Configurar a interface de dados FTD para syslog sobre túnel VPN

Contents

Introdução

Este documento descreve como configurar a interface de dados do Cisco FTD como origem para Syslogs enviados pelo túnel VPN.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração de syslog no Cisco Secure Firewall Threat Defense (FTD)
- Syslog geral
- Cisco Secure Firewall Management Center (FMC)

Componentes Utilizados

As informações neste documento são baseadas nesta versão de software e hardware:

- Cisco FTD versão 7.3.1
- Cisco FMC versão 7.3.1

Aviso de isenção de responsabilidade: as redes e os endereços IP mencionados neste documento não estão associados a nenhum usuário, grupo ou organização individual. Essa configuração foi criada exclusivamente para uso em um ambiente de laboratório.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Este documento descreve uma solução para usar uma das interfaces de dados do FTD como origem para syslogs que precisam ser enviados por um túnel VPN para o Servidor Syslog localizado no site remoto.

Diagrama

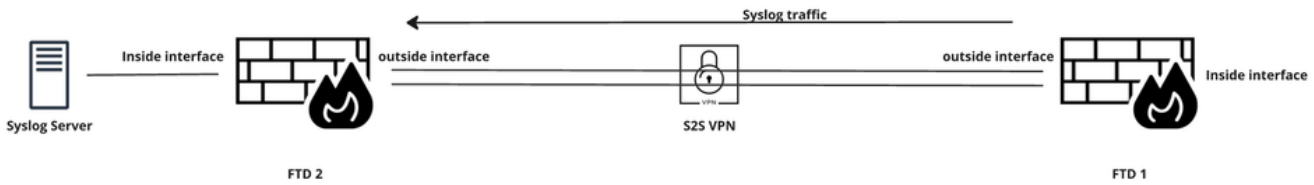
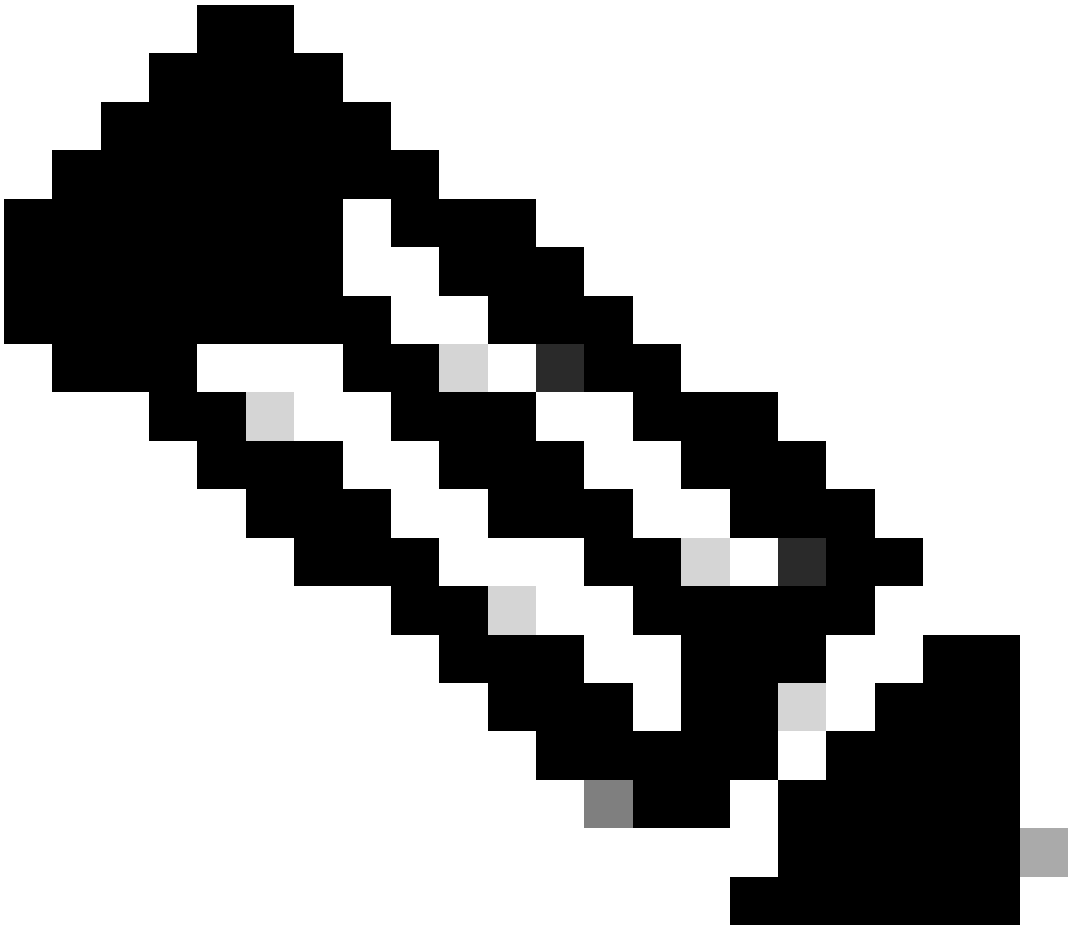


Diagrama de Rede

Para especificar a interface da qual o tráfego Syslog enviado pelo túnel será originado, você pode aplicar o comando **management-**access por meio do Flex Config.

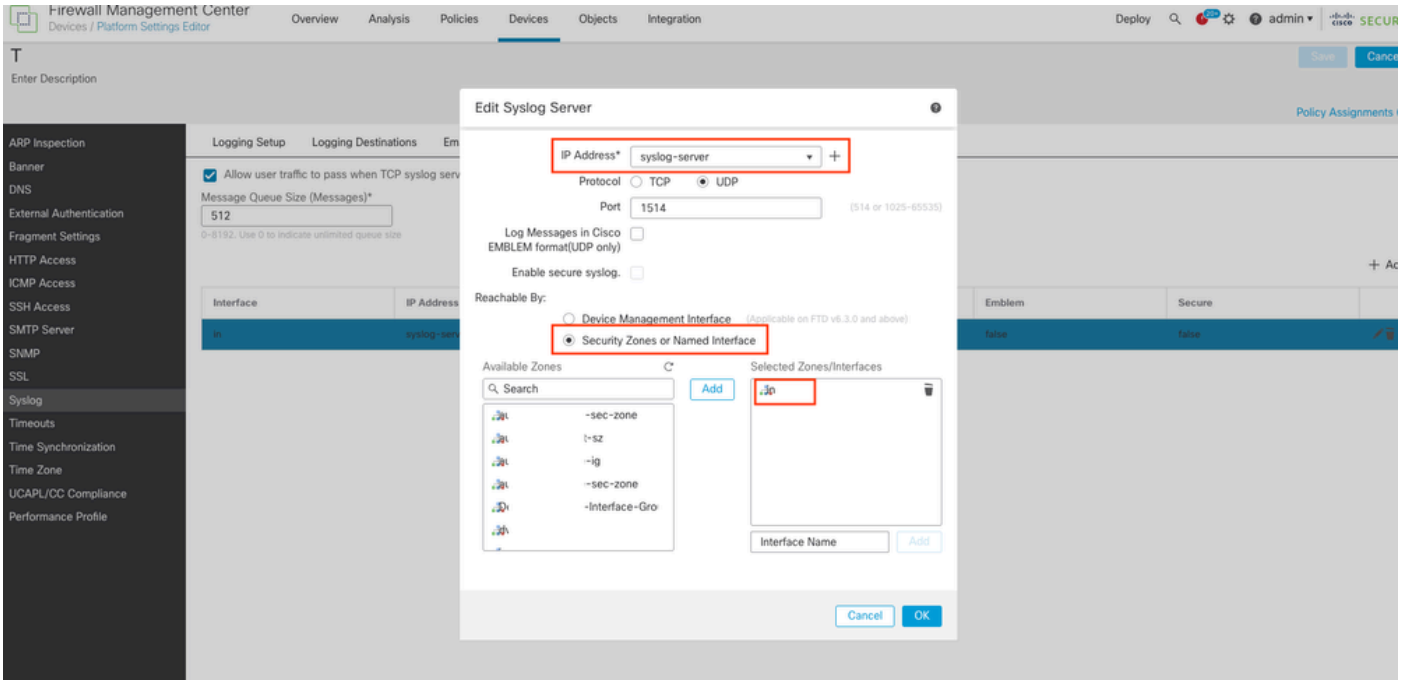
Esse comando não só permite que você use uma interface de acesso de gerenciamento como a interface de origem para mensagens de Syslog enviadas pelo túnel VPN, mas também para se conectar a uma interface de dados via SSH e Ping ao usar um VPN IPsec de túnel completo ou um cliente VPN SSL ou através de um túnel IPsec de site a site.



Note: Você pode definir apenas uma interface de acesso de gerenciamento.

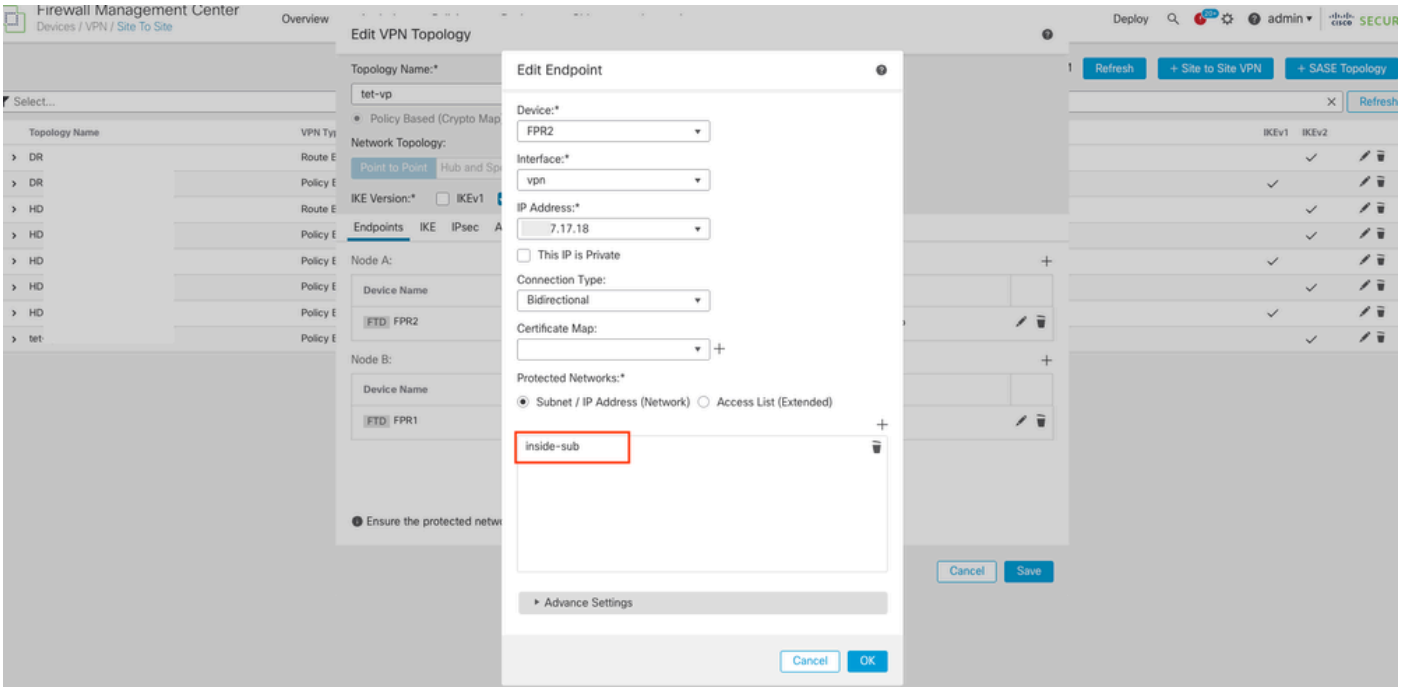
Configurar

1. Configure o Syslog em Devices > Platform Settings para o FTD. Certifique-se de selecionar a opção Security Zones ou Named Interface em vez de Device Management Interface ao configurar o Servidor Syslog e escolha management-access interface para originar o tráfego Syslog.



Configuração do Servidor Syslog

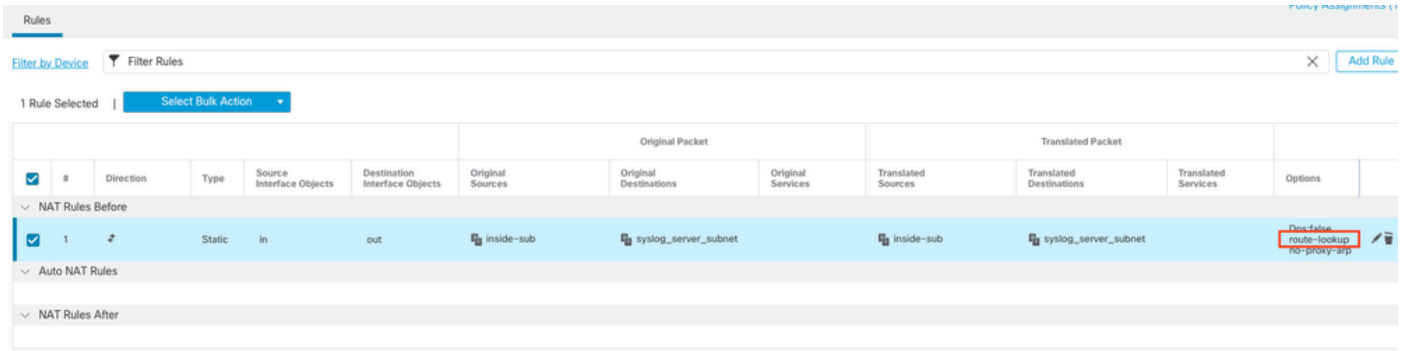
2. Certifique-se de adicionar a rede da interface de acesso de gerenciamento em Redes Protegidas do Ponto de Extremidade VPN. (Em Devices > Site To Site > VPN Topology > Node).



Configuração de redes protegidas

3. Certifique-se de configurar um NAT de identidade entre a rede da interface de gerenciamento-acesso e as redes VPN (uma configuração NAT comum para o tráfego VPN). Você deve selecionar a opção Perform Route Lookup for Destination Interface na seção Advanced da regra NAT.

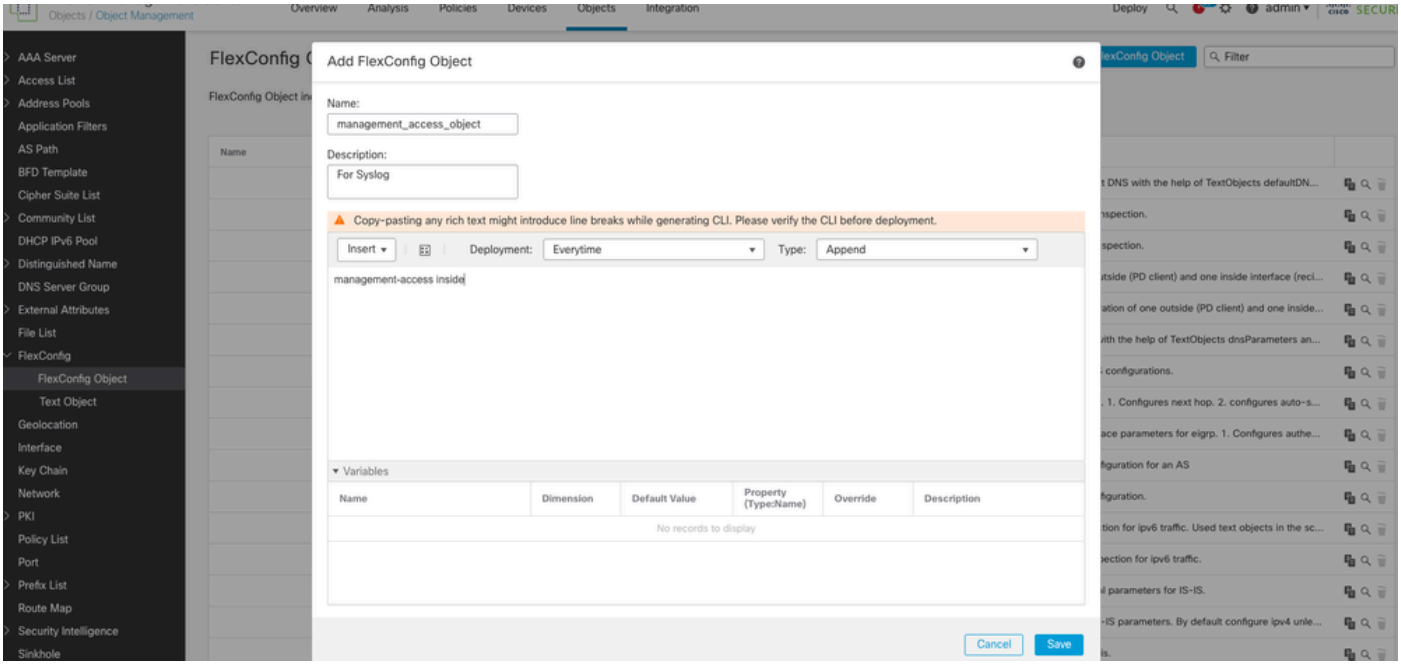
Sem a pesquisa de rota, o FTD envia o tráfego através da interface especificada na configuração do NAT, independentemente do que a tabela de roteamento diz.



Configuração de NAT de identidade

4. Agora você pode configurar management-access <nome da interface> (neste cenário management-access inside) em Objetos > Object Management > FlexConfig Object .

Atribua-o ao dispositivo de destino FlexConfig Policy e Deploy a configuração.



Configuração FlexConfig

Verificar

Configuração do Acesso de Gerenciamento:

<#root>

```
firepower#
```

show run | in management-access

```
management-access inside
```

Configuração de Syslog:

<#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

Tráfego de syslog enviado por túnel VPN:

<#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
```

Informações Relacionadas

- Configurar o registro no FTD usando o FMC
- Configurar a VPN site a site no FTD gerenciado pelo FMC

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.