Voeg FDM-toegang toe via data-interface wanneer de beheerinterface uitvalt

Inhoud

Inleiding

Dit document beschrijft hoe u toegang tot een Firepower Thread Defence (FTD) kunt toevoegen van HyperText Transfer Protocol (HTTP) wanneer de beheerpoort mislukt.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Toegang tot het apparaat via console

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Firepower 1120 Thread Defence versie 7.4.2

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Configuraties

Stap 1. Maak vanaf de consolesessie van het apparaat verbinding met de FTD Command Line Interface Shell (CLISH):

```
Cisco Firepower Extensible Operating System (FX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2009-2019, Cisco Systems, Inc. All rights reserved.

The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license.

Certain components of this software are licensed under the "GNU General Public
License, version 3" provided with ABSOLUTELY NO WARRANTY under the terms of
"GNU General Public License, Version 3", available here:
http://www.gnu.org/licenses/gpl.html. See User Manual (''Licensing'') for
details.

Certain components of this software are licensed under the "GNU General Public
License, version 2" provided with ABSOLUTELY NO WARRANTY under the terms of
"GNU General Public License, version 2", available here:
http://www.gnu.org/licenses/old-licenses/gpl-2.0.html. See User Manual
(''Licensing'') for details.

Certain components of this software are licensed under the "GNU LESSER GENERAL
PUBLIC LICENSE, version 3" provided with ABSOLUTELY NO WARRANTY under the terms
of "GNU LESSER GENERAL PUBLIC LICENSE" Version 3", available here:
http://www.gnu.org/licenses/lgpl.html. See User Manual (''Licensing'') for
details.

Certain components of this software are licensed under the "GNU Lesser General
Public License, version 2.1" provided with ABSOLUTELY NO WARRANTY under the
terms of "GNU Lesser General Public License, version 2", available here:
http://www.gnu.org/licenses/old-licenses/lgpl-2.1.html. See User Manual
(''Licensing'') for details.

Certain components of this software are licensed under the "GNU Library General
Public License, version 2" provided with ABSOLUTELY NO WARRANTY under the terms
of "GNU Library General Public License, version 2", available here:
http://www.gnu.org/licenses/old-licenses/lgpl-2.0.html. See User Manual
(''Licensing'') for details.

KSEC-FPR1140-1# connect ftd
```

Stap 2. Van de FTD CLISH, heb toegang tot de Linux shell via deskundig bevel en verhef aan admin voorrechten:

```
>
> expert
admin@KSEC-FPR1140-1:/$ sudo su
Password:
root@KSEC-FPR1140-1:/#
```

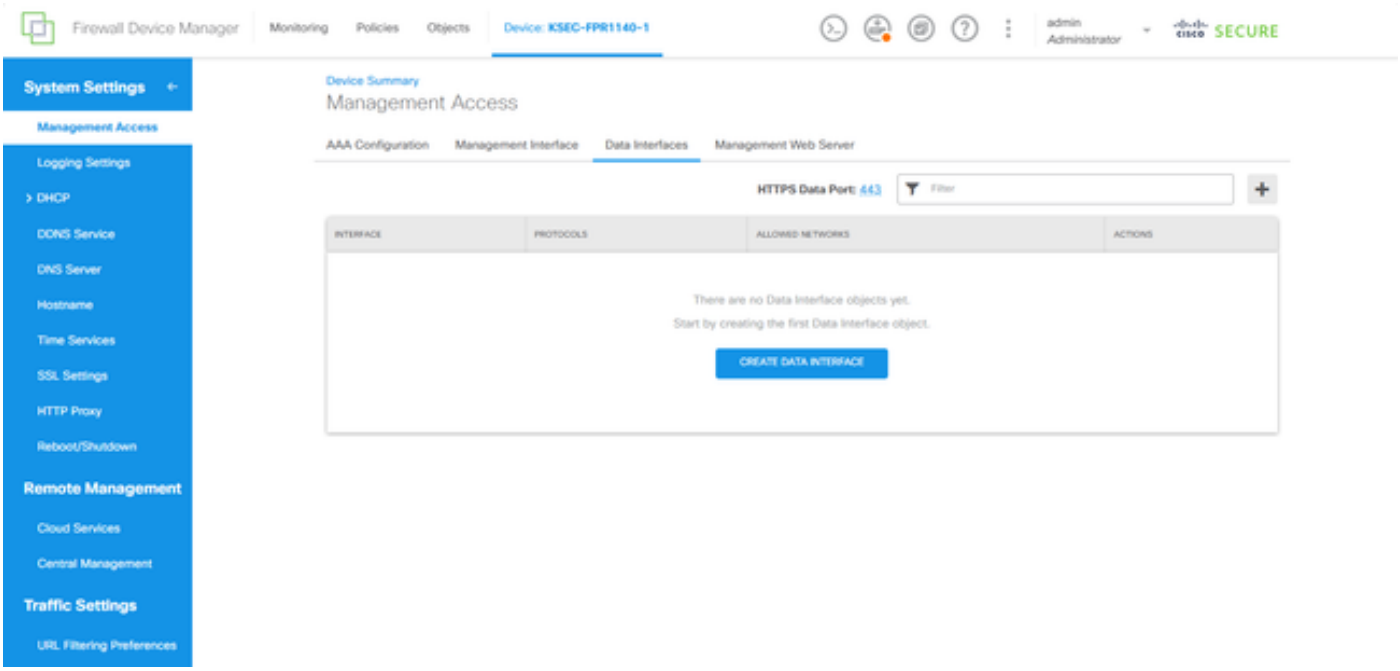
Stap 3. Duw de HTTP-opdrachtvermeldingen naar de Lina-configuratie met de LinaConfigTool en maak een statische route om het verkeer van de webserver die op de Linux-kant draait, naar de interface nlp_int_tap aan de Lina-kant te verzenden:

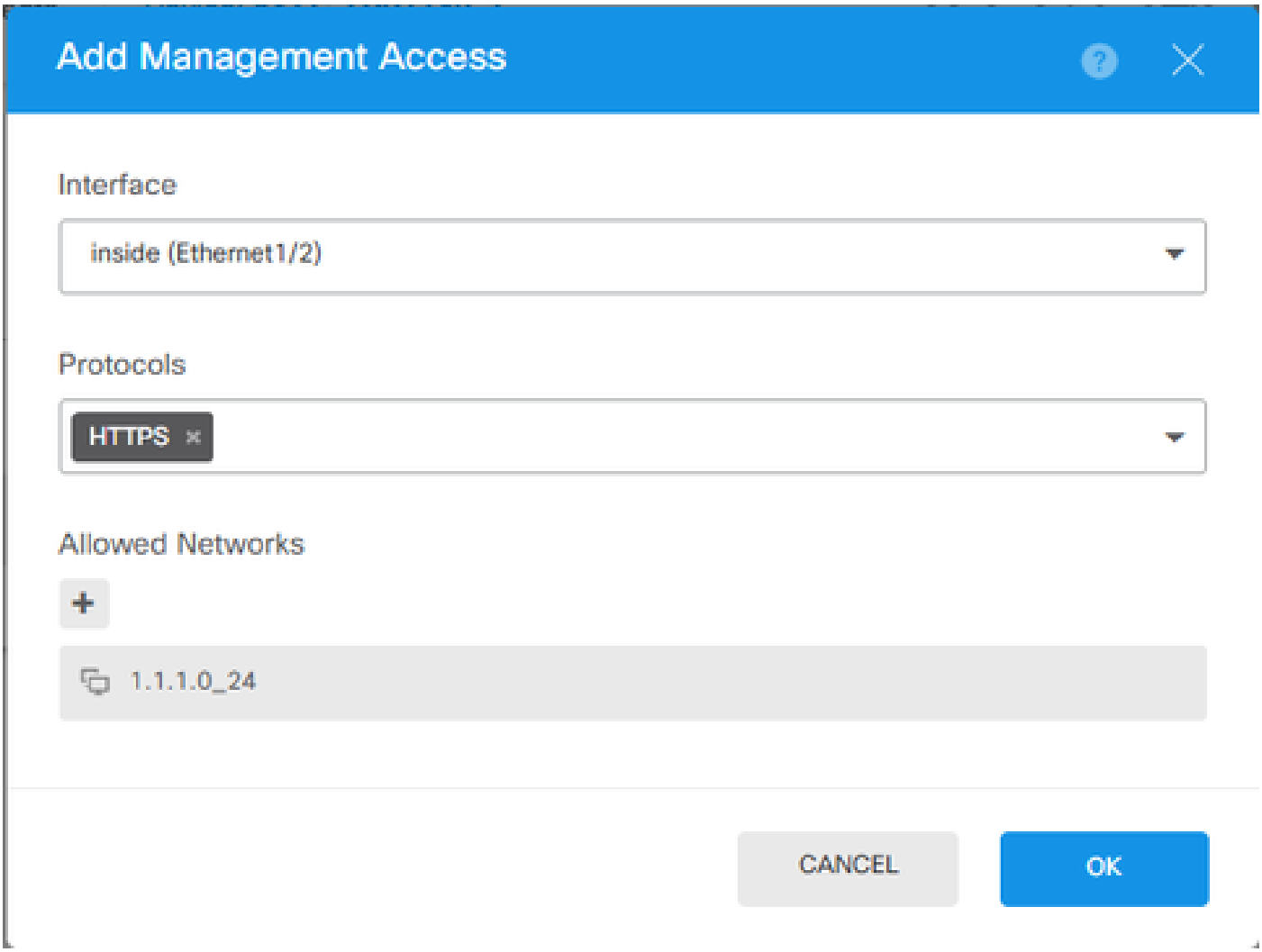
```
root@KSEC-FPR1140-1:/# LinaConfigTool "http 192.168.1.0 255.255.255.0 inside"
root@KSEC-FPR1140-1:/#
root@KSEC-FPR1140-1:/# ip route add 192.168.1.0/24 via 169.254.1.1
root@KSEC-FPR1140-1:/#
root@KSEC-FPR1140-1:/#
```

Stap 4. Ga terug naar de FTD-CLISH en bevestig dat de NAT-regel (Network Address Translation) automatisch wordt gemaakt:

```
root@KSEC-FPR1140-1:/#
root@KSEC-FPR1140-1:/#
root@KSEC-FPR1140-1:/# exit
exit
admin@KSEC-FPR1140-1:/$ exit
logout
> show nat detail
Manual NAT Policies Implicit (Section 0)
1 (nlp_int_tap) to (inside) source static nlp_server__http_192.168.1.0_intf4 interface  destination sta
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 169.254.1.3/32, Translated: 10.10.105.87/24
    Destination - Origin: 192.168.1.0/24, Translated: 192.168.1.0/24
    Service - Protocol: tcp Real: https Mapped: https
```

Stap 5. Open de FDM UI op de data-interface en maak de beheertoegang op de data-interface van de UI om de wijzigingen permanent te houden:





Verifiëren

Open een browser en probeer FDM te bereiken met behulp van de data-interface IP adres.

Problemen oplossen

Voer een pakketopname uit en bevestig dat:

- Het verkeer bereikt de data-interface.
- Het verkeer wordt doorgestuurd naar de interface nlp_int_tap.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.