



## Firepower Threat Defense Virtual の展開

この章では、Firepower Threat Defense 仮想を VMware vSphere 環境（vSphere vCenter またはスタンドアロンの ESXi ホストのどちらか）に展開する手順について説明します。

- [VMware の展開について](#)（1 ページ）
- [vSphere vCenter への Firepower Threat Defense Virtual の展開](#)（2 ページ）
- [vSphere ESXi ホストへの Firepower Threat Defense Virtual の展開](#)（6 ページ）
- [CLI を使用した Firepower Threat Defense Virtual のセットアップの実行](#)（11 ページ）

### VMware の展開について

Firepower Threat Defense 仮想（FTDv）は、スタンドアロンの ESXi サーバに展開でき、vCenter vSphere を使用している場合は、vSphere Client または vSphere Web Client を使用して展開できます。FTDv を正常に展開するには、vSphere のネットワーキング、ESXi ホストのセットアップと設定、仮想マシンのゲスト展開など、VMware と vSphere についての詳しい知識が必要です。

FTDv VMware 用の FTDv はオープン仮想化フォーマット（OVF）を使用して配布されます。OVF は、仮想マシンをパッケージ化して展開する標準的な方法です。VMware では、vSphere 仮想マシンをプロビジョニングするための方法がいくつか用意されています。お使いの環境に最適な方法は、インフラストラクチャの規模やタイプ、達成目標などの要因によって異なります。

VMware vSphere Web Client と vSphere Client は、vCenter Server、ESXi ホスト、および仮想マシンへのインターフェイスです。vSphere Web Client と vSphere Client を使用して、vCenter Server にリモート接続できます。vSphere Client では、任意の Windows システムから ESXi に直接接続することもできます。vSphere Web Client と vSphere Client は、vSphere 環境のすべての側面を管理するための主要なインターフェイスです。これらはコンソールによる仮想マシンへのアクセスも提供します。

vSphere Web Client では、すべての管理機能を使用できます。vSphere Client では、これらの機能の一部を使用できます。

# vSphere vCenter への Firepower Threat Defense Virtual の展開

この手順を使用して、Firepower Threat Defense 仮想 (FTDv) アプライアンスを VMware vSphere vCenter に展開します。vSphere Web Client (または vSphere Client) を使用して、FTDv 仮想マシンを展開し、設定できます。

## 始める前に

- FTDv を導入する前に、vSphere (管理用) で少なくとも 1 つのネットワークを設定しておく必要があります。

## 手順

- 
- ステップ 1** vSphere Web Client (または vSphere Client) にログインします。
- ステップ 2** vSphere Web Client (または vSphere Client) を使用し、[ファイル (File)] > [OVF テンプレートの展開 (Deploy OVF Template)] をクリックして、以前にダウンロードした OVF テンプレート ファイルを展開します。
- [OVF テンプレートの導入 (Deploy OVF Template)] ウィザードが表示されます。
- ステップ 3** ファイルシステムで OVF テンプレートソースの場所を参照し、[次へ (Next)] をクリックします。
- 次の Firepower Threat Defense Virtual VI OVF テンプレートを選択します。
- Cisco\_Firepower\_Threat\_Defense\_Virtual-VI-X.X.X-xxx.ovf*
- ここで、X.X.X-xxx は、ダウンロードしたアーカイブファイルのバージョンとビルド番号を表します。
- ステップ 4** [OVF テンプレートの詳細 (OVF Template Details)] ページを確認し、OVF テンプレートの情報 (製品名、バージョン、ベンダー、ダウンロードサイズ、ディスク上のサイズ、説明) を確認して、[次へ (Next)] をクリックします。
- ステップ 5** [エンドユーザライセンス契約書 (End User License Agreement)] ページが表示されます。OVF テンプレート (VI テンプレートのみ) でパッケージ化されたライセンス契約書を確認し、[承認 (Accept)] をクリックしてライセンスの条件に同意し、[次へ (Next)] をクリックします。
- ステップ 6** [名前と場所 (Name and Location)] ページで、この展開の名前を入力し、FTDv を展開するインベントリ内の場所 (ホストまたはクラスタ) を選択して、[次へ (Next)] をクリックします。名前はインベントリフォルダ内で一意である必要があります、最大 80 文字を使用できます。
- VSphere Web Client では、インベントリビューに管理対象オブジェクトの組織階層が表示されます。インベントリは、vCenter Server またはホストが管理対象オブジェクトを整理する目的で使用する階層構造です。この階層には、vCenter Server にあるすべての監視対象オブジェクトが含まれています。

- ステップ 7** Firepower Threat Defense Virtual を実行するリソースプールに移動して選択し、[次へ (Next)] をクリックします。
- (注) このページは、クラスタにリソースプールが含まれている場合にのみ表示されます。
- ステップ 8** [導入設定 (Deployment Configuration)] を選択します。[設定 (Configuration)] ドロップダウンリストから、サポートされている 3 つの vCPU/メモリ値のいずれかを選択し、[次へ (Next)] をクリックします。
- 重要** バージョン 6.4 以降では、FTDv は、調整可能な vCPU およびメモリリソースを使用して展開されます。6.4 より前のバージョンでは、FTDv は、固定構成の 4 vCPU/8 GB デバイスとして展開されていました。「[システム要件](#)」を参照してください。
- ステップ 9** 仮想マシンファイルを保存する [保存 (Storage)] 場所を選択し、[次へ (Next)] をクリックします。
- このページで、宛先クラスタまたはホストですでに設定されているデータストアから選択します。仮想マシン コンフィギュレーション ファイルおよび仮想ディスク ファイルが、このデータストアに保存されます。仮想マシンとそのすべての仮想ディスクファイルを保存できる十分なサイズのデータストアを選択してください。
- ステップ 10** 仮想マシンの仮想ディスクを保存するための「ディスク形式」を選択し、[次へ (Next)] をクリックします。
- [シックプロビジョン (Thick Provisioned)] を選択すると、すべてのストレージは、ただちに割り当てられます。[シンプロビジョン (Thin Provisioned)] を選択すると、データが仮想ディスクに書き込まれるときに、必要に応じてストレージが割り当てられます。また、シンプロビジョニングにより、仮想アプライアンスの展開に要する時間を短縮できます。
- ステップ 11** [ネットワークマッピング (Network Mapping)] ページで、OVF テンプレートで指定されたネットワークをインベントリ内のネットワークにマッピングし、[次へ (Next)] をクリックします。
- Management 0-0 インターフェイスが、インターネットから到達可能な VM ネットワークと関連付けられていることを確認します。非管理インターフェイスは、管理モードに応じて Firepower Management Center または Firepower Device Manager から設定できます。
- 重要** FTDv VMware では、仮想デバイスを作成するときに、デフォルトが vmxnet3 インターフェイスになりました。以前は、デフォルトは e1000 でした。e1000 インターフェイスを使用している場合は、切り替えることを強く推奨します。Vmxnet3 のデバイスドライバとネットワーク処理は ESXi ハイパーバイザと統合されているため、使用するリソースが少なくなり、ネットワークパフォーマンスが向上します。
- ネットワークはアルファベット順になっていない可能性があります。ネットワークを見つけることが非常に困難な場合は、後で [設定の編集 (Edit Settings)] ダイアログボックスからネットワークを変更できます。展開後、FTDv インスタンスを右クリックして [設定の編集 (Edit Settings)] を選択します。ただし、この画面には FTDv の ID は表示されません (ネットワークアダプタ ID のみ)。

以下に示す、FTDv インターフェイスのネットワークアダプタ、送信元ネットワーク、宛先ネットワークの対応を参照してください（これらは vmxnet3 デフォルトのインターフェイスです）。

表 1: 送信元から宛先ネットワークへのマッピング : *vmxnet3*

ネットワークアダプタ	送信元ネットワーク	宛先ネットワーク	機能
Network adapter 1	Management0-0	Management0/0	管理
Network adapter 2	Diagnostic 0-0	Diagnostic 0/0	診断
ネットワークアダプタ 3	GigabitEthernet0-0	GigabitEthernet 0/0	外部データ
ネットワークアダプタ 4	GigabitEthernet0-1	GigabitEthernet 0/1	内部日付
ネットワークアダプタ 5	GigabitEthernet0-2	GigabitEthernet 0/2	データトラフィック (オプション)
ネットワークアダプタ 6	GigabitEthernet 0-3	GigabitEthernet 0/3	データトラフィック (オプション)
ネットワークアダプタ 7	GigabitEthernet 0-4	GigabitEthernet 0/4	データトラフィック (オプション)
ネットワークアダプタ 8	GigabitEthernet 0-5	GigabitEthernet 0/5	データトラフィック (オプション)
ネットワークアダプタ 9	GigabitEthernet 0-6	GigabitEthernet 0/6	データトラフィック (オプション)
ネットワークアダプタ 10	GigabitEthernet 0-7	GigabitEthernet 0/7	データトラフィック (オプション)

FTDv を展開する際には、合計 10 個のインターフェイスを指定できます。データインターフェイスについて、送信元ネットワークが正しい宛先ネットワークにマッピングされ、各データインターフェイスが一意のサブネットまたは VLAN にマッピングされていることを確認します。すべての FTDv インターフェイスを使用する必要はありません。使用する予定がないインターフェイスについては、FTDv 設定内でそのインターフェイスを無効のままにしておいて構いません。

**ステップ 12** [プロパティ (Properties) ] ページで、OVF テンプレート (VI テンプレートのみ) でパッケージ化された、ユーザ設定可能なプロパティを設定します。

a) パスワード

FTDv 管理アクセス用のパスワードを設定します。

b) ネットワーク

完全修飾ドメイン名 (FQDN)、DNS、検索ドメイン、ネットワークプロトコル (IPv4 または IPv6) などのネットワーク情報を設定します。

c) 管理

管理モードを設定します。[ローカルマネージャを有効にする (Enable Local Manager)] のドロップダウン矢印をクリックし、Web ベースの Firepower Device Manager 統合設定ツールを使用する場合は [はい (Yes)] を選択します。Firepower Management Center を使用してこのデバイスを管理する場合は、[いいえ (No)] を選択します。管理オプションの選択方法の概要については、「[Firepower デバイスの管理方法](#)」を参照してください。

d) ファイアウォールモード

初期ファイアウォールモードを設定します。[ファイアウォールモード (Firewall Mode)] のドロップダウン矢印をクリックし、サポートされている 2 つのモードである [ルーテッド (Routed)] または [トランスペアレント (Transparent)] のどちらかを選択します。

[ローカルマネージャを有効にする (Enable Local Manager)] で [はい (Yes)] を選択した場合は、[ルーテッド (Routed)] ファイアウォールモードのみを選択できます。ローカルの Firepower Device Manager を使用してトランスペアレント ファイアウォールモードのインターフェイスを設定することはできません。

e) 登録

[ローカルマネージャを有効にする (Enable Local Manager)] で [いいえ (No)] を選択した場合は、管理を行う Firepower Management Center にこのデバイスを登録するのに必要なクレデンシャルを指定する必要があります。次の情報を入力します。

- [管理を行う Defense Center (Managing Defense Center)] : FMC のホスト名または IP アドレスを入力します。
- [登録キー (Registration Key)] : 登録キーは、ユーザが生成するキーで、1 回限り使用でき、37 文字以下にする必要があります。有効な文字には、英数字 (A~Z、a~z、0~9)、およびハイフン (-) があります。デバイスを FMC に追加するときに、この登録キーを思い出す必要があります。
- [NAT ID] : FTDv と FMC がネットワーク アドレス変換 (NAT) デバイスによって分離されていて、Firepower Management Center が NAT デバイスの背後にある場合は、一意の NAT ID を入力します。これは、ユーザが生成するキーで、1 回限り使用でき、37 文字以下にする必要があります。有効な文字には、英数字 (A~Z、a~z、0~9)、およびハイフン (-) があります。

f) [次へ (Next)] をクリックします。

**ステップ 13** [準備完了 (Ready To Complete)] セクションで、表示された情報を確認します。これらの設定を使用して展開を開始するには、[終了 (Finish)] をクリックします。変更を加えるには、[戻る (Back)] をクリックして前の各画面に戻ります。

オプションで、[展開後に電源をオン (Power on after deployment)] オプションにチェックマークを付けて、FTDv の電源をオンにし、[終了 (Finish)] をクリックします。

ウィザードが完了すると、vSphere Web Client によって仮想マシンが処理されます。[グローバル情報 (Global Information)] 領域の [最近使用したタスク (Recent Tasks)] ペインで [OVF 展開の初期設定 (Initialize OVF deployment)] ステータスを確認できます。

この手順が終了すると、[OVF テンプレートの展開 (Deploy OVF Template)] 完了ステータスが表示されます。

FTDv 仮想インスタンスがインベントリ内の指定されたデータセンターの下に表示されます。新しい VM の起動には、最大 30 分かかることがあります。

(注) Cisco Licensing Authority に FTDv を正常に登録するには、FTDv にインターネットアクセスが必要です。インターネットに接続してライセンス登録を完了させるには、導入後に追加の設定が必要になることがあります。

---

### 次のタスク

次の手順は、選択した管理モードによって異なります。

- [ローカルマネージャを有効にする (Enable Local Manager)] で [いいえ (No)] を選択した場合は、Firepower Management Center を使用して FTDv を管理します。「[Firepower Management Center を使用した Firepower Threat Defense Virtual の管理](#)」を参照してください。
- [ローカルマネージャを有効にする (Enable Local Manager)] で [はい (Yes)] を選択した場合は、統合されている Firepower Device Manager を使用して FTDv を管理します。「[Firepower Device Manager を使用した Firepower Threat Defense Virtual の管理](#)」を参照してください。

管理オプションの選択方法の概要については、「[Firepower デバイスの管理方法](#)」を参照してください。

## vSphere ESXi ホストへの Firepower Threat Defense Virtual の展開

この手順を使用して、Firepower Threat Defense 仮想 (FTDv) アプライアンスを単一の ESXi ホストに展開します。VMware Host Client (または vSphere Client) を使用して、単一の ESXi ホストを管理でき、FTDv 仮想マシンの展開や設定といった仮想化の基本的な操作などの管理タスクを実行できます。



- (注) VMware Host Client は vSphere Web Client とユーザインターフェイスが似ていますが、まったく異なるものであることに注意してください。vSphere Web Client は、vCenter Server に接続して複数の ESXi ホストを管理する場合に使用します。一方、VMware Host Client は単一の ESXi ホストを管理する場合に使用します。

vCenter 環境に Firepower Threat Defense 仮想 アプライアンスを展開する方法については、「[vSphere vCenter への Firepower Threat Defense Virtual の展開 \(2 ページ\)](#)」参照してください。

#### 始める前に

- FTDv を展開する前に、vSphere (管理用) で少なくとも 1 つのネットワークを設定しておく必要があります。

#### 手順

- ステップ 1** Cisco.com から VMware ESXi 用の Firepower Threat Defense 仮想 インストールパッケージをダウンロードして、ローカル管理コンピュータに保存します。

<https://www.cisco.com/go/ftd-software>

Cisco.com のログインおよびシスコサービス契約が必要です。

- ステップ 2** tar ファイルを作業ディレクトリに解凍します。ディレクトリからファイルを削除しないでください。次のファイルが含まれています。

- Cisco\_Firepower\_Threat\_Defense\_Virtual-VI-X.X.X-xx.ovf : vCenter 展開用
- Cisco\_Firepower\_Threat\_Defense\_Virtual-ESXi-X.X.X-xx.ovf : ESXi 展開用
- Cisco\_Firepower\_Threat\_Defense\_Virtual-X.X.X-xx.vmdk : VMware 仮想ディスク ファイル
- Cisco\_Firepower\_Threat\_Defense\_Virtual-VI-X.X.X-xx.mf : vCenter 展開用マニフェストファイル
- Cisco\_Firepower\_Threat\_Defense\_Virtual-ESXi-X.X.X-xx.mf : ESXi 展開用マニフェストファイル

ここで、X.X.X-xx は、ダウンロードしたアーカイブファイルのバージョンとビルド番号を表します。

- ステップ 3** ブラウザで、`http://` (ホスト名) `/ui` または `http://` (ホスト IP アドレス) `/ui` という形式を使用して、ESXi ターゲットのホスト名または IP アドレスを入力します。

ログイン画面が表示されます。

- ステップ 4** 管理者のユーザ名とパスワードを入力します。

- ステップ 5** [ログイン (Login) ] をクリックして続行します。  
これで、ターゲットの ESXi ホストにログインしました。
- ステップ 6** VMware Host Client のインベントリで、[ホスト (Host) ] を右クリックし、[VMの作成/登録 (Create/Register VM) ] を選択します。  
[新規仮想マシンウィザード (New Virtual Machine Wizard) ] が開きます。
- ステップ 7** [作成タイプの選択 (Select creation type) ] ページで、[OVFまたはOVAファイルから仮想マシンを導入 (Deploy a virtual machine from an OVF or OVA file) ] を選択し、[次へ (Next) ] をクリックします。
- ステップ 8** ウィザードの [OVFおよびVMDKファイルの選択 (Select OVF and VMDK files) ] ページで次の操作を行います。
- FTDv 仮想マシンの名前を入力します。  
仮想マシン名には 80 文字まで含めることができます。マシン名は各 ESXi インスタンスの中で一意にする必要があります。
  - 青いペインをクリックし、FTDv tar ファイルを解凍したディレクトリを参照して、ESXi OVF テンプレートと付随する VMDK ファイルを選択します。  
`Cisco_Firepower_Threat_Defense_Virtual-ESXi-X.X.X-xx.ovf`  
`Cisco_Firepower_Threat_Defense_Virtual-X.X.X-xx.vmdk`  
ここで、X.X.X-xx は、ダウンロードしたアーカイブファイルのバージョンとビルド番号を表します。  
**注目** 必ず ESXi OVF を選択してください。
- ステップ 9** [次へ (Next) ] をクリックします。  
使用しているローカルシステムストレージが開きます。
- ステップ 10** ウィザードの [ストレージの選択 (Select storage) ] ページで、アクセス可能なデータストアのリストからデータストアを選択します。  
仮想マシンの設定ファイルとすべての仮想ディスクが、このデータストアに保存されます。データストアはそれぞれ、サイズ、速度、可用性などのプロパティが異なる場合があります。
- ステップ 11** [次へ (Next) ] をクリックします。
- ステップ 12** FTDv の ESXi OVF と一緒にパッケージ化されている [展開オプション (Deployment options) ] を設定します。
- [ネットワークマッピング (Network Mapping) ] : OVF テンプレートで指定されたネットワークをインベントリ内のネットワークにマッピングし、[次へ (Next) ] をクリックします。  
Management 0-0 インターフェイスが、インターネットから到達可能な VM ネットワークと関連付けられていることを確認します。非管理インターフェイスは、管理モードに応じて Firepower Management Center または Firepower Device Manager から設定できます。



**重要** FTDv VMware では、仮想デバイスを作成するときに、デフォルトが vmxnet3 インターフェイスになりました。以前は、デフォルトは e1000 でした。e1000 インターフェイスを使用している場合は、切り替えることを強く推奨します。Vmxnet3 のデバイスドライバとネットワーク処理は ESXi ハイパーバイザと統合されているため、使用するリソースが少なくなり、ネットワークパフォーマンスが向上します。

ネットワークはアルファベット順になっていない可能性があります。ネットワークを見つけることが非常に困難な場合は、後で [設定の編集 (Edit Settings)] ダイアログボックスからネットワークを変更できます。展開後、FTDv インスタンスを右クリックして [設定の編集 (Edit Settings)] を選択します。ただし、この画面には FTDv の ID は表示されません (ネットワークアダプタ ID のみ)。

以下に示す、FTDv インターフェイスのネットワークアダプタ、送信元ネットワーク、宛先ネットワークの対応を参照してください (これらは vmxnet3 デフォルトのインターフェイスです)。

表 2: 送信元から宛先ネットワークへのマッピング : *vmxnet3*

ネットワークアダプタ	送信元ネットワーク	宛先ネットワーク	機能
Network adapter 1	Management0-0	Management0/0	管理
Network adapter 2	Diagnostic 0-0	Diagnostic 0/0	診断
ネットワークアダプタ 3	GigabitEthernet0-0	GigabitEthernet 0/0	外部データ
ネットワークアダプタ 4	GigabitEthernet0-1	GigabitEthernet 0/1	内部日付
ネットワークアダプタ 5	GigabitEthernet0-2	GigabitEthernet 0/2	データトラフィック (オプション)
ネットワークアダプタ 6	GigabitEthernet 0-3	GigabitEthernet 0/3	データトラフィック (オプション)
ネットワークアダプタ 7	GigabitEthernet 0-4	GigabitEthernet 0/4	データトラフィック (オプション)
ネットワークアダプタ 8	GigabitEthernet 0-5	GigabitEthernet 0/5	データトラフィック (オプション)
ネットワークアダプタ 9	GigabitEthernet 0-6	GigabitEthernet 0/6	データトラフィック (オプション)
ネットワークアダプタ 10	GigabitEthernet 0-7	GigabitEthernet 0/7	データトラフィック (オプション)

FTDv を展開する際には、合計 10 個のインターフェイスを指定できます。データインターフェイスについて、送信元ネットワークが正しい宛先ネットワークにマッピングされ、各データインターフェイスが一意的なサブネットまたは VLAN にマッピングされていることを確認します。すべての FTDv インターフェイスを使用する必要はありません。使用する予定がないインターフェイスについては、FTDv 設定内でそのインターフェイスを無効のままにしておいて構いません。

- b) [ディスクプロビジョニング (Disk provisioning)] : 仮想マシンの仮想ディスクを保存するためのディスク形式を選択します。

[シック (Thick)] プロビジョニングを選択すると、すべてのストレージがただちに割り当てられます。[シン (Thin)] プロビジョニングを選択すると、データが仮想ディスクに書き込まれるときに、必要に応じてストレージが割り当てられます。また、シンプロビジョニングにより、仮想アプライアンスの展開に要する時間を短縮できます。

**ステップ 13** 新規仮想マシンウィザードの [準備完了 (Ready To Complete)] ページで、仮想マシンの設定を確認します。

- a) (任意) ウィザードの設定を確認または変更するには、[戻る (back)] をクリックして戻ります。
- b) (任意) 作成タスクを破棄してウィザードを閉じるには、[キャンセル (Cancel)] をクリックします。
- c) [終了 (Finish)] をクリックして作成タスクを完了し、ウィザードを終了します。

ウィザードが完了すると、ESXi ホストによって VM が処理されます。展開のステータスは [最近使用したタスク (Recent Tasks)] で確認できます。展開が成功すると、[結果 (Results)] 列に [正常に完了 (Completed successfully)] が表示されます。

新しい FTDv 仮想マシンインスタンスが、ESXi ホストの仮想マシンインベントリの下に表示されます。新しい仮想マシンの起動には、最大 30 分かかることがあります。

(注) Cisco Licensing Authority に FTDv を正常に登録するには、FTDv にインターネットアクセスが必要です。インターネットに接続してライセンス登録を完了させるには、導入後に追加の設定が必要になることがあります。

### 次のタスク

- CLI を使用して仮想デバイスのセットアップを完了します。これは、ESXi OVF テンプレートを使用して FTDv を展開する場合の次の手順になります。「[CLI を使用した Firepower Threat Defense Virtual のセットアップの実行 \(11 ページ\)](#)」を参照してください。

# CLI を使用した Firepower Threat Defense Virtual のセットアップの実行

ESXi OVF テンプレートをを使用して展開した場合は、CLI を使用して FTDv をセットアップする必要があります。Firepower Threat Defense 仮想 アプライアンスには Web インターフェイスがありません。また、VIOVF テンプレートをを使用して展開し、かつ展開時にセットアップウィザードを使用しなかった場合は、CLI を使用して、Firepower システムに必要な設定を行うことができます。



- (注) VIOVF テンプレートをを使用して展開し、かつセットアップウィザードを使用した場合は、仮想デバイスが設定済みであり、それ以上のデバイス設定は必要ありません。以降の手順は、選択する管理モードによって異なります。

新しく設定されたデバイスに初めてログインするときに、EULA を読んで同意する必要があります。次に、セットアッププロンプトに従って管理パスワードを変更し、デバイスのネットワーク設定およびファイアウォールモードを設定します。

セットアッププロンプトに従う際に、複数の選択肢がある質問では、選択肢が (y/n) のように括弧で囲まれて示されます。デフォルト値は、[y] のように大カッコ内に列挙されます。選択を確定するには、Enter キーを押します。

## 手順

- ステップ 1 VMware コンソールを開きます。
- ステップ 2 [firepower ログイン (firepower login) ] プロンプトで、ユーザ名 **admin** とパスワード **Admin123** のデフォルトのクレデンシャルでログインします。
- ステップ 3 Firepower Threat Defense システムが起動すると、セットアップウィザードでシステムの設定に必要な次の情報の入力を求められます。
  - 使用許諾契約の同意
  - 新しい管理者パスワード
  - IPv4 または IPv6 の構成
  - IPv4 または IPv6 の DHCP 設定
  - 管理ポートの IPv4 アドレスとサブネットマスク、または IPv6 アドレスとプレフィックス
  - システム名
  - デフォルトゲートウェイ
  - DNS セットアップ

- HTTP プロキシ
- 管理モード（ローカル管理が Firepower Device Manager を使用）

**ステップ 4** セットアップウィザードの設定を確認します。デフォルト値または以前に入力した値がカッコ内に表示されます。以前に入力した値をそのまま使用する場合は、Enter を押します。

設定が実装されたときに、VMware コンソールにメッセージが表示される場合があります。

**ステップ 5** プロンプトに従ってシステム設定を行います。

**ステップ 6** コンソールが firepower# プロンプトに戻るときに、設定が正常に行われたことを確認します。

- (注) Cisco Licensing Authority に FTDv を正常に登録するには、FTDv にインターネットアクセスが必要です。インターネットに接続してライセンス登録を完了させるには、導入後に追加の設定が必要になることがあります。

---

## 次のタスク

次の手順は、選択した管理モードによって異なります。

- [ローカルマネージャを有効にする (Enable Local Manager) ] で [いいえ (No) ] を選択した場合は、Firepower Management Center を使用して FTDv を管理します。「[Firepower Management Center を使用した Firepower Threat Defense Virtual の管理](#)」を参照してください。
- [ローカルマネージャを有効にする (Enable Local Manager) ] で [はい (Yes) ] を選択した場合は、統合されている Firepower Device Manager を使用して FTDv を管理します。「[Firepower Device Manager を使用した Firepower Threat Defense Virtual の管理](#)」を参照してください。

管理オプションの選択方法の概要については、「[Firepower デバイスの管理方法](#)」を参照してください。