Threat Defense Virtual の Alibaba Cloud への展開

概要

Alibaba Cloud はパブリッククラウド環境です。Threat Defense Virtual は、Alibaba Cloud 環境でゲストとして実行されます。

Alibaba がサポートするインスタンスタイプ

Alibaba 上の Threat Defense Virtual では、次のインスタンスタイプを使用できます。

ネットワーク拡張マシンタイプ			
設定	vCPU の数	メモリ（GB）	サポートされるインターフェイスの最大数
ecs.g5ne.xlarge	4	16	4
ecs.g5ne.2xlarge	8	32	[6]
ecs.g5ne.4xlarge	16	64	8

Note Threat Defense Virtual では、インスタンスをサポートするために少なくとも 4 つのインターフェイス（ENI）が必要です。

Note インスタンスタイプのサイズ変更と Threat Defense Virtual の展開はサポートされていません。新規展開でのみ、異なるインスタンスサイズで Threat Defense Virtual を展開できます。

ネットワーク要件

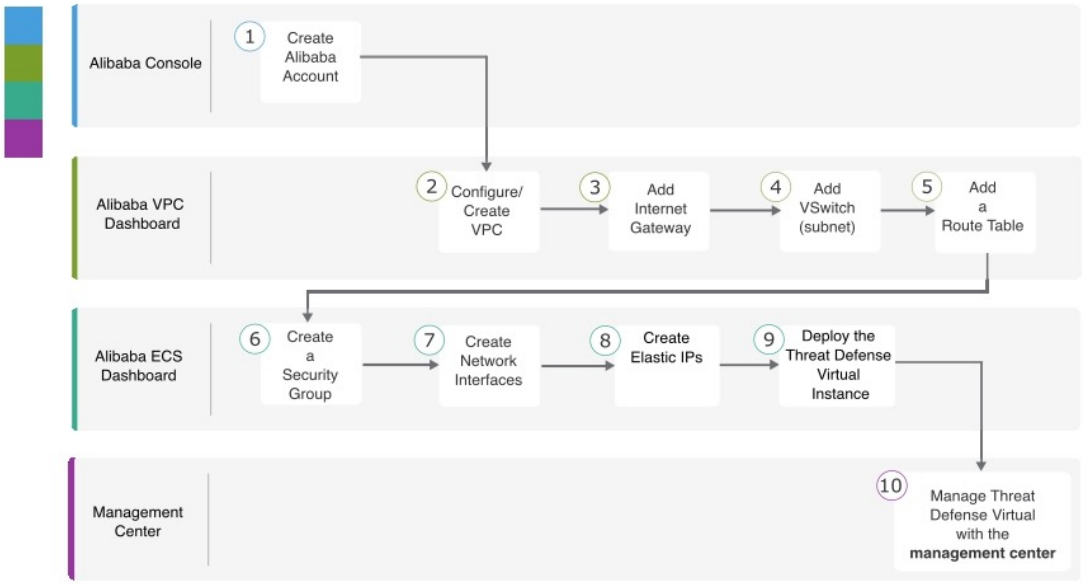
- Threat Defense Virtual の基本サポート用に、4 つの Vswitch（サブネット）を備えた VPC を 1 つ作成できます。
- 管理 Vswitch は、インスタンスの展開先と同じゾーン内に必要があります。同じゾーン内にない場合は、作成する必要があります。

関連資料

インスタンスタイプとその設定の詳細については、『Alibaba Cloud』を参照してください。

エンドツーエンドの手順

Threat Defense Virtual を Alibaba に展開するには、次のタスクを参照してください。



	ワークスペース	手順
1	Alibaba コンソール	https://marketplace.alibabacloud.com/：Alibaba コンソールでユーザーアカウントを作成します。
2	Alibaba VPC ダッシュボード	VPC の作成 （7 ページ）：Alibaba アカウント専用の VPC を作成および設定します。
3	Alibaba VPC ダッシュボード	インターネット ゲートウェイの追加 （8 ページ）：VPC をインターネットに接続するために、インターネットゲートウェイを追加します。
4	Alibaba VPC ダッシュボード	vSwitch の追加 （8 ページ）：VPC に VSwitch（サブネット）を追加します。
5	Alibaba VPC ダッシュボード	ルート テーブルの追加 （9 ページ）：VPC 用に設定したゲートウェイにルートテーブルを接続します。
6	Alibaba ECS ダッシュボード	セキュリティ グループの作成 （10 ページ）：許可されるプロトコル、ポート、送信元 IP 範囲を指定するルールを使用して、セキュリティグループを作成します。
7	Alibaba ECS ダッシュボード	ネットワーク インターフェイスの作成 （11 ページ）：静的 IP アドレスを使用して、Threat Defense Virtual のネットワーク インターフェイスを作成します。
8	Alibaba ECS ダッシュボード	Elastic IP アドレスの作成 （12 ページ）：Elastic IP は、Threat Defense Virtual および他のインスタンスへのリモートアクセスに使用されるパブリック IP 用に予約されます。
9	Management Center または Device Manager	Threat Defense Virtual の展開 （13 ページ）：Alibaba ポータルから Threat Defense Virtual を展開します。
10	Management Center	Threat Defense Virtual を管理します。 • Firepower Management Center を使用した Firepower Threat Defense Virtual の管理

前提条件

- Alibaba のアカウント。https://www.alibaba.com/ で 1 つ作成できます。
- Threat Defense Virtual コンソールにアクセスするには、SSH クライアント（Windows の PuTTY、Macintosh のターミナルなど）が必要です。

- Cisco スマートアカウント。Cisco Software Central で作成できますhttps://software.cisco.com/ 。
- Threat Defense Virtual へのライセンス付与。
  - Management Center Virtual 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。
  - ライセンスの管理方法の詳細については、『Cisco Secure Firewall Management Center Configuration Guide』 の「Licensing」を参照してください。
- Threat Defense Virtual インターフェイスの要件：
  - 管理インターフェイス（1）：Threat Defense Virtual を Management Center Virtual に接続するために使用されます。
  - 2 番目のインターフェイスは診断に使用されます。トラフィック転送には使用できません。

    バージョン 6.7 以降では、必要に応じて、管理インターフェイスの代わりにデータインターフェイスを FMC の管理に使用できます。管理インターフェイスはデータインターフェイス管理の前提条件であるため、初期設定でこれを設定する必要があります。データインターフェイスから FMC へのアクセスは、高可用性の展開ではサポートされません。

    FMC アクセスに対するデータインターフェイスの設定に関する詳細については、『FTD command reference』の **configure network management-data-interface** コマンドを参照してください。
  - トラフィックインターフェイス（2）：Threat Defense Virtual を内部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：
  - Threat Defense Virtual にアクセスするためのパブリックおよび Elastic IP。

サポートされるソフトウェア プラットフォーム

Threat Defense Virtual Auto Scale ソリューションは、ソフトウェアバージョンに依存せず、Management Center によって管理される Threat Defense Virtual デバイスに適用可能です。オペレーティングシステムとホスティング環境の要件を含めたシスコのソフトウェアおよびハードウェアの互換性については、『Cisco Secure Firewall Threat Defense Compatibility Guide』を参照してください。

- 『Firewall Management Center Virtual Compatibility Guide』の表には、Alibaba 上の Management Center Virtual における互換性および仮想ホスティング環境の要件が一覧表示されています。
- 『Cisco Secure Firewall Threat Defense Compatibility Guide』の表には、Alibaba 上の Threat Defense Virtual における互換性および仮想ホスティング環境の要件が一覧表示されています。

注意事項と制約事項

サポートされる機能

- 基本的な製品の稼働
- Day-0 構成
- 公開キーまたはパスワードを使用した SSH。
- デバッグ目的で Threat Defense Virtual にアクセスするための Alibaba UI コンソール。
- Alibaba UI の停止/再起動
- サポートされているインスタンスタイプ：ecs.g5ne.xlarge、ecs.g5ne.2xlarge、ecs.g5ne.4xlarge。
- ハイパー スレッディング
- 所有ライセンス持ち込み（BYOL）ライセンスのサポート。

Threat Defense Virtual スマートライセンスのパフォーマンス階層

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。

Table 1: 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	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
FTDv、16Gbps	16 コア/34 GB	16 Gbps	10,000

- シスコ スマート ライセンス アカウントを使用する BYOL（Bring Your Own License）。

Threat Defense Virtual デバイスのライセンス供与に関するガイドラインについては、*Threat Defense Virtual Management Center* コンフィギュレーション ガイド [英語] の「Licensing the Threat Defense Virtual System」の章を参照してください。

パフォーマンスの最適化

Threat Defense Virtual の最高のパフォーマンスを実現するために、VM とホストの両方を調整することができます。詳細については、「Alibaba Cloud での仮想化の調整と最適化」を参照してください。

Receive Side Scaling：Threat Defense Virtual は Receive Side Scaling（RSS）をサポートしています。これは、ネットワークアダプタによって複数のプロセッサコアにネットワーク受信トラフィックを分散するために使用されるテクノロジーです。バージョン 7.0 以降でサポートされています。詳細については、「Receive Side Scaling（RSS）用の複数の RX キュー」を参照してください。

サポートされない機能

- FDM
- ハイアベイラビリティの機能
- 自動スケール
- IPv6
- SR-IOV

制限事項

- バージョン7.2リリースでは、トランスペアレントモード、インラインモード、およびパッシブモードはサポートされていません。
- East-West トラフィックは、Alibaba ではサポートされていません。
- ジャンボフレームは、Alibaba のいくつかのインスタンスタイプに限定されているため、サポートされていません。詳細については、Alibaba Cloud を参照してください。

Note Threat Defense Virtual には、起動する 4 つのインターフェイスが必要です。

ライセンシング

- シスコ スマート ライセンス アカウントを使用する BYOL（Bring Your Own License）がサポートされています。

ポリシーとデバイス設定の設定

Threat Defense Virtual をインストールし、デバイスを Management Center Virtual に追加すると、Management Center Virtual ユーザーインターフェイスを使用して、Alibaba で実行されている Threat Defense Virtual のデバイス管理設定を設定できます。アクセス コントロール ポリシーや

その他の関連ポリシーを設定して適用すると、Threat Defense Virtual インスタンスを使用してトラフィックを管理できます。

セキュリティ ポリシーは、Next Generation IPS のフィルタリングやアプリケーションのフィルタリングなど、Threat Defense Virtual で提供されるサービスを制御します。Management Center Virtual を使用して、Threat Defense Virtual 上でセキュリティ ポリシーを設定します。セキュリティポリシーの設定方法の詳細については、*Cisco Secure Firewall* コンフィギュレーション ガイド [英語] または Management Center Virtual のオンラインヘルプを参照してください。

VPC の作成

仮想プライベートクラウド（VPC）は、Alibaba アカウント専用の仮想ネットワークです。これは、Alibaba クラウド内の他の仮想ネットワークから論理的に分離されています。Management Center Virtual インスタンスや Threat Defense Virtual インスタンスなどの Alibaba Cloud リソースを VPC で起動できます。VPC を設定できます。さらに、その IP アドレス範囲を選択し、VSwitch（サブネット）を作成し、ルートテーブル、ネットワークゲートウェイ、およびセキュリティ設定を作成できます。

Procedure

ステップ 1 https://www.alibabacloud.com にログインし、地域を選択します。

Alibaba Cloud は互いに分離さ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 [製品（Products）] > [VPC] の順にクリックします。

ステップ 3 [VPCダッシュボード（VPC Dashboard）] > [使用するVPC（Your VPCs）] の順にクリックします。

ステップ 4 [VPCの作成（Create VPC）] をクリックします。

ステップ 5 [VPCの作成（Create VPC）] ダイアログボックスで、次のものを入力します。

a) VPC を識別するユーザー定義の [名前タグ（Name tag）]。

b) 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。

c) 仮想プライベートクラウドで IPv4 を有効にするには、**Alibaba Cloud 提供の IPv4 CIDR ブロック**として **IPv4 CIDR ブロック**を選択します。

d) デフォルトの [テナント（Tenancy）] 設定。この VPC で起動されたインスタンスが、起動時に指定されたテナント属性を使用するようにします。

ステップ 6 [OK] をクリックして VPC を作成します。

What to do next

次のセクションで説明されているように、VPCにインターネット ゲートウェイを追加します。

インターネット ゲートウェイの追加

VPCをインターネットに接続するために、インターネットゲートウェイ（NATゲートウェイ）を追加できます。VPC の外部の IP アドレスのトラフィックをインターネット ゲートウェイにルーティングできます。

はじめる前に

- Threat Defense Virtual インスタンスの VPC を作成します。

Procedure

ステップ 1 **[製品（Products）]** > **[VPC]** の順にクリックします。

ステップ 2 **[VPC ダッシュボード（VPC Dashboard）]** > **[インターネットゲートウェイ（Internet Gateway）]** の順にクリックしてから、[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 3 ユーザー定義の [名前タグ（Name tag）] を入力してゲートウェイを特定し、[OK] をクリックしてゲートウェイを作成します。

ステップ 4 前のステップで作成したゲートウェイを選択します。

ステップ 5 [VPC にバインド（Bind to VPC）] をクリックして、以前に作成した VPC を選択します。

ステップ 6 [OK] をクリックして、ゲートウェイを VPC にバインドします。

デフォルトでは、NAT ゲートウェイが作成されて VPC にバインドされるまで、VPC で起動されたインスタンスはインターネットと通信できません。

What to do next

次のセクションで説明されているように、VPC に VSwitch（サブネット）を追加します。

vSwitch の追加

Threat Defense Virtual インスタンスが接続できる VPC の IP アドレス範囲をセグメント化することができます。セキュリティおよび運用のニーズに応じて、インスタンスをグループ化するための vSwitch（サブネット）を作成できます。Threat Defense Virtual では、管理用の vSwitch とトラフィック用の vSwitch を作成する必要があります。

はじめる前に

- Threat Defense Virtual インスタンス用の 4 つの VPC を作成します。VPC の作成に関するセクションを参照してください。

• VPC ごとに 1 つの vSwitch（サブネット）を追加します。

Procedure

ステップ 1 **[製品（Products）]** > **[VPC]** の順にクリックします。

ステップ 2 **[VPC ダッシュボード（VPC Dashboard）]** > **[vSwitch（VSwitches）]** の順にクリックし、[vSwitch をクリック（Click vSwitch）] をクリックします。

ステップ 3 [vSwitch の作成（Create vSwitch）] ダイアログボックスで、次のものを入力します。

a) vSwitch を識別するユーザー定義の [名前タグ（Name tag）]。

b) この vSwitch に使用する [VPC]。

c) この vSwitch が存在する [ゾーン（Zone）]。[設定なし（No Preference）] を選択して、Alibaba Cloud が選択するゾーンを選びます。

d) IP アドレスの [CIDR ブロック（CIDR block）]（IPv4）。vSwitch の IP アドレスの範囲は、VPC の IP アドレス範囲のサブセットである必要があります。ブロック サイズは、/16 ネットワーク マスクから /28 ネットワーク マスクの範囲で指定する必要があります。vSwitch のサイズは VPC のサイズと同じにすることができます。

ステップ 4 [OK] をクリックして vSwitch を作成します。

ステップ 5 必要な数の vSwitch について、手順を繰り返します。管理トラフィックには別の vSwitch を作成し、データ トラフィックに必要な数の vSwitch を作成します。

What to do next

次のセクションで説明されているように、VPC にルート テーブルを追加します。

ルート テーブルの追加

VPC 用に設定したゲートウェイにルート テーブルを接続できます。また、複数のサブネットを 1 つのルート テーブルに関連付けることができます。しかし、1 つのサブネットは一度に 1 つのルート テーブルにしか関連付けることができません。

Procedure

ステップ 1 **[製品（Products）]** > **[VPC]** の順にクリックします。

ステップ 2 **[VPC ダッシュボード（VPC Dashboard）]** > **[ルートテーブル（Route Tables）]** の順にクリックしてから、[ルートの作成（Create Route）] をクリックします。

ステップ 3 ルート テーブルを識別するユーザー定義の [名前タグ（Name tag）] を入力します。

ステップ 4 このルート テーブルを使用する [VPC] をドロップダウン リストから選択します。

ステップ 5 [OK] をクリックして、ルートテーブルを作成します。

ステップ 6 作成したルートテーブルを選択します。

ステップ 7 [ルート（Routes）] タブをクリックして、詳細ペインにルート情報を表示します。

ステップ 8 [編集（Edit）] をクリックして、[別のルートを追加（Add another route）] をクリックします。

a) [宛先（Destination）] 列で、すべての IPv4 トラフィックについて **0.0.0.0/0** と入力します。

b) [ターゲット（Target）] 列で、ゲートウェイを選択します。

ステップ 9 [保存（Save）] をクリックします。

What to do next

次のセクションで説明するように、セキュリティ グループを作成します。

セキュリティ グループの作成

許可されるプロトコル、ポート、送信元 IP 範囲を指定するルールを使用して、セキュリティ グループを作成できます。各インスタンスに割り当てることができる、さまざまな異なるルールを使用して、複数のセキュリティ グループを作成できます。

Procedure

ステップ 1 **[製品（Products）]** > **[ECS]** の順にクリックします。

ステップ 2 **[ECS ダッシュボード（ECS Dashboard）]** > **[セキュリティグループ（Security Groups）]** の順にクリックします。

ステップ 3 [セキュリティグループの作成（Create Security Group）] をクリックします。

ステップ 4 [セキュリティ グループの作成（Create Security Group）] ダイアログボックスで、次のものを入力します。

a) セキュリティ グループを識別するユーザー定義の [セキュリティグループ名（Security Group Name）]。

b) このセキュリティ グループの [説明（Description）]。

c) このセキュリティ グループに関連付けられた VPC。

ステップ 5 [セキュリティグループルール（Security Group Rules）] を設定します。

a) [インバウンドルール（Inbound Rules）] タブをクリックして、[ルールの追加（Add Rule）] をクリックします。

Note
Management Center Virtual を Alibaba の外部から管理するには、HTTPS および SSH アクセスが必要です。それに基づいて、送信元 IP アドレスを指定する必要があります。また、Management Center Virtual と Threat Defense Virtual の両方を Alibaba VPC 内で設定している場合、プライベート IP 管理サブネット アクセスを許可する必要があります。

b) [アウトバウンドルール（Outbound Rules）] タブをクリックしてから、[ルールの追加（Add Rule）] をクリックして、アウトバウンドトラフィックのルールを追加するか、デフォルトの [すべてのトラフィッ

ク（All traffic）]（[タイプ（Type）] の場合）および [任意の宛先（Anywhere）]（[宛先（Destination）] の場合）のままにします。

ステップ 6 セキュリティ グループを作成するには、[作成（Create）] をクリックします。

What to do next

次のセクションで説明されているように、ネットワーク インターフェイスを作成します。

ネットワーク インターフェイスの作成

Threat Defense Virtual のネットワーク インターフェイスは、静的 IP アドレス（IPv4）または DHCP を使用して作成できます。具体的な展開の必要に応じてネットワーク インターフェイス（内部および外部）を作成します。

Procedure

ステップ 1 **[サービス（Services）]** > **[Elastic Network Interface]** の順にクリックします。

ステップ 2 [ネットワーク インターフェイス（Network Interfaces）] をクリックします。

ステップ 3 [ネットワークインターフェイスの作成（Create Network Interface）] をクリックします。

ステップ 4 [ネットワークインターフェイスの作成（Create Network Interface）] ダイアログボックスで、次のものを入力します。

a) ネットワーク インターフェイスに関するオプションのユーザー定義の [説明（Description）]。

b) ドロップダウンリストから [vSwitch] を選択します。Threat Defense Virtual インスタンスを作成する VPC の vSwitch が選択されていることを確認します。

c) [プライベートIP（Private IP）] アドレスを入力します。静的 IP アドレス（IPv4）または自動生成（DHCP）を使用できます。

d) [セキュリティグループ（Security groups）] を 1 つ以上選択します。セキュリティ グループの必要なポートがすべて開いていることを確認します。

ステップ 5 [ネットワーク インターフェイスの作成（Create network interface）] をクリックして、ネットワーク インターフェイスを作成します。

ステップ 6 作成したネットワーク インターフェイスを選択します。

ステップ 7 右クリックして、[送信元/宛先の変更の確認（Modify Source/Dest. Check）]を選択します。

ステップ 8 [送信元または送信先の確認（Source/destination check）] の下にある [有効化（Enable）] チェックボックスをオフにして、[保存（Save）] をクリックします。

What to do next

次のセクションで説明するように、Elastic IP アドレスを作成します。

Elastic IP アドレスの作成

インスタンスが作成されると、パブリック IP アドレスはそのインスタンスに関連付けられます。インスタンスを停止してから開始すると、そのパブリック IP アドレス（IPv4）は自動的に変更されます。この問題を解決するには、Elastic IP アドレッシングを使用して、永続的なパブリック IP アドレスをそのインスタンスに割り当てます。Elastic IP アドレスは、Threat Defense Virtual および他のインスタンスへのリモートアクセスに使用されるパブリック IP アドレス用に予約されます。

Procedure

ステップ 1 **[製品（Products）] > [Elastic コンピューティングサービス（Elastic Compute Service）]** の順にクリックします。

ステップ 2 [Elastic コンピューティングサービス（Elastic Compute Service）] ダッシュボードで、左側のメニューから [Elastic IP] をクリックします。

ステップ 3 [Elastic IP アドレスの割り当て（Allocate Elastic IP Address）] をクリックします。

ステップ 4 EIP 設定を指定します。

a) EIP を割り当てる [リージョン（Region）] を選択します。
b) EIP に必要な帯域幅プランを選択します。[BYOL] や [サブスクリプション（Subscription）] などです。
c) 必要な帯域幅量を指定します。
d) 選択内容を確認し、[OK] をクリックして EIP を割り当てます。

ステップ 5 EIP をインスタンスに関連付けます。

a) EIP を割り当てたら、[Elastic コンピューティングサービス（Elastic Compute Service）] ダッシュボードの [Elastic IP] セクションに移動します。
b) 作成した EIP を見つけ、[関連付け（Associate）] をクリックします。
c) EIP に関連付ける ECS インスタンスを選択し、[OK] をクリックします。

ステップ 6 EIP が、関連付けられた ECS インスタンスの下に示されていることを確認し、その接続を確認します。

What to do next

次のセクションで説明されているように、Threat Defense Virtual を展開します。

Alibaba 環境の設定

Threat Defense Virtual を Alibaba に展開するには、展開に固有の要件および設定を使用して Alibaba VPC を設定する必要があります。ほとんどの環境では、セットアップ ウィザードに従ってセットアップを実行できます。Alibaba では、概要から詳細機能に至るまで、サービスに関する有用な情報を扱ったオンラインドキュメントを提供しています。詳細については、Alibaba Cloud のドキュメントを参照してください。

Threat Defense Virtual の展開には、Threat Defense Virtualを展開する前に 4 つのネットワーク仮想プライベートクラウド（VPC）を作成する必要があります。

4 つのネットワーク VPC は、次のとおりです。

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

Alibaba のセットアップを適切に制御するために、続くセクションでは、Threat Defense Virtual インスタンスの起動前の VPC および EC2 構成について説明します。

はじめる前に

- Alibaba Cloud のアカウントを作成します。

Threat Defense Virtual の展開

Procedure

ステップ 1 Threat Defense Virtual を展開するには、https://marketplace.alibabacloud.com/ に移動し、「**Cisco Firepower NGFW Virtual (NGFWv) - BYOL**」製品を検索します。

Note
Alibaba は互いに分離された複数の地域に分割されています。地域は、ウィンドウ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 製品リンクをクリックして、[Cisco Firepower NGFW Virtual (NGFWv) - BYOL] ページを開きます。

ステップ 3 [プランの選択（Choose Your Plan）] をクリックします。[Elastic コンピューティングサービス（Elastic Compute Service）] ページにリダイレクトされます。

ステップ 4 [カスタム起動（Custom Launch）] セクションに次の詳細情報を入力します。

- [請求方法（Billing Method）]：要件に従って選択。

  Note
  請求方法は、Alibaba Cloud 上のインフラストラクチャに関するもので、要件に従って選択できます。

- [地域（Region）]：要件に従って選択。
- [ネットワークとゾーン（Network and Zone）]：以前に作成した VPC および管理 vSwitch をドロップダウンリストから選択するか、[VPC の作成（Create VPC）] リンクと [vSwitch の作成（Create vSwitch）] リンクを使用して新しく作成します。

ステップ 5 [インスタンスとイメージ（Instances and Images）] ページに移動します。

[すべてのインスタンスタイプ（All Instance Types）] セクションで、次の手順を実行します。

- [インスタンス（Instance）]：サポートされているインスタンスタイプ（**ecs.g5ne.xlarge**、**ecs.g5ne.2xlarge**、**ecs.g5ne.4xlarge**）のいずれかを選択します。
- [イメージ（Image）]：[マーケットプレイスイメージ REC（Marketplace Image REC）] セクションに最新の Threat Defense Virtual マーケットプレイス バージョンが表示されます。
  - **a.** [イメージの再選択（Reselect Image）] をクリックします。[Alibaba Cloud マーケットプレイスイメージ（Alibaba Cloud Marketplace Image）] ダイアログボックスが表示され、展開する Threat Defense Virtual イメージの詳細が示されます。
  - **b.** ドロップダウンリストから Threat Defense Virtual バージョンを選択し、[選択（Select）] をクリックします。

ステップ 6 [ストレージ（Storage）] セクションに移動します。デフォルト値を保持して続行します。

ステップ 7 [帯域幅とセキュリティグループ（Bandwidth and Security Groups）] セクションに移動し、次の手順を実行します。

- **ENI**
  - [セキュリティグループ（Security Group）]：適切なセキュリティグループを選択します。
  - [プライマリ ENI（Primary ENI）]：[ネットワークとゾーン（Network and Zone）] フィールドで選択したように、管理 vSwitch であるプライマリインターフェイスを入力します。
  - [セカンダリ ENI（Secondary ENI）]：[既存のセキュリティ インターフェイス（Existing Secondary Interface）] ドロップダウンリストからセカンダリインターフェイスを選択するか、必要な vSwitch を選択して新しいセカンダリインターフェイスを作成します。

    Note
    インスタンス起動フェーズでは、インスタンスを 2 つの インターフェイスで展開でき、展開後に他の 2 つの インターフェイスを ECS コンソールからアタッチできます。
  - [キーペア（Key Pair）]：ドロップダウンリストから既存のキーペアを選択するか、新しいキーペアを作成します。

ステップ 8 [詳細設定（Advance Settings）] に移動し、次の手順を実行します。

- [インスタンス名（Instance Name）]：適切なインスタンスの名前。
- [ユーザーデータ（User Data）]：要件に従って Day-0 構成を指定します（[Base64 でエンコードされた情報を入力（Enter Base64 Encoded Information）] チェックボックスはオンにしないでください）。

  Management Center を使用して Threat Defense Virtual を管理するためのサンプル Day-0 構成：

```
{
"AdminPassword": "<your_password>",
"Hostname": "<your_hostname>",
"ManageLocally": "No",
"FmcIp":  "<IP address of FMC>",
```

```
"FmcRegKey":"<registration_passkey>",
"FmcNatId":"<NAT_ID_if_required>"
}
```

Note
Day 0 構成でパスワードを指定しない場合、デフォルトのパスワードが、Alibaba コンソールまたは CLI に表示される Threat Defense Virtual のインスタンス ID になります。

ステップ 9 [ECS の利用規約（ECS Terms of Service）] に同意し、[注文の作成（Create Order）] をクリックします。Threat Defense Virtual は 2 つのインターフェイスで起動され、それらは ECS コンソールで表示できます。

Note
起動プロセスを完了するには、4 つのインターフェイスで Threat Defense Virtual を設定する必要があります。

ステップ 10 Threat Defense Virtual を他の 2 つのインターフェイスで設定するには、次の手順を実行します。

a) Alibaba Cloud で、**[Elastic コンピューティングサービス（Elastic Compute Service）]** に移動します。
b) 左側のペインにある [ネットワークとセキュリティ（Network & Security）] の下の [Elastic Network Interface] をクリックします。
c) 以前に作成したトラフィック インターフェイスを検索します。
d) トラフィック インターフェイスに対応するチェックボックスをオンにして、[インスタンスにバインド（Bind to Instance）] をクリックします。[インスタンスにバインド（Bind to Instance）] ダイアログボックスが表示されます。
e) [インスタンス（Instance）] フィールドに Threat Defense Virtual の名前を入力します。
f) [確認（Confirm）] をクリックして、それをインスタンスの **eth2** インターフェイスとして設定します。
g) **手順 c** ～**手順 f** を繰り返して、Threat Defense Virtual の **eth3** インターフェイスを設定します。

ステップ 11 **[ECS ダッシュボード（ECS Dashboard）]** > **[インスタンス（Instances）]** の順にクリックします。

ステップ 12 起動が完了すると、Threat Defense Virtual を Management Center Virtual に登録できるはずです。

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。