Firepower Threat Defense Virtual と Google Cloud Platform の利用開始

Firepower Threat Defense Virtual（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、ワークロードを把握します。

この章では、Google Cloud Platform（GCP）環境内における Firepower Threat Defense Virtual の機能について解説し、機能のサポート、システム要件、ガイドライン、制限事項などを説明します。また、この章では FTDv を管理するため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 を使用できます。

GCP への FTDv の展開について

Firepower Threat Defense Virtual（FTDv）は、物理的な Cisco FTD と同じソフトウェアを実行して、仮想フォームファクタにおいて実証済みのセキュリティ機能を提供します。FTDvは、パブリック GCP に展開できます。その後設定を行うことで、時間の経過とともにロケーションを展開、契約、またはシフトする仮想および物理データセンターのワークロードを保護できます。

GCP マシンタイプのサポート

FTDv のニーズに合わせて Google 仮想マシンのタイプとサイズを選択します。現在、FTDv は、コンピューティング最適化された汎用マシンの標準タイプ、ハイメモリマシンタイプ、および高 CPU マシンタイプのいずれもサポートしています。

（注） サポートされるマシンタイプは、予告なく変更されることがあります。

表 *1:* サポートされるコンピューティング最適化マシンタイプ

コンピューティング最適化マシンタイプ	属性	
	vCPU	**RAM（GB）**
c2-standard-4	4	16 GB
c2-standard-8	8	32 GB
c2-standard-16	16	64 GB

表 *2:* サポートされる汎用マシンタイプ

汎用マシンタイプ	属性	
	vCPU	**RAM（GB）**
n1-standard-4	4	15
n1-standard-8	8	30
n1-standard-16	16	60
n2-standard-4	4	16
n2-standard-8	8	32
n2-standard-16	16	64
n1-highcpu-8	8	7.2
n1-highcpu-16	16	14.4
n2-highcpu-8	8	8
n2-highmem-4	4	32
n2-highmem-8	8	64
n2-highmem-16	16	128

- FTDv には、少なくとも 4 つのインターフェイスが必要です。
- サポートされる vCPU の最大数は 16 です。

ユーザーは、GCP でアカウントを作成し、GCP Marketplace の Cisco Firepower NGFW 仮想ファイアウォール（NGFWv）製品を使用して VM インスタンスを起動し、GCP マシンタイプを選択します。

FTDv と GCP の前提条件

- https://cloud.google.com で GCP アカウントを作成します。
- GCP プロジェクトを作成します。Google ドキュメントの『Creating Your Project』を参照してください。
- Cisco スマートアカウント。Cisco Software Central（https://software.cisco.com/）で作成できます。
- Firepower Threat Defense Virtual へのライセンス付与。
  - Firepower 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。
  - ライセンスを管理する方法の詳細については、『Firepower Management Center Configuration Guide』の「*Licensing the Firepower System*」を参照してください。
- インターフェイスの要件：
  - 管理インターフェイス（2）：1 つは Firepower Threat Defense Virtual を Firepower Management Center に接続するために使用されます。もう 1 つは診断目的に使用され、通過トラフィックには使用できません。
  - トラフィック インターフェイス（2）：Firepower Threat Defense Virtual を内部のホストおよびパブリック ネットワークに接続するために使用されます。
- 通信パス：
  - Firepower Threat Defense Virtual にアクセスするためのパブリック IP。
- FTDv のシステム要件については、『Cisco Firepower Compatibility Guide』を参照してください。

FTDv と GCP のガイドラインおよび制限事項

サポートされる機能

- GCP Compute Engine での展開
- インスタンスあたり最大 16 個の vCPU
- ルーテッド モード（デフォルト）
- ライセンス：BYOL のみをサポート
- Firepower Management Center サポートのみ。

FTDv スマートライセンスのパフォーマンス階層

FTDv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。

表 *3: FTDv* 権限付与に基づくライセンス機能の制限

パフォーマンス階層	デバイス仕様（コア/RAM）	レート制限（Rate Limit）	RA VPN セッション制限
FTDv5、100Mbps	4 コア/8 GB	100Mbps	50
FTDv10、1Gbps	4 コア/8 GB	1Gbps	250
FTDv20、3Gbps	4 コア/8 GB	3 Gbps	250
FTDv30、5Gbps	8 コア/16 GB	5 Gbps	250
FTDv50、10Gbps	12 コア/24 GB	10 Gbps	750
FTDv100、16 Gbps	16 コア/32 GB	16 Gbps	10,000

FTDv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 Configuration Guide*』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FTDvデバイスの電源をオフにする必要があります。

サポートされない機能

- IPv6
- FTDv ネイティブ HA
- 自動スケール
- トランスペアレント/インライン/パッシブ モード
- ジャンボ フレーム

GCP 上の FTDv のネットワークトポロジの例

次の図は、FTDv 用に 4 つのサブネット（管理、診断、内部、外部）が GCP 内に設定されたルーテッド ファイアウォール モードの FTDv の推奨トポロジを示しています。

図 *1 : GCP* 展開での *FTDv* の例