Firepower Threat Defense Virtual と KVM の利用開始

Cisco Firepower Threat Defense 仮想（FTDv）は、シスコの Firepower 次世代ファイアウォール機能を仮想化環境にもたらし、一貫性のあるセキュリティポリシーを実現して、物理、仮想、クラウドの各環境にわたって、またクラウド間で、ワークロードを実行します。

この章では、カーネルベース仮想マシン（KVM）のハイパーバイザ環境で FTDv が機能する仕組みについて説明します。機能のサポート、システム要件、ガイドライン、および制限事項について取り上げます。また、FTDv を管理する際のオプションについても説明します。

展開を開始する前に、管理オプションを理解しておくことが重要です。FTDv の管理と監視には Firepower Management Center または Firepower Device Manager を使用できます。その他の管理オプションを使用できる場合もあります。

KVM を使用した FTDv の展開について

KVM は、仮想化拡張機能（Intel VT など）を搭載した x86 ハードウェア上の Linux 向け完全仮想化ソリューションです。KVM は、コア仮想化インフラストラクチャを提供するロード可能なカーネル モジュール（kvm.ko）と kvm-intel.ko などのプロセッサ固有のモジュールで構成されています。

KVM を使用して、修正されていない OS イメージを実行している複数の仮想マシンを実行できます。各仮想マシンには、ネットワーク カード、ディスク、グラフィック アダプタなどのプライベートな仮想化ハードウェアが搭載されています。

Firepower デバイスの管理方法

Firepower Threat Defense デバイスの管理には次の 2 つのオプションを選択できます。

Firepower Device Manager

Firepower Device Manager（FDM）オンボード統合マネージャ。

FDM は、一部の Firepower Threat Defense デバイスに組み込まれている Web ベースの設定インターフェイスです。FDM では、小規模ネットワークで最も一般的に使用されるソフトウェアの基本機能を設定できます。また、これは多くの Firepower Threat Defense デバイスを含む大規模なネットワークを制御するために強力な複数デバイスのマネージャを使用することがない、単一のデバイスまたは限られた数のデバイスを含むネットワークのために特に設計されています。

（注） FDM をサポートしている Firepower Threat Defense デバイスのリストについては、『Cisco Firepower Threat Defense Configuration Guide for Firepower Device Manager』を参照してください。

Firepower Management Center

Cisco Firepower Management Center（FMC）。

多数のデバイスを管理している場合、または Firepower Threat Defense で許可される、より複雑な機能や設定を使用したい場合は、組み込みの FDM の代わりに FMC を使用してデバイスを設定します。

重要 FDM と FMC の両方を使用して Firepower デバイスを管理することはできません。いったん FDM の統合管理を有効にすると、ローカル管理を無効にして、FMC を使用するように管理を再設定しない限り、FMC を使用して Firepower デバイスを管理することはできなくなります。一方、Firepower を FMC に登録すると、FDM のオンボード管理サービスは無効になります。

注意 現在、シスコには FDM Firepower 設定を FMC に移行するオプションはありません。その逆も同様です。Firepower デバイス用に設定する管理のタイプを選択する際は、このことを考慮してください。

システム要件

Firepower Threat Defense 仮想のハイパーバイザのサポートに関する最新情報については、『Cisco Firepower Compatibility Guide』を参照してください。

メモリ、vCPU、およびディスクのサイジング

Firepower Threat Defense 仮想 の導入に使用される特定のハードウェアは、導入されるインスタンスの数や使用要件によって異なります。FTDv の各インスタンスには、サーバ上での最小リソース割り当て（メモリ容量、CPU 数、およびディスク容量）が必要です。

（注） 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。

表 *1*：バージョン *6.4* 以降の *FTDv* アプライアンスの設定

設定	デフォルト	設定調整の可否
メモリ	8 GB	はい（最大 32GB）
cCPU	4	はい（最大 16 個の vCPU）
ハードディスク プロビジョニング サイズ	50 GB	はい。virtio ブロック デバイスをサポート

次の 3 つの推奨/サポートされている vCPU/メモリ値があります。

- 4 vCPU/8 GB（デフォルト）
- 8 vCPU/16 GB
- 12 vCPU/24 GB

重要 その他の vCPU/メモリ値を設定できますが、上記の 3 つの組み合わせのみがサポートされています。vCPU/メモリの値を変更するには、最初に FTDv デバイスの電源をオフにする必要があります。

表 *2*：バージョン *6.3* 以前の *FTDv* アプライアンスの設定

設定	デフォルト	設定調整の可否
メモリ	8 GB	なし
vCPU	4	なし

設定	デフォルト	設定調整の可否
ハード ディスク プロビジョニング サイズ	50 GB	はい。virtio ブロック デバイスをサポート

（注） FTDv は固定構成 4vCPU/8GB デバイスとして展開されます。バージョン 6.3 以前では、vCPU とメモリの調整はサポートされていません。

ネットワーキング ガイドラインとベストプラクティス

- ブートするには 2 つの管理インターフェイスと 2 つのデータ インターフェイスが必要

  （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に配置されます。

  - virtio ドライバをサポート
  - SR-IOV の ixgbe-vf ドライバをサポート
  - 合計 10 個のインターフェイスをサポート

- FTDv のデフォルト設定では、管理インターフェイス（管理と診断）および内部インターフェイスが**同じサブネット**上にあり、管理アドレスはインターネットへのゲートウェイとして内部アドレスを使用すると仮定します（外部インターフェイス経由）。
- FTDv は、少なくとも 4 つのインターフェイスを備え、firstboot で電源がオンになる必要があります。4 つのインターフェイスがなければ展開は実行されません。
- 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。
  - 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 ～ 10. データ インターフェイス（オプション）

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、宛先ネットワークに関する以下の用語索引を参照してください。

表 *3*: 送信元から宛先ネットワークへのマッピング

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
vnic0*	Management0-0	Management0/0	管理
vnic1	診断	診断	診断
vnic2*	GigabitEthernet0-0	GigabitEthernet 0/0	外部
vnic3*	GigabitEthernet0-1	GigabitEthernet 0/1	内部
* 重要同じサブネットに接続します。			

- OpenStack 環境に FTDv を導入する場合は、無差別モードで実行し、ポート セキュリティ（パケット フィルタリング）を無効にする必要があります。この操作を行うときに、セキュリティ グループまたは許可されたアドレス ペアがインターフェイスに割り当てられていると、ポート セキュリティを無効にできないことに注意してください。ポート レベルのセキュリティを無効にすると、すべてのトラフィック（イングレスとイーグレス）が許可されます。
- 仮想マシンの複製はサポートされません。
- コンソールアクセスでは、Telnet を介したターミナルサーバをサポートします。

SR-IOV のサポート

SR-IOV 仮想機能には特定のシステムリソースが必要です。SR-IOV 対応 PCIe アダプタに加えて、SR-IOV をサポートするサーバが必要です。以下のハードウェア検討事項に留意する必要があります。

- 使用可能な VF の数を含む SR-IOV NIC の機能は、ベンダーやデバイスによって異なります。次の NIC がサポートされています。
  - Intel Ethernet Server Adapter X710
  - Intel Ethernet Server Adapter X520 - DA2
- すべての PCIe スロットが SR-IOV をサポートしているわけではありません。
- SR-IOV 対応 PCIe スロットは機能が異なる場合があります。
- x86_64 マルチコア CPU：Intel Sandy Bridge 以降（推奨）。

（注） シスコでは、FTDv を 2.3GHz の Intel Broadwell CPU（E5-2699-v4）でテストしました。

- コア
  - CPU ソケットあたり 8 個以上の物理コア。
  - 単一のソケット上で 8 コアにする必要があります。

（注） CPU ピンニングは、フルスループットを実現するために推奨されています。

- メーカーのマニュアルで、お使いのシステムの SR-IOV サポートを確認する必要があります。KVM の場合は、SR-IOV サポートの CPU の互換性を確認できます。KVM 上の FTDv では、x86 ハードウェアしかサポートされないことに注意してください。