# Syslog Over VPN 터널을 위한 FTD 데이터 인터페이스 구성

## 목차



## 소개

이 문서에서는 Cisco FTD 데이터 인터페이스를 VPN 터널을 통해 전송되는 Syslog의 소스로 구성하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco FTD(Secure Firewall Threat Defense)의 Syslog 컨피그레이션
- 일반 시스템 로그
- Cisco FMC(Secure Firewall Management Center)

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco FTD 버전 7.3.1
- Cisco FMC 버전 7.3.1

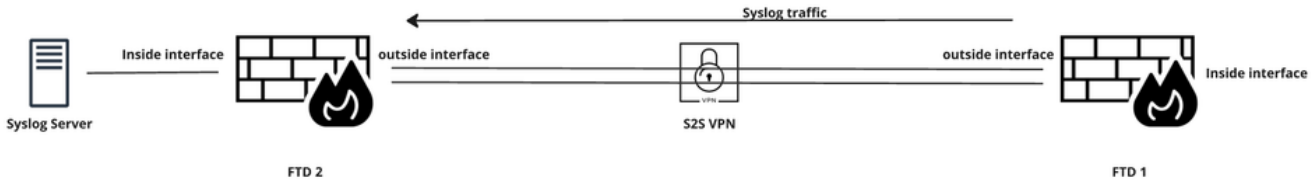
경고문: 이 문서에서 참조하는 네트워크 및 IP 주소는 개별 사용자, 그룹 또는 조직과 연결되어 있지 않습니다. 이 컨피그레이션은 랩 환경에서만 사용하도록 만들어졌습니다.

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.

## 배경 정보

이 문서에서는 VPN 터널을 통해 원격 사이트에 있는 Syslog 서버로 전송해야 하는 Syslog의 소스로 FTD의 데이터 인터페이스 중 하나를 사용하는 솔루션에 대해 설명합니다.

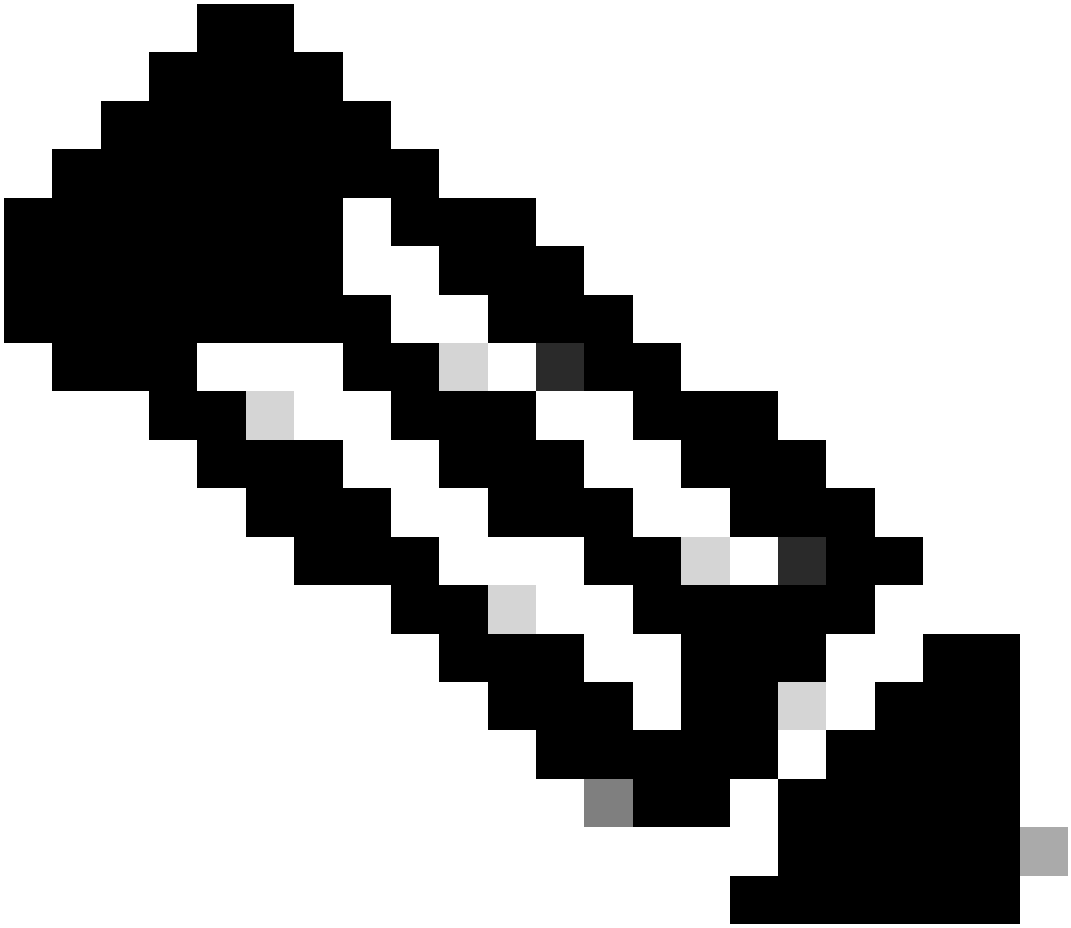
### 다이어그램



네트워크 다이어그램

터널을 통해 전송된 Syslog 트래픽을 소싱할 인터페이스를 지정하려면 Flex Config를 통해 **management-accesscommand**를 적용할 수 있습니다.

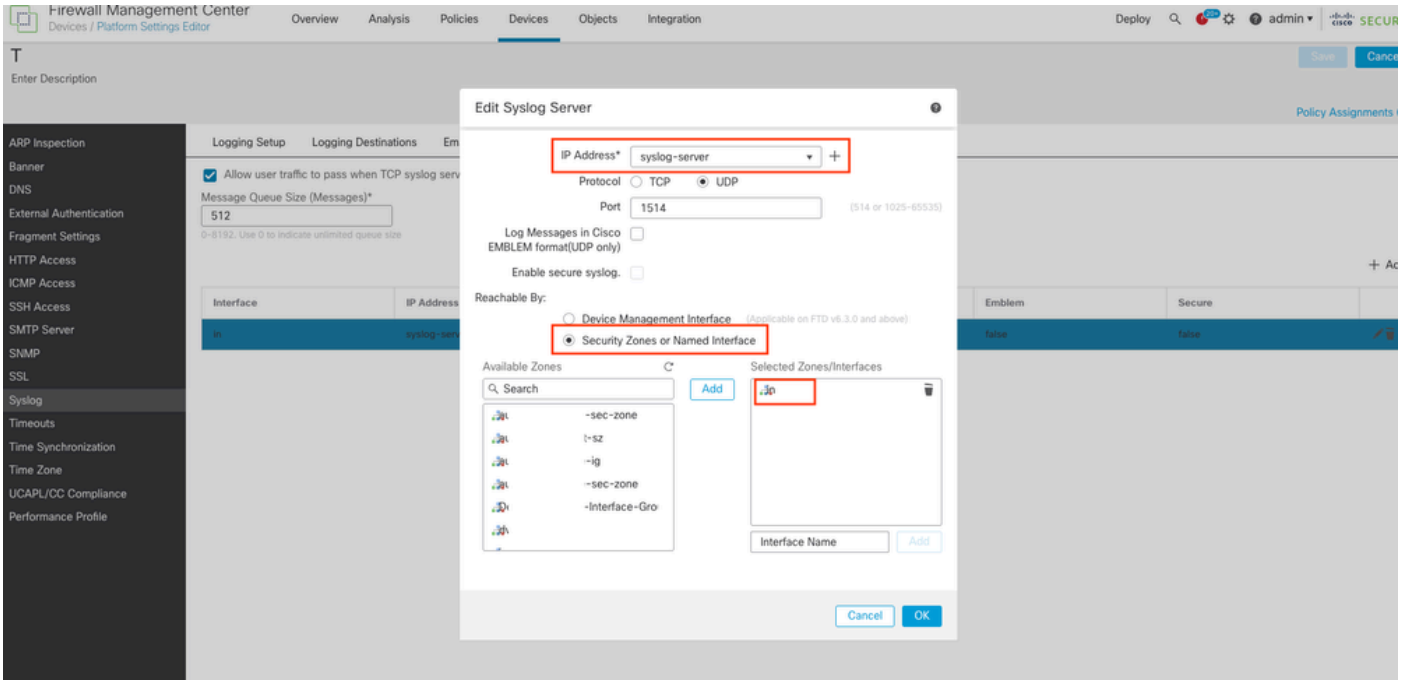
이 명령을 사용하면 VPN 터널을 통해 전송되는 Syslog 메시지에 대한 소스 인터페이스로 관리 액세스 인터페이스를 사용할 수 있을 뿐만 아니라, 전체 터널 IPsec VPN 또는 SSL VPN 클라이언트를 사용하거나 사이트 대 사이트 IPsec 터널을 통해 SSH 및 Ping을 통해 데이터 인터페이스에 연결할 수 있습니다.



참고: 관리 액세스 인터페이스는 하나만 정의할 수 있습니다.

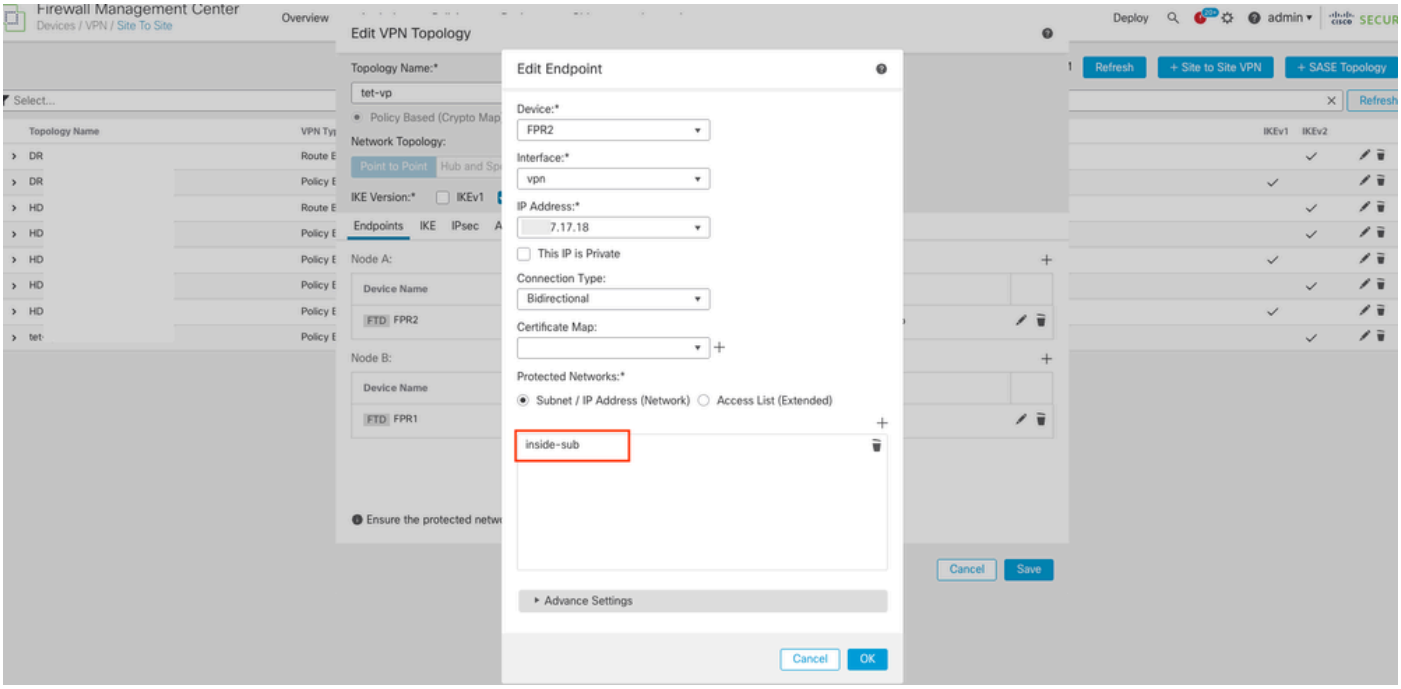
## 구성

1. Devices(디바이스) > Platform Settings(플랫폼 설정)에서 FTD에 대한 Syslog를 구성합니다. Syslog 서버를 구성하는 동안 Device Management Interface 대신 Security Zones 또는 Named Interface 옵션을 선택하고 Syslog 트래픽을 소싱할 management-access interface를 선택합니다.




Syslog 서버 컨피그레이션

2. VPN 엔드포인트의 Protected Networks(보호되는 네트워크) 아래에 관리 액세스 인터페이스 네트워크를 추가해야 합니다. (Devices(디바이스) > Site To Site(사이트 대 사이트) > VPN Topology(VPN 토폴로지) > Node(노드)에서).

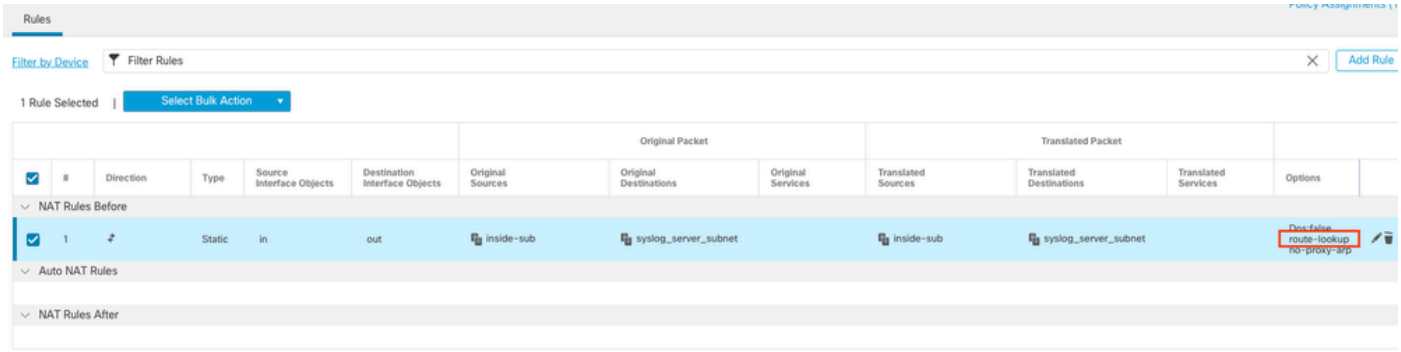



보호된 네트워크 컨피그레이션

3. 관리-액세스 인터페이스 네트워크와 VPN 네트워크 간에 아이덴티티 NAT를 구성해야 합니다(VPN 트래픽에 대한 일반적인 NAT 컨피그레이션). NAT 규칙의 Advanced(고급) 섹션에서 Perform Route Lookup for Destination Interface(대상 인터페이스에 대한 경로 조회 수행) 옵션을 선택해야 합니다.

경로 조회가 없으면 FTD는 라우팅 테이블의 내용과 상관없이 NAT 컨피그레이션에 지정된 인터페

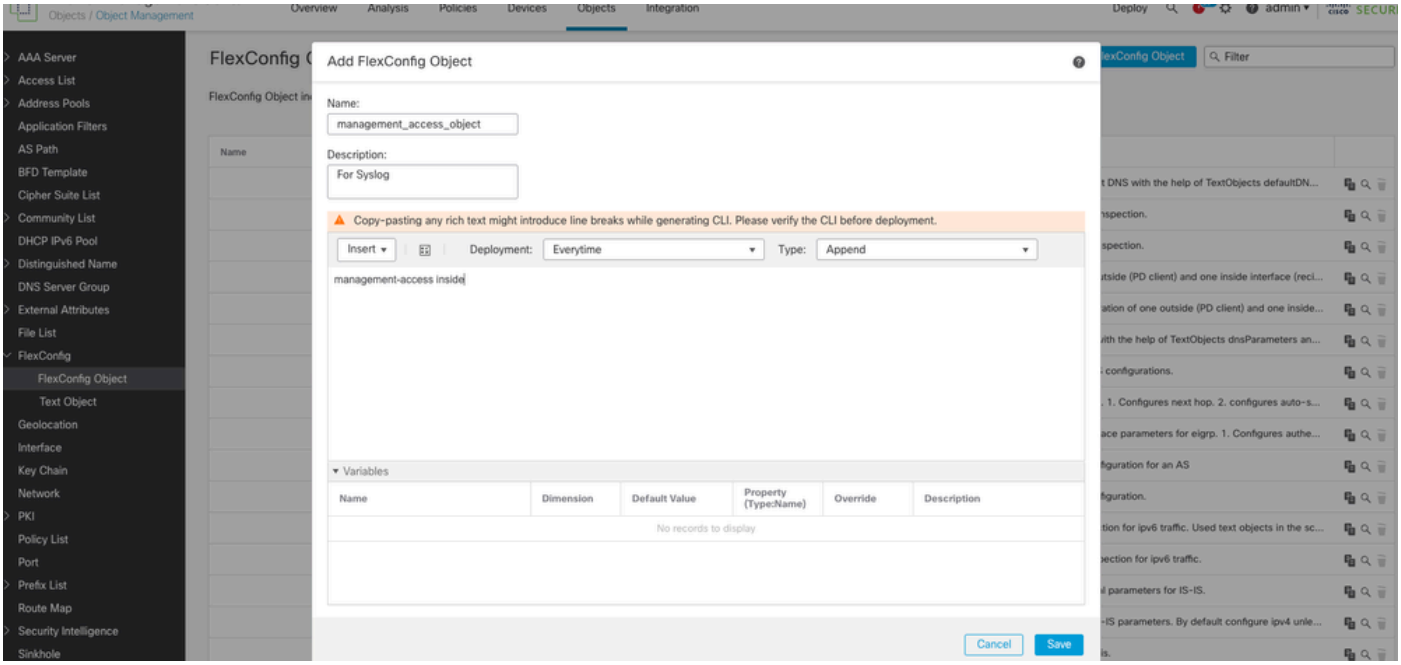
이스를 통해 트래픽을 전송합니다.




ID NAT 컨피그레이션

4. 이제 Objects > Object Management > FlexConfig Object 아래에서 management-access <interface name>(이 시나리오에서는 management-access inside)를 구성할 수 있습니다.

대상 디바이스 FlexConfig 정책에 할당하고 컨피그레이션을 구축합니다.




FlexConfig 컨피그레이션

## 다음을 확인합니다.

관리 액세스 구성:

```
<#root>

firepower#

show run | in management-access

management-access inside
```

Syslog 구성:

<#root>

```
firepower#

show run logging


logging enable
logging timestamp
logging trap debugging
logging FMC MANAGER_VPN_EVENT_LIST

logging host inside 192.168.17.17 17/1514


logging debug-trace persistent
logging permit-hostdown
logging class vpn trap debugging
```

VPN 터널을 통해 전송된 Syslog 트래픽:

<#root>

```
FTD 2:
firepower#

show conn


36 in use, 46 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

UDP vpn 192.168.17.17:1514 inside 10.17.17.18:514, idle 0:00:02, bytes 35898507, flags -

FTD 1:
firepower#

show conn


6 in use, 9 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

UDP server 192.168.17.17:1514 vpn 10.17.17.18:514, idle 0:00:00, bytes 62309790, flags -

firepower#

show crypto ipsec sa


interface: vpn
Crypto map tag: CSM_vpn_map, seq num: 1, local addr: 17.xx.xx.18

access-list CSM_IPSEC_ACL_2 extended permit ip 10.17.17.0 255.255.255.0 192.168.17.0 255.255.255.0
Protected vrf (ivrf):
```

```
local ident (addr/mask/prot/port): (10.17.17.0/255.255.255.0/0/0)

---------------> Inside interface subnet

remote ident (addr/mask/prot/port): (192.168.17.0/255.255.255.0/0/0)

------------> Syslog server subnet
current_peer: 17.xx.xx.17


#pkts encaps: 309957, #pkts encrypt: 309957, #pkts digest: 309957


#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 309957, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0
```

## 관련 정보

- FMC를 통해 FTD에 로깅 구성
- FMC에서 관리하는 FTD에서 사이트 대 사이트 VPN 구성

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.