Google Cloud Platform への ASAv の展開

Google Cloud Platform（GCP）に ASAv を導入できます。

- GCP への ASAv の展開について （1 ページ）
- ASAv と GCP の前提条件 （3 ページ）
- ASAv および GCP のガイドラインと制限事項 （3 ページ）
- GCP 上の ASAv のネットワークトポロジの例 （4 ページ）
- Google Cloud Platform への ASAv の展開 （5 ページ）
- GCP 上の ASAv インスタンスへのアクセス （9 ページ）
- CPU 使用率とレポート （11 ページ）

GCP への ASAv の展開について

GCP を使用すると、Google と同じインフラストラクチャでアプリケーション、Web サイト、サービスを構築、展開、および拡張できます。

ASAvは、物理ASA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。ASAv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

ASAv 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。

ASAv は、次の汎用 *N1*、*N2*、およびコンピューティング最適化 *C2* GCP マシンタイプをサポートしています。

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	**メモリ（GB）**
c2-standard-4	4	16

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

表 *2:* サポートされる汎用マシンタイプ

マシンタイプ	属性	
	vCPU	メモリ（**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-highcpu-16	16	16
n2-highmem-4	4	32
n2-highmem-8	8	64
n2-highmem-16	16	128

- ASAv には、少なくとも 3 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。
- メモリ最適化マシンタイプはサポートされていません。

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

C2 コンピューティング最適化マシンタイプの制限事項

コンピューティング最適化 C2 マシンタイプには、次の制約があります。

- コンピューティング最適化マシンタイプでは、リージョン永続ディスクを使用できません。詳細については、Google のドキュメント「Adding or resizing regional persistent disks」を参照してください。
- 汎用マシンタイプおよびメモリ最適化マシンタイプとは異なるディスク制限が適用されます。詳細については、Google のドキュメント「Block storage performance」を参照してください。
- 一部のゾーンとリージョンでのみ使用できます。詳細については、Google のドキュメント「Available regions and zones」を参照してください。
- 一部の CPU プラットフォームでのみ使用できます。詳細については、Google のドキュメント「CPU platforms」を参照してください。

ASAv 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。
- ASAv へのライセンス付与。ASAv にライセンスを付与するまでは、100 回の接続と 100 Kbps のスループットのみが許可される縮退モードで実行されます。「Licenses: Smart Software Licensing」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：ASDM に ASAv を接続するために使用され、トラフィックの通過には使用できません。
  - 内部インターフェイス：内部ホストに ASAv を接続するために使用されます。
  - 外部インターフェイス：ASAv を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：
  - ASAv にアクセスするためのパブリック IP。
- ASAv システム要件については、Cisco ASA の互換性 [英語] を参照してください。

ASAv および GCP のガイドラインと制限事項

サポートされる機能

GCP 上の ASAv は、次の機能をサポートしています。

- GCP 仮想プライベートクラウド（VPC）への展開
- 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

サポートされない機能

GCP 上の ASAv は、次の機能をサポートしていません。

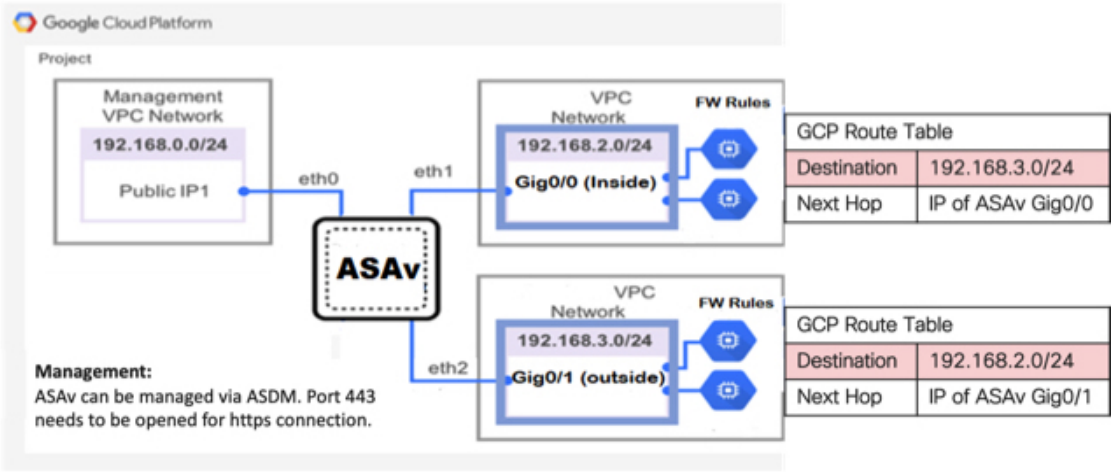
- IPv6
  - インスタンスレベルの IPv6 設定は GCP ではサポートされません
  - ロードバランサだけが IPv6 接続を受け入れて IPv4 経由で GCP インスタンスにプロキシできます
- ジャンボ フレーム
- ASAv ネイティブ HA
- 自動スケール
- トランスペアレント/インライン/パッシブ モード

GCP 上の ASAv のネットワークトポロジの例

次の図は、ASAv 用の 3 つのサブネット（管理、内部、外部）が GCP 内に設定されているルーテッド ファイアウォール モードの ASAv の推奨ネットワークトポロジを示しています。

Google Cloud Platform への ASAv の展開

図 *1 : GCP* 展開での *ASAv* の例



Google Cloud Platform への ASAv の展開

Google Cloud Platform（GCP）に ASAv を導入できます。

VPC ネットワークの作成

始める前に

ASAv の導入では、ASAv を導入する前に 3 つのネットワークを作成する必要があります。ネットワークは次のとおりです。

- 管理サブネットの管理 VPC。
- 内部サブネットの内部 VPC。
- 外部サブネットの外部 VPC。

さらに、ASAv を通過するトラフィックフローを許可するようにルートテーブルと GCP ファイアウォールルールを設定します。ルートテーブルとファイアウォールルールは、ASAv 自体に

設定されているものとは別になっています。関連するネットワークと機能に応じて、GCP ルートテーブルとファイアウォールルールに名前を付けます。「GCP 上の ASAv のネットワークトポロジの例 （4 ページ）」を参照してください。

ステップ 1 GCP コンソールで、**[Networking]** > **[VPC network]** > **[VPC networks]** を選択し、[Create VPC Network] をクリックします。

ステップ 2 [Name] フィールドに、VPC ネットワークのわかりやすい名前を入力します（例：*vpc-asiasouth-mgmt*）。

ステップ 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。

ステップ 4 [New subnet] の [Name] フィールドに、適切な名前を入力します（例：*vpc-asiasouth-mgmt*）。

ステップ 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。3 つのネットワークはすべて同じリージョン内にある必要があります。

ステップ 6 [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。

ステップ 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。

ステップ 8 ステップ 1 ー 7 を繰り返して、VPC の残り 2 つのネットワークを作成します。

ファイアウォールルールの作成

ASAvインスタンスの展開中に（SSHおよびHTTPS接続を許可するために）管理インターフェイスのファイアウォールルールを適用します。GCP 上の ASAv インスタンスの作成 （7 ページ）を参照してください。要件に応じて、内部および外部インターフェイスのファイアウォールルールを作成することもできます。

ステップ 1 GCP コンソールで、**[ネットワーキング（Networking）]** > **[VPC ネットワーク（VPC network）]** > **[ファイアウォール（Firewall）]**を選択し、**[ファイアウォールルールの作成（Create Firewall Rule）]** をクリックします。

ステップ 2 **[名前（Name）]** フィールドに、ファイアウォールルールのわかりやすい名前を入力します（例：*vpc-asiasouth-inside-fwrule*）。

ステップ 3 [Network] ドロップダウンリストから、ファイアウォールルールを作成する VPC ネットワークの名前を選択します（例：*asav-south-inside*）。

ステップ 4 **[ターゲット（Targets）]** ドロップダウンリストから、ファイアウォールルールに適用可能なオプションを選択します（例：**[ネットワーク内のすべてのインスタンス（All instances in the network）]**）。

ステップ 5 **[送信元 IP 範囲（Source IP Ranges）]** フィールドに、送信元 IP アドレスの範囲を CIDR 形式で入力します（例：0.0.0.0/0）。

トラフィックは、これらの IP アドレス範囲内の送信元からのみ許可されます。

ステップ 6 **[プロトコルとポート（Protocols and ports）]** の下で、**[指定されたプロトコルとポート（Specified protocols and ports）]** を選択します。

ステップ 7 セキュリティルールを追加します。

ステップ 8 [作成（Create）] をクリックします。

GCP 上の ASAv インスタンスの作成

以下の手順を実行して、GCP Marketplace から提供される Cisco ASA 仮想ファイアウォール（ASAv）を使用して ASAv インスタンスを導入します。

ステップ 1 GCP コンソールにログインします。

ステップ 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。

ステップ 3 マーケットプレイスで「Cisco ASA virtual firewall (ASAv)」を検索して、製品を選択します。

ステップ 4 [作成（Launch）] をクリックします。

ステップ 5 [Deployment name] でインスタンスの一意の名前を指定します。

ステップ 6 [ゾーン（Zone）] で ASAv を導入するゾーンを選択します。

ステップ 7 [Machine type] で適切なマシンタイプを選択します。サポートされるマシンタイプの一覧については、GCP への ASAv の展開について （1 ページ）を参照してください。

ステップ 8 （オプション）[SSH key (optional)] で 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、ユーザー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。

ステップ 9 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 キーを許可するかブロック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。

ステップ 10 （任意）[起動スクリプト（Startup script）] で ASAv の第 0 日用構成を指定します。day0 構成は、ASAv の初回起動時に適用されます。

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ことができる day0 構成の例を示します。

ASA コマンドの詳細については、『ASA 構成ガイド』および『ASA コマンドリファレンス』を参照してください。

重要 この例からテキストをコピーする場合は、サードパーティのテキストエディタまたは検証エンジンでスクリプトを検証して、形式エラーを防止し、無効な Unicode 文字を削除する必要があります。

```
!ASA Version 9.15.1

interface management0/0

management-only
nameif management
security-level 100
ip address dhcp setroute
no shut
```

```
!
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
!
crypto key generate rsa modulus 2048
ssh 0 0 management
ssh timeout 60
ssh version 2
username admin password cisco123 privilege 15
username admin attributes
service-type admin
! required config end
dns domain-lookup management
dns server-group DefaultDNS
name-server 8.8.8.8
```

ステップ 11 プロビジョニングされるディスク容量についてデフォルトの [Boot disk type] と [Boot disk size in GB] を維持します。

ステップ 12 [Network interfaces] でインターフェイスを設定します。

- 管理
- inside
- outside

（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。

a) **[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-asiasouth-mgmt* など）を選択します。

b) **[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。内部および外部インターフェイスでは、これはオプションです。

c) [完了（Done）] をクリックします。

ステップ 13 [Firewall] で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。
- [Allow HTTPS traffic from the Internet (ASDM access)] チェックボックスをオンにして、HTTPS 接続を許可します。

ステップ 14 **[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。

ステップ 15 [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 上の ASAv インスタンスへのアクセス

展開中に 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有効化されていることを確認します。詳細については、GCP 上の ASAv インスタンスの作成 （7 ページ）を参照してください。

このファイアウォールルールにより、ASAv 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（External IP）
  - 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 ドキュメントの 『Connecting to instances』を参照してください。

（注） 第 0 日用構成で指定したログイン情報を使用するか、インスタンスの起動時に作成した SSH キーペアを使用して、ASAv インスタンスにログインできます。

外部 IP を使用した ASAv インスタンスへの接続

ASAv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ASAvインスタンスにアクセスできます。

ステップ 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。

ステップ 2 ASAv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。

ステップ 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。

ステップ 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ASAvインスタンスに接続できます。

- 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 ドキュメントの「Connecting using third-party tools」を参照してください。

（注） 第 0 日用構成で指定したログイン情報を使用するか、インスタンスの起動時に作成した SSH キーペアを使用して、ASAv インスタンスにログインできます。

SSH を使用した ASAv インスタンスへの接続

UNIX スタイルのシステムから ASAv インスタンスに接続するには、SSH を使用してインスタンスにログインします。

ステップ 1 次のコマンドを使用して、ファイルの権限を設定し、自分だけがファイルを読み取れるようにします。

```
$ chmod 400 <private_key>
```

ここで、

<private_key> は、アクセスするインスタンスに関連付けられた秘密キーを含むファイルのフルパスと名前です。

ステップ 2 インスタンスにアクセスするには、次の SSH コマンドを使用します。

```
$ ssh -i <private_key> <username>@<public-ip-address>
```

ここで、

<private_key> は、アクセスするインスタンスに関連付けられた秘密キーを含むファイルのフルパスと名前です。

<username> は、ASAv インスタンスのユーザー名です。

<public-ip-address> は、コンソールから取得したインスタンスの IP アドレスです。

シリアルコンソールを使用した ASAv インスタンスへの接続

ステップ 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。

ステップ 2 ASAv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。

ステップ 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 ドキュメントの「シリアルコンソールとのやり取り」を参照してください。

Gcloud を使用した ASAv インスタンスへの接続

ステップ 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。

ステップ 2 ASAv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。

ステップ 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。

ステップ 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 ドキュメントの「gcloud コマンドラインツールの概要」、および「gcloud compute ssh」を参照してください。

CPU 使用率とレポート

CPU使用率レポートには、指定された時間内に使用されたCPUの割合の要約が表示されます。通常、コアはピーク時以外には合計 CPU 容量の約 30 ～ 40% で動作し、ピーク時は約 60 ～ 70% の容量で動作します。

ASA Virtual の vCPU 使用率

ASA Virtual の vCPU 使用率には、データパス、制御ポイント、および外部プロセスで使用されている vCPU の量が表示されます。

GCP で報告される vCPU 使用率には、ASA Virtual 使用率に加えて、次のものが含まれます。

- ASA Virtual アイドル時間
- ASA Virtual マシンに使用された %SYS オーバーヘッド
- vSwitch、vNICおよびpNICの間を移動するパケットのオーバーヘッド。このオーバーヘッドは非常に大きくなる場合があります。

CPU 使用率の例

CPU 使用率の統計情報を表示するには、**show cpu usage** コマンドを使用します。

例

```
Ciscoasa#show cpu usage

CPU □□□□5□□□ 1%□1 □□□ 2%□5 □□□ 1%
```

報告された vCPU の使用率が大幅に異なる例を次に示します。

- ASA Virtual レポート：40%
- DP：35%
- 外部プロセス：5%
- ASA（ASA Virtual レポート）：40%
- ASA アイドル ポーリング：10%
- オーバーヘッド：45%

オーバーヘッドは、ハイパーバイザ機能の実行、および vSwitch を使用した NIC と vNIC の間のパケット転送に使用されています。

GCP CPU 使用率レポート

GCP コンソールでインスタンス名をクリックし、[モニタリング（Monitoring）] タブをクリックします。CPU 使用率が表示されます。

Compute Engine では、使用状況エクスポート機能を使用して、Compute Engine の使用状況の詳細レポートを Google Cloud Storage バケットにエクスポートできます。使用状況レポートには、リソースの有効期間に関する情報が表示されます。たとえば、プロジェクト内で `n2-standard-4` マシンタイプを実行している VM インスタンスの数と、各インスタンスの実行時間を確認できます。永続ディスクのストレージスペースや、Compute Engine の他の機能に関する情報も確認できます。

ASA Virtual と GCP のグラフ

ASA Virtual と GCP の間には CPU % の数値に違いがあります。

- GCP グラフの数値は ASA Virtual の数値よりも常に大きくなります。
- GCP ではこの値は「%CPU usage」と呼ばれ、ASA Virtual ではこの値は「%CPU utilization」と呼ばれます。

用語「%CPU utilization」と「%CPU usage」は別のものを意味しています。

- CPU utilization は、物理 CPU の統計情報を提供します。
- CPU usage は CPU のハイパースレッディングに基づいた論理 CPU の統計情報を提供します。しかし、1 つの vCPU のみが使用されるため、ハイパースレッディングは動作しません。

GCP では「%CPU usage」は次のように計算されます。

アクティブに使用された仮想 CPU の量。使用可能な CPU の合計に対する割合として指定されます。

この計算は、ホストから見た CPU 使用率であり、ゲスト オペレーティング システムから見た CPU 使用率ではありません。また、これは仮想マシンで使用可能なすべての仮想 CPU の平均 CPU 使用率になります。

たとえば、1 個の仮想 CPU を搭載した 1 つの仮想マシンが、4 個の物理 CPU を搭載した 1 台のホストで実行されており、その CPU 使用率が 100% の場合、仮想マシンは、1 個の物理 CPU をすべて使用しています。仮想 CPU の使用率は、「MHz 単位の使用率 / 仮想 CPU の数 x コア周波数」として計算されます。

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。