Konfiguration des FDM On-Box Management Service für FirePOWER 2100

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie den FirePOWER Device Management (FDM) On-Box Management Service für die Firepower 2100 Serie mit installiertem FTD konfigurieren.

Voraussetzungen

Anforderungen

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

- Cisco Firepower 2100, FTD-Softwareinstallation
- Grundlegende Konfiguration und Fehlerbehebung mit Cisco FTD (Firepower Threat Defense).

Verwendete Komponenten

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

- Cisco Firepower 2100-Serie.
- Cisco FTD Version 6.2.3

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 verstehen.

Hintergrundinformationen

Dieses Dokument soll Sie in erster Linie durch die Schritte führen, die für die FDM On-Box-Verwaltung für die Firepower 2100-Serie erforderlich sind.

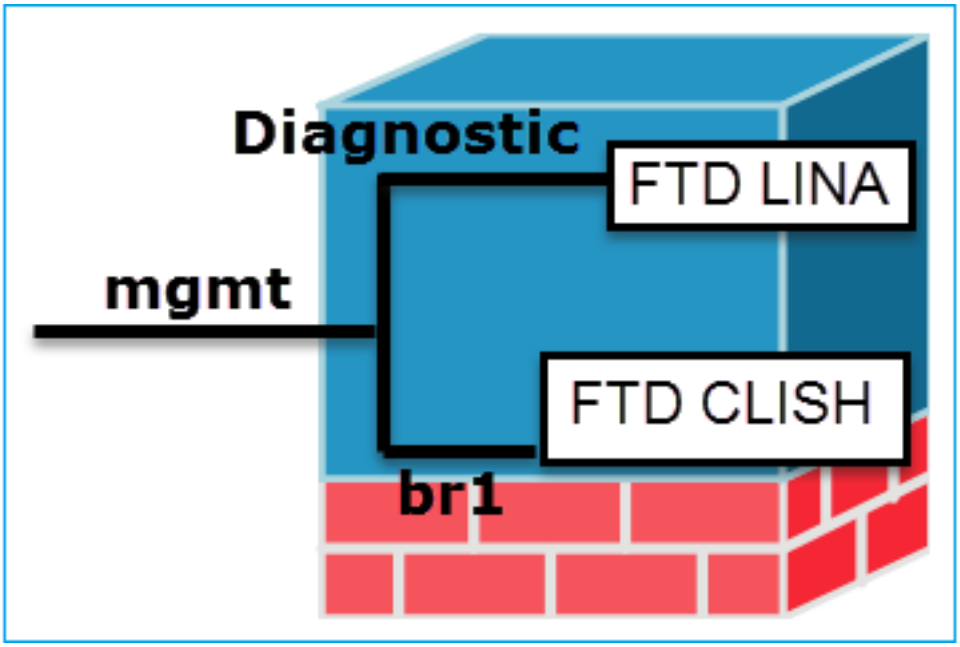
Sie haben zwei Optionen, um die Firepower Threst Defense (FTD) zu verwalten, die auf einem firepower 2100 installiert ist:

- Das FDM On-Box Management.
- Das Cisco FMC (FirePOWER Management Center)

Hinweis: Sie können FDM und FMC nicht zur Verwaltung eines FTD verwenden, das in einem Firepower 2100 installiert ist. Sobald die FDM On-Box-Verwaltung auf dem Firepower 2100 FTD aktiviert ist, kann ein FMC nicht mehr zur Verwaltung des FTD verwendet werden, es sei denn, Sie deaktivieren die lokale Verwaltung und konfigurieren die Verwaltung neu, sodass ein FMC verwendet wird. Andererseits wird durch die Registrierung des FTD bei einem FMC der FDM On-Box-Managementservice auf dem FTD deaktiviert.

Achtung: Cisco hat derzeit keine Möglichkeit, die FDM-Firewall-Konfiguration auf ein FMC zu migrieren und umgekehrt. Berücksichtigen Sie dies, wenn Sie die Art der Verwaltung für das auf der firepower 2100 installierte FTD konfigurieren.

Die Management-Schnittstelle ist in zwei logische Schnittstellen, br1 (management0 auf FPR2100/4100/9300-Appliances) und Diagnose unterteilt:



	Management: br1/management0	Management - Diagnose
Zweck	• Diese Schnittstelle wird verwendet, um die FTD-IP zuzuweisen, die für die FTD/FMC-Kommunikation verwendet wird. • Beendet den Sftunnel zwischen FMC/FTD. • Wird als Quelle für regelbasierte Syslogs verwendet. • SSH- und HTTPS-Zugriff auf die FTD-	• Bietet Remote-Zugriff (z. B. SNMP) auf die ASA-Engine. • Wird als Quelle für LINA-Syslogs, AAA, SNMP usw. verwendet.

	Box	
Mandatory (Obligatorisch)	Ja, da es für FTD/FMC Kommunikation verwendet wird (der Sftunnel endet darauf).	Nein, und es wird nicht empfohlen, sie zu konfigurieren. Es wird empfohlen, stattdesse eine Datenschnittstelle zu verwenden (siehe Hinweis unten).

Hinweis: Wenn Sie die IP-Adresse nicht auf der Diagnoseschnittstelle verwenden, können Sie die Verwaltungsschnittstelle im selben Netzwerk wie jede andere Datenschnittstelle platzieren. Wenn Sie die Diagnoseschnittstelle konfigurieren, muss sich ihre IP-Adresse im selben Netzwerk wie die IP-Adresse für die Verwaltung befinden. Sie gilt als reguläre Schnittstelle, die sich nicht im selben Netzwerk wie andere Datenschnittstellen befinden darf. Da die Management-Schnittstelle für Updates einen Internetzugang benötigt, bedeutet das Einfügen der Management-Schnittstelle in dasselbe Netzwerk wie eine interne FTD-Schnittstelle, dass Sie die FTD nur mit einem Switch im LAN bereitstellen und die interne Schnittstelle als Standard-Gateway für die Management-Schnittstelle festlegen können (dies gilt nur, wenn die FTD im Routing-Modus bereitgestellt wird).

Der FTD kann in eine firepower 2100-Appliance installiert werden. Das Firepower-Chassis führt ein eigenes Betriebssystem mit der Bezeichnung FXOS (FirePOWER eXtensible Operating System) aus, um den Basisbetrieb des Geräts zu steuern, während das logische FTD-Gerät auf einem Modul/Blade installiert ist.

Hinweis: Sie können die FXOS-GUI (Graphic User Interface) mit dem Namen FCM (Firepower Chassis Manager) oder die FXOS-CLI (Command Line Interface) verwenden, um die Funktionen des Firepower-Chassis zu konfigurieren. Die FCM-GUI ist jedoch nicht verfügbar, wenn die FTD auf der Firepower 2100-Serie installiert ist, sondern nur auf der FXOS-CLI.

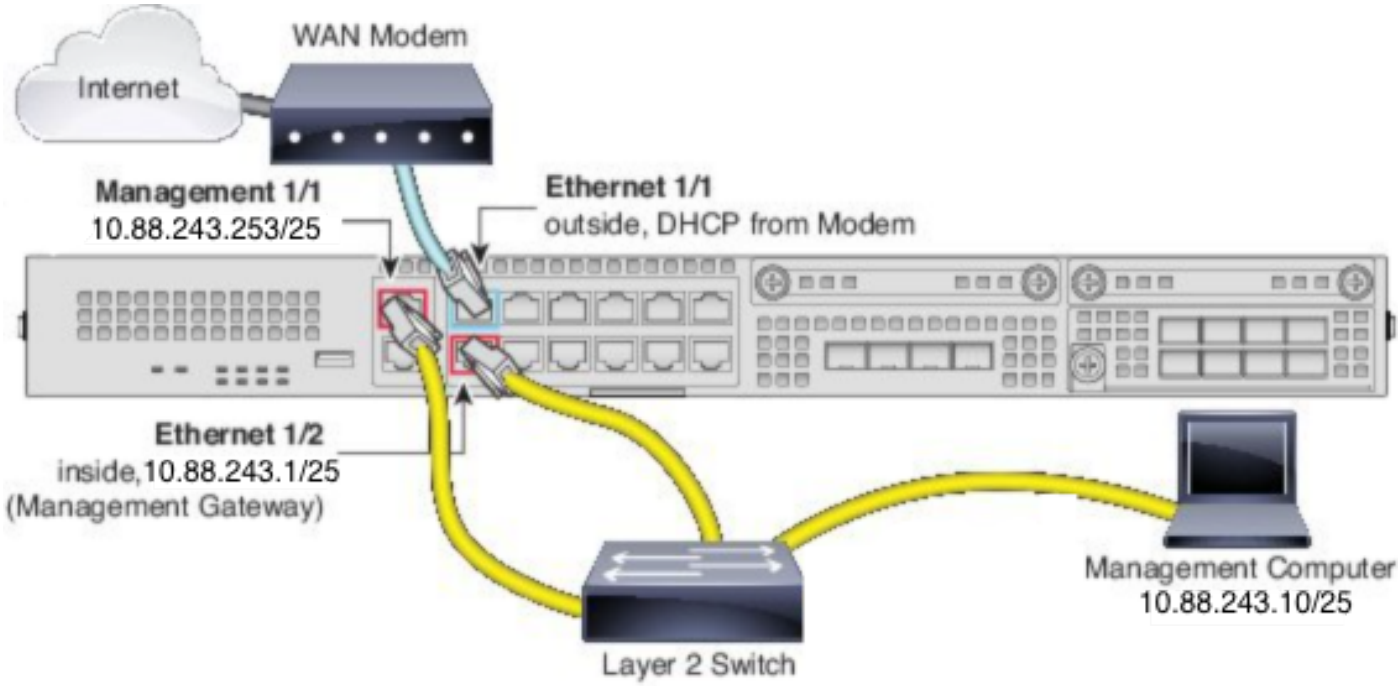
FirePOWER 21xx Appliance:

Hinweis: Auf der Firewall-Serie 2100 wird die Verwaltungsschnittstelle vom FXOS-Chassis und dem logischen FTD-Gerät gemeinsam genutzt.

Konfigurieren

Netzwerkdiagramm

Bei der Standardkonfiguration wird davon ausgegangen, dass bestimmte firepower 2100-Schnittstellen für das interne und das externe Netzwerk verwendet werden. Die Erstkonfiguration gestaltet sich einfacher, wenn Sie Netzwerkkabel entsprechend dieser Erwartungen an die Schnittstellen anschließen. Die Verkabelung der Firepower 2100-Serie finden Sie im nächsten Bild.



Hinweis: Das Bild zeigt eine einfache Topologie, die einen Layer-2-Switch verwendet. Andere Topologien können verwendet werden, und Ihre Bereitstellung kann je nach den grundlegenden Anforderungen an die logische Netzwerkverbindung, die Ports, die Adressierung und die Konfiguration variieren.

Konfigurationen

Um die FDM On-Box-Verwaltung auf der Firepower 2100 Serie zu aktivieren, gehen Sie wie folgt vor.

1. Konsolenzugriff auf das FPR2100-Gehäuse und Verbindung zur FTD-Anwendung.

```
firepower# connect ftd
>
```

2. Konfigurieren Sie die FTD-Verwaltungs-IP-Adresse.

```
>configure network ipv4 manual 10.88.243.253 255.255.255.128 10.88.243.1
```

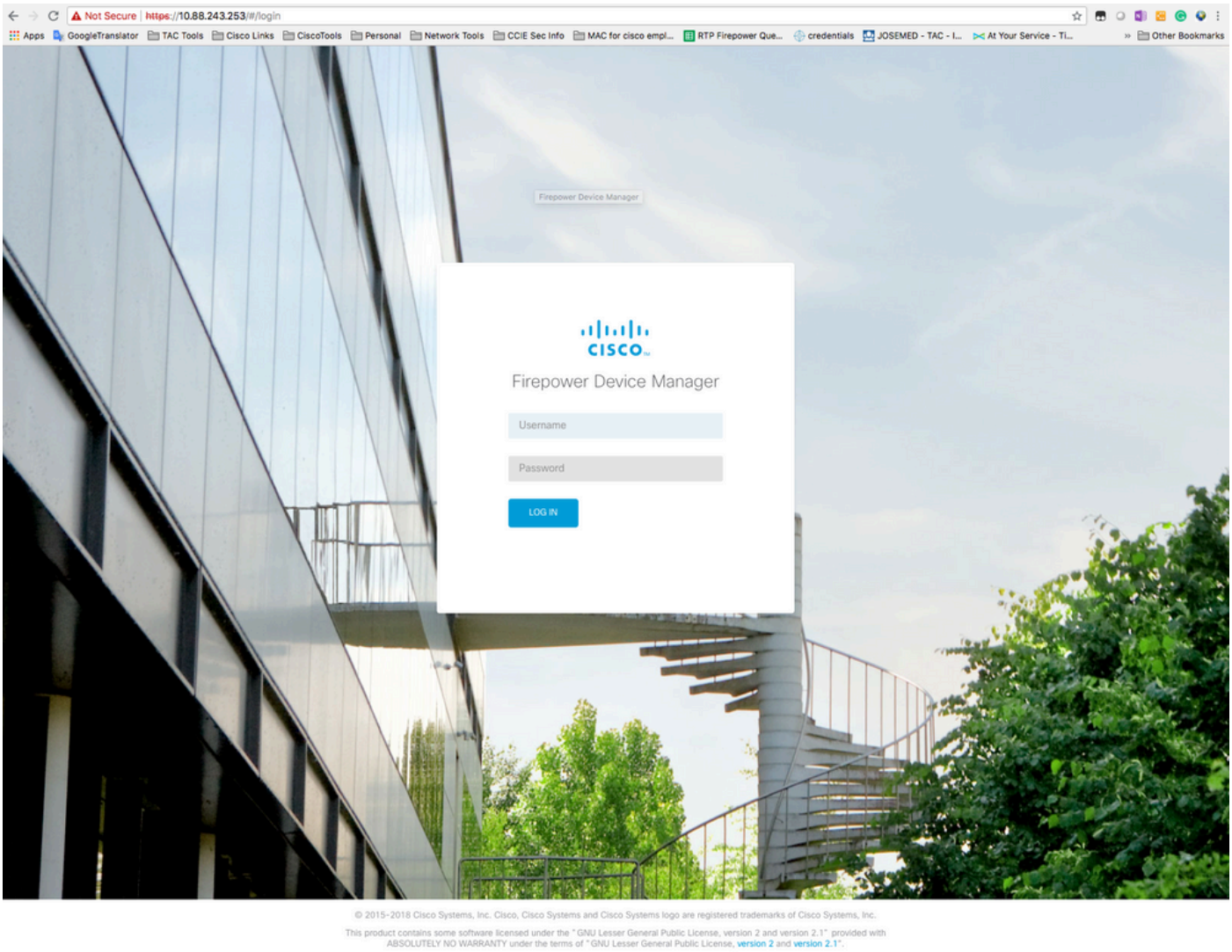
3. Konfigurieren Sie den Verwaltungstyp als lokal.

```
>configure manager local
```

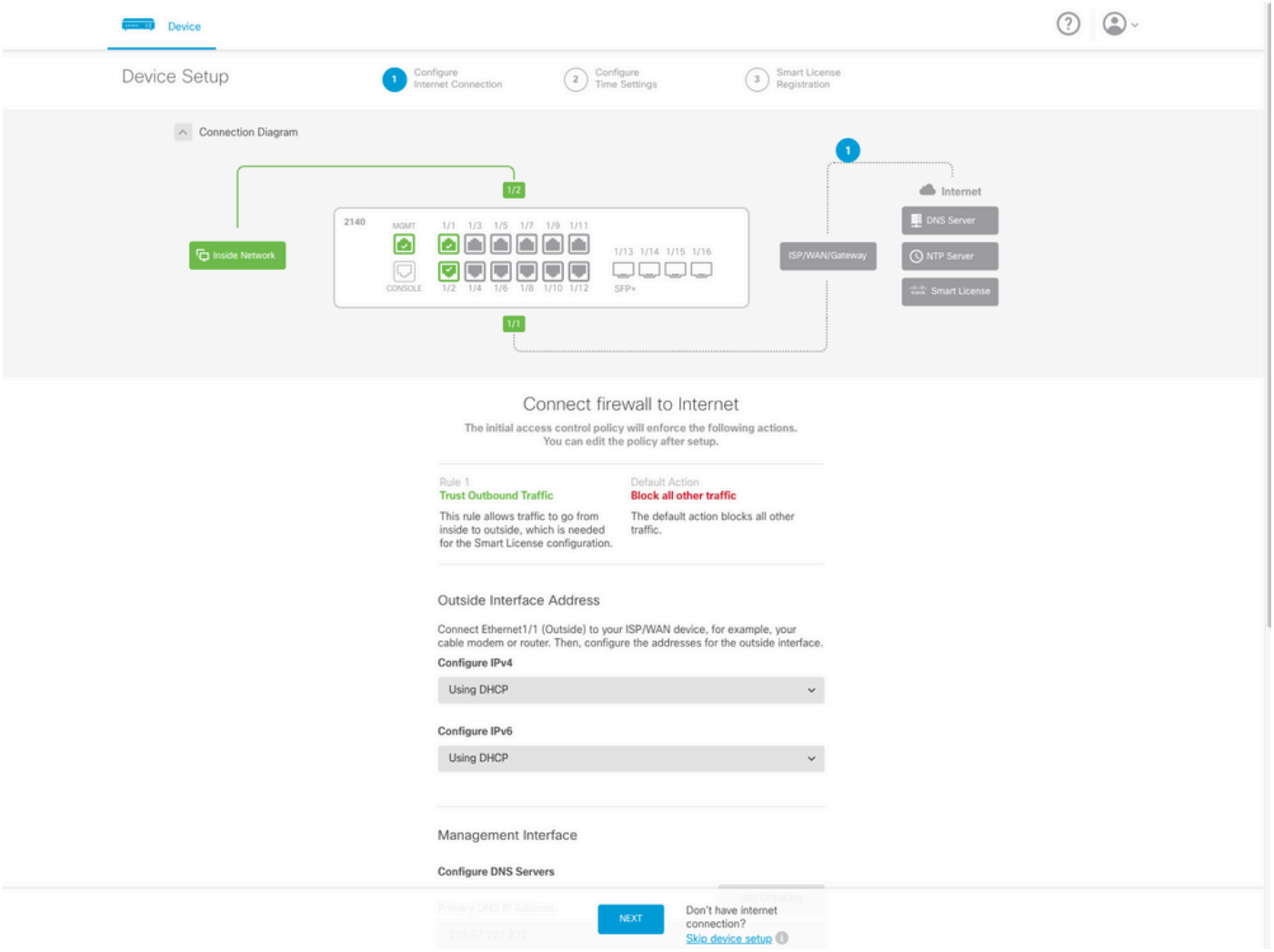
4. Konfigurieren Sie, von welchen IP-Adressen/Subnetzen aus der On-Box-Managementzugriff auf den FTD zugelassen werden kann.

```
>configure https-access-list 0.0.0.0/0
```

5. Öffnen Sie einen Browser und geben Sie https in die IP-Adresse ein, die Sie zur Verwaltung des FTD konfiguriert haben. Dadurch kann der FDM-Manager (On-Box) geöffnet werden.



6. Melden Sie sich an, und verwenden Sie die Standardanmeldeinformationen für firepower, den Benutzernamen admin und das Kennwort admin123.



Überprüfung

1. Überprüfen Sie mit dem nächsten Befehl die Netzwerkeinstellungen, die Sie für den FTD konfiguriert haben.

```
> show network
===============[ System Information ]===============
Hostname                  : firepower
DNS Servers               : 208.67.222.222
                            208.67.220.220
Management port           : 8305
IPv4 Default route
  Gateway                 : 10.88.243.129

==================[ management0 ]===================
State                     : Enabled
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
MAC Address               : 00:2C:C8:41:09:80
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.88.243.253
Netmask                   : 255.255.255.128
Broadcast                 : 10.88.243.255
----------------------[ IPv6 ]----------------------
```

```
Configuration             : Disabled

===============[ Proxy Information ]================
State                     : Disabled
Authentication            : Disabled
```

2. Überprüfen Sie mit dem nächsten Befehl den Verwaltungstyp, den Sie für den FTD konfiguriert haben.

```
> show managers
Managed locally.
```

Zugehörige Informationen

Cisco FirePOWER Gerätemanager

Cisco Firepower Threat Defense für die Firepower 2100-Serie mit Firepower Management Center - Kurzreferenz

Konfigurieren der Managementschnittstelle für Firepower Threat Defense (FTD)

Erstellen Sie ein neues Image der Firepower Serie 2100

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.