VPNトンネルを介したsyslog用のFTDデータインターフェイスの設定

内容

[はじめに](#)

[前提条件](#)

- [要件](#)
- [使用するコンポーネント](#)

[背景説明](#)

- [図](#)

[設定](#)

[確認](#)

[関連情報](#)

はじめに

このドキュメントでは、VPNトンネル経由で送信されるsyslogの送信元としてCisco FTDデータインターフェイスを設定する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Secure Firewall Threat Defense(FTD)のsyslog設定
- 一般的なsyslog
- Cisco Secure Firewall Management Center(FMC)

使用するコンポーネント

このドキュメントの情報は、このソフトウェアとハードウェアのバージョンに基づいています。

- Cisco FTDバージョン7.3.1
- Cisco FMCバージョン7.3.1

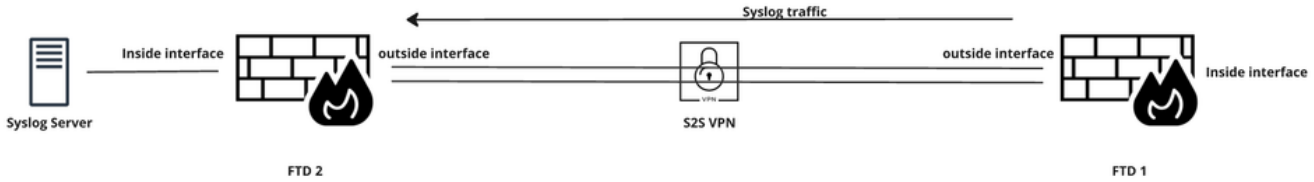
免責事項：このドキュメントで参照されているネットワークおよびIPアドレスは、個々のユーザ、グループ、または組織に関連付けられていません。この設定は、ラボ環境での使用のみを目的として作成されています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

このドキュメントでは、リモートサイトにあるsyslogサーバにVPNトンネル経由で送信する必要があるsyslogの送信元として、FTDのデータインターフェイスの1つを使用するソリューションについて説明します。

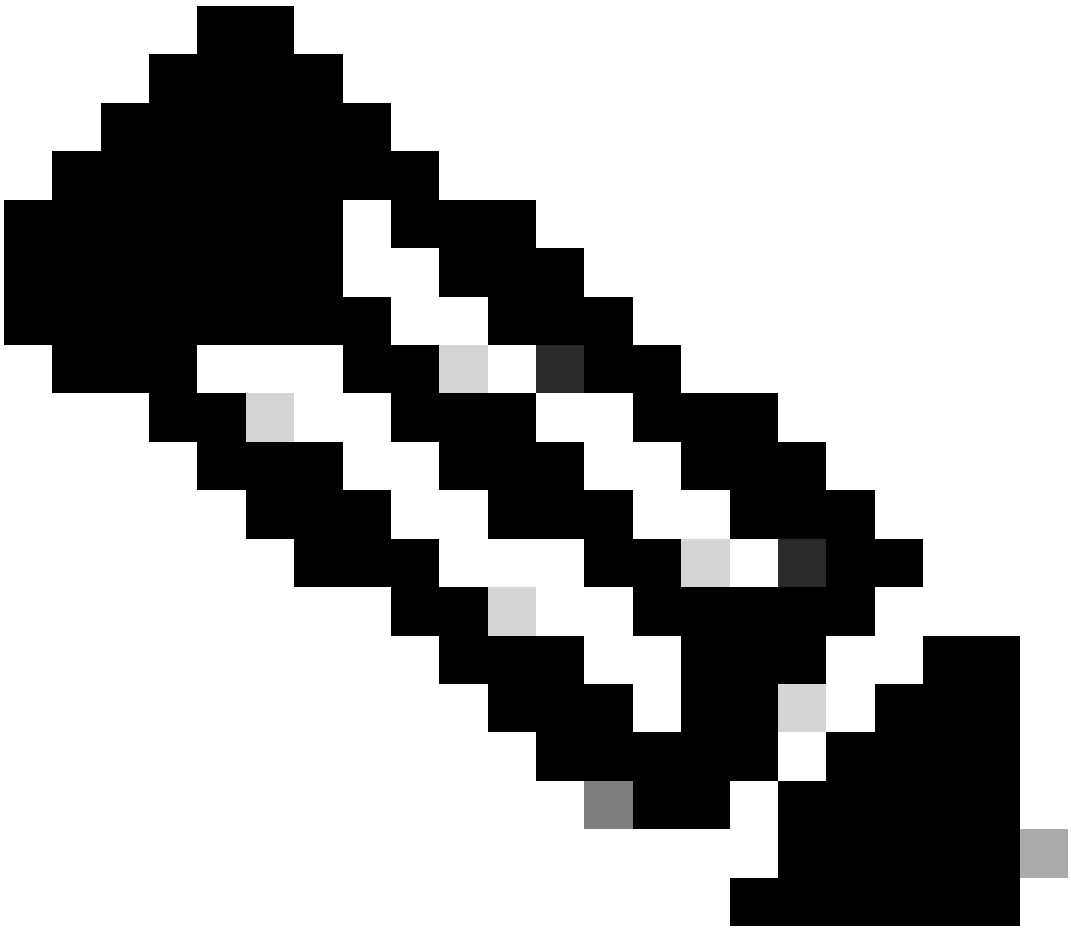
図



ネットワーク図

トンネルを介して送信されるSyslogトラフィックの送信元インターフェイスを指定するには、Flex Configで**management-**accesscommandを適用できます。

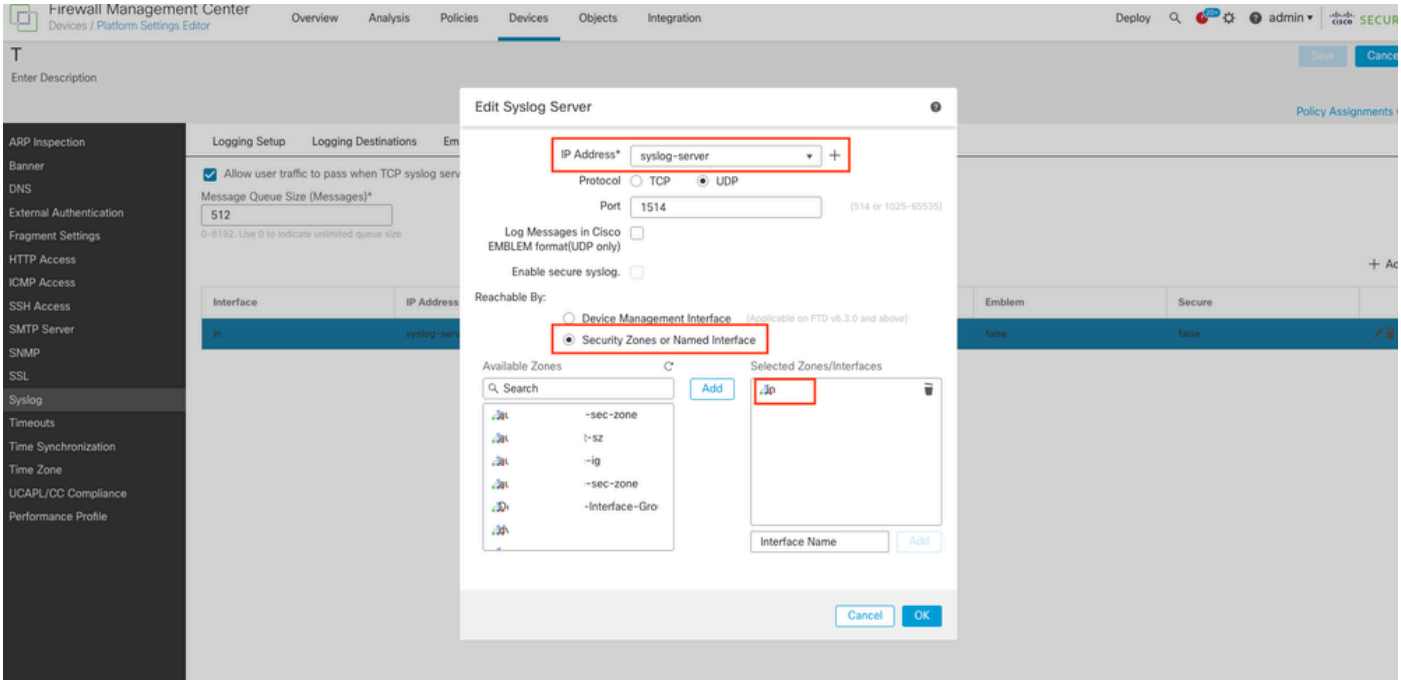
このコマンドを使用すると、VPNトンネルを介して送信されるsyslogメッセージの送信元インターフェイスとして管理アクセスインターフェイスを使用できるだけでなく、フルトンネルIPSec VPNまたはSSL VPNクライアントを使用している場合、またはサイト間IPSecトンネルを介している場合に、SSHおよびPingを介してデータインターフェイスに接続することもできます。



注：定義できる管理アクセスインターフェイスは1つだけです。

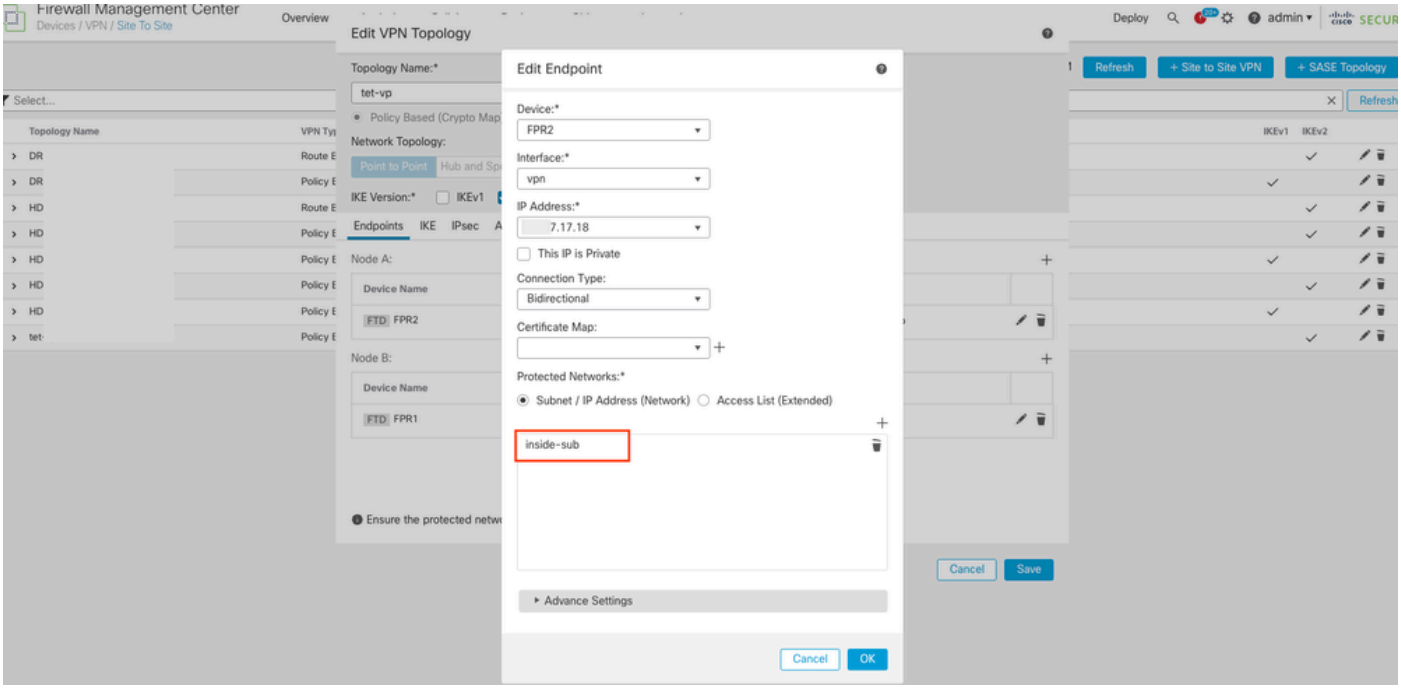
設定

1. FTDのDevices > Platform Settingsでsyslogを設定します。Syslogサーバの設定時には、Device Management Interfaceではなく、Security ZonesまたはNamed Interfaceオプションを必ず選択してから、management-access interfaceを選択してSyslogトラフィックを送信してください。



Syslogサーバの設定

2. VPNエンドポイントのProtected Networksの下に、management-access interfaceネットワークが追加されていることを確認します。(Devices > Site To Site > VPN Topology > Nodeの順に選択)。

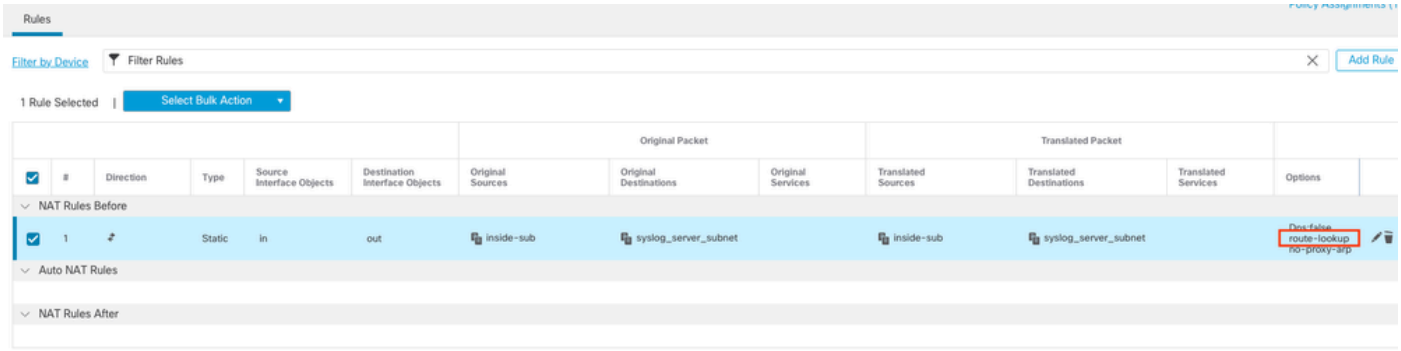


保護されたネットワークの設定

3.管理アクセスインターフェイスネットワークとVPNネットワークの間にアイデンティティNATを必ず設定してください（VPNトラフィック用の一般的なNAT設定）。 NATルールの

Advancedセクションで、Perform Route Lookup for Destination Interfaceオプションを選択する必要があります。

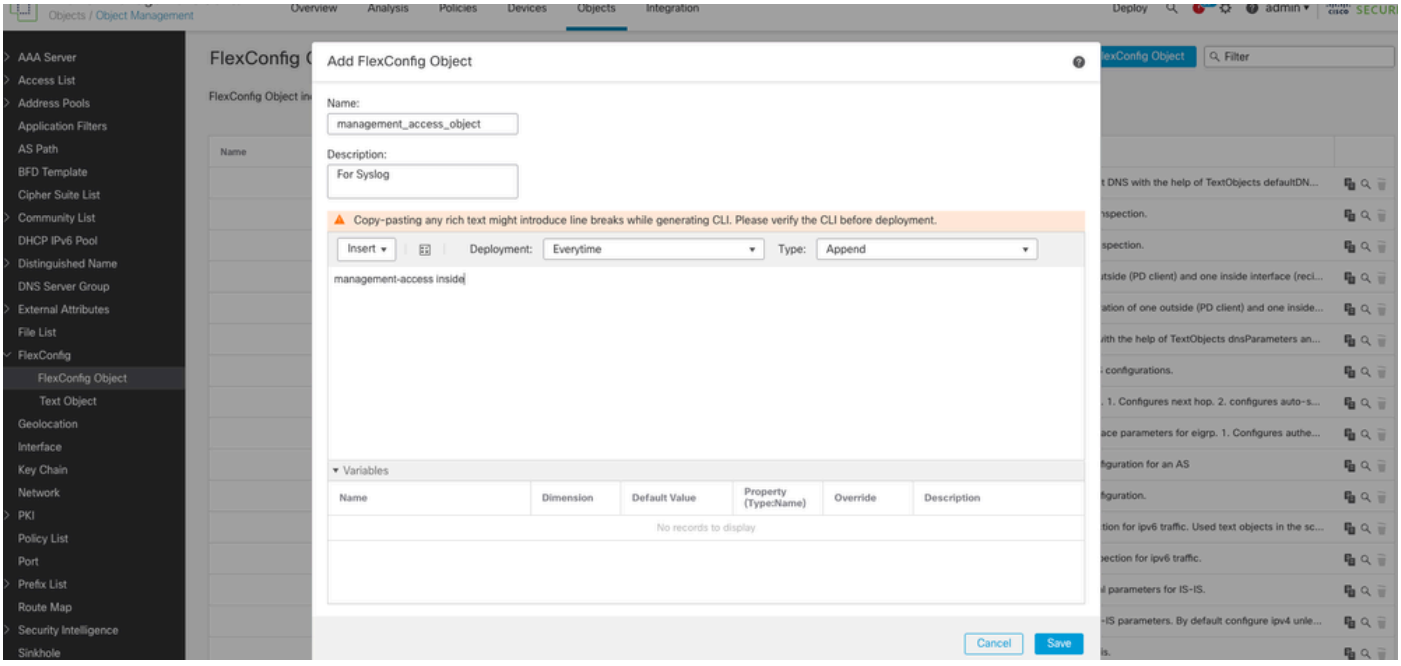
ルートルックアップを行わない場合、FTDは、ルーティングテーブルの内容にかかわらず、NAT設定で指定されているインターフェイスからトラフィックを送信します。



アイデンティティNATの設定

4. Objects > Object Management > FlexConfig Objectの下で、management-access <interface name>(このシナリオではmanagement-access inside)を設定できるようになりました。

これを対象デバイスのFlexConfigポリシーに割り当て、設定を展開します。



FlexConfigの設定

確認

管理アクセスの設定：

<#root>

```
firepower#
```

```
show run | in management-access
```

```
management-access inside
```

Syslog設定：

<#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トンネル経由で送信されるsyslogトラフィック：

<#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
```

関連情報

- FMC を介して FTD にロギングを設定
- FMCによって管理されるFTDのサイト間VPNの設定

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。