Configuración de la Interfaz de Datos FTD para el Túnel Syslog Over VPN

Contenido

Introducción

Prerequisites

- Requirements
- Componentes Utilizados

Antecedentes

- Diagrama

Configurar

Verificación

Información Relacionada

Introducción

Este documento describe cómo configurar la interfaz de datos de Cisco FTD como origen para los registros del sistema enviados a través del túnel VPN.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración de Syslog en Cisco Secure Firewall Threat Defence (FTD)
- Syslog general
- Cisco Secure Firewall Management Center (FMC)

Componentes Utilizados

La información de este documento se basa en esta versión de software y hardware:

- Cisco FTD versión 7.3.1
- Cisco FMC versión 7.3.1

Renuncia: las redes y direcciones IP a las que se hace referencia en este documento no están asociadas con ningún usuario, grupo u organización individual. Esta configuración se ha creado exclusivamente para su uso en un entorno de laboratorio.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Este documento describe una solución para utilizar una de las interfaces de datos de FTD como origen para los syslogs que deben enviarse a través de un túnel VPN al servidor Syslog que se encuentra en el sitio remoto.

Diagrama

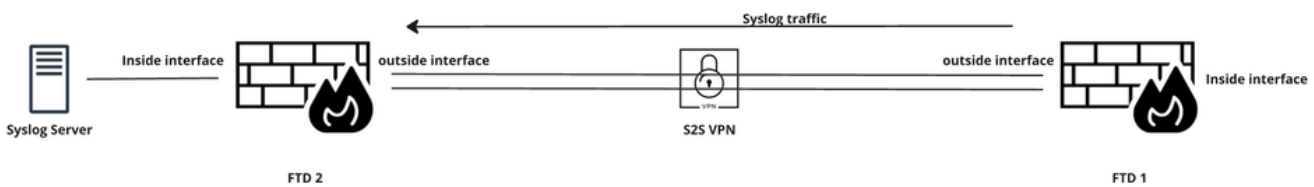
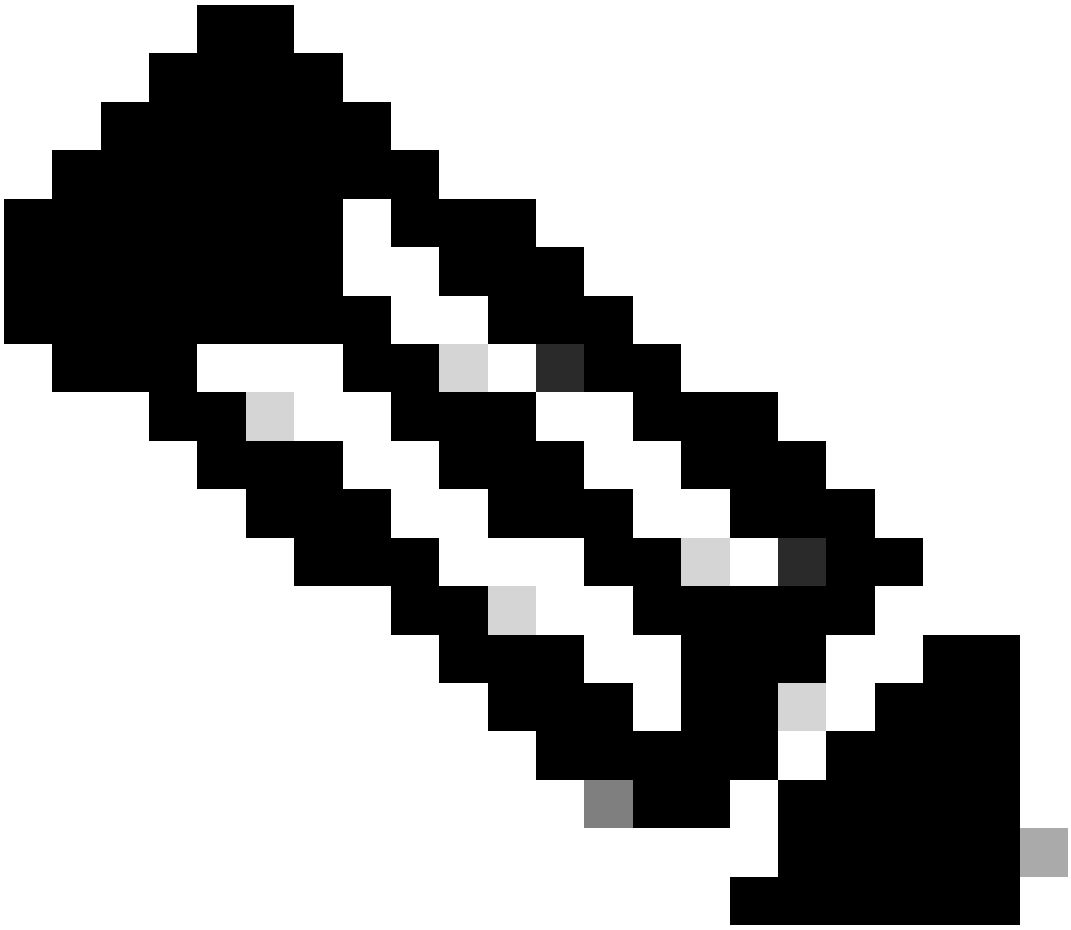


Diagrama de la red

Para especificar la interfaz desde la cual se originará el tráfico Syslog enviado a través del túnel, puede aplicar el comando **management-**accesscommand a través de Flex Config.

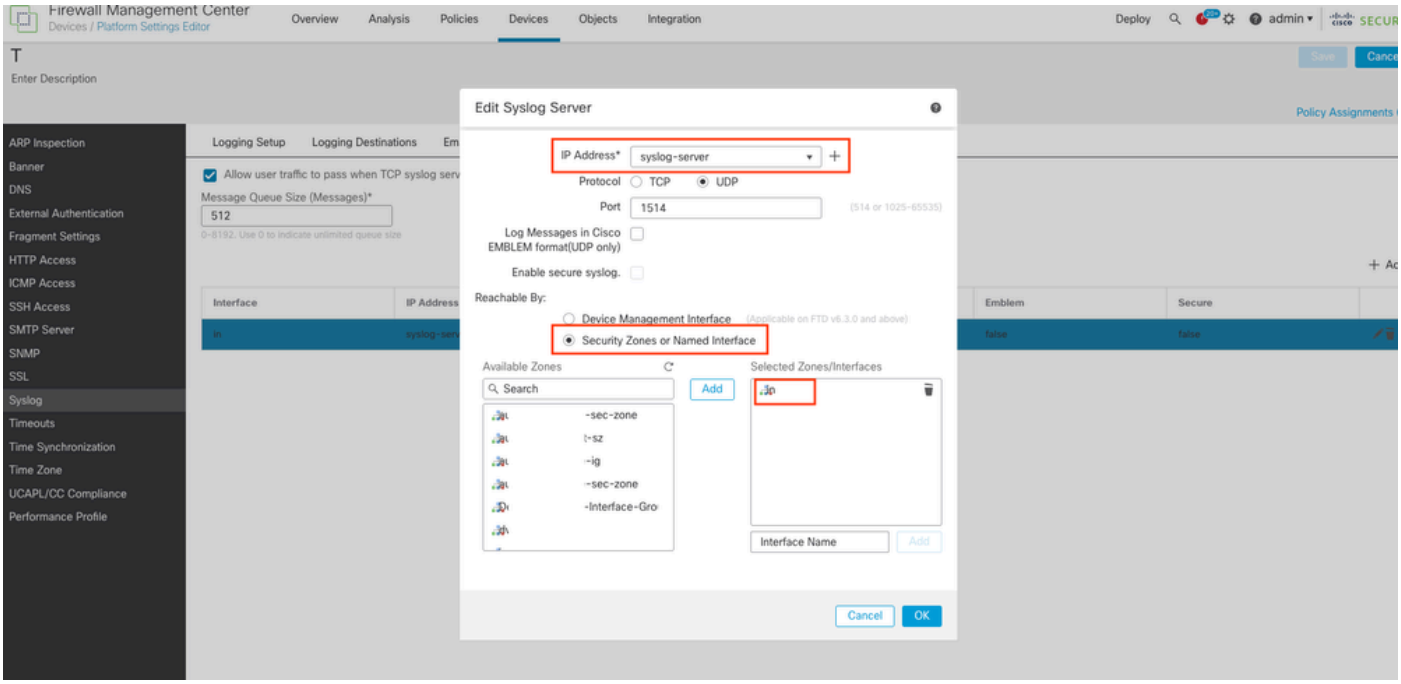
Este comando no solo le permite utilizar una interfaz de acceso a la administración como interfaz de origen para los mensajes Syslog enviados a través del túnel VPN, sino también conectarse a una interfaz de datos a través de SSH y Ping cuando se utiliza una VPN IPsec de túnel completo o un cliente VPN SSL o a través de un túnel IPsec de sitio a sitio.



Nota: Sólo puede definir una interfaz de acceso a la gestión.

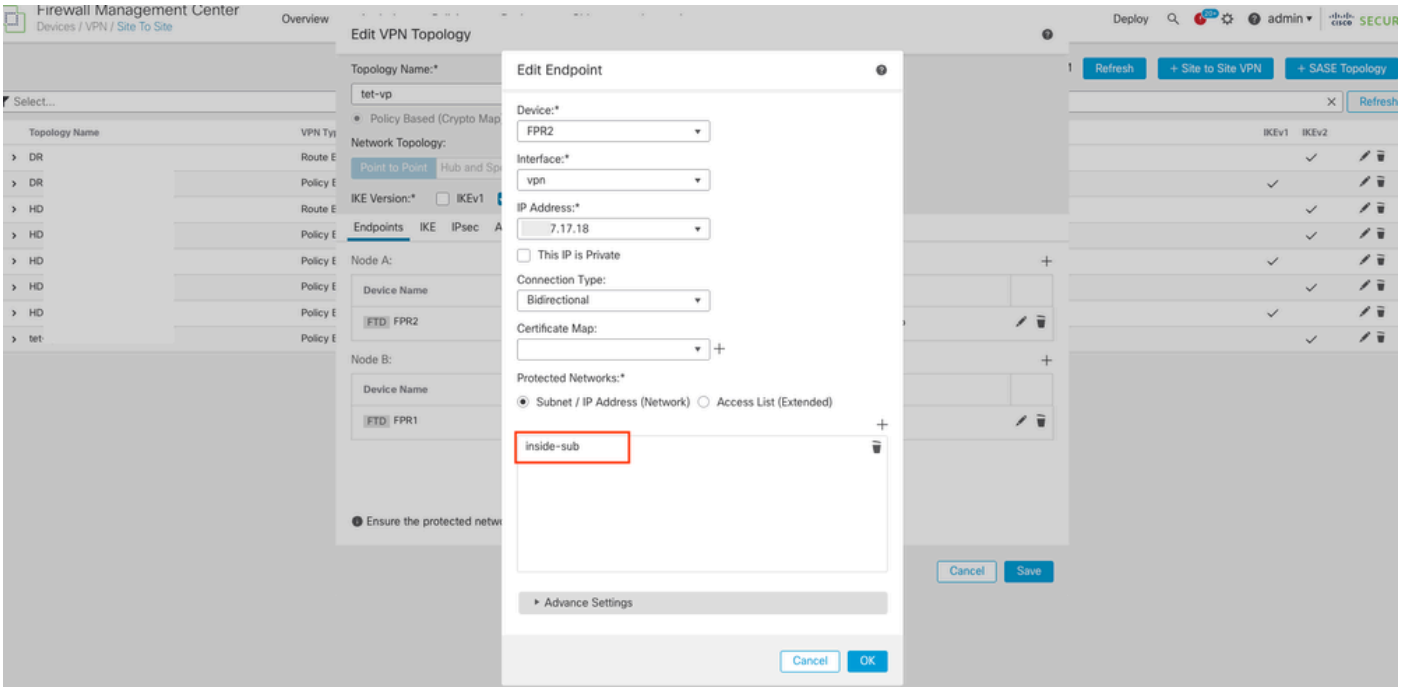
Configurar

1. Configure Syslog en Devices > Platform Settings para el FTD. Asegúrese de seleccionar la opción Security Zones o Named Interface en lugar de Device Management Interface mientras configura el servidor Syslog y elija management-access interface para originar el tráfico de Syslog.



Configuración del servidor Syslog

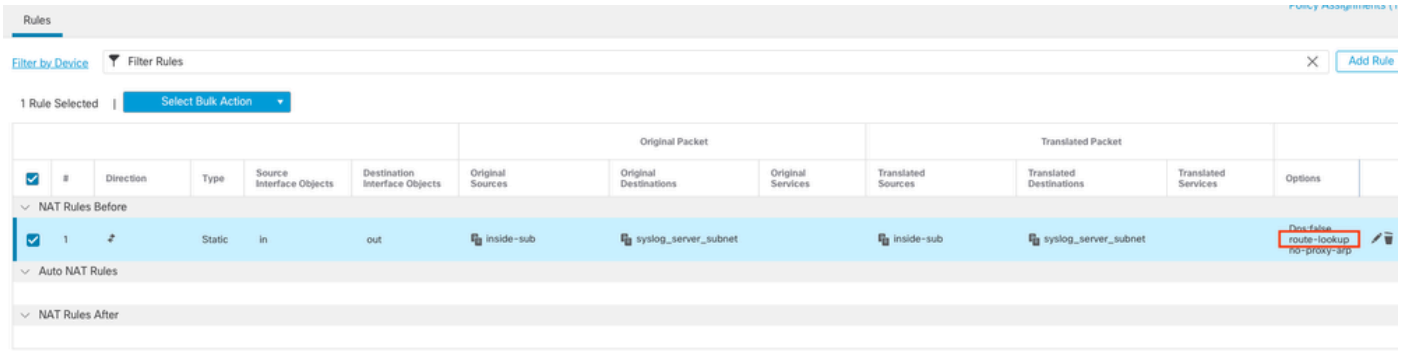
2. Asegúrese de agregar la red de la interfaz de acceso a la administración en Redes protegidas del extremo VPN. (En Dispositivos > Sitio a sitio > Topología VPN > Nodo).



Configuración de redes protegidas

3. Asegúrese de configurar una identidad NAT entre la red de interfaz de acceso a la administración y las redes VPN (una configuración NAT común para el tráfico VPN). Debe seleccionar la opción Realizar Búsqueda de Ruta para la Interfaz de Destino en la sección Avanzado de la regla NAT.

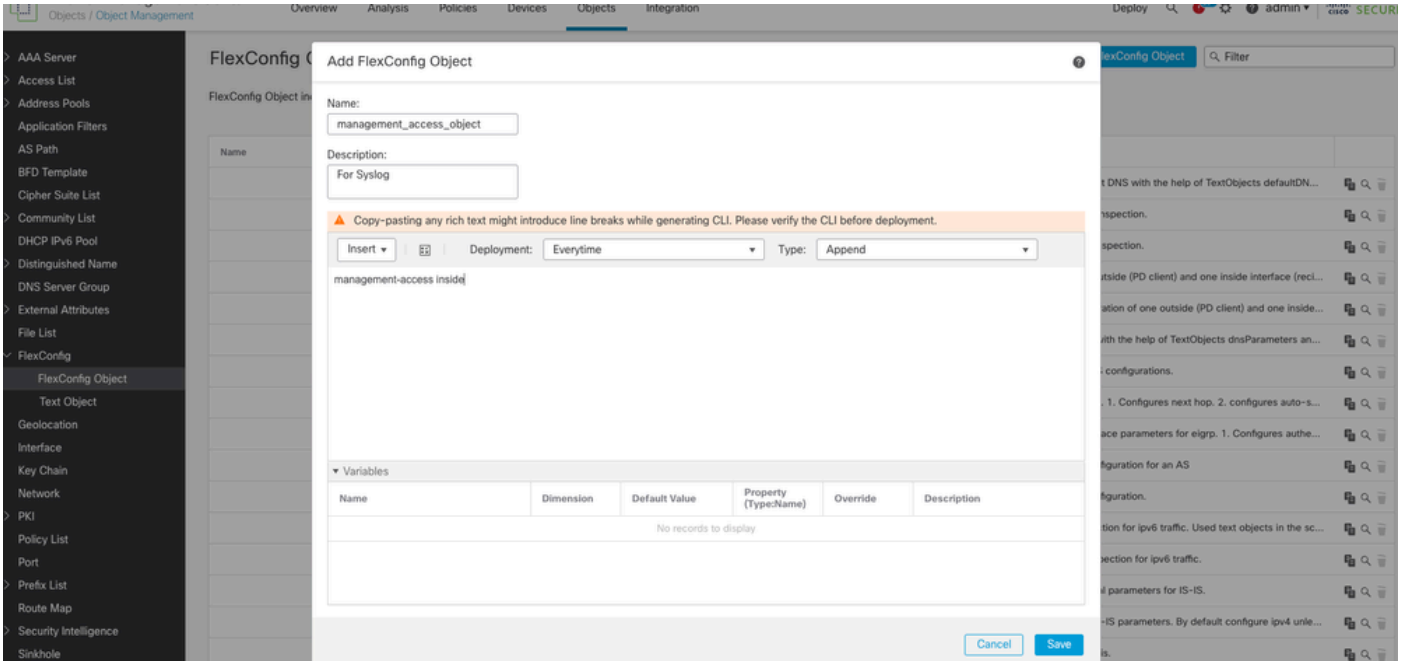
Sin la búsqueda de rutas, el FTD envía el tráfico a través de la interfaz especificada en la configuración de NAT, independientemente de lo que diga la tabla de ruteo.



Configuración NAT de identidad

4. Ahora puede configurar management-access <nombre de interfaz> (en este escenario management-access inside) en Objetos > Administración de objetos > Objeto FlexConfig .

Asígnelo a la política FlexConfig del dispositivo de destino e implemente la configuración.



Configuración de FlexConfig

Verificación

Configuración de acceso a la gestión:

<#root>

```
firepower#
```

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

```
management-access inside
```

Configuración 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

Tráfico de Syslog enviado a través del 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
```

Información Relacionada

- Configuración del inicio de sesión en FTD mediante el FMC
- Configuración de VPN de sitio a sitio en FTD gestionado por FMC

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).