Firepower Threat Defense Virtual の展開

この章では、Firepower Threat Defense 仮想 を KVM 環境に展開する手順について説明します。

- KVM を使用した導入の前提条件 （1 ページ）
- 第 0 日のコンフィギュレーション ファイルの準備 （2 ページ）
- Firepower Threat Defense Virtual の起動 （4 ページ）

KVM を使用した導入の前提条件

- Cisco.com から Firepower Threat Defense Virtual の qcow2 ファイルをダウンロードし、Linux ホストに格納します。

  https://software.cisco.com/download/navigator.html

  （注） Cisco.com のログインおよびシスコ サービス契約が必要です。

- このマニュアルの導入例では、ユーザが Ubuntu 18.04 LTS を使用していることを前提としています。Ubuntu 18.04 LTS ホストの最上部に次のパッケージをインストールします。
  - qemu-kvm
  - libvirt bin
  - bridge-utils
  - Virt-Manager
  - virtinst
  - virsh tools
  - genisoimage

- パフォーマンスはホストとその設定の影響を受けます。ホストを調整することで、KVM での Firepower Threat Defense Virtual のスループットを最大化できます。一般的なホスト調

整の概念については、『Network Function Virtualization: Quality of Service in Broadband Remote Access Servers with Linux and Intel Architecture』を参照してください。

- 以下の機能は Ubuntu 18.04 LTS の最適化に役立ちます。
  - macvtap：高性能の Linux ブリッジ。Linux ブリッジの代わりに macvtap を使用できます。ただし、Linux ブリッジの代わりに macvtap を使用する場合は、特定の設定を行う必要があります。
  - Transparent Huge Pages：メモリ ページ サイズを増加させます。Ubuntu 18.04 では、デフォルトでオンになっています。
  - Hyperthread disabled：2 つの vCPUを 1 つのシングル コアに削減します。
  - txqueuelength：デフォルトの txqueuelength を 4000 パケットに増加させ、ドロップ レートを低減します。
  - pinning：qemu および vhost プロセスを特定のCPU コア にピン接続します。特定の条件下では、ピン接続によってパフォーマンスが大幅に向上します。
- RHEL ベースのディストリビューションの最適化については、『Red Hat Enterprise Linux6 Virtualization Tuning and Optimization Guide』を参照してください。
- KVM と Firepower System の互換性については、「Cisco Firepower Threat Defense Virtual Compatibility」を参照してください。

第 0 日のコンフィギュレーション ファイルの準備

FTDv を起動する前に、第 0 日用のコンフィギュレーション ファイルを準備できます。このファイルは、仮想マシンの導入時に適用される初期設定データを含むテキストファイルです。この初期設定は、「day0-config」というテキストファイルとして指定の作業ディレクトリに格納され、さらに day0.iso ファイルへと処理されます。この day0.iso ファイルが最初の起動時にマウントされて読み取られます。

重要 day0.iso ファイルは、最初のブート時に使用できる必要があります。

第 0 日のコンフィギュレーション ファイルを使用して展開する場合、プロセスで、FTDv アプライアンスの初期設定全体を実行できます。次を指定することができます。

- エンド ユーザ ライセンス契約書（EULA）の承認。
- システムのホスト名。
- 管理者アカウントの新しい管理者パスワード。
- 管理モード。Firepower デバイスの管理方法を参照してください。

[ローカルに管理（ManageLocally）] を [はい（Yes）] に設定するか、または Firepower Management Center フィールド（[FmcIp]、[FmcRegKey]、および [FmcNatId]）に情報を入力することができます。使用していない管理モードでは、フィールドを空のままにします。

- 最初のファイアウォール モード。最初のファイアウォール モード（**ルーテッド**または**トランスペアレント**）を設定します。

  ローカルの Firepower Device Manager（FDM）を使用して展開を管理する予定の場合は、ファイアウォール モードに**ルーテッド**のみ入力できます。FDM 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は設定できません。

- アプライアンスが管理ネットワークで通信することを許可するネットワーク設定。

第 0 日のコンフィギュレーション ファイルを使用せずに展開する場合は、起動後に Firepower システムの必須設定を指定する必要があります。詳細については、「第 0 日のコンフィギュレーション ファイルを使用しない起動 （9 ページ）」を参照してください。

（注） この例では Linux が使用されていますが、Windows の場合にも同様のユーティリティがあります。

手順の概要

1. 「day0-config」というテキストファイルに Firepower Threat Defense Virtual の CLI 設定を記入します。ネットワーク設定と Firepower Management Center の管理に関する情報を追加します。
2. テキスト ファイルを ISO ファイルに変換して仮想CD-ROM を生成します。
3. 手順を繰り返して、導入する FTDv ごとに一意のデフォルト設定ファイルを作成します。

手順の詳細

ステップ 1 「day0-config」というテキストファイルに Firepower Threat Defense Virtual の CLI 設定を記入します。ネットワーク設定と Firepower Management Center の管理に関する情報を追加します。

例：

```
#Firepower Threat Defense
{
    "EULA": "accept",
    "Hostname": "ftdv-production",
    "AdminPassword": "Admin123",
    "FirewallMode": "routed",
    "DNS1": "1.1.1.1",
    "DNS2": "1.1.1.2",
    "DNS3": "",
    "IPv4Mode": "manual",
    "IPv4Addr": "10.12.129.44",
    "IPv4Mask": "255.255.0.0",
    "IPv4Gw": "10.12.0.1",
    "IPv6Mode": "disabled",
```

```
    "IPv6Addr": "",
    "IPv6Mask": "",
    "IPv6Gw": "",
    "FmcIp": "",
    "FmcRegKey": "",
    "FmcNatId": "",
    "ManageLocally":"Yes"

}
```

ローカルの Firepower Device Manager（FDM）を使用するには、第 0 日のコンフィギュレーション ファイル内で [ローカルに管理（ManageLocally）] に対して [はい（Yes）] と入力します。または、Firepower Management Center のフィールド（[FmcIp]、[FmcRegKey]、および [FmcNatId]）に入力します。使用していない管理オプションの場合は、これらのフィールドを空白のままにします。

ステップ 2 テキスト ファイルを ISO ファイルに変換して仮想CD-ROM を生成します。

例：

```
/usr/bin/genisoimage -r -o day0.iso day0-config
```

または

例：

```
/usr/bin/mkisofs -r -o day0.iso day0-config
```

ステップ 3 手順を繰り返して、導入する FTDv ごとに一意のデフォルト設定ファイルを作成します。

次のタスク

- virt-install を使用している場合は、virt-install コマンドに次の行を追加します。

  ```
  --disk path=/home/user/day0.iso,format=iso,device=cdrom \
  ```

- virt-manager を使用している場合、virt-manager の GUI を使用して仮想 CD-ROM を作成できます。「Virtual Machine Manager を使用した起動 （7 ページ）」を参照してください。

Firepower Threat Defense Virtual の起動

導入スクリプトを使用した起動

virt-install ベースの導入スクリプトを使用して FTDv を起動できます。

環境に最適なゲスト キャッシング モードを選択してパフォーマンスを最適化できることに注意してください。使用中のキャッシュ モードは、データ損失が発生するかどうかに影響を与え、キャッシュ モードはディスクのパフォーマンスにも影響します。

各 KVM ゲスト ディスク インターフェイスで、指定されたいずれかのキャッシュモード（*writethrough*、*writeback*、*none*、*directsync*、または *unsafe*）を指定できます。*writethrough* モードは読み取りキャッシュを提供します。*writeback* は読み取り/書き込みキャッシュを提供しま

す。*directsync* はホストページキャッシュをバイパスします。*unsafe* はすべてのコンテンツをキャッシュし、ゲストからのフラッシュ要求を無視する可能性があります。

- *cache=writethrough* は、ホストで突然の停電が発生した場合の KVM ゲスト マシン上のファイル破損を低減できます。*writethrough* モードの使用をお勧めします。
- ただし、*cache=writethrough* は、*cache=none* よりディスク I/O 書き込みが多いため、ディスク パフォーマンスに影響する可能性もあります。
- *--disk* オプションの cache パラメータを削除する場合、デフォルトは *writethrough* になります。
- キャッシュ オプションを指定しないと、VM を作成するために必要な時間も大幅に短縮される場合もあります。これは、古いRAID コントローラにはディスク キャッシング能力が低いものがあることが原因です。そのため、ディスク キャッシングを無効にして（*ache=none*）、*writethrough* をデフォルトに設定すると、データの整合性を確保できます。
- 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。バージョン 6.4 より前のバージョンでは、FTDv は、固定構成 4vCPU/8GB デバイスとして展開されていました。各 FTDv プラットフォームサイズの --vcpus および --ram パラメータでサポートされている値については、次の表を参照してください。

表 *1 : virt-install* でサポートされる *vCPU* およびメモリ パラメータ

--vcpus	**--ram**	**FTDv プラットフォームのサイズ**
4	8192	4vCPU/8GB（デフォルト）
8	16384	8vCPU/16GB
12	24576	12vCPU/24GB

ステップ 1 「virt_install_ftdv.sh」という virt-install スクリプトを作成します。

FTDv VM の名前は、この KVM ホスト上の他の仮想マシン（VM）全体において一意であることが必要です。FTDv は最大 10 個のネットワーク インターフェイスをサポートできます。この例では、4 つのインターフェイスを使用しています。仮想 NIC は Virtio でなければなりません。

（注） FTDv のデフォルト設定では、管理インターフェイス、診断インターフェイス、および内部インターフェイスは**同じサブネット**上に配置すると仮定します。システムでは、少なくとも 4 つのインターフェイスが正常に起動する必要があります。仮想 NIC は Virtio でなければなりません。ネットワークへのインターフェイスの割り当ては、次の順番であることが必要です。

- 1. 管理インターフェイス（必須）
- 2. 診断インターフェイス（必須）
- 3. 外部インターフェイス（必須）
- 4. 内部インターフェイス（必須）

- 5. （オプション）データインターフェイス：最大6

例：

```
virt-install \
   --connect=qemu:///system \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --network network=default,model=virtio \
   --name=ftdv \
   --arch=x86_64 \
   --cpu host \
   --vcpus=8 \
   --ram=16384 \
   --os-type=linux \
   --os-variant=generic26 \
   --virt-type=kvm \
   --import \
   --watchdog i6300esb,action=reset
   --disk path=<ftd_filename>.qcow2,format=qcow2,device=disk,bus=virtio,cache=none \
   --disk path==<day0_filename>.iso,format=iso,device=cdrom \
   --console pty,target_type=serial \
   --serial tcp,host=127.0.0.1:<port>,mode=bind,protocol=telnet
   --force
```

ステップ 2 virt_install スクリプトを実行します。

例：

```
/usr/bin/virt_install_ftdv.sh

Starting install...
Creating domain...
```

ウィンドウが開き、VMのコンソールが表示されます。VMが起動中であることを確認できます。VMが起動するまでに数分かかります。VM が起動したら、コンソール画面から CLI コマンドを実行できます。

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。

- [ローカルに管理（ManageLocally）] 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。
- [ローカルに管理（ManageLocally）] で [はい（Yes）] を選択した場合は、統合された 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。

Virtual Machine Manager を使用した起動

virt-manager（Virtual Machine Manager とも呼ばれる）を使用して FTDv を起動します。virt-manager は、ゲスト仮想マシンを作成および管理するためのグラフィカル ツールです。

ステップ 1 virt-manager を起動します（**[アプリケーション（Applications）] > [システムツール（System Tools）] > [仮想マシンマネージャ（Virtual Machine Manager）]**）。

ハイパーバイザの選択、およびルート パスワードの入力を求められる可能性があります。

ステップ 2 左上隅のボタンをクリックし、[VMの新規作成（New VM）] ウィザードを開きます。

ステップ 3 仮想マシンの詳細を入力します。

a) オペレーティング システムの場合、[既存のディスクイメージをインポート（Import existing disk image）] を選択します。

この方法でディスク イメージ（事前にインストールされた、ブート可能なオペレーティング システムを含んでいるもの）をインポートできます。

b) [次へ（Forward）] をクリックして続行します。

ステップ 4 ディスク イメージをロードします。

a) [参照...（Browse...）] をクリックしてイメージ ファイルを選択します。
b) [OSタイプ（OS type）] には [汎用（Generic）] を選択します。
c) [次へ（Forward）] をクリックして続行します。

ステップ 5 メモリおよび CPU オプションを設定します。

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。バージョン 6.4 より前のバージョンでは、FTDv は、固定構成 4vCPU/8GB デバイスとして展開されていました。各 FTDv プラットフォームサイズの --vcpus および --ram パラメータでサポートされている値については、次の表を参照してください。

表 *2:* 仮想マシンマネージャでサポートされる *vCPU* およびメモリパラメータ

CPU	メモリ	FTDv プラットフォームのサイズ
4	8192	4vCPU/8GB（デフォルト）
8	16384	8vCPU/16GB
12	24576	12vCPU/24GB

a) FTDv プラットフォームサイズに対応する**メモリ（RAM）**パラメータを設定します。
b) FTDv プラットフォーム サイズに対応する **CPU** パラメータを設定します。
c) [次へ（Forward）] をクリックして続行します。

ステップ 6 [インストール前に設定をカスタマイズする（Customize configuration before install）] チェックボックスをオンにして、[名前（Name）] を指定してから [完了（Finish）] をクリックします。

この操作を行うと、別のウィザードが開き、仮想マシンのハードウェア設定を追加、削除、設定することができます。

ステップ 7 CPU 構成を次のように変更します。

左側のパネルから [プロセッサ（Processor）] を選択し、**[設定（Configuration）] > [ホストCPU構成のコピー（Copy host CPU configuration）]** を選択します。

これによって、物理ホストの CPU モデルと設定が仮想マシンに適用されます。

ステップ 8 仮想ディスクを設定します。

a) 左側のパネルから [ディスク1（Disk 1）] を選択します。
b) [詳細オプション（Advanced Options）] をクリックします。
c) [ディスクバス（Disk bus）] を [Virtio] に設定します。
d) [ストレージ形式（Storage format）] を [qcow2] に設定します。

ステップ 9 シリアル コンソールを設定します。

a) 左側のパネルから [コンソール（Console）] を選択します。
b) [削除（Remove）] を選択してデフォルト コンソールを削除します。
c) [ハードウェアを追加（Add Hardware）] をクリックしてシリアル デバイスを追加します。
d) [デバイスタイプ（Device Type）] で、[TCP net console (tcp)] を選択します。
e) [モード（Mode）] で、[サーバモード（バインド）（Server mode (bind)）] を選択します。
f) [ホスト（Host）] には「**0.0.0.0**」と入力し、IP アドレスと一意の**ポート**番号を入力します。
g) [Telnetを使用（Use Telnet）] ボックスをオンにします。
h) デバイス パラメータを設定します。

ステップ 10 KVMゲストがハングまたはクラッシュしたときに何らかのアクションが自動でトリガーされるようウォッチドッグ デバイスを設定します。

a) [ハードウェアを追加（Add Hardware）] をクリックしてウォッチドック デバイスを追加します。
b) [モデル（Model）] で、[デフォルト（default）] を選択します。
c) [アクション（Action）] で、[ゲストを強制的にリセット（Forcefully reset the guest）] を選択します。

ステップ 11 少なくとも 4 つの仮想ネットワーク インターフェイスを設定します。

[ハードウェアの追加（Add Hardware）] をクリックしてインターフェイスを追加し、**macvtap** を選択するか、共有デバイス名を指定します（ブリッジ名を使用）。

（注） KVM 上の FTDv では、合計で 10 個のインターフェイスをサポートします（管理インターフェイス X 1 個、診断インターフェイス X 1 個、データ トラフィック用ネットワーク インターフェイス X 最大 8 個）。ネットワークへのインターフェイスの割り当ては、次の順番であることが必要です。

vnic0：管理インターフェイス（必須）

vnic1：診断インターフェイス（必須）

vnic2：外部インターフェイス（必須）

vnic3：内部インターフェイス（必須）

vnic4-9：データ インターフェイス（オプション）

重要　vnic0、vnic1、および vnic3 は、必ず同じサブネットにマップするようにしてください。

ステップ 12　第 0 日のコンフィギュレーション ファイルを使用して展開する場合、ISO の仮想 CD-ROM を作成します。

a) [ハードウェアを追加（Add Hardware）] をクリックします。
b) [ストレージ（Storage）] を選択します。
c) [管理対象またはその他既存のストレージを選択（Select managed or other existing storage）] をクリックし、ISO ファイルの場所を参照します。
d) [デバイスタイプ（Device type）] で、[IDE CDROM] を選択します。

ステップ 13　仮想マシンのハードウェアを設定した後、[適用（Apply）] をクリックします。

ステップ 14　virt-manager の [インストールの開始（Begin installation）] をクリックして、指定したハードウェア設定で仮想マシンを作成します。

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。

- [ローカルに管理（ManageLocally）] 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。
- [ローカルに管理（ManageLocally）] で [はい（Yes）] を選択した場合は、統合された 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。

第 0 日のコンフィギュレーション ファイルを使用しない起動

FTDv アプライアンスには Web インターフェイスがないため、第 0 日のコンフィギュレーション ファイルを使用せずに展開した場合には、CLI を使用して仮想デバイスを設定する必要があります。

新しく展開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。

（注） 初期セットアップの完了後に仮想デバイスに関するこれらの設定を変更するには、CLI を使用する必要があります。

ステップ 1 FTDv で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が求められます。

- 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（ローカル管理が必要）

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。

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。

ステップ 7 CLI を閉じます。

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。