OCI への ASA 仮想 の導入

Oracle Cloud Infrastructure（OCI）に ASA 仮想 を導入できます。

概要

OCI は、オラクル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。

ASA 仮想は、物理 ASA 仮想 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。ASA 仮想 は、パブリック OCI で展開できます。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。

OCI のコンピューティングシェイプ

シェイプは、インスタンスに割り当てられる CPU の数、メモリの量、およびその他のリソースを決定するテンプレートです。ASA 仮想 は、次の「標準：汎用」の OCI シェイプタイプをサポートします。

表 *1 : x86* 展開でサポートされるコンピューティングシェイプ

OCI シェイプ	サポートされている ASAv のバージョン	属性		インターフェイス
		oCPU	RAM（GB）	
インテル VM.DenseIO2.8	9.19 以降	8	120	最小 4、最大 8

OCI シェイプ	サポートされている ASAv のバージョン	属性		インターフェイス
		oCPU	RAM（GB）	
インテル VM.StandardB1.4	9.19 以降	4	48	最小 4、最大 4
インテル VM.StandardB1.8	9.19 以降	4	96	最小 4、最大 8
インテル VM.Standard1.4	9.19 以降	4	28	最小 4、最大 4
インテル VM.Standard1.8	9.19 以降	8	56	最小 4、最大 8
インテル VM.Standard2.4	9.15、9.16、9.17、9.18、9.19、9.20、9.21、および 9.22 以降	4	60	最小 4、最大 4
IntelVM.Standard2.8	9.15、9.16、9.17、9.18、9.19、9.20、9.21、および 9.22 以降	8	120	最小 4、最大 8
インテル VM.Standard3.Flex	9.19 以降	4	16	最小 4、最大 4
	9.19 以降	6	24	最小 4、最大 6
	9.19 以降	8	32	最小 4、最大 8
インテル VM.Optimized3.Flex	9.19 以降	4	16	最小 4、最大 8
	9.19 以降	6	24	最小 4、最大 10
	9.19 以降	8	32	最小 4、最大 10
AMD VM.Standard.E4.Flex	9.19 以降	4	16	最小 4、最大 4
	9.19 以降	6	24	最小 4、最大 6
	9.19 以降	8	32	最小 4、最大 8

表 *2 : ARM* 展開でサポートされるコンピューティングシェイプ

OCI シェイプ	サポートされている ASAv のバージョン	属性		インターフェイス
		oCPU	RAM（GB）	
Ampere VM.Standard.A1.Flex からの Altra プロセッサ	9.24.1 以降	4	8	最小 4、最大 4
	9.24.1 以降	8	16	最小 4、最大 8
	9.24.1 以降	12	24	最小 4、最大 10
	9.24.1 以降	16	32	最小 4、最大 10
Ampere VM.Standard.A2.Flex からの AmpereOne プロセッサ	9.24.1 以降	2	8	最小 4、最大 4
	9.24.1 以降	4	16	最小 4、最大 8
	9.24.1 以降	6	24	最小 4、最大 10
	9.24.1 以降	8	32	最小 4、最大 10

（注） Flex コンピューティングシェーピングを使用することを推奨します。

（注） VM. Standard.A1.Flex シェイプの場合、1 OCPU は 1 vCPU に相当します。

残りのコンピューティングシェイプでは、1 OCPU は 2 vCPU に相当します。

サポートされる vCPU の最大数は 16（8 個の oCPU）です。

Oracle Cloud Infrastructure（OCI）は、次の OCI シェイプタイプで ASA Virtual をサポートします。

- VM.Standard2.4（ASAv5、ASAv10、および ASAv30）
- VM.Standard2.8（ASAv50 および ASAv100）
- ASA 仮想 には、少なくとも 3 つのインターフェイスが必要です。

バージョン ASA 仮想9.19 以降でサポートされている OCI コンピューティングシェイプの使用に関する推奨事項。

- OCI マーケットプレイス イメージ バージョン **9.19.1-v3** 以降は、ASA 仮想 9.19 以降の OCI コンピューティングシェイプとのみ互換性があります。
- ASA 仮想 9.19 以降でサポートされている OCI コンピューティングシェイプは、新しい展開でのみ使用できます。

- OCI コンピューティング シェイプ バージョン **9.19.1-v3** 以降は、ASA 仮想 9.19 より前の OCI コンピューティング シェイプ バージョンを使用して ASA 仮想 で展開された VM をアップグレードすることと互換性がありません。
- インスタンスをシャットダウンした後でも、**VM.DenseIO2.8** コンピューティング シェイプ サブスクリプションの課金は継続されます。詳細については、OCI のドキュメントを参照してください。

ユーザーは、OCI でアカウントを作成し、Oracle Cloud Marketplace の Cisco ASA 仮想ファイアウォール（ASA 仮想）製品を使用してコンピューティング インスタンスを起動し、OCI のシェイプを選択します。

ファームウェアサポート：

デフォルトでは、Threat Defense Virtual インスタンスは UEFI モードを使用して展開されます。

（注） OCI はセキュアブート機能をサポートしていません。

既存のブラウンフィールド展開は、影響なしでバージョン 9.24 にアップグレードできます。展開後の起動モードの変更はサポートされていません。

前提条件

- https://www.oracle.com/cloud/sign-in.html でアカウントを作成します。
- ASA 仮想 へのライセンス付与。ASA 仮想 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。

（注） これまで ASA Virtual 向けにシスコが提供していたすべてのデフォルトのソフトウェア利用資格で IPv6 の設定がサポートされます。

- インターフェイスの要件：
  - 管理インターフェイス
  - 内部および外部インターフェイス
  - （任意）追加のサブネット（DMZ）
- 通信パス：
  - 管理インターフェイス：ASDM に ASA 仮想 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（必須）：内部ホストに ASA 仮想 を接続するために使用されます。
- 外部インターフェイス（必須）：ASA 仮想 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。
- DMZ インターフェイス（任意）：DMZ ネットワークに ASA 仮想 を接続するために使用されます。

- ASA 仮想 システム要件については、Cisco Secure Firewall ASA の互換性 [英語] を参照してください。

注意事項と制約事項

サポートされる機能

OCI 上の ASA 仮想 は、次の機能をサポートしています。

- OCI 仮想クラウドネットワーク（VCN）での展開
- インスタンスあたり最大 16 個の vCPU（8 個の oCPU）
- 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
- Single Root I/O Virtualization（SR-IOV）をサポート
- IPv6

ASA 仮想 スマートライセンスのパフォーマンス階層

ASA 仮想 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。

パフォーマンス階層	インスタンスタイプ（コア/RAM）	レート制限	RA VPN セッション制限
ASAv5	VM.Standard2.4 4 コア/60 GB	100 Mbps	50
ASAv10	VM.Standard2.4 4 コア/60 GB	1 Gbps	250
ASAv30	VM.Standard2.4 4 コア/60 GB	2 Gbps	750

パフォーマンス階層	インスタンスタイプ（コア/RAM）	レート制限	RA VPN セッション制限
ASAv50	VM.Standard2.8 8 コア/120 GB	NA	10,000
ASAv100	VM.Standard2.8 8 コア/120 GB	NA	20,000

サポートされない機能

OCI 上の ASA 仮想 は、次の機能をサポートしていません。

- ASA 仮想 ネイティブ HA
- 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

制限事項

- OCI に ASA 仮想 を展開する場合、Mellanox 5 は SR-IOV モードの vNIC としてサポートされません。
- OCI はデュアルスタックモード（IPv4 および IPv6）設定のみをサポートし、スタンドアロンの IPv6 設定は仮想プライベートネットワーク（VPN）ではサポートされません。
- 静的設定と DHCP 設定の両方で ASAv に必要な個別のルーティングルール。

OCI Ampere A1（ARM）インスタンスの考慮事項

- レガシーハイパーバイザで展開された場合、特に SR-IOV が有効になっている場合、OCI Ampere A1（ARM）インスタンスでスループットが低下する可能性があります。このような展開でパフォーマンスの低下が見られる場合は、サービスリクエストを開いて、Oracle Cloud Infrastructure（OCI）サポートにお問い合わせください。
- OCI チームは、Ampere A1 インスタンスの SR-IOV 対応ネットワークに関する既知の制限事項を文書化しました。詳細については、Oracle Cloud Infrastructure の既知の問題に関するドキュメントを参照してください。

  https://docs.oracle.com/en-us/iaas/Content/Compute/known-issues.htm

- **VM.Standard.A1.Flex インスタンスのネットワーク制限**
  - VM.Standard.A1.Flex シェイプは、準仮想化ネットワーク起動オプションのみをサポートします。
  - ハードウェア支援（SR-IOV）ネットワークで起動されたインスタンスでは、パフォーマンスが低下し、場合によってはデータが破損することがあります。これらの問題を回避するために、Ampere A1 Compute（aarch64）の OCI プラットフォームイメージ

は、準仮想化ネットワークのみを使用するように事前設定されています。インスタンスの作成時にハードウェア支援ネットワークが選択された場合、「インスタンスの起動オプションの検証に失敗しました」のようなエラーメッセージが表示され、起動に失敗します。

- OCI Ampere A1 Compute と互換性のあるカスタムイメージが、SR-IOV が有効になっている状態で正常に起動することがあります。ただし、シスコでは、パフォーマンスおよびデータ完全性に関する問題の発生を防ぐため、ハードウェア支援ネットワークを回避することを強く推奨します。

回避策

プラットフォームイメージを使用して VM.Standard.A1.Flex インスタンスを作成する場合、推奨される準仮想化ネットワーク起動タイプを Oracle が自動的に選択できるようにします。カスタムイメージの場合、ハードウェア支援（SR-IOV）ネットワークは選択しないでください。

アップグレードの制約事項と制限事項

アップグレード復元の制約事項

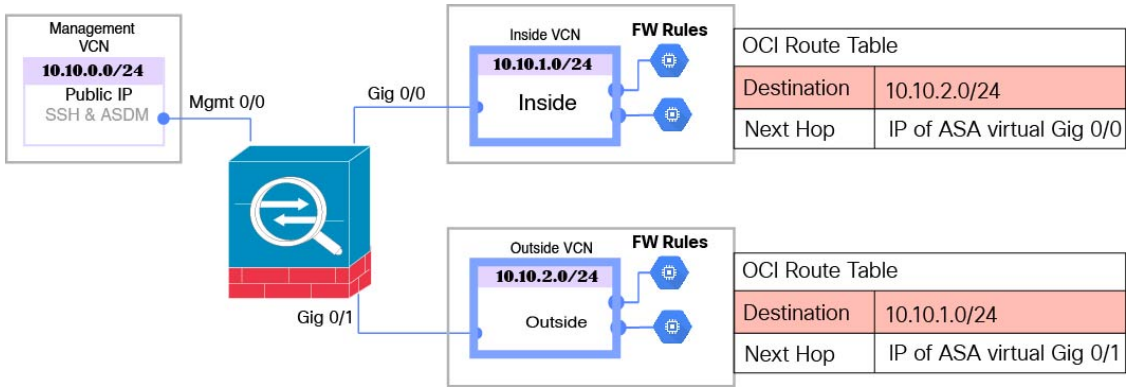
注意 アップグレードの復元はサポートされていません。

アップグレード前に必ずバックアップを作成してください。ASA Virtual 9.24.1 にアップグレードした後、以前のソフトウェアバージョンにロールバックすることはできません。以前のバージョンに戻すには、Management Center を再展開する必要があります。

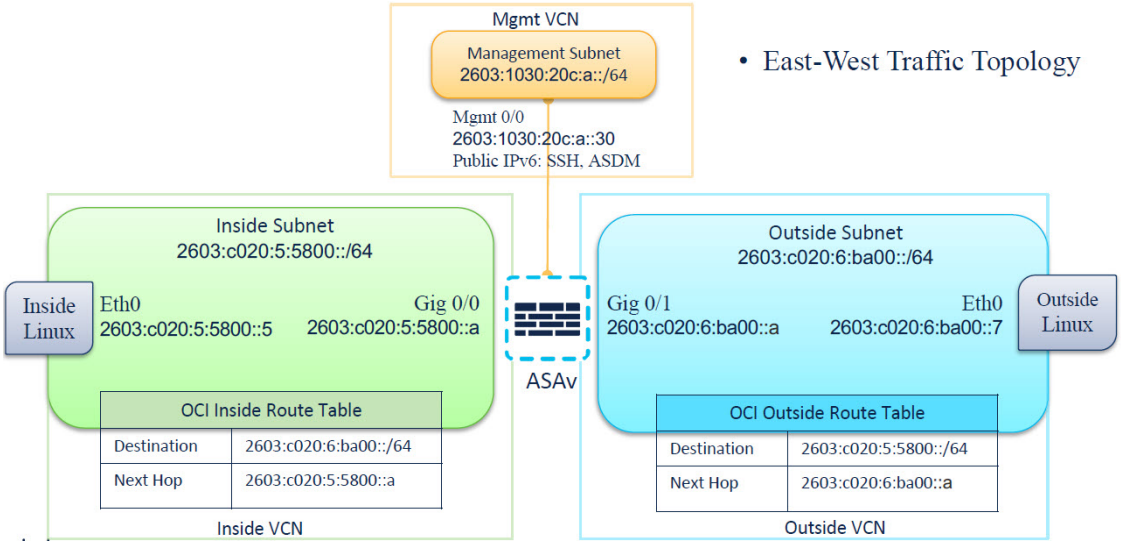
ネットワークトポロジの例

次の図は、ASA 仮想 用の 3 つのサブネット（管理、内部、外部）が OCI 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 ASA 仮想 の推奨ネットワークトポロジを示しています。

図 *1 : OCI* 上の *ASA* 仮想 の展開例



ASA Virtual の IPv6 展開トポロジ



ASA 仮想 の導入

次の手順では、OCI 環境を準備し、ASA 仮想 インスタンスを起動する方法について説明します。OCI ポータルにログインし、OCI Marketplace で Cisco ASA 仮想ファイアウォール（ASA 仮想）製品を検索し、コンピューティングインスタンスを起動します。ASA 仮想 の起動後に、トラフィックの送信元と接続先に応じて、トラフィックをファイアウォールに転送するようにルートテーブルを設定する必要があります。

仮想クラウドネットワーク（VCN）の作成

ASA 仮想 展開用の仮想クラウドネットワーク（VCN）を設定します。少なくとも、ASA 仮想 の各インターフェイスに 1 つずつ、合計 3 つの VCN が必要です。

次の手順に進み、管理 VCN を完了できます。次に、[Networking] に戻り、内部インターフェイスおよび外部インターフェイスの VCN を作成します。

始める前に

（注） ナビゲーションメニューからサービスを選択すると、左側のメニューにコンパートメントリストが表示されます。コンパートメントはリソースの整理に役立ち、リソースへのアクセスを制御しやすくなります。ルートコンパートメントは、テナントがプロビジョニングされるときに Oracleによって作成されます。管理者は、ルートコンパートメントにさらに多くのコンパートメントを作成し、アクセスルールを追加して、どのユーザーがそれらのコンパートメントを表示してアクションを実行できるかを制御できます。詳細については、Oracle のドキュメント『コンパートメントの管理（Managing Compartments）』を参照してください。

手順

ステップ 1 OCI にログインし、地域を選択します。

OCI は互いに分かれた複数の地域に分割されています。地域は、画面の右上隅に表示されます。ある地域内のリソースは、別の地域には表示されません。目的の地域内に存在していることを定期的に確認してください。

ステップ 2 **[Networking]** > **[Virtual Cloud Networks]** を選択し、[Create Virtual Cloud Networks] をクリックします。

ステップ 3 [Name] に、VCN のわかりやすい名前を入力します（例：*ASAvManagement*）。

ステップ 4 VCN の **CIDR ブロック**を入力します。

a) IP アドレスの **IPv4 CIDR ブロック**。CIDR（クラスレス ドメイン間ルーティング）の表記法は、IP アドレスとそれに関連付けられているルーティング プレフィクスのコンパクトな表現です。たとえば、「10.0.0.0/24」と入力します。

（注）
この VCN でDNS ホスト名を使用します。

b) [Oracleが割り当てたIPv6/56を割り当てる（Assign an Oracle allocated IPv6/56）] チェックボックスを選択して、Oracle が割り当てた単一の IPv6 アドレスを VCN に追加します。

ステップ 5 **[VCN の作成（Create VCN）]** をクリックします。

ネットワーク セキュリティ グループの作成

ネットワーク セキュリティ グループは、一連の vNIC と、vNIC に適用される一連のセキュリティルールで構成されます。

手順

ステップ 1 **[ネットワーキング（Networking）]** > **[仮想クラウドネットワーク（Virtual Cloud Networks）]** > **[仮想クラウドネットワークの詳細（Virtual Cloud Network Details）]**>**[ネットワーク セキュリティ グループ（Network Security Groups）]**を選択し、**[ネットワーク セキュリティ グループの作成（Create Network Security Group）]** をクリックします。

ステップ 2 [Name] に、ネットワーク セキュリティ グループのわかりやすい名前を入力します（例：*ASAv-Mgmt-Allow-22-443* ）。

ステップ 3 [Next] をクリックします。

ステップ 4 セキュリティルールを追加します。

a) ASA 仮想 コンソールへの SSH アクセスに TCP ポート 22 を許可するルールを追加します。

b) ASDM への HTTPS アクセスに TCP ポート 443 を許可するルールを追加します。

ASA 仮想 は ASDM を介して管理できます。管理するには、HTTPS 接続用にポート 443 を開く必要があります。

ステップ 5 [作成（Create）] をクリックします。

インターネットゲートウェイの作成

管理サブネットを公的にアクセス可能にするには、インターネットゲートウェイが必要です。

手順

ステップ 1 **[ネットワーキング（Networking）] > [仮想クラウドネットワーク（Virtual Cloud Networks）] > [仮想クラウドネットワークの詳細（Virtual Cloud Network Details）] > [インターネットゲートウェイ（Internet Gateways）]**を選択し、**[インターネットゲートウェイの作成（Create Internet Gateway）]** をクリックします。

ステップ 2 [Name] にインターネットゲートウェイのわかりやすい名前を入力します（例：*ASAv-IG*）。

ステップ 3 **[インターネットゲートウェイの作成（Create Internet Gateway）** をクリックします。

ステップ 4 インターネットゲートウェイへのルートを追加します。

a) **[ネットワーキング（Networking）] > [仮想クラウドネットワーク（Virtual Cloud Networks）] > [仮想クラウドネットワークの詳細（Virtual Cloud Network Details）] > [ルートテーブル（Route Tables）]**を選択します。

b) ルートルールを追加するには、デフォルトのルートテーブルのリンクをクリックします。

c) **[ルートルールの追加（Add Route Rules）]** をクリックします。

d) **[ターゲットタイプ（Target Type）]** ドロップダウンから、**[インターネットゲートウェイ（Internet Gateway）]** を選択します。

e) 宛先の IPv4 CIDR ブロックを入力します（例：0.0.0.0/0）。

f) 宛先の IPv6 CIDR ブロックを入力します（例：[::/]）。

g) **[ターゲット インターネット ゲートウェイ（Target Internet Gateway）]** ドロップダウンから、作成したゲートウェイを選択します。

h) **[ルートルールの追加（Add Route Rules）]** をクリックします。

サブネットの作成

各 VCN には、少なくとも 1 つのサブネットがあります。管理 VCN の管理サブネットを作成します。また、内部 VCN の内部サブネット、および外部 VCN の外部サブネットも必要です。

手順

ステップ 1 **[ネットワーキング（Networking）] > [仮想クラウドネットワーク（Virtual Cloud Networks）] > [仮想クラウドネットワークの詳細（Virtual Cloud Network Details）] > [サブネット（Subnets）]**を選択し、**[サブネットの作成（Create Subnet）]** をクリックします。

ステップ 2 [Name] にサブネットのわかりやすい名前を入力します（例：*Management*）。

ステップ 3 **[サブネットタイプ（Subnet Type）]** を選択します（推奨されるデフォルトの **[地域（Regional）]** のままにします）。

ステップ 4 **CIDR ブロック**を入力します（例：10.10.0.0/24）。サブネットの内部（非公開）IP アドレスは、この CIDR ブロックから取得されます。

ステップ 5 [Oracleが割り当てたIPv6/56プレフィックスを割り当てる（Assign an Oracle allocated IPv6/56 prefix）] チェックボックスをオンにします。
一意の IPv6 アドレスが生成されますが、最後の 2 桁の 16 進数を手動で入力する必要があります。ただし、サブネット内の IPv6 プレフィックスは常に **/64** に固定されています。

ステップ 6 **[ルートテーブル（Route Table）]** ドロップダウンから、以前に作成したルートテーブルのいずれかを選択します。

ステップ 7 サブネットの **[サブネットアクセス（Subnet Access）]** を選択します。

管理サブネットの場合、これは**パブリックサブネット**である必要があります。

ステップ 8 **[DHCP オプション（DHCP Option）]** を選択します。

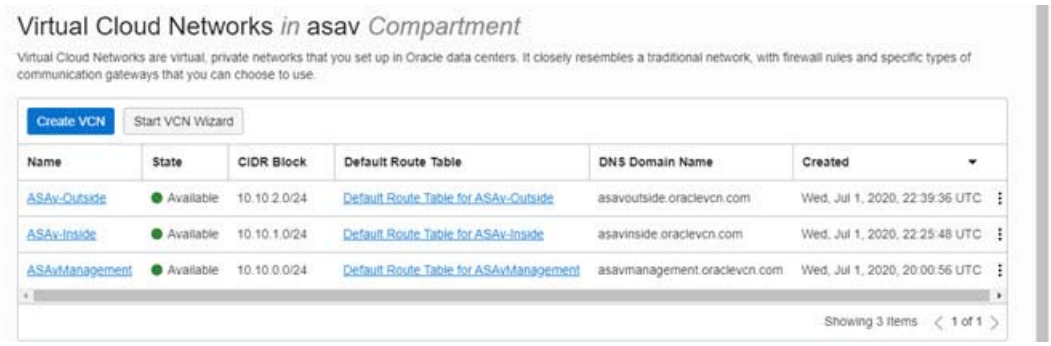
ステップ 9 以前作成した **[セキュリティリスト（Security List）]** を選択します。

ステップ 10 **[サブネットの作成（Create Subnet）]** をクリックします。

次のタスク

VCN（管理、内部、外部）を設定すると、ASA 仮想 を起動できます。ASA 仮想 VCN 構成の例については、次の図を参照してください。

図 *2 : ASA* 仮想 クラウドネットワーク



クラウドシェルを使用した IPv6 ゲートウェイアドレス

OCI では、各サブネットに一意の IPv6 ゲートウェイアドレスがあり、IPv6 トラフィックが機能するように ASAv で設定する必要があります。このゲートウェイアドレスは、クラウドシェルで OCI コマンドを実行しているサブネットの詳細から取得されます。

手順

ステップ 1 **[OCI]** > **[CloudShellを開く（OCIクラウドターミナル）]**（**Open CloudShell (OCI Cloud Terminal)**）に移動します。

ステップ 2 次のコマンドを実行して、サブネットから IPv6 の詳細を取得します。

```
oci network subnet get –subnet_id <subnet_OCID>
```

ステップ 3 コマンドの結果から `ipv6-virtual-router-ip` キーを見つけます。

ステップ 4 このキーの値をコピーし、必要に応じて使用します。

OCI での ASA 仮想 インスタンスの作成

Oracle Cloud Marketplace の Cisco ASA 仮想ファイアウォール（ASA 仮想）製品を使用して、コンピューティング インスタンスを介して OCI に ASA 仮想 を導入します。CPU の数、メモリの量、ネットワークリソースなどの特性に基づいて、最適なマシンシェイプを選択します。

手順

ステップ 1 OCI ポータルにログインします。

地域は、画面の右上隅に表示されます。目的の地域内に存在していることを確認してください。

ステップ 2 **[マーケットプレイス（Marketplace）]** > **[アプリケーション（Applications）]**を選択します。

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 契約条件を確認し、[Oracle の利用規約とパートナーの契約条件を確認して同意します。（I have reviewed and accept the Oracle Terms of Use and the Partner terms and conditions.）] チェックボックスをオンにします。

ステップ 5 [インスタンスの起動（Launch Instance）] をクリックします。

ステップ 6 [Name] に、インスタンスのわかりやすい名前を入力します（例：*ASAv-9-15*）。

ステップ 7 [シェイプの変更（Change Shape）] をクリックし、ASA 仮想 に必要な oCPU の数、RAM の量、およびインターフェイスの数が指定されたシェイプ（VM.Standard2.4 など）を選択します（表 1 : x86 展開でサポートされるコンピューティングシェイプ （1 ページ）を参照）。

ステップ 8 **[仮想クラウドネットワーク（Virtual Cloud Network）]** ドロップダウンから、[管理 VCN（Management VCN）] を選択します。

ステップ 9 自動入力されていない場合は、**[サブネット（Subnet）]** ドロップダウンから [管理サブネット（Management subnet）] を選択します。

ステップ 10 **[ネットワーク セキュリティ グループを使用してトラフィックを制御する（Use Network Security Groups to Control Traffic）]** にチェックを入れ、管理 VCN に設定したセキュリティグループを選択します。

ステップ 11 **[パブリック IP アドレスの割り当て（Assign a Public Ip Address）]** オプションボタンをクリックします。

ステップ 12 **[SSH キーの追加（Add SSH keys）]** の下で、**[公開キーの貼り付け（Paste Public Keys）]** オプションボタンをクリックして、SSH キーを貼り付けます。

Linux ベースのインスタンスは、パスワードの代わりに SSH キーペアを使用してリモートユーザーを認証します。キーペアは、秘密キーと公開キーで構成されます。インスタンスを作成するときに、秘密キーをコンピュータに保持し、公開キーを提供します。ガイドラインについては、『Linux インスタンスでのキーペアの管理（Managing Key Pairs on Linux Instances）』https://docs.cloud.oracle.com/en-us/iaas/Content/Compute/Tasks/managingkeypairs.htmを参照してください。

ステップ 13 **[詳細オプションの表示（Show Advanced Options）]** リンクをクリックして、オプションを展開します。

ステップ 14 （任意）[スクリプトの初期化（Initialization Script）] の下で、[クラウド初期化スクリプトの貼り付け（Paste Cloud-Init Script）] オプションボタンをクリックして、 ASA 仮想 の第 0 日用構成を指定します。第 0 日用構成は、ASA 仮想 の起動時に適用されます。

次に、**[クラウド初期化スクリプト（Cloud-Init 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 9.18.1
interface management0/0
management-only
nameif management
security-level 100
ip address dhcp setroute
ipv6 enable
ipv6 address dhcp default
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 ::/0 management

ssh timeout 60
ssh version 2
username admin nopassword privilege 15
username admin attributes
service-type admin
http server enable
http 0 0 management
```

```
aaa authentication ssh console LOCAL
```

ステップ 15 [作成（Create）] をクリックします。

次のタスク

[作成（Create）] ボタンをクリックした後、状態が [プロビジョニング（Provisioning）] として表示される ASA 仮想 インスタンスをモニターします。

重要 ステータスをモニターすることが重要です。ASA 仮想 インスタンスの状態が [プロビジョニング（Provisioning）] から [実行中（Running）] に移行したら、ASA 仮想 ブートが完了する前に必要に応じて VNIC を接続する必要があります。

インターフェイスの接続

ASA 仮想 は、1 つの VNIC が接続された状態で実行状態になります（**[コンピューティング（Compute）] > [インスタンス（Instances）] > [インスタンスの詳細（Instance Details）] > [接続された VNIC （Attached VNICs）]**を参照）。これはプライマリ VNIC と呼ばれ、管理 VCN にマッピングされます。ASA 仮想 が最初の起動を完了する前に、vNIC が ASA 仮想 で正しく検出されるように、以前作成した他の VCN サブネット（内部、外部）の vNIC を接続する必要があります。

手順

ステップ 1 新しく起動した ASA 仮想 インスタンスを選択します。

ステップ 2 **[接続された VNIC（Attached VNICs）] > [VNIC の作成（Create VNIC）]**の順に選択します。

ステップ 3 [名前（Name）] に、VNIC のわかりやすい名前を入力します（例：*Inside*）。

ステップ 4 [仮想クラウドネットワーク（Virtual Cloud Network）] ドロップダウンから VCN を選択します。

ステップ 5 [サブネット（Subnet）] ドロップダウンからサブネットを選択します。

ステップ 6 **[ネットワーク セキュリティ グループを使用してトラフィックを制御する（Use Network Security Groups to Control Traffic）]** をオンにして、選択した VCN 用に設定したセキュリティグループを選択します。

ステップ 7 [送信元と宛先のチェックをスキップ（Skip Source Destination Check）] をオンにします。

ステップ 8 （オプション）[プライベート IP アドレス（Private IP Address）] を指定します。これは、VNIC に対して特定の IP を選択する場合にのみ必要です。

IP を指定しない場合、OCI はサブネットに割り当てられた CIDR ブロックから IP アドレスを割り当てます。

IPv6 アドレスを設定している場合は、一意の IPv6 アドレスを選択して、各インターフェイスに割り当てます。

ステップ 9 [変更の保存 (Save Changes)] をクリックし、VNIC を作成します。

ステップ 10 展開で必要となる各 VNIC について、この手順を繰り返します。

接続された VNIC のルートルールの追加

内部および外部のルートテーブルにルートテーブルルールを追加します。

手順

ステップ 1 **[Networking]** > **[Virtual Cloud Networks]** を選択し、VCN に関連付けられているデフォルトルートテーブル（内部または外部）をクリックします。

ステップ 2 **[ルートルールの追加（Add Route Rules）]** をクリックします。

ステップ 3 [ターゲットタイプ（Target Type）] ドロップダウンから、[プライベート IP（Private IP）] を選択します。

ステップ 4 [宛先タイプ（Destination Type）] ドロップダウンから、[CIDR ブロック（CIDR Block）] を選択します。

ステップ 5 [宛先のIPv4 CIDRブロック（Destination IPv4 CIDR Block）] に宛先の IPv4 CIDR ブロックを入力します（例：0.0.0.0/0）。

ステップ 6 [宛先のIPv6 CIDRブロック（Destination IPv6 CIDR Block）] に宛先の IPv6 CIDR ブロックを入力します（例：[::/0]）。

ステップ 7 [ターゲット選択（Target Selection）] フィールドに VNIC のプライベート IP アドレスを入力します。

VNICにIPアドレスを明示的に割り当てていない場合は、VNICの詳細（**[コンピューティング（Compute）]**> **[インスタンス（Instances）]** > **[インスタンスの詳細（Instance Details）]** > **[接続された VNIC（Attached VNICs）]**）で自動割り当てされた IP アドレスを確認できます。

ステップ 8 **[ルートルールの追加（Add Route Rules）]** をクリックします。

ステップ 9 展開で必要となる各 VNIC について、この手順を繰り返します。

（注）
ASA Virtual の（静的および DHCP）設定に必要な個別のルーティングルール。

ipv6 route <interface_name> <interface_subnet_CIDR> <ipv6_virtual_router_ip>

例

- ipv6 route inside 2603:c020:5:5800::/64 fe80::200:17ff:fe96:921b
- ipv6 route outside 2603:c020:6:ba00::/64 fe80::200:17ff:fe21:748c

OCI 上の ASA 仮想 インスタンスへのアクセス

セキュアシェル（SSH）接続を使用して、実行中のインスタンスに接続できます。

- ほとんどの UNIX スタイルのシステムには、デフォルトで SSH クライアントが含まれています。
- Windows 10 および Windows Server 2019 システムには、OpenSSH クライアントが含まれている必要があります。Oracle Cloud Infrastructure によって生成された SSH キーを使用してインスタンスを作成した場合に必要になります。
- その他の Windows バージョンの場合は、http://www.putty.org から無償の SSH クライアントである PuTTY をダウンロードできます。

前提条件

インスタンスに接続するには、次の情報が必要です。

- インスタンスのパブリック IP アドレス。アドレスは、コンソールの [インスタンスの詳細（Instance Details）] ページから取得できます。ナビゲーションメニューを開きます。**[コアインフラストラクチャ（Core Infrastructure）]** の下で、**[コンピューティング（Compute）]** に移動し、**[インスタンス（Instances）]** をクリックします。次に、インスタンスを選択します。あるいは、コアサービス API の ListVnicAttachments および GetVnic 操作を使用できます。
- インスタンスのユーザー名とパスワード。
- インスタンスを起動したときに使用した SSH キーペアの秘密キー部分へのフルパス。キーペアの詳細については、「Managing Key Pairs on Linux 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、ASA 仮想 インスタンスにログインできます。

SSH を使用した ASA 仮想 インスタンスへの接続

UNIX スタイルのシステムから ASA 仮想 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。

手順

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、ASA 仮想 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。

<ipv6-address> はインスタンス管理インターフェイスの IPv6 アドレスです。

OpenSSH を使用した ASA 仮想 インスタンスへの接続

Windows システムから ASA 仮想 インスタンスに接続するには、OpenSSH を使用してインスタンスにログインします。

手順

ステップ 1 このキーペアを初めて使用する場合は、自分だけがファイルを読み取れるようにファイルの権限を設定する必要があります。

次の手順を実行します。

a) Windows Explorer で、秘密キーファイルに移動し、ファイルを右クリックして **[プロパティ（Properties）]** をクリックします。
b) **[セキュリティ（Security）]** タブで、**[詳細設定（Advanced）]** をクリックします。
c) **[オーナー（Owner）]** が自分のユーザーアカウントであることを確認します。
d) **[継承の無効化（Disable Inheritance）]** をクリックし、**[継承された権限をこのオブジェクトの明示的な権限に変換する（Convert inherited permissions into explicit permissions on this object）]** を選択します。
e) 自分のユーザーアカウントではない各権限エントリを選択し、**[削除（Remove）]** をクリックします。
f) 自分のユーザーアカウントのアクセス権限が **[フルコントロール（Full Control）]** であることを確認します。
g) 変更を保存します。

ステップ 2 インスタンスに接続するには、Windows PowerShell を開き、次のコマンドを実行します。

```
$ 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、ASA 仮想 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。

PuTTY を使用した ASA 仮想 インスタンスへの接続

PuTTY を使用して Windows システムから ASA 仮想 インスタンスに接続するには、次の手順を実行します。

手順

ステップ 1 PuTTY を開きます。

ステップ 2 **[カテゴリ（Category）]** ペインで、**[セッション（Session）]** を選択し、次の内容を入力します。

- **ホスト名または IP アドレス**：

  <username>@<public-ip-address>

  ここで、

  <username> は、ASA 仮想 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パブリック IP アドレスです。

- **ポート**： 22
- **接続タイプ**： SSH

ステップ 3 **[カテゴリ（Category）]** ペインで、**[Window]** を展開し、**[変換（Translation）]** を選択します。

ステップ 4 **[リモート文字セット（Remote character set）]** ドロップダウンリストで、**[UTF-8]** を選択します。

Linux ベースのインスタンスでデフォルトのロケール設定は UTF-8 です。これにより、PuTTY は同じロケールを使用するように設定されます。

ステップ 5 **[カテゴリ（Category）]** ペインで、**[接続（Connection）]**、**[SSH]** の順に展開し、**[認証（Auth）]** をクリックします。

ステップ 6 **[参照（Browse）]** をクリックして、秘密キーを選択します。

ステップ 7 **[開く（Open）]** をクリックして、セッションを開始します。

インスタンスに初めて接続する場合は、「サーバーのホストキーがレジストリにキャッシュされていない（the server's host key is not cached in the registry）」というメッセージが表示されることがあります。**[はい（Yes）]** をクリックして、接続を続行します。

トラブルシューティング

問題 SSH：IPv6 を使用した ASA Virtual が機能していない

- **解決法** インターネットゲートウェイ経由の ::/0 のルートが VPC ルートテーブルに存在するかどうかを確認します。
- **解決法** 管理サブネットまたはインターフェイスに関連付けられたセキュリティグループでポート 22 が許可されているかどうかを確認します。
- **解決法** 管理インターフェイスが IPv6 アドレスで設定されているかどうかを IPv4 SSH セッション経由で確認します。
- **解決法** ASA Virtual の「ssh config」で必要なすべての設定が Day-0 の一環として指定されているか、あるいは後で設定するのかを確認します。

問題 水平方向のトラフィックが機能していない。

- **解決法** **[EC2]** > **[インスタンス（Instance）]** > **[ネットワーキング（Networking）]**で、「送信元または送信先の確認の変更」が停止されているかどうかを確認します。
- **解決法** ルートが内部/外部の Linux で適切に設定されていることを確認します。
- **解決法** 手動による IPv6 アドレッシングの場合は、ASA Virtual に適切なルートを追加します。
- **解決法** 「show asp drop」でパケットドロップが発生していないかを確認し、適宜対応します。

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。

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。