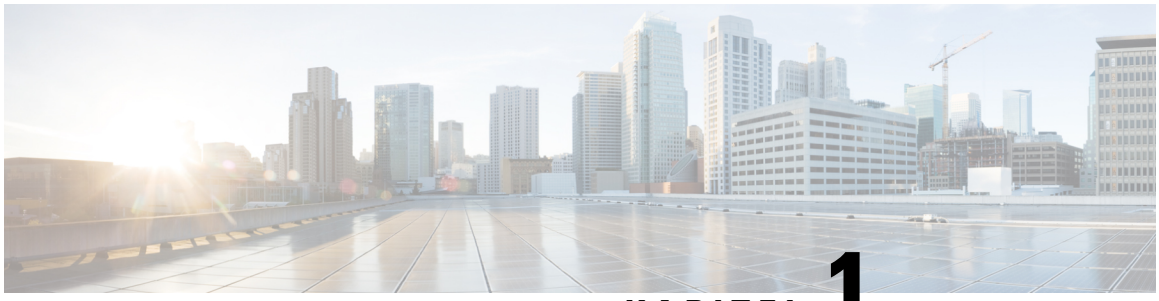
Leitfaden zu den ersten Schritten mit Cisco Firepower 1010

Erste Veröffentlichung: 13. Juni 2019

Letzte Änderung: 28. Februar 2022

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



KAPITEL 1

Welche Betriebssysteme und Manager sind für Sie geeignet?

Ihre Hardwareplattform kann eine von zwei Auswahlmöglichkeiten der Betriebssysteme ausführen. Bei allen Betriebssystemen haben Sie eine Auswahl an Managern. In diesem Kapitel werden die Auswahlmöglichkeiten für Betriebssysteme und Manager erläutert.

Betriebssysteme

Sie können entweder Secure Firewall ASA- oder Secure Firewall Threat Defense (früher Firepower Threat Defense) Betriebssysteme auf Ihrer Hardwareplattform verwenden:

- ASA: Die ASA ist eine traditionelle erweiterte Stateful-Firewall und ein VPN-Konzentrator.

  Sie können die ASA verwenden, wenn Sie die erweiterten Funktionen von Threat Defense nicht benötigen oder wenn Sie eine reine ASA-Funktion benötigen, die in Threat Defense noch nicht verfügbar ist. Cisco bietet Tools für die Migration von ASA zu Threat Defense, mit denen Sie Ihr ASA-System in ein Threat Defense-System konvertieren können, wenn Sie mit ASA beginnen und später ein neues Image für Threat Defense erstellen.

- Threat Defense: Threat Defense ist eine Next-Generation Firewall, die eine erweiterte Stateful-Firewall, einen VPN-Konzentrator und ein IPS der nächsten Generation kombiniert. Threat Defense kombiniert also die besten ASA-Funktionen mit den besten Next-Generation Firewall- und IPS-Funktionen.

  Wir empfehlen die Verwendung von Threat Defense anstelle der ASA, da FTD die meisten Hauptfunktionen der ASA sowie zusätzliche Next-Generation Firewall- und IPS-Funktionen enthält.

Um ein neues Image zwischen der ASA und Threat Defense zu erstellen, lesen Sie den Abschnitt zu Cisco Secure Firewall ASA und Threat Defense-Leitfaden zur Erstellung eines neuen Images.

Manager

Threat Defense und ASA unterstützen mehrere Manager.

Threat Defense-Manager

Tabelle 1: Threat Defense-Manager

Manager	Beschreibung
Secure Firewall Management Center (früher Firepower Management Center)	Management Center ist ein leistungsstarker, webbasierter Multi-Device-Manager, der auf seiner eigenen Serverhardware oder als virtuelles Gerät auf einem Hypervisor ausgeführt wird. Sie sollten Management Center verwenden, wenn Sie einen Multi-Device-Manager wünschen und alle Funktionen von Threat Defense benötigen. Management Center bietet zudem eine leistungsstarke Analyse- und Monitoring-Funktionen für Traffic und Ereignisse. Ab Version 6.7 kann Management Center die Threat Defenses über die externe Schnittstelle (oder sonstige Datenschnittstelle) verwalten, anstatt über die standardmäßige Management-Schnittstelle. Diese Funktion ist für Remote-Zweigstellenbereitstellungen nützlich. **Hinweis** Management Center ist nicht mit anderen Managern kompatibel, da das Management Center die Threat Defense-Konfiguration besitzt und Sie Threat Defense nicht direkt unter Umgehung des Management Center konfigurieren können. Informationen zu den ersten Schritten mit Management Center im Management-Netzwerk finden Sie unter Threat Defense-Bereitstellung mit dem Management Center, auf Seite 5. Informationen zu den ersten Schritten mit Management Center in einem Remote-Netzwerk finden Sie unter Threat Defense-Bereitstellung mit einem Remote-Management Center, auf Seite 49.
Secure Firewall Device Manager (früher Firepower Device Manager)	Device Manager ist ein webbasierter, vereinfachter On-Device-Manager. Da es sich um eine vereinfachte Version handelt, werden einige Threat Defense-Funktionen mit Device Manager nicht unterstützt. Sie sollten Device Manager verwenden, wenn Sie nur eine kleine Anzahl von Geräten verwalten und keinen Multi-Device-Manager benötigen. **Hinweis** Da sowohl Device Manager als auch CDO im FDM-Modus die Konfiguration in der Firewall erkennen können, ist es möglich, ein und dieselbe Firewall mit Device Manager und CDO zu verwalten. Management Center ist nicht mit anderen Managern kompatibel. Informationen zu den ersten Schritten mit Device Manager finden Sie unter Threat Defense Bereitstellung mit Device Manager, auf Seite 95.

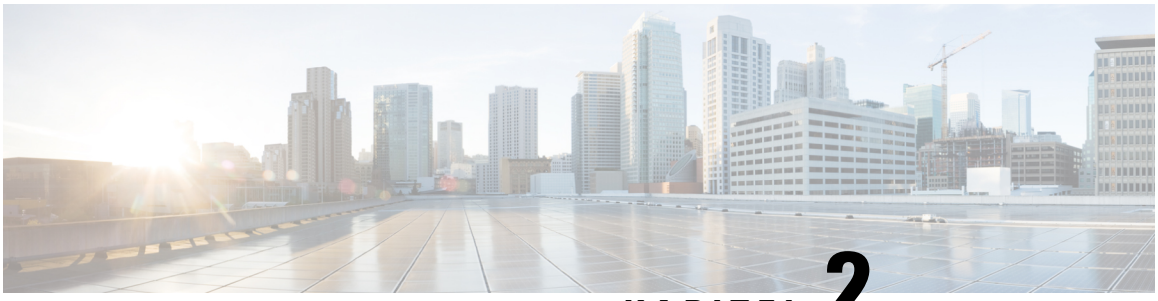
Manager	Beschreibung
Cisco Defense Orchestrator (CDO)	CDO bietet zwei Managementmodi: • (7.2 und höher) In der Cloud bereitgetellter Management Center-Modus mit allen Konfigurationsfunktionen eines lokalen Management Centers. Für die Analysefunktionen können Sie entweder Secure Cloud Analytics in der Cloud oder ein lokales Management Center verwenden. • Gerätemanager-Modus mit vereinfachter Benutzererfahrung. Dieser Modus wird in diesem Handbuch nicht behandelt. Da CDO Cloud-basiert ist, entsteht kein Kostenaufwand für den Betrieb von CDO auf Ihren eigenen Servern. CDO verwaltet auch andere Sicherheitsgeräte wie ASAs, sodass Sie einen einzigen Manager für alle Ihre Sicherheitsgeräte verwenden können. Informationen zu den ersten Schritten mit der CDO-Bereitstellung finden Sie unter Threat Defense-Bereitstellung mit CDO, auf Seite 125.
Secure Firewall Threat Defense-REST-API	Mit der Threat Defense-REST-API können Sie die direkte Konfiguration von Threat Defense automatisieren. Diese API ist mit der Verwendung von Device Manager und CDO kompatibel, da beide die Konfiguration auf der Firewall erkennen können. Sie können diese API nicht verwenden, wenn Sie Threat Defense mit Management Center verwalten. Die Threat Defense-REST-API wird in diesem Handbuch nicht behandelt. Weitere Informationen finden Sie unter Leitfaden zur REST-API in Cisco Secure Firewall Threat Defense.
Secure Firewall Management Center-REST-API	Mit der Management Center-REST-API können Sie die Konfiguration von Management Center-Richtlinien automatisieren, die dann auf verwaltete Threat Defenses angewendet werden können. Diese API verwaltet Threat Defense nicht direkt. Die Management Center-REST-API wird in diesem Handbuch nicht behandelt. Weitere Informationen finden Sie unter Kurzanleitung zur Cisco Secure Firewall Management Center-REST-API.

ASA-Manager

Tabelle 2: ASA-Manager

Manager	Beschreibung
Adaptive Security Device Manager (ASDM)	ASDM ist ein Java-basierter On-Device-Manager, der die volle ASA-Funktionalität bietet. Sie sollten ASDM verwenden, wenn Sie eine grafische Benutzeroberfläche (GUI) gegenüber der Befehlszeilenschnittstelle (CLI) bevorzugen und nur eine kleine Anzahl von ASAs verwalten müssen. Da ASDM die Konfiguration in der Firewall erkennen kann, können Sie auch die CLI, den CDO oder den CSM mit ASDM verwenden. Informationen zu den ersten Schritten mit ASDM finden Sie unter ASA-Bereitstellung mit ASDM, auf Seite 177.

Manager	Beschreibung
CLI	Sie sollten die ASA-CLI verwenden, wenn Sie CLIs gegenüber GUIs bevorzugen. Die CLI wird in diesem Handbuch nicht behandelt. Weitere Informationen finden Sie in den Konfigurationsleitfäden für ASA.
CDO	CDO ist ein vereinfachter, Cloud-basierter Manager für mehrere Geräte (Multi-Device Manager). Da es sich um eine vereinfachte Version handelt, werden einige ASA-Funktionen von CDO nicht unterstützt. Sie sollten CDO verwenden, wenn Sie einen Manager für mehrere Geräte wünschen, der ein vereinfachtes Management bietet. Und da CDO Cloud-basiert ist, entsteht kein Kostenaufwand für den Betrieb von CDO auf Ihren eigenen Servern. CDO verwaltet auch andere Sicherheitsgeräte wie Threat Defenses, sodass Sie einen einzigen Manager für alle Ihre Sicherheitsgeräte verwenden können. Da CDO die Konfiguration in der Firewall erkennen kann, können Sie auch die CLI oder ASDM verwenden. CDO wird in diesem Handbuch nicht behandelt. Informationen zu den ersten Schritten mit CDO finden Sie auf der CDO-Homepage.
Cisco Security Manager (CSM)	CSM ist ein leistungsstarker Manager für mehrere Geräte (Multi-Device-Manager), der auf seiner eigenen Serverhardware ausgeführt wird. Sie sollten CSM verwenden, wenn Sie eine große Anzahl von ASAs verwalten müssen. Da CSM die Konfiguration in der Firewall erkennen kann, können Sie auch die CLI oder ASDM verwenden. CSM unterstützt kein Management von Threat Defenses. CSM wird in diesem Handbuch nicht behandelt. Weitere Informationen zu diesem Thema entnehmen Sie bitte dem CSM-Benutzerhandbuch.
ASA-REST-API	Mit der ASA-REST-API können Sie die ASA-Konfiguration automatisieren. Die API enthält jedoch nicht alle ASA-Funktionen und wird nicht mehr erweitert. Die ASA-REST-API wird in diesem Handbuch nicht behandelt. Weitere Informationen finden Sie unter Schnellstarterdhandbuch für die Cisco ONE ASA Secure Firewall-REST-API.



KAPITEL 2

Threat Defense-Bereitstellung mit dem Management Center

Enthält dieses Kapitel die Informationen, nach denen Sie suchen?

Um alle verfügbaren Betriebssysteme und Manager anzuzeigen, sehen Sie sich Welche Betriebssysteme und Manager sind für Sie geeignet?, auf Seite 1 an. Dieses Kapitel gilt für Threat Defense mit Management Center.

In diesem Kapitel wird erläutert, wie Sie die Erstkonfiguration Ihres Threat Defense-Systems abschließen und wie Sie das Gerät bei einem Management Center in Ihrem Managementnetzwerk registrieren. Informationen zur Remote-Bereitstellung in einer Zweigstelle, bei der sich Management Center in einer zentralen Hauptgeschäftsstelle befindet, finden Sie unter Threat Defense-Bereitstellung mit einem Remote-Management Center, auf Seite 49.

In einer typischen Bereitstellung in einem großen Netzwerk installieren Sie mehrere verwaltete Geräte in Netzwerksegmenten. Jedes Gerät steuert, untersucht, überwacht und analysiert den Traffic und meldet die Ergebnisse dann einem verwaltenden Management Center. Management Center bietet eine Konsole für zentrales Management mit einer Weboberfläche, über die Sie Administrations-, Management-, Analyse- und Berichtsaufgaben zum Schutz Ihres lokalen Netzwerks durchführen können.

Informationen zur Firewall

Auf der Hardware kann entweder Threat Defense-Software oder ASA-Software ausgeführt werden. Beim Wechsel zwischen Threat Defense und ASA müssen Sie ein neues Image des Geräts erstellen. Sie sollten auch ein neues Image erstellen, wenn Sie eine andere Softwareversion als derzeit installiert benötigen. Weitere Informationen hierzu finden Sie unter Reimage the Cisco ASA or Firepower Threat Defense Device (Erstellen eines neuen Images für Cisco ASA oder Firepower Threat Defense-Gerät).

Die Firewall führt ein zugrunde liegendes Betriebssystem namens Secure Firewall Extensible Operating System (FXOS) aus. Die Firewall unterstützt die FXOS-Secure Firewall Chassis Manager nicht. Es wird nur in begrenztem Umfang eine CLI für Fehlerbehebungszwecke unterstützt. Weitere Informationen finden Sie unter Cisco FXOS-Leitfaden zur Fehlerbehebung für die Firepower 1000/2100-Serie mit Firepower Threat Defense.

Datenschutzerklärung zur Datenerfassung: Die Firewall erfordert keine personenbezogenen Informationen und nimmt keine aktive Erfassung derartiger Informationen vor. Sie können jedoch personenbezogene Informationen in der Konfiguration verwenden, z. B. bei Benutzernamen. In diesem Fall kann ein Administrator diese Informationen möglicherweise sehen, wenn er mit der Konfiguration arbeitet oder SNMP verwendet.

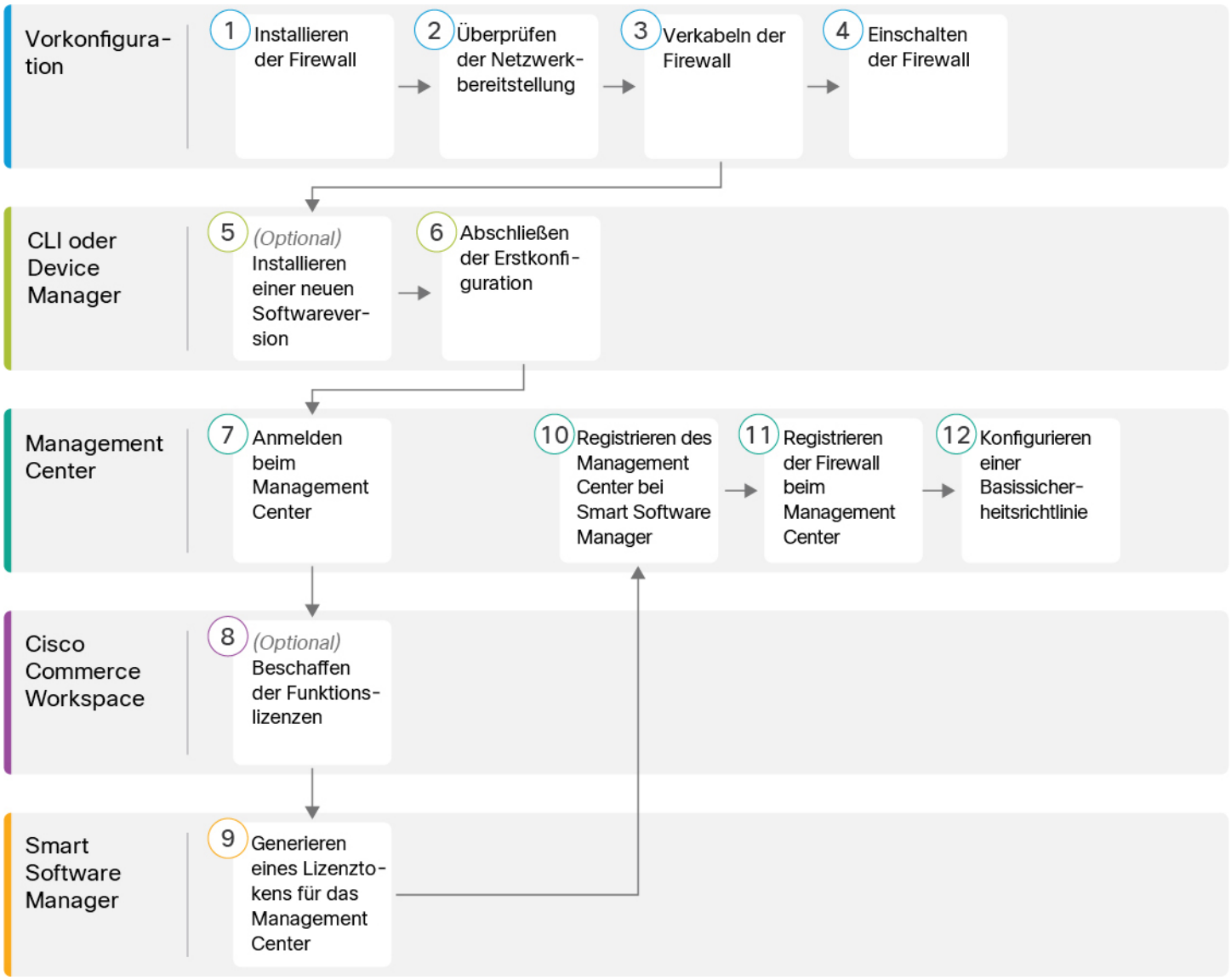
- Vorbereitung, auf Seite 6
- Vollständiges Verfahren, auf Seite 6

Vorbereitung

Stellen Sie Management Center bereit, und führen Sie die Erstkonfiguration durch. Siehe Hardwareinstallationshandbuch für Cisco Firepower Management Center 1600, 2600 und 4600 oder Leitfaden zu den ersten Schritten mit Cisco Secure Firewall Management Center Virtual.

Vollständiges Verfahren

Lesen Sie die folgenden Aufgaben zur Bereitstellung von Threat Defense mit Management Center auf Ihrem Chassis.



1	Vorkonfiguration	Installieren der Firewall. Weitere Informationen finden Sie im Hardware-Installationshandbuch.
2	Vorkonfiguration	Überprüfen der Netzwerkbereitstellung, auf Seite 8-
3	Vorkonfiguration	Verkabeln des Geräts (6.5 und höher), auf Seite 10 Verkabeln des Geräts (6.4), auf Seite 12-
4	Vorkonfiguration	Einschalten der Firewall, auf Seite 13-
5	CLI	(Optional) Prüfen der Software und Installieren einer neuen Version, auf Seite 14

6	CLI oder Device Manager	Abschließen der Threat Defense-Erstkonfiguration, auf Seite 15.
7	Management Center	Anmelden bei Management Center, auf Seite 24.
8	Cisco Commerce Workspace	Abrufen von Lizenzen für Management Center, auf Seite 24: Erwerben Sie Funktionslizenzen.
9	Smart Software Manager	Abrufen von Lizenzen für Management Center, auf Seite 24: Generieren Sie ein Lizenztoken für das Management Center.
10	Management Center	Abrufen von Lizenzen für Management Center, auf Seite 24: Registrieren Sie das Management Center beim Smart Licensing-Server.
11	Management Center	Registrieren des Threat Defense beim Management Center, auf Seite 25
12	Management Center	Konfigurieren einer Basissicherheitsrichtlinie, auf Seite 28

Überprüfen der Netzwerkbereitstellung

Bereitstellung ab Version 6.5

Die dedizierte Management 1/1-Schnittstelle ist eine spezielle Schnittstelle mit eigenen Netzwerkeinstellungen. Standardmäßig ist die Management 1/1-Schnittstelle aktiviert und als DHCP-Client konfiguriert. Wenn Ihr Netzwerk keinen DHCP-Server enthält, können Sie die Management-Schnittstelle so einstellen, dass während der Ersteinrichtung am Konsolen-Port eine statische IP-Adresse verwendet wird. Sie können andere Schnittstellen konfigurieren, nachdem Sie Threat Defense mit Management Center verbunden haben. Beachten Sie, dass Ethernet1/2 bis 1/8 standardmäßig als Switch-Ports aktiviert sind.

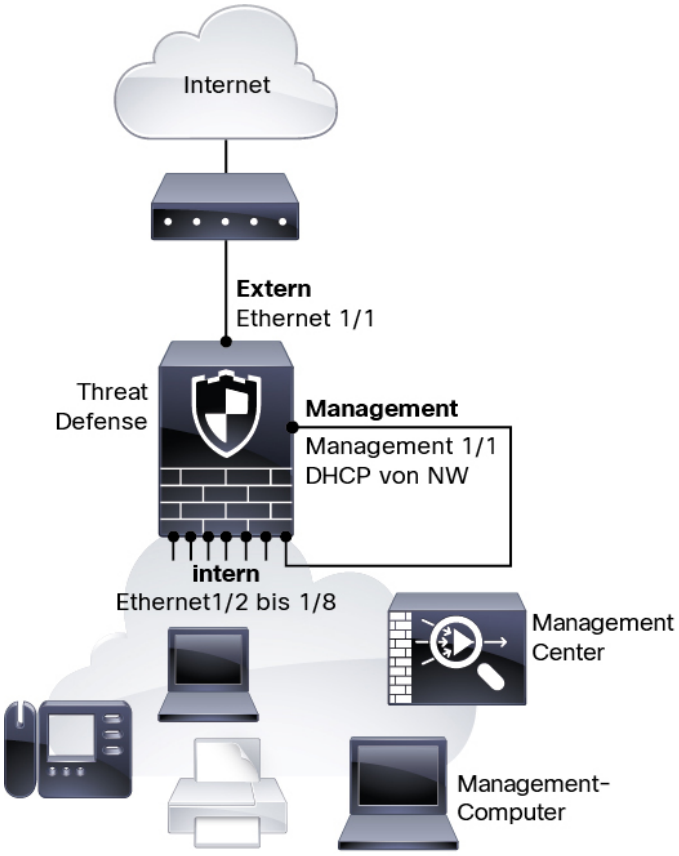
Hinweis In Version 6.5 und früher ist die Management-Schnittstelle mit einer IP-Adresse (192.168.45.45) konfiguriert.

Die folgende Abbildung zeigt die empfohlene Netzwerkbereitstellung für das Firepower 1010-System.

Management Center kann nur über die Management-Schnittstelle mit Threat Defense kommunizieren. Darüber hinaus benötigen sowohl Management Center als auch Threat Defense für die Lizenzierung und Updates einen Internetzugang vom Management aus.

Im folgenden Diagramm fungiert das Firepower 1010-System als Internet-Gateway für die Management-Schnittstelle und das Management Center, indem Management 1/1 direkt mit einem internen Switch-Port verbunden wird und das Management Center sowie der Management-Computer mit anderen internen Switch-Ports verbunden werden. (Diese direkte Verbindung ist zulässig, da die Management-Schnittstelle von den anderen Schnittstellen auf der Threat Defense-Instanz getrennt ist.)

Abbildung 1: Empfohlene Netzwerkbereitstellung



Bereitstellung in Version 6.4

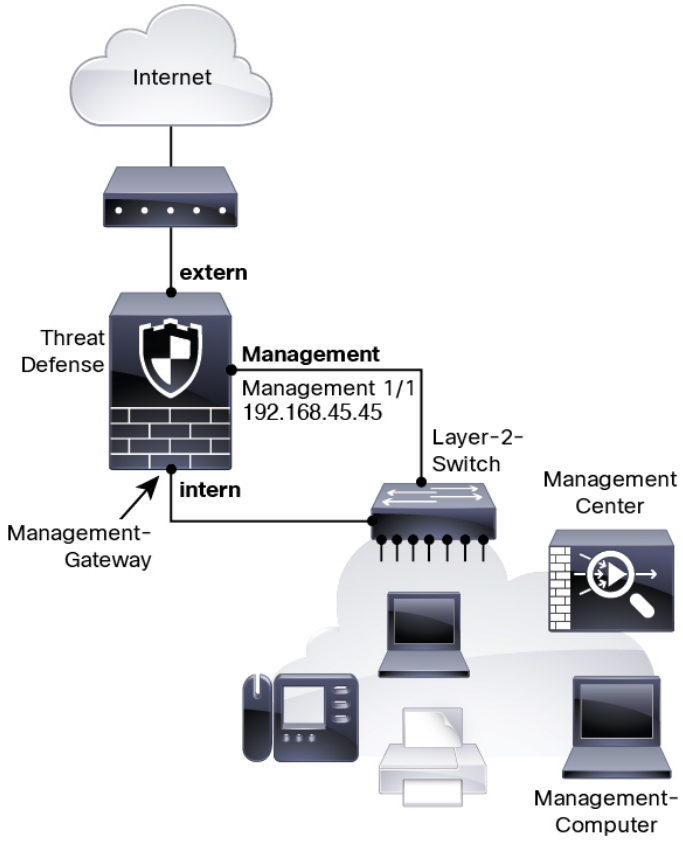
Die dedizierte Management 1/1-Schnittstelle ist eine spezielle Schnittstelle mit eigenen Netzwerkeinstellungen. Standardmäßig ist nur die Management 1/1-Schnittstelle aktiviert und mit einer IP-Adresse (192.168.45.45) konfiguriert. Über diese Schnittstelle wird zunächst auch ein DHCP-Server ausgeführt. Nachdem Sie bei der Ersteinrichtung Management Center als Manager ausgewählt haben, wird der DHCP-Server deaktiviert. Sie können andere Schnittstellen konfigurieren, nachdem Sie Threat Defense mit Management Centerverbunden haben.

Die folgende Abbildung zeigt die empfohlene Netzwerkbereitstellung für das Firepower 1010-System.

Management Center kann nur über die Management-Schnittstelle mit Threat Defense kommunizieren. Darüber hinaus benötigen sowohl Management Center als auch Threat Defense für die Lizenzierung und Updates einen Internetzugang vom Management aus.

Im folgenden Diagramm fungiert das Firepower 1010-System als Internet-Gateway für die Management-Schnittstelle und das Management Center, indem Management 1/1 über einen Layer-2-Switch mit einer internen Schnittstelle verbunden wird und das Management Center sowie der Management-Computer mit dem Switch verbunden werden. (Diese direkte Verbindung ist zulässig, da die Management-Schnittstelle von den anderen Schnittstellen auf der Threat Defense-Instanz getrennt ist.)

Abbildung 2: Empfohlene Netzwerkbereitstellung

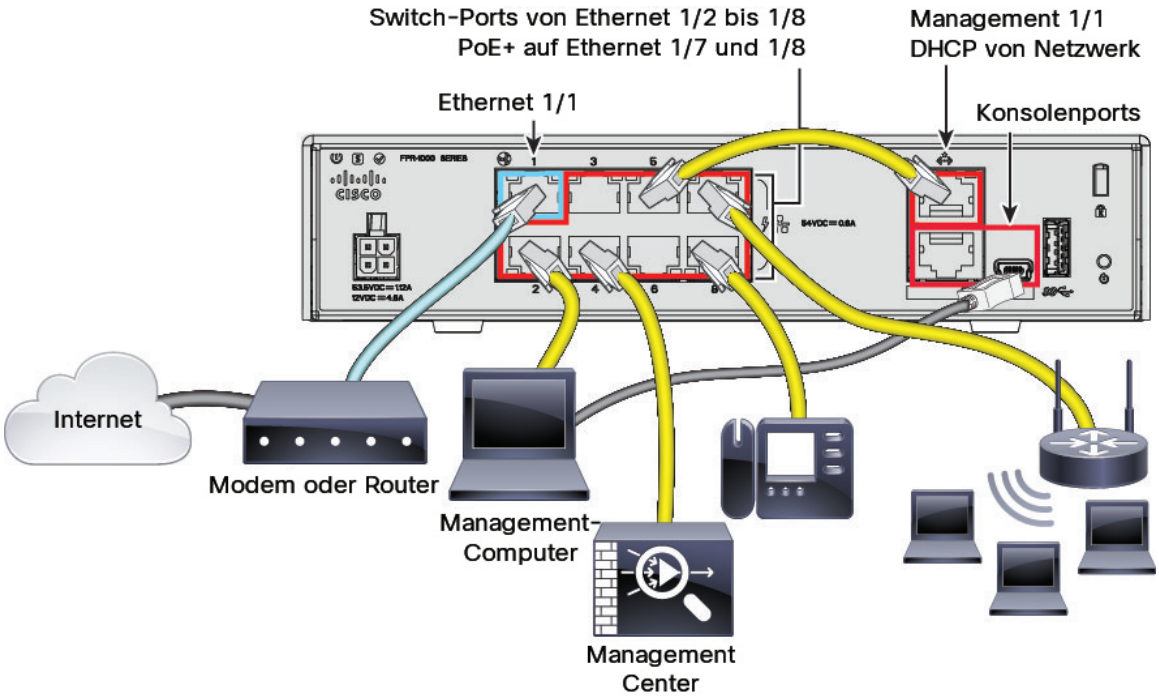


Verkabeln des Geräts (6.5 und höher)

Das empfohlene Szenario für die Verkabelung des Firepower 1010-Systems wird in der folgenden Abbildung veranschaulicht. Dort ist eine Beispieltopologie mit Ethernet 1/1 als externe Schnittstelle und den verbleibenden Schnittstellen als Switch-Ports im internen Netzwerk dargestellt.

Hinweis Andere Topologien können verwendet werden, und Ihre Bereitstellung variiert je nach Ihren Anforderungen. Sie können beispielsweise die Switch-Ports in Firewall-Schnittstellen konvertieren.

Abbildung 3: Verkabelung des Firepower 1010-Geräts



Hinweis Bei Version 6.5 und früheren Versionen lautet die Standard-IP-Adresse von Management 1/1 192.168.45.45.

Prozedur

Schritt 1 Installieren des Chassis Weitere Informationen finden Sie im Hardware-Installationshandbuch.

Schritt 2 Verbinden Sie Management 1/1 direkt mit einem der Switch-Ports (Ethernet 1/2 bis 1/8).

Schritt 3 Verbinden Sie Folgendes mit den Switch-Ports (Ethernet 1/2 bis 1/8):

- Management Center
- Management-Computer
- Zusätzliche Endpunkte

Schritt 4 Verbinden Sie den Management-Computer mit dem Konsolenport. Sie müssen den Konsolenport verwenden, um auf die CLI für die Ersteinrichtung zuzugreifen, wenn Sie SSH für die Management-Schnittstelle nicht verwenden. Oder verwenden Sie Device Manager für die Ersteinrichtung.

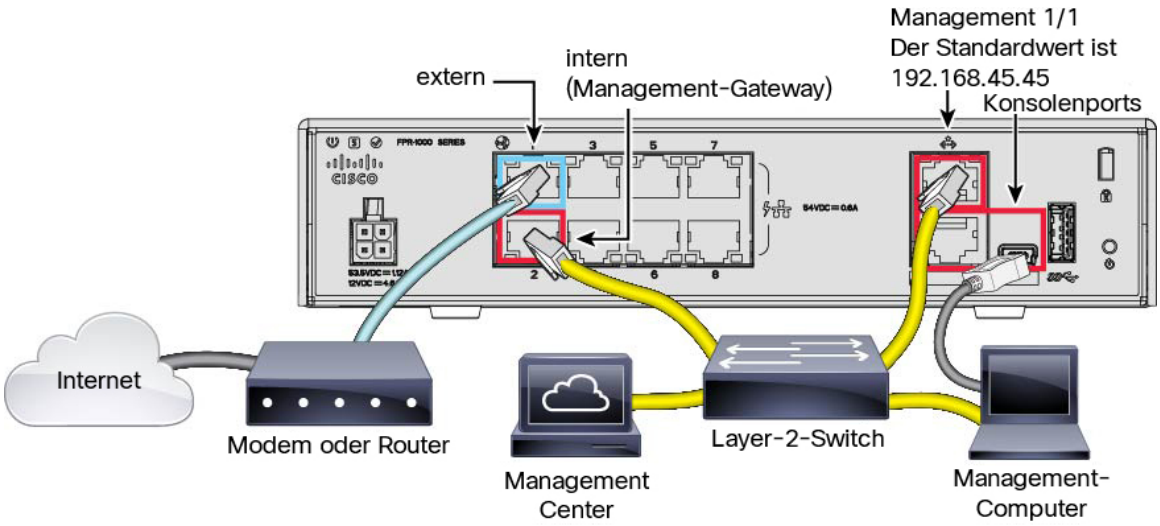
Schritt 5 Verbinden Sie Ethernet 1/1 mit Ihrem externen Router.

Verkabeln des Geräts (6.4)

Das empfohlene Szenario der Verkabelung des Firepower 1010-Geräts wird in der folgenden Abbildung veranschaulicht, die eine Beispieltopologie mit einem Layer-2-Switch zeigt.

Hinweis Andere Topologien können verwendet werden, und Ihre Bereitstellung variiert je nach Ihren Anforderungen.

Abbildung 4: Verkabelung des Firepower 1010-Geräts



Prozedur

Schritt 1 Installieren Sie die Hardware, und machen Sie sich mit der Hardware-Installationsanleitung vertraut.

Schritt 2 Verbinden Sie folgende Elemente mit einem Layer-2-Ethernet-Switch:

- Interne Schnittstelle (z. B. Ethernet 1/2)
- Management 1/1-Schnittstelle
- Management Center
- Management-Computer

Hinweis Firepower 1010 und das Management Center haben beide die gleiche standardmäßige Management-IP-Adresse: 192.168.45.45. In diesem Handbuch wird davon ausgegangen, dass Sie bei der Ersteinrichtung unterschiedliche IP-Adressen für Ihre Geräte festlegen. Beachten Sie, dass das Management Center ab Version 6.5 standardmäßig einen DHCP-Client für die Management-Schnittstelle verwendet. Wenn jedoch kein DHCP-Server vorhanden ist, wird standardmäßig 192.168.45.45 verwendet.

Schritt 3 Verbinden Sie den Management-Computer mit dem Konsolenport. Sie müssen den Konsolenport verwenden, um auf die CLI für die Ersteinrichtung zuzugreifen, wenn Sie SSH für die Management-Schnittstelle nicht verwenden.

Schritt 4 Verbinden Sie die externe Schnittstelle (z. B. Ethernet 1/1) mit Ihrem externen Router.

Schritt 5 Verbinden Sie andere Netzwerke mit den verbleibenden Schnittstellen.

Einschalten der Firewall

Die Systemstromversorgung wird über das Netzkabel gesteuert. Es gibt keinen Netzschalter.

Hinweis Wenn Sie den Threat Defense zum ersten Mal starten, kann die Initialisierung etwa 15 bis 30 Minuten dauern.

Vorbereitungen

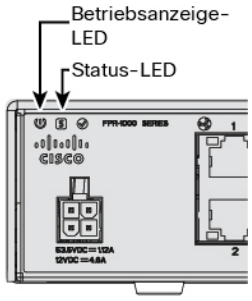
Es ist wichtig, dass Sie Ihr Gerät zuverlässig mit Strom versorgen (z. B. mit einer unterbrechungsfreien Stromversorgung (USV)). Ein Stromausfall ohne vorheriges Herunterfahren kann zu ernsthaften Schäden am Dateisystem führen. Im Hintergrund laufen ständig viele Prozesse ab, und eine Unterbrechung der Stromversorgung ermöglicht kein ordnungsgemäßes Herunterfahren des Systems.

Prozedur

Schritt 1 Schließen Sie das Netzkabel am Gerät und dann an einer Steckdose an.

Wenn Sie das Netzkabel an die Stromversorgung anschließen, ist das Gerät automatisch eingeschaltet.

Schritt 2 Prüfen Sie die Betriebs-LED auf der Rückseite oder Oberseite des Geräts; leuchtet sie dauerhaft grün, ist das Gerät eingeschaltet.



Schritt 3 Prüfen Sie die Status-LED auf der Rückseite oder Oberseite des Geräts; wenn sie dauerhaft grün leuchtet, hat das System die Einschaltdiagnose durchlaufen.

(Optional) Prüfen der Software und Installieren einer neuen Version

Gehen Sie wie folgt vor, um die Softwareversion zu überprüfen und ggf. eine andere Version zu installieren. Wir empfehlen, dass Sie Ihre Zielversion installieren, bevor Sie die Firewall konfigurieren. Alternativ können Sie ein Upgrade im Anschluss an die Inbetriebnahme durchführen. Ein Upgrade, bei dem Ihre Konfiguration erhalten bleibt, kann jedoch länger dauern als dieses Verfahren.

Welche Version sollte ich ausführen?

Cisco empfiehlt, eine Gold Star-Version auszuführen, die durch einen goldenen Stern neben der Versionsnummer auf der Software-Download-Seite gekennzeichnet ist. Sie können sich auch auf die Release-Strategie beziehen, die in https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html beschrieben ist. Beispielsweise beschreibt dieses Bulletin die Nummerierung von kurzfristigen Releases (mit den neuesten Funktionen), die Nummerierung von langfristigen Releases (Wartungsversionen und Patches für einen längeren Zeitraum) oder die Nummerierung von extra langfristigen Releases (Wartungsversionen und Patches für den längsten Zeitraum für die staatliche Zertifizierung).

Prozedur

Schritt 1 Stellen Sie eine Verbindung zur CLI her. Weitere Informationen finden Sie unter Zugriff auf die Threat Defense- und FXOS-CLI, auf Seite 44. Dieses Verfahren zeigt die Verwendung des Konsolenports, aber Sie können stattdessen SSH verwenden.

Melden Sie sich mit dem Benutzer **admin** und dem Standardkennwort **Admin123** an.

Sie stellen eine Verbindung zum FXOS-CLI her. Wenn Sie sich zum ersten Mal anmelden, werden Sie aufgefordert, das Kennwort zu ändern. Dieses Kennwort wird auch zur Threat Defense-Anmeldung für SSH verwendet.

Hinweis Wenn das Kennwort bereits geändert wurde und Sie es nicht kennen, müssen Sie das Gerät auf die Werkseinstellungen zurücksetzen, um das Kennwort auf den Standardwert zurückzusetzen. Weitere Informationen hierzu finden Sie im Abschnitt über das Verfahren zum Zurücksetzen auf die Werkseinstellungen im Handbuch zur FXOS-Fehlerbehebung.

Beispiel:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

Schritt 2 Zeigen Sie in der FXOS-CLI die aktuelle Version an.

scope ssa

show app-instance

Beispiel:

```
Firepower# scope ssa
Firepower /ssa # show app-instance

Application Name     Slot ID    Admin State     Operational State    Running Version Startup
 Version Cluster Oper State
-------------------- ---------- --------------- -------------------- ---------------
--------------- ------------------
ftd                  1          Enabled         Online               7.2.0.65        7.2.0.65
        Not Applicable
```

Schritt 3 Wenn Sie eine neue Version installieren möchten, führen Sie diese Schritte aus.

a) Informationen zum Festlegen einer statischen IP-Adresse für die Management-Schnittstelle finden Sie unter Abschließen der Threat Defense-Erstkonfiguration mit der CLI, auf Seite 20. Standardmäßig verwendet die Management-Schnittstelle DHCP.

Sie müssen das neue Image von einem Server herunterladen, auf den über die Managementschnittstelle zugegriffen werden kann.

b) Führen Sie das Verfahren zum Erstellen eines neuen Images im Handbuch zur FXOS-Fehlerbehebung durch.

Abschließen der Threat Defense-Erstkonfiguration

Sie können Sie die Threat Defense-Erstkonfiguration mit der CLI oder Device Manager abschließen.

Abschließen der Threat Defense-Erstkonfiguration mit Device Manager

Stellen Sie eine Verbindung zu Device Manager her, um die Ersteinrichtung des Threat Defense-Systems durchzuführen. Wenn Sie die Ersteinrichtung mit Device Manager durchführen, werden *alle* in Device Manager abgeschlossenen Schnittstellenkonfigurationen beibehalten, wenn Sie für das Management zu Management Center wechseln, zusätzlich zu den Einstellungen für die Management-Schnittstelle und den Managerzugriff. Beachten Sie, dass andere Standardkonfigurationseinstellungen, wie z. B. die Zugriffskontrollrichtlinie oder Sicherheitszonen, nicht beibehalten werden. Wenn Sie die CLI verwenden, werden nur die Management-Schnittstellen- und Managerzugriffseinstellungen beibehalten (z. B. wird die standardmäßige interne Schnittstellenkonfiguration nicht beibehalten).

Vorbereitungen

- Stellen Sie Management Center bereit, und führen Sie die Erstkonfiguration durch. Siehe Hardwareinstallationshandbuch für Cisco Firepower Management Center 1600, 2600 und 4600. Sie müssen die IP-Adresse oder den Host-Namen des Management Center kennen, bevor Sie Threat Defense einrichten.

- Verwenden Sie eine aktuelle Version von Firefox, Chrome, Safari, Edge oder Internet Explorer.

Prozedur

Schritt 1 Melden Sie sich bei Device Manager an.

a) Geben Sie eine der folgenden URLs in Ihren Browser ein.

- Intern (Ethernet 1/2 bis 1/8) – **https://192.168.95.1**.Sie können an jedem internen Switch-Port (Ethernet 1/2 bis 1/8) eine Verbindung zur internen Adresse herstellen.
- Management: **https://***Management-IP*. Da die Management-Schnittstelle ein DHCP-Client ist, hängt die IP-Adresse von Ihrem DHCP-Server ab. Möglicherweise müssen Sie im Rahmen dieses Verfahrens die Management-IP-Adresse auf eine statische Adresse festlegen. Daher empfehlen wir Ihnen, die interne Schnittstelle zu verwenden, damit die Verbindung nicht getrennt wird.

b) Melden Sie sich mit dem Benutzernamen **admin** und dem Standardkennwort **Admin123** an.

c) Sie werden aufgefordert, den Endbenutzerlizenzvertrag zu lesen und zu akzeptieren und das Administratorkennwort zu ändern.

Schritt 2 Verwenden Sie bei der ersten Anmeldung in Device Manager den Einrichtungsassistenten, um die Erstkonfiguration abzuschließen. Sie können den Einrichtungsassistenten optional überspringen, indem Sie unten auf der Seite auf **Skip device setup** (Gerätekonfiguration überspringen) klicken.

Nachdem Sie den Einrichtungsassistenten abgeschlossen haben, haben Sie zusätzlich zur Standardkonfiguration für die interne Schnittstelle (Ethernet 1/2 bis 1/8, die Switch-Ports auf VLAN1 sind) eine Konfiguration für eine externe Schnittstelle (Ethernet 1/1), die beibehalten wird, wenn Sie zum Management Center-Management wechseln.

a) Konfigurieren Sie die folgenden Optionen für die externe Schnittstelle und die Management-Schnittstellen, und klicken Sie auf **Next** (Weiter).

1. **Outside Interface Address** (Externe Schnittstellenadresse): Diese Schnittstelle ist in der Regel das Internet-Gateway und kann als Managerzugriffsschnittstelle verwendet werden. Sie können während der Ersteinrichtung des Geräts keine alternative externe Schnittstelle auswählen. Die erste Datenschnittstelle ist die standardmäßige externe Schnittstelle.

   Wenn Sie eine andere externe (oder interne) Schnittstelle für den Managerzugriff verwenden möchten, müssen Sie sie nach Abschluss des Einrichtungsassistenten manuell konfigurieren.

   Configure IPv4 (IPv4 konfigurieren): Die IPv4-Adresse für die externe Schnittstelle. Sie können DHCP verwenden oder eine statische IP-Adresse, eine Subnetzmaske und ein Gateway manuell eingeben. Sie können auch **Off** (Aus) auswählen, wenn keine IPv4-Adresse konfiguriert werden soll. Sie können PPPoE nicht mit dem Einrichtungsassistenten konfigurieren. PPPoE kann erforderlich sein, wenn die Schnittstelle mit einem DSL-Modem, Kabelmodem oder einem anderen ISP-Anschluss verbunden ist und Ihr ISP PPPoE verwendet, um Ihre IP-Adresse bereitzustellen. Sie können PPPoE konfigurieren, nachdem Sie den Assistenten abgeschlossen haben.

   Configure IPv6 (IPv6 konfigurieren): Die IPv6-Adresse für die externe Schnittstelle. Sie können DHCP verwenden oder eine statische IP-Adresse, ein Präfix und ein Gateway manuell eingeben. Sie können auch **Off** (Aus) auswählen, wenn keine IPv6-Adresse konfiguriert werden soll.

2. **Management-Schnittstelle**

Die Einstellungen der Management-Schnittstelle werden nicht angezeigt, wenn Sie die Ersteinrichtung über die CLI durchgeführt haben. Beachten Sie, dass das Festlegen der IP-Adresse der Managementschnittstelle nicht Teil des Einrichtungsassistenten ist. Siehe Schritt 3, auf Seite 17 zum Festlegen der Management-IP-Adresse.

DNS Servers (DNS-Server): Der DNS-Server für die Management-Schnittstelle der Firewall. Geben Sie eine oder mehrere Adressen von DNS-Servern für die Namensauflösung ein. Der Standardwert sind die öffentlichen DNS-Server von OpenDNS. Wenn Sie die Felder bearbeiten und zum Standardwert zurückkehren möchten, klicken Sie auf **OpenDNS** verwenden, um die entsprechenden IP-Adressen erneut in die Felder zu laden.

Firewall Hostname (Firewall-Host-Name): Der Host-Name für die Management-Schnittstelle der Firewall.

b) Konfigurieren Sie die **Zeiteinstellung (NTP)**, und klicken Sie auf **Next** (Weiter).

1. **Time Zone** (Zeitzone): Wählen Sie die Zeitzone für das System aus.
2. **NTP Time Server** (NTP-Zeitserver): Wählen Sie aus, ob Sie die Standard-NTP-Server verwenden oder die Adressen Ihrer NTP-Server manuell eingeben möchten. Sie können mehrere Server hinzufügen, um Backups bereitzustellen.

c) Wählen Sie **Start 90 day evaluation period without registration** (90-tägigen Evaluierungszeitraum ohne Registrierung starten) aus.

Registrieren Sie das Threat Defense-System nicht beim Smart Software Manager. Die gesamte Lizenzierung erfolgt im Management Center.

d) Klicken Sie auf **Finish** (Fertigstellen).

e) Sie werden aufgefordert, **Cloud Management** (Cloud-Management) oder **Standalone** (Eigenständig) zu wählen. Wählen Sie für das Management Center-Management die Option **Standalone** (Eigenständig) und dann **Got It** (Verstanden).

Schritt 3 (Möglicherweise erforderlich) Konfigurieren Sie eine statische IP-Adresse für die Management-Schnittstelle. Klicken Sie auf **Device** (Gerät) und dann auf den Link **System Settings** > **Management Interface** (Systemeinstellungen > Management-Schnittstelle).

Wenn Sie eine statische IP-Adresse konfigurieren möchten, stellen Sie sicher, dass das Standard-Gateway anstelle der Datenschnittstellen ein eindeutiges Gateway ist. Wenn Sie DHCP verwenden, müssen Sie nichts konfigurieren.

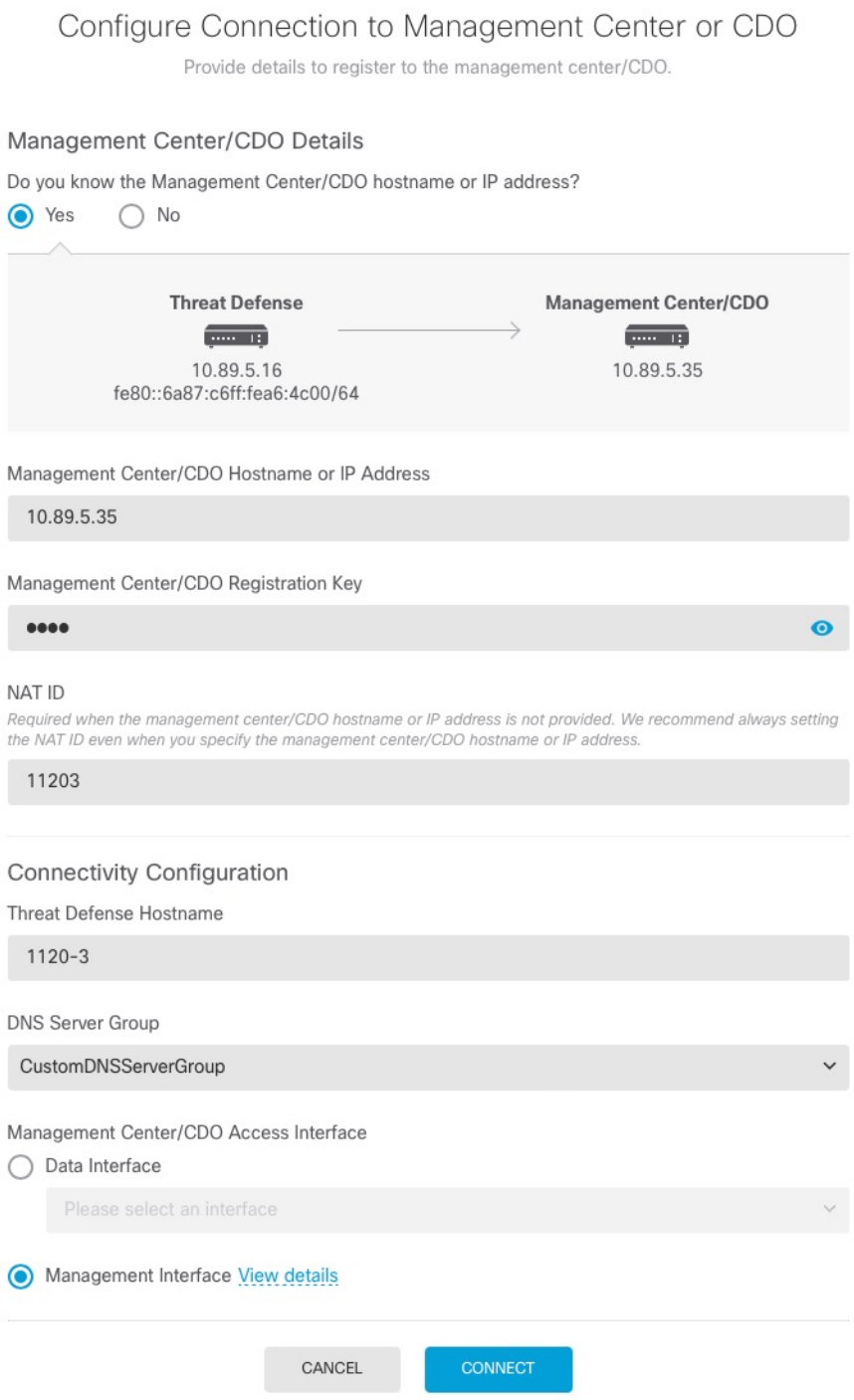
Schritt 4 Wenn Sie zusätzliche Schnittstellen konfigurieren möchten, einschließlich einer anderen als der externen oder internen Schnittstelle, wählen Sie **Device** (Gerät), und klicken Sie dann auf den Link in der Schnittstellenübersicht (**Interfaces**).

Unter Konfigurieren der Firewall in Device Manager, auf Seite 115 finden Sie weitere Informationen zum Konfigurieren von Schnittstellen in Device Manager. Andere Device Manager-Konfigurationen werden nicht beibehalten, wenn Sie das Gerät bei Management Center registrieren.

Schritt 5 Wählen Sie **Device** > **System Settings** > **Central Management**, und klicken Sie auf **Proceed** (Fortfahren), um das Management Center-Management einzurichten.

Schritt 6 Konfigurieren der **Management Center-/CDO-Details**

Abbildung 5: Management Center-/CDO-Details



a) Klicken Sie unter **Do you know the Management Center/CDO hostname or IP address** auf **Yes** (Ja), wenn Sie das Management Center mit einer IP-Adresse oder einem Hostname erreichen können, oder auf **No** (Nein), wenn sich das Management Center hinter NAT befindet oder keine öffentliche IP-Adresse oder keinen Hostnamen hat.

Mindestens eines der Geräte, entweder das Management Center oder das Threat Defense-Gerät muss eine erreichbare IP-Adresse haben, um den bidirektionalen, SSL-verschlüsselten Kommunikationskanal zwischen den beiden Geräten einzurichten.

b) Wenn Sie **Yes** (Ja) ausgewählt haben, geben Sie **Management Center/CDO-Hostname/IP-Adresse** ein.

c) Geben Sie den **Management Center/CDO-Registrierungsschlüssel** an.

Dieser Schlüssel gibt einen einmaligen Registrierungsschlüssel Ihrer Wahl an, den Sie auch bei der Registrierung des Threat Defense-Geräts im Management Center angeben. Der Registrierungsschlüssel darf höchstens 37 Zeichen enthalten. Zu den zulässigen Zeichen zählen alphanumerische Zeichen (A–Z, a–z, 0–9) und der Bindestrich (-). Diese ID kann für mehrere Geräte verwendet werden, die sich beim Management Center registrieren.

d) Geben Sie eine **NAT-ID** an.

Diese ID ist eine eindeutige, einmalige Zeichenfolge Ihrer Wahl, die Sie auch im Management Center angeben. Dieses Feld ist erforderlich, wenn Sie die IP-Adresse nur auf einem der Geräte angeben. Wir empfehlen jedoch, die NAT-ID anzugeben, auch wenn Sie die IP-Adressen beider Geräte kennen. Die NAT-ID darf nicht länger als 37 Zeichen sein. Zu den zulässigen Zeichen zählen alphanumerische Zeichen (A–Z, a–z, 0–9) und der Bindestrich (-). Diese ID *kann nicht* für andere Geräte verwendet werden, die sich beim Management Center registrieren. Die NAT-ID wird in Kombination mit der IP-Adresse verwendet, um zu überprüfen, ob die Verbindung vom richtigen Gerät kommt. Erst nach der Authentifizierung der IP-Adresse/NAT-ID wird der Registrierungsschlüssel überprüft.

Schritt 7 Konfigurieren Sie die **Verbindungskonfiguration**.

a) Geben Sie den **FTD-Hostnamen** an.

b) Geben Sie die **DNS-Servergruppe** an.

Wählen Sie eine vorhandene Gruppe aus oder erstellen Sie eine neue. Die Standard-DNS-Gruppe heißt **CiscoUmbrellaDNSServerGroup** und umfasst die OpenDNS-Server.

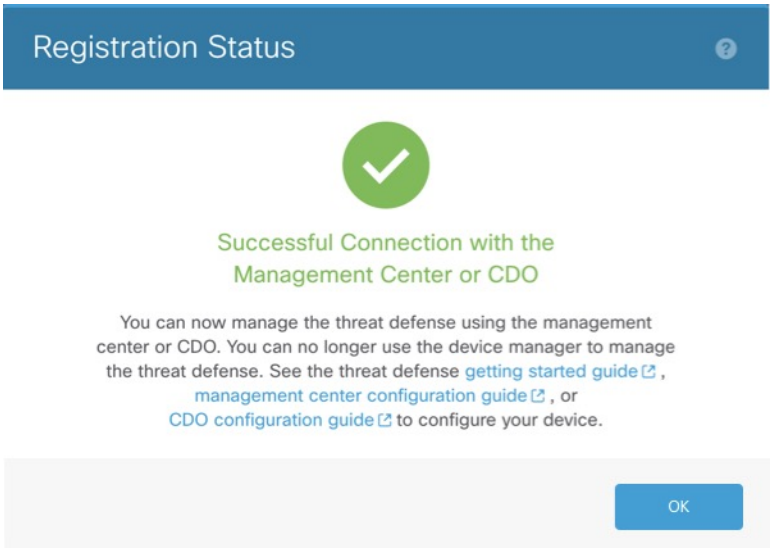
c) Wählen Sie für die **Management Center-/CDO-Zugriffsschnittstelle management** aus.

Schritt 8 Klicken Sie auf **Connect** (Verbinden). Im Dialogfeld **Registrierungsstatus** wird der aktuelle Status des Wechsels zu Management Center angezeigt. Wechseln Sie nach dem Schritt **Speichern von Management Center/CDO-Registrierungseinstellungen** zu Management Center, und fügen Sie die Firewall hinzu.

Wenn Sie den Wechsel zu Management Center abbrechen möchten, klicken Sie auf **Cancel Registration** (Registrierung abbrechen). Andernfalls schließen Sie das Device Manager-Browserfenster erst nach dem Schritt **Speichern von Management Center/CDO-Registrierungseinstellungen**. Wenn Sie dies tun, wird der Prozess angehalten und erst fortgesetzt, wenn Sie erneut eine Verbindung zum Device Manager herstellen.

Wenn Sie nach dem Schritt **Speichern von Management Center/CDO-Registrierungseinstellungen** weiterhin mit dem Device Manager verbunden sind, wird schließlich das Dialogfeld **Erfolgreiche Verbindung mit Management Center oder CDO** angezeigt. Dannach wird die Verbindung zum Device Managergetrennt.

Abbildung 6: Verbindungsversuch erfolgreich



Abschließen der Threat Defense-Erstkonfiguration mit der CLI

Stellen Sie eine Verbindung zur Threat Defense-CLI her, um mithilfe des Einrichtungsassistenten die Ersteinrichtung durchzuführen, einschließlich der Einstellung der Management-IP-Adresse, des Gateways und anderer grundlegender Netzwerkeinstellungen. Die dedizierte Management-Schnittstelle ist eine spezielle Schnittstelle mit eigenen Netzwerkeinstellungen. In 6.7 und höher: Wenn Sie die Management-Schnittstelle nicht für den Managerzugriff verwenden möchten, können Sie stattdessen über die CLI eine Datenschnittstelle konfigurieren. Sie konfigurieren auch die Management Center-Kommunikationseinstellungen. Wenn Sie die Ersteinrichtung mit Device Manager (7.1 und höher) durchführen, werden *alle* Schnittstellenkonfigurationen in Device Manager beibehalten, wenn Sie für das Management zu Management Center wechseln, zusätzlich zu den Einstellungen für die Management-Schnittstelle und den Managerzugriff. Beachten Sie, dass andere Standardkonfigurationseinstellungen, wie z. B. die Zugriffskontrollrichtlinie, nicht beibehalten werden.

Prozedur

Schritt 1 Stellen Sie eine Verbindung zur Threat Defense-CLI her, entweder über den Konsolenport oder über eine SSH-Sitzung mit der Management-Schnittstelle, die standardmäßig eine IP-Adresse von einem DHCP-Server bezieht. Wenn Sie beabsichtigen, die Netzwerkeinstellungen zu ändern, empfehlen wir, den Konsolenport zu verwenden, damit Ihre Verbindung nicht getrennt wird.

Der Konsolenport wird mit der FXOS-CLI verbunden. Die SSH-Sitzung stellt eine direkte Verbindung zur Threat Defense-CLI her.

Schritt 2 Melden Sie sich mit dem Benutzernamen **admin** und dem Kennwort **Admin123** an.

Am Konsolenport stellen Sie eine Verbindung zur FXOS-CLI her. Wenn Sie sich zum ersten Mal bei FXOS anmelden, werden Sie aufgefordert, das Kennwort zu ändern. Dieses Kennwort wird auch zur Threat Defense-Anmeldung für SSH verwendet.

Hinweis Wenn das Kennwort bereits geändert wurde und Sie es nicht kennen, müssen Sie ein neues Image des Geräts erstellen, um das Kennwort auf den Standardwert zurückzusetzen. Weitere Informationen hierzu finden Sie im Abschnitt über das Verfahren zum Erstellen eines neuen Images im Handbuch zur FXOS-Fehlerbehebung.

Beispiel:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

Schritt 3 Wenn Sie über den Konsolenport eine Verbindung zu FXOS hergestellt haben, verbinden Sie sich mit der Threat Defense-CLI

connect ftd

Beispiel:

```
firepower# connect ftd
>
```

Schritt 4 Wenn Sie sich zum ersten Mal bei Threat Defense anmelden, werden Sie aufgefordert, den Endbenutzerlizenzvertrag (EULA) zu akzeptieren und, falls Sie eine SSH-Verbindung verwenden, das Administratorkennwort zu ändern. Anschließend wird das CLI-Einrichtungsskript angezeigt.

Hinweis Sie können den CLI-Einrichtungsassistenten nur wiederholen, wenn Sie die Konfiguration löschen, zum Beispiel im Rahmen der Neuerstellung eines Images. Alle diese Einstellungen können jedoch später in der CLI mit den Befehlen **configure network** geändert werden. Siehe Befehlsreferenz für Secure Firewall Threat Defense.

Standardwerte oder zuvor eingegebene Werte werden in Klammern angezeigt. Um zuvor eingegebene Werte zu akzeptieren, drücken Sie die **Eingabetaste**.

Beachten Sie die folgenden Orientierungshilfen:

- **Geben Sie das IPv4-Standardgateway für die Management-Schnittstelle ein**: Die Einstellung für **Datenschnittstellen** gilt nur für das Remote-Management Center- oder Device Manager-Management. Sie sollten eine Gateway-IP-Adresse für Management 1/1 festlegen, wenn Sie Management Center im Managementnetzwerk verwenden. Im Beispiel für die Edge-Bereitstellung im Abschnitt zur Netzwerkbereitstellung fungiert die interne Schnittstelle als Management-Gateway. In diesem Fall sollten Sie die IP-Adresse des Gateways als *vorgesehene* interne Schnittstellen-IP-Adresse festlegen. Sie müssen später Management Center verwenden, um die interne IP-Adresse festzulegen.
- **Wenn sich Ihre Netzwerkinformationen geändert haben, müssen Sie die Verbindung wiederherstellen.** Wenn Sie mit SSH verbunden sind, aber die IP-Adresse bei der Ersteinrichtung ändern,

wird die Verbindung getrennt. Verbinden Sie sich erneut mit der neuen IP-Adresse und dem Kennwort. Konsolenverbindungen sind nicht betroffen.

- **Manage the device locally?** (Das Gerät lokal verwalten?): Geben Sie **no** (Nein) ein, um Management Center zu verwenden. Die Antwort **yes** (Ja) bedeutet, dass Sie stattdessen Device Manager verwenden werden.
- **Configure firewall mode?** (Firewall-Modus konfigurieren?): Wir empfehlen, den Firewall-Modus bei der Erstkonfiguration festzulegen. Wenn Sie den Firewall-Modus nach der Ersteinrichtung ändern, wird Ihre aktuelle Konfiguration gelöscht.

Beispiel:

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress.  Please stand by.
You must change the password for 'admin' to continue.
Enter new password: ********
Confirm new password: ********
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.10.10.1
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: no
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...

Update policy deployment information
    - add device configuration
    - add network discovery
    - add system policy

You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.

When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required.  In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Firepower Management Center are separated by a
NAT device, you must enter a unique NAT ID, along with the unique registration
key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'
```

```
Later, using the web interface on the Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.
>
```

Schritt 5 Identifizieren Sie das Management Center, das dieses Threat Defense-System verwalten soll.

configure manager add {*Host-Name* | *IPv4-Adresse* | *IPv6-Adresse* | **DONTRESOLVE**} *Registrierungsschlüssel* [*NAT-ID*]

- {*Host-Name* | *IPv4-Adresse* | *IPv6-Adresse* | **DONTRESOLVE**}: Gibt entweder den FQDN oder die IP-Adresse des Management Center an. Wenn das Management Center nicht direkt adressierbar ist, verwenden Sie **DONTRESOLVE**, und geben Sie auch die *nat_id* an. Mindestens eines der Geräte, entweder das Management Center oder Threat Defense, muss eine erreichbare IP-Adresse haben, um den bidirektionalen, SSL-verschlüsselten Kommunikationskanal zwischen den beiden Geräten einzurichten. Wenn Sie **DONTRESOLVE** in diesem Befehl angeben, muss Threat Defense über eine erreichbare IP-Adresse oder einen Host-Namen verfügen.
- *Registrierungsschlüssel*: Gibt einen einmaligen Registrierungsschlüssel Ihrer Wahl an, den Sie auch bei der Registrierung des Threat Defense-Systems im Management Center angeben. Der Registrierungsschlüssel darf höchstens 37 Zeichen enthalten. Zu den zulässigen Zeichen zählen alphanumerische Zeichen (A–Z, a–z, 0–9) und der Bindestrich (-).
- *nat_id*: Gibt eine eindeutige, einmalige Zeichenfolge Ihrer Wahl an, die Sie auch bei der Threat Defense-Registrierung auf dem Management Center angeben, wenn auf einer Seite keine erreichbare IP-Adresse oder kein Host-Name angegeben ist. Dies ist erforderlich, wenn Sie das Management Center auf **DONTRESOLVE** setzen. Die NAT-ID darf nicht länger als 37 Zeichen sein. Zu den zulässigen Zeichen zählen alphanumerische Zeichen (A–Z, a–z, 0–9) und der Bindestrich (-). Diese ID kann nicht für andere Geräte verwendet werden, die sich beim Management Center registrieren.

Beispiel:

```
> configure manager add MC.example.com 123456
Manager successfully configured.
```

Wenn sich Management Center hinter einem NAT-Gerät befindet, geben Sie eine eindeutige NAT-ID zusammen mit dem Registrierungsschlüssel ein, und geben Sie DONTRESOLVE anstelle des Host-Namens an.

Beispiel:

```
> configure manager add DONTRESOLVE regk3y78 natid90
Manager successfully configured.
```

Wenn sich Threat Defense hinter einem NAT-Gerät befindet, geben Sie eine eindeutige NAT-ID zusammen mit der Management Center-IP-Adresse oder dem Host-Namen ein.

Beispiel:

```
> configure manager add 10.70.45.5 regk3y78 natid56
Manager successfully configured.
```

Nächste Maßnahme

Registrieren Sie Ihre Firewall beim Management Center.

Anmelden bei Management Center

Verwenden Sie das Management Center, um Threat Defense zu konfigurieren und zu überwachen.

Vorbereitungen

Informationen zu unterstützten Browsern finden Sie in den Versionshinweisen für die von Ihnen verwendete Version (siehe https://www.cisco.com/go/firepower-notes)

Prozedur

Schritt 1 Geben Sie in einem unterstützten Browser die folgende URL ein.

https://*FMC-IP-Adresse*

Schritt 2 Geben Sie Ihren Benutzernamen und Ihr Kennwort ein.

Schritt 3 Klicken Sie auf **Log In** (Anmelden).

Abrufen von Lizenzen für Management Center

Alle Lizenzen werden vom Management Center für Threat Defense bereitgestellt. Sie können die folgenden Lizenzen erwerben:

- **Threat**: Security Intelligence und Next-Generation IPS
- **Malware**: MalwareDefense
- **URL**: URL-Filterung
- **RA VPN**: AnyConnect Plus, AnyConnect Apex oder AnyConnect VPN Only.

Nähere Informationen über die Lizenzierung bei Cisco erhalten Sie unter cisco.com/go/licensingguide

Vorbereitungen

- Sie müssen über ein Masterkonto bei Smart Software Manager verfügen.

  Wenn Sie noch kein Konto haben, klicken Sie auf den Link, um ein neues Konto einzurichten. Mit dem Smart Software Manager können Sie ein Masterkonto für Ihr Unternehmen erstellen.

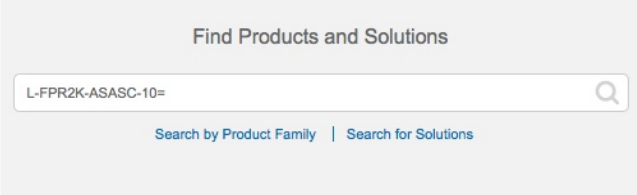
- Ihr Smart Software Licensing-Konto muss für die Strong Encryption-(3DES/AES-)Lizenz qualifiziert sein, um bestimmte Funktionen nutzen zu können (aktiviert mit dem Flag „export-compliance“).

Prozedur

Schritt 1 Stellen Sie sicher, dass Ihr Smart Licensing-Konto die verfügbaren Lizenzen enthält, die Sie benötigen.

Wenn Sie Ihr Gerät bei Cisco oder einem Fachhändler gekauft haben, sollten Ihre Lizenzen mit Ihrem Smart Software License-Konto verknüpft sein. Wenn Sie jedoch selbst Lizenzen hinzufügen müssen, verwenden Sie das Suchfeld **Find Products and Solutions** (Produkte und Lösungen suchen) im Cisco Commerce Workspace. Suchen Sie nach den folgenden Lizenz-PIDs:

Abbildung 7: Lizenzsuche



Hinweis Wenn keine PID gefunden wird, können Sie die PID manuell zu Ihrer Bestellung hinzufügen.

- Kombination aus Threat-, Malware- und URL-Lizenz:
  - L-FPR1010T-TMC =

  Wenn Sie Ihrer Bestellung eine der oben genannten PIDs hinzufügen, können Sie ein befristetes Abonnement auswählen, das einer der folgenden PIDs entspricht:
  - L-FPR1010T-TMC-1Y
  - L-FPR1010T-TMC-3Y
  - L-FPR1010T-TMC-5Y
- VPN für Remotezugriff (RA VPN): Entnehmen Sie die Einzelheiten bitte der Bestellanleitung für Cisco AnyConnect.

Schritt 2 Wenn Sie dies noch nicht getan haben, registrieren Sie Management Center beim Smart Licensing-Server.

Für die Registrierung müssen Sie ein Registrierungstoken im Smart Software Manager generieren. Ausführliche Anweisungen finden Sie im Administratorhandbuch für Cisco Secure Firewall Management Center.

Registrieren des Threat Defense beim Management Center

Registrieren Sie Threat Defense manuell mit der IP-Adresse des Geräts oder dem Host-Namen beim Management Center an.

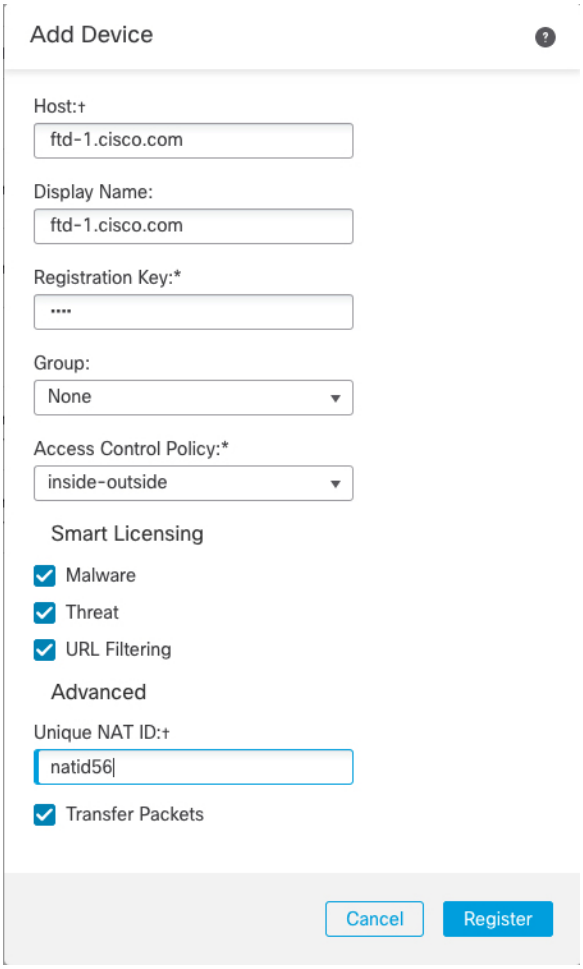
Vorbereitungen

- Sammeln Sie die folgenden Informationen, die Sie in der Erstkonfiguration festgelegt haben:
  - Threat Defense-Management-IP-Adresse oder -Host-Name und NAT-ID
  - Management Center-Registrierungsschlüssel

Prozedur

Schritt 1 Wählen Sie in Management Center nacheinander **Devices** > **Device Management** (Geräte > Gerätemanagement) aus.

Schritt 2 Wählen Sie in der Dropdown-Liste **Add** (Hinzufügen) den Eintrag **Add Device** (Gerät hinzufügen) aus.



Legen Sie die folgenden Parameter fest:

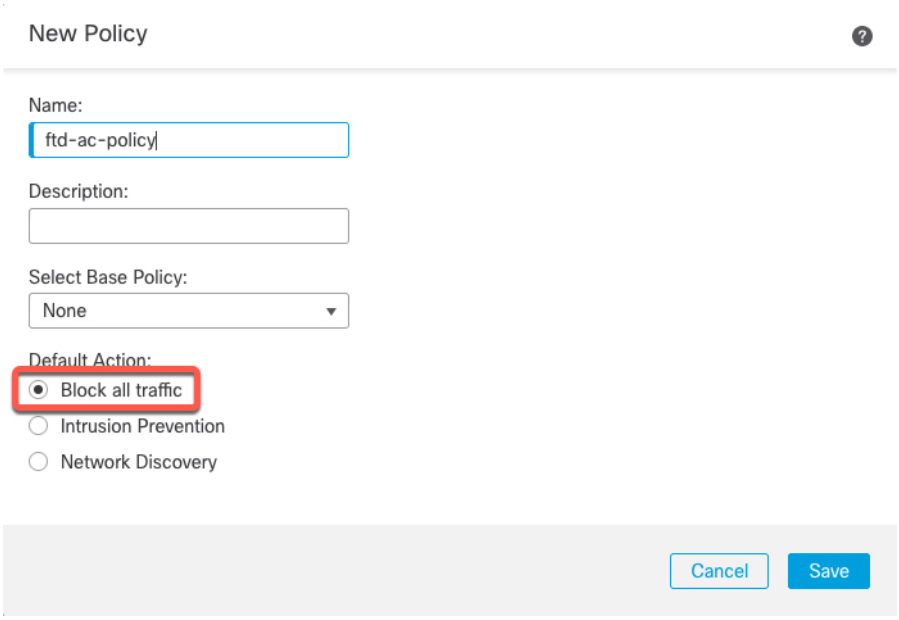
- **Host**: Geben Sie die IP-Adresse oder den Host-Namen des Threat Defense ein, das Sie hinzufügen möchten. Sie können dieses Feld leer lassen, wenn Sie in der anfänglichen Konfiguration von Threat Defense sowohl die Management Center-IP-Adresse als auch eine NAT-ID angegeben haben.

  Hinweis In einer HA-Umgebung, in der sich beide Management Center hinter einem NAT befinden, können Sie den Threat Defense ohne Host-IP oder -Namen im primären Management Center registrieren. Für die Registrierung des Threat Defense in einem sekundären Management Center müssen Sie jedoch die IP-Adresse oder den Hostnamen für den Threat Defense angeben.

- **Display Name** (Anzeigename): Geben Sie den Namen für Threat Defense ein, der im Management Center angezeigt werden soll.

- **Registration Key** (Registrierungsschlüssel): Geben Sie denselben Registrierungsschlüssel ein, den Sie in der anfänglichen Konfiguration von Threat Defense angegeben haben.
- **Domain**: Weisen Sie das Gerät einer Leaf-Domain zu, wenn Sie in einer Multi-Domain-Umgebung arbeiten.
- **Group** (Gruppe): Weisen Sie es einer Gerätegruppe zu, wenn Sie Gruppen verwenden.
- **Access Control Policy** (Zugriffskontrollrichtlinie): Wählen Sie eine anfängliche Richtlinie aus. Sofern Sie nicht bereits über eine benutzerdefinierte Richtlinie verfügen, die Sie verwenden müssen, wählen Sie **Create new policy** (Neue Richtlinie erstellen) und dann **Block all traffic** (Gesamten Traffic blockieren) aus. Sie können dies später ändern, um Traffic zuzulassen; siehe Zulassen des Traffics von innen nach außen, auf Seite 42.

Abbildung 8: Neue Richtlinie



- **Smart Licensing**: Weisen Sie die Smart Licenses zu, die Sie für die Funktionen benötigen, die Sie bereitstellen möchten: **Malware** (wenn Sie eine Malware-Untersuchung verwenden möchten), **Threat** (wenn Sie Intrusion Prevention verwenden möchten) und **URL** (wenn Sie eine kategoriebasierte URL-Filterung implementieren möchten). **Hinweis:** Nach dem Hinzufügen des Geräts können Sie über die Seite **System** > **Licenses** > **Smart Licenses** (System > Lizenzen > Smart Licenses) eine Secure Client-VPN-Lizenz für Remotezugriff anwenden.
- **Unique NAT ID** (Eindeutige NAT-ID): Geben Sie die NAT-ID an, die Sie in der anfänglichen -Threat Defense-Konfiguration angegeben haben.
- **Transfer Packets** (Pakete übertragen): Ermöglicht dem Gerät, Pakete an das Management Center zu übertragen. Wenn diese Option aktiviert ist und Ereignisse wie IPS oder Snort ausgelöst werden, sendet das Gerät Ereignismetadateninformationen und Paketdaten zur Untersuchung an Management Center. Wenn Sie die Option deaktivieren, werden nur Ereignisinformationen an Management Center gesendet, aber keine Paketdaten.

Schritt 3 Klicken Sie auf **Register** (Registrieren). Wenn Sie ein weiteres Gerät hinzufügen möchten, klicken Sie auf **Register and Add Another** (Registrieren und weiteres Gerät hinzufügen), und bestätigen Sie die erfolgreiche Registrierung.

Wenn die Registrierung erfolgreich ist, wird das Gerät der Liste hinzugefügt. Falls sie fehlschlägt, wird eine Fehlermeldung angezeigt. Wenn die Registrierung fehlschlägt, überprüfen Sie die folgenden Punkte:Threat Defense

- Ping: Rufen Sie die Threat Defense CLI auf, und pingen Sie die Management Center-IP-Adresse mit folgendem Befehl an:

  ping system *IP-Adresse*

  Wenn die Ping-Abfrage nicht erfolgreich ist, überprüfen Sie Ihre Netzwerkeinstellungen mit dem Befehl **show network**. Wenn Sie die Threat Defense-Management-IP-Adresse ändern müssen, verwenden Sie den Befehl **configure network** {**ipv4** | **ipv6**} **manual**.

- Registrierungsschlüssel, NAT-ID und Management Center-IP-Adresse: Stellen Sie sicher, dass Sie auf beiden Geräten den gleichen Registrierungsschlüssel und, falls verwendet, die NAT-ID verwenden. Sie können den Registrierungsschlüssel und die NAT-ID auf dem Management Center **configure manager add** mit dem Befehl festlegen.

Weitere Informationen zur Fehlerbehebung finden Sie unter https://cisco.com/go/fmc-reg-error.

Konfigurieren einer Basissicherheitsrichtlinie

In diesem Abschnitt wird beschrieben, wie Sie eine grundlegende Sicherheitsrichtlinie mit den folgenden Einstellungen konfigurieren:

- Interne und externe Schnittstellen: Weisen Sie der internen Schnittstelle eine statische IP-Adresse zu, und verwenden Sie DHCP für die externe Schnittstelle.
- DHCP-Server: Verwenden Sie einen DHCP-Server auf der internen Schnittstelle für Clients.
- Standardroute: Fügen Sie eine Standardroute über die externe Schnittstelle hinzu.
- NAT: Verwenden Sie die Schnittstellen-PAT für die externe Schnittstelle.
- Access Control (Zugriffskontrolle): Lassen Sie Traffic von innen nach außen zu.

Um eine grundlegende Sicherheitsrichtlinie zu konfigurieren, führen Sie die folgenden Aufgaben aus.

1	Konfigurieren von Schnittstellen (6.5 und höher), auf Seite 29 Konfigurieren von Schnittstellen (6.4), auf Seite 33.
2	Konfigurieren des DHCP-Servers, auf Seite 36.
3	Hinzufügen der Standardroute, auf Seite 37.
4	Konfigurieren von NAT, auf Seite 39.

5	Zulassen des Traffics von innen nach außen, auf Seite 42.
6	Bereitstellen der Konfiguration, auf Seite 43.

Konfigurieren von Schnittstellen (6.5 und höher)

Fügen Sie die VLAN1-Schnittstelle für die Switch-Ports hinzu, oder konvertieren Sie Switch-Ports in Firewall-Schnittstellen, weisen Sie Schnittstellen zu Sicherheitszonen zu, und legen Sie die IP-Adressen fest. In der Regel müssen Sie mindestens zwei Schnittstellen konfigurieren, um ein System einzurichten, das sinnvollen Traffic weiterleitet. Normalerweise haben Sie eine externe Schnittstelle, die dem Upstream-Router oder dem Internet zugekehrt ist, und eine oder mehrere Schnittstellen im Inneren für die Netzwerke Ihres Unternehmens. Standardmäßig ist Ethernet1 / 1 eine normale Firewall-Schnittstelle, die Sie für den Außenbereich verwenden können. Die verbleibenden Schnittstellen sind Switch-Ports in VLAN 1; nachdem Sie die VLAN1-Schnittstelle hinzugefügt haben, können Sie sie zu Ihrer internen Schnittstelle machen. Sie können Switch-Ports auch anderen VLANs zuweisen oder Switch-Ports in Firewall-Schnittstellen konvertieren.

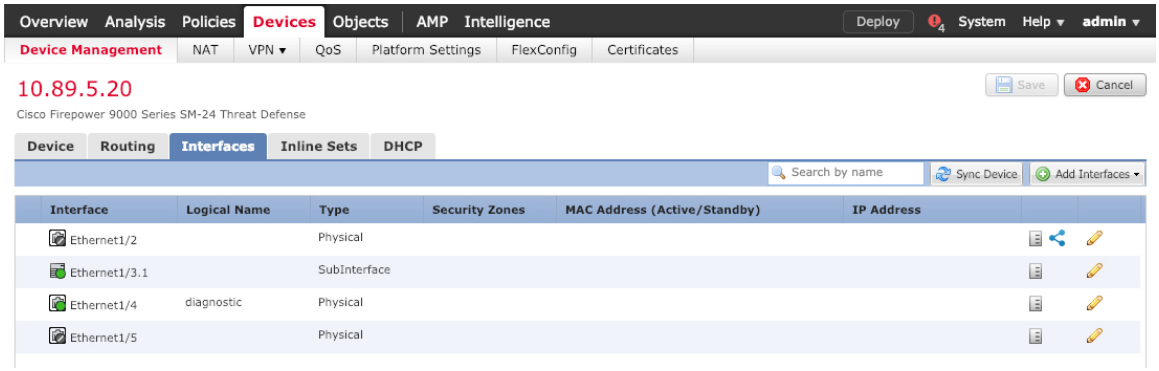
In einer typischen Edge-Routing-Situation beziehen Sie die Adresse der externen Schnittstelle über DHCP von Ihrem ISP, während Sie statische Adressen für die Schnittstellen im Inneren (internen Schnittstellen) definieren.

Im folgenden Beispiel wird eine interne Schnittstelle im Modus „geroutet“ (VLAN1) mit einer statischen Adresse und eine externe Schnittstelle im Modus „geroutet“ unter Verwendung von DHCP (Ethernet1/1) konfiguriert.

Prozedur

Schritt 1 Wählen Sie **Devices** > **Device Management** (Geräte > Gerätemanagement), und klicken Sie für das Gerät auf **Bearbeiten** ( ).

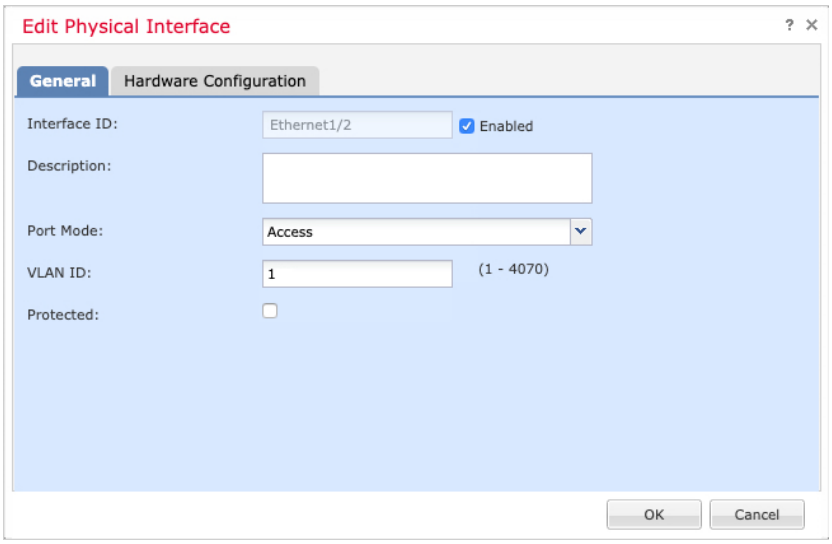
Schritt 2 Klicken Sie auf **Interfaces** (Schnittstellen).



Schritt 3 (optional) Deaktivieren Sie den Switch-Port-Modus für die Switch-Ports (Ethernet1/2 bis 1/8), indem Sie auf den Schieberegler in der Spalte **SwitchPort** klicken, damit er als deaktiviert ( ) angezeigt wird.

Schritt 4 Aktivieren Sie die Switch-Ports.

a) Klicken Sie für den Switch-Port auf **Bearbeiten** ( ).

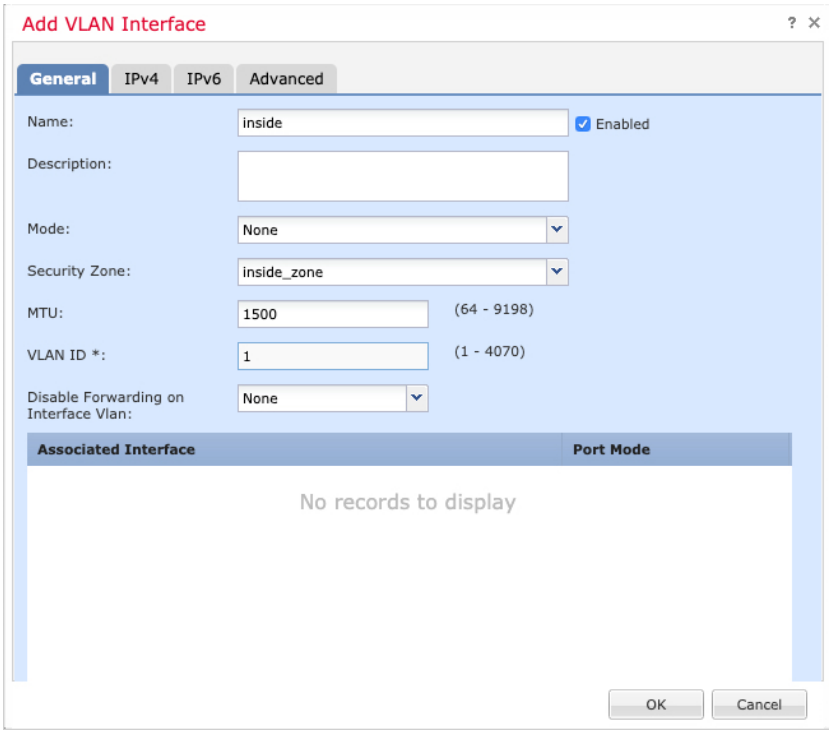


b) Aktivieren Sie die Schnittstelle, indem Sie das Kontrollkästchen **Enabled** (Aktiviert) markieren.
c) (optional) Ändern Sie die VLAN-ID; der Standardwert ist 1. Als Nächstes fügen Sie eine VLAN-Schnittstelle hinzu, die dieser ID entspricht.
d) Klicken Sie auf **OK**.

Schritt 5 Fügen Sie die *interne* VLAN-Schnittstelle hinzu.

a) Klicken Sie auf **Add Interfaces** > **VLAN Interface** (Schnittstellen hinzufügen > VLAN-Schnittstelle).

Die Registerkarte **General** (Allgemein) wird geöffnet.



b) Geben Sie einen **Namen** mit bis zu 48 Zeichen ein.

Nennen Sie die Schnittstelle beispielsweise **inside**.

c) Markieren Sie das Kontrollkästchen **Enabled** (Aktiviert).

d) Übernehmen Sie die Einstellung **None** (Keiner) für **Mode** (Modus).

e) Wählen Sie in der Dropdown-Liste **Security Zone** (Sicherheitszone) eine vorhandene interne Sicherheitszone aus, oder fügen Sie eine neue hinzu, indem Sie auf **New** (Neu) klicken.

Fügen Sie beispielsweise eine Zone mit dem Namen **inside_zone** hinzu. Jede Schnittstelle muss einer Sicherheitszone und/oder Schnittstellengruppe zugewiesen werden. Eine Schnittstelle kann nur zu einer Sicherheitszone, aber gleichzeitig auch zu mehreren Schnittstellengruppen gehören. Sie wenden Ihre Sicherheitsrichtlinie basierend auf Zonen oder Gruppen an. Sie können beispielsweise die interne Schnittstelle der internen Zone zuweisen und die externe Schnittstelle zur Außenzone. Anschließend können Sie Ihre Zugriffskontrollrichtlinie so konfigurieren, dass der Traffic von innen nach außen geleitet wird, aber nicht von außen nach innen. Die meisten Richtlinien unterstützen nur Sicherheitszonen. Sie können Zonen oder Schnittstellengruppen in NAT-Richtlinien, Vorfilterrichtlinien und QoS-Richtlinien verwenden.

f) Setzen Sie die **VLAN-ID** auf **1**.

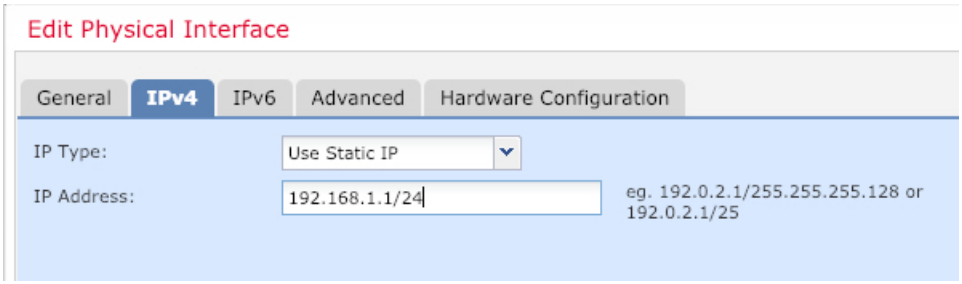
Standardmäßig sind alle Switch-Ports auf VLAN 1 eingestellt. Wenn Sie hier eine andere VLAN-ID auswählen, müssen Sie auch jeden Switch-Port bearbeiten, damit er auf die neue VLAN-ID gesetzt ist.

Sie können die VLAN-ID nicht mehr ändern, nachdem Sie die Schnittstelle gespeichert haben. Die VLAN-ID ist sowohl der verwendete VLAN-Tag als auch die Schnittstellen-ID in Ihrer Konfiguration.

g) Klicken Sie auf die Registerkarte **IPv4** und/oder **IPv6**.

- **IPv4**: Wählen Sie in der Dropdown-Liste **Use Static IP** (Statische IP verwenden) aus, und geben Sie eine IP-Adresse und eine Subnetzmaske in der Schreibweise mit Schrägstrichen ein.

  Geben Sie beispielsweise **192.168.1.1/24** ein.

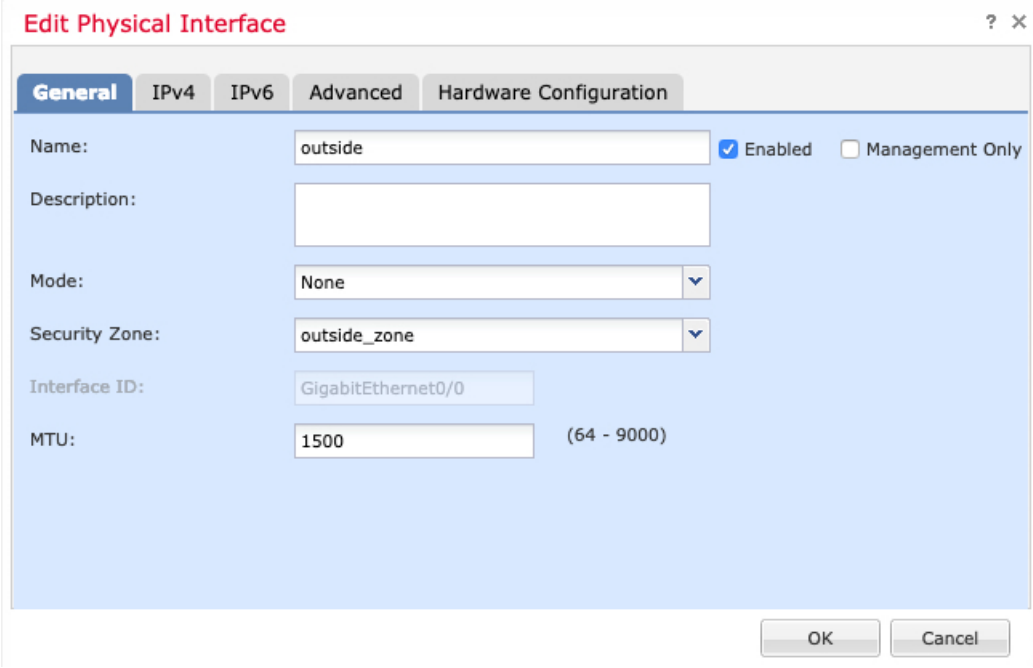


- **IPv6**: Markieren Sie das Kontrollkästchen **Autoconfiguration** (Automatische Konfiguration) für eine automatische Stateless-Konfiguration.

h) Klicken Sie auf **OK**.

Schritt 6 Klicken Sie für die Ethernet1/1-Schnittstelle, die Sie für den *Außenbereich* verwenden möchten, auf **Bearbeiten** (✎).

Die Registerkarte **General** (Allgemein) wird geöffnet.



Hinweis Wenn Sie diese Schnittstelle für den Managerzugriff vorkonfiguriert haben, hat die Schnittstelle bereits einen Namen und ist aktiviert und adressiert. Sie sollten keine dieser Grundeinstellungen ändern, da dadurch die Management Center-Managementverbindung unterbrochen würde. Sie können die Sicherheitszone auf diesem Bildschirm jedoch für Richtlinien bezüglich des Durchgangs-Traffics konfigurieren.

a) Geben Sie einen **Namen** mit bis zu 48 Zeichen ein.

   Nennen Sie die Schnittstelle beispielsweise **outside**.

b) Markieren Sie das Kontrollkästchen **Enabled** (Aktiviert).

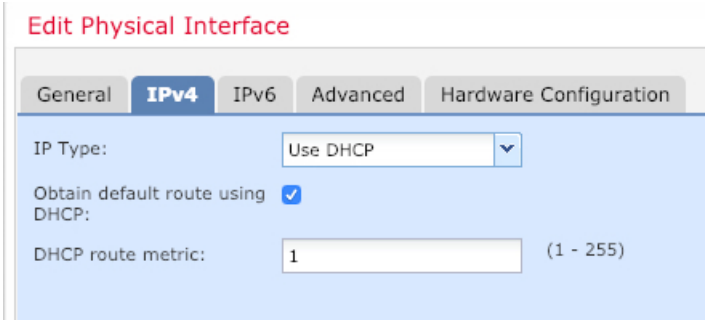
c) Übernehmen Sie die Einstellung **None** (Keiner) für **Mode** (Modus).

d) Wählen Sie in der Dropdown-Liste **Security Zone** (Sicherheitszone) eine vorhandene externe Sicherheitszone aus, oder fügen Sie eine neue hinzu, indem Sie auf **New** (Neu) klicken.

   Fügen Sie beispielsweise eine Zone mit dem Namen **outside_zone** hinzu.

e) Klicken Sie auf die Registerkarte **IPv4** und/oder **IPv6**.

   - **IPv4**: Wählen Sie **Use DHCP** (DHCP verwenden) aus, und konfigurieren Sie die folgenden optionalen Parameter:
     - **Obtain default route using DHCP** (Standardroute über DHCP abrufen): Ruft die Standardroute vom DHCP-Server ab.
     - **DHCP route metric** (DHCP-Routenmetrik): Weist der gelernten Route eine administrative Distanz zwischen 1 und 255 zu. Die standardmäßige administrative Distanz für die gelernten Routen ist 1.



- **IPv6**: Markieren Sie das Kontrollkästchen **Autoconfiguration** (Automatische Konfiguration) für eine automatische Stateless-Konfiguration.

f) Klicken Sie auf **OK**.

Schritt 7 Klicken Sie auf **Save** (Speichern).

Konfigurieren von Schnittstellen (6.4)

Aktivieren Sie Threat Defense-Schnittstellen, weisen Sie sie Sicherheitszonen zu und legen Sie die IP-Adressen fest. In der Regel müssen Sie mindestens zwei Schnittstellen konfigurieren, um ein System einzurichten, das sinnvollen Traffic weiterleitet. Normalerweise haben Sie eine externe Schnittstelle, die dem Upstream-Router oder dem Internet zugekehrt ist, und eine oder mehrere Schnittstellen im Inneren für die Netzwerke Ihres Unternehmens. Einige dieser Schnittstellen sind möglicherweise „demilitarisierte Zonen“ (DMZs), in denen Sie öffentlich zugängliche Ressourcen wie Ihren Webserver platzieren.

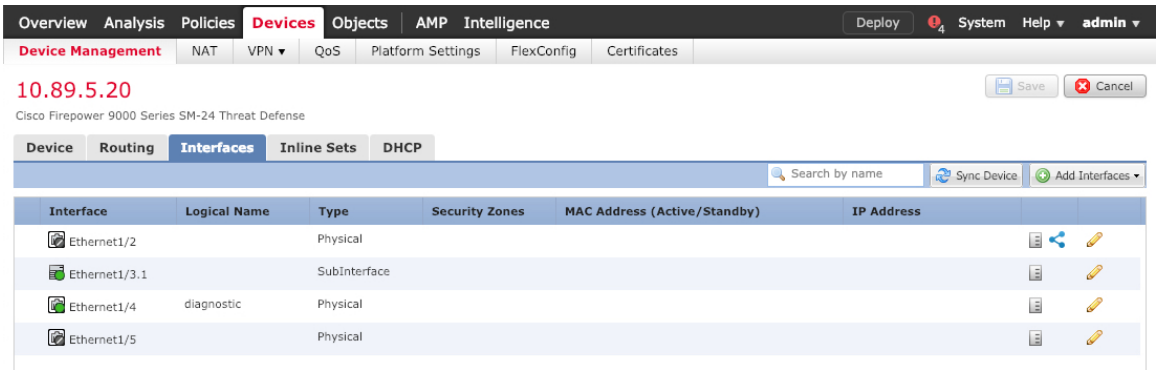
In einer typischen Edge-Routing-Situation beziehen Sie die Adresse der externen Schnittstelle über DHCP von Ihrem ISP, während Sie statische Adressen für die Schnittstellen im Inneren (internen Schnittstellen) definieren.

Im folgenden Beispiel wird eine interne Schnittstelle im Modus „geroutet“ mit einer statischen Adresse und eine externe Schnittstelle im Modus „geroutet“ unter Verwendung von DHCP konfiguriert.

Prozedur

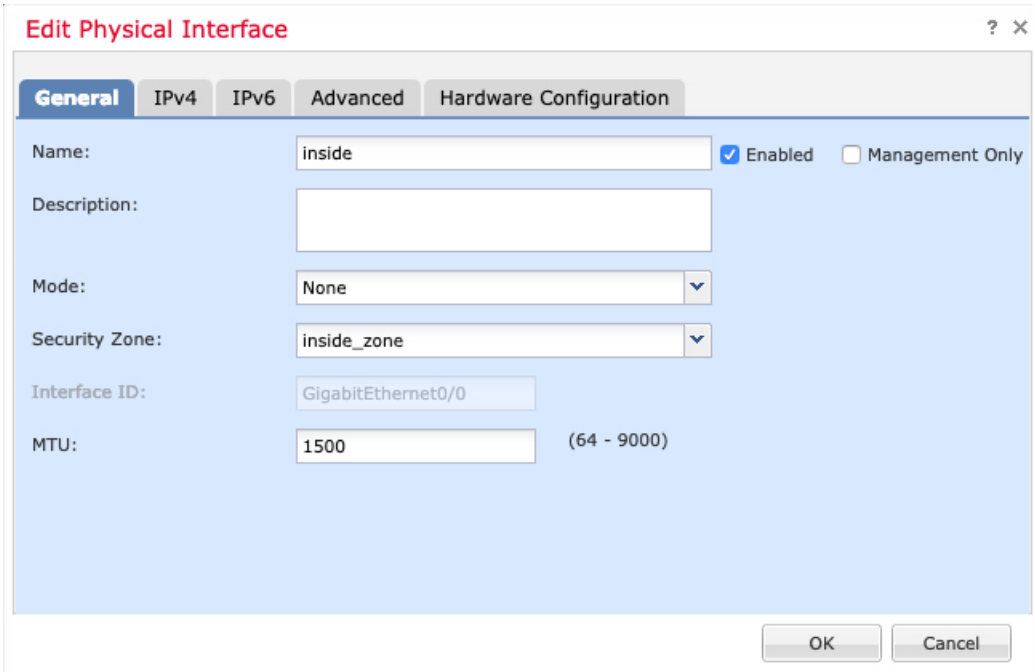
Schritt 1 Wählen Sie **Devices** > **Device Management** (Geräte > Gerätemanagement), und klicken Sie für die Firewall auf **Bearbeiten** ( ).

Schritt 2 Klicken Sie auf **Interfaces** (Schnittstellen).



Schritt 3 Klicken Sie für die Schnittstelle, die Sie *intern* verwenden möchten, auf **Bearbeiten** ( ).

Die Registerkarte **General** (Allgemein) wird geöffnet.



a) Geben Sie einen **Namen** mit bis zu 48 Zeichen ein.

   Nennen Sie die Schnittstelle beispielsweise **inside**.

b) Markieren Sie das Kontrollkästchen **Enabled** (Aktiviert).

c) Übernehmen Sie die Einstellung **None** (Keiner) für **Mode** (Modus).

d) Wählen Sie in der Dropdown-Liste **Security Zone** (Sicherheitszone) eine vorhandene interne Sicherheitszone aus, oder fügen Sie eine neue hinzu, indem Sie auf **New** (Neu) klicken.

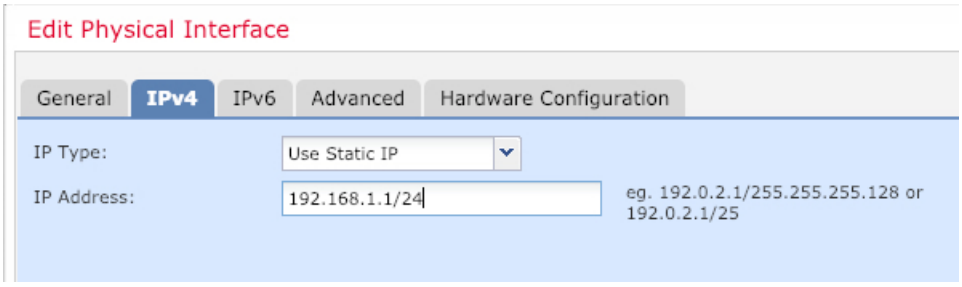
   Fügen Sie beispielsweise eine Zone mit dem Namen **inside_zone** hinzu. Jede Schnittstelle muss einer Sicherheitszone und/oder Schnittstellengruppe zugewiesen werden. Eine Schnittstelle kann nur zu einer Sicherheitszone, aber gleichzeitig auch zu mehreren Schnittstellengruppen gehören. Sie wenden Ihre Sicherheitsrichtlinie basierend auf Zonen oder Gruppen an. Sie können beispielsweise die interne Schnittstelle der internen Zone zuweisen und die externe Schnittstelle zur Außenzone. Anschließend können Sie Ihre Zugriffskontrollrichtlinie so konfigurieren, dass der Traffic von innen nach außen geleitet

wird, aber nicht von außen nach innen. Die meisten Richtlinien unterstützen nur Sicherheitszonen. Sie können Zonen oder Schnittstellengruppen in NAT-Richtlinien, Vorfilterrichtlinien und QoS-Richtlinien verwenden.

e) Klicken Sie auf die Registerkarte **IPv4** und/oder **IPv6**.

- **IPv4**: Wählen Sie in der Dropdown-Liste **Use Static IP** (Statische IP verwenden) aus, und geben Sie eine IP-Adresse und eine Subnetzmaske in der Schreibweise mit Schrägstrichen ein.

  Geben Sie beispielsweise **192.168.1.1/24** ein.

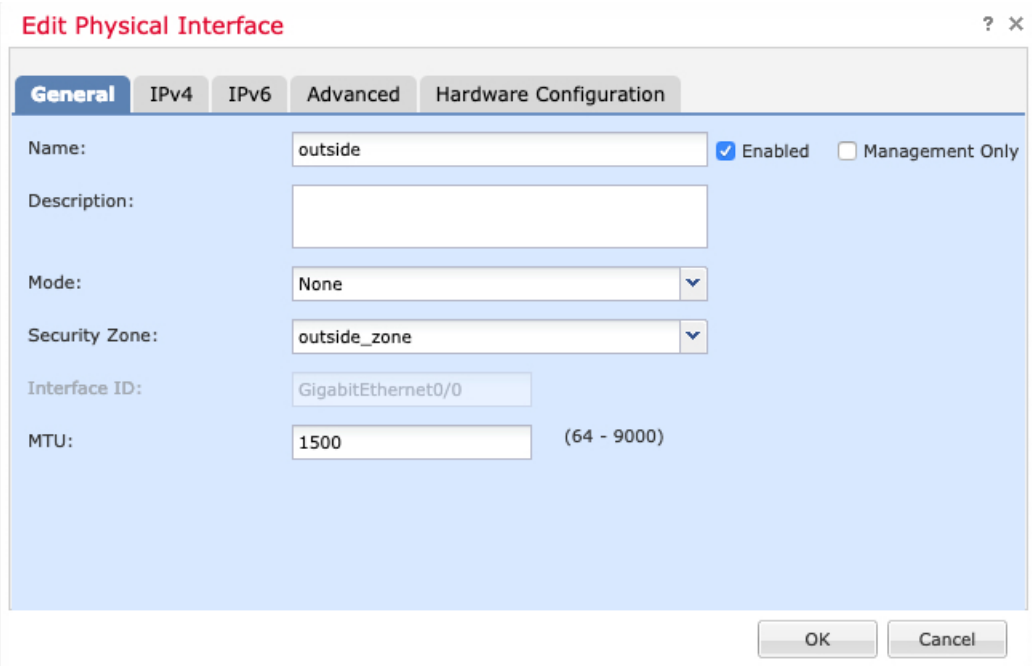


- **IPv6**: Markieren Sie das Kontrollkästchen **Autoconfiguration** (Automatische Konfiguration) für eine automatische Stateless-Konfiguration.

f) Klicken Sie auf **OK**.

Schritt 4 Klicken Sie für die Schnittstelle, die Sie für den *Außenbereich* verwenden möchten, auf **Bearbeiten** ( ).

Die Registerkarte **General** (Allgemein) wird geöffnet.



Hinweis Wenn Sie diese Schnittstelle für den Managerzugriff vorkonfiguriert haben, hat die Schnittstelle bereits einen Namen und ist aktiviert und adressiert. Sie sollten keine dieser Grundeinstellungen ändern, da dadurch die Management Center-Managementverbindung unterbrochen würde. Sie können die Sicherheitszone auf diesem Bildschirm jedoch für Richtlinien bezüglich des Durchgangs-Traffics konfigurieren.

a) Geben Sie einen **Namen** mit bis zu 48 Zeichen ein.

Nennen Sie die Schnittstelle beispielsweise **outside**.

b) Markieren Sie das Kontrollkästchen **Enabled** (Aktiviert).

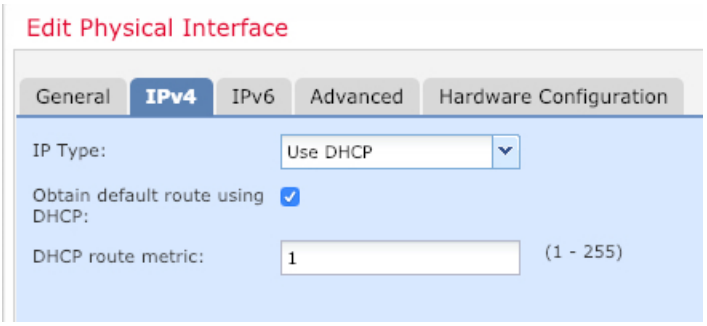
c) Übernehmen Sie die Einstellung **None** (Keiner) für **Mode** (Modus).

d) Wählen Sie in der Dropdown-Liste **Security Zone** (Sicherheitszone) eine vorhandene externe Sicherheitszone aus, oder fügen Sie eine neue hinzu, indem Sie auf **New** (Neu) klicken.

Fügen Sie beispielsweise eine Zone mit dem Namen **outside_zone** hinzu.

e) Klicken Sie auf die Registerkarte **IPv4** und/oder **IPv6**.

- **IPv4**: Wählen Sie **Use DHCP** (DHCP verwenden) aus, und konfigurieren Sie die folgenden optionalen Parameter:
  - **Obtain default route using DHCP** (Standardroute über DHCP abrufen): Ruft die Standardroute vom DHCP-Server ab.
  - **DHCP route metric** (DHCP-Routenmetrik): Weist der gelernten Route eine administrative Distanz zwischen 1 und 255 zu. Die standardmäßige administrative Distanz für die gelernten Routen ist 1.



- **IPv6**: Markieren Sie das Kontrollkästchen **Autoconfiguration** (Automatische Konfiguration) für eine automatische Stateless-Konfiguration.

f) Klicken Sie auf **OK**.

Schritt 5 Klicken Sie auf **Save** (Speichern).

Konfigurieren des DHCP-Servers

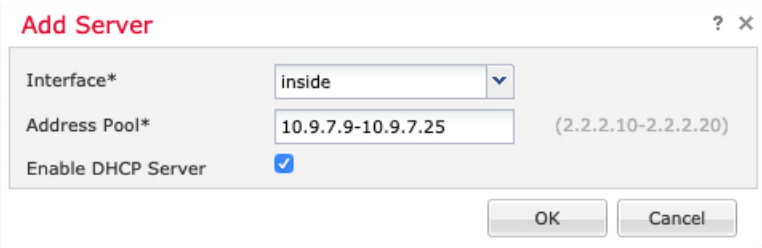
Aktivieren Sie den DHCP-Server, wenn Clients DHCP zum Abrufen von IP-Adressen aus dem Threat Defense verwenden sollen.

Prozedur

Schritt 1 Wählen Sie **Devices** > **Device Management** (Geräte > Gerätemanagement), und klicken Sie für das Gerät auf **Bearbeiten** (✎).

Schritt 2 Wählen Sie **DHCP** > **DHCP Server** (DHCP > DHCP-Server).

Schritt 3 Klicken Sie auf der Seite **Server** auf **Add** (Hinzufügen), und konfigurieren Sie die folgenden Optionen:



- **Interface** (Schnittstelle): Wählen Sie in der Dropdown-Liste die Schnittstelle aus.
- **Address Pool** (Adressen-Pool): Legen Sie den Bereich der niedrigsten bis höchsten IP-Adressen fest, die vom DHCP-Server verwendet werden. Der Bereich der IP-Adressen muss sich im selben Subnetz wie die ausgewählte Schnittstelle befinden und darf die IP-Adresse der Schnittstelle selbst nicht enthalten.
- **Enable DHCP Server** (DHCP-Server aktivieren): Aktiviert den DHCP-Server auf der ausgewählten Schnittstelle.

Schritt 4 Klicken Sie auf **OK**.

Schritt 5 Klicken Sie auf **Save** (Speichern).

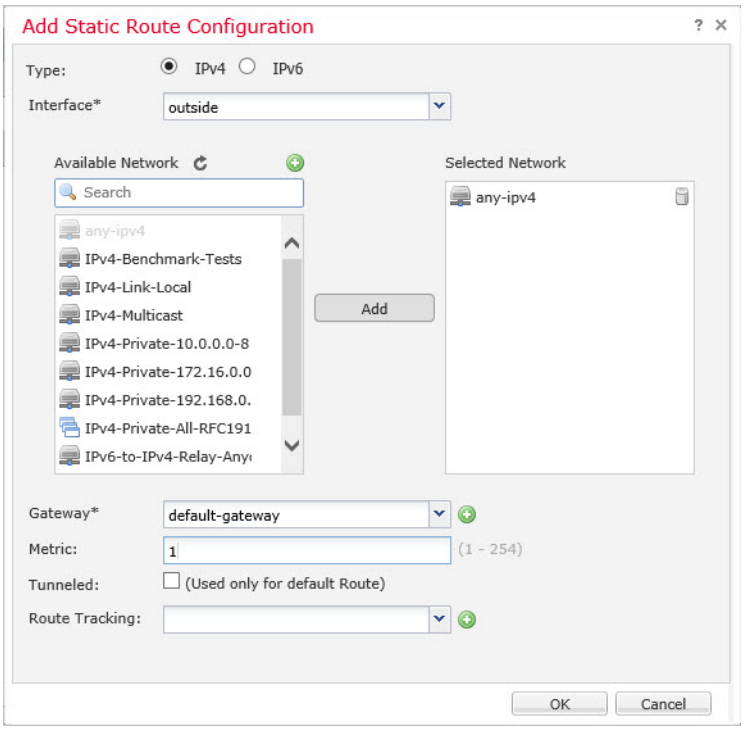
Hinzufügen der Standardroute

Die Standardroute zeigt normalerweise auf den Upstream-Router, der über die externe Schnittstelle erreichbar ist. Wenn Sie DHCP für die externe Schnittstelle verwenden, hat Ihr Gerät möglicherweise bereits eine Standardroute erhalten. Falls Sie die Route manuell hinzufügen müssen, führen Sie dieses Verfahren aus. Wenn Sie eine Standardroute vom DHCP-Server erhalten haben, wird diese in der Tabelle **IPv4 Routes** (IPv4-Routen) oder **IPv6 Routes** (IPv6-Routen) auf der Seite **Devices** > **Device Management** > **Routing** > **Static Route** (Geräte > Gerätemanagement > Routing > Statische Route) angezeigt.

Prozedur

Schritt 1 Wählen Sie **Devices** > **Device Management** (Geräte > Gerätemanagement), und klicken Sie für das Gerät auf **Bearbeiten** (✎).

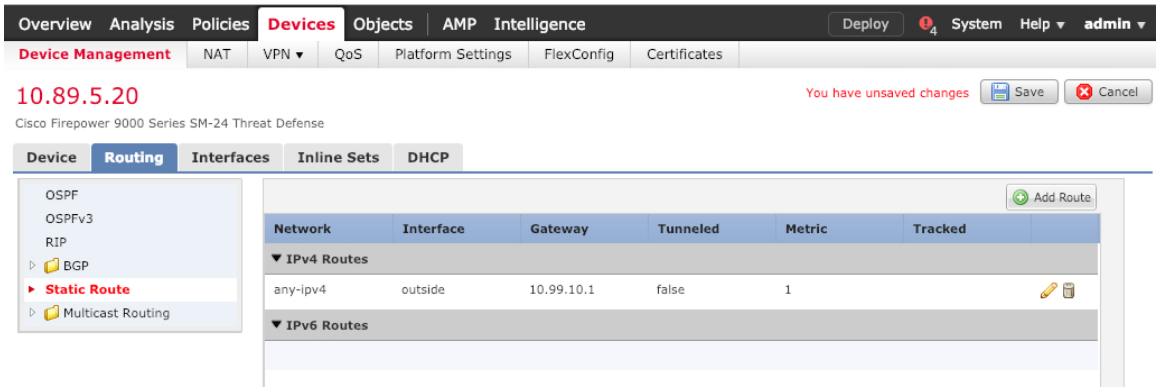
Schritt 2 Wählen Sie **Routing** > **Static Route** (Routing > Statische Route), klicken Sie auf **Add Route** (Route hinzufügen), und legen Sie Folgendes fest:



- **Type** (Typ): Klicken Sie auf das Optionsfeld **IPv4** oder **IPv6**, je nachdem, welche Art von statischer Route Sie hinzufügen.
- **Interface** (Schnittstelle): Wählen Sie die Egress-Schnittstelle aus. Dies ist in der Regel die externe Schnittstelle.
- **Available Network** (Verfügbares Netzwerk): Wählen Sie **any-ipv4** für eine IPv4-Standardroute oder **any-ipv6** für eine IPv6-Standardroute, und klicken Sie auf **Add** (Hinzufügen), um es in die Liste **Selected Network** (Ausgewähltes Netzwerk) zu verschieben.
- **Gateway** oder **IPv6-Gateway**: Geben Sie den Gateway-Router ein, der der nächste Hop für diese Route ist, oder wählen Sie ihn aus. Sie können eine IP-Adresse oder ein Netzwerk-/Hostobjekt angeben.
- **Metric** (Metrik): Geben Sie die Anzahl der Hops zum Zielnetzwerk ein. Gültig sind Werte von 1 bis 255; der Standardwert ist 1.

Schritt 3 Klicken Sie auf **OK**.

Die Route wird der Tabelle mit statischen Routen hinzugefügt.



Schritt 4 Klicken Sie auf **Save** (Speichern).

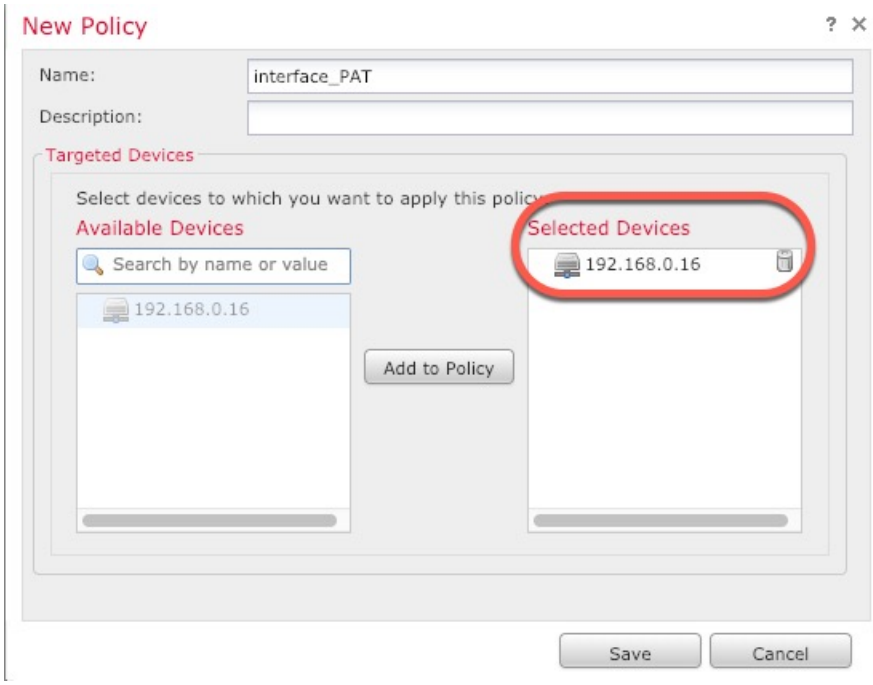
Konfigurieren von NAT

Eine typische NAT-Regel konvertiert interne Adressen in einen Port an der IP-Adresse der externen Schnittstelle. Diese Art von NAT-Regel wird als *Interface Port Address Translation (PAT)* bezeichnet.

Prozedur

Schritt 1 Wählen Sie **Devices** > **NAT** (Geräte > NAT), und klicken Sie auf **New Policy** > **Threat Defense NAT** (Neue Richtlinie > Threat Defense-NAT).

Schritt 2 Geben Sie der Richtlinie einen Namen, wählen Sie die Geräte aus, für die sie gelten soll, und klicken Sie auf **Save** (Speichern).



Die Zuordnung zwischen der Richtlinie und Management Center wird vorgenommen. Sie müssen der Richtlinie noch Regeln hinzufügen.

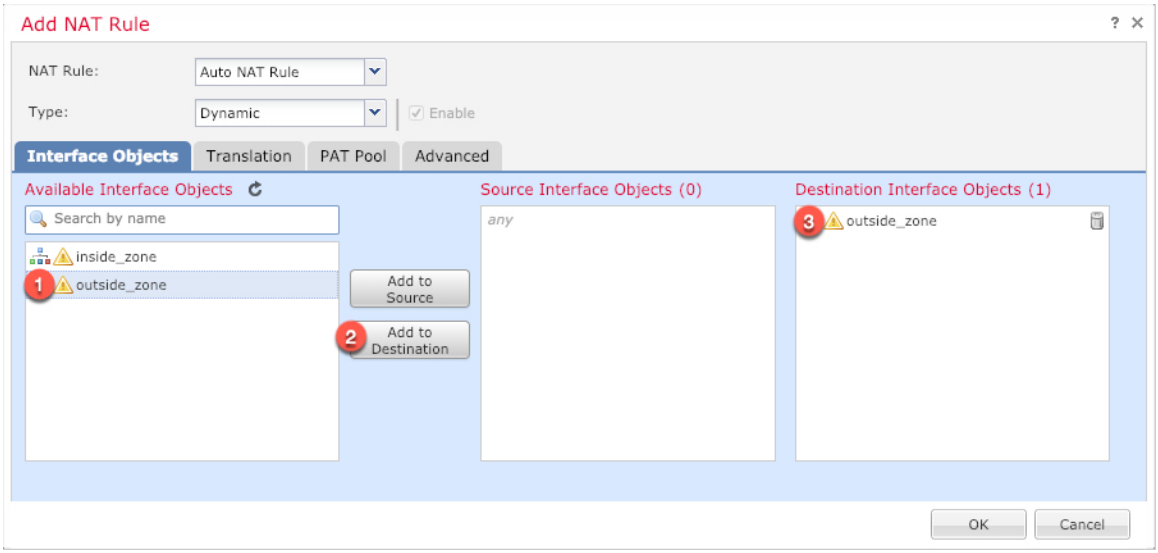
Schritt 3 Klicken Sie auf **Add Rule** (Regel hinzufügen).

Das Dialogfeld **Add NAT Rule** (NAT-Regel hinzufügen) wird angezeigt.

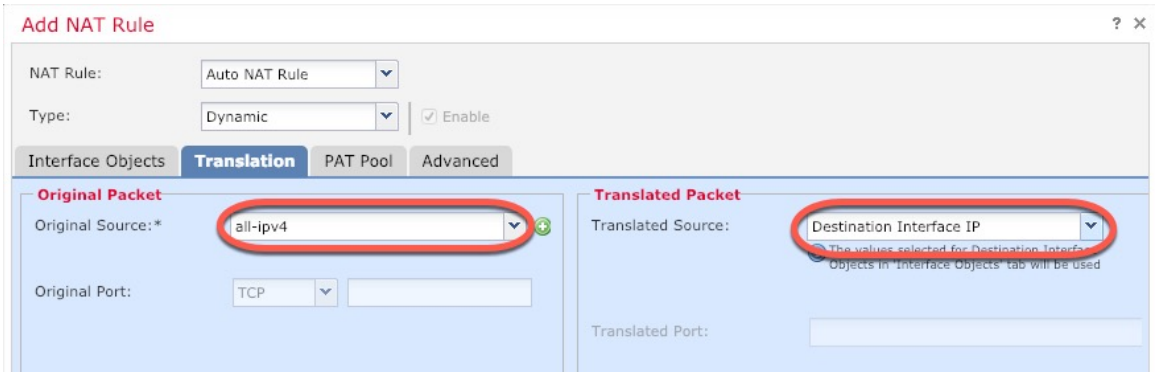
Schritt 4 Konfigurieren Sie die grundlegenden Regeloptionen:

- **NAT Rule** (NAT-Regel): Wählen Sie **Auto NAT Rule** (Automatische NAT-Regel) aus.
- **Type** (Typ): Wählen Sie **Dynamic** (Dynamisch) aus.

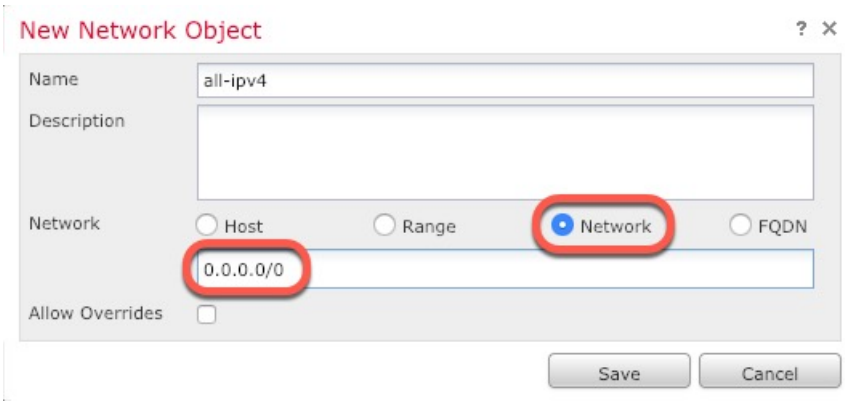
Schritt 5 Fügen Sie auf der Seite **Interface Objects** (Schnittstellenobjekte) die externe Zone aus dem Bereich **Available Interface Objects** (Verfügbare Schnittstellenobjekte) im Bereich **Destination Interface Objects** (Zielschnittstellenobjekte) hinzu.



Schritt 6 Konfigurieren Sie auf der Seite **Translation** (Übersetzung) die folgenden Optionen:



- **Original Source** (Ursprüngliche Quelle): Klicken Sie auf **Hinzufügen** (+), um ein Netzwerkobjekt für den gesamten IPv4-Traffic (0.0.0.0/0) hinzuzufügen.

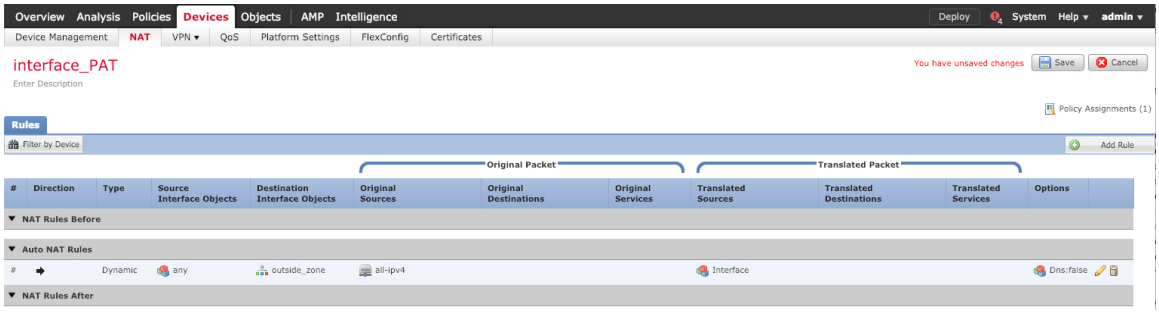


Hinweis Sie können das systemdefinierte Objekt **any-ipv4** nicht verwenden, da Auto-NAT-Regeln NAT als Teil der Objektdefinition hinzufügen, und Sie können systemdefinierte Objekte nicht bearbeiten.

- **Translated Source** (Übersetzte Quelle): Wählen Sie für **Destination Interface IP** (Zielschnittstellen-IP) einen Wert aus.

Schritt 7 Klicken Sie auf **Save** (Speichern), um die Regel hinzuzufügen.

Die Regel wird in der Tabelle **Rules** (Regeln) gespeichert.



Schritt 8 Klicken Sie auf der Seite **NAT** auf **Save** (Speichern), um Ihre Änderungen zu speichern.

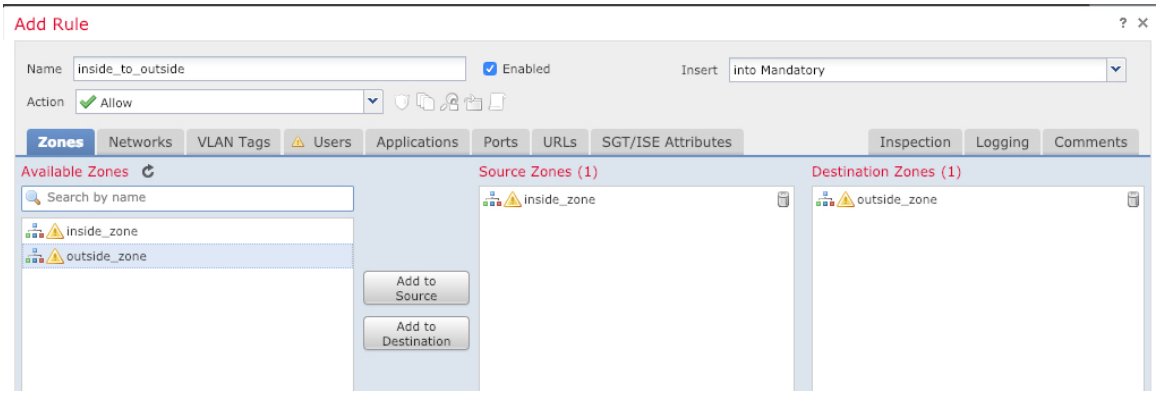
Zulassen des Traffics von innen nach außen

Wenn Sie bei der Registrierung von Threat Defense eine grundlegende Zugriffskontrollrichtlinie zum Blockieren des gesamten Traffics (**Block all traffic**) erstellt haben, müssen Sie der Richtlinie Regeln hinzufügen, um Traffic über das Gerät zuzulassen. Das folgende Verfahren fügt eine Regel hinzu, die Traffic von der internen Zone zur externen Zone zulässt. Wenn Sie über andere Zonen verfügen, müssen Sie Regeln hinzufügen, die den Traffic zu den entsprechenden Netzwerken zulassen.

Prozedur

Schritt 1 Wählen Sie **Policy** > **Access Policy** > **Access Policy** (Richtlinie > Zugriffsrichtlinie > Zugriffsrichtlinie) aus, und klicken Sie auf **Bearbeiten** (✎) für die Zugriffskontrollrichtlinie, die dem Threat Defense zugewiesen ist.

Schritt 2 Klicken Sie auf **Add Rule** (Regel hinzufügen), und legen Sie die folgenden Parameter fest:

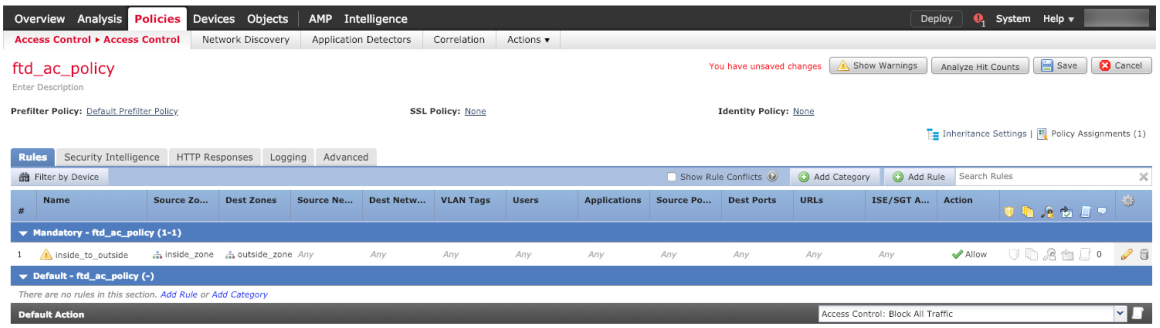


- **Name**: Geben Sie dieser Regel einen Namen, z. B. **inside_to_outside**.
- **Source Zones** (Quellzonen): Wählen Sie in **Available Zones** (Verfügbare Zonen) die interne Zone aus, und klicken Sie auf **Add to Source** (Zu Quelle hinzufügen).
- **Destination Zones** (Zielzonen): Wählen Sie in **Available Zones** (Verfügbare Zonen) die externe Zone aus, und klicken Sie auf **Add to Destination** (Zu Ziel hinzufügen).

Lassen Sie die anderen Einstellungen unverändert.

Schritt 3 Klicken Sie auf **Add** (Hinzufügen).

Die Regel wird der Tabelle **Rules** (Regeln) hinzugefügt.



Schritt 4 Klicken Sie auf **Save** (Speichern).

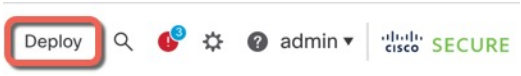
Bereitstellen der Konfiguration

Stellen Sie die Konfigurationsänderungen für Threat Defense bereit. Keine Ihrer Änderungen ist auf dem Gerät aktiv, bis Sie sie bereitstellen.

Prozedur

Schritt 1 Klicken Sie oben rechts auf **Deploy** (Bereitstellen).

Abbildung 9: Bereitstellen



Schritt 2 Klicken Sie entweder auf **Deploy All** (Alle bereitstellen), um die Bereitstellung auf allen Geräten durchzuführen, oder auf **Advanced Deploy** (Erweiterte Bereitstellung), um die Bereitstellung auf ausgewählten Geräten durchzuführen.

Abbildung 10: Alle bereitstellen

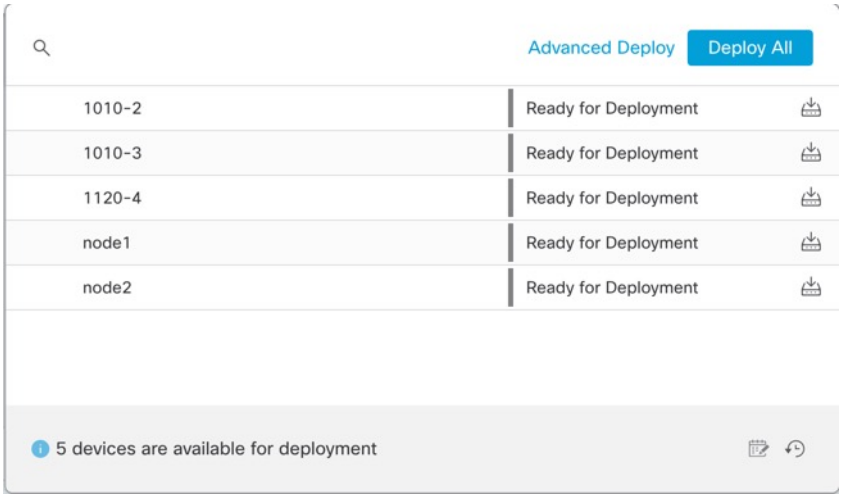
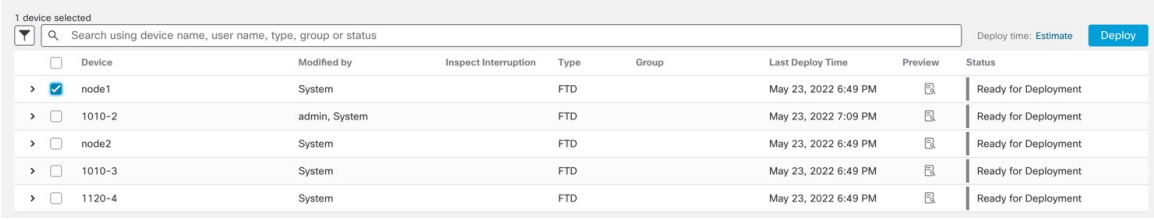
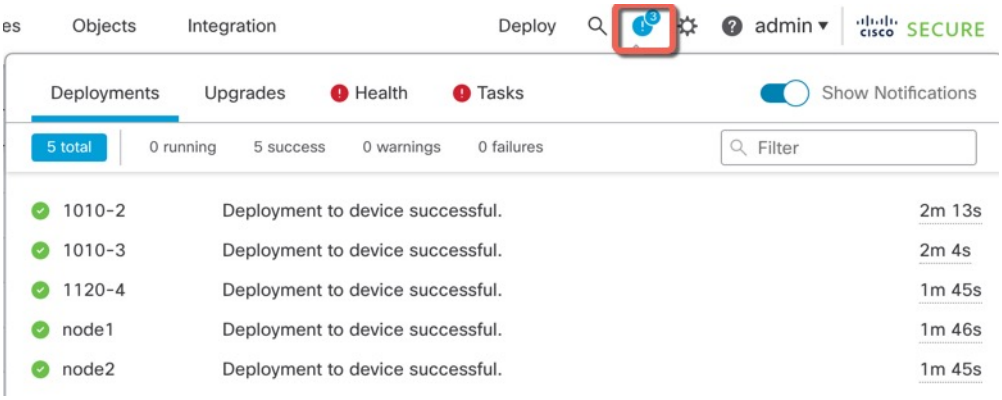


Abbildung 11: Erweiterte Bereitstellung



Schritt 3 Stellen Sie sicher, dass die Bereitstellung erfolgreich ist. Klicken Sie in der Menüleiste rechts neben der Schaltfläche **Deploy** (Bereitstellen) auf das Symbol, um den Status der Bereitstellungen anzuzeigen.

Abbildung 12: Bereitstellungsstatus



Zugriff auf die Threat Defense- und FXOS-CLI

Verwenden Sie die Befehlszeilenschnittstelle (CLI), um das System einzurichten und grundlegende Systemfehlerbehebungen durchzuführen. Sie können Richtlinien nicht über eine CLI-Sitzung konfigurieren. Für den Zugriff auf die CLI (Befehlszeilenschnittstelle) müssen Sie eine Verbindung zum Konsolenport herstellen.

Sie können zur Fehlerbehebung auch auf die FXOS-CLI-CLI zugreifen.

Hinweis Sie können auch eine SSH-Sitzung für die Management-Schnittstelle des Threat Defense-Geräts nutzen. Im Gegensatz zu einer Konsolensitzung verwendet die SSH-Sitzung standardmäßig die Threat Defense-CLI, über die Sie sich mit dem Befehl **connect fxos** mit der FXOS-CLI-CLI verbinden können. Sie können sich später mit der Adresse auf einer Datenschnittstelle verbinden, wenn Sie die Schnittstelle für SSH-Verbindungen öffnen. Der SSH-Zugriff auf Datenschnittstellen ist standardmäßig deaktiviert. Dieses Verfahren beschreibt den Konsolenportzugriff, der standardmäßig auf die FXOS-CLI-CLI eingestellt ist.

Prozedur

Schritt 1 Verbinden Sie Ihren Management-Computer mit dem Konsolenport, um sich bei der CLI anzumelden. Firepower 1000 wird mit einem seriellen USB-A-zu-B-Kabel ausgeliefert. Stellen Sie sicher, dass Sie alle erforderlichen seriellen USB-Treiber für Ihr Betriebssystem installieren (siehe Firepower 1010 -Hardwarehandbuch). Der Konsolenport ist standardmäßig auf die FXOS-CLI-CLI eingestellt. Verwenden Sie die folgenden seriellen Einstellungen:

- 9.600 Baud
- 8 Daten-Bits
- Keine Parität
- 1 Stopp-Bit

Sie stellen eine Verbindung zum FXOS-CLI her. Melden Sie sich bei der CLI mit dem Benutzernamen **admin** und dem Kennwort an, das Sie bei der Ersteinrichtung festgelegt haben (der Standardwert ist **Admin123**).

Beispiel:

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

Schritt 2 Greifen Sie auf die Threat Defense-CLI zu.

connect ftd

Beispiel:

```
firepower# connect ftd
>
```

Geben Sie nach der Anmeldung **help** oder **?** ein, um Informationen zu den Befehlen aufzurufen, die in der CLI verfügbar sind. Informationen zur Verwendung finden Sie unter Befehlsreferenz für Secure Firewall Threat Defense.

Schritt 3 Um die Threat Defense-CLI zu verlassen, geben Sie den Befehl **exit** oder **logout** ein.

Mit diesem Befehl kehren Sie zur FXOS-CLI-CLI-Eingabeaufforderung zurück. Geben Sie **?** ein, um Informationen zu den Befehlen aufzurufen, die in der FXOS-CLI-CLI verfügbar sind.

Beispiel:

```
> exit
firepower#
```

Ausschalten der Firewall

Es ist wichtig, dass Sie Ihr System ordnungsgemäß herunterfahren. Wenn Sie einfach den Netzstecker ziehen, kann das Dateisystem ernsthaft beschädigt werden. Denken Sie daran, dass im Hintergrund ständig viele Prozesse ablaufen, und dass das Ziehen des Netzsteckers oder das Ausschalten der Stromversorgung kein ordnungsgemäßes Herunterfahren Ihres Firewall-Systems ermöglicht.

Das Firepower 1010-Chassis hat keinen externen Netzschalter.Sie können das Gerät über die Management Center-Seite für das Gerätemanagement oder über die FXOS-CLI ausschalten.

Ausschalten der Firewall über die Management Center

Es ist wichtig, dass Sie Ihr System ordnungsgemäß herunterfahren. Wenn Sie einfach den Netzstecker ziehen oder den Netzschalter drücken, kann das Dateisystem ernsthaft beschädigt werden. Denken Sie daran, dass im Hintergrund ständig viele Prozesse ablaufen, und dass das Ziehen des Netzsteckers oder das Ausschalten der Stromversorgung kein ordnungsgemäßes Herunterfahren Ihrer Firewall ermöglicht.

Sie können Ihr System mithilfe von Management Center ordnungsgemäß herunterfahren.

Prozedur

Schritt 1 Wählen Sie **Devices** > **Device Management** (Geräte > Gerätemanagement) aus.

Schritt 2 Klicken Sie neben dem Gerät, das Sie neu starten möchten, auf das Bearbeitungssymbol ( ).

Schritt 3 Klicken Sie auf die Registerkarte **Device** (Gerät).

Schritt 4 Klicken Sie im Abschnitt **System** auf das Symbol zum Herunterfahren des Geräts ( ).

Schritt 5 Bestätigen Sie bei Aufforderung, dass Sie das Gerät herunterfahren möchten.

Schritt 6 Wenn Sie über eine Konsolenverbindung zur Firewall verfügen, prüfen Sie die Systemaufforderungen, wenn die Firewall heruntergefahren wird. Die folgende Aufforderung wird angezeigt:

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

Wenn Sie keine Konsolenverbindung haben, warten Sie circa 3 Minuten, um sicherzustellen, dass das System heruntergefahren wurde.

Schritt 7 Sie können jetzt den Netzstecker ziehen, um die Stromversorgung des Chassis bei Bedarf physisch zu trennen.

Ausschalten des Geräts über die CLI

Sie können die FXOS-CLI verwenden, um das System sicher herunterzufahren und das Gerät auszuschalten. Für den Zugriff auf die CLI (Befehlszeilenschnittstelle bzw. Kommandozeile) müssen Sie eine Verbindung zum Konsolenport herstellen; siehe Zugriff auf die Threat Defense- und FXOS-CLI, auf Seite 44.

Prozedur

Schritt 1 Stellen Sie in der FXOS-CLI eine Verbindung zu local-mgmt her:

firepower # **connect local-mgmt**

Schritt 2 Geben Sie den Befehl **shutdown** aus:

firepower(local-mgmt) # **shutdown**

Beispiel:

```
firepower(local-mgmt)# shutdown
This command will shutdown the system.  Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense......ok
```

Schritt 3 Überwachen Sie die System-Eingabeaufforderungen, während die Firewall heruntergefahren wird. Die folgende Aufforderung wird angezeigt:

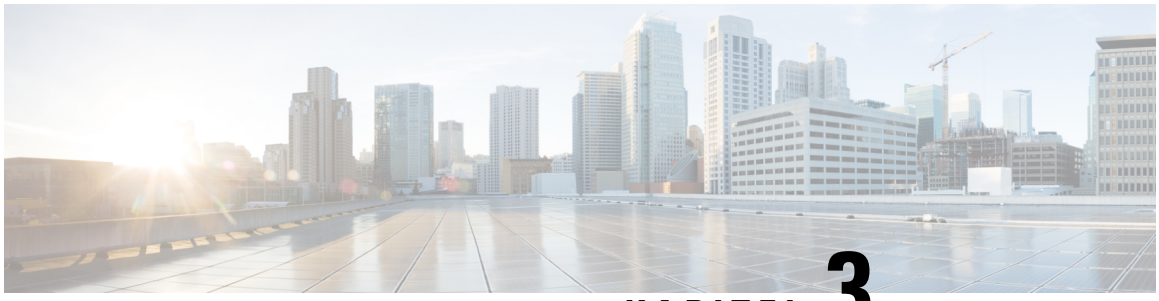
```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

Schritt 4 Sie können jetzt den Netzstecker ziehen, um die Stromversorgung des Chassis bei Bedarf physisch zu trennen.

Nächste Schritte

Um die Konfiguration von Threat Defense fortzusetzen, lesen Sie die Dokumente, die für Ihre Softwareversion verfügbar sind. Siehe Navigation in der Cisco Firepower-Dokumentation.

Informationen zur Verwendung des Management Center finden Sie im Konfigurationsleitfaden für Firepower Management Center.



KAPITEL 3

Threat Defense-Bereitstellung mit einem Remote-Management Center

Enthält dieses Kapitel die Informationen, nach denen Sie suchen?

Um alle verfügbaren Betriebssysteme und Manager anzuzeigen, sehen Sie sich Welche Betriebssysteme und Manager sind für Sie geeignet?, auf Seite 1 an. In diesem Kapitel erfahren Sie, wie Sie Threat Defense in einer Remote-Zweigstelle mit einem Management Center in einer zentralen Hauptgeschäftsstelle bereitstellen.

Jedes Threat Defense steuert, untersucht, überwacht und analysiert den Traffic und meldet die Ergebnisse dann einem verwaltenden Management Center. Management Center bietet eine Konsole für zentrales Management mit einer Weboberfläche, über die Sie Administrations-, Management-, Analyse- und Berichtsaufgaben zum Schutz Ihres lokalen Netzwerks durchführen können.

- Ein Administrator in der zentralen Hauptgeschäftsstelle konfiguriert vorab das Threat Defense in der CLI oder mit Device Manager und sendet das Threat Defense dann an die Remote-Zweigstelle.
- Der Zweigstellenadministrator verkabelt das Threat Defense und schaltet es ein.
- Der Administrator in der Zentrale schließt die Konfiguration des Threat Defense mit dem Management Center ab.

Hinweis Remote-Zweigstellenbereitstellung erfordert Version 6.7 oder höher.

Informationen zur Firewall

Auf der Hardware kann entweder Threat Defense-Software oder ASA-Software ausgeführt werden. Beim Wechsel zwischen Threat Defense und ASA müssen Sie ein neues Image des Geräts erstellen. Sie sollten auch ein neues Image erstellen, wenn Sie eine andere Softwareversion als derzeit installiert benötigen. Weitere Informationen hierzu finden Sie unter Reimage the Cisco ASA or Firepower Threat Defense Device (Erstellen eines neuen Images für Cisco ASA oder Firepower Threat Defense-Gerät).

Die Firewall führt ein zugrunde liegendes Betriebssystem namens Secure Firewall Extensible Operating System (FXOS) aus. Die Firewall unterstützt die FXOS-Secure Firewall Chassis Manager nicht. Es wird nur in begrenztem Umfang eine CLI für Fehlerbehebungszwecke unterstützt. Weitere Informationen finden Sie unter Cisco FXOS-Leitfaden zur Fehlerbehebung für die Firepower 1000/2100-Serie mit Firepower Threat Defense.

Datenschutzerklärung zur Datenerfassung: Die Firewall erfordert keine personenbezogenen Informationen und nimmt keine aktive Erfassung derartiger Informationen vor. Sie können jedoch personenbezogene Informationen in der Konfiguration verwenden, z. B. bei Benutzernamen. In diesem Fall kann ein Administrator diese Informationen möglicherweise sehen, wenn er mit der Konfiguration arbeitet oder SNMP verwendet.

Funktionsweise des Remote-Managements

Damit das Management Center das Threat Defense-System über das Internet verwalten kann, verwenden Sie die externe Schnittstelle für das Management Center-Management anstelle der Management-Schnittstelle. Da die meisten Remote-Zweigstellen nur eine einzige Internetverbindung haben, ermöglicht der externe Management Center-Zugriff ein zentrales Management.

Hinweis Sie können *jede beliebige* Datenschnittstelle für den FMC-Zugriff verwenden, z. B. die interne Schnittstelle, wenn Sie über ein internes Management Center verfügen. In diesem Handbuch wird jedoch hauptsächlich der externe Schnittstellenzugriff behandelt, da dies das wahrscheinlichste Szenario für Remote-Zweigstellen ist.

Die Management-Schnittstelle ist eine spezielle Schnittstelle, die separat von Threat Defense-Datenschnittstellen konfiguriert wird und über eigene Netzwerkeinstellungen verfügt. Die Netzwerkeinstellungen der Management-Schnittstelle werden weiterhin verwendet, auch wenn Sie den Managerzugriff auf einer Datenschnittstelle aktivieren. Der gesamte Management-Traffic geht weiterhin von der Management-Schnittstelle aus oder ist an diese gerichtet. Wenn Sie den Managerzugriff auf einer Datenschnittstelle aktivieren, leitet Threat Defense eingehenden Management-Traffic über die Backplane an die Management-Schnittstelle weiter. Für den ausgehenden Management-Traffic leitet die Management-Schnittstelle den Traffic über die Backplane an die Datenschnittstelle weiter.

Der Managerzugriff über eine Datenschnittstelle hat folgende Einschränkungen:

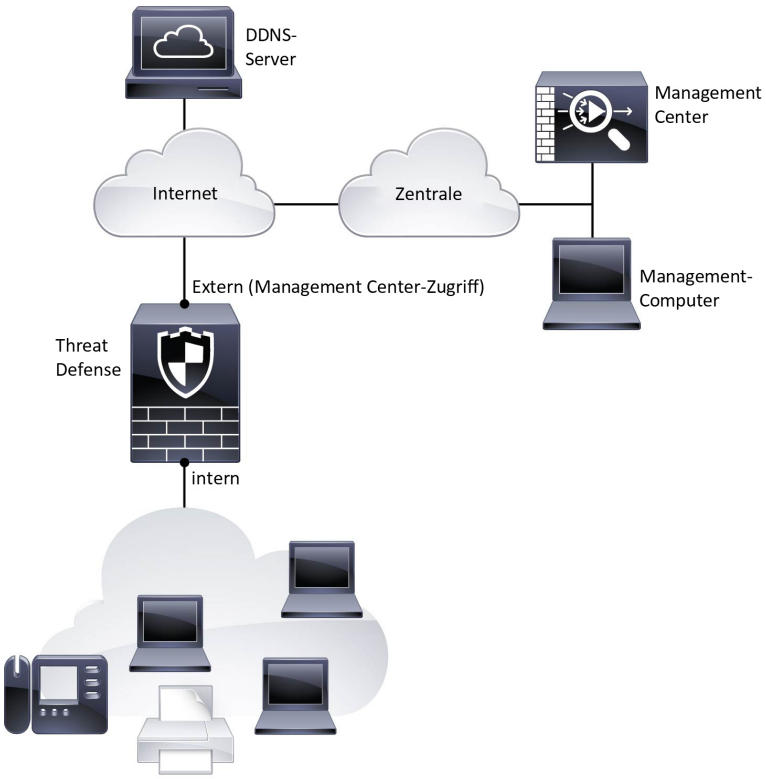
- Sie können den Managerzugriff nur auf einer physischen Datenschnittstelle aktivieren. Sie können keine Unterschnittstellen oder EtherChannels verwenden.
- Diese Schnittstelle kann nicht als reine Management-Schnittstellen verwendet werden.
- Nur Routing-Firewall-Modus mit einer gerouteten Schnittstelle.
- PPPoE wird nicht unterstützt. Wenn Ihr ISP PPPoE benötigt, müssen Sie einen Router mit PPPoE-Unterstützung zwischen Threat Defense und dem WAN-Modem platzieren.
- Die Schnittstelle darf sich nur im globalen VRF befinden.
- SSH ist für Datenschnittstellen nicht standardmäßig aktiviert, daher müssen Sie SSH später mithilfe von Management Center aktivieren. Da das Gateway der Management-Schnittstelle zu den Datenschnittstellen wird, können Sie auch nicht per SSH von einem Remote-Netzwerk auf die Management-Schnittstelle zugreifen, es sei denn, Sie fügen mit dem Befehl **configure network static-routes** eine statische Route für die Management-Schnittstelle hinzu.

- Hochverfügbarkeit wird nicht unterstützt. In diesem Fall müssen Sie die Management-Schnittstelle verwenden.

Die folgende Abbildung zeigt das Management Center in der zentralen Hauptgeschäftsstelle und Threat Defense mit Managerzugriff auf der externen Schnittstelle.

Entweder das Threat Defense-System oder Management Center benötigen eine öffentliche IP-Adresse oder einen Host-Namen, um die eingehende Managementverbindung zu ermöglichen. Sie müssen diese IP-Adresse für die Ersteinrichtung kennen. Sie können optional auch Dynamic DNS (DDNS) für die externe Schnittstelle konfigurieren, um sich ändernde DHCP-IP-Zuweisungen zu berücksichtigen.

Abbildung 13:



Vorbereitung

Stellen Sie Management Center bereit, und führen Sie die Erstkonfiguration durch. Siehe Hardwareinstallationshandbuch für Cisco Firepower Management Center 1600, 2600 und 4600 oder Leitfaden zu den ersten Schritten mit Cisco Secure Firewall Management Center Virtual.

Vollständiges Verfahren

Mit den folgenden Aufgaben können Sie Threat Defense mit Management Center auf Ihrem Chassis.

Abbildung 14: Vollständiges Verfahren

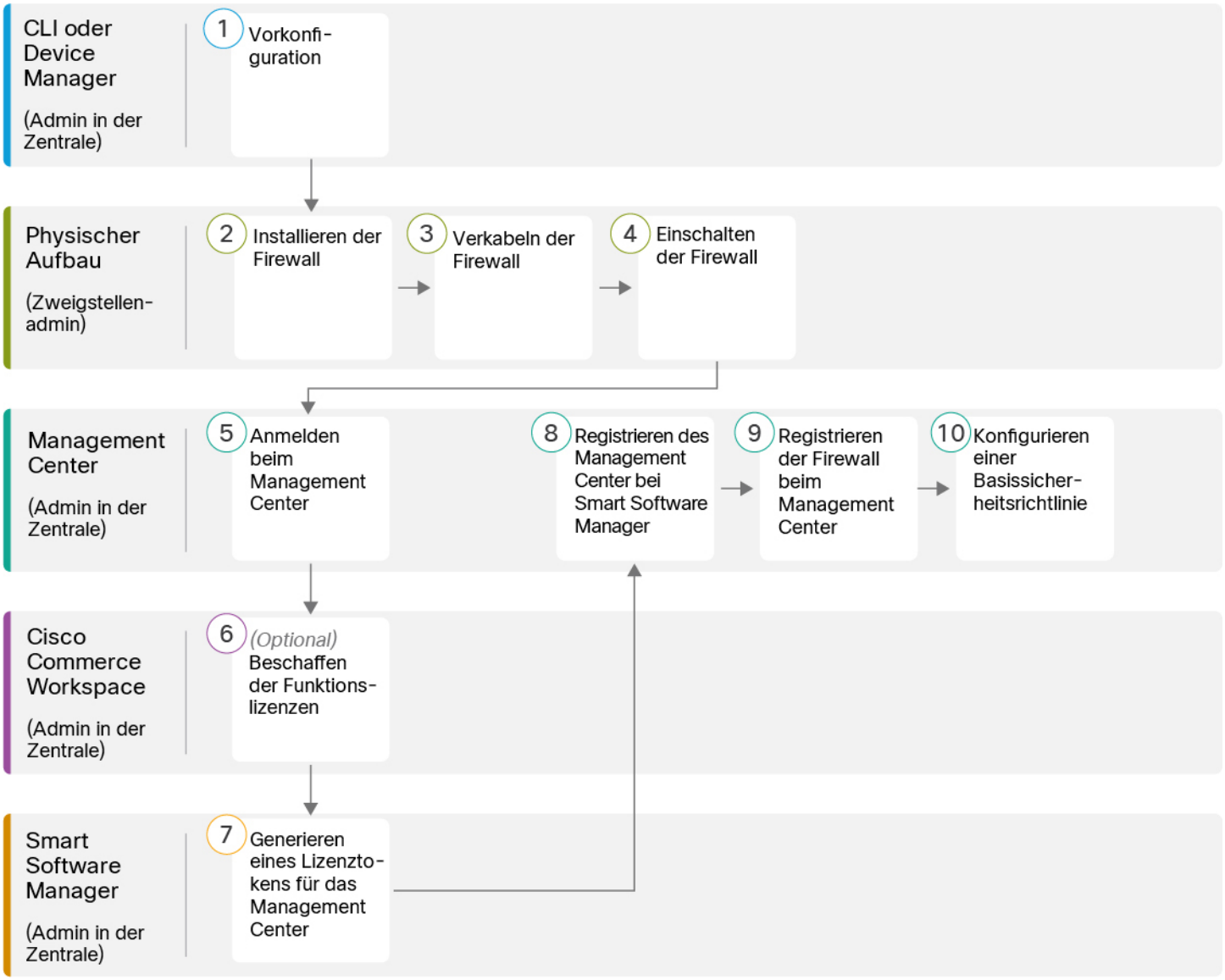


Abbildung 15: Vollständiges Verfahren

1	CLI oder Device Manager (Admin in der Zentrale)	• (Optional) Prüfen der Software und Installieren einer neuen Version, auf Seite 53 • Vorkonfiguration mit der CLI, auf Seite 61 • Vorkonfiguration mit der Device Manager, auf Seite 55
2	Physischer Aufbau (Zweigstellenadmin)	Installieren der Firewall. Weitere Informationen finden Sie im Hardware-Installationshandbuch.

3	Physischer Aufbau (Zweigstellenadmin)	Verkabeln der Firewall, auf Seite 67
4	Physischer Aufbau (Zweigstellenadmin)	Einschalten des Geräts, auf Seite 68
5	Management Center (Admin in der Zentrale)	Administrator in der Zentrale: Anmelden bei Management Center, auf Seite 24
6	Cisco Commerce Workspace (Admin in der Zentrale)	Abrufen von Lizenzen für Management Center, auf Seite 69: Erwerben Sie Funktionslizenzen.
7	Smart Software Manager (Admin in der Zentrale)	Abrufen von Lizenzen für Management Center, auf Seite 69: Generieren Sie ein Lizenztoken für das Management Center.
8	Management Center (Admin in der Zentrale)	Abrufen von Lizenzen für Management Center, auf Seite 69: Registrieren Sie das Management Center beim Smart Licensing-Server.
9	Management Center (Admin in der Zentrale)	Registrieren von Threat Defense beim Management Center , auf Seite 70
10	Management Center (Admin in der Zentrale)	Konfigurieren einer Basissicherheitsrichtlinie, auf Seite 73

Vorkonfiguration des Administrators in der Zentrale

Sie müssen Threat Defense manuell vorkonfigurieren, bevor Sie es an die Zweigstelle senden.

(Optional) Prüfen der Software und Installieren einer neuen Version

Gehen Sie wie folgt vor, um die Softwareversion zu überprüfen und ggf. eine andere Version zu installieren. Wir empfehlen, dass Sie Ihre Zielversion installieren, bevor Sie die Firewall konfigurieren. Alternativ können Sie ein Upgrade im Anschluss an die Inbetriebnahme durchführen. Ein Upgrade, bei dem Ihre Konfiguration erhalten bleibt, kann jedoch länger dauern als dieses Verfahren.

Welche Version sollte ich ausführen?

Cisco empfiehlt, eine Gold Star-Version auszuführen, die durch einen goldenen Stern neben der Versionsnummer auf der Software-Download-Seite gekennzeichnet ist. Sie können sich auch auf die

Release-Strategie beziehen, die in https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html beschrieben ist. Beispielsweise beschreibt dieses Bulletin die Nummerierung von kurzfristigen Releases (mit den neuesten Funktionen), die Nummerierung von langfristigen Releases (Wartungsversionen und Patches für einen längeren Zeitraum) oder die Nummerierung von extra langfristigen Releases (Wartungsversionen und Patches für den längsten Zeitraum für die staatliche Zertifizierung).

Prozedur

Schritt 1 Stellen Sie eine Verbindung zur CLI her. Weitere Informationen finden Sie unter Zugriff auf die Threat Defense- und FXOS-CLI, auf Seite 84. Dieses Verfahren zeigt die Verwendung des Konsolenports, aber Sie können stattdessen SSH verwenden.

Melden Sie sich mit dem Benutzer **admin** und dem Standardkennwort **Admin123** an.

Sie stellen eine Verbindung zum FXOS-CLI her. Wenn Sie sich zum ersten Mal anmelden, werden Sie aufgefordert, das Kennwort zu ändern. Dieses Kennwort wird auch zur Threat Defense-Anmeldung für SSH verwendet.

Hinweis Wenn das Kennwort bereits geändert wurde und Sie es nicht kennen, müssen Sie das Gerät auf die Werkseinstellungen zurücksetzen, um das Kennwort auf den Standardwert zurückzusetzen. Weitere Informationen hierzu finden Sie im Abschnitt über das Verfahren zum Zurücksetzen auf die Werkseinstellungen im Handbuch zur FXOS-Fehlerbehebung.

Beispiel:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

Schritt 2 Zeigen Sie in der FXOS-CLI die aktuelle Version an.

scope ssa

show app-instance

Beispiel:

```
Firepower# scope ssa
Firepower /ssa # show app-instance

Application Name     Slot ID    Admin State     Operational State    Running Version Startup
 Version Cluster Oper State
-------------------- ---------- --------------- -------------------- ---------------
--------------- ------------------
ftd                  1          Enabled         Online               7.2.0.65        7.2.0.65
```

```
Not Applicable
```

Schritt 3 Wenn Sie eine neue Version installieren möchten, führen Sie diese Schritte aus.

a) Informationen zum Festlegen einer statischen IP-Adresse für die Management-Schnittstelle finden Sie unter Vorkonfiguration mit der CLI, auf Seite 61. Standardmäßig verwendet die Managementschnittstelle DHCP.

Sie müssen das neue Image von einem Server herunterladen, auf den über die Managementschnittstelle zugegriffen werden kann.

b) Führen Sie das Verfahren zum Erstellen eines neuen Images im Handbuch zur FXOS-Fehlerbehebung durch.

Vorkonfiguration mit der Device Manager

Stellen Sie eine Verbindung zur Device Manager her, um die Ersteinrichtung des Threat Defense-Systems durchzuführen. Wenn Sie die Ersteinrichtung mit Device Manager durchführen, werden *alle* in Device Manager abgeschlossenen Schnittstellenkonfigurationen beibehalten, wenn Sie für das Management zu Management Center wechseln, zusätzlich zu den Einstellungen für die Management-Schnittstelle und den Managerzugriff. Beachten Sie, dass andere Standardkonfigurationseinstellungen, wie z. B. die Zugriffskontrollrichtlinie oder Sicherheitszonen, nicht beibehalten werden. Wenn Sie die CLI verwenden, werden nur die Management-Schnittstellen- und Managerzugriffseinstellungen beibehalten (z. B. wird die standardmäßige interne Schnittstellenkonfiguration nicht beibehalten).

Vorbereitungen

- Stellen Sie Management Center bereit, und führen Sie die Erstkonfiguration durch. Siehe Hardwareinstallationshandbuch für Cisco Firepower Management Center 1600, 2600 und 4600. Sie müssen die IP-Adresse oder den Host-Namen des Management Center kennen, bevor Sie Threat Defense einrichten.
- Verwenden Sie eine aktuelle Version von Firefox, Chrome, Safari, Edge oder Internet Explorer.

Prozedur

Schritt 1 Verbinden Sie Ihren Management-Computer über die interne Schnittstelle (Ethernet 1/2 bis 1/8).

Schritt 2 Schalten Sie die Firewall ein.

Hinweis Wenn Sie den Threat Defense zum ersten Mal starten, kann die Initialisierung etwa 15 bis 30 Minuten dauern.

Schritt 3 Melden Sie sich bei Device Manager an.

a) Geben Sie die folgende URL in Ihren Browser ein: **https://192.168.95.1**
b) Melden Sie sich mit dem Benutzernamen **admin** und dem Standardkennwort **Admin123** an.
c) Sie werden aufgefordert, den Endbenutzerlizenzvertrag zu lesen und zu akzeptieren und das Administratorkennwort zu ändern.

Schritt 4 Verwenden Sie bei der ersten Anmeldung in Device Manager den Einrichtungsassistenten, um die Erstkonfiguration abzuschließen. Sie können den Einrichtungsassistenten optional überspringen, indem Sie unten auf der Seite auf **Skip device setup** (Gerätekonfiguration überspringen) klicken.

Nachdem Sie den Einrichtungsassistenten abgeschlossen haben, haben Sie zusätzlich zur Standardkonfiguration für die interne Schnittstelle (Ethernet 1/2 bis 1/8, die Switch-Ports auf VLAN1 sind) eine Konfiguration für eine externe Schnittstelle (Ethernet 1/1), die beibehalten wird, wenn Sie zum Management Center-Management wechseln.

a) Konfigurieren Sie die folgenden Optionen für die externe Schnittstelle und die Management-Schnittstellen, und klicken Sie auf **Next** (Weiter).

1. **Outside Interface Address** (Externe Schnittstellenadresse): Diese Schnittstelle ist in der Regel das Internet-Gateway und kann als Managerzugriffsschnittstelle verwendet werden. Sie können während der Ersteinrichtung des Geräts keine alternative externe Schnittstelle auswählen. Die erste Datenschnittstelle ist die standardmäßige externe Schnittstelle.

   Wenn Sie eine andere externe (oder interne) Schnittstelle für den Managerzugriff verwenden möchten, müssen Sie sie nach Abschluss des Einrichtungsassistenten manuell konfigurieren.

   Configure IPv4 (IPv4 konfigurieren): Die IPv4-Adresse für die externe Schnittstelle. Sie können DHCP verwenden oder eine statische IP-Adresse, eine Subnetzmaske und ein Gateway manuell eingeben. Sie können auch **Off** (Aus) auswählen, wenn keine IPv4-Adresse konfiguriert werden soll. Sie können PPPoE nicht mit dem Einrichtungsassistenten konfigurieren. PPPoE kann erforderlich sein, wenn die Schnittstelle mit einem DSL-Modem, Kabelmodem oder einem anderen ISP-Anschluss verbunden ist und Ihr ISP PPPoE verwendet, um Ihre IP-Adresse bereitzustellen. Sie können PPPoE konfigurieren, nachdem Sie den Assistenten abgeschlossen haben.

   Configure IPv6 (IPv6 konfigurieren): Die IPv6-Adresse für die externe Schnittstelle. Sie können DHCP verwenden oder eine statische IP-Adresse, ein Präfix und ein Gateway manuell eingeben. Sie können auch **Off** (Aus) auswählen, wenn keine IPv6-Adresse konfiguriert werden soll.

2. **Management-Schnittstelle**

   Die Einstellungen der Management-Schnittstelle werden nicht angezeigt, wenn Sie die Ersteinrichtung über die CLI durchgeführt haben.

   Es werden die Einstellungen der Management-Schnittstelle verwendet, auch wenn Sie den Managerzugriff auf einer Datenschnittstelle aktivieren. Beispiel: Der Management-Traffic, der über die Backplane durch die Datenschnittstelle geleitet wird, löst FQDNs über die DNS-Server der Management-Schnittstelle und nicht über die DNS-Server der Datenschnittstelle auf.

   DNS Servers (DNS-Server): Der DNS-Server für die Managementadresse des Systems. Geben Sie eine oder mehrere Adressen von DNS-Servern für die Namensauflösung ein. Der Standardwert sind die öffentlichen DNS-Server von OpenDNS. Wenn Sie die Felder bearbeiten und zum Standardwert zurückkehren möchten, klicken Sie auf **OpenDNS** verwenden, um die entsprechenden IP-Adressen erneut in die Felder zu laden.

   Firewall Hostname (Firewall-Host-Name): Der Host-Name für die Managementadresse des Systems.

b) Konfigurieren Sie die **Zeiteinstellung (NTP)**, und klicken Sie auf **Next** (Weiter).

1. **Time Zone** (Zeitzone): Wählen Sie die Zeitzone für das System aus.
2. **NTP Time Server** (NTP-Zeitserver): Wählen Sie aus, ob Sie die Standard-NTP-Server verwenden oder die Adressen Ihrer NTP-Server manuell eingeben möchten. Sie können mehrere Server hinzufügen, um Backups bereitzustellen.

c) Wählen Sie **Start 90 day evaluation period without registration** (90-tägigen Evaluierungszeitraum ohne Registrierung starten) aus.

Registrieren Sie das Threat Defense-System nicht beim Smart Software Manager. Die gesamte Lizenzierung erfolgt im Management Center.

d) Klicken Sie auf **Finish** (Fertigstellen).

e) Sie werden aufgefordert, **Cloud Management** (Cloud-Management) oder **Standalone** (Eigenständig) zu wählen. Wählen Sie für das Management Center-Management die Option **Standalone** (Eigenständig) und dann **Got It** (Verstanden).

Schritt 5 (Möglicherweise erforderlich) Konfigurieren Sie die Managementschnittstelle. Weitere Informationen finden Sie in der Management-Schnittstelle unter **Device** > **Interfaces** (Gerät > Schnittstellen).

Für die Management-Schnittstelle muss das Gateway auf Datenschnittstellen eingestellt sein. Standardmäßig erhält die Management-Schnittstelle eine IP-Adresse und ein Gateway von DHCP. Wenn Sie kein Gateway von DHCP erhalten (z. B. haben Sie diese Schnittstelle nicht mit einem Netzwerk verbunden), verwendet das Gateway standardmäßig Datenschnittstellen, und Sie müssen nichts konfigurieren. Wenn Sie ein Gateway von DHCP erhalten haben, müssen Sie diese Schnittstelle stattdessen mit einer statischen IP-Adresse konfigurieren und das Gateway auf Datenschnittstellen einstellen.

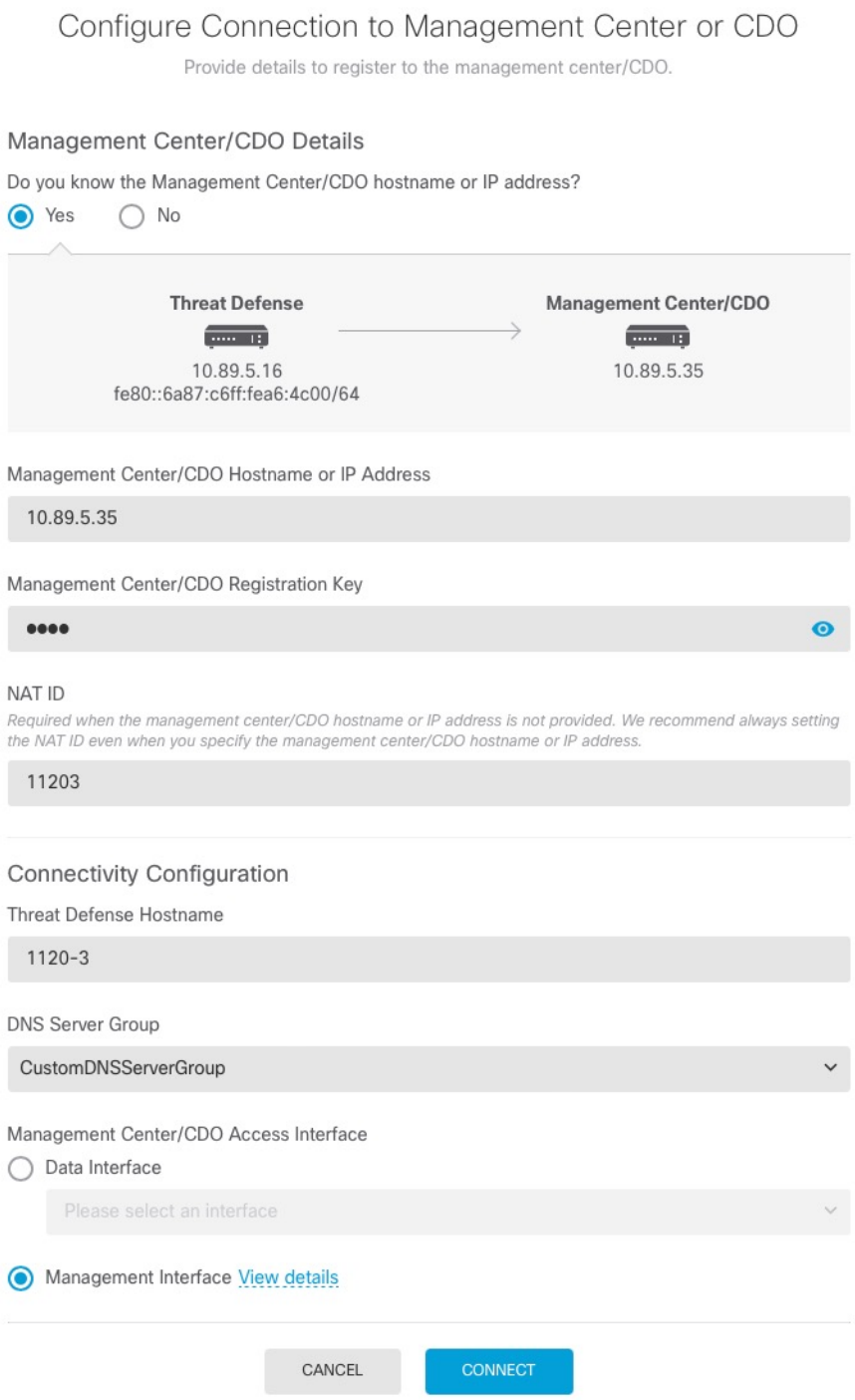
Schritt 6 Wenn Sie zusätzliche Schnittstellen konfigurieren möchten, einschließlich einer anderen als der externen oder internen Schnittstelle, die Sie für den Managerzugriff verwenden möchten, wählen Sie **Device** (Gerät), und klicken Sie dann auf den Link in der Schnittstellenübersicht (**Interfaces**).

Unter Konfigurieren der Firewall in Device Manager, auf Seite 115 finden Sie weitere Informationen zum Konfigurieren von Schnittstellen in Device Manager. Andere Device Manager-Konfigurationen werden nicht beibehalten, wenn Sie das Gerät bei Management Center registrieren.

Schritt 7 Wählen Sie **Device** > **System Settings** > **Central Management**, und klicken Sie auf **Proceed** (Fortfahren), um das Management Center-Management einzurichten.

Schritt 8 Konfigurieren Sie die **Management Center-/CDO-Details**.

Abbildung 16: Management Center-/CDO-Details



a) Klicken Sie unter **Do you know the Management Center/CDO hostname or IP address** auf **Yes** (Ja), wenn Sie das Management Center mit einer IP-Adresse oder einem Hostname erreichen können, oder auf **No** (Nein), wenn sich das Management Center hinter NAT befindet oder keine öffentliche IP-Adresse oder keinen Hostnamen hat.

Mindestens eines der Geräte, entweder das Management Center oder das Threat Defense-Gerät muss eine erreichbare IP-Adresse haben, um den bidirektionalen, SSL-verschlüsselten Kommunikationskanal zwischen den beiden Geräten einzurichten.

b) Wenn Sie **Yes** (Ja) ausgewählt haben, geben Sie **Management Center/CDO-Hostname/IP-Adresse** ein.

c) Geben Sie den **Management Center/CDO-Registrierungsschlüssel** an.

Dieser Schlüssel gibt einen einmaligen Registrierungsschlüssel Ihrer Wahl an, den Sie auch bei der Registrierung des Threat Defense-Geräts im Management Center angeben. Der Registrierungsschlüssel darf höchstens 37 Zeichen enthalten. Zu den zulässigen Zeichen zählen alphanumerische Zeichen (A–Z, a–z, 0–9) und der Bindestrich (-). Diese ID kann für mehrere Geräte verwendet werden, die sich beim Management Center registrieren.

d) Geben Sie eine **NAT-ID** an.

Diese ID ist eine eindeutige, einmalige Zeichenfolge Ihrer Wahl, die Sie auch im Management Center angeben. Dieses Feld ist erforderlich, wenn Sie die IP-Adresse nur auf einem der Geräte angeben. Wir empfehlen jedoch, die NAT-ID anzugeben, auch wenn Sie die IP-Adressen beider Geräte kennen. Die NAT-ID darf nicht länger als 37 Zeichen sein. Zu den zulässigen Zeichen zählen alphanumerische Zeichen (A–Z, a–z, 0–9) und der Bindestrich (-). Diese ID *kann nicht* für andere Geräte verwendet werden, die sich beim Management Center registrieren. Die NAT-ID wird in Kombination mit der IP-Adresse verwendet, um zu überprüfen, ob die Verbindung vom richtigen Gerät kommt. Erst nach der Authentifizierung der IP-Adresse/NAT-ID wird der Registrierungsschlüssel überprüft.

Schritt 9 Konfigurieren Sie die **Verbindungskonfiguration**.

a) Geben Sie den **FTD-Hostnamen** an.

Dieser FQDN wird für die externe Schnittstelle oder die Schnittstelle verwendet, die Sie für die **Management Center-/CDO-Zugriffsschnittstelle** auswählen.

b) Geben Sie die **DNS-Servergruppe** an.

Wählen Sie eine vorhandene Gruppe aus oder erstellen Sie eine neue. Die Standard-DNS-Gruppe heißt **CiscoUmbrellaDNSServerGroup** und umfasst die OpenDNS-Server.

Diese Einstellung legt den DNS-Server der *Datenschnittstelle* fest. Der Management-DNS-Server, den Sie mit dem Einrichtungsassistenten festlegen, wird für den Management-Traffic verwendet. Der Daten-DNS-Server wird für DDNS (sofern konfiguriert) oder für auf diese Schnittstelle angewendete Sicherheitsrichtlinien verwendet. Sie werden wahrscheinlich die gleiche DNS-Servergruppe auswählen, die Sie für das Management verwendet haben, da sowohl der Management- als auch der Daten-Traffic den DNS-Server über die externe Schnittstelle erreichen.

Im Management Center werden die DNS-Server der Datenschnittstelle in der Richtlinie für Plattformeinstellungen konfiguriert, die Sie diesem Threat Defense-System zuweisen. Wenn Sie Threat Defense zum Management Center hinzufügen, werden die lokalen Einstellungen beibehalten, und die DNS-Server werden *keiner* Richtlinie für Plattformeinstellungen hinzugefügt. Wenn Sie jedoch später dem Threat Defense-System eine Richtlinie für Plattformeinstellungen zuweisen, die eine DNS-Konfiguration enthält, überschreibt diese Konfiguration die lokale Einstellung. Wir empfehlen Ihnen, die DNS-Plattformeinstellungen aktiv mit dieser Einstellung zu konfigurieren, um Management Center und Threat Defense zu synchronisieren.

Außerdem werden lokale DNS-Server von Management Center nur beibehalten, wenn die DNS-Server bei der ersten Registrierung erkannt wurden.

c) Wählen Sie für die **Management Center-/CDO-Zugriffsschnittstelle outside** (extern) aus.

Sie können jede konfigurierte Schnittstelle auswählen, aber in diesem Handbuch wird davon ausgegangen, dass Sie sie „outside“ verwenden.

Schritt 10 Wenn Sie eine andere externe Datenschnittstelle ausgewählt haben, fügen Sie eine Standardroute hinzu.

Sie werden in einer Meldung aufgefordert, zu überprüfen, ob Sie eine Standardroute über die Schnittstelle haben. Wenn Sie „outside“ ausgewählt haben, haben Sie diese Route bereits als Teil des Einrichtungsassistenten konfiguriert. Wenn Sie eine andere Schnittstelle ausgewählt haben, müssen Sie eine Standardroute manuell konfigurieren, bevor Sie eine Verbindung zum Management Centerherstellen. Unter Konfigurieren der Firewall in Device Manager, auf Seite 115 finden Sie weitere Informationen zum Konfigurieren statischer Routen im Device Manager.

Schritt 11 Klicken Sie auf **Add a Dynamic DNS (DDNS) method** (Dynamische DNS- (DDNS-)Methode hinzufügen).

DDNS stellt sicher, dass Management Center den Threat Defense unter seinem vollqualifizierten Domain-Namen (FQDN) erreichen kann, wenn sich die IP-Adresse des Threat Defense ändert. Siehe **Device** > **System Settings** > **DDNS Service** (Gerät > Systemeinstellungen > DDNS-Service), um DDNS zu konfigurieren.

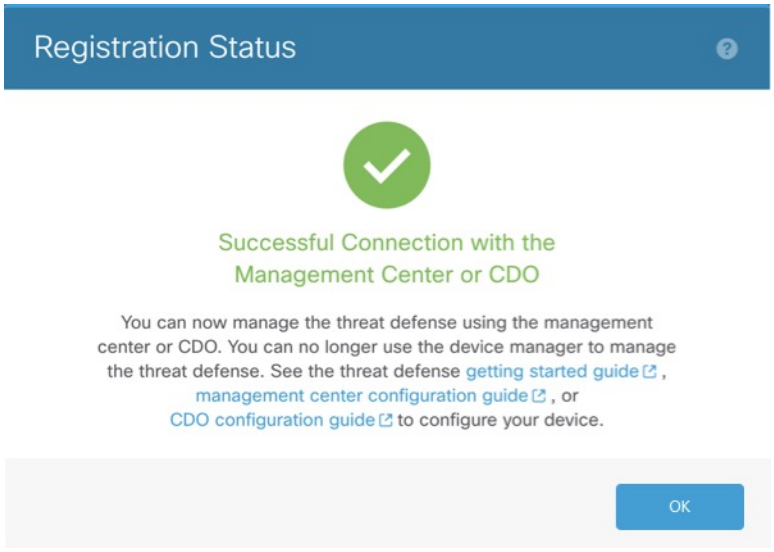
Wenn Sie DDNS konfigurieren, bevor Sie Threat Defense zu Management Center hinzufügen, fügt Threat Defenseautomatisch Zertifikate für alle wichtigen Zertifizierungsstellen aus dem Cisco Trusted Root CA-Paket hinzu, damit das DDNS-Serverzertifikat für Threat Defense die HTTPS-Verbindung validieren kann. Threat Defense unterstützt jeden DDNS-Server, der die DynDNS Remote API-Spezifikation (https://help.dyn.com/remote-access-api/) verwendet.

Schritt 12 Klicken Sie auf **Connect** (Verbinden). Im Dialogfeld **Registrierungsstatus** wird der aktuelle Status des Wechsels zu Management Center angezeigt. Wechseln Sie nach dem Schritt **Speichern von Management Center/CDO-Registrierungseinstellungen** zu Management Center, und fügen Sie die Firewall hinzu.

Wenn Sie den Wechsel zu Management Center abbrechen möchten, klicken Sie auf **Cancel Registration** (Registrierung abbrechen). Andernfalls schließen Sie das Device Manager-Browserfenster erst nach dem Schritt **Speichern von Management Center/CDO-Registrierungseinstellungen**. Wenn Sie dies tun, wird der Prozess angehalten und erst fortgesetzt, wenn Sie erneut eine Verbindung zum Device Manager herstellen.

Wenn Sie nach dem Schritt **Speichern von Management Center/CDO-Registrierungseinstellungen** weiterhin mit dem Device Manager verbunden sind, wird schließlich das Dialogfeld **Erfolgreiche Verbindung mit Management Center oder CDO** angezeigt. Dannach wird die Verbindung zum Device Managergetrennt.

Abbildung 17: Verbindungsversuch erfolgreich



Vorkonfiguration mit der CLI

Stellen Sie eine Verbindung zur Threat Defense-CLI her, um die Ersteinrichtung durchzuführen. Wenn Sie die CLI für die Erstkonfiguration verwenden, werden nur die Management-Schnittstellen- und Managerzugriffseinstellungen beibehalten.Wenn Sie die Ersteinrichtung mit Device Manager (7.1 und höher) durchführen, werden *alle* Schnittstellenkonfigurationen in Device Manager beibehalten, wenn Sie für das Management zu Management Center wechseln, zusätzlich zu den Einstellungen für die Management-Schnittstelle und den Managerzugriff. Beachten Sie, dass andere Standardkonfigurationseinstellungen, wie z. B. die Zugriffskontrollrichtlinie, nicht beibehalten werden.

Vorbereitungen

Stellen Sie Management Center bereit, und führen Sie die Erstkonfiguration durch. Siehe Hardwareinstallationshandbuch für Cisco Firepower Management Center 1600, 2600 und 4600. Sie müssen die IP-Adresse oder den Host-Namen des Management Center kennen, bevor Sie Threat Defense einrichten.

Prozedur

Schritt 1 Schalten Sie die Firewall ein.

Hinweis Wenn Sie den Threat Defense zum ersten Mal starten, kann die Initialisierung etwa 15 bis 30 Minuten dauern.

Schritt 2 Stellen Sie eine Verbindung zur Threat Defense-CLI auf dem Konsolenport her.

Der Konsolenport wird mit der FXOS-CLI verbunden.

Schritt 3 Melden Sie sich mit dem Benutzernamen **admin** und dem Kennwort **Admin123** an.

Wenn Sie sich zum ersten Mal bei FXOS anmelden, werden Sie aufgefordert, das Kennwort zu ändern. Dieses Kennwort wird auch zur Threat Defense-Anmeldung für SSH verwendet.

Hinweis Wenn das Kennwort bereits geändert wurde und Sie es nicht kennen, müssen Sie ein neues Image des Geräts erstellen, um das Kennwort auf den Standardwert zurückzusetzen. Weitere Informationen hierzu finden Sie im Abschnitt über das Verfahren zum Erstellen eines neuen Images im Handbuch zur FXOS-Fehlerbehebung .

Beispiel:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

Schritt 4 Stellen Sie eine Verbindung zur Threat Defense-CLI her.

connect ftd

Beispiel:

```
firepower# connect ftd
>
```

Schritt 5 Wenn Sie sich zum ersten Mal bei Threat Defense anmelden, werden Sie aufgefordert, den Endbenutzerlizenzvertrag (EULA) zu akzeptieren und, falls Sie eine SSH-Verbindung verwenden, das Administratorkennwort zu ändern. Anschließend wird das CLI-Einrichtungsskript für die Einstellungen der Management-Schnittstelle angezeigt.

Es werden die Einstellungen der Management-Schnittstelle verwendet, auch wenn Sie den Managerzugriff auf einer Datenschnittstelle aktivieren.

Hinweis Sie können den CLI-Einrichtungsassistenten nur wiederholen, wenn Sie die Konfiguration löschen, zum Beispiel im Rahmen der Neuerstellung eines Images. Alle diese Einstellungen können jedoch später in der CLI mit den Befehlen **configure network** geändert werden. Siehe Befehlsreferenz für Secure Firewall Threat Defense.

Standardwerte oder zuvor eingegebene Werte werden in Klammern angezeigt. Um zuvor eingegebene Werte zu akzeptieren, drücken Sie die **Eingabetaste**.

Beachten Sie die folgenden Orientierungshilfen:

- **Configure IPv4 via DHCP or manually?** (IPv4 über DHCP oder manuell konfigurieren?): Wählen Sie **manual** (manuell) aus. Auch wenn Sie die Management-Schnittstelle nicht verwenden möchten, müssen Sie eine IP-Adresse festlegen, z. B. eine private Adresse. Sie können keine Datenschnittstelle für das Management konfigurieren, wenn die Management-Schnittstelle auf DHCP eingestellt ist, da die

Standardroute, bei der es sich um **data-interfaces** handeln muss (siehe nächster Punkt), mit einer vom DHCP-Server empfangenen Route überschrieben werden könnte.

- **Geben Sie das IPv4-Standardgateway für die Management-Schnittstelle ein** – Setzen Sie das Gateway auf **data-interfaces**. Diese Einstellung leitet den Management-Traffic über die Backplane weiter, sodass er über die Managerzugriffsdatenschnittstelle geleitet werden kann.
- **Wenn sich Ihre Netzwerkinformationen geändert haben, müssen Sie die Verbindung wiederherstellen**. – Wenn Sie mit SSH verbunden sind, wird die Verbindung getrennt. Sie können die Verbindung mit der neuen IP-Adresse und dem Kennwort wiederherstellen, wenn sich Ihr Management-Computer im Managementnetzwerk befindet. Sie können sich noch nicht erneut von einem Remote-Netzwerk aus verbinden, da die Standardroute geändert wurde (über die Datenschnittstellen). Konsolenverbindungen sind nicht betroffen.
- **Manage the device locally?** (Das Gerät lokal verwalten?): Geben Sie **no** (Nein) ein, um Management Center zu verwenden. Die Antwort **yes** (Ja) bedeutet, dass Sie stattdessen Device Manager verwenden werden.
- **Configure firewall mode?** (Firewall-Modus konfigurieren?): Geben Sie **routed** (geroutet) ein. Externer Managerzugriff wird nur im Routing-Firewall-Modus unterstützt.

Beispiel:

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress.  Please stand by.
You must change the password for 'admin' to continue.
Enter new password: ********
Confirm new password: ********
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]:
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: no
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...

Update policy deployment information
    - add device configuration
    - add network discovery
    - add system policy

You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
```

```
management capabilities.

When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required.  In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Firepower Management Center are separated by a
NAT device, you must enter a unique NAT ID, along with the unique registration
key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'

Later, using the web interface on the Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.
>
```

Schritt 6 Konfigurieren Sie die externe Schnittstelle für den Managerzugriff.

configure network management-data-interface

Anschließend werden Sie aufgefordert, grundlegende Netzwerkeinstellungen für die externe Schnittstelle zu konfigurieren. Lesen Sie die folgenden Informationen zur Verwendung dieses Befehls:

- Die Management-Schnittstelle kann DHCP nicht verwenden, wenn Sie eine Datenschnittstelle für das Management verwenden möchten. Wenn Sie die IP-Adresse bei der Ersteinrichtung nicht manuell festgelegt haben, können Sie sie jetzt mit dem Befehl **configure network** {**ipv4** | **ipv6**} **manual** festlegen. Falls Sie das Gateway der Management-Schnittstelle noch nicht auf **data-interfaces** gesetzt haben, wird es jetzt mit diesem Befehl festgelegt.
- Wenn Sie Threat Defense zu Management Center hinzufügen, erkennt und verwaltet Management Center die Schnittstellenkonfiguration, einschließlich der folgenden Einstellungen: Schnittstellenname und IP-Adresse, statische Route zum Gateway, DNS-Server und DDNS-Server. Weitere Informationen zur Konfiguration des DNS-Servers finden Sie unten. In Management Center können Sie später Änderungen an der Konfiguration der Managerzugriffsschnittstelle vornehmen. Nehmen Sie jedoch keinesfalls Änderungen vor, die verhindern können, dass Threat Defense oder Management Center die Managementverbindung wieder herstellt. Für den Fall, dass die Managementverbindung unterbrochen wird, enthält Threat Defense den Befehl **configure policy rollback** zum Wiederherstellen der vorherigen Bereitstellung.
- Wenn Sie eine DDNS-Server-Update-URL konfigurieren, fügt Threat Defense automatisch Zertifikate für alle wichtigen Zertifizierungsstellen aus dem Cisco Trusted Root CA-Paket hinzu, damit Threat Defense das DDNS-Serverzertifikat für die HTTPS-Verbindung validieren kann. Threat Defense unterstützt jeden DDNS-Server, der die DynDNS Remote API-Spezifikation (https://help.dyn.com/remote-access-api/) verwendet.
- Dieser Befehl legt den DNS-Server der *Datenschnittstelle* fest. Der Management-DNS-Server, den Sie mit dem Einrichtungsskript (oder mit dem Befehl **configure network dns servers**) festlegen, wird für den Management-Traffic verwendet. Der Daten-DNS-Server wird für DDNS (sofern konfiguriert) oder für auf diese Schnittstelle angewendete Sicherheitsrichtlinien verwendet.

  Im Management Center werden die DNS-Server der Datenschnittstelle in der Richtlinie für Plattformeinstellungen konfiguriert, die Sie diesem Threat Defense-System zuweisen. Wenn Sie Threat Defense zum Management Center hinzufügen, werden die lokalen Einstellungen beibehalten, und die DNS-Server werden *keiner* Richtlinie für Plattformeinstellungen hinzugefügt. Wenn Sie jedoch später dem Threat Defense-System eine Richtlinie für Plattformeinstellungen zuweisen, die eine DNS-Konfiguration enthält, überschreibt diese Konfiguration die lokale Einstellung. Wir empfehlen

Ihnen, die DNS-Plattformeinstellungen aktiv mit dieser Einstellung zu konfigurieren, um Management Center und Threat Defense zu synchronisieren.

Außerdem werden lokale DNS-Server von Management Center nur beibehalten, wenn die DNS-Server bei der ersten Registrierung erkannt wurden. Wenn Sie beispielsweise das Gerät über die Management-Schnittstelle registriert haben, aber später eine Datenschnittstelle mit dem Befehl **configure network management-data-interface** konfigurieren, müssen Sie alle diese Einstellungen in Management Center, einschließlich der DNS-Server, manuell so konfigurieren, dass sie mit der Threat Defense-Konfiguration übereinstimmen.

- Sie können die Management-Schnittstelle ändern, nachdem Sie Threat Defense beim Management Center registriert haben, und zwar entweder in die Management-Schnittstelle oder eine andere Datenschnittstelle.
- Für diese Schnittstelle wird der FQDN verwendet, den Sie im Einrichtungsassistenten festgelegt haben.
- Sie können die gesamte Gerätekonfiguration als Teil des Befehls löschen. Diese Option kann in einem Wiederherstellungsszenario sinnvoll sein, aber wir empfehlen nicht, sie für die Ersteinrichtung oder den normalen Betrieb zu verwenden.
- Um das Datenmanagement zu deaktivieren, geben Sie den Befehl **configure network management-data-interface disable** ein.

Beispiel:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://deanwinchester:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Beispiel:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.
```

>

Schritt 7 (optional) Beschränken Sie den Datenschnittstellenzugriff auf Management Center in einem bestimmten Netzwerk.

configure network management-data-interface client *IP-Adressnetzmaske*

Standardmäßig sind alle Netzwerke zulässig.

Schritt 8 Identifizieren Sie das Management Center, das dieses Threat Defense-System verwalten soll.

configure manager add {*Host-Name* | *IPv4-Adresse* | *IPv6-Adresse* | **DONTRESOLVE**} *Registrierungsschlüssel* [*NAT-ID*]

- {*Host-Name* | *IPv4-Adresse* | *IPv6-Adresse* | **DONTRESOLVE**}: Gibt entweder den FQDN oder die IP-Adresse des Management Center an. Wenn das Management Center nicht direkt adressierbar ist, verwenden Sie **DONTRESOLVE**. Mindestens eines der Geräte, entweder das Management Center oder Threat Defense, muss eine erreichbare IP-Adresse haben, um den bidirektionalen, SSL-verschlüsselten Kommunikationskanal zwischen den beiden Geräten einzurichten. Wenn Sie **DONTRESOLVE** in diesem Befehl angeben, muss Threat Defense über eine erreichbare IP-Adresse oder einen Host-Namen verfügen.
- *Registrierungsschlüssel*: Gibt einen einmaligen Registrierungsschlüssel Ihrer Wahl an, den Sie auch bei der Registrierung des Threat Defense-Systems im Management Center angeben. Der Registrierungsschlüssel darf höchstens 37 Zeichen enthalten. Zu den zulässigen Zeichen zählen alphanumerische Zeichen (A–Z, a–z, 0–9) und der Bindestrich (-).
- *NAT-ID*: Gibt eine eindeutige, einmalige Zeichenfolge Ihrer Wahl an, die Sie auch im Management Center angeben. Wenn Sie eine Datenschnittstelle für das Management verwenden, müssen Sie die NAT-ID im Threat Defense-System *und* im Management Center für die Registrierung angeben. Die NAT-ID darf nicht länger als 37 Zeichen sein. Zu den zulässigen Zeichen zählen alphanumerische Zeichen (A–Z, a–z, 0–9) und der Bindestrich (-). Diese ID kann nicht für andere Geräte verwendet werden, die sich beim Management Center registrieren.

Beispiel:

```
> configure manager add fmc-1.example.com regk3y78 natid56
Manager successfully configured.
```

Schritt 9 Fahren Sie das Threat Defense-System herunter, damit Sie das Gerät an die Remote-Zweigstelle senden können.

Es ist wichtig, dass Sie Ihr System ordnungsgemäß herunterfahren. Wenn Sie einfach den Netzstecker ziehen oder den Netzschalter drücken, kann das Dateisystem ernsthaft beschädigt werden. Denken Sie daran, dass im Hintergrund ständig viele Prozesse ablaufen, und dass das Ziehen des Netzsteckers oder das Ausschalten der Stromversorgung kein ordnungsgemäßes Herunterfahren Ihres Systems ermöglicht.

a) Geben Sie den Befehl **shutdown** ein.
b) Beobachten Sie die Betriebs-LED und die Status-LED, um sicherzustellen, dass das Chassis ausgeschaltet ist (unbeleuchtet).
c) Nachdem das Chassis erfolgreich ausgeschaltet wurde, können Sie den Netzstecker ziehen, um die Stromversorgung des Chassis bei Bedarf physisch zu trennen.

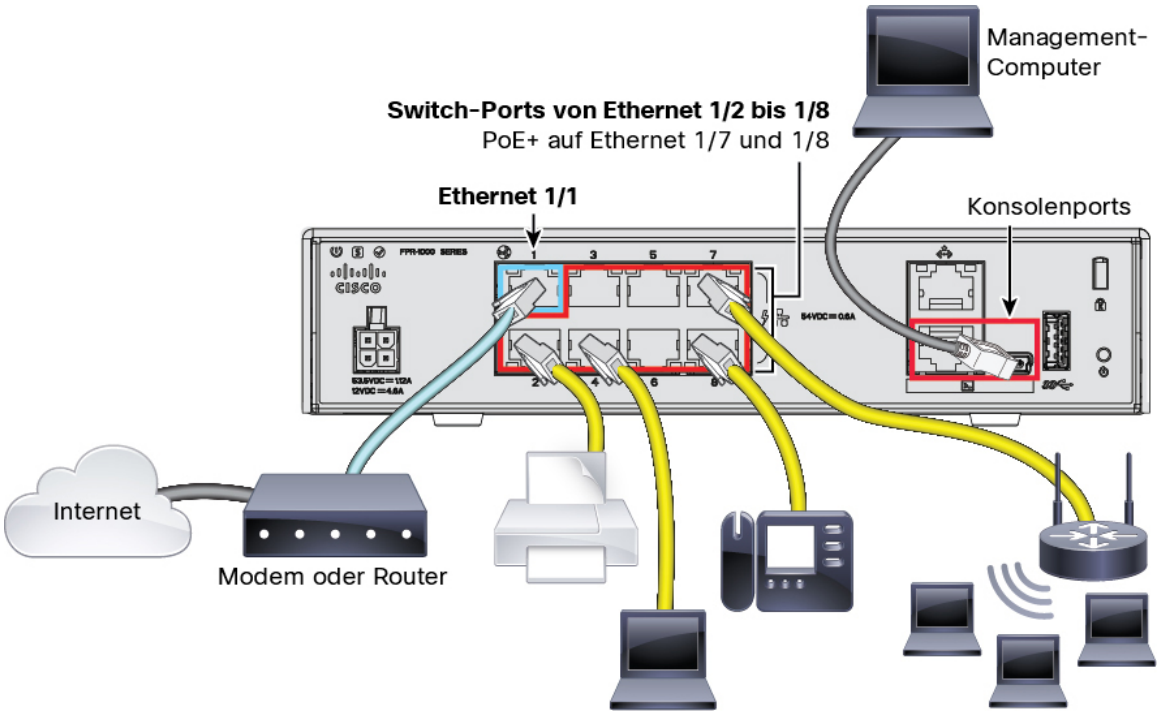
Installation in der Zweigstelle

Nachdem Sie das Threat Defense-System von der zentralen Hauptgeschäftsstelle erhalten haben, müssen Sie die Firewall nur noch per Kabel anschließen und einschalten, damit sie von der externen Schnittstelle aus auf das Internet zugreifen kann. Der Administrator in der Zentrale kann dann die Konfiguration abschließen.

Verkabeln der Firewall

Das Management Center und Ihr Management-Computer befinden sich in einer fernen Hauptgeschäftsstelle und können das Threat Defense-System über das Internet erreichen. Mit den folgenden Schritten kann ein Firepower 1010-System verkabelt werden.

Abbildung 18: Verkabelung einer Remote-Management-Bereitstellung



Prozedur

Schritt 1 Installieren Sie das Chassis. Weitere Informationen finden Sie im Hardware-Installationshandbuch.

Schritt 2 Verbinden Sie die externe Schnittstelle (Ethernet 1/1) mit Ihrem externen Router.

Schritt 3 Verkabeln Sie Ihre internen Endpunkte mit den Switch-Ports (Ethernet1/2 bis 1/8).

Schritt 4 (optional) Verbinden Sie den Management-Computer mit dem Konsolenport.

In der Zweigstelle ist die Konsolenverbindung für den täglichen Gebrauch nicht erforderlich. Sie kann jedoch zur Fehlerbehebung erforderlich sein.

Einschalten des Geräts

Die Systemstromversorgung wird über das Netzkabel gesteuert. Es gibt keinen Netzschalter.

Hinweis Wenn Sie den Threat Defense zum ersten Mal starten, kann die Initialisierung etwa 15 bis 30 Minuten dauern.

Vorbereitungen

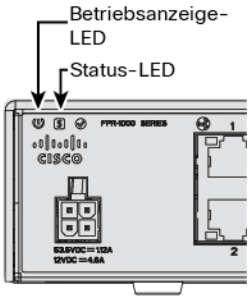
Es ist wichtig, dass Sie Ihr Gerät zuverlässig mit Strom versorgen (z. B. mit einer unterbrechungsfreien Stromversorgung (USV)). Ein Stromausfall ohne vorheriges Herunterfahren kann zu ernsthaften Schäden am Dateisystem führen. Im Hintergrund laufen ständig viele Prozesse ab, und eine Unterbrechung der Stromversorgung ermöglicht kein ordnungsgemäßes Herunterfahren des Systems.

Prozedur

Schritt 1 Schließen Sie das Netzkabel am Gerät und dann an einer Steckdose an.

Wenn Sie das Netzkabel an die Stromversorgung anschließen, ist das Gerät automatisch eingeschaltet.

Schritt 2 Prüfen Sie die Betriebs-LED auf der Rückseite oder Oberseite des Geräts; leuchtet sie dauerhaft grün, ist das Gerät eingeschaltet.



Schritt 3 Prüfen Sie die Status-LED auf der Rückseite oder Oberseite des Geräts; wenn sie dauerhaft grün leuchtet, hat das System die Einschaltdiagnose durchlaufen.

Nachkonfiguration des Administrators in der Zentrale

Nachdem der Administrator der Remote-Zweigstelle das Threat Defense-System verkabelt hat, damit es von der externen Schnittstelle aus auf das Internet zugreifen kann, können Sie das Threat Defense-System beim Management Center registrieren und die Konfiguration des Geräts abschließen.

Anmelden bei Management Center

Verwenden Sie das Management Center, um Threat Defense zu konfigurieren und zu überwachen.

Vorbereitungen

Informationen zu unterstützten Browsern finden Sie in den Versionshinweisen für die von Ihnen verwendete Version (siehe https://www.cisco.com/go/firepower-notes)

Prozedur

Schritt 1 Geben Sie in einem unterstützten Browser die folgende URL ein.

https://*FMC-IP-Adresse*

Schritt 2 Geben Sie Ihren Benutzernamen und Ihr Kennwort ein.

Schritt 3 Klicken Sie auf **Log In** (Anmelden).

Abrufen von Lizenzen für Management Center

Alle Lizenzen werden vom Management Center für Threat Defense bereitgestellt. Sie können optional die folgenden Funktionslizenzen erwerben:

- **Threat**: Security Intelligence und Next-Generation IPS
- **Malware**: MalwareDefense
- **URL**: URL-Filterung
- **RA VPN**: AnyConnect Plus, AnyConnect Apex oder AnyConnect VPN Only.

Nähere Informationen über die Lizenzierung bei Cisco erhalten Sie unter cisco.com/go/licensingguide

Vorbereitungen

- Sie müssen über ein Masterkonto bei Smart Software Manager verfügen.

  Wenn Sie noch kein Konto haben, klicken Sie auf den Link, um ein neues Konto einzurichten. Mit dem Smart Software Manager können Sie ein Masterkonto für Ihr Unternehmen erstellen.

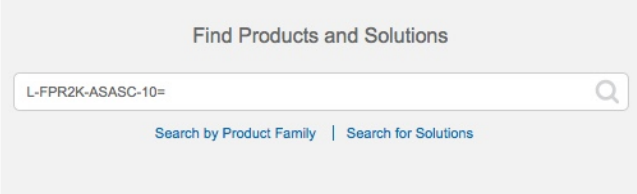
- Ihr Smart Software Licensing-Konto muss für die Strong Encryption-(3DES/AES-)Lizenz qualifiziert sein, um bestimmte Funktionen nutzen zu können (aktiviert mit dem Flag „export-compliance“).

Prozedur

Schritt 1 Stellen Sie sicher, dass Ihr Smart Licensing-Konto die verfügbaren Lizenzen enthält, die Sie benötigen.

Wenn Sie Ihr Gerät bei Cisco oder einem Fachhändler gekauft haben, sollten Ihre Lizenzen mit Ihrem Smart Software License-Konto verknüpft sein. Wenn Sie jedoch selbst Lizenzen hinzufügen müssen, verwenden Sie das Suchfeld **Find Products and Solutions** (Produkte und Lösungen suchen) im Cisco Commerce Workspace. Suchen Sie nach den folgenden Lizenz-PIDs:

Abbildung 19: Lizenzsuche



Hinweis Wenn keine PID gefunden wird, können Sie die PID manuell zu Ihrer Bestellung hinzufügen.

- Kombination aus Threat-, Malware- und URL-Lizenz:
  - L-FPR1010T-TMC =

  Wenn Sie Ihrer Bestellung eine der oben genannten PIDs hinzufügen, können Sie ein befristetes Abonnement auswählen, das einer der folgenden PIDs entspricht:
  - L-FPR1010T-TMC-1Y
  - L-FPR1010T-TMC-3Y
  - L-FPR1010T-TMC-5Y
- VPN für Remotezugriff (RA VPN): Entnehmen Sie die Einzelheiten bitte der Bestellanleitung für Cisco AnyConnect.

Schritt 2 Wenn Sie dies noch nicht getan haben, registrieren Sie Management Center im Smart Software Manager.

Für die Registrierung müssen Sie ein Registrierungstoken im Smart Software Manager generieren. Ausführliche Anweisungen hierzu finden Sie imManagement Center-Konfigurationsleitfaden. Für Low-Touch Provisioning müssen Sie **Cloud Assistance for Low-Touch Provisioning** entweder bei der Registrierung beim Smart Software Manager oder nach der Registrierung aktivieren. Weitere Informationen finden Sie auf der Seite **System** > **Licenses** > **Smart Licenses** (System > Lizenzen > Smart Licenses).

Registrieren von Threat Defense beim Management Center

Registrieren Sie Threat Defense manuell mit der IP-Adresse des Geräts oder dem Host-Namen beim Management Center.

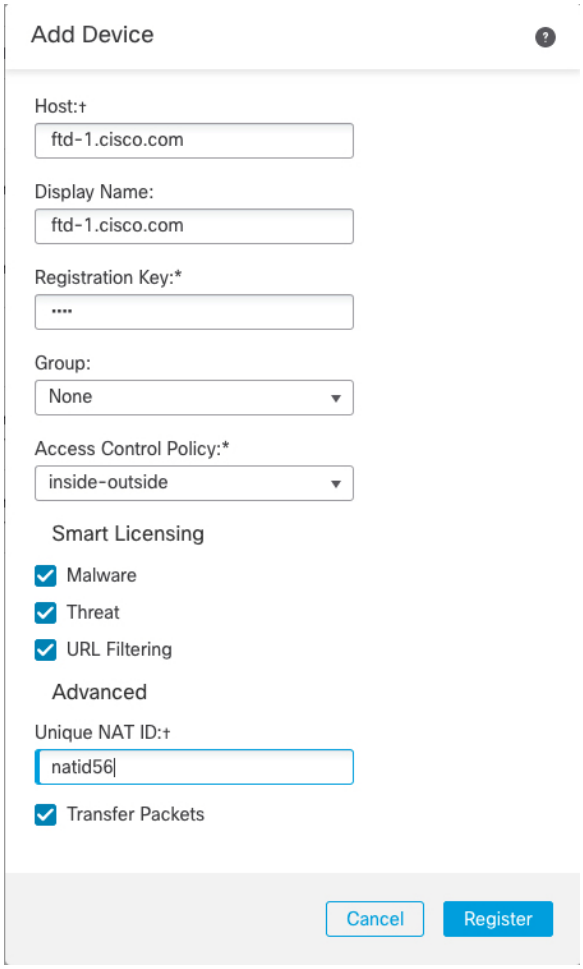
Vorbereitungen

- Sammeln Sie die folgenden Informationen, die Sie in der Threat Defense-Erstkonfiguration festgelegt haben:
  - Threat Defense-Management-IP-Adresse oder -Host-Name und NAT-ID
  - Management Center-Registrierungsschlüssel

Prozedur

Schritt 1 Wählen Sie in Management Center nacheinander **Devices** > **Device Management** (Geräte > Gerätemanagement) aus.

Schritt 2 Wählen Sie in der Dropdown-Liste **Add** (Hinzufügen) den Eintrag **Add Device** (Gerät hinzufügen) aus.



Legen Sie die folgenden Parameter fest:

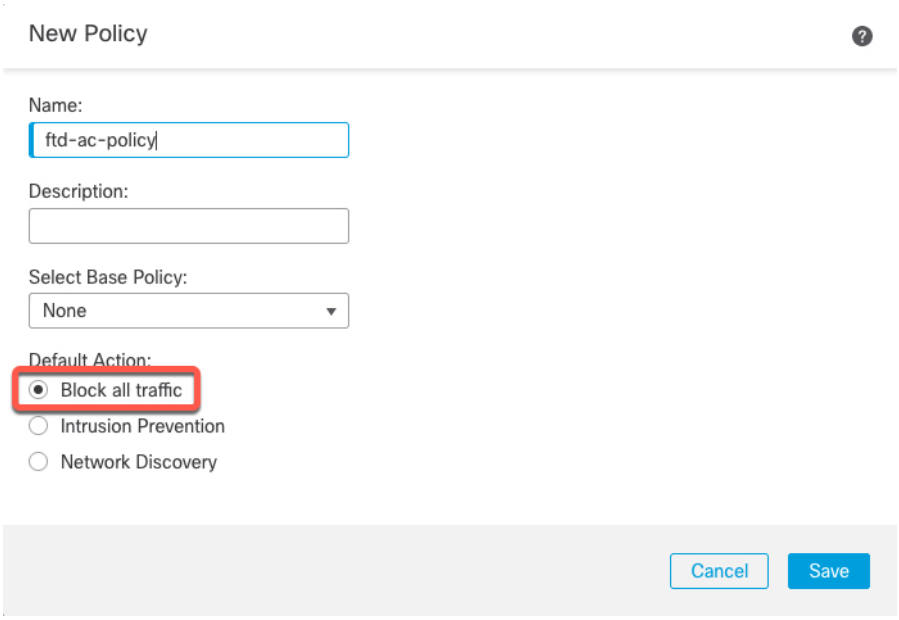
- **Host**: Geben Sie die IP-Adresse oder den Host-Namen des Threat Defense ein, das Sie hinzufügen möchten. Sie können dieses Feld leer lassen, wenn Sie in der anfänglichen Konfiguration von Threat Defense sowohl die Management Center-IP-Adresse als auch eine NAT-ID angegeben haben.

  Hinweis In einer HA-Umgebung, in der sich beide Management Center hinter einem NAT befinden, können Sie den Threat Defense ohne Host-IP oder -Namen im primären Management Center registrieren. Für die Registrierung des Threat Defense in einem sekundären Management Center müssen Sie jedoch die IP-Adresse oder den Hostnamen für den Threat Defense angeben.

- **Display Name** (Anzeigename): Geben Sie den Namen für Threat Defense ein, der im Management Center angezeigt werden soll.

- **Registration Key** (Registrierungsschlüssel): Geben Sie denselben Registrierungsschlüssel ein, den Sie in der anfänglichen Konfiguration von Threat Defense angegeben haben.
- **Domain**: Weisen Sie das Gerät einer Leaf-Domain zu, wenn Sie in einer Multi-Domain-Umgebung arbeiten.
- **Group** (Gruppe): Weisen Sie es einer Gerätegruppe zu, wenn Sie Gruppen verwenden.
- **Access Control Policy** (Zugriffskontrollrichtlinie): Wählen Sie eine anfängliche Richtlinie aus. Sofern Sie nicht bereits über eine benutzerdefinierte Richtlinie verfügen, die Sie verwenden müssen, wählen Sie **Create new policy** (Neue Richtlinie erstellen) und dann **Block all traffic** (Gesamten Traffic blockieren) aus. Sie können dies später ändern, um Traffic zuzulassen; siehe Zulassen des Traffics von innen nach außen, auf Seite 42.

Abbildung 20: Neue Richtlinie



- **Smart Licensing**: Weisen Sie die Smart Licenses zu, die Sie für die Funktionen benötigen, die Sie bereitstellen möchten: **Malware** (wenn Sie eine Malware-Untersuchung verwenden möchten), **Threat** (wenn Sie Intrusion Prevention verwenden möchten) und **URL** (wenn Sie eine kategoriebasierte URL-Filterung implementieren möchten). **Hinweis:** Nach dem Hinzufügen des Geräts können Sie über die Seite **System** > **Licenses** > **Smart Licenses** (System > Lizenzen > Smart Licenses) eine Secure Client-VPN-Lizenz für Remotezugriff anwenden.
- **Unique NAT ID** (Eindeutige NAT-ID): Geben Sie die NAT-ID an, die Sie in der anfänglichen -Threat Defense-Konfiguration angegeben haben.
- **Transfer Packets** (Pakete übertragen): Ermöglicht dem Gerät, Pakete an das Management Center zu übertragen. Wenn diese Option aktiviert ist und Ereignisse wie IPS oder Snort ausgelöst werden, sendet das Gerät Ereignismetadateninformationen und Paketdaten zur Untersuchung an Management Center. Wenn Sie die Option deaktivieren, werden nur Ereignisinformationen an Management Center gesendet, aber keine Paketdaten.

Schritt 3 Klicken Sie auf **Register** (Registrieren). und bestätigen Sie die erfolgreiche Registrierung.

Wenn die Registrierung erfolgreich ist, wird das Gerät der Liste hinzugefügt. Falls sie fehlschlägt, wird eine Fehlermeldung angezeigt. Wenn die Registrierung fehlschlägt, überprüfen Sie die folgenden Punkte:Threat Defense

- Ping: Rufen Sie die Threat Defense-CLI auf, und pingen Sie die Management Center-IP-Adresse mit dem folgenden Befehl an:

  ping system *IP-Adresse*

  Wenn die Ping-Abfrage nicht erfolgreich ist, überprüfen Sie Ihre Netzwerkeinstellungen mit dem Befehl **show network**. Wenn Sie die Threat Defense-Management-IP-Adresse ändern müssen, verwenden Sie den Befehl **configure network management-data-interface**.

- Registrierungsschlüssel, NAT-ID und Management Center-IP-Adresse: Stellen Sie sicher, dass Sie auf beiden Geräten den gleichen Registrierungsschlüssel und, falls verwendet, die NAT-ID verwenden. Sie können den Registrierungsschlüssel und die NAT-ID auf dem Threat Defense **configure manager add** mit dem Befehl festlegen.

Weitere Informationen zur Fehlerbehebung finden Sie unter https://cisco.com/go/fmc-reg-error.

Konfigurieren einer Basissicherheitsrichtlinie

In diesem Abschnitt wird beschrieben, wie Sie eine grundlegende Sicherheitsrichtlinie mit den folgenden Einstellungen konfigurieren:

- Interne und externe Schnittstellen: Weisen Sie der internen Schnittstelle eine statische IP-Adresse zu. Sie haben im Rahmen der Einrichtung des Managerzugriffs grundlegende Einstellungen für die externe Schnittstelle konfiguriert, müssen sie jedoch weiterhin einer Sicherheitszone zuweisen.
- DHCP-Server: Verwenden Sie einen DHCP-Server auf der internen Schnittstelle für Clients.
- NAT: Verwenden Sie die Schnittstellen-PAT für die externe Schnittstelle.
- Access Control (Zugriffskontrolle): Lassen Sie Traffic von innen nach außen zu.
- SSH: Aktivieren Sie SSH auf der Managerzugriffsschnittstelle.

Konfigurieren von Schnittstellen

Fügen Sie die VLAN1-Schnittstelle für die Switch-Ports hinzu, oder konvertieren Sie Switch-Ports in Firewall-Schnittstellen, weisen Sie Schnittstellen zu Sicherheitszonen zu, und legen Sie die IP-Adressen fest. In der Regel müssen Sie mindestens zwei Schnittstellen konfigurieren, um ein System einzurichten, das sinnvollen Traffic weiterleitet. Normalerweise haben Sie eine externe Schnittstelle, die dem Upstream-Router oder dem Internet zugekehrt ist, und eine oder mehrere Schnittstellen im Inneren für die Netzwerke Ihres Unternehmens. Standardmäßig ist Ethernet1 / 1 eine normale Firewall-Schnittstelle, die Sie für den Außenbereich verwenden können. Die verbleibenden Schnittstellen sind Switch-Ports in VLAN 1; nachdem Sie die VLAN1-Schnittstelle hinzugefügt haben, können Sie sie zu Ihrer internen Schnittstelle machen. Sie können Switch-Ports auch anderen VLANs zuweisen oder Switch-Ports in Firewall-Schnittstellen konvertieren.

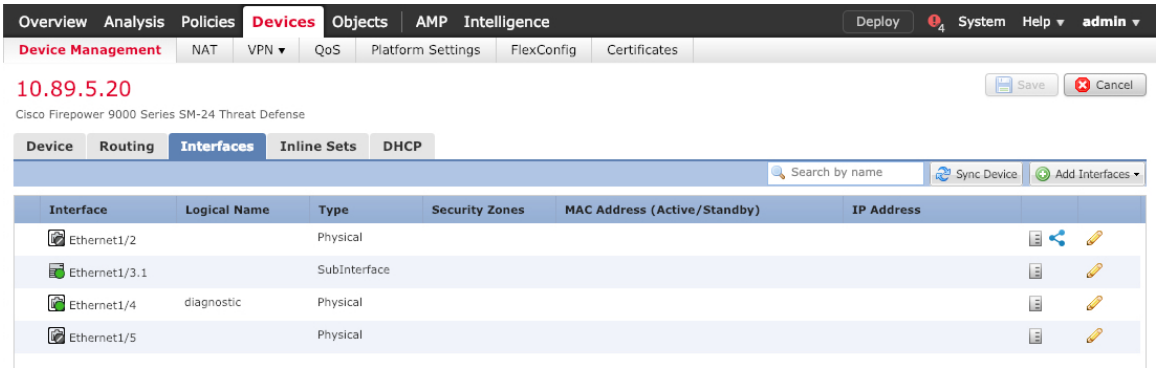
In einer typischen Edge-Routing-Situation beziehen Sie die Adresse der externen Schnittstelle über DHCP von Ihrem ISP, während Sie statische Adressen für die Schnittstellen im Inneren (internen Schnittstellen) definieren.

Im folgenden Beispiel wird eine interne Schnittstelle im Modus „geroutet“ (VLAN1) mit einer statischen Adresse und eine externe Schnittstelle im Modus „geroutet“ unter Verwendung von DHCP (Ethernet1/1) konfiguriert.

Prozedur

Schritt 1 Wählen Sie **Devices** > **Device Management** (Geräte > Gerätemanagement), und klicken Sie für das Gerät auf **Bearbeiten** ( ).

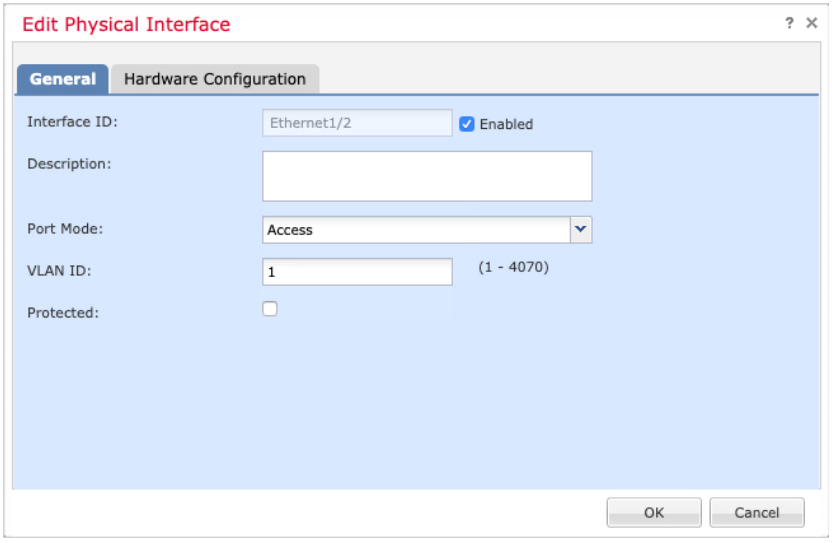
Schritt 2 Klicken Sie auf **Interfaces** (Schnittstellen).



Schritt 3 (optional) Deaktivieren Sie den Switch-Port-Modus für die Switch-Ports (Ethernet 1/2 bis 1/8), indem Sie auf den Schieberegler in der Spalte **SwitchPort** klicken, damit er als deaktiviert ( ) angezeigt wird.

Schritt 4 Aktivieren Sie die Switch-Ports.

a) Klicken Sie für den Switch-Port auf **Bearbeiten** ( ).



b) Aktivieren Sie die Schnittstelle, indem Sie das Kontrollkästchen **Enabled** (Aktiviert) markieren.

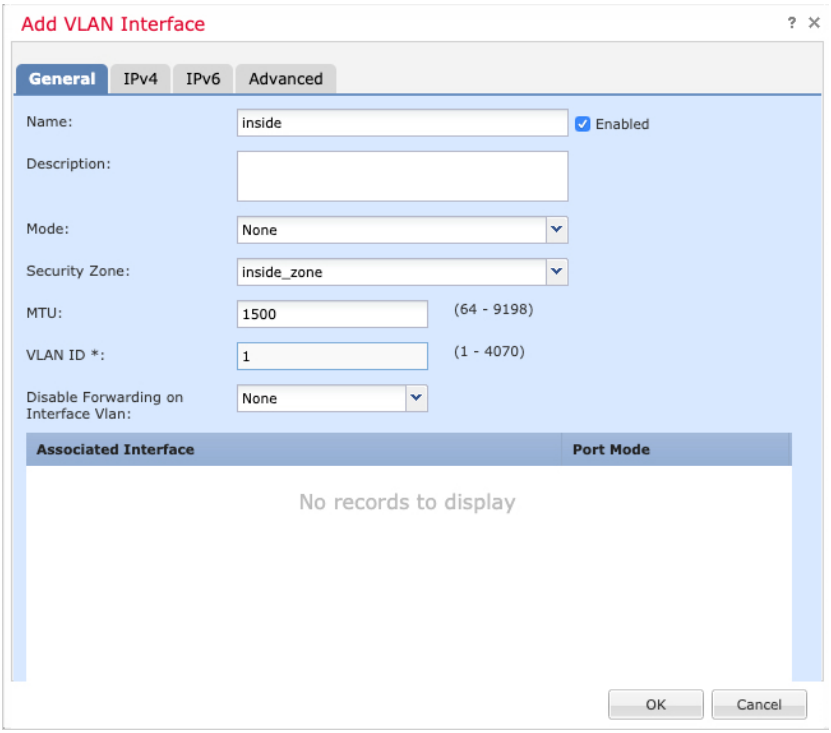
c) (optional) Ändern Sie die VLAN-ID; der Standardwert ist 1. Als Nächstes fügen Sie eine VLAN-Schnittstelle hinzu, die dieser ID entspricht.

d) Klicken Sie auf **OK**.

Schritt 5 Fügen Sie die *interne* VLAN-Schnittstelle hinzu.

a) Klicken Sie auf **Add Interfaces** > **VLAN Interface** (Schnittstellen hinzufügen > VLAN-Schnittstelle).

Die Registerkarte **General** (Allgemein) wird geöffnet.



b) Geben Sie einen **Namen** mit bis zu 48 Zeichen ein.

Nennen Sie die Schnittstelle beispielsweise **inside**.

c) Markieren Sie das Kontrollkästchen **Enabled** (Aktiviert).

d) Übernehmen Sie die Einstellung **None** (Keiner) für **Mode** (Modus).

e) Wählen Sie in der Dropdown-Liste **Security Zone** (Sicherheitszone) eine vorhandene interne Sicherheitszone aus, oder fügen Sie eine neue hinzu, indem Sie auf **New** (Neu) klicken.

Fügen Sie beispielsweise eine Zone mit dem Namen **inside_zone** hinzu. Jede Schnittstelle muss einer Sicherheitszone und/oder Schnittstellengruppe zugewiesen werden. Eine Schnittstelle kann nur zu einer Sicherheitszone, aber gleichzeitig auch zu mehreren Schnittstellengruppen gehören. Sie wenden Ihre Sicherheitsrichtlinie basierend auf Zonen oder Gruppen an. Sie können beispielsweise die interne Schnittstelle der internen Zone zuweisen und die externe Schnittstelle zur Außenzone. Anschließend können Sie Ihre Zugriffskontrollrichtlinie so konfigurieren, dass der Traffic von innen nach außen geleitet wird, aber nicht von außen nach innen. Die meisten Richtlinien unterstützen nur Sicherheitszonen. Sie können Zonen oder Schnittstellengruppen in NAT-Richtlinien, Vorfilterrichtlinien und QoS-Richtlinien verwenden.

f) Setzen Sie die **VLAN-ID** auf **1**.

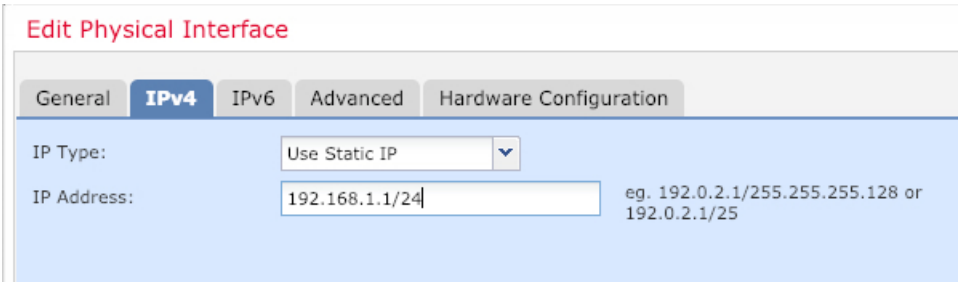
Standardmäßig sind alle Switch-Ports auf VLAN 1 eingestellt. Wenn Sie hier eine andere VLAN-ID auswählen, müssen Sie auch jeden Switch-Port bearbeiten, damit er auf die neue VLAN-ID gesetzt ist.

Sie können die VLAN-ID nicht mehr ändern, nachdem Sie die Schnittstelle gespeichert haben. Die VLAN-ID ist sowohl der verwendete VLAN-Tag als auch die Schnittstellen-ID in Ihrer Konfiguration.

g) Klicken Sie auf die Registerkarte **IPv4** und/oder **IPv6**.

- **IPv4**: Wählen Sie in der Dropdown-Liste **Use Static IP** (Statische IP verwenden) aus, und geben Sie eine IP-Adresse und eine Subnetzmaske in der Schreibweise mit Schrägstrichen ein.

  Geben Sie beispielsweise **192.168.1.1/24** ein.

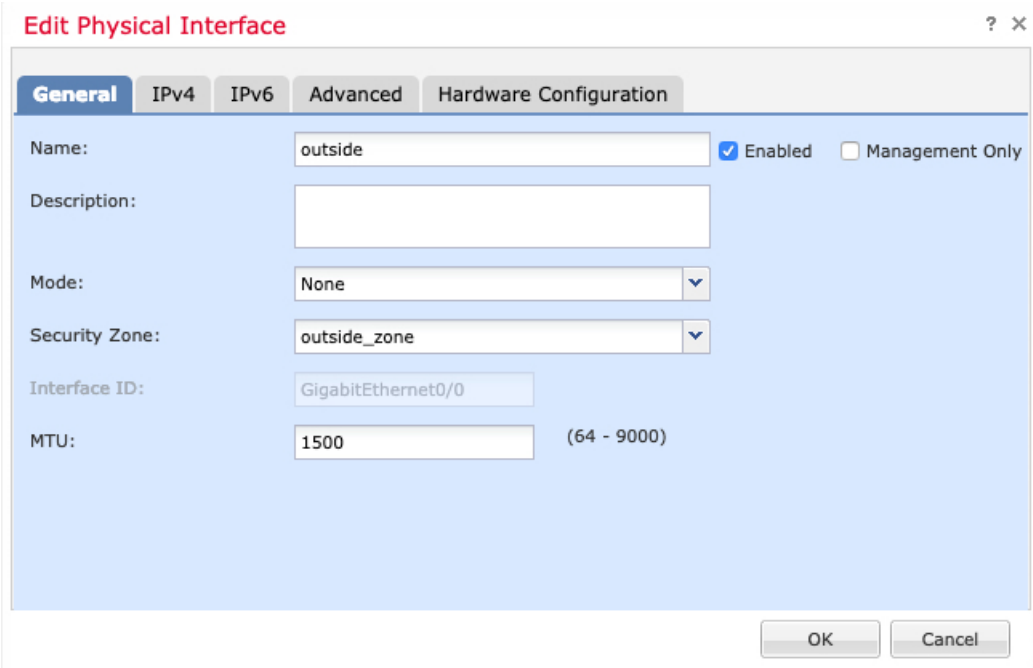


- **IPv6**: Markieren Sie das Kontrollkästchen **Autoconfiguration** (Automatische Konfiguration) für eine automatische Stateless-Konfiguration.

h) Klicken Sie auf **OK**.

Schritt 6 Klicken Sie für die Ethernet1/1-Schnittstelle, die Sie für den *Außenbereich* verwenden möchten, auf **Bearbeiten** (✎).

Die Registerkarte **General** (Allgemein) wird geöffnet.



Sie haben diese Schnittstelle bereits für den Managerzugriff vorkonfiguriert, sodass die Schnittstelle bereits einen Namen hat und aktiviert und adressiert ist. Sie sollten keine dieser Grundeinstellungen ändern, da dadurch die Management Center-Managementverbindung unterbrochen würde. Sie müssen die Sicherheitszone auf diesem Bildschirm jedoch für Richtlinien bezüglich des Durchgangs-Traffics konfigurieren.

a) Wählen Sie in der Dropdown-Liste **Security Zone** (Sicherheitszone) eine vorhandene externe Sicherheitszone aus, oder fügen Sie eine neue hinzu, indem Sie auf **New** (Neu) klicken.

Fügen Sie beispielsweise eine Zone mit dem Namen **outside_zone** hinzu.

b) Klicken Sie auf **OK**.

Schritt 7 Klicken Sie auf **Save** (Speichern).

Konfigurieren des DHCP-Servers

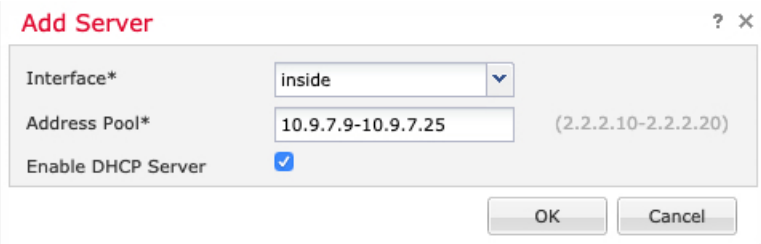
Aktivieren Sie den DHCP-Server, wenn Clients DHCP zum Abrufen von IP-Adressen aus dem Threat Defense verwenden sollen.

Prozedur

Schritt 1 Wählen Sie **Devices** > **Device Management** (Geräte > Gerätemanagement), und klicken Sie für das Gerät auf **Bearbeiten** ( ).

Schritt 2 Wählen Sie **DHCP** > **DHCP Server** (DHCP > DHCP-Server).

Schritt 3 Klicken Sie auf der Seite **Server** auf **Add** (Hinzufügen), und konfigurieren Sie die folgenden Optionen:



- **Interface** (Schnittstelle): Wählen Sie in der Dropdown-Liste die Schnittstelle aus.
- **Address Pool** (Adressen-Pool): Legen Sie den Bereich der niedrigsten bis höchsten IP-Adressen fest, die vom DHCP-Server verwendet werden. Der Bereich der IP-Adressen muss sich im selben Subnetz wie die ausgewählte Schnittstelle befinden und darf die IP-Adresse der Schnittstelle selbst nicht enthalten.
- **Enable DHCP Server** (DHCP-Server aktivieren): Aktiviert den DHCP-Server auf der ausgewählten Schnittstelle.

Schritt 4 Klicken Sie auf **OK**.

Schritt 5 Klicken Sie auf **Save** (Speichern).

Konfigurieren von NAT

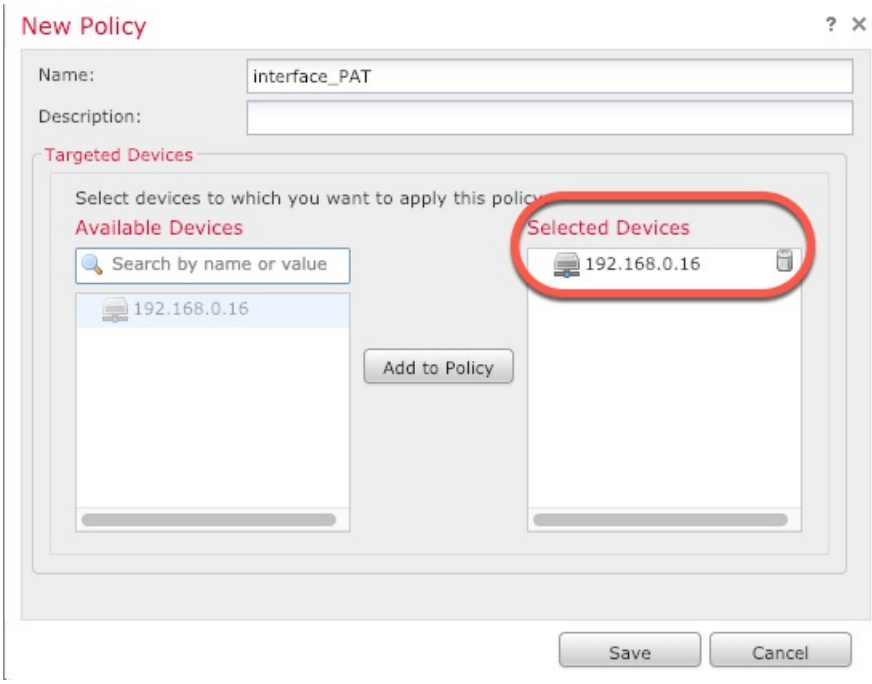
Konfigurieren von NAT

Eine typische NAT-Regel konvertiert interne Adressen in einen Port an der IP-Adresse der externen Schnittstelle. Diese Art von NAT-Regel wird als *Interface Port Address Translation (PAT)* bezeichnet.

Prozedur

Schritt 1 Wählen Sie **Devices** > **NAT** (Geräte > NAT), und klicken Sie auf **New Policy** > **Threat Defense NAT** (Neue Richtlinie > Threat Defense-NAT).

Schritt 2 Geben Sie der Richtlinie einen Namen, wählen Sie die Geräte aus, für die sie gelten soll, und klicken Sie auf **Save** (Speichern).



Die Zuordnung zwischen der Richtlinie und Management Center wird vorgenommen. Sie müssen der Richtlinie noch Regeln hinzufügen.

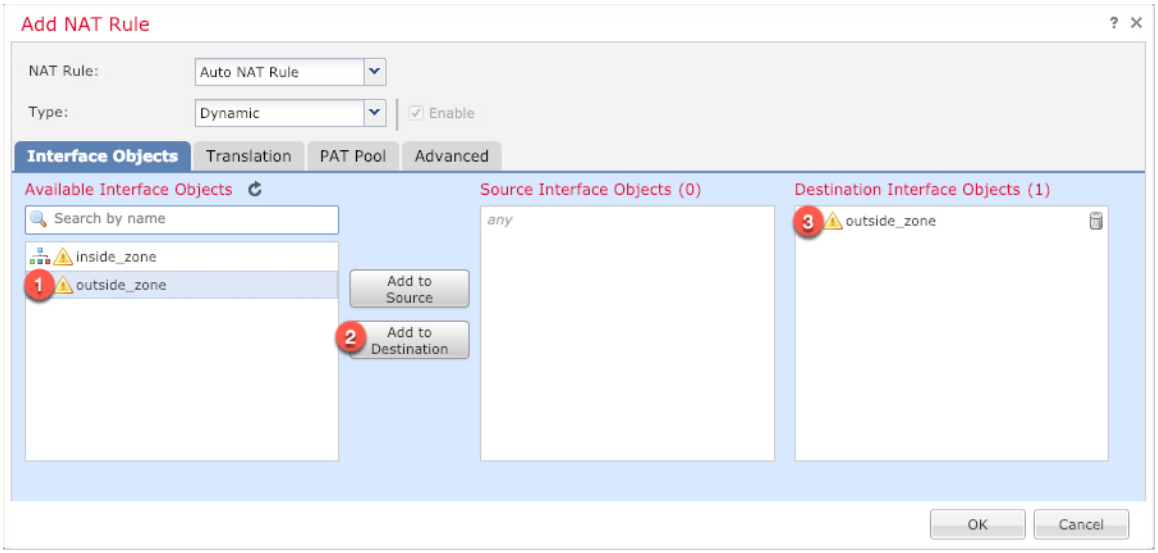
Schritt 3 Klicken Sie auf **Add Rule** (Regel hinzufügen).

Das Dialogfeld **Add NAT Rule** (NAT-Regel hinzufügen) wird angezeigt.

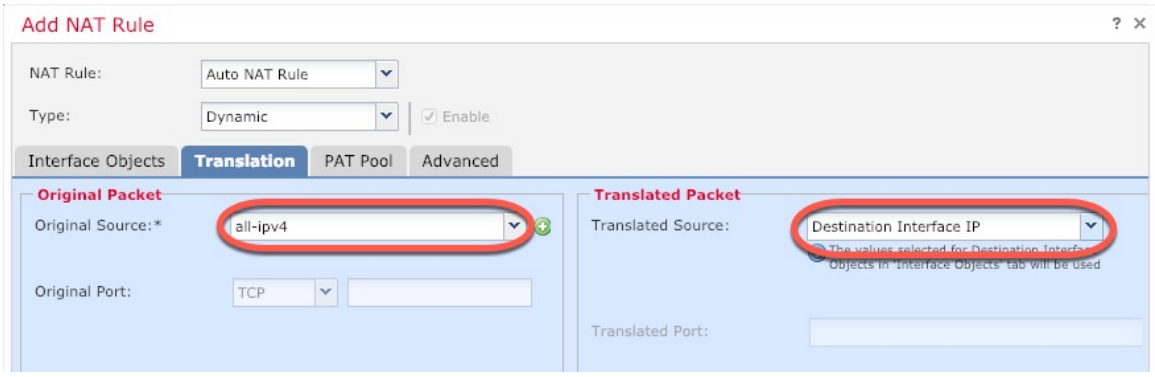
Schritt 4 Konfigurieren Sie die grundlegenden Regeloptionen:

- **NAT Rule** (NAT-Regel): Wählen Sie **Auto NAT Rule** (Automatische NAT-Regel) aus.
- **Type** (Typ): Wählen Sie **Dynamic** (Dynamisch) aus.

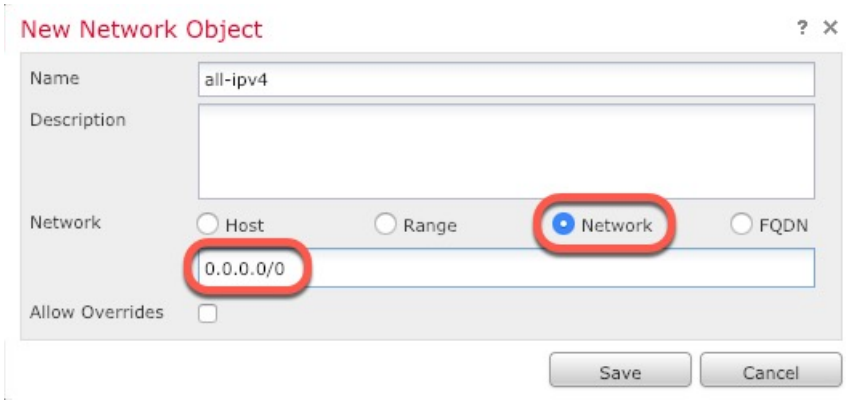
Schritt 5 Fügen Sie auf der Seite **Interface Objects** (Schnittstellenobjekte) die externe Zone aus dem Bereich **Available Interface Objects** (Verfügbare Schnittstellenobjekte) im Bereich **Destination Interface Objects** (Zielschnittstellenobjekte) hinzu.



Schritt 6 Konfigurieren Sie auf der Seite **Translation** (Übersetzung) die folgenden Optionen:



- **Original Source** (Ursprüngliche Quelle): Klicken Sie auf **Hinzufügen** (+), um ein Netzwerkobjekt für den gesamten IPv4-Traffic (0.0.0.0/0) hinzuzufügen.

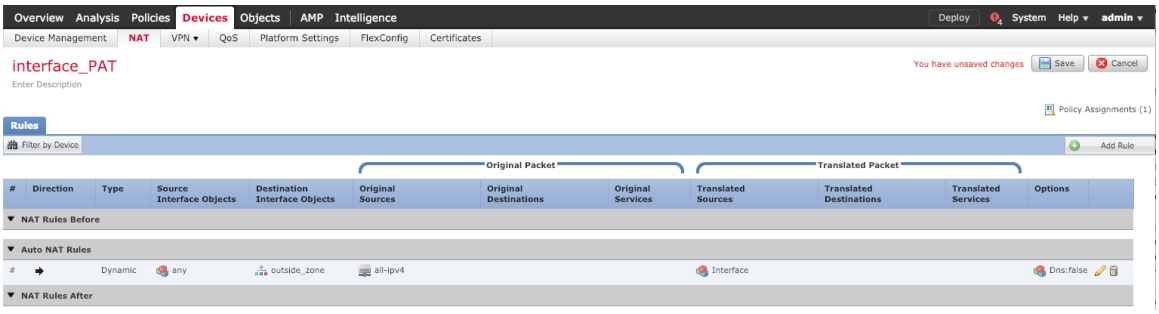


Hinweis Sie können das systemdefinierte Objekt **any-ipv4** nicht verwenden, da Auto-NAT-Regeln NAT als Teil der Objektdefinition hinzufügen, und Sie können systemdefinierte Objekte nicht bearbeiten.

- **Translated Source** (Übersetzte Quelle): Wählen Sie für **Destination Interface IP** (Zielschnittstellen-IP) einen Wert aus.

Schritt 7 Klicken Sie auf **Save** (Speichern), um die Regel hinzuzufügen.

Die Regel wird in der Tabelle **Rules** (Regeln) gespeichert.



Schritt 8 Klicken Sie auf der Seite **NAT** auf **Save** (Speichern), um Ihre Änderungen zu speichern.

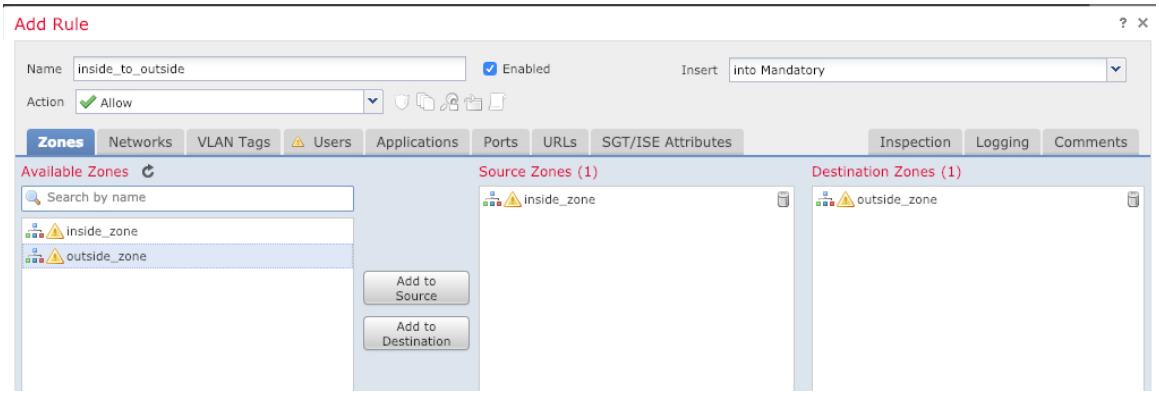
Zulassen des Traffics von innen nach außen

Wenn Sie bei der Registrierung von Threat Defense eine grundlegende Zugriffskontrollrichtlinie zum Blockieren des gesamten Traffics (**Block all traffic**) erstellt haben, müssen Sie der Richtlinie Regeln hinzufügen, um Traffic über das Gerät zuzulassen. Das folgende Verfahren fügt eine Regel hinzu, die Traffic von der internen Zone zur externen Zone zulässt. Wenn Sie über andere Zonen verfügen, müssen Sie Regeln hinzufügen, die den Traffic zu den entsprechenden Netzwerken zulassen.

Prozedur

Schritt 1 Wählen Sie **Policy** > **Access Policy** > **Access Policy** (Richtlinie > Zugriffsrichtlinie > Zugriffsrichtlinie) aus, und klicken Sie auf **Bearbeiten** ( ) für die Zugriffskontrollrichtlinie, die dem Threat Defense zugewiesen ist.

Schritt 2 Klicken Sie auf **Add Rule** (Regel hinzufügen), und legen Sie die folgenden Parameter fest:



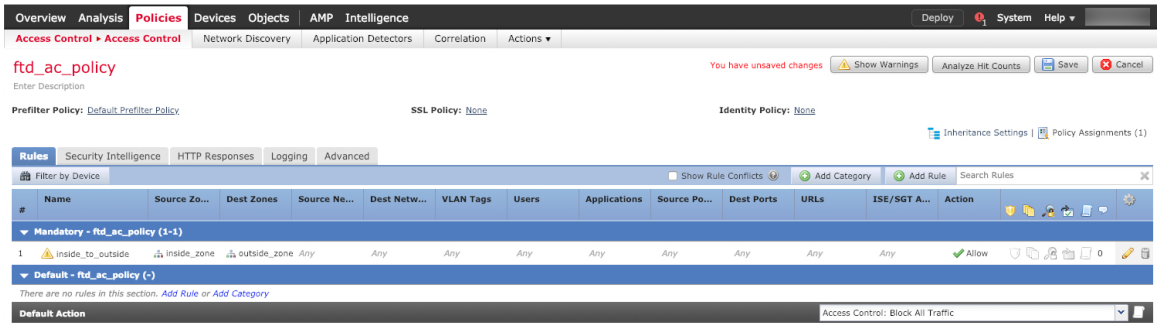
- **Name**: Geben Sie dieser Regel einen Namen, z. B. **inside_to_outside**.

- **Source Zones** (Quellzonen): Wählen Sie in **Available Zones** (Verfügbare Zonen) die interne Zone aus, und klicken Sie auf **Add to Source** (Zu Quelle hinzufügen).
- **Destination Zones** (Zielzonen): Wählen Sie in **Available Zones** (Verfügbare Zonen) die externe Zone aus, und klicken Sie auf **Add to Destination** (Zu Ziel hinzufügen).

Lassen Sie die anderen Einstellungen unverändert.

Schritt 3 Klicken Sie auf **Add** (Hinzufügen).

Die Regel wird der Tabelle **Rules** (Regeln) hinzugefügt.



Schritt 4 Klicken Sie auf **Save** (Speichern).

Konfigurieren von SSH auf der Managerzugriffsdatenschnittstelle

Wenn Sie den Management Center-Zugriff auf einer Datenschnittstelle, z. B. der externen Schnittstelle, aktiviert haben, sollten Sie SSH auf dieser Schnittstelle mit diesem Verfahren aktivieren. In diesem Abschnitt wird beschrieben, wie SSH-Verbindungen zu einer oder mehreren *Datenschnittstellen* auf dem Threat Defense aktiviert werden. SSH wird für die logische Diagnoseschnittstelle nicht unterstützt.

Hinweis SSH ist auf der Management-Schnittstelle standardmäßig aktiviert. Dieser Bildschirm hat jedoch keinen Einfluss auf den Management-SSH-Zugriff.

Die Management-Schnittstelle ist von den anderen Schnittstellen auf dem Gerät getrennt. Sie wird verwendet, um das Gerät einzurichten und bei Management Center zu registrieren. SSH für Datenschnittstellen teilt die interne und externe Benutzerliste mit SSH für die Management-Schnittstelle. Andere Einstellungen werden separat konfiguriert: Aktivieren Sie für Datenschnittstellen SSH und Zugriffslisten über diesen Bildschirm. SSH-Traffic für Datenschnittstellen verwendet die reguläre Routingkonfiguration und keine statischen Routen, die bei der Einrichtung oder in der CLI konfiguriert wurden.

Informationen zur Konfiguration der SSH-Zugriffsliste für die Management-Schnittstelle finden Sie unter dem Befehl **configure ssh-access-list** in der Befehlsreferenz für Secure Firewall Threat Defense. Informationen zum Konfigurieren einer statischen Route finden Sie in den Informationen zum Befehl **configure network static-routes**. Standardmäßig konfigurieren Sie die Standardroute bei der Ersteinrichtung über die Management-Schnittstelle.

Um SSH zu verwenden, benötigen Sie auch keine Zugriffsregel, die die Host-IP-Adresse zulässt. Sie müssen nur den SSH-Zugriff gemäß diesem Abschnitt konfigurieren.

Sie können SSH nur für eine erreichbare Schnittstelle verwenden. Wenn sich Ihr SSH-Host auf der externen Schnittstelle befindet, können Sie eine Managementverbindung nur direkt mit der externen Schnittstelle initiieren.

Das Gerät ermöglicht maximal fünf gleichzeitige SSH-Verbindungen.

Hinweis Das Gerät beendet die SSH-Verbindung, nachdem ein Benutzer dreimal hintereinander erfolglos versucht hat, sich über SSH an der CLI anzumelden.

Vorbereitungen

- Sie können interne SSH-Benutzer in der CLI mit dem Befehl **configure user add** konfigurieren. Standardmäßig gibt es einen **Administrator**-Benutzer, für den Sie das Kennwort bei der Ersteinrichtung konfiguriert haben. Sie können externe Benutzer auch auf LDAP oder RADIUS konfigurieren, indem Sie in den Plattformeinstellungen **External Authentication** (Externe Authentifizierung) konfigurieren.
- Sie benötigen Netzwerkobjekte, die die Hosts oder Netzwerke definieren, die Sie für SSH-Verbindungen mit dem Gerät zulassen dürfen. Sie können Objekte als Teil des Verfahrens hinzufügen. Wenn Sie jedoch mithilfe von Objektgruppen eine Gruppe von IP-Adressen identifizieren möchten, stellen Sie sicher, dass die in den Regeln erforderlichen Gruppen bereits vorhanden sind. Wählen Sie **Objects** > **Object Management** (Objekte > Objektmanagement) aus, um Objekte zu konfigurieren.

Hinweis Sie können das vom System bereitgestellte Netzwerkobjekt **any** nicht verwenden. Verwenden Sie stattdessen **any-ipv4** oder **any-ipv6**.

Prozedur

Schritt 1 Wählen Sie **Devices** > **Platform Settings** (Geräte > Plattformeinstellungen) aus, und erstellen oder bearbeiten Sie die Threat Defense-Richtlinie.

Schritt 2 Wählen Sie **Secure Shell** aus.

Schritt 3 Identifizieren Sie die Schnittstellen und IP-Adressen, die SSH-Verbindungen ermöglichen.

Verwenden Sie diese Tabelle, um einzuschränken, welche Schnittstellen SSH-Verbindungen akzeptieren. Außerdem können Sie die IP-Adressen der Clients einschränken, die diese Verbindungen herstellen dürfen. Sie können anstelle einzelner IP-Adressen auch Netzwerkadressen verwenden.

a) Klicken Sie auf **Add** (Hinzufügen), um eine neue Regel hinzuzufügen, oder auf **Edit** (Bearbeiten), um eine vorhandene Regel zu bearbeiten.

b) Konfigurieren Sie die Regeleigenschaften:

- **IP Address** (IP-Adresse): Das Netzwerkobjekt oder die Gruppe für die Identifizierung der Hosts oder Netzwerke, die Sie für SSH-Verbindungen zulassen. Wählen Sie ein Objekt aus dem Dropdown-Menü aus, oder fügen Sie ein neues Netzwerkobjekt hinzu, indem Sie auf + klicken.
- **Security Zones** (Sicherheitszonen): Fügen Sie die Zonen hinzu, die die Schnittstellen enthalten, zu denen Sie SSH-Verbindungen zulassen. Für Schnittstellen, die sich nicht in einer Zone befinden, können Sie den Schnittstellennamen in das Feld unter der Liste „Selected Security Zone“ (Ausgewählte

Sicherheitszone) eingeben und auf **Add** (Hinzufügen) klicken. Diese Regeln werden auf ein Gerät nur dann angewendet, wenn das Gerät die ausgewählten Schnittstellen oder Zonen enthält.

c) Klicken Sie auf **OK**.

Schritt 4 Klicken Sie auf **Save** (Speichern).

Sie können jetzt **Deploy** > **Deployment** (Bereitstellen > Bereitstellung) aufrufen und die Richtlinie auf zugewiesenen Geräten bereitstellen. Die Änderungen sind erst aktiv, wenn Sie sie bereitstellen.

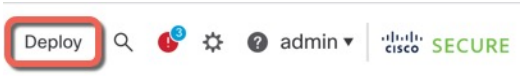
Bereitstellen der Konfiguration

Stellen Sie die Konfigurationsänderungen für Threat Defense bereit. Keine Ihrer Änderungen ist auf dem Gerät aktiv, bis Sie sie bereitstellen.

Prozedur

Schritt 1 Klicken Sie oben rechts auf **Deploy** (Bereitstellen).

Abbildung 21: Bereitstellen



Schritt 2 Klicken Sie entweder auf **Deploy All** (Alle bereitstellen), um die Bereitstellung auf allen Geräten durchzuführen, oder auf **Advanced Deploy** (Erweiterte Bereitstellung), um die Bereitstellung auf ausgewählten Geräten durchzuführen.

Abbildung 22: Alle bereitstellen

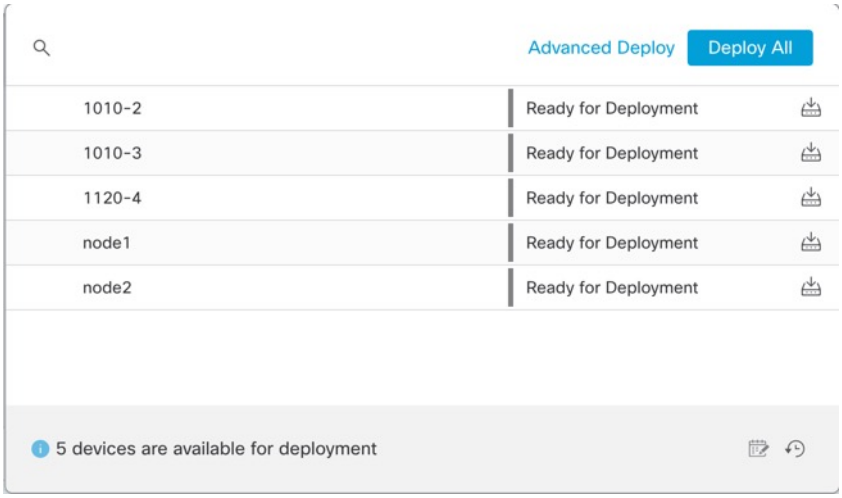
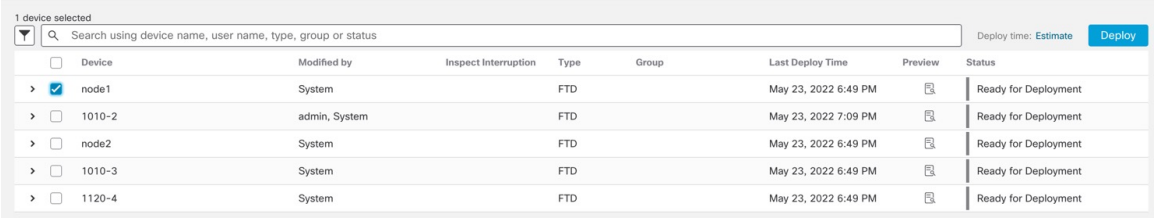
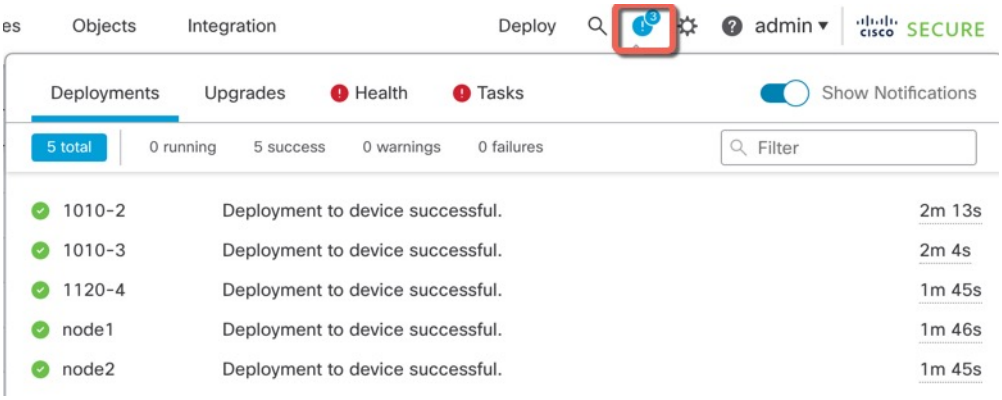


Abbildung 23: Erweiterte Bereitstellung



Schritt 3 Stellen Sie sicher, dass die Bereitstellung erfolgreich ist. Klicken Sie in der Menüleiste rechts neben der Schaltfläche **Deploy** (Bereitstellen) auf das Symbol, um den Status der Bereitstellungen anzuzeigen.

Abbildung 24: Bereitstellungsstatus



Zugriff auf die Threat Defense- und FXOS-CLI

Verwenden Sie die Befehlszeilenschnittstelle (CLI), um das System einzurichten und grundlegende Systemfehlerbehebungen durchzuführen. Sie können Richtlinien nicht über eine CLI-Sitzung konfigurieren. Für den Zugriff auf die CLI (Befehlszeilenschnittstelle) müssen Sie eine Verbindung zum Konsolenport herstellen.

Sie können zur Fehlerbehebung auch auf die FXOS-CLI-CLI zugreifen.

Hinweis Sie können auch eine SSH-Sitzung für die Management-Schnittstelle des Threat Defense-Geräts nutzen. Im Gegensatz zu einer Konsolensitzung verwendet die SSH-Sitzung standardmäßig die Threat Defense-CLI, über die Sie sich mit dem Befehl **connect fxos** mit der FXOS-CLI-CLI verbinden können. Sie können sich später mit der Adresse auf einer Datenschnittstelle verbinden, wenn Sie die Schnittstelle für SSH-Verbindungen öffnen. Der SSH-Zugriff auf Datenschnittstellen ist standardmäßig deaktiviert. Dieses Verfahren beschreibt den Konsolenportzugriff, der standardmäßig auf die FXOS-CLI-CLI eingestellt ist.

Prozedur

Schritt 1 Verbinden Sie Ihren Management-Computer mit dem Konsolenport, um sich bei der CLI anzumelden. Firepower 1000 wird mit einem seriellen USB-A-zu-B-Kabel ausgeliefert. Stellen Sie sicher, dass Sie alle erforderlichen seriellen USB-Treiber für Ihr Betriebssystem installieren (siehe Firepower 1010 -Hardwarehandbuch). Der Konsolenport ist standardmäßig auf die FXOS-CLI-CLI eingestellt. Verwenden Sie die folgenden seriellen Einstellungen:

- 9.600 Baud
- 8 Daten-Bits
- Keine Parität
- 1 Stopp-Bit

Sie stellen eine Verbindung zum FXOS-CLI her. Melden Sie sich bei der CLI mit dem Benutzernamen **admin** und dem Kennwort an, das Sie bei der Ersteinrichtung festgelegt haben (der Standardwert ist **Admin123**).

Beispiel:

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

Schritt 2 Greifen Sie auf die Threat Defense-CLI zu.

connect ftd

Beispiel:

```
firepower# connect ftd
>
```

Geben Sie nach der Anmeldung **help** oder **?** ein, um Informationen zu den Befehlen aufzurufen, die in der CLI verfügbar sind. Informationen zur Verwendung finden Sie unter Befehlsreferenz für Secure Firewall Threat Defense.

Schritt 3 Um die Threat Defense-CLI zu verlassen, geben Sie den Befehl **exit** oder **logout** ein.

Mit diesem Befehl kehren Sie zur FXOS-CLI-CLI-Eingabeaufforderung zurück. Geben Sie **?** ein, um Informationen zu den Befehlen aufzurufen, die in der FXOS-CLI-CLI verfügbar sind.

Beispiel:

```
> exit
firepower#
```

Fehlerbehebung in Bezug auf die Managementkonnektivität auf einer Datenschnittstelle

Unterstützung von Modellen: Threat Defense

Falls Sie eine Datenschnittstelle für Management Center anstelle der dedizierten Management-Schnittstelle verwenden, müssen Sie vorsichtig sein, wenn Sie die Schnittstellen- und Netzwerkeinstellungen für Threat Defense im Management Center ändern, damit die Verbindung nicht unterbrochen wird. Wenn Sie den Typ der Management-Schnittstelle ändern, nachdem Sie Threat Defense zum Management Center hinzugefügt haben (von der Daten- zur Management-Schnittstelle oder umgekehrt), kann die Managementkonnektivität verloren gehen, falls die Schnittstellen- und Netzwerkeinstellungen nicht richtig konfiguriert sind.

Dieses Thema hilft Ihnen bei der Behebung des Verlusts der Managementkonnektivität.

Zeigen Sie den Status der Managementverbindung an

Überprüfen Sie in Management Center den Status der Managementverbindung auf der Seite **Devices** > **Device Management** > **Device** > **Management** > **FMC Access Details** > **Connection Status** (Geräte > Gerätemanagement > Gerät > Management > FMC-Zugriffsdetails > Verbindungsstatus).

Geben Sie in der Threat Defense-CLI den Befehl **sftunnel-status-brief** ein, um den Status der Managementverbindung anzuzeigen. Sie können auch **sftunnel-status** verwenden, um umfassendere Informationen aufzurufen.

Sehen Sie sich die folgende Beispielausgabe für eine ausgefallene Verbindung an; es werden weder Informationen bezüglich einer hergestellten Verbindung zum Peer-Kanal noch Heartbeat-Informationen angezeigt:

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

Sehen Sie sich die folgende Beispielausgabe für eine aktive Verbindung an. Dort werden Peer-Channel- und Heartbeat-Informationen angezeigt:

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

Anzeigen der Threat Defense-Netzwerkinformationen

Zeigen Sie in der Threat Defense-CLI die Netzwerkeinstellungen der Management- und Management Center-Zugriffsdatenschnittstellen an:

show network

```
> show network
===============[ System Information ]===============
Hostname                  : 5516X-4
DNS Servers               : 208.67.220.220,208.67.222.222
Management port           : 8305
IPv4 Default route
  Gateway                 : data-interfaces
IPv6 Default route
  Gateway                 : data-interfaces

======================[ br1 ]======================
State                     : Enabled
Link                      : Up
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
MAC Address               : 28:6F:7F:D3:CB:8D
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.99.10.4
Netmask                   : 255.255.255.0
Gateway                   : 10.99.10.1
----------------------[ IPv6 ]----------------------
Configuration             : Disabled

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

======[ System Information - Data Interfaces ]======
DNS Servers               :
Interfaces                : GigabitEthernet1/1

===============[ GigabitEthernet1/1 ]===============
State                     : Enabled
Link                      : Up
Name                      : outside
MTU                       : 1500
MAC Address               : 28:6F:7F:D3:CB:8F
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.89.5.29
Netmask                   : 255.255.255.192
Gateway                   : 10.89.5.1
----------------------[ IPv6 ]----------------------
Configuration             : Disabled
```

Überprüfen Sie, ob Threat Defense beim Management Center registriert ist.

Überprüfen Sie in der Threat Defense-CLI, ob die Management Center-Registrierung abgeschlossen wurde. Beachten Sie, dass dieser Befehl nicht den *aktuellen* Status der Managementverbindung anzeigt.

show managers

```
> show managers
Type                      : Manager
Host                      : 10.89.5.35
Registration              : Completed

>
```

Anpingen des Management Center

Verwenden Sie in der Threat Defense-CLI den folgenden Befehl, um das Management Center von den Datenschnittstellen aus anzupingen:

ping *FMC-IP*

Verwenden Sie in der Threat Defense-CLI den folgenden Befehl, um das Management Center von der Management-Schnittstelle aus anzupingen; die Route sollte über die Backplane zu den Datenschnittstellen führen:

ping system *FMC-IP*

Erfassen von Paketen auf der internen Threat Defense-Schnittstelle

Erfassen Sie in der Threat Defense-CLI Pakete auf der internen Backplane-Schnittstelle (nlp_int_tap), um zu sehen, ob Managementpakete gesendet werden:

capture *Name* **interface nlp_int_tap trace detail match ip any any**

show capture*Name* **trace detail**

Überprüfen Sie den Status der internen Schnittstelle, die Statistiken und die Paketanzahl

In der Threat Defense-CLI finden Sie Informationen zur internen Backplane-Schnittstelle nlp_int_tap:

show interace detail

```
> show interface detail
[...]
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
  Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
 (Full-duplex), (1000 Mbps)
 Input flow control is unsupported, output flow control is unsupported
 MAC address 0000.0100.0001, MTU 1500
 IP address 169.254.1.1, subnet mask 255.255.255.248
 37 packets input, 2822 bytes, 0 no buffer
 Received 0 broadcasts, 0 runts, 0 giants
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 0 pause input, 0 resume input
 0 L2 decode drops
 5 packets output, 370 bytes, 0 underruns
 0 pause output, 0 resume output
 0 output errors, 0 collisions, 0 interface resets
 0 late collisions, 0 deferred
 0 input reset drops, 0 output reset drops
 input queue (blocks free curr/low): hardware (0/0)
 output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "nlp_int_tap":
 37 packets input, 2304 bytes
 5 packets output, 300 bytes
 37 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
 Interface number is 14
 Interface config status is active
 Interface state is active
```

Überprüfen Sie das Routing und die NAT

Überprüfen Sie in der Threat Defense-CLI, ob die Standardroute (S*) hinzugefügt wurde und ob interne NAT-Regeln für die Management-Schnittstelle (nlp_int_tap) vorhanden sind.

show route

```
> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-ISinter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is 10.89.5.1 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 10.89.5.1, outside
C        10.89.5.0 255.255.255.192 is directly connected, outside
L        10.89.5.29 255.255.255.255 is directly connected, outside

>
```

show nat

```
> show nat

Auto NAT Policies (Section 2)
1 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_intf3 interface  service
 tcp 8305 8305
    translate_hits = 0, untranslate_hits = 6
2 (nlp_int_tap) to (outside) source static nlp_server_0_ssh_intf3 interface  service
tcp ssh ssh
    translate_hits = 0, untranslate_hits = 73
3 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_ipv6_intf3 interface
ipv6  service tcp 8305 8305
    translate_hits = 0, untranslate_hits = 0
4 (nlp_int_tap) to (outside) source dynamic nlp_client_0_intf3 interface
    translate_hits = 174, untranslate_hits = 0
5 (nlp_int_tap) to (outside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6
    translate_hits = 0, untranslate_hits = 0
>
```

Überprüfen Sie sonstige Einstellungen

Überprüfen Sie mit folgenden Befehlen, ob alle anderen Einstellungen vorhanden sind. Sie finden viele dieser Befehle auch auf der Management Center-Seite **Devices** > **Device Management** > **Device** > **Management** > **FMC Access Details** > **CLI Output** (Geräte > Gerätemanagement > Gerät > Management > FMC-Zugriffsdetails > CLI-Ausgabe).

show running-config sftunnel

```
> show running-config sftunnel
sftunnel interface outside
sftunnel port 8305
```

show running-config ip-client

```
> show running-config ip-client
ip-client outside
```

show conn address *FMC-IP*

```
> show conn address 10.89.5.35
5 in use, 16 most used
Inspect Snort:
        preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

TCP nlp_int_tap  10.89.5.29(169.254.1.2):51231 outside  10.89.5.35:8305, idle 0:00:04,
 bytes 86684, flags UxIO
TCP nlp_int_tap  10.89.5.29(169.254.1.2):8305 outside  10.89.5.35:52019, idle 0:00:02,
 bytes 1630834, flags UIO
>
```

Suchen Sie nach einer erfolgreichen DDNS-Aktualisierung

Suchen Sie in der Threat Defense-CLI nach einer erfolgreichen DDNS-Aktualisierung:

debug ddns

```
> debug ddns
DDNS update request = /v3/update?hostname=domain.example.org&myip=209.165.200.225
Successfuly updated the DDNS sever with current IP addresses
DDNS: Another update completed, outstanding = 0
DDNS: IDB SB total = 0
```

Wenn die Aktualisierung fehlgeschlagen ist, verwenden Sie die Befehle **debug http** und **debug ssl**. Überprüfen Sie bei fehlgeschlagenen Zertifikatsüberprüfungen, ob die Stammzertifikate auf dem Gerät installiert sind:

show crypto ca certificates *Trust-Point-Name*

So überprüfen Sie den DDNS-Betrieb:

show ddns update interface *fmc_access_ifc_name*

```
> show ddns update interface outside

Dynamic DNS Update on outside:
    Update Method Name Update Destination
    RBD_DDNS not available

Last Update attempted on 04:11:58.083 UTC Thu Jun 11 2020
Status : Success
FQDN : domain.example.org
IP addresses : 209.165.200.225
```

Überprüfen der Management Center-Protokolldateien

Weitere Informationen finden Sie unter https://cisco.com/go/fmc-reg-error.

Rollback der Konfiguration bei unterbrochener Management Center-Konnektivität

Wenn Sie eine Datenschnittstelle auf dem Threat Defense-System für den Management Center verwenden und eine Konfigurationsänderung über Management Center bereitstellen, die sich auf die Netzwerkkonnektivität auswirkt, können Sie die Konfiguration auf dem Threat Defense-System mit einem Rollback auf die zuletzt bereitgestellte Konfiguration zurücksetzen, um die Managementkonnektivität wiederherzustellen. Sie können dann die Konfigurationseinstellungen in Management Center anpassen, damit die Netzwerkkonnektivität erhalten bleibt, und diese erneut bereitstellen. Sie können die Rollback-Funktion auch verwenden, wenn die Verbindung nicht unterbrochen wird. Sie ist nicht auf diese Situation der Fehlerbehebung beschränkt.

Beachten Sie die folgenden Orientierungshilfen:

- Nur die vorherige Bereitstellung ist lokal auf der Threat Defense-Instanz verfügbar. Sie können kein Rollback zu früheren Bereitstellungen durchführen.
- Das Rollback wird für Hochverfügbarkeits- oder Cluster-Bereitstellungen nicht unterstützt.
- Das Rollback betrifft nur Konfigurationen, die Sie in Management Center festlegen können. Beispiel: Das Rollback wirkt sich nicht auf lokale Konfigurationen im Zusammenhang mit der dedizierten Management-Schnittstelle aus, die Sie nur über die Threat Defense-CLI konfigurieren können. Hinweis: Wenn Sie die Datenschnittstelleneinstellungen nach der letzten Management Center-Bereitstellung mit dem Befehl **configure network management-data-interface** geändert haben und dann den Rollback-Befehl verwenden, werden diese Einstellungen nicht beibehalten. Sie werden stattdessen auf die zuletzt bereitgestellten Management Center-Einstellungen zurückgesetzt.
- Der UCAPL/CC-Modus kann nicht zurückgesetzt werden.
- Out-of-Band-SCEP-Zertifikatdaten, die während der vorherigen Bereitstellung aktualisiert wurden, können nicht zurückgesetzt werden.
- Während des Rollbacks werden die Verbindungen getrennt, da die aktuelle Konfiguration gelöscht wird.

Vorbereitungen

Unterstützung von Modellen: Threat Defense

Prozedur

Schritt 1 Führen Sie in der Threat Defense-CLI ein Rollback zur vorherigen Konfiguration durch.

configure policy rollback

Nach dem Rollback benachrichtigt Threat Defense das Management Center, dass das Rollback erfolgreich abgeschlossen wurde. In Management Center wird im Bereitstellungsbildschirm ein Banner angezeigt, das besagt, dass die Konfiguration zurückgesetzt wurde.

Wenn das Rollback fehlgeschlagen ist, lesen Sie https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.html. Dort finden Sie eine Beschreibung gängiger Bereitstellungsprobleme. In einigen Fällen kann das Rollback fehlschlagen, nachdem der Management Center-Zugriff wiederhergestellt wurde. In diesem Fall können Sie die Management Center-Konfigurationsprobleme lösen und die Bereitstellung über Management Center erneut durchführen.

Beispiel:

```
> configure policy rollback

The last deployment to this FTD was on June 1, 2020 and its status was Successful.
Do you want to continue [Y/N]?

Y

Rolling back complete configuration on the FTD. This will take time.
.....................
Policy rollback was successful on the FTD.
Configuration has been reverted back to transaction id:
Following is the rollback summary:
...................
.....................
>
```

Schritt 2 Überprüfen Sie, ob die Managementverbindung wiederhergestellt wurde.

Überprüfen Sie in Management Center den Status der Managementverbindung auf der Seite **Devices** > **Device Management** > **Device** > **Management** > **FMC Access Details** > **Connection Status** (Geräte > Gerätemanagement > Gerät > Management > FMC-Zugriffsdetails > Verbindungsstatus).

Geben Sie in der Threat Defense-CLI den Befehl **sftunnel-status-brief** ein, um den Status der Managementverbindung anzuzeigen.

Wenn die Wiederherstellung der Verbindung länger als zehn Minuten dauert, sollten Sie eine Fehlerbehebung durchführen. Siehe Fehlerbehebung in Bezug auf die Managementkonnektivität auf einer Datenschnittstelle, auf Seite 86.

Ausschalten der Firewall über die Management Center

Es ist wichtig, dass Sie Ihr System ordnungsgemäß herunterfahren. Wenn Sie einfach den Netzstecker ziehen oder den Netzschalter drücken, kann das Dateisystem ernsthaft beschädigt werden. Denken Sie daran, dass im Hintergrund ständig viele Prozesse ablaufen, und dass das Ziehen des Netzsteckers oder das Ausschalten der Stromversorgung kein ordnungsgemäßes Herunterfahren Ihrer Firewall ermöglicht.

Sie können Ihr System mithilfe von Management Center ordnungsgemäß herunterfahren.

Prozedur

Schritt 1 Wählen Sie **Devices** > **Device Management** (Geräte > Gerätemanagement) aus.

Schritt 2 Klicken Sie neben dem Gerät, das Sie neu starten möchten, auf das Bearbeitungssymbol ( ).

Schritt 3 Klicken Sie auf die Registerkarte **Device** (Gerät).

Schritt 4 Klicken Sie im Abschnitt **System** auf das Symbol zum Herunterfahren des Geräts ( ).

Schritt 5 Bestätigen Sie bei Aufforderung, dass Sie das Gerät herunterfahren möchten.

Schritt 6 Wenn Sie über eine Konsolenverbindung zur Firewall verfügen, prüfen Sie die Systemaufforderungen, wenn die Firewall heruntergefahren wird. Die folgende Aufforderung wird angezeigt:

```
System is stopped.
```

```
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

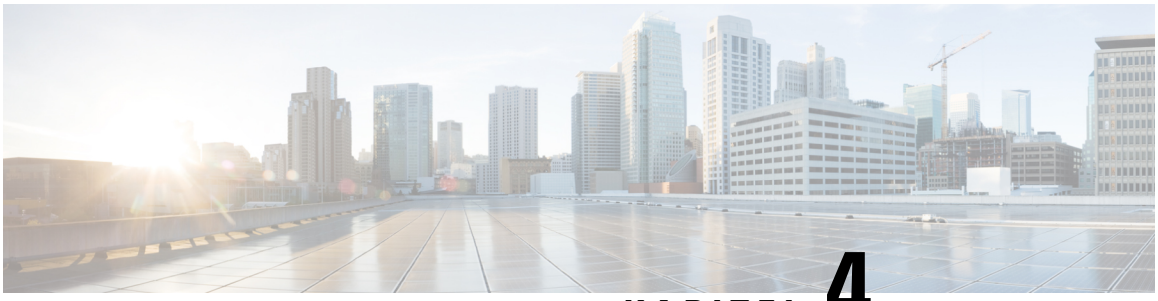
Wenn Sie keine Konsolenverbindung haben, warten Sie circa 3 Minuten, um sicherzustellen, dass das System heruntergefahren wurde.

Schritt 7 Sie können jetzt den Netzstecker ziehen, um die Stromversorgung des Chassis bei Bedarf physisch zu trennen.

Nächste Schritte

Um die Konfiguration von Threat Defense fortzusetzen, lesen Sie die Dokumente, die für Ihre Softwareversion verfügbar sind. Siehe Navigation in der Cisco Firepower-Dokumentation.

Informationen zur Verwendung des Management Center finden Sie im Konfigurationsleitfaden für Firepower Management Center.



KAPITEL 4

Threat Defense Bereitstellung mit Device Manager

Enthält dieses Kapitel die Informationen, nach denen Sie suchen?

Alle verfügbaren Betriebssysteme und Manager finden Sie unter Welche Betriebssysteme und Manager sind für Sie geeignet?, auf Seite 1. Dieses Kapitel gilt für Threat Defense mit Device Manager.

In diesem Kapitel wird erläutert, wie Sie die Ersteinrichtung und -konfiguration Ihres Threat Defense-Geräts mithilfe des webbasierten Geräteeinrichtungsassistenten ausführen

In Device Manager können Sie die grundlegenden Funktionen der Software konfigurieren, die am häufigsten für kleine Netzwerke verwendet werden. Diese Komponente wurde speziell für Netzwerke entwickelt, die nur ein einziges oder einige wenige Geräte umfassen und in denen Sie keinen leistungsstarken Manager für mehrere Geräte verwenden möchten, um ein großes Netzwerk mit vielen Device Manager-Geräten zu steuern.

Informationen zur Firewall

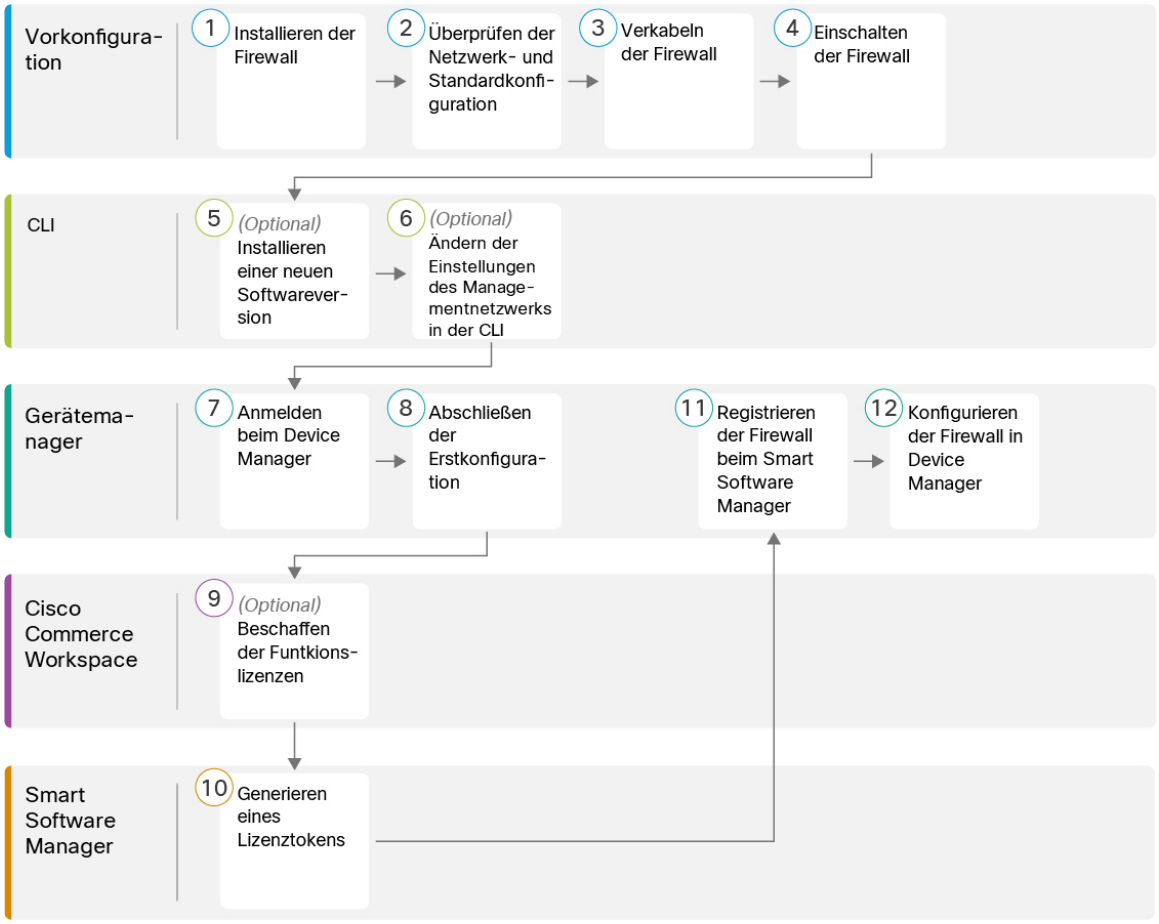
Auf der Hardware kann entweder Threat Defense-Software oder ASA-Software ausgeführt werden. Beim Wechsel zwischen Threat Defense und ASA müssen Sie ein neues Image des Geräts erstellen. Sie sollten auch ein neues Image erstellen, wenn Sie eine andere Softwareversion als derzeit installiert benötigen. Weitere Informationen hierzu finden Sie unter Reimage the Cisco ASA or Firepower Threat Defense Device (Erstellen eines neuen Images für Cisco ASA oder Firepower Threat Defense-Gerät).

Die Firewall führt ein zugrunde liegendes Betriebssystem namens Secure Firewall Extensible Operating System (FXOS) aus. Die Firewall unterstützt die FXOS-Secure Firewall Chassis Manager nicht. Es wird nur in begrenztem Umfang eine CLI für Fehlerbehebungszwecke unterstützt. Weitere Informationen finden Sie unter Cisco FXOS-Leitfaden zur Fehlerbehebung für die Firepower 1000/2100-Serie mit Firepower Threat Defense.

Datenschutzerklärung zur Datenerfassung: Die Firewall erfordert keine personenbezogenen Informationen und nimmt keine aktive Erfassung derartiger Informationen vor. Sie können jedoch personenbezogene Informationen in der Konfiguration verwenden, z. B. bei Benutzernamen. In diesem Fall kann ein Administrator diese Informationen möglicherweise sehen, wenn er mit der Konfiguration arbeitet oder SNMP verwendet.

Vollständiges Verfahren

Lesen Sie die folgenden Aufgaben zur Bereitstellung von Threat Defense mit Device Manager auf Ihrem Chassis.



1	Vorkonfiguration	Installieren der Firewall. Weitere Informationen finden Sie im Hardware-Installationshandbuch.
2	Vorkonfiguration	Überprüfen der Netzwerkbereitstellung und Standardkonfiguration, auf Seite 97

3	Vorkonfiguration	Verkabeln des Geräts, auf Seite 101
4	Vorkonfiguration	Einschalten der Firewall, auf Seite 13
5	CLI	(Optional) Prüfen der Software und Installieren einer neuen Version, auf Seite 103
6	CLI	(Optional) Ändern der Einstellungen des Managementnetzwerks in der CLI, auf Seite 104
7	Device Manager	Anmelden bei Device Manager, auf Seite 107
8	Device Manager	Abschließen der Erstkonfiguration, auf Seite 107
9	Cisco Commerce Workspace	(Optional) Konfigurieren der Lizenzierung, auf Seite 109: Beschaffen Sie sich Funktionslizenzen.
10	Smart Software Manager	Konfigurieren der Lizenzierung, auf Seite 109: Generieren Sie ein Lizenztoken.
11	Device Manager	Konfigurieren der Lizenzierung, auf Seite 109: Registrieren Sie das Gerät beim Smart Licensing-Server.
12	Device Manager	Konfigurieren der Firewall in Device Manager, auf Seite 115

Überprüfen der Netzwerkbereitstellung und Standardkonfiguration

Sie können Threat Defense mit Device Manager entweder über die Schnittstelle Management 1/1 oder über die interne Schnittstelle verwalten. Die dedizierte Management-Schnittstelle ist eine spezielle Schnittstelle mit eigenen Netzwerkeinstellungen.

Die folgende Abbildung zeigt die empfohlene Netzwerkbereitstellung. Wenn Sie die externe Schnittstelle direkt mit einem Kabelmodem oder DSL-Modem verbinden, empfehlen wir, das Modem in den Bridge-Modus zu versetzen, damit Threat Defense das gesamte Routing und die NAT für Ihre internen Netzwerke übernimmt. Falls Sie PPPoE für die externe Schnittstelle konfigurieren müssen, um eine Verbindung zu Ihrem ISP herzustellen, können Sie dies tun, nachdem Sie die Ersteinrichtung in Device Manager abgeschlossen haben.

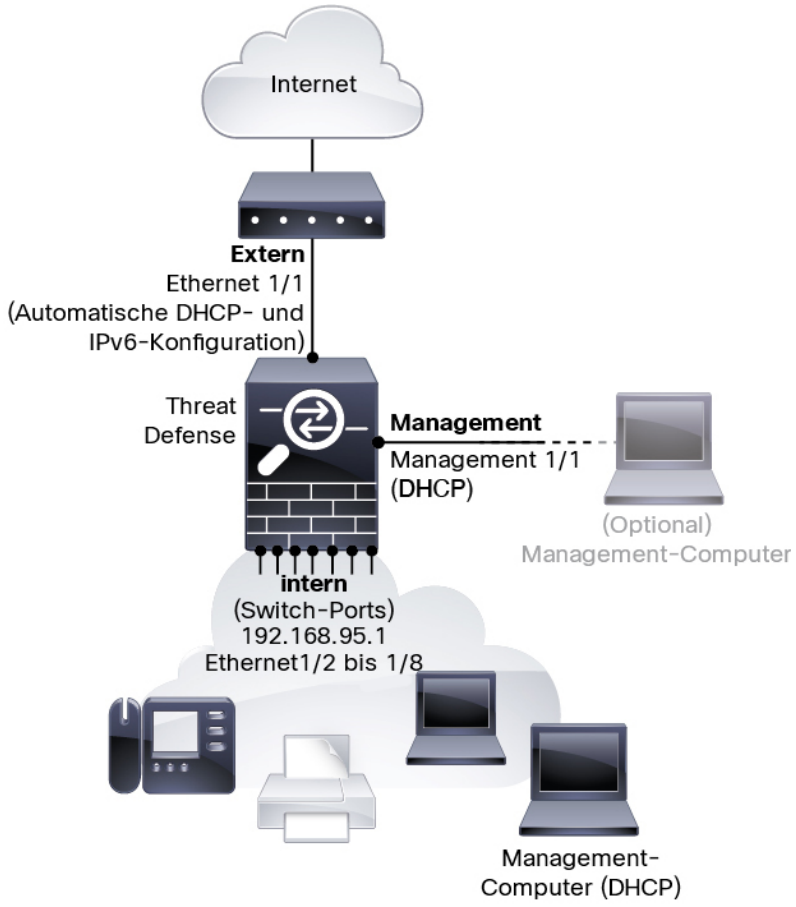
Hinweis Wenn Sie die standardmäßige Management-IP-Adresse nicht verwenden können (da Ihr Managementnetzwerk keinen DHCP-Server enthält), können Sie sich mit dem Konsolenport verbinden und die Ersteinrichtung über die CLI durchführen. Dies umfasst auch die Festlegung der Management-IP-Adresse, des Gateways und anderer grundlegender Netzwerkeinstellungen.

Wenn Sie die interne IP-Adresse ändern müssen, können Sie dies tun, nachdem Sie die Ersteinrichtung in Device Manager abgeschlossen haben. Beispielsweise kann es unter folgenden Umständen erforderlich sein, die interne IP-Adresse zu ändern:

- (Ab Version 7.0) Die interne IP-Adresse lautet 192.168.95.1.(Version 6.7 und früher) Die interne IP-Adresse lautet 192.168.1.1. Wenn die externe Schnittstelle versucht, eine IP-Adresse im Netzwerk 192.168.1.0, einem gängigen Standardnetzwerk, abzurufen, schlägt das DHCP-Lease fehl, und die externe Schnittstelle erhält keine IP-Adresse. Dieses Problem tritt auf, weil es bei Threat Defense keine zwei Schnittstellen im selben Netzwerk geben kann. In diesem Fall müssen Sie die interne IP-Adresse ändern, damit ein neues Netzwerk genutzt wird.
- Wenn Sie Threat Defensezu einem vorhandenen internen Netzwerk hinzufügen, müssen Sie die interne IP-Adresse ändern, damit sie sich im vorhandenen Netzwerk befindet.

Die folgende Abbildung zeigt die Standardnetzwerkbereitstellung für Threat Defense mit Device Manager unter Verwendung der Standardkonfiguration.

Abbildung 25: Empfohlene Netzwerkbereitstellung



Hinweis Bei Version 6.7 und früheren Versionen lautet die interne IP-Adresse von 192.168.1.1.

Bei Version 6.5 und früheren Versionen lautet die Standard-IP-Adresse von Management 1/1 192.168.45.45.

Standardkonfiguration

Die Konfiguration für die Firewall nach der Ersteinrichtung umfasst Folgendes:

- **intern**—IP-Adresse (7.0 und höher) 192.168.95.1; (vor 7.0) 192.168.1.1.
  - (6.5 und höher) **Hardware-Switch**: Ethernet 1/2 bis 1/8 gehören zu VLAN 1
  - (6.4) **Software-Switch** (Integriertes Routing und Bridging): Ethernet 1/2 bis 1/8 gehören zur Bridge Group Interface (BVI) 1
- **extern**: Ethernet 1/1, IP-Adresse aus IPv4-DHCP und automatische IPv6-Konfiguration
- **intern→extern** Traffic-Fluss
- **Management**: Management 1/1 (Management)

- (6.6 und höher) IP-Adresse von DHCP
- (6.5 und früher) IP-Adresse 192.168.45.45

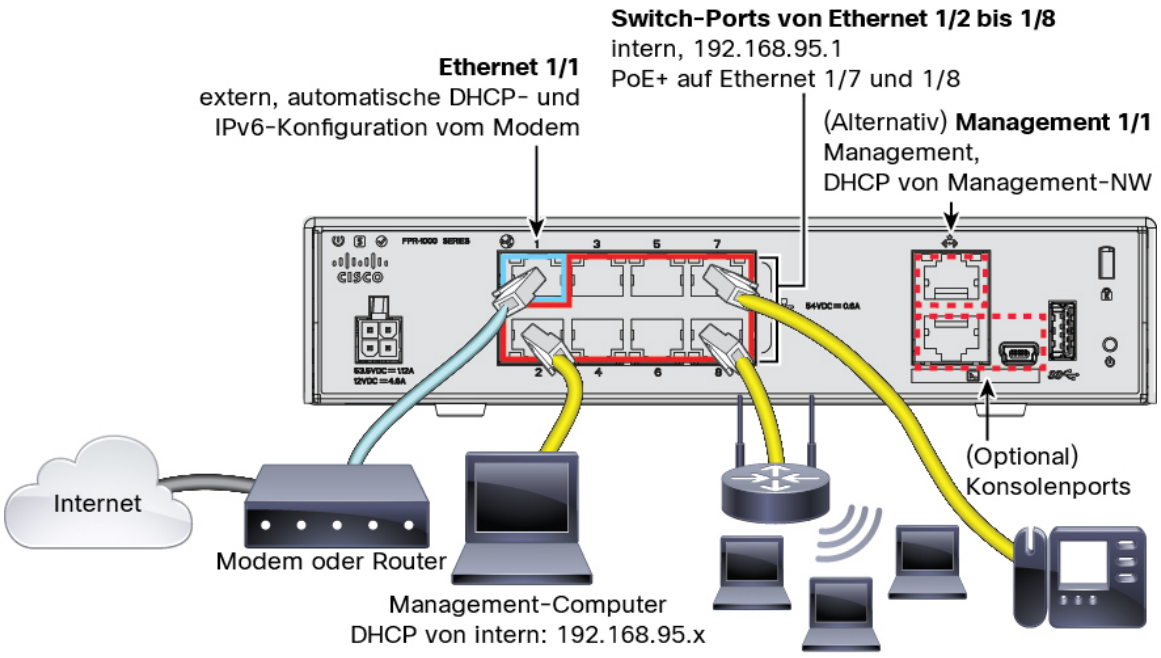
Hinweis Die Schnittstelle Management 1/1 ist eine spezielle, von Datenschnittstellen getrennte Schnittstelle, die für das Management, Smart Licensing und Datenbankaktualisierungen verwendet wird. Die physische Schnittstelle wird mit einer zweiten logischen Schnittstelle gemeinsam verwendet, der Diagnoseschnittstelle („Diagnostic“). Diagnostic ist eine Datenschnittstelle, die jedoch auf andere Arten von Management-Traffic (zum Gerät und vom Gerät) beschränkt ist, z. B. Syslog oder SNMP. Die Diagnoseschnittstelle wird normalerweise nicht verwendet. Weitere Informationen finden Sie unter Konfigurationsleitfaden für Cisco Secure Firewall Device Manager.

- **DNS-Server für das Management**: OpenDNS: (IPv4) 208.67.222.222, 208.67.220.220; (IPv6) 2620:119:35::35 oder Server, die Sie bei der Einrichtung angegeben haben. Von DHCP bezogene DNS-Server werden niemals verwendet.
- **NTP**: Cisco NTP-Server: 0.sourcefire.pool.ntp.org, 1.sourcefire.pool.ntp.org, 2.sourcefire.pool.ntp.org oder Server, die Sie bei der Einrichtung angegeben haben.
- **Standardrouten**
  - **Datenschnittstellen**: Von externem DHCP bezogen, oder eine Gateway-IP-Adresse, die Sie bei der Einrichtung angegeben haben
  - **Management-Schnittstelle**: (6.6 und höher) Abgerufen vom Management-DHCP. Wenn Sie kein Gateway erhalten, führt die Standardroute über die Backplane und über die Datenschnittstellen. (6.5 und früher) Über die Backplane und über die Datenschnittstellen

    Beachten Sie, dass die Management-Schnittstelle für die Lizenzierung und Updates Internetzugriff erfordert, entweder über die Backplane oder über ein separates Internet-Gateway. Beachten Sie, dass nur Traffic, der von der Management-Schnittstelle stammt, über die Backplane geleitet werden kann. Andernfalls lässt Management keinen Durchgangs-Traffic für Traffic zu, der über das Netzwerk in Management gelangt.
- **DHCP-Server**: Aktiviert auf der internen Schnittstelle und (nur 6.5 und früher) Management-Schnittstelle
- **Device Manager-Zugriff**: Alle Hosts sind auf Management- und internen Schnittstellen zulässig.
- **NAT**: Schnittstellen-PAT für sämtlichen Traffic von innen nach außen

Verkabeln des Geräts

Abbildung 26: Verkabelung des Firepower 1010-Geräts



Hinweis Bei 6.7 und früheren Versionen lautet die interne IP-Adresse 192.168.1.1.

Bei Version 6.5 und früheren Versionen lautet die Standard-IP-Adresse von Management 1/1 192.168.45.45.

Hinweis Ab Version 6.5 sind Ethernet1/2 bis 1/8 als Hardware-Switch-Ports konfiguriert. PoE+ ist auch für Ethernet1/7 und 1/8 verfügbar. In Version 6.4 sind Ethernet1/2 bis 1/8 als Bridge-Gruppenmitglieder (Software-Switch-Ports) konfiguriert. PoE+ ist nicht verfügbar. Die Erstverkabelung ist bei beiden Versionen identisch.

Verwalten Sie das Firepower 1010-System entweder auf Management 1/1 oder Ethernet 1/2 bis 1/8. Die Standardkonfiguration konfiguriert Ethernet1/1 auch als extern.

Prozedur

Schritt 1 Installieren Sie die Hardware, und machen Sie sich mit der Hardware-Installationsanleitung vertraut.

Schritt 2 Verbinden Sie Ihren Management-Computer mit einer der folgenden Schnittstellen:

- Ethernet 1/2 bis 1/8: Verbinden Sie Ihren Management-Computer direkt mit einem der internen Switch-Ports (Ethernet 1/2 bis 1/8). Die interne Schnittstelle hat eine Standard-IP-Adresse (192.168.95.1) und führt auch einen DHCP-Server aus, um IP-Adressen für Clients (einschließlich des

Management-Computers) bereitzustellen. Stellen Sie daher sicher, dass diese Einstellungen nicht mit vorhandenen internen Netzwerkeinstellungen in Konflikt stehen (siehe Standardkonfiguration, auf Seite 99).

- Management 1/1 (mit MGMT gekennzeichnet):Verbinden Sie Management 1/1 mit Ihrem Managementnetzwerk, und stellen Sie sicher, dass sich Ihr Management-Computer im Managementnetzwerk befindet oder Zugriff darauf hat. Management 1/1 erhält eine IP-Adresse von einem DHCP-Server in Ihrem Managementnetzwerk. Wenn Sie diese Schnittstelle verwenden, müssen Sie die IP-Adresse ermitteln, die Threat Defense zugewiesen ist, damit Sie sich von Ihrem Management-Computer aus mit der IP-Adresse verbinden können.

  Wenn Sie die Standard-IP-Adresse für Management 1/1 ändern müssen, um eine statische IP-Adresse zu konfigurieren, müssen Sie auch Ihren Management-Computer mit dem Konsolenport verkabeln. Siehe (Optional) Ändern der Einstellungen des Managementnetzwerks in der CLI, auf Seite 104.

Schritt 3 Verbinden Sie das externe Netzwerk mit der Ethernet 1/1-Schnittstelle.

Standardmäßig wird die IP-Adresse mit der automatischen Konfiguration von IPv4-DHCP und IPv6 bezogen, Sie können aber während der Erstkonfiguration eine statische Adresse festlegen.

Schritt 4 Verbinden Sie interne Geräte mit den verbleibenden Switch-Ports (Ethernet 1/2 bis 1/8).

Ethernet 1/7 und 1/8 sind PoE+-Ports.

Einschalten der Firewall

Die Systemstromversorgung wird über das Netzkabel gesteuert. Es gibt keinen Netzschalter.

Hinweis Wenn Sie den Threat Defense zum ersten Mal starten, kann die Initialisierung etwa 15 bis 30 Minuten dauern.

Vorbereitungen

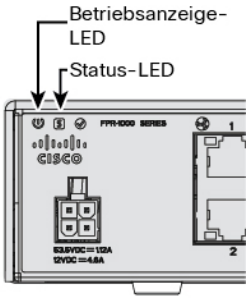
Es ist wichtig, dass Sie Ihr Gerät zuverlässig mit Strom versorgen (z. B. mit einer unterbrechungsfreien Stromversorgung (USV)). Ein Stromausfall ohne vorheriges Herunterfahren kann zu ernsthaften Schäden am Dateisystem führen. Im Hintergrund laufen ständig viele Prozesse ab, und eine Unterbrechung der Stromversorgung ermöglicht kein ordnungsgemäßes Herunterfahren des Systems.

Prozedur

Schritt 1 Schließen Sie das Netzkabel am Gerät und dann an einer Steckdose an.

Wenn Sie das Netzkabel an die Stromversorgung anschließen, ist das Gerät automatisch eingeschaltet.

Schritt 2 Prüfen Sie die Betriebs-LED auf der Rückseite oder Oberseite des Geräts; leuchtet sie dauerhaft grün, ist das Gerät eingeschaltet.



Schritt 3 Prüfen Sie die Status-LED auf der Rückseite oder Oberseite des Geräts; wenn sie dauerhaft grün leuchtet, hat das System die Einschaltdiagnose durchlaufen.

(Optional) Prüfen der Software und Installieren einer neuen Version

Gehen Sie wie folgt vor, um die Softwareversion zu überprüfen und ggf. eine andere Version zu installieren. Wir empfehlen, dass Sie Ihre Zielversion installieren, bevor Sie die Firewall konfigurieren. Alternativ können Sie ein Upgrade im Anschluss an die Inbetriebnahme durchführen. Ein Upgrade, bei dem Ihre Konfiguration erhalten bleibt, kann jedoch länger dauern als dieses Verfahren.

Welche Version sollte ich ausführen?

Cisco empfiehlt, eine Gold Star-Version auszuführen, die durch einen goldenen Stern neben der Versionsnummer auf der Software-Download-Seite gekennzeichnet ist. Sie können sich auch auf die Release-Strategie beziehen, die in https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html beschrieben ist. Beispielsweise beschreibt dieses Bulletin die Nummerierung von kurzfristigen Releases (mit den neuesten Funktionen), die Nummerierung von langfristigen Releases (Wartungsversionen und Patches für einen längeren Zeitraum) oder die Nummerierung von extra langfristigen Releases (Wartungsversionen und Patches für den längsten Zeitraum für die staatliche Zertifizierung).

Prozedur

Schritt 1 Stellen Sie eine Verbindung zur CLI her. Weitere Informationen finden Sie unter Zugriff auf die Threat Defense- und FXOS-CLI, auf Seite 119. Dieses Verfahren zeigt die Verwendung des Konsolenports, aber Sie können stattdessen SSH verwenden.

Melden Sie sich mit dem Benutzer **admin** und dem Standardkennwort **Admin123** an.

Sie stellen eine Verbindung zum FXOS-CLI her. Wenn Sie sich zum ersten Mal anmelden, werden Sie aufgefordert, das Kennwort zu ändern. Dieses Kennwort wird auch zur Threat Defense-Anmeldung für SSH verwendet.

Hinweis Wenn das Kennwort bereits geändert wurde und Sie es nicht kennen, müssen Sie das Gerät auf die Werkseinstellungen zurücksetzen, um das Kennwort auf den Standardwert zurückzusetzen. Weitere Informationen hierzu finden Sie im Abschnitt über das Verfahren zum Zurücksetzen auf die Werkseinstellungen im Handbuch zur FXOS-Fehlerbehebung.

Beispiel:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

Schritt 2 Zeigen Sie in der FXOS-CLI die aktuelle Version an.

scope ssa

show app-instance

Beispiel:

```
Firepower# scope ssa
Firepower /ssa # show app-instance

Application Name     Slot ID    Admin State     Operational State    Running Version Startup
 Version Cluster Oper State
-------------------- ---------- --------------- -------------------- ---------------
--------------- ------------------
ftd                  1          Enabled         Online               7.2.0.65        7.2.0.65
        Not Applicable
```

Schritt 3 Wenn Sie eine neue Version installieren möchten, führen Sie diese Schritte aus.

a) Informationen zum Festlegen einer statischen IP-Adresse für die Management-Schnittstelle finden Sie unter (Optional) Ändern der Einstellungen des Managementnetzwerks in der CLI, auf Seite 104. Standardmäßig verwendet die Managementschnittstelle DHCP.

Sie müssen das neue Image von einem Server herunterladen, auf den über die Managementschnittstelle zugegriffen werden kann.

b) Führen Sie das Verfahren zum Erstellen eines neuen Images im Handbuch zur FXOS-Fehlerbehebung durch.

(Optional) Ändern der Einstellungen des Managementnetzwerks in der CLI

Wenn Sie die Standard-Management-IP-Adresse nicht verwenden können, können Sie eine Verbindung zum Konsolenport herstellen und die Ersteinrichtung über die CLI durchführen. Dies umfasst auch die Festlegung der Management-IP-Adresse, des Gateways und anderer grundlegender Netzwerkeinstellungen. Sie können

nur die Einstellungen der Management-Schnittstelle konfigurieren. Sie können keine internen oder externen Schnittstellen konfigurieren. Dies ist später in der GUI möglich.

Hinweis Sie können das CLI-Einrichtungsskript nur wiederholen, wenn Sie die Konfiguration löschen, zum Beispiel im Rahmen der Neuerstellung eines Images. Alle diese Einstellungen können jedoch später in der CLI mit den Befehlen **configure network** geändert werden. Siehe Befehlsreferenz für Secure Firewall Threat Defense.

Prozedur

Schritt 1 Stellen Sie eine Verbindung zum Threat Defense-Konsolenport her. Weitere Informationen finden Sie unter Zugriff auf die Threat Defense- und FXOS-CLI, auf Seite 119.

Melden Sie sich mit dem Benutzer **admin** und dem Standardkennwort **Admin123** an.

Sie stellen eine Verbindung zur FXOS-CLI her. Wenn Sie sich zum ersten Mal anmelden, werden Sie aufgefordert, das Kennwort zu ändern. Dieses Kennwort wird auch zur Threat Defense-Anmeldung für SSH verwendet.

Hinweis Wenn das Kennwort bereits geändert wurde und Sie es nicht kennen, müssen Sie ein neues Image des Geräts erstellen, um das Kennwort auf den Standardwert zurückzusetzen. Weitere Informationen hierzu finden Sie im Abschnitt über das Verfahren zum Erstellen eines neuen Images im Handbuch zur FXOS-Fehlerbehebung.

Beispiel:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

Schritt 2 Stellen Sie eine Verbindung zur Threat Defense-CLI her.

connect ftd

Beispiel:

```
firepower# connect ftd
>
```

Schritt 3 Wenn Sie sich zum ersten Mal bei Threat Defense anmelden, werden Sie aufgefordert, den Endbenutzerlizenzvertrag (EULA). Anschließend wird das CLI-Einrichtungsskript angezeigt.

Standardwerte oder zuvor eingegebene Werte werden in Klammern angezeigt. Um zuvor eingegebene Werte zu akzeptieren, drücken Sie die **Eingabetaste**.

Beachten Sie die folgenden Orientierungshilfen:

- **Geben Sie das IPv4-Standardgateway für die Management-Schnittstelle ein.** Wenn Sie eine manuelle IP-Adresse festlegen, geben Sie entweder **data-interfaces** oder die IP-Adresse des Gateway-Routers ein. Die Einstellung **data-interfaces** sendet ausgehenden Management-Traffic über die Backplane, um eine Datenschnittstelle zu verlassen. Diese Einstellung ist nützlich, wenn Sie kein separates Management-Netzwerk haben, das auf das Internet zugreifen kann. Traffic, der von der Management-Schnittstelle stammt, umfasst die Lizenzregistrierung und Datenbankaktualisierungen, die einen Internetzugang erfordern. Falls Sie **data-interfaces** verwenden, können Sie weiterhin Device Manager (oder SSH) auf der Management-Schnittstelle verwenden, wenn Sie direkt mit dem Management-Netzwerk verbunden sind. Für das Remote-Management für bestimmte Netzwerke oder Hosts sollten Sie eine statische Route mit dem Befehl **configure network static-routes** hinzufügen. Beachten Sie, dass das Device Manager-Management auf Datenschnittstellen von dieser Einstellung nicht betroffen ist. Wenn Sie DHCP verwenden, verwendet das System das von DHCP bereitgestellte Gateway und nutzt die **data-interfaces** als Fallback-Methode, wenn DHCP kein Gateway bereitstellt.
- **Wenn sich Ihre Netzwerkinformationen geändert haben, müssen Sie die Verbindung wiederherstellen.** Wenn Sie über SSH mit der Standard-IP-Adresse verbunden sind, aber die IP-Adresse bei der Ersteinrichtung ändern, wird die Verbindung getrennt. Verbinden Sie sich erneut mit der neuen IP-Adresse und dem Kennwort. Konsolenverbindungen sind nicht betroffen.
- **Manage the device locally?** (Das Gerät lokal verwalten?): Geben Sie **yes** (Ja) ein, um Device Manager oder CDO/Device Manager zu verwenden. Ein Nein (**no**) bedeutet, dass Sie das Management Center für das Management des Geräts verwenden möchten.

Beispiel:

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress.  Please stand by.
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]: 10.10.10.1
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: yes

>
```

Schritt 4 Melden Sie sich mit der neuen Management-IP-Adresse bei Device Manager an.

Anmelden bei Device Manager

Melden Sie sich bei Device Manager an, um Ihr Threat Defense zu konfigurieren.

Vorbereitungen

- Verwenden Sie eine aktuelle Version von Firefox, Chrome, Safari, Edge oder Internet Explorer.

Prozedur

Schritt 1 Geben Sie die folgende URL in Ihren Browser ein.

- (7.0 und höher) Intern (Ethernet1/2 bis 1/8)—**https://192.168.95.1**.Sie können an jedem internen Switch-Port (Ethernet1/2 bis 1/8) eine Verbindung zur internen Adresse herstellen.
- (6.7 und früher) Intern (Ethernet1/2 bis 1/8)—**https://192.168.1.1**.Sie können an jedem internen Switch-Port (Ethernet1/2 bis 1/8) eine Verbindung zur internen Adresse herstellen.
- (6.6 und höher) Management—**https://***Management-IP*. Da die Management-Schnittstelle ein DHCP-Client ist, hängt die IP-Adresse von Ihrem DHCP-Server ab. Wenn Sie die Management-IP-Adresse bei der CLI-Einrichtung geändert haben, geben Sie diese Adresse ein.
- (6.5 und früher) Management—**https://192.168.45.45**. Wenn Sie die Management-IP-Adresse bei der CLI-Einrichtung geändert haben, geben Sie diese Adresse ein.

Schritt 2 Melden Sie sich mit dem Benutzernamen **admin** und demStandardkennwort **Admin123** an.

Nächste Maßnahme

- Führen Sie die Schritte im Device Manager-Einrichtungsassistenten aus; siehe Abschließen der Erstkonfiguration, auf Seite 107.

Abschließen der Erstkonfiguration

Verwenden Sie bei der ersten Anmeldung in Device Manager den Einrichtungsassistenten, um die Erstkonfiguration abzuschließen. Nachdem Sie den Einrichtungsassistenten durchlaufen haben, sollten Sie über ein funktionsfähiges Gerät mit einigen grundlegenden Richtlinien verfügen:

- Eine externe Schnittstelle (Ethernet1/1) und eine interne Schnittstelle. Ethernet1/2 bis 1/8 sind Switch-Ports auf der internen VLAN1-Schnittstelle (6.5 und höher) oder Mitglieder der internen Bridge-Gruppe auf BVI1 (6.4).
- Sicherheitszonen für die internen und externen Schnittstellen.
- Eine Zugriffsregel, die dem gesamten Traffic vertraut, der von innen nach außen gerichtet ist.
- Eine Schnittstellen-NAT-Regel, die den gesamten Traffic von innen nach außen in eindeutige Ports an der IP-Adresse der externen Schnittstelle übersetzt.

- Ein DHCP-Server, der auf der internen Schnittstelle ausgeführt wird.

Hinweis Wenn Sie das Verfahren (Optional) Ändern der Einstellungen des Managementnetzwerks in der CLI, auf Seite 104 durchgeführt haben, sollten einige dieser Aufgaben, insbesondere die Änderung des Administratorkennworts und die Konfiguration der externen und der Management-Schnittstellen, bereits abgeschlossen sein.

Prozedur

Schritt 1 Sie werden aufgefordert, den Endbenutzerlizenzvertrag zu lesen und zu akzeptieren und das Administratorkennwort zu ändern.

Sie müssen diese Schritte ausführen, um fortzufahren.

Schritt 2 Konfigurieren Sie die folgenden Optionen für die externe Schnittstelle und die Management-Schnittstellen, und klicken Sie auf **Next** (Weiter).

Hinweis Ihre Einstellungen werden auf dem Gerät bereitgestellt, wenn Sie auf **Next** (Weiter) klicken. Die Schnittstelle erhält den Namen „outside“ und wird der Sicherheitszone „outside_zone“ hinzugefügt. Stellen Sie sicher, dass Ihre Einstellungen korrekt sind.

a) **Outside Interface** (Externe Schnittstelle): Dies ist der Datenport, den Sie mit Ihrem Gateway-Router verbunden haben. Sie können während der Ersteinrichtung des Geräts keine alternative externe Schnittstelle auswählen. Die erste Datenschnittstelle ist die standardmäßige externe Schnittstelle.

Configure IPv4 (IPv4 konfigurieren): Die IPv4-Adresse für die externe Schnittstelle. Sie können DHCP verwenden oder eine statische IP-Adresse, eine Subnetzmaske und ein Gateway manuell eingeben. Sie können auch **Off** (Aus) auswählen, wenn keine IPv4-Adresse konfiguriert werden soll. Sie können PPPoE nicht mit dem Einrichtungsassistenten konfigurieren. PPPoE kann erforderlich sein, wenn die Schnittstelle mit einem DSL-Modem, Kabelmodem oder einem anderen ISP-Anschluss verbunden ist und Ihr ISP PPPoE verwendet, um Ihre IP-Adresse bereitzustellen. Sie können PPPoE konfigurieren, nachdem Sie den Assistenten abgeschlossen haben.

Configure IPv6 (IPv6 konfigurieren): Die IPv6-Adresse für die externe Schnittstelle. Sie können DHCP verwenden oder eine statische IP-Adresse, ein Präfix und ein Gateway manuell eingeben. Sie können auch **Off** (Aus) auswählen, wenn keine IPv6-Adresse konfiguriert werden soll.

b) **Management-Schnittstelle**

DNS Servers (DNS-Server): Der DNS-Server für die Managementadresse des Systems. Geben Sie eine oder mehrere Adressen von DNS-Servern für die Namensauflösung ein. Der Standardwert sind die öffentlichen DNS-Server von OpenDNS. Wenn Sie die Felder bearbeiten und zum Standardwert zurückkehren möchten, klicken Sie auf **OpenDNS** verwenden, um die entsprechenden IP-Adressen erneut in die Felder zu laden.

Firewall Hostname (Firewall-Host-Name): Der Host-Name für die Managementadresse des Systems.

Schritt 3 Konfigurieren Sie die Systemzeiteinstellungen, und klicken Sie auf **Next** (Weiter).

a) **Time Zone** (Zeitzone): Wählen Sie die Zeitzone für das System aus.

b) **NTP Time Server** (NTP-Zeitserver): Wählen Sie aus, ob Sie die Standard-NTP-Server verwenden oder die Adressen Ihrer NTP-Server manuell eingeben möchten. Sie können mehrere Server hinzufügen, um Backups bereitzustellen.

Schritt 4 (optional) Konfigurieren Sie die Smart Licenses für das System.

Ihr Kauf eines Threat Defense-Geräts umfasst automatisch eine Basislizenz („Base“). Alle zusätzlichen Lizenzen sind optional.

Sie benötigen ein Smart License-Konto, um die für das System erforderlichen Lizenzen abzurufen und anzuwenden. Anfänglich können Sie die 90-tägige Evaluierungslizenz verwenden und Smart Licensing später einrichten.

Falls Sie das Gerät jetzt registrieren möchten, klicken Sie auf den Link, um sich bei Ihrem Smart Software Manager-Konto anzumelden, und lesen Sie Konfigurieren der Lizenzierung, auf Seite 109.

Wenn Sie die Evaluierungslizenz verwenden möchten, wählen Sie **Start 90 day evaluation period without registration** (90-tägigen Evaluierungszeitraum ohne Registrierung starten) aus.

Schritt 5 Klicken Sie auf **Finish** (Fertigstellen).

Nächste Maßnahme

- Obwohl Sie die Evaluierungslizenz weiterhin verwenden können, empfehlen wir Ihnen, Ihr Gerät zu registrieren und zu lizenzieren; siehe Konfigurieren der Lizenzierung, auf Seite 109.
- Sie können das Gerät auch mit Device Manager konfigurieren; siehe Konfigurieren der Firewall in Device Manager, auf Seite 115.

Konfigurieren der Lizenzierung

Threat Defense verwendet Cisco Smart Software Licensing, mit dem Sie einen Lizenzpool zentral erwerben und verwalten können.

Wenn Sie das Chassis registrieren, stellt der Smart Software Manager ein ID-Zertifikat für die Kommunikation zwischen dem Chassis und dem Smart Software Manager aus. Außerdem wird das Chassis dem entsprechenden virtuellen Konto zugewiesen.

Nähere Informationen über die Lizenzierung bei Cisco erhalten Sie unter cisco.com/go/licensingguide

Die Base-Lizenz (Basislizenz) ist automatisch enthalten. Smart Licensing hindert Sie nicht daran, Produktfunktionen zu nutzen, die Sie noch nicht erworben haben. Sie können sofort mit der Nutzung einer Lizenz beginnen, sofern Sie beim Smart Software Manager registriert sind, und die Lizenz später erwerben. Dadurch können Sie eine Funktion bereitstellen und verwenden und Verzögerungen aufgrund der Genehmigung von Bestellungen vermeiden. Lesen Sie die Informationen zu folgenden Lizenzen:

- **Threat**: Security Intelligence und Next-Generation IPS
- **Malware**: MalwareDefense
- **URL**: URL-Filterung
- **RA VPN**: AnyConnect Plus, AnyConnect Apex oder AnyConnect VPN Only.

Vorbereitungen

- Sie müssen über ein Masterkonto bei Smart Software Manager verfügen.

  Wenn Sie noch kein Konto haben, klicken Sie auf den Link, um ein neues Konto einzurichten. Mit dem Smart Software Manager können Sie ein Masterkonto für Ihr Unternehmen erstellen.

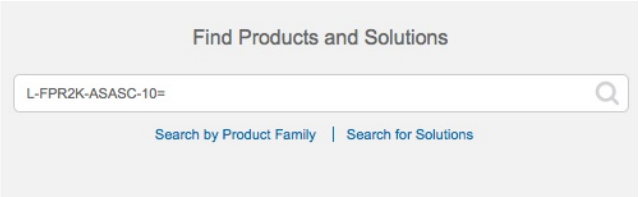
- Ihr Smart Software Licensing-Konto muss für die Strong Encryption-(3DES/AES-)Lizenz qualifiziert sein, um bestimmte Funktionen nutzen zu können (aktiviert mit dem Flag „export-compliance“).

Prozedur

Schritt 1 Stellen Sie sicher, dass Ihr Smart Licensing-Konto die verfügbaren Lizenzen enthält, die Sie benötigen.

Wenn Sie Ihr Gerät bei Cisco oder einem Fachhändler gekauft haben, sollten Ihre Lizenzen mit Ihrem Smart Software License-Konto verknüpft sein. Wenn Sie jedoch selbst Lizenzen hinzufügen müssen, verwenden Sie das Suchfeld **Find Products and Solutions** (Produkte und Lösungen suchen) im Cisco Commerce Workspace. Suchen Sie nach den folgenden Lizenz-PIDs:

Abbildung 27: Lizenzsuche



Hinweis Wenn keine PID gefunden wird, können Sie die PID manuell zu Ihrer Bestellung hinzufügen.

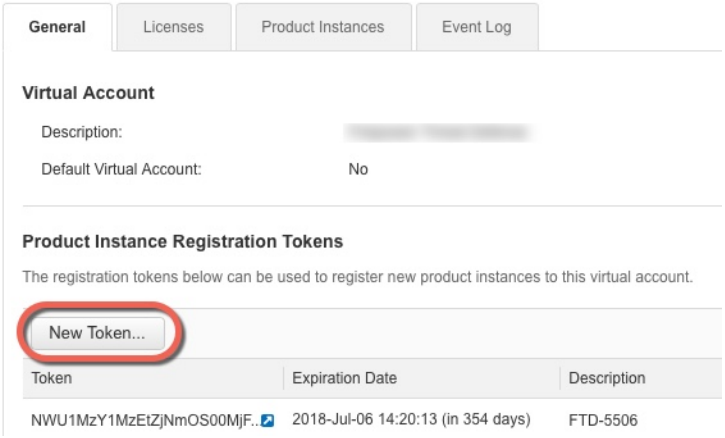
- Kombination aus Threat-, Malware- und URL-Lizenz:
  - L-FPR1010T-TMC =

  Wenn Sie Ihrer Bestellung eine der oben genannten PIDs hinzufügen, können Sie ein befristetes Abonnement auswählen, das einer der folgenden PIDs entspricht:
  - L-FPR1010T-TMC-1Y
  - L-FPR1010T-TMC-3Y
  - L-FPR1010T-TMC-5Y
- VPN für Remotezugriff (RA VPN): Entnehmen Sie die Einzelheiten bitte der Bestellanleitung für Cisco AnyConnect.

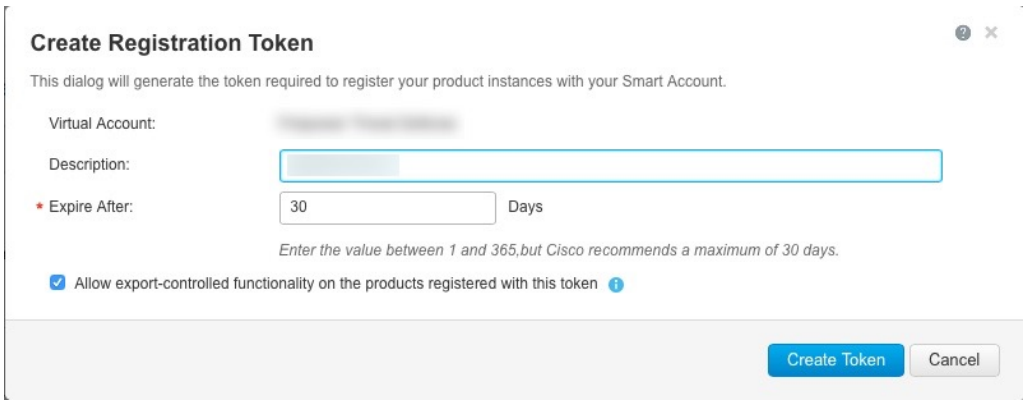
Schritt 2 Fordern Sie in Smart Software Manager ein Registrierungstoken für das virtuelle Konto an, zu dem Sie dieses Gerät hinzufügen möchten, und kopieren Sie es.

a) Klicken Sie auf **Inventory** (Bestand).

b) Klicken Sie auf der Registerkarte **General** (Allgemein) auf **New Token** (Neues Token).



c) Geben Sie im Dialogfeld **Create Registration Token** (Registrierungstoken erstellen) die folgenden Einstellungen ein, und klicken Sie dann auf **Create Token** (Token erstellen):



- **Beschreibung**
- **Expire after** (Ablauf nach): Cisco empfiehlt 30 Tage.
- **Allow export-controlled functionality on the products registered with this token** (Exportgesteuerte Funktion für die mit diesem Token registrierten Produkte zulassen): Aktiviert das Flag export-compliance, wenn Sie sich in einem Land befinden, das eine starke Verschlüsselung ermöglicht. Sie müssen diese Option jetzt auswählen, wenn Sie diese Funktion verwenden möchten. Wenn Sie diese Funktion später aktivieren, müssen Sie Ihr Gerät mit einem neuen Produktschlüssel erneut registrieren und das Gerät neu laden. Wenn diese Option nicht angezeigt wird, unterstützt Ihr Konto keine exportgesteuerten Funktionen.

Das Token wird Ihrem Bestand hinzugefügt.

d) Klicken Sie auf das Pfeilsymbol rechts neben dem Token, um das Dialogfeld **Token** zu öffnen, damit Sie die Token-ID in Ihre Zwischenablage kopieren können. Halten Sie dieses Token für die Threat Defense-Registrierung bereit, die Sie später in diesem Verfahren ausführen müssen.

Abbildung 28: Token anzeigen

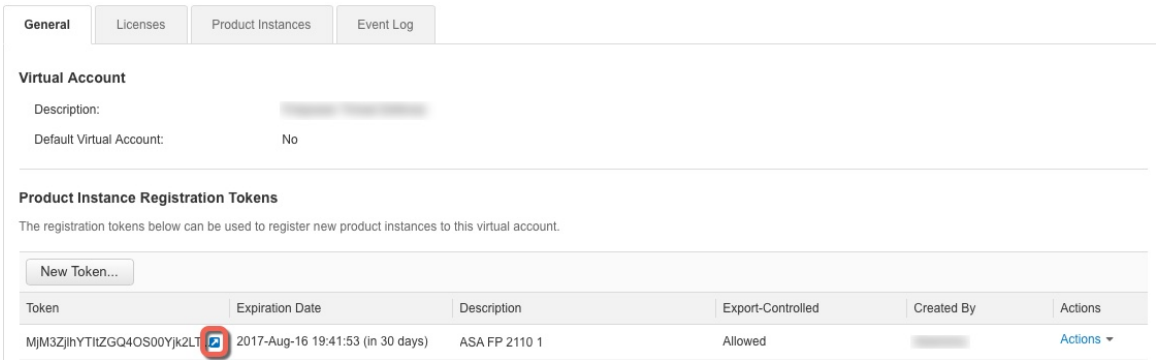
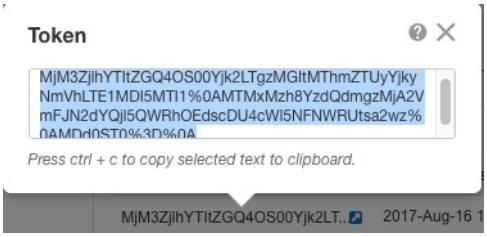


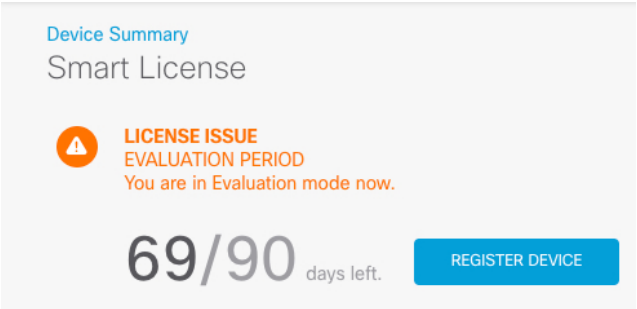
Abbildung 29: Token kopieren



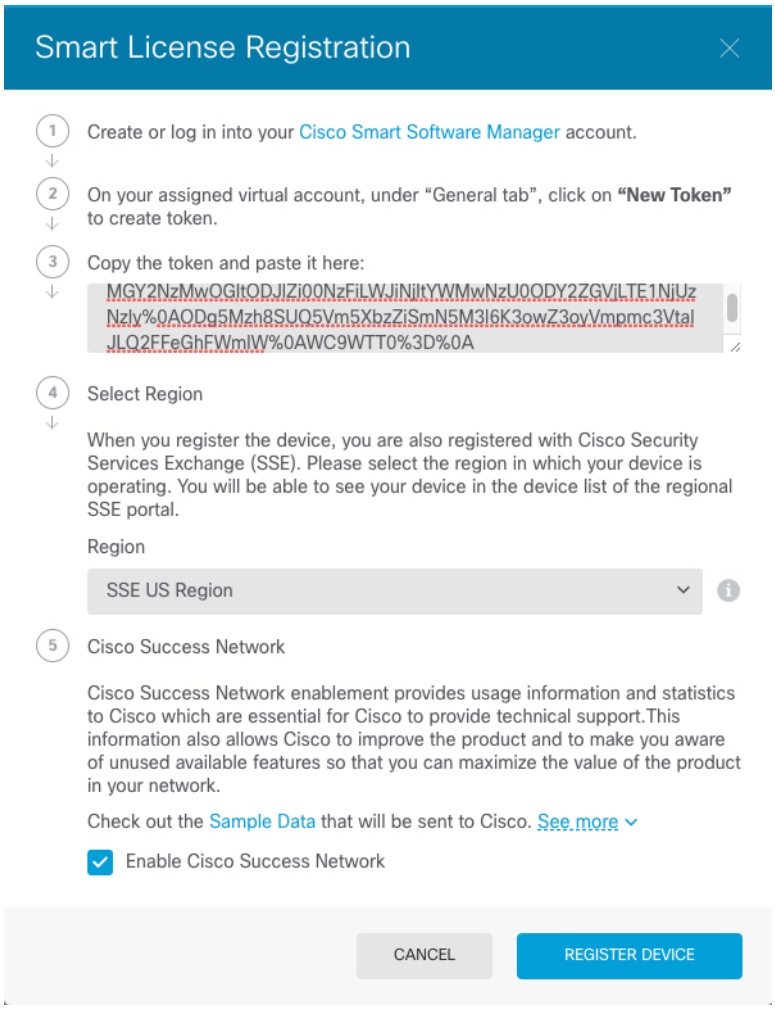
Schritt 3 Klicken Sie in Device Manager auf **Device** (Gerät) und dann in der **Smart License**-Zusammenfassung auf **View Configuration** (Konfiguration anzeigen).

Die Seite **Smart License** wird angezeigt.

Schritt 4 Klicken Sie auf **Register Device** (Gerät registrieren).

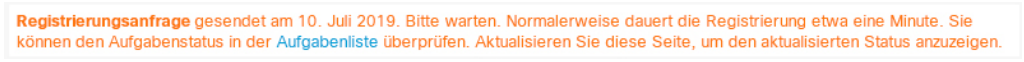


Befolgen Sie dann die Anweisungen im Dialogfeld **Smart License Registration** (Smart License-Registrierung), um Ihr Token einzufügen:

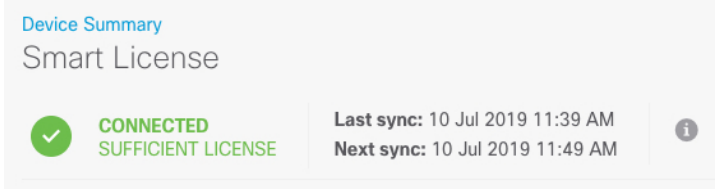


Schritt 5 Klicken Sie auf **Register Device** (Gerät registrieren).

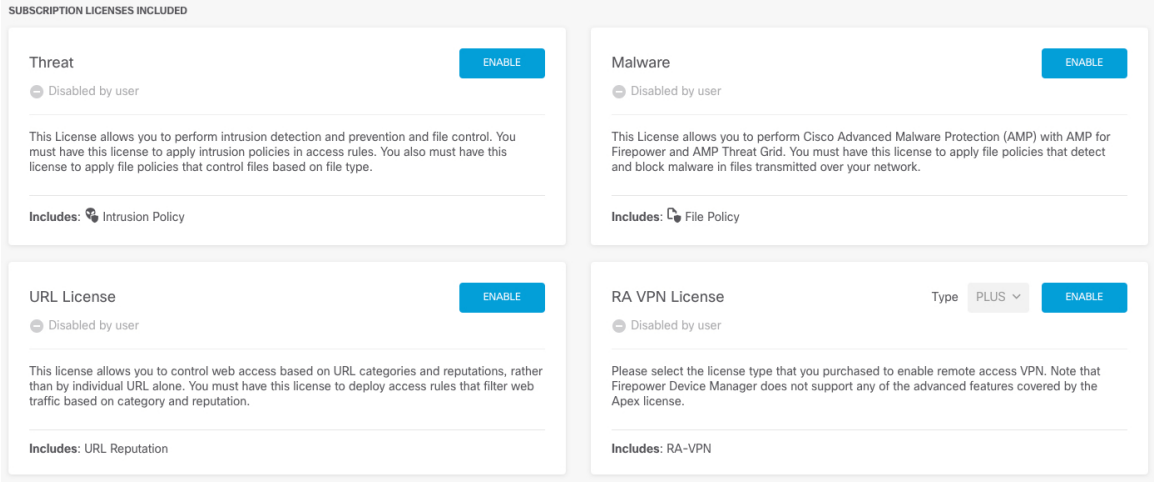
Daraufhin kehren Sie zur **Smart License**-Seite zurück. Während das Gerät registriert wird, wird die folgende Meldung angezeigt:



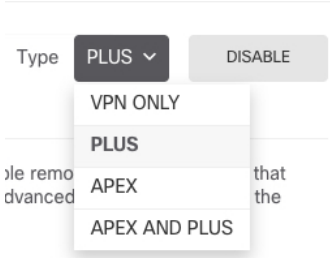
Nach der erfolgreichen Registrierung des Geräts und der Aktualisierung der Seite wird Folgendes angezeigt:



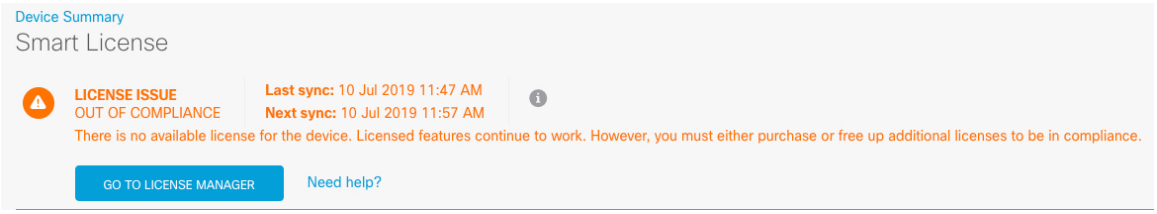
Schritt 6 Klicken Sie bei Bedarf für jede optionale Lizenz auf das Kontrollkästchen **Enable/Disable** (Aktivieren/Deaktivieren).



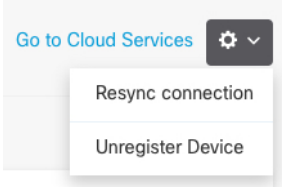
- **Enable** (Aktivieren): Registriert die Lizenz bei Ihrem Cisco Smart Software Manager-Konto und aktiviert die gesteuerten Funktionen. Sie können jetzt Richtlinien konfigurieren und bereitstellen, die durch die Lizenz gesteuert werden.
- **Disable** (Deaktivieren): Hebt die Registrierung der Lizenz bei Ihrem Cisco Smart Software Manager-Konto auf und deaktiviert die gesteuerten Funktionen. Sie können die Funktionen weder in neuen Richtlinien konfigurieren noch Richtlinien bereitstellen, die die Funktion verwenden.
- Wenn Sie die **RA VPN**-Lizenz aktiviert haben, wählen Sie den gewünschten Lizenztyp aus: **Plus**, **Apex**, **VPN Only** oder **Plus and Apex**.



Nachdem Sie die Funktionen aktiviert haben und wenn die Lizenzen nicht in Ihrem Konto vorhanden sind, wird nach dem Aktualisieren der Seite die folgende Nichtkonformitätsmeldung angezeigt:



Schritt 7 Wählen Sie in der Zahnrad-Dropdown-Liste die Option **Resync Connection** (Verbindung synchronisieren) aus, um Lizenzinformationen mit Cisco Smart Software Manager zu synchronisieren.



Konfigurieren der Firewall in Device Manager

Die folgenden Schritte geben einen Überblick über zusätzliche Funktionen, die Sie möglicherweise konfigurieren möchten. Klicken Sie auf die Hilfe-Schaltfläche (**?**) einer Seite, um detaillierte Informationen zu den einzelnen Schritten zu erhalten.

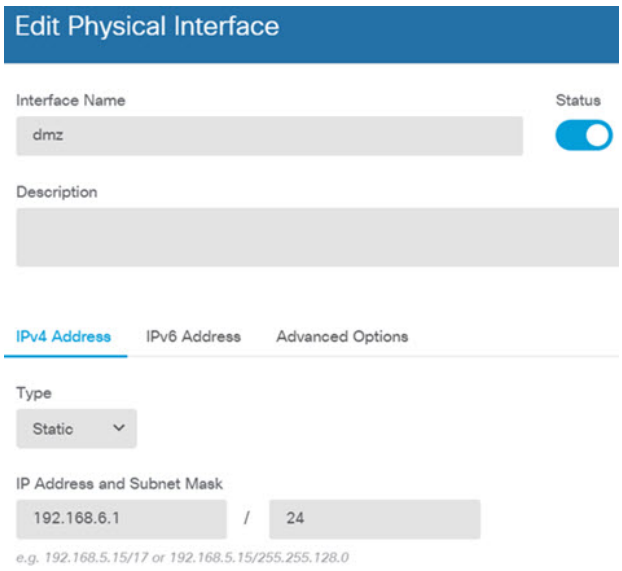
Prozedur

Schritt 1 Wenn Sie eine Schnittstelle einer Bridge-Gruppe konvertieren möchten (6.4) oder Sie einen Switch-Port in eine Firewall-Schnittstelle konvertieren möchten (6.5 und höher), wählen Sie **Gerät**, und klicken Sie dann auf den Link in der Zusammenfassung **Schnittstellen**.

Klicken Sie auf das Bearbeitungssymbol ( ) für jede Schnittstelle, um den Modus festzulegen und die IP-Adresse und andere Einstellungen zu definieren.

Im folgenden Beispiel wird eine Schnittstelle als „demilitarisierte Zone“ (DMZ) konfiguriert, in der Sie öffentlich zugängliche Ressourcen wie Ihren Webserver platzieren. Wenn Sie fertig sind, klicken Sie auf **Save (Speichern)**.

Abbildung 30: Bearbeiten der Schnittstelle



Schritt 2 Wenn Sie neue Schnittstellen konfiguriert haben, wählen Sie **Objects** (Objekte) und dann **Security Zones** (Sicherheitszonen) aus dem Inhaltsverzeichnis.

Bearbeiten oder erstellen Sie neue Zonen. Jede Schnittstelle muss zu einer Zone gehören, da Sie Richtlinien basierend auf Sicherheitszonen und nicht auf Schnittstellen konfigurieren. Sie können die Schnittstellen bei der Konfiguration nicht in Zonen platzieren. Daher müssen Sie die Zonenobjekte immer bearbeiten, nachdem Sie neue Schnittstellen erstellt oder den Zweck vorhandener Schnittstellen geändert haben.

Das folgende Beispiel zeigt, wie Sie eine neue dmz-zone für die dmz-Schnittstelle erstellen.

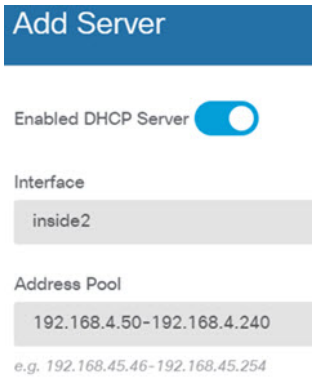
Abbildung 31: Sicherheitszonenobjekt

Schritt 3 Wenn Sie möchten, dass interne Clients DHCP verwenden, um eine IP-Adresse vom Gerät abzurufen, wählen Sie **Device** > **System Settings** > **DHCP Server** (Gerät > Systemeinstellungen > DHCP-Server) und anschließend die Registerkarte **DHCP Servers** (DHCP-Server) aus.

Für die interne Schnittstelle ist bereits ein DHCP-Server konfiguriert, aber Sie können den Adressen-Pool bearbeiten oder ihn sogar löschen. Wenn Sie andere interne Schnittstellen konfiguriert haben, ist es sehr üblich, einen DHCP-Server auf diesen Schnittstellen einzurichten. Klicken Sie auf +, um den Server und den Adressen-Pool für jede interne Schnittstelle zu konfigurieren.

Sie können auch die WINS- und DNS-Liste, die den Clients zur Verfügung gestellt wird, auf der Registerkarte **Configuration** (Konfiguration) anpassen. Das folgende Beispiel veranschaulicht, wie Sie einen DHCP-Server auf der inside2-Schnittstelle mit dem Adressen-Pool 192.168.4.50-192.168.4.240 einrichten.

Abbildung 32: DHCP-Server



Schritt 4 Wählen Sie **Device** (Gerät), und klicken Sie dann in der Gruppe **Routing** auf **View Configuration** (Konfiguration anzeigen) (oder **Create First Static Route** (Erste statische Route erstellen)), und konfigurieren Sie eine Standardroute.

Die Standardroute zeigt normalerweise auf den Upstream- oder ISP-Router, der sich außerhalb der externen Schnittstelle befindet. Eine Standard-IPv4-Route ist für any-ipv4 (0.0.0.0/0) vorgesehen, während eine Standard-IPv6-Route für any-ipv6 (:: 0/0) vorgesehen ist. Erstellen Sie Routen für jede verwendete IP-Version. Wenn Sie DHCP verwenden, um eine Adresse für die externe Schnittstelle zu erhalten, verfügen Sie möglicherweise bereits über die erforderlichen Standardrouten.

Hinweis Die Routen, die Sie auf dieser Seite definieren, gelten nur für die Datenschnittstellen. Sie haben keine Auswirkungen auf die Management-Schnittstelle. Legen Sie das Management-Gateway unter **Device** > **System Settings** > **Management Interface** (Gerät > Systemeinstellungen > Management-Schnittstelle) fest.

Das folgende Beispiel zeigt eine Standardroute für IPv4. In diesem Beispiel ist isp-gateway ein Netzwerkobjekt, das die IP-Adresse des ISP-Gateways identifiziert (Sie müssen die Adresse von Ihrem ISP erhalten). Sie können dieses Objekt erstellen, indem Sie unten in der Dropdown-Liste **Gateway** auf **Create New Network** (Neues Netzwerk erstellen) klicken.

Abbildung 33: Standardroute

Schritt 5 Wählen Sie **Policies** (Richtlinien) aus, und konfigurieren Sie die Sicherheitsrichtlinien für das Netzwerk.

Der Assistent für die Geräteeinrichtung ermöglicht den Traffic-Fluss zwischen der internen Zone und der externen Zone sowie die Schnittstellen-NAT für alle Schnittstellen, wenn der Traffic an die externe Schnittstelle gerichtet ist. Selbst wenn Sie neue Schnittstellen konfigurieren und diese dem Objekt der internen Zone hinzufügen, wird die Zugriffskontrollregel automatisch auf sie angewendet.

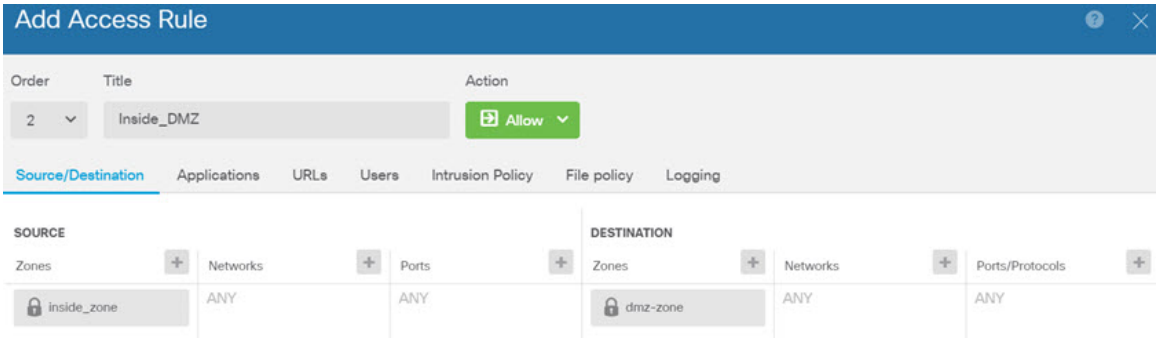
Wenn Sie jedoch mehrere interne Schnittstellen haben, benötigen Sie eine Zugriffskontrollregel, um den Traffic von einer internen Zone zu einer anderen internen Zone zuzulassen. Wenn Sie andere Sicherheitszonen hinzufügen, benötigen Sie Regeln, um Traffic zu und von diesen Zonen zuzulassen. Dies wären Ihre minimalen Änderungen.

Darüber hinaus können Sie weitere Richtlinien konfigurieren, um zusätzliche Dienste bereitzustellen, und die NAT und Zugriffsregeln optimieren, um die für Ihr Unternehmen erforderlichen Ergebnisse zu erzielen. Sie können die folgenden Richtlinien konfigurieren:

- **SSL Decryption** (SSL-Entschlüsselung): Wenn Sie verschlüsselte Verbindungen (z. B. HTTPS) auf Intrusions, Malware usw. untersuchen möchten, müssen Sie die Verbindungen entschlüsseln. Verwenden Sie die SSL-Entschlüsselungsrichtlinie, um zu bestimmen, welche Verbindungen entschlüsselt werden müssen. Das System verschlüsselt die Verbindung nach der Untersuchung erneut.
- **Identity** (Identität): Wenn Sie die Netzwerkaktivität mit einzelnen Benutzern korrelieren oder den Netzwerkzugriff basierend auf der Mitgliedschaft von Benutzern oder Benutzergruppen steuern möchten, verwenden Sie die Identitätsrichtlinie, um den Benutzer zu bestimmen, der einer bestimmten Quell-IP-Adresse zugeordnet ist.
- **Security Intelligence**: Verwenden Sie die Security Intelligence-Richtlinie, um Verbindungen von oder zu IP-Adressen oder URLs, die in der Blacklist aufgeführt sind, schnell zu trennen. Wenn Sie bekannte schädliche Websites auf die Blacklist setzen, müssen Sie diese nicht in Ihrer Richtlinie für die Zugriffskontrolle berücksichtigen. Cisco stellt regelmäßig aktualisierte Feeds bekannter schädlicher Adressen und URLs bereit, damit die Security Intelligence-Blacklist dynamisch aktualisiert wird. Wenn Sie Feeds verwenden, müssen Sie die Richtlinie nicht bearbeiten, um Elemente zur Blacklist hinzuzufügen oder zu entfernen.
- **NAT (Network Address Translation)**: Verwenden Sie die NAT-Richtlinie, um interne IP-Adressen in extern routbare Adressen zu konvertieren.
- **Access Control** (Zugriffskontrolle): Verwenden Sie die Zugriffskontrollrichtlinie, um zu bestimmen, welche Verbindungen im Netzwerk zulässig sind. Sie können nach Sicherheitszone, IP-Adresse, Protokoll, Port, Anwendung, URL, Benutzer oder Benutzergruppe filtern. Sie wenden auch Intrusion- und Datei-Richtlinien (Malware) mit Zugriffskontrollregeln an. Verwenden Sie diese Richtlinie, um die URL-Filterung zu implementieren.
- **Intrusion**: Verwenden Sie die Intrusion-Richtlinien, um nach bekannten Bedrohungen zu suchen. Obwohl Sie Intrusion-Richtlinien mithilfe von Zugriffskontrollregeln anwenden, können Sie die Intrusion-Richtlinien bearbeiten, um bestimmte Intrusion-Regeln selektiv zu aktivieren oder zu deaktivieren.

Das folgende Beispiel zeigt, wie Traffic zwischen der internen Zone (inside-zone) und der demilitarisierten Zone (dmz-zone) in der Zugriffskontrollrichtlinie zugelassen wird. In diesem Beispiel sind auf keiner der anderen Registerkarten Optionen festgelegt, mit Ausnahme der Registerkarte **Logging**, bei der die Option **At End of Connection** (Am Ende der Verbindung) ausgewählt ist.

Abbildung 34: Zugriffskontrollrichtlinie



Schritt 6 Wählen Sie **Device** (Gerät) aus, und klicken Sie dann in der Gruppe **Updates** (Aktualisierungen) auf **View Configuration** (Konfiguration anzeigen). Konfigurieren Sie die Aktualisierungszeitpläne für die Systemdatenbanken.

Wenn Sie Intrusion-Richtlinien verwenden, richten Sie regelmäßige Aktualisierungen für die Regel- und VDB-Datenbanken ein. Wenn Sie Security Intelligence-Feeds verwenden, legen Sie einen Aktualisierungszeitplan für sie fest. Wenn Sie die Geolokation in Sicherheitsrichtlinien als Übereinstimmungskriterien verwenden, legen Sie einen Aktualisierungszeitplan für diese Datenbank fest.

Schritt 7 Klicken Sie im Menü auf die Schaltfläche **Deploy** (Bereitstellen) und dann auf die Schaltfläche „Deploy Now“ (Jetzt bereitstellen) ( ), um Ihre Änderungen auf dem Gerät bereitzustellen.

Änderungen sind auf dem Gerät erst aktiv, nachdem Sie sie bereitgestellt haben.

Zugriff auf die Threat Defense- und FXOS-CLI

Verwenden Sie die Befehlszeilenschnittstelle (CLI), um das System einzurichten und grundlegende Systemfehlerbehebungen durchzuführen. Sie können Richtlinien nicht über eine CLI-Sitzung konfigurieren. Für den Zugriff auf die CLI (Befehlszeilenschnittstelle) müssen Sie eine Verbindung zum Konsolenport herstellen.

Sie können zur Fehlerbehebung auch auf die FXOS-CLI-CLI zugreifen.

Hinweis Sie können auch eine SSH-Sitzung für die Management-Schnittstelle des Threat Defense-Geräts nutzen. Im Gegensatz zu einer Konsolensitzung verwendet die SSH-Sitzung standardmäßig die Threat Defense-CLI, über die Sie sich mit dem Befehl **connect fxos** mit der FXOS-CLI-CLI verbinden können. Sie können sich später mit der Adresse auf einer Datenschnittstelle verbinden, wenn Sie die Schnittstelle für SSH-Verbindungen öffnen. Der SSH-Zugriff auf Datenschnittstellen ist standardmäßig deaktiviert. Dieses Verfahren beschreibt den Konsolenportzugriff, der standardmäßig auf die FXOS-CLI-CLI eingestellt ist.

Prozedur

Schritt 1 Verbinden Sie Ihren Management-Computer mit dem Konsolenport, um sich bei der CLI anzumelden. Firepower 1000 wird mit einem seriellen USB-A-zu-B-Kabel ausgeliefert. Stellen Sie sicher, dass Sie alle erforderlichen seriellen USB-Treiber für Ihr Betriebssystem installieren (siehe Firepower 1010 -Hardwarehandbuch). Der Konsolenport ist standardmäßig auf die FXOS-CLI-CLI eingestellt. Verwenden Sie die folgenden seriellen Einstellungen:

- 9.600 Baud
- 8 Daten-Bits
- Keine Parität
- 1 Stopp-Bit

Sie stellen eine Verbindung zum FXOS-CLI her. Melden Sie sich bei der CLI mit dem Benutzernamen **admin** und dem Kennwort an, das Sie bei der Ersteinrichtung festgelegt haben (der Standardwert ist **Admin123**).

Beispiel:

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

Schritt 2 Greifen Sie auf die Threat Defense-CLI zu.

connect ftd

Beispiel:

```
firepower# connect ftd
>
```

Geben Sie nach der Anmeldung **help** oder **?** ein, um Informationen zu den Befehlen aufzurufen, die in der CLI verfügbar sind. Informationen zur Verwendung finden Sie unter Befehlsreferenz für Secure Firewall Threat Defense.

Schritt 3 Um die Threat Defense-CLI zu verlassen, geben Sie den Befehl **exit** oder **logout** ein.

Mit diesem Befehl kehren Sie zur FXOS-CLI-CLI-Eingabeaufforderung zurück. Geben Sie **?** ein, um Informationen zu den Befehlen aufzurufen, die in der FXOS-CLI-CLI verfügbar sind.

Beispiel:

```
> exit
firepower#
```

Anzeigen von Hardwareinformationen

Verwenden Sie die CLI (Befehlszeilenschnittstelle bzw. Kommandozeile), um Informationen zu Ihrer Hardware anzuzeigen, einschließlich Gerätemodell, Hardwareversion, Seriennummer und Chassis-Komponenten mit Netzteilen und Netzwerkmodulen. Für den Zugriff auf die CLI müssen Sie eine Verbindung zum Konsolenport herstellen; siehe Zugriff auf die Threat Defense- und FXOS-CLI, auf Seite 119.

Prozedur

Schritt 1 Um das Hardwaremodell des Geräts anzuzeigen, verwenden Sie den Befehl **show model**.

> **show model**

Beispiel:

```
> show model
Cisco Firepower 1010 Threat Defense
```

Schritt 2 Um die Seriennummer des Chassis anzuzeigen, verwenden Sie den Befehl **show serial-number**.

> **show serial-number**

Beispiel:

```
> show serial-number
JMX1943408S
```

Diese Informationen werden auch in der Ausgabe von **show version system**, **show running-config** und **show inventory** angezeigt.

Schritt 3 Verwenden Sie den Befehl **show inventory**, um Informationen zu allen im Netzwerkgerät installierten Cisco Produkten anzuzeigen, denen eine Produkt-ID (PID), eine Versions-ID (VID) und eine Seriennummer (SN) zugewiesen sind.

> **show inventory**

a) Über die Threat Defense-CLI:

Beispiel:

```
> show inventory
Name: "module 0", DESCR: "Firepower 1010 Appliance, Desktop, 8 GE, 1 MGMT"
PID: FPR-1010          , VID: V00     , SN: JMX1943408S
```

b) Über die FXOS-CLI:

Beispiel:

```
firepower /chassis # show inventory
Chassis    PID             Vendor            Serial (SN) HW Revision
---------- --------------- ----------------- ----------- -----------
         1 FPR-1010        Cisco Systems, In JMX1943408S 0.3
```

Ausschalten der Firewall

Es ist wichtig, dass Sie Ihr System ordnungsgemäß herunterfahren. Wenn Sie einfach den Netzstecker ziehen, kann das Dateisystem ernsthaft beschädigt werden. Denken Sie daran, dass im Hintergrund ständig viele Prozesse ablaufen, und dass das Ziehen des Netzsteckers oder das Ausschalten der Stromversorgung kein ordnungsgemäßes Herunterfahren Ihres Firewall-Systems ermöglicht.

Das Firepower 1010-Chassis hat keinen externen Netzschalter.Sie können die Firewall mit Device Manager oder über die FXOS-CLI ausschalten.

Ausschalten der Firewall über die Device Manager

Sie können Ihr System mithilfe von Device Manager ordnungsgemäß herunterfahren.

Prozedur

Schritt 1 Verwenden Sie Device Manager, um die Firewall herunterzufahren.

Hinweis Geben Sie bei Version 6.4 und früheren Versionen in der Device Manager-CLI den Befehl **shutdown** ein.

a) Klicken Sie auf **Device** (Gerät) und anschließend auf den Link **System Settings** > **Reboot/Shutdown** (Systemeinstellungen > Neu starten/Herunterfahren).
b) Klicken Sie auf **Shut Down** (Herunterfahren).

Schritt 2 Wenn Sie über eine Konsolenverbindung zur Firewall verfügen, prüfen Sie die Systemaufforderungen, wenn die Firewall heruntergefahren wird. Die folgende Aufforderung wird angezeigt:

```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

Wenn Sie keine Konsolenverbindung haben, warten Sie circa 3 Minuten, um sicherzustellen, dass das System heruntergefahren wurde.

Schritt 3 Sie können jetzt den Netzstecker ziehen, um die Stromversorgung des Chassis bei Bedarf physisch zu trennen.

Ausschalten des Geräts über die CLI

Sie können die FXOS-CLI verwenden, um das System sicher herunterzufahren und das Gerät auszuschalten. Für den Zugriff auf die CLI (Befehlszeilenschnittstelle bzw. Kommandozeile) müssen Sie eine Verbindung zum Konsolenport herstellen; siehe Zugriff auf die Threat Defense- und FXOS-CLI, auf Seite 119.

Prozedur

Schritt 1 Stellen Sie in der FXOS-CLI eine Verbindung zu local-mgmt her:

firepower # **connect local-mgmt**

Schritt 2 Geben Sie den Befehl **shutdown** aus:

firepower(local-mgmt) # **shutdown**

Beispiel:

```
firepower(local-mgmt)# shutdown
This command will shutdown the system.  Continue?
Please enter 'YES' or 'NO': yes
INIT: Stopping Cisco Threat Defense......ok
```

Schritt 3 Überwachen Sie die System-Eingabeaufforderungen, während die Firewall heruntergefahren wird. Die folgende Aufforderung wird angezeigt:

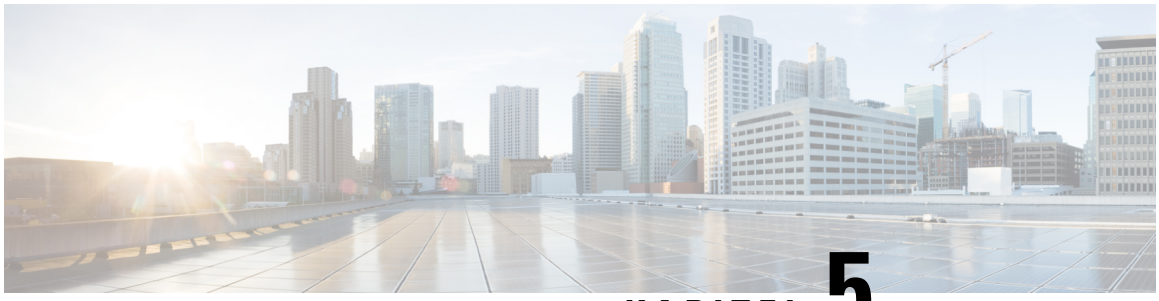
```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

Schritt 4 Sie können jetzt den Netzstecker ziehen, um die Stromversorgung des Chassis bei Bedarf physisch zu trennen.

Nächste Schritte

Um die Konfiguration von Threat Defense fortzusetzen, lesen Sie die Dokumente, die für Ihre Softwareversion verfügbar sind. Siehe Navigation in der Cisco Firepower-Dokumentation.

Informationen zur Verwendung des Device Manager finden Sie unter Cisco Firepower Threat Defense – Konfigurationsleitfaden für Firepower Device Manager.



KAPITEL 5

Threat Defense-Bereitstellung mit CDO

Enthält dieses Kapitel die Informationen, nach denen Sie suchen?

Um alle verfügbaren Betriebssysteme und Manager anzuzeigen, sehen Sie sich Welche Betriebssysteme und Manager sind für Sie geeignet?, auf Seite 1 an. Dieses Kapitel bezieht sich auf Threat Defense mit Cisco Defense Orchestrator in der Cloud bereitgestelltem (CDO)Secure Firewall Management Center. Informationen zur Verwendung von CDO mit Device Manager-Funktionen finden Sie in der CDO-Dokumentation.

Hinweis Die in der Cloud bereitgestellte Management Center-Version unterstützt Threat Defense 7.2 und höher. Für frühere Versionen können Sie die Device Manager-Funktionalität von CDO verwenden.

Jedes Threat Defense-System steuert, untersucht, überwacht und analysiert den Traffic. CDO bietet eine Konsole für zentrales Management mit einer Weboberfläche, über die Sie Administrations- und Managementaufgaben zum Schutz Ihres lokalen Netzwerks durchführen können.

Informationen zur Firewall

Auf der Hardware kann entweder Threat Defense-Software oder ASA-Software ausgeführt werden. Beim Wechsel zwischen Threat Defense und ASA müssen Sie ein neues Image des Geräts erstellen. Sie sollten auch ein neues Image erstellen, wenn Sie eine andere Softwareversion als derzeit installiert benötigen. Weitere Informationen hierzu finden Sie unter Reimage the Cisco ASA or Firepower Threat Defense Device (Erstellen eines neuen Images für Cisco ASA oder Firepower Threat Defense-Gerät).

Die Firewall führt ein zugrunde liegendes Betriebssystem namens Secure Firewall Extensible Operating System (FXOS) aus. Die Firewall unterstützt die FXOS-Secure Firewall Chassis Manager nicht. Es wird nur in begrenztem Umfang eine CLI für Fehlerbehebungszwecke unterstützt. Weitere Informationen finden Sie unter Cisco FXOS-Leitfaden zur Fehlerbehebung für die Firepower 1000/2100-Serie mit Firepower Threat Defense.

Datenschutzerklärung zur Datenerfassung: Die Firewall erfordert keine personenbezogenen Informationen und nimmt keine aktive Erfassung derartiger Informationen vor. Sie können jedoch personenbezogene Informationen in der Konfiguration verwenden, z. B. bei Benutzernamen. In diesem Fall kann ein Administrator diese Informationen möglicherweise sehen, wenn er mit der Konfiguration arbeitet oder SNMP verwendet.

Informationen zu Threat Defense Management über CDO

Cloud-Delivered Firewall Management Center

Die in der Cloud bereitgestellte Management Center-Lösung bietet viele der gleichen Funktionen wie eine lokale Management Center-Lösung und verfügt über dasselbe Erscheinungsbild. Wenn Sie CDO als primären Manager verwenden, können Sie ein lokales Management Center-System nur für Analysen verwenden. Das lokale Management Center-System unterstützt keine Richtlinienkonfiguration oder kein Upgrade.

CDO-Onboarding-Methoden

Sie haben folgende Möglichkeiten für das Onboarding eines Geräts:

- Low-Touch Provisioning mit der Seriennummer −
  - Ein Administrator in der zentralen Hauptgeschäftsstelle sendet das Threat Defense an die Remote-Zweigstelle. Es ist keine Vorkonfiguration erforderlich. Tatsächlich sollten Sie nichts auf dem Gerät konfigurieren, da die Low-Touch Provisioning nicht mit vorkonfigurierten Geräten funktioniert.

Hinweis Der zentrale Administrator kann das Threat Defense-Gerät im CDO mit der Threat Defense-Seriennummer vorregistrieren, bevor es das Gerät an die Zweigstelle sendet.

  - Der Zweigstellenadministrator verkabelt das Threat Defense und schaltet es ein.
  - Der Administrator in der Zentrale schließt die Konfiguration des Threat Defense mit dem CDO ab.

  Sie können für das Onboarding auch eine Seriennummer verwenden, wenn Sie bereits mit der Konfiguration des Geräts in Device Manager begonnen haben. Dieses Verfahren wird im vorliegenden Handbuch jedoch nicht behandelt.

- Onboarding-Assistent mit CLI-Registrierung: Verwenden Sie diese manuelle Methode, wenn Sie eine Vorkonfiguration durchführen müssen oder eine Manageroberfläche verwenden, die Low-Touch Provisioning nicht unterstützt.

Threat Defense-Managerzugriffsschnittstelle

Sie können die Managementschnittstelle oder die externe Datenschnittstelle für den Managerzugriff verwenden. Dieses Handbuch behandelt jedoch den externen Schnittstellenzugriff. Low-Touch Provisioning unterstützt nur die externe Schnittstelle.

Die Management-Schnittstelle ist eine spezielle Schnittstelle, die separat von Threat Defense-Datenschnittstellen konfiguriert wird und über eigene Netzwerkeinstellungen verfügt. Die Netzwerkeinstellungen der Management-Schnittstelle werden weiterhin verwendet, auch wenn Sie den Managerzugriff auf einer

Datenschnittstelle aktivieren. Der gesamte Management-Traffic geht weiterhin von der Management-Schnittstelle aus oder ist an diese gerichtet. Wenn Sie den Managerzugriff auf einer Datenschnittstelle aktivieren, leitet Threat Defense eingehenden Management-Traffic über die Backplane an die Management-Schnittstelle weiter. Für den ausgehenden Management-Traffic leitet die Management-Schnittstelle den Traffic über die Backplane an die Datenschnittstelle weiter.

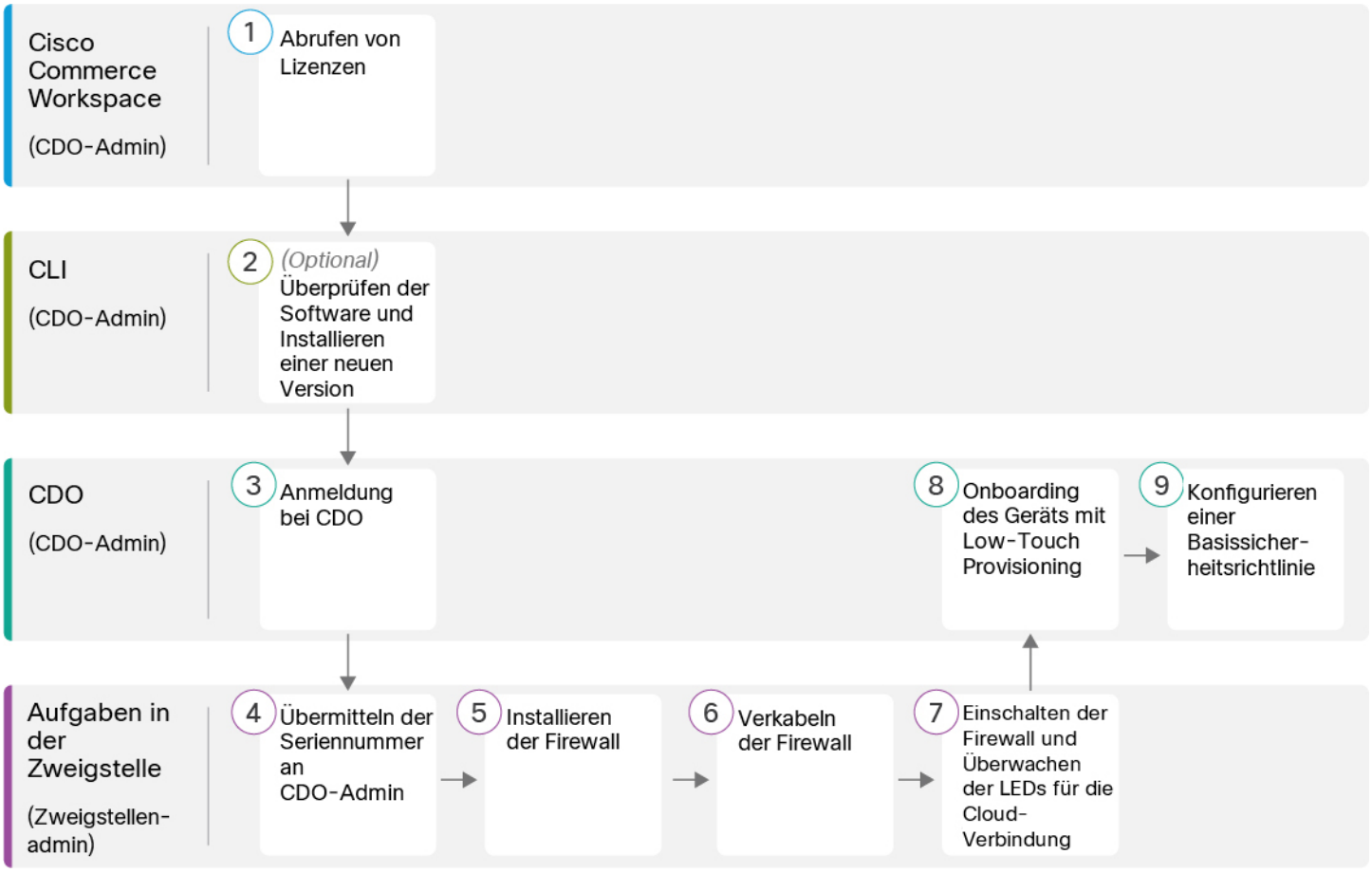
Der Managerzugriff über eine Datenschnittstelle hat folgende Einschränkungen:

- Sie können den Managerzugriff nur auf einer physischen Datenschnittstelle aktivieren. Sie können keine Unterschnittstellen oder EtherChannels verwenden.
- Diese Schnittstelle kann nicht als reine Management-Schnittstellen verwendet werden.
- Nur Routing-Firewall-Modus mit einer gerouteten Schnittstelle.
- PPPoE wird nicht unterstützt. Wenn Ihr ISP PPPoE benötigt, müssen Sie einen Router mit PPPoE-Unterstützung zwischen Threat Defense und dem WAN-Modem platzieren.
- Die Schnittstelle darf sich nur im globalen VRF befinden.
- SSH ist für Datenschnittstellen nicht standardmäßig aktiviert, daher müssen Sie SSH später mithilfe von Management Center aktivieren. Da das Gateway der Management-Schnittstelle zu den Datenschnittstellen wird, können Sie auch nicht per SSH von einem Remote-Netzwerk auf die Management-Schnittstelle zugreifen, es sei denn, Sie fügen mit dem Befehl **configure network static-routes** eine statische Route für die Management-Schnittstelle hinzu.

Vollständiges Verfahren: Low-Touch Provisioning

Mit den folgenden Aufgaben können Sie Threat Defense mit CDO auf Ihrem Chassis mithilfe von Low-Touch Provisioning bereitstellen.

Abbildung 35: Vollständiges Verfahren: Low-Touch Provisioning



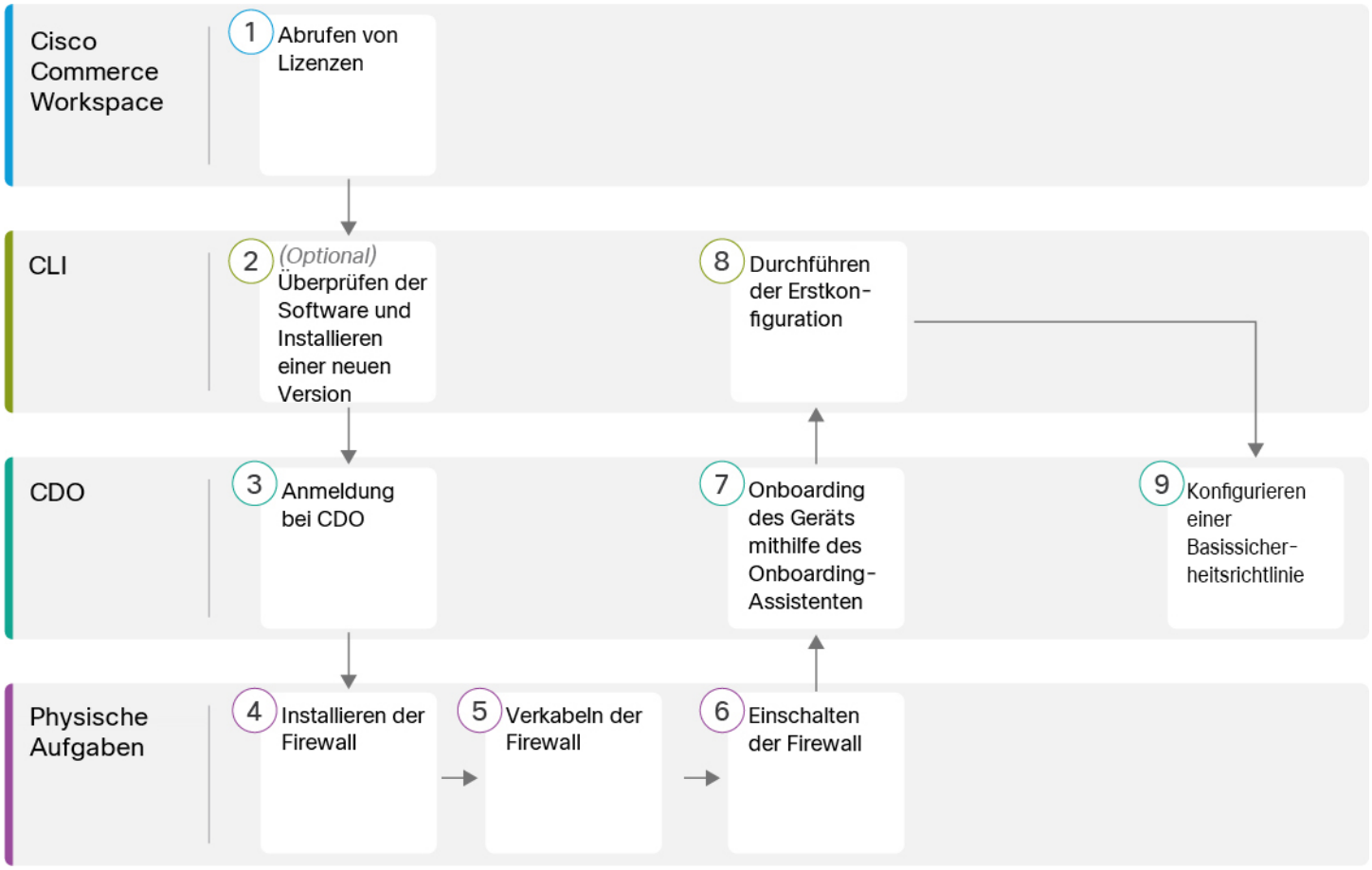
1	Cisco Commerce Workspace (CDO-Admin)	Abrufen von Lizenzen, auf Seite 130
2	CLI (CDO-Admin)	(Optional) Prüfen der Software und Installieren einer neuen Version, auf Seite 131
3	CDO (CDO-Admin)	Anmeldung bei CDO, auf Seite 133
4	Aufgaben in der Zweigstelle (Zweigstellenadmin)	Weitergeben der Firewall-Seriennummer an den Administrator in der Zentrale, auf Seite 137
5	Aufgaben in der Zweigstelle (Zweigstellenadmin)	Installieren der Firewall. Weitere Informationen finden Sie im Hardware-Installationshandbuch.

6	Aufgaben in der Zweigstelle (Zweigstellenadmin)	Verkabeln der Firewall, auf Seite 138
7	Aufgaben in der Zweigstelle (Zweigstellenadmin)	Schalten Sie die Firewall ein., auf Seite 139-
8	CDO (CDO-Admin)	Onboarding eines Geräts mit Low-Touch Provisioning, auf Seite 140
9	CDO (CDO-Admin)	Konfigurieren einer Basissicherheitsrichtlinie, auf Seite 155

Vollständiges Verfahren: Onboarding-Assistent

Lesen Sie die folgenden Aufgaben, um den Threat Defense mit dem Onboarding-Assistenten zu integrieren.

Abbildung 36: Vollständiges Verfahren: Onboarding-Assistent



1	Cisco Commerce Workspace	Abrufen von Lizenzen, auf Seite 130
2	CLI	(Optional) Prüfen der Software und Installieren einer neuen Version, auf Seite 131
3	CDO	Anmeldung bei CDO, auf Seite 133
4	Physische Aufgaben	Installieren der Firewall. Weitere Informationen finden Sie im Hardware-Installationshandbuch.
5	Physische Aufgaben	Verkabeln der Firewall, auf Seite 141
6	Physische Aufgaben	Einschalten der Firewall, auf Seite 143
7	CDO	Onboarding eines Geräts mit dem Onboarding-Assistenten, auf Seite 143
8	CLI oder Device Manager	• Durchführen der Startkonfiguration über die CLI, auf Seite 145. • Durchführen der Startkonfiguration über die Device Manager, auf Seite 150.
9	CDO	Konfigurieren einer Basissicherheitsrichtlinie, auf Seite 155

Vorkonfiguration des Administrators in der Zentrale

In diesem Abschnitt wird beschrieben, wie Sie Funktionslizenzen für Ihre Firewall erhalten, wie Sie eine neue Softwareversion vor der Bereitstellung installieren und wie Sie sich bei CDO anmelden können.

Abrufen von Lizenzen

Alle Lizenzen werden vom CDO für Threat Defense bereitgestellt. Sie können optional die folgenden Funktionslizenzen erwerben:

- **Threat**: Security Intelligence und Next-Generation IPS
- **Malware**: MalwareDefense
- **URL**: URL-Filterung
- **RA VPN**: AnyConnect Plus, AnyConnect Apex oder AnyConnect VPN Only.

Nähere Informationen über die Lizenzierung bei Cisco erhalten Sie unter cisco.com/go/licensingguide

Vorbereitungen

- Sie müssen über ein Masterkonto bei Smart Software Manager verfügen.

Wenn Sie noch kein Konto haben, klicken Sie auf den Link, um ein neues Konto einzurichten. Mit dem Smart Software Manager können Sie ein Masterkonto für Ihr Unternehmen erstellen.

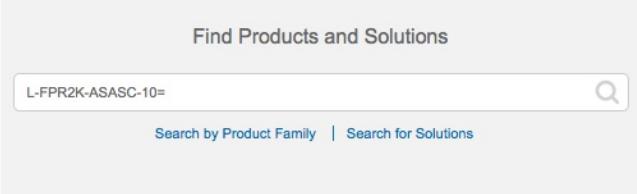
- Ihr Smart Software Licensing-Konto muss für die Strong Encryption-(3DES/AES-)Lizenz qualifiziert sein, um bestimmte Funktionen nutzen zu können (aktiviert mit dem Flag „export-compliance“).

Prozedur

Schritt 1 Stellen Sie sicher, dass Ihr Smart Licensing-Konto die verfügbaren Lizenzen enthält, die Sie benötigen.

Wenn Sie Ihr Gerät bei Cisco oder einem Fachhändler gekauft haben, sollten Ihre Lizenzen mit Ihrem Smart Software License-Konto verknüpft sein. Wenn Sie jedoch selbst Lizenzen hinzufügen müssen, verwenden Sie das Suchfeld **Find Products and Solutions** (Produkte und Lösungen suchen) im Cisco Commerce Workspace. Suchen Sie nach den folgenden Lizenz-PIDs:

Abbildung 37: Lizenzsuche



Hinweis Wenn keine PID gefunden wird, können Sie die PID manuell zu Ihrer Bestellung hinzufügen.

- Kombination aus Threat-, Malware- und URL-Lizenz:
  - L-FPR1010T-TMC =

  Wenn Sie Ihrer Bestellung eine der oben genannten PIDs hinzufügen, können Sie ein befristetes Abonnement auswählen, das einer der folgenden PIDs entspricht:
  - L-FPR1010T-TMC-1Y
  - L-FPR1010T-TMC-3Y
  - L-FPR1010T-TMC-5Y
- VPN für Remotezugriff (RA VPN): Entnehmen Sie die Einzelheiten bitte der Bestellanleitung für Cisco AnyConnect.

Schritt 2 Wenn Sie dies noch nicht getan haben, registrieren Sie CDO im Smart Software Manager.

Für die Registrierung müssen Sie ein Registrierungstoken im Smart Software Manager generieren. Detaillierte Anweisungen finden Sie in der CDO-Dokumentation.

(Optional) Prüfen der Software und Installieren einer neuen Version

Gehen Sie wie folgt vor, um die Softwareversion zu überprüfen und ggf. eine andere Version zu installieren. Wir empfehlen, dass Sie Ihre Zielversion installieren, bevor Sie die Firewall konfigurieren. Alternativ können

Sie ein Upgrade im Anschluss an die Inbetriebnahme durchführen. Ein Upgrade, bei dem Ihre Konfiguration erhalten bleibt, kann jedoch länger dauern als dieses Verfahren.

Welche Version sollte ich ausführen?

Cisco empfiehlt, eine Gold Star-Version auszuführen, die durch einen goldenen Stern neben der Versionsnummer auf der Software-Download-Seite gekennzeichnet ist. Sie können sich auch auf die Release-Strategie beziehen, die in https://www.cisco.com/c/en/us/products/collateral/security/firewalls/bulletin-c25-743178.html beschrieben ist. Beispielsweise beschreibt dieses Bulletin die Nummerierung von kurzfristigen Releases (mit den neuesten Funktionen), die Nummerierung von langfristigen Releases (Wartungsversionen und Patches für einen längeren Zeitraum) oder die Nummerierung von extra langfristigen Releases (Wartungsversionen und Patches für den längsten Zeitraum für die staatliche Zertifizierung).

Vorbereitungen

Bei Low-Touch Provisioning deaktivieren Sie den Low-Touch-Bereitstellungsprozess, wenn Sie sich anmelden und das Kennwort ändern. Sie sollten sich nur dann anmelden und ein neues Image erstellen, wenn Sie bereits wissen, dass Sie die Softwareversion ändern müssen. Wenn Sie sich angemeldet haben und die Low-Touch Provisioning-Funktion ohne Softwareinstallation wiederherstellen möchten, können Sie die Werkseinstellungen wiederherstellen. Weitere Informationen hierzu finden Sie im Handbuch zur FXOS-Fehlerbehebung.

Prozedur

Schritt 1 Schalten Sie die Firewall ein und stellen Sie eine Verbindung zum Konsolenport her. Weitere Informationen finden Sie unter Einschalten der Firewall, auf Seite 143 und Zugriff auf die Threat Defense- und FXOS-CLI, auf Seite 166.

Melden Sie sich mit dem Benutzer **admin** und dem Standardkennwort **Admin123** an.

Sie stellen eine Verbindung zum FXOS-CLI her. Wenn Sie sich zum ersten Mal anmelden, werden Sie aufgefordert, das Kennwort zu ändern. Dieses Kennwort wird auch zur Threat Defense-Anmeldung für SSH verwendet.

Hinweis Wenn das Kennwort bereits geändert wurde und Sie es nicht kennen, müssen Sie das Gerät auf die Werkseinstellungen zurücksetzen, um das Kennwort auf den Standardwert zurückzusetzen. Weitere Informationen hierzu finden Sie im Abschnitt über das Verfahren zum Zurücksetzen auf die Werkseinstellungen im Handbuch zur FXOS-Fehlerbehebung.

Beispiel:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

Schritt 2 Zeigen Sie in der FXOS-CLI die aktuelle Version an.

scope ssa

show app-instance

Beispiel:

```
Firepower# scope ssa
Firepower /ssa # show app-instance

Application Name     Slot ID    Admin State     Operational State    Running Version Startup
 Version Cluster Oper State
-------------------- ---------- --------------- -------------------- ---------------
--------------- ------------------
ftd                  1          Enabled         Online               7.2.0.65        7.2.0.65
        Not Applicable
```

Schritt 3 Wenn Sie eine neue Version installieren möchten, führen Sie diese Schritte aus.

a) Informationen zum Festlegen einer statischen IP-Adresse für die Management-Schnittstelle finden Sie unter Durchführen der Startkonfiguration über die CLI, auf Seite 145. Standardmäßig verwendet die Management-Schnittstelle DHCP.

Sie müssen das neue Image von einem Server herunterladen, auf den über die Managementschnittstelle zugegriffen werden kann.

b) Führen Sie das Verfahren zum Erstellen eines neuen Images im Handbuch zur FXOS-Fehlerbehebung durch.

Schritt 4 Für Low-Touch Provisioning *melden Sie sich nach dem Erstellen eines neuen Image nicht bei der Firewall an*. Durch die Anmeldung wird die Ersteinrichtung gestartet. Low-Touch Provisioning funktioniert nur bei Firewalls mit Erstinstallationen, die nicht eingerichtet wurden.

Anmeldung bei CDO

CDO verwendet Cisco Secure Sign-On als Identitätsanbieter und Duo Security für die Multi-Faktor-Authentifizierung (MFA). CDO erfordert die MFA, die eine zusätzliche Sicherheitsebene zum Schutz Ihrer Benutzeridentität bietet. Die Zwei-Faktor-Authentifizierung, eine Art von MFA, erfordert zwei Komponenten oder Faktoren, um die Identität des Benutzers, der sich bei CDO anmeldet, sicherzustellen.

Der erste Faktor ist ein Benutzername und ein Kennwort, der zweite ein Einmalkennwort (OTP), das bei Bedarf von Duo Security generiert wird.

Nachdem Sie Ihre Cisco Secure Sign-On-Anmeldeinformationen eingerichtet haben, können Sie sich über Ihr Cisco Secure Sign-On-Dashboard bei CDO anmelden. Über das Cisco Secure Sign-On-Dashboard können Sie sich auch bei allen anderen unterstützten Cisco Produkten anmelden.

- Wenn Sie über ein Cisco Secure Sign-On-Konto verfügen, fahren Sie mit Anmeldung bei CDO mit Cisco Secure Sign-On, auf Seite 136 fort.
- Wenn Sie kein Cisco Secure Sign-On-Konto haben, fahren Sie mit Erstellen eines neuen Cisco Secure Sign-On-Kontos, auf Seite 134 fort.

Erstellen eines neuen Cisco Secure Sign-On-Kontos

Der Workflow für die erste Anmeldung besteht aus vier Schritten. Sie müssen alle vier Schritte ausführen.

Vorbereitungen

- **Installieren von DUO Security**: Wir empfehlen Ihnen, die Duo Security-App auf einem Mobiltelefon zu installieren. Lesen Sie die Dokumentation Duo Guide to Two Factor Authentication: Enrollment Guide, wenn Sie Fragen zur Installation von Duo haben.
- **Synchronisierung der Uhrzeit**: Sie werden Ihr Mobilgerät verwenden, um ein Einmalkennwort zu generieren. Es ist wichtig, dass die Uhrzeit Ihres Geräts mit der Echtzeit synchronisiert wird, da das Einmalkennwort zeitbasiert ist. Stellen Sie sicher, dass die Uhrzeit Ihres Geräts richtig eingestellt ist.
- Verwenden Sie eine aktuelle Version von Firefox oder Chrome.

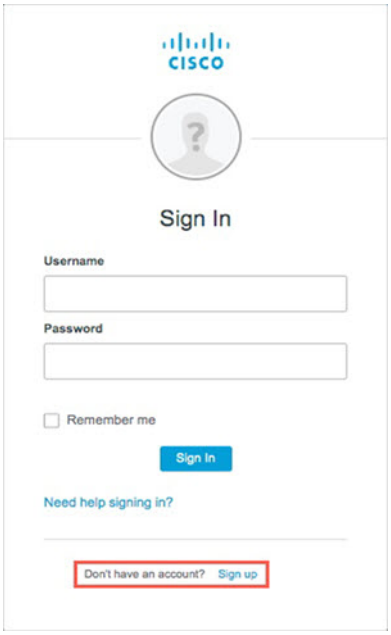
Prozedur

Schritt 1 **Registrieren Sie sich für ein neues Cisco Secure Sign-On-Konto.**

a) Rufen Sie https://sign-on.security.cisco.com auf.

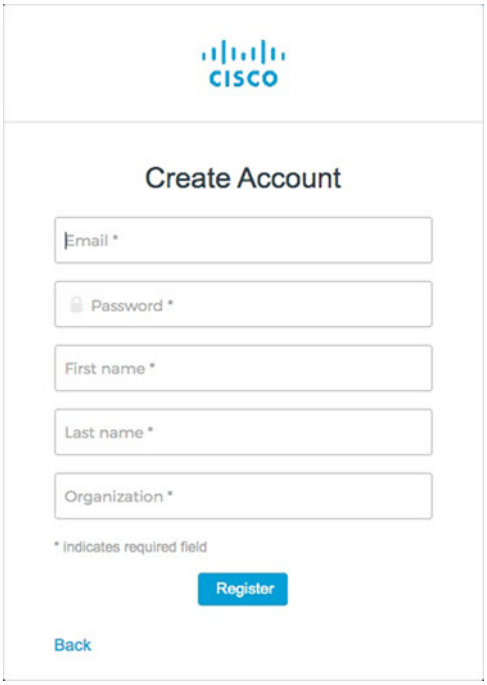
b) Klicken Sie unten auf dem Anmeldebildschirm auf **Sign up** (Anmelden).

Abbildung 38: Cisco SSO-Anmeldung



c) Füllen Sie die Felder im Dialogfeld **Create Account** (Konto erstellen) aus, und klicken Sie auf **Register** (Registrieren).

Abbildung 39: Konto erstellen



Tipp Geben Sie die E-Mail-Adresse ein, mit der Sie sich bei CDO anmelden möchten, und fügen Sie einen Organisationsnamen hinzu, der Ihr Unternehmen repräsentiert.

d) Nachdem Sie auf **Register** (Registrieren) geklickt haben, sendet Cisco Ihnen eine Bestätigungs-E-Mail an die Adresse, unter der Sie sich registriert haben. Öffnen Sie die E-Mail, und klicken Sie auf **Activate Account** (Konto aktivieren).

Schritt 2 **Richten Sie die Multi-Faktor-Authentifizierung mit Duo ein.**

a) Klicken Sie im Bildschirm **Set up multi-factor authentication** (Multi-Faktor-Authentifizierung einrichten) auf **Configure** (Konfigurieren).

b) Klicken Sie auf **Start setup** (Einrichtung starten), und befolgen Sie die Anweisungen, um ein Gerät auszuwählen und die Kopplung dieses Geräts mit Ihrem Konto zu überprüfen.

Weitere Informationen finden Sie in der Dokumentation Duo Guide to Two Factor Authentication: Enrollment Guide. Wenn Sie die Duo-App bereits auf Ihrem Gerät installiert haben, erhalten Sie einen Aktivierungscode für dieses Konto. Duo unterstützt mehrere Konten auf einem Gerät.

c) Klicken Sie am Ende des Assistenten auf **Continue to Login** (Weiter zur Anmeldung).

d) Melden Sie sich mit der Zwei-Faktor-Authentifizierung bei Cisco Secure Sign-On an.

Schritt 3 (optional) **Richten Sie Google Authenticator als zusätzlichen Authentifikator ein.**

a) Wählen Sie das Mobilgerät aus, das Sie mit Google Authenticator koppeln möchten, und klicken Sie auf **Next** (Weiter).

b) Befolgen Sie die Anweisungen des Einrichtungsassistenten, um Google Authenticator einzurichten.

Schritt 4 **Konfigurieren Sie Kontowiederherstellungsoptionen für Ihr Cisco Secure Sign-On-Konto.**

a) Wählen Sie eine Frage und Antwort für „Kennwort vergessen“ aus.

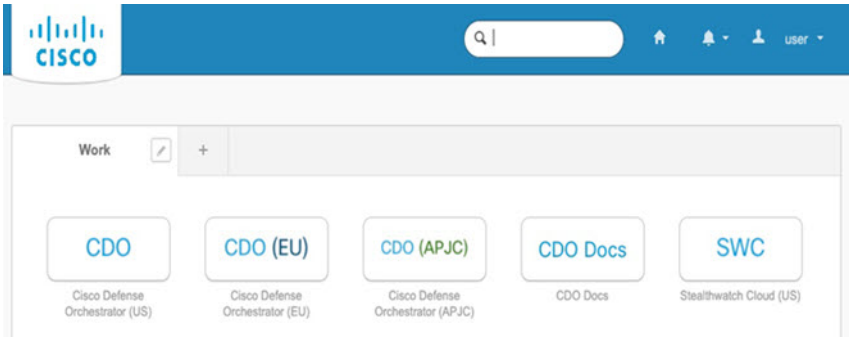
b) Wählen Sie eine Telefonnummer zur Wiederherstellung aus, um Ihr Konto per SMS zurückzusetzen.

c) Wählen Sie ein Sicherheitsbild aus.
d) Klicken Sie auf **Create My Account** (Mein Konto erstellen).

Sie sehen jetzt das Cisco Security Sign-On-Dashboard mit den Kacheln der CDO-App. Möglicherweise sehen Sie auch andere App-Kacheln.

Tipp Sie können die Kacheln auf dem Dashboard ziehen, um sie nach Belieben zu ordnen, Registerkarten zum Gruppieren von Kacheln erstellen und Registerkarten umbenennen.

Abbildung 40: Cisco SSO-Dashboard



Anmeldung bei CDO mit Cisco Secure Sign-On

Melden Sie sich bei CDO an, um Ihr Gerät zu integrieren und zu verwalten.

Vorbereitungen

Cisco Defense Orchestrator (CDO) verwendet Cisco Secure Sign-On als Identitätsanbieter und Duo Security für die Multi-Faktor-Authentifizierung (MFA).

- Um sich bei CDO anzumelden, müssen Sie zunächst Ihr Konto in Cisco Secure Sign-On erstellen und MFA mit Duo konfigurieren. Weitere Informationen hierzu finden Sie unter Erstellen eines neuen Cisco Secure Sign-On-Kontos, auf Seite 134
- Verwenden Sie eine aktuelle Version von Firefox oder Chrome.

Prozedur

Schritt 1 Rufen Sie im Webbrowser https://sign-on.security.cisco.com/ auf.

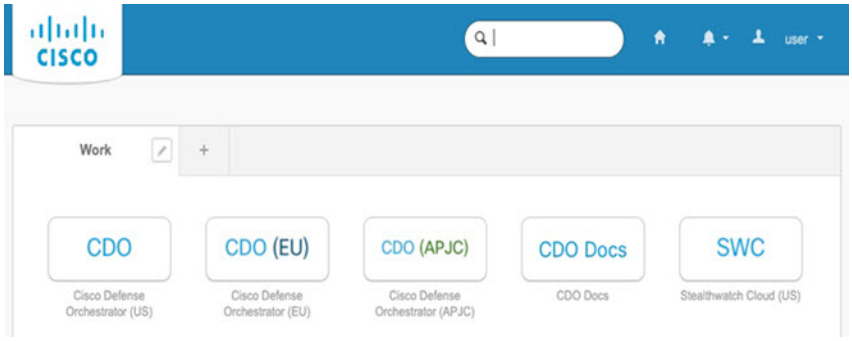
Schritt 2 Geben Sie Ihren **Benutzernamen** und Ihr **Kennwort** ein.

Schritt 3 Klicken Sie auf **Log in** (Anmelden).

Schritt 4 Rufen Sie mit Duo Security einen weiteren Authentifizierungsfaktor ab, und bestätigen Sie Ihre Anmeldung. Das System bestätigt Ihre Anmeldung und zeigt das Cisco Secure Sign-On-Dashboard an.

Schritt 5 Klicken Sie im Cisco Secure Sign-on-Dashboard auf die entsprechende CDO-Kachel. Die Kachel **CDO** leitet Sie zu https://defenseorchestrator.com, die Kachel **CDO (EU)** führt Sie zu https://defenseorchestrator.eu, und die Kachel **CDO (APJC)** leitet Sie zu https://www.apj.cdo.cisco.com.

Abbildung 41: Cisco SSO-Dashboard



Schritt 6 Klicken Sie auf das Authentifikator-Logo, um **Duo Security** oder **Google Authenticator** auszuwählen (falls Sie beide Authentifikatoren eingerichtet haben).

- Wenn Sie bereits einen Benutzerdatensatz für einen vorhandenen Tenant haben, werden Sie bei diesem Tenant angemeldet.
- Wenn Sie bereits über einen Benutzerdatensatz für mehrere Tenants verfügen, können Sie auswählen, zu welchem CDO-Tenant eine Verbindung hergestellt werden soll.
- Wenn Sie noch keinen Benutzerdatensatz für einen vorhandenen Tenant haben, können Sie sich näher über CDO informieren oder ein Testkonto anfordern.

Bereitstellen der Firewall mit Low-Touch Provisioning

Nachdem Sie das Threat Defense-System von der zentralen Hauptgeschäftsstelle erhalten haben, müssen Sie die Firewall nur noch per Kabel anschließen und einschalten, damit sie von der externen Schnittstelle aus auf das Internet zugreifen kann. Der Administrator in der Zentrale kann dann die Konfiguration abschließen.

Weitergeben der Firewall-Seriennummer an den Administrator in der Zentrale

Bevor Sie die Firewall einsetzen oder die Versandverpackung entsorgen, notieren Sie die Seriennummer, damit Sie sie mit dem Administrator in der Zentrale abstimmen können.

Prozedur

Schritt 1 Packen Sie das Chassis und die Chassis-Komponenten aus.

Machen Sie eine Bestandsaufnahme Ihrer Firewall und des Paketinhalts, bevor Sie Kabel anschließen oder die Firewall einschalten. Sie sollten sich auch mit dem Chassis-Layout, den Komponenten und den LEDs vertraut machen.

Schritt 2 Notieren Sie die Seriennummer der Firewall.

Die Seriennummer befindet sich auf der Verpackung. Sie befindet sich auch auf einem Aufkleber an der Unterseite des Firewall-Chassis.

Schritt 3 Senden Sie die Firewall-Seriennummer an den CDO-Netzwerkadministrator in Ihrer IT-Abteilung/Hauptgeschäftsstelle.

Ihr Netzwerkadministrator benötigt die Seriennummer Ihrer Firewall, um die Low-Touch Provisioning zu ermöglichen, eine Verbindung zur Firewall herzustellen und sie per Remotezugriff zu konfigurieren.

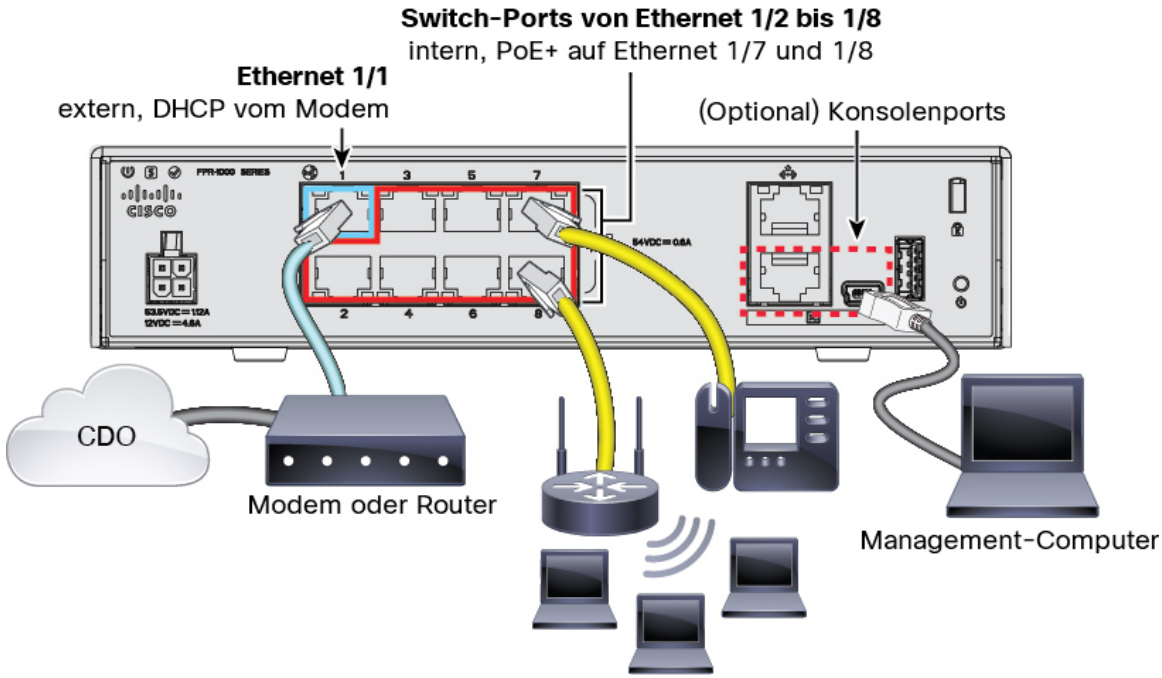
Arbeiten Sie gemeinsam mit dem CDO-Administrator einen Onboarding-Zeitrahmen aus.

Verkabeln der Firewall

In diesem Thema wird beschrieben, wie Sie das Firepower 1010-Gerät mit Ihrem Netzwerk verbinden, damit es von CDO verwaltet werden kann.

Wenn Sie in Ihrer Zweigstelle eine Firewall erhalten haben und diese an Ihr Netzwerk anschließen möchten, sehen Sie sich dieses Video an. Das Video beschreibt Ihre Firewall und die LED-Sequenzen auf der Firewall, die den Status der Firewall anzeigen. Bei Bedarf können Sie den Status der Firewall mit Ihrer IT-Abteilung abklären, indem Sie einfach einen Blick auf die LEDs werfen.

Abbildung 42: Verkabelung des Firepower 1010-Geräts



Low-Touch Provisioning unterstützt die Verbindung mit CDO über Ethernet 1/1 (extern).

Hinweis Ethernet 1/2 bis 1/8 sind als Hardware-Switch-Ports konfiguriert. PoE+ ist auch für Ethernet 1/7 und 1/8 verfügbar.

Prozedur

Schritt 1 Installieren des Chassis Weitere Informationen finden Sie im Hardware-Installationshandbuch.

Schritt 2 Stecken Sie das Netzwerkkabel von der Ethernet 1/1-Schnittstelle in Ihr WAN-Modem (Wide Area Network). Ihr WAN-Modem ist die Verbindung Ihrer Zweigstelle mit dem Internet und wird auch die Route Ihrer Firewall zum Internet sein.

Schritt 3 Verkabeln Sie Ihre internen Endpunkte mit den Switch-Ports (Ethernet 1/2 bis 1/8).

Ethernet 1/7 und 1/8 sind PoE+-Ports.

Schritt 4 (optional) Verbinden Sie den Management-Computer mit dem Konsolenport.

In der Zweigstelle ist die Konsolenverbindung für den täglichen Gebrauch nicht erforderlich. Sie kann jedoch zur Fehlerbehebung erforderlich sein.

Schalten Sie die Firewall ein.

Die Systemstromversorgung wird über das Netzkabel gesteuert. Es gibt keinen Netzschalter.

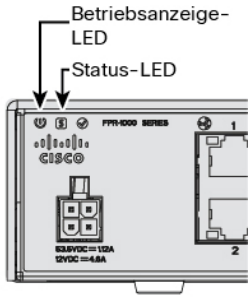
Hinweis Wenn Sie den Threat Defense zum ersten Mal starten, kann die Initialisierung etwa 15 bis 30 Minuten dauern.

Prozedur

Schritt 1 Schließen Sie das Netzkabel am Gerät und dann an einer Steckdose an.

Wenn Sie das Netzkabel an die Stromversorgung anschließen, ist das Gerät automatisch eingeschaltet.

Schritt 2 Prüfen Sie die Betriebs-LED auf der Rückseite oder Oberseite des Geräts; leuchtet sie dauerhaft grün, ist das Gerät eingeschaltet.



Schritt 3 Prüfen Sie die Status-LED auf der Rückseite oder Oberseite des Geräts; wenn sie dauerhaft grün leuchtet, hat das System die Einschaltdiagnose durchlaufen.

Schritt 4 Beobachten Sie die Status-LED auf der Rückseite oder Oberseite des Geräts. Wenn das Gerät ordnungsgemäß bootet, blinkt die Status-LED schnell grün.

Falls ein Problem besteht, blinkt die Status-LED schnell gelb. Wenden Sie sich in diesem Fall an Ihre IT-Abteilung.

Schritt 5 Beobachten Sie die Status-LED auf der Rückseite oder Oberseite des Geräts. Wenn das Gerät eine Verbindung zur Cisco Cloud herstellt, blinkt die Status-LED langsam grün.

Falls ein Problem besteht, blinkt die Status-LED gelb und grün. In diesem Fall hat das Gerät die Cisco Cloud nicht erreicht. Stellen Sie in diesem Fall sicher, dass das Netzwerkkabel mit der Ethernet 1/1-Schnittstelle und dem WAN-Modem verbunden ist. Wenn das Gerät nach der Anpassung des Netzwerkkabels die Cisco Cloud nach weiteren zehn Minuten nicht erreicht, wenden Sie sich an Ihre IT-Abteilung.

Nächste Maßnahme

- Kommunizieren Sie mit Ihrer IT-Abteilung, um Ihren Onboarding-Zeitrahmen und Ihre Aktivitäten zu bestätigen. Sie sollten über einen Kommunikationsplan mit dem CDO-Administrator in Ihrer zentralen Hauptgeschäftsstelle verfügen.
- Nachdem Sie diese Aufgabe abgeschlossen haben, kann Ihr CDO-Administrator das Gerät remote konfigurieren und verwalten. Das war‘s!

Onboarding eines Geräts mit Low-Touch Provisioning

Onboarding von Threat Defense mit Low-Touch Provisioning und der Seriennummer.

Prozedur

Schritt 1 Klicken Sie im CDO-Navigationsbereich auf **Inventory** (Bestand) und dann auf die blaue Plus-Schaltfläche (), um ein Gerät zu **integrieren**.

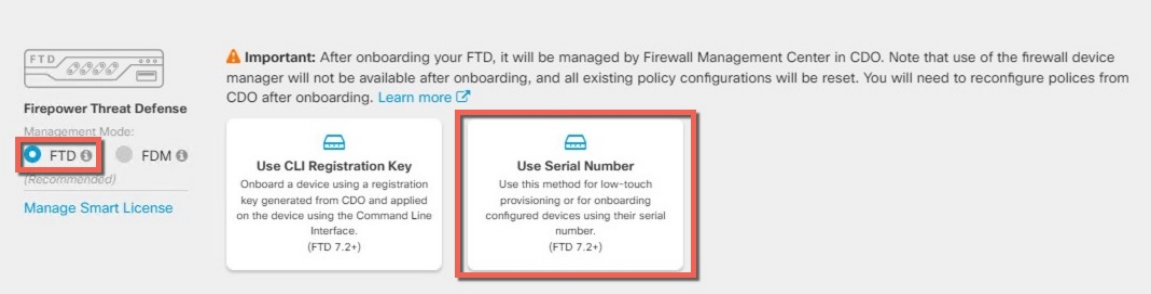
Schritt 2 Wählen Sie die **FTD**-Kachel aus.

Schritt 3 Stellen Sie unter **Management Mode** (Managementmodus) sicher, dass **FTD** ausgewählt ist.

Nachdem Sie **FTD** als Managementmodus ausgewählt haben, können Sie jederzeit auf **Manage Smart License** (Smart License verwalten) klicken, um sich anzumelden oder die vorhandenen für Ihr Gerät verfügbaren Smart Licenses zu ändern. Unter Abrufen von Lizenzen, auf Seite 130 sehen Sie, welche Lizenzen verfügbar sind.

Schritt 4 Wählen Sie **Use Serial Number** (Seriennummer verwenden) als Onboarding-Methode aus.

Abbildung 43: Verwenden der Seriennummer



Schritt 5 Geben Sie im Bereich **Connection** (Verbindung) die **Geräteseriennummer** und den **Gerätenamen** ein, und klicken Sie dann auf **Next** (Weiter).

Schritt 6 Klicken Sie im Bereich **Password Reset** (Kennwortzurücksetzung) auf das Optionsfeld **Yes, this new device has never been logged into or configured for a manager** (Ja, dieses neue Gerät wurde noch nie bei einem Manager angemeldet oder für einen Manager konfiguriert), und klicken Sie dann auf **Next** (Weiter).

Schritt 7 Wählen Sie für **Policy Assignment** (Richtlinienzuweisung) über das Dropdown-Menü eine Zugriffssteuerungsrichtlinie für das Gerät aus. Wenn Sie keine Richtlinien konfiguriert haben, wählen Sie **Default Access Control Policy** (Standard-Zugriffssteuerungsrichtlinie) aus.

Schritt 8 Aktivieren Sie für **Subscription License** (Abonnementlizenz) alle Funktionslizenzen, die Sie aktivieren möchten. Klicken Sie auf **Next** (Weiter).

Schritt 9 (optional) Fügen Sie Ihrem Gerät Bezeichnungen hinzu, um die Seite **Inventory** (Bestand) zu sortieren und zu filtern. Geben Sie eine Bezeichnung ein und wählen Sie die blaue Plus-Schaltfläche (+). Bezeichnungen werden auf das Gerät angewendet, nachdem es in CDO integriert wurde.

Nächste Maßnahme

Wählen Sie auf der Seite **Inventory** (Bestand) das Gerät aus, das Sie gerade integriert haben, und wählen Sie eine der im Bereich **Management** aufgeführten Optionen aus.

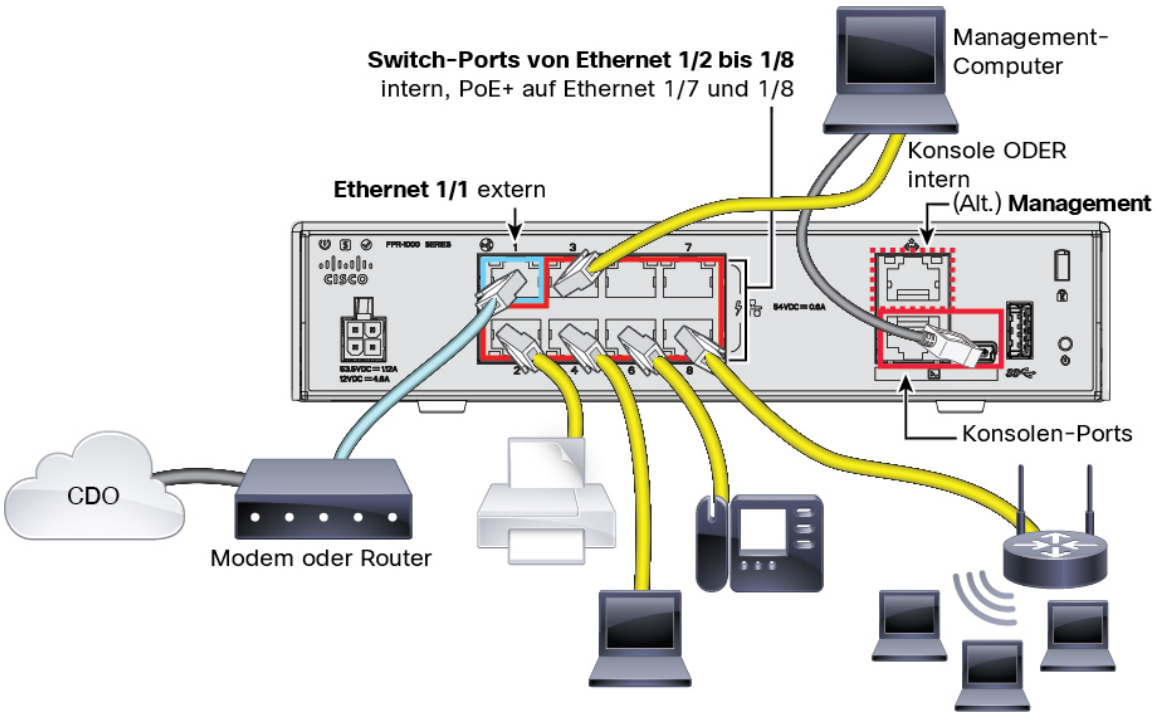
Bereitstellen der Firewall für den Onboarding-Assistenten

In diesem Abschnitt wird beschrieben, wie Sie die Firewall für das Onboarding mithilfe des CDO-Onboarding-Assistenten konfigurieren.

Verkabeln der Firewall

In diesem Thema wird beschrieben, wie Sie das Firepower 1010-Gerät mit Ihrem Netzwerk verbinden, damit es von CDO verwaltet werden kann.

Abbildung 44: Verkabelung des Firepower 1010-Geräts



Sie können eine Verbindung zu CDO über die externe Schnittstelle oder die Management-Schnittstelle herstellen, je nachdem, welche Schnittstelle Sie während der Ersteinrichtung für den Managerzugriff festlegen. Dieses Handbuch zeigt die externe Schnittstelle.

Hinweis Ethernet1/2 bis 1/8 sind als Hardware-Switch-Ports konfiguriert. PoE+ ist auch für Ethernet1/7 und 1/8 verfügbar.

Prozedur

Schritt 1 Installieren des Chassis Weitere Informationen finden Sie im Hardware-Installationshandbuch.

Schritt 2 Verbinden Sie die externe Schnittstelle (Ethernet 1/1) mit Ihrem externen Router.

Sie können alternativ die Management-Schnittstelle für den Managerzugriff verwenden. In diesem Handbuch wird jedoch hauptsächlich der externe Schnittstellenzugriff behandelt, da dies das wahrscheinlichste Szenario für Remote-Zweigstellen ist.

Schritt 3 Verkabeln Sie Ihre internen Endpunkte mit den Switch-Ports (Ethernet1/2 bis 1/8).

Ethernet 1/7 und 1/8 sind PoE+-Ports.

Schritt 4 Verbinden Sie den Management-Computer mit dem Konsolenport oder einer internen Schnittstelle.

Wenn Sie die Ersteinrichtung über die CLI durchführen, müssen Sie eine Verbindung zum Konsolenport herstellen. Der Konsolenport kann auch zur Fehlerbehebung erforderlich sein. Wenn Sie die Ersteinrichtung mit Device Manager durchführen, stellen Sie eine Verbindung zu einer internen Schnittstelle her.

Einschalten der Firewall

Die Systemstromversorgung wird über das Netzkabel gesteuert. Es gibt keinen Netzschalter.

Hinweis Wenn Sie den Threat Defense zum ersten Mal starten, kann die Initialisierung etwa 15 bis 30 Minuten dauern.

Vorbereitungen

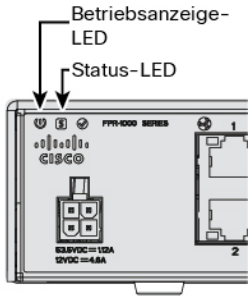
Es ist wichtig, dass Sie Ihr Gerät zuverlässig mit Strom versorgen (z. B. mit einer unterbrechungsfreien Stromversorgung (USV)). Ein Stromausfall ohne vorheriges Herunterfahren kann zu ernsthaften Schäden am Dateisystem führen. Im Hintergrund laufen ständig viele Prozesse ab, und eine Unterbrechung der Stromversorgung ermöglicht kein ordnungsgemäßes Herunterfahren des Systems.

Prozedur

Schritt 1 Schließen Sie das Netzkabel am Gerät und dann an einer Steckdose an.

Wenn Sie das Netzkabel an die Stromversorgung anschließen, ist das Gerät automatisch eingeschaltet.

Schritt 2 Prüfen Sie die Betriebs-LED auf der Rückseite oder Oberseite des Geräts; leuchtet sie dauerhaft grün, ist das Gerät eingeschaltet.



Schritt 3 Prüfen Sie die Status-LED auf der Rückseite oder Oberseite des Geräts; wenn sie dauerhaft grün leuchtet, hat das System die Einschaltdiagnose durchlaufen.

Onboarding eines Geräts mit dem Onboarding-Assistenten

Onboarding des Threat Defense mit dem Onboarding-Assistenten mithilfe eines CLI-Registrierungsschlüssels

Prozedur

Schritt 1 Klicken Sie im CDO-Navigationsbereich auf **Inventory** (Bestand) und dann auf die blaue Plus-Schaltfläche (+), um ein Gerät zu **integrieren**.

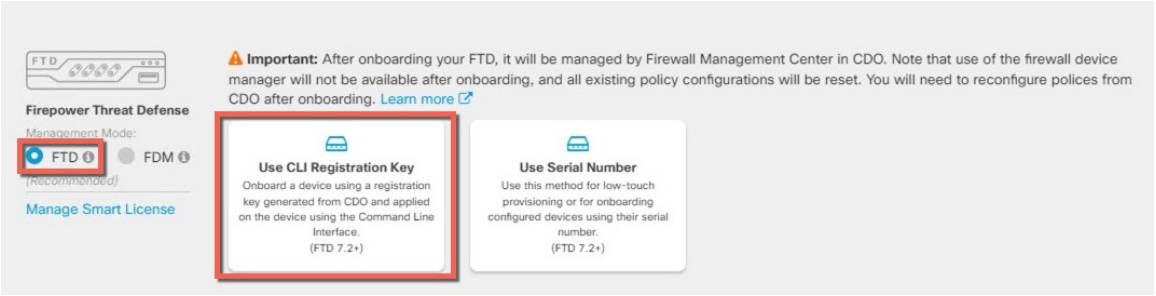
Schritt 2 Wählen Sie die **FTD**-Kachel.

Schritt 3 Stellen Sie unter **Managementmodus** sicher, dass **FTD** ausgewählt ist.

Nachdem Sie **FTD** als Managementmodus ausgewählt haben, können Sie jederzeit auf **Manage Smart License** (Smart License verwalten) klicken, um sich anzumelden oder die vorhandenen für Ihr Gerät verfügbaren Smart Licenses zu ändern. Unter Abrufen von Lizenzen, auf Seite 130 finden Sie die verfügbaren Lizenzen.

Schritt 4 Wählen Sie **Use CLI Registration Key** (CLI-Registrierungsschlüssel verwenden) als Onboarding-Methode aus.

Abbildung 45: Verwenden des CLI-Registrierungsschlüssels



Schritt 5 Geben Sie den **Gerätenamen** ein und klicken Sie auf **Next** (Weiter).

Schritt 6 Wählen Sie für **Policy Assignment** (Richtlinienzuweisung) über das Dropdown-Menü eine Zugriffssteuerungsrichtlinie für das Gerät aus. Wenn Sie keine Richtlinien konfiguriert haben, wählen Sie **Default Access Control Policy** (Standard-Zugriffssteuerungsrichtlinie) aus.

Schritt 7 Klicken Sie für die **Abonnementlizenz** auf das Optionsfeld **Physical FTD Device** (Physisches FTD-Gerät), und aktivieren Sie dann alle Funktionslizenzen, die Sie aktivieren möchten. Klicken Sie auf **Next** (Weiter).

Schritt 8 Für den **CLI-Registrierungsschlüssel** generiert CDO einen Befehl mit dem Registrierungsschlüssel und anderen Parametern. Sie müssen diesen Befehl kopieren und in der anfänglichen Konfiguration von Threat Defense verwenden.

configure manager add *cdo_hostname registration_key nat_id display_name*

Abschließen der Erstkonfiguration mit der CLI oder mithilfe von Device Manager:

- Durchführen der Startkonfiguration über die CLI, auf Seite 145: Kopieren Sie diesen Befehl in der FTD-CLI, nachdem Sie das Startskript abgeschlossen haben.
- Durchführen der Startkonfiguration über die Device Manager, auf Seite 150: Kopieren Sie die Teile des Befehls *cdo_hostname*, *registration_key* und *nat_id* in die Felder **Management Center/CDO-Hostname/IP-Adresse**, **Management Center/CDO-Registrierungsschlüssel** und **NAT-ID**.

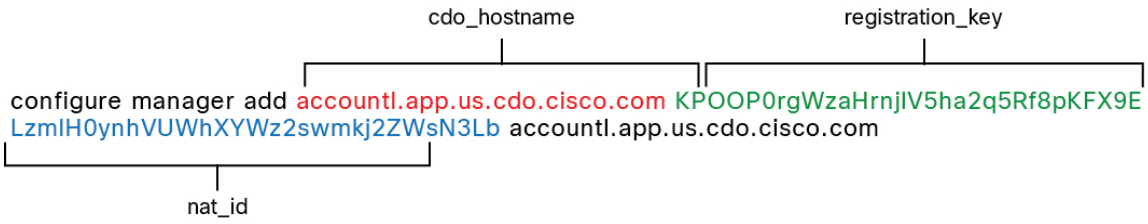
Beispiel:

Beispielbefehl für die CLI-Einrichtung:

```
configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.cdo.cisco.com
```

Beispielbefehlskomponenten für die GUI-Einrichtung:

Abbildung 46: configure manager add Befehlskomponenten



Schritt 9 Klicken Sie im Onboarding-Assistenten auf **Next** (Weiter), um mit der Registrierung des Geräts zu beginnen.

Schritt 10 (optional) Fügen Sie Ihrem Gerät Bezeichnungen hinzu, um die Seite **Inventory** (Bestand) zu sortieren und zu filtern. Geben Sie eine Kennzeichnung ein und wählen Sie die blaue Plus-Schaltfläche ( ). Die Kennzeichnungen werden dem Gerät nach dem Onboarding in CDO hinzugefügt.

Nächste Maßnahme

Wählen Sie auf der Seite **Inventory** (Bestand) das Gerät aus, das Sie gerade integriert haben, und wählen Sie eine der im Bereich **Management** aufgeführten Optionen aus.

Durchführen der Erstkonfiguration

Führen Sie die Threat Defense-Erstkonfiguration von mit Device Manager oder über die CLI durch.

Durchführen der Startkonfiguration über die CLI

Stellen Sie eine Verbindung zur Threat Defense-CLI her, um die Ersteinrichtung durchzuführen. Wenn Sie die CLI für die Erstkonfiguration verwenden, werden nur die Einstellungen für die Management-Schnittstelle und die Managerzugriffsschnittstelle beibehalten. Wenn Sie die Ersteinrichtung mithilfe von Device Manager ausführen, werden *alle* in Device Manager abgeschlossenen Schnittstellenkonfigurationen beibehalten, wenn Sie für das Management zu CDO wechseln, zusätzlich zu den Einstellungen für die Management-Schnittstelle und die Managerzugriffsschnittstelle. Beachten Sie, dass andere Standardkonfigurationseinstellungen, wie z. B. die Zugriffskontrollrichtlinie, nicht beibehalten werden.

Prozedur

Schritt 1 Stellen Sie eine Verbindung zur Threat Defense-CLI auf dem Konsolenport her.

Der Konsolenport wird mit der FXOS-CLI verbunden.

Schritt 2 Melden Sie sich mit dem Benutzernamen **admin** und dem Kennwort **Admin123** an.

Wenn Sie sich zum ersten Mal bei FXOS anmelden, werden Sie aufgefordert, das Kennwort zu ändern. Dieses Kennwort wird auch zur Threat Defense-Anmeldung für SSH verwendet.

Hinweis Wenn das Kennwort bereits geändert wurde und Sie es nicht kennen, müssen Sie ein neues Image des Geräts erstellen, um das Kennwort auf den Standardwert zurückzusetzen. Weitere Informationen hierzu finden Sie im Abschnitt über das Verfahren zum Erstellen eines neuen Images im Handbuch zur FXOS-Fehlerbehebung.

Beispiel:

```
firepower login: admin
Password: Admin123
Successful login attempts for user 'admin' : 1

[...]

Hello admin. You must change your password.
Enter new password: ********
Confirm new password: ********
Your password was updated successfully.

[...]

firepower#
```

Schritt 3 Stellen Sie eine Verbindung zur Threat Defense-CLI her.

connect ftd

Beispiel:

```
firepower# connect ftd
>
```

Schritt 4 Wenn Sie sich zum ersten Mal bei Threat Defense anmelden, werden Sie aufgefordert, den Endbenutzerlizenzvertrag (EULA) zu akzeptieren. Anschließend wird das CLI-Einrichtungsskript für die Einstellungen der Management-Schnittstelle angezeigt.

Es werden die Einstellungen der Management-Schnittstelle verwendet, auch wenn Sie den Managerzugriff auf einer Datenschnittstelle aktivieren.

Hinweis Sie können den CLI-Einrichtungsassistenten nur wiederholen, wenn Sie die Konfiguration löschen, zum Beispiel im Rahmen der Neuerstellung eines Images. Alle diese Einstellungen können jedoch später in der CLI mit den Befehlen **configure network** geändert werden. Siehe Befehlsreferenz für Secure Firewall Threat Defense.

Standardwerte oder zuvor eingegebene Werte werden in Klammern angezeigt. Um zuvor eingegebene Werte zu akzeptieren, drücken Sie die **Eingabetaste**.

Beachten Sie die folgenden Orientierungshilfen:

- **Configure IPv4 via DHCP or manually?** (IPv4 über DHCP oder manuell konfigurieren?): Wählen Sie **manual** (manuell) aus. Auch wenn Sie die Management-Schnittstelle nicht verwenden möchten, müssen Sie eine IP-Adresse festlegen, z. B. eine private Adresse. Sie können keine Datenschnittstelle für das Management konfigurieren, wenn die Management-Schnittstelle auf DHCP eingestellt ist, da die Standardroute, bei der es sich um **data-interfaces** handeln muss (siehe nächster Punkt), mit einer vom DHCP-Server empfangenen Route überschrieben werden könnte.

- **Geben Sie das IPv4-Standardgateway für die Management-Schnittstelle ein** – Setzen Sie das Gateway auf **data-interfaces**. Diese Einstellung leitet den Management-Traffic über die Backplane weiter, sodass er über die Managerzugriffsdatenschnittstelle geleitet werden kann.
- **Manage the device locally?** (Das Gerät lokal verwalten?): Geben Sie **no** (Nein) ein, um CDO zu verwenden. Die Antwort **yes** (Ja) bedeutet, dass Sie stattdessen Device Manager verwenden werden.
- **Configure firewall mode?** (Firewall-Modus konfigurieren?): Geben Sie **routed** (geroutet) ein. Externer Managerzugriff wird nur im Routing-Firewall-Modus unterstützt.

Beispiel:

```
You must accept the EULA to continue.
Press <ENTER> to display the EULA:
End User License Agreement
[...]

Please enter 'YES' or press <ENTER> to AGREE to the EULA:

System initialization in progress.  Please stand by.
You must change the password for 'admin' to continue.
Enter new password: ********
Confirm new password: ********
You must configure the network to continue.
You must configure at least one of IPv4 or IPv6.
Do you want to configure IPv4? (y/n) [y]:
Do you want to configure IPv6? (y/n) [n]:
Configure IPv4 via DHCP or manually? (dhcp/manual) [manual]:
Enter an IPv4 address for the management interface [192.168.45.45]: 10.10.10.15
Enter an IPv4 netmask for the management interface [255.255.255.0]: 255.255.255.192
Enter the IPv4 default gateway for the management interface [data-interfaces]:
Enter a fully qualified hostname for this system [firepower]: ftd-1.cisco.com
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.220.220]:
Enter a comma-separated list of search domains or 'none' []:
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'

Manage the device locally? (yes/no) [yes]: no
Configure firewall mode? (routed/transparent) [routed]:
Configuring firewall mode ...

Update policy deployment information
    - add device configuration
    - add network discovery
    - add system policy

You can register the sensor to a Firepower Management Center and use the
Firepower Management Center to manage it. Note that registering the sensor
to a Firepower Management Center disables on-sensor Firepower Services
management capabilities.

When registering the sensor to a Firepower Management Center, a unique
alphanumeric registration key is always required.  In most cases, to register
a sensor to a Firepower Management Center, you must provide the hostname or
the IP address along with the registration key.
'configure manager add [hostname | ip address ] [registration key ]'

However, if the sensor and the Firepower Management Center are separated by a
NAT device, you must enter a unique NAT ID, along with the unique registration
key.
'configure manager add DONTRESOLVE [registration key ] [ NAT ID ]'
```

```
Later, using the web interface on the Firepower Management Center, you must
use the same registration key and, if necessary, the same NAT ID when you add
this sensor to the Firepower Management Center.
>
```

Schritt 5 Konfigurieren Sie die externe Schnittstelle für den Managerzugriff.

configure network management-data-interface

Anschließend werden Sie aufgefordert, grundlegende Netzwerkeinstellungen für die externe Schnittstelle zu konfigurieren. Lesen Sie die folgenden Informationen zur Verwendung dieses Befehls:

- Die Management-Schnittstelle kann DHCP nicht verwenden, wenn Sie eine Datenschnittstelle für das Management verwenden möchten. Wenn Sie die IP-Adresse bei der Ersteinrichtung nicht manuell festgelegt haben, können Sie sie jetzt mit dem Befehl **configure network** {**ipv4** | **ipv6**} **manual** festlegen. Falls Sie das Gateway der Management-Schnittstelle noch nicht auf **data-interfaces** gesetzt haben, wird es jetzt mit diesem Befehl festgelegt.
- Wenn Sie Threat Defense zu CDO hinzufügen, erkennt und verwaltet CDO die Schnittstellenkonfiguration, einschließlich der folgenden Einstellungen: Schnittstellenname und IP-Adresse, statische Route zum Gateway, DNS-Server und DDNS-Server. Weitere Informationen zur Konfiguration des DNS-Servers finden Sie unten. In CDO können Sie später Änderungen an der Konfiguration der Managerzugriffsschnittstelle vornehmen. Nehmen Sie jedoch keinesfalls Änderungen vor, die verhindern können, dass Threat Defense oder CDO die Managementverbindung wieder herstellt. Für den Fall, dass die Managementverbindung unterbrochen wird, enthält Threat Defense den Befehl **configure policy rollback** zum Wiederherstellen der vorherigen Bereitstellung.
- Wenn Sie eine DDNS-Server-Update-URL konfigurieren, fügt Threat Defense automatisch Zertifikate für alle wichtigen Zertifizierungsstellen aus dem Cisco Trusted Root CA-Paket hinzu, damit Threat Defense das DDNS-Serverzertifikat für die HTTPS-Verbindung validieren kann. Threat Defense unterstützt jeden DDNS-Server, der die DynDNS Remote API-Spezifikation (https://help.dyn.com/remote-access-api/) verwendet.
- Dieser Befehl legt den DNS-Server der *Datenschnittstelle* fest. Der Management-DNS-Server, den Sie mit dem Einrichtungsskript (oder mit dem Befehl **configure network dns servers**) festlegen, wird für den Management-Traffic verwendet. Der Daten-DNS-Server wird für DDNS (sofern konfiguriert) oder für auf diese Schnittstelle angewendete Sicherheitsrichtlinien verwendet.

  Im CDO werden die DNS-Server der Datenschnittstelle in der Richtlinie für Plattformeinstellungen konfiguriert, die Sie diesem Threat Defense-System zuweisen. Wenn Sie Threat Defense zum CDO hinzufügen, werden die lokalen Einstellungen beibehalten, und die DNS-Server werden *keiner* Richtlinie für Plattformeinstellungen hinzugefügt. Wenn Sie jedoch später dem Threat Defense-System eine Richtlinie für Plattformeinstellungen zuweisen, die eine DNS-Konfiguration enthält, überschreibt diese Konfiguration die lokale Einstellung. Wir empfehlen Ihnen, die DNS-Plattformeinstellungen aktiv mit dieser Einstellung zu konfigurieren, um CDO und Threat Defense zu synchronisieren.

  Außerdem werden lokale DNS-Server von CDO nur beibehalten, wenn die DNS-Server bei der ersten Registrierung erkannt wurden. Wenn Sie beispielsweise das Gerät über die Management-Schnittstelle registriert haben, aber später eine Datenschnittstelle mit dem Befehl **configure network management-data-interface** konfigurieren, müssen Sie alle diese Einstellungen in CDO, einschließlich der DNS-Server, manuell so konfigurieren, dass sie mit der Threat Defense-Konfiguration übereinstimmen.
- Sie können die Management-Schnittstelle ändern, nachdem Sie Threat Defense beim CDO registriert haben, und zwar entweder in die Management-Schnittstelle oder eine andere Datenschnittstelle.
- Für diese Schnittstelle wird der FQDN verwendet, den Sie im Einrichtungsassistenten festgelegt haben.

- Sie können die gesamte Gerätekonfiguration als Teil des Befehls löschen. Diese Option kann in einem Wiederherstellungsszenario sinnvoll sein, aber wir empfehlen nicht, sie für die Ersteinrichtung oder den normalen Betrieb zu verwenden.
- Um das Datenmanagement zu deaktivieren, geben Sie den Befehl **configure network management-data-interface disable** ein.

Beispiel:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]:
IP address (manual / dhcp) [dhcp]:
DDNS server update URL [none]:
https://deanwinchester:pa$$w0rd17@domains.example.com/nic/update?hostname=<h>&myip=<a>
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Beispiel:

```
> configure network management-data-interface
Data interface to use for management: ethernet1/1
Specify a name for the interface [outside]: internet
IP address (manual / dhcp) [dhcp]: manual
IPv4/IPv6 address: 10.10.6.7
Netmask/IPv6 Prefix: 255.255.255.0
Default Gateway: 10.10.6.1
Comma-separated list of DNS servers [none]: 208.67.222.222,208.67.220.220
DDNS server update URL [none]:
Do you wish to clear all the device configuration before applying ? (y/n) [n]:

Configuration done with option to allow manager access from any network, if you wish to
change the manager access network
use the 'client' option in the command 'configure network management-data-interface'.

Setting IPv4 network configuration.
Network settings changed.

>
```

Schritt 6 Identifizieren Sie das CDO, das Threat Defense verwaltet, mit dem vom CDO generierten Befehl **configure manager add**. Siehe Onboarding eines Geräts mit dem Onboarding-Assistenten, auf Seite 143, um den Befehl zu generieren.

Beispiel:

```
> configure manager add account1.app.us.cdo.cisco.com KPOOP0rgWzaHrnj1V5ha2q5Rf8pKFX9E
Lzm1HOynhVUWhXYWz2swmkj2ZWsN3Lb account1.app.us.cdo.cisco.com
Manager successfully configured.
```

Durchführen der Startkonfiguration über die Device Manager

Stellen Sie eine Verbindung zur Device Manager her, um die Ersteinrichtung des Threat Defense-Systems durchzuführen. Wenn Sie die Ersteinrichtung mit Device Manager durchführen, werden *alle* in Device Manager abgeschlossenen Schnittstellenkonfigurationen beibehalten, wenn Sie für das Management zu CDO wechseln, zusätzlich zu den Einstellungen für die Management-Schnittstelle und den Managerzugriff. Beachten Sie, dass andere Standardkonfigurationseinstellungen, wie z. B. die Zugriffskontrollrichtlinie oder Sicherheitszonen, nicht beibehalten werden. Wenn Sie die CLI verwenden, werden nur die Management-Schnittstellen- und Managerzugriffseinstellungen beibehalten (z. B. wird die standardmäßige interne Schnittstellenkonfiguration nicht beibehalten).

Prozedur

Schritt 1 Verbinden Sie Ihren Management-Computer mit einer der folgenden Schnittstellen: Ethernet 1/2 bis 1/8.

Schritt 2 Melden Sie sich bei Device Manager an.

a) Geben Sie die folgende URL in Ihren Browser ein: **https://192.168.95.1**
b) Melden Sie sich mit dem Benutzernamen **admin** und dem Standardkennwort **Admin123** an.
c) Sie werden aufgefordert, den Endbenutzerlizenzvertrag zu lesen und zu akzeptieren und das Administratorkennwort zu ändern.

Schritt 3 Verwenden Sie bei der ersten Anmeldung in Device Manager den Einrichtungsassistenten, um die Erstkonfiguration abzuschließen. Sie können den Einrichtungsassistenten optional überspringen, indem Sie unten auf der Seite auf **Skip device setup** (Geräteeinrichtung überspringen) klicken.

Nachdem Sie den Einrichtungsassistenten abgeschlossen haben, haben Sie zusätzlich zur Standardkonfiguration für die interne Schnittstelle (Ethernet 1/2 bis 1/8, die Switch-Ports auf VLAN1 sind) eine Konfiguration für eine externe Schnittstelle (Ethernet 1/1), die beibehalten wird, wenn Sie zum CDO-Management wechseln.

a) Konfigurieren Sie die folgenden Optionen für die externe Schnittstelle und die Management-Schnittstellen, und klicken Sie auf **Next** (Weiter).

1. **Outside Interface Address** (Externe Schnittstellenadresse): Diese Schnittstelle ist in der Regel das Internet-Gateway und kann als Managerzugriffsschnittstelle verwendet werden. Sie können während der Ersteinrichtung des Geräts keine alternative externe Schnittstelle auswählen. Die erste Datenschnittstelle ist die standardmäßige externe Schnittstelle.

   Wenn Sie eine andere externe (oder interne) Schnittstelle für den Managerzugriff verwenden möchten, müssen Sie sie nach Abschluss des Einrichtungsassistenten manuell konfigurieren.

   Configure IPv4 (IPv4 konfigurieren): Die IPv4-Adresse für die externe Schnittstelle. Sie können DHCP verwenden oder eine statische IP-Adresse, eine Subnetzmaske und ein Gateway manuell eingeben. Sie können auch **Off** (Aus) auswählen, wenn keine IPv4-Adresse konfiguriert werden soll. Sie können PPPoE nicht mit dem Einrichtungsassistenten konfigurieren. PPPoE kann erforderlich sein, wenn die Schnittstelle mit einem DSL-Modem, Kabelmodem oder einem anderen ISP-Anschluss verbunden ist und Ihr ISP PPPoE verwendet, um Ihre IP-Adresse bereitzustellen. Sie können PPPoE konfigurieren, nachdem Sie den Assistenten abgeschlossen haben.

   Configure IPv6 (IPv6 konfigurieren): Die IPv6-Adresse für die externe Schnittstelle. Sie können DHCP verwenden oder eine statische IP-Adresse, ein Präfix und ein Gateway manuell eingeben. Sie können auch **Off** (Aus) auswählen, wenn keine IPv6-Adresse konfiguriert werden soll.

2. **Management-Schnittstelle**

Die Einstellungen der Management-Schnittstelle werden nicht angezeigt, wenn Sie die Ersteinrichtung über die CLI durchgeführt haben.

Es werden die Einstellungen der Management-Schnittstelle verwendet, auch wenn Sie den Managerzugriff auf einer Datenschnittstelle aktivieren. Beispiel: Der Management-Traffic, der über die Backplane durch die Datenschnittstelle geleitet wird, löst FQDNs über die DNS-Server der Management-Schnittstelle und nicht über die DNS-Server der Datenschnittstelle auf.

DNS Servers (DNS-Server): Der DNS-Server für die Managementadresse des Systems. Geben Sie eine oder mehrere Adressen von DNS-Servern für die Namensauflösung ein. Der Standardwert sind die öffentlichen DNS-Server von OpenDNS. Wenn Sie die Felder bearbeiten und zum Standardwert zurückkehren möchten, klicken Sie auf **OpenDNS** verwenden, um die entsprechenden IP-Adressen erneut in die Felder zu laden.

Firewall Hostname (Firewall-Host-Name): Der Host-Name für die Managementadresse des Systems.

b) Konfigurieren Sie die **Time Setting (NTP)** (Zeiteinstellung (NTP)), und klicken Sie auf **Next** (Weiter).

1. **Time Zone** (Zeitzone): Wählen Sie die Zeitzone für das System aus.
2. **NTP Time Server** (NTP-Zeitserver): Wählen Sie aus, ob Sie die Standard-NTP-Server verwenden oder die Adressen Ihrer NTP-Server manuell eingeben möchten. Sie können mehrere Server hinzufügen, um Backups bereitzustellen.

c) Wählen Sie **Start 90 day evaluation period without registration** (90-tägigen Evaluierungszeitraum ohne Registrierung starten) aus.

Registrieren Sie das Threat Defense-System nicht beim Smart Software Manager. Die gesamte Lizenzierung erfolgt in CDO.

d) Klicken Sie auf **Finish** (Fertigstellen).

e) Sie werden aufgefordert, **Cloud Management** (Cloud-Management) oder **Standalone** (Eigenständig) zu wählen. Wählen Sie für Cloud-basiertes Management Center die Option **Standalone** und dann **Got It** aus.

Die Option **Cloud Management** ist für ältere CDO/FDM-Funktionen vorgesehen.

Schritt 4 (Möglicherweise erforderlich) Konfigurieren Sie die Management-Schnittstelle. Weitere Informationen finden Sie in der Management-Schnittstelle unter **Device** > **Interfaces** (Gerät > Schnittstellen).

Für die Management-Schnittstelle muss das Gateway auf Datenschnittstellen eingestellt sein. Standardmäßig erhält die Management-Schnittstelle eine IP-Adresse und ein Gateway von DHCP. Wenn Sie kein Gateway von DHCP erhalten (z. B. haben Sie diese Schnittstelle nicht mit einem Netzwerk verbunden), verwendet das Gateway standardmäßig Datenschnittstellen, und Sie müssen nichts konfigurieren. Wenn Sie ein Gateway von DHCP erhalten haben, müssen Sie diese Schnittstelle stattdessen mit einer statischen IP-Adresse konfigurieren und das Gateway auf Datenschnittstellen einstellen.

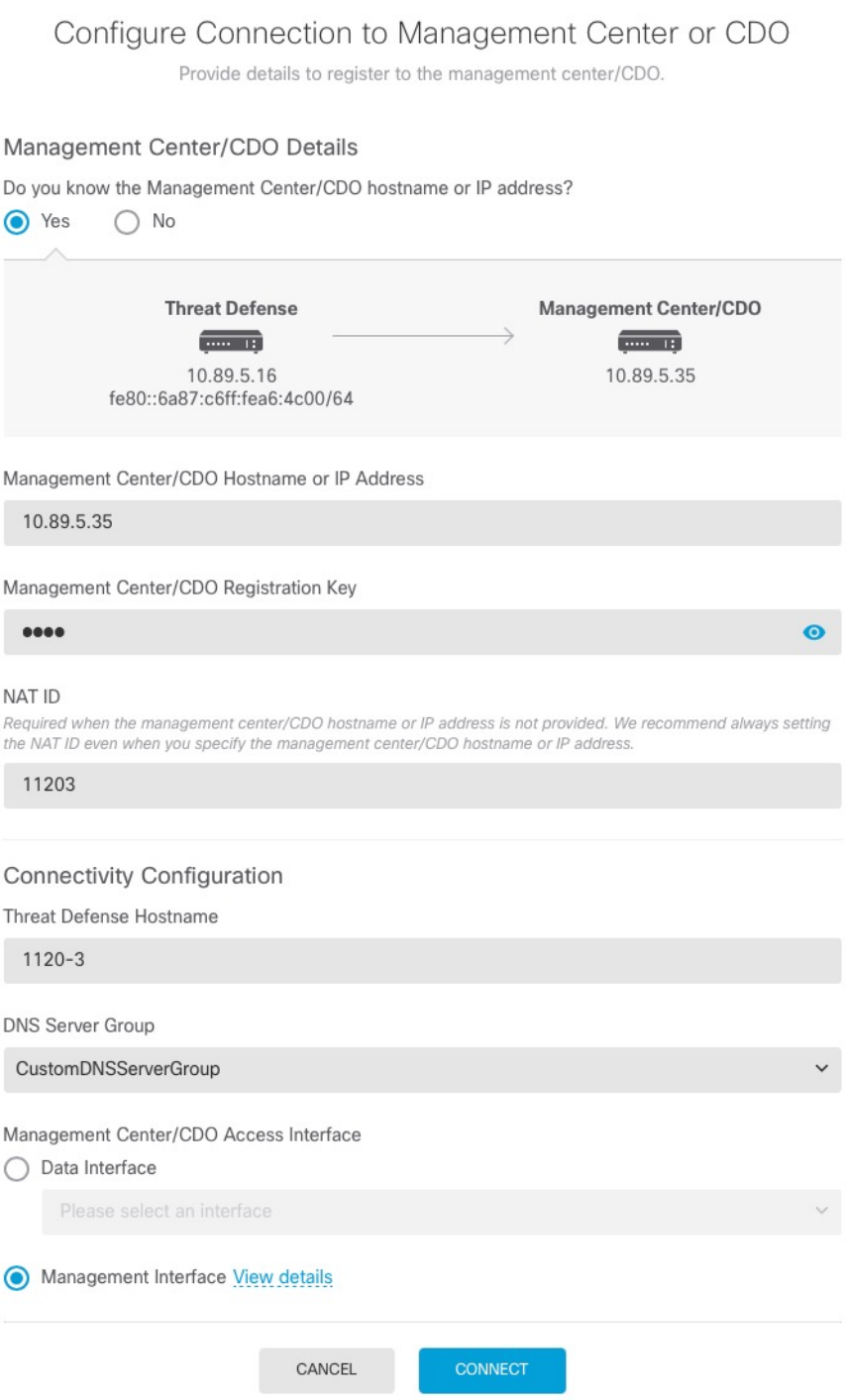
Schritt 5 Wenn Sie zusätzliche Schnittstellen konfigurieren möchten, einschließlich einer anderen als der externen oder internen Schnittstelle, die Sie für den Managerzugriff verwenden möchten, wählen Sie **Device** (Gerät), und klicken Sie dann auf den Link in der Schnittstellenübersicht (**Interfaces**).

Unter Konfigurieren der Firewall in Device Manager, auf Seite 115 finden Sie weitere Informationen zum Konfigurieren von Schnittstellen in Device Manager. Andere Device Manager-Konfigurationen werden nicht beibehalten, wenn Sie das Gerät bei CDO registrieren.

Schritt 6 Wählen Sie **Device** > **System Settings** > **Central Management**, und klicken Sie auf **Proceed** (Fortfahren), um das Management Center-Management einzurichten.

Schritt 7 Konfigurieren der **Management Center-/CDO-Details**.

Abbildung 47: Management Center-/CDO-Details



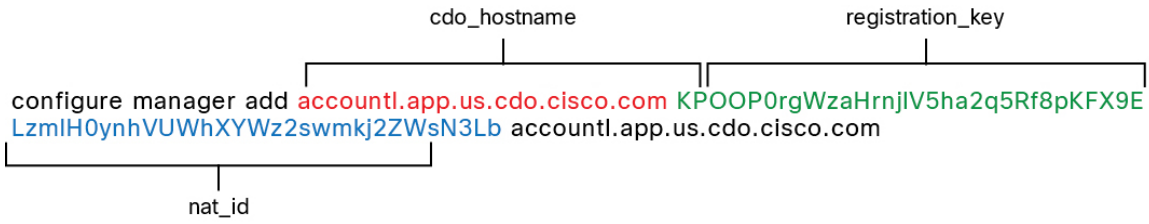
a) Klicken Sie unter **Do you know the Management Center/CDO hostname or IP address** (Kennen Sie den Management Center-/CDO-Hostnamen oder die IP-Adresse?) auf **Yes** (Ja).

CDO generiert den Befehl **configure manager add**. Siehe Onboarding eines Geräts mit dem Onboarding-Assistenten, auf Seite 143, um den Befehl zu generieren.

configure manager add *cdo_hostname registration_key nat_id display_name*

Beispiel:

Abbildung 48: configure manager add Befehlskomponenten



b) Kopieren Sie die Teile des Befehls *cdo_hostname*, *registration_key* und *nat_id* in die Felder **Management Center/CDO-Hostname/IP-Adresse**, **Management Center/CDO-Registrierungsschlüssel** und **NAT-ID**.

Schritt 8 Konfigurieren Sie die **Verbindungskonfiguration**.

a) Geben Sie den **FTD-Hostnamen** an.

Dieser FQDN wird für die externe Schnittstelle oder die Schnittstelle verwendet, die Sie für die **Management Center-/CDO-Zugriffsschnittstelle** auswählen.

b) Geben Sie die **DNS-Servergruppe** an.

Wählen Sie eine vorhandene Gruppe aus oder erstellen Sie eine neue. Die Standard-DNS-Gruppe heißt **CiscoUmbrellaDNSServerGroup** und umfasst die OpenDNS-Server.

Diese Einstellung legt den DNS-Server der *Datenschnittstelle* fest. Der Management-DNS-Server, den Sie mit dem Einrichtungsassistenten festlegen, wird für den Management-Traffic verwendet. Der Daten-DNS-Server wird für DDNS (sofern konfiguriert) oder für auf diese Schnittstelle angewendete Sicherheitsrichtlinien verwendet. Sie werden wahrscheinlich die gleiche DNS-Servergruppe auswählen, die Sie für das Management verwendet haben, da sowohl der Management- als auch der Daten-Traffic den DNS-Server über die externe Schnittstelle erreichen.

Im CDO werden die DNS-Server der Datenschnittstelle in der Richtlinie für Plattformeinstellungen konfiguriert, die Sie diesem Threat Defense-System zuweisen. Wenn Sie Threat Defense zum FMC hinzufügen, werden die lokalen Einstellungen beibehalten, und die DNS-Server werden *keiner* Richtlinie für Plattformeinstellungen hinzugefügt. Wenn Sie jedoch später dem Threat Defense-System eine Richtlinie für Plattformeinstellungen zuweisen, die eine DNS-Konfiguration enthält, überschreibt diese Konfiguration die lokale Einstellung. Wir empfehlen Ihnen, die DNS-Plattformeinstellungen aktiv mit dieser Einstellung zu konfigurieren, um CDO und Threat Defense zu synchronisieren.

Außerdem werden lokale DNS-Server von CDO nur beibehalten, wenn die DNS-Server bei der anfänglichen Registrierung erkannt wurden.

c) Wählen Sie für die **Management Center-/CDO-Zugriffsschnittstelle outside** (extern) aus.

Sie können jede konfigurierte Schnittstelle auswählen, aber in diesem Handbuch wird davon ausgegangen, dass Sie „outside“ verwenden.

Schritt 9 Wenn Sie eine andere externe Datenschnittstelle ausgewählt haben, fügen Sie eine Standardroute hinzu.

Sie werden in einer Meldung aufgefordert, zu überprüfen, ob Sie eine Standardroute über die Schnittstelle haben. Wenn Sie „outside“ ausgewählt haben, haben Sie diese Route bereits als Teil des Einrichtungsassistenten konfiguriert. Wenn Sie eine andere Schnittstelle ausgewählt haben, müssen Sie eine Standardroute manuell konfigurieren, bevor Sie eine Verbindung zu CDO herstellen. Unter Konfigurieren der Firewall in Device Manager, auf Seite 115 finden Sie weitere Informationen zum Konfigurieren statischer Routen im Device Manager.

Schritt 10 Klicken Sie auf **Add a Dynamic DNS (DDNS) method** (Dynamische DNS- (DDNS-)Methode hinzufügen).

DDNS stellt sicher, dass CDO den Threat Defense unter seinem vollqualifizierten Domain-Namen (FQDN) erreichen kann, wenn sich die IP-Adresse von Threat Defense ändert. Siehe **Device** > **System Settings** > **DDNS Service** (Gerät > Systemeinstellungen > DDNS-Service), um DDNS zu konfigurieren.

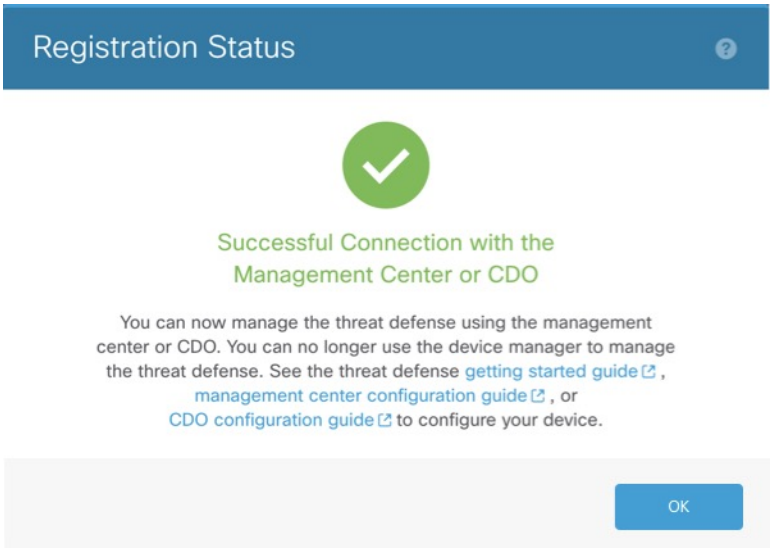
Wenn Sie DDNS konfigurieren, bevor Sie Threat Defense zu CDO hinzufügen, fügt Threat Defense automatisch Zertifikate für alle wichtigen Zertifizierungsstellen aus dem Cisco Trusted Root CA-Paket hinzu, damit Threat Defense das DDNS-Serverzertifikat für die HTTPS-Verbindung validieren kann. Threat Defense unterstützt jeden DDNS-Server, der die DynDNS Remote API-Spezifikation (https://help.dyn.com/remote-access-api/) verwendet.

Schritt 11 Klicken Sie auf **Connect** (Verbinden). Im Dialogfeld **Registrierungsstatus** wird der aktuelle Status des Wechsels zu CDO angezeigt. Gehen Sie nach dem Schritt **Speichern der Registrierungseinstellungen für Management Center/CDO** zu CDO und fügen Sie die Firewall hinzu.

Wenn Sie den Wechsel zu CDO abbrechen möchten, klicken Sie auf **Cancel Registration** (Registrierung abbrechen). Andernfalls schließen Sie das Device Manager-Browserfenster erst nach dem Schritt **Speichern der Registrierungseinstellungen für Management Center/CDO**. Wenn Sie dies tun, wird der Prozess angehalten und erst fortgesetzt, wenn Sie erneut eine Verbindung zu Device Manager herstellen.

Wenn Sie nach dem Schritt **Speichern der Registrierungseinstellungen für Management Center/CDO** weiterhin mit dem Device Manager verbunden sind, wird schließlich das Dialogfeld **Successful Connection with Management Center or CDO** (Erfolgreiche Verbindung mit Management Center oder CDO) angezeigt. Danach wird die Verbindung zum Device Manager getrennt.

Abbildung 49: Verbindungsversuch erfolgreich



Konfigurieren einer Basissicherheitsrichtlinie

In diesem Abschnitt wird beschrieben, wie Sie eine grundlegende Sicherheitsrichtlinie mit den folgenden Einstellungen konfigurieren:

- Interne und externe Schnittstellen: Weisen Sie der internen Schnittstelle eine statische IP-Adresse zu. Sie haben im Rahmen der Einrichtung des Managerzugriffs grundlegende Einstellungen für die externe Schnittstelle konfiguriert, müssen sie jedoch weiterhin einer Sicherheitszone zuweisen.
- DHCP-Server: Verwenden Sie einen DHCP-Server auf der internen Schnittstelle für Clients.
- NAT: Verwenden Sie die Schnittstellen-PAT für die externe Schnittstelle.
- Access Control (Zugriffskontrolle): Lassen Sie Traffic von innen nach außen zu.
- SSH: Aktivieren Sie SSH auf der Managerzugriffsschnittstelle.

Konfigurieren von Schnittstellen

Fügen Sie die VLAN1-Schnittstelle für die Switch-Ports hinzu, oder konvertieren Sie Switch-Ports in Firewall-Schnittstellen, weisen Sie Schnittstellen zu Sicherheitszonen zu, und legen Sie die IP-Adressen fest. In der Regel müssen Sie mindestens zwei Schnittstellen konfigurieren, um ein System einzurichten, das sinnvollen Traffic weiterleitet. Normalerweise haben Sie eine externe Schnittstelle, die dem Upstream-Router oder dem Internet zugekehrt ist, und eine oder mehrere Schnittstellen im Inneren für die Netzwerke Ihres Unternehmens. Standardmäßig ist Ethernet1 / 1 eine normale Firewall-Schnittstelle, die Sie für den Außenbereich verwenden können. Die verbleibenden Schnittstellen sind Switch-Ports in VLAN 1; nachdem Sie die VLAN1-Schnittstelle hinzugefügt haben, können Sie sie zu Ihrer internen Schnittstelle machen. Sie können Switch-Ports auch anderen VLANs zuweisen oder Switch-Ports in Firewall-Schnittstellen konvertieren.

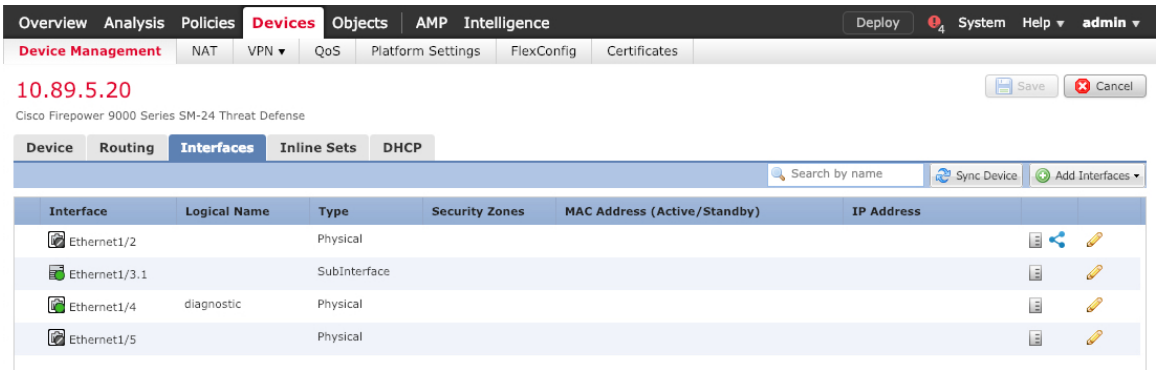
In einer typischen Edge-Routing-Situation beziehen Sie die Adresse der externen Schnittstelle über DHCP von Ihrem ISP, während Sie statische Adressen für die Schnittstellen im Inneren (internen Schnittstellen) definieren.

Im folgenden Beispiel wird eine interne Schnittstelle im Modus „geroutet“ (VLAN1) mit einer statischen Adresse und eine externe Schnittstelle im Modus „geroutet“ unter Verwendung von DHCP (Ethernet1/1) konfiguriert.

Prozedur

Schritt 1 Wählen Sie **Devices** > **Device Management** (Geräte > Gerätemanagement), und klicken Sie für das Gerät auf **Bearbeiten** ( ).

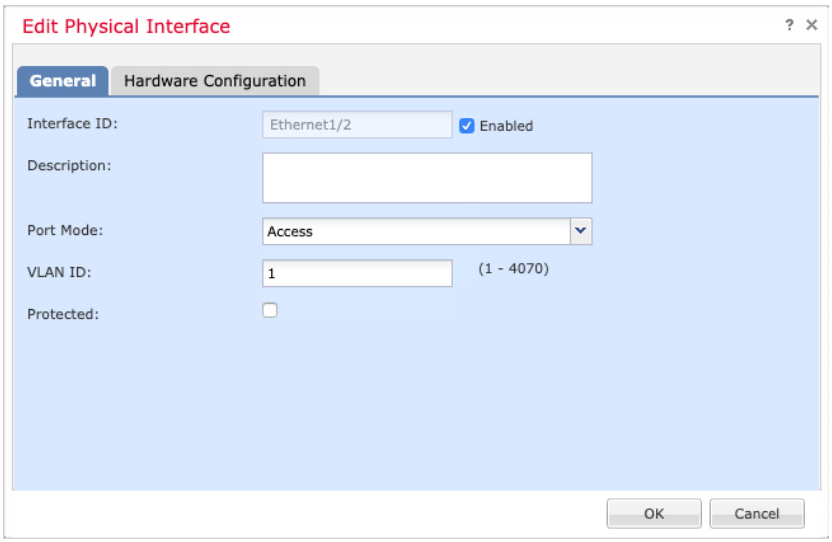
Schritt 2 Klicken Sie auf **Interfaces** (Schnittstellen).



Schritt 3 (optional) Deaktivieren Sie den Switch-Port-Modus für die Switch-Ports (Ethernet 1/2 bis 1/8), indem Sie auf den Schieberegler in der Spalte **SwitchPort** klicken, damit er als deaktiviert ( ) angezeigt wird.

Schritt 4 Aktivieren Sie die Switch-Ports.

a) Klicken Sie für den Switch-Port auf **Bearbeiten** ( ).



b) Aktivieren Sie die Schnittstelle, indem Sie das Kontrollkästchen **Enabled** (Aktiviert) markieren.

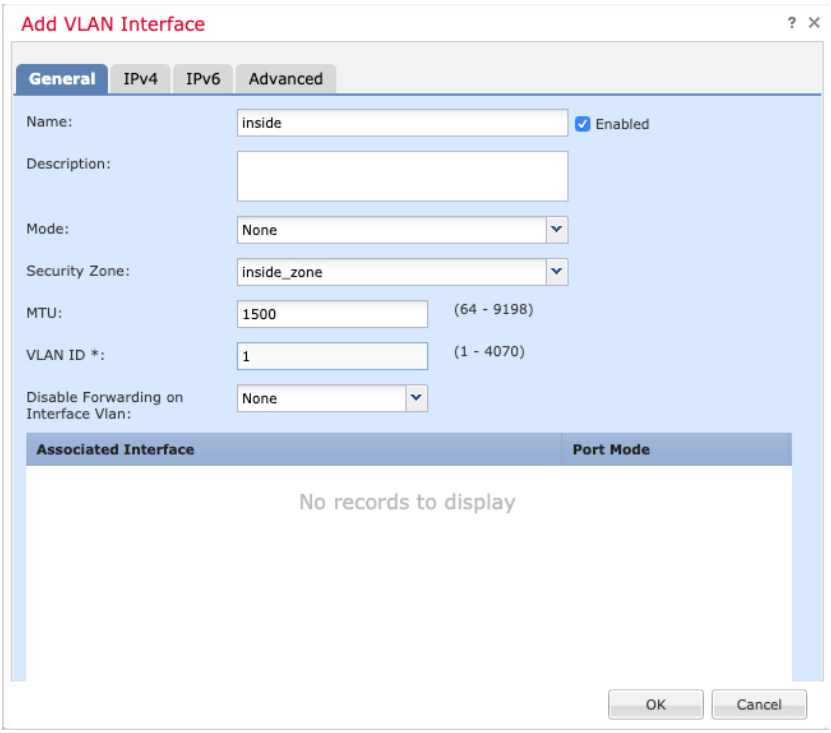
c) (optional) Ändern Sie die VLAN-ID; der Standardwert ist 1. Als Nächstes fügen Sie eine VLAN-Schnittstelle hinzu, die dieser ID entspricht.

d) Klicken Sie auf **OK**.

Schritt 5 Fügen Sie die *interne* VLAN-Schnittstelle hinzu.

a) Klicken Sie auf **Add Interfaces** > **VLAN Interface** (Schnittstellen hinzufügen > VLAN-Schnittstelle).

Die Registerkarte **General** (Allgemein) wird geöffnet.



b) Geben Sie einen **Namen** mit bis zu 48 Zeichen ein.

Nennen Sie die Schnittstelle beispielsweise **inside**.

c) Markieren Sie das Kontrollkästchen **Enabled** (Aktiviert).

d) Übernehmen Sie die Einstellung **None** (Keiner) für **Mode** (Modus).

e) Wählen Sie in der Dropdown-Liste **Security Zone** (Sicherheitszone) eine vorhandene interne Sicherheitszone aus, oder fügen Sie eine neue hinzu, indem Sie auf **New** (Neu) klicken.

Fügen Sie beispielsweise eine Zone mit dem Namen **inside_zone** hinzu. Jede Schnittstelle muss einer Sicherheitszone und/oder Schnittstellengruppe zugewiesen werden. Eine Schnittstelle kann nur zu einer Sicherheitszone, aber gleichzeitig auch zu mehreren Schnittstellengruppen gehören. Sie wenden Ihre Sicherheitsrichtlinie basierend auf Zonen oder Gruppen an. Sie können beispielsweise die interne Schnittstelle der internen Zone zuweisen und die externe Schnittstelle zur Außenzone. Anschließend können Sie Ihre Zugriffskontrollrichtlinie so konfigurieren, dass der Traffic von innen nach außen geleitet wird, aber nicht von außen nach innen. Die meisten Richtlinien unterstützen nur Sicherheitszonen. Sie können Zonen oder Schnittstellengruppen in NAT-Richtlinien, Vorfilterrichtlinien und QoS-Richtlinien verwenden.

f) Setzen Sie die **VLAN-ID** auf **1**.

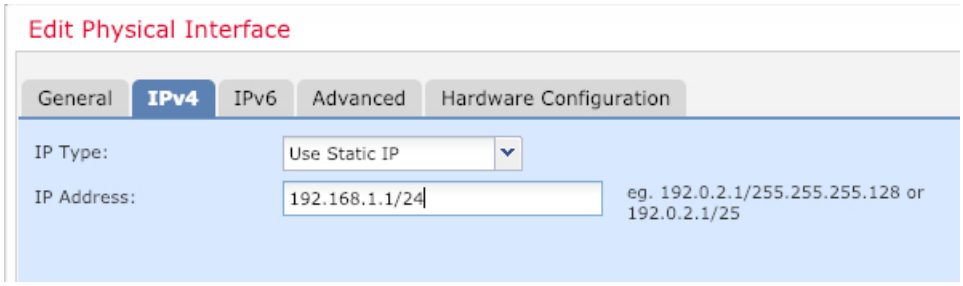
Standardmäßig sind alle Switch-Ports auf VLAN 1 eingestellt. Wenn Sie hier eine andere VLAN-ID auswählen, müssen Sie auch jeden Switch-Port bearbeiten, damit er auf die neue VLAN-ID gesetzt ist.

Sie können die VLAN-ID nicht mehr ändern, nachdem Sie die Schnittstelle gespeichert haben. Die VLAN-ID ist sowohl der verwendete VLAN-Tag als auch die Schnittstellen-ID in Ihrer Konfiguration.

g) Klicken Sie auf die Registerkarte **IPv4** und/oder **IPv6**.

- **IPv4**: Wählen Sie in der Dropdown-Liste **Use Static IP** (Statische IP verwenden) aus, und geben Sie eine IP-Adresse und eine Subnetzmaske in der Schreibweise mit Schrägstrichen ein.

Geben Sie beispielsweise **192.168.1.1/24** ein.

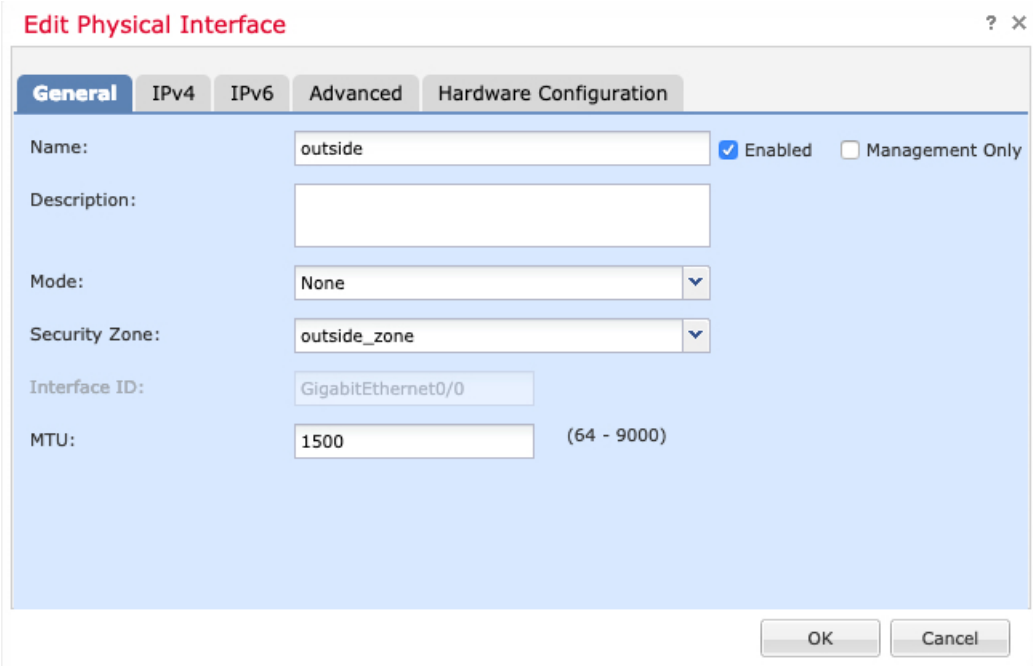


- **IPv6**: Markieren Sie das Kontrollkästchen **Autoconfiguration** (Automatische Konfiguration) für eine automatische Stateless-Konfiguration.

h) Klicken Sie auf **OK**.

Schritt 6 Klicken Sie für die Ethernet1/1-Schnittstelle, die Sie für den *Außenbereich* verwenden möchten, auf **Bearbeiten** (✎).

Die Registerkarte **General** (Allgemein) wird geöffnet.



Sie haben diese Schnittstelle bereits für den Managerzugriff vorkonfiguriert, sodass die Schnittstelle bereits einen Namen hat und aktiviert und adressiert ist. Sie sollten keine dieser Grundeinstellungen ändern, da dadurch die Management Center-Managementverbindung unterbrochen würde. Sie müssen die Sicherheitszone auf diesem Bildschirm jedoch für Richtlinien bezüglich des Durchgangs-Traffics konfigurieren.

a) Wählen Sie in der Dropdown-Liste **Security Zone** (Sicherheitszone) eine vorhandene externe Sicherheitszone aus, oder fügen Sie eine neue hinzu, indem Sie auf **New** (Neu) klicken.

   Fügen Sie beispielsweise eine Zone mit dem Namen **outside_zone** hinzu.

b) Klicken Sie auf **OK**.

Schritt 7 Klicken Sie auf **Save** (Speichern).

Konfigurieren des DHCP-Servers

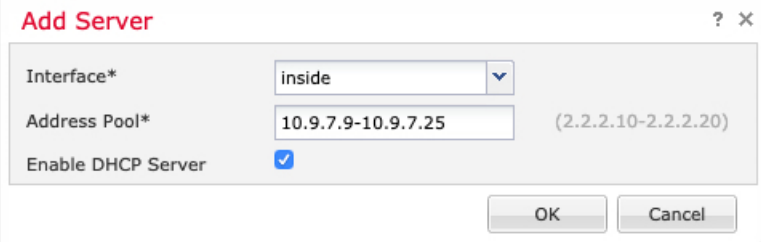
Aktivieren Sie den DHCP-Server, wenn Clients DHCP zum Abrufen von IP-Adressen aus dem Threat Defense verwenden sollen.

Prozedur

Schritt 1 Wählen Sie **Devices** > **Device Management** (Geräte > Gerätemanagement), und klicken Sie für das Gerät auf **Bearbeiten** (✎).

Schritt 2 Wählen Sie **DHCP** > **DHCP Server** (DHCP > DHCP-Server).

Schritt 3 Klicken Sie auf der Seite **Server** auf **Add** (Hinzufügen), und konfigurieren Sie die folgenden Optionen:



- **Interface** (Schnittstelle): Wählen Sie in der Dropdown-Liste die Schnittstelle aus.
- **Address Pool** (Adressen-Pool): Legen Sie den Bereich der niedrigsten bis höchsten IP-Adressen fest, die vom DHCP-Server verwendet werden. Der Bereich der IP-Adressen muss sich im selben Subnetz wie die ausgewählte Schnittstelle befinden und darf die IP-Adresse der Schnittstelle selbst nicht enthalten.
- **Enable DHCP Server** (DHCP-Server aktivieren): Aktiviert den DHCP-Server auf der ausgewählten Schnittstelle.

Schritt 4 Klicken Sie auf **OK**.

Schritt 5 Klicken Sie auf **Save** (Speichern).

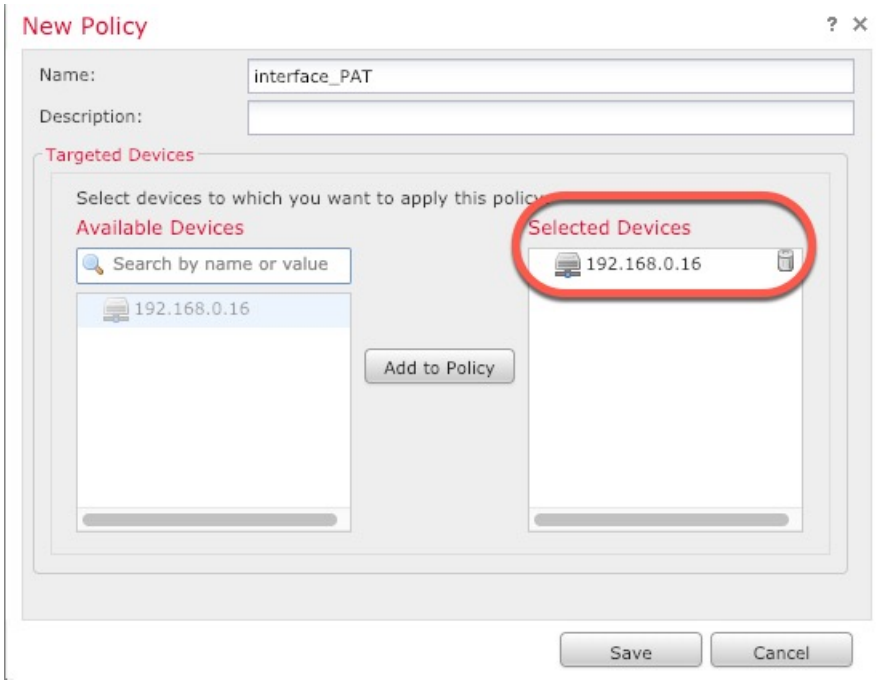
Konfigurieren von NAT

Eine typische NAT-Regel konvertiert interne Adressen in einen Port an der IP-Adresse der externen Schnittstelle. Diese Art von NAT-Regel wird als *Interface Port Address Translation (PAT)* bezeichnet.

Prozedur

Schritt 1 Wählen Sie **Devices** > **NAT** (Geräte > NAT), und klicken Sie auf **New Policy** > **Threat Defense NAT** (Neue Richtlinie > Threat Defense-NAT).

Schritt 2 Geben Sie der Richtlinie einen Namen, wählen Sie die Geräte aus, für die sie gelten soll, und klicken Sie auf **Save** (Speichern).



Die Zuordnung zwischen der Richtlinie und Management Center wird vorgenommen. Sie müssen der Richtlinie noch Regeln hinzufügen.

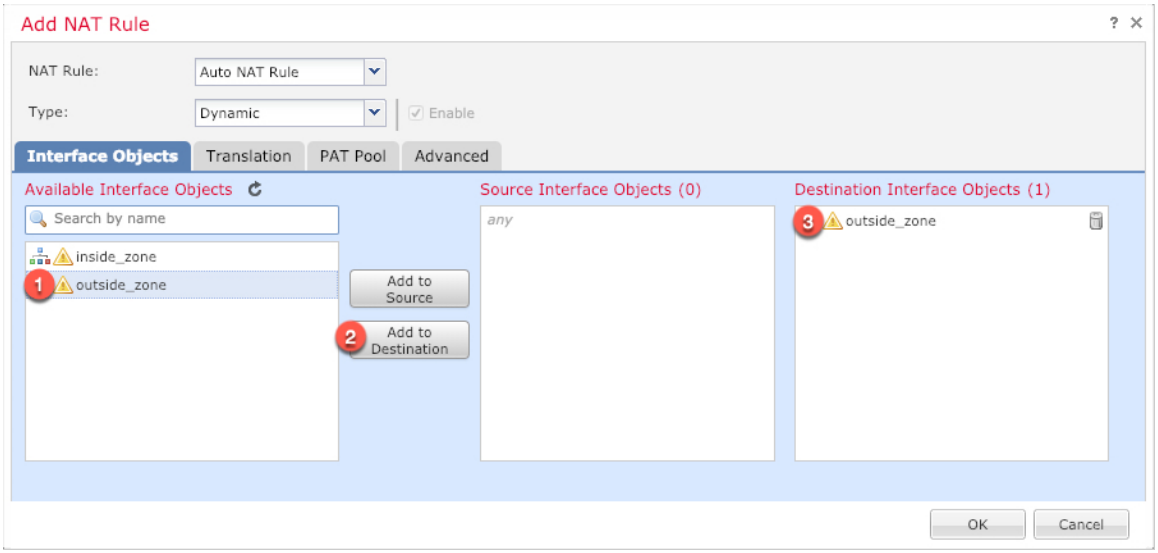
Schritt 3 Klicken Sie auf **Add Rule** (Regel hinzufügen).

Das Dialogfeld **Add NAT Rule** (NAT-Regel hinzufügen) wird angezeigt.

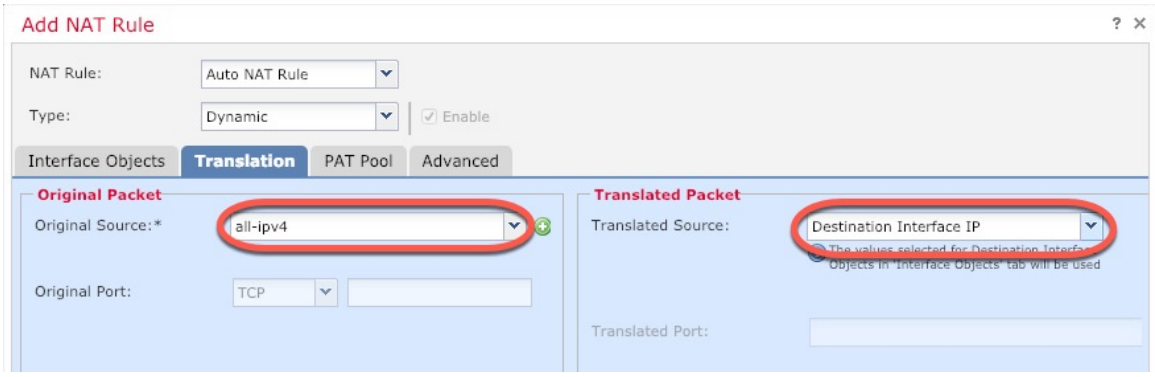
Schritt 4 Konfigurieren Sie die grundlegenden Regeloptionen:

- **NAT Rule** (NAT-Regel): Wählen Sie **Auto NAT Rule** (Automatische NAT-Regel) aus.
- **Type** (Typ): Wählen Sie **Dynamic** (Dynamisch) aus.

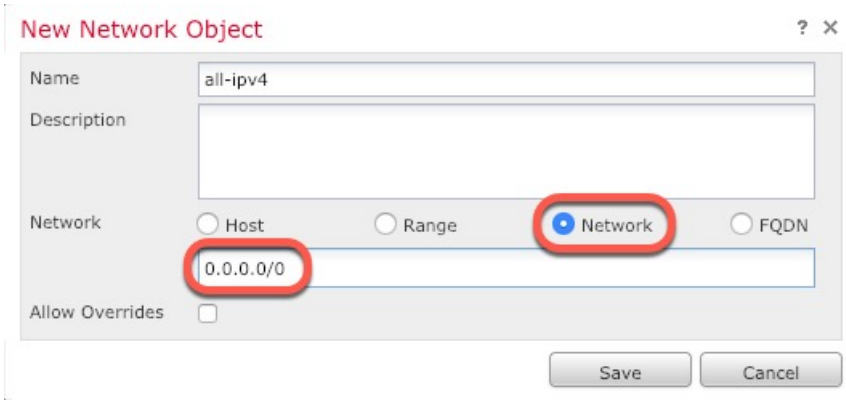
Schritt 5 Fügen Sie auf der Seite **Interface Objects** (Schnittstellenobjekte) die externe Zone aus dem Bereich **Available Interface Objects** (Verfügbare Schnittstellenobjekte) im Bereich **Destination Interface Objects** (Zielschnittstellenobjekte) hinzu.



Schritt 6 Konfigurieren Sie auf der Seite **Translation** (Übersetzung) die folgenden Optionen:



- **Original Source** (Ursprüngliche Quelle): Klicken Sie auf **Hinzufügen** (+), um ein Netzwerkobjekt für den gesamten IPv4-Traffic (0.0.0.0/0) hinzuzufügen.

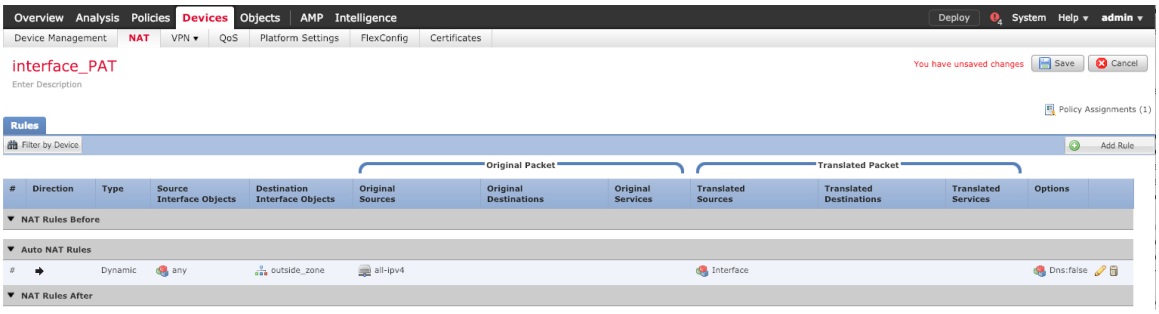


Hinweis Sie können das systemdefinierte Objekt **any-ipv4** nicht verwenden, da Auto-NAT-Regeln NAT als Teil der Objektdefinition hinzufügen, und Sie können systemdefinierte Objekte nicht bearbeiten.

- **Translated Source** (Übersetzte Quelle): Wählen Sie für **Destination Interface IP** (Zielschnittstellen-IP) einen Wert aus.

Schritt 7 Klicken Sie auf **Save** (Speichern), um die Regel hinzuzufügen.

Die Regel wird in der Tabelle **Rules** (Regeln) gespeichert.



Schritt 8 Klicken Sie auf der Seite **NAT** auf **Save** (Speichern), um Ihre Änderungen zu speichern.

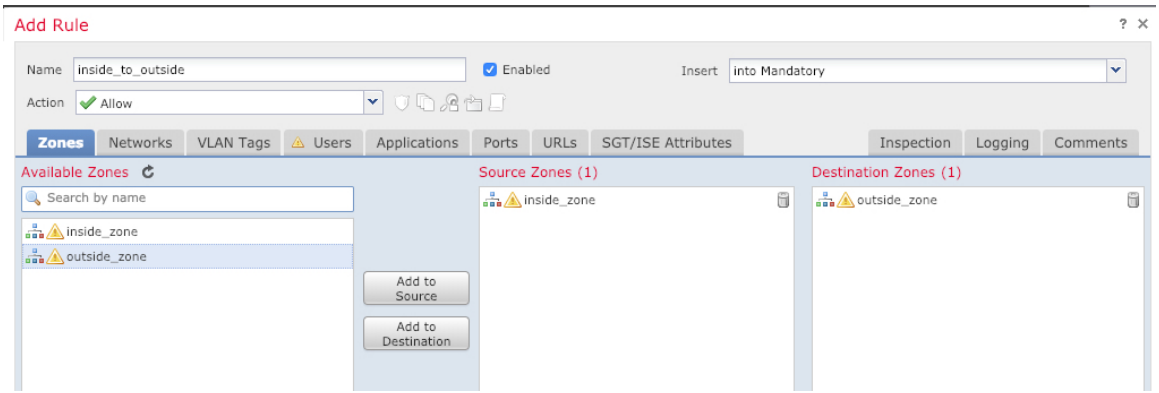
Zulassen des Traffics von innen nach außen

Wenn Sie bei der Registrierung von Threat Defense eine grundlegende Zugriffskontrollrichtlinie zum Blockieren des gesamten Traffics (**Block all traffic**) erstellt haben, müssen Sie der Richtlinie Regeln hinzufügen, um Traffic über das Gerät zuzulassen. Das folgende Verfahren fügt eine Regel hinzu, die Traffic von der internen Zone zur externen Zone zulässt. Wenn Sie über andere Zonen verfügen, müssen Sie Regeln hinzufügen, die den Traffic zu den entsprechenden Netzwerken zulassen.

Prozedur

Schritt 1 Wählen Sie **Policy** > **Access Policy** > **Access Policy** (Richtlinie > Zugriffsrichtlinie > Zugriffsrichtlinie) aus, und klicken Sie auf **Bearbeiten** (✎) für die Zugriffskontrollrichtlinie, die dem Threat Defense zugewiesen ist.

Schritt 2 Klicken Sie auf **Add Rule** (Regel hinzufügen), und legen Sie die folgenden Parameter fest:



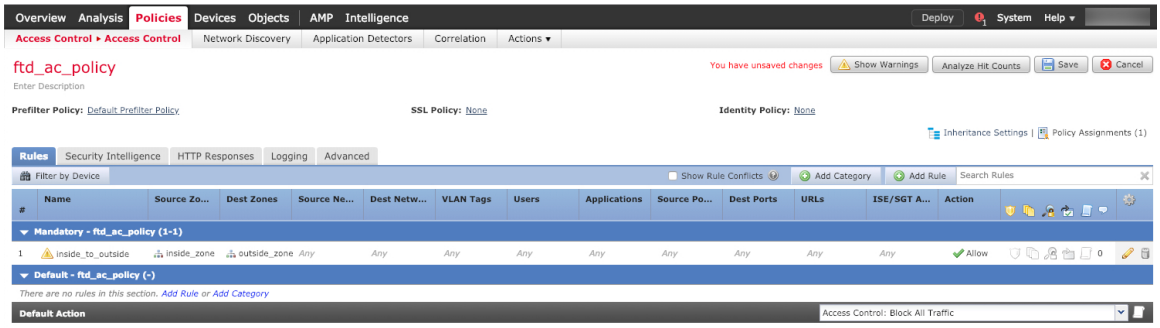
- **Name**: Geben Sie dieser Regel einen Namen, z. B. **inside_to_outside**.

- **Source Zones** (Quellzonen): Wählen Sie in **Available Zones** (Verfügbare Zonen) die interne Zone aus, und klicken Sie auf **Add to Source** (Zu Quelle hinzufügen).
- **Destination Zones** (Zielzonen): Wählen Sie in **Available Zones** (Verfügbare Zonen) die externe Zone aus, und klicken Sie auf **Add to Destination** (Zu Ziel hinzufügen).

Lassen Sie die anderen Einstellungen unverändert.

Schritt 3 Klicken Sie auf **Add** (Hinzufügen).

Die Regel wird der Tabelle **Rules** (Regeln) hinzugefügt.



Schritt 4 Klicken Sie auf **Save** (Speichern).

Konfigurieren von SSH auf der Managerzugriffsdatenschnittstelle

Wenn Sie den Management Center-Zugriff auf einer Datenschnittstelle, z. B. der externen Schnittstelle, aktiviert haben, sollten Sie SSH auf dieser Schnittstelle mit diesem Verfahren aktivieren. In diesem Abschnitt wird beschrieben, wie SSH-Verbindungen zu einer oder mehreren *Datenschnittstellen* auf dem Threat Defense aktiviert werden. SSH wird für die logische Diagnoseschnittstelle nicht unterstützt.

Hinweis SSH ist auf der Management-Schnittstelle standardmäßig aktiviert. Dieser Bildschirm hat jedoch keinen Einfluss auf den Management-SSH-Zugriff.

Die Management-Schnittstelle ist von den anderen Schnittstellen auf dem Gerät getrennt. Sie wird verwendet, um das Gerät einzurichten und bei Management Center zu registrieren. SSH für Datenschnittstellen teilt die interne und externe Benutzerliste mit SSH für die Management-Schnittstelle. Andere Einstellungen werden separat konfiguriert: Aktivieren Sie für Datenschnittstellen SSH und Zugriffslisten über diesen Bildschirm. SSH-Traffic für Datenschnittstellen verwendet die reguläre Routingkonfiguration und keine statischen Routen, die bei der Einrichtung oder in der CLI konfiguriert wurden.

Informationen zur Konfiguration der SSH-Zugriffsliste für die Management-Schnittstelle finden Sie unter dem Befehl **configure ssh-access-list** in der Befehlsreferenz für Secure Firewall Threat Defense. Informationen zum Konfigurieren einer statischen Route finden Sie in den Informationen zum Befehl **configure network static-routes**. Standardmäßig konfigurieren Sie die Standardroute bei der Ersteinrichtung über die Management-Schnittstelle.

Um SSH zu verwenden, benötigen Sie auch keine Zugriffsregel, die die Host-IP-Adresse zulässt. Sie müssen nur den SSH-Zugriff gemäß diesem Abschnitt konfigurieren.

Sie können SSH nur für eine erreichbare Schnittstelle verwenden. Wenn sich Ihr SSH-Host auf der externen Schnittstelle befindet, können Sie eine Managementverbindung nur direkt mit der externen Schnittstelle initiieren.

Das Gerät ermöglicht maximal fünf gleichzeitige SSH-Verbindungen.

Hinweis Das Gerät beendet die SSH-Verbindung, nachdem ein Benutzer dreimal hintereinander erfolglos versucht hat, sich über SSH an der CLI anzumelden.

Vorbereitungen

- Sie können interne SSH-Benutzer in der CLI mit dem Befehl **configure user add** konfigurieren. Standardmäßig gibt es einen **Administrator**-Benutzer, für den Sie das Kennwort bei der Ersteinrichtung konfiguriert haben. Sie können externe Benutzer auch auf LDAP oder RADIUS konfigurieren, indem Sie in den Plattformeinstellungen **External Authentication** (Externe Authentifizierung) konfigurieren.
- Sie benötigen Netzwerkobjekte, die die Hosts oder Netzwerke definieren, die Sie für SSH-Verbindungen mit dem Gerät zulassen dürfen. Sie können Objekte als Teil des Verfahrens hinzufügen. Wenn Sie jedoch mithilfe von Objektgruppen eine Gruppe von IP-Adressen identifizieren möchten, stellen Sie sicher, dass die in den Regeln erforderlichen Gruppen bereits vorhanden sind. Wählen Sie **Objects** > **Object Management** (Objekte > Objektmanagement) aus, um Objekte zu konfigurieren.

Hinweis Sie können das vom System bereitgestellte Netzwerkobjekt **any** nicht verwenden. Verwenden Sie stattdessen **any-ipv4** oder **any-ipv6**.

Prozedur

Schritt 1 Wählen Sie **Devices** > **Platform Settings** (Geräte > Plattformeinstellungen) aus, und erstellen oder bearbeiten Sie die Threat Defense-Richtlinie.

Schritt 2 Wählen Sie **Secure Shell** aus.

Schritt 3 Identifizieren Sie die Schnittstellen und IP-Adressen, die SSH-Verbindungen ermöglichen.

Verwenden Sie diese Tabelle, um einzuschränken, welche Schnittstellen SSH-Verbindungen akzeptieren. Außerdem können Sie die IP-Adressen der Clients einschränken, die diese Verbindungen herstellen dürfen. Sie können anstelle einzelner IP-Adressen auch Netzwerkadressen verwenden.

a) Klicken Sie auf **Add** (Hinzufügen), um eine neue Regel hinzuzufügen, oder auf **Edit** (Bearbeiten), um eine vorhandene Regel zu bearbeiten.

b) Konfigurieren Sie die Regeleigenschaften:

- **IP Address** (IP-Adresse): Das Netzwerkobjekt oder die Gruppe für die Identifizierung der Hosts oder Netzwerke, die Sie für SSH-Verbindungen zulassen. Wählen Sie ein Objekt aus dem Dropdown-Menü aus, oder fügen Sie ein neues Netzwerkobjekt hinzu, indem Sie auf + klicken.
- **Security Zones** (Sicherheitszonen): Fügen Sie die Zonen hinzu, die die Schnittstellen enthalten, zu denen Sie SSH-Verbindungen zulassen. Für Schnittstellen, die sich nicht in einer Zone befinden, können Sie den Schnittstellennamen in das Feld unter der Liste „Selected Security Zone“ (Ausgewählte

Sicherheitszone) eingeben und auf **Add** (Hinzufügen) klicken. Diese Regeln werden auf ein Gerät nur dann angewendet, wenn das Gerät die ausgewählten Schnittstellen oder Zonen enthält.

c) Klicken Sie auf **OK**.

Schritt 4 Klicken Sie auf **Save** (Speichern).

Sie können jetzt **Deploy** > **Deployment** (Bereitstellen > Bereitstellung) aufrufen und die Richtlinie auf zugewiesenen Geräten bereitstellen. Die Änderungen sind erst aktiv, wenn Sie sie bereitstellen.

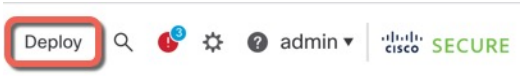
Bereitstellen der Konfiguration

Stellen Sie die Konfigurationsänderungen für Threat Defense bereit. Keine Ihrer Änderungen ist auf dem Gerät aktiv, bis Sie sie bereitstellen.

Prozedur

Schritt 1 Klicken Sie oben rechts auf **Deploy** (Bereitstellen).

Abbildung 50: Bereitstellen



Schritt 2 Klicken Sie entweder auf **Deploy All** (Alle bereitstellen), um die Bereitstellung auf allen Geräten durchzuführen, oder auf **Advanced Deploy** (Erweiterte Bereitstellung), um die Bereitstellung auf ausgewählten Geräten durchzuführen.

Abbildung 51: Alle bereitstellen

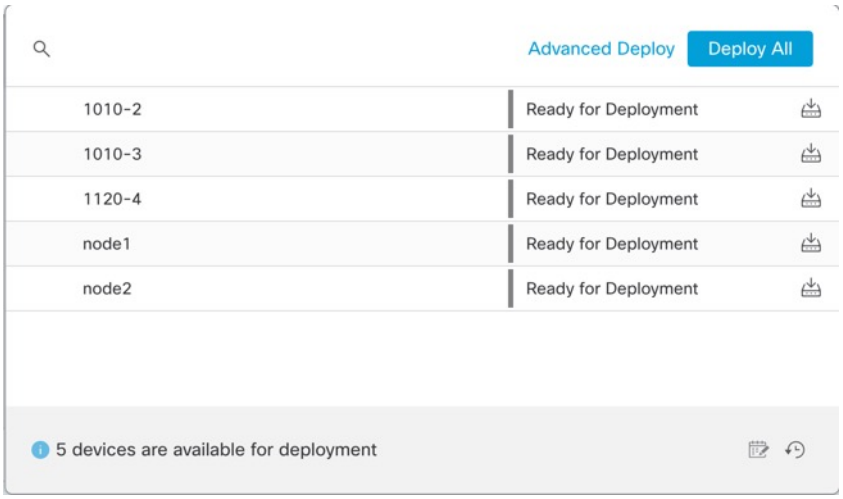
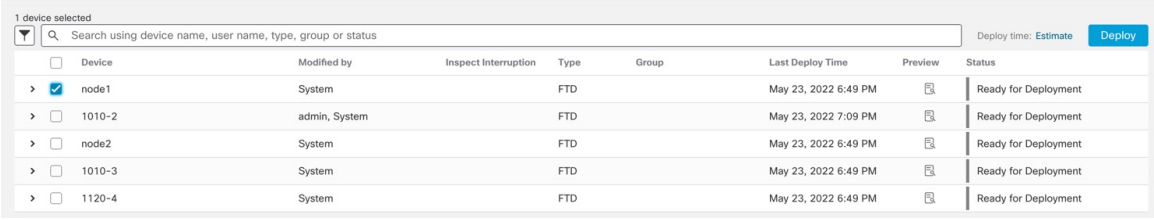
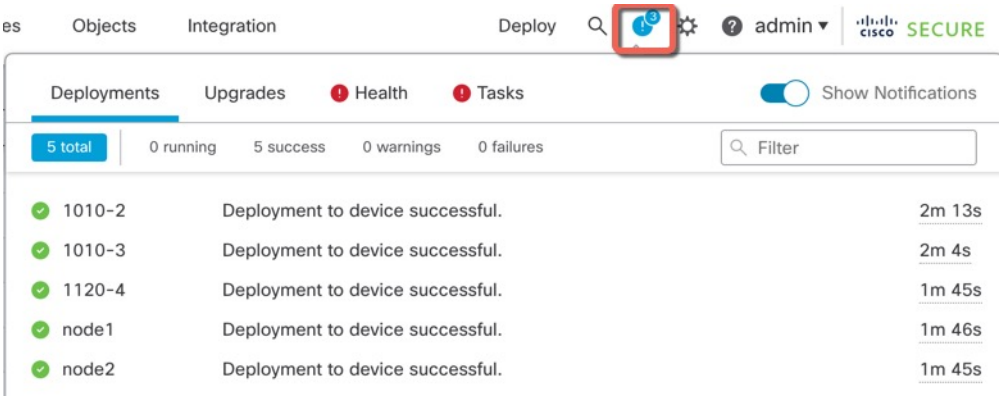


Abbildung 52: Erweiterte Bereitstellung



Schritt 3 Stellen Sie sicher, dass die Bereitstellung erfolgreich ist. Klicken Sie in der Menüleiste rechts neben der Schaltfläche **Deploy** (Bereitstellen) auf das Symbol, um den Status der Bereitstellungen anzuzeigen.

Abbildung 53: Bereitstellungsstatus



Fehlerbehebung und Wartung

Zugriff auf die Threat Defense- und FXOS-CLI

Verwenden Sie die Befehlszeilenschnittstelle (CLI), um das System einzurichten und grundlegende Systemfehlerbehebungen durchzuführen. Sie können Richtlinien nicht über eine CLI-Sitzung konfigurieren. Für den Zugriff auf die CLI (Befehlszeilenschnittstelle) müssen Sie eine Verbindung zum Konsolenport herstellen.

Sie können zur Fehlerbehebung auch auf die FXOS-CLI-CLI zugreifen.

Hinweis Sie können auch eine SSH-Sitzung für die Management-Schnittstelle des Threat Defense-Geräts nutzen. Im Gegensatz zu einer Konsolensitzung verwendet die SSH-Sitzung standardmäßig die Threat Defense-CLI, über die Sie sich mit dem Befehl **connect fxos** mit der FXOS-CLI-CLI verbinden können. Sie können sich später mit der Adresse auf einer Datenschnittstelle verbinden, wenn Sie die Schnittstelle für SSH-Verbindungen öffnen. Der SSH-Zugriff auf Datenschnittstellen ist standardmäßig deaktiviert. Dieses Verfahren beschreibt den Konsolenportzugriff, der standardmäßig auf die FXOS-CLI-CLI eingestellt ist.

Prozedur

Schritt 1 Verbinden Sie Ihren Management-Computer mit dem Konsolenport, um sich bei der CLI anzumelden. Firepower 1000 wird mit einem seriellen USB-A-zu-B-Kabel ausgeliefert. Stellen Sie sicher, dass Sie alle erforderlichen seriellen USB-Treiber für Ihr Betriebssystem installieren (siehe Firepower 1010 -Hardwarehandbuch). Der Konsolenport ist standardmäßig auf die FXOS-CLI-CLI eingestellt. Verwenden Sie die folgenden seriellen Einstellungen:

- 9.600 Baud
- 8 Daten-Bits
- Keine Parität
- 1 Stopp-Bit

Sie stellen eine Verbindung zum FXOS-CLI her. Melden Sie sich bei der CLI mit dem Benutzernamen **admin** und dem Kennwort an, das Sie bei der Ersteinrichtung festgelegt haben (der Standardwert ist **Admin123**).

Beispiel:

```
firepower login: admin
Password:
Last login: Thu May 16 14:01:03 UTC 2019 on ttyS0
Successful login attempts for user 'admin' : 1

firepower#
```

Schritt 2 Greifen Sie auf die Threat Defense-CLI zu.

connect ftd

Beispiel:

```
firepower# connect ftd
>
```

Geben Sie nach der Anmeldung **help** oder **?** ein, um Informationen zu den Befehlen aufzurufen, die in der CLI verfügbar sind. Informationen zur Verwendung finden Sie unter Befehlsreferenz für Secure Firewall Threat Defense.

Schritt 3 Um die Threat Defense-CLI zu verlassen, geben Sie den Befehl **exit** oder **logout** ein.

Mit diesem Befehl kehren Sie zur FXOS-CLI-CLI-Eingabeaufforderung zurück. Geben Sie **?** ein, um Informationen zu den Befehlen aufzurufen, die in der FXOS-CLI-CLI verfügbar sind.

Beispiel:

```
> exit
firepower#
```

Fehlerbehebung in Bezug auf die Managementkonnektivität auf einer Datenschnittstelle

Falls Sie eine Datenschnittstelle für den Managerzugriff anstelle der dedizierten Management-Schnittstelle verwenden, müssen Sie vorsichtig sein, wenn Sie die Schnittstellen- und Netzwerkeinstellungen für Threat Defense im CDO ändern, damit die Verbindung nicht unterbrochen wird. Wenn Sie den Typ der Management-Schnittstelle ändern, nachdem Sie Threat Defense zum hinzugefügt haben (von der Daten- zur Management-Schnittstelle oder umgekehrt), kann die Managementkonnektivität verloren gehen, falls die Schnittstellen- und Netzwerkeinstellungen nicht richtig konfiguriert sind.

Dieses Thema hilft Ihnen bei der Behebung des Verlusts der Managementkonnektivität.

Zeigen Sie den Status der Managementverbindung an

Überprüfen Sie in CDO den Status der Managementverbindung auf der Seite **Devices** > **Device Management** > **Device** > **Management** > **Manager Access - Configuration Details** > **Connection Status** (Geräte > Gerätemanagement > Gerät > Management > Managerzugriff − Konfigurationsdetails > Verbindungsstatus).

Geben Sie in der Threat Defense-CLI den Befehl **sftunnel-status-brief** ein, um den Status der Managementverbindung anzuzeigen. Sie können auch **sftunnel-status** verwenden, um umfassendere Informationen aufzurufen.

Sehen Sie sich die folgende Beispielausgabe für eine ausgefallene Verbindung an; es werden weder Informationen bezüglich einer hergestellten Verbindung zum Peer-Kanal noch Heartbeat-Informationen angezeigt:

```
> sftunnel-status-brief
PEER:10.10.17.202
Registration: Completed.
Connection to peer '10.10.17.202' Attempted at Mon Jun 15 09:21:57 2020 UTC
Last disconnect time : Mon Jun 15 09:19:09 2020 UTC
Last disconnect reason : Both control and event channel connections with peer went down
```

Sehen Sie sich die folgende Beispielausgabe für eine aktive Verbindung an. Dort werden Peer-Channel- und Heartbeat-Informationen angezeigt:

```
> sftunnel-status-brief
PEER:10.10.17.202
Peer channel Channel-A is valid type (CONTROL), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Peer channel Channel-B is valid type (EVENT), using 'eth0', connected to '10.10.17.202'
 via '10.10.17.222'
Registration: Completed.
IPv4 Connection to peer '10.10.17.202' Start Time: Wed Jun 10 14:27:12 2020 UTC
Heartbeat Send Time: Mon Jun 15 09:02:08 2020 UTC
Heartbeat Received Time: Mon Jun 15 09:02:16 2020 UTC
```

Anzeigen der Threat Defense-Netzwerkinformationen

Zeigen Sie in der Threat Defense-CLI die Netzwerkeinstellungen der Management- und -Managerzugriffsdatenschnittstellen an:

show network

```
> show network
===============[ System Information ]===============
Hostname                  : 5516X-4
DNS Servers               : 208.67.220.220,208.67.222.222
Management port           : 8305
IPv4 Default route
  Gateway                 : data-interfaces
IPv6 Default route
  Gateway                 : data-interfaces

======================[ br1 ]======================
State                     : Enabled
Link                      : Up
Channels                  : Management & Events
Mode                      : Non-Autonegotiation
MDI/MDIX                  : Auto/MDIX
MTU                       : 1500
MAC Address               : 28:6F:7F:D3:CB:8D
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.99.10.4
Netmask                   : 255.255.255.0
Gateway                   : 10.99.10.1
----------------------[ IPv6 ]----------------------
Configuration             : Disabled

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

======[ System Information - Data Interfaces ]======
DNS Servers               :
Interfaces                : GigabitEthernet1/1

===============[ GigabitEthernet1/1 ]===============
State                     : Enabled
Link                      : Up
Name                      : outside
MTU                       : 1500
MAC Address               : 28:6F:7F:D3:CB:8F
----------------------[ IPv4 ]----------------------
Configuration             : Manual
Address                   : 10.89.5.29
Netmask                   : 255.255.255.192
Gateway                   : 10.89.5.1
----------------------[ IPv6 ]----------------------
Configuration             : Disabled
```

Überprüfen Sie, ob Threat Defense bei CDO registriert ist.

Überprüfen Sie in der Threat Defense-CLI, ob die CDO-Registrierung abgeschlossen wurde. Beachten Sie, dass dieser Befehl nicht den *aktuellen* Status der Managementverbindung anzeigt.

show managers

```
> show managers
Type                      : Manager
Host                      : account1.app.us.cdo.cisco.com
Display name              : account1.app.us.cdo.cisco.com
Identifier                : f7ffad78-bf16-11ec-a737-baa2f76ef602
Registration              : Completed
```

```
Management type           : Configuration
```

Anpingen von CDO

Verwenden Sie in der Threat Defense-CLI den folgenden Befehl, um CDO von den Datenschnittstellen aus anzupingen:

ping *cdo_hostname*

Verwenden Sie in der Threat Defense-CLI den folgenden Befehl, um CDO von der Management-Schnittstelle aus anzupingen; die Route sollte über die Backplane zu den Datenschnittstellen führen:

ping system *cdo_hostname*

Erfassen der Pakete auf der internen Threat Defense-Schnittstelle

Erfassen Sie in der Threat Defense-CLI Pakete auf der internen Backplane-Schnittstelle (nlp_int_tap), um zu sehen, ob Managementpakete gesendet werden:

capture *Name* **interface nlp_int_tap trace detail match ip any any**

show capture*Name* **trace detail**

Überprüfen Sie den Status der internen Schnittstelle, die Statistiken und die Paketanzahl

In der Threat Defense-CLI finden Sie Informationen zur internen Backplane-Schnittstelle nlp_int_tap:

show interace detail

```
> show interface detail
[...]
Interface Internal-Data0/1 "nlp_int_tap", is up, line protocol is up
  Hardware is en_vtun rev00, BW Unknown Speed-Capability, DLY 1000 usec
 (Full-duplex), (1000 Mbps)
 Input flow control is unsupported, output flow control is unsupported
 MAC address 0000.0100.0001, MTU 1500
 IP address 169.254.1.1, subnet mask 255.255.255.248
 37 packets input, 2822 bytes, 0 no buffer
 Received 0 broadcasts, 0 runts, 0 giants
 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
 0 pause input, 0 resume input
 0 L2 decode drops
 5 packets output, 370 bytes, 0 underruns
 0 pause output, 0 resume output
 0 output errors, 0 collisions, 0 interface resets
 0 late collisions, 0 deferred
 0 input reset drops, 0 output reset drops
 input queue (blocks free curr/low): hardware (0/0)
 output queue (blocks free curr/low): hardware (0/0)
  Traffic Statistics for "nlp_int_tap":
 37 packets input, 2304 bytes
 5 packets output, 300 bytes
 37 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
  Control Point Interface States:
 Interface number is 14
 Interface config status is active
```

```
 Interface state is active
```

Überprüfen Sie das Routing und die NAT

Überprüfen Sie in der Threat Defense-CLI, ob die Standardroute (S*) hinzugefügt wurde und ob interne NAT-Regeln für die Management-Schnittstelle (nlp_int_tap) vorhanden sind.

show route

```
> show route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, V - VPN
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, + - replicated route
       SI - Static InterVRF
Gateway of last resort is 10.89.5.1 to network 0.0.0.0

S*       0.0.0.0 0.0.0.0 [1/0] via 10.89.5.1, outside
C        10.89.5.0 255.255.255.192 is directly connected, outside
L        10.89.5.29 255.255.255.255 is directly connected, outside

>
```

show nat

```
> show nat

Auto NAT Policies (Section 2)
1 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_intf3 interface  service
 tcp 8305 8305
    translate_hits = 0, untranslate_hits = 6
2 (nlp_int_tap) to (outside) source static nlp_server_0_ssh_intf3 interface  service
tcp ssh ssh
    translate_hits = 0, untranslate_hits = 73
3 (nlp_int_tap) to (outside) source static nlp_server_0_sftunnel_ipv6_intf3 interface
ipv6  service tcp 8305 8305
    translate_hits = 0, untranslate_hits = 0
4 (nlp_int_tap) to (outside) source dynamic nlp_client_0_intf3 interface
    translate_hits = 174, untranslate_hits = 0
5 (nlp_int_tap) to (outside) source dynamic nlp_client_0_ipv6_intf3 interface ipv6
    translate_hits = 0, untranslate_hits = 0
>
```

Überprüfen Sie sonstige Einstellungen

Überprüfen Sie mit folgenden Befehlen, ob alle anderen Einstellungen vorhanden sind. Sie finden viele dieser Befehle auch auf der CDO-Seite **Devices** > **Device Management** > **Device** > **Management** > **Manager Access - Configuration Details** > **CLI Output** (Geräte > Gerätemanagement > Gerät > Management > Managerzugriff − Konfigurationsdetails > CLI-Ausgabe).

show running-config sftunnel

```
> show running-config sftunnel
sftunnel interface outside
sftunnel port 8305
```

show running-config ip-client

```
> show running-config ip-client
ip-client outside
```

show conn address *FMC-IP*

```
> show conn address 10.89.5.35
5 in use, 16 most used
Inspect Snort:
        preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

TCP nlp_int_tap  10.89.5.29(169.254.1.2):51231 outside  10.89.5.35:8305, idle 0:00:04,
 bytes 86684, flags UxIO
TCP nlp_int_tap  10.89.5.29(169.254.1.2):8305 outside  10.89.5.35:52019, idle 0:00:02,
 bytes 1630834, flags UIO
>
```

Suchen Sie nach einer erfolgreichen DDNS-Aktualisierung

Suchen Sie in der Threat Defense-CLI nach einer erfolgreichen DDNS-Aktualisierung:

debug ddns

```
> debug ddns
DDNS update request = /v3/update?hostname=domain.example.org&myip=209.165.200.225
Successfuly updated the DDNS sever with current IP addresses
DDNS: Another update completed, outstanding = 0
DDNS: IDB SB total = 0
```

Wenn die Aktualisierung fehlgeschlagen ist, verwenden Sie die Befehle **debug http** und **debug ssl**. Überprüfen Sie bei fehlgeschlagenen Zertifikatsüberprüfungen, ob die Stammzertifikate auf dem Gerät installiert sind:

show crypto ca certificates *Trust-Point-Name*

So überprüfen Sie den DDNS-Betrieb:

show ddns update interface *fmc_access_ifc_name*

```
> show ddns update interface outside

Dynamic DNS Update on outside:
    Update Method Name Update Destination
    RBD_DDNS not available

Last Update attempted on 04:11:58.083 UTC Thu Jun 11 2020
Status : Success
FQDN : domain.example.org
IP addresses : 209.165.200.225
```

Überprüfen Sie die CDO-Protokolldateien

Weitere Informationen finden Sie unter https://cisco.com/go/fmc-reg-error.

Rollback der Konfiguration bei unterbrochener CDO-Konnektivität

Wenn Sie eine Datenschnittstelle auf dem Threat Defense-System für den Managerzugriff verwenden und eine Konfigurationsänderung über CDO bereitstellen, die sich auf die Netzwerkkonnektivität auswirkt, können Sie die Konfiguration auf dem Threat Defense-System mit einem Rollback auf die zuletzt bereitgestellte Konfiguration zurücksetzen, um die Managementkonnektivität wiederherzustellen. Sie können dann die Konfigurationseinstellungen in CDO anpassen, damit die Netzwerkkonnektivität erhalten bleibt, und die Bereitstellung erneut durchführen. Sie können die Rollback-Funktion auch verwenden, wenn die Verbindung nicht unterbrochen wird. Sie ist nicht auf diese Situation der Fehlerbehebung beschränkt.

Beachten Sie die folgenden Orientierungshilfen:

- Nur die vorherige Bereitstellung ist lokal auf der Threat Defense-Instanz verfügbar. Sie können kein Rollback zu früheren Bereitstellungen durchführen.
- Das Rollback betrifft nur Konfigurationen, die Sie in CDO festlegen können. Beispiel: Das Rollback wirkt sich nicht auf lokale Konfigurationen im Zusammenhang mit der dedizierten Management-Schnittstelle aus, die Sie nur über die Threat Defense-CLI konfigurieren können. Hinweis: Wenn Sie die Datenschnittstelleneinstellungen nach der letzten CDO-Bereitstellung mit dem Befehl **configure network management-data-interface** geändert haben und dann den Rollback-Befehl verwenden, werden diese Einstellungen nicht beibehalten. Sie werden stattdessen auf die zuletzt bereitgestellten CDO-Einstellungen zurückgesetzt.
- Out-of-Band-SCEP-Zertifikatdaten, die während der vorherigen Bereitstellung aktualisiert wurden, können nicht zurückgesetzt werden.
- Während des Rollbacks werden die Verbindungen getrennt, da die aktuelle Konfiguration gelöscht wird.

Prozedur

Schritt 1 Führen Sie in der Threat Defense-CLI ein Rollback zur vorherigen Konfiguration durch.

configure policy rollback

Nach dem Rollback benachrichtigt Threat Defense CDO, dass das Rollback erfolgreich abgeschlossen wurde. In CDO wird im Bereitstellungsbildschirm ein Banner angezeigt, das besagt, dass die Konfiguration zurückgesetzt wurde.

Hinweis Wenn das Rollback fehlgeschlagen ist und das CDO-Management wiederhergestellt wird, lesen Sie https://www.cisco.com/c/en/us/support/docs/security/firepower-ngfw-virtual/215258-troubleshooting-firepower-threat-defense.html. Dort finden Sie eine Beschreibung gängiger Bereitstellungsprobleme. In einigen Fällen kann das Rollback fehlschlagen, nachdem der CDO-Managementzugriff wiederhergestellt wurde. In diesem Fall können Sie die CDO-Konfigurationsprobleme lösen und die Bereitstellung über CDO erneut durchführen.

Beispiel:

Für den Threat Defense, der eine Datenschnittstelle für den Managerzugriff verwendet:

```
> configure policy rollback

The last deployment to this FTD was on June 1, 2022 and its status was Successful.
Do you want to continue [Y/N]?

Y
```

```
Rolling back complete configuration on the FTD. This will take time.
.....................
Policy rollback was successful on the FTD.
Configuration has been reverted back to transaction id:
Following is the rollback summary:
...................
.....................
>
```

Schritt 2 Überprüfen Sie, ob die Managementverbindung wiederhergestellt wurde.

Überprüfen Sie in CDO den Status der Managementverbindung auf der Seite **Devices** > **Device Management** > **Device** > **Management** > **Manager Access - Configuration Details** > **Connection Status** (Geräte > Gerätemanagement > Gerät > Management > Managerzugriff – Konfigurationsdetails > Verbindungsstatus).

Geben Sie in der Threat Defense-CLI den Befehl **sftunnel-status-brief** ein, um den Status der Managementverbindung anzuzeigen.

Wenn die Wiederherstellung der Verbindung länger als zehn Minuten dauert, sollten Sie eine Fehlerbehebung durchführen. Siehe Fehlerbehebung in Bezug auf die Managementkonnektivität auf einer Datenschnittstelle, auf Seite 168.

Ausschalten der Firewall mit CDO

Es ist wichtig, dass Sie Ihr System ordnungsgemäß herunterfahren. Wenn Sie einfach den Netzstecker ziehen oder den Netzschalter drücken, kann das Dateisystem ernsthaft beschädigt werden. Denken Sie daran, dass im Hintergrund ständig viele Prozesse ablaufen, und dass das Ziehen des Netzsteckers oder das Ausschalten der Stromversorgung kein ordnungsgemäßes Herunterfahren Ihrer Firewall ermöglicht.

Sie können Ihr System mithilfe von CDO ordnungsgemäß herunterfahren.

Prozedur

Schritt 1 Wählen Sie **Geräte** > **Gerätemanagement** aus.

Schritt 2 Klicken Sie neben dem Gerät, das Sie neu starten möchten, auf das Bearbeitungssymbol ( ).

Schritt 3 Klicken Sie auf die Registerkarte **Device** (Gerät).

Schritt 4 Klicken Sie im Abschnitt **System** auf das Symbol zum Herunterfahren des Geräts ( ).

Schritt 5 Bestätigen Sie bei Aufforderung, dass Sie das Gerät herunterfahren möchten.

Schritt 6 Wenn Sie eine Konsolenverbindung zur Firewall haben, überwachen Sie die Systemaufforderungen, wenn die Firewall heruntergefahren wird. Die folgende Eingabeaufforderung wird angezeigt:

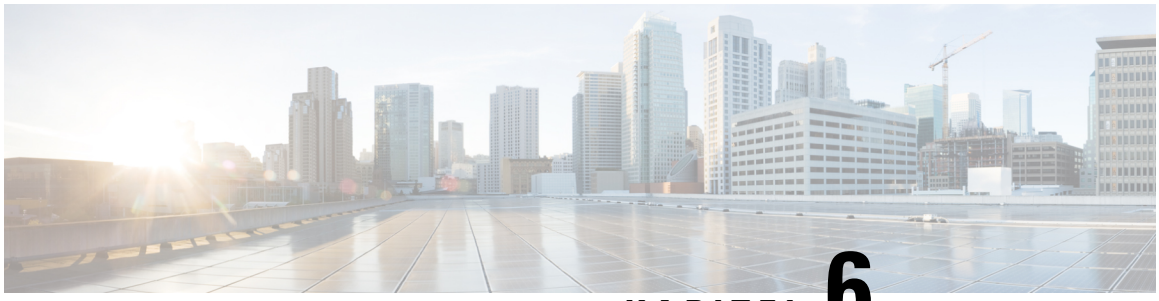
```
System is stopped.
It is safe to power off now.
Do you want to reboot instead? [y/N]
```

Wenn Sie keine Konsolenverbindung haben, warten Sie etwa 3 Minuten, um sicherzustellen, dass das System heruntergefahren wurde.

Schritt 7 Sie können jetzt den Netzstecker ziehen, um die Stromversorgung des Chassis bei Bedarf physisch zu trennen.

Nächste Schritte

Um mit der Konfiguration von Threat Defense mit CDO fortzufahren, besuchen Sie die Cisco Defense Orchestrator-Homepage.



KAPITEL 6

ASA-Bereitstellung mit ASDM

Enthält dieses Kapitel die Informationen, nach denen Sie suchen?

Um alle verfügbaren Betriebssysteme und Manager anzuzeigen, sehen Sie sich Welche Betriebssysteme und Manager sind für Sie geeignet?, auf Seite 1 an. Dieses Kapitel gilt für ASA mit ASDM.

In diesem Kapitel werden die folgenden Bereitstellungen nicht behandelt; Informationen zu diesen Bereitstellungen finden Sie im ASA-Konfigurationsleitfaden:

- Failover
- CLI-Konfiguration

Dieses Kapitel führt Sie auch durch die Konfiguration einer grundlegenden Sicherheitsrichtlinie. Wenn Sie komplexere Anforderungen haben, lesen Sie den Konfigurationsleitfaden.

Informationen zur Firewall

Auf der Hardware kann entweder Threat Defense-Software oder ASA-Software ausgeführt werden. Beim Wechsel zwischen Threat Defense und ASA müssen Sie ein neues Image des Geräts erstellen. Sie sollten auch ein neues Image erstellen, wenn Sie eine andere Softwareversion als derzeit installiert benötigen. Weitere Informationen hierzu finden Sie unter Reimage the Cisco ASA or Firepower Threat Defense Device (Erstellen eines neuen Images für Cisco ASA oder Firepower Threat Defense-Gerät).

Die Firewall führt ein zugrunde liegendes Betriebssystem namens Secure Firewall Extensible Operating System (FXOS) aus. Die Firewall unterstützt die FXOS-Secure Firewall Chassis Manager nicht. Es wird nur in begrenztem Umfang eine CLI für Fehlerbehebungszwecke unterstützt. Weitere Informationen finden Sie unter Cisco FXOS-Leitfaden zur Fehlerbehebung für die Firepower 1000/2100-Serie mit Firepower Threat Defense.

Datenschutzerklärung zur Datenerfassung: Die Firewall erfordert keine personenbezogenen Informationen und nimmt keine aktive Erfassung derartiger Informationen vor. Sie können jedoch personenbezogene Informationen in der Konfiguration verwenden, z. B. bei Benutzernamen. In diesem Fall kann ein Administrator diese Informationen möglicherweise sehen, wenn er mit der Konfiguration arbeitet oder SNMP verwendet.

Informationen zur ASA

Die ASA bietet die Funktionalität für eine erweiterte Stateful-Firewall und einen VPN-Konzentrator in einem Gerät.

Sie können die ASA mit einem der folgenden Manager verwalten:

- ASDM (in diesem Handbuch behandelt): Ein Manager für ein Einzelgerät, der auf dem Gerät enthalten ist.
- CLI
- CDO: Vereinfachter Cloud-basierter Manager für mehrere Geräte (Multi-Device Manager).
- Cisco Security Manager: Ein Manager für mehrere Geräte auf einem separaten Server.

Sie können zur Fehlerbehebung auch auf die FXOS-CLI zugreifen.

Nicht unterstützte Funktionen

Allgemeine nicht unterstützte ASA-Funktionen

Die folgenden ASA-Funktionen werden von Firepower 1010 nicht unterstützt:

- Multiple-Context-Modus
- Aktiv/Aktiv-Failover
- Redundante Schnittstellen
- Clustering
- ASA-REST-API
- Modul ASA Firepower
- Botnet Traffic Filter
- Folgende Untersuchungen:
  - SCTP-Untersuchungszuordnungen (Stateful SCTP-Untersuchung mit ACLs wird unterstützt)
  - Durchmesser
  - GTP/GPRS

Nicht unterstützte Funktionen von VLAN-Schnittstellen und Switch-Ports

VLAN-Schnittstellen und Switch-Ports unterstützen Folgendes nicht:

- Dynamisches Routing
- Multicast-Routing
- Richtlinienbasiertes Routing
- Equal-Cost Multi-Path-Routing (ECMP)
- Inline-Gruppen oder passive Schnittstellen
- VXLAN
- EtherChannels
- Failover und Statusverbindung
- Traffic-Zonen
- Sicherheitsgruppen-Tagging (SGT)

Migrieren einer ASA 5500-X-Konfiguration

Sie können eine ASA 5500-X-Konfiguration kopieren und im Appliance-Modus in Firepower 1010 einfügen. Sie müssen jedoch Ihre Konfiguration ändern. Beachten Sie auch einige Verhaltensunterschiede zwischen den Plattformen.

1. Um die Konfiguration zu kopieren, geben Sie den Befehl **more system:running-config** auf der ASA 5500-X ein.
2. Bearbeiten Sie die Konfiguration nach Bedarf (siehe unten).
3. Verbinden Sie sich im Appliance-Modus mit dem Konsolenport von Firepower 1010, und wechseln Sie in den globalen Konfigurationsmodus:

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa# configure terminal
ciscoasa(config)#
```

4. Löschen Sie die aktuelle Konfiguration mit dem Befehl **clear configure all**.
5. Fügen Sie die geänderte Konfiguration in die ASA-CLI ein.

In diesem Handbuch wird von einer werkseitigen Standardkonfiguration ausgegangen. Wenn Sie also eine vorhandene Konfiguration einfügen, gelten einige der Verfahren in diesem Handbuch nicht für Ihre ASA.

ASA 5500-X-Konfiguration	Konfiguration im Appliance-Modus von Firepower 1010

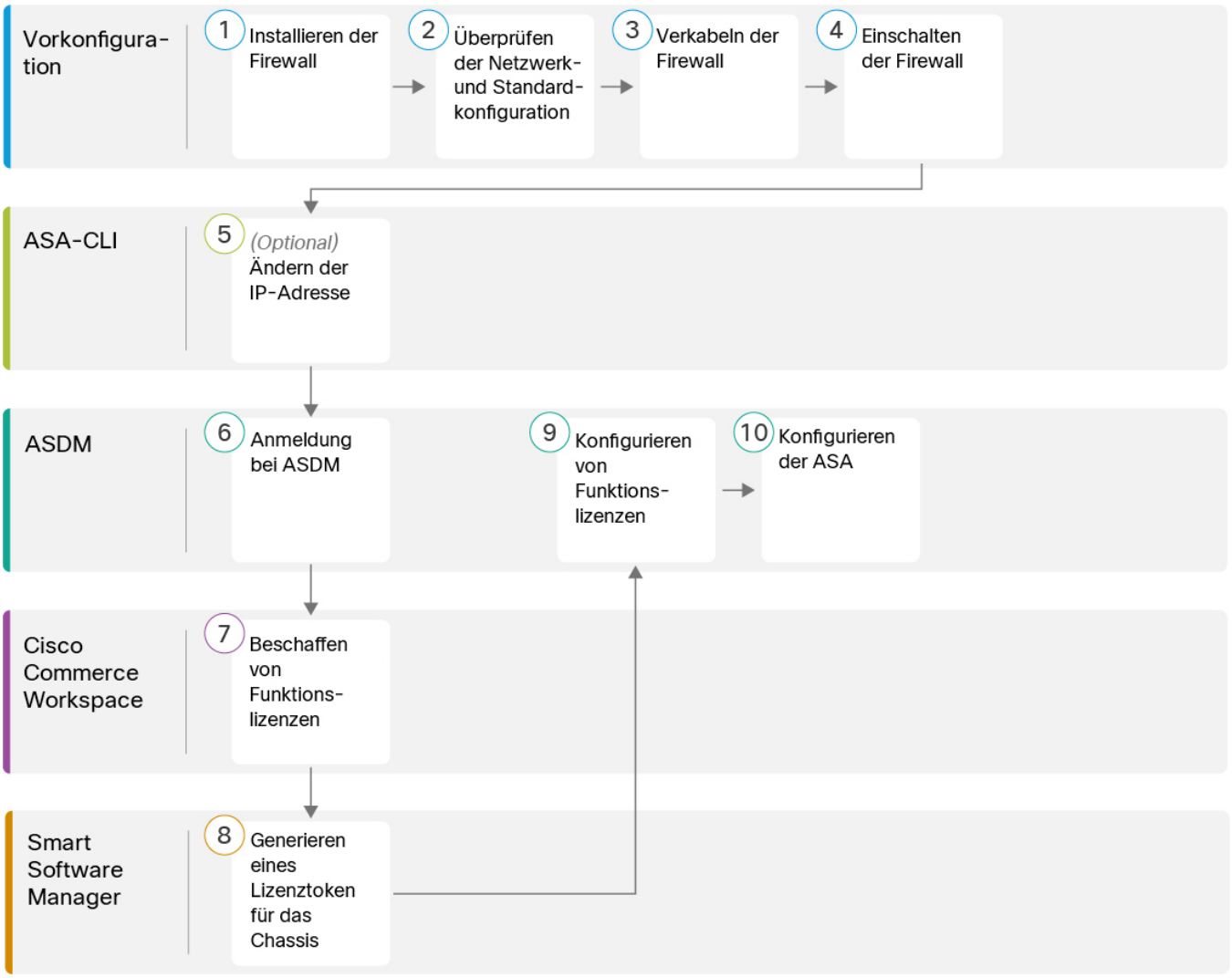
Firewall-Schnittstellen Ethernet 1/2 bis 1/8	Switch-Ports von Ethernet 1/2 bis 1/8
	Diese Ethernet-Ports sind standardmäßig als Switch-Ports konfiguriert. Fügen Sie für jede Schnittstelle in Ihrer Konfiguration den Befehl **no switchport** hinzu, um sie zu einer regulären Firewall-Schnittstelle zu machen. Beispiele:
	`interface ethernet 1/2`
	`  no switchport`
	`  ip address 10.8.7.2 255.255.255.0`
	`  nameif inside`

PAK-Lizenz	Smart License Die PAK-Lizenzierung wird nicht angewendet, wenn Sie Ihre Konfiguration kopieren und einfügen. Es sind standardmäßig keine Lizenzen installiert. Smart Licensing erfordert, dass Sie sich mit dem Smart Licensing-Server verbinden, um Ihre Lizenzen zu erhalten. Smart Licensing wirkt sich auch auf den ASDM- oder SSH-Zugriff aus (siehe unten).
ASDM-Erstzugriff	Entfernen Sie alle Konfigurationen für VPN oder andere starke Verschlüsselungsfunktionen – auch wenn Sie nur eine schwache Verschlüsselung konfiguriert haben –, wenn Sie keine Verbindung zu ASDM herstellen oder sich nicht beim Smart Licensing-Server registrieren können. Sie können diese Funktionen wieder aktivieren, nachdem Sie die 3DES-Lizenz (Strong Encryption) erhalten haben. Der Grund für dieses Problem ist, dass die ASA standardmäßig 3DES-Funktionen nur für den Managementzugriff enthält. Wenn Sie eine starke Verschlüsselungsfunktion aktivieren, werden der ASDM- und HTTPS-Traffic (z. B. zum und vom Smart Licensing-Server) blockiert. Die Ausnahme von dieser Regel ist, wenn Sie mit einer reinen Management-Schnittstelle verbunden sind, z. B. Management 1/1. SSH ist nicht betroffen.
Schnittstellen-IDs	Stellen Sie sicher, dass Sie die Schnittstellen-IDs so ändern, dass sie mit den neuen Hardware-IDs übereinstimmen. Beispiel: ASA 5525-X umfasst Management 0/0 und GigabitEthernet 0/0 bis 0/5. Firepower 1120 umfasst Management 1/1 und Ethernet 1/1 bis 1/8.

ASA 5500-X-Konfiguration	Konfiguration im Appliance-Modus von Firepower 1010
boot system Befehle Die ASA 5500-X erlaubt bis zu vier **boot system**-Befehle für die Angabe des zu verwendenden Boot-Images.	Firepower 1010 erlaubt nur einen einzigen **boot system**-Befehl. Daher sollten Sie bis auf einen Befehl alle Befehle entfernen, bevor Sie Daten einfügen. Tatsächlich müssen Sie *keine* **boot system**-Befehle in Ihrer Konfiguration hinterlegen, da diese beim Start nicht gelesen wird, um das Boot-Image zu bestimmen. Beim erneuten Laden wird immer das zuletzt geladene Boot-Image ausgeführt. Der Befehl **boot system** führt eine Aktion aus, wenn Sie ihn eingeben: Das System validiert das Image, entpackt es und kopiert es in den Boot-Speicherort (einen internen Speicherort auf der von FXOS verwalteten Festplatte0). Das neue Image wird geladen, wenn Sie die ASA neu laden.

Vollständiges Verfahren

Befolgen Sie die folgenden Aufgaben, um die ASA auf Ihrem Chassis bereitzustellen und zu konfigurieren.



1	Vorkonfiguration	Installieren der Firewall. Weitere Informationen finden Sie im Hardware-Installationshandbuch.
2	Vorkonfiguration	Überprüfen der Netzwerkbereitstellung und Standardkonfiguration, auf Seite 183
3	Vorkonfiguration	Verkabeln des Geräts, auf Seite 186
4	Vorkonfiguration	Einschalten der Firewall, auf Seite 13
5	ASA-CLI	(Optional) Ändern der IP-Adresse, auf Seite 188
6	ASDM	Anmeldung bei ASDM, auf Seite 189

7	Cisco Commerce Workspace	Konfigurieren der Lizenzierung, auf Seite 190: Beschaffen Sie sich Funktionslizenzen.
8	Smart Software Manager	Konfigurieren der Lizenzierung, auf Seite 190: Generieren Sie ein Lizenztoken für das Chassis.
9	ASDM	Konfigurieren der Lizenzierung, auf Seite 190: Konfigurieren Sie Funktionslizenzen.
10	ASDM	Konfigurieren der ASA, auf Seite 194

Überprüfen der Netzwerkbereitstellung und Standardkonfiguration

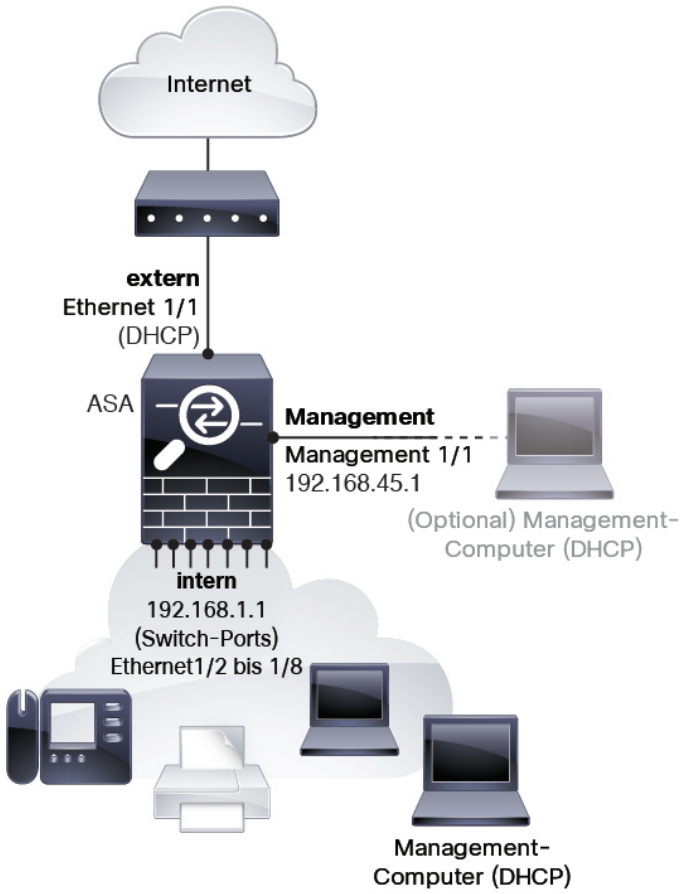
Die folgende Abbildung zeigt die Standardnetzwerkbereitstellung für das Firepower 1010-System mit der Standardkonfiguration.

Wenn Sie die externe Schnittstelle direkt mit einem Kabelmodem oder DSL-Modem verbinden, empfehlen wir, das Modem in den Bridge-Modus zu versetzen, damit ASA das gesamte Routing und die NAT für Ihre internen Netzwerke übernimmt. Falls Sie PPPoE für die externe Schnittstelle konfigurieren müssen, um eine Verbindung zu Ihrem ISP herzustellen, können Sie dies im ASDM Startup Wizard (ASDM-Startassistent) tun.

Hinweis Wenn Sie die standardmäßige Management-IP-Adresse nicht für den ASDM-Zugriff verwenden können, können Sie die Management-IP-Adresse in der ASA-CLI festlegen. Siehe (Optional) Ändern der IP-Adresse, auf Seite 188.

Wenn Sie die interne IP-Adresse ändern müssen, können Sie dies mit dem ASDM-Startassistenten tun. Beispielsweise kann es unter folgenden Umständen erforderlich sein, die interne IP-Adresse zu ändern:

- Wenn die externe Schnittstelle versucht, eine IP-Adresse im Netzwerk 192.168.1.0, einem gängigen Standardnetzwerk, abzurufen, schlägt das DHCP-Lease fehl, und die externe Schnittstelle erhält keine IP-Adresse. Dieses Problem tritt auf, weil es bei ASA keine zwei Schnittstellen im selben Netzwerk geben kann. In diesem Fall müssen Sie die interne IP-Adresse ändern, damit ein neues Netzwerk genutzt wird.
- Wenn Sie ASA zu einem vorhandenen internen Netzwerk hinzufügen, müssen Sie die interne IP-Adresse ändern, damit sie sich im vorhandenen Netzwerk befindet.



Firepower 1010-Standardkonfiguration

In der werkseitigen Standardkonfiguration für Firepower 1010 wird Folgendes konfiguriert:

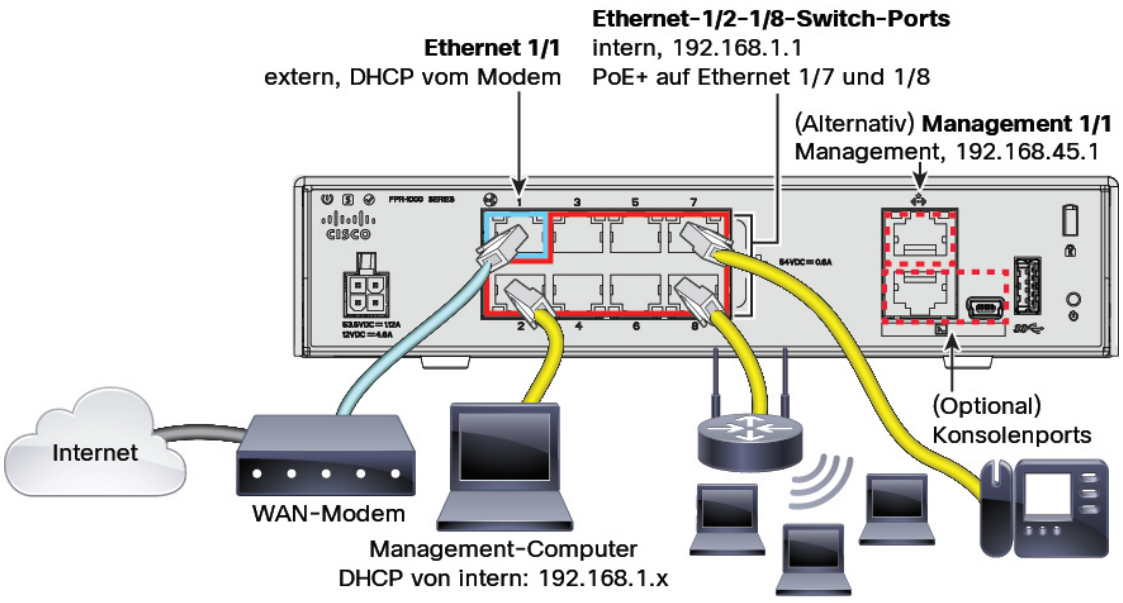
- **Hardware-Switch**: Ethernet 1/2 bis 1/8 gehören zu VLAN 1
- Traffic-Fluss **intern→extern**: Ethernet 1/1 (extern), VLAN1 (intern)
- **Management**: Management 1/1 (Management), IP-Adresse 192.168.45.1
- **externe IP-Adresse** aus DHCP, interne IP-Adresse 192.168.1.1
- **DHCP-Server** auf interner Schnittstelle, Management-Schnittstelle
- **Standardroute** von außerhalb von DHCP
- **ASDM**-Zugriff: Management und interne Hosts sind zulässig. Management-Hosts sind auf das Netzwerk 192.168.45.0/24 und interne Hosts auf das Netzwerk 192.168.1.0/24 beschränkt.
- **NAT**: Schnittstellen-PAT für sämtlichen Traffic von innen nach außen.
- **DNS**-Server: OpenDNS-Server sind vorkonfiguriert.

Die Konfiguration besteht aus den folgenden Befehlen:

```
interface Vlan1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
no shutdown
!
interface Management1/1
managment-only
nameif management
no shutdown
security-level 100
ip address 192.168.45.1 255.255.255.0
!
interface Ethernet1/1
nameif outside
ip address dhcp setroute
no shutdown
!
interface Ethernet1/2
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/3
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/4
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/5
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/6
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/7
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/8
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
object network obj_any
   subnet 0.0.0.0 0.0.0.0
   nat (any,outside) dynamic interface
```

```
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd address 192.168.45.10-192.168.45.12 management
dhcpd enable inside
dhcpd enable management
!
http server enable
http 192.168.45.0 255.255.255.0 management
http 192.168.1.0 255.255.255.0 inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

Verkabeln des Geräts



Verwalten Sie das Firepower 1010-System entweder auf Management 1/1 oder Ethernet 1/2 bis 1/8 (interne Switch-Ports) Die Standardkonfiguration konfiguriert Ethernet 1/1 auch als extern.

Prozedur

Schritt 1 Installieren Sie die Hardware, und machen Sie sich mit der Hardware-Installationsanleitung vertraut.

Schritt 2 Verbinden Sie Ihren Management-Computer mit einer der folgenden Schnittstellen:

- Ethernet 1/2 bis 1/8: Verbinden Sie Ihren Management-Computer direkt mit einem der internen Switch-Ports (Ethernet 1/2 bis 1/8). Die interne Schnittstelle hat eine Standard-IP-Adresse (192.168.1.1) und führt auch einen DHCP-Server aus, um IP-Adressen für Clients (einschließlich des Management-Computers) bereitzustellen. Stellen Sie daher sicher, dass diese Einstellungen nicht mit

vorhandenen internen Netzwerkeinstellungen in Konflikt stehen (siehe Firepower 1010-Standardkonfiguration, auf Seite 184).

- Management 1/1: Verbinden Sie Ihren Management-Computer direkt mit Management 1/1. Alternativ können Sie Management 1/1 mit Ihrem Managementnetzwerk verbinden. Stellen Sie sicher, dass sich Ihr Management-Computer im Managementnetzwerk befindet, da nur Clients in diesem Netzwerk auf die ASA zugreifen können. Management 1/1 hat eine Standard-IP-Adresse (192.168.45.1) und führt auch einen DHCP-Server aus, um IP-Adressen für Clients (einschließlich des Management-Computers) bereitzustellen. Stellen Sie daher sicher, dass diese Einstellungen nicht mit vorhandenen Einstellungen des Managementnetzwerks in Konflikt stehen (siehe Firepower 1010-Standardkonfiguration, auf Seite 184).

  Wenn Sie die Standard-IP-Adresse für Management 1/1 ändern müssen, müssen Sie auch Ihren Management-Computer mit dem Konsolenport verkabeln. Siehe (Optional) Ändern der IP-Adresse, auf Seite 188.

Schritt 3 Verbinden Sie das externe Netzwerk mit der Ethernet 1/1-Schnittstelle.

Für Smart Software Licensing benötigt die ASA Internetzugriff, damit sie auf die Lizenzbehörde zugreifen kann.

Schritt 4 Verbinden Sie interne Geräte mit den verbleibenden internen Switch-Ports (Ethernet 1/2 bis 1/8).

Ethernet 1/7 und 1/8 sind PoE+-Ports.

Einschalten der Firewall

Die Systemstromversorgung wird über das Netzkabel gesteuert. Es gibt keinen Netzschalter.

Hinweis Wenn Sie den Threat Defense zum ersten Mal starten, kann die Initialisierung etwa 15 bis 30 Minuten dauern.

Vorbereitungen

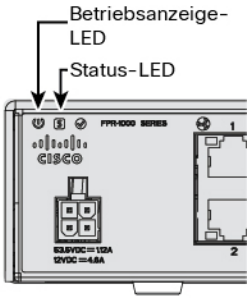
Es ist wichtig, dass Sie Ihr Gerät zuverlässig mit Strom versorgen (z. B. mit einer unterbrechungsfreien Stromversorgung (USV)). Ein Stromausfall ohne vorheriges Herunterfahren kann zu ernsthaften Schäden am Dateisystem führen. Im Hintergrund laufen ständig viele Prozesse ab, und eine Unterbrechung der Stromversorgung ermöglicht kein ordnungsgemäßes Herunterfahren des Systems.

Prozedur

Schritt 1 Schließen Sie das Netzkabel am Gerät und dann an einer Steckdose an.

Wenn Sie das Netzkabel an die Stromversorgung anschließen, ist das Gerät automatisch eingeschaltet.

Schritt 2 Prüfen Sie die Betriebs-LED auf der Rückseite oder Oberseite des Geräts; leuchtet sie dauerhaft grün, ist das Gerät eingeschaltet.



Schritt 3 Prüfen Sie die Status-LED auf der Rückseite oder Oberseite des Geräts; wenn sie dauerhaft grün leuchtet, hat das System die Einschaltdiagnose durchlaufen.

(Optional) Ändern der IP-Adresse

Wenn Sie die Standard-IP-Adresse nicht für den ASDM-Zugriff verwenden können, können Sie die IP-Adresse der Management-Schnittstelle in der ASA-CLI festlegen.

Hinweis Dieses Verfahren stellt die Standardkonfiguration wieder her und legt die ausgewählte IP-Adresse fest. Wenn Sie also Änderungen an der ASA-Konfiguration vorgenommen haben, die Sie beibehalten möchten, sollten Sie dieses Verfahren nicht verwenden.

Prozedur

Schritt 1 Verbinden Sie sich mit dem ASA-Konsolenport, und rufen Sie den globalen Konfigurationsmodus auf. Weitere Informationen finden Sie unter Zugriff auf die ASA- und FXOS-CLI, auf Seite 196.

Schritt 2 Stellen Sie die Standardkonfiguration mit der ausgewählten IP-Adresse wieder her.

configure factory-default [*IP-Adresse* [*Maske*]]

Beispiel:

```
ciscoasa(config)# configure factory-default 10.1.1.151 255.255.255.0
Based on the management IP address and mask, the DHCP address
pool size is reduced to 103 from the platform limit 256

WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.

Begin to apply factory-default configuration:
Clear all configuration
Executing command: interface management1/1
Executing command: nameif management
INFO: Security level for "management" set to 0 by default.
Executing command: ip address 10.1.1.151 255.255.255.0
Executing command: security-level 100
```

```
Executing command: no shutdown
Executing command: exit
Executing command: http server enable
Executing command: http 10.1.1.0 255.255.255.0 management
Executing command: dhcpd address 10.1.1.152-10.1.1.254 management
Executing command: dhcpd enable management
Executing command: logging asdm informational
Factory-default configuration is completed
ciscoasa(config)#
```

Schritt 3 Speichern Sie die Standardkonfiguration im Flash-Speicher.

write memory

Anmeldung bei ASDM

Starten Sie ASDM, um die ASA zu konfigurieren.

Die ASA verfügt standardmäßig über 3DES-Funktionen nur für den Managementzugriff, sodass Sie sich mit Smart Software Manager verbinden und ASDM sofort verwenden können. Sie können auch SSH und SCP verwenden, wenn Sie später den SSH-Zugriff auf die ASA konfigurieren. Für andere Funktionen, die eine starke Verschlüsselung erfordern (z. B. VPN), muss die starke Verschlüsselung (Strong Encryption) aktiviert sein. Dazu müssen Sie sich zunächst bei Smart Software Manager registrieren.

Hinweis Wenn Sie versuchen, Funktionen zu konfigurieren, die eine starke Verschlüsselung verwenden können, bevor Sie sich registrieren, wird Ihre HTTPS-Verbindung auf dieser Schnittstelle getrennt, und Sie können die Verbindung nicht wiederherstellen. Dies gilt selbst dann, wenn Sie eine schwache Verschlüsselung konfigurieren. Die Ausnahme von dieser Regel ist, wenn Sie mit einer reinen Management-Schnittstelle verbunden sind, z. B. Management 1/1. SSH ist nicht betroffen. Wenn Ihre HTTPS-Verbindung getrennt wird, können Sie eine Verbindung zum Konsolenport herstellen, um die ASA neu zu konfigurieren, eine Verbindung zu einer reinen Management-Schnittstelle herstellen oder eine Verbindung zu einer Schnittstelle herstellen, die nicht für eine starke Verschlüsselungsfunktion konfiguriert ist.

Vorbereitungen

- Unter ASDM-Dokumentation auf Cisco.com finden Sie Infos zu den Anforderungen für die Ausführung von ASDM.

Prozedur

Schritt 1 Geben Sie die folgende URL in Ihren Browser ein.

- **https://192.168.1.1**—Interne Schnittstellen-IP-Adresse.Sie können an jedem internen Switch-Port (Ethernet1/2 bis 1/8) eine Verbindung zur internen Adresse herstellen.
- **https://192.168.45.1**: IP-Adresse der Management-Schnittstelle.

Hinweis Geben Sie unbedingt **https://** ein, nicht **http://** oder lediglich die IP-Adresse (die standardmäßig den Wert HTTP annimmt); die ASA leitet eine HTTP-Anfrage nicht automatisch an HTTPS weiter.

Die **Cisco ASDM**-Webseite wird angezeigt. Möglicherweise werden Browser-Sicherheitswarnungen angezeigt, da in der ASA kein Zertifikat installiert ist. Sie können diese Warnungen gefahrlos ignorieren und die Webseite besuchen.

Schritt 2 Klicken Sie auf eine dieser verfügbaren Optionen: **Install ASDM Launcher** (ASDM Launcher installieren) oder **Run ASDM** (ASDM ausführen).

Schritt 3 Befolgen Sie die Anweisungen auf dem Bildschirm, um ASDM entsprechend der ausgewählten Option zu starten.

Der **Cisco ASDM IDM Launcher** wird angezeigt.

Schritt 4 Lassen Sie die Felder für den Benutzernamen und das Kennwort leer, und klicken Sie auf **OK**.

Das ASDM-Hauptfenster wird angezeigt.

Konfigurieren der Lizenzierung

ASA verwendet Smart Licensing. Sie können das reguläre Smart Licensing verwenden, das einen Internetzugang erfordert. Alternativ dazu können Sie für das Offline-Management Permanent License Reservation oder einen Smart Software Manager On-Prem (früher Satellitenserver) konfigurieren. Weitere Informationen zu diesen Offline-Lizenzierungsmethoden finden Sie in der Dokumentation zu den Funktionslizenzen der Cisco ASA-Serie. Dieser Leitfaden gilt für das reguläre Smart Licensing.

Nähere Informationen über die Lizenzierung bei Cisco erhalten Sie unter cisco.com/go/licensingguide

Wenn Sie das Chassis registrieren, stellt Smart Software Manager ein ID-Zertifikat für die Kommunikation zwischen der Firewall und Smart Software Manager aus. Außerdem wird die Firewall dem entsprechenden virtuellen Konto zugewiesen. können Sie bis zur Registrierung bei Smart Software Manager keine Konfigurationsänderungen mehr vornehmen beschränkt, für die spezielle Lizenzen erforderlich sind. Ansonsten wird der Betrieb jedoch nicht beeinträchtigt. Zu den lizenzierten Funktionen zählen:

- Standard
- Security Plus: Für Aktiv/Standby-Failover
- Strong Encryption (3DES/AES): Wenn Ihr Smart Account nicht für eine starke Verschlüsselung autorisiert ist, Cisco jedoch festgestellt hat, dass Sie eine starke Verschlüsselung verwenden dürfen, können Sie Ihrem Konto manuell eine Lizenz für starke Verschlüsselung hinzufügen.
- AnyConnect:- AnyConnect Plus, AnyConnect Apex oder AnyConnect VPN Only.

Die ASA verfügt standardmäßig über 3DES-Funktionen nur für den Managementzugriff, sodass Sie sich mit Smart Software Manager verbinden und ASDM sofort verwenden können. Sie können auch SSH und SCP verwenden, wenn Sie später den SSH-Zugriff auf die ASA konfigurieren. Für andere Funktionen, die eine starke Verschlüsselung erfordern (z. B. VPN), muss die starke Verschlüsselung (Strong Encryption) aktiviert sein. Dazu müssen Sie sich zunächst bei Smart Software Manager registrieren.

Hinweis Wenn Sie versuchen, Funktionen zu konfigurieren, die eine starke Verschlüsselung verwenden können, bevor Sie sich registrieren, wird Ihre HTTPS-Verbindung auf dieser Schnittstelle getrennt, und Sie können die Verbindung nicht wiederherstellen. Dies gilt selbst dann, wenn Sie eine schwache Verschlüsselung konfigurieren. Die Ausnahme von dieser Regel ist, wenn Sie mit einer reinen Management-Schnittstelle verbunden sind, z. B. Management 1/1. SSH ist nicht betroffen. Wenn Ihre HTTPS-Verbindung getrennt wird, können Sie eine Verbindung zum Konsolenport herstellen, um die ASA neu zu konfigurieren, eine Verbindung zu einer reinen Management-Schnittstelle herstellen oder eine Verbindung zu einer Schnittstelle herstellen, die nicht für eine starke Verschlüsselungsfunktion konfiguriert ist.

Wenn Sie das Registrierungstoken für die ASA vom Smart Software Manager anfordern, aktivieren Sie das Kontrollkästchen **Allow export-controlled functionality on the products registered with this token** (Exportgesteuerte Funktionalität für die mit diesem Token registrierten Produkte zulassen), damit die vollständige Strong Encryption-Lizenz angewendet wird (Ihr Konto muss für deren Nutzung berechtigt sein). Die Strong Encryption-Lizenz wird für infrage kommende Kunden automatisch aktiviert, wenn Sie das Registrierungstoken auf das Chassis anwenden. Daher sind keine zusätzlichen Maßnahmen erforderlich. Wenn Ihr Smart Account nicht für eine starke Verschlüsselung autorisiert ist, Cisco jedoch festgestellt hat, dass Sie eine starke Verschlüsselung verwenden dürfen, können Sie Ihrem Konto manuell eine Lizenz für starke Verschlüsselung hinzufügen.

Vorbereitungen

- Sie müssen über ein Masterkonto bei Smart Software Manager verfügen.

  Wenn Sie noch kein Konto haben, klicken Sie auf den Link, um ein neues Konto einzurichten. Mit dem Smart Software Manager können Sie ein Masterkonto für Ihr Unternehmen erstellen.

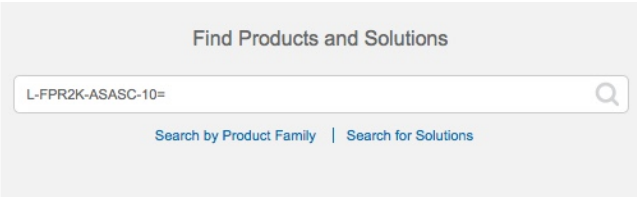
- Ihr Smart Software Manager-Konto muss für die Strong Encryption-(3DES/AES-)Lizenz qualifiziert sein, um bestimmte Funktionen nutzen zu können (aktiviert mit dem „Flag export-compliance“).

Prozedur

Schritt 1 Stellen Sie sicher, dass Ihr Smart Licensing-Konto die verfügbaren erforderlichen Lizenzen enthält, einschließlich mindestens der Standard-Lizenz.

Wenn Sie Ihr Gerät bei Cisco oder einem Fachhändler gekauft haben, sollten Ihre Lizenzen mit Ihrem Smart Software Manager-Konto verknüpft sein. Wenn Sie jedoch selbst Lizenzen hinzufügen müssen, verwenden Sie das Suchfeld **Find Products and Solutions** (Produkte und Lösungen suchen) im Cisco Commerce Workspace. Suchen Sie nach den folgenden Lizenz-PIDs:

Abbildung 54: Lizenzsuche



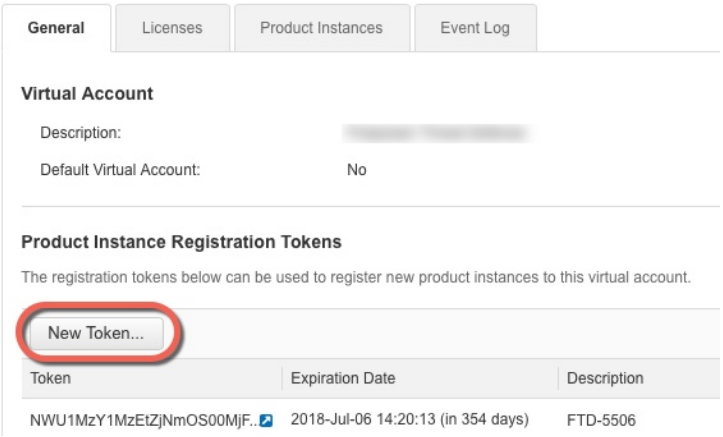
- Standard-Lizenz: L-FPR1000-ASA=. Die Standard-Lizenz ist kostenlos, aber Sie müssen sie dennoch zu Ihrem Smart Software Licensing-Konto hinzufügen.

- Security Plus-Lizenz: L-FPR1010-SEC-PL=. Die Security Plus-Lizenz ermöglicht ein Failover.
- Strong Encryption-Lizenz (3DES/AES): L-FPR1K-ENC-K9=. Nur erforderlich, wenn Ihr Konto nicht für eine starke Verschlüsselung autorisiert ist.
- Anyconnect: Entnehmen Sie die Einzelheiten bitte der Bestellanleitung für Cisco AnyConnect. Sie aktivieren diese Lizenz nicht direkt in der ASA.

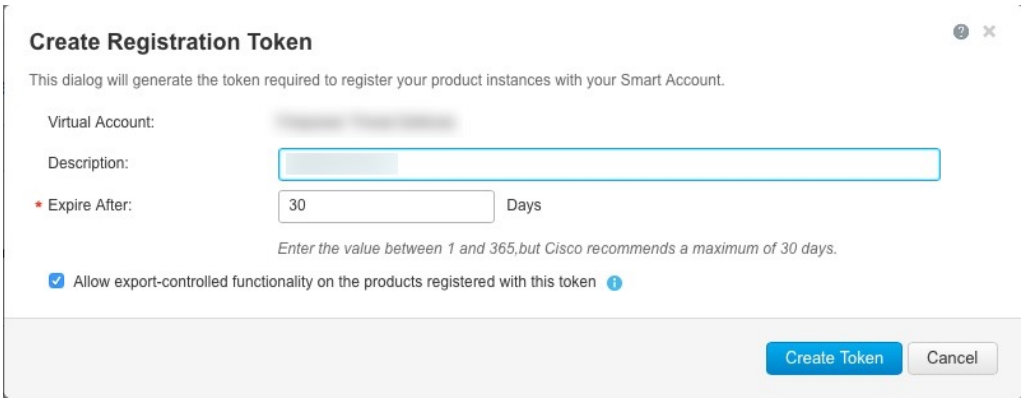
Schritt 2 Fordern Sie in Cisco Smart Software Manager ein Registrierungstoken für das virtuelle Konto an, zu dem Sie dieses Gerät hinzufügen möchten, und kopieren Sie es.

a) Klicken Sie auf **Inventory** (Bestand).

b) Klicken Sie auf der Registerkarte **General** (Allgemein) auf **New Token** (Neues Token).



c) Geben Sie im Dialogfeld **Create Registration Token** (Registrierungstoken erstellen) die folgenden Einstellungen ein, und klicken Sie dann auf **Create Token** (Token erstellen):



- **Beschreibung**

- **Expire after** (Ablauf nach): Cisco empfiehlt 30 Tage.
- **Allow export-controlled functionality on the products registered with this token** (Exportgesteuerte Funktion für die mit diesem Token registrierten Produkte zulassen): Aktiviert das export-compliance-Flag.

Das Token wird Ihrem Bestand hinzugefügt.

d) Klicken Sie auf das Pfeilsymbol rechts neben dem Token, um das Dialogfeld **Token** zu öffnen, damit Sie die Token-ID in Ihre Zwischenablage kopieren können. Halten Sie dieses Token für die ASA-Registrierung bereit, die Sie später in diesem Verfahren ausführen müssen.

Abbildung 55: Token anzeigen

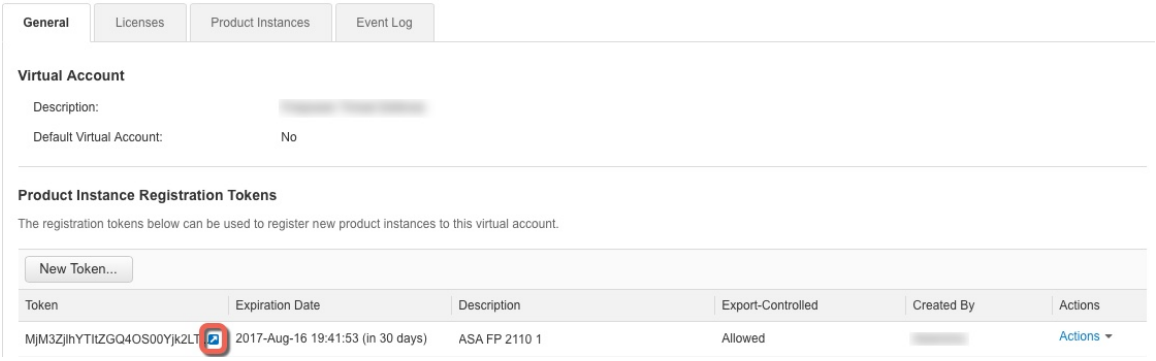
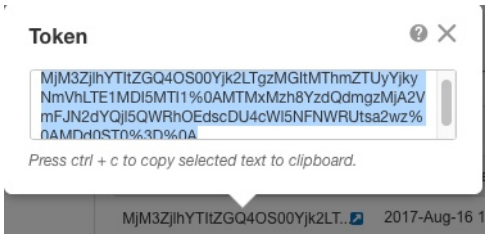


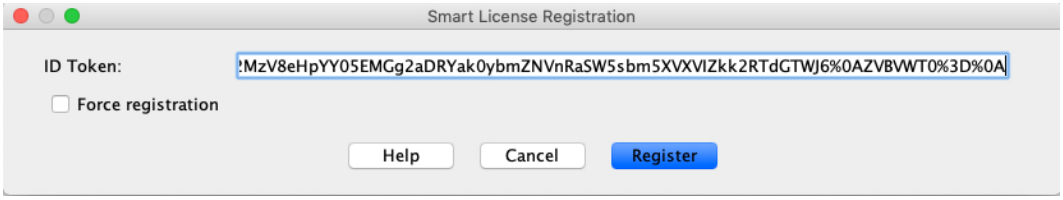
Abbildung 56: Token kopieren



Schritt 3 Wählen Sie in ASDM **Configuration** > **Device Management** > **Licensing** > **Smart Licensing** (Konfiguration > Gerätemanagement > Lizenzierung > Smart Licensing) aus.

Schritt 4 Klicken Sie auf **Register** (Registrieren).

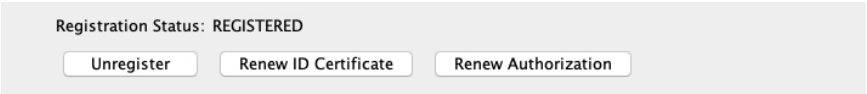
Schritt 5 Geben Sie das Registrierungstoken in das Feld **ID Token** (ID-Token) ein.



Sie können optional das Kontrollkästchen **Force registration** (Registrierung erzwingen) markieren, um eine ASA zu registrieren, die bereits registriert, aber möglicherweise nicht mit Smart Software Manager synchronisiert ist. Verwenden Sie beispielsweise **Force registration** (Registrierung erzwingen), wenn die ASA versehentlich aus Smart Software Manager entfernt wurde.

Schritt 6 Klicken Sie auf **Register** (Registrieren).

Die ASA registriert sich bei Smart Software Manager über die vorkonfigurierte externe Schnittstelle und fordert eine Autorisierung für die konfigurierten Lizenzberechtigungen an. Der Smart Software Manager wendet auch die Strong Encryption-Lizenz (3DES/AES) an, wenn Ihr Konto dies zulässt. ASDM aktualisiert die Seite, wenn der Lizenzstatus aktualisiert wird. Sie können auch **Monitoring** > **Properties** > **Smart License** (Monitoring > Eigenschaften > Smart License) auswählen, um den Lizenzstatus zu prüfen. Dies ist insbesondere dann hilfreich, wenn die Registrierung fehlschlägt.



Schritt 7 Legen Sie die folgenden Parameter fest:

a) Markieren Sie **Enable Smart license configuration** (Smart License-Konfiguration aktivieren).

b) Wählen Sie in der Dropdown-Liste **Feature Tier** (Funktionsstufe) **Standard** aus.

Es ist nur die Standard-Stufe verfügbar.

c) (optional) Markieren Sie **Enable Security Plus** (Security Plus aktivieren).

Die Security Plus-Stufe aktiviert das Aktiv/Standby-Failover.

Schritt 8 Klicken Sie auf **Apply** (Anwenden).

Schritt 9 Klicken Sie in der Symbolleiste auf das Symbol **Speichern**.

Schritt 10 Beenden Sie ASDM und starten Sie das Programm neu.

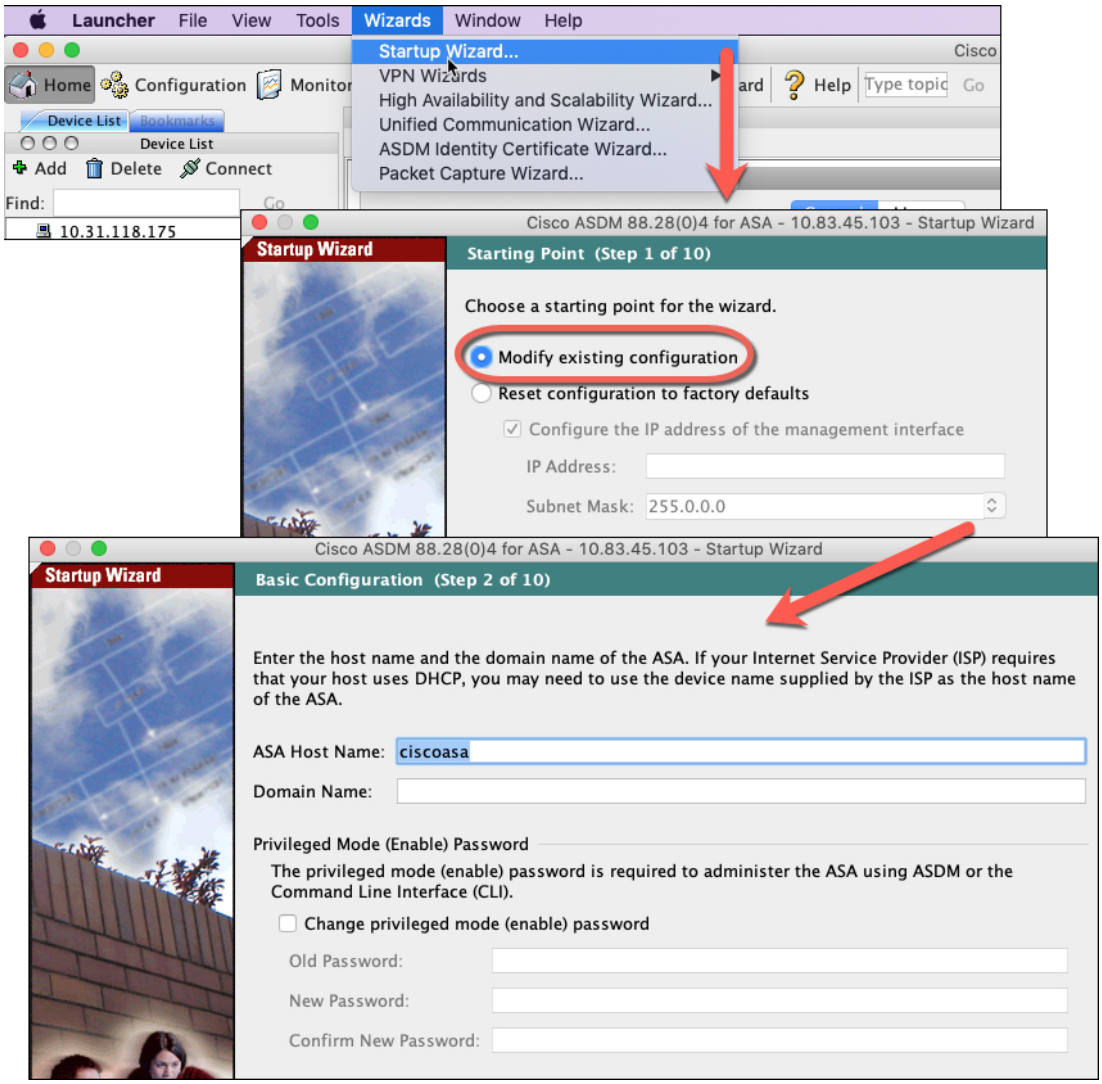
Wenn Sie Lizenzen ändern, müssen Sie ASDM neu starten, damit die Bildschirminhalte aktualisiert werden.

Konfigurieren der ASA

Wenn Sie ASDM verwenden, können Sie mithilfe von Assistenten grundlegende und erweiterte Funktionen konfigurieren. Sie können auch Funktionen konfigurieren, die nicht in Assistenten enthalten sind.

Prozedur

Schritt 1 Wählen Sie **Wizards > Startup Wizard** (Assistent > Startassistent), und klicken Sie auf das Optionsfeld **Modify existing configuration** (Vorhandene Konfiguration ändern).



Schritt 2 Der **Startassistent** führt Sie durch die Konfiguration der folgenden Elemente:

- Aktivierungskennwort
- Schnittstellen; dies umfasst auch die Festlegung der internen und externen Schnittstellen-IP-Adressen und Aktivierung von Schnittstellen.
- Statische Routen
- DHCP-Server
- Und vieles mehr ...

Schritt 3 (optional) Führen Sie im Menü **Wizards** (Assistenten) andere Assistenten aus.

Schritt 4 Um die Konfiguration Ihrer ASA fortzusetzen, lesen Sie die Dokumente, die für Ihre Softwareversion verfügbar sind, siehe Navigieren der Dokumentation zur Cisco ASA-Serie.

Zugriff auf die ASA- und FXOS-CLI

Sie können anstelle von ASDM die ASA-CLI verwenden, um Fehler zu beheben oder die ASA zu konfigurieren. Für den Zugriff auf die CLI (Befehlszeilenschnittstelle) müssen Sie eine Verbindung zum Konsolenport herstellen. Sie können den SSH-Zugriff auf die ASA später auf jeder Schnittstelle konfigurieren. Der SSH-Zugriff ist standardmäßig deaktiviert. Weitere Informationen finden Sie in der Dokumentation ASA General Operations Configuration Guide.

Sie können zur Fehlerbehebung auch über die ASA-CLI auf die FXOS-CLI zugreifen.

Prozedur

Schritt 1 Verbinden Sie Ihren Management-Computer mit dem Konsolenport. Firepower 1000 wird mit einem seriellen USB-A-zu-B-Kabel ausgeliefert. Stellen Sie sicher, dass Sie alle erforderlichen seriellen USB-Treiber für Ihr Betriebssystem installieren (siehe Firepower 1010 Hardwarehandbuch). Verwenden Sie die folgenden seriellen Einstellungen:

- 9.600 Baud
- 8 Daten-Bits
- Keine Parität
- 1 Stopp-Bit

Sie stellen eine Verbindung zur ASA-CLI her. Für den Konsolenzugriff sind standardmäßig keine Benutzeranmeldeinformationen erforderlich.

Schritt 2 Greifen Sie auf den privilegierten EXEC-Modus zu.

enable

Bei der ersten Eingabe des Befehls **enable** werden Sie aufgefordert, das Kennwort zu ändern.

Beispiel:

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat Password: ******
ciscoasa#
```

Das Aktivierungskennwort, das Sie auf der ASA festlegen, ist auch das Kennwort des FXOS-Administratorbenutzers (**admin**), wenn die ASA nicht hochfährt und Sie den FXOS-Failsafe-Modus aktivieren.

Alle Nicht-Konfigurationsbefehle sind im privilegierten EXEC-Modus verfügbar. Sie können den Konfigurationsmodus auch über den privilegierten EXEC-Modus aufrufen.

Um den privilegierten EXEC-Modus zu beenden, geben Sie den Befehl **disable**, **exit** oder **quit** ein.

Schritt 3 Rufen Sie den globalen Konfigurationsmodus auf.

configure terminal

Beispiel:

```
ciscoasa# configure terminal
ciscoasa(config)#
```

Sie können mit der Konfiguration der ASA im globalen Konfigurationsmodus beginnen. Wenn Sie den globalen Konfigurationsmodus beenden möchten, geben Sie den Befehl **exit**, **quit** oder **end** ein.

Schritt 4 (optional) Stellen Sie eine Verbindung zum FXOS-CLI her.

connect fxos [**admin**]

- **admin**: Bietet Zugriff auf Administratorebene. Ohne diese Option haben Benutzer nur Lesezugriff. Beachten Sie, dass auch im Administratormodus keine Konfigurationsbefehle verfügbar sind.

Sie werden nicht zur Eingabe von Benutzeranmeldeinformationen aufgefordert. Der aktuelle ASA-Benutzername wird an FXOS weitergegeben, und es ist keine zusätzliche Anmeldung erforderlich. Um zur ASA-CLI zurückzukehren, geben Sie **exit** oder **Strg+Umschalttaste-6**, **x** ein.

In FXOS können Sie Benutzeraktivitäten mit dem Befehl **scope security/show audit-logs** angeben.

Beispiel:

```
ciscoasa# connect fxos admin
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.
firepower#
firepower# exit
Connection with FXOS terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

Nächste Schritte

- Um die Konfiguration von ASA fortzusetzen, lesen Sie die Dokumente, die für Ihre Softwareversion verfügbar sind, siehe Navigieren der Dokumentation zur Cisco ASA-Serie.
- Informationen zur Fehlerbehebung finden Sie im FXOS-Leitfaden zur Fehlerbehebung.