Deploy the Threat Defense Virtual on the Alibaba Cloud

- Overview, on page 1
- Prerequisites, on page 2
- Guidelines and Limitations, on page 3
- Configuring Policies and Device Settings, on page 4
- Deploy the Threat Defense Virtual, on page 4

Overview

Alibaba Cloud is a public cloud environment. The Threat Defense Virtual runs as a guest in the Alibaba Cloud environment.

Alibaba Supported Instance Types

Threat Defense Virtual on Alibaba can use the following instance types:

Network Enhanced Machine Types			
Configuration	**No of vCPUs**	**Memory (GB)**	**Maximum Interfaces Supported**
ecs.g5ne.xlarge	4	16	4
ecs.g5ne.2xlarge	8	32	6
ecs.g5ne.4xlarge	16	64	8

Note Threat Defense Virtual needs a minimum of four interfaces (ENIs) to support the instance.

Network Requirement

- You can create one VPC with four Vswitch (Subnet) for basic Threat Defense Virtual support.

- Management Vswitch must be available in the same zone in which instance is being deployed, otherwise, you have to create it.

Related Documentation

For more information on instance types and their configuration, see Alibaba Cloud

Prerequisites

- An Alibaba account. You can create one at https://www.alibaba.com/.
- An SSH client (for example, PuTTY on Windows or Terminal on Macintosh) is required to access the Threat Defense Virtual console.
- Download the Threat Defense Virtual QCOW2 file from Cisco.com.

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

Note A Cisco.com login and Cisco service contract are required.

- A Cisco Smart Account. You can create one at Cisco Software Central. https://software.cisco.com/
- License the Threat Defense Virtual.
  - Configure all license entitlements for the security services from the Management Center Virtual.
  - See "Licensing the Secure Firewall System" in the Secure Firewall Management Center Configuration Guide for more information about how to manage licenses.
- Threat Defense Virtual interface requirements:
  - Management interfaces (1)—Used to connect the Threat Defense Virtual to the Management Center Virtual,
  - Second Interface is used for diagnostics; can't be used for through traffic.

    In 6.7 and later, you can optionally configure a data interface for FMC management instead of the Management interface. The Management interface is a prerequisite for data interface management, so you still need to configure it in your initial setup. FMC access from a data interface isn't supported in High Availability deployments. For more information about configuring a data interface for FMC access, see the **configure network management-data-interface** command in the FTD command reference.
  - Traffic interfaces (2)—Used to connect the Threat Defense Virtual to inside hosts and to the public network.
- Communication Paths:
  - Public and elastic IPs for access into the Threat Defense Virtual.

Guidelines and Limitations

Supported Features

- QCOW2 Image package
- Basic Product Bringup
- Day-0 Configuration
- SSH using Public Key or Password.
- Alibaba UI Console to access Threat Defense Virtual for any debugging purpose.
- Alibaba UI Stop/Restart
- Instance Type Supported: ecs.g5ne.xlarge, ecs.g5ne.2xlarge, and ecs.g5ne.4xlarge.
- Hyperthreading
- Bring Your Own License (BYOL) License Support.

Performance Tiers for Threat Defense Virtual Smart Licensing

The supports performance-tiered licensing that provides different throughput levels and VPN connection limits based on deployment requirements.

Table 1: Licensed Feature Limits Based on Entitlement

Performance Tier	Device Specifications (Core/RAM)	Rate Limit	RA VPN Session Limit
FTDv5, 100Mbps	4 core/8 GB	100Mbps	50
FTDv10, 1Gbps	4 core/8 GB	1Gbps	250
FTDv20, 3Gbps	4 core/8 GB	3Gbps	250
FTDv30, 5Gbps	8 core/16 GB	5Gbps	250
FTDv50, 10Gbps	12 core/24 GB	10Gbps	750
FTDv, 16Gbps	16 core/34 GB	16Gbps	10,000

- BYOL (Bring Your Own License) using a Cisco Smart License Account.

See the "Licensing the Threat Defense Virtual System" chapter in the *Threat Defense Virtual Management Center Configuration* for guidelines when licensing your Threat Defense Virtual device.

Performance Optimizations

To achieve the best performance out of the Threat Defense Virtual, you can make adjustments to the both the VM and the host. See Virtualization Tuning and Optimization on Alibaba Cloud for more information.

Receive Side Scaling—The Threat Defense Virtual supports Receive Side Scaling (RSS), which is a technology utilized by network adapters to distribute network receive traffic to multiple processor cores. Supported on Version 7.0 and later. See Multiple RX Queues for Receive Side Scaling (RSS) for more information.

Unsupported Features

- FDM
- High Availability Functionality
- Autoscale
- IPv6
- SR-IOV

Limitations

- Transparent, inline, and passive modes are not supported in 7.2 release.
- East-West Traffic is not supported in Alibaba.
- Jumbo Frames is not supported as its availability is limited to a few instance types from Alibaba. For more information, see Alibaba Cloud.

Note Threat Defense Virtual must have four interfaces to launch.

Configuring Policies and Device Settings

After you install Threat Defense Virtual and add the device to a Management Center Virtual, you can use the management center virtual user interface to configure device management settings for Threat Defense Virtual running on Alibaba. You can configure and apply access control policies and other related policies to manage traffic using your Threat Defense Virtual instance.

The security policy controls the services provided by the Threat Defense Virtual, such as Next Generation IPS filtering and application filtering. You configure the security policy on the Threat Defense Virtual using the Management Center Virtual. For information about how to configure the security policy, see the *Secure Firewall Configuration Guide* or the online help in Management Center Virtual.

Deploy the Threat Defense Virtual

Ensure that the image of the Threat Defense Virtual that you plan to deploy apears on the **Image Configuration**.

Step 1 Log into https://www.alibabacloud.com/ and choose your region.

Note Alibaba is divided into multiple regions that are isolated from each other. The region is displayed in the upper right corner of your window. Resources in one region do not appear in another region. Check periodically to make sure you are in the intended region.

Step 2 **Create Custom Virtualized Image**

Alibaba supports QCOW2 image only.

a) Go to Object Storage Service (OSS), then create a bucket that contains the QCOW2 image and do the following:

Bucket names must be globally unique within your Alibaba project.

1. Upload QCOW2 image from local directory to Alibaba bucket.
2. From the left Navigation pane, click **Buckets** > **Threat Defense Virtual Bucket** > **Upload**
3. Choose **Private** as ACL and copy the OSS Object address mentioned in the object details after the upload is completed successfully.
4. Paste the OSS object address of custom image from the bucket.
5. Choose **Linux** as OS and **Others Linux** as variant type.
6. Choose **x86_64** as System Architecture.
7. Choose Image format as **QCOW2.**
8. Choose license type as BYOL.

b) Create an instance from the para-virtualized image from the previous step.

1. From the left side Navigation pane, click **Images** > **Custom Image** > **Actions** > **Create Instance**

Step 3 **Create Instance from Custom Virtualized Image**

a) Go to the **Elastic Compute Service** > **Create Instance** and select the following:

1. **Billing Method**: Pay-As-You-Go
2. **Region**: As per requirement.
3. **Instance Type**: ecs.g5ne.xlarge /ecs.g5ne.2xlarge /ecs.g5ne.4xlarge
4. **Quantity**: As required.
5. **Image**: Custom image you created in the previous section.
6. **System Disk**: Select 49GB (Default) as the minimum value.

b) To proceed further, do the following:

1. **VPC**: You plan to deploy Threat Defense Virtual.
2. **Vswitch**: Subnet of the Primary Interface.
3. **Assign Public IPv4 Address:** It's required to connect using SSH (If not selected, then the Threat Defense Virtual can only be accessed via Console connection of Alibaba).
4. **Security Group**: Choose the appropriate Security Group.
5. **Interfaces**: Primary interface belongs to the subnet chosen in step 2. An instance can be deployed with two interfaces and the rest can be attached after deployment.

c) Move to the next section and do the following.

1. **Key-Pair**: For key-based login, generate a key-pair if not done already. You can also access the instance with a password.

   Note You can select an existing key pair, or create a new key pair. The key pair consists of a public key that Alibaba stores and a private key file that the user stores. Together, they allow you to connect to your instance securely. Be sure to save the key pair to a known location, as it may be required to connect to the instance.

2. **Instance-name**: Name of instance as suitable.
3. **Day-0 (User Data)**: Provide the Day-0 configuration as per the requirement (Do not choose **64 base** encoded).

   Sample Day-0 Configuration to manage Threat Defense Virtual using the Management Center:

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

   Note In case the user does not provide any password in the day-0 configuration, the default password will be the instance ID of the Threat Defense Virtual as seen on Alibaba Console or CLI.

d) Accept the Terms of Service and Create the Instance.

Step 4 Click **Review and Launch**.

Step 5 Click **Launch**.

Step 6 Select an existing key pair or create a new key pair.

Step 7 Click **Launch Instances**.

Step 8 Click **View Launch** and follow the prompts.

Step 9 Click **EC2 Dashboard > Instances**.

Step 10 You should be able to register your Threat Defense Virtual to the Management Center Virtual after it finishes booting up.