



# BIG-IP VE in Alibaba Cloud

In this release of BIG-IP VE in Alibaba Cloud, you can configure BIG-IP VE with one NIC (called a single NIC deployment) or with multiple NICs. This document walks you through the creation of a single NIC and a three-NIC deployment.

Config Sync and High Availability are not currently available in Alibaba Cloud.

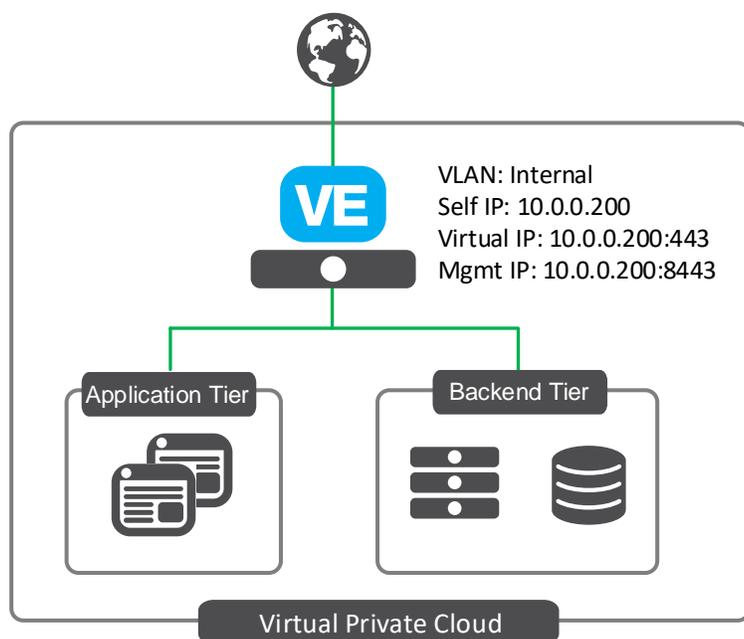
This content is also available online at [https://clouddocs.f5.com/cloud/public/v1/alibaba\\_index.html](https://clouddocs.f5.com/cloud/public/v1/alibaba_index.html)

- [Alibaba Cloud: Single NIC BIG-IP VE](#)
- [Alibaba Cloud: Three-NIC BIG-IP VE](#)

## Alibaba Cloud: Single NIC BIG-IP VE

The following diagram shows a basic single NIC deployment of BIG-IP VE in an Alibaba Virtual Private Cloud (VPC). Traffic is flowing through BIG-IP VE to application servers. The BIG-IP virtual server is listening for traffic destined for port 443. Port 8443 is for management traffic.

In this configuration, all access to the BIG-IP VE appliance is through the same IP address and virtual network interface (vNIC). (**Note:** vNICs are called ENIs in Alibaba.)



This document shows a specific example, which you can use to test a single NIC deployment. When done, you should be able to send traffic to your application servers through BIG-IP VE.

## Steps

The steps to create a single-NIC deployment are:

- [Create a VPC with one subnet](#)
- [Edit security rules for the VPC](#)
- [Create or add a key pair](#)
- [Deploy a BIG-IP VE instance](#)
- [Set the admin password](#)
- [License BIG-IP VE](#)
- [Provision BIG-IP VE](#)
- [Create a pool and add members to it](#)
- [Create a virtual server](#)

If you plan to use BYOL (Bring Your Own License) from F5, [learn more about F5 licensing](#). You can [get a trial license](#) if you need one.

### Create a VPC with one subnet

A BIG-IP VE instance must be in an Alibaba virtual private cloud (VPC). In this example, create a VPC with one subnet (called a VSwitch in Alibaba).

1. In the Alibaba Console, from the left menu, click **Virtual Private Cloud**.
2. On the top toolbar, select the region you want.
3. Click **Create VPC**.
4. Complete the fields. Note that "VSwitch" is the name Alibaba uses for subnet.  
For more information, see: <https://www.alibabacloud.com/help/doc-detail/65398.htm>
5. Click **OK**.
6. On the success screen, click **Complete**.

The VPC is displayed in the list.

### Edit security rules for the VPC

You must set rules that determine which traffic can access instances in the VPC.

1. In the list of VPCs, in the row for your VPC, in the Actions column, click **Manage**.
2. In the Network Resources section, next to Security Group, click the **0**.
3. In the top right, click **Create Security Group**.
4. Complete the fields.

Field	Value
Template	Customize
Security Group Name	A name you choose.
Network Type	VPC
VPC	The VPC you created earlier.

5. Click **OK**.
6. On the Notes dialog, click **Create Rules Now**.
7. In the top right, click **Add Security Group Rule**.
8. Complete the fields to allow SSH access to BIG-IP VE.

Field	Value
<b>Rule Direction</b>	<b>Ingress</b>
<b>Action</b>	<b>Allow</b>
<b>Protocol Type</b>	<b>SSH (22)</b>
<b>Priority</b>	<b>1</b>
<b>Authorization Type</b>	<b>IPv4 CIDR Block</b>
<b>Authorization Objects</b>	IP address or range on your network; these IP addresses can access the VPC.

9. Click **OK**.
10. Repeat steps 7-9 and complete the fields to allow access to the BIG-IP Configuration utility web interface:

Field	Value
<b>Rule Direction</b>	<b>Ingress</b>
<b>Action</b>	<b>Allow</b>
<b>Protocol Type</b>	<b>Customized TCP</b>
<b>Port Range</b>	<b>8443</b>
<b>Priority</b>	<b>1</b>
<b>Authorization Type</b>	<b>IPv4 CIDR Block</b>
<b>Authorization Objects</b>	IP address or range on your network; these IP addresses can access the VPC.

11. Click **OK**.

The rules are displayed in the list. Your application should also be in this VPC, so open the port for the application traffic as well.

## Create or add an SSH key pair

You will need a key pair to connect to BIG-IP VE and set the admin password.

1. In the Alibaba Console, from the left menu, click **Elastic Compute Service**.
2. On the left menu, under Networks and Security, click **SSH Key Pair**.
3. In the top right, click **Create SSH Key Pair**.
4. Type a name and either create or import a key pair.
5. Click **OK**.

The key pair name is displayed in the list.

## Deploy a BIG-IP VE instance

To create an instance of BIG-IP VE in Alibaba, you deploy a BIG-IP VE image from the Alibaba Marketplace.

1. In the Alibaba Console, from the left menu, click **Elastic Compute Service**.
2. On the left menu, click **Instances**.
3. In the top right, click **Create Instance**.
4. Complete the fields.

Field	Value
<b>Billing Method</b>	<p><b>Subscription</b> – You pay monthly for the instance.</p> <p><b>Pay-As-You-Go</b> – You pay based on time. If you are going to choose a BIG-IP VE PAYG image, you should choose this method.</p> <p><b>Preemptible Instance</b> is not supported.</p> <p>For more information, see <a href="#">Billing method comparison</a>.</p>
<b>Region</b>	Keep the default or change it.
<b>Instance Type</b>	<p>Choose at least 2 vCPU and 4 GB memory. For each vCPU, add at least 2 GB of memory.</p> <p>Also, ensure the instance type you choose has the number of available NICs you need. In this example, you only need one.</p>
<b>Image</b>	<p>Click <b>Marketplace Image</b> and search for F5.</p> <p>If you choose BYOL, you need <a href="#">an F5 license</a>. You can <a href="#">get a trial license</a> if you need one.</p> <p>If you expect to upgrade BIG-IP VE in the future, choose an image with 2 boot locations. If you do not need room to upgrade (if you intend to create a new instance when a new version of BIG-IP VE is released), choose an image with 1 boot location.</p>
<b>Storage</b>	<p>Accept the default or change it.</p> <p>For LTM, set the <b>System Disk</b> value to the minimum available size.</p>

5. Click **Next: Networking**.
6. Complete the fields.

Field	Value
<b>Network</b>	The VPC you created earlier and an associated VSwitch.
<b>Network Billing Method</b>	<p>Select <b>Assign public IP</b>.</p> <p>This IP address is for initial management access to BIG-IP VE and you can remove it later.</p> <p>If you have a jump host on the same VSwitch then you do not need this IP address.</p>

<b>Security Group</b>	Leave the default VPC security group.
<b>Elastic Network Interface</b>	Eth0 is displayed by default. In this example, you don't need to add another NIC. For other configurations, you can.

7. Click **Next: System Configurations**.
8. Complete the fields.

Field	Value
<b>Key Pair</b>	The key pair you created or imported earlier.  <b>Important:</b> A key pair is the only type of logon credentials you can use to connect to BIG-IP VE for the first time. The other settings ( <b>Inherit Password From Image, Password, and Set Later</b> ) do not work.
<b>Instance Name</b>	A name you choose.
<b>Host</b>	<b>Important:</b> This setting has no effect on BIG-IP VE.

9. Click **Next: Grouping**.
10. Click **Add Tag**. You may want to add a tag key named **Name** and a tag value with the name of your instance.
11. Click **Next: Preview**.
12. Optional. If you chose **Pay-As-You-Go** for the billing method, choose the duration you want.
13. Select the check box to accept the terms of service and click **Create Instance**.
14. On the page that shows billing, click **Pay**.

The instance is displayed in the list. Wait approximately five minutes for the instance to be ready.

## Set the admin password

The first time you boot BIG-IP VE, you must connect to the instance and create a strong admin password. You will use the admin account and password to access the BIG-IP Configuration utility web page.

This management interface may be accessible to the Internet, so ensure the password is secure.

1. Connect to BIG-IP VE.
  - At the command prompt, navigate to the folder where you saved your ssh key and type: `ssh -i <private_key_file.pem> admin@<bigip_management_ip_address>`
  - If you prefer, you can use PuTTY :
    - a. In the Host Name (or IP address) field, enter the external IP address.
    - b. In the Category pane on the left, click **Connection > SSH > Auth**.
    - c. In the **Private key file for authentication** field, choose your .ppk file.
    - d. Click **Open**.
    - e. If a host key warning appears, click **OK**.
    - f. The terminal screen displays: `login as:`
    - g. Type `admin` and press Enter.
    - h. You are now at the `tmsh` command prompt.

2. Modify the admin password:  

```
modify auth password admin
```

The terminal screen displays the message:  

```
changing password for admin
new password:
```
3. Type the new password and press Enter.  
The terminal screen displays the message:  

```
confirm password
```
4. Re-type the new password and press Enter.  
Ensure that the system retains the password change and press Enter.  

```
save sys config
```

The terminal screen displays the message:  

```
Saving Ethernet mapping...done
```

## License BIG-IP VE

You must enter license information before you can use BIG-IP VE.

1. Open a web browser and log in to the BIG-IP Configuration utility by using https with the external IP address and port 8443, for example: `https://<external-ip-address>:8443`. The username is `admin` and the password is the one you set previously.
2. On the Setup Utility Welcome page, click **Next**.
3. On the General Properties page, click **Activate**.
4. In the **Base Registration key** field, enter the case-sensitive registration key from F5.
5. For Activation Method, if you have a production or Eval license, choose **Automatic** and click **Next**.
6. If you chose Manual, complete these steps:
  - a. In the Step 1: Dossier field, copy all of the text and then click **Click here to access F5 Licensing Server**.
  - b. A separate web page opens.
  - c. On the new page, click **Activate License**.
  - d. In the **Enter your dossier** field, paste the text and click **Next**.
  - e. Accept the agreement and click **Next**.
  - f. On the Activate F5 Product page, copy the license text in the box. Now go back to the BIG-IP Configuration utility and paste the text into the **Step 3: License** field.
  - g. Click **Next**.

The BIG-IP VE system registers the license and logs you out. When the configuration change is successful, click **Continue to provision BIG-IP VE**.

## Provision BIG-IP VE

You must confirm the modules you want to run before you can begin to work in the BIG-IP Configuration utility.

1. Open a web browser and log in to the BIG-IP Configuration utility.
2. On the Resource Provisioning screen, change settings if necessary and click **Next**.
3. On the Device Certificates screen, click **Next**.
4. On the Platform screen, in the **Admin Account** field, re-enter the password for the `admin` account and click **Next**.  
BIG-IP VE logs you out.

- When you log back in, on the **Setup Utility > Network** screen, in the Advanced Network Configuration area, click **Finished**.

## Create a pool and add members to it

Traffic goes through BIG-IP VE to a pool. Your application servers should be members of this pool.

- Open a web browser and go to the BIG-IP Configuration utility, for example: `https://<external-ip-address>:8443`.
- On the Main tab, click **Local Traffic > Pools**.
- Click **Create**.
- In the **Name** field, type `web_pool`. Names must begin with a letter, be fewer than 63 characters, and can contain only letters, numbers, and the underscore (`_`) character.
- For Health Monitors, move `https` from the **Available** to the **Active** list.
- Choose the load balancing method or retain the default setting.
- In the New Members section, in the **Address** field, type the IP address of the application server.
- In the **Service Port** field, type a service port, for example, `443`.
- Click **Add**.  
The list now contains the member.
- Add additional pool members as needed and click **Finished**.

## Create a virtual server

A virtual server listens for packets destined for the external IP address. You must create a virtual server that points to the pool you created.

- In the BIG-IP Configuration utility, on the Main tab, click **Local Traffic > Virtual Servers**.
- Click **Create** and populate the following fields.

Field	Value
Name	A unique name
Destination Address/Mask	BIG-IP VE's private IP address
Service Port	443
HTTP Profile	http
SSL Profile (Client)	clientssl
SSL Profile (Server)	serverssl
Source Address Translation	Auto Map
Default Pool	web_pool

**Note:** These settings are for demonstration only. For details about securing a web application with SSL, see the product documentation at [askf5.com](http://askf5.com).

- Click **Finished**.

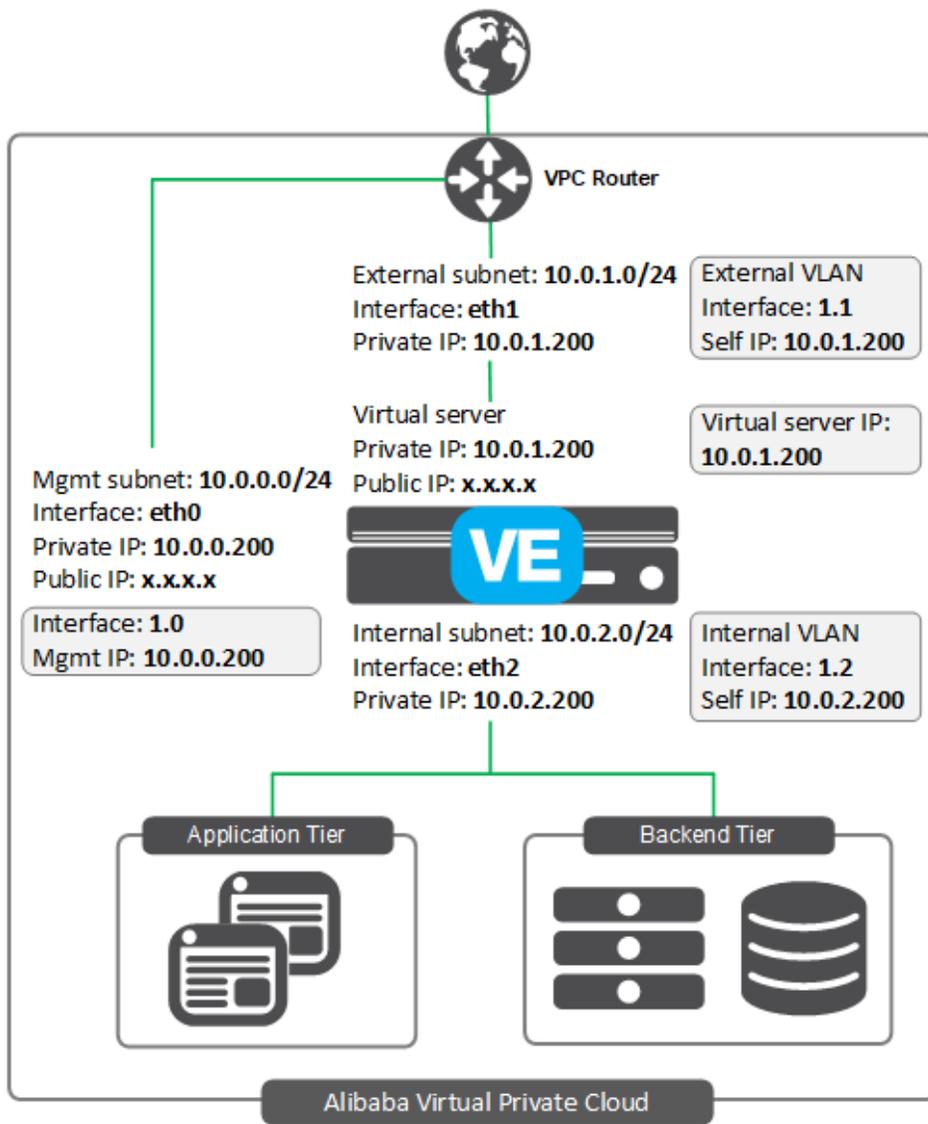
Traffic to the BIG-IP VE external IP address will now go to the pool members. To test in a browser, type: <https://<external-IP-address>>.



## Alibaba Cloud: Three-NIC BIG-IP VE

The following diagram shows a basic three-NIC deployment of BIG-IP VE in an Alibaba Virtual Private Cloud (VPC).

Complete the tasks in this guide to create this deployment.



**Note:** Your IP addresses may not match the diagram exactly.

This deployment shows three subnets:

- An external, public subnet, where you'll create a virtual server to accept Internet traffic.
- An internal, private subnet, where your application servers live.
- A management subnet, where you can access the BIG-IP Configuration utility; you use the Configuration utility to configure BIG-IP VE.

Traffic flows from clients through BIG-IP VE to application servers.

You create all IP addresses and network interfaces in Alibaba. Then in BIG-IP VE, you create corresponding objects for the same IP addresses, represented by the shaded boxes in the diagram.

## Prepare

To create a multi-NIC configuration, you must first create an Alibaba virtual private cloud (VPC) and subnets (known as *VSwitches*). This is the network environment where your instances will reside.

You must also edit security rules, which determine access to BIG-IP VE and related resources, and create or upload an SSH key pair, which you'll use to connect to the BIG-IP VE instance.

- [Create a VPC and management subnet](#)
- [Add an external and internal VSwitch to the VPC](#)
- [Edit security rules for the VPC](#)
- [Create or add an SSH key pair](#)

### Create a VPC and management subnet

A BIG-IP VE instance must be in an Alibaba virtual private cloud (VPC). In this example, BIG-IP VE will be in the VPC on the subnet (or *VSwitch*) intended for management traffic.

1. In the Alibaba Console, from the left menu, click **Virtual Private Cloud**.
2. On the top toolbar, select the region you want.
3. Click **Create VPC**.
4. Complete the fields.

For more information, see: <https://www.alibabacloud.com/help/doc-detail/65398.htm>

Field	Value
<b>Name</b>	A descriptive name.
<b>IPv4 CIDR Block</b>	10.0.0.0/8
<b>VSwitch Name</b>	<b>Management</b>
<b>Zone</b>	The same zone you chose when you created the VPC.

5. Click **OK**.
6. On the success screen, click **Complete**.

The VPC is displayed in the list.

## Add an external and internal VSwitch to the VPC

In Alibaba Cloud, subnets are called VSwitches. In this example, you create two additional VSwitches: external and internal.

All subnets must be in the same zone, so before you proceed, ensure you know which zone you created the VPC's first VSwitch in.

To create the external subnet:

1. In the list of VPCs, in the row for your VPC, in the Actions column, click **Manage**.
2. In the Network Resources area, click the number next to **VSwitch**.
3. Click **Create VSwitch**.
4. Complete the fields.

Field	Value
VPC	The VPC you just created.
Name	<b>External</b>
Zone	The same zone you chose when you created the VPC.
IPv4 CIDR Block	10.0.1.0/24

5. Click **OK**.

To create the internal subnet:

1. Click **Create VSwitch**.
2. Complete the fields.

Field	Value
VPC	The VPC you just created.
Name	<b>Internal</b>
Zone	The same zone you chose when you created the VPC.
IPv4 CIDR Block	10.0.2.0/24

3. Click **OK**.

You should now have three VSwitches: management, external, and internal.

## Edit security rules for the VPC

You must set rules that determine which traffic can access instances in the VPC.

To create a security group for the management subnet:

1. In the list of VPCs, in the row for your VPC, in the Actions column, click **Manage**.
2. In the Network Resources section, next to Security Group, click the **0**.

3. In the top right, click **Create Security Group**.
4. Complete the fields.

Field	Value
<b>Template</b>	<b>Customize</b>
<b>Security Group Name</b>	A name you choose, for example, <b>ManagementTraffic</b> .
<b>Network Type</b>	VPC
<b>VPC</b>	The VPC you created earlier.

5. Click **OK**.
6. On the Notes dialog, click **Create Rules Now**.
7. In the top right, click **Add Security Group Rule**.
8. Complete the fields to allow SSH access to BIG-IP VE.

Field	Value
<b>Rule Direction</b>	<b>Ingress</b>
<b>Action</b>	<b>Allow</b>
<b>Protocol Type</b>	<b>SSH (22)</b>
<b>Port Range</b>	<b>22/22</b>
<b>Priority</b>	<b>1</b>
<b>Authorization Type</b>	<b>IPv4 CIDR Block</b>
<b>Authorization Objects</b>	IP address or range on your network; these IP addresses can access the VPC.

9. Click **OK**.
10. Repeat steps 7-9 and complete the fields to allow access to the BIG-IP Configuration utility web interface:

Field	Value
<b>Rule Direction</b>	<b>Ingress</b>
<b>Action</b>	<b>Allow</b>
<b>Protocol Type</b>	<b>HTTPS (443)</b>
<b>Port Range</b>	<b>443/443</b>
<b>Priority</b>	<b>1</b>
<b>Authorization Type</b>	<b>IPv4 CIDR Block</b>
<b>Authorization Objects</b>	IP address or range on your network; these IP addresses can access the VPC.

11. Click **OK**.

The rules are displayed in the list.

To create a security group for the external (virtual server) subnet:

1. In the left pane, click **Virtual Private Cloud**.
2. In the list of VPCs, in the row for your VPC, in the Actions column, click **Manage**.
3. In the Network Resources section, next to Security Group, click the **1**.
4. In the top right, click **Create Security Group**.
5. Complete the fields.

Field	Value
<b>Template</b>	<b>Customize</b>
<b>Security Group Name</b>	A name you choose, for example, <b>ExternalTraffic</b> .
<b>Network Type</b>	<b>VPC</b>
<b>VPC</b>	The VPC you created earlier.

6. Click **OK**.
7. On the Notes dialog, click **Create Rules Now**.
8. In the top right, click **Add Security Group Rule**.
9. Complete the fields to allow internet access to the BIG-IP VE virtual server.

Field	Value
<b>Rule Direction</b>	<b>Ingress</b>
<b>Action</b>	<b>Allow</b>
<b>Protocol Type</b>	<b>HTTPS (443) or HTTP (80), depending on your needs</b>
<b>Port Range</b>	<b>443/443 or 80/80</b>
<b>Priority</b>	<b>1</b>
<b>Authorization Type</b>	<b>IPv4 CIDR Block</b>
<b>Authorization Objects</b>	IP address or range on your network; these IP addresses can access the VPC.

10. Click **OK**.

To create a security group for the internal subnet:

1. In the left pane, click **Virtual Private Cloud**.
2. In the list of VPCs, in the row for your VPC, in the Actions column, click **Manage**.
3. In the Network Resources section, next to Security Group, click the **1**.
4. In the top right, click **Create Security Group**.
5. Complete the fields.

Field	Value
<b>Template</b>	<b>Customize</b>

<b>Security Group Name</b>	A name you choose, for example, <b>InternalTraffic</b> .
<b>Network Type</b>	<b>VPC</b>
<b>VPC</b>	The VPC you created earlier.

6. Click **OK**.
7. On the Notes dialog, click **Create Rules Now**.
8. In the top right, click **Add Security Group Rule**.
9. Complete the fields to allow internet access to the BIG-IP VE virtual server.

<b>Field</b>	<b>Value</b>
<b>Rule Direction</b>	<b>Ingress</b>
<b>Action</b>	<b>Allow</b>
<b>Protocol Type</b>	Your choice, depending on access needed for your application servers.
<b>Port Range</b>	Your choice, depending on access needed for your application servers.
<b>Priority</b>	<b>1</b>
<b>Authorization Type</b>	<b>IPv4 CIDR Block</b>
<b>Authorization Objects</b>	IP address or range on your network; these IP addresses can access the VPC.

10. Click **OK**.

### Create or add an SSH key pair

You need a key pair to connect to BIG-IP VE and set the admin password.

1. In the Alibaba Console, from the left menu, click **Elastic Compute Service**.
2. On the left menu, under Networks and Security, click **SSH Key Pair**.
3. In the top right, click **Create SSH Key Pair**.
4. Type and name and either create or import a key pair.
5. Click **OK**.

The key pair name is displayed in the list. You will use this key later, to connect to the BIG-IP VE instance.

## Deploy

Now deploy a BIG-IP VE instance and configure basic networking for it.

- [Deploy a BIG-IP VE instance](#)
- [Change the security group associated with the external ENI](#)
- [Create an internal elastic network interface \(ENI\)](#)
- [Create an Elastic IP address for the virtual server](#)
- [Bind the EIP to the external ENI](#)

### Deploy a BIG-IP VE instance

To create an instance of BIG-IP VE in Alibaba, you deploy a BIG-IP VE image from the Alibaba Marketplace.

1. In the Alibaba Console, from the left menu, click **Elastic Compute Service**.
2. On the left menu, click **Instances**.
3. In the top right, click **Create Instance**.
4. Complete the fields.

Field	Value
<b>Billing Method</b>	<b>Subscription</b> – You pay monthly for the instance. <b>Pay-As-You-Go</b> – You pay based on time. If you are going to choose a BIG-IP VE PAYG image, you should choose this method. <b>Preemptible Instance</b> is not supported.  For more information, see <a href="#">Billing method comparison</a> .
<b>Region</b>	Select the zone where you created your VSwitches.
<b>Instance Type</b>	Choose at least 2 vCPU and 4 GB memory. For each vCPU, add at least 2 GB of memory.  Also, ensure the instance type you choose has the number of available Elastic Network Interfaces (ENIs) you need. In this example, you need three.
<b>Image</b>	Click <b>Marketplace Image</b> and search for F5.  If you choose BYOL, need <a href="#">an F5 license</a> . You can <a href="#">get a trial license</a> if you need one.  If you expect to upgrade BIG-IP VE in the future, choose an image with 2 boot locations. If you do not need room to upgrade (if you intend to create a new instance when a new version of BIG-IP VE is released), choose an image with 1 boot location.
<b>Storage</b>	Accept the default or change it.  For LTM, set the <b>System Disk</b> value to the minimum available size.

5. Click **Next: Networking**.
6. Complete the fields.

Field	Value
<b>Network</b>	The VPC you created earlier and the <b>Management</b> VSwitch you created.
<b>Network Billing Method</b>	Select <b>Assign public IP</b> .  This IP address is for initial management access to BIG-IP VE and you can remove it later.  If you have a jump host on the same VSwitch then you do not need this IP address.
<b>Security Group</b>	Select the <b>ManagementTraffic</b> group.
<b>Elastic Network Interface</b>	Eth0 is displayed by default.  Add an additional ENI for eth1 and associate it with the <b>External</b> VSwitch.  <b>Note:</b> This ENI is associated with the same security group as eth0. You will change this in a later task.

7. Click **Next: System Configurations**.
8. Complete the fields.

Field	Value
<b>Key Pair</b>	The key pair you created or imported earlier.  <b>Important:</b> A key pair is the only type of logon credentials you can use to connect to BIG-IP VE for the first time. The other settings ( <b>Inherit Password From Image</b> , <b>Password</b> , and <b>Set Later</b> ) do not work.
<b>Instance Name</b>	A name you choose.
<b>Host</b>	<b>Important:</b> This setting has no effect on BIG-IP VE.

9. Click **Next: Grouping**.
10. Click **Add Tag**. You may want to add a tag key named **Name** and a tag value with the name of your instance.
11. Click **Next: Preview**.
12. Optional. If you chose **Pay-As-You-Go** for the billing method, choose the duration you want.
13. Select the check box to accept the terms of service and click **Create Order**.
14. On the page that shows billing, click **Pay**.

Return to the console and click **Elastic Compute Service > Instances**. The instance is displayed in the list. Wait approximately five minutes for the instance to be ready.

## Change the security group associated with the external ENI

When you deployed BIG-IP VE and selected a second NIC for the external network, that NIC was associated with the same security group as the primary NIC, which is used for management.

You must associate the second NIC with a security group meant for external traffic.

1. In the Alibaba Console, from the left menu, click **Elastic Compute Service**.
2. On the left menu, under Networks and Security, click **ENI**.
3. For the secondary NIC meant for external traffic, in the Actions column, click **Modify**.
4. For **Security Group**, select the **ExternalTraffic** group and remove the **ManagementTraffic** group.
5. Click **OK**.

The list refreshes.

## Create an internal elastic network interface (ENI)

When you created the BIG-IP VE instance, you associated two network interfaces with it (one for management and one for external). To connect BIG-IP VE with your internal servers, create an internal network interface, and attach it to your BIG-IP VE instance.

1. In the Alibaba Console, from the left menu, click **Elastic Compute Service**.
2. On the left menu, under Networks and Security, click **ENI**.
3. Click **Create ENI**.
4. Complete the fields.

Field	Value
Network Interface Name	InternalENI
VPC	Your VPC
VSwitch	Internal
Primary Private IP	10.0.2.200
Security Group	InternalTraffic

The ENI is displayed in the list. Now attach it to the BIG-IP VE instance.

1. In the list, for your ENI, in the Actions column, click **Bind to Instance**.
2. Select the instance and click **OK**.

**Important:** You must now reboot the BIG-IP VE so that it can register the new NIC. To do this, in the Instances list, in the Actions column, click **More > Instance Status > Restart**. For Restart Mode, click **Restart** and **OK**.

## Create an Elastic IP address for the virtual server

You must create an Elastic IP (EIP) address for your virtual server to be available from the internet.

In this task, you create the EIP. In the next task you will associate the EIP with the external elastic network interface (ENI).

1. In the Alibaba Console, from the left menu, click **Virtual Private Cloud**.
2. In the left menu, click **Elastic IP Addresses**.
3. Click **Create EIP**.
4. Select your region and other details and click **Buy Now**.
5. Agree to the terms of service and click **Activate**.

Return to the console.

### **Bind the EIP to the external ENI**

Before you begin this task, find the ID of the external ENI.

Your virtual server address is the primary private IP address associated with the external ENI. The EIP is the public address of the virtual server.

1. Return to the list of elastic IP addresses and find the IP address you just created.
2. In the Actions column for the EIP, click **Bind**.
3. Complete the fields.

<b>Field</b>	<b>Value</b>
<b>Instance Type</b>	<b>Secondary ENI</b>
<b>Mode</b>	<b>Nat Mode</b>
<b>Secondary ENI</b>	The ID of your external ENI.

4. Click **OK**.

The EIP is now associated with the external ENI.

## Configure

Finally, configure BIG-IP VE so that traffic passes through it to your application servers.

- [Set the admin password](#)
- [License BIG-IP VE](#)
- [Provision BIG-IP VE](#)
- [Create internal and external VLANs](#)
- [Create internal and external self IP addresses](#)
- [Create a pool and add members to it](#)
- [Create a virtual server](#)

### Set the admin password

The first time you boot BIG-IP VE, you must connect to the instance and create a strong admin password. You will use the admin account and password to access the BIG-IP Configuration utility web page.

This management interface may be accessible to the Internet, so ensure the password is secure.

1. Connect to BIG-IP VE.
  - At the command prompt, navigate to the folder where you saved your ssh key and type: `ssh -i <private_key_file.pem> admin@<bigip_management_ip_address>`
  - If you prefer, you can use PuTTY :
    - a. In the Host Name (or IP address) field, enter the external IP address.
    - b. In the Category pane on the left, click **Connection > SSH > Auth**.
    - c. In the **Private key file for authentication** field, choose your .ppk file.
    - d. Click **Open**.
    - e. If a host key warning appears, click **OK**.
    - f. The terminal screen displays: `login as:`
    - g. Type `admin` and press `Enter`.
    - h. You are now at the `tmsh` command prompt.
2. Modify the admin password:

```
modify auth password admin
```

The terminal screen displays the message:

```
changing password for admin
new password:
```
3. Type the new password and press `Enter`.  
The terminal screen displays the message:

```
confirm password
```
4. Re-type the new password and press `Enter`.  
Ensure that the system retains the password change and press `Enter`.

```
save sys config
```

The terminal screen displays the message:

```
Saving Ethernet mapping...done
```

## License BIG-IP VE

You must enter license information before you can use BIG-IP VE.

1. Open a web browser and log in to the BIG-IP Configuration utility by using https with the external IP address, for example: `https://<external-ip-address>`.  
The username is `admin` and the password is the one you set previously.  
On the Setup Utility Welcome page, click **Next**.
2. On the General Properties page, click **Activate**.
3. In the **Base Registration key** field, enter the case-sensitive registration key from F5.
4. For Activation Method, if you have a production or Eval license, choose **Automatic** and click **Next**.
5. If you chose Manual, complete these steps:
  - h. In the Step 1: Dossier field, copy all of the text and then click **Click here to access F5 Licensing Server**.
  - i. A separate web page opens.
  - j. On the new page, click **Activate License**.
  - k. In the **Enter your dossier** field, paste the text and click **Next**.
  - l. Accept the agreement and click **Next**.
  - m. On the Activate F5 Product page, copy the license text in the box. Now go back to the BIG-IP Configuration utility and paste the text into the **Step 3: License** field.
  - n. Click **Next**.

The BIG-IP VE system registers the license and logs you out. When the configuration change is successful, click **Continue** to provision BIG-IP VE.

## Provision BIG-IP VE

You must confirm the modules you want to run before you can begin to work in the BIG-IP Configuration utility.

1. Open a web browser and log in to the BIG-IP Configuration utility.
2. On the Resource Provisioning screen, change settings if necessary and click **Next**.
3. On the Device Certificates screen, click **Next**.
4. On the Platform screen, in the **Admin Account** field, re-enter the password for the `admin` account and click **Next**.  
BIG-IP VE logs you out.
5. When you log back in, on the **Setup Utility > Network** screen, in the Advanced Network Configuration area, click **Finished**.

## Create internal and external VLANs

In BIG-IP VE, you must create an external and internal VLAN that correspond to the Alibaba subnets.

1. In the BIG-IP VE Configuration utility, on the Setup Utility Network page, under Advanced Network Configuration, **Finished**.
2. On the Main tab, click **Network > VLANs**.
3. Click **Create** and populate the appropriate fields for the external VLAN.

Field	Value
Name	external

<b>Interface</b>	<b>1.1</b>
<b>Tagging</b>	<b>Untagged</b>

4. In the Resources section, click **Add**.
5. Click **Finished**.
6. Now click **Create** again and populate the appropriate fields for the internal VLAN.

<b>Field</b>	<b>Value</b>
<b>Name</b>	<b>internal</b>
<b>Interface</b>	<b>1.2</b>
<b>Tagging</b>	<b>Untagged</b>

7. In the Resources section, click **Add**.
8. Click **Finished**.

The screen refreshes, and the two new VLANs are in the list.

### Create internal and external self IP addresses

Before starting these steps, note the primary private IP address for the internal VSwitch.

Then in BIG-IP VE, create an internal self IP address.

1. In the BIG-IP VE Configuration utility, on the Main tab, click **Network > Self IPs**.
2. Click **Create** and populate the appropriate fields for the external self IP address.

<b>Field</b>	<b>Value</b>
<b>Name</b>	ExternalSelfIP
<b>IP Address</b>	10.0.1.200
<b>Netmask</b>	255.255.255.0
<b>VLAN/Tunnel</b>	<b>external</b>
<b>Port Lockdown</b>	<b>Allow All</b>

3. Click **Repeat** and populate the appropriate fields for the internal self IP address.

<b>Field</b>	<b>Value</b>
<b>Name</b>	InternalSelfIP
<b>IP Address</b>	10.0.2.200
<b>Netmask</b>	255.255.255.0
<b>VLAN/Tunnel</b>	<b>internal</b>
<b>Port Lockdown</b>	<b>Allow All</b>

4. Click **Finished**.

The screen refreshes, and the two new self IP addresses are in the list.

### Create a pool and add members to it

Traffic goes through BIG-IP VE to a pool. Your application servers should be members of this pool. In this example, the app server is a web server on port 443.

1. Open a web browser and go to the BIG-IP Configuration utility.
2. On the Main tab, click **Local Traffic > Pools**.
3. Click **Create**.
4. In the **Name** field, type `web_pool`. Names must begin with a letter, be fewer than 63 characters, and can contain only letters, numbers, and the underscore (`_`) character.
5. For Health Monitors, move `https` from the **Available** to the **Active** list.
6. Choose the load balancing method or retain the default setting.
7. In the New Members section, in the **Address** field, type the IP address of the application server.
8. In the **Service Port** field, type a service port, for example, `443`.
9. Click **Add**.  
The list now contains the member.
10. Add additional pool members as needed and click **Finished**.

### Create a virtual server

A virtual server listens for packets destined for the external IP address. You must create a virtual server that points to the pool you created.

1. In the BIG-IP Configuration utility, on the Main tab, click **Local Traffic > Virtual Servers**.
2. Click **Create** and populate the following fields.

Field	Value
Name	A unique name.
Destination Address/Mask	A wildcard (0.0.0.0) or the private IP address on the external network.
Service Port	<b>443</b>
HTTP Profile	<b>http</b>
SSL Profile (Client)	<b>clientssl</b>
SSL Profile (Server)	<b>serverssl</b>
Source Address Translation	<b>Auto Map</b>
Default Pool	<b>web_pool</b>

**Note:** These settings are for demonstration only. For details about securing a web application with SSL, see the product documentation at [askf5.com](http://askf5.com).

3. Click **Finished**.

Traffic to the BIG-IP VE external IP address will now go to the pool members. To test in a browser, type: <https://<elastic-IP-address>>.

## **Troubleshooting**

If you have any problems with your configuration, see the following information.

### **Virtual servers**

Ensure that the external ENI is associated with the Elastic IP address, and that the security group associated with the external ENI allows traffic to the port you want.

You cannot currently create more than one virtual server in Alibaba Cloud. You can use a wildcard virtual server (0.0.0.0) or the external private IP address.

### **Elastic Network Interfaces and security groups**

Each Elastic Network Interface (ENI) has an associated security group.

If you have trouble connecting to your application server, check the security groups associated with each ENI.

### **Zones**

Ensure all of your VSwitches (your subnets) are within the same zone.

### **Instance types**

When you deploy BIG-IP VE, the instance type you choose must allow the number of NICs you need.

The instance type must also be I/O optimized.