Multicloud Defense での Cisco Secure Firewall Threat Defense Virtual スタートアップガイド

最終更新：2026 年 1 月 19 日

Multicloud Defense での Cisco Secure Firewall Threat Defense Virtual デバイスの設定と展開

該当するユースケースであることの確認

このユースケースは、以下を対象としています。

- クラウド提供型 Firewall Management Center（cdFMC）の Cisco Secure Firewall Threat Defense Virtual（FTDv）および Multicloud Defense、Amazon Web Services（AWS）、および Azure プラットフォームのユーザーで、クラウドを介して資産を保護することを検討している方。
- AWS および Azure クラウド サービス プロバイダー。
- シスコ外部および内部の顧客管理チームおよび管理者。

Multicloud Defense での Cisco Secure Firewall Threat Defense Virtual の概要

仮想ファイアウォールまたはゲートウェイの展開は、複雑な手動プロセスになる可能性があります。そのため、セキュア VPC、VPC/VNet、サブネット、セキュリティグループ、ルート、トランジットゲートウェイ、ゲートウェイロードバランサなどのクラウドコンポーネントを構築して設定し、トラフィックフローなどを設定する必要があります。また、スケーリングニーズへの対応も考慮する必要があります。そのため、展開時間が遅くなり、設定中のヒューマンエラーのリスクが高くなります。また、インフラストラクチャに複数のサービスプロバイダーがあり、それぞれの設定や管理に関するニーズが異なるため、複雑性が増大します。Multicloud Defense は、そのような複雑性に対処するのに役立ちます。

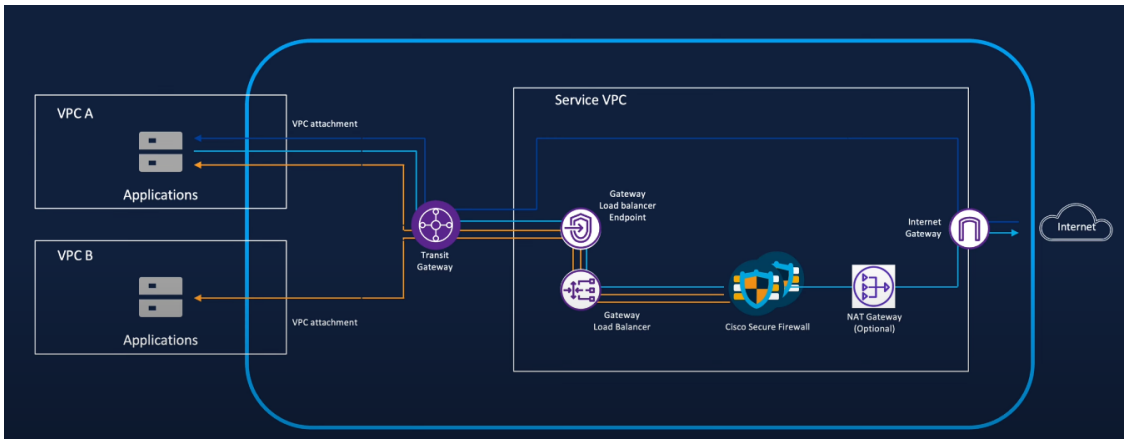
Multicloud Defense は、複数のクラウドプロバイダーにわたって Cisco Secure Firewall Threat Defense Virtual デバイスの展開を完全にオーケストレーションできます。Multicloud Defense は、すべてのクラウド インフラストラクチャの VPC、サブネット、ロードバランサ、セキュリティグループの作成を自動化するのに役立つオーケストレーションを行い、ルートテーブル

とピアの設定を簡素化します。Multicloud Defense を使用すると、FTDv デバイスをクラウド提供型 Firewall Management Center（cdFMC）に自動的にオンボードして登録することができ、そこからポリシーを効果的に管理できます。Multicloud Defense は、FTDv デバイスのリアルタイムトラフィックと正常性に基づいて、自動スケーリングのニーズにも対応します。

Multicloud Defense Controller による FTDv オーケストレーションに関するビデオをご覧ください。

Multicloud Defense で Firewall Threat Defense Virtual を設定するためのワークフロー

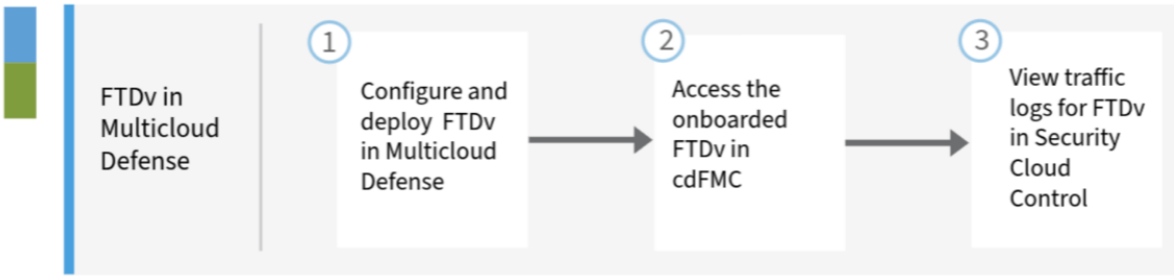
次のイメージは、出力/水平方向のユースケースで、Multicloud Defense のクラウド提供型 Firewall Management Center によって管理される AWS FTDv のオーケストレーションを示しています。



process_workflow

イメージに示された VPC A および VPC B は、保護する必要がある資産です。Multicloud Defense は、サービス VPC、トランジットゲートウェイとその VPC A および VPC B へのアタッチメント、ゲートウェイロードバランサ、ゲートウェイ ロード バランサ エンドポイント、および 1 つの NAT ゲートウェイ（オプション）を作成します。Multicloud Defense コントローラは、これらのリソースの自動設定を管理し、すべてのリソースの展開をオーケストレーションします。クラウドサービスプロバイダーのアカウントで設定する必要はありません。すべてのバックエンドコンポーネント設定は、Multicloud Defense Controller によってシームレスに管理されます。保護されたトラフィックが Cisco Secure Firewall からインターネットに伝送されるようになりました。

次のワークフローは、Multicloud Defense での FTDv の設定について説明しています。



番号	手順
1.	FTDv を設定および展開します。詳細については、「Multicloud Defense での FTDv の設定と展開」を参照してください。
2.	cdFMC でオンボードされた FTDv にアクセスします。詳細については、「cdFMC でオンボードされた FTDv へのアクセス」を参照してください。
3.	Security Cloud Control で FTDv のトラフィックログを表示します。詳細については、「Security Cloud Control での FTDv のトラフィックログの表示」を参照してください。

Firewall Threat Defense Virtual の設定に関するガイドライン

前提条件として、Security Cloud Control で作成された、cdFMC が有効になっているテナントが必要です。FTDv を設定する場合は、関連するガイドで次のガイドラインを参照してください。

- Multicloud Defense 関連のガイドラインについては、「Secure Firewall Threat Defense Virtual」を参照してください。
- cdFMC 関連のガイドラインについては、「Guidelines for Managing an FTDv Created in Multicloud Defense」を参照してください。

Multicloud Defense での Firewall Threat Defense Virtual の設定と展開

手順

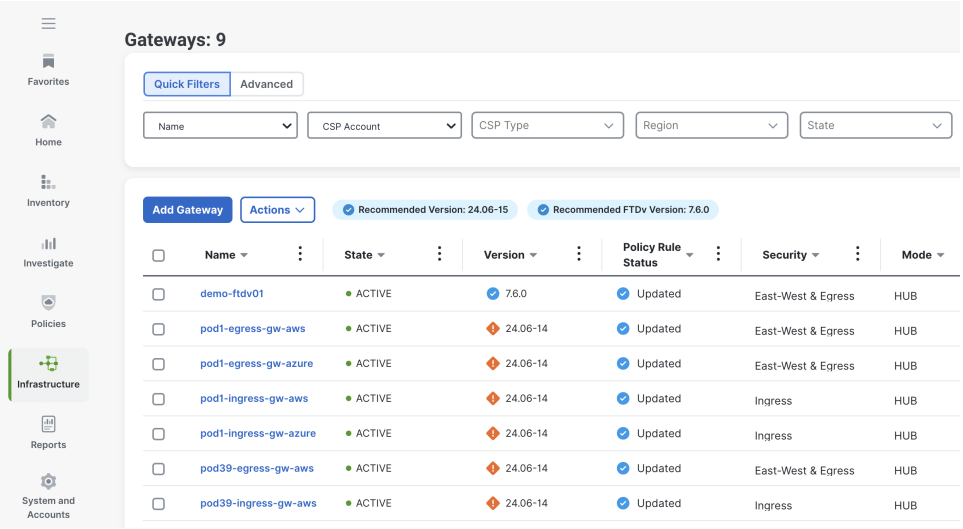
ステップ 1 Security Cloud Control にログインします。

ステップ 2 左側のペインで、[Multicloud Defense] をクリックします。

ステップ 3 右上隅にある [Multicloud Defense Controller] をクリックして、コントローラを開きます。

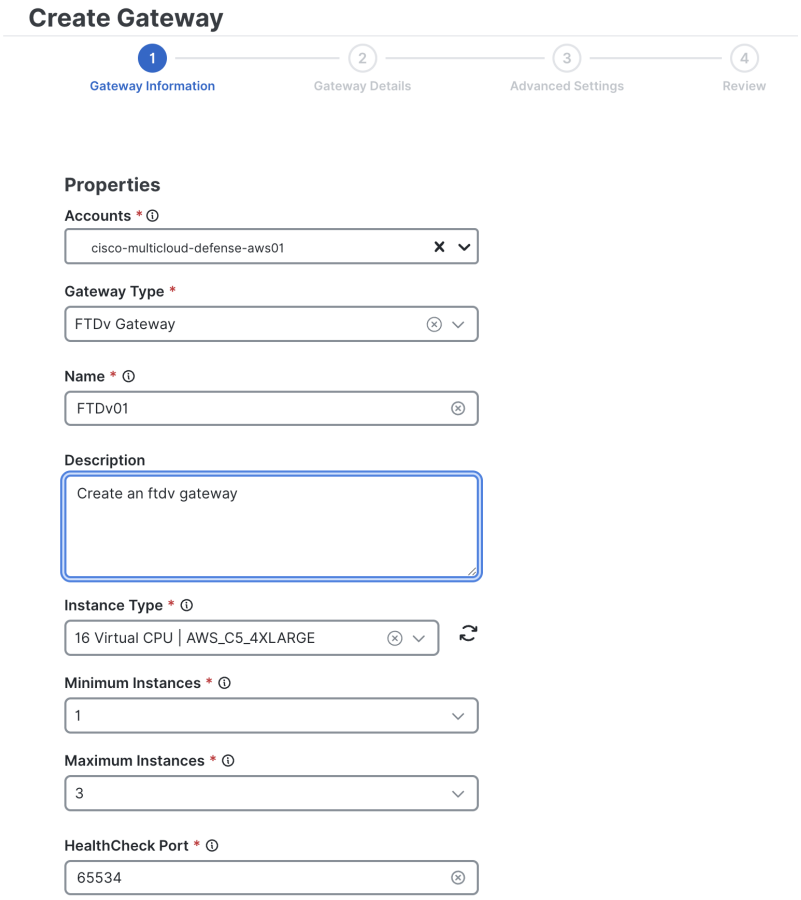
ステップ 4 Multicloud Defense ポータルで、**[インフラストラクチャ（Infrastructure）]** > > **[ゲートウェイ（Gateways）]** > > **[ゲートウェイ（Gateways）]** > に移動します。

ステップ 5 [ゲートウェイの追加（Add Gateway）] をクリックします。



ステップ 6 次のフィールドに詳細事項を入力します。

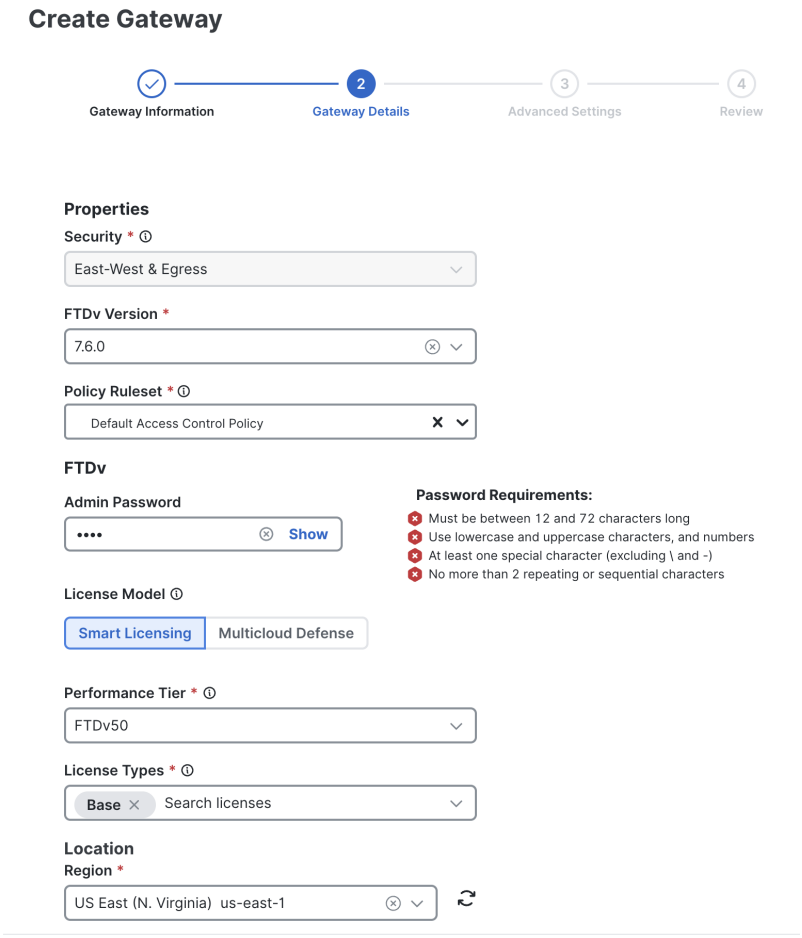
- [アカウント（Accounts）]：cisco-multicloud-defense-aws01 など
- [ゲートウェイタイプ（Gateway Type）]：FTDv ゲートウェイを選択します。
- [名前（Name）]：この例では、名前として「FTDv01」と入力します。
- [説明（Description）]：説明を入力します。
- [インスタンスタイプ（Instance Type）]：ドロップダウンリストからインスタンスを選択します（16 Virtual CPU AWS_C5_4XLARGE など）。
- [インスタンスの最小数（Minimum Instances）]：ドロップダウンリストから値を選択します（1 など）。
- [インスタンスの最大数（Maximum Instances）]：ドロップダウンリストから値を選択します（3 など）。
- [ヘルスチェックポート（Healthcheck Port）]：ドロップダウンリストから値を選択します（65534 など）。



ステップ 7 [プロパティ（Properties）] セクションでゲートウェイの詳細を入力します。[セキュリティ（Security）] フィールドは、デフォルトで [水平方向および出力（East-West & Egress）] に設定されます。

- [FTDバージョン（FTD Version）]：7.6 以降のサポートされているバージョンを選択します。
- [ポリシールールセット（Policy Ruleset）]：cdFMC アカウントですでに作成したアクセス コントロール ポリシーを選択するか、新しいアクセス コントロール ポリシーを作成します。たとえば Default Access Control Policy のように指定します。
- [管理者パスワード（Admin Password）] を入力します。入力したパスワードがパスワード要件を満たしていることを確認します。
- [ライセンスモデル（License Model）]：スマートライセンシングまたは Multicloud Defense を選択します。スマートライセンシングは既存の FTDv ライセンシングモデルであり、Multicloud Defense ライセンシングモデルは時間ベースのライセンスモデルです。
- [パフォーマンス階層（Performance Tier）]：ドロップダウンリストから階層を選択します（FTDv50 など）。

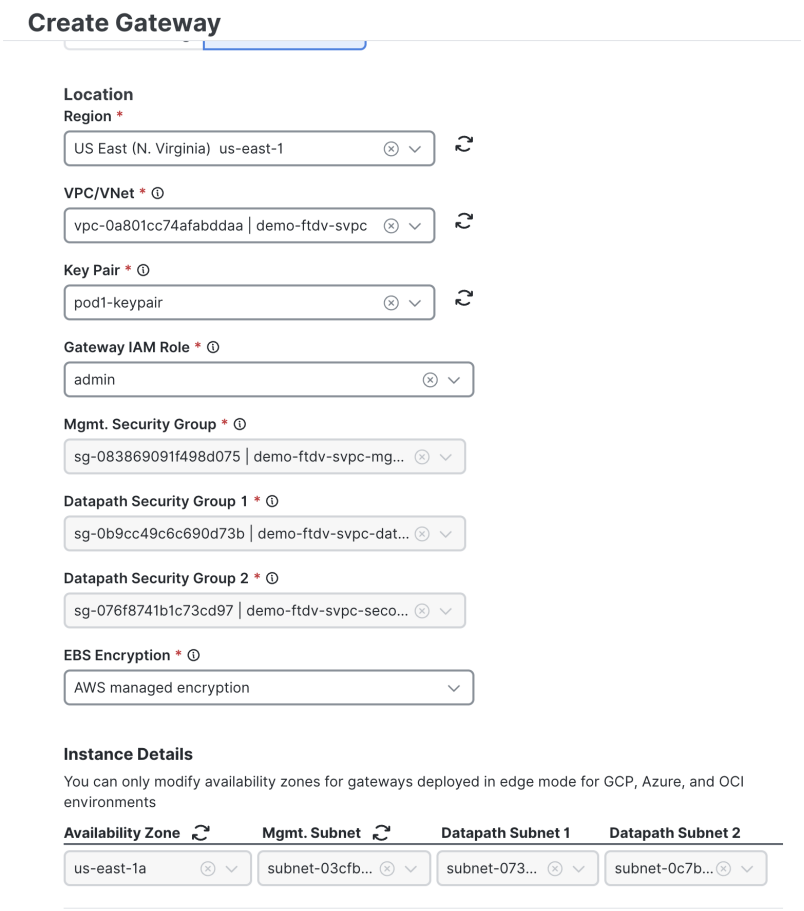
- [ライセンスタイプ（License Type）]：ドロップダウンリストからライセンスタイプを選択します（Base など）。必要に応じて、複数のライセンスタイプを選択できます。
- [地域（Region）]：FTDv を展開する地域を選択します（米国東部（N. バージニア）us-east-1 など）。



ステップ 8　次の [プロパティ（Properties）] セクションで、追加のゲートウェイの詳細を入力します。

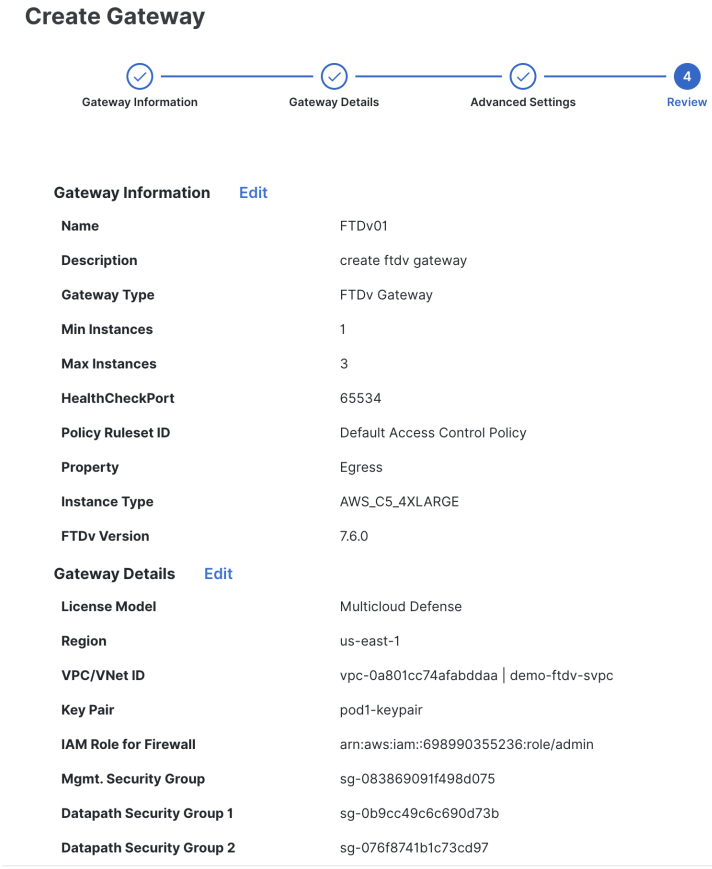
- [VPC/VNet]：ドロップダウンリストから値を選択します。**[インフラストラクチャ（Infrastructure）]** > > **[ゲートウェイ（Gateways）]** > > **[VPC/VNet（VPC/VNets）]** > で VPC または VNet を作成できます。
- [キーペア（Key Pair）]：ドロップダウンリストから、このインスタンスにアタッチするキーペアを選択します（pod1-keypair など）。
- [ゲートウェイIAMロール（Gateway IAM Role）]：ドロップダウンリストからロールを選択します（admin など）。
- [管理セキュリティグループ（Mgmt. Security Group）]：ドロップダウンリストからセキュリティグループを選択します。

- [データパスセキュリティグループ1（Datapath Security Group 1）]：ドロップダウンリストからセキュリティグループを選択します。
- [データパスセキュリティグループ2（Datapath Security Group 2）]：ドロップダウンリストからセキュリティグループを選択します。
- [EBS暗号化（EBS Encryption）]：ドロップダウンリストから暗号化を選択します（AWS管理による暗号化など）。
- [インスタンスの詳細（Instance Details）]。一覧表示されているインスタンスの詳細を表示して確認します。



ステップ 9 [詳細設定（Advanced Settings）] セクションで、トグルを使用して [パブリックIP（Public IP）] を有効または無効にします。

ステップ 10 入力した情報を確認します。



ステップ 11 確認が完了したら、[完了（Finish）] をクリックします。

ゲートウェイが正常に作成され、指定した VPC の AWS アカウントで FTDv の展開が開始されます。FTDv がクラウド サービス プロバイダー アカウントに展開されるまでに約 30 分かかります。FTDv が稼働中になると、FTDv は cdFMC にもオンボードされます。FTDv は ENABLING 状態から ACTIVE PENDING 状態になり、その後 ACTIVE 状態に移行します。

クラウド提供型 Firewall Management Center での Firewall Threat Defense Virtual デバイスへのアクセス

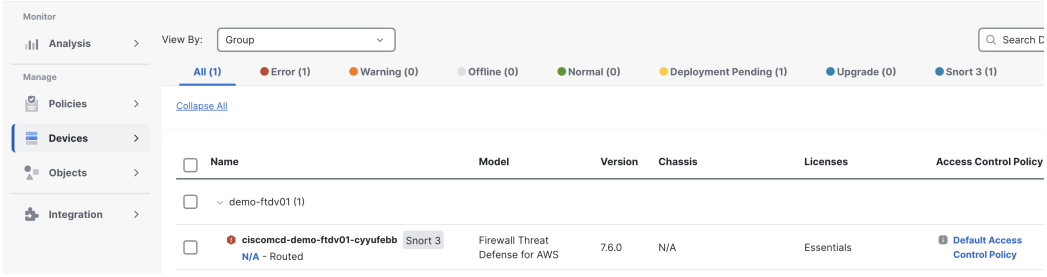
FTDv デバイスがアクティブになると、Multicloud Defense は、テナントに関連付けられている cdFMC に対して FTDv デバイスのオンボーディングを開始します。

手順

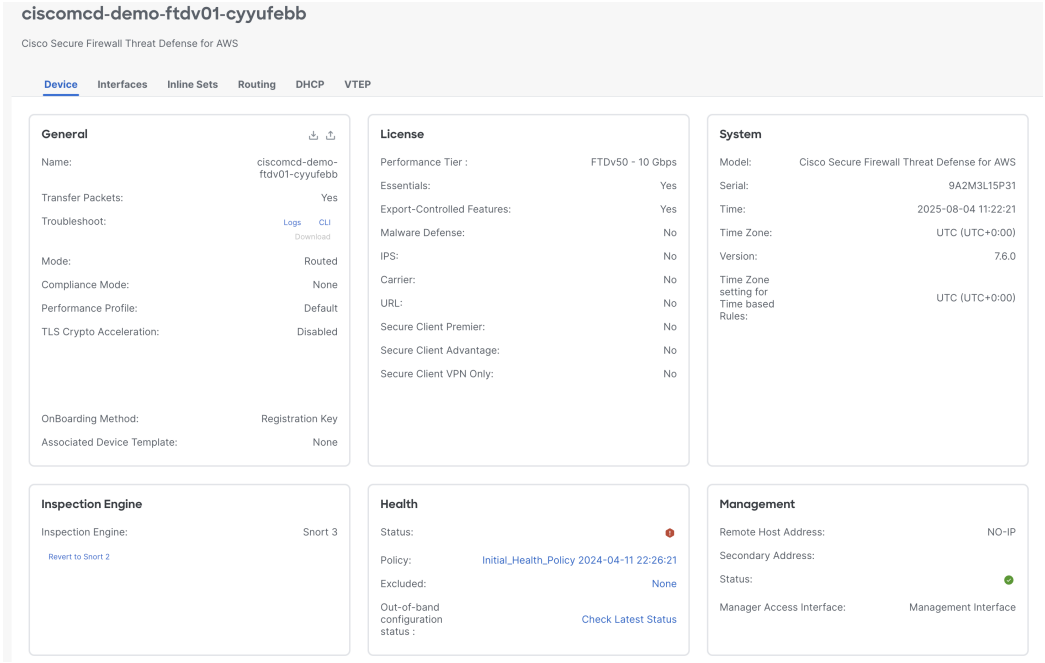
ステップ 1 [Security Cloud Control] メニューから、[管理（Administration）]>[統合（Integrations）]>[Firewall Management Center] に移動し、[クラウド提供型FMCの有効化（Enable Cloud-Delivered FMC）] をクリックします。

ステップ 2 [デバイス（Device）] [管理（Management）] に移動します。

ステップ 3 デバイスグループの下に、オンボードされた FTDv デバイスを表示できます。FTDv デバイス用に、内部インターフェイス、外部インターフェイス、VNI インターフェイス、セキュリティゾーン、およびルーティングが事前設定されています。



[デバイス（Device）]ページから、ネットワーク インターフェイス、セキュリティゾーン、アクセス コントロール ポリシー、プラットフォーム設定などの設定が行われていることを確認できます。すべての詳細を表示できますが、編集はできません。



Multicloud Defense で FTDv デバイスにポリシーをアタッチすると、cdFMC 内からルールやポリシーの書き込みなどのポリシー管理アクティビティを実行できるようになります。

- Multicloud Defense は、cdFMC への FTDv の展開やオンボーディングを実施し、正常性やトラフィックに基づいて、インターフェイスの設定、基本的なアクセス コントロール ポリシーのアタッチ、インスタンスのスケールインとスケールアウトなどの基本的な設定を行います。
- クラウド提供型 Firewall Management Center は、ポリシー設定、ポリシー管理、およびポリシーに関するアクセスコントロールルールに対応します。
- Security Cloud Control は、ログとイベントのビューを提供します。

Security Cloud Control での Firewall Threat Defense Virtual のトラフィックログの表示

Security Cloud Control で、[イベントとログ（Events & Logs）] > [イベントロギング（Event Logging）] に移動します。FTDv デバイスのトラフィックログを表示できます。

Multicloud Defense での Cisco Secure Firewall Threat Defense Virtual の障害対応

発生する可能性のある一般的な問題を回避するために、次の点を考慮する必要があります。

- ポリシーを変更するたびに、そのポリシーを使用するすべての FTDv インスタンスに変更を展開してください。
- インスタンスを手動でデバイスグループに追加したりデバイスグループから削除したりしないでください。
- HTTP 関連のプラットフォーム設定は編集しないでください。
- BYOL ライセンスの場合、オートスケーリングシナリオを計画し、パフォーマンス階層およびライセンス機能を把握して、スマート ライセンス アカウントを確認します。
- クラウド サービス プロバイダー アカウントで Multicloud Defense によって直接管理される設定を編集しないでください。
- クラウド サービス プロバイダーからの FTDv インスタンスは停止しないでください。Multicloud Defense は、これらのインスタンスを障害が発生しているインスタンスと見なし、新しいインスタンスに置き換えます。

サポートについては、Cisco Technical Assistance Center（TAC） にお問い合わせください。

Multicloud Defense での Firewall Threat Defense Virtual の追加リソース

以下の追加リソースを使用して、Multicloud Defense での Firewall Threat Defense Virtual の詳細を確認してください。

- Cisco Secure Firewall Threat Defense Virtual
- Create an FTDv Gateway
- Manage Multicloud Defense-Onboarded Secure Firewall Threat Defense Virtual Devices
- FTDv Orchestration by Multicloud Defense Controller に関するビデオ

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。