



## Firepower Management Center を使用したデバイスの管理方法

初版：2018年11月28日

最終更新：2018年11月28日

### シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

**【注意】** シスコ製品をご使用になる前に、安全上の注意（[www.cisco.com/jp/go/safety\\_warning/](http://www.cisco.com/jp/go/safety_warning/)）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェアライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

Tシスコが導入する TCP ヘッダー圧縮は、カリフォルニア大学バークレー校 (UCB) により、UNIX オペレーティング システムの UCB パブリック ドメインバージョンの一部として開発されたプログラムを適応したものです。 Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

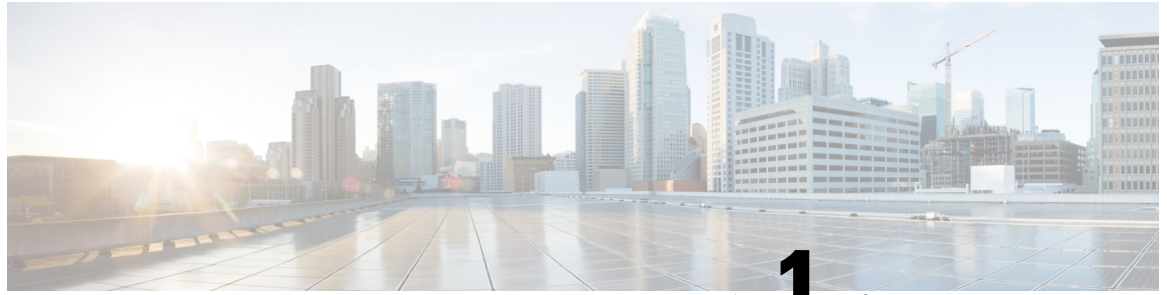
このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

ハードコピーおよびソフトコピーの複製は公式版とみなされません。最新版はオンライン版を参照してください。

シスコは世界各国 200 箇所にオフィスを開設しています。各オフィスの住所、電話番号、FAX 番号は当社の Web サイト（[www.cisco.com/go/offices](http://www.cisco.com/go/offices)）をご覧ください。

Cisco および Cisco ロゴは、シスコまたはその関連会社の米国およびその他の国における商標または登録商標です。シスコの商標の一覧は、[www.cisco.com go trademarks](http://www.cisco.com/go/trademarks) でご確認いただけます。掲載されている第三者の商標はそれぞれの権利者の財産です。「パートナー」または「partner」という用語の使用はシスコと他社との間のパートナーシップ関係を意味するものではありません。(1721R)

© 2018 Cisco Systems, Inc. All rights reserved.



# 第 1 章

## このマニュアルについて

この How-To ガイドでは、Firepower Management Center Version 6.2.3 デバイスをセットアップして、Firepower Threat Defense Version 6.2.3 デバイスを管理して内部ネットワークと外部ネットワーク（インターネット）を含むサンプルネットワークにインスペクションとセキュリティの機能を装備する方法を説明します。このガイドのすべての手順を実行すると、本ガイドと同一のシステムを設定できます。

- [このガイドの内容（1 ページ）](#)
- [ネットワークのセットアップについて（3 ページ）](#)
- [ネットワーク セットアップ タスクの概要（4 ページ）](#)

## このガイドの内容

このガイドでは、Firepower Version 6.2.3 システム（バージョン 6.2.3 を実行している Firepower Management Center および Firepower Threat Defense デバイス）を使用して基本ネットワークをセットアップする方法を説明します。この基本セットアップは、Firepower Management Center をアクセス制御、侵入防御、およびモニタリングに使用するために必要です。Firepower システムで他の操作を実行する前に、以下のタスクを実行する必要があります。



- (注) このガイドでは、お使いのシステムで使用可能な IP アドレスの例を示しています。ただし、これらの IP アドレスがお使いのネットワーク内のアドレスと競合しないことを前提としています。このガイドで説明されている IP アドレスと同じ IP アドレスを使用することができますか、お使いのネットワークと互換性がある IP アドレスを使用することも可能です。お使いのネットワークに適合するように IP アドレスを変更する場合は、Firepower Threat Defense 管理インターフェイスと Firepower Management Center のインターフェイスが同じサブネット上に存在するようにしてください。

### このガイドで説明するセットアップタスク

このガイドでは、サンプル値を使用して以下のタスクを実行する方法を、手順を追って説明します。

- ネットワーク上に Firepower Management Center を設定する。
- ネットワーク上に Firepower Threat Defense を設定する。
- Firepower Management Center にライセンスを適用する。
- Firepower Management Center を使用して Firepower Threat Defense デバイスを管理する。
- NAT ポリシーとスタティック ルートを設定する。
- すべてのトラフィックを許可する初期アクセスコントロールルールをセットアップする。これにより、内部ネットワークに接続されているクライアントからインターネットアクセスをテストできるようになり、管理対象デバイスがトラフィックをフィルタリングしていることを確認できます。

### このガイドの対象読者

Firepower システムを構成するユーザ（管理者やインテグレータを含む）。

### 必要となる事項

このガイドで説明するタスクを完了するには、以下の項目が必要となります。

- バージョン 6.2.3 を実行している Firepower Management Center（物理または仮想を問わず任意のモデル）
- バージョン 6.2.3 を実行している Firepower Threat Defense（物理または仮想を問わず任意のモデル）

Firepower Management Center または Firepower Threat Defense デバイスのアップグレードについての詳細は、『[Firepower Management Center アップグレードガイド](#)』を参照してください。



---

(注) 別のバージョンの Firepower システム ソフトウェアも使用できませんが、追加タスクまたは異なるタスクが必要となる場合があります。詳細については、ご使用のバージョンに該当するコンフィグレーションガイドまたはクイック スタートガイドをご覧ください。

---

- ハイパーバイザ マネージャおよびクライアント（仮想デバイスの場合）。
- プライベート ネットワーク。このシステムで使用される IP アドレスがネットワークで使用されている IP アドレスと競合しないようにするため。たとえば、仮想 LAN (VLAN) をセットアップできます。このシステムをネットワークの残りの部分から分離する方法の説明は、このガイドの対象外です。
- (オプション) シスコスマートライセンス。スマートライセンスをお持ちでない場合は、90 日間の評価用ライセンスを使用できます。

バージョン 6.2.3 のスマート ライセンスの詳細については、[Firepower システムのスマート ライセンス \(英語\)](#) を参照してください。

#### 関連トピック

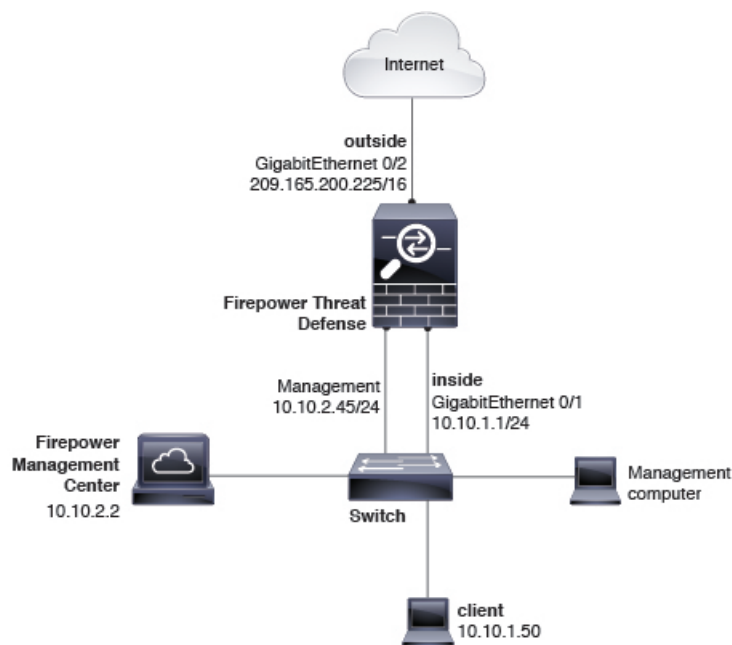
[ネットワークのセットアップについて \(3 ページ\)](#)

[ネットワーク セットアップ タスクの概要 \(4 ページ\)](#)

## ネットワークのセットアップについて

このガイドでは、次のネットワークのセットアップについて順を追って説明します。

図 1: このガイドで使用されるサンプル ネットワーク



### Firepower Threat Defense インターフェイス

このサンプル ネットワークでは Firepower Threat Defense デバイスに管理、内部および外部の 3 つのインターフェイスがあります。外部インターフェイスは、インターネットに直接接続します。許可のアクセス コントロール ルールを使用して、内部ネットワークに接続されているクライアントは Firepower Threat Defense デバイスを介してインターネットに接続できます。このタイプの構成は、ブートストラップと呼ばれることがあります。これは、インターネットに接続するための最小限の構成であるためです。

#### 管理 (1 / 1)

IP アドレス 10.10.2.45。Firepower Management Center との通信にのみ使用されます。管理 IP アドレスは、Firepower Management Center と同じサブネット上に存在する必要があります。

**内部 (GigabitEthernet 1 / 2)**

IP アドレス 10.10.2.1。内部インターフェイスに接続されているコンピュータには、アクセスコントロールポリシーと侵入防御ポリシーを適用できます。内部ネットワークのデフォルト ゲートウェイは 10.10.2.254 です。

**外部 (GigabitEthernet 1 / 1)**

IP アドレス 209.165.200.255。インターネットへの接続に使用します。外部ネットワークのデフォルト ゲートウェイは、209.165.200.254 です。



- (注) このガイドでは、お使いのシステムで使用可能な IP アドレスの例を示しています。ただし、これらの IP アドレスがお使いのネットワーク内のアドレスと競合しないことを前提にしています。このガイドで説明されている IP アドレスと同じ IP アドレスを使用することができますか、お使いのネットワークと互換性がある IP アドレスを使用することも可能です。お使いのネットワークに適合するように IP アドレスを変更する場合は、Firepower Threat Defense 管理インターフェイスと Firepower Management Center のインターフェイスが同じサブネット上に存在するようにしてください。



- (注) 管理しているデバイスのタイプに応じて、インターフェイスはこのガイドの例とは異なって識別される場合があります。たとえば、仮想管理対象デバイスには、gigabitethernet0/0、GigabitEthernet0/1 などと番号付けされたインターフェイスがあります。Firepower Threat Defense 4100 または 9300 シリーズデバイスには、ethernet1/1、Ethernet2/1、Ethernet3/1 などと番号付けされたインターフェイスがあります。

**Firepower Management Center**

Firepower Management Center には、IP アドレス 10.10.2.2 のインターフェイスが 1 つあります。このインターフェイスは、Firepower Threat Defense デバイスの管理に使用します。各デバイスは、すべて同じサブネット上の管理 IP アドレスを持つ必要があります。

## ネットワーク セットアップ タスクの概要

このトピックでは、[ネットワークのセットアップについて \(3 ページ\)](#) で説明したネットワークのセットアップの高レベルの概要を説明します。

**手順**

	コマンドまたはアクション	目的
ステップ 1	前提条件。	<a href="#">このガイドの内容 (1 ページ)</a>
ステップ 2	Firepower Management Center を Firepower Threat Defense に、および Firepower Management Center へのアクセスに使用するコンピュータからアクセス	

	コマンドまたはアクション	目的
	可能なネットワークに接続するスイッチに、Firepower Management Center を接続します。	
ステップ 3	ネットワーク上で Firepower Management Center をセットアップします。	SSH またはターミナル サーバを使用してデバイスにアクセスし、 <b>configure-network</b> コマンドを実行してデバイスの管理 IP アドレス、サブネット、DNS サーバなどを設定します。 <a href="#">Firepower Management Center をネットワークに接続する (7 ページ)</a> を参照してください。
ステップ 4	ネットワークで Firepower Threat Defense をセットアップします。	Firepower Threat Defense にはセットアップスクリプトが搭載されており Firepower Management Center と同じタスクを実行します。また、ルーテッドモードを選択でき、デバイスを Firepower Management Center で管理できます。 <a href="#">管理対象デバイスをネットワークに接続する (8 ページ)</a> を参照してください。
ステップ 5	Firepower Management Center を初期設定します。	Web ブラウザで Firepower Management Center にアクセスし、タイムゾーン、タイムサーバ、自動バックアップなどを含む追加オプションを設定します。 <a href="#">Firepower Management Center の初期設定 (11 ページ)</a> を参照してください。
ステップ 6	Firepower Management Center のライセンスを適用する	スマートライセンスまたは 90 日間評価ライセンスのいずれかを適用します。評価ライセンスは完全に機能しますが、実稼働にはスマートライセンスを使用する必要があります。 <a href="#">Firepower Management Center の初期設定 (11 ページ)</a> を参照してください。
ステップ 7	Firepower Threat Defense を管理対象デバイスとして Firepower Management Center に追加します。	管理対象デバイスを追加したら、Firepower Management Center ですべての詳細な設定を行います。 <a href="#">Firepower Management Center に管理対象デバイスを追加する (17 ページ)</a> を参照してください。
ステップ 8	Firepower Threat Defense のインターフェイス、スタティックルート、および NAT ルールを設定します。	内部および外部インターフェイスと NAT ルールを設定して、トラフィックを任意のネットワークから外部インターフェイスに送信します。外部インターフェイスへのスタティックルートを設定します。 <a href="#">管理対象デバイスの設定 (17 ページ)</a> を参照してください。
ステップ 9	アクセスコントロールポリシーを編集して、インターネットアクセスを許可します。	この一時的なアクセスコントロールルールは、外部インターフェイスへのトラフィックを許可しま

	コマンドまたはアクション	目的
		す。 <a href="#">アクセス コントロール ポリシーの編集 (27 ページ)</a> を参照してください。
<b>ステップ 10</b>	内部ネットワークにクライアントを接続して、クライアントがインターネットに確実にアクセスできることを確認します。	クライアントがインターネットへアクセスできること、および管理対象デバイスがトラフィックをフィルタリングしていることを確認します。 <a href="#">システムのトラブルシューティング (32 ページ)</a> を参照してください。
<b>ステップ 11</b>	問題が発生した場合は、トラブルシューティングします。	通常、問題は物理的なネットワークの問題に関連したもの、または不適切に設定されているスタティックルートやNATポリシーに関連したものです。 <a href="#">システムのテスト (29 ページ)</a> を参照してください。





## 第 2 章

# デバイスをセットアップしてネットワークに接続する

初めに、Firepower Management Center と Firepower Threat Defense デバイスをネットワークに接続します。組織におけるネットワークデバイスの管理方法によっては、デバイスをラックに設置するために支援が必要な場合があります。

- [デバイスのセットアップ \(7 ページ\)](#)
- [Firepower Management Center をネットワークに接続する \(7 ページ\)](#)
- [管理対象デバイスをネットワークに接続する \(8 ページ\)](#)

## デバイスのセットアップ

物理デバイスおよび仮想デバイスはモデルによりセットアップ方法が異なるため、Firepower Management Center と Firepower Threat Defense デバイスのマニュアルを参照して次の作業を実行してください。

- (物理アプライアンス) : [ハードウェアのインストールガイド](#)を使用して、開梱とラックへの設置を行い、デバイスをネットワークに接続します。
- (仮想デバイス) : [仮想デバイスのクイック スタート ガイド](#)を使用して、仮想マシンイメージをインストールして電源をオンにします。

これらのタスクを実行した後は、次のセクションに進んで IP アドレスを設定し、Firepower システムを稼働させるために必要なその他のタスクを実行します。

## Firepower Management Center をネットワークに接続する

このタスクでは、インターネットにアクセスするための Firepower Management Center の初期設定を行います。IP アドレス、サブネットマスク、およびその他のパラメータを指定します。ネットワーク構成図の例 [ネットワークのセットアップについて \(3 ページ\)](#) を参照してください。

### 始める前に

[デバイスをセットアップしてネットワークに接続する \(7 ページ\)](#) を参照してください。

**ステップ 1** VSphere で、または物理アプライアンスのコンソール ポートで、または Secure Shell (SSH) を使用して、仮想マシンのコンソールに接続します。

**ステップ 2** Firepower Management Center に `admin` ユーザでログインします (デフォルトのパスワードは `Admin123`)。

**ステップ 3** プロンプトで、次のコマンドを入力します。

```
sudo configure-network
```

**ステップ 4** プロンプトが表示されたら、パスワード `Admin123` を入力します。

**ステップ 5** プロンプトで次の情報を入力します。

```
Do you want to configure IPv4 (y or n)? y
Management IP address [192.168.45.45]? 10.10.2.2
Management netmask [255.255.255.0]? 255.255.255.0
Management default gateway? 10.10.2.254
Are these settings correct (y or n)? y
Do you wish to configure IPv6? n
```

**ステップ 6** 次のメッセージが表示され、設定が成功したことを示します。

```
Updated network configuration
Updated comms. channel communication
```

### 次のタスク

[管理対象デバイスをネットワークに接続する \(8 ページ\)](#) を参照してください。

## 管理対象デバイスをネットワークに接続する

Firepower Threat Defense のネットワークへの接続は、Firepower Management Center のネットワークへの接続とほぼ同じです。その管理インターフェイスの IP アドレスとサブネットマスクを指定し、さらにデバイスがルーテッドモードで動作するように、また Firepower Management Center によって管理されるように指定します。ネットワーク構成図の例 [ネットワークのセットアップについて \(3 ページ\)](#) を参照してください。

ルーテッドモードの詳細については、「[About Routed Firewall Mode \(ルーテッドファイアウォールモードについて\)](#)」を参照してください。

### 始める前に

[デバイスをセットアップしてネットワークに接続する \(7 ページ\)](#) を参照してください。

- ステップ 1 VSphere で、または物理アプライアンスのコンソールポートで、または Secure Shell (SSH) を使用して、仮想マシンのコンソールに接続します。
- ステップ 2 デフォルトのユーザ名 `admin` とパスワード `Admin123` でログインします。
- ステップ 3 デバイスで必要な場合は、`connect ftd` と入力します。
- ステップ 4 `Enter` を押して EULA を表示し、スペースを押してページを送ります。
- ステップ 5 プロンプトが表示されたら `yes` と入力して、EULA に同意します。
- ステップ 6 `Enter new password` プロンプトで管理対象デバイスのパスワードを入力して、プロンプトが表示されたら、パスワードを確認します。

- ステップ 7 次のプロンプトで以下の情報を入力します。

```
Do you want to configure IPv4 (y/n)? [y] y
Do you want to configure IPv6 (y/n)? [n] n
Configure IPv4 via DHCP or manually? (dhcp/manually) [manual] manual
Enter an IPv4 address for the management interface [192.168.45.1] 10.10.2.45
Enter an IPv4 netmask for the management interface [255.255.255.0] 255.255.255.0
Enter an IPv4 default gateway for the management interface 10.10.2.254
Enter a fully qualified hostname for this device [firepower] firepower
Enter a comma-separated list of DNS servers or 'none' [208.67.222.222,208.67.202.202] 8.8.8.8
Enter a comma-separated list of search domains or 'none' [] none
Are these settings correct (y or n)? y
```

- ステップ 8 次のプロンプトが表示されます。

```
If your networking information has changed, you will need to reconnect.
For HTTP Proxy configuration, run 'configure network http-proxy'
```

- ステップ 9 次の情報を入力します。

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

- ステップ 10 次のプロンプトが表示されます。

```
Configuring firewall mode ...
```

- ステップ 11 次のプロンプトで、以下のコマンドを入力します。

```
configure manager add 10.10.2.2 cisco123
```

- ステップ 12 次のプロンプトで、アクションが成功したことを確認します。

```
Manager successfully configured.
```

## 次のタスク

[Firepower Management Center の設定 \(11 ページ\)](#) を参照してください。





## 第 3 章

# Firepower Management Center の設定

デバイスの管理やネットワークへのアクセス制御を行う前に、Firepower Management Center に追加のインターネット設定やライセンスを構成する必要があります。

- [Firepower Management Center の初期設定](#) (11 ページ)
- [Firepower Management Center にライセンスを適用する](#) (14 ページ)

## Firepower Management Center の初期設定

始める前に

[Firepower Management Center をネットワークに接続する](#) (7 ページ) を参照してください。

**ステップ 1** ブラウザのアドレスまたはロケーションのフィールドで、`https://10.10.2.2` を入力します。

**ステップ 2** ユーザ名 `admin` およびパスワード `Admin123` でログインします。  
初期設定のページが表示されます。以下の手順では、セクションごとに設定を説明します。

**ステップ 3** 次のフィールドに、Firepower Management Center の新しいパスワードを入力します。

**Change Password**

Use these fields to change the password for the admin account. Cisco recommends that you use a password that has at least eight alphanumeric characters of mixed case and includes at least one numeric character. Avoid using words that appear in a dictionary.

New Password	<input type="text"/>
Confirm	<input type="text"/>

**ステップ 4** 次の図に示すネットワーク設定を入力します。組織に固有の DNS サーバを入力します (該当する場合)。

**Network Settings**

Use these fields to specify network-related information for the management interface on the appliance.

Protocol  IPv4  IPv6  Both

IPv4 Management IP

Netmask

IPv4 Default Network Gateway

Hostname

Domain

Primary DNS Server

Secondary DNS Server

Tertiary DNS Server

**Time Settings**

**ステップ 5** 次の図に示すタイム サーバとタイム ゾーンの設定を入力します。必要に応じて [America/New York] をクリックして、画面の指示に従ってタイム ゾーンを選択します。

**Time Settings**

Use these fields to specify how you want to set the time for the Defense Center.

Set My Clock  Via NTP from   
 Manually  /  /  :  :

Current Time

Set Display Time Zone

**ステップ 6** 定期的な更新と自動バックアップのオプションを選択します。

- [Recurring Rule Update Imports] : 新しい脆弱性が発見されると、脆弱性調査チーム (VRT) は侵入ルールの更新をリリースします。ルールの更新では、新規および更新された侵入ルールおよびプリプロセスルール、既存のルールの変更されたステータス、変更されたデフォルト侵入ポリシーの設定が提供されます。また、ルール更新ではルールが削除されたり、新しいルールカテゴリとシステム変数が提供されたりすることもあります。

それぞれのルール更新の後で、システムが侵入についての [Policy Reapply] を実行するよう設定するだけでなく、[Import Frequency] も指定することができます。初期設定プロセスの一部としてルールの更新を実行するには、[Install Now] をオンにします。

ルールの更新には、新しいバイナリが含まれている場合があります。ルール更新のダウンロードおよびインストールのプロセスが、自身のセキュリティポリシーに適合していることを確認します。加えて、ルール更新のサイズが大きい場合があるため、ネットワーク使用率の低い時間帯にルールをインポートするようにしてください。

- [Recurring Geolocation Updates] : Firepower Management Centers は、システムで生成されたイベントに関連付けられているルーテッド IP アドレスの地理情報を表示できるほか、ダッシュボードおよび Context Explorer の地理情報統計も監視できます。

Firepower Management Center の地理情報データベース (GeoDB) には、IP アドレスに関連するインターネット サービス プロバイダ (ISP)、接続タイプ、プロキシ情報、正確な位置情報などの情報が含まれています。定期的な GeoDB の更新を有効にすることで、システムが常に最新の地理情報を使用するようになります。

GeoDB について、週次の更新頻度を指定できます。初期設定プロセスの一部としてデータベースをダウンロードするには、[Install Now] をオンにします。

GeoDB の更新は、ダウンロード後のインストールに最大で 45 分かかることがあります。GeoDB は、ネットワークの使用量が少ないときに更新してください。

- [Enable automatic backup] : スケジュールされたタスクが作成され、このタスクによって Firepower Management Center の設定のバックアップが週次に作成されます。

The screenshot shows three sections of configuration options:

- Recurring Rule Update Imports**: Includes an "Install Now" checkbox and "Enable Recurring Rule Update Imports from the Support Site" checkbox, both currently unchecked.
- Recurring Geolocation Updates**: Includes an "Install Now" checkbox and "Enable Recurring Weekly Updates from the Support Site" checkbox, both currently unchecked.
- Automatic Backups**: Includes "Enable Automatic Backups" checkbox, currently unchecked.

- ステップ 7** [License Settings] セクションは、クラシック ライセンスのみに適用されるため空白のままにしてください。後でスマート ライセンスを適用します。

The screenshot shows the "License Settings" section with the following details:

- Instructions: "To obtain your license, navigate to <https://www.cisco.com/go/license/> where you will be prompted for the license key (66:00:50:56:8D:1A:5D) and the activation key, which was emailed to the contact person on your support contract. Follow the on-screen instructions to generate a license, which will be emailed to you. Paste the license below and click Add/Verify. If your browser cannot access the Internet, switch to a host that can."
- License Key: 66:00:50:56:8D:1A:5D
- A large empty text input field for pasting the license.
- An "Add/Verify" button at the bottom left.

- ステップ 8** ライセンス契約をスクロールし、同意する場合は [I have read and agree to the End User License Agreement] をオンにして [Apply] をクリックします。

**End User License Agreement**

End User License Agreement

Effective: May 22, 2017

This is an agreement between You and Cisco Systems, Inc. or its affiliates ("Cisco") and governs your Use of Cisco Software. "You" and "Your" means the individual or legal entity licensing the Software under this EULA. "Use" or "Using" means to download, install, activate, access or otherwise use the Software. "Software" means the Cisco computer programs and any Upgrades made available to You by an Approved Source and licensed to You by Cisco. "Documentation" is the Cisco user or technical manuals, training materials, specifications or other documentation applicable to the Software and made available to You by an Approved Source. "Approved Source" means (i) Cisco or (ii) the Cisco authorized reseller, distributor or systems integrator from whom you acquired the Software. "Entitlement" means the license detail; including license metric, duration, and quantity provided in a product ID (PID) published on Cisco's price list, claim certificate or right to use notification. "Upgrades" means all updates, upgrades, bug fixes, error corrections, enhancements and other modifications to the Software and backup copies thereof.

This agreement, any supplemental license terms and any specific product terms at [www.cisco.com/go/softwareterms](http://www.cisco.com/go/softwareterms) (collectively, the "EULA") govern Your Use of the Software.

1. **Acceptance of Terms. By Using the Software, You agree to be bound by the terms of the EULA. If you are entering into this EULA on**

I have read and agree to the End User License Agreement.

Apply

**ステップ 9** 入力した情報を Firepower Management Center が処理するまで待機します。この時点で、ダッシュボードが表示されます。

#### 次のタスク

[Firepower Management Center にライセンスを適用する \(14 ページ\)](#) を参照してください。

## Firepower Management Center にライセンスを適用する

このタスクでは、Firepower Management Center および管理対象デバイスで 90 日間の評価ライセンスを使用する方法について説明します。スマートライセンスがあれば、代わりに使用することができます。

**ステップ 1** 必要に応じて、Firepower Management Center にログインします。

**ステップ 2** **[System] > [Licenses] > [Smart Licenses]** をクリックします。

**ステップ 3** 90 日間評価ライセンスの **[Evaluation Mode]** をクリックするか、**[Register]** をクリックしてスマートライセンスを登録します。

**Welcome to Smart Licenses**

Before you use Smart Licenses, obtain a registration token from [Cisco Smart Software Manager](#), then click Register

Register Evaluation Mode

**ステップ 4** 評価ライセンスを使用する場合は、**[Yes]** をクリックして 90 日間の評価期間を開始します。評価ライセンスを選択した場合、次のページが表示されます。



## Smart License Status

[Cisco Smart Software Manager](#)

Usage Authorization:	N/A
Product Registration:	 Evaluation Period (Expires in 89 days)
Assigned Virtual Account:	Evaluation Mode
Export-Controlled Features:	Disabled
Cisco Success Network:	Disabled 

## Smart Licenses

Filter Devices... 

Edit Licenses

License Type/Device Name	License Status	Device Type	Domain	Group
<b>Base (0)</b>				
<b>Malware (0)</b>				
<b>Threat (0)</b>				
<b>URL Filtering (0)</b>				
<b>AnyConnect Apex (0)</b>				
<b>AnyConnect Plus (0)</b>				
<b>AnyConnect VPN Only (0)</b>				

## 次のタスク

[管理対象デバイスの設定 \(17 ページ\)](#) を参照してください。





## 第 4 章

# 管理対象デバイスの設定

---

管理対象デバイスの設定は、デバイスを Firepower Management Center に追加してそのインターフェイスをセットアップすることを意味します。

- [Firepower Management Center に管理対象デバイスを追加する \(17 ページ\)](#)
- [管理対象デバイスのインターフェイスの設定 \(19 ページ\)](#)
- [スタティック ルートの追加 \(21 ページ\)](#)
- [NAT ポリシーの追加 \(22 ページ\)](#)

## Firepower Management Center に管理対象デバイスを追加する

管理対象デバイスとして Firepower Threat Defense を追加した後に、Firepower Management Center を使用してその詳細を設定します。

### 始める前に

初めに、次のタスクを完了する必要があります。

- [Firepower Management Center をネットワークに接続する \(7 ページ\)](#)
- [管理対象デバイスをネットワークに接続する \(8 ページ\)](#)
- [Firepower Management Center の設定 \(11 ページ\)](#)

---

**ステップ 1** Firepower Management Center で、**[Devices] > [Device Management]** をクリックします。

**ステップ 2** **[Add] > [Device]** をクリックします。  
次の図に示された情報を入力します。

**Add Device** ? x

Host:† 10.10.2.45

Display Name: 10.10.2.45

Registration Key:\* cisco123

Group: None

Access Control Policy:\* Create new policy

**Smart Licensing**

Malware:

Threat:

URL Filtering:

**Advanced**

Unique NAT ID:†

Transfer Packets:

On Firepower Threat Defense devices version 6.2.1 onwards, AnyConnect VPN licenses can be enabled from [smart license page](#)

Access control policy is required.

Register Cancel

**ステップ 3** [Access Control Policy] リストで、[Create New Policy] をクリックします。

**ステップ 4** 次の図に示すように、[New Policy] ダイアログボックスで名前を入力し、必要に応じてポリシーの説明を入力して、[Block all traffic] をクリックします（後でデフォルトのポリシー アクションを変更します）。

**New Policy** ? x

Name: Initial policy

Description:

Select Base Policy: None

Default Action:  Block all traffic  Intrusion Prevention  Network Discovery

Save Cancel

**ステップ 5** [Save] をクリックします。

**ステップ 6** [Add Device] ダイアログボックスで、[Smart Licensing] セクションのすべてのチェックボックスをオンにします。

**ステップ 7** [Transfer Packets] をオンにします。

**ステップ 8** [Register] をクリックして、デバイスの検出と登録が完了するまで待機します。デバイスが追加されると、次のページが表示されます。

**Device Management**  
List of all the devices currently registered on the Firepower Management Center.

View By:  | All (1) | Error (0) | Warning (0) | Offline (0) | Normal (1) | Deployment Pending (1) | Search Device | Add

Name	Model	Version	Licenses	Access Control Policy	Group
Ungrouped (1)					
10.10.2.45 10.10.2.45 - Routed	Cisco Firepower Threat Defense for VMWare	6.2.3	Base, Threat, Malware, URL Filtering	Initial policy	

### 次のタスク



[管理対象デバイスのインターフェイスの設定 \(19 ページ\)](#) を参照してください。

## 管理対象デバイスのインターフェイスの設定

このタスクは、管理対象デバイスの内部インターフェイスと外部インターフェイスに IP アドレスとサブネットマスクを設定する方法を示します。ネットワーク構成図の例 [ネットワークのセットアップについて \(3 ページ\)](#) を参照してください。

### 始める前に

[管理対象デバイスのインターフェイスの設定 \(19 ページ\)](#) を参照してください。

- ステップ 1** Firepower Management Center で、**[Devices] > [Device Management]** をクリックします。
- ステップ 2** 管理対象デバイスの横にある  (編集) をクリックします。  
[Interfaces] タブが表示されます。
- ステップ 3** [gigabitethernet0/0] の横にある  (編集) をクリックして、内部インターフェイスを設定します。
- ステップ 4** [Mode] リストで、[None] をクリックします。
- ステップ 5** [Enabled] をオンにします。
- ステップ 6** [Name] フィールドに **inside** と入力します。
- ステップ 7** [Security Zone] リストで [New] をクリックします。
- ステップ 8** [New Security Zone] ダイアログボックスで **insidezone** と入力し、[OK] をクリックします。
- ステップ 9** [IPv4] タブをクリックします。
- ステップ 10** [IP Type] リストで [Use static IP] をクリックします。
- ステップ 11** [IP Address] フィールドに **10.10.1.1/24** と入力します。  
次の図は例を示しています。

ステップ 12 [OK] をクリックします。

ステップ 13 以上のタスクを繰り返して、残りのインターフェイスを次のように設定します。

- a) [Name] : **outside**  
 [Interface] : **GigabitEthernet0/1**  
 [Security Zone] : **outsidezone**  
 [IPV4 Address] : **209.165.200.255/16**

(注) 管理しているデバイスのタイプに応じて、インターフェイスはこのガイドの例とは異なって識別される場合があります。たとえば、仮想管理対象デバイスには、**gigabitethernet0/0**、**GigabitEthernet0/1** などと番号付けされたインターフェイスがあります。Firepower Threat Defense 4100 または 9300 シリーズ デバイスには、**ethernet1/1**、**Ethernet2/1**、**Ethernet3/1** などと番号付けされたインターフェイスがあります。

ステップ 14 ページの上部にある [保存 (Save) ] をクリックします。  
 インターフェイスは、次のように表示されます。

10.10.2.45 Save Cancel

Cisco Firepower Threat Defense for VMWare

Device Routing **Interfaces** Inline Sets DHCP

Sync Device Add Interfaces

St...	Interface	Logical Name	Type	Security Zones	MAC Address (Active/Standby)	IP Address
	GigabitEthernet0/0	Inside	Physical	insidezone		10.10.1.1/24(Static)
	GigabitEthernet0/1	Outside	Physical	outsidezone		209.165.200.225/16(Static)
	GigabitEthernet0/2		Physical			
	GigabitEthernet0/3		Physical			

### 次のタスク

[スタティック ルートの追加 \(21 ページ\)](#) を参照してください。

## スタティック ルートの追加

スタティック ルートは、マッピングされたリソースにネットワーク トラフィックを直接移動させる 1 ホップのルートです。この場合は、外部ゲートウェイです。スタティックルートをこのような単純なネットワークでセットアップすることをお勧めします。

スタティックルーティングとダイナミックルーティングの詳細については、「[Supported Route Types \(サポートされるルートタイプ\)](#)」を参照してください。

**ステップ 1** Firepower Management Center で、**[デバイス (Devices)] > [デバイス管理 (Device Management)]** をクリックします。

**ステップ 2** 管理対象デバイスの横にある (編集) をクリックします。

**ステップ 3** **[ルーティング (Routing)]** タブをクリックします。

**ステップ 4** **[Static Route]** をクリックします。

**ステップ 5** **[ルートを追加 (Add Route)]** をクリックします。

**ステップ 6** **[Add Static Route Configuration]** ダイアログボックスで、次の情報を入力します。

#### インターフェイス

**outside** をクリックします。

#### 使用可能なネットワーク

**[Selected Networks]** に **any-ipv4** を追加します。

#### ゲートウェイ

(追加) をクリックして、**[Name]** でゲートウェイの名前を **outsidegateway** に指定し、**[Network]** の値を **209.165.200.254** に指定します。

次の図は例を示しています。

**Add Static Route Configuration**

Type:  IPv4  IPv6

Interface\*:

Available Network

- any-ipv4
- IPv4-Benchmark-Tests
- IPv4-Link-Local
- IPv4-Multicast
- IPv4-Private-10.0.0.0-8
- IPv4-Private-172.16.0.0-12
- IPv4-Private-192.168.0.0-1
- IPv4-Private-All-RFC1918
- IPv6-to-IPv4-Relay-Anycast

Selected Network

- any-ipv4

Gateway\*:

Metric:  (1 - 254)

Tunneled:  (Used only for default Route)

Route Tracking:

ステップ7 [OK] をクリックします。

ステップ8 ページの上部にある [保存 (Save) ] をクリックします。

### 次のタスク

[NAT ポリシーの追加 \(22 ページ\)](#) を参照してください。

## NAT ポリシーの追加

管理対象デバイスは、NAT を使用して内部のルーティング不可 IP アドレス (10.10.2.1 など) とインターネット間の通信を可能にしています。ルーティング可能なパブリック IP アドレスには限りがあるため、NAT を使用しない場合は使用できる IP アドレスが厳しく制限される可能性があります。このタスクでセットアップする NAT ポリシーは、パケットを内部インターフェイスから外部インターフェイスに転送します。

NAT の詳細については、「[Why Use NAT? \(NAT を使用する理由\)](#)」を参照してください。



ステップ 1 Firepower Management Center で、 **[Devices] > [NAT]** をクリックします。

ステップ 2 **[New Policy] > [Threat Defense NAT]** をクリックします。

ステップ 3 **[New Policy]** ダイアログボックスに、次の情報を入力します。

**[名前 (Name) ]**

**Inside-Outside-NAT** と入力します。

**説明**

任意で説明を入力します。

**[選択されたデバイス (Selected Devices) ]**

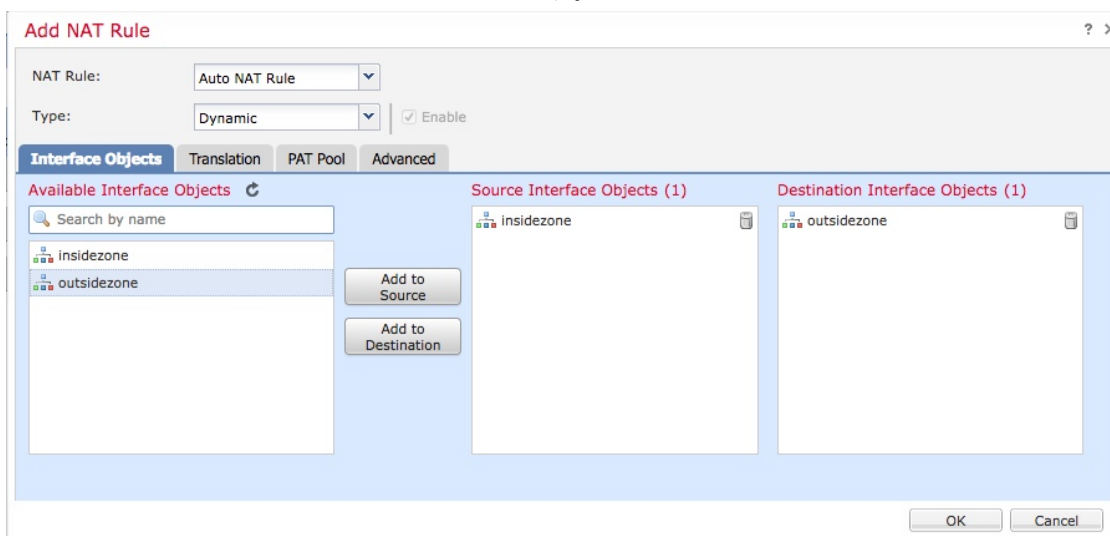
**[Selected Devices]** に 10.10.2.45 を追加します。

ステップ 4 **[保存 (Save) ]** をクリックします。

ステップ 5 ページが更新されたら、 **[Add Rule]** をクリックします。

ステップ 6 **[Interface Object]** タブをクリックします。

ステップ 7 以前に作成したセキュリティゾーンを、次のように送信元インターフェイスオブジェクトおよび宛先インターフェイス オブジェクトとして追加します。



ステップ 8 **[Translation]** タブをクリックします。

ステップ 9 **[Original Source]** の横にある **+** (追加) をクリックします。

ステップ 10 **[New Network Objects]** ダイアログボックスに、次の情報を入力します。

**[名前 (Name) ]**

**insidesubnet** と入力します。

**説明**

任意で説明を入力します。

**ネットワーク**

**10.10.2.0/24** と入力します。

ステップ 11 **[Translated Source]** リストで、 **[Destination Interface IP]** をクリックします。

次の図は、 **[Add a NAT Rule]** ダイアログボックスの例を示しています。

**Add NAT Rule**

NAT Rule: Auto NAT Rule

Type: Dynamic  Enable

Interface Objects **Translation** PAT Pool Advanced

**Original Packet**

Original Source:\* insidesubnet

Original Port: TCP

**Translated Packet**

Translated Source: Destination Interface IP  
The values selected for Destination Interface Objects in 'Interface Objects' tab will be used

Translated Port:

OK Cancel

**ステップ 12** [OK] をクリックします。

**ステップ 13** ページの上部にある [保存 (Save) ] をクリックします。

**ステップ 14** 変更を展開します。

- a) ページの上部にある [Deploy] をクリックします。
- b) オプションデバイスを展開して、変更する内容を表示します。
- c) デバイスの左にあるチェックボックスをオンにします。  
次の図は例を示しています。

**Deploy Policies** Version: 2018-05-02 01:36 PM

<input checked="" type="checkbox"/>	Device	Inspect Interruption	Type	Group	Current Ver
<input checked="" type="checkbox"/>	10.10.2.45	No	FTD		2018-05-01

- ⌂ Nat Policy: Inside-Outside-NAT
- ✔ Access Control Policy: Initial Policy
- ✔ Intrusion Policy: Balanced Security and Connectivity
- ✔ Intrusion Policy: No Rules Active
- ✔ DNS Policy: Default DNS Policy
- ✔ Prefilter Policy: Default Prefilter Policy
- ✔ Network Discovery
- ✔ Device Configuration (Details)
- ✔ Rule Update (2017-09-13-001-vrt)
- ✔ VDB (Build 290 - 2017-09-20 18:50:28)
- ✔ Snort Version 2.9.12 (Build 136 - daq7)

Selected devices: 1

Deploy

- [展開 (Deploy) ] をクリックします。
- 変更内容が展開されるのを待機します。展開には数分かかることがあります。展開の進行状況を示すメッセージが表示されます。

### 次のタスク

[システムのテスト \(27 ページ\)](#) を参照してください。





## 第 5 章

# システムのテスト

すべてのセットアップが適切であることを確認するために、アクセス コントロール ポリシーを作成してすべてのトラフィックを許可し、クライアントを内部ネットワークに接続し、クライアントがインターネットに接続できることを確認します。最後に、管理対象デバイス上のトラフィックを直接モニタし、Firepower Management Center 上のトラフィックもモニタします。

- [アクセス コントロール ポリシーの編集 \(27 ページ\)](#)
- [システムのテスト \(29 ページ\)](#)
- [システムのトラブルシューティング \(32 ページ\)](#)


## アクセス コントロール ポリシーの編集

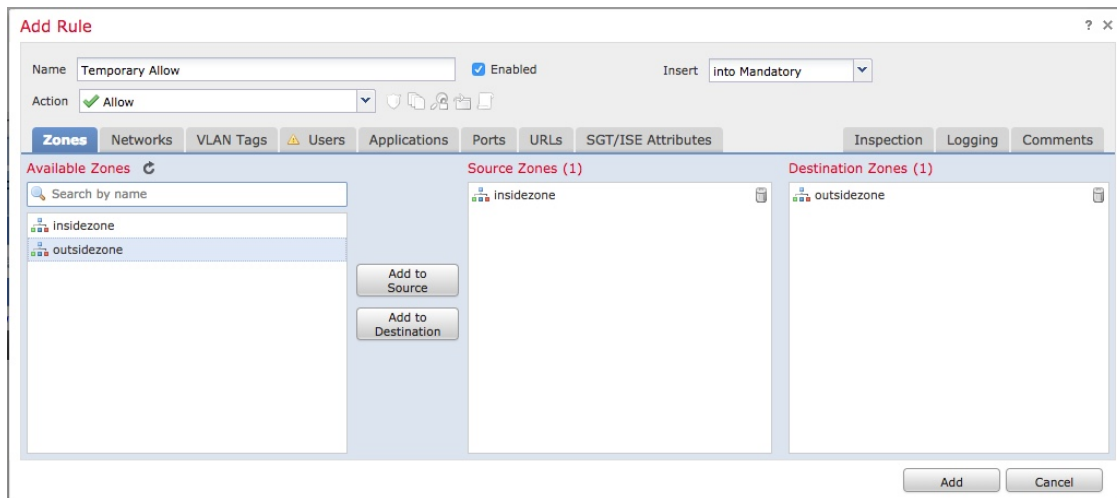
内部ネットワークから外部ネットワークへのすべてのトラフィックを許可するインスペクションなしの一時的なアクセス コントロール ポリシーを作成して、以下をテストします。


- 内部ネットワークに接続しているクライアントがインターネットに接続できる。
- Firepower Threat Defense デバイスを介してトラフィックがフィルタリングされている。(管理対象デバイスは、トラフィックがフィルタリングされていなくても、すべてのトラフィックを確認する必要があります)

### 始める前に

続行する前に、このガイドで説明した他のすべてのタスクを完了していることを確認してください。

- ステップ 1** Firepower Management Center で、**[Policies] > [Access Control] > [Access Control]** を選択します。
- ステップ 2** [Initial Policy] の横にある  (編集) をクリックします。
- ステップ 3** [ルール の追加 (Add Rule)] をクリックします。
- ステップ 4** [Add Rule] ダイアログボックスで、次の情報を入力します。



- ステップ 5** [ロギング (Logging) ] タブをクリックします。
- ステップ 6** [Log at End of Connection] をオンにします。
- ステップ 7** [追加 (Add) ] をクリックします。  
ポリシーのページが表示されます。
- ステップ 8** [Initial Policy] ページの [Default Action] リストで、[Intrusion Prevention: Balanced Security and Connectivity] をクリックします。
- ステップ 9** リストの横にある  (ロギング) をクリックします。
- ステップ 10** [接続の終了時にロギングする (Log at End of Connection) ] をオンにします。
- ステップ 11** [OK] をクリックします。
- ステップ 12** ページの上部にある [保存 (Save) ] をクリックします。
- ステップ 13** 変更を展開します。
- a) ページの上部にある [展開 (Deploy) ] をクリックします。
  - b) オプションデバイスを展開して、変更する内容を表示します。
  - c) デバイスの左にあるチェックボックスをオンにします。  
次の図は例を示しています。



- [展開 (Deploy)] をクリックします。
- 変更内容が展開されるのを待機します。展開には数分かかることがあります。展開の進行状況を示すメッセージが表示されます。

### 次のタスク

[システムのテスト \(29 ページ\)](#) を参照してください。

## システムのテスト


システムが正常に動作していることを確認するには、クライアントを内部ネットワークに接続してインターネットに到達できることを確認します。クライアントがインターネットに接続しているときに、Firepower Management Center の診断を使用して、トラフィックが通過していることを確認します。接続イベントを表示することもできます。

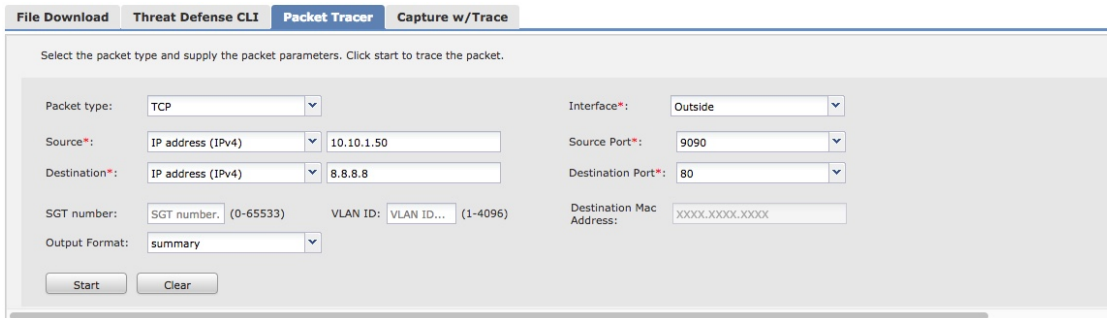
### 始める前に

[アクセスコントロールポリシーの編集 \(27 ページ\)](#) を参照してください。

**ステップ 1** 管理対象デバイスの内部ネットワークにクライアントを接続します。

クライアントは、Windows、Mac、UNIX、など、実行しているオペレーティングシステムを問いません。クライアントを接続する方法の詳細はネットワークのセットアップ方法に応じて異なり、このガイドの対象外です。管理対象デバイスがインストールされているネットワークラックに手が届く状態であれば、デバイスの GigabitEthernet 0/1 ポートにクライアントを直接接続できます。

- ステップ 2** クライアントに静的 IP アドレス 10.10.1.50、デフォルトゲートウェイ 10.10.1.1、およびアクセス可能な任意の DNS サーバをセットアップします。  
デフォルトゲートウェイは、内部インターフェイスの IP アドレスである必要があります。クライアントは、初めにこのゲートウェイに接続してから、トラフィックを内部または外部アドレスに送信します。
- ステップ 3** Firepower Management Center にログインします。
- ステップ 4** [デバイス (Devices)] > [デバイス管理 (Device Management)] をクリックします。
- ステップ 5** 管理対象デバイスの横にある  (トラブルシューティング) をクリックします。
- ステップ 6** [高度なトラブルシューティング (Advanced Troubleshooting)] をクリックします。
- ステップ 7** [パケットトレーサ (Packet Tracer)] タブをクリックします。
- ステップ 8** [Packet Tracer] タブ ページで、次の情報を入力します。



The screenshot shows the Packet Tracer configuration window. The 'Packet type' is set to TCP. The 'Source' is an IP address (IPv4) of 10.10.1.50. The 'Destination' is an IP address (IPv4) of 8.8.8.8. The 'Interface\*' is set to Outside. The 'Source Port\*' is 9090 and the 'Destination Port\*' is 80. The 'SGT number' is 0-65533 and the 'VLAN ID' is 1-4096. The 'Destination Mac Address' is XXXX.XXXX.XXXX. The 'Output Format' is set to summary. There are 'Start' and 'Clear' buttons at the bottom.

[Source] の IP アドレスと [Source Port] には、任意の値を指定できます。ここでテストするのは、トラフィックが内部インターフェイスから外部インターフェイスに転送されるかどうかです。この例では、[Destination] IP アドレスと [Destination Port] の値のみが使用されます。

- ステップ 9** クライアントで、ping を実行するかインターネットサイトを閲覧します。
- ステップ 10** [Packet Tracer] タブ ページで [Start] をクリックします。  
結果の解釈については [結果の解釈 \(33 ページ\)](#) を参照してください。
- ステップ 11** [Capture w/Trace] タブをクリックします。
- ステップ 12** [Enable Auto-Refresh] をオンにして、必要に応じて更新間隔を変更します。
- ステップ 13** [キャプチャの追加 (Add Capture)] をクリックします。
- ステップ 14** [Add Capture] ダイアログボックスで、次の情報を入力します。



**ステップ 15** [保存 (Save) ] をクリックします。

**ステップ 16** クライアントで、ping を実行するかインターネット サイトを参照します。

**ステップ 17** 下部のペインで  (更新) をクリックします。


Firepower Management Center の下部ペインに、パケットのキャプチャとトレースの結果が表示されます。次のようなメッセージを見つけます。このメッセージは、管理対象デバイスの内部インターフェイスからのトラフィックがアクセス コントロール ポリシーと一致していることを裏付けています。

```
Phase: 5
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: TCP, ACK, seq 2101701398, ack 3091508482
AppID: service HTTP (676), application Adobe Analytics (2846), out-of-order
Firewall: allow rule, 'Temporary Allow Policy', allow
Snort id 1, NAP id 1, IPS id 0, Verdict PASS
Snort Verdict: (pass-packet) allow this packet
```

結果の解釈についてのその他の情報は[結果の解釈 \(33 ページ\)](#) を参照してください。

パケット トレーサの詳細については、「[Packet Tracer Overview \(パケット トレーサの概要\)](#)」を参照してください。

**ステップ 18** [Analysis] > [Connections] > [Events] をクリックします。

**ステップ 19** 右上隅の  をクリックしてページの更新頻度を調整します。

**ステップ 20** [Preferences] タブをクリックします。

**ステップ 21** [Refresh Interval (minutes)] フィールドに 1 を入力します。

**ステップ 22** [適用 (Apply) ] をクリックします。

ステップ 23 ページから移動して、[Connection Events] ページに戻ります。

ステップ 24 ページが更新されるまで待機します。  
次のような接続イベントが表示されます。

Connection Events (switch, workflow)  
Connections with Application Details | Table View of Connection Events  
No Search Constraints (Edit Search) 2018-04-20 08:34:00 - 2018-04-20 09:46:23 Expanding

Jump to	First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code	Application Protocol	Client	Web Application	URL Category	URL Reputation	Device
\$	2018-04-20 08:40:18	2018-04-20 08:40:22	Allow		10.10.1.50	USA	13.78.233.133	USA	insidezone	outsidezone	49228 / tcp	443 / https						10.10.2.45
\$	2018-04-20 08:39:57	2018-04-20 08:40:06	Allow		10.10.1.50	USA	13.78.233.133	USA	insidezone	outsidezone	49227 / tcp	443 / https						10.10.2.45
\$	2018-04-20 08:39:36	2018-04-20 08:39:45	Allow		10.10.1.50	USA	13.78.233.133	USA	insidezone	outsidezone	49226 / tcp	443 / https						10.10.2.45
\$	2018-04-20 08:39:15	2018-04-20 08:39:24	Allow		10.10.1.50	USA	13.78.233.133	USA	insidezone	outsidezone	49225 / tcp	443 / https						10.10.2.45
\$	2018-04-20 08:38:54	2018-04-20 08:39:03	Allow		10.10.1.50	USA	13.78.233.133	USA	insidezone	outsidezone	49224 / tcp	443 / https						10.10.2.45
\$	2018-04-20 08:38:33	2018-04-20 08:38:42	Allow		10.10.1.50	USA	13.78.233.133	USA	insidezone	outsidezone	49223 / tcp	443 / https						10.10.2.45
\$	2018-04-20 08:38:12	2018-04-20 08:38:21	Allow		10.10.1.50	USA	8.8.8.8	USA	insidezone	outsidezone	51253 / udp	53 (domain) / udp		<input type="checkbox"/> DNS	<input type="checkbox"/> dns client			10.10.2.45
\$	2018-04-20 08:38:12	2018-04-20 08:38:21	Allow		10.10.1.50	USA	8.8.8.8	USA	insidezone	outsidezone	51253 / udp	53 (domain) / udp		<input type="checkbox"/> DNS	<input type="checkbox"/> dns client			10.10.2.45
\$	2018-04-20 08:38:12	2018-04-20 08:38:21	Allow		10.10.1.50	USA	52.165.21.12	USA	insidezone	outsidezone	49222 / tcp	443 / https						10.10.2.45

ステップ 25 ビューをカスタマイズするには、[Table View of Connection Events] をクリックします。

詳細については、「[Connection and Security Intelligence Event Fields \(接続およびセキュリティインテリジェンス イベントフィールド\)](#)」および「[Using Connection and Security Intelligence Event Tables \(接続およびセキュリティインテリジェンスのイベントテーブルの使用\)](#)」を参照してください。

ステップ 26 パケットキャプチャメッセージと接続イベントが表示されれば成功です。システムは正常にセットアップされています。

### 次のタスク

エラーが表示される場合、またはクライアントがインターネットに接続できない場合は、[システムのトラブルシューティング \(32 ページ\)](#) を参照してください。

## システムのトラブルシューティング

このトピックでは、システムで発生する可能性がある問題に対する解決策について説明します。多くは、ネットワーククライアントがインターネットにアクセスできない問題です。

### スタティックルートとデフォルトゲートウェイを確認する

次のように管理対象デバイスからインターネットサイトの ping を実行して、スタティックルートとデフォルトゲートウェイをチェックします。

1. SSHクライアントまたは仮想デバイスの管理コンソールを使用して、管理対象デバイスにログインします。
2. 管理対象デバイスで必要な場合は、次を入力します。 **connect ftd**
3. Enter **ping 8.8.8.8**

成功した場合、結果は次のように表示されます。

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echoes to 8.8.8.8, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/av/max = 60/62/70 ms
```

インターネット IP アドレスに対する ping が成功しない場合は、管理対象デバイスのインターフェイスが正しく接続されていることを確認してください。ケーブル両端のリンクとアクティビティの LED が点灯（アクティビティ LED は点滅）していることを確認してください。

#### 接続イベントが表示されない

接続イベントが表示されない最も可能性が高い理由は、アクセス コントロール ルールまたはアクセスコントロールポリシーでロギングを有効にしていないことです。[アクセスコントロールポリシーの編集 \(27 ページ\)](#) を参照してください。

## 結果の解釈

このトピックでは、パケット キャプチャおよび traceroute コマンドの結果を解釈する方法について説明します。

#### パケットトレーサの解釈

以下のパケットトレーサからの抜粋は、重要な情報および内部インターフェイスから外部インターフェイスへのトラフィック転送における判断が示されています。このガイドで説明した設定情報の一部が強調表示されています。次の点に注意してください。

- Phase 3 は、外部ゲートウェイを 209.165.200.254 に解決しています。
- Phase 4 は、一時的な許可ポリシー（Temporary Allow Policy）の初回の呼び出しを示しています。
- Phase 6 は、内部のクライアントから外部インターフェイスへ転送する NAT ポリシーを示しています。
- Phase 16 は、一時的な許可ポリシーに基づいてトラフィックを許可する、インスペクションエンジン（Snort）を示しています。

これらのいずれかのフェーズでのエラーは、ポリシーが誤って設定されているかどうか、またはトラフィックをブロックするように設定されているかどうかに応じて、トラフィックの拒否またはドロップの原因となり得ます。

```
Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 209.165.200.254 using egress ifc Outside
```

```
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group CSM_FW_ACL_global
access-list CSM_FW_ACL_advanced permit ip ifc Inside any ifc Outside any rule-id 268434433
```

```
access-list CSM_FW_ACL_remark rule-id 268434433: ACCESS POLICY: Initial Policy - Mandatory
access-list CSM_FW_ACL_remark rule-id 268434433: L7 RULE: Temporary Allow Policy
Additional Information:
  This packet will be sent to snort for additional processing where a verdict will be
  reached

Phase: 6
Type: NAT
Subtype:
Result: ALLOW
Config:
object network insidesubnet
  nat (Inside,Outside) dynamic interface
Additional Information:
Dynamic translate 10.10.1.50/52177 to 209.165.200.225/52177
Phase: 15
Type: EXTERNAL-INSPECT
Subtype:
Result: ALLOW
Config:
Additional Information:
Application: 'SNORT Inspect'

Phase: 16
Type: SNORT
Subtype:
Result: ALLOW
Config:
Additional Information:
Snort Trace:
Packet: UDP
Session: new snort session
AppID: service DNS (617), application unknown (0)
Firewall: allow rule, 'Temporary Allow Policy' , allow
Snort id 1, NAP id 1, IPS id 0, Verdict PASS
Snort Verdict: (pass-packet) allow this packet
```



---

(注) [Packet Tracker]と [Capture w/Trace] には異なるフェーズ番号が表示されますが、各フェーズで表示される情報はほぼ同一です。

---



- (注) 最終的な SNORT フェーズがない場合は、ROUTE-LOOKUP フェーズでエラーを探します。たとえば、次は外部インターフェイスに問題があることを示している場合があります。該当インターフェイスの IP アドレスと外部ゲートウェイの IP アドレスを確認してください。

```
Phase: 15
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 209.165.200.254 using egress ifc  outside
```

```
Result:
input-interface: inside
input-status: up
input-line-status: up
output-interface: outside
output-status: up
output-line-status: up
Action: drop
Drop-reason: (no-adjacency) No valid adjacency
```

#### 症状：ネットワークが変換されない

パケット キャプチャに次のような行が存在しない場合、多くの場合 NAT が正しくセットアップされていないことを意味します。

```
Dynamic translate 10.10.1.50/65413 to 209.165.200.225/65413
```

**解決策：** [NAT ポリシーの追加 \(22 ページ\)](#) の説明に従ってダイナミック NAT を設定します。

#### 症状：アクセス コントロール ポリシーがトラフィックをブロックする

アクセス コントロール ポリシーがトラフィックを許可するのではなくトラフィックをブロックするように設定されている場合、パケット キャプチャには次の行が含まれます。

```
Drop-reason: (acl-drop) Flow is denied by configured rule
```

これに該当するかどうかは、**[Analysis] > [Connections] > [Events]** で接続イベントを調べて確認できます。

**解決策：** [アクセス コントロール ポリシーの編集 \(27 ページ\)](#) の説明に従って、トラフィックを許可するようにアクセス コントロール ポリシーを設定します。

