配置FTD数据接口以通过VPN隧道进行系统日志

目录

简介

本文档介绍如何将Cisco FTD数据接口配置为通过VPN隧道发送的系统日志的源。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科安全防火墙威胁防御(FTD)上的系统日志配置
- 常规系统日志
- 思科安全防火墙管理中心(FMC)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 思科FTD版本7.3.1
- 思科FMC版本7.3.1

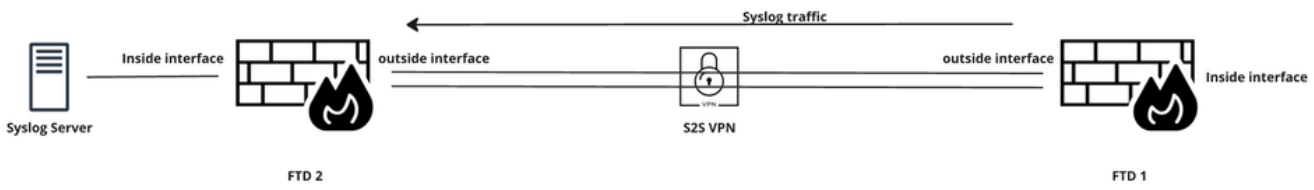
免责声明：本文档中引用的网络和IP地址未与任何单个用户、组或组织关联。此配置专为实验环境而创建。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

本文档介绍使用FTD的一个数据接口作为必须通过VPN隧道发送到位于远程站点的Syslog服务器的系统日志源的解决方案。

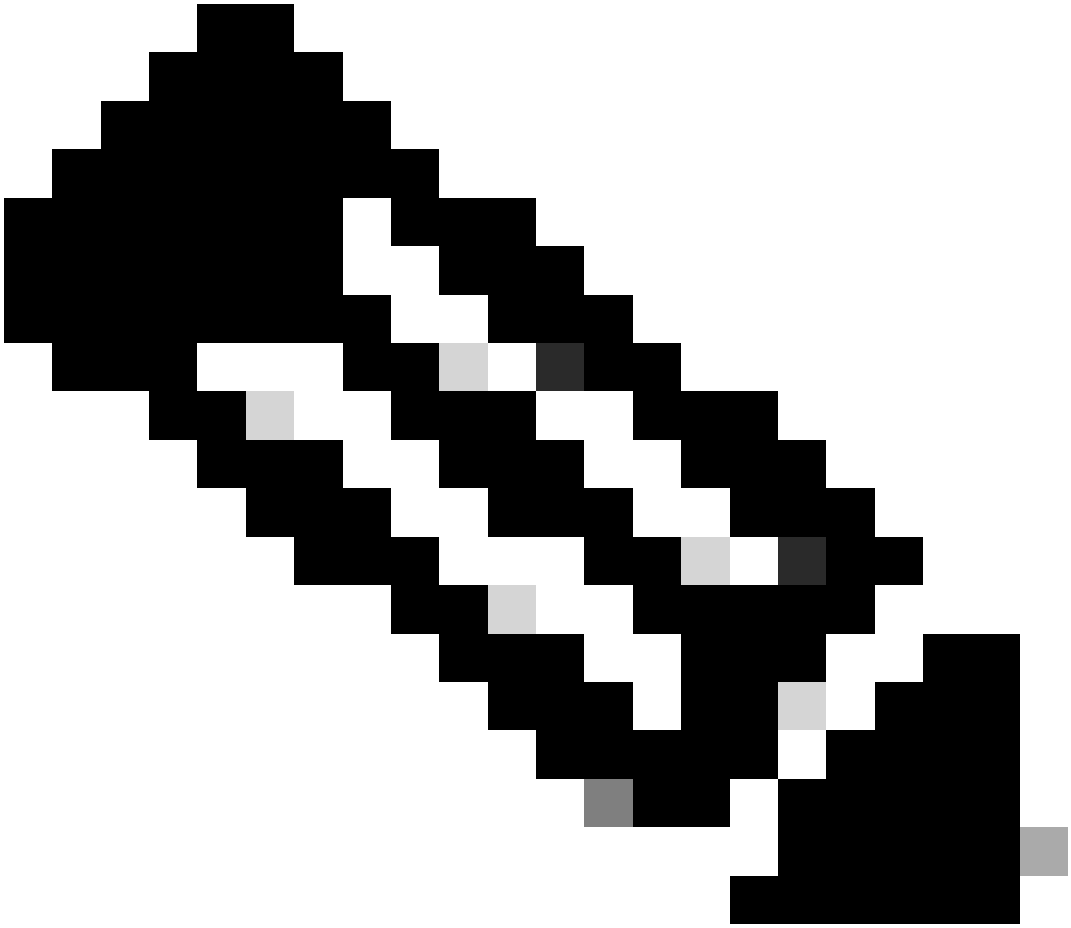
图解



网络图

要指定用于发送通过隧道发送的系统日志流量的源接口，可以通过**Flex Config**应用**management**-access命令。

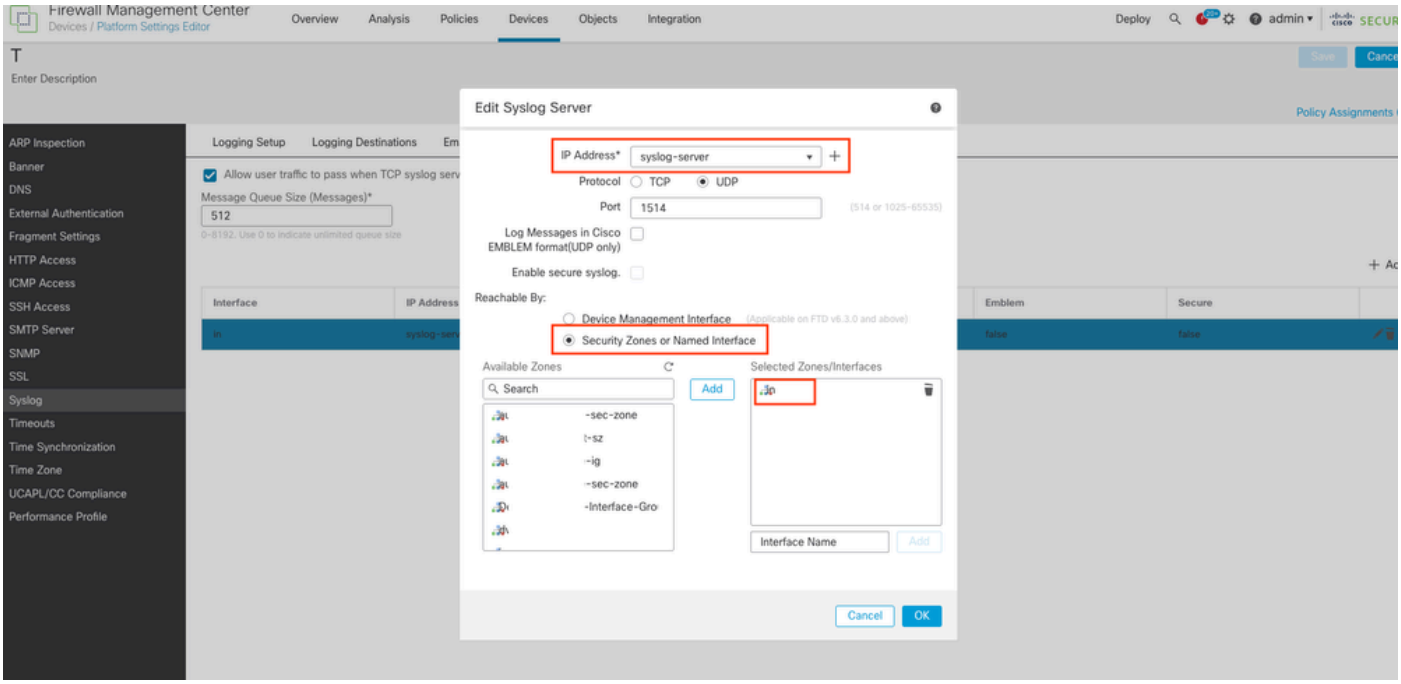
此命令不仅允许您使用管理访问接口作为通过VPN隧道发送的系统日志消息的源接口，还允许您在使用全隧道IPsec VPN或SSL VPN客户端或通过站点到站点IPsec隧道时通过SSH和Ping连接到数据接口。



注意：您只能定义一个管理访问接口。

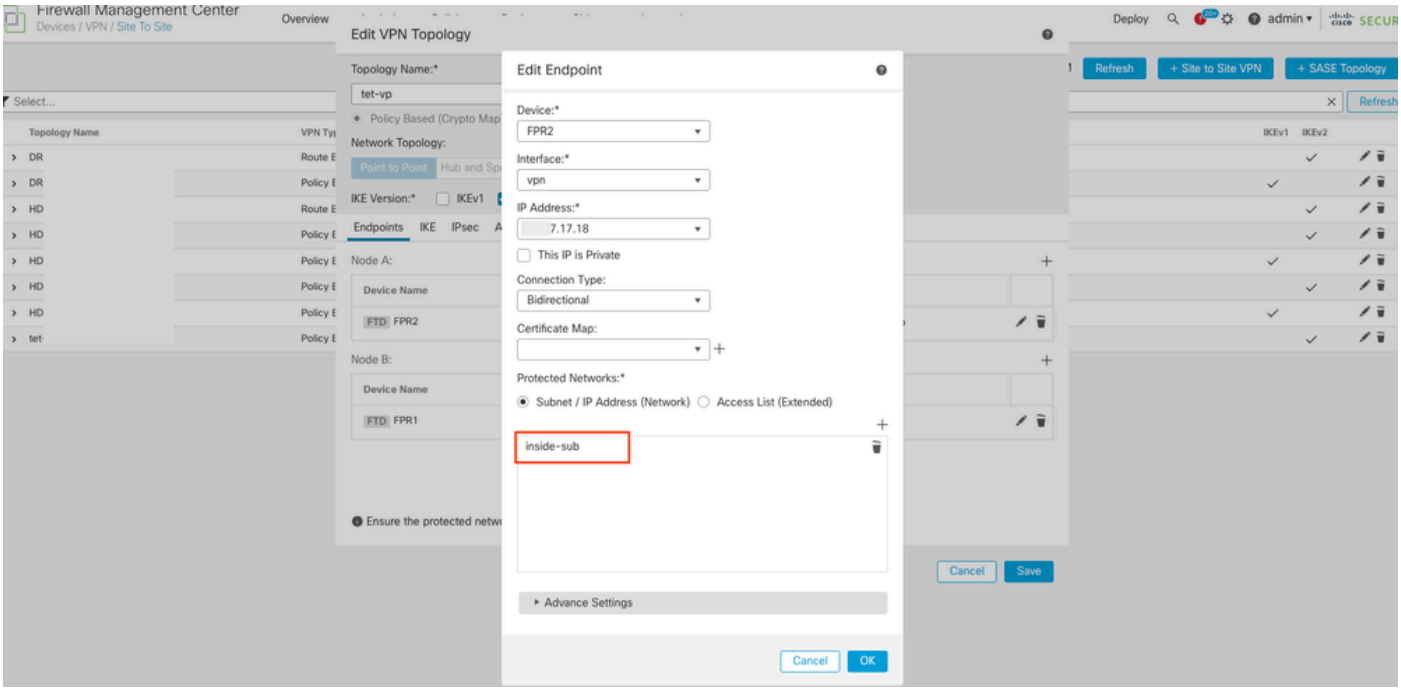
配置

1.在Devices > Platform Settings下为FTD配置系统日志。配置系统日志服务器时，请确保选择Security Zones 或Named Interface选项而不是Device Management Interface，然后选择management-access interface以源系统日志流量。



系统日志服务器配置

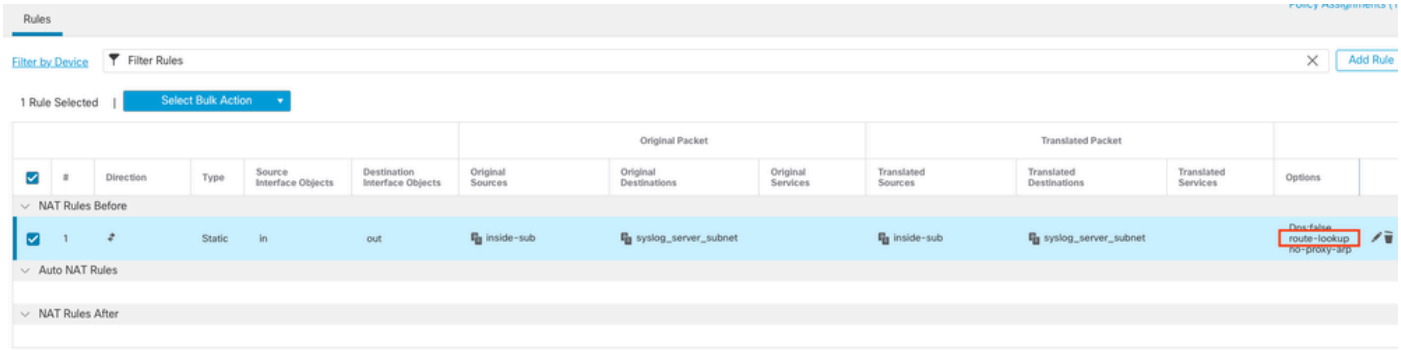
2.确保在VPN终端的受保护网络下添加管理访问接口网络。(在Devices > Site To Site > VPN Topology > Node下)。



受保护的网络配置

3.确保在管理访问接口网络和VPN网络之间配置身份标识NAT（VPN流量的通用NAT配置）。 必须在NAT规则的Advanced部分下选择Perform Route Lookup for Destination Interface选项。

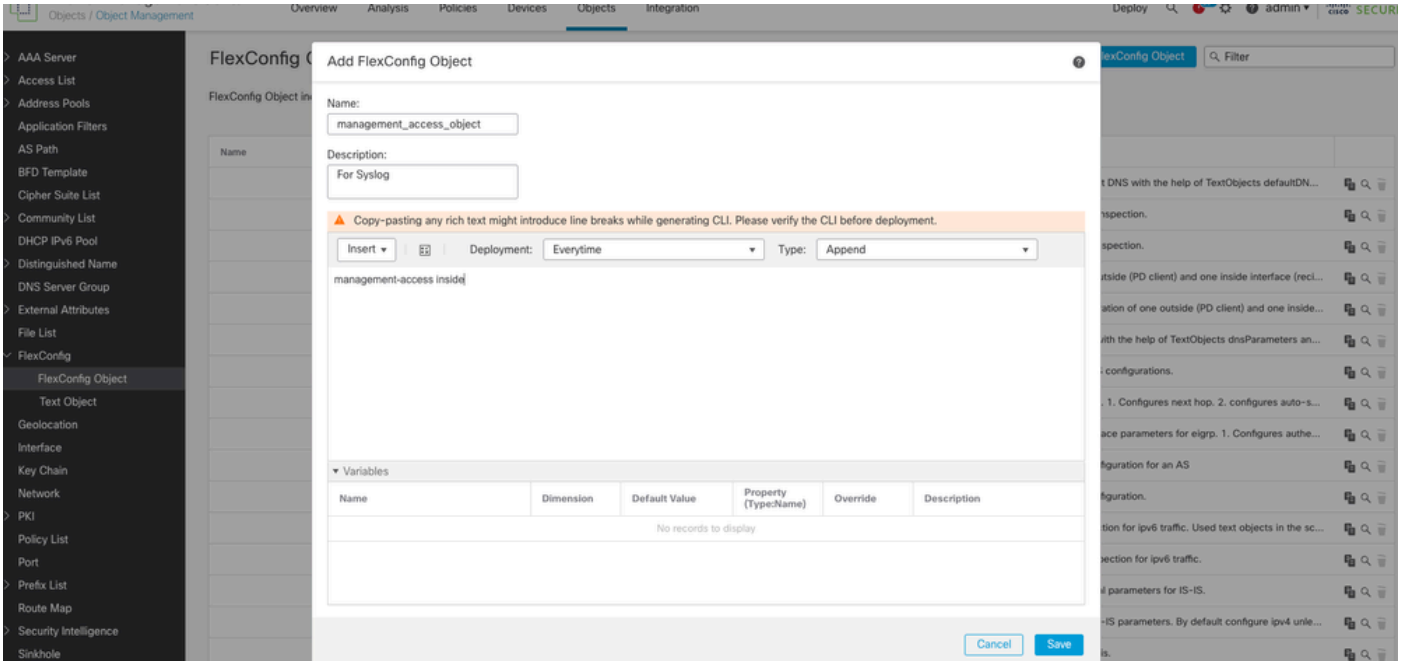
如果没有路由查找，FTD将通过NAT配置中指定的接口发送流量，无论路由表如何显示。



身份NAT配置

4.您现在可以在对象>对象管理> FlexConfig对象下配置management-access <interface name>(在本场景中，为management-access inside)。

将其分配到目标设备FlexConfig策略并部署配置。



FlexConfig配置

验证

管理访问配置：

<#root>

firepower#

show run | in management-access

management-access inside

系统日志配置：

<#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

通过VPN隧道发送的系统日志流量：

<#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
```

相关信息

- 通过 FMC 在 FTD 上配置日志记录
- 在FMC管理的FTD上配置站点到站点VPN

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。