FTD-gegevensinterface voor Syslog over VPN-tunnel configureren

Inhoud

Inleiding

Dit document beschrijft hoe u de Cisco FTD Data interface kunt configureren als bron voor syslogs die via een VPN-tunnel worden verzonden.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Syslog-configuratie op Cisco Secure Firewall Threat Defence (FTD)
- General Syslog
- Cisco Secure Firewall Management Center (FMC)

Gebruikte componenten

De informatie in dit document is gebaseerd op deze software- en hardwareversie:

- Cisco FTD versie 7.3.1
- Cisco FMC versie 7.3.1

Vrijwaring: de netwerken en IP-adressen waarnaar in dit document wordt verwezen, zijn niet gekoppeld aan individuele gebruikers, groepen of organisaties.

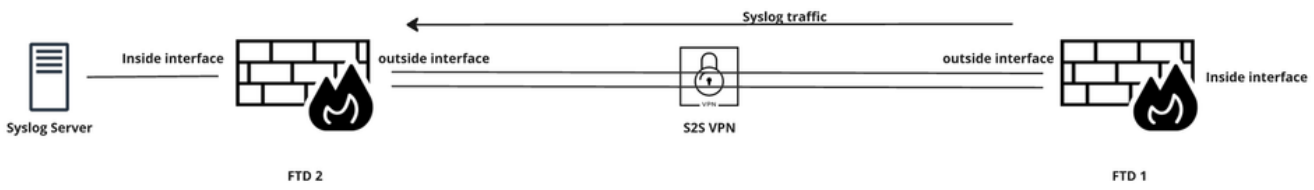
Deze configuratie is exclusief gemaakt voor gebruik in een laboratoriumomgeving.

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.

Achtergrondinformatie

Dit document beschrijft een oplossing voor het gebruik van een van de gegevensinterfaces van FTD als bron voor syslogs die via een VPN-tunnel naar Syslog Server moeten worden verzonden die zich op een externe site bevindt.

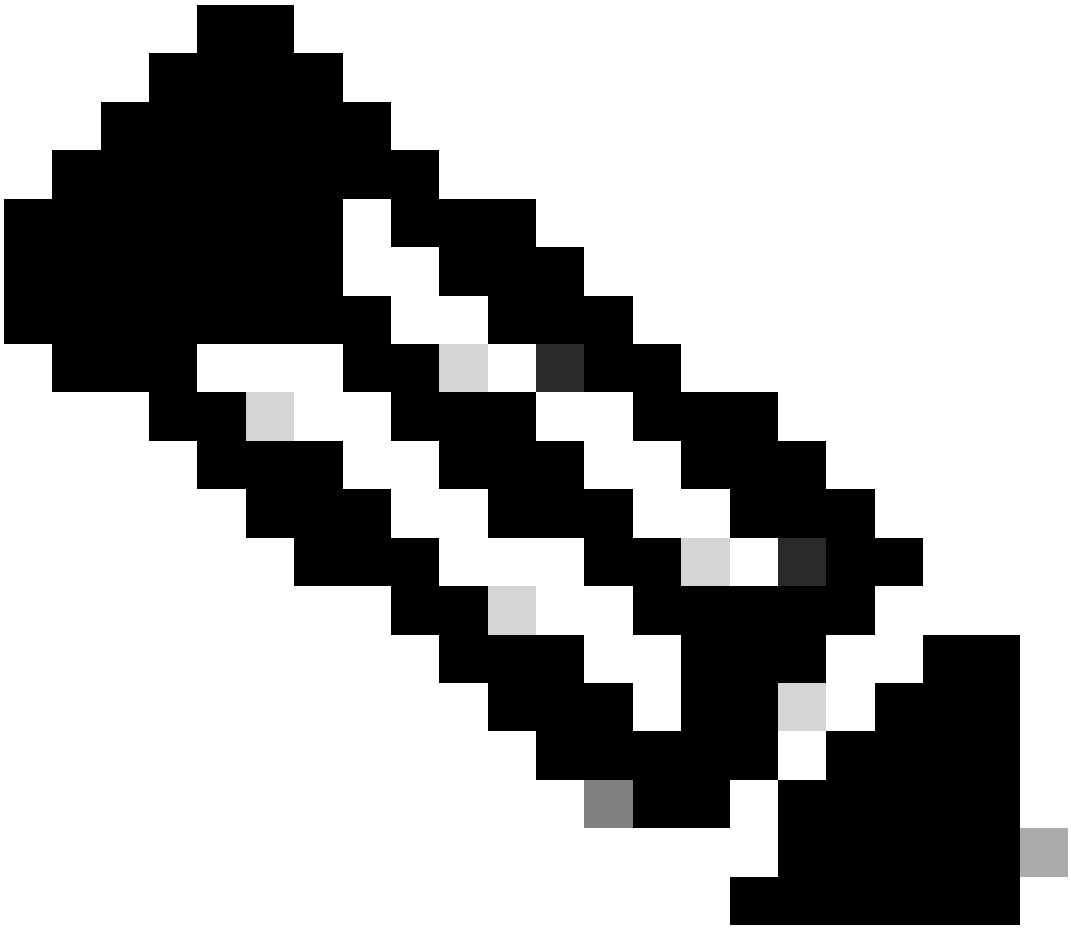
Diagram



Netwerkdiagram

Om de interface te specificeren van waaruit het Syslog-verkeer moet worden aangeschaft dat via de tunnel wordt verzonden, kunt u **beheer-**toegangsopdracht toepassen via Flex Config.

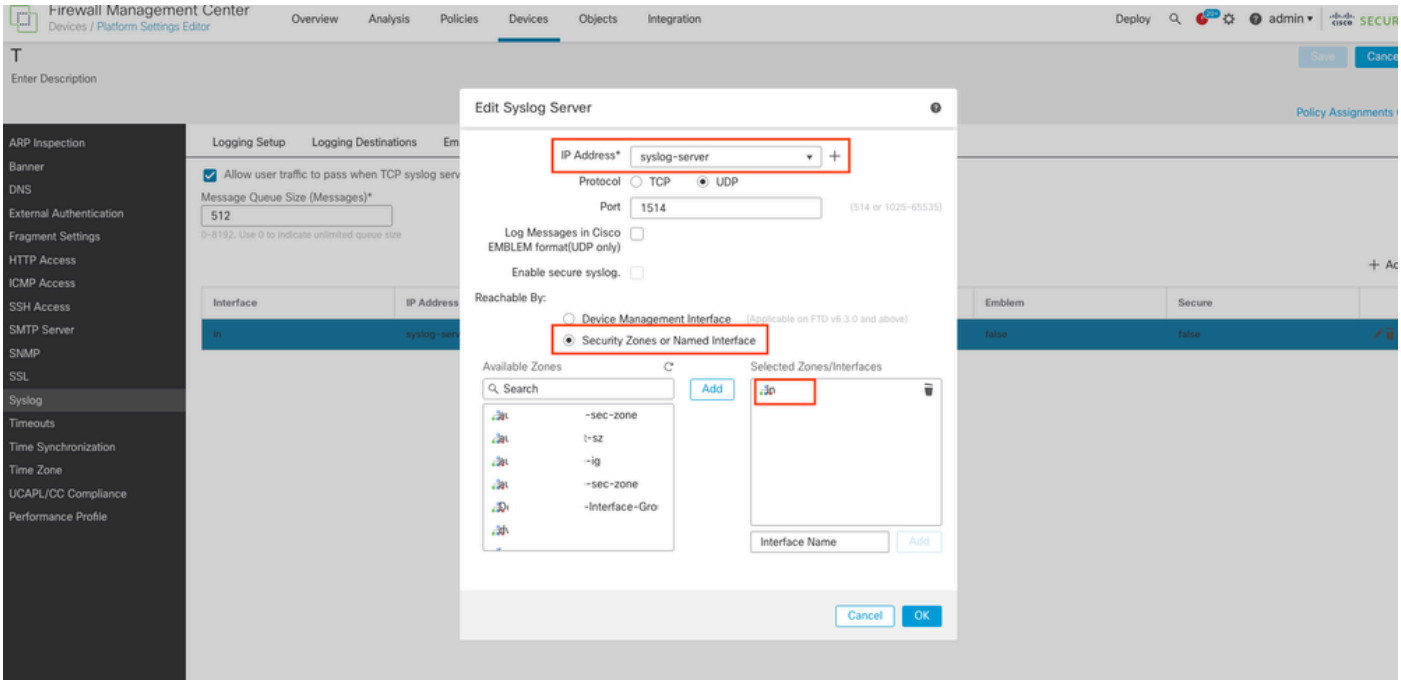
Met deze opdracht kunt u niet alleen een beheertoegangsinterface gebruiken als de broninterface voor Syslog-berichten die door de VPN-tunnel worden verzonden, maar ook verbinding maken met een gegevensinterface via SSH en Ping wanneer u een volledige tunnel van IPsec VPN of SSL VPN-client gebruikt of via een site-to-site IPsec-tunnel.



Opmerking: U kunt slechts één beheer-toegang interface bepalen.

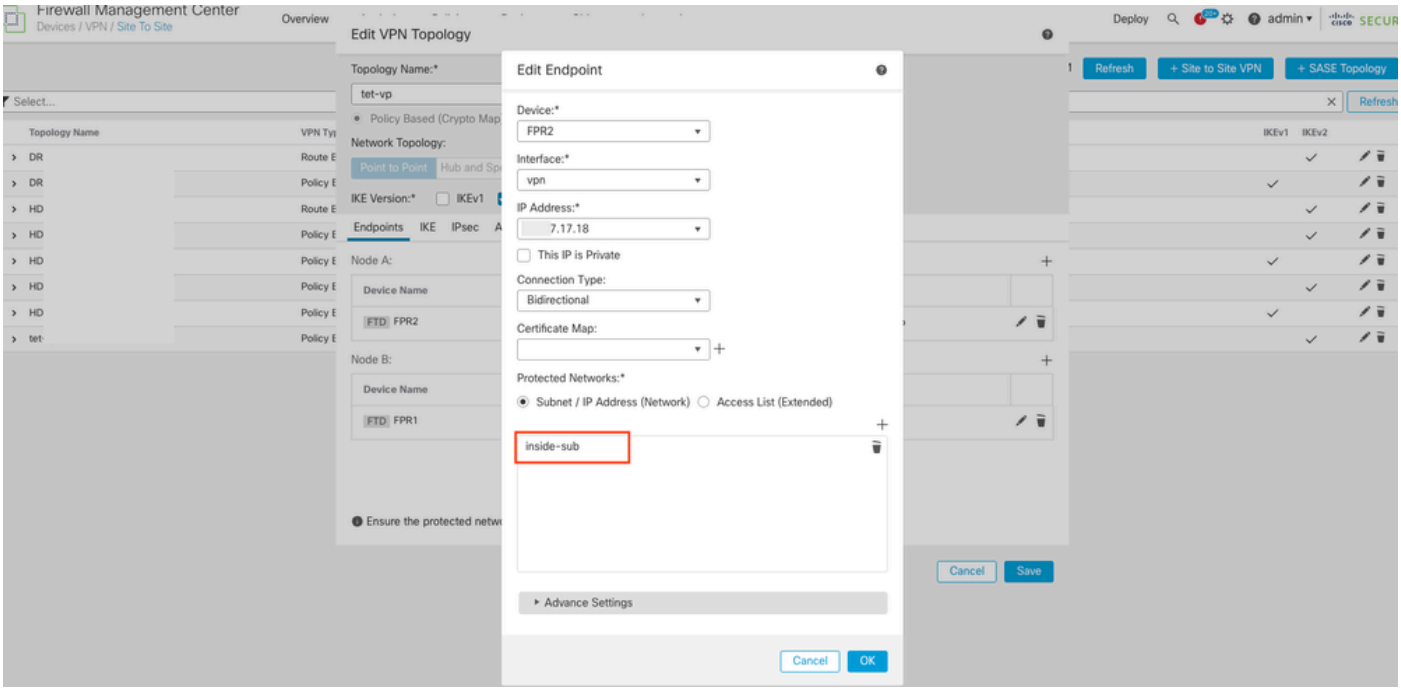
Configureren

1. Configureer Syslog onder Apparaten > Platform-instellingen voor de FTD. Zorg ervoor dat u Security Zones of Benoemde interfaceoptie selecteert in plaats van Device Management Interface terwijl u Syslog Server configureert en kies een interface voor beheertoegang om het Syslog-verkeer te bronnen.



Configuratie van syslogserver

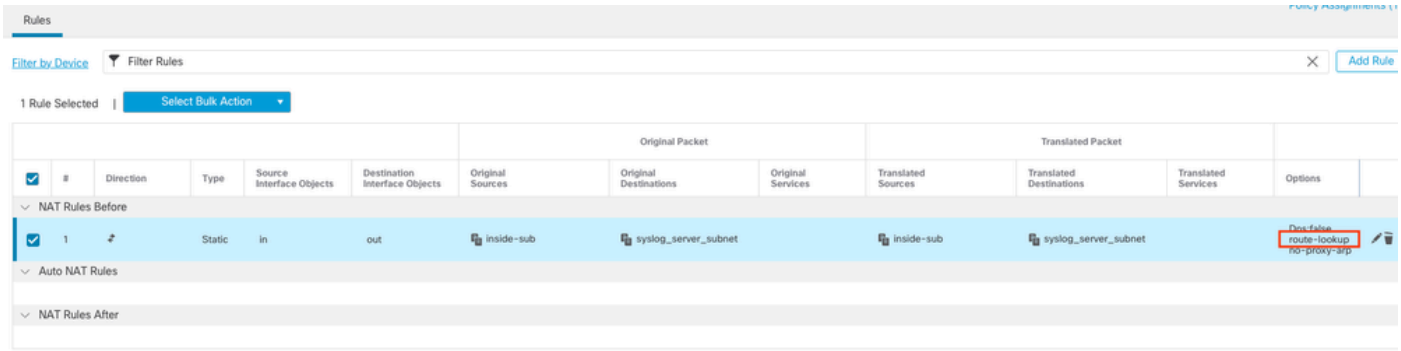
2. Zorg ervoor dat u het netwerk van de beheertoegangsinterface toevoegt onder Beschermde netwerken van VPN-endpoints. (onder Apparaten > Site to Site > VPN-topologie > Knooppunt).



Configuratie van beschermde netwerken

3. Zorg ervoor dat u een identiteit-NAT configureert tussen het netwerk van de beheer-toegangsinterface en VPN-netwerken (een gemeenschappelijke NAT-configuratie voor VPN-verkeer). U moet optie Uitvoeren Route Lookup voor Bestemmingsinterface onder Geavanceerde sectie van NAT-regel selecteren.

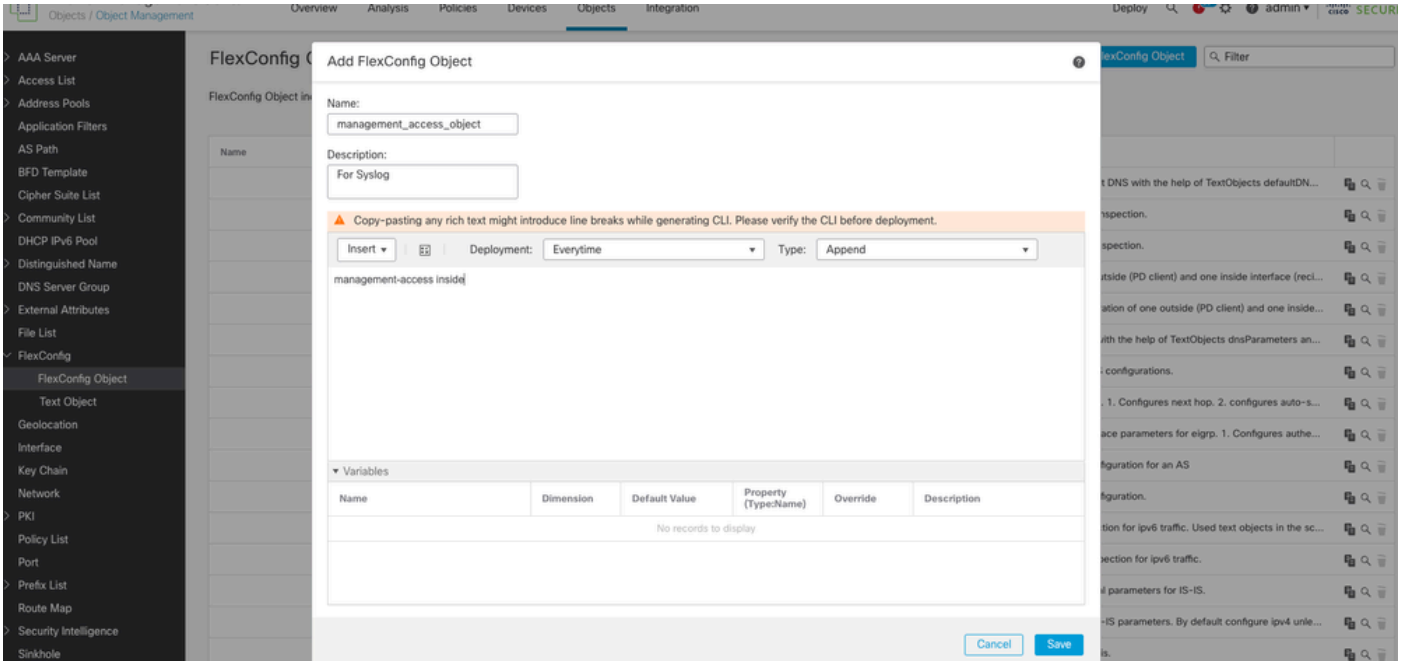
Zonder routerraadpleging, verstuurt de FTD verkeer door de interface die in de NAT-configuratie is gespecificeerd, ongeacht wat de routeringstabel zegt.



Configuratie van Identity NAT

4. U kunt beheer-toegang <interface name> configureren (in dit scenario beheer-toegang binnen) onder Objecten > Objectbeheer > FlexConfig Object.

Wijs het toe aan het doelapparaat FlexConfig Policy en implementeer de configuratie.



Configuratie FlexConfig

Verifiëren

Toegangsconfiguratie voor beheer:

<#root>

```
firepower#
```

show run | in management-access

```
management-access inside
```

Syslog-configuratie:

<#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

Syslog-verkeer via VPN-tunnel:

<#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
```

Gerelateerde informatie

- Logboekregistratie configureren op FTD via FMC
- De site configureren naar site VPN op FTD beheerd door FMC

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.