Deploy the ASA Virtual on Alibaba Cloud

The Cisco Adaptive Security Appliance Virtual runs the same software as physical Cisco ASAs to deliver proven security functionality in a virtual form factor. You can deploy and configure the ASA Virtual in the public Alibaba cloud to protect virtual and physical data center workloads. The ASA Virtual can expand, contract, or shift their location over time.

Important Beginning with 9.13(1), You can use any ASA Virtual license on any supported ASA Virtual vCPU/memory configuration. The ASA Virtual license allows ASA Virtual customers to run on a wide variety of VM resource footprints. This ASA Virtual license also increases the number of supported Alibaba instances types.

Overview

The ASA Virtual support the following Alibaba instance types.

Alibaba Cloud Supported Instance Types and ASA Virtual Versions

Alibaba ECS Instance Type	Attributes		Maximum Number of Interfaces	ASA Virtual Version
	vCPUs	Memory (GB)		
ecs.g5ne.large	2	8	2	9.20 and later
ecs.g5ne.xlarge	4	16	4	9.20 and later
ecs.g5ne.2xlarge	8	32	4	9.20 and later
ecs.g5ne.4xlarge	16	64	4	9.20 and later

Alibaba ECS Instance Type	Attributes		Maximum Number of Interfaces	ASA Virtual Version
	vCPUs	Memory (GB)		
ecs.c7.large	2	8	2	9.20 and later
ecs.c7.xlarge	4	16	4	9.20 and later
ecs.c7.2xlarge	8	32	4	9.20 and later
ecs.c7.4xlarge	16	64	4	9.20 and later
ecs.c7nex.large	2	8	2	9.20 and later
ecs.c7nex.xlarge	4	16	4	9.20 and later
ecs.c7nex.2xlarge	8	32	4	9.20 and later
ecs.c7nex.4xlarge	16	64	4	9.20 and later
ecs.c6.large	2	8	2	9.20 and later
ecs.c6.xlarge	4	16	4	9.20 and later
ecs.c6.2xlarge	8	32	4	9.20 and later
ecs.c6.4xlarge	16	64	4	9.20 and later
ecs.c6e.large	2	8	2	9.20 and later
ecs.c6e.xlarge	4	16	4	9.20 and later
ecs.c6e.2xlarge	8	32	4	9.20 and later
ecs.c6e.4xlarge	16	64	4	9.20 and later
ecs.c8i.xlarge	4	8	4	9.24.10 and later
ecs.c8i.2xlarge	8	16	4	9.24.10 and later
ecs.c8i.4xlarge	16	32	8	9.24.10 and later
ecs.c8ine.xlarge	4	8	4	9.24.10 and later
ecs.c8ine.2xlarge	8	16	6	9.24.10 and later
ecs.c8ine.4xlarge	16	32	8	9.24.10 and later
ecs.c7nex.xlarge	4	8	4	9.24.10 and later
ecs.c7nex.2xlarge	8	16	6	9.24.10 and later
ecs.c7nex.4xlarge	16	32	8	9.24.10 and later
ecs.c9i.xlarge	4	8	4	9.24.10 and later
ecs.c9i.2xlarge	8	16	8	9.24.10 and later

Alibaba ECS Instance Type	Attributes		Maximum Number of Interfaces	ASA Virtual Version
	vCPUs	Memory (GB)		
ecs.c9i.4xlarge	16	32	8	9.24.10 and later

Note

- ASA virtual maximum vCPU limit: ASA virtual supports a maximum of 16 vCPUs. Instances exceeding this capacity are not supported. ASAvU (ASAv-Unlimited) is supported only on KVM, VMware, and AWS.
- ASA virtual minimum vCPU requirement: ASA virtual requires a minimum of 4 vCPUs. Instances with fewer than 4 vCPUs are not supported.
- The ASAv50 and ASAv100 models are not supported on Alibaba Cloud.

Note Resizing the instance type of an ASA Virtual installed on Alibaba Cloud is not supported. You can only deploy a new ASA Virtual with a different instance type.

Note

- By default, ASA Virtual instances are deployed using UEFI mode.
- **Limitation**: Secure Boot functionality is not supported due to cloud limitation.

Network Requirement

- Create one VPC with a minimum of one Vswitch (Subnet) for basic ASA Virtual support.
- 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

- Create an account on https://www.alibabacloud.com/.
- License the ASA Virtual. Until you license the ASA Virtual, it runs in degraded mode, which allows only 100 connections and throughput of 100 Kbps. See Licensing for the ASA Virtual.
- Interface requirements:
  - Management interface

- Inside and outside interfaces.

- Communications paths:
  - Management interface—Used for SSH access and to connect the ASA Virtual to the ASDM.
  - Inside interface (required)—Used to connect the ASA Virtual to inside hosts.
  - Outside interface (required)—Used to connect the ASA Virtual to the public network.
- For ASA Virtual system requirements, see Cisco ASA Compatibility.

Guidelines and Limitations

Supported Features

The ASA Virtual on Alibaba supports the following features:

- Basic Product Bringup
- Day-0 Configuration
- SSH using Public Key or Password
- Alibaba UI Console to access ASA Virtual for any debugging purpose.
- Alibaba UI Stop/Restart
- Instance Type Supported: ecs.g5ne.large, ecs.g5ne.xlarge, ecs.g5ne.2xlarge, and ecs.g5ne.4xlarge
- BYOL License Support

Unsupported Features

The ASA Virtual on Alibaba does not support the following in version 7.2:

- High Availability functionality
- Autoscale
- IPv6
- SR-IOV

Limitations

- East-West Traffic in the same VPC is not supported in Alibaba as subnet level routing is not allowed.
- Transparent, inline, and passive modes are not currently supported.
- It is recommended to use the network enhanced instance specification family g5ne to deploy ASA Virtual applications.
- Jumbo Frames is not supported as its availability is limited to few instance types from Alibaba.

Upgrade Restrictions and Limitations

Revert upgrade restrictions

Caution Reverting an upgrade is not supported.

Ensure that you take a backup before upgrading. After upgrading to ASA Virtual 9.24, you cannot roll back to a previous software version. To return to an earlier version, you must redeploy the Management Center.

Related Documentation

For more information, see Alibaba Cloud.

Configuring Policies and Device Settings

The following sections provide more information about the resources you need to create and configure before deploying the ASA Virtual.

Creating the VPC

A virtual private cloud (VPC) is a virtual network dedicated to your Alibaba account. It is logically isolated from other virtual networks in the Alibaba cloud. You can launch your Alibaba Cloud resources, such as the Management Center Virtual and the ASA Virtual instances, into your VPC. You can configure your VPC; you can select its IP address range, create VSwitches (subnets), and configure route tables, network gateways, and security settings.

Procedure

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

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

Step 2 Click **Products** > **VPC**.

Step 3 Click **VPC Dashboard** > **Your VPCs**.

Step 4 Click **Create VPC**.

Step 5 Enter the following in the **Create VPC** dialog box:

a) A user-defined **Name tag** to identify the VPC.

b) An **IPv4 CIDR block** of IP addresses. CIDR (Classless Inter-Domain Routing) notation is a compact representation of an IP address and its associated routing prefix. For example, 10.0.0.0/24.

c) A **Tenancy setting** of default to ensure that instances launched in this VPC use the tenancy attribute specified at launch.

Step 6 Click **OK** to create your VPC.

What to do next

Add an Internet gateway to your VPC as described in the next section.

Adding the Internet Gateway

You can add an Internet gateway (NAT Gateway) to connect your VPC to the Internet. You can route traffic for IP addresses outside your VPC to the Internet gateway.

Before You Begin

- Create a VPC for your ASA Virtual instances.

Procedure

Step 1 Click **Products** > **VPC**.

Step 2 Click **VPC Dashboard** > **Internet Gateways**, and then click **Create Internet Gateway**.

Step 3 Enter a user-defined **Name tag** to identify the gateway and click **OK** to create the gateway.

Step 4 Select the gateway created in the previous step.

Step 5 Click **Bind to VPC**and select the VPC you created previously.

Step 6 Click **OK** to bind the gateway to your VPC.

By default, the instances launched in the VPC cannot communicate with the Internet until a NAT Gateway is created and bound to the VPC.

What to do next

Add VSwitch (subnets) to your VPC as described in the next section.

Adding vSwitch

You can segment the IP address range of your VPC that the ASA Virtual instances can be attached to. You can create vSwitch (subnets) to group instances according to security and operational needs. For the ASA Virtual you need to create a vSwitch for management as well as vSwitches for traffic.

Before You Begin

- Create four VPCs for your ASA Virtual instances. As mentioned in creating VPC section.
- Add one vSwitch (subnet) for each VPC.

Procedure

Step 1 Click **Products** > **VPC**.

Step 2 Click **VPC Dashboard** > **VSwitches**, and then click **Click vSwitch**.

Step 3 Enter the following in the **Create vSwitch** dialog box:

a) A user-defined **Name tag** to identify the vSwitch.
b) A **VPC** to use for this vSwitch.
c) The **Zone** where this vSwitch will reside. Select **No Preference** to let Alibaba Cloud select the zone.
d) A **CIDR block** of IP addresses (IPv4). The range of IP addresses in the vSwitch must be a subset of the range of IP addresses in the VPC. Block sizes must be between a /16 network mask and a /28 network mask. The size of the vSwitch can equal the size of the VPC.

Step 4 Click **OK** to create your vSwitch.

Step 5 Repeat for as many vSwitchs' required. Create a separate vSwitch for management traffic and create as many vSwitchs' as needed for data traffic.

What to do next

Add a route table to your VPC as described in the next section.

Adding a Route Table

You can attach a route table to the gateway you configured for your VPC. You can also associate multiple subnets with a single route table, but a subnet can be associated with only one route table at a time.

Procedure

Step 1 Click **Products** > **VPC**.

Step 2 Click **VPC Dashboard** > **Route Tables**, and then click **Create Route**.

Step 3 Enter a user-defined **Name tag** to identify the route table.

Step 4 Select the **VPC** from the drop-down list that will use this route table.

Step 5 Click **OK** to create your route table.

Step 6 Select the route table that you created.

Step 7 Click the **Routes** tab to display the route information in the details pane.

Step 8 Click **Edit**, then click **Add another route**.

a) In the **Destination** column, enter **0.0.0.0/0**for all IPv4 traffic.
b) In the **Target** column, select your gateway.

Step 9 Click **Save**.

What to do next

Create a security group as described in the next section.

Creating a Security Group

You can create a security group with rules specifying allowed protocols, ports and source IP ranges. Multiple security groups can be created with different rules which you can assign to each instance.

Procedure

Step 1 Click **Products** > **ECS**.

Step 2 Click **ECS Dashboard** > **Security Groups**.

Step 3 Click **Create Security Group**.

Step 4 Enter the following in the **Create Security Group** dialog box:

a) A user-defined **Security Group Name** to identify the security group.

b) A **Description** for this security group.

c) The **VPC** associated with this security group.

Step 5 Configure **Security Group Rules**:

a) Click the **Inbound Rules** tab, then click **Add Rule**.

Note
HTTPS and SSH access is required to manage the Management Center Virtual from outside Alibaba. You should specify the Source IP addresses accordingly. Also, if you are configuring both the Management Center Virtual and ASA Virtual within the Alibaba VPC, you should allow the private IP management subnet access.

b) Click the **Outbound Rules** tab, then click **Add Rule** to add a rule for outbound traffic, or leave the defaults of **All traffic** (for **Type**) and **Anywhere** (for **Destination**).

Step 6 Click **Create** to create your security group.

What to do next

Create network interfaces as described in the next section.

Creating Network Interfaces

You can create network interfaces for the ASA Virtual using static IP addresses (IPv4) or DHCP. Create network interfaces (external and internal) as needed for your particular deployment.

Procedure

Step 1 Click **Services** > **Elastic Network Interface**.

Step 2 Click **Network Interfaces**.

Step 3 Click **Create Network Interface**.

Step 4 Enter the following in the **Create Network Interface** dialog box:

a) A optional user-defined **Description** for the network interface.
b) Select a **vSwitch** from the drop-down list. Make sure to select the vSwitch of the VPC where you want to create the ASA Virtual instance.
c) Enter a **Private IP** address. You can use a static IP address (IPv4) or Auto-generate (DHCP).
d) Select one or more **Security groups**. Make sure the security group has all the required ports open.

Step 5 Click **Create network interface** to create your network interface.

Step 6 Select the network interface that you just created.

Step 7 Right-click and select **Modify Source/Dest. Check**.

Step 8 Uncheck the **Enable** check box under **Source/destination check** and click **Save**.

What to do next

Create elastic IP addresses as described in the next section.

Creating Elastic IP Address

When an instance is created, a public IP address is associated with the instance. That public IP address (IPv4) changes automatically when you STOP and START the instance. To resolve this issue, assign a persistent public IP address to the instance using Elastic IP addressing. Elastic IP address is a reserved public IP address that are used for remotely accessing the ASA Virtual as well as other instances.

Procedure

Step 1 Click **Products** > **Elastic Compute Service**.

Step 2 In the **Elastic Compute Service** dashboard, click **Elastic IP** from the left-hand menu.

Step 3 Click **Allocate Elastic IP Address**.

Step 4 Configure EIP settings:

a) Choose the **Region** where you want to allocate the EIP.
b) Select the desired bandwidth plan for the EIP. For example, BYOL or Subscription.
c) Specify the bandwidth amount required.
d) Review your selections and click **OK** to allocate the EIP.

Step 5 Associate the EIP with an instance:

a) After EIP allocation, go to the **Elastic IP** section in the **Elastic Compute Service** dashboard.
b) Find the EIP you created and click **Associate**.
c) Choose the ECS instance you want to associate with the EIP and click **OK**.

Step 6 Ensure that the EIP is now listed under the associated ECS instance and verify its connectivity.

What to do next

Deploy the ASA Virtual as described in the next section.

Configuring Alibaba Environment

To deploy the ASA Virtual on Alibaba you need to configure an Alibaba VPC with your deployment-specific requirements and settings. In most situations a setup wizard can guide you through your setup. Alibaba provides online documentation where you can find useful information about the services ranging from introductions to advanced features. For more information, see Alibaba Cloud Documentation.

The ASA Virtual deployment requires four network virtual private cloud (VPC) which you must create prior to deploying the ASA Virtual.

The three networks VPCs are:

- Management VPC for the management subnet.
- Inside VPC for the inside subnet.
- Outside VPC for the outside subnet.

For greater control over your Alibaba setup, the following sections offer a guide to your VPC and EC2 configurations prior to launching the ASA Virtual instances:

Before You Begin

- Create your Alibaba Cloud account.

Deploy the ASA Virtual

The following procedure is a top-level list of steps to deploy ASA Virtual on Alibaba Cloud.

Procedure

Step 1 Go to https://marketplace.alibabacloud.com/ and search for **`Cisco Secure Firewall ASA Virtual - BYOL`** offering to deploy the ASA Virtual.

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 Click the offering link to open **Cisco Secure Firewall ASA Virtual - BYOL** page.

Step 3 Click **Choose Your Plan**. You will be redirected to the **Elastic Compute Service** page.

Step 4 Enter the following details in the **Custom Launch** section.

- **Billing Method**: As per requirement.

Note

The billing method is for infrastructure on the Alibaba Cloud, which you can select according to your requirement.

- **Region**: As per requirement.
- **Network and Zone**: Select a VPC and management vSwitch, which you have previously created, from the drop-down list or use the **Create VPC** and **Create vSwitch** links to create newly.

Step 5 Move to the **Instances and Images** page.

Under the **All Instance Types** section, perform the following:

- **Instance**: Select any of the following supported instance type - **ecs.g5ne.large**, **ecs.g5ne.xlarge**, **ecs.g5ne.2xlarge**, or **ecs.g5ne.4xlarge**.
- **Image**: The latest ASA Virtual marketplace version is displayed in the **Marketplace Image REC** section.
  a. Click **Reselect Image**. The Alibaba Cloud Marketplace Image dialog box is displayed with ASA Virtual image details you are deploying.
  b. Choose the ASA Virtual version from the drop-down list and click **Select**.

Step 6 Move to the **Storage** section. Retain the default values and proceed.

Step 7 Move to the **Bandwidth and Security Groups** section and perform the following:

- **ENI**
  - **Security Group**: Choose the appropriate security group.
  - **Primary ENI**: Enter the primary interface, which is the management vSwitch, as selected in the **Network and Zone** field.
  - **Secondary ENI**: Choose the secondary interface from the **Existing Secondary Interface** drop-down list or create a new secondary interface by selecting the required vSwitch.

    Note
    During instance launch phase, an instance can be deployed with *one* or *two* (primary or both primary and secondary ENIs) interfaces and the other interfaces can be attached after deployment from ECS console.

  - **Key Pair**: Select an existing key pair from the drop-down list or create a new key pair.

Step 8 Move to the **Advance Settings** and perform the following:

- **Instance Name**: Name of the instance as suitable.
- **User Data**: Provide the Day-0 configuration as per the requirement (Do not choose the **Enter Base64 Encoded iInformation** check box).

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

```
{
"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
}
```

Step 9 Accept the **ECS Terms of Service** and click **Create Order**.
ASA Virtual is launched with *one* interface and you can view the interface on ECS console.

Step 10 To configure the ASA Virtual with two other interfaces, perform the following:

a) On the Alibaba Cloud, go to **Elastic Compute Service**.
b) Click **Elastic Network Interface** under **Network & Security** on the left pane.
c) Search for the traffic interface that is previously created.
d) Select the check box corresponding to a traffic interface, and click **Bind to Instance**. The **Bind to Instance** dialog box is displayed.
e) Enter the ASA Virtual name in the **Instance** field.
f) Click **Confirm** to configure it as **eth2** interface for your instance.

Step 11 Click **ECS Dashboard** > **Instances**.

What to do next

Continue configuration using CLI commands available for input via SSH or use ASDM. See Start ASDM for instructions for accessing the ASDM.

Performance Tuning

VPN Optimization

The Alibaba c5 instances offer much higher performance than the older c3, c4, and m4 instances. The approximate RA VPN throughput (DTLS using 450B TCP traffic with AES-CBC encryption) on the c5 instance family should be:

- 0.5Gbps on c5.large
- 1Gbps on c5.xlarge
- 2Gbps on c5.2xlarge

- 4Gbps on c5.4xlarge