Configurazione del syslog compatibile con VRF su FTD

Sommario

Introduzione

In questo documento viene descritto come configurare il syslog con riconoscimento VRF su un FTD.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Syslog
- Firepower Threat Defense (FTD)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e

hardware:

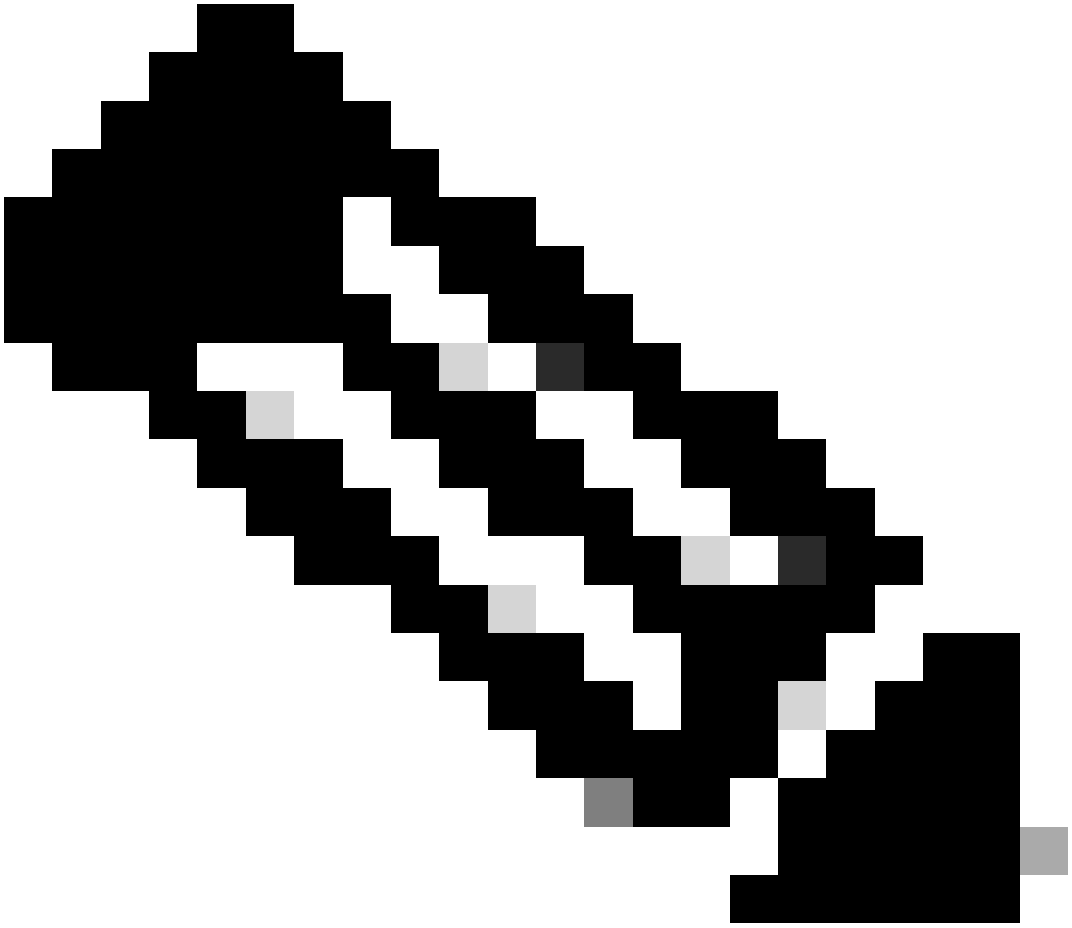
- Secure Firewall Management Center (FMCv) v7.4.2
- Secure Firewall Threat Defense Virtual (FTDv) v7.4.2

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Piattaforme software e hardware minime

- Applicazione e versione minima: Secure Firewall 7.4.1
- Piattaforme gestite supportate e versione: Tutti i sistemi che supportano FTD 7.4.1
- Responsabili:
  1) FMC on perm + FMC REST API
  2) FMC fornito tramite cloud
  3) FDM + API REST

Snort3, supporto multi-istanza/contesto e HA/clustering

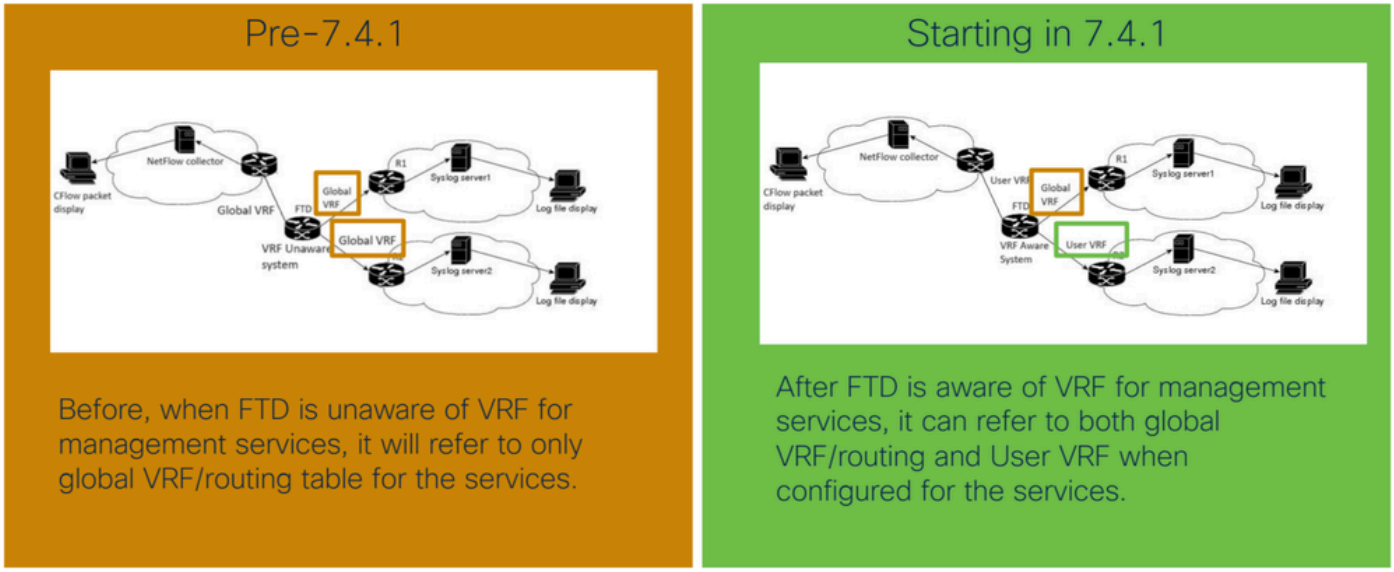


Nota: Funziona con server syslog IPv4 e IPv6. IPv6 non è ancora supportato nel server ftp Syslog.

- Supportato con Multi-instance.
- Supportato con dispositivi HA'd.
- Supportato su dispositivi del cluster.

Configurazione

Esempio di rete



Confronto tra schemi di rete precedenti e successivi alla 7.4.

Configurazioni

VRF (Virtual Routing and Forwarding) è una tecnologia utilizzata nelle reti per consentire la coesistenza di più istanze di una tabella di routing all'interno dello stesso router e fornire l'isolamento della rete tra reti virtuali diverse. Ogni istanza VRF è indipendente dalle altre e il traffico tra di esse viene mantenuto separato. Multi-VRF è una funzionalità che consente ai provider di servizi di supportare più VPN e servizi, anche se i relativi indirizzi IP si sovrappongono. Utilizza interfacce di input per designare percorsi per vari servizi e creare tabelle di inoltro pacchetti virtuali assegnando interfacce di layer 3 a ciascun VRF. I servizi di gestione (Syslog, NetFlow) utilizzano il VRF globale come impostazione predefinita. Gli utenti desiderano utilizzare la VRF utente per i servizi di gestione e la VRF globale, in quanto non tutte le destinazioni di caricamento sono raggiungibili tramite la VRF globale.

In questo documento, Globale + Utente VRF = Multi-VRF

Abilitare Syslog per VRF utente.

- Syslog può utilizzare il servizio ftp in un contesto multi VRF.

Come funziona

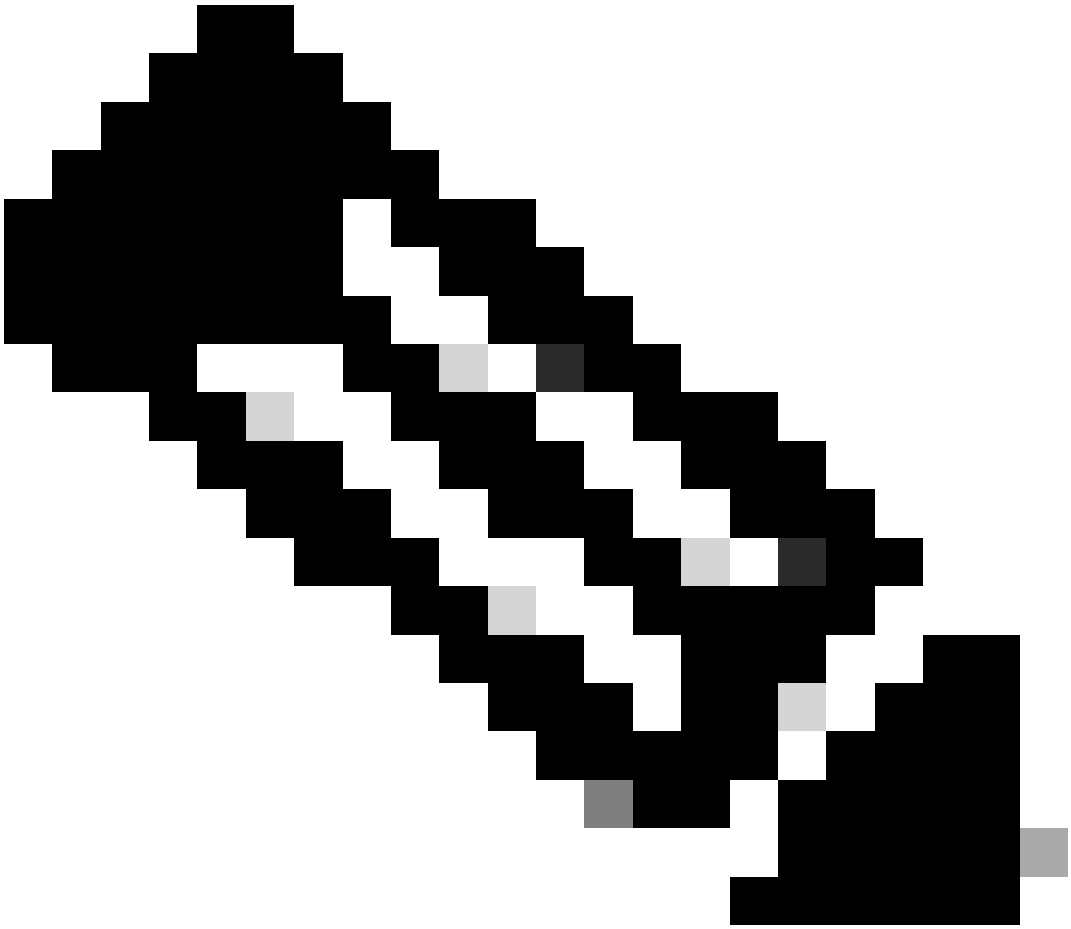
Quando l'interfaccia è configurata con VRF utente, la ricerca della route viene eseguita nel dominio di routing VRF anziché nel dominio di routing globale predefinito.

- Sono supportati due tipi di configurazioni server:

1. Inviare messaggi di registrazione ai server Syslog per monitorare e risolvere i problemi relativi al traffico di rete.
2. Invio del contenuto del buffer di registro a un server FTP come file di testo

- Syslog invia i log ai rispettivi server UDP/TCP all'interno del VRF.
- Per i syslog di wrapping del buffer, i log vengono inviati al server FTP configurato all'interno

di tale VRF.

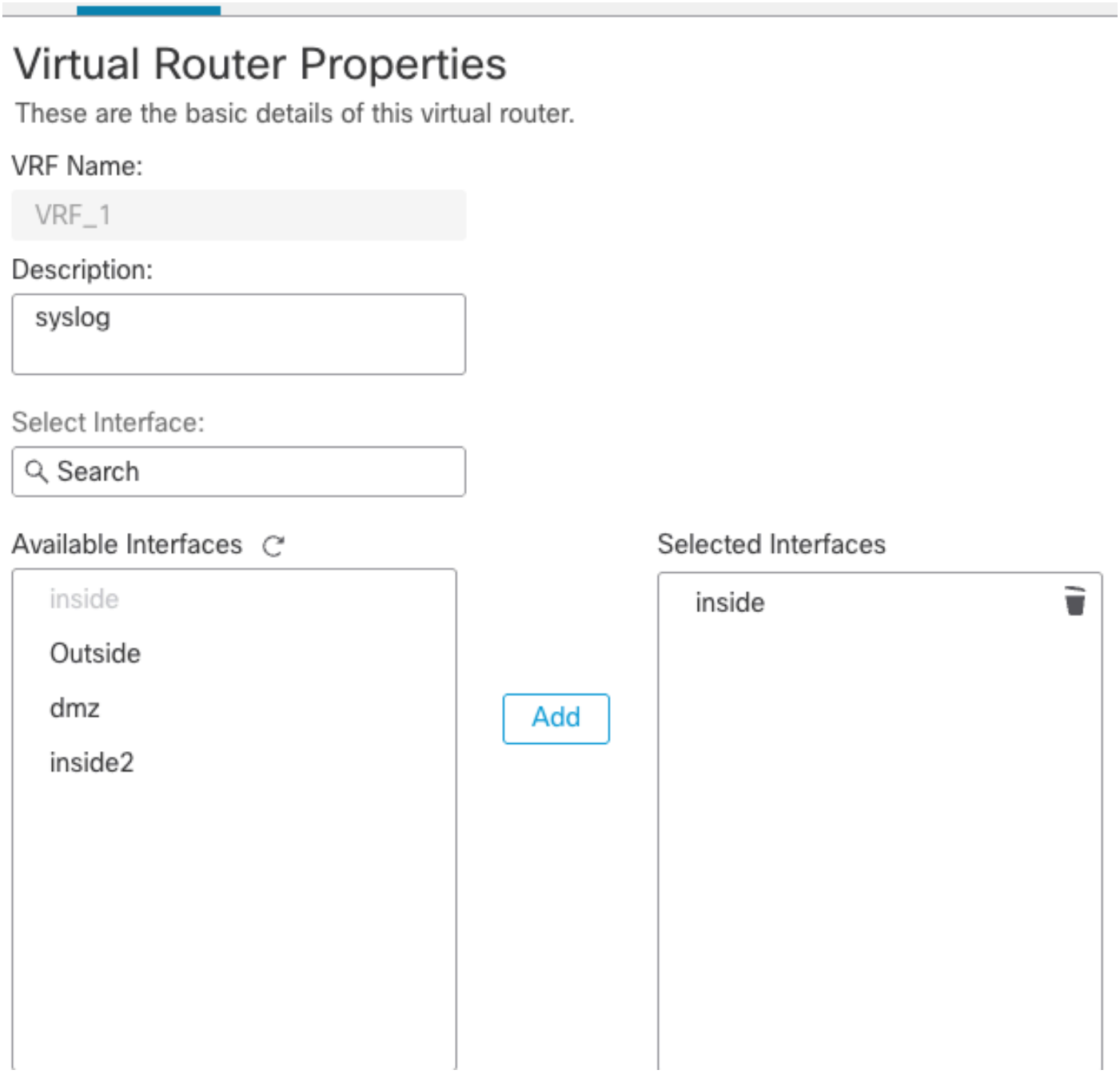


Nota: Il server Syslog e il server FTP possono far parte di diversi VRF.

Configurazione router virtuale

Passaggio 1. Creare un VRF

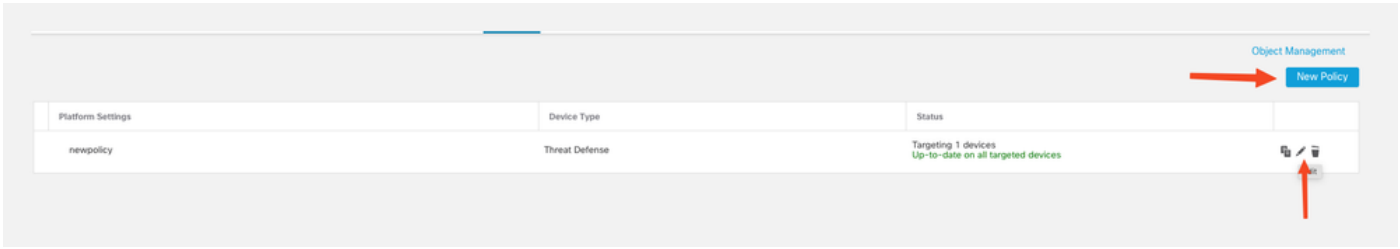
- Accedere a FMC e selezionare Device > Device Management (Gestione dispositivi).
- Selezionare la periferica e fare clic sull'icona Matita per modificarla.
- Selezionare Routing> Manage Virtual Router > Add Virtual Router.
- Immettere il nome in Nome VRF.
- Selezionare l'interfaccia e fare clic su Add and Save.



Aggiunta dell'interfaccia al VRF

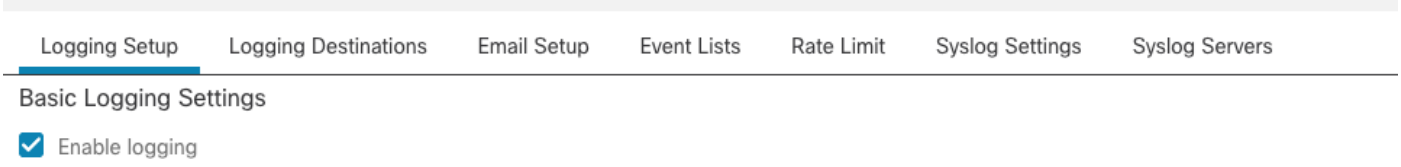
Passaggio 2. Configurare l'impostazione della registrazione.

- Selezionare Dispositivi > Impostazioni piattaforma.
- Creare un nuovo criterio o modificare l'icona Matita nel criterio esistente.



Creazione delle impostazioni della piattaforma

- Selezionare Impostazione registrazione e Attiva registrazione.

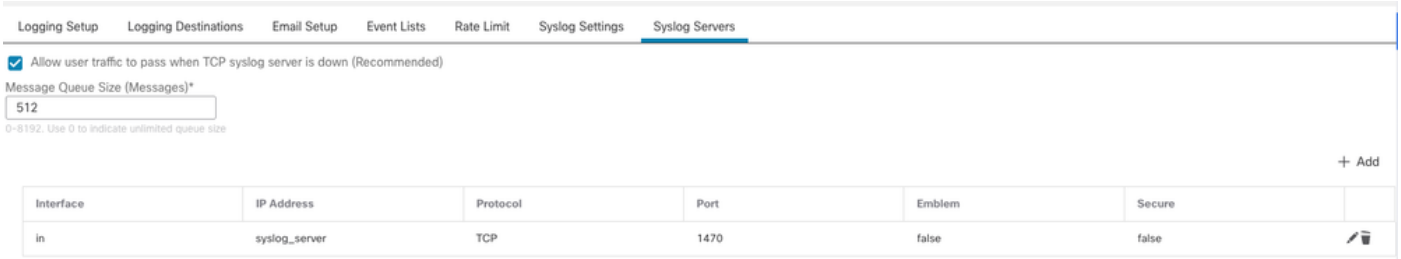


Abilita registrazione

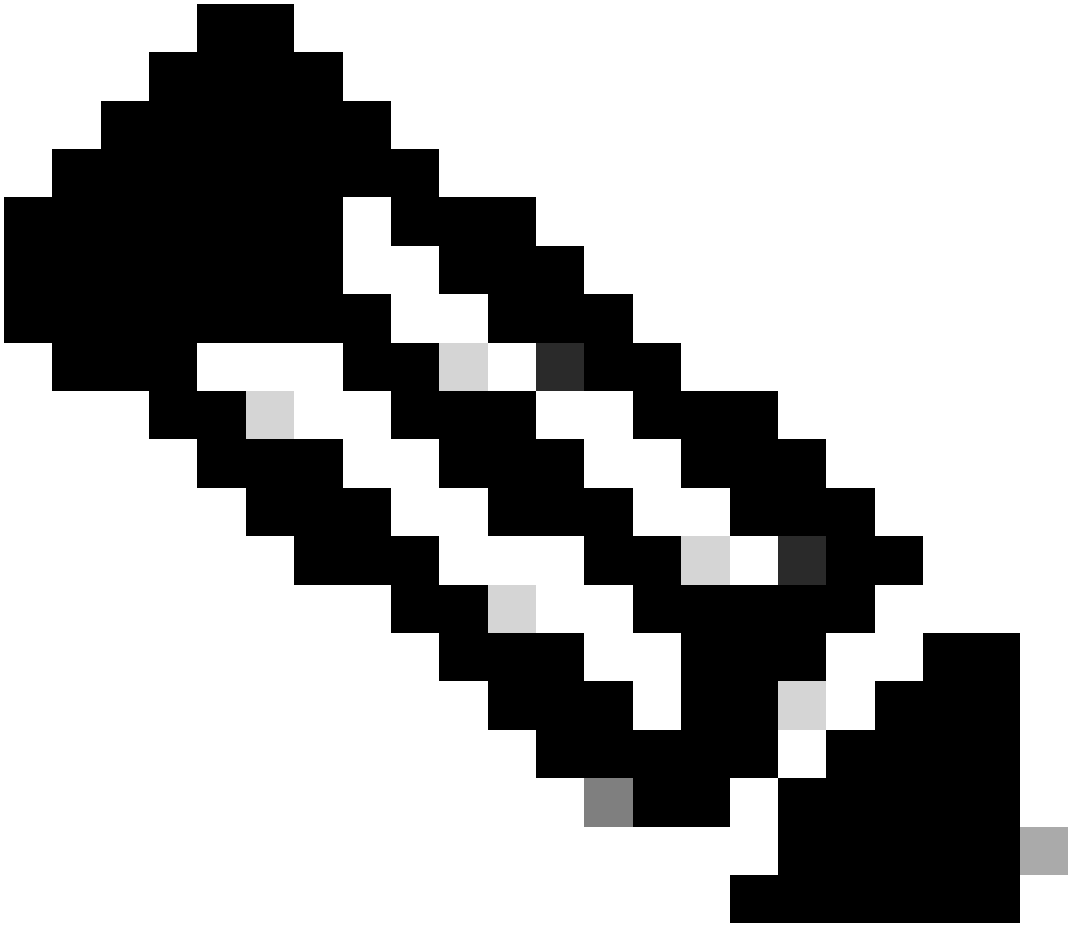
- Selezionare Logging Destination (Destinazione registrazione) e fare clic su Add (Aggiungi).
- Impostare la destinazione di registrazione come server Syslog.

Registrazione della destinazione come server syslog

- Selezionare Syslog Server > Aggiungi.



Aggiunta di Syslog Server con interfaccia compatibile con VRF



Nota: L'interfaccia interna fa parte dell'area di sicurezza di.

- L'interfaccia configurata nel comando host di registrazione ora riconosce VRF.
- Fare clic su Save (Salva).

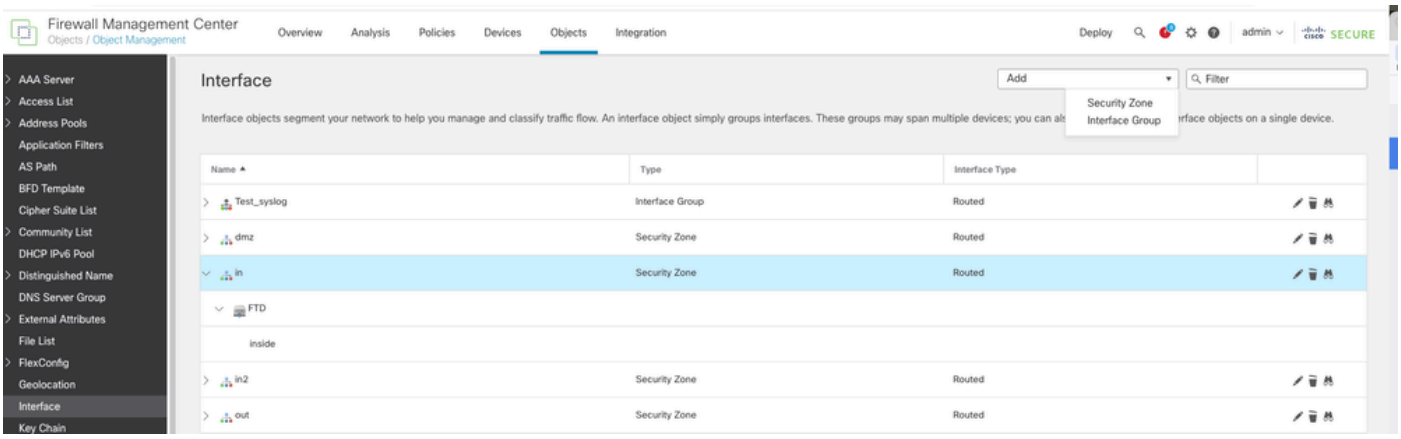
Prerequisiti per la configurazione del server FTP in FMC

- Utilizza oggetto gruppo interfaccia.
- L'oggetto gruppo di interfacce può avere sia VRF utente che globale.

Configurazione

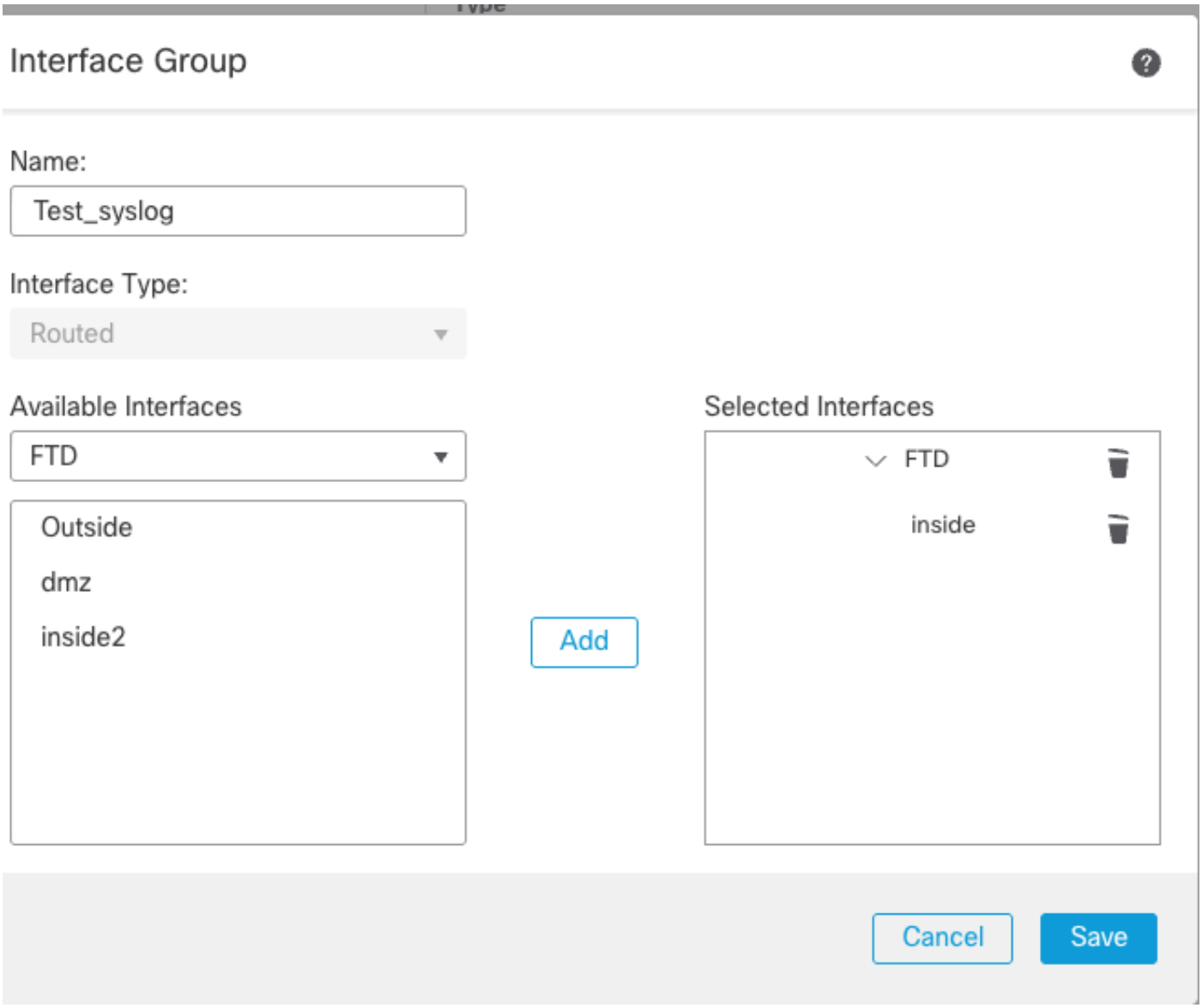
Passaggio 1.

- Passare a Oggetto > Gestione oggetti > Interfaccia > Aggiungi > Gruppo di interfacce.



Aggiunta del gruppo di interfacce

- Selezionare il dispositivo dal menu a discesa e aggiungere l'interfaccia VRF.



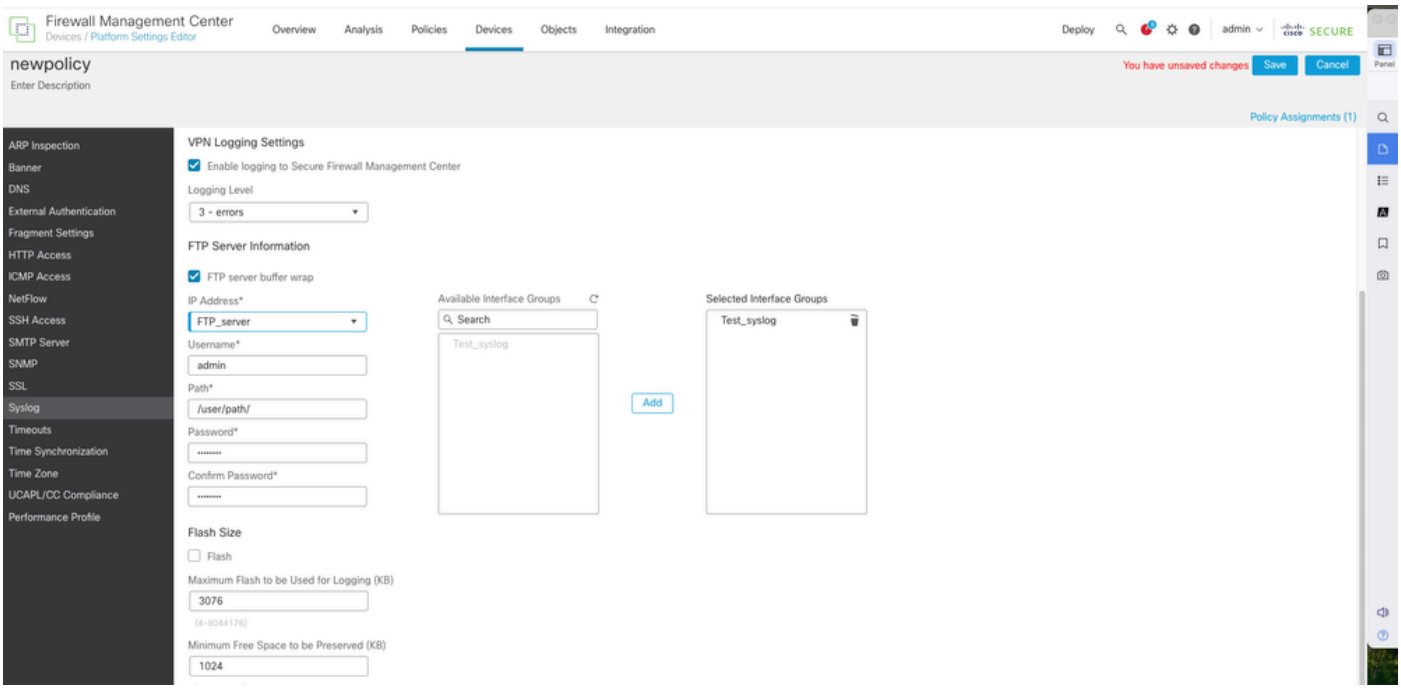
Aggiunta dell'interfaccia compatibile con VRF

Passaggio 2.

- Selezionare Dispositivi > Impostazioni piattaforma > Syslog > Impostazione registrazione.

Abilitare il wrapping del buffer del server FTP.

- Fare clic su Save (Salva).



Abilita server FTP con interfaccia compatibile con VRF

Verifica

Punto 7.4.1

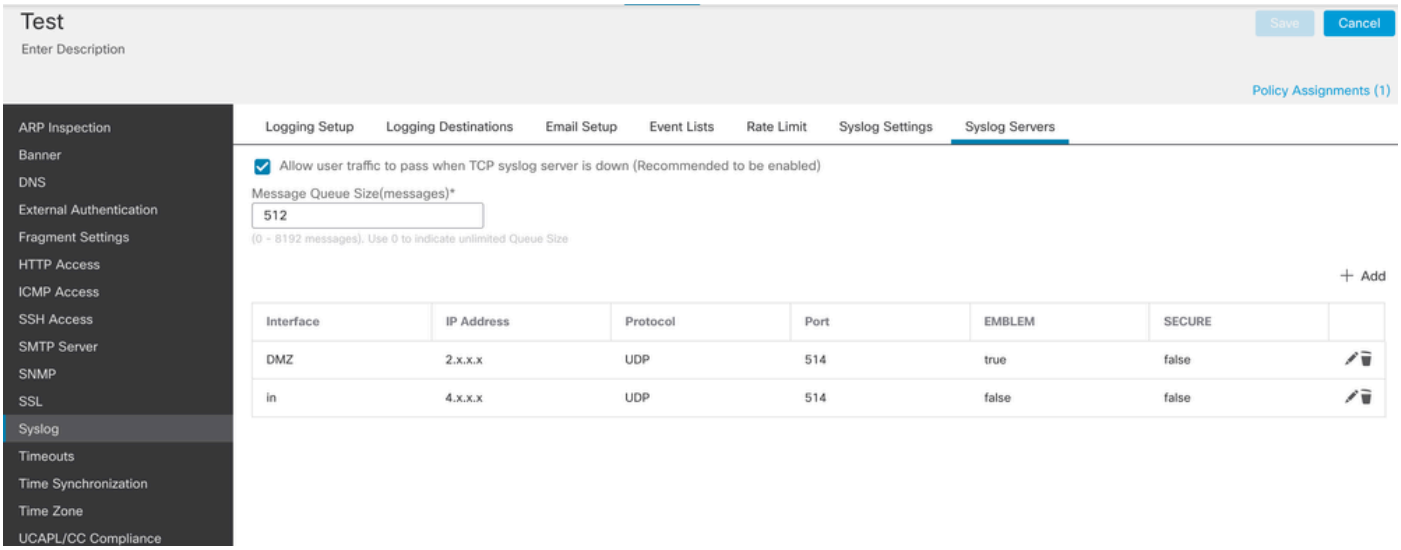
In questa prova, FTD e FMC sono 7.0.5.

FTD è configurato con VRF e l'interfaccia dmz è stata assegnata a VRF.

L'interfaccia dmz è configurata con l'host di registrazione del server syslog.

Inoltre, l'interfaccia interna è configurata con l'impostazione syslog.

L'interfaccia interna fa parte di Global VRF.

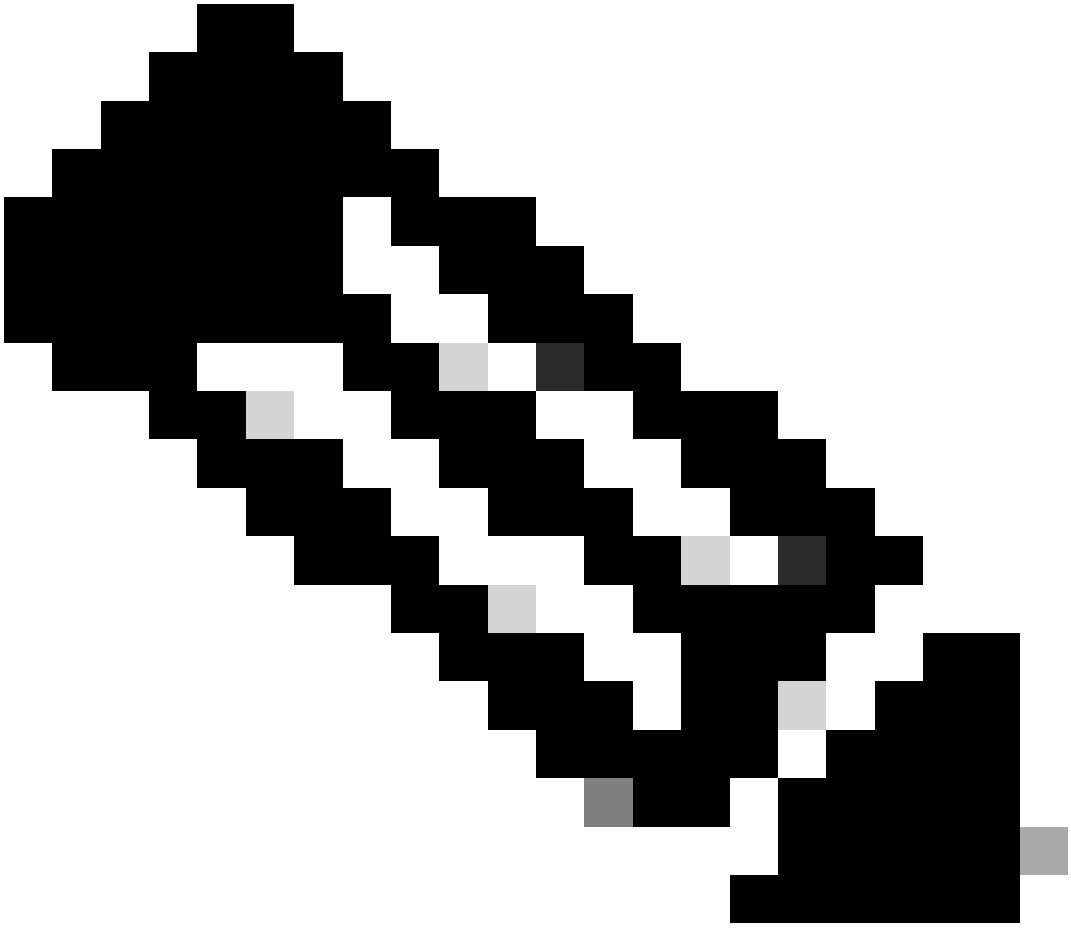


Impostazione di Syslog Server su FMC 7.0.5

Verifica 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
```



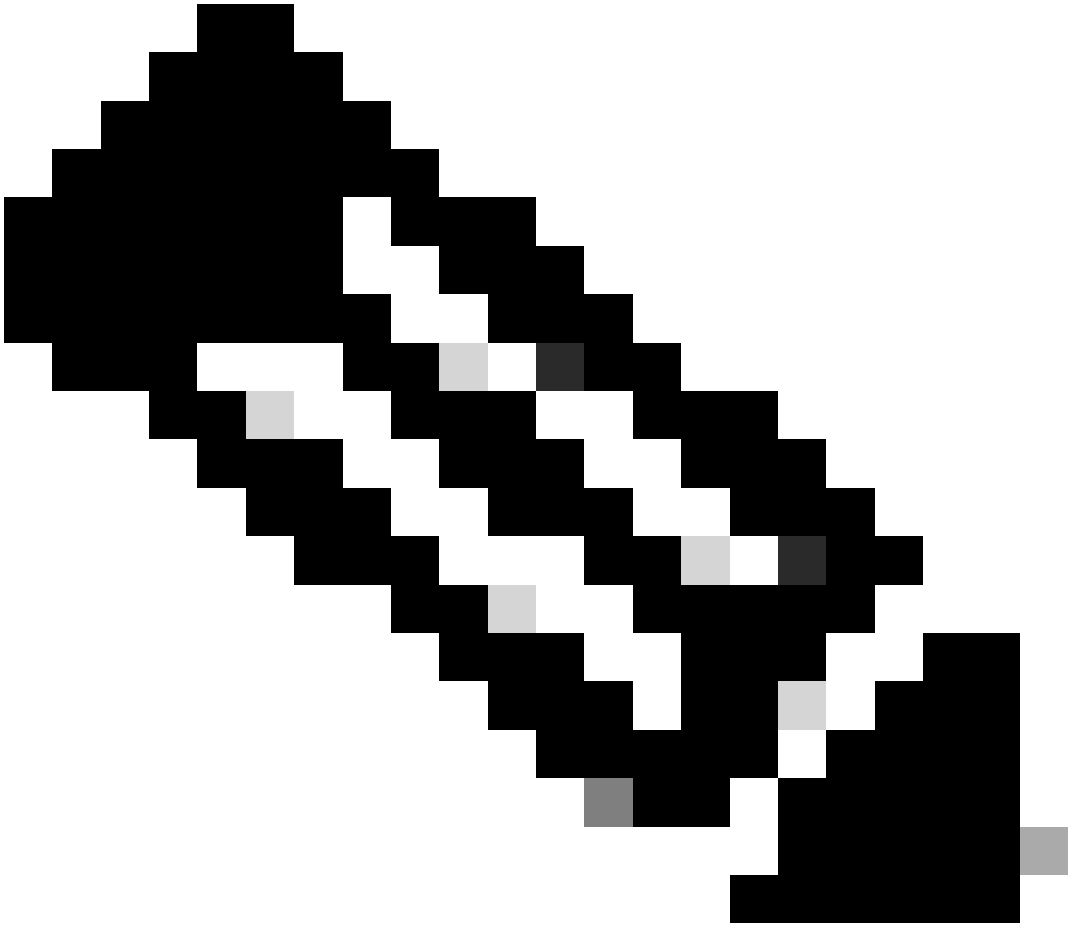
Nota: Il server Syslog con destinazione 2.x.x.x non è disponibile nell'impostazione di registrazione per la CLI FTD. Questo fa parte di User VRF.
Il server Syslog con destinazione 4.x.x.x è disponibile nell'impostazione di registrazione per la CLI FTD. Questo fa parte di Global VRF.

Post 7.4.1

Verifica 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
```



Nota: L'host del server Syslog 192.x.x.x utilizza l'interfaccia interna con riconoscimento VRF.

Verifica server FTP

Punto 7.4.1

- In FMC, l'impostazione del server FTP non consente di selezionare l'interfaccia da utilizzare. È disponibile solo l'indirizzo IP dell'opzione server 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)

3076

(4-8044176)

Minimum free Space to be preserved(KB)

1024

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).