Alibaba Cloud への ASA Virtual の導入

Cisco 適応型セキュリティ仮想アプライアンスは、物理的な Cisco 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。パブリック Alibaba Cloud に ASA Virtual を導入および設定して、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。ASA Virtual では、時間の経過とともに場所を拡張、縮小、または移動できます。

重要 9.13(1) 以降では、サポートされているすべての ASA Virtual vCPU/メモリ構成ですべての ASA Virtual ライセンスを使用できるようになり、ASA Virtual ライセンスを使用し、ASA Virtual を使用しているお客様は、さまざまな VM リソースフットプリントで実行できます。また、ASA Virtual ライセンスでは、サポート対象の Alibaba インスタンスタイプの数も増えます。

概要

ASA Virtual は、次の Alibaba インスタンスタイプをサポートしています。

Alibaba Cloud がサポートするインスタンスタイプ

ネットワーク拡張マシンタイプ		
設定	vCPU の数	メモリ（GB）
ecs.g5ne.large	2	8

ネットワーク拡張マシンタイプ		
設定	vCPU の数	メモリ（GB）
ecs.g5ne.xlarge	4	16
ecs.g5ne.2xlarge	8	32
ecs.g5ne.4xlarge	16	64

（注） Alibaba Cloud にインストールされている ASA Virtual のインスタンスタイプのサイズ変更は、サポートされていません。別のインスタンスタイプを持つ新しい ASA Virtual の展開のみが可能です。

ネットワーク要件

- 基本的な ASA Virtual サポート用に、最低 1 つの vSwitch（サブネット）を持つ 1 つの VPC を作成します。
- vSwitch は、インスタンスの導入先と同じゾーンにある必要があり、同じゾーン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。

前提条件

- https://www.alibabacloud.com/ でアカウントを作成します。
- ASA Virtual にライセンスを付与します。ライセンスを付与するまで、ASA Virtual 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。「ASA 仮想 のライセンス」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
  - 内部および外部インターフェイス
- 通信パス：
  - 管理インターフェイス：SSH アクセスと、ASA Virtual を ASDM に接続するために使用されます。
  - 内部インターフェイス（必須）：内部ホストに ASA Virtual 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 Virtual 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。

- ASA Virtual の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。

注意事項と制約事項

サポートされる機能

Alibaba 上の ASA Virtual は、次の機能をサポートしています。

- 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 ASA 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.large、ecs.g5ne.xlarge、ecs.g5ne.2xlarge、および ecs.g5ne.4xlarge
- BYOL ライセンスのサポート

サポートされない機能

Alibaba 上の ASA Virtual は、バージョン 7.2 では次の機能をサポートしていません。

- 高可用性機能
- 自動スケール
- IPv6
- SR-IOV

制限事項

- サブネットレベルのルーティングが許可されていないため、Alibaba では同じ VPC 内の East-West トラフィックはサポートされていません。
- 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現在サポートされていません。
- ASA Virtual アプリケーションを導入するには、ネットワーク拡張インスタンス仕様ファミリ g5ne を使用することを推奨します。

- ジャンボフレームは、Alibaba の少数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。

関連資料

詳細については、Alibaba Cloud を参照してください。

ポリシーとデバイス設定の設定

ここでは、ASA 仮想 を展開する前に作成および設定する必要があるリソースについて詳しく説明します。

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 ASA 仮想 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) 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

- ASA 仮想 のインスタンスの 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

ASA 仮想 の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。ASA 仮想 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

- ASA 仮想 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 ASA 仮想 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

ASA 仮想 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。ASA 仮想 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、ASA 仮想 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、ASA 仮想 を展開します。

Alibaba 環境の設定

ASA 仮想 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。

ASA 仮想 の展開には、ASA 仮想を展開する前に 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。

3 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。
- 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、ASA 仮想 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。

ASA 仮想 の導入

次の手順は、Alibaba Cloud で ASA 仮想 を展開する手順の概略です。

手順

ステップ 1 ASA 仮想 を展開するには、https://marketplace.alibabacloud.com/ に移動し、「**Cisco Secure Firewall ASA Virtual - BYOL**」製品を検索します。

（注）
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 Secure Firewall ASA Virtual - 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。

  （注）
  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.large**、**ecs.g5ne.xlarge**、**ecs.g5ne.2xlarge**、または **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 ASA 仮想 マーケットプレイス バージョンが表示されます。
  1. [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 ASA 仮想イメージの詳細が示されます。
  2. ドロップダウンリストから ASA 仮想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。

    （注）
    インスタンス起動フェーズでは、インスタンスを *1* つまたは *2* つ（プライマリ ENI またはプライマリとセカンダリの 2 つの ENI）のインターフェイスで展開でき、展開後に他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 ASA 仮想 を管理するためのサンプル Day 0 構成：

```
{
"ASA Version
!
interface management0/0
nameif management
security-level 100
no shut

interface gigabitethernet0/0
nameif inside
security-level 100
no shut

interface gigabitethernet1/0
nameif outside
security-level 100
no shut

crypto key generate rsa general-keys modulus 4096
ssh ::/0 inside
ssh timeout 60
ssh version 2
aaa authentication ssh console LOCAL

dns domain-lookup management
dns server-group DefaultDNS
name-server 8.8.8.8
}
```

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。ASA 仮想 は *1* つのインターフェイスで起動され、そのインターフェイスは ECS コンソールで表示できます。

ステップ 10 ASA 仮想 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 ASA 仮想 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。

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。

次のタスク

SSH を介して入力できる CLI コマンドを使用するか、または ASDM を使用して、設定を続行します。ASDM にアクセスする手順については、「ASDM の開始」を参照してください。

パフォーマンスの調整

VPN の最適化

Alibaba c5 インスタンスは、以前の c3、c4、および m4 インスタンスよりもはるかに高いパフォーマンスを提供します。c5 インスタンスファミリでのおおよその RA VPN スループット（AES-CBC 暗号化による 450B TCP トラフィックを使用する DTLS）は、以下のようである必要があります。

- 0.5 Gbps（c5.large）
- 1 Gbps（c5.xlarge）
- 2 Gbps（c5.2xlarge）
- 4Gbps（c5.4xlarge）

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。