Add FDM Access Through Data Interface When Management Interface Fails

Contents

Introduction

This document describes how to add HyperText Transfer Protocol (HTTP) access to a Firepower Thread Defense (FTD) when the management port fails.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Console access to the device

Components Used

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

- Cisco Firepower 1120 Thread Defense version 7.4.2

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.

Configure

Configurations

Step 1. From the console session of the device, connect to the 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
```

Step 2. From the FTD CLISH, access the Linux shell via expert command and elevate to admin privileges:

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

Step 3. Push the HTTP command entries to the Lina configuration using the LinaConfigTool and create a static route to send the traffic from the Web server running on the Linux side to the nlp_int_tap interface on the Lina side:

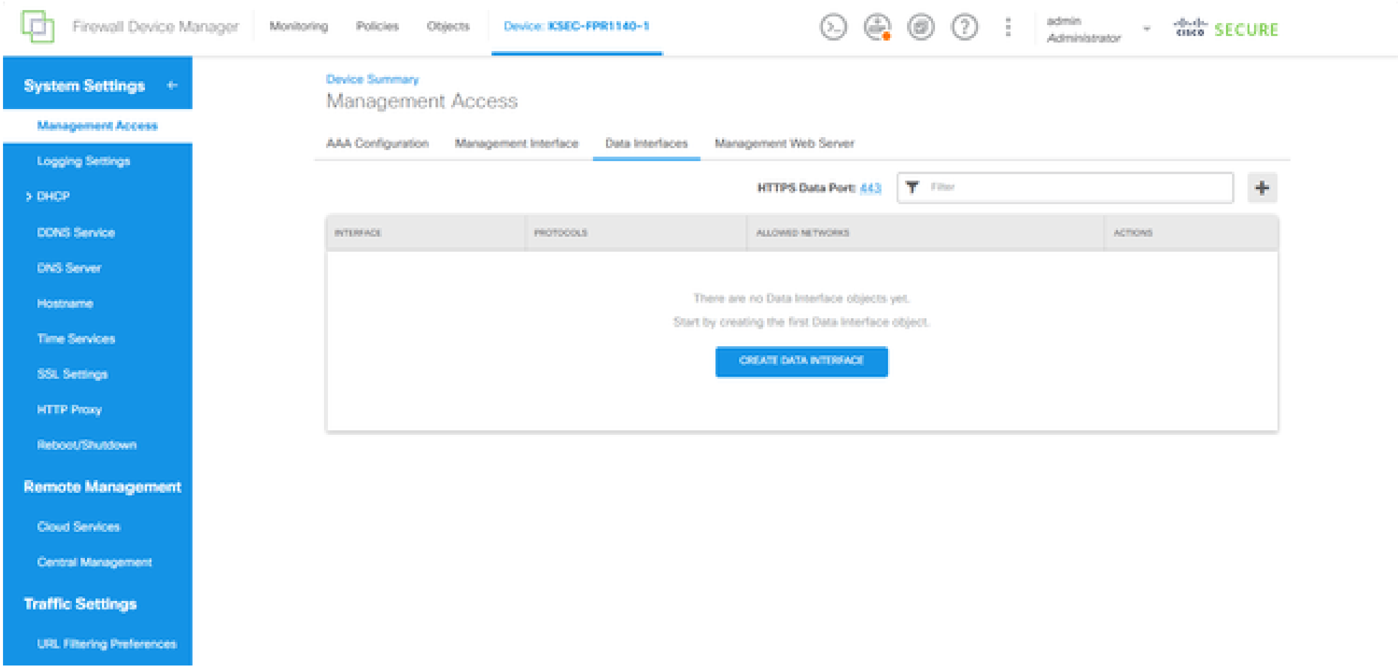
```
root@KSEC-FPR1140-1:/# LinaConfigTool "http 192.168.1.0 255.255.255.0 inside"
root@KSEC-FPR1140-1:/#
root@KSEC-FPR1140-1:/# ip route add 192.168.1.0/24 via 169.254.1.1
```

```
root@KSEC-FPR1140-1:/#
root@KSEC-FPR1140-1:/#
```

Step 4. Go back to the FTD CLISH and confirm that the Network Address Translation (NAT) rule is automatically created:

```
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
```

Step 5. Access the FDM UI on the data interface and create the management access on the data interface from the UI to keep the changes permanent:

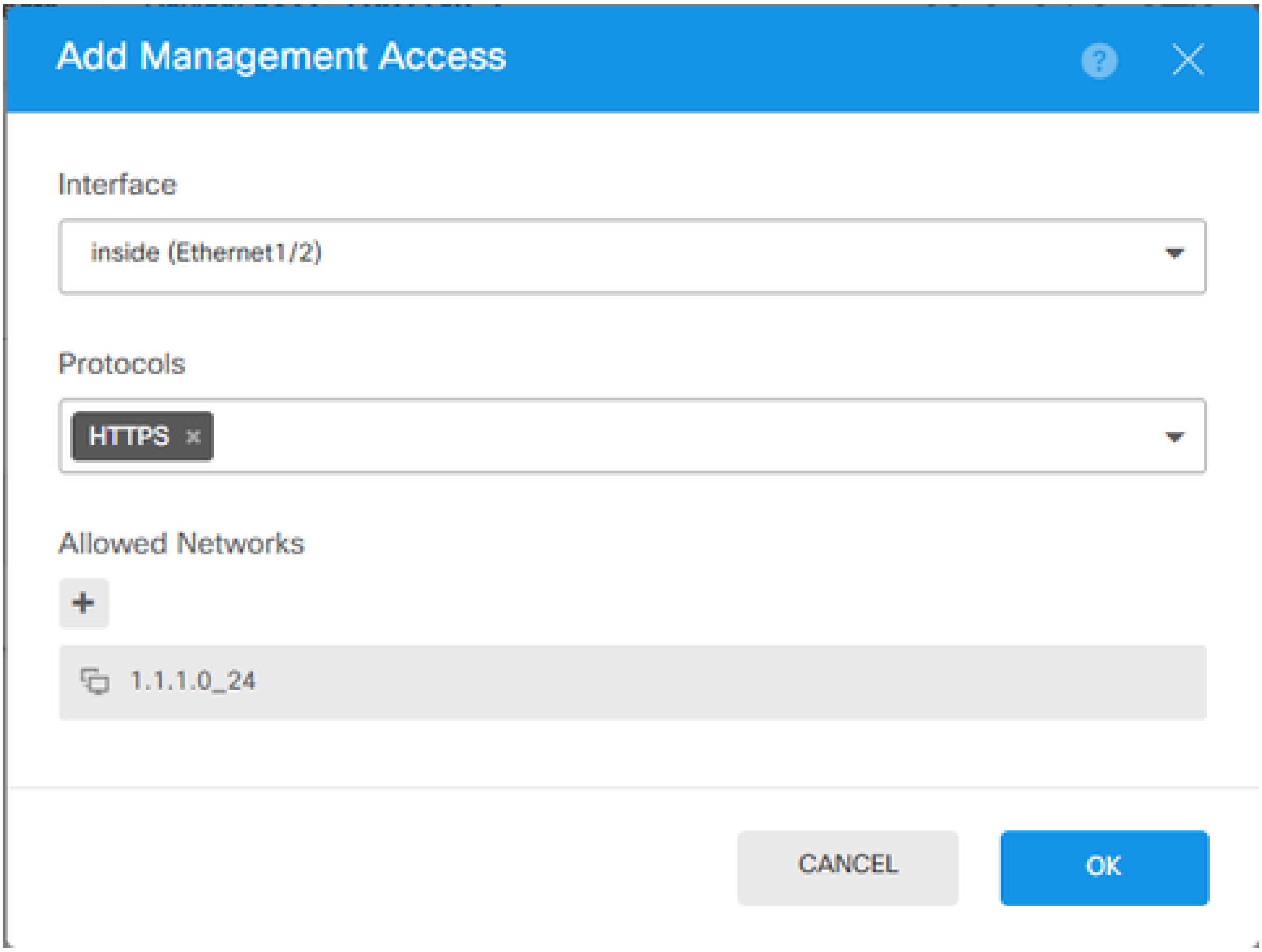


Management Access

HTTPS Data Port: 443

INTERFACE	PROTOCOLS	ALLOWED NETWORKS	ACTIONS

There are no Data Interface objects yet.
Start by creating the first Data Interface object.



Add Management Access

Interface

inside (Ethernet1/2)

Protocols

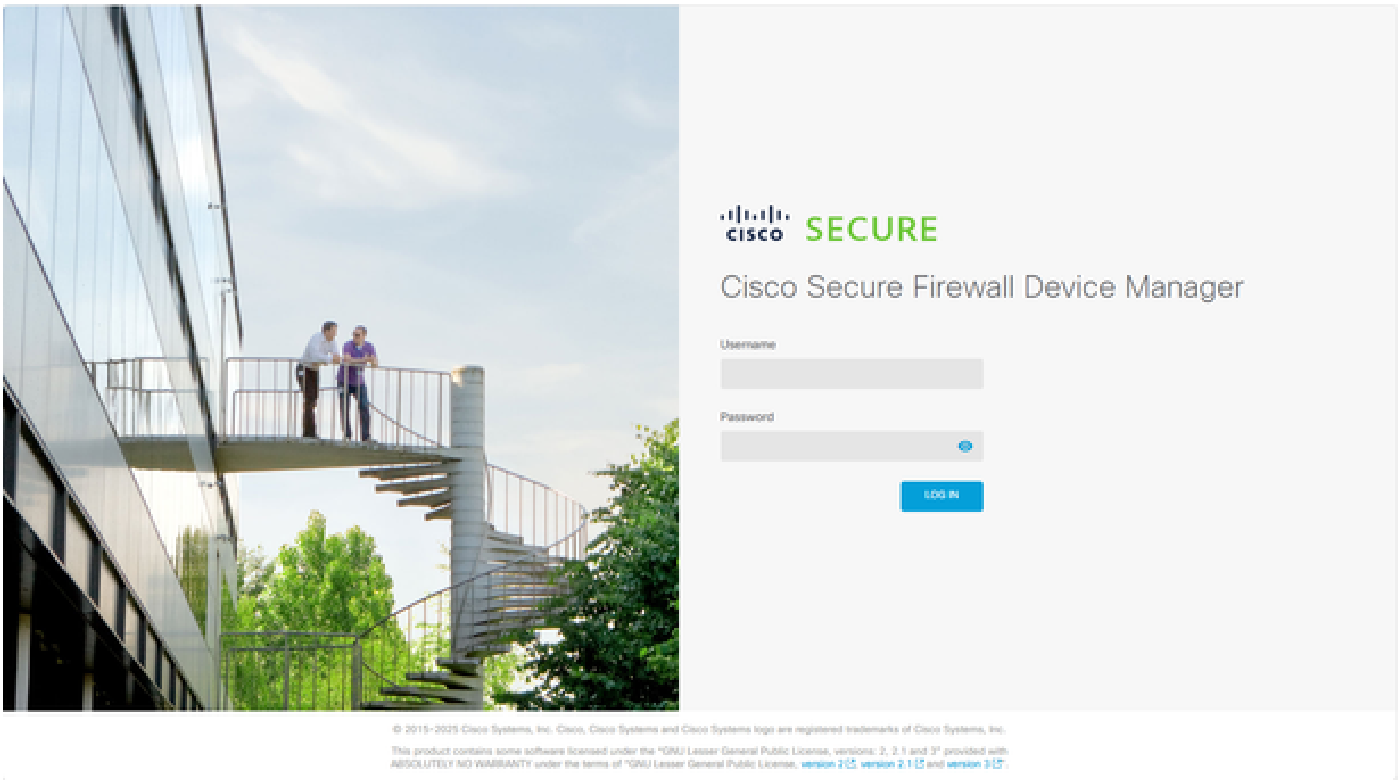
HTTPS

Allowed Networks

1.1.1.0_24

Verify

Open a browser and attempt to reach FDM using the data interface IP address.



Cisco Secure Firewall Device Manager

Troubleshoot

Perform a packet capture and confirm that:

- Traffic is reaching the data interface.
- Traffic is being forwarded to the nlp_int_tap interface.