Google Cloud Platform への Firepower Management Center Virtual の展開

最終更新日:2020 年 12 月 13 日

Google Cloud Platform(GCP)上で FMCv を展開できます。GCP は、Google が提供する可用性の高いホスト環境でアプリケーションを実行できるパブリック クラウド コンピューティング サービスです。

FMCv の展開と GCP について

Cisco Firepower Management Center Virtual(FMCv)は、物理の Cisco FMC 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。FMCv は、パブリック GCP に展開できます。その後、仮想 Firepower デバイスおよび物理 Firepower デバイスを管理するように設定できます。

GCP マシンタイプのサポート

FMCv は、コンピューティング最適化された汎用マシンのハイメモリマシンタイプ、および高 CPU マシンタイプの両方をサポートしています。FMCv は、次の GCP マシンタイプを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-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-8	8	30 GB
n1-standard-16	16	60 GB
n1-highmem-8	8	52 GB
n1-highmem-16	16	104 GB
n1-highcpu-32	32	28.8 GB
n2-standard-8	8	32 GB
n2-standard-16	16	64 GB
n2-highmem-4	4	32 GB
n2-highmem-8	8	64 GB
n2-highcpu-32	32	32 GB

GCP での FMCv の前提条件

- https://cloud.google.com で GCP アカウントを作成します。
- 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 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：Firepower デバイスを Firepower Management Center に接続するために使用されるインターフェイス。
- 通信パス：
  - Firepower Management Center Virtual にアクセスするためのパブリック IP。
- Firepower Management Center Virtual と Firepower System の互換性については、『Cisco Firepower Compatibility』を参照してください。

FMCv 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 8 つの vCPU
- ライセンス：BYOL のみをサポート

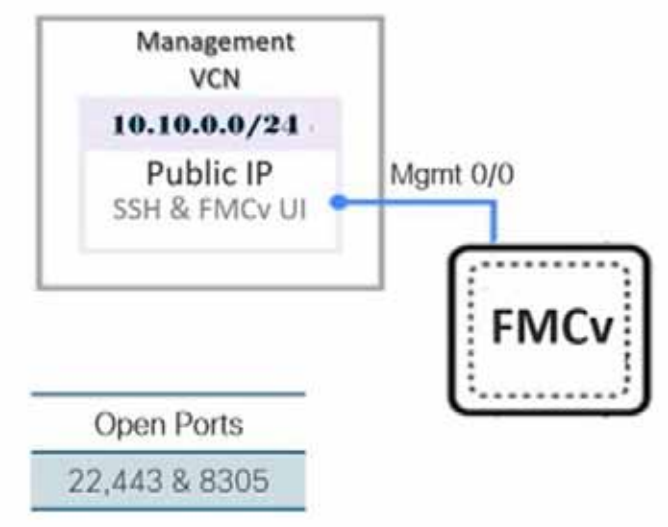
サポートされない機能

- IPv6
- FMCv 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
- マルチ コンテキスト モード

GCP での FMCv のネットワークトポロジ

図 1(3 ページ)に、GCP でサブネットが 1 つ設定された FMCv の推奨トポロジを示します。

図 1　GCP での FMCv 展開のトポロジ例



GCP への FMCv の展開

次の手順では、GCP 環境を準備し、FMCv インスタンスを起動する方法について説明します。

VPC ネットワークの作成

FMCv の展開には、管理サブネット用の管理 VPC が必要です。図 1(3 ページ)をガイドとして参照してください。

手順

1. GCP コンソールで、[VPC ネットワーク(VPC networks)] を選択し、[VPC ネットワークの作成(Create VPC Network)] をクリックします。
2. [名前(Name)] フィールドに、VPC ネットワークを記述する名前を入力します。
3. サブネット作成モードで、[カスタム(Custom)] をクリックします。
4. 新しいサブネットで [名前(Name}] フィールドに、特定の名前を入力します。

5. [地域(Region)] ドロップダウンリストから、展開に適した地域を選択します。
6. [IP アドレス範囲(IP address range)] フィールドで、最初のネットワークのサブネットを CIDR 形式(10.10.0.0/24 など)で入力します。
7. その他すべての設定はデフォルトのままで、[作成(Create)] をクリックします。

GCP での FMCv インスタンスの作成

次の手順に従って、GCP コンソールから FMCv インスタンスを展開できます。

手順

1. GCP コンソールにログインします。
2. ナビゲーションメニューの [マーケットプレイス(Marketplace)] をクリックします。
3. [マーケットプレイス(Marketplace)] で「Cisco Firepower Management Center Virtual(FMCv)BYOL」を検索し、製品を選択します。
4. [作成(Launch)] をクリックします。
   a. [展開名(Deployment name)]: インスタンスの一意の名前を指定します。
   b. [イメージバージョン(Image version)]: ドロップダウンリストからバージョンを選択します。
   c. [ゾーン(Zone)]: FMCv を展開するゾーンを選択します。
   d. [マシンタイプ(Machine type)]: GCP マシンタイプのサポート(1 ページ)に基づいて正しいマシンタイプを選択します。
   e. **[SSH キー(SSH key)](オプション)**: SSH キーペアから公開キーを貼り付けます。

      キーペアは、GCP が保存する公開キーと、ユーザが保存する秘密キーファイルで構成されます。これらを一緒に使用すると、インスタンスに安全に接続できます。キーペアはインスタンスへの接続に必要となるため、必ず既知の場所に保存してください。
   f. このインスタンスにアクセスするためのプロジェクト全体の SSH キーをブロックするか許可するかを選択します。Google ドキュメント『Allowing or blocking project-wide public SSH keys from a Linux instance』を参照してください。
   g. [起動スクリプト(Startup script)]: FMCv の day0 構成を指定します。

      次に、[起動スクリプト(Startup script)] フィールドにコピーして貼り付ける day0 構成の例を示します。

      ```
      {
      "Hostname": "cisco-fmcv",
      "AdminPassword": "myPassword@123456"
      }
      ```

      ヒント: 実行エラーを防ぐには、JSON 検証ツールを使用して day0 構成を検証する必要があります。
   h. ドロップダウンリストから [起動ディスクの種類(Boot disk type)] を選択します。

      デフォルトでは、[標準の永続ディスク(Standard Persistent Disk)] が選択されています。デフォルトの起動ディスクの種類を使用することを推奨します。
   i. [起動ディスクのサイズ(GB 単位)(Boot disk size in GB)] のデフォルト値は 250 GB です。シスコでは、デフォルトの起動ディスクのサイズを維持することを推奨しています。250 GB 未満にすることはできません。
   j. 管理インターフェイスを設定するには、[ネットワークインターフェイスの追加(Add network interface)] をクリックします。

(注) インスタンスを作成した後では、インスタンスにインターフェイスを追加できません。不適切なインターフェイス構成でインスタンスを作成した場合は、インスタンスを削除し、適切なインターフェイス構成で再作成する必要があります。

- [ネットワーク(Network)] ドロップダウンリストから、[VPC network(VPC ネットワーク)](*vpc-branch-mgmt* など)を選択します。
- [外部 IP(External IP)] ドロップダウンリストから、適切なオプションを選択します。

  管理インターフェイスには、[外部 IP からエフェメラルへ(External IP to Ephemeral)] を選択します。
- [完了(Done)] をクリックします。

k. [Firewall(ファイアウォール)]:ファイアウォールルールを適用します。

- [インターネットからの TCP ポート 22 のトラフィックを許可する(SSH アクセス)(Allow TCP port 22 traffic from the Internet (SSH access))] チェックボックスをオンにして、SSH を許可します。
- [インターネットからの HTTPS トラフィックを許可する(FMC GUI)(Allow HTTPS traffic from the Internet (FMC GUI))] チェックボックスをオンにして、HTTPS 接続を許可します。
- [インターネットからの TCP ポート 8305 のトラフィックを許可する(SFT トンネル通信)] チェックボックスをオンにして、FMCv および管理対象デバイスが双方向の SSL 暗号化通信チャネルを使用して通信できるようにします。

l. [詳細(More)] をクリックしてビューを展開し、[IP 転送(IP Forwarding)] が [オン(On)] に設定されていることを確認します。

5. [展開(Deploy)] をクリックします。

   GCP コンソールの [VM インスタンス(VM instance)] ページからインスタンスの詳細を表示します。インスタンスを停止および開始するための内部 IP アドレス、外部 IP アドレス、およびコントロールが表示されます。編集する場合は、インスタンスを停止する必要があります。

GCP での FMCv インスタンスへのアクセス

SSH(ポート 22 経由の TCP 接続)を許可するファイアウォールルールがすでに作成されていることを確認します。

このファイアウォールルールにより、FMCv インスタンスへのアクセスが可能になり、次の方法を使用してインスタンスに接続できます。

- 外部 IP
  - ブラウザ ウィンドウ
  - その他の SSH クライアントまたはサードパーティ製ツール
- シリアル コンソール
  - Gcloud コマンドライン

詳細については、Google のドキュメント『インスタンスへの接続(Connecting to instances)』を参照してください。

注: Day0 構成を追加しない場合は、デフォルトのログイン情報を使用して FMCv インスタンスにログインできます。最初のログイン試行時にパスワードを設定するように求められます。

外部 IP を使用した FMCv インスタンスへの接続

FMCv インスタンスには、内部 IP と外部 IP が割り当てられます。外部 IP を使用して FMCv インスタンスにアクセスできます。

手順

1. GCP コンソールで、[コンピューティングエンジン(Compute Engine)] > [VM インスタンス(VM instances)] を選択します。
2. FMCv のインスタンス名をクリックすると、[VM インスタンスの詳細(VM instance details)] ページが開きます。
3. [詳細(Details)] タブで、[SSH] フィールドのドロップダウンメニューをクリックします。
4. [SSH] ドロップダウンメニューから、目的のオプションを選択します。

   次の方法を使用して FMCv インスタンスに接続できます。

   - ブラウザウィンドウ:カスタムポートのブラウザウィンドウでインスタンスを開くことも、指定された秘密 SSH キーを使用してインスタンスを開くこともできます。詳細については、Google のドキュメント『SSH from the browser』を参照してください。
   - その他の SSH クライアントまたはサードパーティ製ツール:詳細については、Google のドキュメント『サードパーティ製ツールを使用した接続(Connecting using Third-party tools)』を参照してください。

シリアルコンソールを使用した FMCv インスタンスへの接続

手順

1. GCP コンソールで、[コンピューティングエンジン(Compute Engine)] > [VM インスタンス(VM instances)] を選択します。
2. FMCv のインスタンス名をクリックすると、[VM インスタンスの詳細(VM instance details)] ページが開きます。
3. [詳細(Details)] タブで、[シリアルコンソールへの接続(Connect to serial console)] をクリックします。

   詳細については、Google のドキュメント『シリアルコンソールとのやり取り(Interacting with the serial console)』を参照してください。

Gcloud を使用した FMCv インスタンスへの接続

手順

1. GCP コンソールで、[コンピューティングエンジン(Compute Engine)] > [VM インスタンス(VM instances)] を選択します。
2. FMCv のインスタンス名をクリックすると、[VM インスタンスの詳細(VM instance details)] ページが開きます。
3. [詳細(Details)] タブで、[SSH] フィールドのドロップダウンメニューをクリックします。
4. [gcloud コマンドを表示(View gcloud command)] > [Cloud Shell で実行(Run in Cloud Shell)] をクリックします。

   [Cloud Shell] ターミナルウィンドウが開きます。詳細については、Google のドキュメント『gcloud command-line tool overview』、および『gcloud compute ssh』を参照してください。