Configure FTD Data Interface For Syslog Over VPN Tunnel

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

- Diagram

Configure

Verify

Related information

Introduction

This document describes how to configure Cisco FTD Data interface as source for Syslogs sent over VPN tunnel.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Syslog configuration on Cisco Secure Firewall Threat Defense (FTD)
- General Syslog
- Cisco Secure Firewall Management Center (FMC)

Components Used

The information in this document is based on this software and hardware version:

- Cisco FTD version 7.3.1
- Cisco FMC version 7.3.1

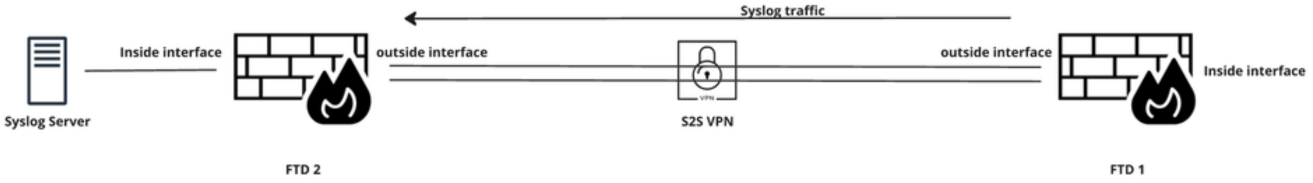
Disclaimer: The networks and IP addresses referenced in this document are not associated with any individual users, groups, or organizations. This configuration has been created exclusively for use in a lab environment.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

This document describes a solution to use one of the data interface of FTD as a source for syslogs that have to be sent over a VPN tunnel to Syslog Server that is located in remote site.

Diagram



Network Diagram

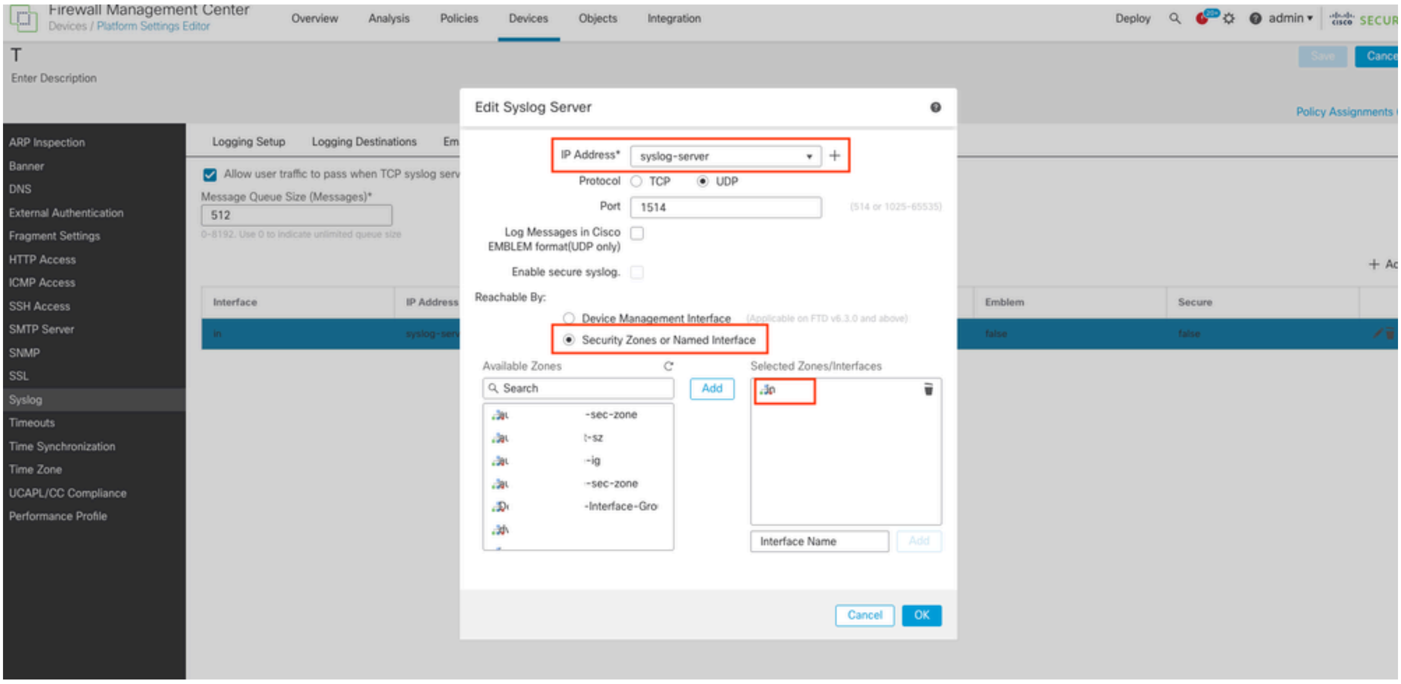
In order to specify the interface from which to source the Syslog traffic sent over the tunnel, you can apply **management-access**command via Flex Config.

This command not only allows you to use a management access interface as the source interface for Syslog messages sent through the VPN tunnel, but also to connect to a data interface via SSH and Ping when using a full tunnel IPsec VPN or SSL VPN client or across a site-to-site IPsec tunnel.

Note: You can define only one management-access interface.

Configure

1. Configure Syslog under **Devices > Platform Settings** for the FTD. Make sure to select **Security Zones** or **Named Interface** option instead of **Device Management Interface** while configuring Syslog Server and choose **management-access interface** to source the Syslog traffic.



Edit Syslog Server

IP Address*: syslog-server

Protocol ○ TCP ● UDP

Port: 1514 (514 or 1025-65535)

Log Messages in Cisco EMBLEM format(UDP only) □

Enable secure syslog. □

Reachable By:

○ Device Management Interface (Applicable on FTD v6.3.0 and above)

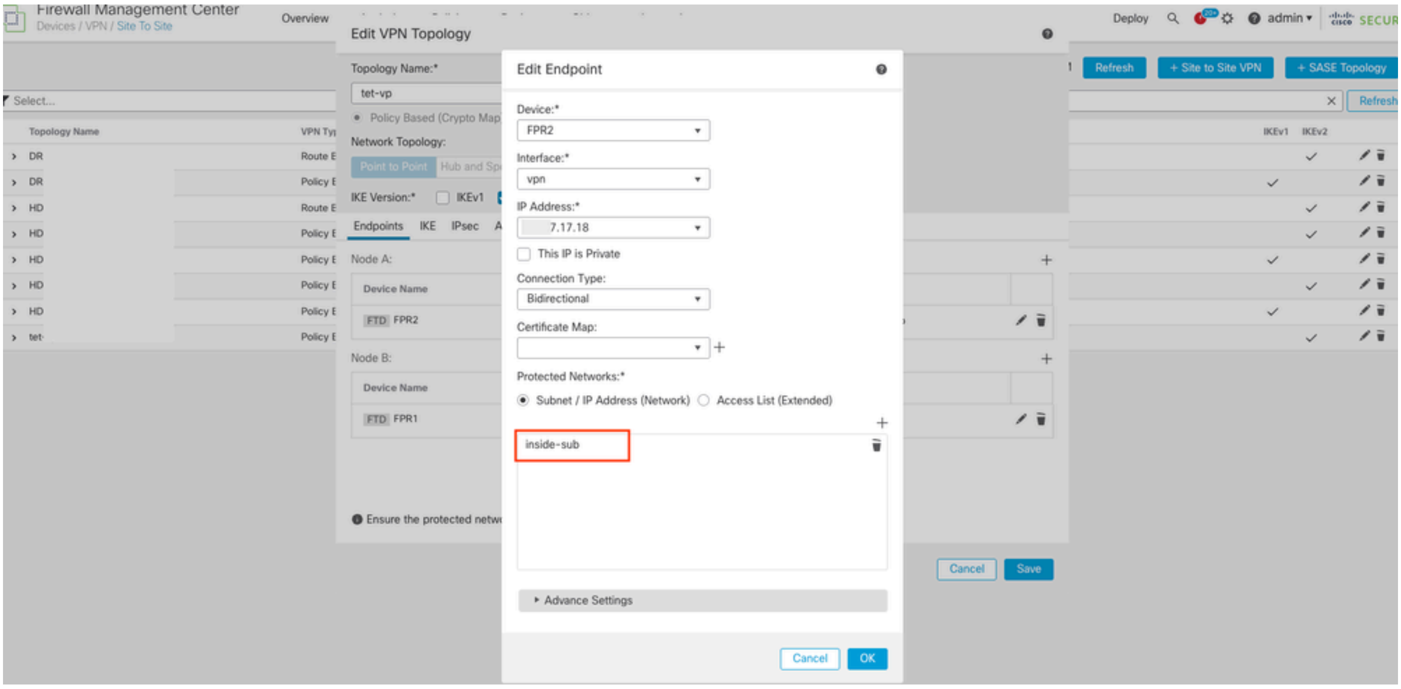
● Security Zones or Named Interface

Available Zones: -sec-zone, -sz, -ig, -sec-zone, -Interface-Gro

Selected Zones/Interfaces: ip

Syslog Server Configuration

2. Make sure to add the **management-access interface** network under **Protected Networks** of VPN Endpoint. (Under **Devices > Site To Site > VPN Topology > Node**).



Edit Endpoint

Device:* FPR2

Interface:* vpn

IP Address:* 7.17.18

□ This IP is Private

Connection Type: Bidirectional

Certificate Map:

Protected Networks:*

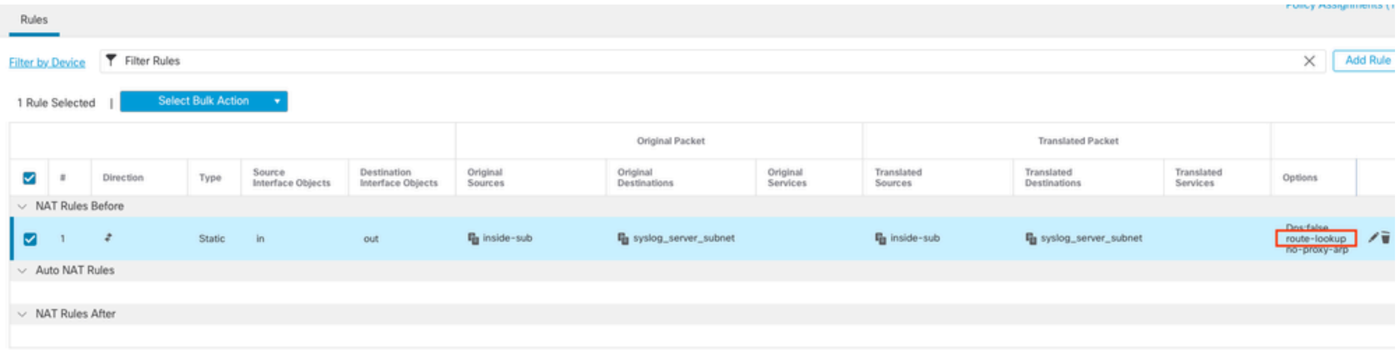
● Subnet / IP Address (Network) ○ Access List (Extended)

inside-sub

Protected Networks Configuration

3. Make sure to configure an identity NAT between the management-access interface network and VPN networks (a common NAT configuration for VPN traffic). You must select option **Perform Route Lookup for Destination Interface** under **Advanced** section of NAT rule.

Without route lookup, the FTD sends traffic out through the interface specified in the NAT configuration, regardless of what the routing table says.

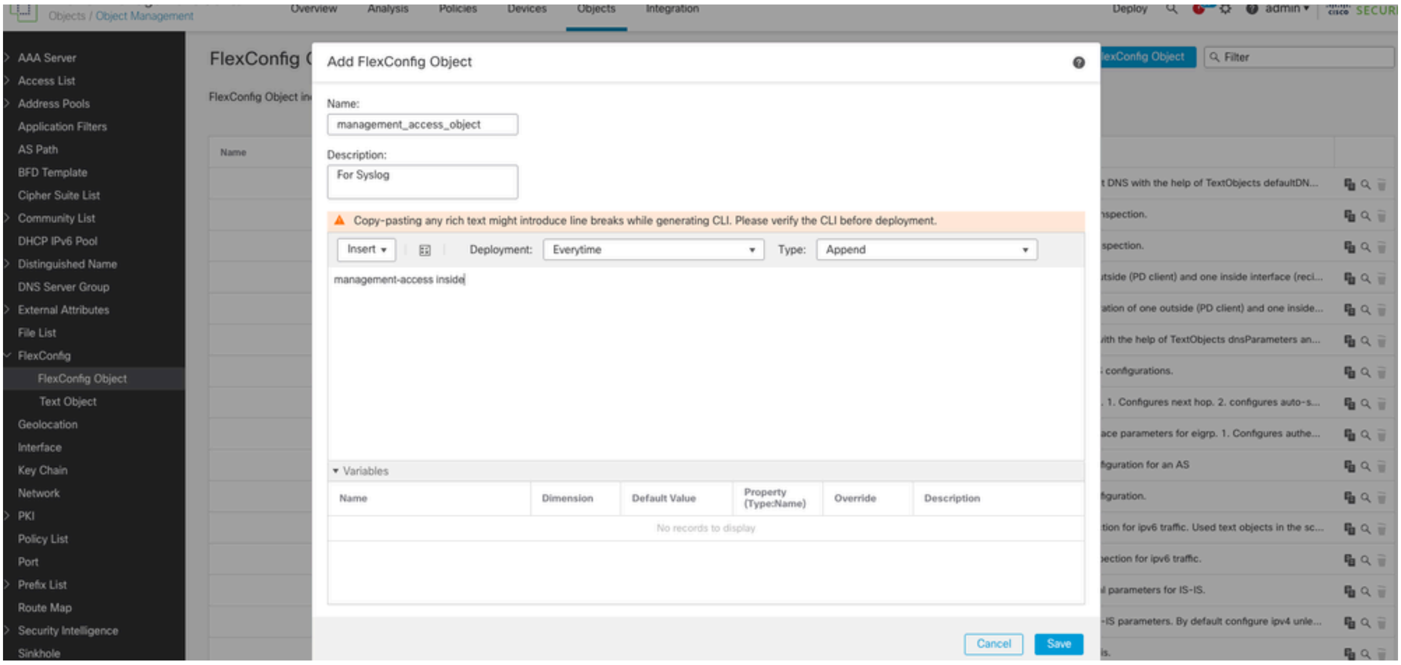


	#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Packet Original Sources	Original Destinations	Original Services	Translated Packet Translated Sources	Translated Destinations	Translated Services	Options
NAT Rules Before												
☑	1	⇄	Static	in	out	inside-sub	syslog_server_subnet		inside-sub	syslog_server_subnet		Dns:false route-lookup no-proxy-arp
Auto NAT Rules												
NAT Rules After												

Identity NAT Configuration

4. You can now configure **management-access <interface name>** (in this scenario **management-access inside**) under **Objects > Object Management > FlexConfig Object** .

Assign it to targeted device **FlexConfig Policy** and **Deploy** the configuration.



Add FlexConfig Object

Name: management_access_object

Description: For Syslog

Copy-pasting any rich text might introduce line breaks while generating CLI. Please verify the CLI before deployment.

Insert ▾ Deployment: Everytime ▾ Type: Append ▾

```
management-access inside
```

▾ Variables

Name	Dimension	Default Value	Property (Type:Name)	Override	Description
No records to display					

FlexConfig Configuration

Verify

Management Access configuration:

<#root>

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

management-access inside
```

Syslog configuration:

<#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 traffic sent over VPN tunnel:

<#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
```

Related information

- Configure Logging on FTD via FMC
- Configure Site to Site VPN on FTD Managed by FMC