Configurazione dell'interfaccia dati FTD per Syslog su tunnel VPN

Sommario

Introduzione

In questo documento viene descritto come configurare Cisco FTD Data interface come origine per i syslog inviati tramite tunnel VPN.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione syslog su Cisco Secure Firewall Threat Defense (FTD)
- Syslog generale
- Cisco Secure Firewall Management Center (FMC)

Componenti usati

Le informazioni di questo documento si basano sulla seguente versione software e hardware:

- Cisco FTD versione 7.3.1
- Cisco FMC versione 7.3.1

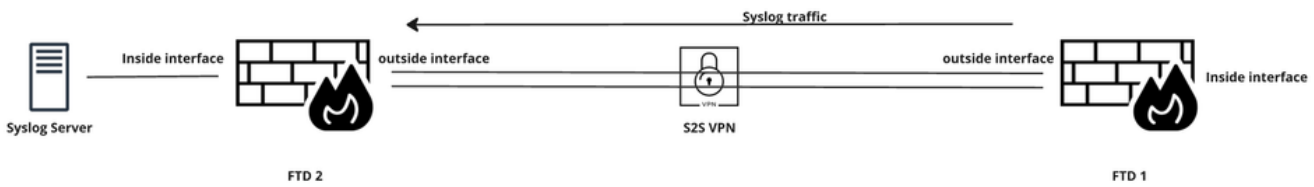
Avvertenza: le reti e gli indirizzi IP menzionati in questo documento non sono associati a singoli utenti, gruppi o organizzazioni. Questa configurazione è stata creata esclusivamente per l'uso in ambienti lab.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Questo documento descrive una soluzione per usare una delle interfacce dati di FTD come origine per i syslog che devono essere inviati su un tunnel VPN al server Syslog che si trova nel sito remoto.

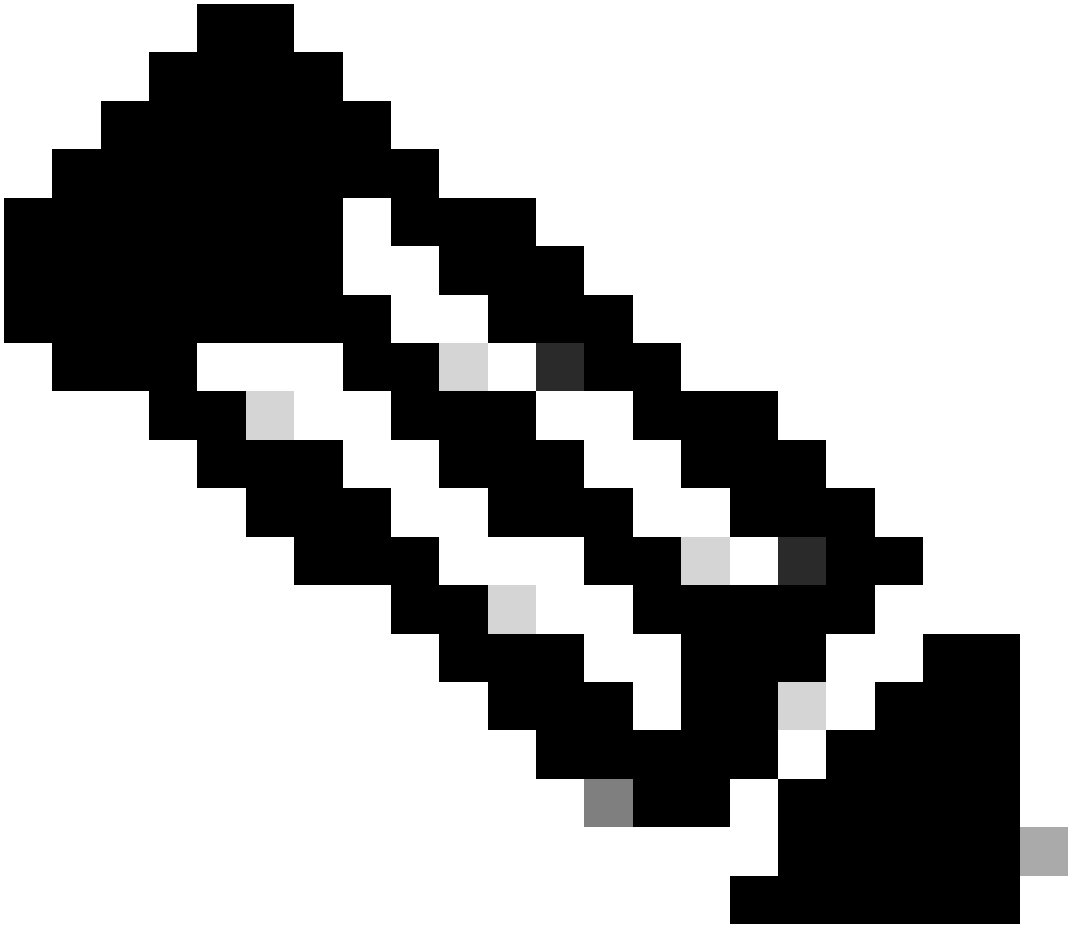
Diagramma



Esempio di rete

Per specificare l'interfaccia da cui originare il traffico Syslog inviato sul tunnel, è possibile applicare il comando **management-**access tramite la configurazione Flex.

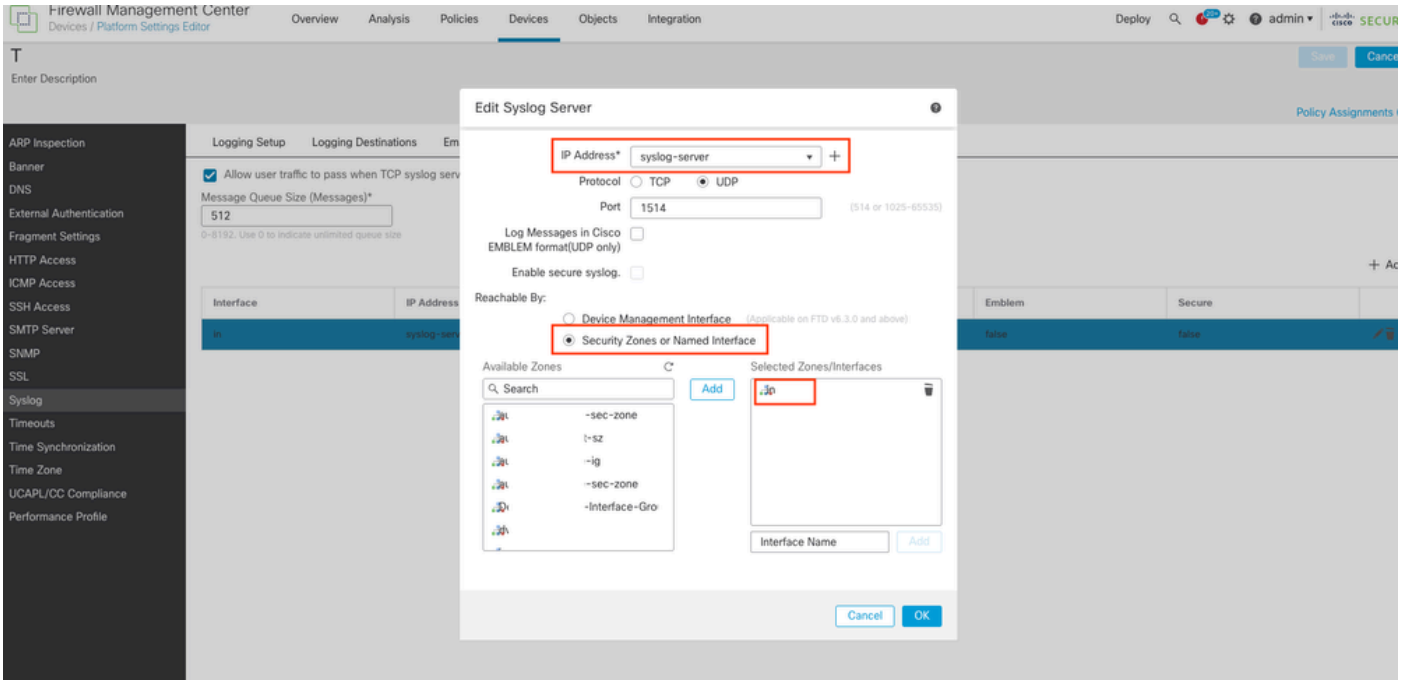
Questo comando non solo consente di utilizzare un'interfaccia di accesso di gestione come interfaccia di origine per i messaggi Syslog inviati tramite il tunnel VPN, ma anche di connettersi a un'interfaccia dati tramite SSH e Ping quando si utilizza un client VPN IPsec o SSL per un tunnel IPsec da sito a sito.



Nota: È possibile definire una sola interfaccia di accesso alla gestione.

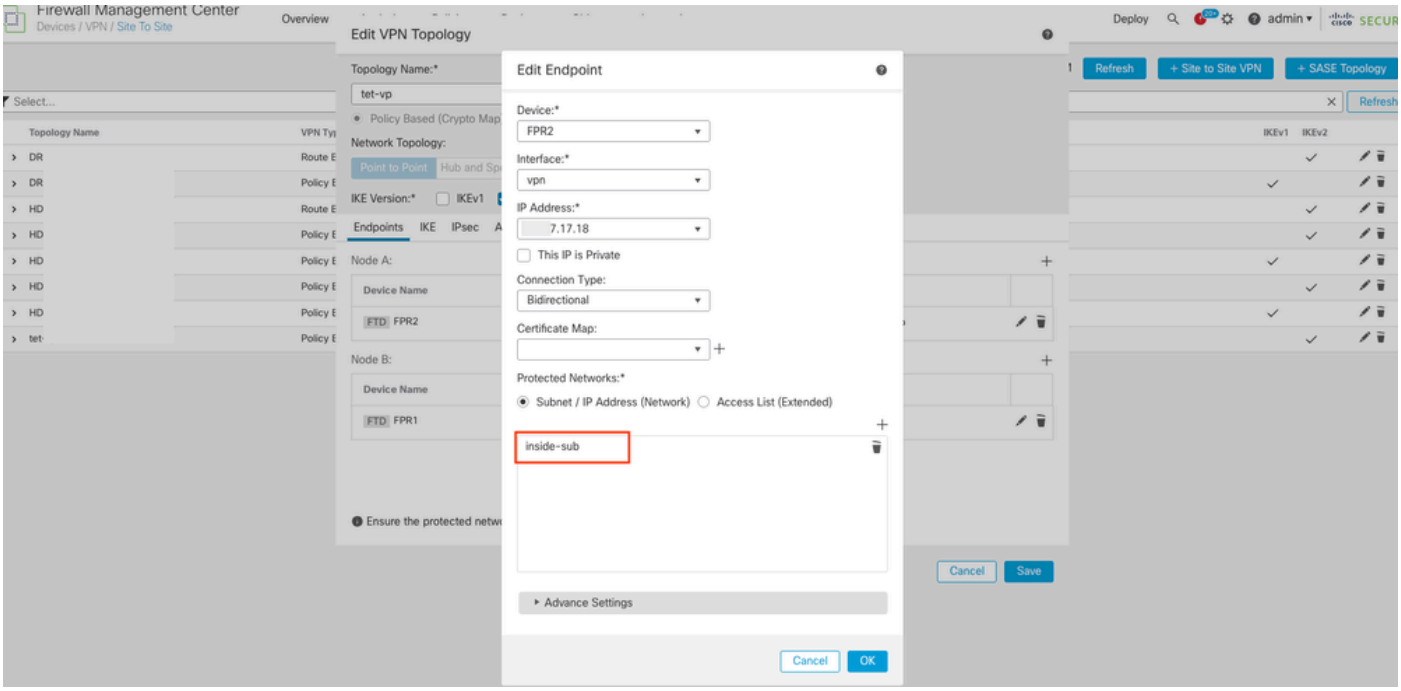
Configurazione

1. Configurare Syslog in Dispositivi > Impostazioni piattaforma per FTD. Accertarsi di selezionare l'opzione Security Zones o Named Interface invece di Device Management Interface durante la configurazione del server Syslog e scegliere l'interfaccia di accesso alla gestione per originare il traffico Syslog.



Configurazione server Syslog

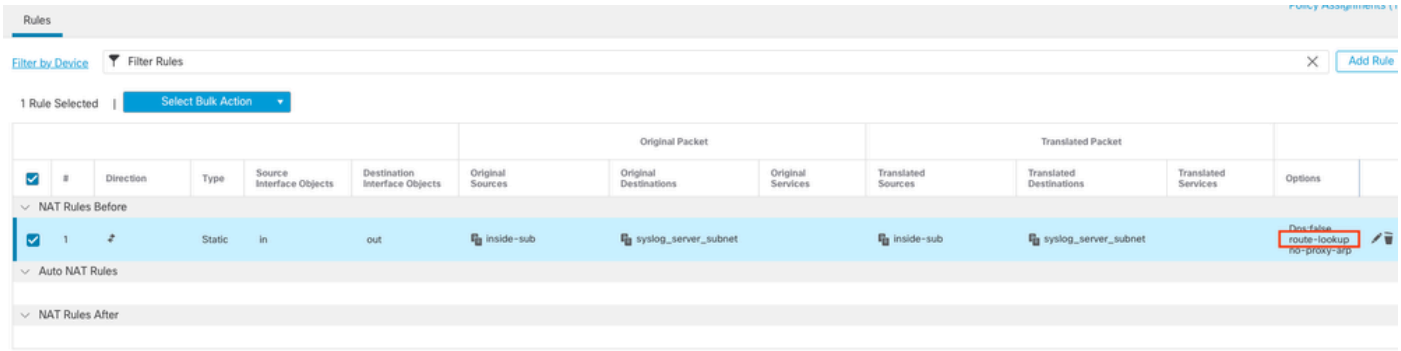
2. Accertarsi di aggiungere la rete dell'interfaccia di accesso alla gestione sotto Reti protette di VPN Endpoint. (In Dispositivi > Da Sito A Sito > Topologia VPN > Nodo).



Configurazione reti protette

3. Accertarsi di configurare un NAT di identità tra la rete dell'interfaccia di accesso alla gestione e le reti VPN (una configurazione NAT comune per il traffico VPN). È necessario selezionare l'opzione Esegui ricerca route per l'interfaccia di destinazione nella sezione Advanced della regola NAT.

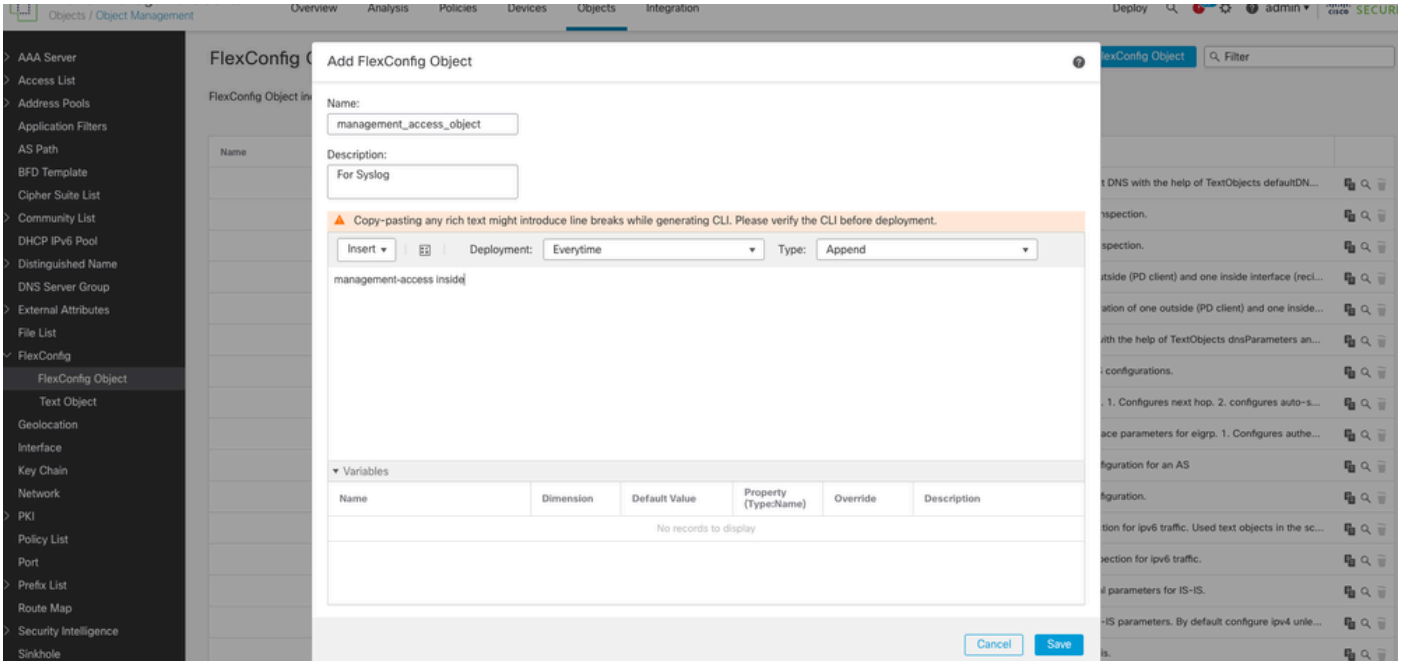
Senza la ricerca del percorso, l'FTD invia il traffico attraverso l'interfaccia specificata nella configurazione NAT, a prescindere da quello che dice la tabella di routing.



Configurazione Identity NAT

4. È ora possibile configurare management-access <nome interfaccia> (in questo scenario management-access interno) in Oggetti > Gestione oggetti > Oggetto FlexConfig .

Assegnarlo al criterio FlexConfig del dispositivo di destinazione e distribuire la configurazione.



Configurazione FlexConfig

Verifica

Configurazione dell'accesso alla gestione:

<#root>

```
firepower#
```

show run | in management-access

```
management-access inside
```

Configurazione 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

Traffico syslog inviato tramite 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
```

Informazioni correlate

- Configurazione dei log sull'FTD tramite FMC
- Configura VPN da sito a sito su FTD Gestito da FMC

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).