FTD-Datenschnittstelle für Syslog über VPN-Tunnel konfigurieren

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie die FTD-Datenschnittstelle von Cisco als Quelle für Syslogs konfiguriert wird, die über den VPN-Tunnel gesendet werden.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Syslog-Konfiguration auf Cisco Secure Firewall Threat Defense (FTD)
- Allgemeines Syslog
- Cisco Secure Firewall Management Center (FMC)

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der folgenden Software- und Hardwareversion:

- Cisco FTD Version 7.3.1
- Cisco FMC Version 7.3.1

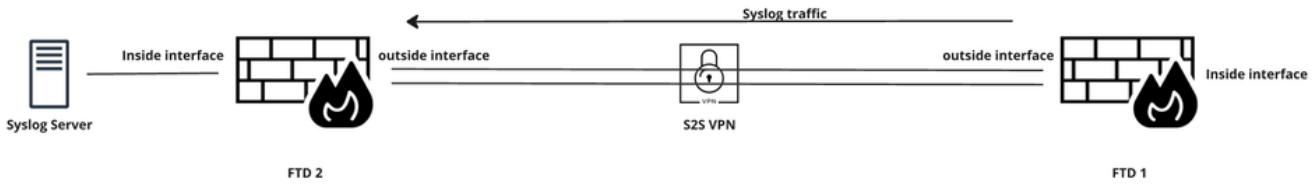
Haftungsausschluss: Die in diesem Dokument erwähnten Netzwerke und IP-Adressen sind keinen einzelnen Benutzern, Gruppen oder Organisationen zugeordnet. Diese Konfiguration wurde exklusiv für den Einsatz in einer Laborumgebung erstellt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Dieses Dokument beschreibt eine Lösung zur Verwendung einer der Datenschnittstellen von FTD als Quelle für Syslogs, die über einen VPN-Tunnel an den Syslog-Server an einem Remote-Standort gesendet werden müssen.

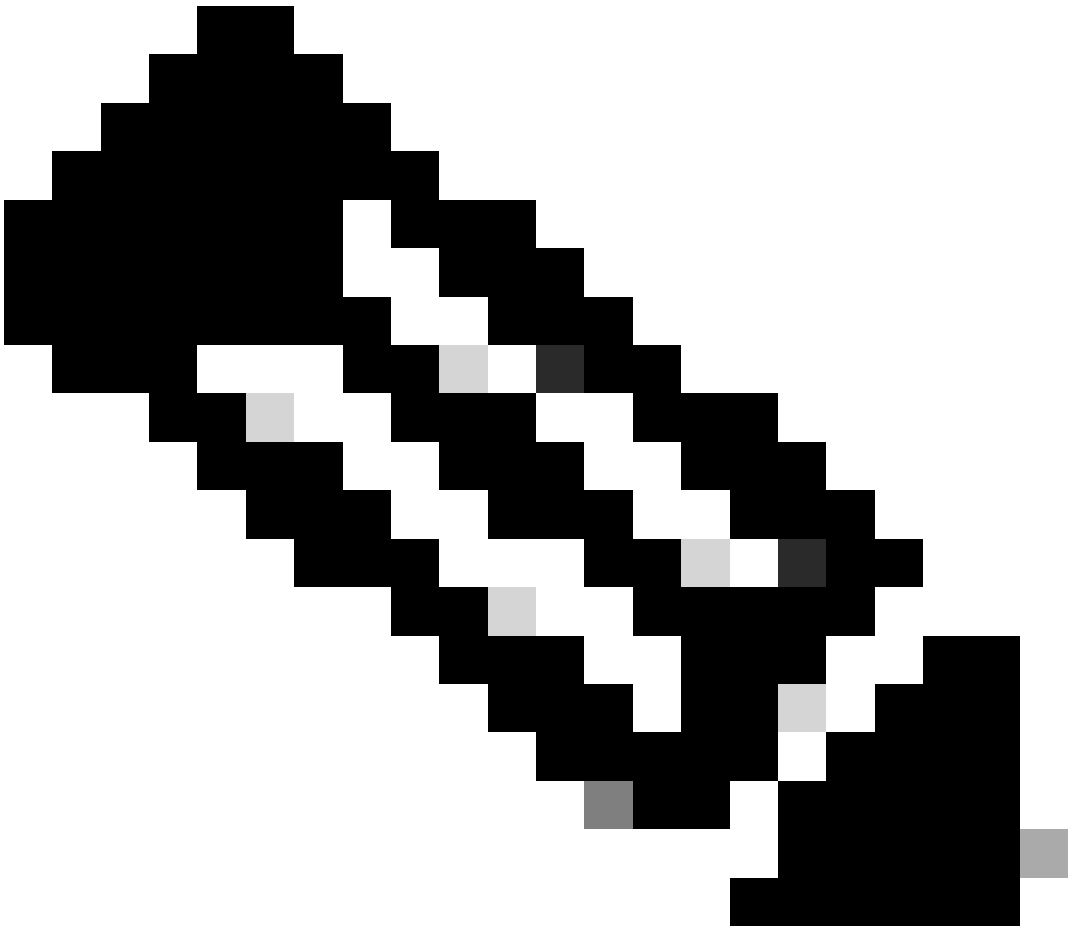
Diagramm



Netzwerkdiagramm

Um die Schnittstelle festzulegen, von der der über den Tunnel gesendete Syslog-Datenverkehr bezogen werden soll, können Sie den Befehl **management-**access über Flex Config anwenden.

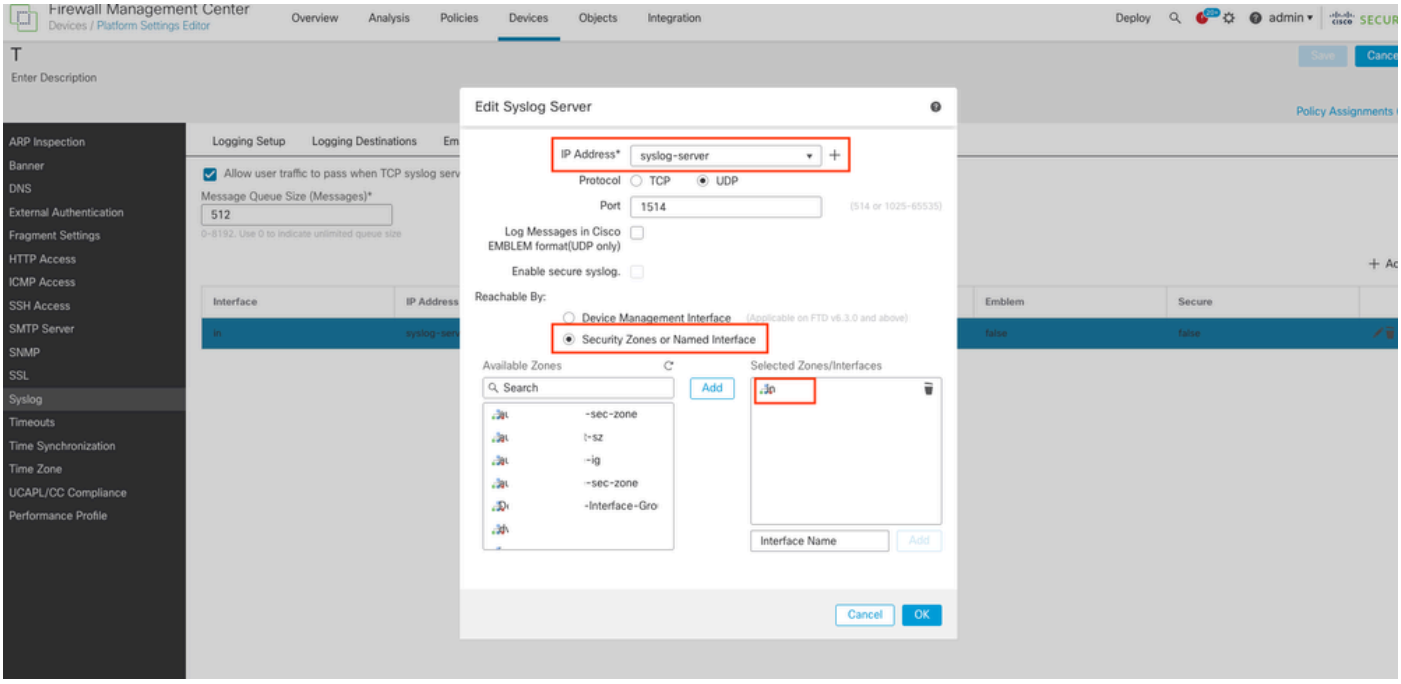
Mit diesem Befehl können Sie nicht nur eine Management-Zugriffsschnittstelle als Quellschnittstelle für Syslog-Meldungen verwenden, die über den VPN-Tunnel gesendet werden, sondern auch eine Verbindung zu einer Datenschnittstelle über SSH und Ping herstellen, wenn Sie einen vollständigen Tunnel-IPsec-VPN- oder SSL-VPN-Client oder einen Site-to-Site-IPsec-Tunnel verwenden.



Anmerkung: Sie können nur eine Management-Zugriffsoberfläche definieren.

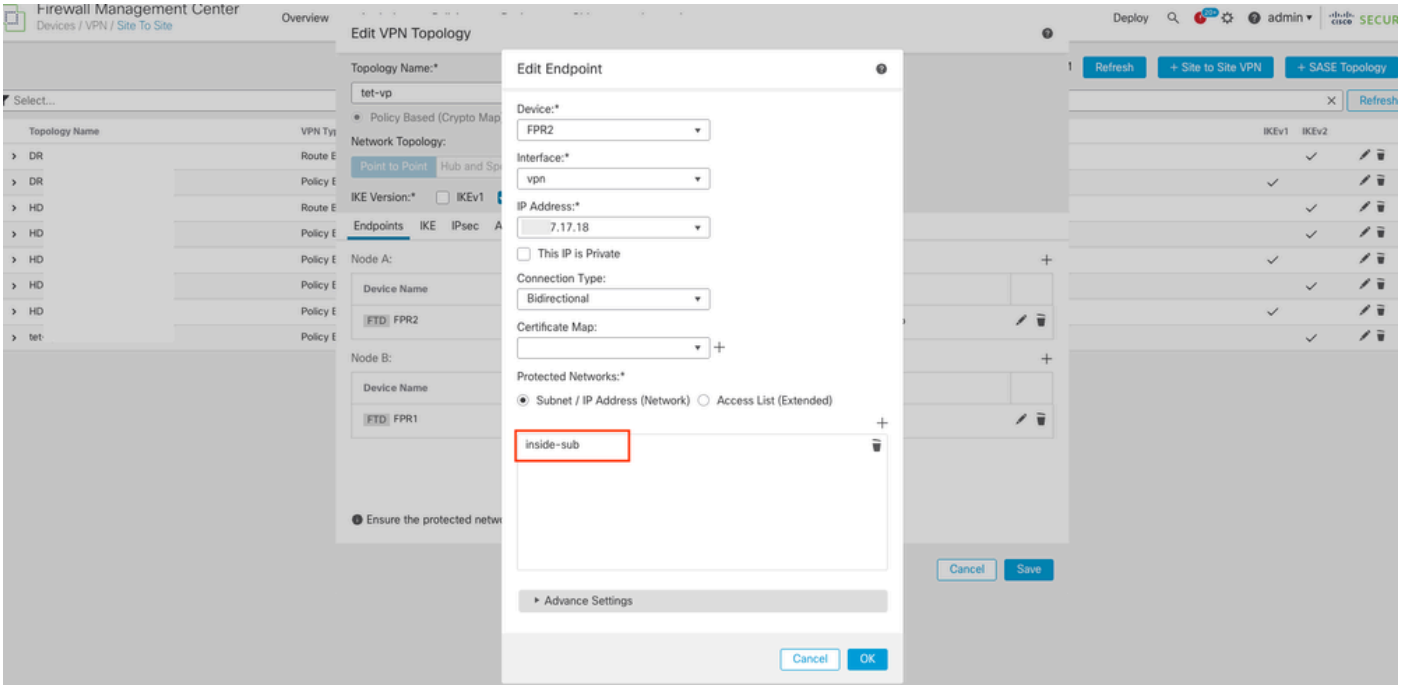
Konfigurieren

1. Konfigurieren Sie Syslog unter Geräte > Plattformeinstellungen für das FTD. Wählen Sie bei der Konfiguration des Syslog-Servers die Option Sicherheitszonen oder Benannte Schnittstelle anstelle der Gerätemanagement-Schnittstelle aus, und wählen Sie Management-Zugriffsschnittstelle aus, um den Syslog-Datenverkehr zu generieren.



Syslog-Serverkonfiguration

2. Stellen Sie sicher, dass Sie das Management-Access-Interface-Netzwerk unter Protected Networks of VPN Endpoint (Geschützte Netzwerke von VPN-Endpunkten) hinzufügen. (Unter Geräte > Site-to-Site > VPN-Topologie > Knoten).

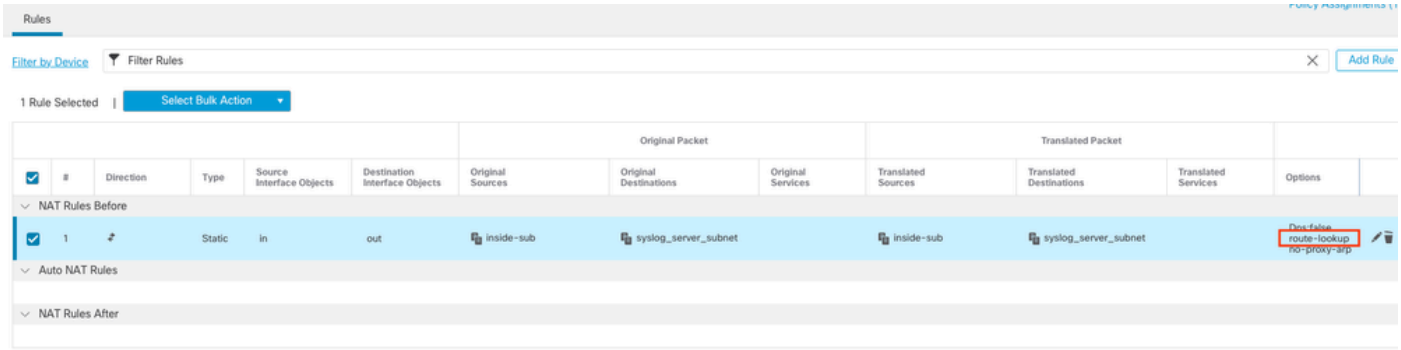


Protected Networks-Konfiguration

3. Stellen Sie sicher, dass Sie eine Identitäts-NAT zwischen dem Management-Access-Interface-

Netzwerk und den VPN-Netzwerken konfigurieren (eine gemeinsame NAT-Konfiguration für den VPN-Verkehr). Sie müssen die Option "Route Lookup for Destination Interface" (Routensuche für Zielschnittstelle durchführen) im Abschnitt "Advanced" (Erweitert) der NAT-Regel auswählen.

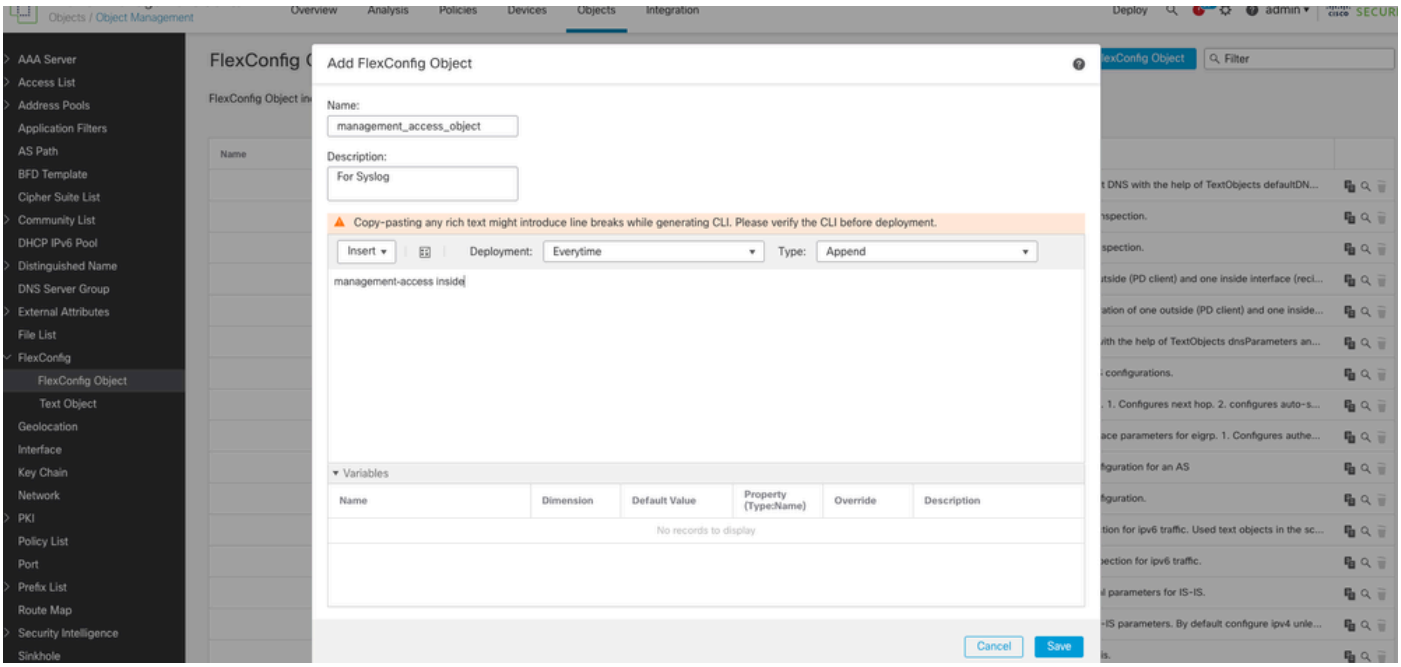
Ohne Routen-Suche sendet das FTD Datenverkehr über die in der NAT-Konfiguration angegebene Schnittstelle, unabhängig davon, was in der Routing-Tabelle steht.



NAT-Identitätskonfiguration

4. Sie können jetzt den Managementzugriff <Schnittstellenname> (in diesem Szenario den Managementzugriff innerhalb) unter Objekte > Objektmanagement > FlexConfig Objekt konfigurieren.

Weisen Sie sie einer FlexConfig-Richtlinie für das Zielgerät zu, und stellen Sie die Konfiguration bereit.



FlexConfig-Konfiguration

Überprüfung

Konfiguration des Managementzugriffs:

<#root>

```
firepower#
```

show run | in management-access

```
management-access inside
```

Syslog-Konfiguration:

<#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-Datenverkehr, der über den VPN-Tunnel gesendet wird:

<#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
```

Zugehörige Informationen

- Konfigurieren der Protokollierung auf FTD über FMC
- Site-to-Site-VPN auf von FMC verwaltetem FTD konfigurieren

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.