

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

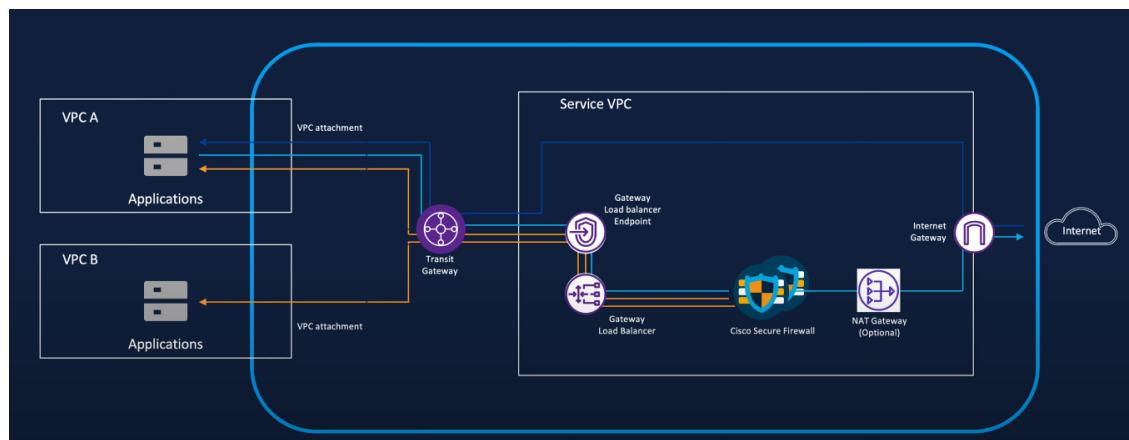
Multicloud Defense で Firewall Threat Defense Virtual を設定するためのワークフロー

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

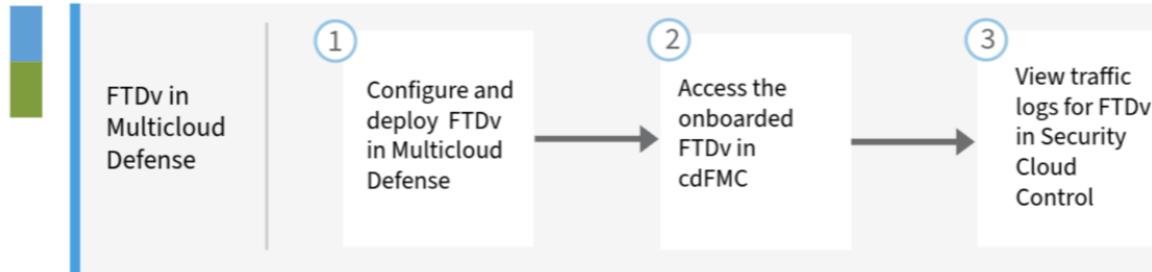
次のイメージは、出力/水平方向のユースケースで、Multicloud Defense のクラウド提供型 Firewall Management Center によって管理される AWS FTDv のオーケストレーションを示しています。



process_workflow

イメージに示された VPCA および VPCB 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 VPCA および VPCB 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。

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

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。

Name	State	Version	Policy Rule Status	Security	Mode
demo-ftdv01	ACTIVE	7.6.0	Updated	East-West & Egress	HUB
pod1-egress-gw-aws	ACTIVE	24.06-14	Updated	East-West & Egress	HUB
pod1-egress-gw-azure	ACTIVE	24.06-14	Updated	East-West & Egress	HUB
pod1-ingress-gw-aws	ACTIVE	24.06-14	Updated	Ingress	HUB
pod1-ingress-gw-azure	ACTIVE	24.06-14	Updated	Ingress	HUB
pod39-egress-gw-aws	ACTIVE	24.06-14	Updated	East-West & Egress	HUB
pod39-ingress-gw-aws	ACTIVE	24.06-14	Updated	Ingress	HUB

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)。

Create Gateway

1 Gateway Information 2 Gateway Details 3 Advanced Settings 4 Review

Properties

Accounts * ①

cisco-multicloud-defense-aws01

Gateway Type *

FTDv Gateway

Name * ①

FTDv01

Description

Create an ftdv gateway

Instance Type * ①

16 Virtual CPU | AWS_C5_4XLARGE

Minimum Instances * ①

1

Maximum Instances * ①

3

HealthCheck Port * ①

65534

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。
- [ライセンスマodel (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マodel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)。

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

- [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)。

Create Gateway



Properties

Security * ⓘ
East-West & Egress

FTDv Version *
7.6.0

Policy Ruleset * ⓘ
Default Access Control Policy

FTDv

Admin Password
**** Show

Password Requirements:
Must be between 12 and 72 characters long
Use lowercase and uppercase characters, and numbers
At least one special character (excluding \ and -)
No more than 2 repeating or sequential characters

License Model ⓘ
Smart Licensing Multicloud Defense

Performance Tier * ⓘ
FTDv50

License Types * ⓘ
Base Search licenses

Location

Region *
US East (N. Virginia) us-east-1

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。

Create Gateway

Location

Region *

US East (N. Virginia) us-east-1

VPC/VNet * ⓘ

vpc-0a801cc74afabddaa | demo-ftdv-svpc

Key Pair * ⓘ

pod1-keypair

Gateway IAM Role * ⓘ

admin

Mgmt. Security Group * ⓘ

sg-083869091f498d075 | demo-ftdv-svpc-mg...

Datapath Security Group 1 * ⓘ

sg-0b9cc49c6c690d73b | demo-ftdv-svpc-dat...

Datapath Security Group 2 * ⓘ

sg-076f8741b1c73cd97 | demo-ftdv-svpc-seco...

EBS Encryption * ⓘ

AWS managed encryption

Instance Details

You can only modify availability zones for gateways deployed in edge mode for GCP, Azure, and OCI environments

Availability Zone ⓘ	Mgmt. Subnet ⓘ	Datapath Subnet 1	Datapath Subnet 2
us-east-1a	subnet-03cfb... ⓘ	subnet-073... ⓘ	subnet-0c7b... ⓘ

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。

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

Create Gateway

Public IP

 Disable Public IP

ステップ 10 入力した情報を確認します。

Create Gateway



Gateway Information [Edit](#)

Name	FTDv01
Description	create ftdv gateway
Gateway Type	FTDv Gateway
Min Instances	1
Max Instances	3
HealthCheckPort	65534
Policy Ruleset ID	Default Access Control Policy
Property	Egress
Instance Type	AWS_C5_4XLARGE
FTDv Version	7.6.0

Gateway Details [Edit](#)

License Model	Multicloud Defense
Region	us-east-1
VPC/VNet ID	vpc-a0801cc74afabddaa demo-ftdv-svpc
Key Pair	pod1-keypair
IAM Role for Firewall	arn:aws:iam::698990355236:role/admin
Mgmt. Security Group	sg-083869091f498d075
Datapath Security Group 1	sg-0b9cc49c6c690d73b
Datapath Security Group 2	sg-076f8741b1c73cd97

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。

The screenshot shows the 'Devices' section of the Cisco Cloud Security Management interface. The left sidebar includes 'Monitor', 'Analysis', 'Manage' (selected), 'Policies', 'Devices' (selected), 'Objects', and 'Integration'. The main area displays a table of devices. The table columns are 'Name', 'Model', 'Version', 'Chassis', 'Licenses', and 'Access Control Policy'. A search bar at the top right is labeled 'Search D'. The device list shows one entry: 'demo-ftdv01 (1)' under 'Name', 'Snort 3' under 'Model', '7.6.0' under 'Version', 'N/A' under 'Chassis', 'Essentials' under 'Licenses', and 'Default Access Control Policy' under 'Access Control Policy'. A status indicator 'Error (1)' is shown above the device list.

[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。

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

The screenshot shows the configuration page for a Cisco Secure Firewall Threat Defense Virtual device. The device name is 'ciscoacd-demo-ftdv01-cyyufebb'. The General section includes fields like Name, Transfer Packets, Troubleshoot, Mode, Compliance Mode, Performance Profile, TLS Crypto Acceleration, OnBoarding Method, and Associated Device Template. The License section lists various features and their status. The System section provides device details like Model, Serial, Time, Time Zone, Version, and Time Zone setting for Time based Rules. The Inspection Engine section shows the selected engine as Snort 3. The Health section displays the status, policy (Initial_Health_Policy), excluded items, and out-of-band configuration status. The Management section shows remote host and secondary addresses, status, and manager access interface.

General		License		System	
Name:	ciscoacd-demo-ftdv01-cyyufebb	Performance Tier :	FTDv50 - 10 Gbps	Model:	Cisco Secure Firewall Threat Defense for AWS
Transfer Packets:	Yes	Essentials:	Yes	Serial:	9A2M3L15P31
Troubleshoot:	Logs, CLI, Downloaded	Export-Controlled Features:	Yes	Time:	2025-08-04 11:22:21
Mode:	Routed	Malware Defense:	No	Time Zone:	UTC (UTC+0:00)
Compliance Mode:	None	IPS:	No	Version:	7.6.0
Performance Profile:	Default	Carrier:	No	Time Zone setting for Time based Rules:	UTC (UTC+0:00)
TLS Crypto Acceleration:	Disabled	URL:	No		
OnBoarding Method:	Registration Key	Secure Client Premier:	No		
Associated Device Template:	None	Secure Client Advantage:	No		
		Secure Client VPN Only:	No		
Inspection Engine		Health		Management	
Inspection Engine:	Snort 3	Status:	●	Remote Host Address:	NO-IP
Revert to Snort 2		Policy:	Initial_Health_Policy 2024-04-11 22:26:21	Secondary Address:	
		Excluded:	None	Status:	●
		Out-of-band configuration status:	Check Latest Status	Manager Access Interface:	Management Interface

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

© 2025 Cisco Systems, Inc. All rights reserved.

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。