Configurer l'interface de données FTD pour le tunnel Syslog sur VPN

Table des matières

Introduction

Ce document décrit comment configurer l'interface de données Cisco FTD comme source pour les Syslogs envoyés sur le tunnel VPN.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration Syslog sur Cisco Secure Firewall Threat Defense (FTD)
- Syslog général
- Cisco Secure Firewall Management Center (FMC)

Composants utilisés

Les informations contenues dans ce document sont basées sur la version logicielle et matérielle suivante :

- Cisco FTD version 7.3.1
- Cisco FMC version 7.3.1

Avertissement : les réseaux et les adresses IP référencés dans ce document ne sont associés à aucun utilisateur, groupe ou organisation individuel. Cette configuration a été créée exclusivement pour une utilisation dans un environnement de travaux pratiques.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Ce document décrit une solution pour utiliser l'une des interfaces de données de FTD comme source pour les syslogs qui doivent être envoyés sur un tunnel VPN au serveur Syslog qui est situé dans le site distant.

Diagramme

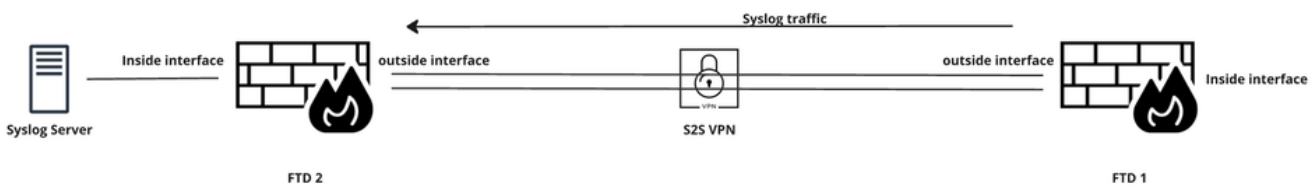
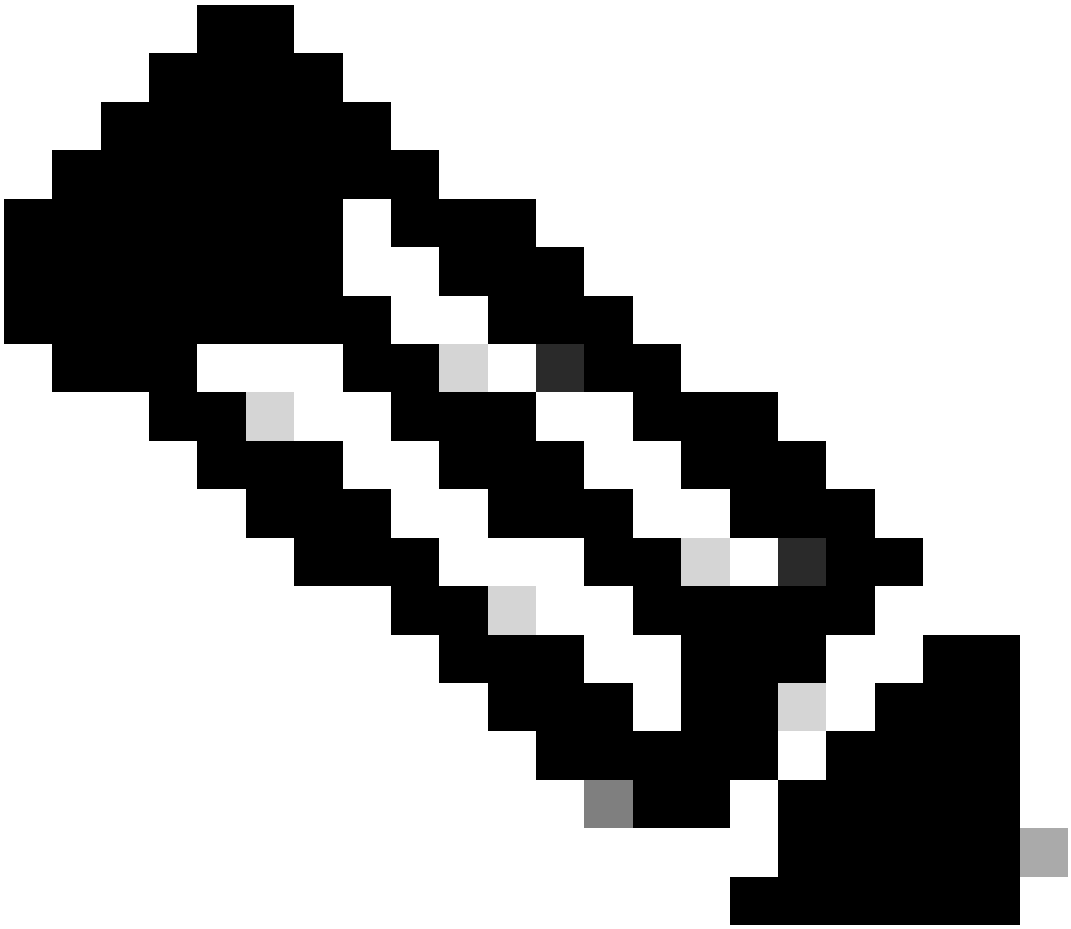


Diagramme du réseau

Afin de spécifier l'interface à partir de laquelle la source du trafic Syslog envoyé sur le tunnel, vous pouvez appliquer la commande **management-**access via Flex Config.

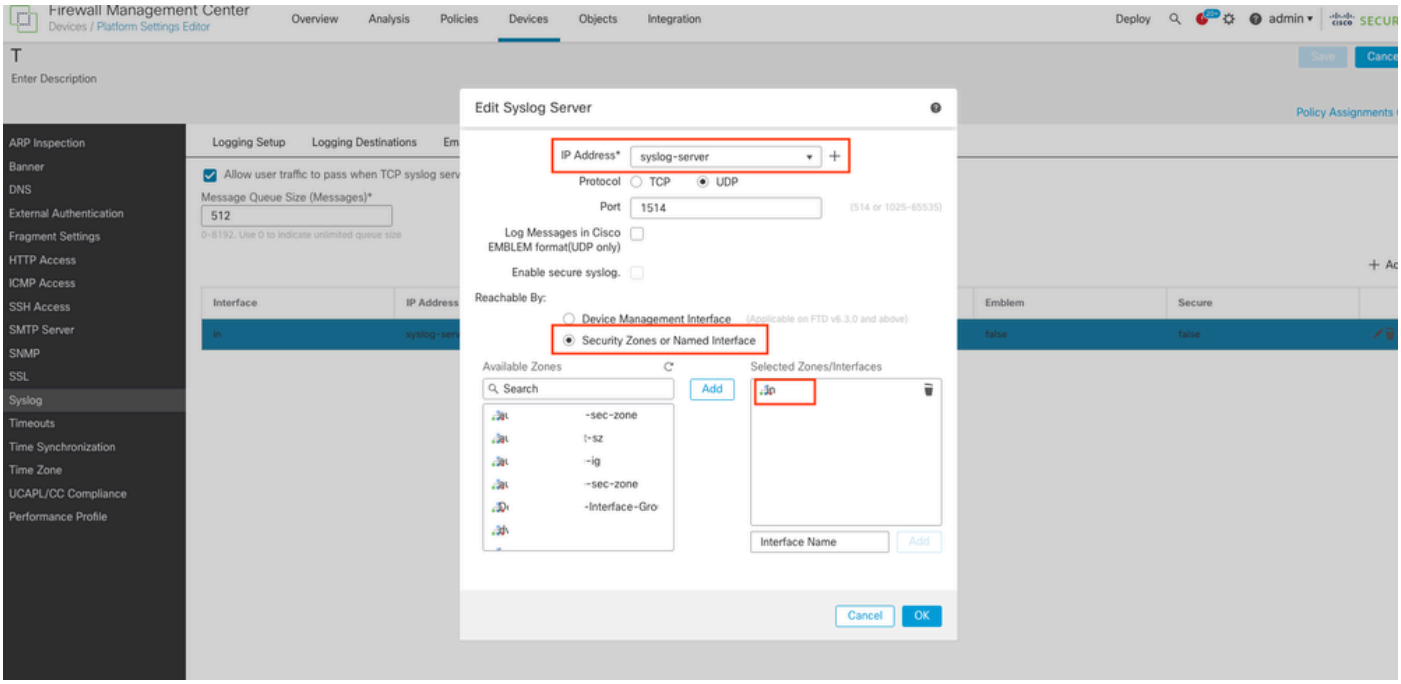
Cette commande vous permet non seulement d'utiliser une interface d'accès à la gestion comme interface source pour les messages Syslog envoyés via le tunnel VPN, mais aussi de vous connecter à une interface de données via SSH et Ping lors de l'utilisation d'un tunnel complet VPN IPsec ou d'un client VPN SSL ou via un tunnel IPsec site à site.



Remarque : Vous ne pouvez définir qu'une seule interface d'accès à la gestion.

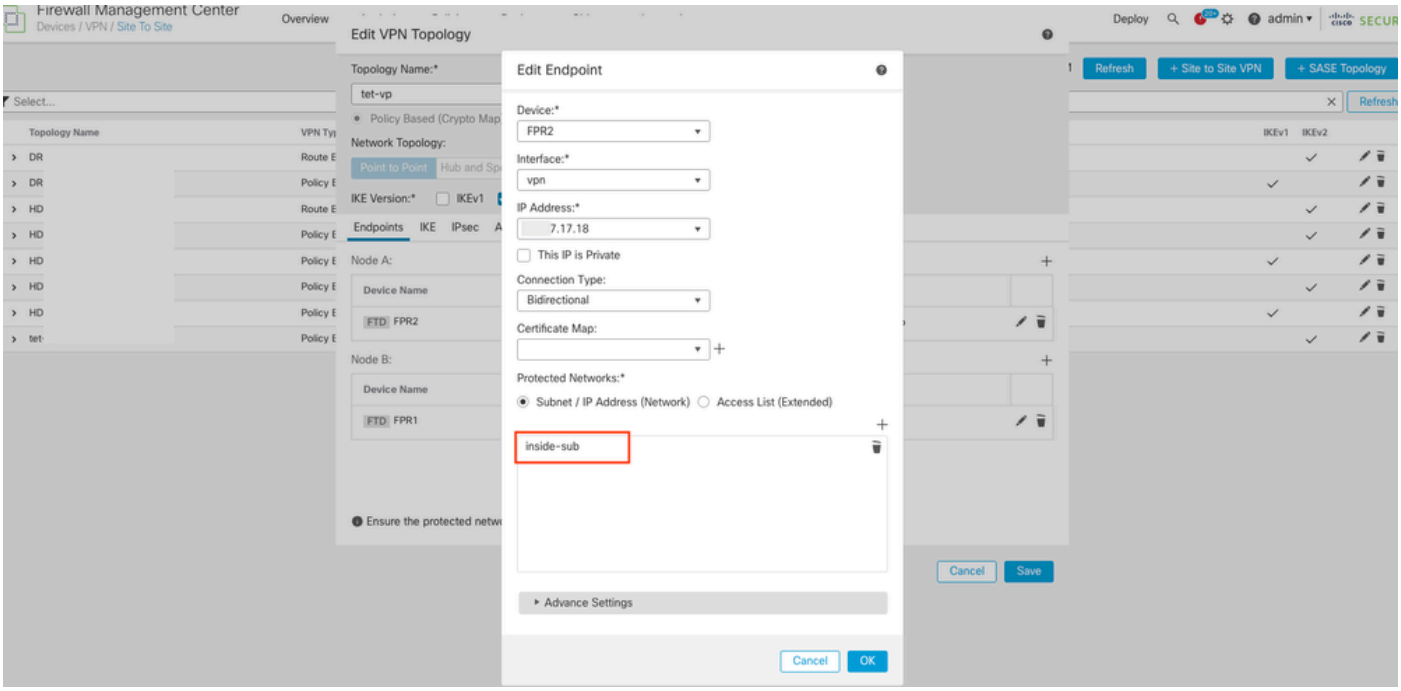
Configurer

1. Configurez Syslog sous Devices > Platform Settings pour le FTD. Veillez à sélectionner l'option Security Zones ou Named Interface au lieu de l'option Device Management Interface lors de la configuration du serveur Syslog et choisissez management-access interface pour générer le trafic Syslog.



Configuration du serveur Syslog

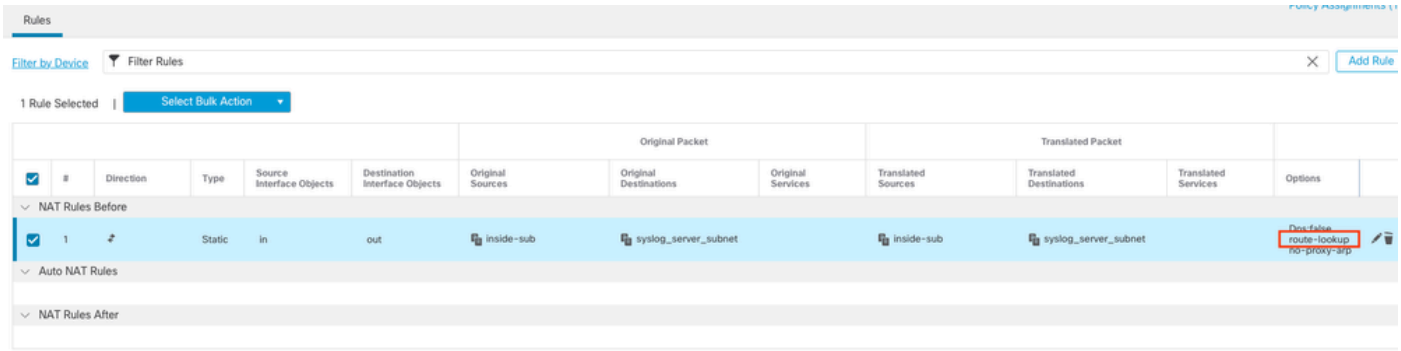
2. Assurez-vous d'ajouter le réseau d'interface d'accès à la gestion sous Réseaux protégés du terminal VPN. (Sous Devices > Site To Site > VPN Topology > Node).



Configuration des réseaux protégés

3. Assurez-vous de configurer une NAT d'identité entre le réseau d'interface d'accès à la gestion et les réseaux VPN (configuration NAT commune pour le trafic VPN). Vous devez sélectionner l'option Perform Route Lookup for Destination Interface sous la section Advanced de la règle NAT.

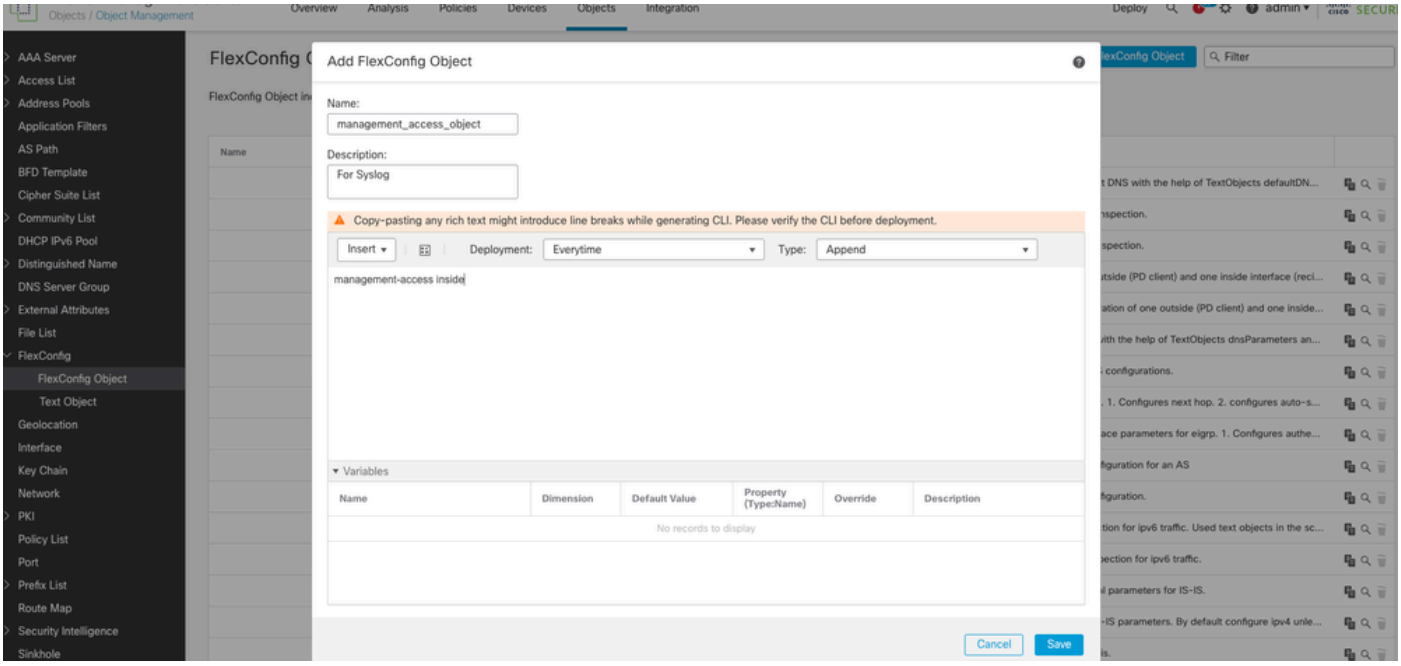
Sans recherche de route, le FTD envoie le trafic par l'interface spécifiée dans la configuration NAT, indépendamment de ce que dit la table de routage.



Configuration NAT d'identité

4. Vous pouvez maintenant configurer management-access <nom de l'interface> (dans ce scénario management-access inside) sous Objets > Gestion des objets > FlexConfig Object .

Attribuez-le à la politique FlexConfig du périphérique ciblé et déployez la configuration.



Configuration FlexConfig

Vérifier

Configuration d'accès de gestion :

<#root>

```
firepower#
```

`show run | in management-access`

```
management-access inside
```

Configuration 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

Trafic Syslog envoyé sur le tunnel 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
```

Informations connexes

- Configurez la connexion sur Cisco FTD à l'aide de Cisco FMC
- Configurer un VPN site à site sur FTD géré par FMC

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.