

FTD ىلع VRF ل ؤكردملا syslog نيوكت

تاي وتحمل

[قمدقملا](#)

[قيس اس أل ا تابلطتملا](#)

[تابلطتملا](#)

[قمدختسملا تانوكملما](#)

[قيس اس أل ا قزمجأ او جماربلل دلأا دحلا](#)

[ماظنونو SNORT3 لىغشتلا ماظن معن HA/Cluster](#)

[نيوكتللا](#)

[لکب شرلل يطي طختلا مس رللا](#)

[تانيوكتللا](#)

[لمعوي فيك](#)

[يرهاظلا وجوملا نيوكت](#)

[فـ FTP مـ داخـ نـ يـ وـ كـ تـ لـ قـيـ سـ اـ سـ اـ لـ اـ تـ اـ بـ لـ طـ تـ مـ لـ](#)

[نيوكتللا](#)

[قـ حـ صـ لـ لـ اـ تـ مـ قـ قـ حـ تـ لـ لـ](#)

[لـ لـ بـ فـ اـ مـ](#)

[Post 7.4.1](#)

[مـ دـ اـ خـ نـ مـ قـ قـ حـ تـ لـ لـ](#)

[لـ لـ بـ فـ اـ مـ](#)

[Post 7.4.1](#)

قـ مدـ قـ مـ لـ

FTD ىلع VRF ل ؤكردملا syslog نيوكتلا تاوطخ دنتسملا اذه فصي.

قيس اس أل ا تابلطتملا

تابلطتملا

CISCO يصوت: قـيلـاتـلـا عـيـضـاـوـمـلـابـ قـفـرعـمـ كـيـدـلـ نـوـكـتـ نـأـبـ

- Syslog
- Firepower Threat Defense (FTD)

قـ مدـ خـتـسـمـلـا تـانـوـكـمـلـا

QoS: قـيلـاتـلـا ئـيـدـامـلـا تـانـوـكـمـلـا وجـمارـبـلـا تـارـادـصـاـىـلـا دـنـتـسـمـلـا اـذهـ يـفـ قـدرـاـوـلـا تـامـوـلـعـمـلـا دـنـتـسـتـ

- Secure Firewall Management Center (FMCv) 7.4.2
- Secure Firewall Threat Defense Virtual (FTDv) v7.4.2

ةـصـاخـ ةـيـلـمـعـمـ ةـئـيـبـ يـفـ ةـدـوـجـوـمـلـاـ ةـزـهـجـأـلـاـ نـمـ دـنـتـسـمـلـاـ اـذـهـ يـفـ ةـدـرـاـوـلـاـ تـامـوـلـعـمـلـاـ ءـاعـشـنـاـ مـتـ
تـنـاـكـ اـذـاـ .(ـيـضـارـتـفـاـ)ـ حـوـسـمـمـ نـيـوـكـتـبـ دـنـتـسـمـلـاـ اـذـهـ يـفـ ةـمـدـخـتـسـمـلـاـ ةـزـهـجـأـلـاـ عـيـمـجـ تـأـدـبـ
رـمـأـ يـأـلـ لـمـتـحـمـلـاـ رـيـثـأـتـلـلـ كـمـهـفـ نـمـ دـكـأـتـفـ ،ـلـيـغـشـتـلـاـ دـيـقـ كـتـكـبـشـ.

ةـيـسـاسـأـلـاـ ةـزـهـجـأـلـاـ اوـ جـمـارـبـلـلـ ئـنـدـأـلـاـ دـحـلـاـ

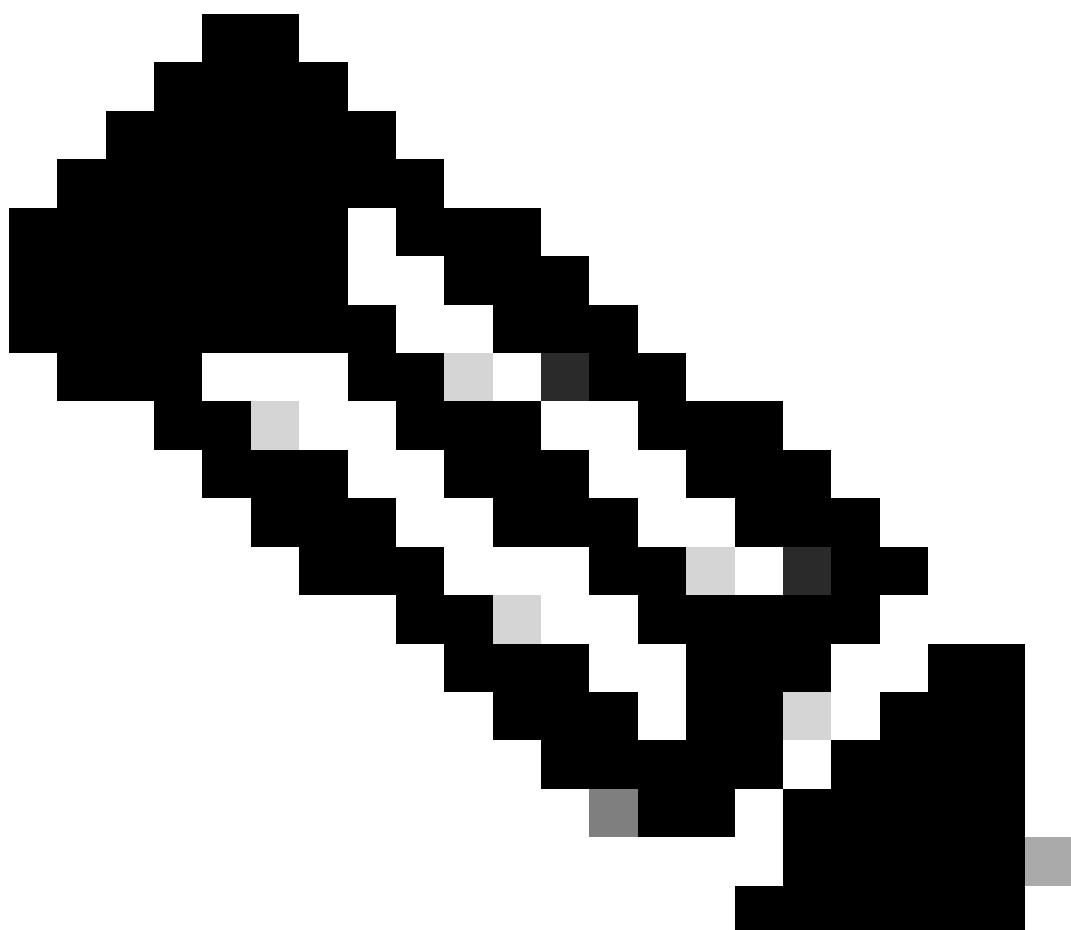
- رـادـصـإـلـلـ ئـنـدـأـلـاـ دـحـلـاـوـ قـيـبـطـتـلـاـ Secure Firewall 7.4.1
- مـعـدـيـ اـمـ لـكـ :ـةـمـوـعـدـمـلـاـ رـادـصـإـلـاـوـ رـادـمـلـاـ ةـيـسـاسـأـلـاـ ةـمـظـنـأـلـاـ FTD 7.4.1
- نـورـيـدـمـلـاـ

ةـدـحـوـبـ ةـصـاخـلـاـ RESTـ تـاقـيـبـطـتـ ةـجـمـرـبـ ةـهـجـاـوـ +ـ مـدـاـخـلـاـ ئـلـعـ FMCـ تـاقـيـبـطـتـ ةـجـمـرـبـ ةـهـجـاـوـ (ـ1ـ)
ةـبـاحـسـلـاـ رـبـعـ اـهـمـيـلـسـتـ مـتـيـ يـتـلـاـ (ـFMCـ)ـ ةـيـسـاسـأـلـاـ ةـحـوـلـلـاـ ةـرـاـدـاـ يـفـ مـكـحـتـلـاـ ةـدـحـوـ (ـ2ـ)

3) FDM + REST API

ةـبـاحـسـلـاـ رـبـعـ اـهـمـيـلـسـتـ مـتـيـ يـتـلـاـ (ـFMCـ)ـ ةـيـسـاسـأـلـاـ ةـحـوـلـلـاـ ةـرـاـدـاـ يـفـ مـكـحـتـلـاـ ةـدـحـوـ (ـ2ـ)

ةـبـاحـسـلـاـ رـبـعـ اـهـمـيـلـسـتـ مـتـيـ يـتـلـاـ (ـFMCـ)ـ ةـيـسـاسـأـلـاـ ةـحـوـلـلـاـ ةـرـاـدـاـ يـفـ مـكـحـتـلـاـ ةـدـحـوـ (ـ2ـ)



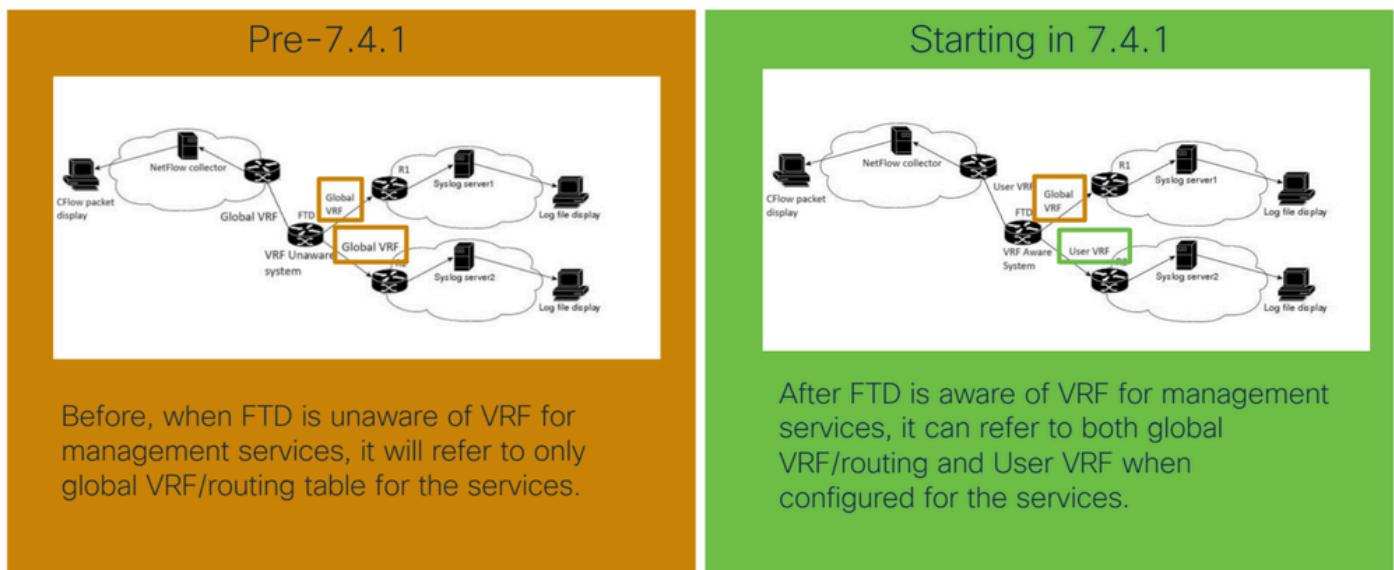
تـنـرـتـنـ إـلـاـ لـوـكـوـتـوـرـبـ نـمـ عـبـارـلـاـ رـادـصـإـلـاـبـ ةـصـاخـلـاـ syslogـ مـداـخـ نـمـ لـكـ عـمـ لـمـعـيـ :ـةـظـحـاـلـمـ

(IPv4 و IPv6) مع دم متي الـ Syslog FTP مداخ يف نآلا ىتح IPv6 مع دم متي الـ.

- ع مع دم Multi-instance.
- ۆزهجأب موعد HA.
- ۆعجملا ۆزهجألا ىلع موعد.

نیوکتلا

ةكبشلل یطیطختلا مسربلا



7. قحاللاو قباسلا نیزارتلا نیب ةكبشلل یطیطختلا مسربلا ۆنراقم.

تانيوکتلا

تالي ثم لـ ۆامسلل ۆكبشلا یف مدخلتست ۆينقت یه (VRF) یرهاظلا ھي جوتلا ۆداع او ھي جوتلا نیب ۆكبشلا لزع رفوي امم، سفن ھجوملا لخاد شيعاتلاب ھي جوتلا لودجل ۆددعتملا، یرخألا نع ۆلقتسم (VRF) وي دارلا درت تالاح نم ۆللاح لک. ۆفلت خمللا ۆي رهاظلا تاكبشلا مع دم دخللا یدوزمل حیتت ۆزيم یه Multi-VRF. ۆلصفنم اهنیب رورملا ۆکرحب ظافتحا متي و تاهجاو مدخلتسی ۵۰۰. ۆب ۆصالخلا IP نیوانع لخادت اذا ىتح، تامدخل او ۆددعتم VPN تاكب بش لالخ نم ۆي ضارت فا مزح ھي جوت ۆداعا لواج عاشن او ۆفلت خم تامدخل تاراسمللا نیي عتل لاخ دالا دادع إک ماععلـا VRF (Syslog، NetFlow) ۆرادإلا تامدخل مدخلتست. لـ 3 ۆقبطلـا تاهجاو نـيـيـعـتـ ىـلـا ۆـفـاـضـ إـلـاـبـ ۆـرـادـإـلـاـ تـامـدـخـ مـدـخـتـسـمـلـاـبـ صـاـخـلـاـ VRF مـادـخـتـسـاـ نـوـمـدـخـتـسـمـلـاـ دـيـرـيـ. ۆـيـضـارتـ فـاـ VRF ربـعـ اـهـيـلـاـ لـوـصـوـلـاـ نـكـمـيـ لـيـمـحـتـلـاـ تـاهـجـوـلـكـ سـيـلـ نـأـلـ يـمـوـمـعـلـاـ.

لـمـعـتـسـمـ + لـمـاـشـ، ۆـقـيـثـوـاـذـهـ یـفـ

syslog مدخلتست VRF.

- قـاـيـسـ يـفـ ftp مـدـخـتـسـتـ نـأـنـكـمـيـ multi-VRF.

لـمـعـيـ فـيـكـ

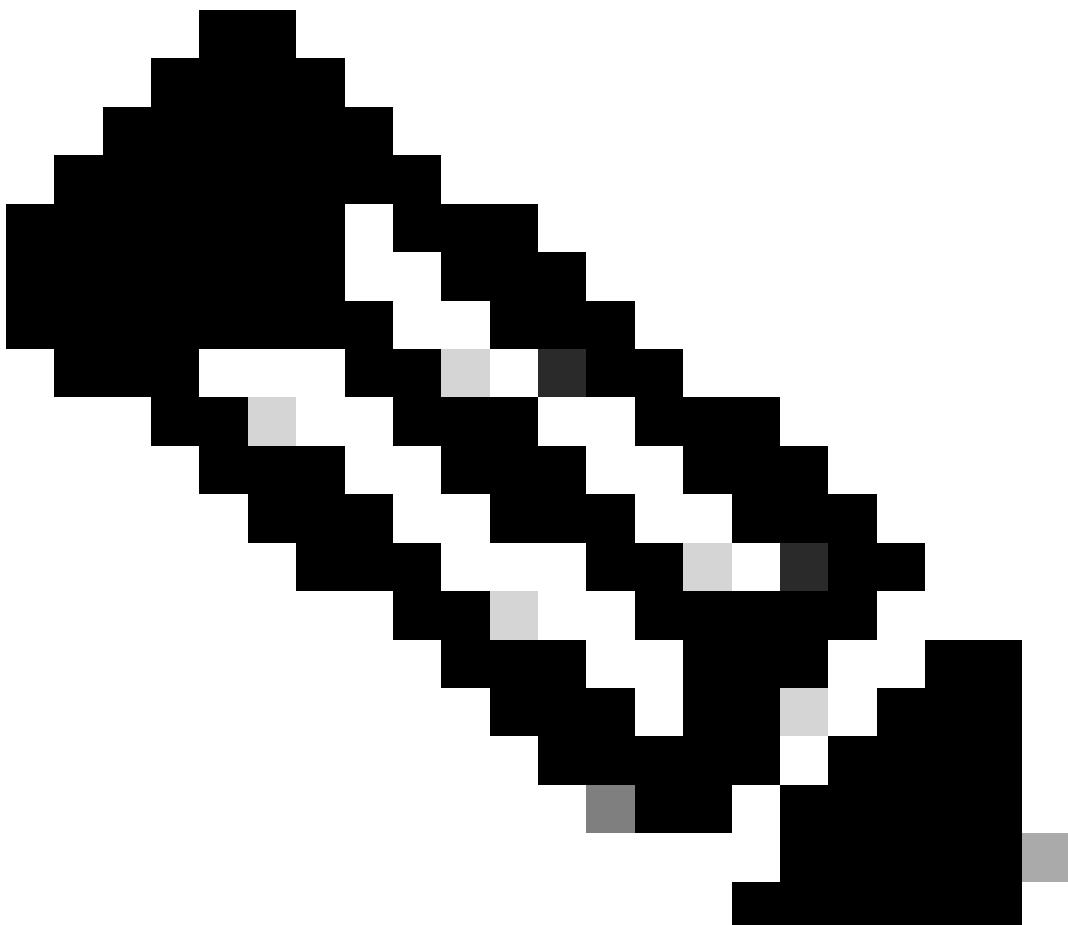
هیجوت لاجم یف راسملاء ثحب ثدحي ،مدختسملل VRF مادختساب ۃجاؤلا نیوکت متی امدنع
یضارتفالا ماعلا هیجوتلا لاجم نم الدب ،

- مداخلا تانیوکت نم نیعون معنی دمتی:

فاشكتساو ۃكبشلا رورم ۃکرخ ۃبقارمل Syslog مداوخ یلا ليجستلا لیاسر لاسرا .
اھحالص او اھیا طخأ.

2. یصن فلمک FTP مداخ یلا لجسلل تقؤملانیزختلا یوتحم لاسرا

- اذه VRF لوکوتورب لخاد ۃلباقملان UDP/TCP مداوخ یلا تالجسلالاسراب Syslog موقعت
- مت یذلا FTP مداخ یلا تالجسلالاسرا متی ،تقؤملانزخملافافتلا مظنل ۃبسنلاب اذه VRF لخاد هنیوکت



فلتخم VRFs نم عزج تنك عیطتسی لدان FTP ولدان Syslog: ۃظحالم.

یرهاظلما هجوملا نیوکت

1. ۋەطخىل VRF ئاشنە

- زەھجىڭىلا ئارادا > زاھىجلا ئىلى لېقتنى او FMC ئىلى لۇخدىلا لىجىس.
- رېيىحەتلىك مەلۇقلارنىڭ ئۈچۈن زاھىجلا دەدەن.
- يەھا ئۆچۈم ئەفاسىدا > يەھا ئۆچۈم ئارادا > زەھجىنى ئىلى لېقتنى.
- مىسىز VRF ئەپسەن ئەلەتلىخىد.
- ئەظەن ئەفاسىدا زەھنە ئەھجىۋەلە دەدەن.

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

Selected Interfaces

inside

Add

ئىلى ئەھجىۋە ئەفاسى

2. ۋەطخىل لېجىستلى دادعى نىوكتىب مق.

- سەسلىك مەظنۇلدا تادادعى > زەھجىڭىلا ئىلى لېقتنى.
- دەۋەجەنلارنىڭ ئۆچۈم ئەپسەن ئەلەتلىخىت وە دىدەجەن ئاشنە.

يـسـاسـأـلـا مـاظـنـلـا تـادـادـعـا عـاشـنـا

- لـيـجـسـتـلـا نـيـكـمـتـو لـيـجـسـتـلـا دـادـعـا دـدـحـ.

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

Basic Logging Settings

Enable logging

لـيـجـسـتـلـا نـيـكـمـتـ

ةـفـاضـا قـوـفـ رـقـنـا وـلـيـجـسـتـلـا ةـهـجـو دـدـحـ.

- لـدـانـا logging كـ ئـيـاعـ لـا تـتـبـثـ.

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				

مـداـوـخـكـ ةـهـجـوـلـا لـيـجـسـتـ

- ظـفـاضـا > Syslog مـداـوـخـ دـدـحـ.

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

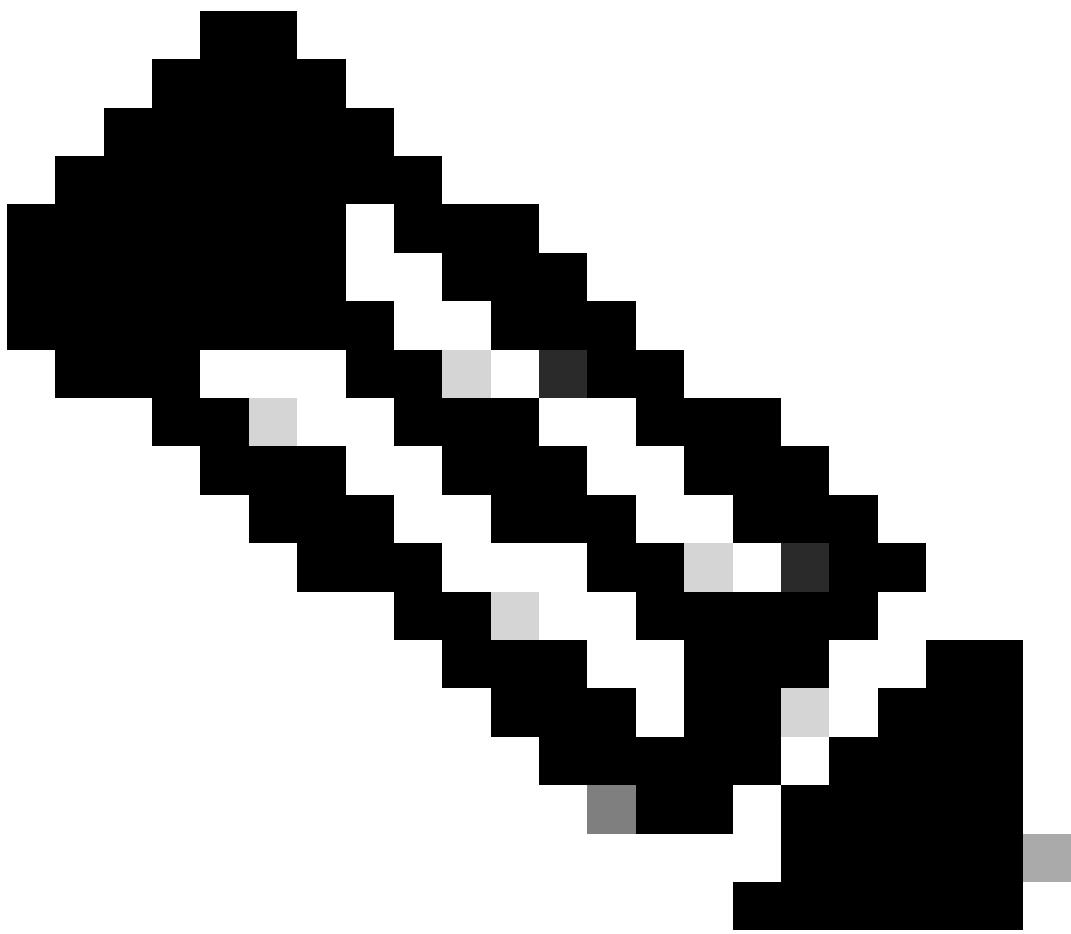
Allow user traffic to pass when TCP syslog server is down (Recommended)

Message Queue Size (Messages)*
512
0-8192. Use 0 to indicate unlimited queue size

+ Add

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

ةـسـاسـجـلـا VRF ةـهـجـوـا مـادـخـتـسـابـ syslog مـداـخـ ظـفـاضـا



يـف نـامـاـلـاـ ةـقـطـنـمـ نـمـ عـزـجـ يـهـ ةـيـلـخـادـلـاـ ةـهـجـاـوـلـاـ:ـظـحـاـلـمـ.

- لـ ةـكـرـدـمـ نـآـلـاـ نـوـكـتـ رـمـأـلـاـ يـفـ اـهـنـيـوـكـتـ مـتـ يـتـلـاـ ةـهـجـاـوـلـاـ VRFـ.
- ظـفـحـ قـوـفـ رـقـنـاـ.

يـفـ FMCـ مـدـاـخـ نـيـوـكـتـلـ ةـيـسـاسـأـلـاـ تـابـلـطـتـمـلـاـ

- ةـهـجـاـوـلـاـ ةـعـوـمـجـمـ نـئـاـكـ مـاـدـخـتـسـاـ.
- يـمـوـمـعـلـاـ VRFـ وـ Userـ نـمـ لـكـ يـلـعـ ةـهـجـاـوـلـاـ ةـعـوـمـجـمـ نـئـاـكـ يـوـتـحـيـ نـأـ نـكـمـيـ.

نـيـوـكـتـلـاـ

1ـ ةـوـطـخـلـاـ

- ةـهـجـاـوـلـاـ ةـعـوـمـجـمـ >ـ ةـفـاـضـاـ >ـ ةـهـجـاـوـ >ـ نـئـاـكـلـاـ ةـرـاـدـاـ >ـ نـئـاـكـ يـلـاـ لـقـتـنـاـ.

The screenshot shows the 'Interface' object list in the Cisco Firewall Management Center. The table includes columns for Name, Type, Interface Type, and status. Key entries include 'Test_syslog' (Interface Group, Routed), 'dmz' (Security Zone, Routed), 'in' (Security Zone, Routed), 'FTD' (Interface Group, Routed), 'inside' (Security Zone, Routed), 'in2' (Security Zone, Routed), and 'out' (Security Zone, Routed).

وھج او تھج موجم وھج او تھج

- ۋەھج او تھج موجم دەن سەنملە قىلىنما نەم زاھىلدا دەح VRF.

The screenshot shows the 'Interface Group' configuration dialog. The 'Name' field is set to 'Test_syslog'. The 'Interface Type' dropdown is set to 'Routed'. In the 'Available Interfaces' list, 'FTD' is selected. The 'Selected Interfaces' list contains 'FTD' and 'inside'. An 'Add' button is visible between the two lists. At the bottom right are 'Cancel' and 'Save' buttons.

وھج او تھج VRF Aware

2. ۋەھج او تھج

- نېكىم تېب مق. لىچىستىلدا دادعى > يىس اس أىلا ماظنلى تادادعى > ۋەھج أىلا ىلى لىقتنى

- م داخل ت قوملا نزخمل ا فافتلا ظفح قوف رقنا.

The screenshot shows the FMC interface with the 'Devices' tab selected. In the main configuration area, under 'FTP Server Information', the 'IP Address*' field is set to 'FTP_server', 'Username*' is 'admin', 'Path*' is '/user/path/', and 'Password*' and 'Confirm Password*' are both masked. An 'Available Interface Groups' list contains 'Test_syslog'. An 'Add' button is visible next to it. To the right, a 'Selected Interface Groups' panel shows 'Test_syslog' listed. The left sidebar includes options like 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.

م داخل ت قوملا نزخمل ا فافتلا ظفح قوف رقنا

ةحصـلـا نـم قـقـحـتـلـا

لـبـقـ اـم 7.4.1

ةـهـجـاـوـ صـيـصـخـتـ مـتـ وـ FTDـ وـ FMCـ 7. 0. 5ـ .

ةـهـجـاـوـ صـيـصـخـتـ مـتـ وـ VRFـ مـادـخـتـسـاـبـ FTDـ لـ DMZـ لـ VRFـ .

مـداـخـ لـيـجـسـتـ فـيـضـمـ مـادـخـتـسـاـبـ DMZـ ةـهـجـاـوـ نـيـوـكـتـ مـتـ .

دادـعـ مـادـخـتـسـاـبـ ةـيـلـخـادـلـاـ ةـهـجـاـوـلـاـ نـيـوـكـتـ مـتـ ،ـكـلـذـىـلـاـ ةـفـاضـلـابـ .

لـمـاـشـ VRFـ نـمـ عـزـ يـلـخـادـ نـرـاقـلـاـ .

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	

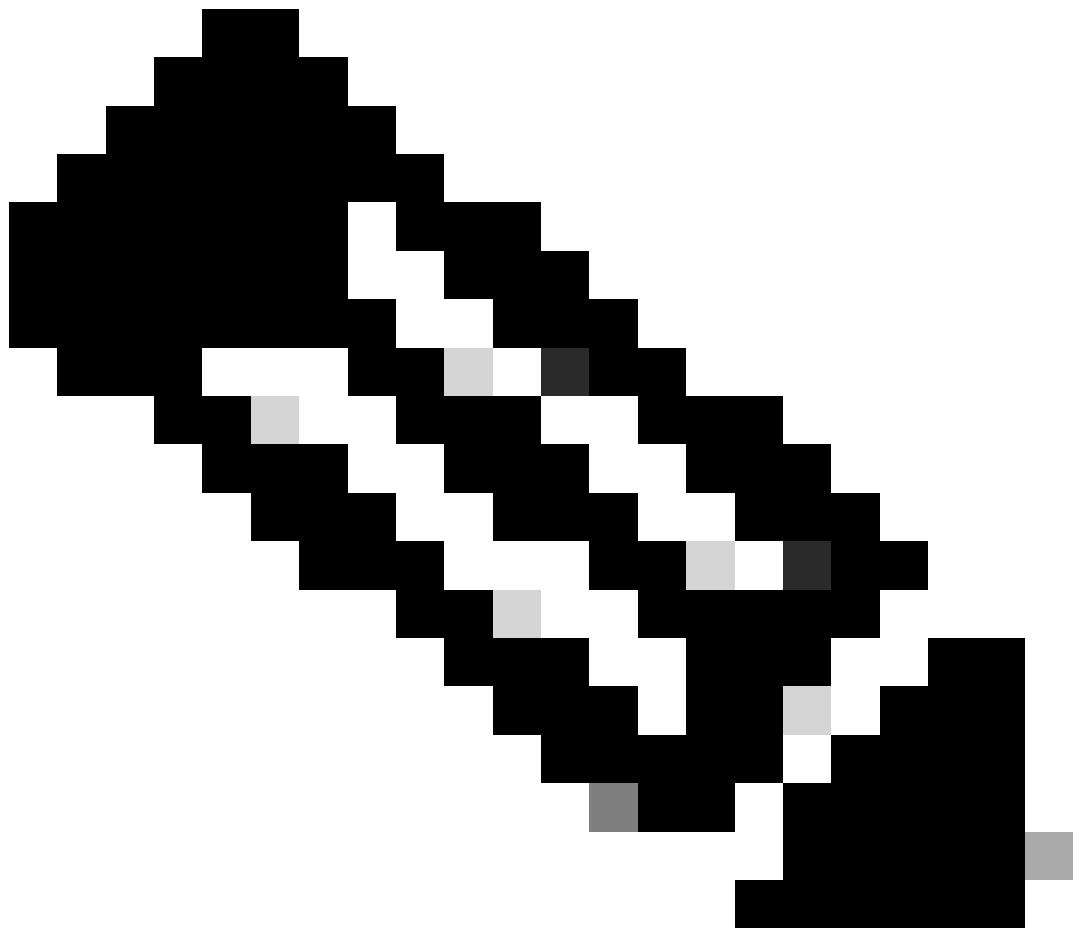
اداع Syslog Server علی 7.0.5 FMC

رم اولیا رطس ۋەج او نم قۇچتىلا (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



عژ اذه ل ليجستلا دادعإ يف Syslog 2.x.x.x ۆجهو لا يذ FTD CLI. مداخ رفوتي ال: ظحال م دختسملل نم VRF.

نم عژ اذه ل ليجستلا دادعإ ىلع Syslog 4.x.x.x ۆجهو لا عم مداخ رفوتي يملاعلا.

Post 7.4.1

رماؤألا رطس ۆهنجاو نم قُقحتلا (CLI)

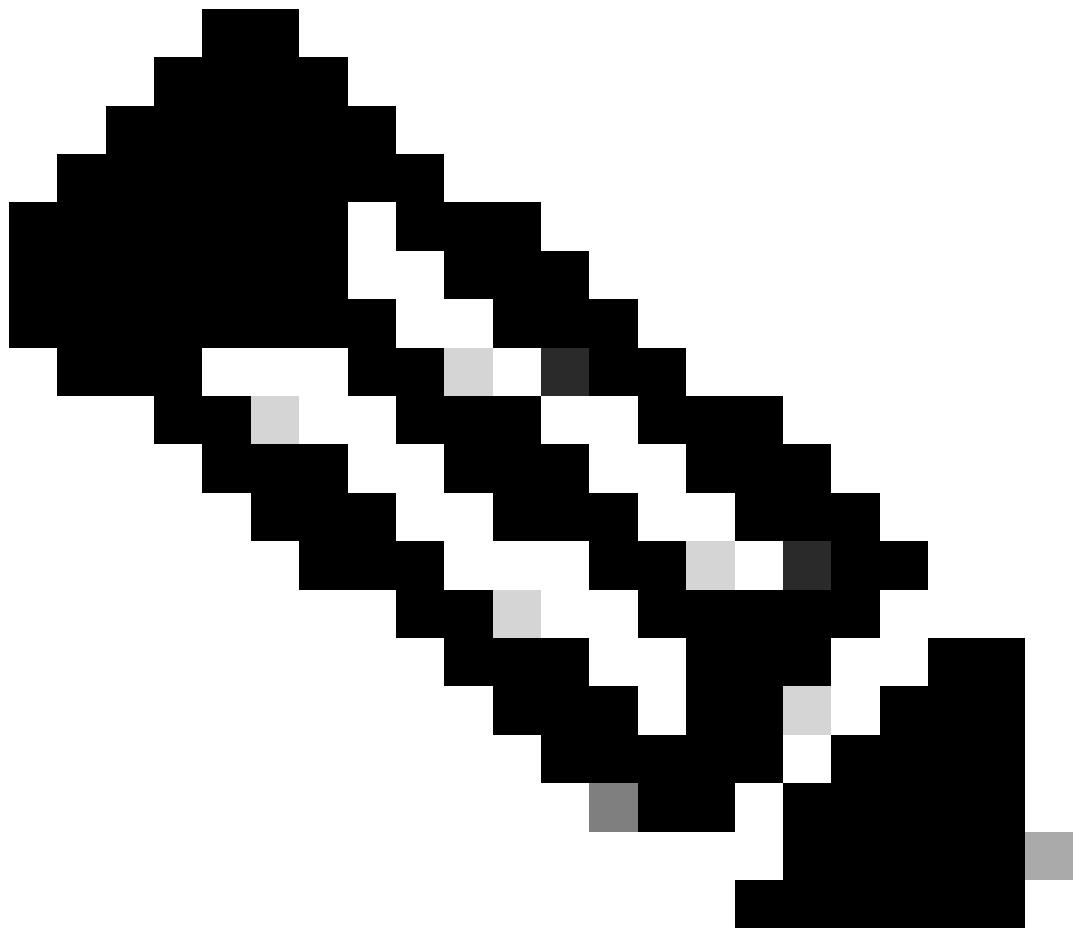
```
ftd1# show vrf
```

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
```



عضو مت يتلا ئيلخادلا ئهجاولا Syslog 192.x.x.x مداخ فيضم مدخلتسي: ئەظحالم اهيلع.

مداخ نم ققحتلا FTP

لبق ام 7.4.1

- اهمادخلتسا ديرت يتلا ئهجاولا ديدهت رايخل ع FMC ، اىل ع FMC دادع اي وتحي ال . مداخ طقف IP ناونع رفوتي syslog.

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)

(4-8044176)

Minimum free Space to be preserved(KB)

(0-8044176)

هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).