# Threat Defense Virtual の Alibaba Cloud への展開



# Alibaba Cloud への展開について

Alibaba はパブリッククラウド環境です。Secure Firewall Threat Defense Virtual は、Alibaba 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 |

（注） 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 つのインターフェース（ENI）が必要です。

### 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。

# Cisco Secure Firewall Threat Defense Virtual の前提条件

- Alibaba のアカウント。https://www.alibaba.com/ で 1 つ作成できます。
- Threat Defense Virtual のコンソールにアクセスするには、SSH クライアント（例：Windows の場合は PuTTY、Macintosh の場合はターミナル）が必要です。
- Cisco.com から Threat Defense Virtual の QCOW2 ファイルをダウンロードします。

  https://software.cisco.com/download/navigator.html

（注） Cisco.com のログインおよびシスコ サービス契約が必要です。

- Cisco スマートアカウント。Cisco Software Central で作成できます。 https://software.cisco.com/
- Cisco Secure Firewall Threat Defense Virtual のライセンス
  - Cisco Secure Firewall 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。
- Cisco Secure Firewall Threat Defense Virtual インターフェイスのシステム要件
  - 管理インターフェイス（1）：Cisco Secure Firewall Threat Defense Virtual を Cisco Secure Firewall Management Center 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。

    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）：Cisco Secure Firewall Threat Defense Virtual を内部の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：
  - Cisco Secure Firewall Threat Defense Virtual にアクセスするためのパブリック IP と Elastic IP。

# Threat Defense Virtual と Alibaba の機能サポートと制限事項

### サポートされる機能

- QCOW2 イメージパッケージ
- 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。

**表 *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 |
|---|---|---|---|
| Threat Defense Virtual5、100 Mbps | 4 コア/8 GB | 100Mbps | 50 |

| 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 |
|---|---|---|---|
| Threat Defense Virtual10、1 Gbps | 4 コア/8 GB | 1Gbps | 250 |
| Threat Defense Virtual20、3 Gbps | 4 コア/8 GB | 3 Gbps | 250 |
| Threat Defense Virtual30、5 Gbps | 8 コア/16 GB | 5 Gbps | 250 |
| Threat Defense Virtual50、10 Gbps | 12 コア/24 GB | 10 Gbps | 750 |
| Threat Defense Virtual100、16 Gbps | 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 Configuration*』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

FTDv 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。

**受信側スケーリング**：FTDv 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

- 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。

（注） Threat Tefense Virtual では、4 つのインターフェイスを起動する必要があります。

# ポリシーとデバイス設定の設定

Cisco Secure Firewall Threat Defense Virtual をインストールして、デバイスを Cisco Secure Firewall Management Center に追加したら、Cisco Secure Firewall Management Center のユーザーインターフェイスを使用して、Alibaba プラットフォーム上で稼働している Cisco Secure Firewall Threat Defense Virtual のデバイス管理を設定できます。アクセス コントロール ポリシーおよびその他の関連ポリシーを設定して適用すると、Cisco Secure Firewall 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、Cisco Secure Firewall Threat Defense Virtual で提供されるサービスを制御します。Cisco Secure Firewall Threat Defense Virtual でセキュリティポリシーを設定するには、Cisco Secure Firewall Management Center を使用します。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 Configuration Guide*』または Cisco Secure Firewall Management Center のオンライン ヘルプを参照してください。

# Cisco Secure Firewall Threat Defense Virtual インスタンスの展開

展開する Threat Defense Virtual のイメージが [イメージの設定（Image Configuration）] ページに表示されていることを確認します。

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

（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** **カスタム仮想化イメージの作成**

Alibaba は QCOW2 イメージのみをサポートしています。

a) Object Storage Service（OSS）に移動して、QCOW2 イメージを含むバケットを作成し、以下を実行します。

バケット名は、Alibaba プロジェクト内でグローバルに一意である必要があります。

1. ローカルディレクトリから Alibaba バケットに QCOW2 イメージをアップロードします。
2. 左側のナビゲーションウィンドウで**[バケット（Buckets）]** > **[Threat Defense Virtualバケット（Threat Defense Virtual Bucket）]** > **[アップロード（Upload）]**の順に選択します。
3. アップロードが正常に完了したら、[プライベート（Private）] を ACL として選択し、オブジェクトの詳細に記載されている OSS オブジェクトアドレスをコピーします。
4. バケットからカスタムイメージの OSS オブジェクトアドレスを貼り付けます。
5. [Linux] を OS としてを選択し、[その他のLinux（Others Linux）] をバリアントタイプとして選択します。
6. システムアーキテクチャには [x86_64] をシステムアーキテクチャとして選択します。
7. イメージ形式には [QCOW2] を選択します。
8. [BYOL] をライセンス タイプとして 選択します。

b) 前のステップの準仮想化イメージからインスタンスを作成します。

1. 左側のナビゲーションウィンドウで**[イメージ（Images）]**>**[カスタムイメージ（Custom Image）]**> **[アクション（Actions）]** > **[インスタンスの作成（Create Instance）]**の順に選択します。

**ステップ 3　カスタム仮想化イメージからインスタンスを作成**

a) **Elasticコンピューティング サービス（Elastic Compute Service）]** > **[インスタンスの作成（Create Instance）]**に移動して、以下を選択します。

1. [課金方式 （Billing Method）] : 従量制課金（Pay-As-You-Go）
2. [地域（Region）] : 要件に従って選択。
3. [インスタンスタイプ（Instance Type）] : ecs.g5ne.xlarge /ecs.g5ne.2xlarge /ecs.g5ne.4xlarge
4. [数量（Quantity）] : 必要に応じて設定します。
5. [イメージ（Image）] : 前の項で作成したカスタム イメージ。
6. [システムディスク（System Disk）] : 最小値として 49GB（デフォルト）を選択します。

b) さらに続行するには、以下を実行します。

1. [VPC] : Threat Defense Virtual を展開する予定です。
2. [Vswitch] : プライマリインターフェイスのサブネット。
3. [パブリックIPv4アドレスの割り当て（Assign Public IPv4 Address）] : SSH を使用して接続する必要があります（選択されていない場合、Threat Defense Virtual には、Alibaba のコンソール接続を介してのみアクセスできます）。
4. [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。

5. [インターフェイス（Interfaces）]：プライマリ インターフェイスは、手順2で選択したサブネットに属しています。インスタンスは2つのインターフェイスで展開でき、残りは展開後に紐づけできます。

c) 次のセクションに移動して、以下を実行します。

1. [キーペア（Key-Pair）]：キーベースのログインの場合、まだ行われていない場合はキー ペアを生成します。パスワードを使用してインスタンスにアクセスすることもできます。

（注） 既存のキーペアを選択することも、新しいキーペアを作成することもできます。キーペアは、Alibaba 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場合があるため、必ず既知の場所に保存してください。

2. [インスタンス名（Instance-name）]：適切なインスタンスの名前。

3. [Day-0（ユーザーデータ）（Day-0 (User Data)）]：要件に従って Day-0 構成を指定します（**Base64** でのエンコードは選択しないでください）。

**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**：

```
#Sensor
{
            "AdminPassword": "<your_password>",
            "Hostname": "<your_hostname>",
            "ManageLocally": "No",
            "FmcIp":  "<IP address of FMC>",
            "FmcRegKey":"<registration_passkey>",
            "FmcNatId":"<NAT_ID_if_required>"
}
```

（注） 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は、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。

d) 利用規約に同意してインスタンスを作成します。

**ステップ 4** [確認して起動する（Review and Launch）] をクリックします。

**ステップ 5** [起動（Launch）] をクリックします。

**ステップ 6** 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 7** [インスタンスの起動（Launch Instances）] をクリックします。

**ステップ 8** [起動の表示（View Launch）] をクリックし、プロンプトに従います。

**ステップ 9** [EC2ダッシュボード（EC2 Dashboard）] > [インスタンス（Instances）] の順にクリックします。

**ステップ 10** 起動が完了するとすぐに、脅威防御を Management Center 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。