# FDM-Zugriff über Datenschnittstelle bei Ausfall der Verwaltungsschnittstelle

## Inhalt



## Einleitung

In diesem Dokument wird beschrieben, wie der HTTP-Zugriff (HyperText Transfer Protocol) zu einem FirePOWER Thread Defense (FTD) hinzugefügt wird, wenn der Management-Port ausfällt.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Konsolenzugriff auf das Gerät

### Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Firepower 1120 Thread Defense Version 7.4.2

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

## Konfigurieren

### Konfigurationen

Schritt 1: Verbinden Sie sich von der Konsolensitzung des Geräts aus mit der FTD-Befehlszeilenschnittstelle 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
```

Schritt 2: Greifen Sie von der FTD-CLISH aus über den Expertenbefehl auf die Linux-Shell zu, und erweitern Sie die Administratorberechtigungen:

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

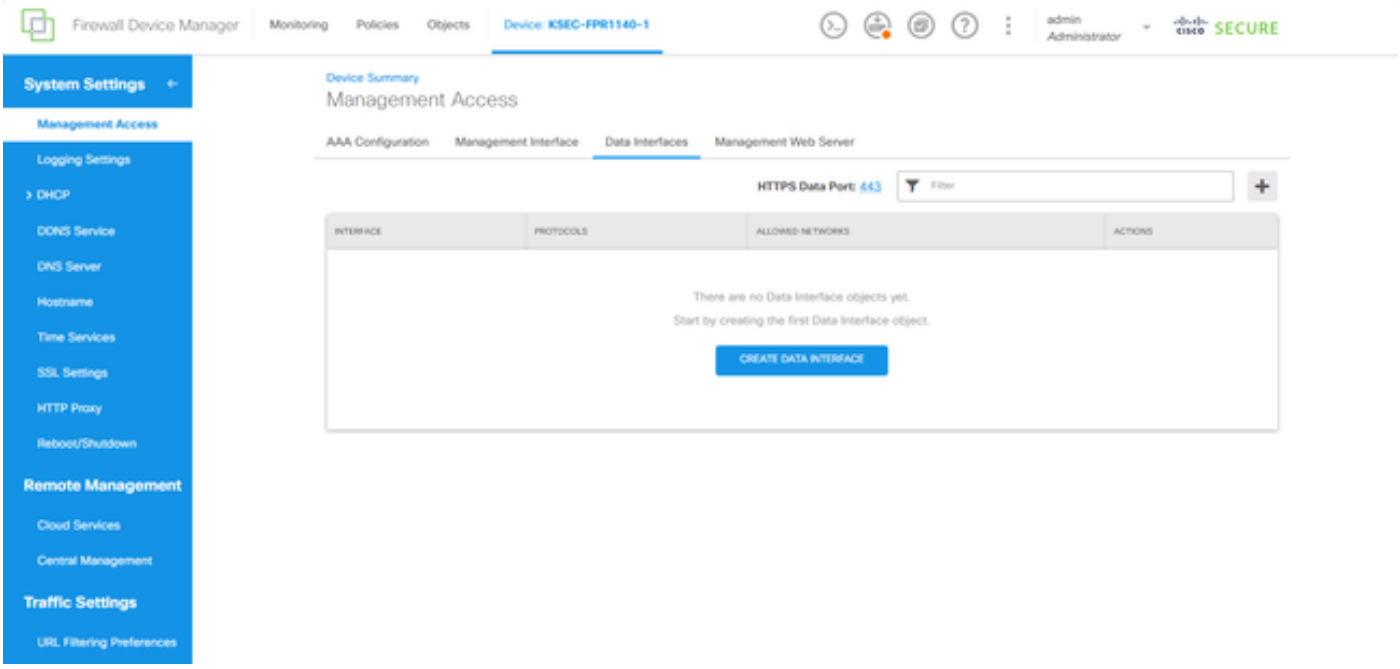
Schritt 3: Push der HTTP-Befehlseinträge in die Lina-Konfiguration mit dem LinaConfigTool und Erstellen einer statischen Route, um den Datenverkehr vom Linux-basierten Webserver an die Schnittstelle nlp_int_tap auf der Lina-Seite zu senden:

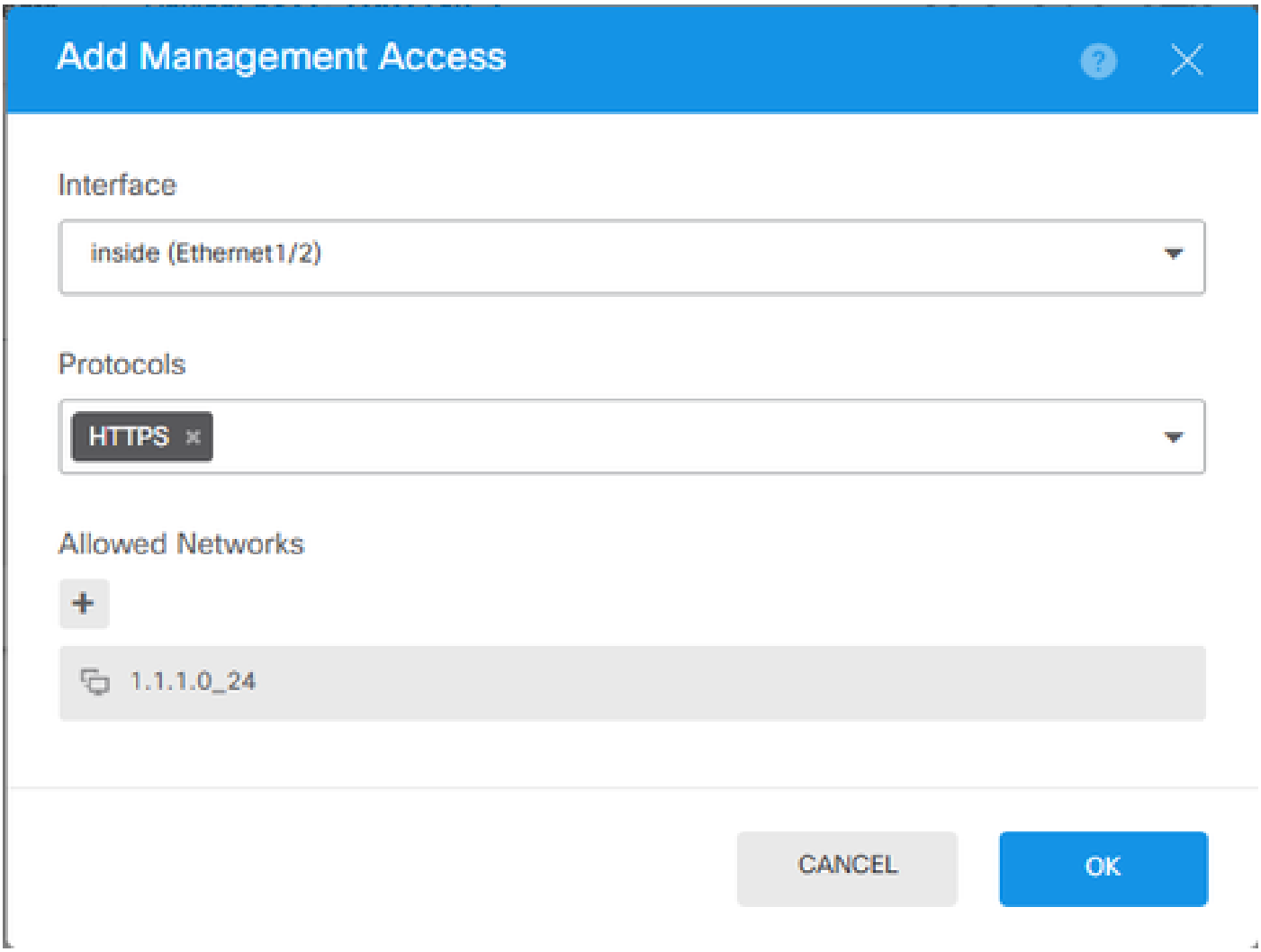
```
root@KSEC-FPR1140-1:/# LinaConfigTool "http 192.168.1.0 255.255.255.0 inside"
root@KSEC-FPR1140-1:/#
root@KSEC-FPR1140-1:/# ip route add 192.168.1.0/24 via 169.254.1.1
root@KSEC-FPR1140-1:/#
root@KSEC-FPR1140-1:/#
```

Schritt 4: Kehren Sie zur FTD-CLISH zurück, und bestätigen Sie, dass die NAT-Regel (Network Address Translation) automatisch erstellt wird:

```
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
```

Schritt 5: Greifen Sie auf die FDM-Benutzeroberfläche auf der Datenschnittstelle zu, und erstellen Sie den Verwaltungszugriff auf der Datenschnittstelle von der Benutzeroberfläche aus, um die Änderungen dauerhaft beizubehalten:




## Überprüfung

Öffnen Sie einen Browser, und versuchen Sie, FDM über die IP-Adresse der Datenschnittstelle zu erreichen.


# Fehlerbehebung

Führen Sie eine Paketerfassung durch, und bestätigen Sie, dass:

- Der Datenverkehr erreicht die Datenschnittstelle.
- Der Datenverkehr wird an die Schnittstelle nlp_int_tap weitergeleitet.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.