FTD에서 VRF 인식 Syslog 구성

목차

소개

이 문서에서는 FTD의 VRF 인식 syslog에 대한 컨피그레이션 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Syslog
- FTD(Firepower Threat Defense)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

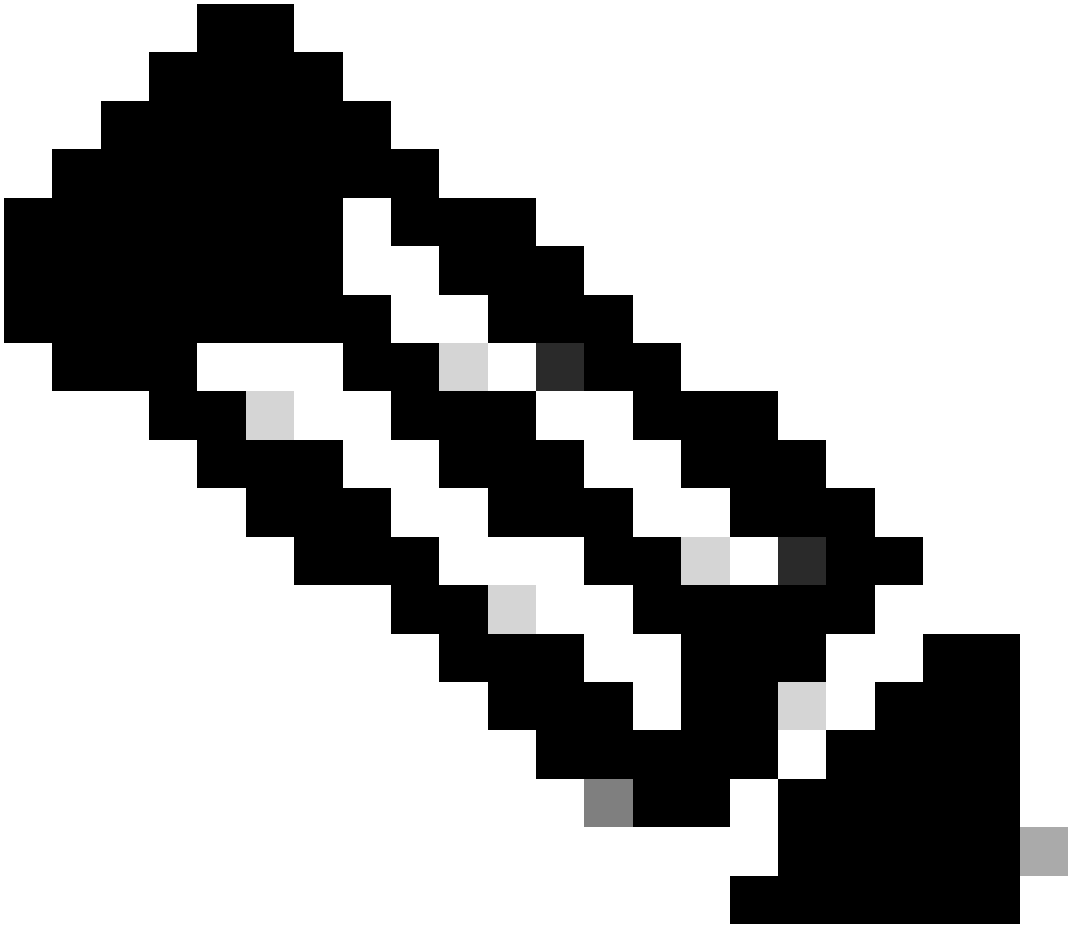
- FMCv(Secure Firewall Management Center) v7.4.2
- FTDv(Secure Firewall Threat Defense Virtual) v7.4.2

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

최소 소프트웨어 및 하드웨어 플랫폼

- 응용 프로그램 및 최소 버전: Secure Firewall 7.4.1
- 지원되는 관리 플랫폼 및 버전: 모두 FTD 7.4.1을 지원합니다.
- 관리자:
  1) FMC on-perm + FMC REST API
  2) 클라우드 기반 FMC
  3) FDM + REST API

Snort3, 다중 인스턴스/컨텍스트 및 HA/클러스터링 지원

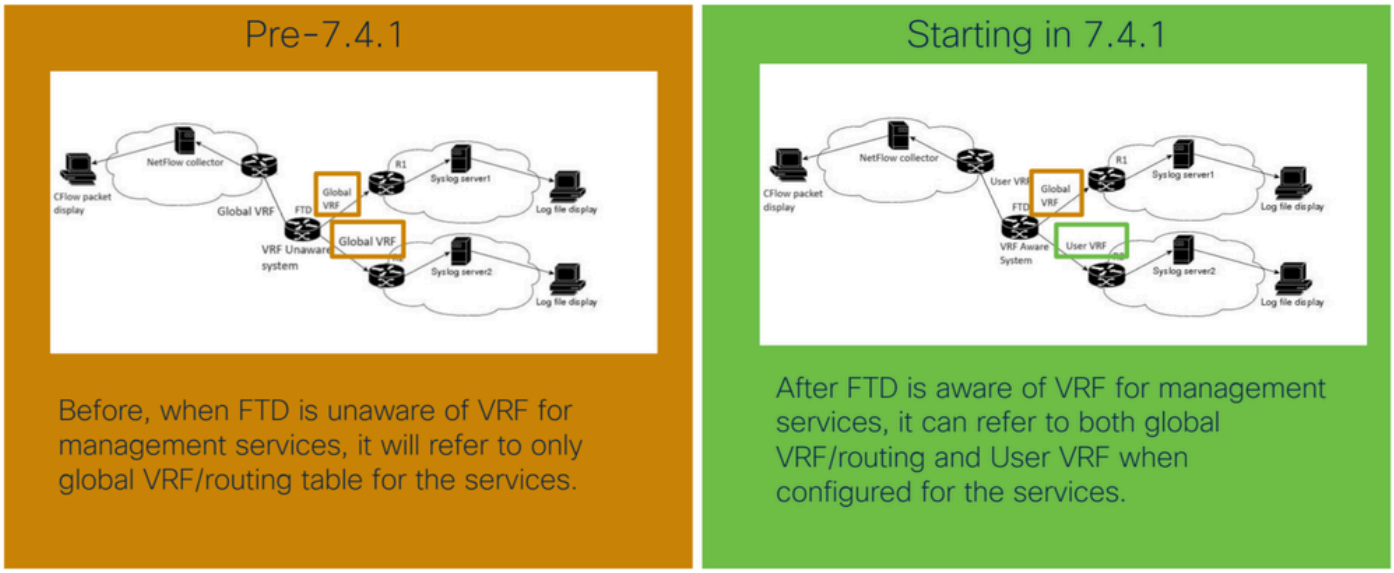


참고: IPv4 및 IPv6 syslog 서버 모두에서 작동합니다. IPv6는 Syslog ftp 서버에서 아직 지원되지 않습니다.

- 다중 인스턴스에서 지원됩니다.
- HA 디바이스에서 지원됩니다.
- 클러스터링된 디바이스에서 지원됩니다.

구성

네트워크 다이어그램



사전 및 사후 7.4의 네트워크 다이어그램 비교.

설정

VRF(Virtual Routing and Forwarding)는 네트워킹에서 라우팅 테이블의 여러 인스턴스가 동일한 라우터 내에서 공존할 수 있도록 하여 서로 다른 가상 네트워크 간에 네트워크를 격리하는 기술입니다. 각 VRF 인스턴스는 다른 인스턴스와 독립적이며, 각 인스턴스 간의 트래픽은 별도로 유지됩니다. Multi-VRF는 서비스 공급자가 IP 주소가 겹치더라도 여러 VPN 및 서비스를 지원할 수 있도록 하는 기능입니다. 입력 인터페이스를 사용하여 다양한 서비스에 대한 경로를 지정하고 각 VRF에 레이어 3 인터페이스를 할당하여 가상 패킷 포워딩 테이블을 생성합니다. 관리 서비스(Syslog, NetFlow)는 글로벌 VRF를 기본값으로 사용합니다. 모든 업로드 대상이 전역 VRF를 통해 연결할 수 있는 것은 아니므로 사용자는 전역 VRF뿐만 아니라 관리 서비스에 사용자 VRF를 사용하려고 합니다.

이 문서에서 글로벌 + 사용자 VRF = 다중 VRF

사용자 VRF에 대해 Syslog를 활성화합니다.

- Syslog는 다중 VRF 컨텍스트에서 ftp 서비스를 사용할 수 있습니다.

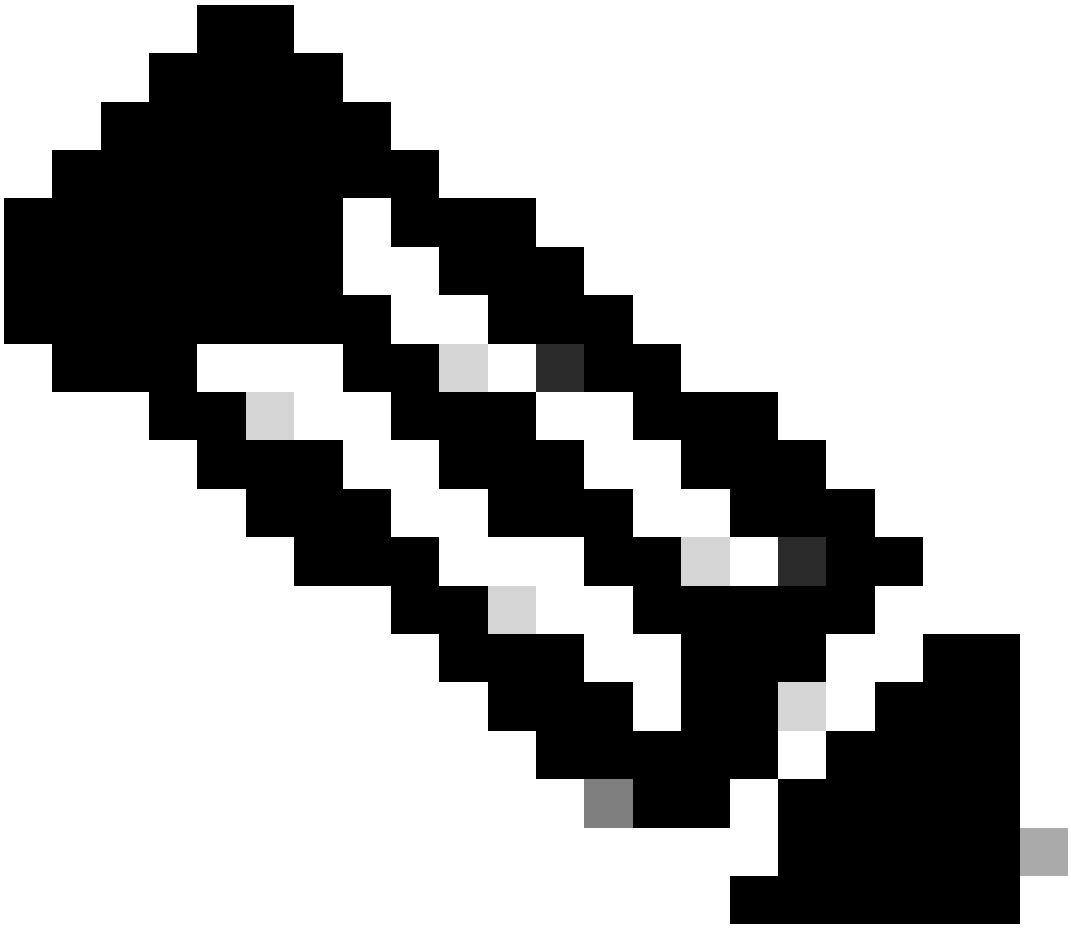
운영 방식

인터페이스가 사용자 VRF로 구성된 경우, 기본 전역 라우팅 도메인이 아닌 VRF 라우팅 도메인에서 경로 조회가 발생합니다.

- 두 가지 유형의 서버 컨피그레이션이 지원됩니다.

1. 네트워크 트래픽을 모니터링하고 문제를 해결하려면 로깅 메시지를 Syslog 서버로 전송합니다.
2. 로그 버퍼 내용을 FTP 서버에 텍스트 파일로 보냅니다.

- Syslog는 해당 VRF 내의 각 UDP/TCP 서버로 로그를 방출합니다.
- 버퍼 랩 syslog의 경우, 로그는 해당 VRF 내의 구성된 FTP 서버로 전송됩니다.



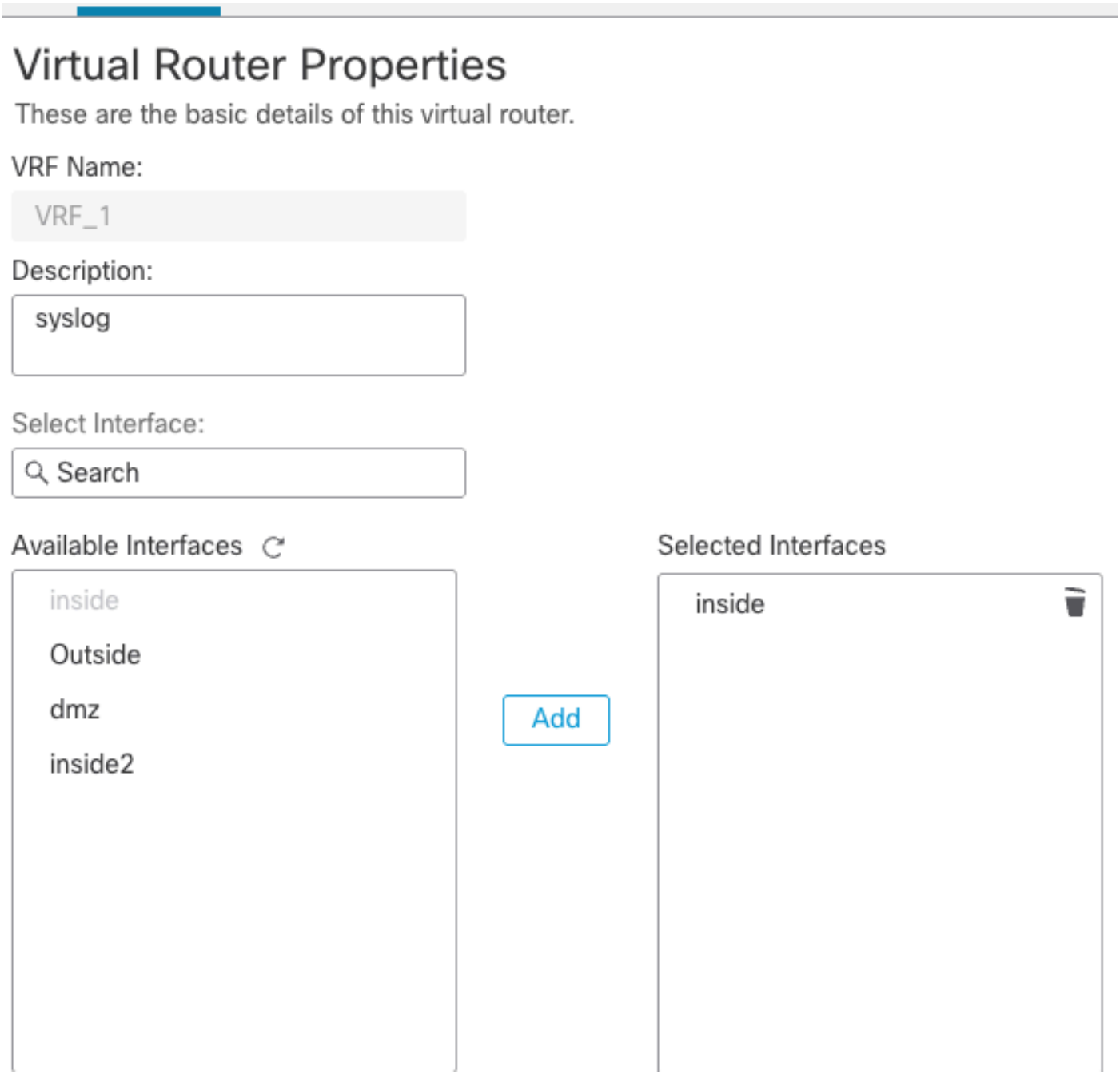
참고: Syslog 서버와 FTP 서버는 서로 다른 VRF에 속할 수 있습니다.

가상 라우터 구성

1단계. VRF 생성

- FMC에 로그인하고 Device(디바이스) > Device Management(디바이스 관리)로 이동합니다.
- 디바이스를 선택하고 연필 아이콘을 클릭하여 수정합니다.

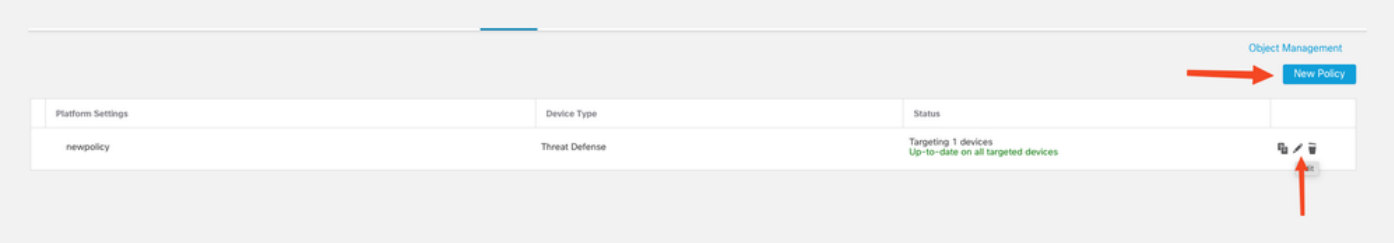
- Routing(라우팅) > Manage Virtual Router(가상 라우터 관리) > Add Virtual Router(가상 라우터 추가)로 이동합니다.
- VRF Name(VRF 이름)에 이름을 입력합니다.
- 인터페이스를 선택하고 Add and Save를 클릭합니다.



VRF에 인터페이스 추가

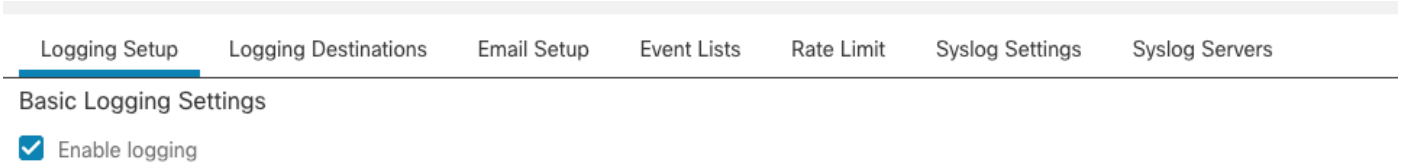
2단계. 로깅 설정을 구성합니다.

- Devices(디바이스) > Platform Settings(플랫폼 설정)로 이동합니다.
- 새 정책을 생성하거나 기존 정책에서 연필 아이콘을 수정합니다.



플랫폼 설정 생성

- Logging Setup 및 Enable logging을 선택합니다.

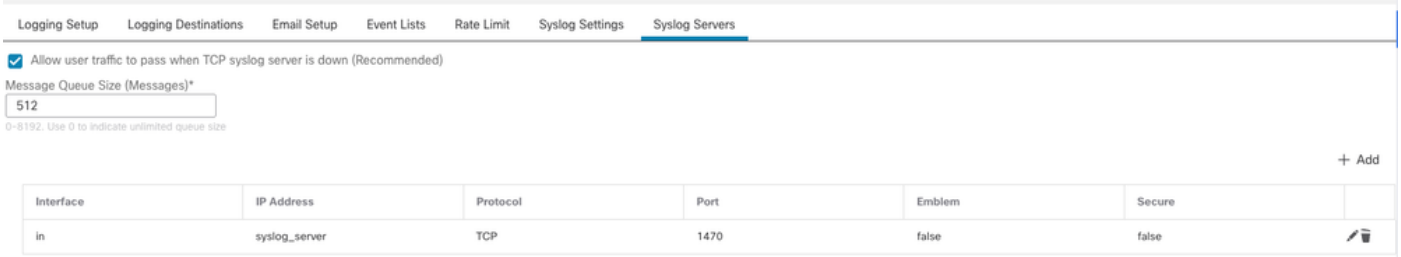


로깅 사용

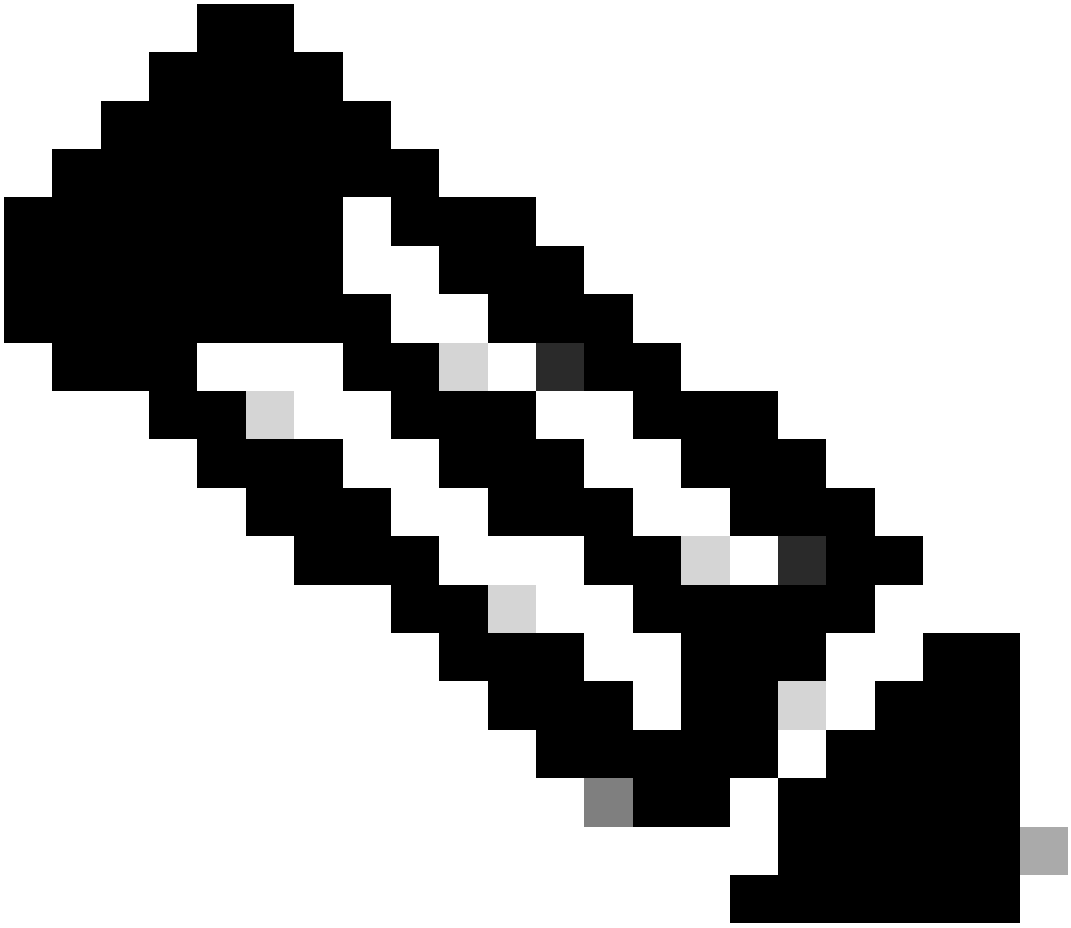
- Logging Destination을 선택하고 Add를 클릭합니다.
- 로깅 대상을 Syslog 서버로 설정합니다.

대상을 Syslog 서버로 로깅

- Syslog Servers(Syslog 서버) > Add(추가)를 선택합니다.



VRF 인식 인터페이스를 사용하여 Syslog 서버 추가



참고: 내부 인터페이스는 의 보안 영역에 속합니다.

- logging host 명령에 구성된 인터페이스가 이제 VRF를 인식합니다.
- 저장을 클릭합니다.

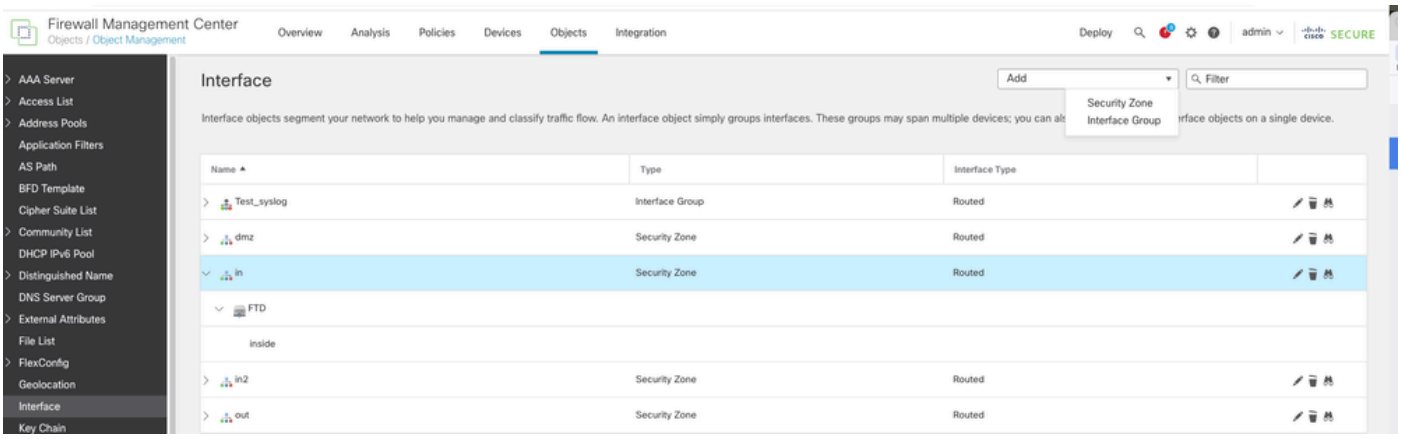
FMC에서 FTP 서버 컨피그레이션을 위한 사전 요구 사항

- 인터페이스 그룹 개체를 사용합니다.
- 인터페이스 그룹 개체는 사용자 VRF와 전역 VRF를 모두 가질 수 있습니다.

설정

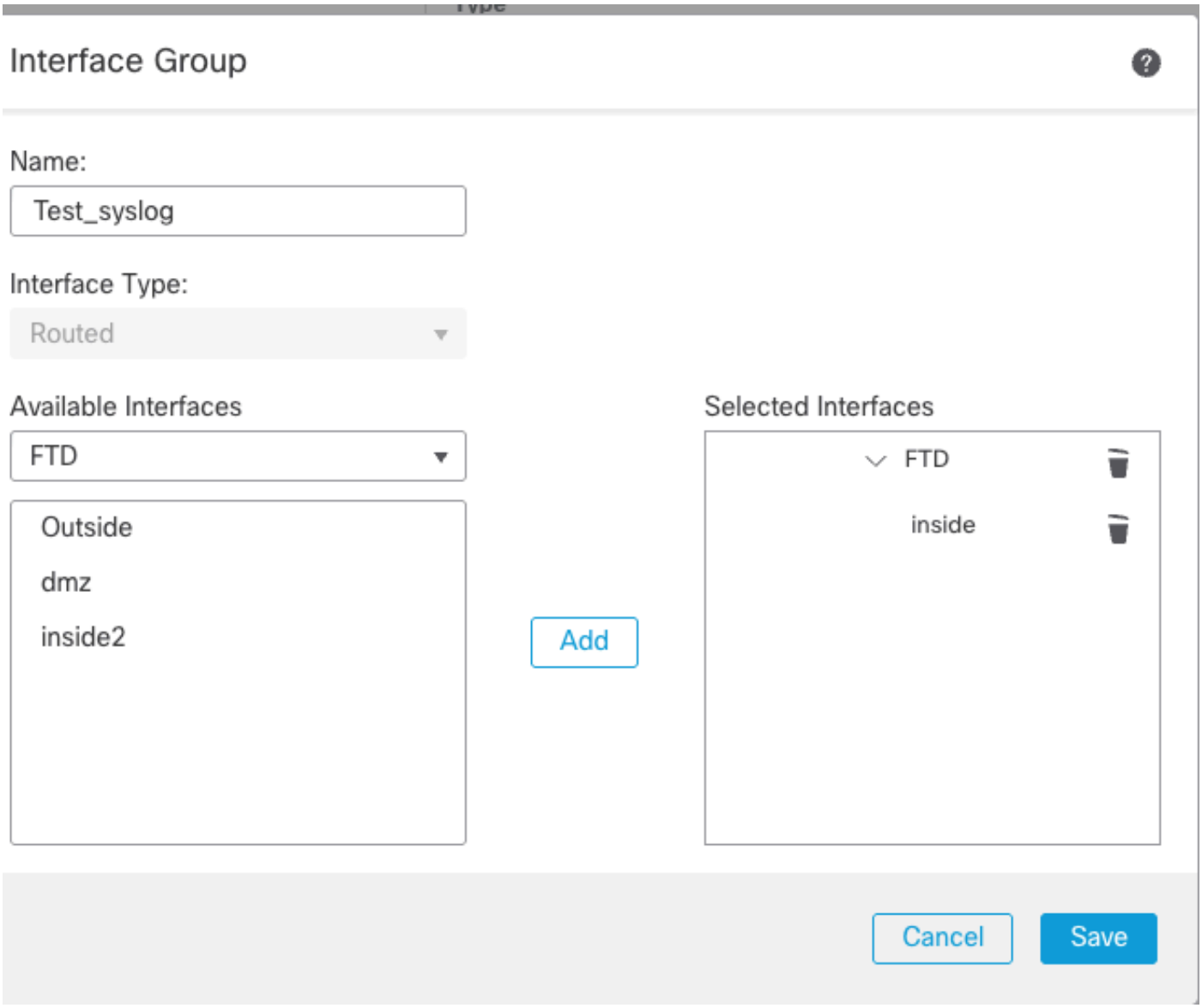
1단계.

- Object(개체) > Object Management(개체 관리) > Interface(인터페이스) > Add(추가) > Interface Group(인터페이스 그룹)으로 이동합니다.



인터페이스 그룹 추가

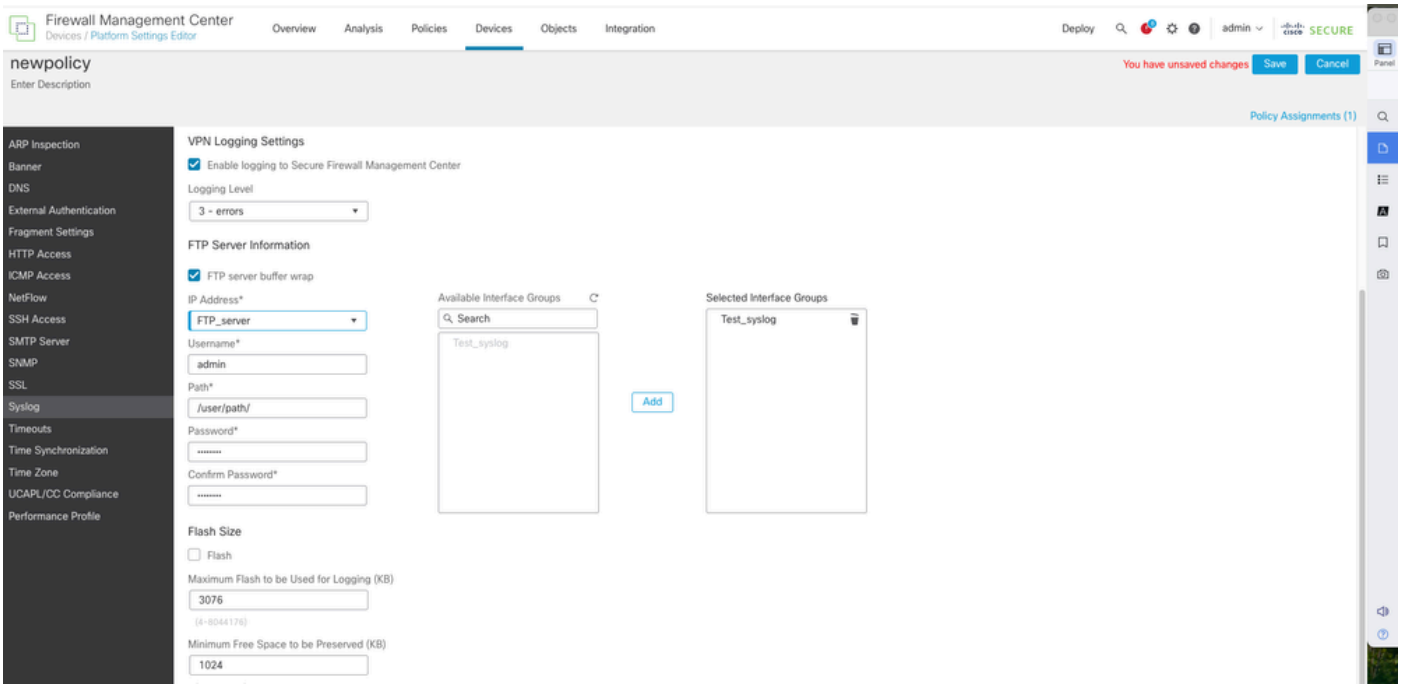
- 드롭다운에서 Device(디바이스)를 선택하고 Add the VRF Interface(VRF 인터페이스 추가)를 클릭합니다.



VRF 인식 인터페이스 추가

2단계.

- Devices(디바이스) > Platform Settings(플랫폼 설정) > Syslog > Logging Setup(로깅 설정)으로 이동합니다. FTP 서버 버퍼 랩을 활성화합니다.
- 저장을 클릭합니다.



VRF 인식 인터페이스를 사용하여 FTP 서버 활성화

다음을 확인합니다.

7.4.1 이전

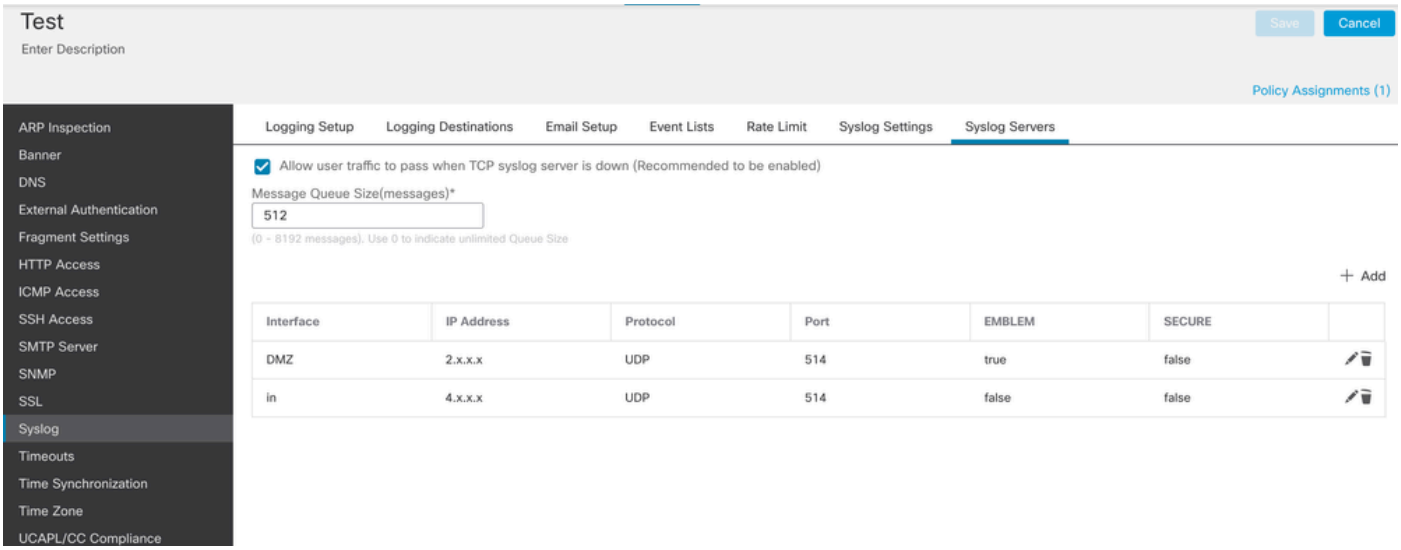
이 테스트에서 FTD와 FMC는 7.0.5입니다.

FTD가 VRF로 구성되고 dmz 인터페이스가 VRF에 할당되었습니다.

DMZ 인터페이스는 syslog 서버 로깅 호스트로 구성됩니다.

또한 내부 인터페이스는 syslog 설정으로 구성됩니다.

내부 인터페이스는 글로벌 VRF의 일부입니다.

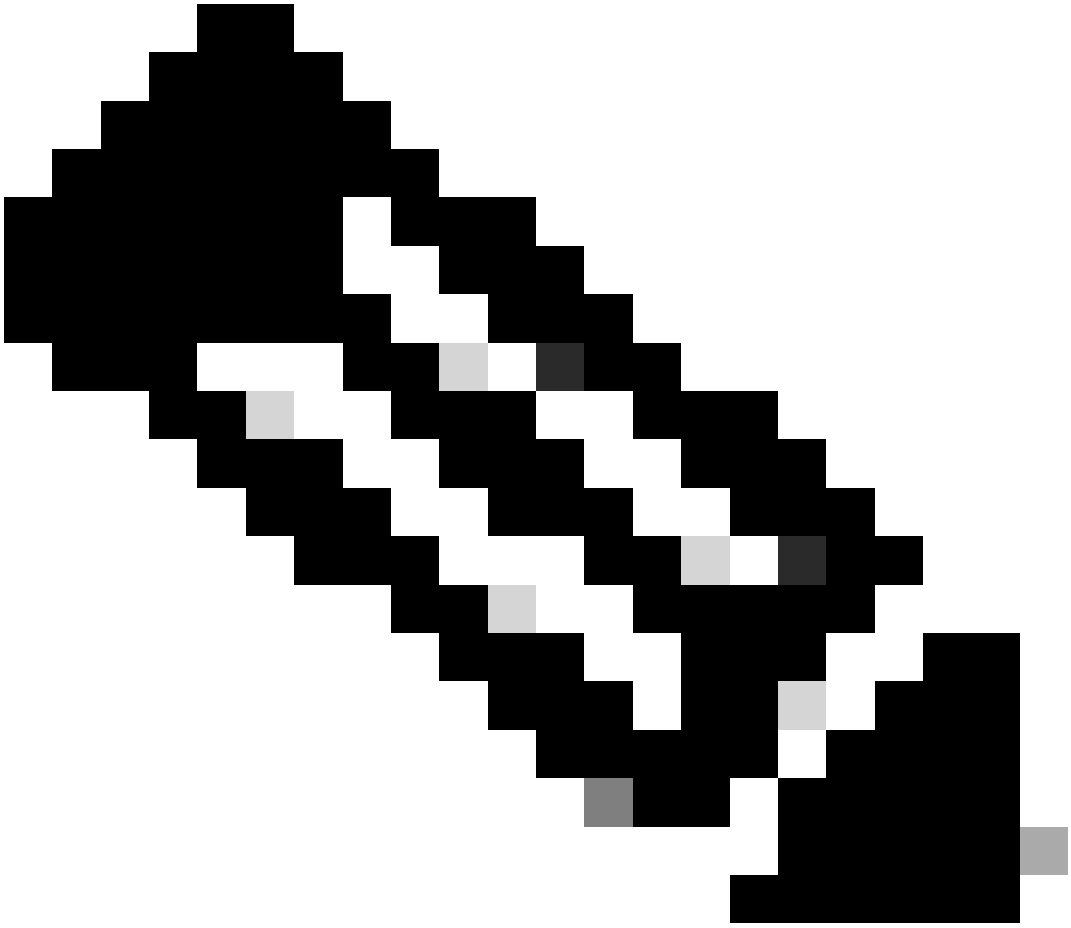


7.0.5 FMC의 Syslog 서버 설정

CLI 확인

```
> 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
```



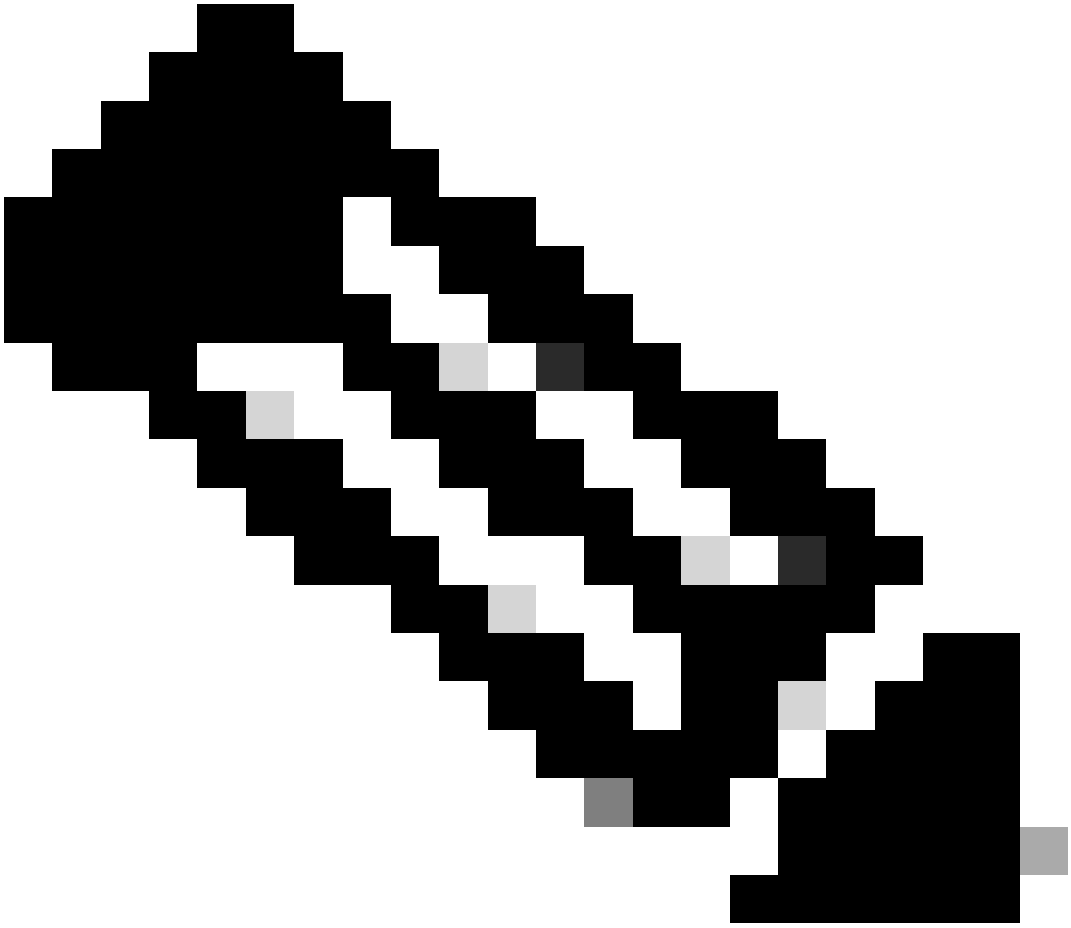
참고: 대상 2.x.x.x의 Syslog 서버는 FTD CLI에 대한 로깅 설정에서 사용할 수 없습니다. 사용자 VRF의 일부입니다.
대상 4.x.x.x의 Syslog 서버는 FTD CLI에 대한 로깅 설정에서 사용할 수 있습니다. 이는 글로벌 VRF의 일부입니다.

게시물 7.4.1

CLI 확인

```
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
```



참고: Syslog 서버 호스트 192.x.x.x가 VRF 인식 내부 인터페이스를 사용하고 있습니다.

FTP 서버 확인

7.4.1 이전

- FMC에서 FTP 서버 설정에는 사용할 인터페이스를 선택할 수 있는 옵션이 없습니다. syslog 서버 옵션의 IP 주소만 사용할 수 있습니다.

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

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.