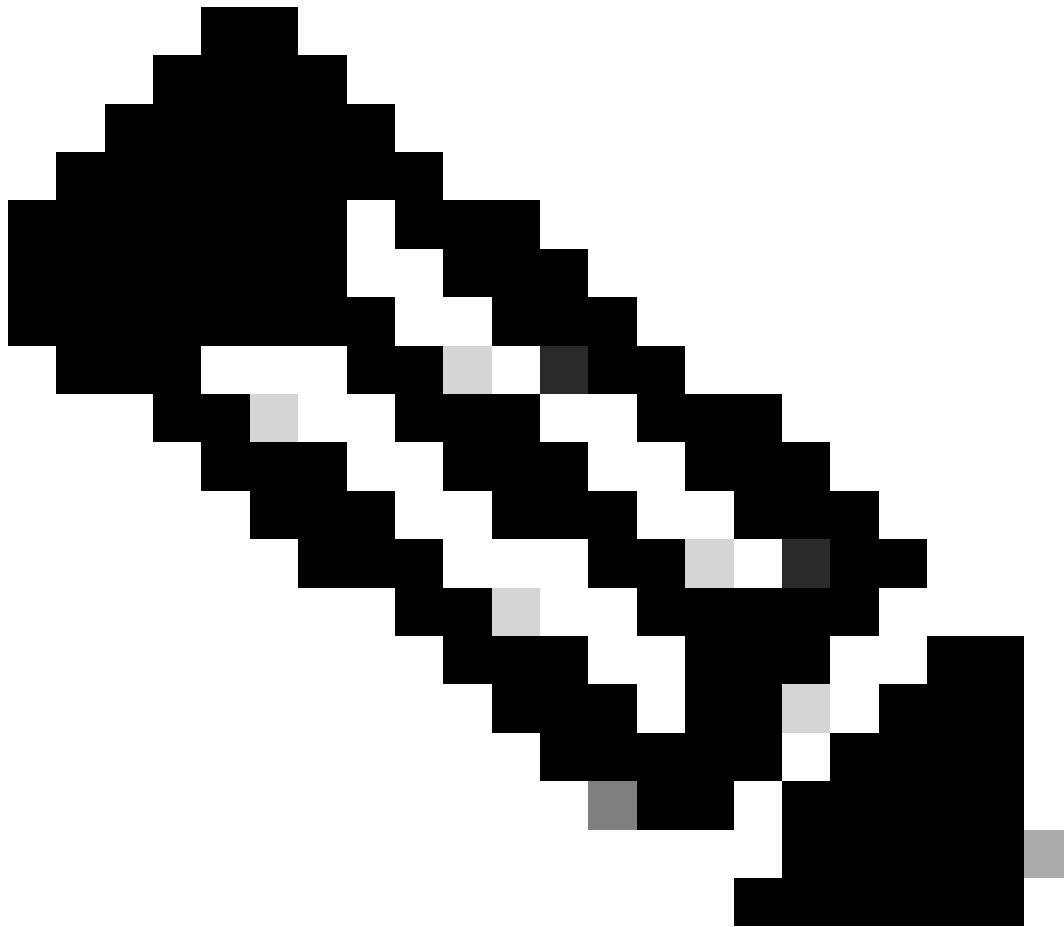
Message Queue Size (Messages)*

0-8192. Use 0 to indicate unlimited queue size

+ Add

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

Syslog-server toevoegen met VRF-bewuste interface



Opmerking: De binneninterface maakt deel uit van Security-zone in.

- De interface die in de opdracht van de logboekhost is geconfigureerd, is nu bewust van VRF.
- Klik op Save (Opslaan).

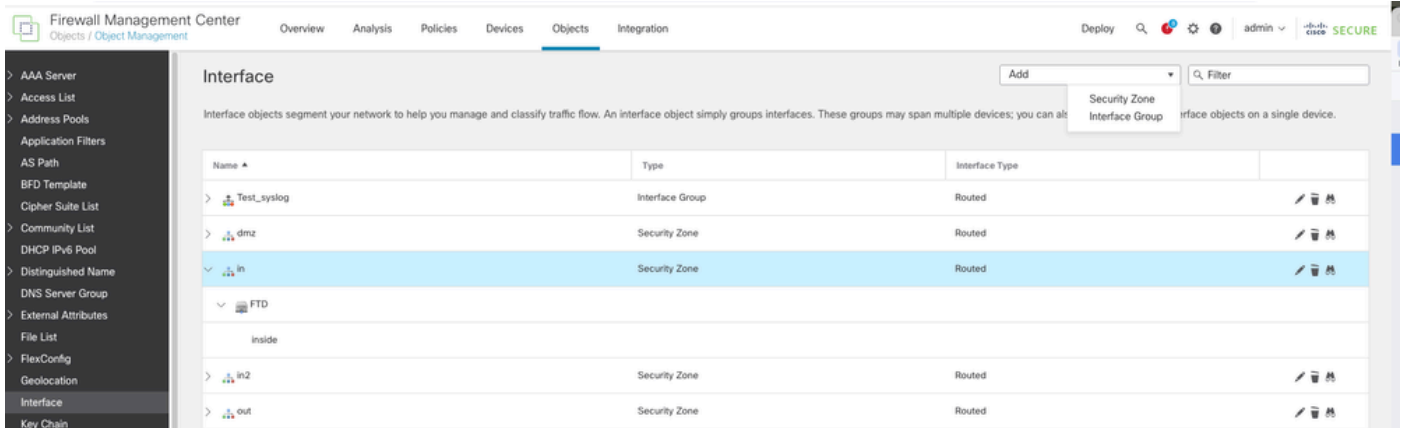
Voorwaarden voor FTP-serverconfiguratie in VCC

- Gebruik het object van de interfacegroep.
- De Voorwerp van de interfacegroep kan zowel Gebruiker als Globale VRF hebben.

Configuratie

Stap 1.

- Navigeer naar Object > Objectbeheer > Interface > Add > Interface Group.



Interfacegroep toevoegen

- Selecteer het apparaat uit de uitrollijst en voeg de VRF-interface toe.

Interface Group

Name:

Test_syslog

Interface Type:

Routed

Available Interfaces

FTD

Outside

dmz

inside2

Add

Selected Interfaces

FTD

inside

Cancel Save

VRF-bewuste interface toevoegen

Stap 2.

- Ga naar Apparaten > Platform-instellingen > Syslog > Logging Setup. Schakel FTP-

serverbuffer wrap in.

- Klik op Save (Opslaan).

The screenshot shows the Cisco Firewall Management Center (FMC) configuration page for a new policy named 'newpolicy'. The left sidebar contains a list of configuration categories: ARP Inspection, Banner, DNS, External Authentication, Fragment Settings, HTTP Access, ICMP Access, NetFlow, SSH Access, SMTP Server, SNMP, SSL, Syslog, Timeouts, Time Synchronization, Time Zone, UCAPL/CC Compliance, and Performance Profile. The 'Syslog' category is selected. The main configuration area is titled 'newpolicy' and includes a description field. The 'VPN Logging Settings' section is expanded, showing the following configuration options:

- 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*:** (masked)
 - Confirm Password*:** (masked)
- Flash Size:**
 - ☐ Flash
 - Maximum Flash to be Used for Logging (KB):** 3076
 - Minimum Free Space to be Preserved (KB):** 1024

The 'Available Interface Groups' list contains 'Test_syslog'. The 'Selected Interface Groups' list also contains 'Test_syslog'. An 'Add' button is located between the two lists.

FTP-server inschakelen met VRF-bewuste interface

Verifiëren

Vooraf 7.4.1

Voor deze test bedraagt het FTD en het FMC 7.0.5.

FTD wordt geconfigureerd met VRF en de dmz-interface is toegewezen aan VRF.

De dmz interface is geconfigureerd met syslog server logging host.

Bovendien wordt de binnenkant van de interface geconfigureerd met syslog-instelling.

De binneninterface maakt deel uit van Global VRF.

Test

Enter Description

Save

Cancel

Policy Assignments (1)

ARP Inspection

Banner

DNS

External Authentication

Fragment Settings

HTTP Access

ICMP Access

SSH Access

SMTP Server

SNMP

SSL

Syslog

Timeouts

Time Synchronization

Time Zone

UCAPL/CC Compliance

Logging Setup

Logging Destinations

Email Setup

Event Lists

Rate Limit

Syslog Settings

Syslog Servers

☒ 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

+ Add

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	 

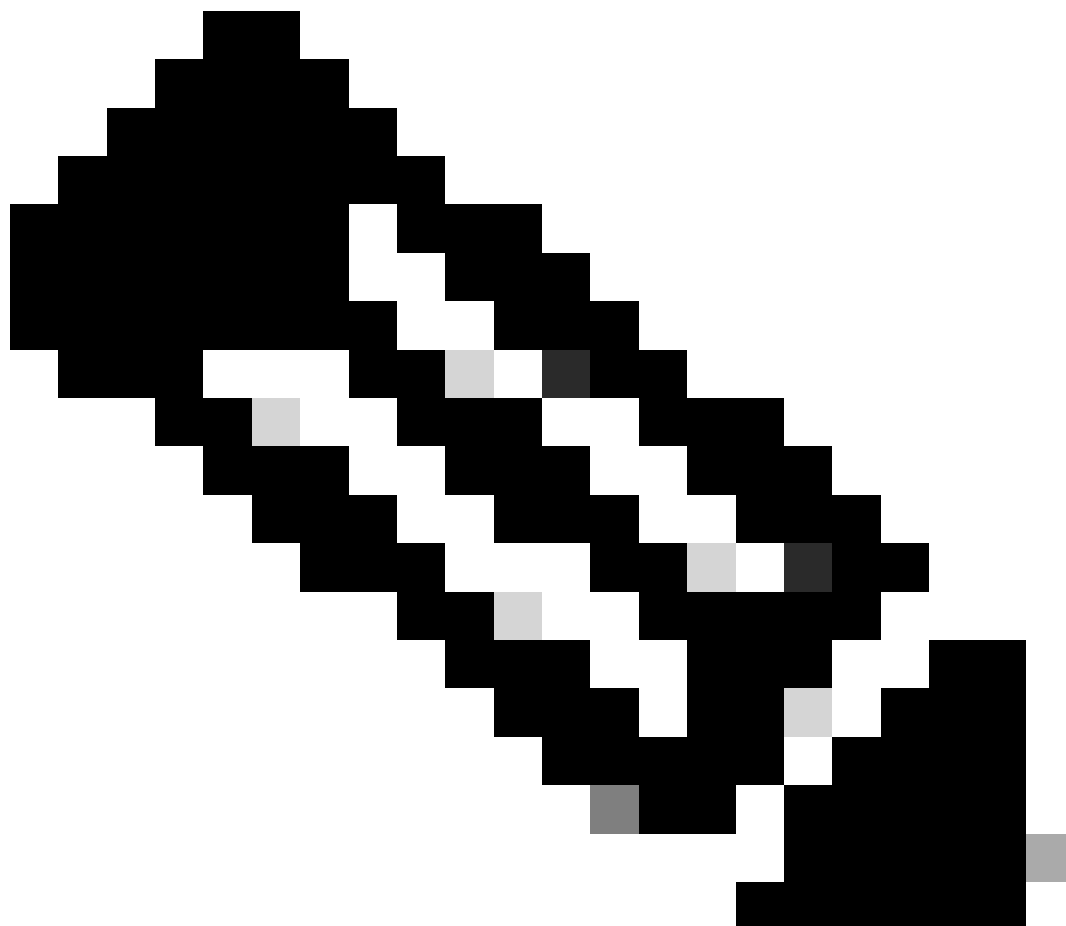
Syslog Server-instelling op 7.0.5 FMC

CLI-verificatie

```
> 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	



Opmerking: Syslog-server met bestemming 2.x.x.x is niet beschikbaar op logboekinstelling voor FTD CLI. Dit maakt deel uit van Gebruiker VRF.
Syslog server met bestemming 4.x.x.x is beschikbaar op logboekinstelling voor FTD CLI.
Dit maakt deel uit van Global VRF.

Post 7.4.1

CLI-verificatie

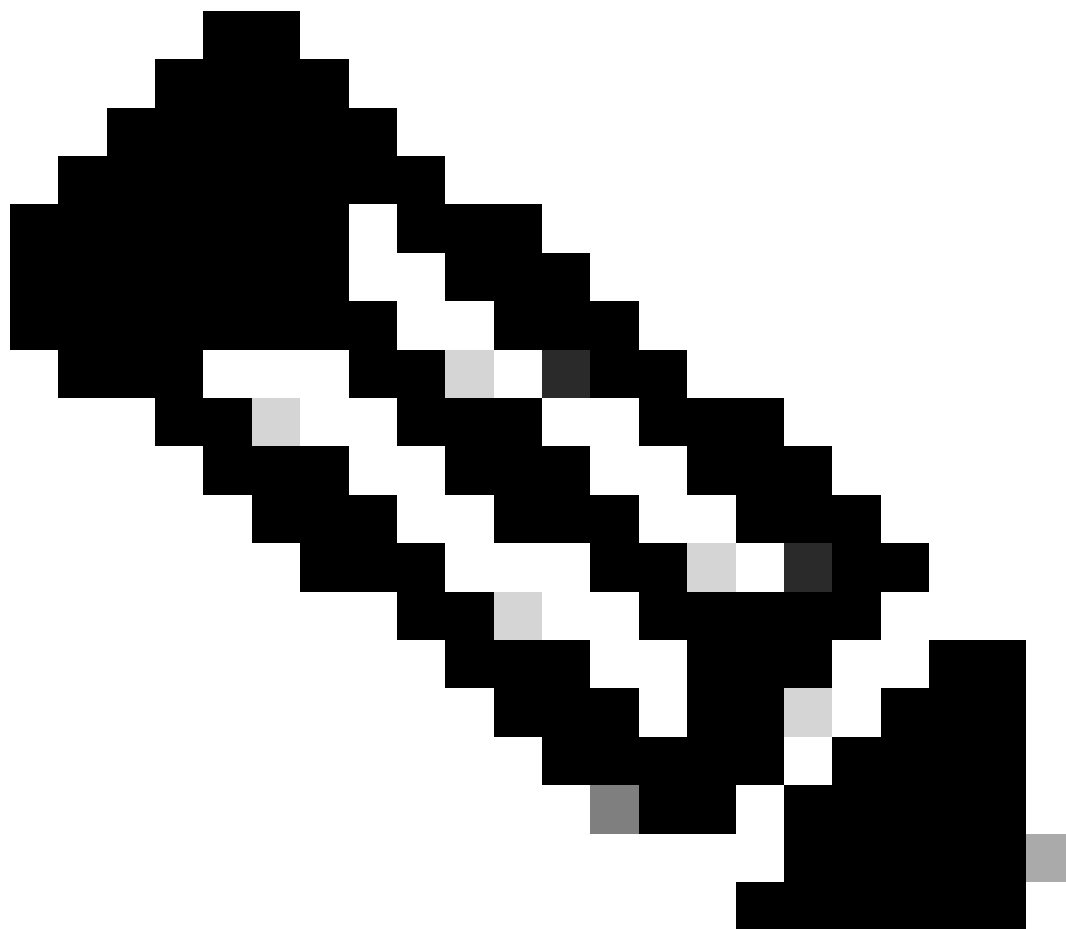
```
ftd1# show vrf
```

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



Opmerking: Syslog server host 192.x.x.x gebruikt de VRF bewuste binnenkant interface.

Verificatie van FTP-server

Vooraf 7.4.1

- Voor FMC heeft FTP-serverinstelling niet de optie om de te gebruiken interface te selecteren. Er is alleen IP-adres van de syslogserveroptie beschikbaar.

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)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.