Cisco HyperFlex への Threat Defense Virtual の展開

この章では、vCenter サーバーまたはスタンドアロン ESXi ホストの Cisco HyperFlex に Threat Defense Virtual を展開する際の手順について説明します。

概要

Cisco Secure Firewall Threat Defense Virtual（旧称 Firepower Threat Defense Virtual）は、Cisco Secure Firewall 機能を仮想化環境にもたらします。物理環境、仮想環境、クラウド環境全体を通して、またクラウド間で一貫性のあるセキュリティポリシーを実現し、ワークロードをサポートします。

HyperFlex システムは、あらゆる場所であらゆるアプリケーションにハイパーコンバージェンスを提供します。Cisco Unified Computing System（Cisco UCS）テクノロジーを備える HyperFlex は、Cisco Intersight クラウド運用プラットフォームを通じて管理され、場所を問わずアプリケーションとデータを強力にサポートし、コアデータセンターからエッジ、そしてパブリッククラウドまでの運用を最適化し、DevOps 手法を推進して俊敏性を高めることができます。

この章では、Cisco HyperFlex 環境内における Threat Defense Virtual の機能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、制限事項などを取り上げます。また、この章では Threat Defense Virtual を管理するためのオプションについても説明します。導入を開始す

る前に、管理オプションを理解しておくことが重要です。Secure Firewall Management Center（旧称 Firepower Management Center）または Secure Firewall Device Manager （旧称 Firepower Device Manager）を使用して Threat Defense Virtual を管理および監視できます。その他の管理オプションを使用できる場合もあります。

エンドツーエンドの手順

次のフローチャートは、Cisco HyperFlex に Threat Defense Virtual を展開する際のワークフローを示しています。

	ワークスペース	手順
1	HyperFlex	Threat Defense Virtual の導入：Cisco.com から Threat Defense Virtual の VI OVF テンプレートファイルをダウンロードします。
2	HyperFlex	Threat Defense Virtual の導入：OVF テンプレート情報を確認します。
3	HyperFlex	Threat Defense Virtual の導入：展開設定をカスタマイズします。
4	HyperFlex	Threat Defense Virtual の導入：表示される情報に目を通して確認します。[終了（Finish）] をクリックして、OVF テンプレートの展開を開始します。
5	Management Center または Device Manager	Threat Defense Virtual の管理： • Management Center を使用 • Device Manager を使用

システム要件

バージョン

マネージャバージョン	デバイスバージョン
Device Manager 7.0	Threat Defense 7.0
Management Center 7.0	

Threat Defense Virtual 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。

Threat Defense Virtual メモリ、ディスクのサイジング、および vCPU

Threat Defense Virtual の導入に使用される特定のハードウェアは、導入するインスタンス数や使用要件によって異なります。Threat Defense Virtual の各インスタンスには、サーバー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。

設定	値
パフォーマンス階層	**バージョン 7.0 以降** Threat Defense Virtual は、導入要件に基づいて異なるスループットレベルと VPN 接続制限を提供するパフォーマンス階層型ライセンスをサポートしています。 • FTDv5 4vCPU/8GB（100 Mbps） • FTDv10 4vCPU/8GB（1 Gbps） • FTDv20 4vCPU/8GB（3 Gbps） • FTDv30 8vCPU/16GB（5 Gbps） • FTDv50 12vCPU/24GB（10 Gbps） • FTDv100 16vCPU/32GB（16 Gbps） Threat Defense Virtual デバイスのライセンスを取得する場合のガイドラインについては、『*Firepower Management Center* コンフィギュレーション ガイド』の「Firepower システムのライセンス」の章を参照してください。 （注） vCPU/メモリの値を変更するには、最初に Threat Defense Virtual デバイスの電源をオフにする必要があります。

設定	値
ストレージ	ディスク形式の選択に基づきます。 • シンプロビジョニングのディスクサイズは 48.24 GB です。
vNIC	Threat Defense Virtual は次の仮想ネットワークアダプタをサポートしています。 • **VMXNET3**：VMware 上の Threat Defense Virtual 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。（7.1 以降）vmxnet3 ドライバは、最初のイーサネットアダプタを管理に使用します。2番目のアダプタは未使用です。（7.0 以前） VMXNET3 ドライバは、2 つの管理インターフェイスを使用します。最初の 2 つのイーサネット アダプタは、管理インターフェイスとして設定する必要があります。1つはデバイス管理/登録用で、もう 1 つは診断用です。

Threat Defense Virtual ライセンス

- Management Center からセキュリティ サービスのすべてのライセンス資格を設定します。
- ライセンスの管理方法の詳細については、『Firepower Management Center コンフィギュレーション ガイド』の「*Firepower* システムのライセンス」を参照してください。

HyperFlex HX シリーズの設定とクラスタ

設定	クラスタ
HX220c コンバージドノード	• フラッシュクラスタ • 最小 3 ノードクラスタ（データベース、VDI、VSI）
HX240c コンバージドノード	• フラッシュクラスタ • 最小 3 ノードクラスタ（VSI：T/Biz アプリケーション、テスト/開発）
HX220C とエッジ（VDI、VSI、ROBO） HX240C（VDI、VSI、テスト/開発）	• ハイブリッドクラスタ • 最小 3 ノードクラスタ
B200 + C240/C220	コンピューティング バウンド アプリ/VDI

HyperFlex HX シリーズの導入オプション：

- ハイブリッドクラスタ
- フラッシュクラスタ
- HyperFlex HX エッジ
- SED ドライブ
- NVME キャッシュ
- GPU

HyperFlex HX クラウドを利用した管理オプションについては、『Cisco HyperFlex システム設置ガイド』の「*HyperFlex* ファブリック インターコネクトに接続されたクラスタの展開」のセクションを参照してください。

HyperFlex コンポーネントとバージョン

コンポーネント	バージョン
VMware vSphere/VMware ESXI	7.0 Threat Defense Virtual と VMware vSphere/VMware ESXI との互換性の詳細については、「Threat Defense Virtual の互換性：VMware」を参照してください。
HyperFlex Data Platform	4.5.1a-39020 以降 .

注意事項と制約事項

サポートされる機能

- 展開モード：ルーテッド（スタンドアロン）、ルーテッド（HA）、インラインタップ、インライン、パッシブ、およびトランスペアレント
- ライセンス：BYOL のみ
- IPv6
- Threat Defense Virtual ネイティブ HA
- ジャンボフレーム
- HyperFlex データセンタークラスタ（ストレッチ クラスタを除く）
- HyperFlex Edge クラスタ

- HyperFlex すべての NVMe、オールフラッシュ、およびハイブリッド コンバージド ノード
- HyperFlex コンピューティング専用ノード

サポートされない機能

SR-IOV を使用した Threat Defense Virtualの実行は、HyperFlex で認定されていません。

（注） HyperFlex は SR-IOV をサポートしていますが、MLOM VIC に加えて PCI-e NIC も必要です。

一般的なガイドライン

HyperFlex の vSwitch を設定するには、GUI またはコマンド ライン インターフェイスを使用します。vSwitch を設定すると、複数の ESX サーバーをインストールして、vSwitch 設定のスクリプトを構築する際に便利です。詳細については、『Cisco HyperFlex Systems Network and External Storage Management Guide』の「Configure the vSwitches」の項を参照してください。

Threat Defense Virtual 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用語索引を以下に記載します。

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	診断	診断
ネットワークアダプタ 3	GigabitEthernet0-0	GigabitEthernet 0/0	外部
ネットワークアダプタ 4	GigabitEthernet0-1	GigabitEthernet 0/1	内部
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 10			

パフォーマンスの最適化

Threat Defense Virtual の最高のパフォーマンスを実現するために、VM とホストの両方を調整することができます。詳細については、「HyperFlex での仮想化の調整と最適化」を参照してください。

Receive Side Scaling：Threat Defense Virtual は Receive Side Scaling（RSS）をサポートしています。これは、ネットワークアダプタによって複数のプロセッサコアにネットワーク受信トラ

フィックを分散するために使用されるテクノロジーです。バージョン 7.0 以降でサポートされています。詳細については、「Receive Side Scaling（RSS）用の複数の RX キュー」を参照してください。

Snort

- Snort のシャットダウンに時間がかかったり、VM が全体的に遅くなったりといった異常な動作が見られる場合や、特定のプロセスが実行されるときには、Threat Defense Virtual および VM ホストからログを収集します。全体的な CPU 使用率、メモリ、I/O 使用率、および読み取り/書き込み速度のログの収集は、問題のトラブルシューティングに役立ちます。
- Snort のシャットダウン時には、CPU と I/O の使用率が高くなります。十分なメモリがなく、専用の CPU がない単一のホスト上に多数の Threat Defense Virtual インスタンスが作成されている場合は、Snort のシャットダウンに時間がかかって Snort コアが作成されます。

vSphere 標準スイッチのセキュリティポリシー設定の変更

vSphere 標準スイッチの場合、レイヤ 2 セキュリティポリシーには、無差別モード、MAC アドレスの変更、不正送信という 3 つの要素があります。Threat Defense Virtual は無差別モードを使用して稼働します。また、Threat Defense Virtual の高可用性が正常に機能するかは、アクティブとスタンバイ間での MAC アドレスの切り替えにかかっています。

デフォルト設定では、Threat Defense Virtual の適切な動作が阻止されます。以下の必須の設定を参照してください。

表 *1 : vSphere* 標準スイッチのセキュリティ ポリシー オプション

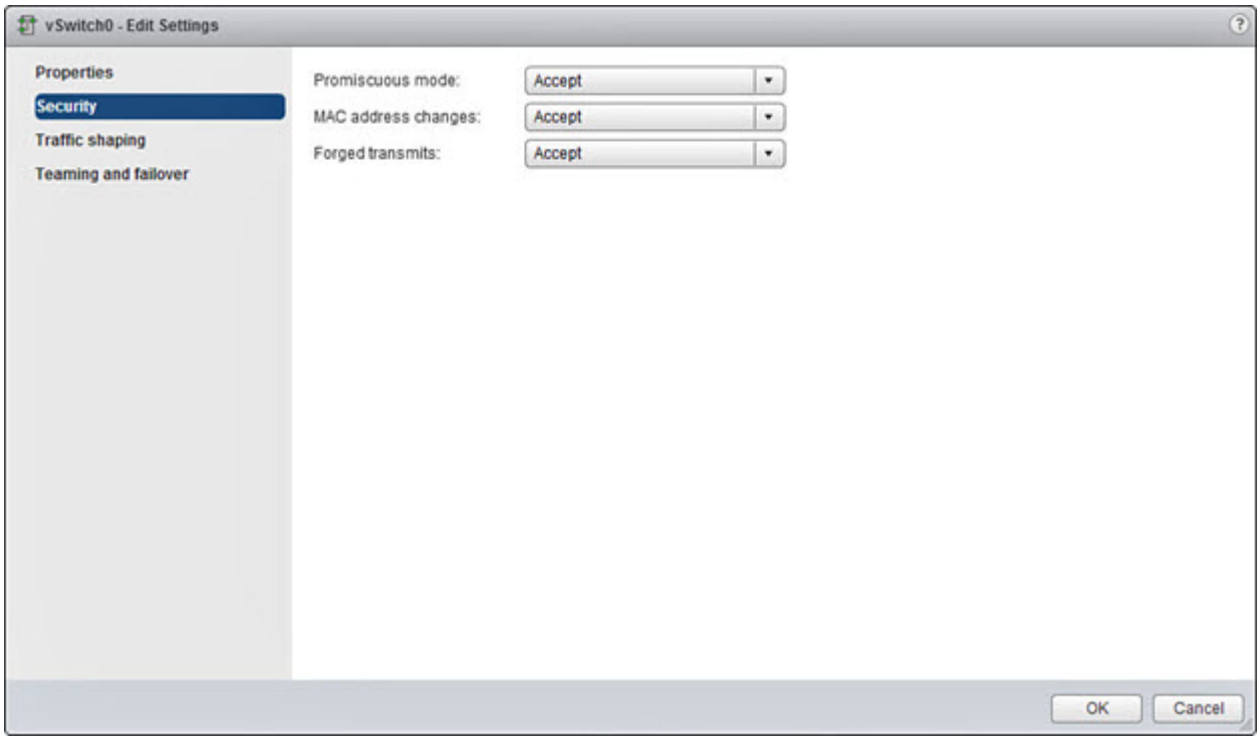
オプション	必須の設定	アクション
無差別モード（Promiscuous Mode）	承認（Accept）	vSphere Web Client の vSphere 標準スイッチのセキュリティポリシーを編集し、[無差別モード（Promiscuous mode）] オプションを [承認（Accept）] に設定する必要があります。 ファイアウォール、ポートスキャナ、侵入検知システムなどは無差別モードで実行する必要があります。

オプション	必須の設定	アクション
MAC アドレスの変更（MAC Address Changes）	承認（Accept）	vSphere Web Client の vSphere 標準スイッチのセキュリティポリシーを検証し、[MAC アドレスの変更（MAC address changes）] オプションが [承認（Accept）] に設定されていることを確認する必要があります。
不正送信（Forged Transmits）	承認（Accept）	vSphere Web Client の vSphere 標準スイッチのセキュリティポリシーを検証し、[不正転送（Forged transmits）] オプションが [承認（Accept）] に設定されていることを確認する必要があります。

Threat Defense Virtual を正しく動作させるためのデフォルト設定にするには、次の手順を実行します。

1. vSphere Web クライアントで HyperFlex クラスタに移動します。
2. [管理（Manage）] タブで、[ネットワーク（Networking）] をクリックし、[仮想スイッチ（Virtual switches）] を選択します。
3. リストから標準スイッチを選択し、[設定の編集（Edit settings）] をクリックします。
4. [セキュリティ（Security）] を選択し、現在の設定を表示します。
5. 標準スイッチに接続された仮想マシンのゲスト オペレーティング システムで無差別モードの有効化、MAC アドレスの変更、および不正送信の [承認（Accept）] を選択します。

図 *1 : vSwitch* の編集設定



6. [OK] をクリックします。

（注） これらの設定が、Threat Defense Virtual デバイスの管理インターフェイスおよびフェールオーバー（HA）インターフェイスに設定されているすべてのネットワーク上で同じであることを確認します。

関連資料

『Release Notes for Cisco HX Data Platform』

Configuration Guides for Cisco HX Data Platform

Cisco HyperFlex 4.0 for Virtual Server Infrastructure with VMware ESXi

Cisco HyperFlex Systems Solutions Overview

Cisco HyperFlex Systems ドキュメンテーション ロードマップ

Secure Firewall Threat Defense Virtual デバイスの管理方法

Secure Firewall Threat Defense Virtual 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。

Secure Firewall Management Center

多数のデバイスを管理している場合、または 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 Device Manager の代わりに Management Center を使用してデバイスを設定します。

重要 Device Manager と Management Center の両方を使用して Threat Defense デバイスを管理することはできません。いったん Device Manager の統合管理を有効にすると、ローカル管理を無効にして、Management Center を使用するように管理を再設定しない限り、Management Center を使用して Threat Defense デバイスを管理することはできなくなります。一方、Threat Defense デバイスを Management Center に登録すると、Device Manager 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 Device Manager の設定を Management Center に移行するオプションはありません。その逆も同様です。Threat Defense 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。

Secure Firewall Device Manager

Device Manager はオンボード統合マネージャです。

Device Manager は一部の Threat Defense デバイスに搭載された Web ベースの設定インターフェイスです。Device Manager 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 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） Device Manager をサポートする Threat Defense デバイスのリストについては、「Cisco Secure Firewall Device Manager Configuration Guide」を参照してください。

概要

VMware vCenter サーバー上の Cisco HyperFlex に Threat Defense Virtual を展開できます。

Threat Defense Virtual 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。

Cisco HyperFlex 向けの Threat Defense Virtual 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 クライアントを使用して、Cisco HyperFlex 環境にアクセスできます。

Threat Defense Virtual の導入

以下の手順を使用して、vSphere vCenter Server 上の Cisco Hyperflex に Threat Defense Virtual アプライアンスを展開します。

始める前に

- Cisco HyperFlex を展開してインストール後の構成タスクをすべて実行済みであることを確認します。詳細については、『Cisco HyperFlex Systems Documentation Roadmap』を参照してください。
- Threat Defense Virtual 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。
- Cisco.com から Threat Defense Virtual VI OVF テンプレートファイル（*Cisco_Firepower_Threat_Defense_Virtual-VI-X.X.X-xxx.ovf*）をダウンロードします。*X.X.X-xxx* はバージョンとビルド番号です。

ステップ 1 vSphere Web クライアントにログインします。

ステップ 2 Threat Defense Virtual を展開する HyperFlex クラスタを選択し、**[アクション（ACTIONS）]** > **[OVFテンプレートの展開（Deploy OVF Template）]** の順にクリックします。

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 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 Threat Defense Virtual の名前と場所を指定し、[次へ（NEXT）] をクリックします。

ステップ 5 コンピューティングリソースを選択し、互換性チェックが完了するまで待ちます。

互換性チェックが成功したら、[次へ（NEXT）] をクリックします。

ステップ 6 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 7 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て承認し、[次へ（NEXT）] をクリックします。

ステップ 8 展開の構成（vCPU/メモリ値）を選択し、[次へ（NEXT）] をクリックします。

ステップ 9 ストレージの場所と仮想ディスク形式を選択し、[次へ（NEXT）] をクリックします。

このウィンドウで、宛先の HyperFlex クラスタですでに設定されているデータストアから選択します。仮想マシンの構成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。

[シックプロビジョン（Thick Provisioned）] を仮想ディスク形式として選択すると、すべてのストレージがただちに割り当てられます。[シンプロビジョン（Thin Provisioned）] を仮想ディスク形式として選択すると、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 10 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 Management Center または Device Manager から設定できます。

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、Threat Defense Virtual 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 Threat Defense Virtual 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、Threat Defense Virtual 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）。

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	送信元ネットワーク	宛先ネットワーク	機能
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）

Threat Defense Virtual 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 Threat Defense Virtual 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、Threat Defense Virtual の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 11 OVF テンプレートでパッケージ化された、ユーザー設定可能なプロパティを設定します。

（注） このステップでは、必須のカスタマイズ項目をすべて設定することを推奨します。必要なすべてのカスタマイズ項目を設定しなかった場合は、展開後に CLI にログインして設定を完了する必要があります。この説明については、CLI を使用した Threat Defense Virtual のセットアップの完了 （15 ページ） を参照してください。

a) **パスワード**

Threat Defense Virtual 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 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。Management Center を使用してこのデバイスを管理するには、[いいえ（No）] を選択します。

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 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は設定できません。

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）]：Management Center 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、ユーザーが生成するキーで、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（-）などがあります。デバイスを Management Center に追加するときに、この登録キーが必要になります。
- [NAT ID]：Threat Defense Virtual と Management Center 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、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、ユーザーが生成するキーで、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（-）などがあります。

f) [次へ（NEXT）] をクリックします。

ステップ 12 表示された情報を確認して検証します。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。

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。

Threat Defense Virtual 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 Threat Defense Virtual を正常に登録するには、Threat Defense Virtual にインターネットアクセスが必要です。インターネットアクセスを実行して正常にライセンス登録するには、展開後に追加の構成が必要になります。

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、Management Center を使用して Threat Defense Virtual を管理します。「Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理」を参照してください。

（注） Threat Defense Virtual の展開時に必要なすべてのカスタマイズ項目を設定しなかった場合は、CLI を使用して設定を完了する必要があります。この説明については、CLI を使用した Threat Defense Virtual のセットアップの完了 （15 ページ） を参照してください。

CLI を使用した Threat Defense Virtual のセットアップの完了

Threat Defense Virtual の展開時に必要なすべてのカスタマイズ項目を設定しなかった場合は、CLI を使用して設定を完了する必要があります。

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、ユーザー名 **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 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（ローカル管理で 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 # 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 Threat Defense Virtual を正常に登録するには、Threat Defense Virtual 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、Management Center を使用して Threat Defense Virtual を管理します。「Secure Firewall Management Center を使用した Secure Firewall Threat Defense Virtual の管理」を参照してください。

ジャンボ フレームの有効化

MTU が大きいほど、大きいパケットを送信できます。パケットが大きいほど、ネットワークの効率が良くなる可能性があります。次のガイドラインを参照してください。

- トラフィック パスの MTU の一致：すべての ASAv インターフェイスとトラフィック パス内のその他のデバイスのインターフェイスでは、MTU が同じになるように設定することを推奨します。MTU の一致により、中間デバイスでのパケットのフラグメント化が回避できます。
- ジャンボ フレームへの対応：MTU を最大 9198 バイトに設定できます。ASAv の最大値は 9000 です。

この手順では、次の環境でジャンボフレームを有効にする方法について説明します。

vSphere 7.0.1 上の HyperFlex クラスタ > VMware vSphere vSwitch> Cisco UCS ファブリック インターコネクト（FI）

ステップ 1 ASAv を展開した ASAv ホストの MTU 設定を変更します。

1. vSphere Web クライアントを使用して vCenter サーバーに接続します。
2. HyperFlex ホストの [詳細システム設定（Advanced System Settings）] で、[Net.Vmxnet3NonTsoPacketGtMtuAllowed] の設定パラメータの値を `1` にします。
3. 変更を保存してホストを再起動します。

詳細については、「https://kb.vmware.com/s/article/1038578」を参照してください。

ステップ 2 VMware vSphere vSwitch の MTU 設定を変更します。

1. vSphere Web クライアントを使用して vCenter サーバーに接続します。
2. VMware vSphere vSwitch のプロパティを編集し、[MTU] の値を `9000` に設定します。

ステップ 3 Cisco UCS ファブリック インターコネクト（FI）の MTU 設定を変更します。

1. Cisco UCS Management コンソールにログインします。

2. QoS システムクラスを編集するには、**[LAN]** > **[LANクラウド（LAN Cloud）]** > **QoS システム クラス（QoS System Class）** の順に選択します。[全般（General）] タブで、[MTU] の値を 9216 に設定します。
3. vNIC を編集するには、**[LAN]** > **[ポリシー（Policies）]** > **[ルート（root）]** > **[サブ組織（Sub-Organizations）]**

   <your-hyperflex-org>**vNIC テンプレート** <your-vnic> の順に選択します。[全般（General）] タブで、[MTU] の値を 9000 に設定します。

トラブルシューティング

ここでは、仮想マシンへの Hyperflex 導入に関連する基本的なトラブルシューティング手順について説明します。

仮想マシンが HyperFlex を実行しているかどうかを確認

Threat Defense Virtual アプライアンスが ESX OS を搭載した HyperFlex に設置されている場合、HX post_install スクリプトによって作成されたデフォルトの vSphere HA ポリシーにより、Threat Defense Virtual の電源がオンになったときにエラーメッセージが表示されます。エラーメッセージの内容は以下のとおりです。

「電源オンに失敗：vSphere HA 向けに設定されたフェールオーバーレベルを満たすために必要なリソースが不足しています。」

回避策

1. VMware vCenter で**[HXクラスタ（HX cluster）** > **[設定（Configure）]** > **[vSphereの可用性（vSphere Availability）]** > **[vSphere HAの編集（Edit vSphere HA）]** > **[アドミッションコントロール（Admission Control）]** > **[ホストのフェールオーバー キャパシティの定義（Define host failover capacity）]** > **[計算済みフェールオーバー キャパシティのオーバーライド（Override Calculated failover capacity）]**に移動します。
2. 予約済みのフェールオーバー CPU とメモリ容量の割合を変更および調整します。
3. Threat Defense Virtual VM の電源を入れます。

翻訳について
このドキュメントは、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。