Hillstone Networks

CloudEdge Deployment Guide

Version 5.5R10

TechDocs | docs.hillstonenet.com

Hillstone Networks

Contact Information:

US Headquarters:

Hillstone Networks

292 Gibraltar Drive, Suite 105

Sunnyvale, CA 94089

Phone: 1-408-508-6750

http://www.hillstonenet.com/about-us/contact/

About this Guide:

This guide gives you comprehensive installation instructions of Hillstone NetworksCloudEdge .

For more information, refer to the documentation site: http://www.hillstonenet.com/resources/.

To provide feedback on the documentation, please write to us at:

TechDocs@hillstonenet.com

Hillstone Networks www.hillstonenet.com

TWNO: TW-DPL-VFW-EN-5.5R10-EN-V1.0-1/17/2023

Table of Contents

Overview

The virtualization product of Hillstone Networks is CloudEdge virtual firewall (vFW). vFW is a software product, a StoneOS system running on a virtual machine.

About This Guide

This guide introduces how to install CloudEdge on different virtualization platforms: KVM, Xen, Openstack, AWS, VMware ESXi, Hyper-V,Azure and Alibaba Cloud. This document does not cover how to configure StoneOS itself. For information of how to set up StoneOS, please refer to documents of StoneOS (click here).

Targeted Readers

This guide is intended for administrators who want to deploy CloudEdge of Hillstone Networks. Before deploying vFW on different platforms, the administrator should be familiar with the concept and components of KVM, Xen, OpenStack, AWS VMware ESXi (with vCenter and vSphere Client), Hyper-V, Azure or Alibaba Cloud. This document is written with readers in mind that have already known basic virtualization knowledge, and it will only introduce operations of how to install vFW.

vFW Models

vFW is available in multiple models. All models can be deployed on KVM, Xen, Openstack, AWS, ESXi, Hyper-V, Azure and Alibaba Cloud with formally purchased license ("Licensing CloudEdge" on Page 4). The required minimum configuration of virtual machine for each model is as follows:

Platform Models	Minimum Configuration
SG-6000-VM01	2 vCPU,2 GB memory
SG-6000-VM02	2 vCPU,4 GB memory
SG-6000-VM04	4 vCPU,8 GB memory
SG-6000-VM04	8vCPU,16GB memory

Notes: The model of CloudEdge is determined by the CPU number authorized by the CPU license and the specification (CPU and memory) of the configuration of VM, and the model of CloudEdge is finally determined by the lower value of the two. If the configuration of VM does not reach the minimum configuration required above, the corresponding model cannot be started normally.

Supported Features

vFW supports the following features:

- Firewall (policy, zone, NAT, etc)
- Application Identification
- Attack Defense (AD)
- Intrusion Prevention System (IPS)
- IPSec VPN
- SSL VPN
- User Management
- Access Control
- High Availability (HA)
- Link Load Balance (LLB)
- Logging
- Statistics Set
- QoS

VMware Tools

CloudEdge is integrated with VMware Tools in order to be automatically deployed in VMware platform. After the CloudEdge deployment is complete, power on the virtual machine which is running with CloudEdge in vCenter, and then click this virtual machine's Summary page to view the basic information about the IP address of the management interface , CPU, memory, and interface traffic.

Cloud-init

Cloud-init is a tool developed for the initialization of virtual machines in the cloud environment, which reads data from a variety of data sources by the "URL" or "configdrive" mode and then configures the virtual machine accordingly. The common configuration includes setting the user name & password, policy, nat rule, routing and so on.

CloudEdge is integrated with cloud-init, which will run with CloudEdge's startup , so that CloudEdge can be deployed automatically in the virtualization platform.

Notes:

- There may be a delay when cloud-init configuration file is injected to CloudEdge virtual machine. You have to wait for a few minutes before viewing the virtual machine's configuration. If it is not injected yet in 10 minutes, you can make a soft restart to solve the problem.
- If there is a command which is not injected, check that whether the command is wrong or use the abbreviation.

Licensing CloudEdge

CloudEdge SG6000-VM provides license controlled capacities. Only after installing formal license can the CloudEdge reach the listed capacity. To purchase a license, please contact sales people (click here).

Licenses

CloudEdgelicenses are categorized to platform licenses, sub licenses, and function licenses . A platform license is the base to install all other types of licenses. You can apply for all kinds of licenses through SN number (i.e., old version license mechanism). If the virtual firewall is reinstalled, due to the change of SN number, you have to re-apply for a license.

From the version 5.5R5, the CloudEdge license has been upgraded to the latest version, with a different licensing mechanism. After the installation of the new platform license, the SN number of the device will be changed to a virtual SN (vSN for short). If you want to continue to obtain function or sub licenses, they can be applied through the vSN number. For the new license does not depend on the SN number of the original system after the re-installation of system, the new license that was originally applied for can still be effective. At the same time, Hillstone provides LMS (license management system) to verify and manage licenses, which can ensure the security of licenses.

Notes: If your CloudEdge is a full license product, you do not need to purchase or install any license. It is already a full feature firewall when you purchase it.

Platform Licenses

CloudEdge is pre-installed with a free default license without application.You can apply for the platform license (the old version of the platform license) through the SN number or directly apply for the new version of the license. Old version platform license is divided into base license and trial license. The new platform license is divided into base license and sub license.

- **Default License**

  CloudEdge has a built-in free default license. All features are available in system with default license, such as SSL VPN, iQoS and IPS. However, performance is limited, e.g., only 2 IPSec VPN tunnels and 2 SSL VPN users are supported. The license is valid for 30 days. After expiration, all functions of the system can not be used, the OS version and all the signature databases can not be upgraded.

- **Platform Trial License**

  After the installation of Platform Trial License, you will get the same features as system with Platform Base License. But the duration will be shorter. The duration is determined by the agreement you signed, which is a relative period, for example, one month. After expiration, the existing configuration can not be modified. After the reboot, the original configuration can not be displayed, the default configuration instead, and only the platform functions are available while the performance is limited. So, reboot is not recommended.

- **Platform Sub License**

  After the installation of Platform Sub License, you will get the same features as system with Platform Base License. But the duration will be shorter. The duration is determined by the agreement you signed, which is an absolute period, for example, March 1 to March 31. After expiration, the existing configuration can not be modified. After the reboot, only the platform functions are available while the performance is limited.

- **Platform Base License**

  When a CloudEdge is officially purchased, you can buy a Platform Base License. Platform Base License provides fundamental firewall features.

  When it expires, the system can be normally functioning, but cannot be upgraded to higher version.

Sub Licenses

Sub licenses control whether corresponding functions are enabled or not and the time limit as well.

- **IPSec VPN Sub License**

  IPSec VPN sub License enables IPSec VPN function and authorizes the maximum number of IPSec VPN accesses. After installing multiple IPSec VPN licenses, you can increment the maximum number of IPSec VPN accesses. When the license expires, the IPSec VPN connection will be disconnected. IPSec VPN function will not be allowed to configure. Until the device is restarted, all the configurations of IPSec VPN will not be lost.

- **SSL VPN Sub License**

  SSL VPN Sub License enables SSL VPN function and authorizes the maximum number of SSL VPN accesses. After installing multiple SSL VPN licenses, you can increment the maximum number of SSL VPN accesses. When the license expires, the SSL VPN connection will be disconnected. SSL VPN function will not be allowed to configure. Until the device is restarted, all the configurations of SSL VPN will not be lost.

- **iQoS Sub License**

  iQoS sub license enables iQoS function. When the iQoS sub license expires, all the configurations of iQoS will not be lost until the device is restarted.

- **CPU Sub License**

  CPU Sub License authorizes the maximum number of vCPUs available to the CloudEdge. The CPU license has both base and trial types, and the base CPU license does not expire. After the trial license expires, system will restart and the number of available vCPUs will revert to 2vCPU, which is the configuration of the minimum model SG-6000-VM01.

Function Licenses

Some functions are only enabled when that corresponding license is installed. The function service includes:

- **Intrusion Prevention System (IPS) License**

  IPS License provides IPS function and its signature database upgrade. IPS License has its own validity. When it expires, the IPS function works normally, but IPS signature database cannot be upgraded.

- **Anti-Virus (AV) License**

  AV License provides anti-virus function and its signature database upgrade. AV License has its own validity. When it expires, the anti-virus function works normally, but AV signature database cannot be upgraded.

- **Sandbox License**

  Sandbox License provides sandbox function, which controls the suspicious file quantity allowed to be uploaded to the cloud sandbox every day, also, it provides white list upgrade. Sandbox License has its own validity. When it expires, the cloud analysis is stopped and the white list can not be upgraded. However, if the suspicious traffic still matches the analysis entries in the local cache, the sandbox function is still valid. After the system is restarted, the sandbox function will not be used.

- **URL DB License**

  URL DB License provides URL filter function and allows URL database to upgrade. URL DB License has its own validity. When it expires, the URL filter function works normally, but URL database cannot be upgraded.

- **APP DB License**

  APP DB License allows APP database to upgrade. APP DB license is issued with platform license. There is no need to apply for it. The validity of APP DB License also follows platform license. When the platform license expires, APP signature database cannot be upgraded.

Notes:

- Besides the licenses listed above, a hardware platform from Hillstone Networks can install other types of licenses, e.g. StoneShield, but currently, CloudEdge does not support licenses other than those listed here.

- Perimeter Traffic Filtering (PTF) function can be seen in StoneOS, but it is not available for the moment. Future versions will support the two functions.
- Currently, Anti-Virus (AV) License and Sandbox License are not available in CloudEdge for private cloud platform.

Generating Application Code

To install a license, log in the StoneOS and generate application code. After receiving the application code, the vender or salesperson will send you license information. Before logging in your CloudEdge, you need to refer to the installation instructions to set up your CloudEdge firewall first (KVM, Xen, Openstack, AWS, Hyper-V , Azure, Alibaba Cloud or VMware ESXi).

To generate application code in WebUI:

1. Log in the StoneOS system.
2. Select **System > License** to enter the license page.
3. Fill in the required fields under the **License Request** section.
4. Click **Generate**, and a series of code appears.
5. Copy and send the code to salesperson or vendor. They will return the license to you soon.

Installing License

After receiving license, you need to upload the license to make it take effect.

To install a license:

1. Select **System > License** to enter the license page.

2. Under **License Request**, choose one of the following two methods:

   - **Upload License File**: select this radio button and click **Browse**, select the license plain text file (.txt) to upload it to the system.

   - **Manual Input**: Select this radio button, and copy and paste license code into the text box.

3. Click **OK** to save the license.

4. Go to **System > Device Management**, and click the **Option** tab.

5. Click **Reboot**, and select **Yes** in the prompt.

6. The system will reboot. When it starts again, installed license(s) will take effect.

Verifying License

For Hillstone CloudEdge virtual firewall, after installing the license, you need to connect to the license server to verify the validity of the license to prevent the license from being cloned. System supports two ways, one is connected to the public Internet license server check, another is by LAN connection to the LMS (License Management System), you can choose one of these ways according to need.

- The way by public Internet license server is suitable for some small private or public cloud scenarios. After the virtual firewall connects to the public server, the server will provide the validation of the license (currently the public network server does not provide the distribution and management of the licenses). If the cloned license is found or the virtual firewall is not checked by server, the virtual firewall will be restarted in 30 days.

- The way by LAN LMS is suitable for large private or industry cloud scenarios. After the virtual firewall connect to the LMS, the LMS not only provides license validation, but also provides automatic distribution and management of licenses. If the cloned license is found or the virtual firewall is not checked by server, the server will recover all virtual firewall(clone or be cloned firewall) license and restart the virtual firewall; if the virtual firewall does not connect to the server to check, virtual firewall will restart in 30 days.

To verify licenses, take the following steps:

1. Select System > License> License Verify.

2. At the top of the page is the License Server Status bar, which shows the server's connection status,IP Address, port, Virtual Router, and verify type.

3. Below the page is the License Verify Setting bar, you can use one of the following two ways according to need:

    - Internet： select "Internet" and " Virtual Router" , click OK. The virtual firewall will verify the license through the public server.

    - Intrane: select "Intrane", and specify the server's " Address" , "Port" and " Virtual Router",and click OK.The virtual firewall's license will be checked, distributed and managed through the LMS.

4. Go to System > Device Management, and click the Option tab.

5. Click Reboot, and select Yes in the prompt.

6. The system will reboot. When it starts again, installed license(s) will take effect.

Notes: When you verify your license through a public server, make sure that the VRouter used to connect to the public network server is bound to zone, and the interface bound to the zone can access the Internet. For more information about LMS, refer to <LMS User Guide>.

Deploying CloudEdge on KVM

Using a Linux server running Kernel-based Virtual Machine (KVM) to deploy vFW is the most usual method to use vFW on a single host.

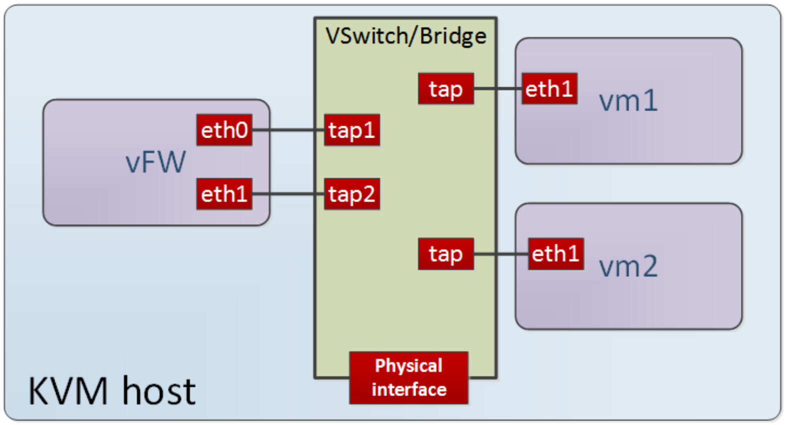
System Requirements

To deploy vFW on KVM, the host should meet the following requirements:

- Require at least 2 vCPU and 2 GB memory.
- For KVM environment establishment, the Linux system should have installed KVM, qumu, bridge-utils, uml-utilities, libvirt, virtinst, virt-viewer and virt-manager (To install these components, use command: **sudo apt-get install kvm qemu bridge-utils uml-utilities libvirt-bin virtinst virt-manager virt-viewer**).

How vFW Works on KVM Host

vFW on a KVM host usually works as gateway for virtual machines. In order to be able to forward data from/to the internal virtual machines, you need to connect the vFW tap interface to the Open Switch or Linux bridge of KVM host, and the internal virtual machines define vFW as their gateway.



Preparation

Before installing vFW, make sure you have a Linux host running a Linux system (Ubuntu 14.02 is recommended), and you have installed KVM and its components, including qemu, bridge-utils, uml-utilities, libvirt, virtinst, virt-viewer and virt-manager).

To install those components, use the command:

```
sudo apt-get install kvm qemu bridge-utils uml-utilities libvirt-bin virtinst virt-manager virt-viewer。
```

Notes: Before installing， you need create a bridge on the KVM in advance and add the interface of the KVM to the bridge.

Installing vFW on KVM Host

To install vFW on a KVM host, take the following steps:

Step 1: Acquiring vFW software package

1. Please login to the following path to download vFW KVM script file (with name "hsvfw"). The script file contains commands that can install, upgrade or restart vFW.

   path: ftp://ftp.hillstonenet.com/CloudEdge/hsvfw

   user/password: hillstonenet/hillstonenet

2. Please login to the following path to download vFW KVM image file (an .qcow2 file, e.g. SG6000-VFW02-V6-r1230.qcow2), the vFW system image.

   path: ftp://release.hillstonenet.com/StoneOS

   user/password: release/release

3. Save the package in your local PC.

Step 2: Importing script and image files

The following steps use Windows system to access KVM host.

1. In Windows, log into KVM host, enter the following command, and a dialog box will prompt.

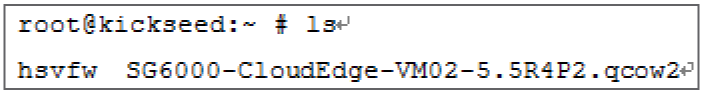
   rz

2. In the dialog box, browse your computer and select script and image file respectively. The files will be uploaded to the root directory of KVM host.

3. Enter the following command to check if the files are uploaded.

   ls

4. The output should display the following two files as below:



```
root@kickseed:~ # ls
hsvfw  SG6000-CloudEdge-VM02-5.5R4P2.qcow2
```

5. To install the image, use the following command:

   sudo ./hsvfw install ./*vfw_qcow2* [**vm01|vm02vm03|vm04|vm08**] *vm_name if_num*

sudo	A tool to execute system admin command.
`./hsvfw install`	Execute the install command in the script "hsvfw" which is under root directory .
./*vfw_qcow2*	Define the vFW image name, including suffix ".".
`vm01 | vm02| vm03 |vm04 | vm08`	Define the vFW model. Such as vm01 represents SG6000-VM01.
vm_name	Specifies a name for your vFW.
if_num	Specifies how many interfaces in your

	vFW. VM01 and VM02 can have up to 10 interfaces. VM04 and VM08 can have up to 20 interfaces. By default, your vFW has four interfaces.

For instance, use the following command to create a vFW named "vfwname" of model SG6000-VM02 with 4 interfaces.

```
./hsvfw install SG6000-CloudEdge-VM02-5.5R3P4-kvm.qcow2
vm02 vfwname -n 4
```

6. Linux will print the port number of Console.

Step 3: Initial login of vFW

A newly installed vFW only has Console access. You may visit vFW by accessing the Console port.

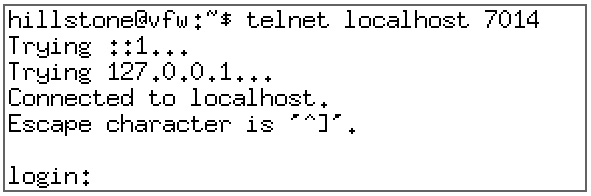
To access vFW Console port:

1. In Linux, use the following command:

   telnet localhost *port_num*

port_num	Console port number. It is the printed Console number, like "7014" in the example above.

For instance, the command below will access to vFW of Console port 7014:



```
hillstone@vfw:~$ telnet localhost 7014
Trying ::1...
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

login:
```

2. Aftr login prompt, enter username and password "hillstone"/"hillstone".

   login: hillstone

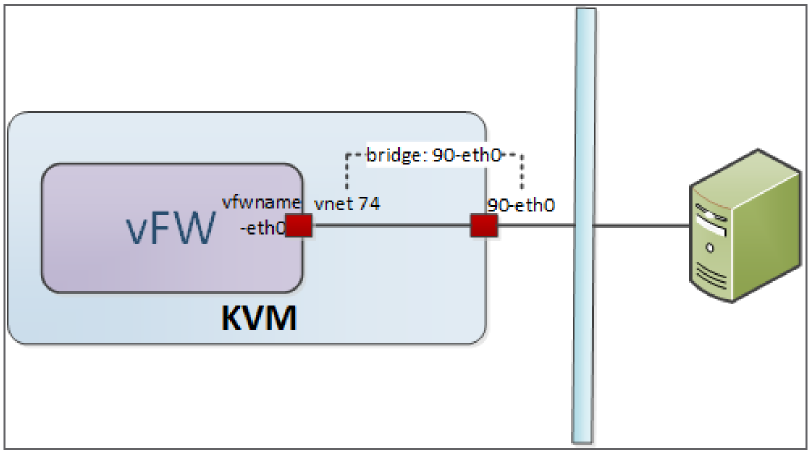
   password: hillstone

3. From now on, you can use command line interface to manage vFW. It is recommended to change your password at earliest convenience. For information about how to configure StoneOS, refer to StoneOS documents (click here).

Networking the vFW

After installation, each interface becomes a virtual swtich, and automatically connects to a vnet interface of KVM. If the vFW wants to access to other networks (internal network or Internet), place the vnet interface of vFW and the interface of intended network under the same vSwtich, the two networks will connect to each other.

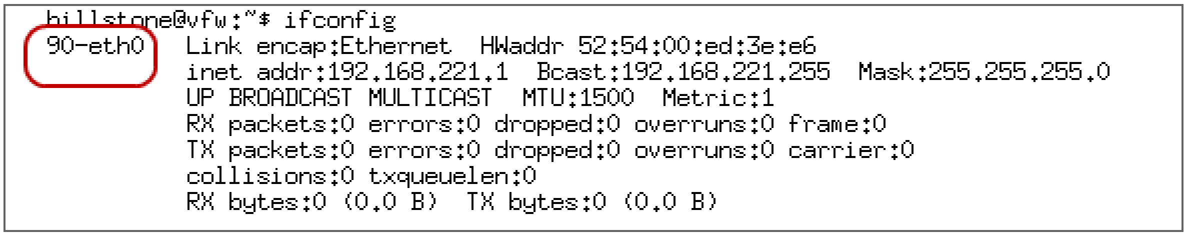
Using the example below, we will introduce how to connect "vnet0" (vFW) to "90-eth0" (a physical interface of KVM host).



Step 1: Viewing interfaces

In this example, a physical network (e.g. company's internal network) is connected to the physical interface of KVM host. You may view the interface information of KVM host interface and vFW interfaces.

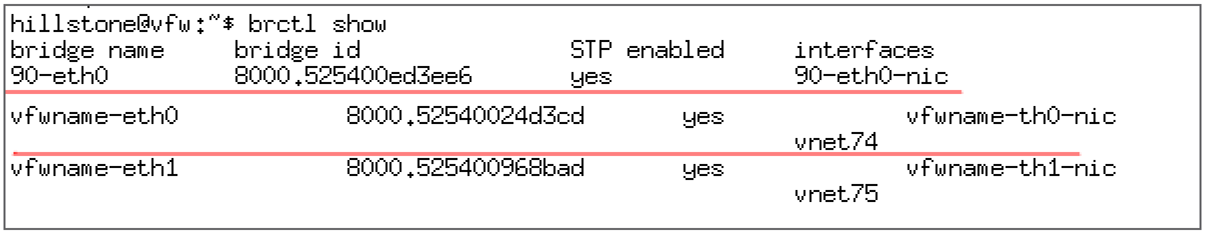
1. In Linux, use the command **ifconfig** to view interface. The KVM host interface is "90-eth0" as below:



```
hillstone@vfw:~$ ifconfig
90-eth0   Link encap:Ethernet  HWaddr 52:54:00:ed:3e:e6
          inet addr:192.168.221.1  Bcast:192.168.221.255  Mask:255.255.255.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

2. In Linux, use command **brctl show** to show vSwitch and interfaces.

   In this print message, vFW's "eth0" connects to KVM's "vnet74" under the bridge "vfwname-eth0", which means vFW's eth0 also belongs to bridge "vfwname-eth0". The physical interface 90-eth0 belongs to bridge "90-eth0".



```
hillstone@vfw:~$ brctl show
bridge name     bridge id               STP enabled     interfaces
90-eth0         8000.525400ed3ee6       yes             90-eth0-nic
vfwname-eth0            8000.52540024d3cd       yes             vfwname-th0-nic
                                                        vnet74
vfwname-eth1            8000.525400968bad       yes             vfwname-th1-nic
                                                        vnet75
```

Step 2: Connecting interfaces

To allow two networks communicate, just put their interfaces under the same bridge. In this example, in order to connect VFW's eth0 and physical interface 90-eth0, you can either move vFW's vnet74 into physical interface's bridge "90-eth0", or you can place physical interface under vFW interface's bridge.

Normally, we move new interfaces into the old bridge, so we will remove vFW's interface from its auto-created bridge and move it under the physical interface's old bridge.

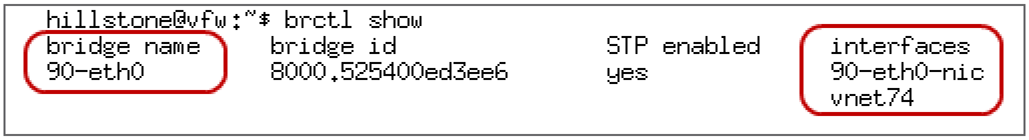
1. In Linux, to remove vFW's vnet74 from its auto bridge "vfwname-eth0", use the following command:

   sudo brctl delif vfwname-eth0 vnet74

2. Add the just removed interface into the intend bridge:

   sudo brctl addif 90-eth0 vnet74

3. Enter the command **brctl show** to check if the two interfaces belong to the same bridge now.



```
hillstone@vfw:~$ brctl show
bridge name     bridge id               STP enabled     interfaces
90-eth0         8000.525400ed3ee6       yes             90-eth0-nic
                                                        vnet74
```

4. From now on, vFW can communicate with KVM host's network.

Other Operations

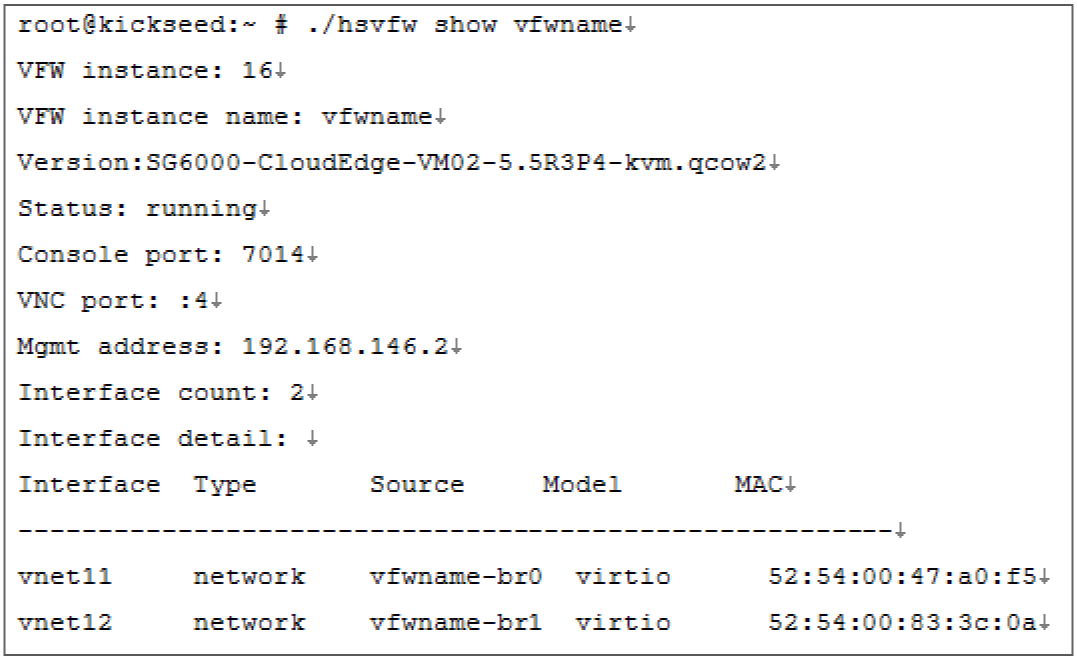
Viewing vFW

To view vFW information, use the command:

sudo ./hsvfw show *vm_name*

./hsvfw show	This is the show command in the script.
vm_name	Specify the name of vFW you want to view.

For instance, to view information of vFW whose name is "vfwname":



```
root@kickseed:~ # ./hsvfw show vfwname↓
VFW instance: 16↓
VFW instance name: vfwname↓
Version:SG6000-CloudEdge-VM02-5.5R3P4-kvm.qcow2↓
Status: running↓
Console port: 7014↓
VNC port: :4↓
Mgmt address: 192.168.146.2↓
Interface count: 2↓
Interface detail: ↓
Interface  Type       Source     Model       MAC↓
-------------------------------------------------------↓
vnet11     network    vfwname-br0  virtio      52:54:00:47:a0:f5↓
vnet12     network    vfwname-br1  virtio      52:54:00:83:3c:0a↓
```

Starting vFW

To start an existing vFW on KVM host, use the command:

sudo ./hsvfw start *vm_name*

`./hsvfw start`	This is the start command in the script.
`vm_name`	Specify the name of vFW you want to start.

Shutting Down vFW

To shut down a vFW, use the command:

sudo ./hsvfw shutdown *vm_name*

`./hsvfw shutdown`	This is the shutdown command in the script.
`vm_name`	Specify the name of vFW you want to shut down.

Upgrading vFW

Since StoneOS 5.5R1P7.1, CloudEdge can be upgraded online. You can just visit StoneOS WebUI on **System > Upgrade Management** page to upgrade the firewall. This upgrade method is recommended. For detailed operations, you may refer to *StoneOS WebUI User Guide*.

Restarting vFW

To restart vFW, use the command:

sudo ./hsvfw reboot *vm_name*

`./hsvfw reboot`	This is the restart command in the script.
`vm_name`	Specify the name of vFW you want to restart.

Uninstalling vFW

To uninstall an existing vFW, use the command:

sudo ./hsvfw uninstall *vm_name*

./hsvfw uninstall	This is the uninstall command in the script.
vm_name	Specify the name of vFW you want to uninstall.

Visiting vFW's WebUI

The first interface of vFW, eth0/0, is enabled with DHCP by default. If vFW is connected to a network with DHCP server, eth0/0 will get an IP address automatically. You can open vFW's WebUI interface by visiting eth0/0's address in a browser.

To visit vFW's WebUI:

1. Use telnet to visit vFW's Console interface (refer to "Deploying CloudEdge on KVM" on Page 11)
2. To view IP address of eth0/0, use the command:

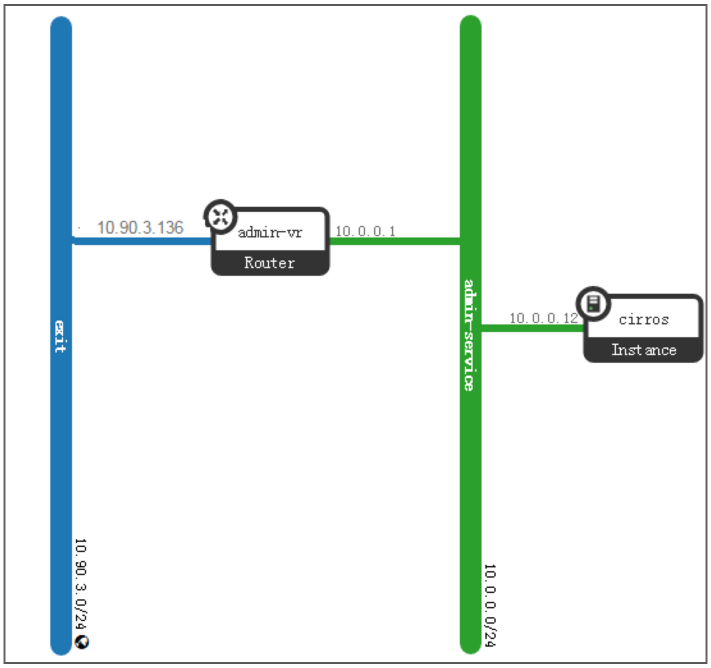
   show interface ethernet0/0
3. Configure a route , the destination address is 0.0.0.0/0 , and the next hop is the getway of the KVM host(192.168.221.254).
4. Open a browser (Chrome is recommended), enter eth0/0's IP address in the address bar.
5. Enter login name and password (hillstone/hillstone).
6. Click **Login**, and you will enter StoneOS's WebUI manager.
7. About how to use StoneOS, refer to StoneOS related documents (click here).

Deploying CloudEdge on OpenStack

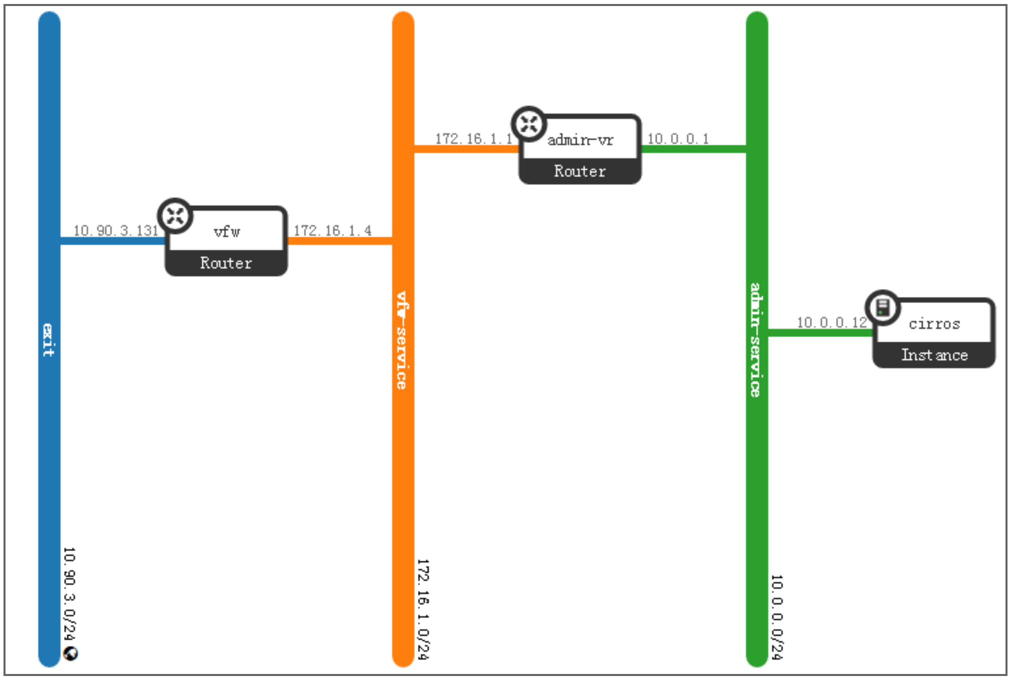
This example describes how to deploy CloudEdge at the edge of the router of OpenStack platform to protect the server in the original virtual network.

Deployment Scenarios

There was a server **cirros** deployed on the OpenStack platform connected with the external public network **exit** through the router **admin-vr**. The following is the original virtual network topology:



In this example , a CloudEdge instance **vfw** is deployed at the edge of the router **admin-vr**, and then it is connected with the external public network **exit**. At the same time, SNAT, DNAT rules and security policies are configured on CloudEdge **vfw** to protect the server **cirros**.



Note: For user reference, the parameters such as subnet, interface, and IP addresses described in this example's steps are exactly the same as those in the topology diagram.

System Requirements

To deploy CloudEdge on an OpenStack platform, the following requirements should be met:

- CloudEdge requires at least 2 vCPU and 2 GB memory. For the specification of product models, refer to the vFW Models .
- The Linux system is installed with OpenStack (Icehouse version), and its components, including Horizon, Nova, Neutron, Glance and Cinder (For OpenStack installation guide, refer to http://docs.openstack.org/icehouse/install-guide/install/apt/content/).
- OpenStack is required to provide KVM virtual machine.

Deploying CloudEdge on OpenStack

- Step 1: Importing Image File
- Step 2: Creating a Flavor
- Step 3: Create a Network
- Step 4: Starting the Instance
- Step 5: Login and Configure CloudEdge
- Step 6: Reconfigure OpenStack's Router
- Step 7: Release OpenStack's IP checking of CloudEdge's interfaces
- Step 8: Configure Routing, NAT, and Security policies on CloudEdge

Step 1: Import the Image File

To import the CloudEdge image file into the OpenStack platform as an image , take the following steps:

1. Log in to the OpenStack W WebUI with a normal account, and select **Project > Compute> Images**.

2. Click **Create Image** on the top right corner.

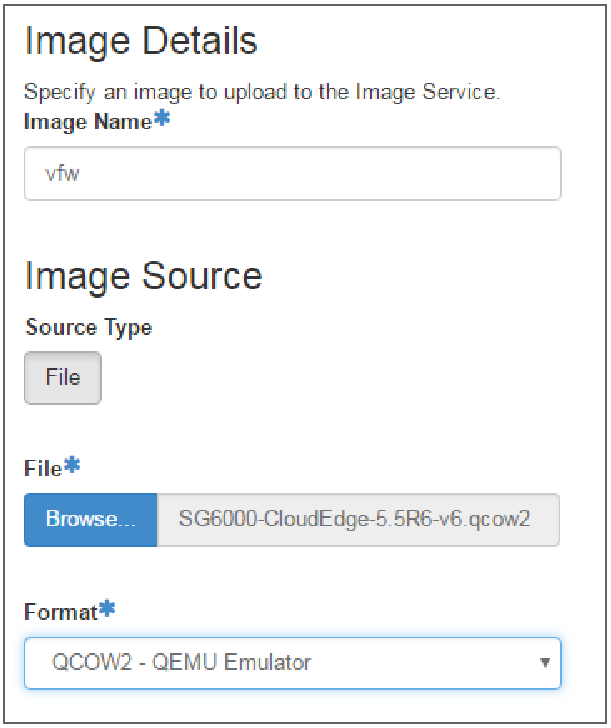


Image Details

Specify an image to upload to the Image Service.

Image Name*

vfw

Image Source

Source Type

File

File*

Browse... SG6000-CloudEdge-5.5R6-v6.qcow2

Format*

QCOW2 - QEMU Emulator

3. In the <Create Image> dialog, configure following options.

Option	Description
Image Name	Enter the image name, such as "vfw".
Image Source	Click **Browse**, and select the image file in the qcow2 format from the local PC.
Format	Select **QCOW2-QEMUEmulator** from the **Format** drop-down list.

4. Click **Create Image**. The image file will be imported successfully and displayed in the list.

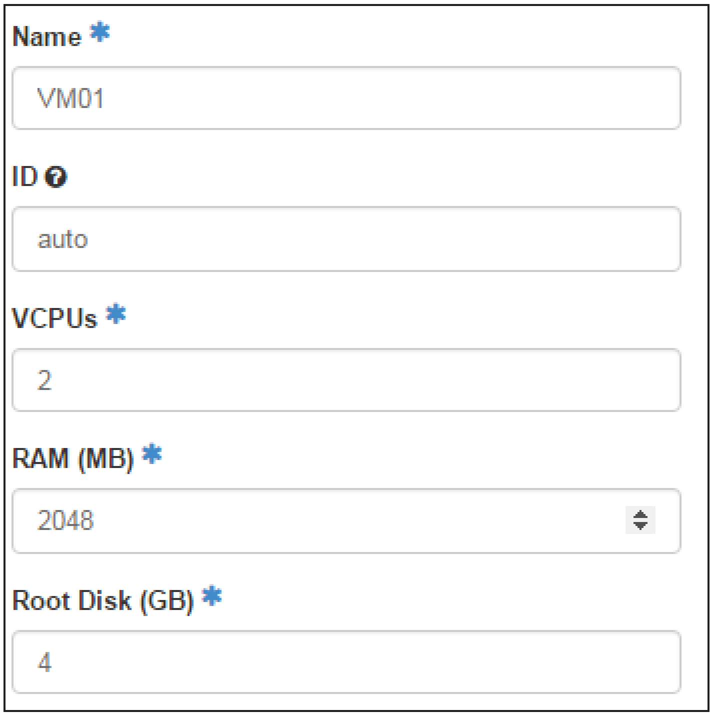
Step 2: Create a Flavor

Normally, a non-admin user cannot change the properties of an instance, including core, and memory. If you want to change an instance, you can change the flavor it belongs to, since the instance inherits what its flavor has. To create a flavor, take the following steps:

1. Log in to OpenStack WebUI with the admin account.

2. Select **Admin> System> Flavors**, and click **Create Flavor** on the top right corner.

3. In the <Create Flavor> dialog, configure the flavor.



Name *

VM01

ID

auto

VCPUs *

2

RAM (MB) *

2048

Root Disk (GB) *

4

In the <Flavor Information> tab, set the basic information.

Name	Enter the flavor name, such as "VM01".
ID	Skip this step since ID is automatically generated by OpenStack.
VCPUs	Specify the number of CPU cores as 2.
RAM （MB）	Specify the RAM size of the virtual machine as 2048MB.
Root Disk	Specify the size of root disk .The minimum is 4 GB.

(GB)	

4. Click **Create Flavor**.

Step 3: Create a Network

To create a network, take the following steps:

1. Log in to OpenStack WebUI with the admin account.

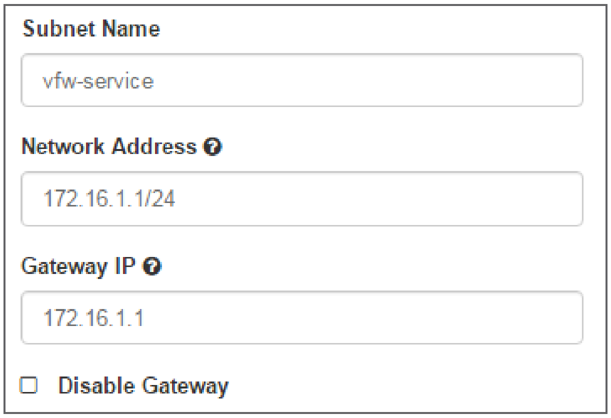
2. Select **Project > Network > Networks** and click **Network** on the top right corner.

To create a network, take the following steps:

1. Log in to OpenStack WebUI with the admin account.

2. Select **Project > Network > Networks**and click **Network** on the top right corner.

3. In the < Create Network> Dialog box, create a network as "vfw-service", click **Next** and continue to configure the subnet information.



Subnet Name: vfw-service

Network Address: 172.16.1.1/24

Gateway IP: 172.16.1.1

☐ Disable Gateway

In the <Subnet> tab, set the flowing information

Network Name	Enter the subnet name as "vfw-service".

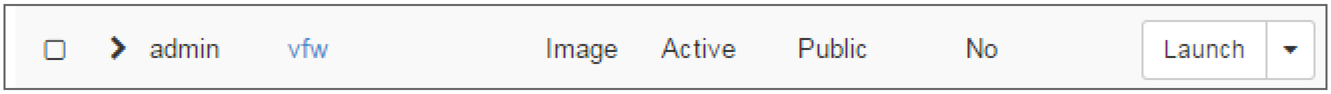
Network Address	Enter the network address as “172.16.1.0/24” .
Gateway IP	Enter the Gateway IP as “172.16.1.1” .

4. Click **Next** , and then click **Create** to complete configurations.

Step 4: Start the Instance

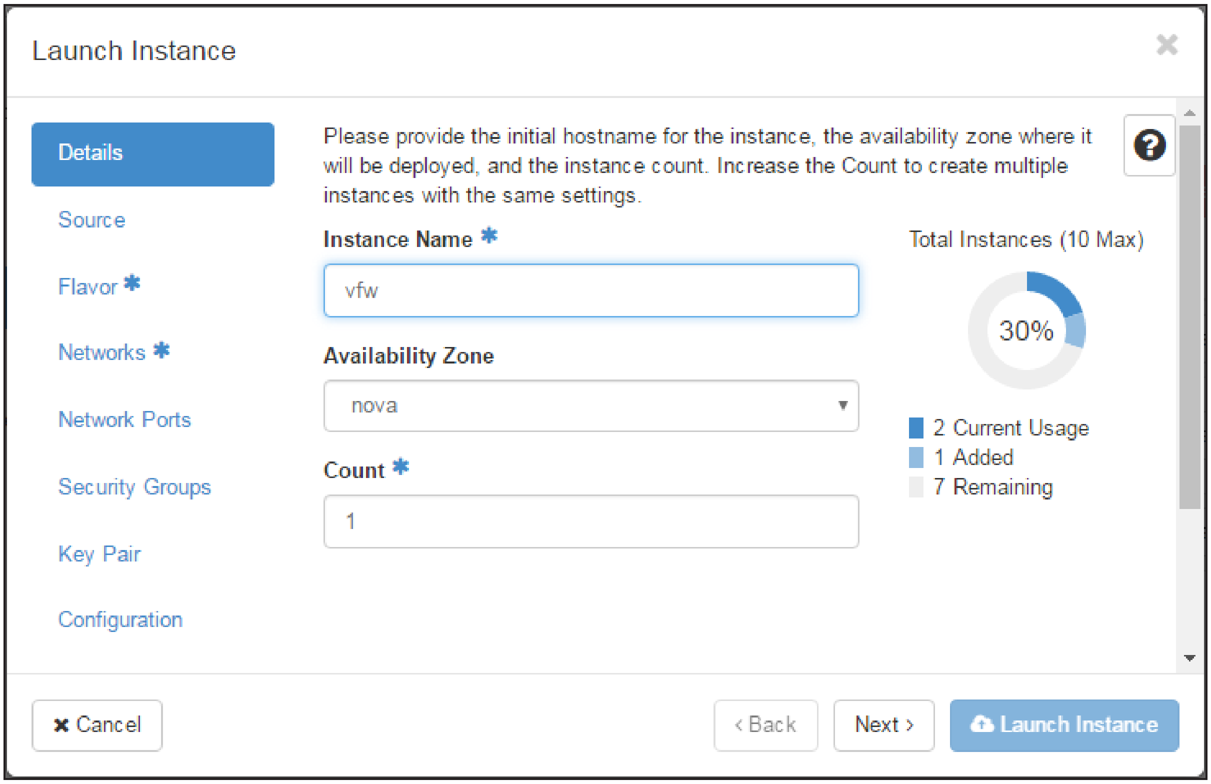
Log in to OpenStack WebUI with admin account. To boot the CloudEdge instance, take the following steps:

1. Select **Project > Compute> Instance** , and click **Launch** after the image list created in step 1.



☐ › admin vfw Image Active Public No Launch ▾

2. In the < Launch Instance> dialog box, configure the followings.



Launch Instance ×

Please provide the initial hostname for the instance, the availability zone where it will be deployed, and the instance count. Increase the Count to create multiple instances with the same settings.

Instance Name *

vfw

Availability Zone

nova ▾

Count *

1

Total Instances (10 Max)

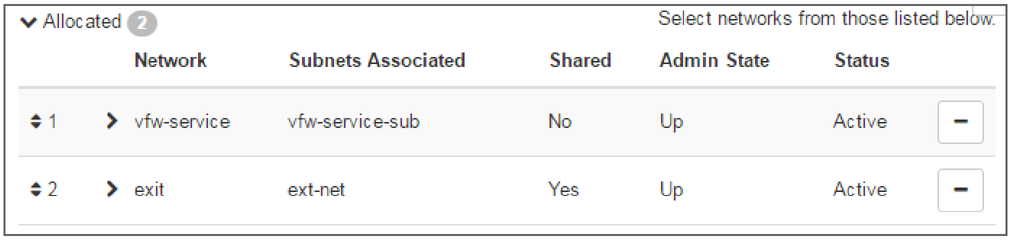
30%

■ 2 Current Usage
■ 1 Added
□ 7 Remaining

3. In the <Details> tab, enter the **Instance Name** as "vfw".

4. In the <Flavor>tab, select the flavor "VM01" configured in step 2.

In <Networks> tab, select the network "exit" and "vfw-service".



⌄ Allocated 2 Select networks from those listed below.

		Network	Subnets Associated	Shared	Admin State	Status	
⇕ 1	›	vfw-service	vfw-service-sub	No	Up	Active	−
⇕ 2	›	exit	ext-net	Yes	Up	Active	−

5. In the <Security Groups> tab, the selected security group needs to be configured with the rules that allow both internal and external traffic to enter the instance. CloudEdge will provide the more comprehensive access control policies than security groups.

6. Click **Launch Instance**.

Step 5: Login and Configure CloudEdge

After the above steps, you can take the following steps to login CloudEdge :

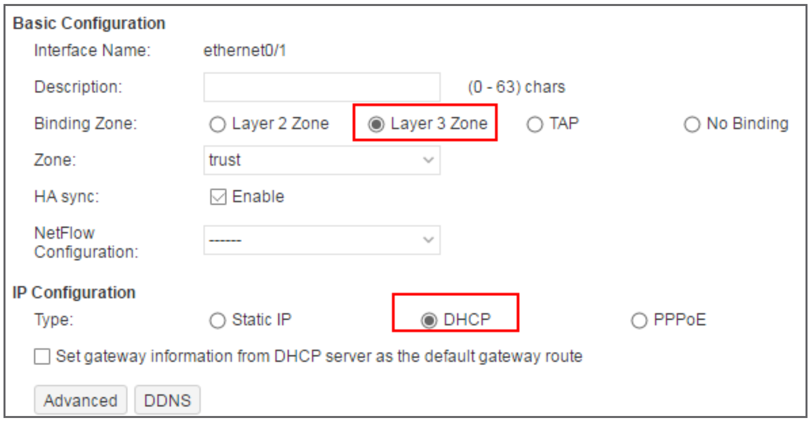
1. Log in to OpenStack WebUI, select **Project > Compute> Instance**.

2. In the instance list, click **vfw** to enter the details page. Click **Console** tab, and you can access CloudEdge via the embedded command interface..

3. You can also open the browser (Chrome browser is recommended and the HTTPS management is enabled by default), and enter the IP address of the "exit" network (such as https://10.90.3.131). In the login interface, type the username and password. The default username and password is hillstone and hillstone. Click **Login**, and the device system will initiate.

4. Click **Network > Interface**, select ethernet 0/1, and configure the **Binding Zone** as "Layer 3 zone" and IP configuration as "DHCP". The interface ethernet 0/1 will get the IP address

assigned by OpenStack automatically.



Basic Configuration

Interface Name: ethernet0/1

Description: (0 - 63) chars

Binding Zone: ○ Layer 2 Zone ● Layer 3 Zone ○ TAP ○ No Binding

Zone: trust

HA sync: ☑ Enable

NetFlow Configuration: ------

IP Configuration

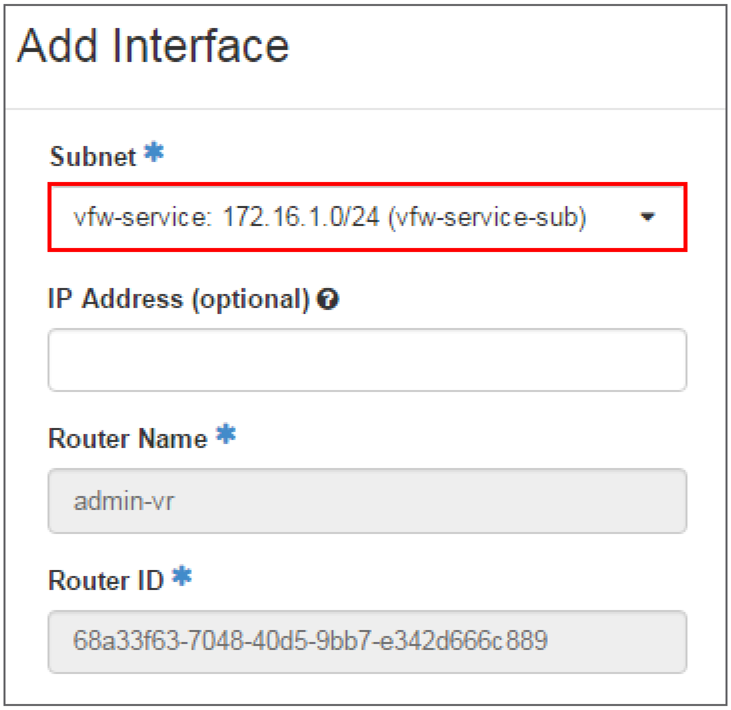
Type: ○ Static IP ● DHCP ○ PPPoE

□ Set gateway information from DHCP server as the default gateway route

Step 6: Reconfigure OpenStack's Router

Log in to Openstack WebUI with admin account. To reconfigure the router, take the following steps:

1. Select **Project > Network > Network Topology**, click the router "admin-vr", and delete the interface originally connected to the "exit" network.



Add Interface

Subnet *

vfw-service: 172.16.1.0/24 (vfw-service-sub)

IP Address (optional)

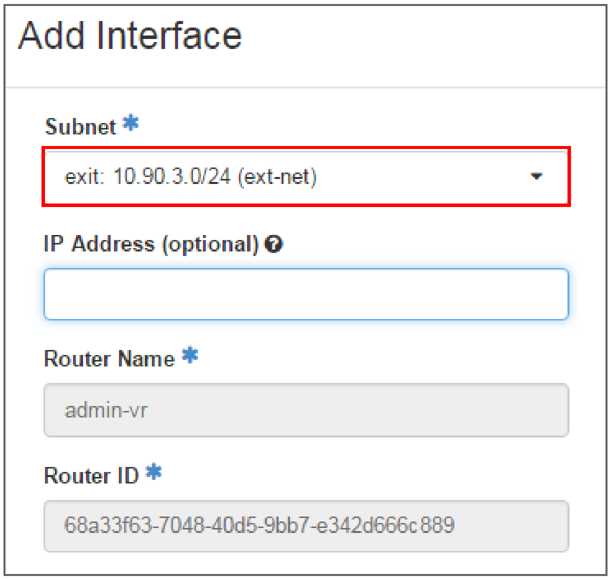
Router Name *

admin-vr

Router ID *

68a33f63-7048-40d5-9bb7-e342d666c889

2. Click **Add Interface** to reconnect to the network "vfw-service".



Add Interface

Subnet *

exit: 10.90.3.0/24 (ext-net)

IP Address (optional)

Router Name *

admin-vr

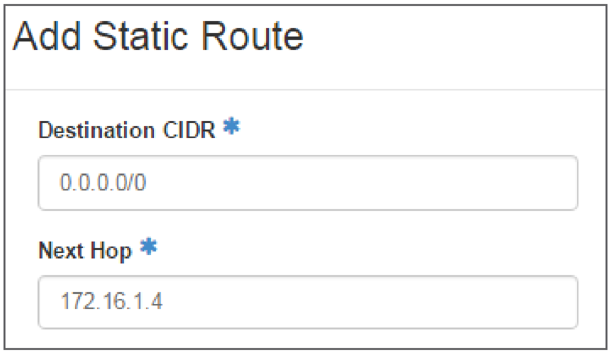
Router ID *

68a33f63-7048-40d5-9bb7-e342d666c889

3. Click **Submit**.

4. Select **Project > Network >Routers**, and click on the route name to view the details.

5. Click <Static Routes>tab, and add a static routing to the "vfw" instance.



Add Static Route

Destination CIDR *

0.0.0.0/0

Next Hop *

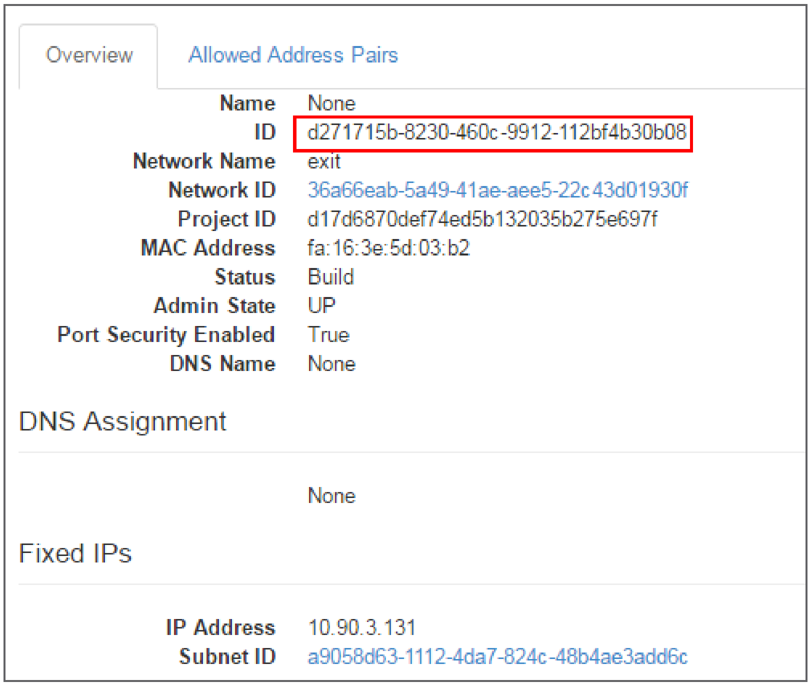
172.16.1.4

Step 7: Disable OpenStack's IP checking of CloudEdge's interfaces

To disable OpenStack's IP checking of CloudEdge's interfaces take the following steps:

1. Select **Project > Network > Network** , click the "exit" network to view the details .

2. Select the <Port> tab, click the port whose IP address is 10.90.3.131. On the port details page, copy the port ID.



Name	None
ID	d271715b-8230-460c-9912-112bf4b30b08
Network Name	exit
Network ID	36a66eab-5a49-41ae-aee5-22c43d01930f
Project ID	d17d6870def74ed5b132035b275e697f
MAC Address	fa:16:3e:5d:03:b2
Status	Build
Admin State	UP
Port Security Enabled	True
DNS Name	None

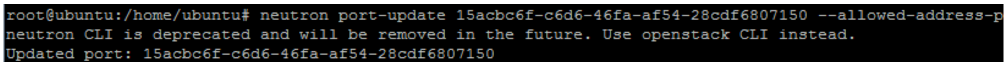
DNS Assignment

None

Fixed IPs

IP Address	10.90.3.131
Subnet ID	a9058d63-1112-4da7-824c-48b4ae3add6c

3. Execute environment variables on the control node, and then execute command:**neutron port-update** *15acbc6f-c6d6-46fa-af54-28cdf6807150* **--allowed-address-pairs type=dict list=true ip_address=0.0.0.0/0**("15acbc6f-c6d6-46fa-af54-28cdf6807150" is the port ID coped in the last step.)



```
root@ubuntu:/home/ubuntu# neutron port-update 15acbc6f-c6d6-46fa-af54-28cdf6807150 --allowed-address-p
neutron CLI is deprecated and will be removed in the future. Use openstack CLI instead.
Updated port: 15acbc6f-c6d6-46fa-af54-28cdf6807150
```

4. Repeat steps 1-3 above to disable OpenStack's IP checking of another interface of CloudEdge.

Step 8: Configure Routing, NAT, and Security policies on CloudEdge

To protect the "cirros" server instances, you need to continue to configure static routing, source NAT, destination NAT and access control policies on the CloudEdge instances. For the detailed configurations, take the following steps:

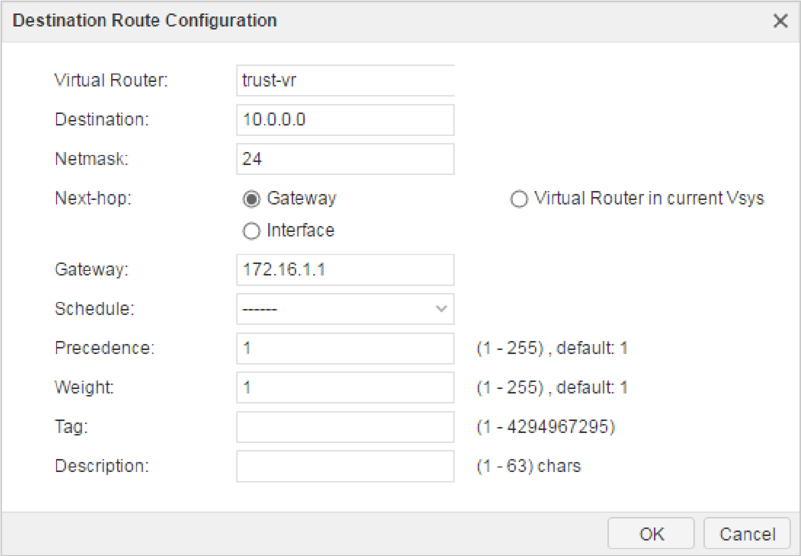
1. Log in to the CloudEdge instance **vfw** via WebUI.

2. Select **Network > Routing > Destination Route**,and configure a static route connected to the **cirros** server.

    - Destination：10.0.0.0

    - Netmask：24

    - Next-hop：Gateway 172.16.1.1



Destination Route Configuration ✕

Virtual Router: trust-vr

Destination: 10.0.0.0

Netmask: 24

Next-hop: ● Gateway ○ Virtual Router in current Vsys
○ Interface

Gateway: 172.16.1.1

Schedule: ------

Precedence: 1 (1 - 255) , default: 1

Weight: 1 (1 - 255) , default: 1

Tag: (1 - 4294967295)

Description: (1 - 63) chars

3. Select **Policy > NAT > SNAT**, and configure a source NAT rule.

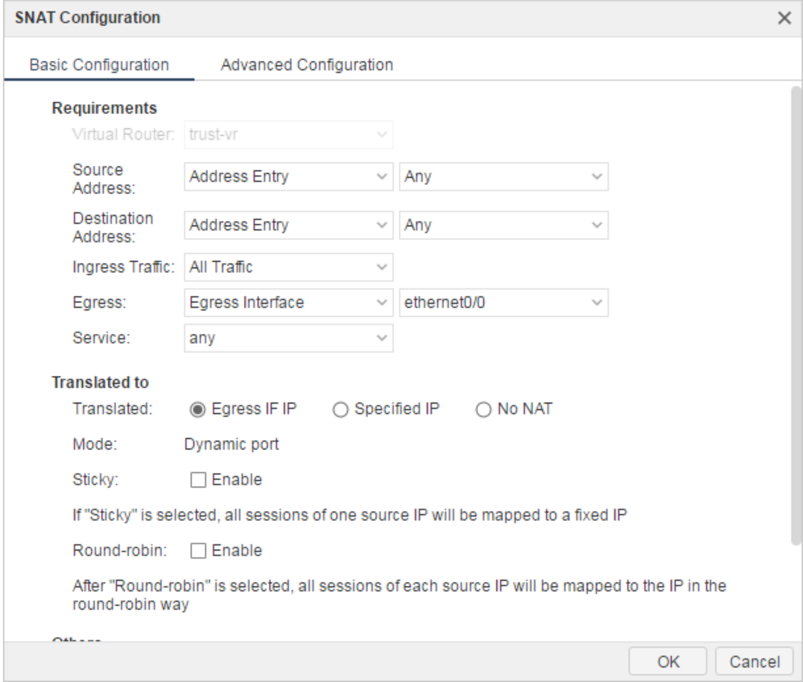
    - Source Address: Any

    - Destination Address: Any

    - Ingress Traffic: All Traffic

    - Egress Traffic: Egress Interface etherent 0/0

- Translate to : Egress IF IP



SNAT Configuration

Basic Configuration | Advanced Configuration

Requirements

Virtual Router: trust-vr

Source Address: Address Entry | Any

Destination Address: Address Entry | Any

Ingress Traffic: All Traffic

Egress: Egress Interface | ethernet0/0

Service: any

Translated to

Translated: ● Egress IF IP ○ Specified IP ○ No NAT

Mode: Dynamic port

Sticky: □ Enable

If "Sticky" is selected, all sessions of one source IP will be mapped to a fixed IP

Round-robin: □ Enable

After "Round-robin" is selected, all sessions of each source IP will be mapped to the IP in the round-robin way

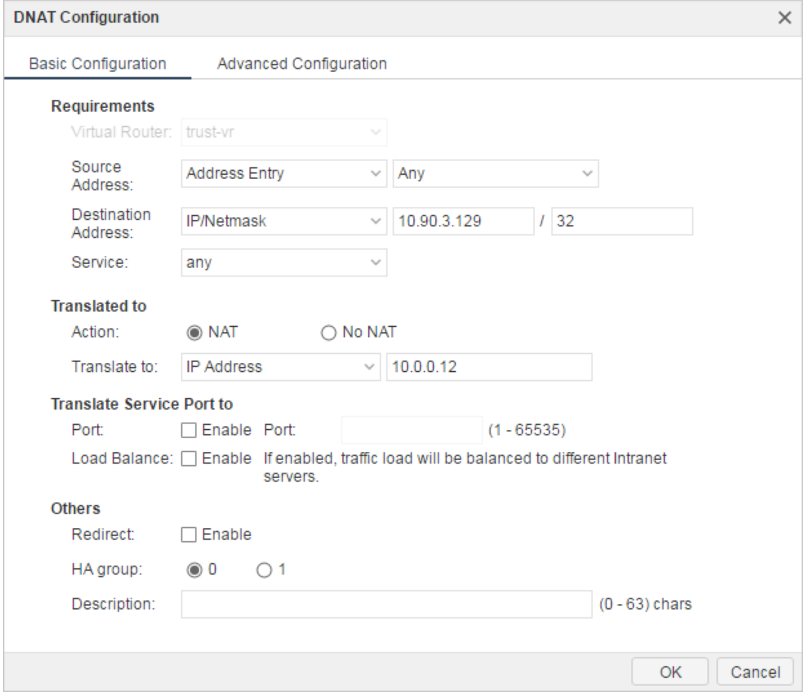
4. Select **Policy > NAT > DNAT**, and configure a destination NAT rule.

    - Source Address: Any

    - Destination Address: 10.90.3.129/32

    - Action: NAT

- Translate to IP: 10.0.0.12



DNAT Configuration ✕

Basic Configuration | Advanced Configuration

Requirements

Virtual Router: trust-vr

Source Address: Address Entry | Any

Destination Address: IP/Netmask | 10.90.3.129 / 32

Service: any

Translated to

Action: ● NAT ○ No NAT

Translate to: IP Address | 10.0.0.12

Translate Service Port to

Port: □ Enable Port: (1 - 65535)

Load Balance: □ Enable If enabled, traffic load will be balanced to different Intranet servers.

Others

Redirect: □ Enable

HA group: ● 0 ○ 1

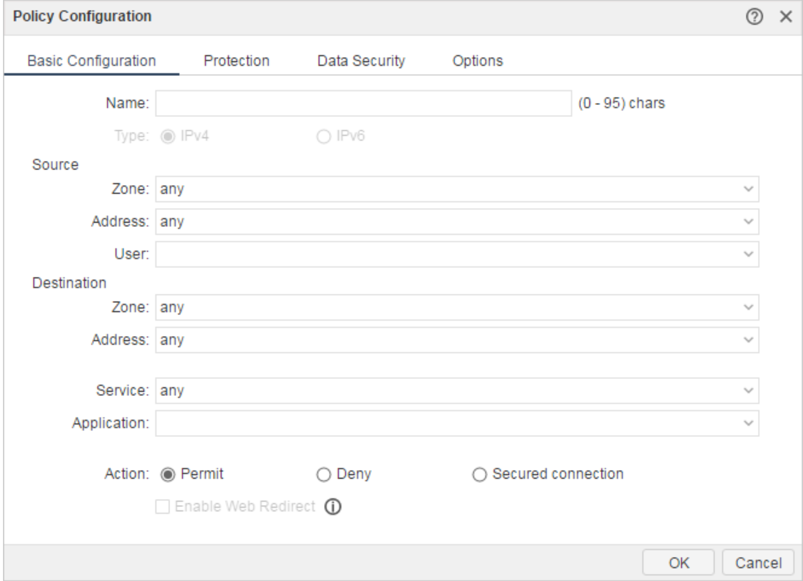
Description: (0 - 63) chars

5. Select **Policy > Security Policy**, and configure a security policy.

   - Source: Any

   - Destination: Any

- Action: Permit



Name: (0 - 95) chars

Type: ● IPv4 ○ IPv6

Source

Zone: any

Address: any

User:

Destination

Zone: any

Address: any

Service: any

Application:

Action: ● Permit ○ Deny ○ Secured connection

□ Enable Web Redirect

6. For more information about how to set up StoneOS, refer to StoneOS documentation (click here).

Results

After above configurations, the IP address of the cirros server will be translated to a public IP address through DNAT rules for the access of Internet users. At the same time, the source IP address of the cirros server’ s traffic sending to the Internet will be translated to the IP address of the CloudEdge's exit interface through SNAT rules, so as to protect the server from external attacks.

Deploying CloudEdge to Replace Routers of Openstack

CloudEdge supports to replace the built-in virtual router of Openstack. After the configuration is finished, when you create a new router, system will boot CloudEdge virtual machine as the router automatically. At the same time, the virtual firewall rule of Openstack will be translated to corresponding policies and be issued to the CloudEdge VM.

System Requirements

To replace virtual routers of Openstack by deploying CloudEdge, the following requirements should be met:

- The Linux system is installed with OpenStack (L version required), and its components, including Horizon, Nova, Neutron, Glance and Cinder (For OpenStack installation guide, refer to http://docs.openstack.org/icehouse/install-guide/install/apt/content/).
- Hillstone-Agent files include：

  1. hs-manager image files: hs-manager VM requires at least 2 vCPU, 4GB memory and 15GB root disk.

  2. patch files

Deploying CloudEdge to Replace Routers of Openstack

Step 1: Download plug-in files of Hillstone-Agent

The plug-in files of Hillstone-Agent include hs-manager image files and patch files. Hs-manager manages the CloudEdge VM (which can replace router) to achieve an auto-deployment; the patch files are used to configure replacement.

You can download`hs-manager-agent-1030.qcow2` and`patch.tgz` files by visiting the following path:

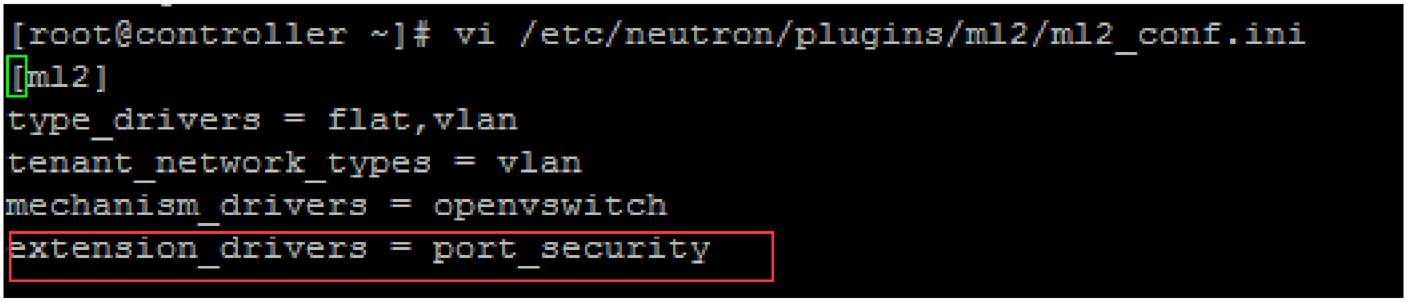
Path:ftp://ftp.hillstonenet.com/CloudEdge/Hillstone-Agent

User/ Password:hillstonenet/ hillstonenet

Step 2: Configure port_security

Open **etc/neutron/plugins/ml2** on the controller of Openstack and find the ml2_conf.ini file. Then modify the value of**extension_drivers** parameter to "port_security" .

Command`vi /etc/neutron/plugins/ml2/ml2_conf.ini`



```
[root@controller ~]# vi /etc/neutron/plugins/ml2/ml2_conf.ini
[ml2]
type_drivers = flat,vlan
tenant_network_types = vlan
mechanism_drivers = openvswitch
extension_drivers = port_security
```

Step 3: Install hs-manager

1. On the Openstack platform, create a program and user (the user should have the permission of administrator), such as program: vfw/ user: test.
2. Upload the hs-manager image to the program and then install. For the details, refer to "Deploying CloudEdge on OpenStack" on Page 21.

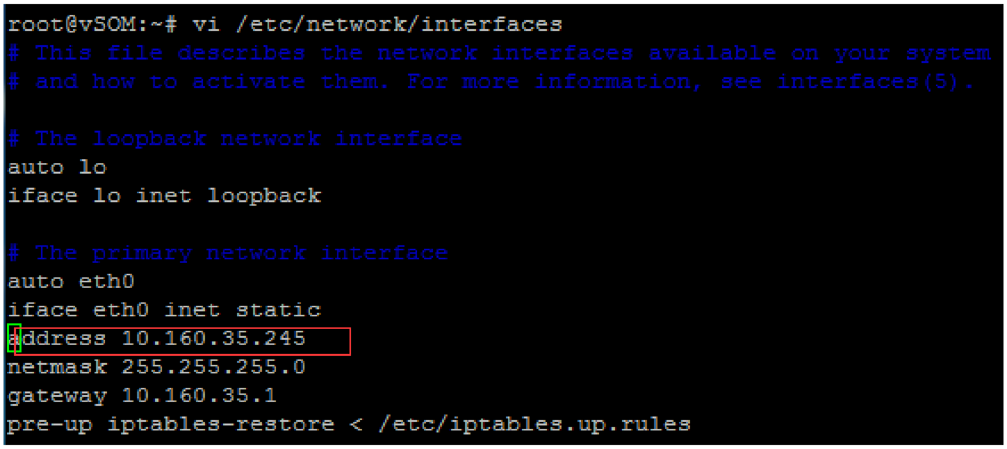
   Note: When creating the type of cloud host, you should configure 2 vCPU, 4GB memory and 15GB root disk. When you configure the network, the network should be connected to the Internet.
3. Start hs-manager instance and hs-manager will manage the CloudEdge VM which is used to replace router.

Step 4: Configure on the hs-manager

Log in hs-manager and configure as follows:

1. Configure the management interface and write the hs-manager IP assigned by Openstack to the corresponding files of MGT interface.

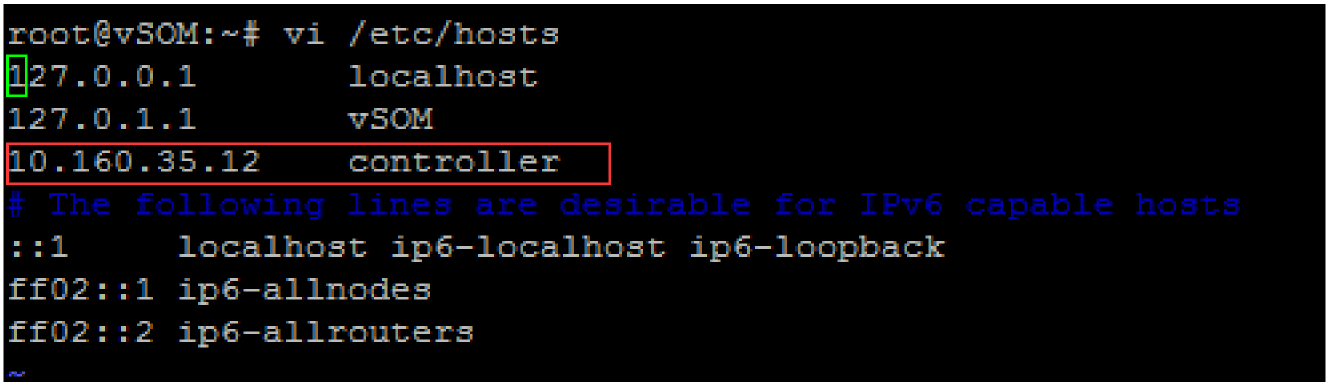
   Command:`vi /etc/network/interfaces`



```
root@vSOM:~# vi /etc/network/interfaces
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto eth0
iface eth0 inet static
address 10.160.35.245
netmask 255.255.255.0
gateway 10.160.35.1
pre-up iptables-restore < /etc/iptables.up.rules
```

2. Configure the IP of Openstack controller.

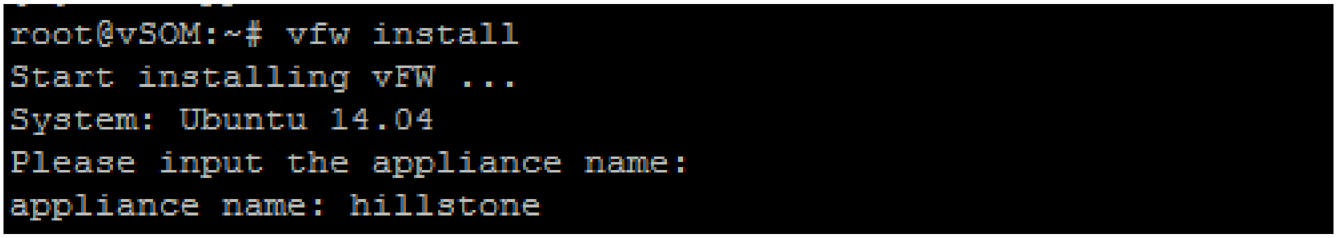
   Command:`vi /etc/hosts`



```
root@vSOM:~# vi /etc/hosts
127.0.0.1       localhost
127.0.1.1       vSOM
10.160.35.12    controller
# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
~
```

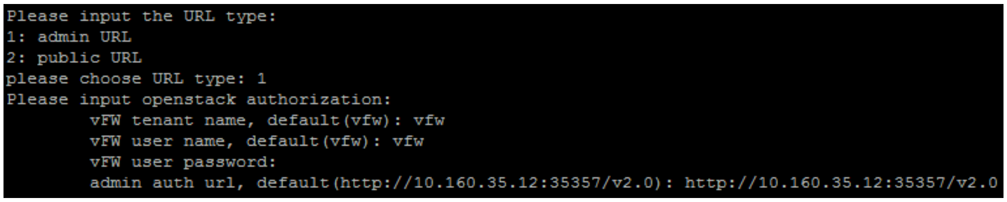
Step 5: Install CloudEdge on the hs-manager

1. Log in the hs-manager console and execute `vfw install` command to install CloudEdge. Input the appliance name (the name can be any) and press **Enter**. The example is as follows:



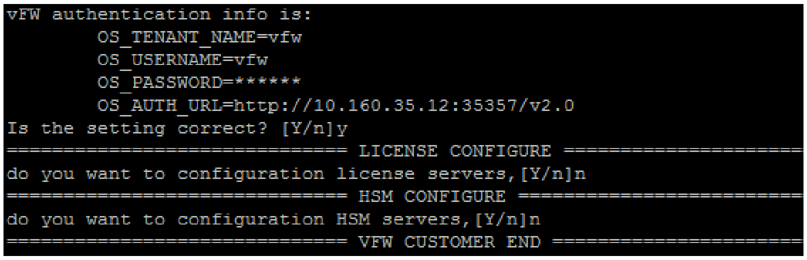
```
root@vSOM:~# vfw install
Start installing vFW ...
System: Ubuntu 14.04
Please input the appliance name:
appliance name: hillstone
```

2. Choose the type of endpoint URL as 1, input the program information of installing CloudEdge, user information and admin authentication URL, and then press Enter. The example is as follows:



```
Please input the URL type:
1: admin URL
2: public URL
please choose URL type: 1
Please input openstack authorization:
        vFW tenant name, default(vfw): vfw
        vFW user name, default(vfw): vfw
        vFW user password:
        admin auth url, default(http://10.160.35.12:35357/v2.0): http://10.160.35.12:35357/v2.0
```

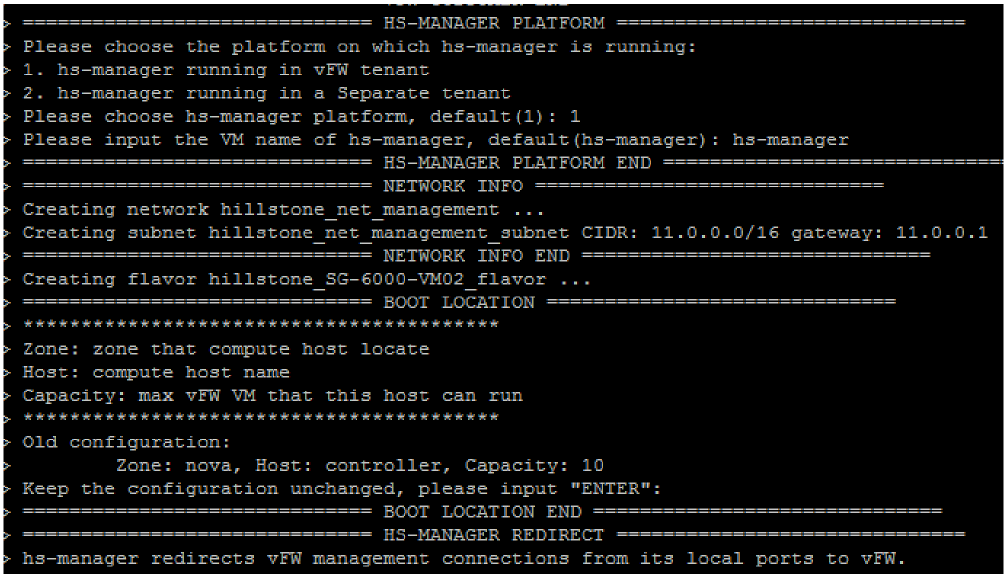
3. Input "y" and press Enter if the setting is correct. Input "n" to decide whether to install license servers and HSM servers, and then press **Enter**. The example is as follows:



```
vFW authentication info is:
        OS_TENANT_NAME=vfw
        OS_USERNAME=vfw
        OS_PASSWORD=******
        OS_AUTH_URL=http://10.160.35.12:35357/v2.0
Is the setting correct? [Y/n]y
============================== LICENSE CONFIGURE =====================
do you want to configuration license servers,[Y/n]n
============================== HSM CONFIGURE =========================
do you want to configuration HSM servers,[Y/n]n
============================== VFW CUSTOMER END ======================
```

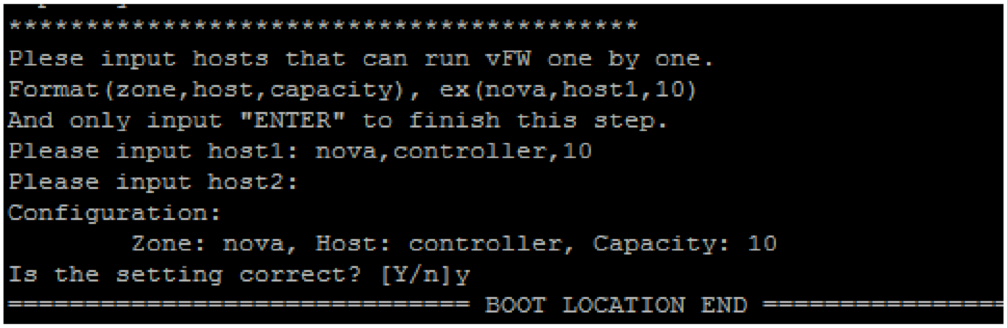
4. Please choose the platform on which hs-manager is running. The recommended selection is 1, which means hs-manager is running on the CloudEdge tenant. Input the name of hs-manager VM

and press Enter. The example is as follows:



```
> ============================== HS-MANAGER PLATFORM ==============================
> Please choose the platform on which hs-manager is running:
> 1. hs-manager running in vFW tenant
> 2. hs-manager running in a Separate tenant
> Please choose hs-manager platform, default(1): 1
> Please input the VM name of hs-manager, default(hs-manager): hs-manager
> ============================== HS-MANAGER PLATFORM END ==============================
> ============================== NETWORK INFO ==============================
> Creating network hillstone_net_management ...
> Creating subnet hillstone_net_management_subnet CIDR: 11.0.0.0/16 gateway: 11.0.0.1
> ============================== NETWORK INFO END ==============================
> Creating flavor hillstone_SG-6000-VM02_flavor ...
> ============================== BOOT LOCATION ==============================
> *****************************************
> Zone: zone that compute host locate
> Host: compute host name
> Capacity: max vFW VM that this host can run
> *****************************************
> Old configuration:
>         Zone: nova, Host: controller, Capacity: 10
> Keep the configuration unchanged, please input "ENTER":
> ============================== BOOT LOCATION END ==============================
> ============================== HS-MANAGER REDIRECT ==============================
> hs-manager redirects vFW management connections from its local ports to vFW.
```

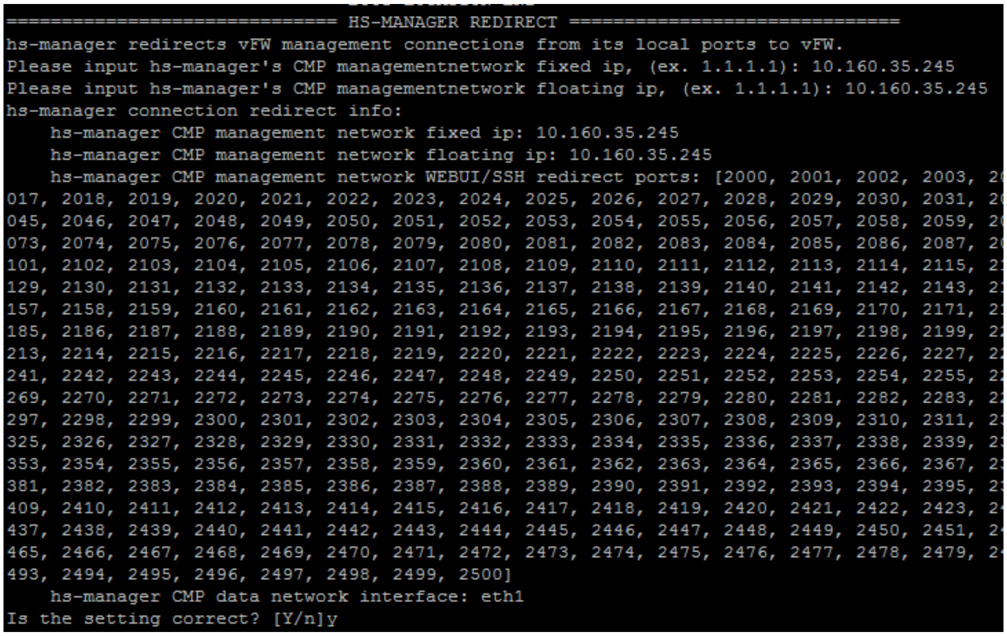
5. Input the information of hosts to be installed (you can input several hosts). Press Enter when one host has finished setting. If you press Enter directly without inputting anything, the setting will be finished. The example is as follows:



```
*****************************************
Plese input hosts that can run vFW one by one.
Format(zone,host,capacity), ex(nova,host1,10)
And only input "ENTER" to finish this step.
Please input host1: nova,controller,10
Please input host2:
Configuration:
        Zone: nova, Host: controller, Capacity: 10
Is the setting correct? [Y/n]y
============================== BOOT LOCATION END ================
```

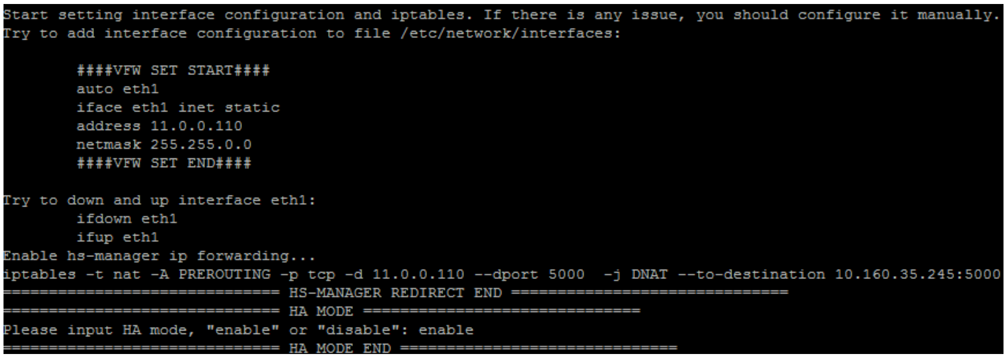
6. After inputting "y", you need to input the fixed IP and floating IP of hs-manager's MGT interface. If the network is provide, the floating IP should be configured as the MGT interface IP

or hs-manager’s floating IP. Then type “y” if the setting is correct. The example is as follows:



```
=============================== HS-MANAGER REDIRECT ===============================
hs-manager redirects vFW management connections from its local ports to vFW.
Please input hs-manager's CMP managementnetwork fixed ip, (ex. 1.1.1.1): 10.160.35.245
Please input hs-manager's CMP managementnetwork floating ip, (ex. 1.1.1.1): 10.160.35.245
hs-manager connection redirect info:
    hs-manager CMP management network fixed ip: 10.160.35.245
    hs-manager CMP management network floating ip: 10.160.35.245
    hs-manager CMP management network WEBUI/SSH redirect ports: [2000, 2001, 2002, 2003, 20
017, 2018, 2019, 2020, 2021, 2022, 2023, 2024, 2025, 2026, 2027, 2028, 2029, 2030, 2031, 20
045, 2046, 2047, 2048, 2049, 2050, 2051, 2052, 2053, 2054, 2055, 2056, 2057, 2058, 2059, 20
073, 2074, 2075, 2076, 2077, 2078, 2079, 2080, 2081, 2082, 2083, 2084, 2085, 2086, 2087, 20
101, 2102, 2103, 2104, 2105, 2106, 2107, 2108, 2109, 2110, 2111, 2112, 2113, 2114, 2115, 2
129, 2130, 2131, 2132, 2133, 2134, 2135, 2136, 2137, 2138, 2139, 2140, 2141, 2142, 2143, 2
157, 2158, 2159, 2160, 2161, 2162, 2163, 2164, 2165, 2166, 2167, 2168, 2169, 2170, 2171, 2
185, 2186, 2187, 2188, 2189, 2190, 2191, 2192, 2193, 2194, 2195, 2196, 2197, 2198, 2199, 2
213, 2214, 2215, 2216, 2217, 2218, 2219, 2220, 2221, 2222, 2223, 2224, 2225, 2226, 2227, 2
241, 2242, 2243, 2244, 2245, 2246, 2247, 2248, 2249, 2250, 2251, 2252, 2253, 2254, 2255, 2
269, 2270, 2271, 2272, 2273, 2274, 2275, 2276, 2277, 2278, 2279, 2280, 2281, 2282, 2283, 2
297, 2298, 2299, 2300, 2301, 2302, 2303, 2304, 2305, 2306, 2307, 2308, 2309, 2310, 2311, 2
325, 2326, 2327, 2328, 2329, 2330, 2331, 2332, 2333, 2334, 2335, 2336, 2337, 2338, 2339, 2
353, 2354, 2355, 2356, 2357, 2358, 2359, 2360, 2361, 2362, 2363, 2364, 2365, 2366, 2367, 2
381, 2382, 2383, 2384, 2385, 2386, 2387, 2388, 2389, 2390, 2391, 2392, 2393, 2394, 2395, 2
409, 2410, 2411, 2412, 2413, 2414, 2415, 2416, 2417, 2418, 2419, 2420, 2421, 2422, 2423, 2
437, 2438, 2439, 2440, 2441, 2442, 2443, 2444, 2445, 2446, 2447, 2448, 2449, 2450, 2451, 2
465, 2466, 2467, 2468, 2469, 2470, 2471, 2472, 2473, 2474, 2475, 2476, 2477, 2478, 2479, 2
493, 2494, 2495, 2496, 2497, 2498, 2499, 2500]
    hs-manager CMP data network interface: eth1
Is the setting correct? [Y/n]y
```

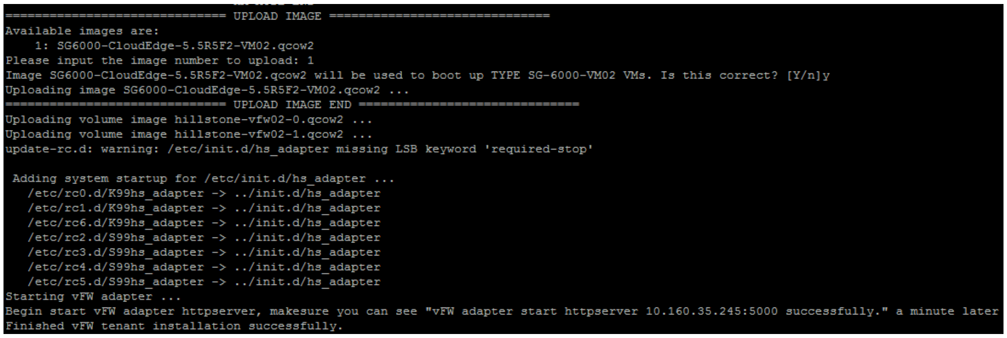
7. Hs-manager will configure interface and IP first, and then configure whether to enable HA function of CloudEdge. You can enable it as needed. The example is as follows:



```
Start setting interface configuration and iptables. If there is any issue, you should configure it manually.
Try to add interface configuration to file /etc/network/interfaces:

        ####VFW SET START####
        auto eth1
        iface eth1 inet static
        address 11.0.0.110
        netmask 255.255.0.0
        ####VFW SET END####

Try to down and up interface eth1:
        ifdown eth1
        ifup eth1
Enable hs-manager ip forwarding...
iptables -t nat -A PREROUTING -p tcp -d 11.0.0.110 --dport 5000  -j DNAT --to-destination 10.160.35.245:5000
============================== HS-MANAGER REDIRECT END ==============================
============================== HA MODE ==============================
Please input HA mode, "enable" or "disable": enable
============================== HA MODE END ==============================
```

8. Select image files of CloudEgde and press **Enter** to install CloudEdge. When the window displays “Finished vFW tenant installation successfully”, it means the installation is finished suc-

cessfully.



```
============================== UPLOAD IMAGE ==============================
Available images are:
    1: SG6000-CloudEdge-5.5R5F2-VM02.qcow2
Please input the image number to upload: 1
Image SG6000-CloudEdge-5.5R5F2-VM02.qcow2 will be used to boot up TYPE SG-6000-VM02 VMs. Is this correct? [Y/n]y
Uploading image SG6000-CloudEdge-5.5R5F2-VM02.qcow2 ...
============================== UPLOAD IMAGE END ==============================
Uploading volume image hillstone-vfw02-0.qcow2 ...
Uploading volume image hillstone-vfw02-1.qcow2 ...
update-rc.d: warning: /etc/init.d/hs_adapter missing LSB keyword 'required-stop'

 Adding system startup for /etc/init.d/hs_adapter ...
   /etc/rc0.d/K99hs_adapter -> ../init.d/hs_adapter
   /etc/rc1.d/K99hs_adapter -> ../init.d/hs_adapter
   /etc/rc6.d/K99hs_adapter -> ../init.d/hs_adapter
   /etc/rc2.d/S99hs_adapter -> ../init.d/hs_adapter
   /etc/rc3.d/S99hs_adapter -> ../init.d/hs_adapter
   /etc/rc4.d/S99hs_adapter -> ../init.d/hs_adapter
   /etc/rc5.d/S99hs_adapter -> ../init.d/hs_adapter
Starting vFW adapter ...
Begin start vFW adapter httpserver, makesure you can see "vFW adapter start httpserver 10.160.35.245:5000 successfully." a minute later
Finished vFW tenant installation successfully.
```

Appendix: hs-manager command

The Program users can manage CloudEdge by hs-manager VM. The related commands of hs-manager VM are as follows:

`vfw help`- Displays help information.

`vfw install` - Install vfw images, MGT network and so on

`vfw uninstall` - Uninstall vfw images, MGT network and so on

`vfw shutdown` - Force to delete all vfw

`vfw create-vfw` - Create vfw for a router manually

`vfw delete-vfw` - Delete vfw of a router

`vfw change-image` - Change vfw image

`vfw ha-mode` - Enable or disable HA mode

`vfw ha-host-mode` - Set startup position of vfw in HA mode

`vfw host-add` - Add hosts that create vfw

`vfw host-del` - Delete hosts that create vfw

`vfw show-nat-pool` - Shows the used and unused nat ports

`vfw nat-port-add` - Add nat ports for nat-pool

`vfw nat-port-del` - Delete nat ports in nat-pool

`vfw show-config` - Shows configuration information of hs-manager `vfw show-vfw-pool` - Shows all vfw information in brief

`vfw show-vfw-map` - Shows all vfw information in details

`vfw show-adapter` - Shows the status of adapter

`vfw start-adapter` - Start adapter service (opened by default)

`vfw stop-adapter` - Stop adapter service

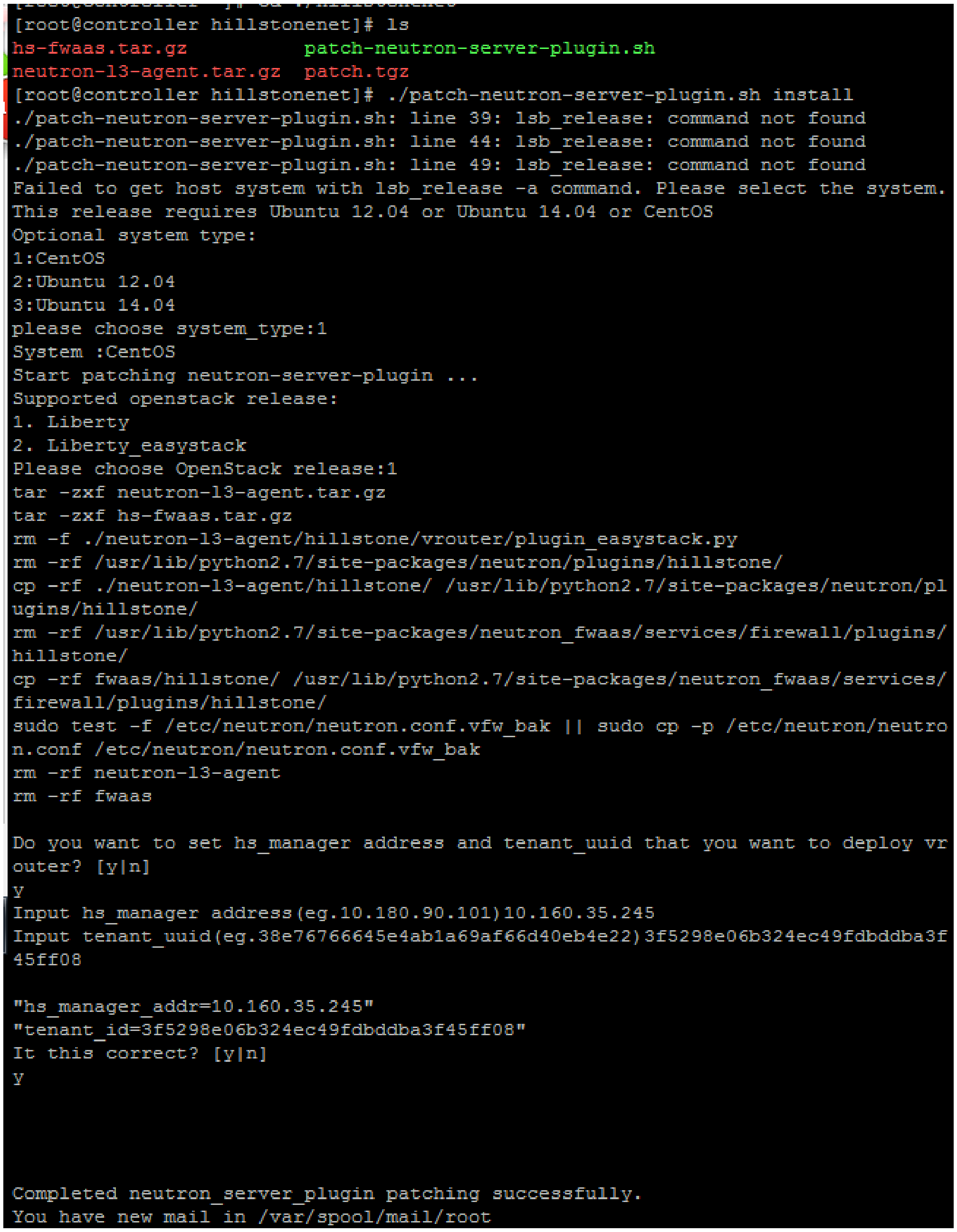
`vfw enable-adapter-log` - Enable debugging logs

`vfw disable-adapter-log` - Disable debugging logs

Step 6: Install patch files on controller

1. Log in the controller of Openstack, find patch files and execute the command to extract the `patch.tgz` file.

2. Execute the installation command to install patch files. When the file is installed, the page will show "Completed neutron_server_plugin patching successfully". The example is as follows:



```
[root@controller hillstonenet]# ls
hs-fwaas.tar.gz          patch-neutron-server-plugin.sh
neutron-l3-agent.tar.gz  patch.tgz
[root@controller hillstonenet]# ./patch-neutron-server-plugin.sh install
./patch-neutron-server-plugin.sh: line 39: lsb_release: command not found
./patch-neutron-server-plugin.sh: line 44: lsb_release: command not found
./patch-neutron-server-plugin.sh: line 49: lsb_release: command not found
Failed to get host system with lsb_release -a command. Please select the system.
This release requires Ubuntu 12.04 or Ubuntu 14.04 or CentOS
Optional system type:
1:CentOS
2:Ubuntu 12.04
3:Ubuntu 14.04
please choose system_type:1
System :CentOS
Start patching neutron-server-plugin ...
Supported openstack release:
1. Liberty
2. Liberty_easystack
Please choose OpenStack release:1
tar -zxf neutron-l3-agent.tar.gz
tar -zxf hs-fwaas.tar.gz
rm -f ./neutron-l3-agent/hillstone/vrouter/plugin_easystack.py
rm -rf /usr/lib/python2.7/site-packages/neutron/plugins/hillstone/
cp -rf ./neutron-l3-agent/hillstone/ /usr/lib/python2.7/site-packages/neutron/pl
ugins/hillstone/
rm -rf /usr/lib/python2.7/site-packages/neutron_fwaas/services/firewall/plugins/
hillstone/
cp -rf fwaas/hillstone/ /usr/lib/python2.7/site-packages/neutron_fwaas/services/
firewall/plugins/hillstone/
sudo test -f /etc/neutron/neutron.conf.vfw_bak || sudo cp -p /etc/neutron/neutro
n.conf /etc/neutron/neutron.conf.vfw_bak
rm -rf neutron-l3-agent
rm -rf fwaas

Do you want to set hs_manager address and tenant_uuid that you want to deploy vr
outer? [y|n]
y
Input hs_manager address(eg.10.180.90.101)10.160.35.245
Input tenant_uuid(eg.38e76766645e4ab1a69af66d40eb4e22)3f5298e06b324ec49fdbddba3f
45ff08

"hs_manager_addr=10.160.35.245"
"tenant_id=3f5298e06b324ec49fdbddba3f45ff08"
It this correct? [y|n]
y




Completed neutron_server_plugin patching successfully.
You have new mail in /var/spool/mail/root
```

Notes:

1. When the patch is installed, the neutron.conf file will be backed up as the neutron.conf.vfw_bak file.
2. When the patch is uninstalled, the neutron.conf file will be overlapped by the neutron.conf.vfw_bak file automatically.
3. Before updating the patch, you need to uninstall the old version first. When you use CloudEdge, the manually modified configuration information in neutron.conf will be lost.
4. If there' s a problem on the hs-manager, execute service adapter restart to restart adapter process. If the hs-manager still cannot work, you can uninstall patch, delete routers and other configurations first, and then re-install as the above steps.

Step 7: Complete configuration

After the above steps are executed, you will complete all configurations of replacing routers. When routers and firewall of Openstack are used, the corresponding CloudEdge VMs will change as follows:

- When you create route on Openstack, one or two CloudEdge VMs will boot automatically to replace virtual routers. (When HA is enabled, if you create one router, two CloudEdge VMs which are in a HA group will start; when HA is disabled, if you create one router, only one CloudEdge VM will start.)
- When you set/ clear gateway for the Openstack router and bind/ unbind subnet, the corresponding CloudEdge VM of the router will add/ delete interface automatically.
- When you add router for the Openstack firewall, the policy of firewall will be translated to that of CloudEdge and be issued to the corresponding VM.

- When you modify the rule sequence or content of the Openstack firewall policy, the policy of CloudEdge VM will change too.

- When you bind/ unbind floating IPs for the VM connected to the Openstack router, the corresponding CloudEdge VM of the router will add/ delete nat rules automatically.

Notes:

1. CloudEdge supports at most 10 interfaces and two of them are HA interface and MGT interface. Therefore, at most 8 router interfaces can be supported. When the route is failed to create, you’ re suggested to check whether the environment resource is insufficient first.
2. When the route is created, system will configure for some minutes. Don’ t refresh the page at the time.
3. If the route is failed to delete, check whether there’ s static routing table or floating IP.
4. If the route is failed to add/ delete and a prompt showing “Error: cannot add an interface now: Slave vfw connection failed, the slave vfw will reboot.” Please wait for 2 minutes and operate later.
5. When you select several interfaces of router to delete, if the interfaces are failed to delete, please delete again. (It is because there are users in other programs are deleting interface, the problem is from Openstack not from CloudEdge.)
6. During the process of deleting routers, don’ t operate the hs-manager.
7. When the route is failed to delete on the Openstack routing interface since the CloudEdge VM has problems, you should execute `vfw delete-vfw` to delete CloudEdge VM first and then delete the router.

8. To upgrade CloudEdge, in the HA mode, you’ re suggested to upgrade the backup device first and upgrade the master device after rebooting by WebUI. When upgrading CloudEdge by changing image, you should execute `vfw change-image` command first on hs-manager, and then configure the route. After CloudEdge is upgraded, the original route can still be used. If you create a new route, the new CloudEdge image will be used and a new VM will boot automatically.

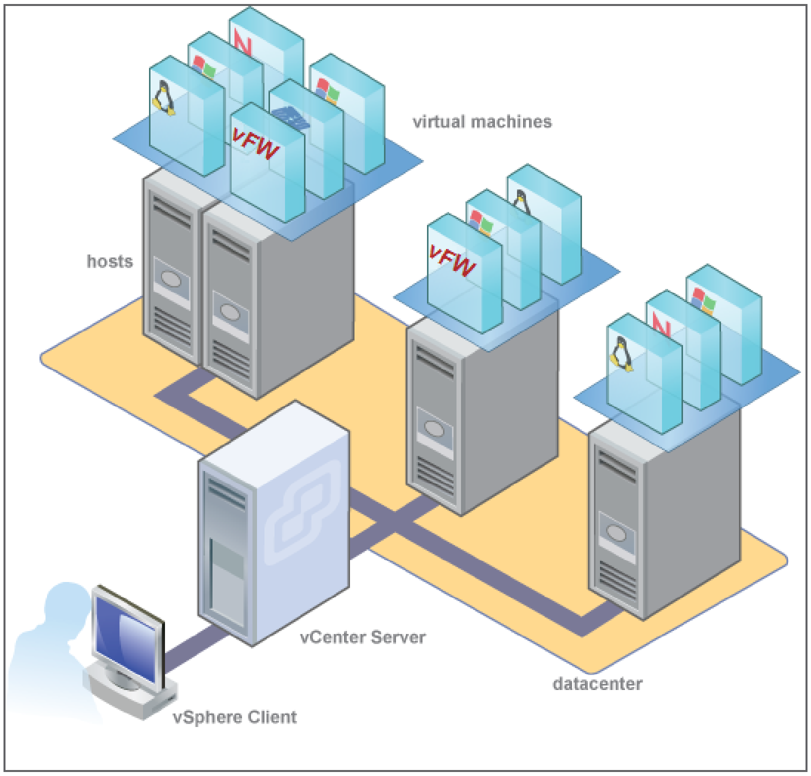
Deploying CloudEdge on VMware ESXi

CloudEdge is packed in VMDK and OVA file, and can be installed on a VMware ESXi server in a X86 device.

Before deploying vFW, you should be already familiar with VMware vSphere hypervisor, ESXi host and VMware virtual machines.

Deployment Scenarios

You can deploy one or more virtual firewalls on ESXi servers.



System Requirements and Limits

To deploy CloudEdge , the VMware ESXi server should be:

- VMware ESXi 5.0, 5.5 or 6.0.
- Requires at least 2 vCPU and 2 GB memory.
- It is suggested to create at least three vmNICs on a vFW: a management interface, a date ingress and a data egress.
- NIC type must be E1000 or vmxnet3. It is recommended that each VM can only be installed the same type of NIC, not both E1000 and vmxnet-3.

Installing vFW

To improve manageability and make full use of vSphere Hypervisor, we suggest you use vCenter and vSphere Client to manage ESXi servers.

You can deploy vFW by importing VMDK file or OVA file(VMDK and OVA file only from 5.5R4), importing OVA file is recommended, and then you can upgrade online using .img file; if the version of VMware vSphere Hypervisor is 6.0, deploying vFW by importing OVA file is recommended.

Installing vFW

Installing vFW by Importing OVA

Set up your ESXi Server, vCenter Server and vSphere Client host before installing vFW, and then get the OVA file.

1. Save the OVA file in your local computer.
2. Double click the local Sphere Client to enter the login page. In the login page, enter the IP address/Name , username and password of vCenter, and click **Login** to enter the main interface.
3. After logging in vCenter, click the localhost node in the left pane, then select **File > Deploy OVF Template**.
4. In the pop-up dialog box, click **Browse**, browse your PC and import vFW's OVA file to vCenter, click **Next**.
5. Confirm the details of the OVF template, click **Next**.
6. Enter the name of the OVF template, and select the location of list, click **Next**.
7. Select the host or cluster to deploy the OVF template on it, click **Next**.

8. Select the resource pool to run the OVF template in it, click **Next**.

   This page is displayed only when the cluster contains a resource pool.

9. The data storage to store the deployed OVF template has been selected by default, then click **Next**

10. Select the VM networks which OVF template use, then click **Next**.

11. Configure the service binding to vCenter Extension vService, click **Next**.

12. Click **Finish** to start the deployment.

    Wait for a while, and your vFW will be deployed successfully.

Installing CloudEdge by Importing VMDK

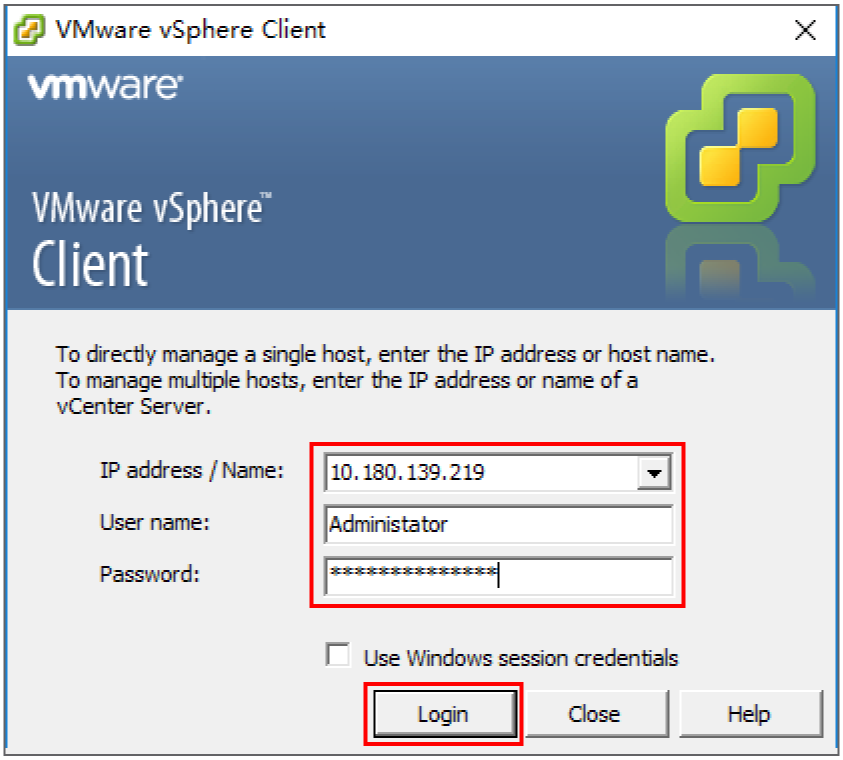
Contact Hillstone sales persons to get the trial or official CloudEdge VMDK file before installing. Then you can install CloudEdge by importing VMDK using three steps:

- Step 1: Importing VMDK
- Step 2: Creating a Virtual Machine
- Step 3: Selecting the CloudEdge VMDK File for VM

Step 1: Importing VMDK

1. Save the CloudEdge VMDK file in your local computer.

2. Double-click the local Sphere Client to enter the login page. In the login page, enter the IP address/Name , username and password of vCenter, and click **Login** to enter the main interface.



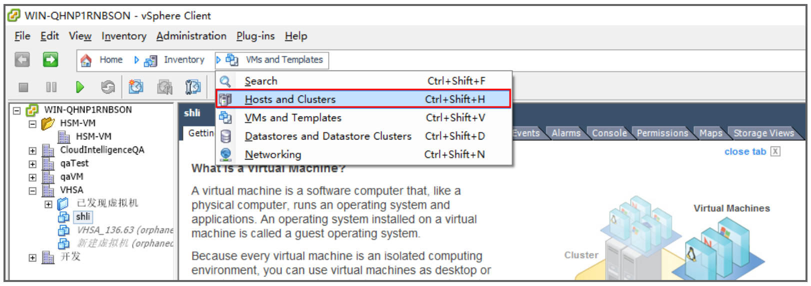
To directly manage a single host, enter the IP address or host name. To manage multiple hosts, enter the IP address or name of a vCenter Server.

IP address / Name: 10.180.139.219

User name: Administator

Password: ***************

3. In the main interface, select **Home** > **Inventory** > **Hosts and Clusters** to enter the Hosts and Clusters page.

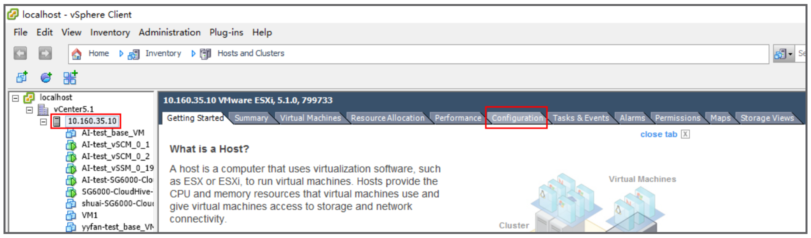


What is a Virtual Machine?

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.

Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or

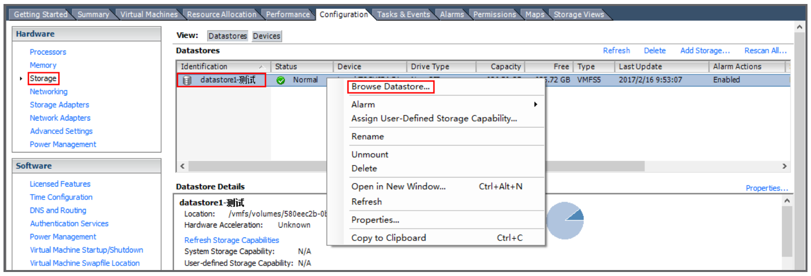
4. In the Hosts and Clusters page, choose the ESXi host which CloudEdge will belong to, and click the **Configuration** tab appears on the right pane to enter the configuration page.



What is a Host?

A host is a computer that uses virtualization software, such as ESX or ESXi, to run virtual machines. Hosts provide the CPU and memory resources that virtual machines use and give virtual machines access to storage and network connectivity.

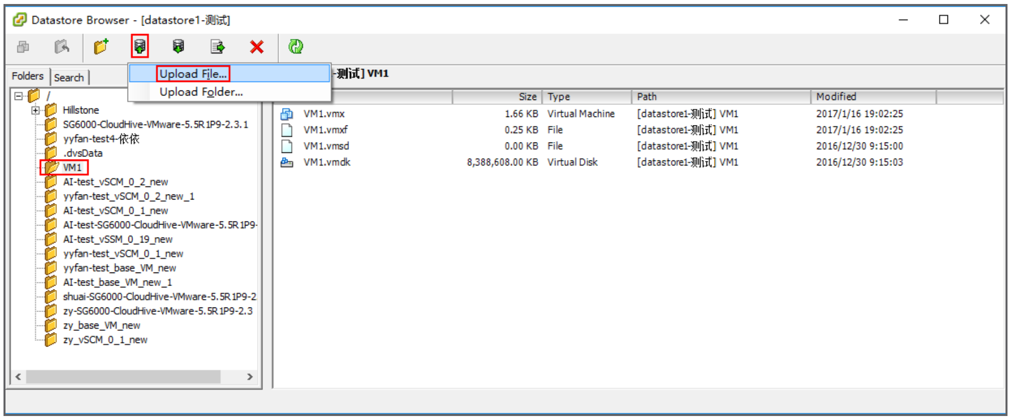
5. Under the **Configuration** tab, click **Storage** to enter the storage pane. In the storage pane, right-click the datastore you want to browse, and select **Browse Datastore** to enter the Datastore Browse page.



Identification	Status	Device	Drive Type	Capacity	Free	Type	Last Update	Alarm Actions
datastore1-测试	Normal				.72 GB	VMFS5	2017/2/16 9:53:07	Enabled

datastore1-测试
Location: /vmfs/volumes/580eec2b-0b
Hardware Acceleration: Unknown
System Storage Capability: N/A
User-defined Storage Capability: N/A

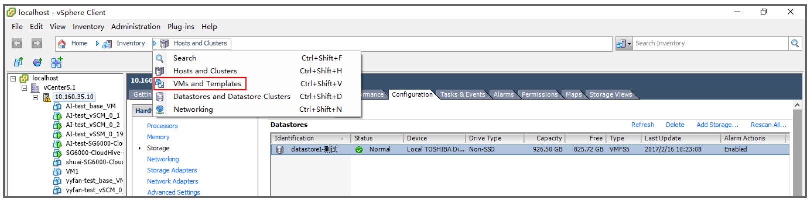
6. In the Datastore Browse page, select the folder to save file and click upload button . In the drop-down list, click **Upload File** to browse your PC to import CloudEdge's VMDK file to the datastore.



	Size	Type	Path	Modified
VM1.vmx	1.66 KB	Virtual Machine	[datastore1-测试] VM1	2017/1/16 19:02:25
VM1.vmxf	0.25 KB	File	[datastore1-测试] VM1	2017/1/16 19:02:25
VM1.vmsd	0.00 KB	File	[datastore1-测试] VM1	2016/12/30 9:15:00
VM1.vmdk	8,388,608.00 KB	Virtual Disk	[datastore1-测试] VM1	2016/12/30 9:15:03

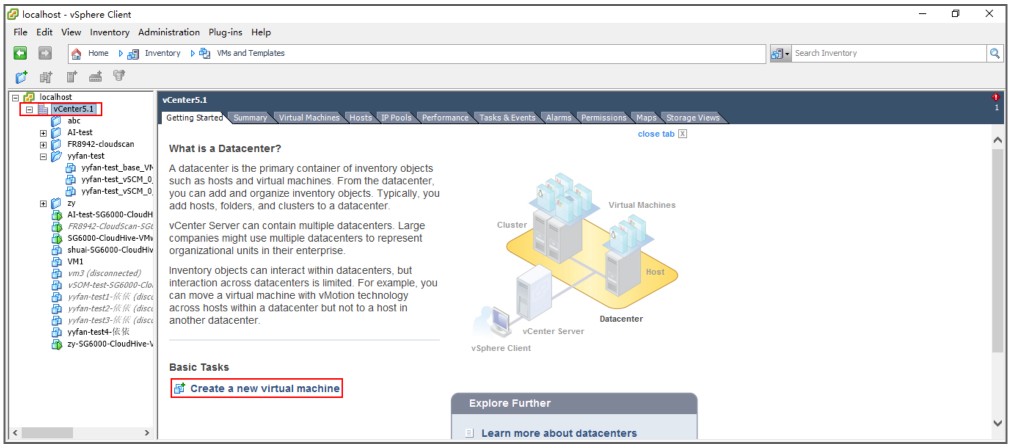
Step 2: Creating a Virtual Machine

1. In the vSphere Client main interface, select **Home > Inventory > VMs and Templates** to enter the VMs and Templates page.



Identification	Status	Device	Drive Type	Capacity	Free	Type	Last Update	Alarm Actions
datastore1-测试	Normal	Local TOSHIBA Di...	Non-SSD	926.50 GB	825.72 GB	VMFS5	2017/2/16 10:23:08	Enabled

2. In the VMs and Templates page, select a datacenter in the left pane and click **Create a new virtual machine** appears in the right pane. The Create New Virtual Machine wizard pops up.



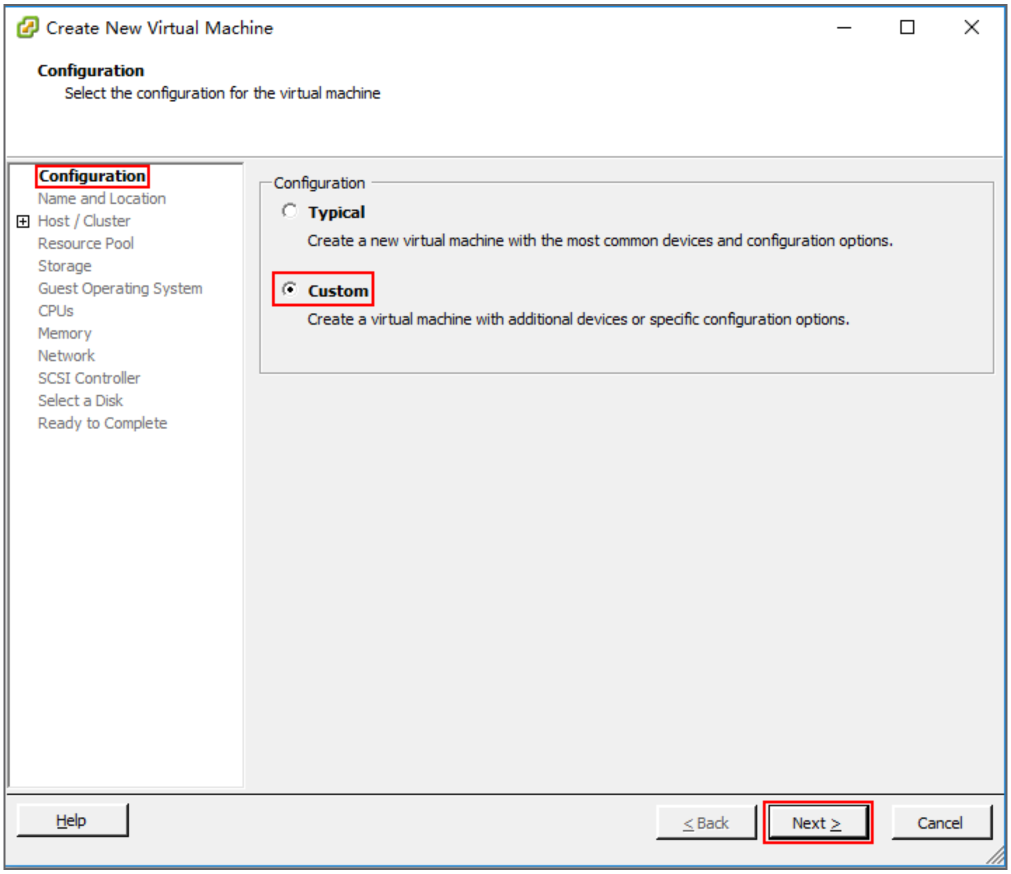
What is a Datacenter?

A datacenter is the primary container of inventory objects such as hosts and virtual machines. From the datacenter, you can add and organize inventory objects. Typically, you add hosts, folders, and clusters to a datacenter.

vCenter Server can contain multiple datacenters. Large companies might use multiple datacenters to represent organizational units in their enterprise.

Inventory objects can interact within datacenters, but interaction across datacenters is limited. For example, you can move a virtual machine with vMotion technology across hosts within a datacenter but not to a host in another datacenter.

3. In the Create New Virtual Machine wizard, select **Custom** under the **Configuration** tab, and click **Next**.



Create New Virtual Machine

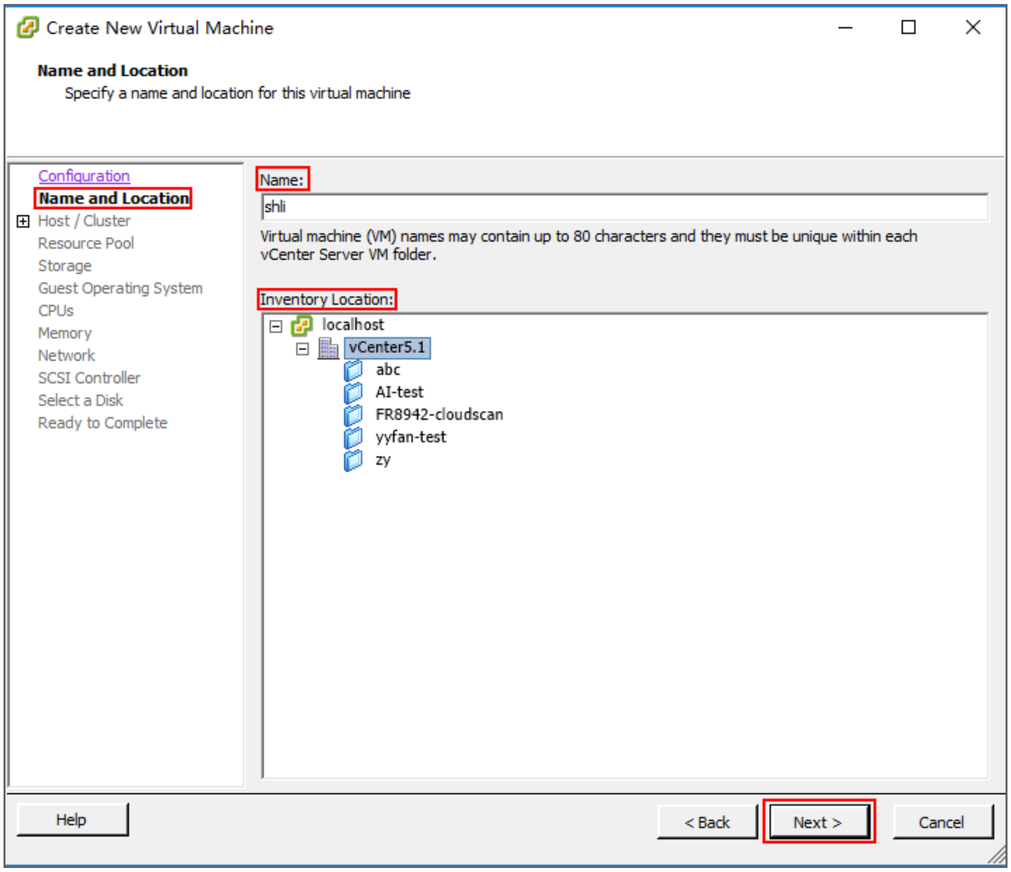
Configuration
Select the configuration for the virtual machine

Configuration

○ **Typical**
Create a new virtual machine with the most common devices and configuration options.

● **Custom**
Create a virtual machine with additional devices or specific configuration options.

4. Under the **Name and Location** tab, enter a name and select the inventory location for virtual machine , and click **Next**.



Create New Virtual Machine

Name and Location

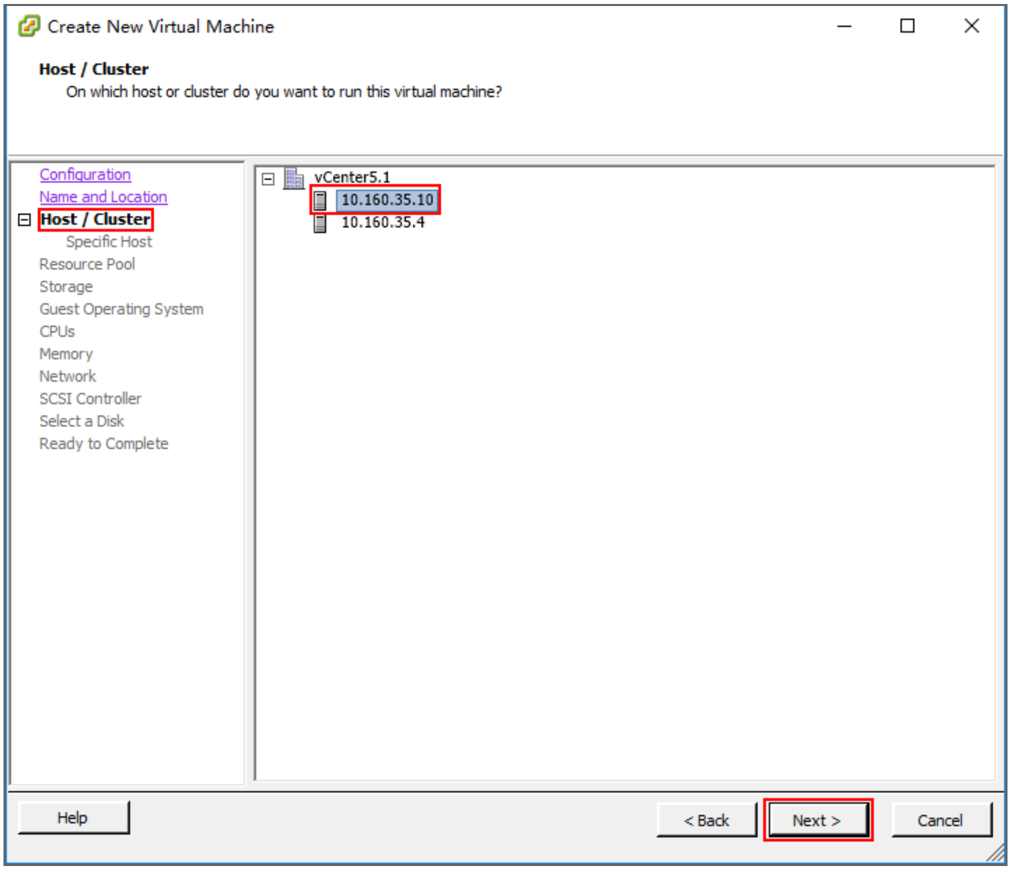
Specify a name and location for this virtual machine

Name: shli

Virtual machine (VM) names may contain up to 80 characters and they must be unique within each vCenter Server VM folder.

Inventory Location: localhost > vCenter5.1

5. Under the **Host/Cluster** tab, select your target ESXi host, and click **Next**.

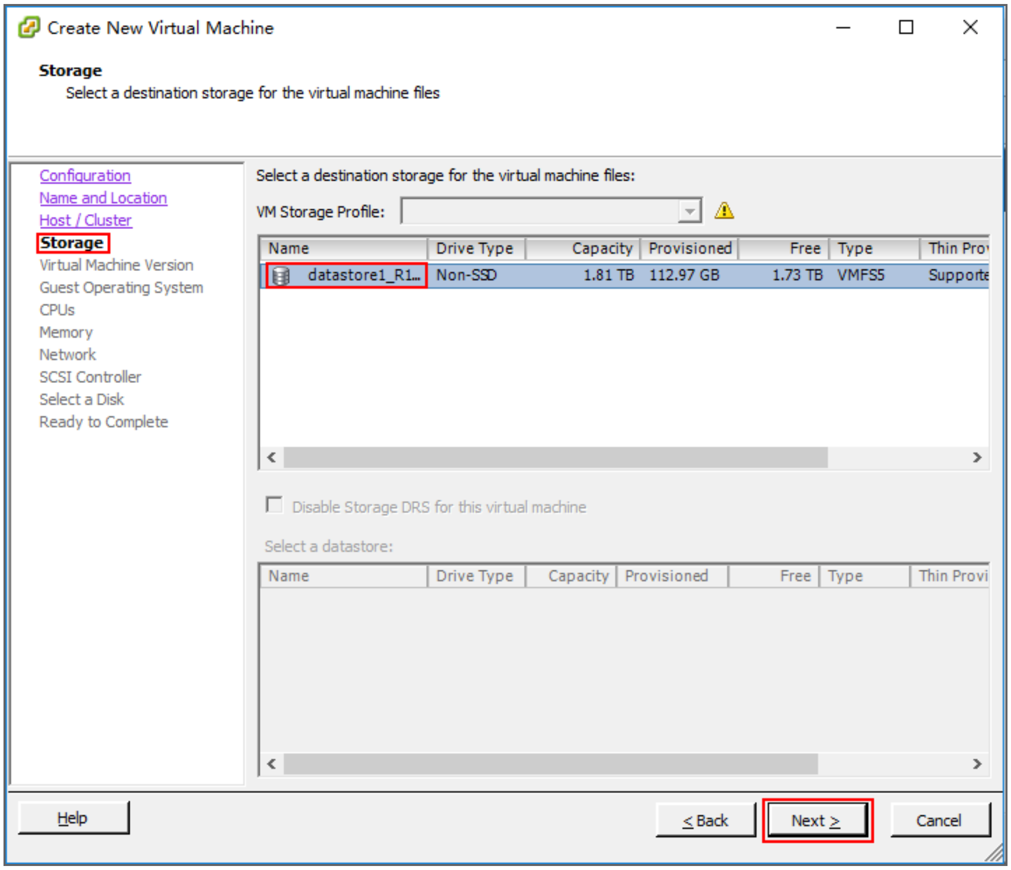


Create New Virtual Machine

Host / Cluster

On which host or cluster do you want to run this virtual machine?

6. Under the **Storage** tab, select a datastore for virtual machine files, and click **Next**.



Storage

Select a destination storage for the virtual machine files

Select a destination storage for the virtual machine files:

VM Storage Profile:

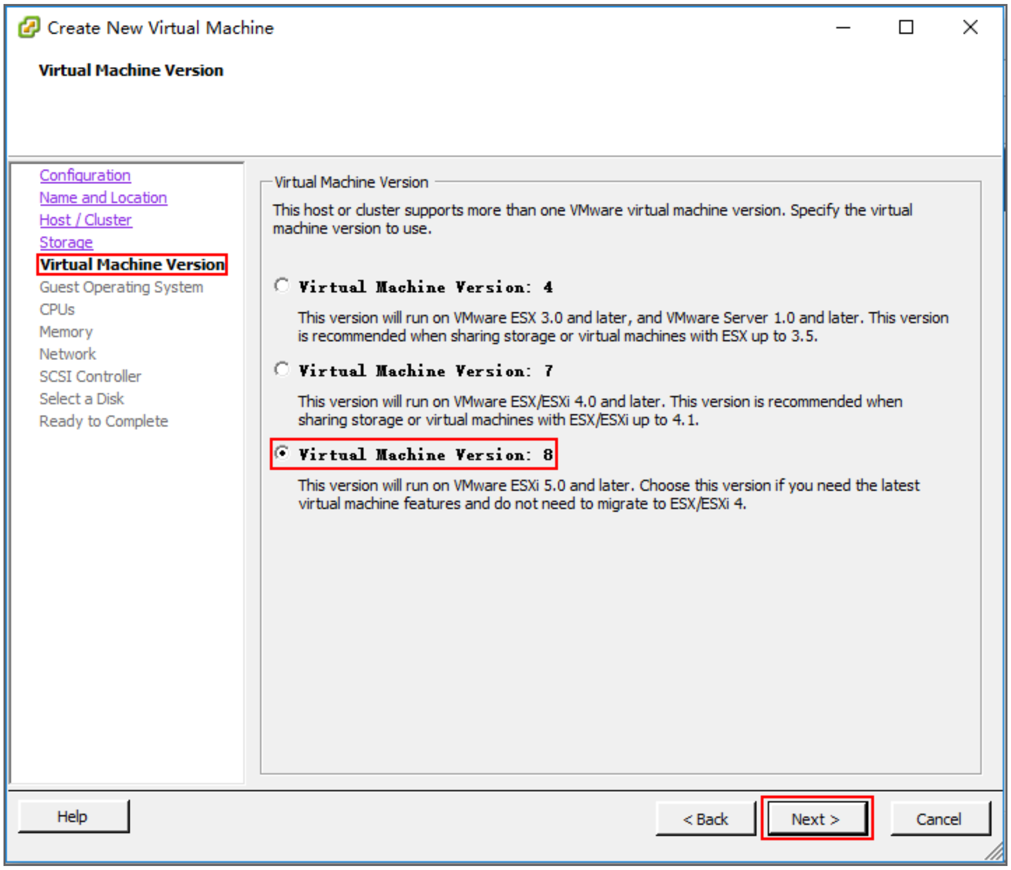
Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Pro
datastore1_R1...	Non-SSD	1.81 TB	112.97 GB	1.73 TB	VMFS5	Supporte

□ Disable Storage DRS for this virtual machine

Select a datastore:

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Provi

7. Under the **Virtual Machine Version** tab, select **Virtual Machine Version: 8**, and click **Next**.



Create New Virtual Machine

Virtual Machine Version

Virtual Machine Version

This host or cluster supports more than one VMware virtual machine version. Specify the virtual machine version to use.

○ Virtual Machine Version: 4

This version will run on VMware ESX 3.0 and later, and VMware Server 1.0 and later. This version is recommended when sharing storage or virtual machines with ESX up to 3.5.

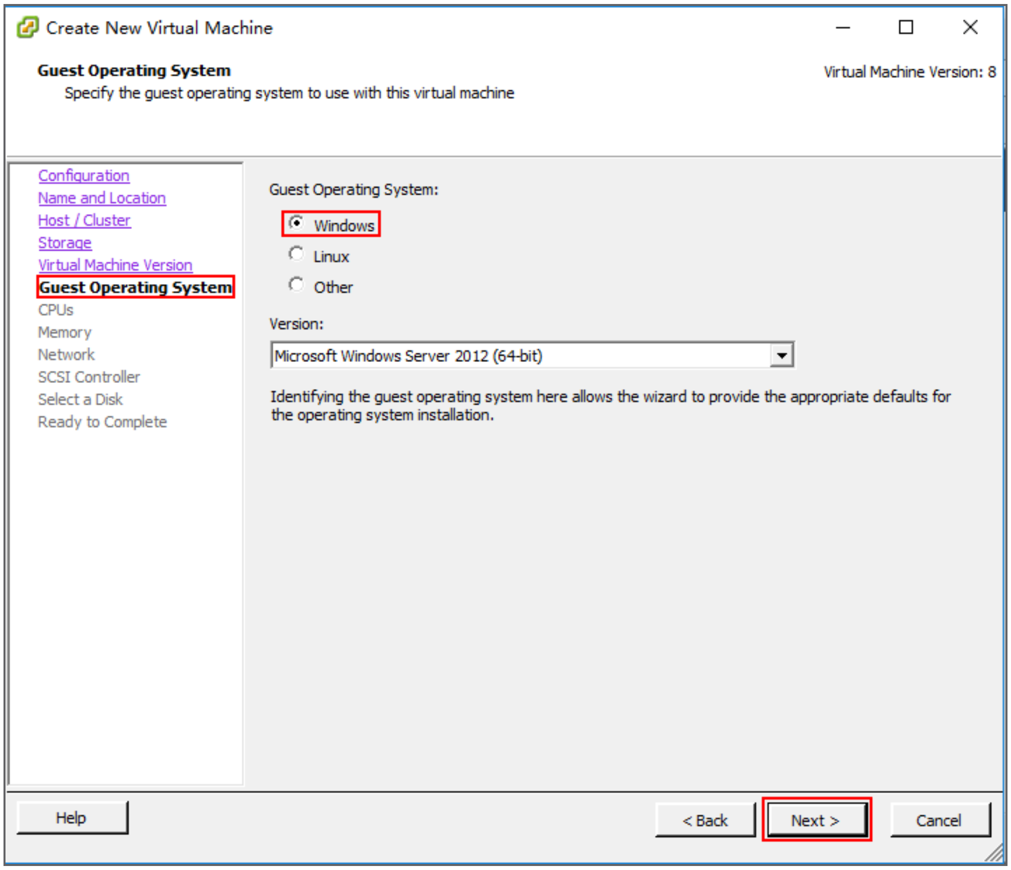
○ Virtual Machine Version: 7

This version will run on VMware ESX/ESXi 4.0 and later. This version is recommended when sharing storage or virtual machines with ESX/ESXi up to 4.1.

● Virtual Machine Version: 8

This version will run on VMware ESXi 5.0 and later. Choose this version if you need the latest virtual machine features and do not need to migrate to ESX/ESXi 4.

8. Under the **Guest Operating System** tab, select **Windows**, and click **Next**.



Create New Virtual Machine

Guest Operating System

Specify the guest operating system to use with this virtual machine

Virtual Machine Version: 8

Guest Operating System:

● Windows

○ Linux

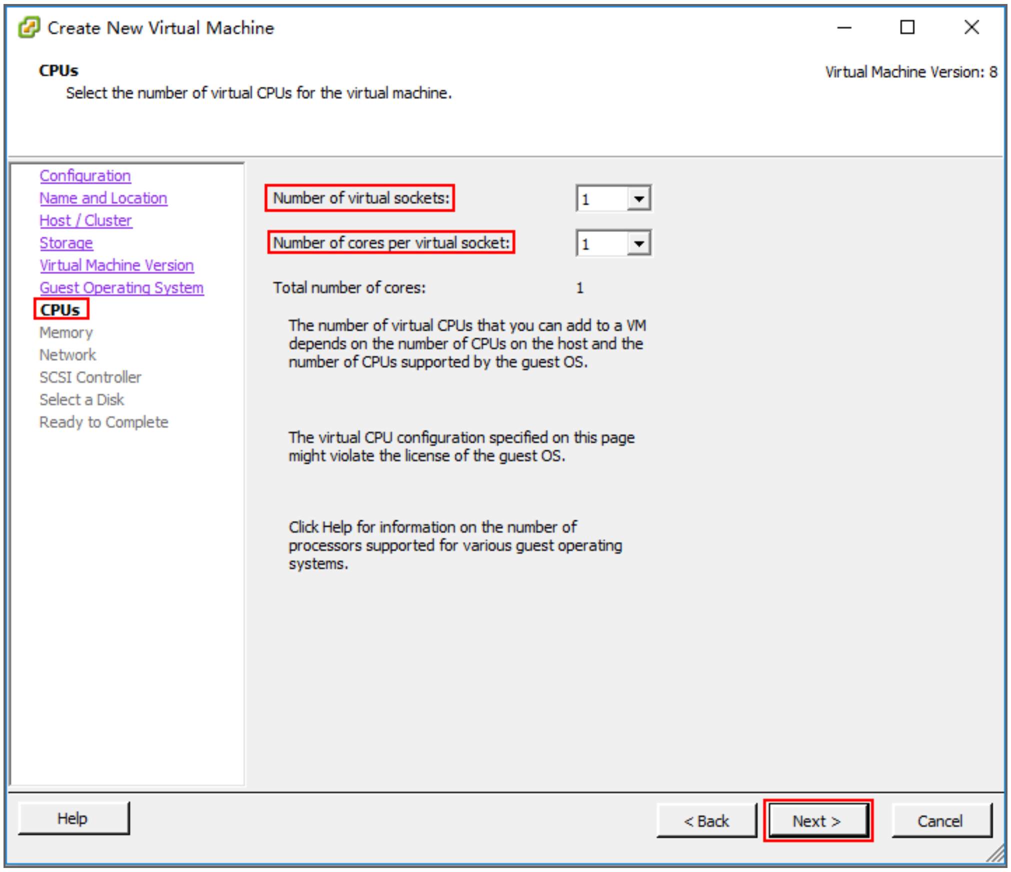
○ Other

Version:

Microsoft Windows Server 2012 (64-bit)

Identifying the guest operating system here allows the wizard to provide the appropriate defaults for the operating system installation.

9. Under the **CPUs** tab, apply appropriate value for CPU and core. Click **Next**.



Create New Virtual Machine

CPUs

Select the number of virtual CPUs for the virtual machine.

Virtual Machine Version: 8

Number of virtual sockets: 1

Number of cores per virtual socket: 1

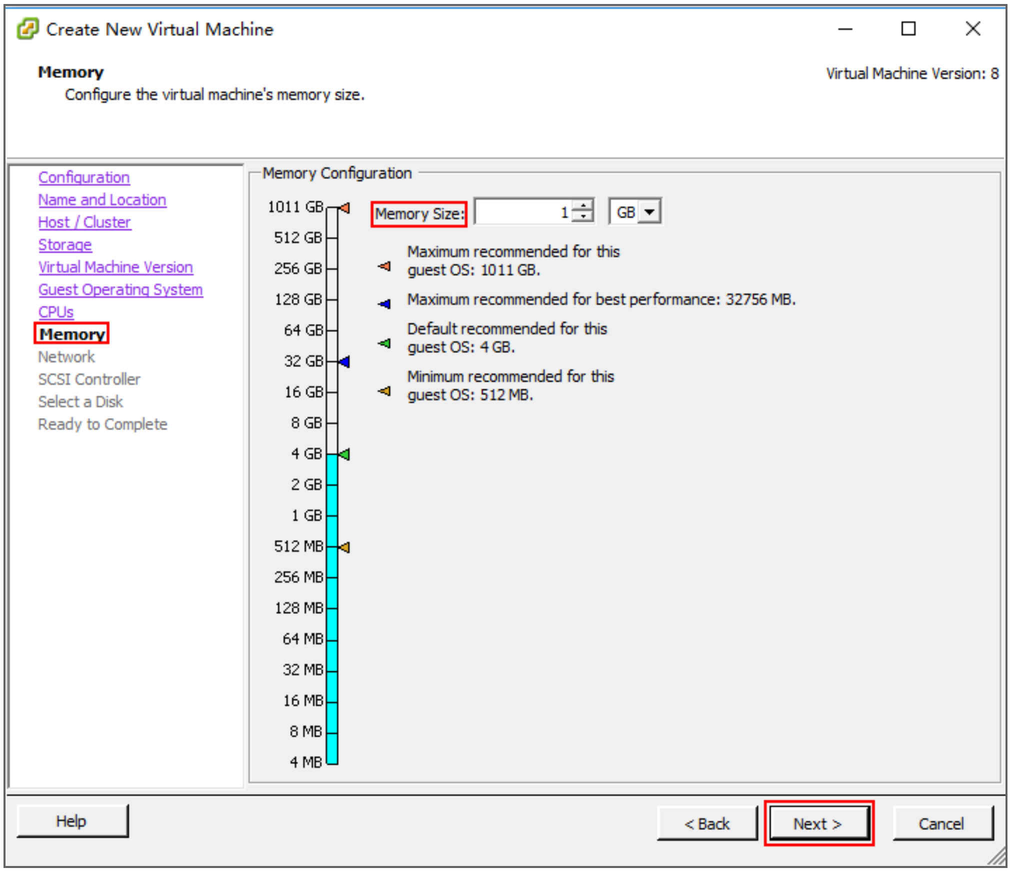
Total number of cores: 1

The number of virtual CPUs that you can add to a VM depends on the number of CPUs on the host and the number of CPUs supported by the guest OS.

The virtual CPU configuration specified on this page might violate the license of the guest OS.

Click Help for information on the number of processors supported for various guest operating systems.

10. Under the **Memory** tab, assign a memory value for CloudEdge . Click **Next**.



Memory Size: 1 GB

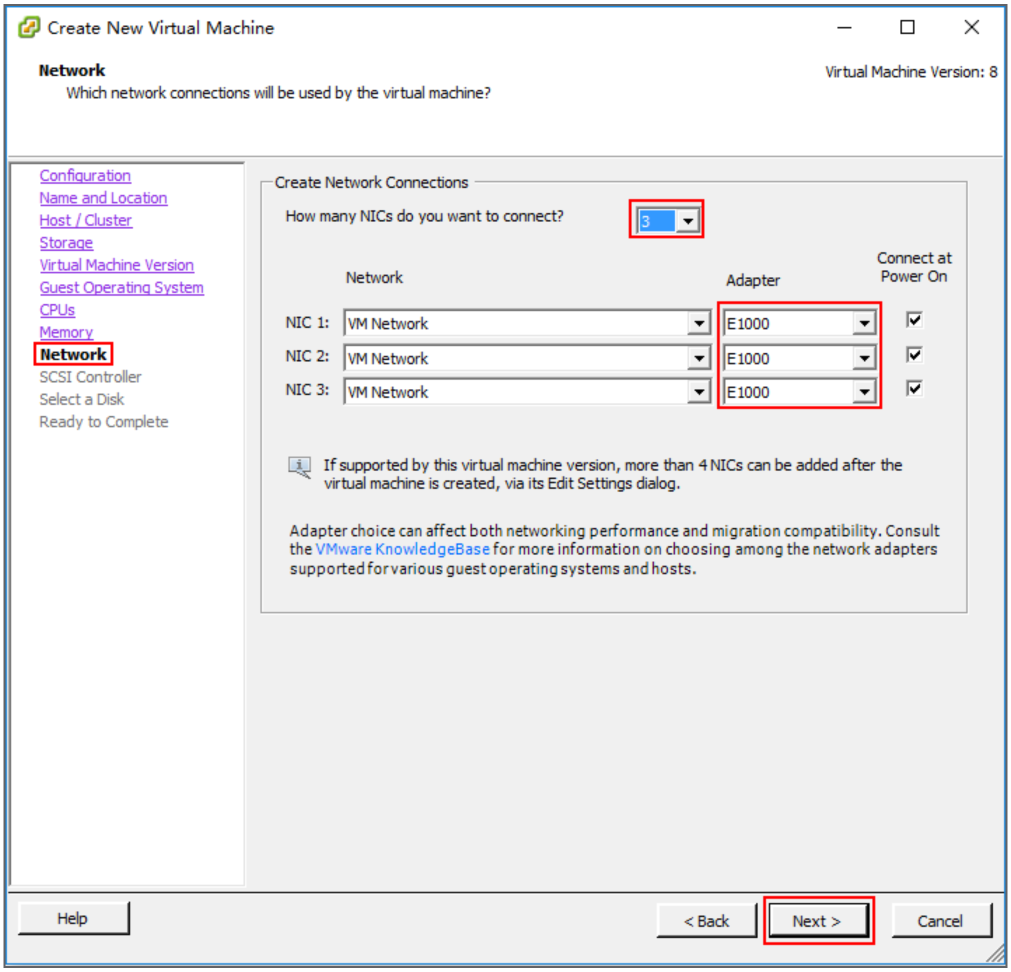
Maximum recommended for this guest OS: 1011 GB.

Maximum recommended for best performance: 32756 MB.

Default recommended for this guest OS: 4 GB.

Minimum recommended for this guest OS: 512 MB.

11. Under the **Network** tab, select at least 3 NICs, including management interface, data ingress and data egress. All NIC types should be E1000 or VMNET3. Click **Next**.



Create New Virtual Machine

Network

Which network connections will be used by the virtual machine?

Virtual Machine Version: 8

Create Network Connections

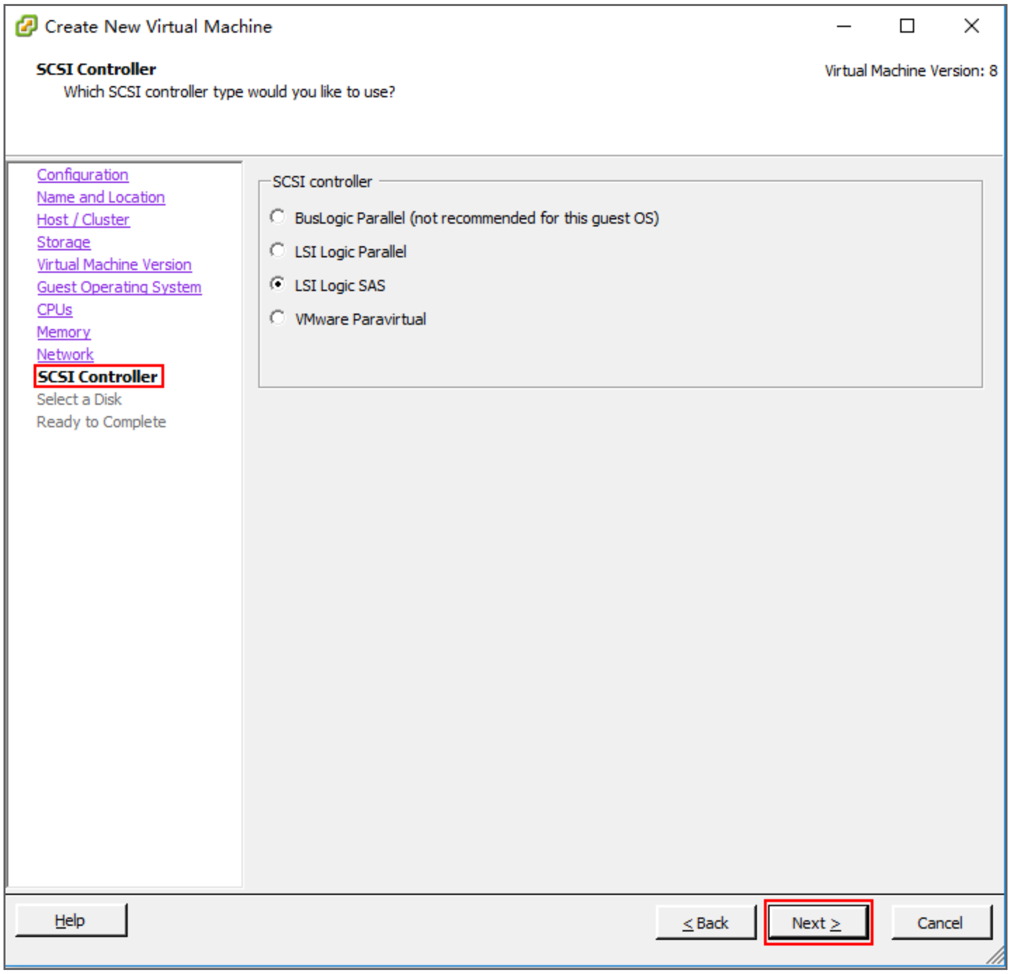
How many NICs do you want to connect? 3

	Network	Adapter	Connect at Power On
NIC 1:	VM Network	E1000	☑
NIC 2:	VM Network	E1000	☑
NIC 3:	VM Network	E1000	☑

If supported by this virtual machine version, more than 4 NICs can be added after the virtual machine is created, via its Edit Settings dialog.

Adapter choice can affect both networking performance and migration compatibility. Consult the VMware KnowledgeBase for more information on choosing among the network adapters supported for various guest operating systems and hosts.

12. Under the **SCSI Controller** tab, keep the default value, and click **Next**.



Create New Virtual Machine

SCSI Controller

Which SCSI controller type would you like to use?

Virtual Machine Version: 8

SCSI controller

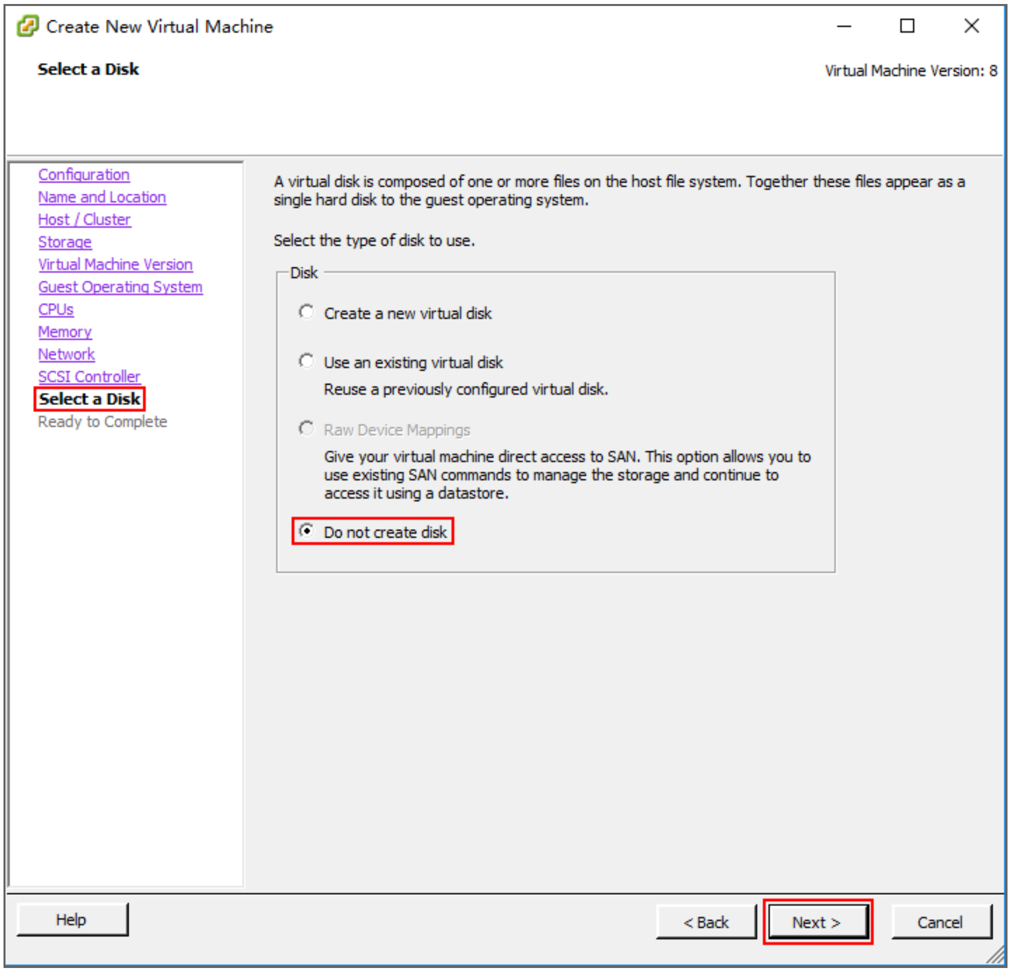
○ BusLogic Parallel (not recommended for this guest OS)

○ LSI Logic Parallel

● LSI Logic SAS

○ VMware Paravirtual

13. Under the **Select a Disk** tab, select **Do not create disk** , and click **Next**.



Create New Virtual Machine

Select a Disk

Virtual Machine Version: 8

A virtual disk is composed of one or more files on the host file system. Together these files appear as a single hard disk to the guest operating system.

Select the type of disk to use.

Disk

○ Create a new virtual disk

○ Use an existing virtual disk
Reuse a previously configured virtual disk.

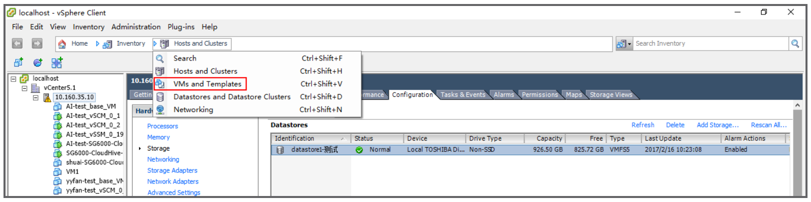
○ Raw Device Mappings
Give your virtual machine direct access to SAN. This option allows you to use existing SAN commands to manage the storage and continue to access it using a datastore.

● Do not create disk

14. Click **Finish** to complete.

Step 3: Selecting the CloudEdge VMDK File for VM

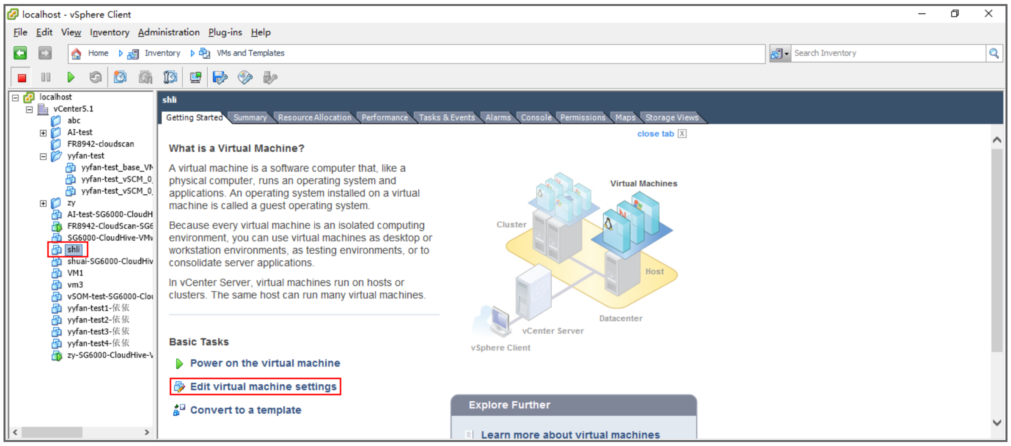
1. In the vSphere Client main interface, select **Home > Inventory > VMs and Templates** to enter the VMs and Templates page.



Datastores

Identification	Status	Device	Drive Type	Capacity	Free	Type	Last Update	Alarm Actions
datastore1-测试	Normal	Local TOSHIBA Di...	Non-SSD	926.50 GB	825.72 GB	VMFS5	2017/2/16 10:23:08	Enabled

2. In the VMs and Templates page, click the CloudEdge virtual machine created in Step 2, and select **Editing virtual machine settings** appears in the right pane. The **Virtual Machine Properties** dialog pops up.



What is a Virtual Machine?

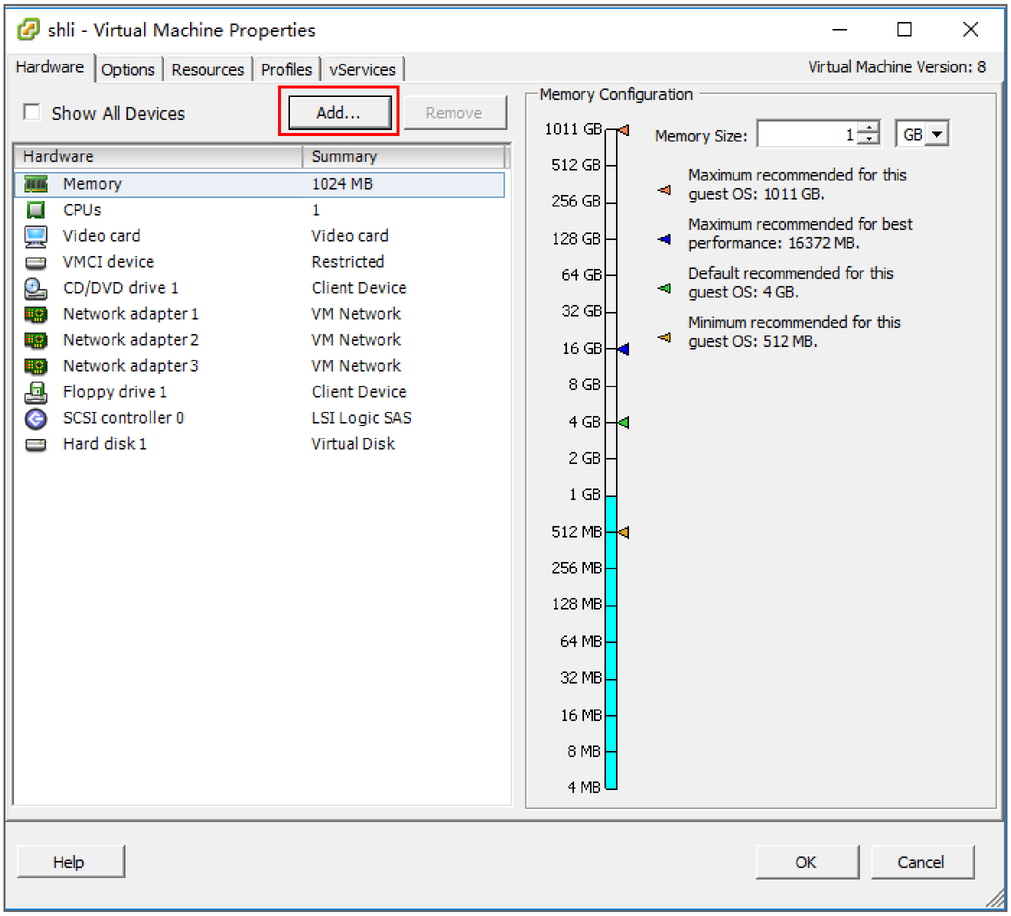
A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.

Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.

In vCenter Server, virtual machines run on hosts or clusters. The same host can run many virtual machines.

Basic Tasks

3. In the **Virtual Machine Properties** dialog, click **Add** to enter the Add Hardware wizard.



□ Show All Devices

Hardware	Summary
Memory	1024 MB
CPUs	1
Video card	Video card
VMCI device	Restricted
CD/DVD drive 1	Client Device
Network adapter 1	VM Network
Network adapter 2	VM Network
Network adapter 3	VM Network
Floppy drive 1	Client Device
SCSI controller 0	LSI Logic SAS
Hard disk 1	Virtual Disk

Memory Size: 1 GB

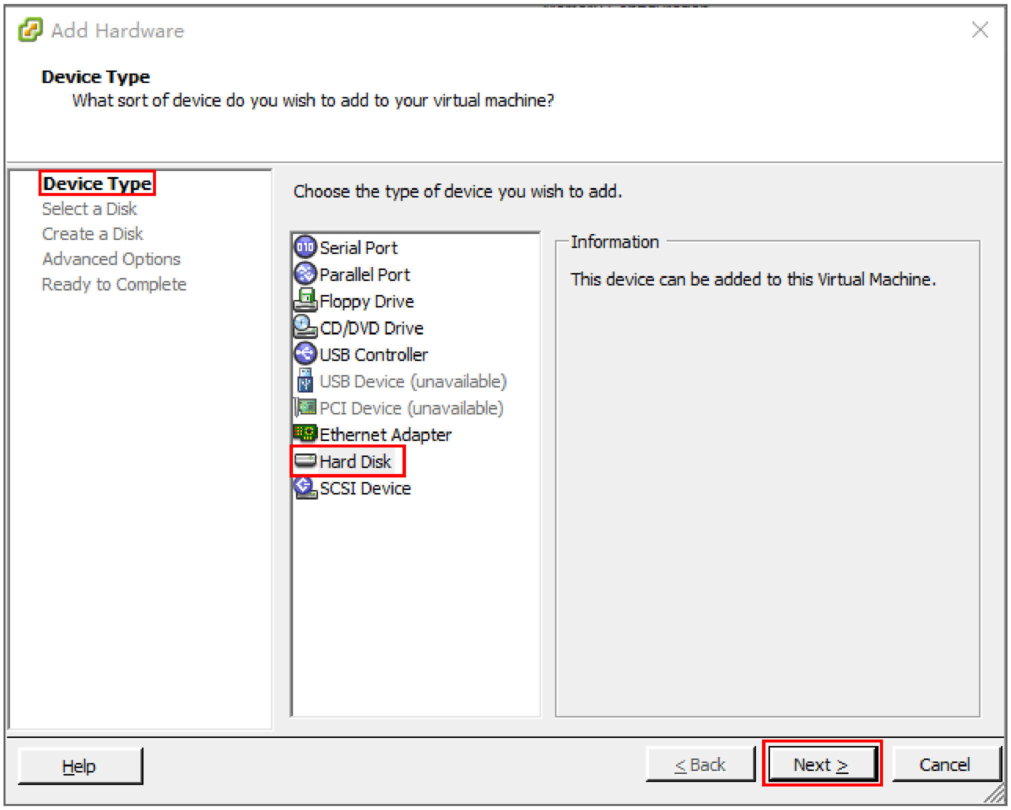
Maximum recommended for this guest OS: 1011 GB.

Maximum recommended for best performance: 16372 MB.

Default recommended for this guest OS: 4 GB.

Minimum recommended for this guest OS: 512 MB.

4. In the **Add Hardware** wizard, select **Hard disk** under the **Device Type** tab, and click **Next**.



Add Hardware

Device Type

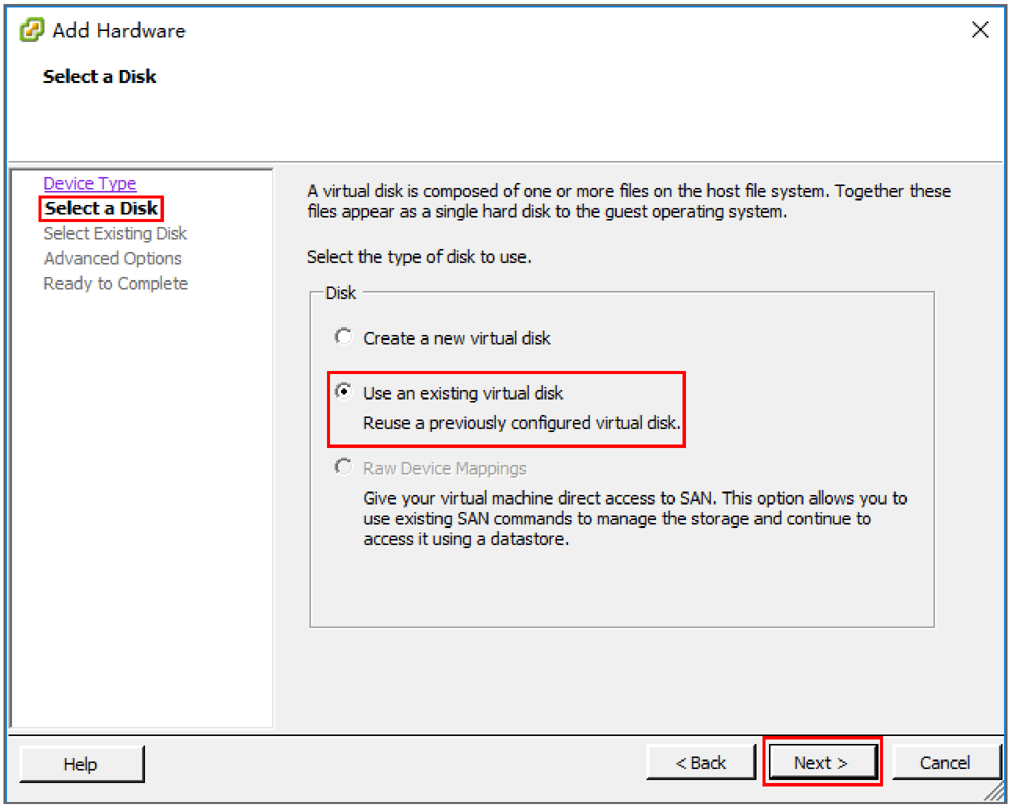
What sort of device do you wish to add to your virtual machine?

Choose the type of device you wish to add.

Information

This device can be added to this Virtual Machine.

5. Under the **Select a Disk** tab, select **Use an existing virtual disk**, and click **Next**.



A virtual disk is composed of one or more files on the host file system. Together these files appear as a single hard disk to the guest operating system.

Select the type of disk to use.

Disk

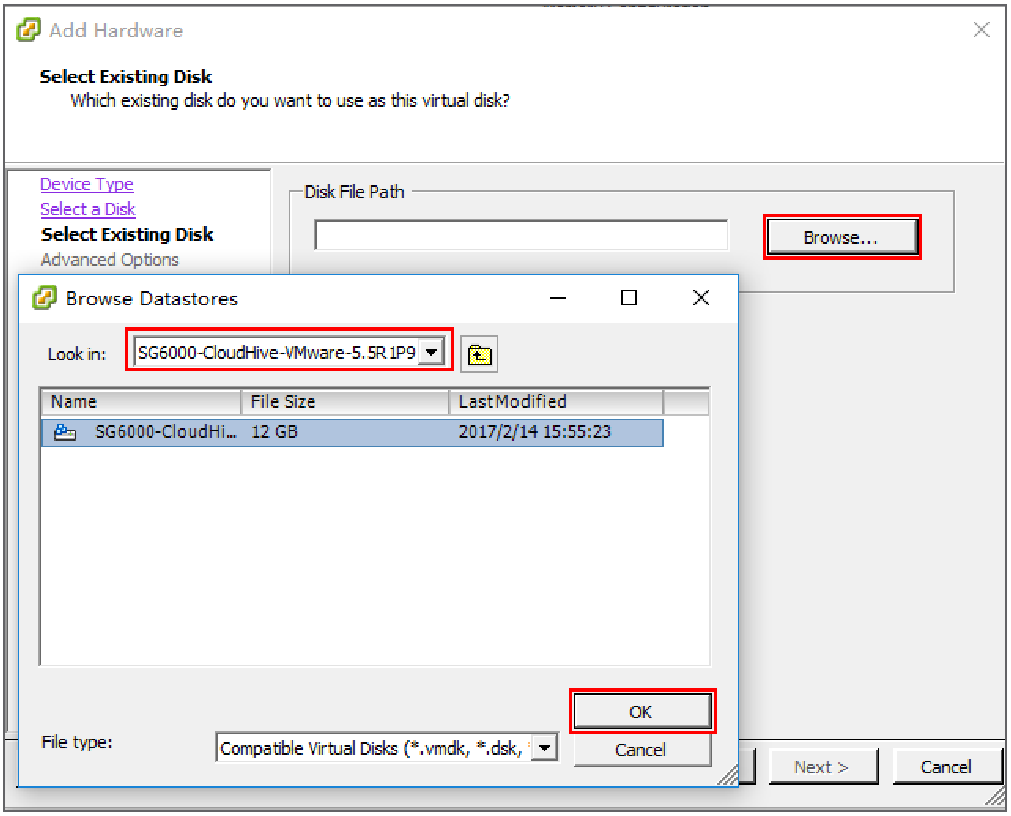
○ Create a new virtual disk

● Use an existing virtual disk
Reuse a previously configured virtual disk.

○ Raw Device Mappings
Give your virtual machine direct access to SAN. This option allows you to use existing SAN commands to manage the storage and continue to access it using a datastore.

6. Under the **Select Existing Disk** tab, click **Browse** and the **Browse Datastores** dialog pops up. In the **Browse Datastores** dialog, select the VMDK file imported in Step 1, and click **OK**.Then

click **Next**.


Add Hardware

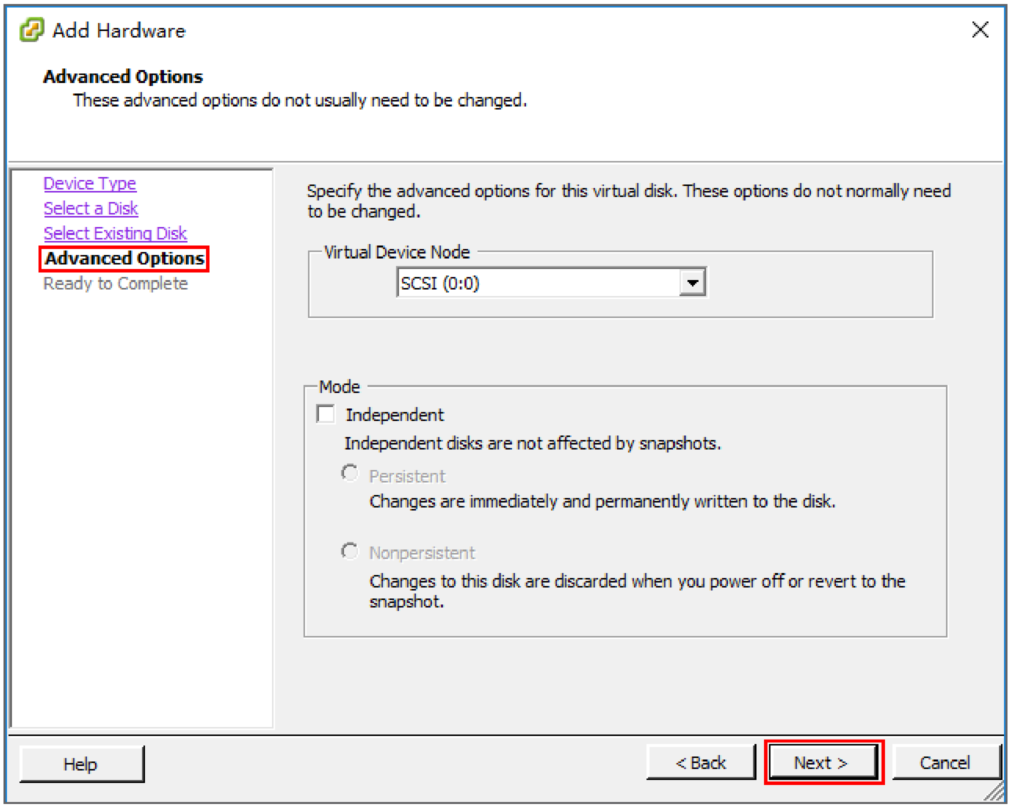
Select Existing Disk
Which existing disk do you want to use as this virtual disk?

Look in: SG6000-CloudHive-VMware-5.5R1P9

Name	File Size	Last Modified
SG6000-CloudHi...	12 GB	2017/2/14 15:55:23

File type: Compatible Virtual Disks (*.vmdk, *.dsk,

7. Under the **Advanced Options** tab, keep the default value, and click **Next**.



Add Hardware

Advanced Options

These advanced options do not usually need to be changed.

Specify the advanced options for this virtual disk. These options do not normally need to be changed.

Virtual Device Node: SCSI (0:0)

Mode

□ Independent

Independent disks are not affected by snapshots.

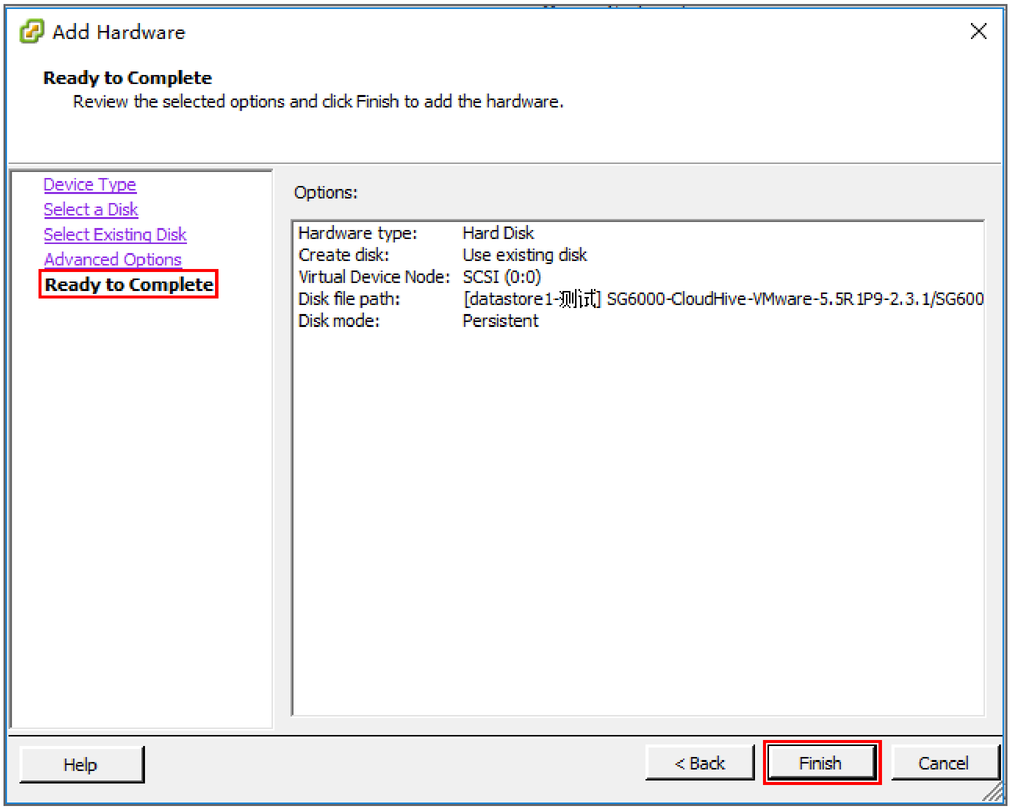
○ Persistent

Changes are immediately and permanently written to the disk.

○ Nonpersistent

Changes to this disk are discarded when you power off or revert to the snapshot.

8. Under the **Ready to Complete** tab, click **Finish** to complete.



Add Hardware

Ready to Complete

Review the selected options and click Finish to add the hardware.

Options:

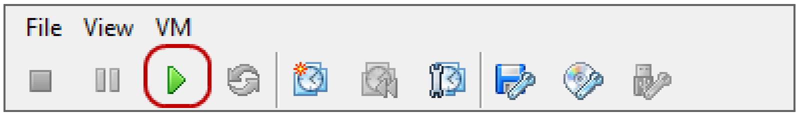
```
Hardware type:        Hard Disk
Create disk:          Use existing disk
Virtual Device Node:  SCSI (0:0)
Disk file path:       [datastore1-测试] SG6000-CloudHive-VMware-5.5R1P9-2.3.1/SG600
Disk mode:            Persistent
```

After the above three steps, you will deploy CloudEdge by importing VMDK successfully.

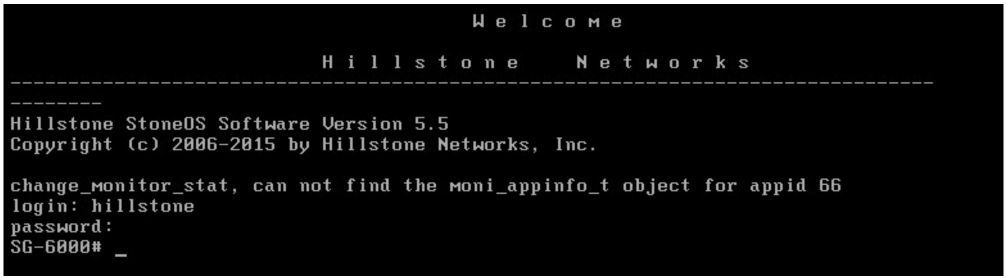
Starting and Visiting vFW

After all the setups above, you can now start your vFW.

1. In vShpere Client, click **Home > Inventory > VMs and Templates**.
2. Right click vFW, and select **Open Console**. In the prompt, you are accessing to vFW's console port.
3. Click the green button to start the vFW virtual machine.



4. Wait for a while, and the system will be up.
5. When the prompt shows the command line interface below, enter default username and password (hillstone/hillstone) to log in StoneOS.



```
                                    Welcome

                              Hillstone    Networks
--------------------------------------------------------------------------------
--------
Hillstone StoneOS Software Version 5.5
Copyright (c) 2006-2015 by Hillstone Networks, Inc.

change_monitor_stat, can not find the moni_appinfo_t object for appid 66
login: hillstone
password:
SG-6000# _
```

Visiting WebUI of StoneOS

After logging in StoneOS, you will be able to manage StoneOS via vSphere Client. However, you need to configure vFW's management interface before you can visit its Web interface.

1. Collect necessary information from your network administrator. You need to have the management interface's IP address, network mask, and gateway IP address.
2. Configure the vFW's management IP address. By default, eth0/0 is the management interface and it is enabled with DHCP. To assign an IP address to eth0/0, you need to disable its DHCP and allocate a static IP address you collected from administrator.
   Use the following command:

```
SG-6000# config
SG-6000(config)# interface ethernet0/0
SG-6000(config)# no ip address dhcp
SG-6000(config-if-eth0/0)# ip address a.b.c.d/netmask
SG-6000(config-if-eth0/0)# manage http | https | telnet | snmp | ssh
SG-6000(config-if-eth0/0)# exit
```

no ip address dhcp	Disable this interface's DHCP.
ip address *a.b.c.d/netmask*	Enter a static IP address for this interface.
manage {http | https | telnet | snmp | ssh | ping}	This command allows access via http, https, telent, snmp, SSH and ping.

3. Add a static route. Use the command below to add a route whose next hop is the gateway.

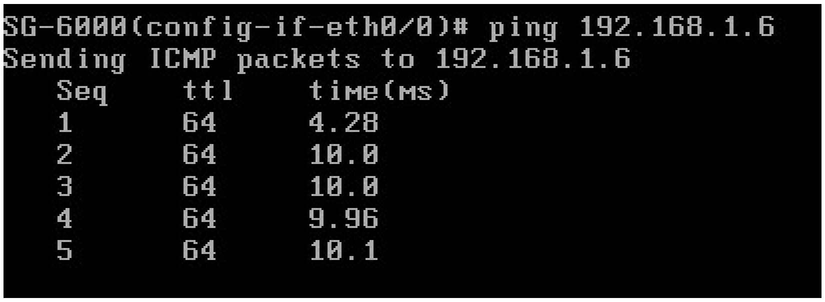
```
SG-6000(config)# ip vrouter trust-vr
SG-6000(config)# ip route a.b.c.d/netmask A.B.C.D
SG-6000(config)#
```

a.b.c.d/netmask	Specify the destination. If you may visit any destination, enter 0.0.0.0/0.
A.B.C.D	Enter the next hop's address. In this case, this is the gateway's IP address.

4. Save the settings.

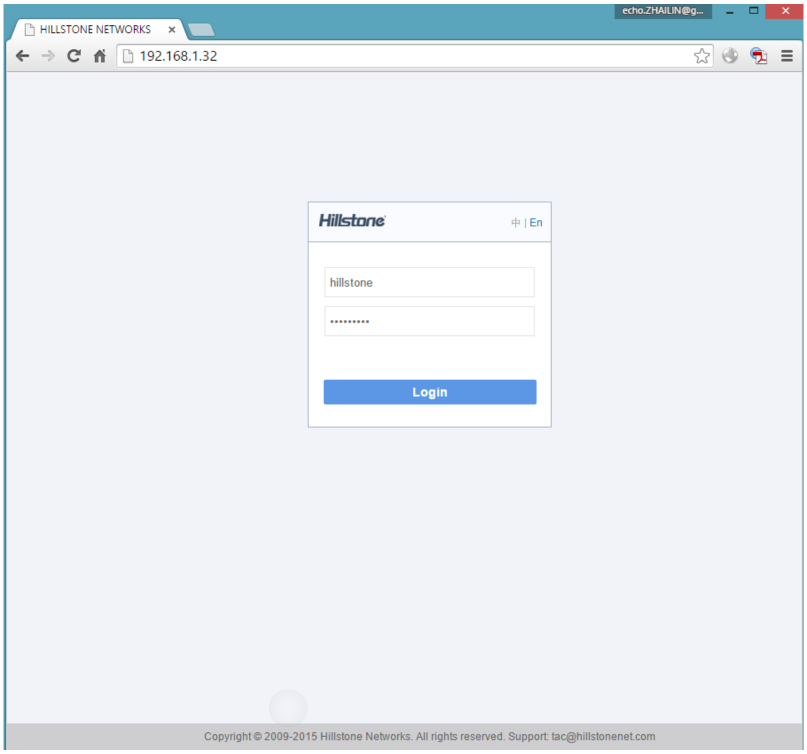
```
SG-6000# save
```

5. Test if the gateway is accessible.



```
SG-6000(config-if-eth0/0)# ping 192.168.1.6
Sending ICMP packets to 192.168.1.6
   Seq     ttl     time(ms)
   1       64      4.28
   2       64      10.0
   3       64      10.0
   4       64      9.96
   5       64      10.1
```

6. Enter eth0/0 IP address in the address bar of your browser. You will see the WebUI login page (make sure you have used **manage http** command to enable http access).


HILLSTONE NETWORKS
echo.ZHAILIN@g...
192.168.1.32
Hillstone
中 | En
hillstone
•••••••••
Login
Copyright © 2009-2015 Hillstone Networks. All rights reserved. Support: tac@hillstonenet.com

Upgrading StoneOS

Since StoneOS 5.5R1P7.1, CloudEdge can be upgraded online. If CloudEdge is deployed by importing ISO file , you can not upgrade the system through the online method. You can just visit StoneOS WebUI on **System > Upgrade Management** page to upgrade the firewall when CloudEdge is deployed by importing OVA file or VMDK file. This upgrade method is recommended. For detailed operations, you may refer to *StoneOS WebUI User Guide*.

Deploying CloudEdge on Xen

CloudEdge is packed in an VHD file, and can be installed on a Citrix XenServer.

Before deploying vFW on Xen platform, you should be already familiar with knowledge about Xen.

System Requirements

vFW has to be installed on a X86-based XenServer host. The XenServer host should meet the following requirements:

- Support Intel VT or AMD-V
- Be able to allocate at least two virtual network cards and the speed can be up to 100MB/s
- 64 bit CPU and the frequency can be up to 1.5GHz
- 2G memory is recommended
- 16G hard disk or above, whose type can be SATA, SCSI and PATA

Installing vFW

Before installation of vFW, you have to complete the configuration of the XenServer host and the XenCenter client.

Step 1: Acquiring vFW software package

Contact salesperson to get the address of downloading vFW software package, and save the VHD image into your local host.

Step 2: Importing the VHD file

Using the Import wizard, you can import a disk image into a resource pool or into a specific host as a VM.

1. Double-click the XenCenter client, and then click the **Add new server** button on toolbar, enter a XenServer IP address or name in the pop-up dialog box, and then enter the user name and password, click **Add**.

2. on the **File** menu, select **Import**, the Import wizard dialog box appears.

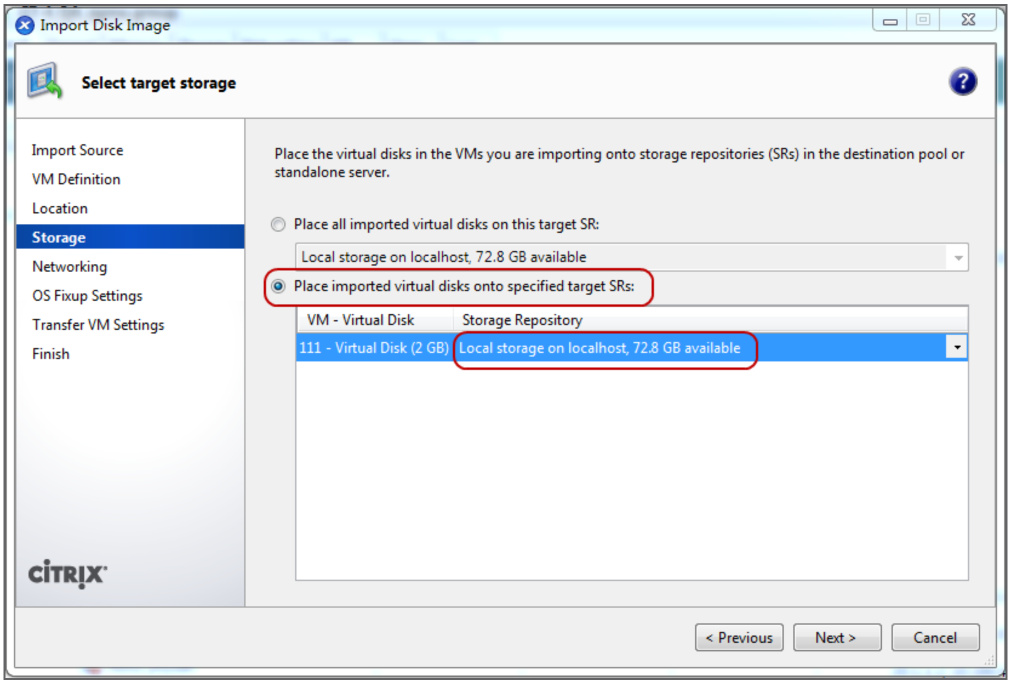
3. On the first page of the wizard, locate the disk image file you want to import, click **Next** to continue.

4. Specify the VM name and allocate CPU and memory resources, click **Next** to continue.

5. Specify where to place the new VM and choose a home server(optionally) , click **Next** to continue.

6. Configure storage for the new VM , click **Next** to continue.

   On the **Storage** page, select a storage repository (SR) where the imported virtual disk will be placed.



Import Disk Image

Select target storage

Place the virtual disks in the VMs you are importing onto storage repositories (SRs) in the destination pool or standalone server.

○ Place all imported virtual disks on this target SR:

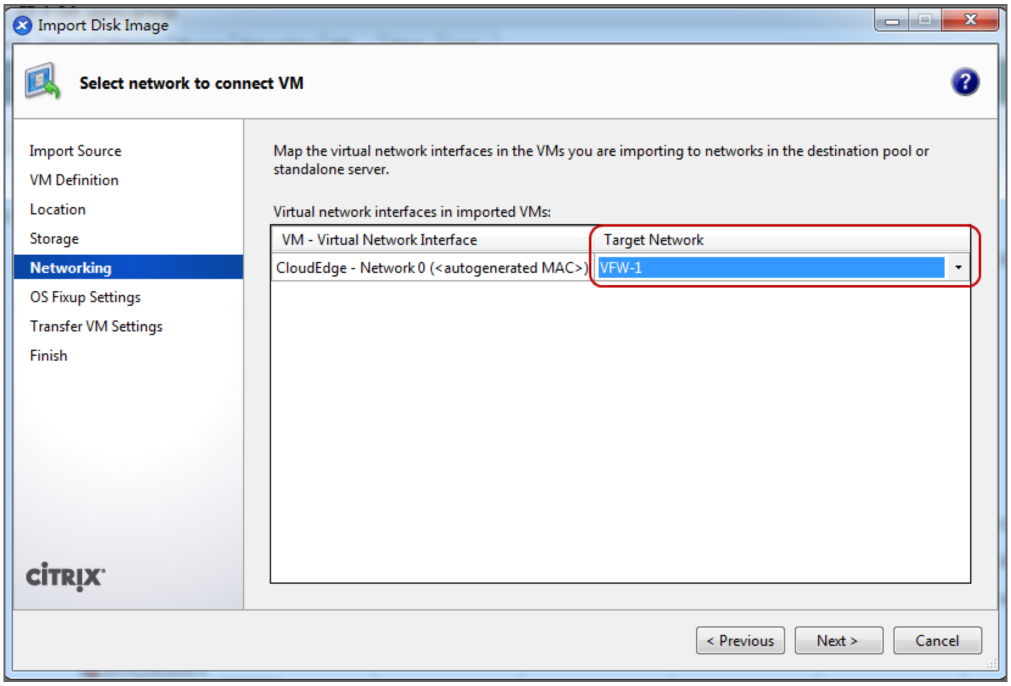
Local storage on localhost, 72.8 GB available

● Place imported virtual disks onto specified target SRs:

VM - Virtual Disk	Storage Repository
111 - Virtual Disk (2 GB)	Local storage on localhost, 72.8 GB available

7. Configure networking for the new VM, click **Next** to continue.

   On the **Networking** page, select a target external network which can visit the Internet in the destination pool/standalone server for the new VM's virtual network interface.



Map the virtual network interfaces in the VMs you are importing to networks in the destination pool or standalone server.

Virtual network interfaces in imported VMs:

VM - Virtual Network Interface	Target Network
CloudEdge - Network 0 (<autogenerated MAC>)	VFW-1

8. Select **Don't use Operating System Fixup** check box, click **Next** to continue.

9. Configure Transfer VM(temporary VM) networking, click **Next** to continue.

   - To use automated Dynamic Host Configuration Protocol (DHCP) to automatically assign networking settings including the IP address, subnet mask and gateway, select **Automatically obtain network settings using DHCP**.

   - If there is no DHCP service deployed on your network, select **Use these network settings** to configure them manually. Make sure the Transfer VM is in the same network segment as XenCenter client.

10. On the **Finish** page, review all the import settings and then click **Finish** to begin the import process and close the wizard.

Step 3: Initial login of vFW

To access vFW initially:

1. In the left Resources pane, select the virtual machine which vFW is located in, right click it and select **Start** .

   Waiting for a while, the virtual machine will start successfully.

2. Aftr login prompt, press the Enter key and enter username and password "hillstone"/"hillstone".

   login: hillstone

   password: hillstone

3. From now on, you can use command line interface to manage vFW. It is recommended to change your password at earliest convenience.

Visiting vFW's WebUI

The first interface of vFW, eth0/0, is enabled with DHCP by default. If vFW is connected to a network with DHCP server, eth0/0 will get an IP address automatically. You can open vFW's WebUI interface by visiting eth0/0's address in a browser.

To visit vFW's WebUI:

1. Visit vFW refering to "Deploying CloudEdge on Xen" on Page 76

2. To view IP address of eth0/0, use the command:

   show interface ethernet0/0

3. Open a browser (Chrome is recommended), enter eth0/0's IP address in the address bar.

4. Enter login name and password (hillstone/hillstone).

5. Click **Login**, and you will enter StoneOS's WebUI manager.

6. About how to use StoneOS, refer to StoneOS related documents (click here).

Upgrading vFW

Since StoneOS 5.5R1P7.1, CloudEdge can be upgraded online with .img format file. You can visit StoneOS WebUI on **System > Upgrade Management** page to upgrade the firewall. For detailed operations, you may refer to *StoneOS WebUI User Guide*.

Deploying CloudEdge on Hyper-V

Hyper-V is a Microsoft virtualization product based on hypervisor. To deploy CloudEdge in Microsoft Azure, CloudEdge should be deployed in Hyper-V at first.

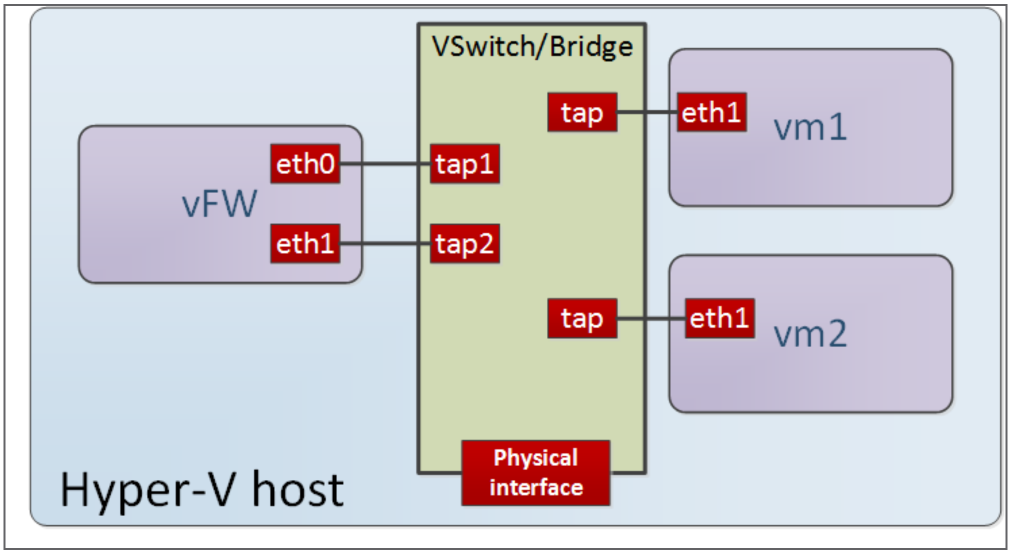
System Requirements

To deploy vFW on Hyper-V, the host should meet the following requirements:

- Support Intel VT or AMD-V
- 64 bit CPU which can provide two virtual cores
- Data execution protection (DEP) function of the hardware must be enabled for CPU
- Be able to allocate at least two virtual network cards
- Windows Server 2012R2 system
- 2G memory at least

How vFW Works on Hyper-V Host

vFW on a Hyper-V host usually works as gateway for virtual machines. In order to be able to forward data from/to the internal virtual machines, you need to connect the vFW tap interface to the Virtual Switch of Hyper-V host, and the internal virtual machines define vFW as their gateway.



Preparation

Before installing vFW, make sure you have a host running a Windows Server system (Windows Server 2012R2 is recommended) and Hyper-V function is added.

Installing vFW on Hyper-V Host

To install vFW on a Hyper-V host, use the following steps:

Step 1: Acquiring vFW software package

Contact salesperson to get the address of downloading vFW software package, and save the VHD image into your Hyper-V host.

Step 2: Creating a Virtual Machine

1. Open Hyper-V Manager, click **Operation** > **New** > **Virtual Machine** in menu bar, the New Virtual Machine Wizard dialog box will prompt.

2. In the dialog box, click **Next** to create an user-defined virtual machine.

3. Specify the name and storage location of virtual machine, click **Next**.

4. Configure the memory in the Allocate Memory page, click **Next**.

5. On the right **Operation** panel of the Hyper-V manager home page, select **Virtual Switch Manager** to create a virtual network card.

6. Select **External** type, and then click **Create Virtual Switch** button.

7. Configure switch name in **Virtual Switch Attribute** area, and select **External Network** in **Connection Type** area, then click **OK**.

8. In the **Configure Network** page of New Virtual Machine Wizard, select the virtual switch that was created just now in the drop-down menu, then click **Next**.

9. Select **Use the existing virtual hard disk**, browse the local PC, select the VHD file in step 1.

10. Click **Finish** button in **Summary** page.

11. If the virtual firewall you installed requries two vCPUs, right click the new created virtual machine in the virtual machine list and then select **Settings**, click the **CPU** node to set the vCPU value to 2.

Step 3: Initial login of vFW

To access vFW initially:

1. Right click the new created virtual machine in the virtual machine list and then select **Connect**, click the ⏻ button in the toolbar of the dialog box.

   Waiting for a while, the virtual machine will start successfully.

2. Aftr login prompt, press the Enter key and enter username and password "hillstone"/"hillstone".
   login: hillstone
   password: hillstone

3. From now on, you can use command line interface to manage vFW. It is recommended to change your password at earliest convenience.

Visiting vFW's WebUI

The first interface of vFW, eth0/0, is enabled with DHCP by default. If vFW is connected to a network with DHCP server, eth0/0 will get an IP address automatically. You can open vFW's WebUI interface by visiting eth0/0's address in a browser.

To visit vFW's WebUI:

1. Visit vFW refering to "Deploying CloudEdge on Hyper-V" on Page 81
2. To view IP address of eth0/0, use the command:

   show interface ethernet0/0
3. Open a browser (Chrome is recommended), enter eth0/0's IP address in the address bar.
4. Enter login name and password (hillstone/hillstone).
5. Click **Login**, and you will enter StoneOS's WebUI manager.
6. About how to use StoneOS, refer to StoneOS related documents (click here).

Upgrading vFW

Since StoneOS 5.5R1P7.1, CloudEdge can be upgraded online. You can visit StoneOS WebUI on **System > Upgrade Management** page to upgrade the firewall. For detailed operations, you may refer to *StoneOS WebUI User Guide*.

Deploying CloudEdge on AWS

Overview

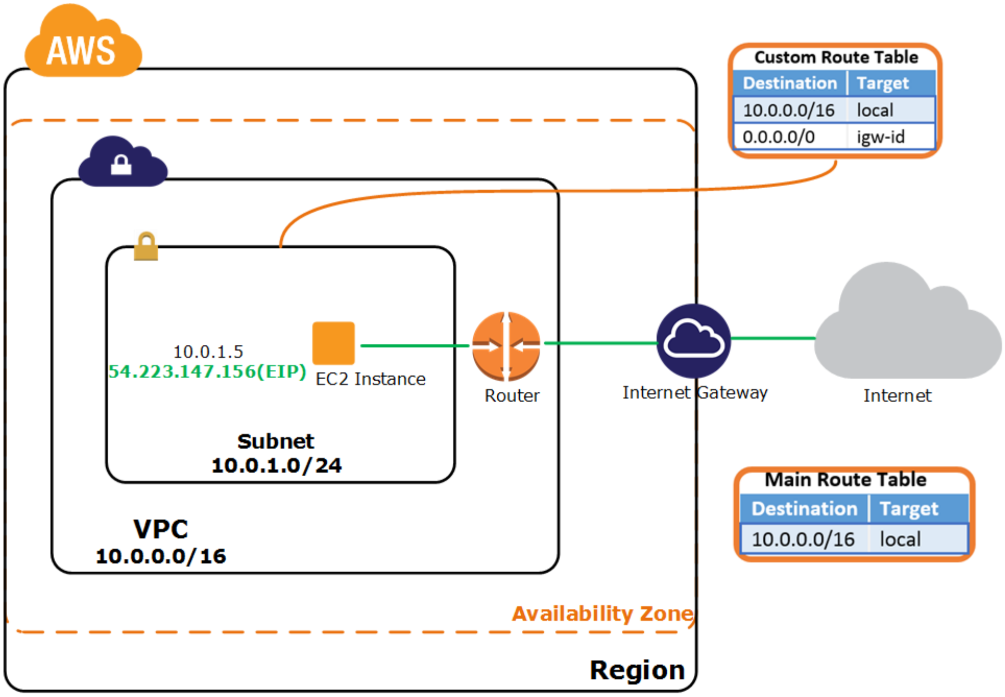
This chapter introduces how to install CloudEdge virtual firewall (abbr. vFW) on Amazon Web Service.

Introduction to AWS

Amazon Web Services (AWS) is a cloud computing platform to provide remote web services.

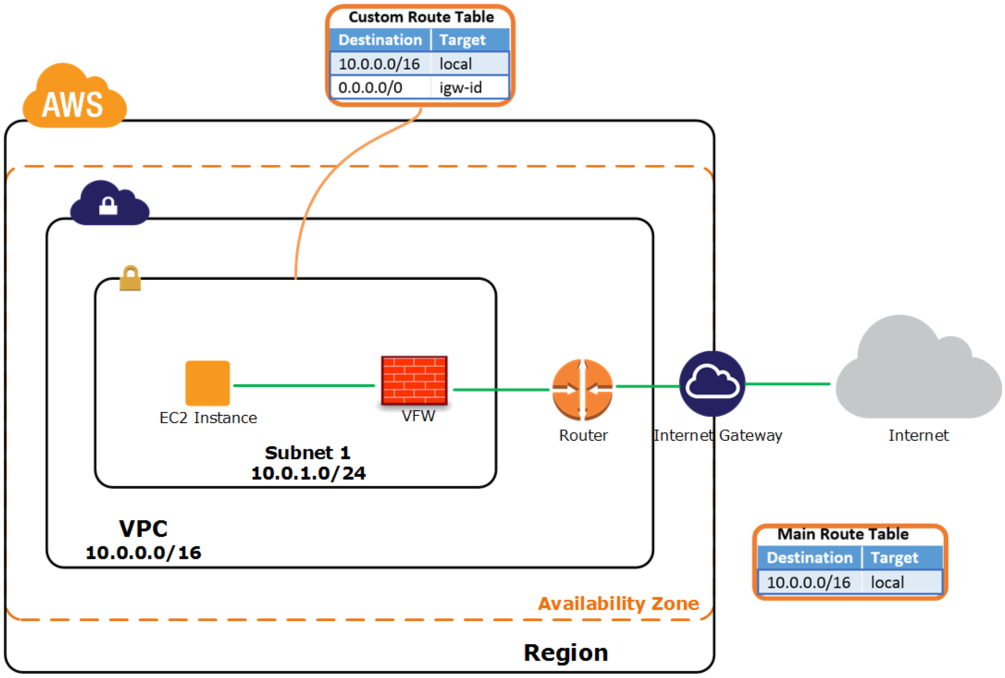
Among all the AWS components, VPC and EC2 are used in deploying vFW.

- Virtual Private Cloud (VPC) is a logical virtual network. VPC users can has its own private IP ranges and subnets, with routing tables and gateways.
- Elastic Compute Cloud (EC2) provides cloud hosting service. EC2 can be used as virtual machine services. When EC2 is connected through VPC, it can provide strong networking capabilities for computing resources.



CloudEdge on AWS

CloudEdge is virtual firewall product. vFW is installed as an EC2 instance to provide firewall function to virtual services in VPC subnets.



Custom Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-id

Main Route Table

Destination	Target
10.0.0.0/16	local

Typical Scenarios

VPC Gateway

A VPC provides network virtualization similar to a traditional physical network in topology and function. CloudEdge is deployed at the service entrance as the VPC gateway to protect your EC2 instances by inspecting all traffic to identify users, applications, content, and to set granular access control policy, block known and unknown threats, as well as to guard against abnormal behavior. In a dynamic AWS deployment solution – when EC2 instances are added or changed to accommodate workload – CloudEdge is rapidly and automatically updated with new security policies and IP addresses.

Corporate VPN

VPN capability is a common requirement in the traditional enterprise network. When enterprise business migrates to AWS, users access cloud data and manage EC2 instances through an encrypted VPN tunnel. CloudEdge offers multiple VPN modes, such as IPSec VPN and SCVPN, to satisfy different requirements. In the hybrid-cloud mode, standards-based site-to-site VPN connections are established between the corporate local network, branches and your AWS virtual service – the virtual firewall applies access control based on application, user, and content to guarantee valid and continuous access to users on remote links.

Server Load Balancing

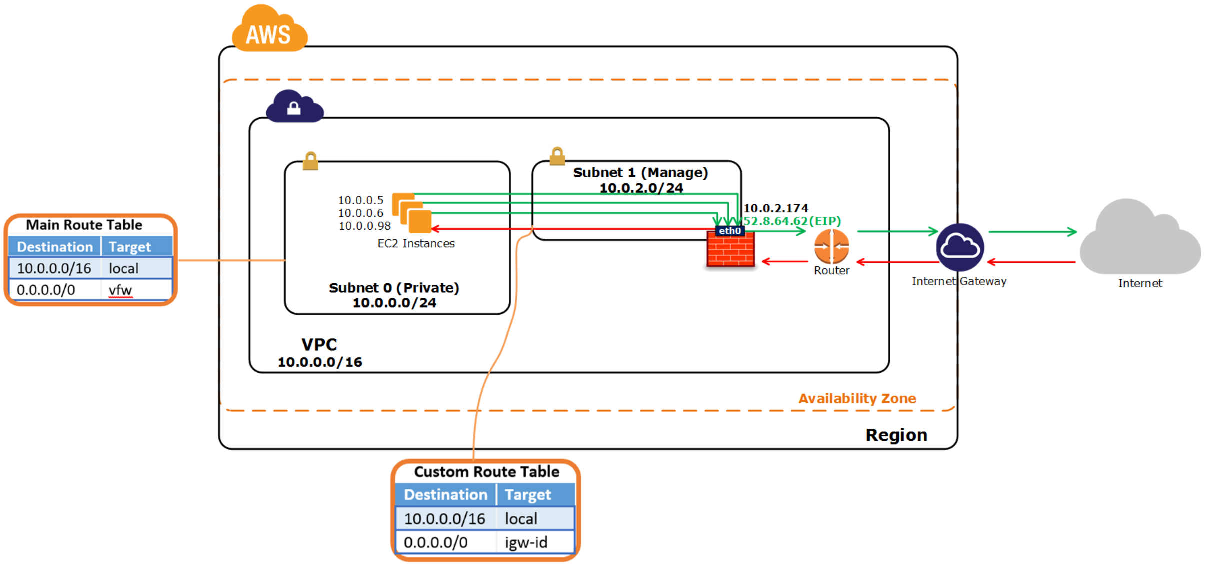
CloudEdge provides DNAT-based server load balancing (SLB), helping enterprises establish an EC2 cluster on AWS − traffic can be assigned equally to different EC2 instances, all providing the same service. When an EC2 instance reaches its workload threshold, CloudEdge forwards the connection request to another instance to avoid discarding the request. Multiple SLB algorithms are supported, including weighted hashing, weighted least-connection and weighted round-robin. The advantage of integrating SLB with the firewall is that the firewall can inspect and analyze all inbound traffic. In the VPC, this means thatCloudEdge can block attack threats hidden in traffic to protect all of your EC2 instances.

Topology of CloudEdge on AWS for This Guide

This guide uses a scenario that CloudEdge virtual firewall (vFW) works as Internet gateway for instances in a VPC. To better understand vFW, every step and screen shot in vFW deployment on AWS is based on this topology. The subnet name, IP address, interfaces in this topology are the actual lab setups we used while we are writing this guide. This topology is only for reference. In your real configurations, you need to change the subnet, interface or IP address to meet your requirements.

In this design, AWS VPC contains two subnets. Subnet 0 is for private internal servers; Subnet 1 connects the interface eth0 of vFW. vFW is deployed as a gateway of VPC and it controls in-and-out traffic of Subnet 0.

Also, eth0 is connected to VPC Internet gateway. If it is configured with DNAT rule, Internet users will be able to visit private servers in Subnet 0. If it is configured with SNAT rule, the private servers will be able to access to Internet.



Main Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	vfw

Custom Route Table

Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-id

- **VPC**: 10.0.0.0/16.
- **Subnet 0 (Manage)**: 10.0.0.0/24. Subnet 0 is the subnet which contains private servers (as EC2 instances). We can simply take Subnet 0 as the internal network of an enterprise in which Web servers, FTP server and mail servers are placed.

- **Subnet 1 (Public)**: 10.0.2.0/24. Subnet 1 represents VPC subnet where vFW will be deployed. Subnet 1 is the subnet of vFW's management interface eth0/0.

Preparing Your VPC

You must have an AWS account in order to use AWS services. To apply or log in, go to AWS website (click here). More information about VPC, please refer to AWS VPC documentation (click here).

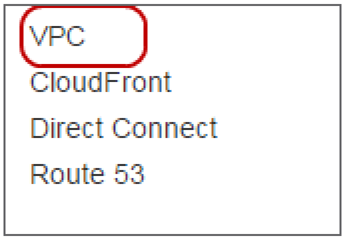
In this guide, we presume that our readers have built a VPC network, and the default subnet, Subnet 0, is named for Manage. The Manage subnet has a default route whose next hop is directed to Internet gateway (IGW). In this chapter, we will introduce to you how to set up a subnet. In the later steps, we will put the firewall's eth0 into this subnet.

After setups in this chapter, you will get the following VPC and its subnets:

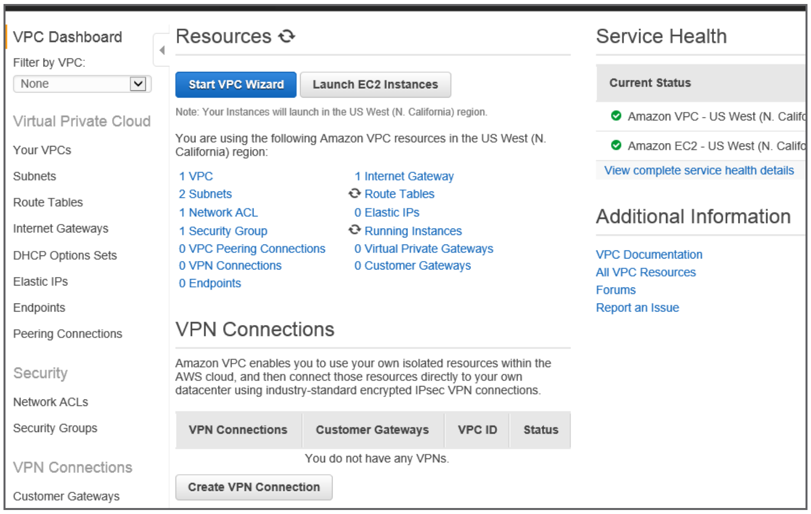
- VPC: 10.0.0.0/16
- Subnet 0 (Manage): 10.0.0.0/24
- Subnet 2 (Public): 10.0.2.0/24

Step 1: Log in Your AWS Account

1. Log in AWS console (click here) with your AWS account.
2. Under the AWS console home, click **VPC**.



3. Enter the VPC dashboard.



Note: Your Instances will launch in the US West (N. California) region.

You are using the following Amazon VPC resources in the US West (N. California) region:

1 VPC	1 Internet Gateway
2 Subnets	Route Tables
1 Network ACL	0 Elastic IPs
1 Security Group	Running Instances
0 VPC Peering Connections	0 Virtual Private Gateways
0 VPN Connections	0 Customer Gateways
0 Endpoints	

Amazon VPC - US West (N. Califo

Amazon EC2 - US West (N. Califo

View complete service health details

Amazon VPC enables you to use your own isolated resources within the AWS cloud, and then connect those resources directly to your own datacenter using industry-standard encrypted IPsec VPN connections.

VPN Connections	Customer Gateways	VPC ID	Status

You do not have any VPNs.

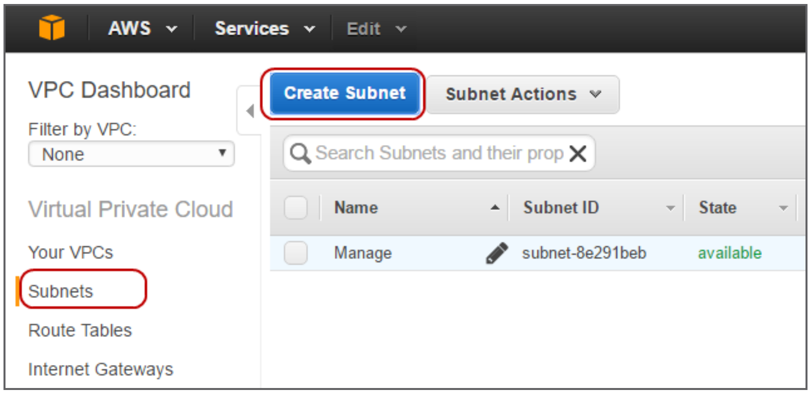
Step 2: Adding Subnets into VPC

In this guide's design, eth0/0 is the management interface for managing CloudEdge system, and also is the business interface to process flow-in traffic. Later, we will use a test EC2 instance to check if the CloudEdge firewall can function.

Subnet 0 (Manage) is already created in the step above. Next, in this step, we will introduce how to create a new subnet.

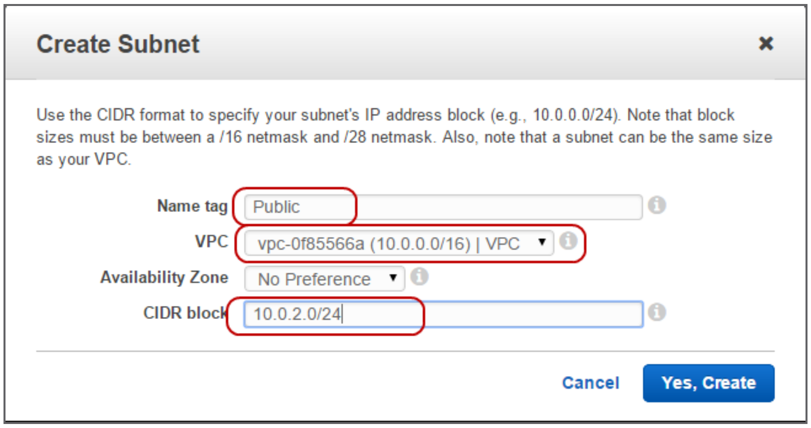
Use the configuration steps below to add a new subnet:

1. In VPC Dashboard, click **Subnets**, and then click **Create Subnet**.



Name	Subnet ID	State
Manage	subnet-8e291beb	available

2. Enter the name "Public", and select your VPC from VPC drop-down menu. In the CIDR block text-box, enter its subnet address "10.0.2.0/24".



Create Subnet

Use the CIDR format to specify your subnet's IP address block (e.g., 10.0.0.0/24). Note that block sizes must be between a /16 netmask and /28 netmask. Also, note that a subnet can be the same size as your VPC.

Name tag: Public

VPC: vpc-0f85566a (10.0.0.0/16) | VPC

Availability Zone: No Preference

CIDR block: 10.0.2.0/24

3. Click **Yes, Create**.

Step 3: Modifying Route Tables

AWS VPC has implicit router. We assume that a main route table with a default route entry whose next hop is Internet gateway has been configured in the router. After the subnet is created, its route table only has a route entry whose next hop is local. In this user guide design (refer to "Topology of CloudEdge on AWS for This Guide" on Page 89), we will make sure that Subnet 1 (Public) is connected to the main route table (whose next hop is Internet gateway) , so that Subnet 1 (Public) can be accessed by the Internet.

In order to modify route tables:

1. In VPC Dashboard, click **Subnets** and select the new created subnet.
2. Click the <Route Table> tab below, and then click **Edit**.
3. Select correct route table from the <change to> drop-down menu to associate Subnet 1 (Public) to main route table.
4. Click **Save** to save the above configurations.

Installing CloudEdge on AWS

CloudEdge is installed in AWS as an EC2 instance.

This section introduces how to install CloudEdge in AWS. After you finish configurations in this section, you will:

- have a running StoneOS system
- see that interface eth0 has acquired private IP addresses and elastic IP addresses (public)
- be able to visit the CLI and WebUI of StoneOS

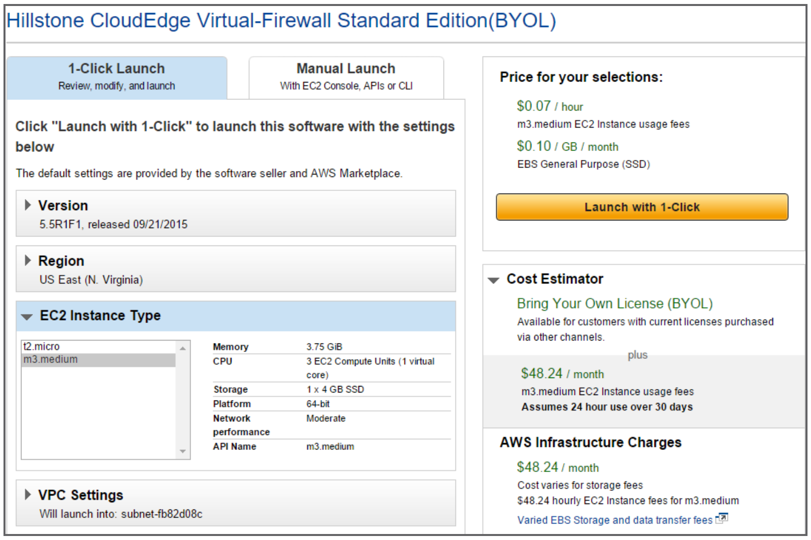
CloudEdge image can be purchased from AWS Marketplace. CloudEdge image includes the following two types: pay-on-demand and BYOL(Bring Your Own License). If you want to know how to select VM models, refer to "Overview" on Page 1. CloudEdge for AWS may be launched either from the AWS Marketplace ‘1-Click Launch’ or directly from the EC2 Console. This guide will introduce both methods step by step.

1-Click Launching CloudEdge

Using 1-Click launching, you will get an instance set up ready for you just with 1 click.

1. Go to the AWS Marketplace and login with your credentials. Hillstone CloudEdge can be found by being searched by the key word "Hillstone".
2. You may select "Standard Edition" or "Advanced Edition" depending on you selection of platform model .
3. After opening the product, click **Continue**.

4. Configure the settings under **1-Click Launch**: Select CloudEdge system version, your intended region to use this instance, and instance type for this instance.



Hillstone CloudEdge Virtual-Firewall Standard Edition(BYOL)

Click "Launch with 1-Click" to launch this software with the settings below

The default settings are provided by the software seller and AWS Marketplace.

Version
5.5R1F1, released 09/21/2015

Region
US East (N. Virginia)

EC2 Instance Type

t2.micro
m3.medium

Memory	3.75 GiB
CPU	3 EC2 Compute Units (1 virtual core)
Storage	1 x 4 GB SSD
Platform	64-bit
Network performance	Moderate
API Name	m3.medium

VPC Settings
Will launch into: subnet-fb82d08c

Price for your selections:

$0.07 / hour
m3.medium EC2 Instance usage fees

$0.10 / GB / month
EBS General Purpose (SSD)

Cost Estimator

Bring Your Own License (BYOL)
Available for customers with current licenses purchased via other channels.

plus

$48.24 / month
m3.medium EC2 Instance usage fees
Assumes 24 hour use over 30 days

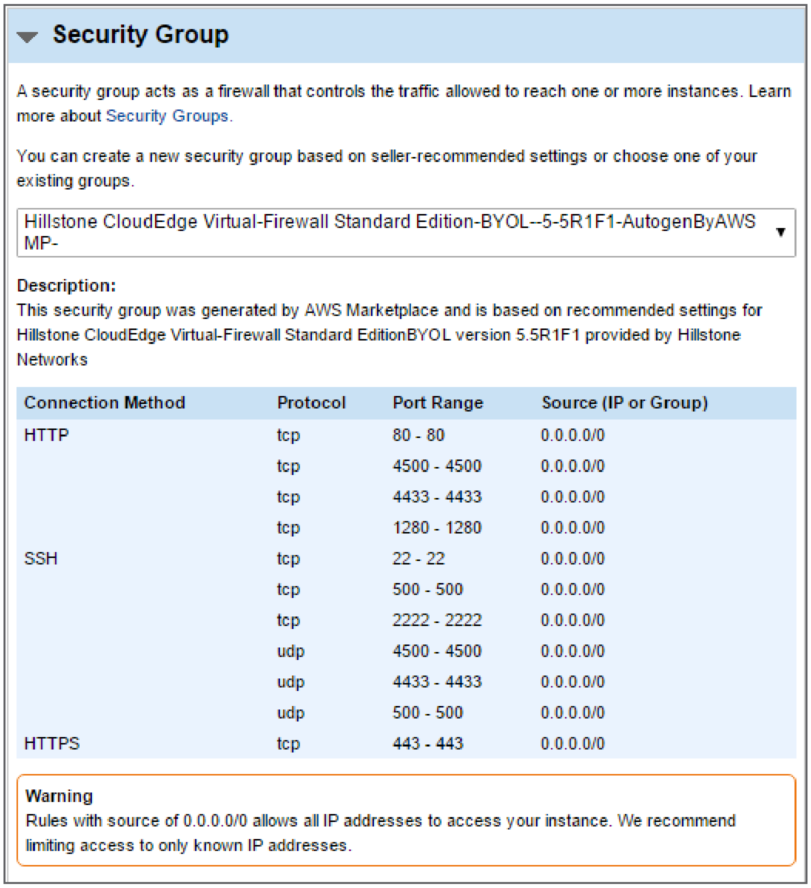
AWS Infrastructure Charges

$48.24 / month
Cost varies for storage fees
$48.24 hourly EC2 Instance fees for m3.medium
Varied EBS Storage and data transfer fees

5. Please be noted that you should have already built a VPC for CloudEdge. Select the VPC and subnet. More subnets can also be added later in management console.

6. For **Security Group**, we recommend you select the existing group with "Hillstone CloudEdge" name on it. The Hillstone security group opens ports to allow all potential communication. Please do not select a security group that does not allow SSH, HTTP or HTTPS connection, which will

incur disconnection.



Security Group

A security group acts as a firewall that controls the traffic allowed to reach one or more instances. Learn more about Security Groups.

You can create a new security group based on seller-recommended settings or choose one of your existing groups.

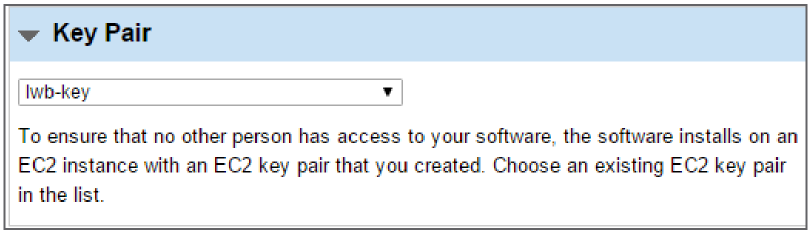
Hillstone CloudEdge Virtual-Firewall Standard Edition-BYOL--5-5R1F1-AutogenByAWSMP- ▼

Description:
This security group was generated by AWS Marketplace and is based on recommended settings for Hillstone CloudEdge Virtual-Firewall Standard EditionBYOL version 5.5R1F1 provided by Hillstone Networks

Connection Method	Protocol	Port Range	Source (IP or Group)
HTTP	tcp	80 - 80	0.0.0.0/0
	tcp	4500 - 4500	0.0.0.0/0
	tcp	4433 - 4433	0.0.0.0/0
	tcp	1280 - 1280	0.0.0.0/0
SSH	tcp	22 - 22	0.0.0.0/0
	tcp	500 - 500	0.0.0.0/0
	tcp	2222 - 2222	0.0.0.0/0
	udp	4500 - 4500	0.0.0.0/0
	udp	4433 - 4433	0.0.0.0/0
	udp	500 - 500	0.0.0.0/0
HTTPS	tcp	443 - 443	0.0.0.0/0

Warning
Rules with source of 0.0.0.0/0 allows all IP addresses to access your instance. We recommend limiting access to only known IP addresses.

7. Select a key pair. It will be used in SSH login.

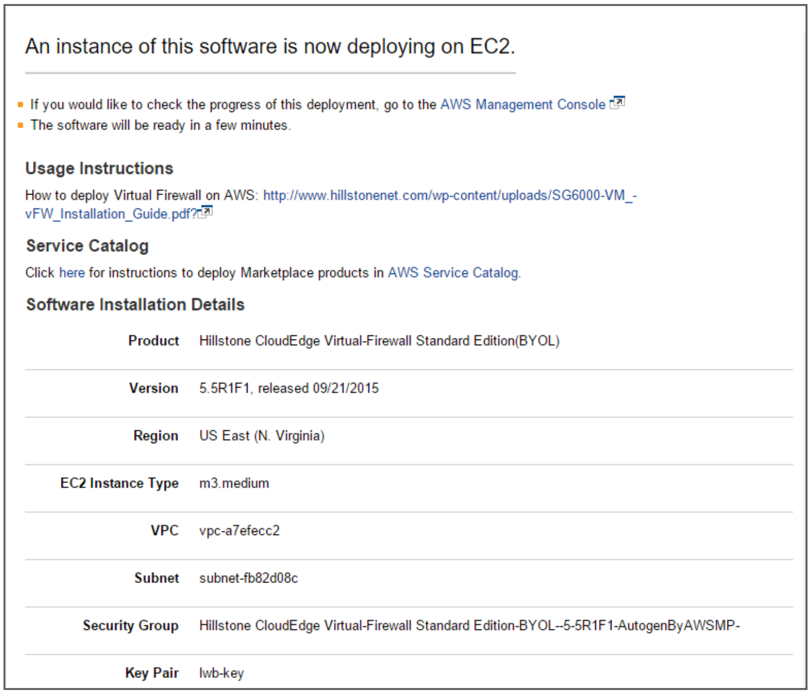


Key Pair

lwb-key ▼

To ensure that no other person has access to your software, the software installs on an EC2 instance with an EC2 key pair that you created. Choose an existing EC2 key pair in the list.

8. Click **Launch with 1-Click**.



An instance of this software is now deploying on EC2.

- If you would like to check the progress of this deployment, go to the AWS Management Console
- The software will be ready in a few minutes.

Usage Instructions

How to deploy Virtual Firewall on AWS: http://www.hillstonenet.com/wp-content/uploads/SG6000-VM_-vFW_Installation_Guide.pdf?

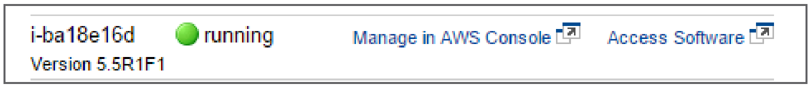
Service Catalog

Click here for instructions to deploy Marketplace products in AWS Service Catalog.

Software Installation Details

Product	Hillstone CloudEdge Virtual-Firewall Standard Edition(BYOL)
Version	5.5R1F1, released 09/21/2015
Region	US East (N. Virginia)
EC2 Instance Type	m3.medium
VPC	vpc-a7efecc2
Subnet	subnet-fb82d08c
Security Group	Hillstone CloudEdge Virtual-Firewall Standard Edition-BYOL--5-5R1F1-AutogenByAWSMP-
Key Pair	lwb-key

9. Click **Manage in AWS Console**. You will jump to EC2 management console where you can view and continue setting up CloudEdge.



i-ba18e16d ● running

Version 5.5R1F1

10. Default logging into CloudEdge is usename "hillstone" and key pair.

Launching CloudEdge from EC2

You can also start CloudEdge EC2 with EC2 wizard.

Step 1: Selecting CloudEdge from AWS Marketplace

1. Go to the AWS Marketplace and login with your credentials. Hillstone CloudEdge can be

found by being searched by the key word "Hillstone".

2. You may select "Standard Edition" or "Advanced Edition" depending on you selection of platform model.

3. After opening the product, click **Continue**.

4. Under **Manual Launch**, select system version and click **Launch with EC2 Console** next to your intended region.

5. You will jump to EC2 installation wizard to continue your setup.

Step 2: Choosing AMI

AMI is a special virtual appliance that includes operating system, applications and any additional software that are required for installing an instance.

It will take a few minutes before you can see vFW AMI in your AWS.

1. You are in the step **1: Choose AMI**. Click AWS Marketplace, and search for CloudEdge products.

2. When you find your intended product, click **Select**.

3. You will move to next step.

Step 3: Choosing Instance Type

Choose the instance type based on the product model. The selected instance should at least meet the minimum requirements of the specified product model. For more information, refer to the vFW Models. Currently, the supported instance types include t2 instance, t3 instance, m5 instance, m5a instance, and c5 instance.

Select the radio button of your intended instance type, click **Next: Configure Instance Details**.

Step 4: Configuring Instance Details

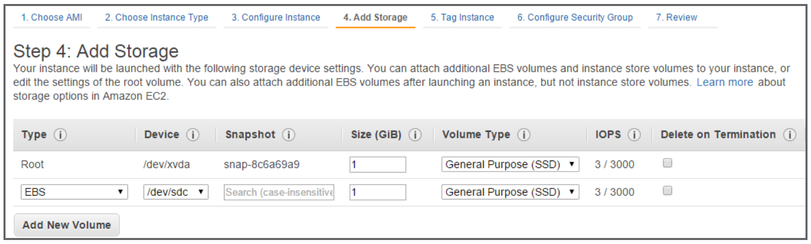
In this step, we choose VPC and VPC subnets for the instance.

1. Under the Network drop-down menu, select the VPC to which vFW belongs. Select the Subnet 1(Public) to associate to eth0 from the drop-down list of Subnet. You can keep other options as default.

2. Click **Next: Add Storage**.

Step 5: Adding Storage

1. vFW needs two volumes. The root volume stores vFW image, and the second volume saves configurations files. If you cannot see two volumes on this page, which means that your AMI has only one default volume in its settings, you can add a new volume by clicking **Add New Volume**. For the second volume, you can keep default values, and the size can be just 1 GB.



Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. Learn more about storage options in Amazon EC2.

Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Delete on Termination
Root	/dev/xvda	snap-8c6a69a9	1	General Purpose (SSD) ▾	3 / 3000	□
EBS ▾	/dev/sdc ▾	Search (case-insensitive	1	General Purpose (SSD) ▾	3 / 3000	□

2. Click **Next: Tag Instance**.

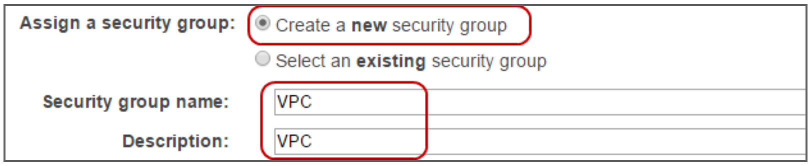
Step 6: Tag Instance

Tag is used to mark an instance. Any tag you add here will not influence configuration of you instance. You can configure or just ignore this step, and click **Next: Configure Security Group**.

Step 7: Configuring Security Group

A security group is a set of firewall rules that control the traffic for your instance. AWS EC2 has a default rule to allow all SSH connections. In order to access to CloudEdge, we need to add a new rule to allow traffic of all types.

1. Select **Create a new security group**, and enter names and description.



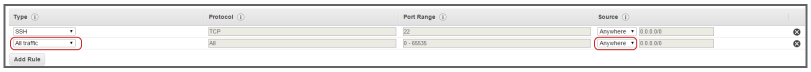
Assign a security group: ● Create a **new** security group

○ Select an **existing** security group

Security group name: VPC

Description: VPC

2. Click **Add Rule** to add a rule which allows all types of traffic.



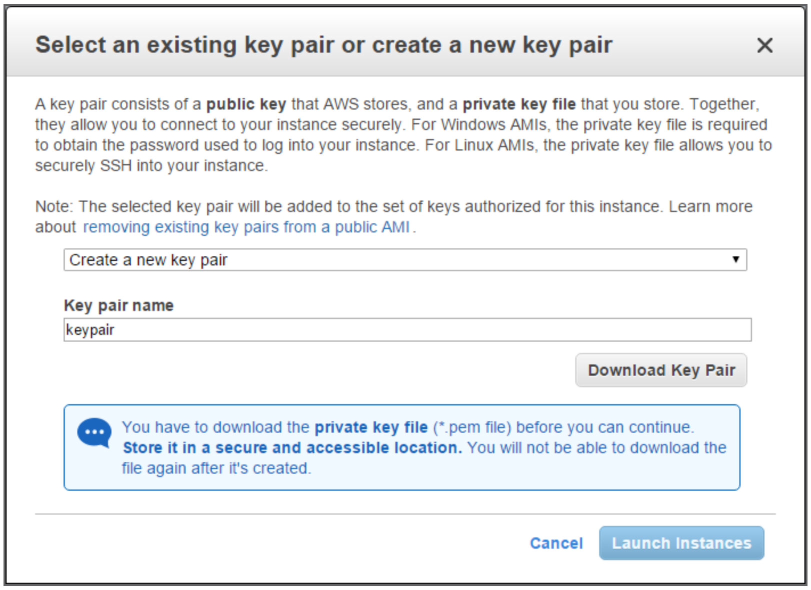
Type	Protocol	Port Range	Source	
SSH	TCP	22	Anywhere 0.0.0.0/0	⊗
All traffic	All	0 - 65535	Anywhere 0.0.0.0/0	⊗

3. Click **Review and Launch**.

Step 8: Launching Instance

1. On the review page, look at all the configurations and click **Launch**.

2. AWS will pop up a prompt to ask you for key pair. Select **Create a new key pair**, and enter a name for the private key file.



Select an existing key pair or create a new key pair ✕

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI .

Create a new key pair ▾

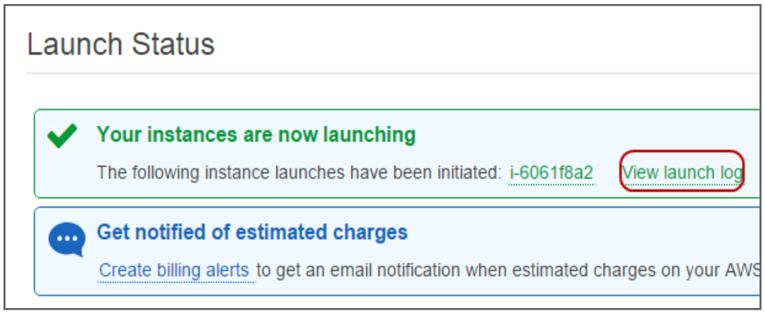
Key pair name

keypair

You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

3. Click **Download Key Pair**, your browser will start downloading a PEM file with the name you just entered. You should save this private key file in a secured location. It will be used later.

4. Click **Launch Instances**. AWS will boot this instance. A message will show up when the instance is launched successfully. You may click **View launch log** to see the launching process logs.



Launch Status

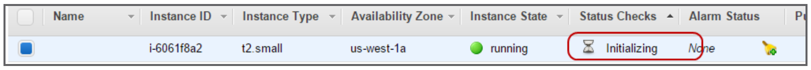
✓ **Your instances are now launching**

The following instance launches have been initiated: i-6061f8a2 View launch log

Get notified of estimated charges

Create billing alerts to get an email notification when estimated charges on your AWS

5. Click **View Instance**, you will be redirected to instance list. The CloudEdge instance is being initialized.



□	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	P
■		i-6061f8a2	t2.small	us-west-1a	● running	⌛ Initializing	None	

Configuring Subnets and Interfaces

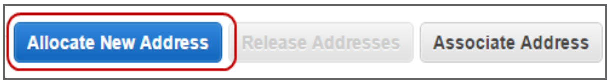
Allocating Elastic IP Addresses

Elastic IP (EIP) is a static public IP address allocated by AWS. When an instance is assigned with an EIP, this instance is open to public and has its public address.

As the DHCP function of eth0 interface is enabled by default, after the virtual firewall is started, the eth0 interface is automatically assigned with a private IP address. We will apply for an elastic IP address for eth0. After that, eth0 interface has a private IP address and public IP address. The two IP addresses are mapped to each other automatically. You do not need to set up rules to allow traffic from one address to the other.

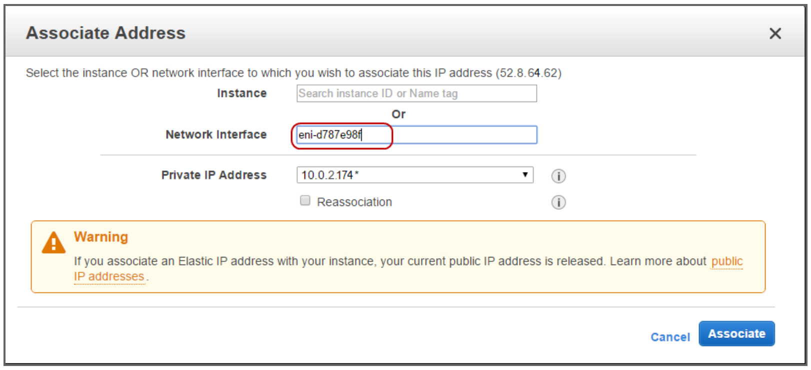
1. In EC2 management console, click **Elastic IPs** from the left navigation.

2. Click **Allocate New Address** to request a new IP address.



3. In the prompt, click **Yes, Allocate**. The new elastic IP address will be assigned to you.

4. Select an EIP, click **Associate Address**. In the prompt, enter the ID of vFW's eth0 (you can find eth0's ID from vFW's instance information). Click **Associate**, this EIP will be the public IP address of vFW's management interface eth0.



Associate Address ×

Select the instance OR network interface to which you wish to associate this IP address (52.8.64.62)

Instance	Search instance ID or Name tag
	Or
Network Interface	eni-d787e98f
Private IP Address	10.0.2.174* ▾
	□ Reassociation

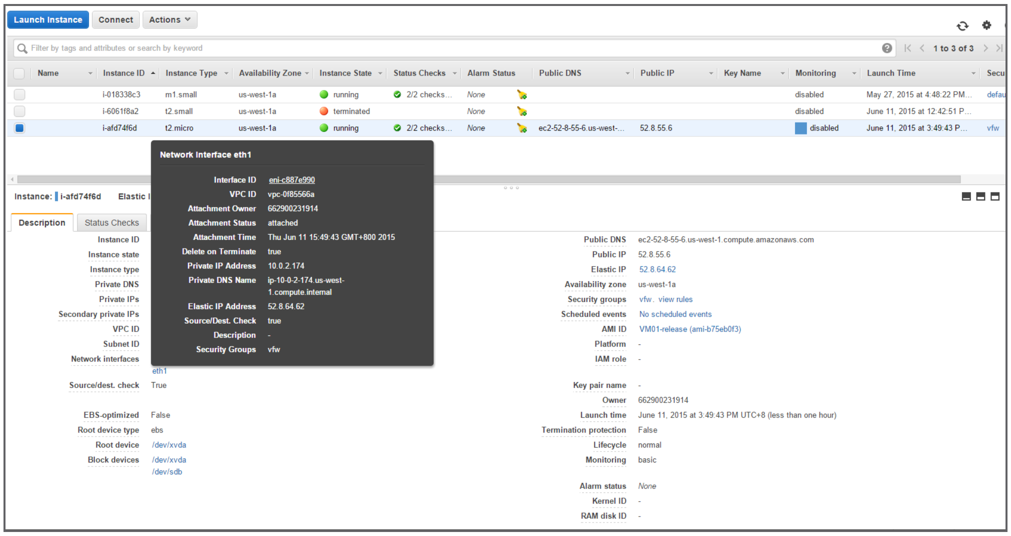
Warning

If you associate an Elastic IP address with your instance, your current public IP address is released. Learn more about public IP addresses.

5. Go back to the EIP list, you will find that the associated EIPs have their private address, interface ID, and public DNS address.

Viewing vFW Instance Information

In the EC2 management console, click **Instances** from left navigation, and then select the vFW instance in the list. The instance detailed information is shown in the pane below the list.



	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS	Public IP	Key Name	Monitoring	Launch Time	Secu
□		i-018338c3	m1.small	us-west-1a	● running	✓ 2/2 checks...	None				disabled	May 27, 2015 at 4:48:22 PM...	defau
□		i-6061f8a2	t2.small	us-west-1a	● terminated		None				disabled	June 11, 2015 at 12:42:51 P...	
■		i-afd74f6d	t2.micro	us-west-1a	● running	✓ 2/2 checks...	None	ec2-52-8-55-6.us-west-...	52.8.55.6		disabled	June 11, 2015 at 3:49:43 P...	vfw

Instance: i-afd74f6d Elastic I

Network Interface eth1

Interface ID	eni-c887e990
VPC ID	vpc-0f85566a
Attachment Owner	662900231914
Attachment Status	attached
Attachment Time	Thu Jun 11 15:49:43 GMT+800 2015
Delete on Terminate	true
Private IP Address	10.0.2.174
Private DNS Name	ip-10-0-2-174.us-west-1.compute.internal
Elastic IP Address	52.8.64.62
Source/Dest. Check	true
Description	-
Security Groups	vfw

Instance ID	
Instance state	
Instance type	
Private DNS	
Private IPs	
Secondary private IPs	
VPC ID	
Subnet ID	
Network interfaces	eth1
Source/dest. check	True
EBS-optimized	False
Root device type	ebs
Root device	/dev/xvda
Block devices	/dev/xvda /dev/sdb

Public DNS	ec2-52-8-55-6.us-west-1.compute.amazonaws.com
Public IP	52.8.55.6
Elastic IP	52.8.64.62
Availability zone	us-west-1a
Security groups	vfw. view rules
Scheduled events	No scheduled events
AMI ID	VM01-release (ami-b75eb0f3)
Platform	-
IAM role	-
Key pair name	-
Owner	662900231914
Launch time	June 11, 2015 at 3:49:43 PM UTC+8 (less than one hour)
Termination protection	False
Lifecycle	normal
Monitoring	basic
Alarm status	None
Kernel ID	-
RAM disk ID	-

Purchase and Apply for License Software

This step is only applicable to the BYOL type of products.

After you purchased BYOL type product, Hillstone next generation virtualization firewall License is also needed, which ensures vFW run normally in AWS. Please contact the Hillstone salesperson to get the license software. To install the license software in vFW, see "Installing License" on Page 8

Visiting CloudEdge

In CloudEdge default settings, only the access to eth0. is enabled. So, we will use SSH connection to visit eth0 before we can visit its other ports.

Visiting CloudEdge from Windows Using PuTTY

We use Windows to explain how to visit ourCloudEdge instance.

Before connecting, you will need to complete the following prerequisites:

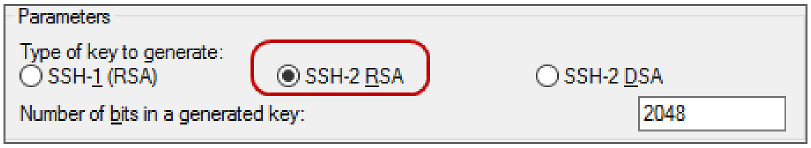
- Install PuTTY (recommend by AWS): Download and install **PuTTYgen** and **PuTTY**. You may download from PuTTy DownLoad Page.
  - Get the Elastic IP of the instance: the eth0's public IP address.
- Locate the private key (PEM file)
  - Enable inbound SSH traffic from your IP address to your instance: this settings is default. If you did not change settings, you will have SSH inbound access.

Step 1: Converting Your Private Key Using PuTTYgen

PuTTY does not natively support the private key format (.pem) generated by Amazon EC2. PuTTY has a tool named PuTTYgen, which can convert keys to the required PuTTY format (.ppk). You must convert your private key into this format (.ppk) before attempting to connect to your instance using PuTTY.

To convert your private key

1. Start PuTTYgen (for example, from the Start menu, click **All Programs** > **PuTTY** > **PuTTYgen**).
2. Under **Type of key to generate**, select **SSH-2 RSA**.



Parameters

Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 2048

3. Click **Load**. By default, PuTTYgen displays only files with the extension .ppk. To locate your .pem file, select the option to display files of all types.
4. Browse and select PEM file.

5. Click **Save private key**, and save it (a .ppk file) to a secured location on your PC. It will be used soon.

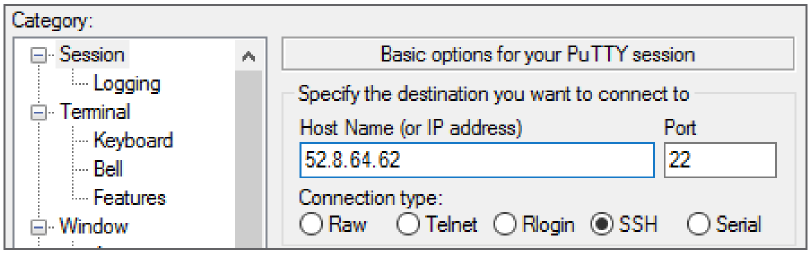
6. Close PuTTYgen.

Step 2: Starting a PuTTY Session

Use the following procedure to connect to your instance using PuTTY. You'll need the .ppk file that you created for your private key.

1. Start PuTTY (from the **Start** menu, click **All Programs > PuTTY > PuTTY**).

2. In the **Category** pane, select **Session** and complete the following fields:



Specify the destination you want to connect to

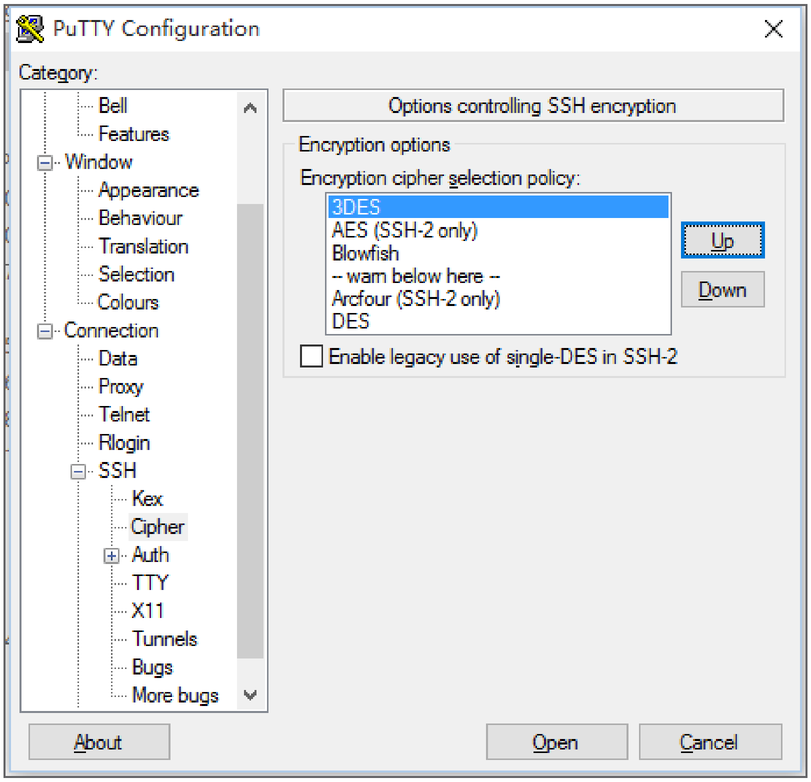
Host Name (or IP address): 52.8.64.62

Port: 22

Connection type:
○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

- In the **Host Name box**, enter instance's public IP (eth0 public address).
  - Under **Connection** type, select **SSH**.
  - Ensure that **Port** is 22.

3. In the **Category** pane, expand **Connection > SSH > Cipher**, and move 3DES up to the top.



Options controlling SSH encryption

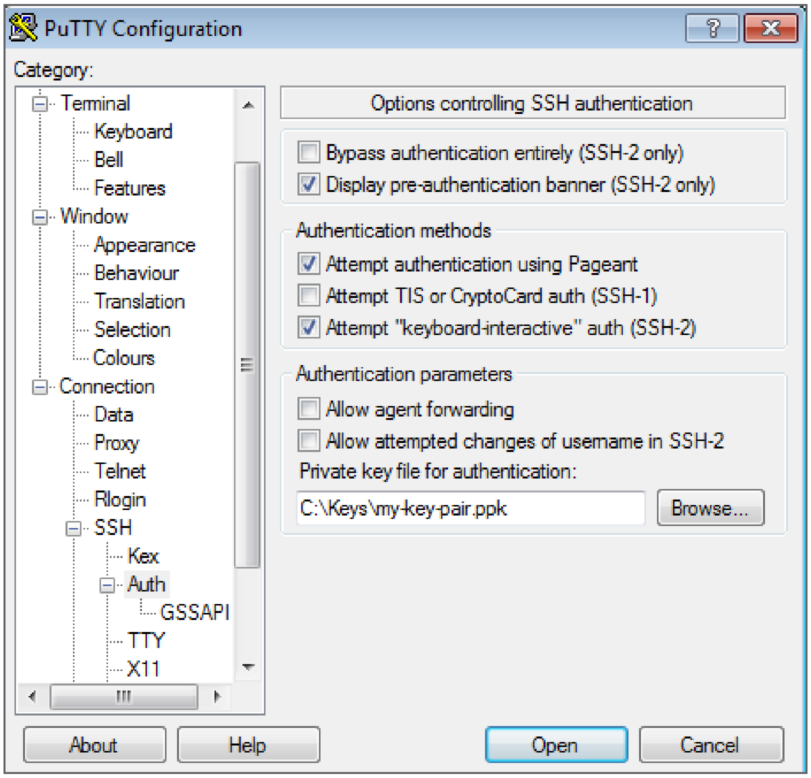
Encryption options

Encryption cipher selection policy:

3DES
AES (SSH-2 only)
Blowfish
-- warn below here --
Arcfour (SSH-2 only)
DES

□ Enable legacy use of single-DES in SSH-2

4. In the **Category** pane, expand **Connection > SSH > Auth**. Click Browse, and select the .ppk file that was generated for private key pair.



Options controlling SSH authentication

□ Bypass authentication entirely (SSH-2 only)

☑ Display pre-authentication banner (SSH-2 only)

Authentication methods

☑ Attempt authentication using Pageant

□ Attempt TIS or CryptoCard auth (SSH-1)

☑ Attempt "keyboard-interactive" auth (SSH-2)

Authentication parameters

□ Allow agent forwarding

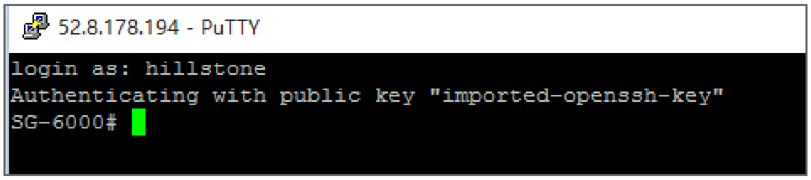
□ Allow attempted changes of username in SSH-2

Private key file for authentication:

C:\Keys\my-key-pair.ppk

5. Click **Open**. If a prompt appears, click OK.

6. A command line dialog appears. It prompts for you to enter username. Type **hillstone**, and you will be connected to your instance.



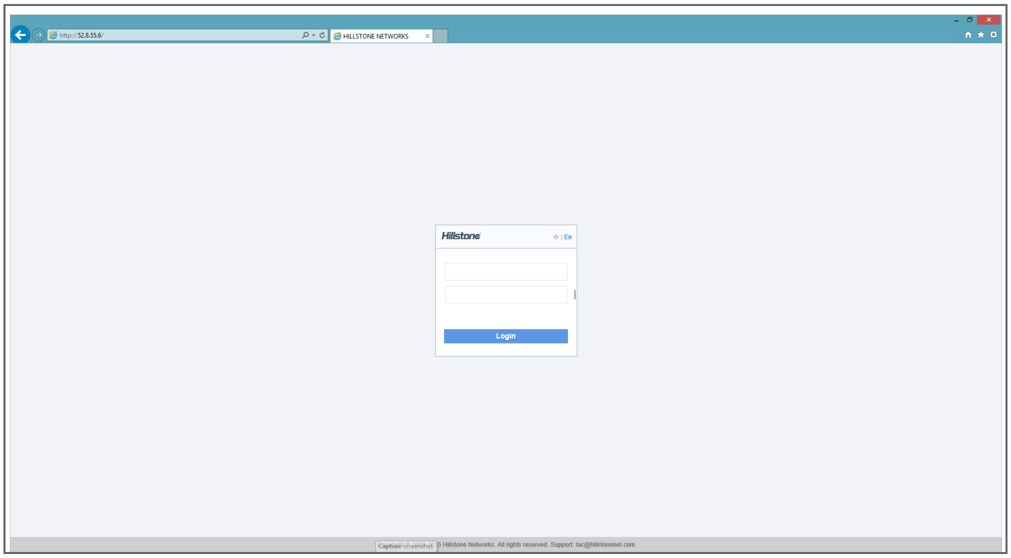
```
login as: hillstone
Authenticating with public key "imported-openssh-key"
SG-6000#
```

Visiting WebUI of StoneOS

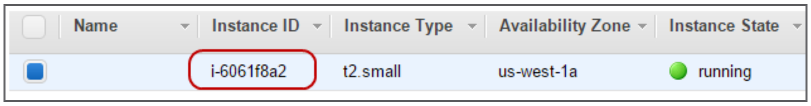
1. In order to enable WebUI access, enter the command below to enable eth0's http protocol first:

```
SG-6000# config
SG-6000(config)# interface ethernet0/0
SG-6000(config-if-eth0/0)# manage http
```

2. Enter the EIP of eth0 into the address bar of you browser, and then you are in the login page of StoneOS.



3. Enter the default username "hillstone". For default password, enter CloudEdge instance ID. The instance ID can be found in AWS EC2 instance page.



	Name	Instance ID	Instance Type	Availability Zone	Instance State
■		i-6061f8a2	t2.small	us-west-1a	● running

4. Click **Login**, you will enter StoneOS web management interface.

Notes: We recommend that users run StoneOS WebUI on Chrome and IE 11 which have been tested for browser compatibility.

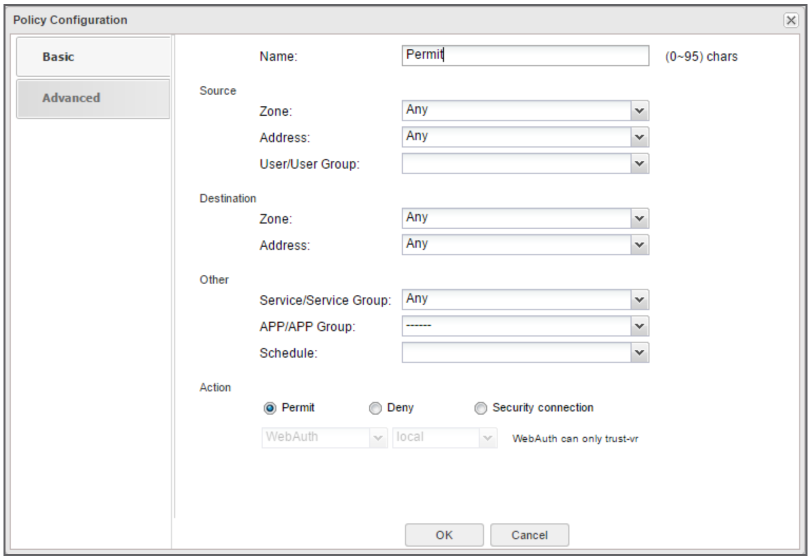
Basic Configurations of StoneOS

Creating a Policy Rule

To create a policy rule that allows all traffics from and to all directions:

1. Select **Policy > Security Policy**.

2. Create a security policy that allows all types of traffic (every field is set to **Any**).



Name: Permit (0~95) chars

Source

Zone: Any

Address: Any

User/User Group:

Destination

Zone: Any

Address: Any

Other

Service/Service Group: Any

APP/APP Group: ------

Schedule:

Action

● Permit ○ Deny ○ Security connection

WebAuth local WebAuth can only trust-vr

3. Click **OK**.

Or, you can use the following command in CLI:

```
SG-6000(config)# rule id 1 from any to any service any permit
```

Testing

In order to test whether the private network traffic can be through the virtual firewall, we will configure the SNAT and DNAT function in the virtual firewall.

We will create a virtual machine with a Windows 2012 Server system in AWS VPC to test that if the servers in private subnet can connect to Internet via vFW.

Creating a Test Virtual Machine (Windows)

In this section, a Windows 2012 Server virtual machine will be created. This virtual server will be an internal server in a company's private network, and it connects to public network by vFW.

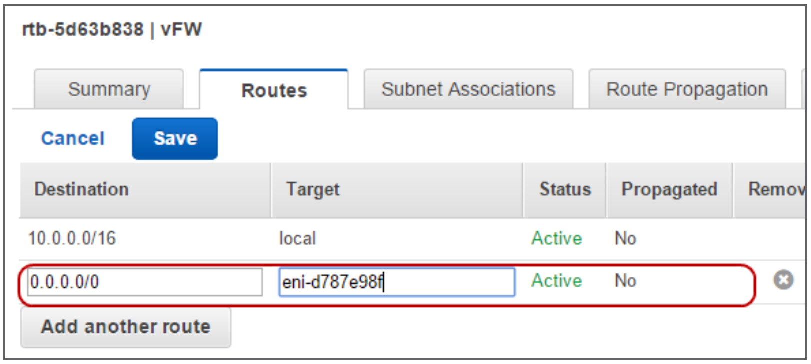
Step 1: Modifying Route Table

Before the SNAT function is enabled, you need to add a route entry for the route table used by the subnet Subnet 0 (Manage), whose destination address is 0.0.0.0/0 and the target is the ID of the interface eth0, in order to make sure packets from Subnet 0 (Manage) can access the Internet through the virtual firewall.

To modify the route table of private subnet:

1. In VPC console, select **Route Tables** from left navigation, modify the route table name of Subnet 0 (Manage) to "vFW" for easier search.
2. In the lower part of this page, click the <Routes> tab, and then click **Edit**.

3. Click **Add another route**, and enter the ID of vFW's eth0.



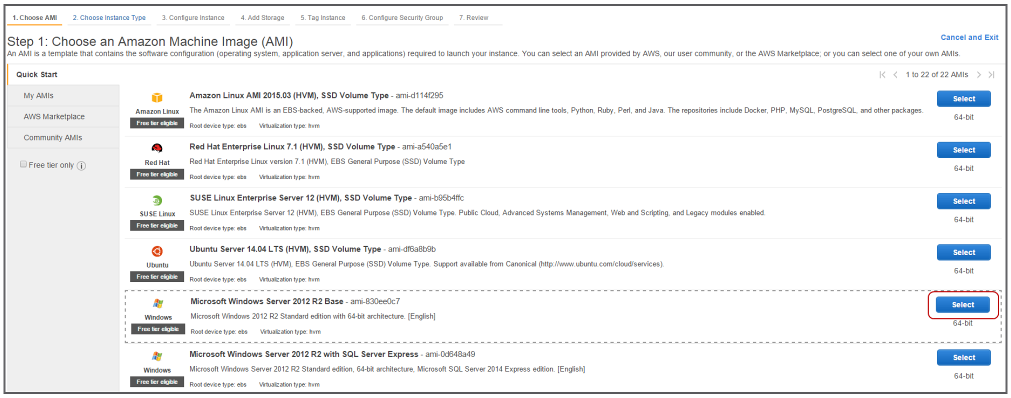
Destination	Target	Status	Propagated	Remov
10.0.0.0/16	local	Active	No	
0.0.0.0/0	eni-d787e98f	Active	No	⊗

4. Click **Save**.

Step 2: Creating EC2 instance

1. Go to EC2 management console, click **Launch Instance**.

2. From AWS AMI community, select a Windows Server 2012, click **Select**.



Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Amazon Linux — Free tier eligible — **Amazon Linux AMI 2015.03 (HVM), SSD Volume Type** - ami-d114f295
The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.
Root device type: ebs Virtualization type: hvm

Red Hat — Free tier eligible — **Red Hat Enterprise Linux 7.1 (HVM), SSD Volume Type** - ami-a540a5e1
Red Hat Enterprise Linux version 7.1 (HVM), EBS General Purpose (SSD) Volume Type
Root device type: ebs Virtualization type: hvm

SUSE Linux — Free tier eligible — **SUSE Linux Enterprise Server 12 (HVM), SSD Volume Type** - ami-b95b4ffc
SUSE Linux Enterprise Server 12 (HVM), EBS General Purpose (SSD) Volume Type. Public Cloud, Advanced Systems Management, Web and Scripting, and Legacy modules enabled.
Root device type: ebs Virtualization type: hvm

Ubuntu — Free tier eligible — **Ubuntu Server 14.04 LTS (HVM), SSD Volume Type** - ami-df6a8b9b
Ubuntu Server 14.04 LTS (HVM), EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services).
Root device type: ebs Virtualization type: hvm

Windows — Free tier eligible — **Microsoft Windows Server 2012 R2 Base** - ami-830ee0c7
Microsoft Windows 2012 R2 Standard edition with 64-bit architecture. [English]
Root device type: ebs Virtualization type: hvm

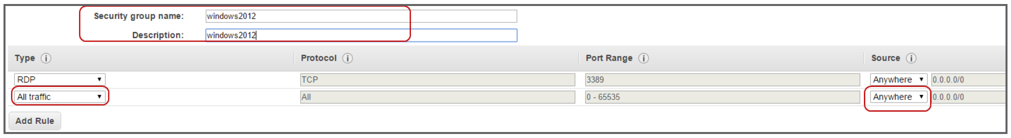
Windows — Free tier eligible — **Microsoft Windows Server 2012 R2 with SQL Server Express** - ami-0d648a49
Microsoft Windows Server 2012 R2 Standard edition, 64-bit architecture, Microsoft SQL Server 2014 Express edition. [English]
Root device type: ebs Virtualization type: hvm

3. Keep the default settings in instance type page, click **Next: Configure Instance Details**.

4. Select your VPC and subnet Private: 10.0.0.0/24.

5. Click **Next** for consecutive three times to keep default values, and move to <6. Configure Security Group> page.

   On this page, add a rule to allow all traffic.



Security group name: windows2012

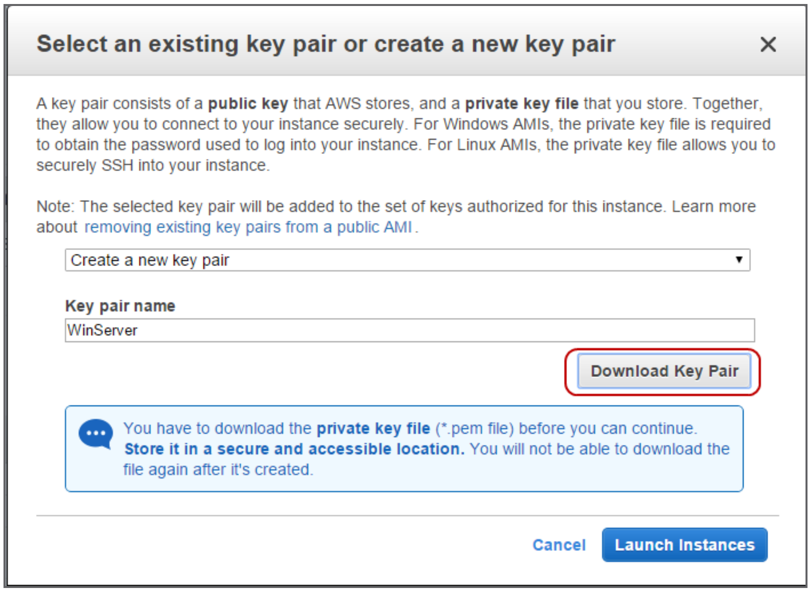
Description: windows2012

Type	Protocol	Port Range	Source	
RDP	TCP	3389	Anywhere	0.0.0.0/0
All traffic	All	0 - 65535	Anywhere	0.0.0.0/0

6. Click **Review and Launch**, and in the review page, click **Launch**.

7. (Important!) In the prompt, select **Create a new key pair** from drop-down menu. Enter any name, and click **Download Key Pair**. Your browser will automatically download the key pair file (.pem).

You should save that file to a secured location and it will be used later.



Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI .

Create a new key pair

Key pair name: WinServer

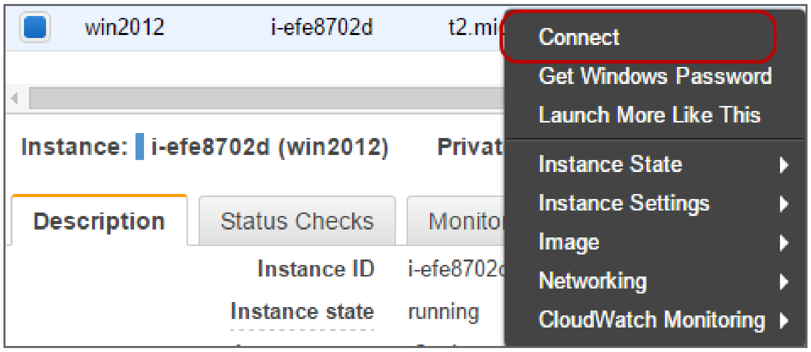
You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

8. Click **Launch Instance**. The Windows EC2 instance will start to boot.

Step 3: Acquiring Password of Test Instance

To connect to the test Windows instance, you will use the key pair file.

1. In EC2 instance list, right click the new Windows instance, and select **Connect**.



win2012 i-efe8702d t2.mi

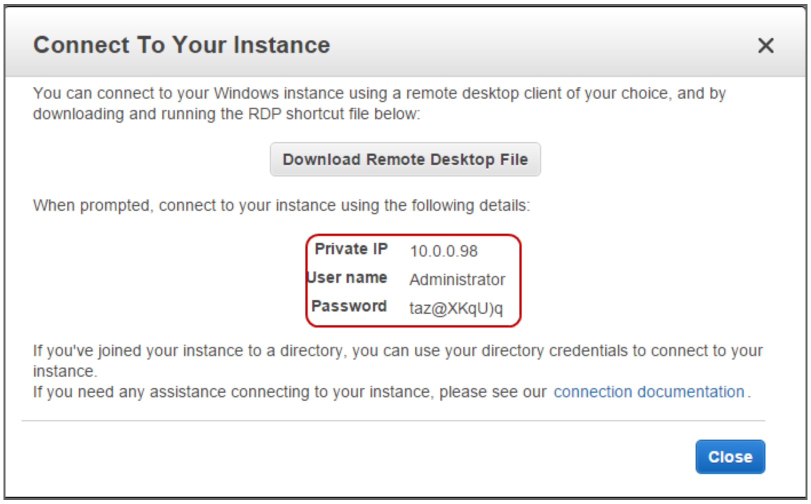
Instance: i-efe8702d (win2012) Privat

Instance ID: i-efe8702d

Instance state: running

2. In the prompt, click **Get Password**, and in the prompt, click **Choose File**, then browse and import the private key file (.pem) which was saved in the previous step.

3. Click **Decrypt Password**, you will see plain text password. You are advised to copy the password to a text file.



Connect To Your Instance

You can connect to your Windows instance using a remote desktop client of your choice, and by downloading and running the RDP shortcut file below:

When prompted, connect to your instance using the following details:

Private IP	10.0.0.98
User name	Administrator
Password	taz@XKqU)q

If you've joined your instance to a directory, you can use your directory credentials to connect to your instance.

If you need any assistance connecting to your instance, please see our connection documentation.

4. Close this dialog.

Step 4: Creating a DNAT rule

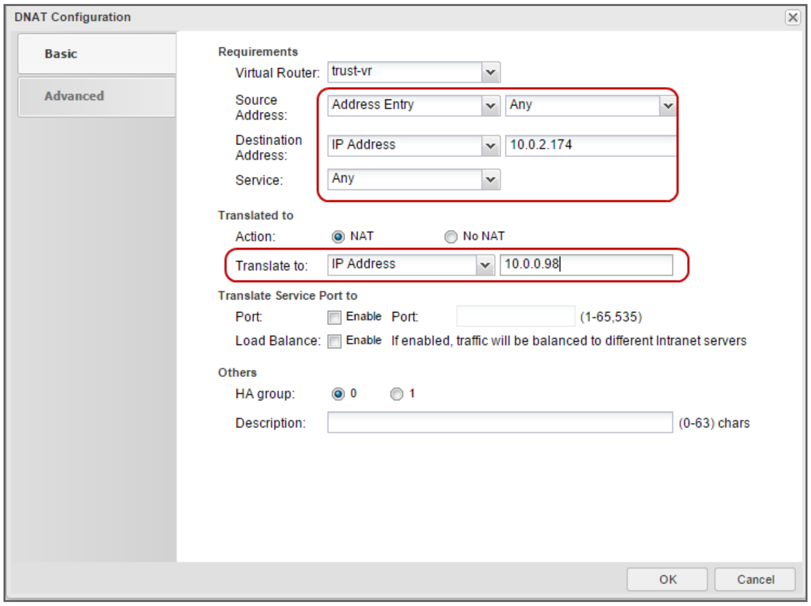
In order to publish interface servers on a publicly accessible address, we should create a DNAT rule for internal servers which provide services to public network.

In this design, the DNAT rule will use eth0.

1. In vFW's StoneOS, select **Policy > NAT > DNAT**, and click **New > Advanced Configuration**.

2. In the prompt, select **Any** for the <Source Address> field, enter the private IP address of eth0 for the <Destination Address> field, and enter the private IP address of your internal server for

the <Translate to> field.



Requirements

Virtual Router: trust-vr

Source Address: Address Entry | Any

Destination Address: IP Address | 10.0.2.174

Service: Any

Translated to

Action: ● NAT ○ No NAT

Translate to: IP Address | 10.0.0.98

Translate Service Port to

Port: □ Enable Port: (1-65,535)

Load Balance: □ Enable If enabled, traffic will be balanced to different Intranet servers

Others

HA group: ● 0 ○ 1

Description: (0-63) chars

3. Click **OK**.

Or, you can use the following command in CLI:

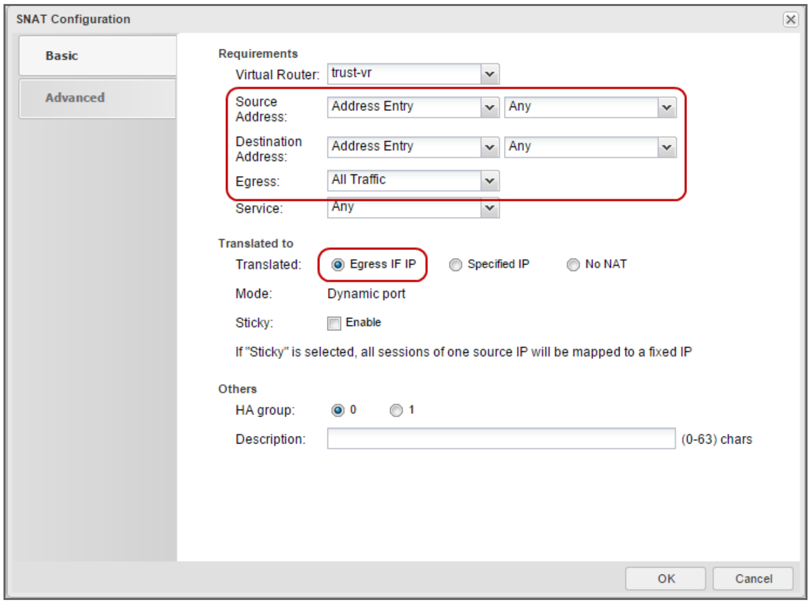
```
SG-6000(config)# ip vrouter trust-vr
SG-6000(config)# dnatrule from any to 10.0.2.174 trans-to 10.0.0.98
```

Step 5: Creating an SNAT rule

SNAT rule is used when your internal servers want to visit public network. If your private server is just used to provide services and will not visit Internet, you can omit this section.

1. Select **Policy > NAT > SNAT**, click **New**.

2. In the prompt, create an SNAT rule to translate any traffic to egress interface.



Requirements

Virtual Router: trust-vr

Source Address: Address Entry | Any

Destination Address: Address Entry | Any

Egress: All Traffic

Service: Any

Translated to

Translated: ● Egress IF IP ○ Specified IP ○ No NAT

Mode: Dynamic port

Sticky: □ Enable

If "Sticky" is selected, all sessions of one source IP will be mapped to a fixed IP

Others

HA group: ● 0 ○ 1

Description: (0-63) chars

3. Click **OK**.

Or, you can use the following command in CLI:

```
SG-6000(config)# ip vrouter trust-vr
SG-6000(config)# snatrule from any to any trans-to eif-ip mode dynamicport
```

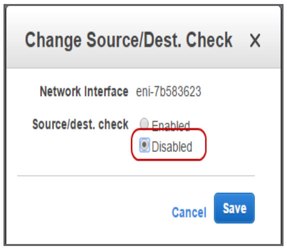
Step 6: Disabling Source/Dest. Check

To make SNAT run normally, you need to disable source/destination check of the network interface.

1. On EC2 management console, click **Networks Interfaces** from the left navigation.

2. Select the interface eth0, click **Actions > Change Source/Dest. Check**.

3. In the prompt, select **Disabled**, and click **Save**.



Change Source/Dest. Check

Network Interface eni-7b583623

Source/dest. check ○ Enabled ● Disabled

Starting Test

Before testing, make sure your vFW has the following settings:

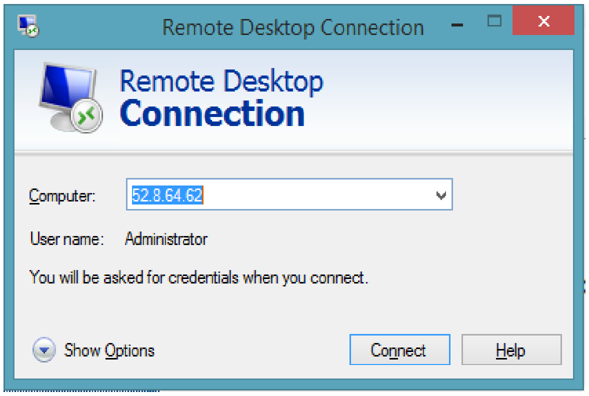
- A security rule that allows all traffic ("Creating a Policy Rule" on Page 109);
- You have disabled Source/Dest. check for interfaces that connect to IGW ("Installing CloudEdge on AWS" on Page 94);
- A DNAT rule that translates eth0's address to private server's address ("Step 4: Creating a DNAT rule" on Page 114);

Test 1: Visiting Private Server

On a PC with Internet connection, you can use remote desktop client to visit private virtual server.

1. Type **mstsc** in Startup of Windows system, press **Enter**.

2. Use Windows remote client, enter the public IP address (i.e. the EIP of eth0).

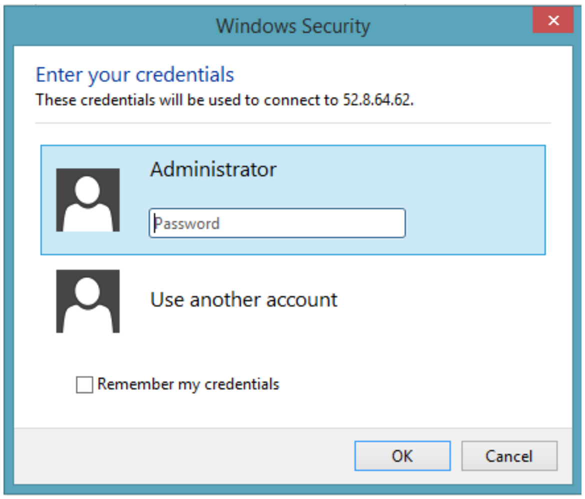


Computer: 52.8.64.62

User name: Administrator

You will be asked for credentials when you connect.

3. Click **Connect**. Copy the encrypted password (you should have already saved the password in text file), and paste the password in the password field. If the system indicates your password is wrong, you may try to manually input the password.



Enter your credentials

These credentials will be used to connect to 52.8.64.62.

Administrator

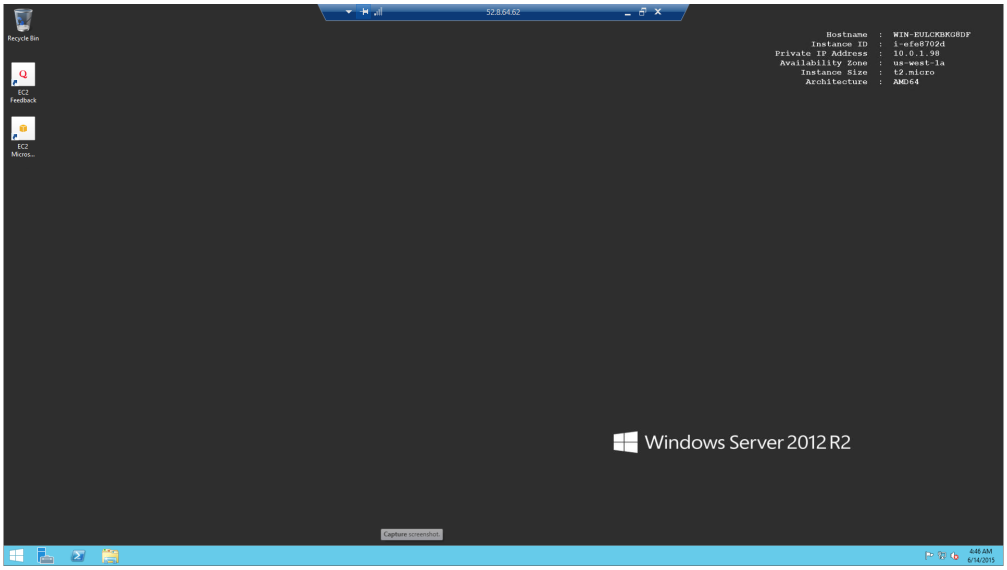
Password

Use another account

□ Remember my credentials

4. In the prompt of certificate warning, click **Yes** to continue.

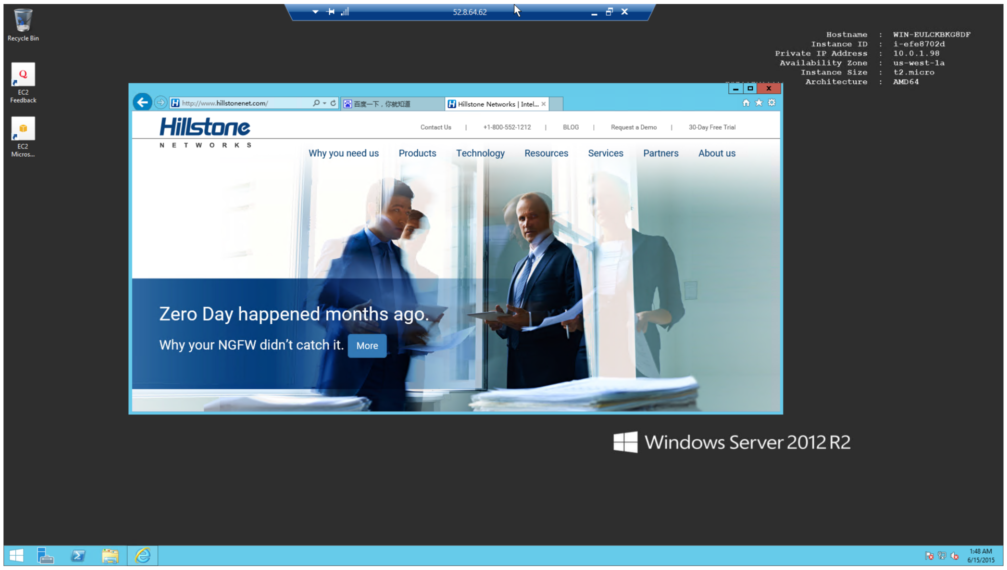
5. Now you have entered the Windows server system.



```
             Hostname  :  WIN-EULCKBKG8DF
          Instance ID  :  i-efe8702d
   Private IP Address  :  10.0.1.98
    Availability Zone  :  us-west-1a
        Instance Size  :  t2.micro
         Architecture  :  AMD64
```

Test 2: Internal Server to Access Internet

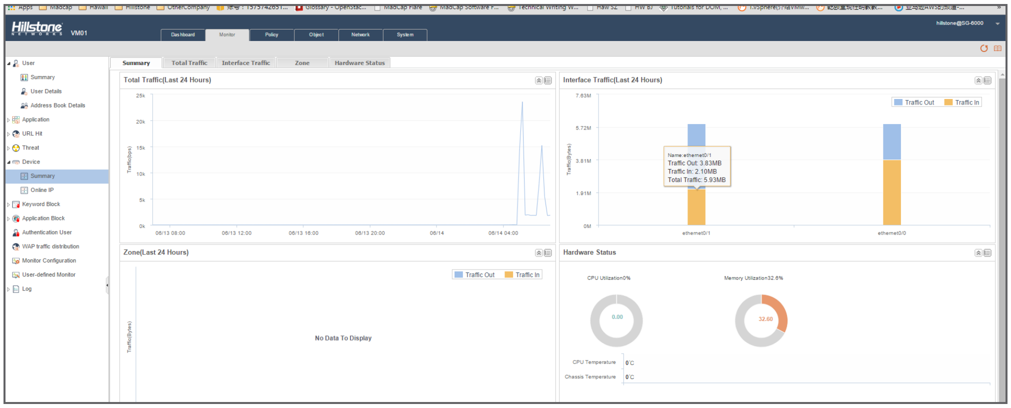
If you have configured the SNAT rule in StoneOS, your private server can visit Internet too.



```
             Hostname  :  WIN-EULCKBKG8DF
          Instance ID  :  i-efe8702d
   Private IP Address  :  10.0.1.98
    Availability Zone  :  us-west-1a
        Instance Size  :  t2.micro
         Architecture  :  AMD64
```

Test 3: Checking In/Out Traffic of vFW

Log in StoneOS, and select **Monitor > Device > Summary**, you will see that vFW's interface has in-and-out traffic.



Name:ethernet0/1
Traffic Out: 3.83MB
Traffic In: 2.10MB
Total Traffic: 5.93MB

No Data To Display

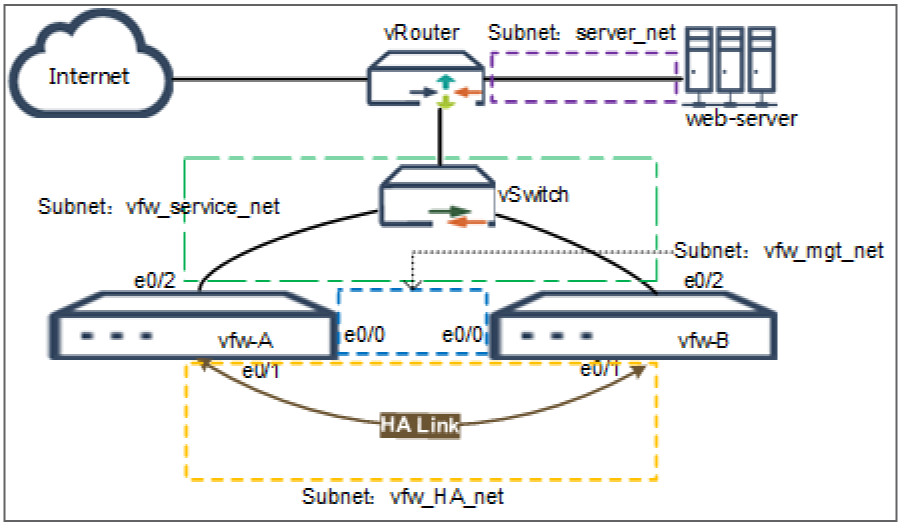
CPU Temperature 0°C
Chassis Temperature 0°C

Deploying HA Scenarios of CloudEdge on AWS

HA Typical Scenarios

There is a cloud server web-server (10.0.2.209) on the AWS platform. You can protect the server by deploying the HA scheme of CloudEdge.The following topology introduces how to deploy HA scenarios of CloudEdge on AWS.

After the deployment, vfw-A will be selected as the master device to protect the web-server and vfw-B will be selected as the backup device. vfw-A will synchronize its configurations and status data to the backup device vfw-B. When the master device vfw-A fails to work, the backup device vfw-B will switch to the master device to protect web-server without interrupting user's communication, which can ensure network stability.



Deployment Steps

"Step 1: Creating VPC and Subnet" on Page 122

"Step 2: Creating and Enabling Internet Gateway" on Page 122

"Step 3: Creating Policies" on Page 124

"Step 4: Creating IAM Roles" on Page 126

Step 1: Creating VPC and Subnet

Log in to the AWS console (click here) with your AWS account to create a VPC and subnet. For details, see Adding subnets into VPC.

Information of VPC and subnet which web-server belong to are as follows:

- VPC(VPC1):10.0.0.0/16
- Subnet 0 (server_net):10.0.2.0/24
- web-server IP： 10.0.2.209

Create the following subnets, and the VPC which subnets and the web-server belong to should be the same:

- VPC(VPC1)： 10.0.0.0/16
- Subnet 1 （vfw_service_net） ： 10.0.1.0/24
- Subnet 2 （vfw_mgt_net） ： 10.0.10.0/24
- Subnet 3 （vfw_HA_net） ： 10.0.100.0/24

Step 2: Creating and Enabling Internet Gateway

Create an Internet gateway for instances in a VPC to communicate with the Internet. For details, take the following steps:

1. In the VPC Dashboard, select “Internet Gateway”, and click **Create internet gateway**.

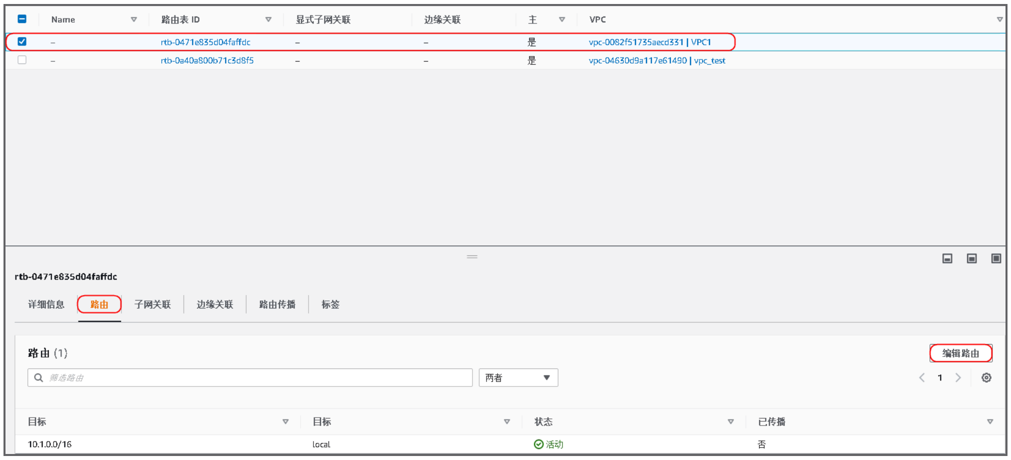
2. In the <Create internet gateway> page, type the tag “Internet_ha”。

3. Click **Create** to save the above configurations.

4. In the Internet gateway list, select the "Internet_ha" item. Then click the **Actions** drop-down list, select **Attach to VPC**, and select "VPC1" created in step 1 .

5. In the VPC Dashboard, select “Route Tables”.

6. Select the corresponded route of the VPC1 created in Step 1, click the <Routes> tab at the bottom of the page, and then click **Edit routes**.



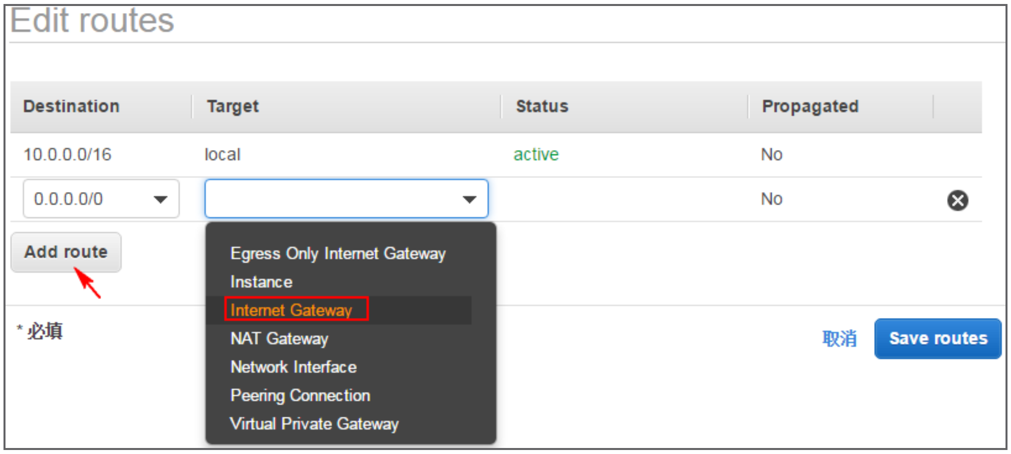
☐	Name	路由表 ID	显式子网关联	边缘关联	主	VPC
☑	–	rtb-0471e835d04faffdc	–	–	是	vpc-0082f51735aecd331 | VPC1
☐	–	rtb-0a40a800b71c3d8f5	–	–	是	vpc-04630d9a117e61490 | vpc_test

rtb-0471e835d04faffdc

路由 (1)

目标	目标	状态	已传播
10.1.0.0/16	local	✓ 活动	否

7. In the <Edit routes> page, click **Add route** and add a route whose next-hop is Internet Gateway "Internet_ha" to enable the Internet gateway.



Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0			No

Step 3: Creating Policies

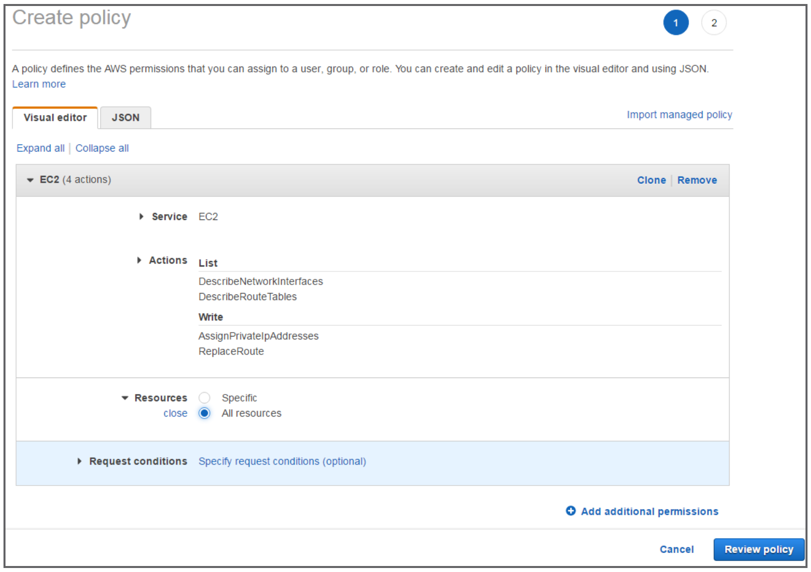
A policy defines the AWS permissions that you can assign to a user, group, or role.You can create policies that refine the functional permissions of cloud platforms that CloudEdge calls. If you don't need to limit the functional permissions that CloudEdge specifically calls, you can skip this step directly. To create an IAM policy ,take the following steps:

1. In the"Security, Identity & Compliance" Dashboard, select "IAM > Policies".

2. Click **Create policy**, and in the <Create policy>page, configure the followings.

    - Service: EC2
    - Actions:
        - List: DescribeNetworkInterfaces and DescribeRouteTables
        - Write: AssignPrivateIpAddress和ReplaceRoute

- Resources: All resources



Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

EC2 (4 actions)

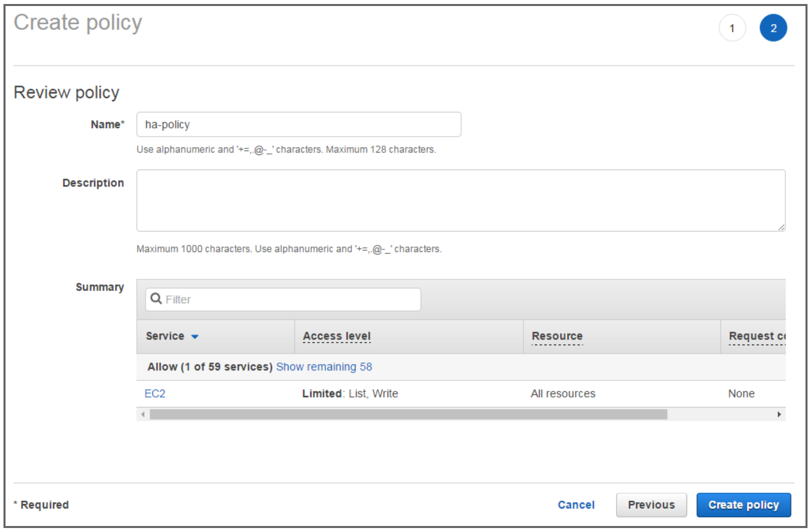
Service: EC2

Actions:
List
DescribeNetworkInterfaces
DescribeRouteTables
Write
AssignPrivateIpAddresses
ReplaceRoute

Resources: ○ Specific ● All resources

Request conditions: Specify request conditions (optional)

3. Click **Review policy**, and in the <Review policy> page, enter the policy Name "ha-policy".



Create policy

Review policy

Name*: ha-policy

Use alphanumeric and '+=,.@-_' characters. Maximum 128 characters.

Description:

Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Summary

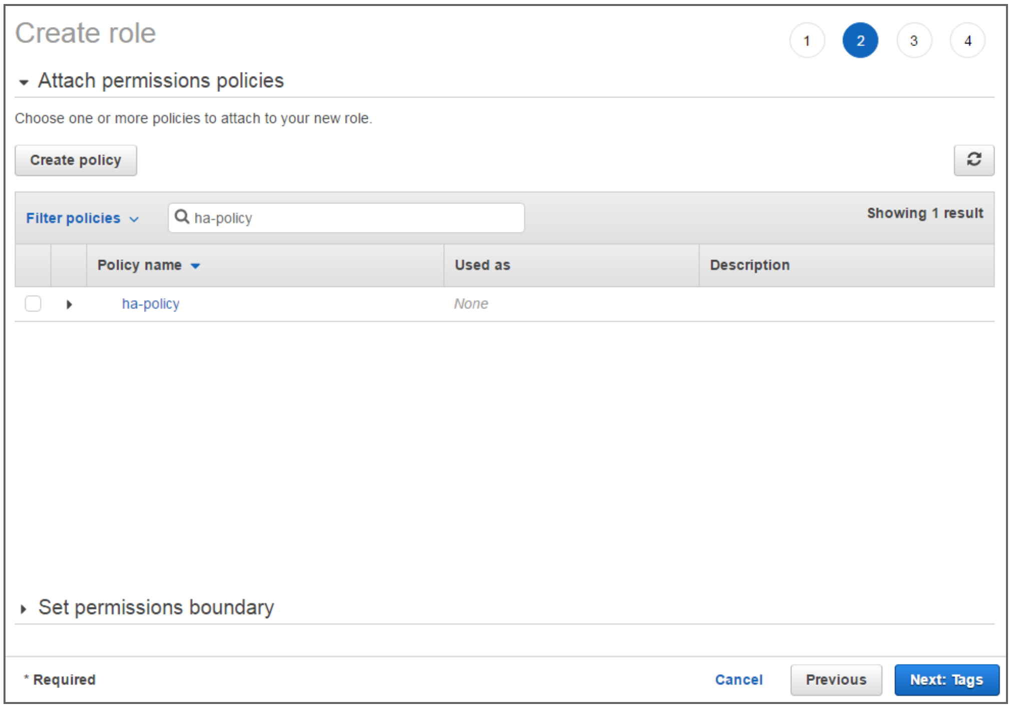
Service	Access level	Resource	Request co
Allow (1 of 59 services) Show remaining 58			
EC2	Limited: List, Write	All resources	None

4. Click **Create policy**.

Step 4: Creating IAM Roles

Create IAM roles and configure permissions to invoke APIs. When an instance references the IAM role, it will obtain the corresponding permissions. To create the IAM role ,take the following steps:

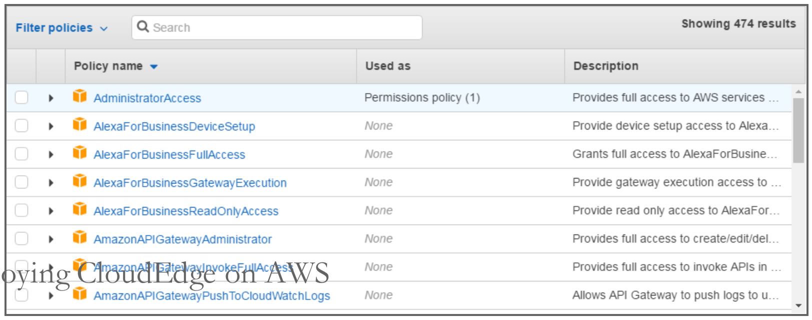
1. In the"Security, Identity & Compliance" Dashboard, select "IAM > Roles".
2. Click **Create role**, and in the <Create role>page, configure the followings.
    - Select the type of trusted entity: AWS service;
    - Choose the service that will use this role :EC2;
3. Click **Next:Pemissions**, and in the policy list of the <Attach permissions> page, select the policy "ha-policy" created in Step 3. If you don't need to limit the functional rights of CloudEdge (that is, you've skipped Step 3: Create Policies), you can directly use the "AdministratorAccess" policy corresponding to the default administrator rights of the system..


Create role
1
2
3
4
▾ Attach permissions policies
Choose one or more policies to attach to your new role.
Create policy
Filter policies
Showing 1 result
▸ Set permissions boundary
* Required
Cancel
Previous
Next: Tags

Search: ha-policy

		Policy name	Used as	Description
□	▸	ha-policy	None	

or



Search

		Policy name	Used as	Description
□	▸	AdministratorAccess	Permissions policy (1)	Provides full access to AWS services ...
□	▸	AlexaForBusinessDeviceSetup	None	Provide device setup access to Alexa...
□	▸	AlexaForBusinessFullAccess	None	Grants full access to AlexaForBusine...
□	▸	AlexaForBusinessGatewayExecution	None	Provide gateway execution access to ...
□	▸	AlexaForBusinessReadOnlyAccess	None	Provide read only access to AlexaFor...
□	▸	AmazonAPIGatewayAdministrator	None	Provides full access to create/edit/del...
□	▸	AmazonAPIGatewayInvokeFullAccess	None	Provides full access to invoke APIs in ...
□	▸	AmazonAPIGatewayPushToCloudWatchLogs	None	Allows API Gateway to push logs to u...

4. Click **Next:Tags**, skip this step and continue to click **Next:Review**.

5. In the <Review>page, type the role name "ha-role".

6. Click **Create role**.

Step 5: Creating EC2 Instances

Create two CloudEdge instances vfw-A and vfw-B on AWS for HA deployment. For details , refer to Deploying CloudEdge on AWS.

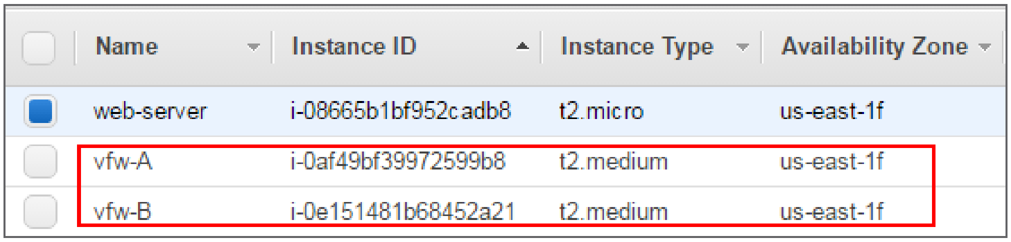
1. **Requirements:** At least 2 vCPU and 2GB memory are required for per instance. The subnet of the two instances should be the same. In this example, select the subnet "vfw_mgt_net" configured in the step 1.

2. **The configurations for the two HA CloudEdge instances are as follows. The parameters not mentioned are consistent with those in Deploying CloudEdge on AWS.**

Option	Description
AMI	In the "1. Select AMI" page, select the 5.5R6F2 or later versions of AMI. If you select an old version, you can upgrade it to 5.5R6F2 or later versions after the instance starts.
Type	In the "2. Select Instance Type" page, select the instance type "Universal t2. medium" (2vCPU, 4GiB memory).
VPC	In the "3. Configuration Instances" page, select the VPC "VPC1" configured in Step 1.
Subnet	In the "3. Configuration Instances" page, select the subnet "vfw_mgt_net" configured in Step 1 as the default network.
IAM role	In the "3 Configuration Instance " page, select the IAM role

Option	Description
	"role-ha" configured in Step 3.

3. After configurations, you can add the names "vfw-A" and "vfw-B" the instances respectively in the instance list.



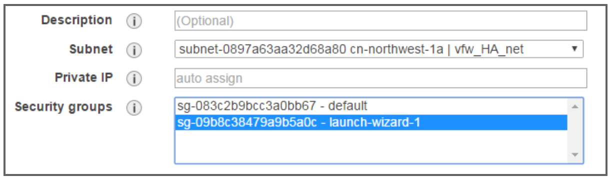
☐	Name	Instance ID	Instance Type	Availability Zone
☑	web-server	i-08665b1bf952cadb8	t2.micro	us-east-1f
☐	vfw-A	i-0af49bf39972599b8	t2.medium	us-east-1f
☐	vfw-B	i-0e151481b68452a21	t2.medium	us-east-1f

Step 6: Creating Network Interfaces

To deploy the HA scenario, besides the default network, you need to add two more network interfaces as the HA network interface and the business interface. To create the network interfaces on vfw_HA_net and vfw_Service_net subnets respectively, and then attach them to CloudEdge instances, take the following steps:

1. In the EC2 Dashboard, select "Network interface" and click **Create Network Interface**.

2. In the <Create Network Interface> dialog, select "vfw_HA_net" as the subnet, and select the security group that all traffic is allowed to pass.



Description: (Optional)
Subnet: subnet-0897a63aa32d68a80 cn-northwest-1a | vfw_HA_net
Private IP: auto assign
Security groups: sg-083c2b9bcc3a0bb67 - default
sg-09b8c38479a9b5a0c - launch-wizard-1

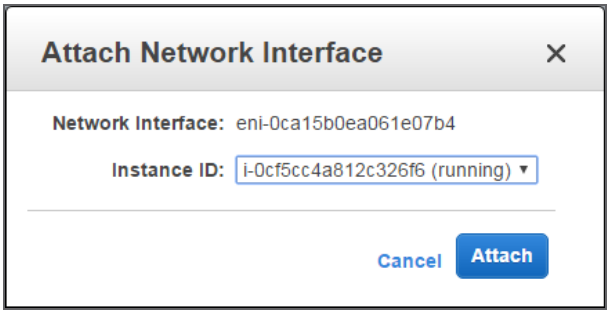
3. Repeat step 1 and 2 to create another vfw_HA_net subnet interface.

4. Repeat step 1 and 2 to create two network interfaces for the vfw_service_net subnet.

5. In the EC2 Dashboard, select "Instance". In the instance page, select the "vfw-A"and "vfw-B". Click "Action" drop-down list, and select **Shutdown** .

6. Select **Network Interface** , and enter the network interface page. Click **Attach**to attach the subnet interfaces created in step 1-4 to the instances vfw-A and vfw-B respectively.

   Note: The interface of "vfw_HA_net" subnet should be attached firstly, followed by the interface of "vfw_service_net".

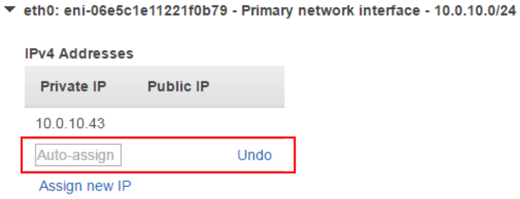
   

   Attach Network Interface

   Network Interface: eni-0ca15b0ea061e07b4

   Instance ID: i-0cf5cc4a812c326f6 (running)

7. Select the vfw_service_net interface of vfw-A (the HA master device in this example), click **Manage IP Addresses** in the "Action" drop-down list, and allocate a secondary IP for the network interface.

   eth0: eni-06e5c1e11221f0b79 - Primary network interface - 10.0.10.0/24

   IPv4 Addresses

Private IP	Public IP
10.0.10.43	
Auto-assign	Undo

8. Repeat step 7 to allocate a secondary IP for the vfw_mgt_net interface of vfw-A and vfw-B separately.

9. Allocate elastic IP addresses for the vfw_mgt_net interface of vfw-A and vfw-B instances and secondary IP of vfw-A. For details , refer to "Allocating Elastic IP Addresses" on Page 102

10. Select the vfw_service_net interface of vfw-A and vfw-B respectively, click **Change Source/Dest. check** in the "Action" drop-down list, and then disable the check.

11. Start the instance vfw-A and vfw-B.

12. View the private IP, public IP and secondary IP of the interfaces of vfw-A and vfw-B :

    - vfw-A Private IP： 10.0.10.32,10.0.100.164,10.0.1.106;
      Secondary private IP:10.0.1.242
      Public IP： 52.83.161.11

    - vfw-B Private IP： 10.0.10.89,10.0.100.100,10.0.1.6;
      Public IP： 52.83.191.210

Step 7: Connecting and Configuring CloudEdge instances

Login vfw-A and vfw-B via the SSH connection. For details , refer to Visiting CloudEdge . After login, configure the following information:

1. Configure routing priority under the interface eth0/0 of vfw-A and vfw-B respectively, and disable the reverse routing check at the same time.

```
SG-6000# configure

SG-6000(config)# interface ethernet0/0

SG-6000(config)# dhcp-client route distance 10 ////IP address and default route of eth0/0 are automatically obtained . In this example, routing priority needs to be set as 10.

SG-6000(config-if-eth0/0)# no reverse-route ////Disable the reverse routing checking of eth0/0.

SG-6000(config-if-eth0/0)# manage ip 10.0.1.242////Configure manage ip for eth0/0, which is the Secondary IP for instances vfw-A and vfw-B.

SG-6000(config-if-eth0/0)# manage https

SG-6000(config-if-eth0/0)# exit

SG-6000(config)# https port 8888////Modify the https port number.

SG-6000(config)# admin user hillstone////Modify the username and password.

SG-6000(config)# password hillstone
```

2. On the vfw-A, configure secondary IP to the vfw-Service-net interface (eth0/2 in the example) of CloudEdge. (This configuration can only be set in the master device, which will be synchronized to the backup device after HA is deployed.)

```
SG-6000# configure

SG-6000(config)# interface ethernet0/2

SG-6000(config)#zone untrust

SG-6000(config-if-eth0/2)# ip address 10.0.1.242/24 ////Configure as the Secondary IP address and its mask.

SG-6000(config-if-eth0/2)# manage ping ////Configure the management.

SG-6000(config-if-eth0/2)# manage ssh

SG-6000(config-if-eth0/2)# manage https

SG-6000(config-if-eth0/2)# exit
```

3. Configure host routing and DNS to make vfw-A and vfw-B to communicate with the AWS platform. (This configuration can only be set in the master device, which will be synchronized to the backup device after HA is deployed.)

```
SG-6000# configure

SG-6000# show dns ////View the device's DNS Server address, which is 10.0.0.2 in this example.

SG-6000(config)# ip vrouter trust-vr

SG-6000(config-vrouter)# ip route 0.0.0.0/0 10.0.1.1 ////Configure static routing, next hop is vfw_Service_net gateway IP, and the default is X.X.X.1.

SG-6000(config-vrouter)#ip route 169.254.169.254/32 10.0.10.1 //// The internal address of AWS platform is 169.254.169.254, through which CloudEdge can obtain Region, VPC id, interface id, etc. The gateway IP of vfw_mgt_net is 10.0.10.1.

SG-6000(config-vrouter)# ip route 10.0.0.2/32 10.0.10.1 ////The DNS Server address is 10.0.0.2 and the gateway IP of vfw_mgt_net is 10.0.10.1 .

SG-6000(config-vrouter)# ip route 52.82.209.55/32 10.0.10.1 ////One of the IP addresses of EC2 URL is 52.82.209.55. There are 3 addresses in total (see "Note" below for the method to get it), so 3 routes need to be added. The gateway IP of vfw_mgt_net is 10.0.10.1 .

SG-6000(config-vrouter)# ip route 52.82.209.81/32 10.0.10.1

SG-6000(config-vrouter)# ip route 52.82.209.31/32 10.0.10.1

SG-6000(config-vrouter)# end
```

Notes:

- "IP addresses for EC2 URLs" can be obtained by continuously executing the command `nslookup` in the cmd window, and finally three different public network IP addresses can be obtained.

- The URL format of China version :*ec2.current region.amazonaws.com.cn*;The URL format of international version :*ec2.-current region.amazonaws.com*。
- In this example, execute the command: **`nslookup`** *`ec2.cn-north-west-1.amazonaws.com.cn`*。

4. Configure HA on the master device vfw-A.

```
SG-6000#configure

SG-6000(config)# track track1 ////Create a track object with the
name “track1”.

SG-6000(config-trackip)# interface ethernet0/2 weight 255
////Configure eth0/2 interface as the HA tracking interface.

SG-6000(config)# ha link interface ethernet0/1 ////Configure
eth0/1 interface as the HA link interface.

SG-6000(config)# ha link ip 10.0.100.164/24 ////Configure the
IP address for HA negotiation according to the IP assigned to eth0/1 by AWS
platform.

SG-6000(config)# ha link mac 1st-interface-mac ////Configure
the control interface of HA to use the  real MAC of interface.

SG-6000(config)# no ha virtual-mac enable ////Configure the HA
business interface to use the real MAC of interface.

SG-6000(config)# ha peer ip 10.0.100.100 mac
0224.f8f3.e5e2 /////Configure the address of the peer device of HA link
interface. The MAC address can be viewed by the command "show interface". (MAC address can be optionally configured.)

SG-6000(config)# ha group 0 ////Join group HA 0.

SG-6000(config-ha-group)# priority 50 ////Set the priority and the
smaller the value, the higher the priority. The device with the higher the priority will be the master device.

SG-6000(config-ha-group)# monitor track track1 ////Add track
object to the HA group.

SG-6000(config-ha-group)# exit

SG-6000(config)# ha cluster 1 ////Add HA cluster 1.
```

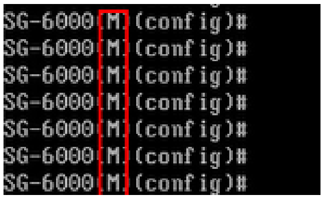
5. On the backup device vfw-B, configure the following information.

```
SG-6000#configure

SG-6000(config)# ha link interface ethernet0/1

SG-6000(config)# ha link ip 10.0.100.100/24

SG-6000(config)# ha link mac 1st-interface-mac

SG-6000(config)# no ha virtual-mac enable

SG-6000(config)# ha peer ip 10.0.100.164 mac
028e.8f79.700e ////The MAC address configuration is optional.

SG-6000(config)# ha group 0

SG-6000(config-ha-group)# priority 100

SG-6000(config-ha-group)# exit

SG-6000(config)# ha cluster 1 ////It is recommended to add HA
cluster 1 after the status of the master device changes to "M".
```

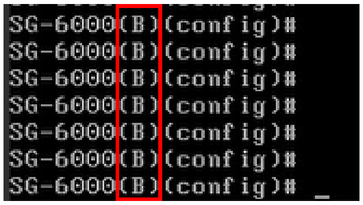
6. On the AWS platform, associate the elastic IP address with the secondary IP address of vfw-A's and vfw-B's eth0/0.

Step 8: View HA Results

After completing the above configurations, the vfw-A with high priority will be selected as the master device automatically, and the vfw-B with low priority will become the backup device. The master device and the backup device are marked with the letter "M" and letter "B" respectively in the console.



```
SG-6000(M)(config)#
SG-6000(M)(config)#
SG-6000(M)(config)#
SG-6000(M)(config)#
SG-6000(M)(config)#
SG-6000(M)(config)#
SG-6000(M)(config)#
```



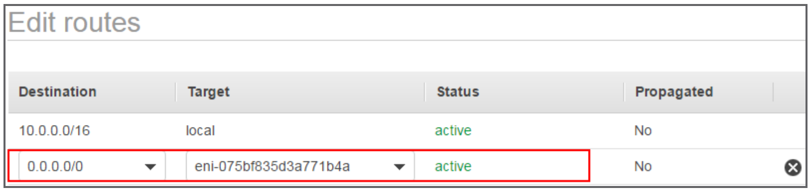
```
SG-6000(B)(config)#
SG-6000(B)(config)#
SG-6000(B)(config)#
SG-6000(B)(config)#
SG-6000(B)(config)#
SG-6000(B)(config)#
SG-6000(B)(config)# _
```

- When the two devices have been successfully negotiated, you only need to configure the master device and the configurations will automatically synchronize to the backup device.

- When vfw-A fails to forward traffic or its ethernet0/2 is disconnected, vfw-B will switch to the master device and start to forward traffic without interrupting user's communication.

Step 9: Configuring the Routing of Web-server on AWS

1. In the VPC Dashboard, select “Route Tables” and enter the routes page.
2. Click **Create route table**, and add a route " “VM_sevice" for VPC1.
3. Select the route "VM_sevice" created in the previous step, click the <Routes> tab at the bottom of the page, and then click **Edit routes**.
4. In the <Edit routes> page, click **Add route** and add a route whose nexthop is the network interface of the Secondary IP address of vfw-A .



Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	eni-075bf835d3a771b4a	active	No

5. In VPC Dashboard, select "subnets" to enter the subnet page, and select the subnet "server_net" of web-server.
6. Click "Route tables" tab at the bottom of page, and then click “Edit” .
7. In the <Route Table ID>drop-down list , select the route item created in step 1-4.

Step 10: Configure Routing, NAT and Security Policies on CloudEdge

You can configure the web-server's inbound and outbound traffic through the CloudEdge instance in the HA deployment scheme to ensure the high reliability of server's business. The configurations are as follows:

1. Configure the source NAT rule on the master device vfw-A, and the source address of the traffic in the web-server network segment will be to translate into the IP of interface eth0/2, i.e., the Secondary IP: 10.0.1.242.

   Command:

   ```
   SG-6000(M)(config-vrouter)# snatrule from 10.0.2.209/24 to any service any eif ethernet0/2 trans-to eif-ip mode dynamicport
   ```

2. Configure the destination NAT rule on the vfw-A, and the destination IP address of the traffic whose destination address is the secondary IP will be translated into the IP address of web-server 10.0.2.209.

   Command:

   ```
   SG-6000(M)(config-vrouter)# dnatrule from any to 10.0.1.1.242 service any trans-to 10.0.2.209
   ```

3. Configure a security policy rule on vfw-A that allows all traffic to pass.

   Command:

   ```
   SG-6000(M)(config-policy)# rule from any to any service any permit
   ```

4. After the configurations, web-server will not need to be bound with the elastic IP. The intranet address of web-server will be translated to the secondary IP of the vfw_service_net subnet of CloudEdge through DNA T rules, and Internet users can access the server by accessing the public address of secondary IP. At the same time, the source IP address of the traffic sent by web-server to Internet will also be translated to the Secondary IP address of CloudEdge through SNAT rules, so as to protect web-server against external attacks.

Results

When the master device vfw-A fails, the backup device vfw-B will automatically switch to the master device. The secondary IP, routing, information of security policy, source NAT and destination NAT on the original master device will be switched automatically without manual reconfiguration, and the communication will not be affected, thus realizing a high reliable security guarantee for cloud servers.

About how to use StoneOS, refer to StoneOS related documents (click here).

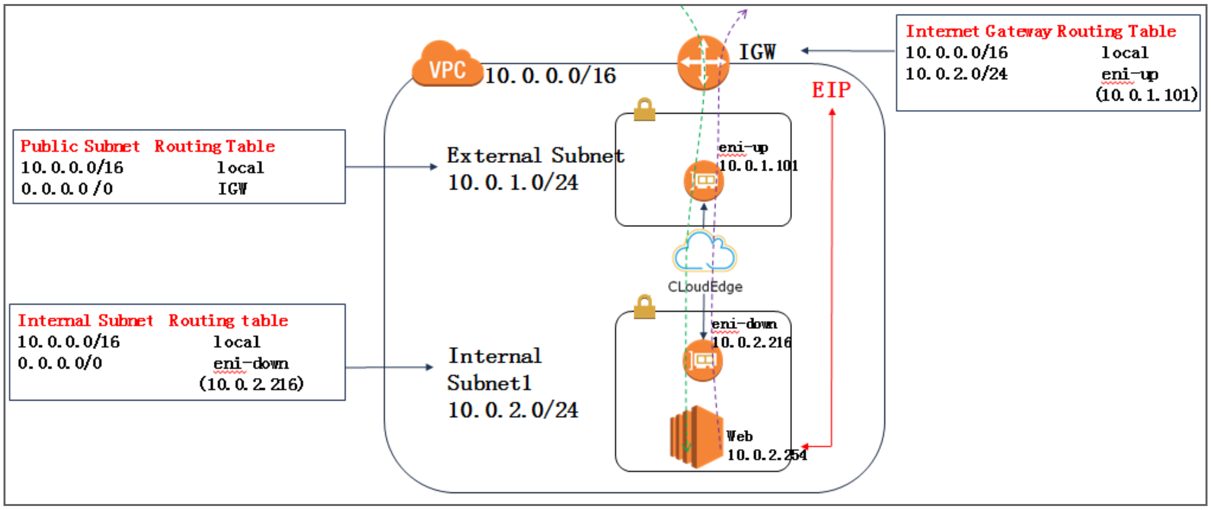
Deploy CloudEdge through Amazon VPC Ingress Routing

Scenarios Introduction

A cloud server "Web-server" has been deployed on the AWS platform in a company. The VPC and subnet of the server are as follows:

- VPC(VPC1)： 10.0.0.0/16
- Subnet 0 （Internal Subnet1） ： 10.0.2.0/24
- Web-server IP： 10.0.2.254, （EIP） :52.83.163.91

Now we need to deploy a CloudEdge virtual firewall, and through Amazon VPC ingress routing, we can provide security protection for the cloud server "Web server". According to this scenario, the deployed network topology and routing plan are as follows:



Public Subnet Routing Table	
10. 0. 0. 0/16	local
0. 0. 0. 0 /0	IGW

Internal Subnet Routing table	
10. 0. 0. 0/16	local
0. 0. 0. 0/0	eni-down (10. 0. 2. 216)

Internet Gateway Routing Table	
10. 0. 0. 0/16	local
10. 0. 2. 0/24	eni-up (10. 0. 1. 101)

Deployment Steps

Step 1: Creating VPC and Subnet

Log in to the AWS console (click here) with your AWS account to create the subnet (External Subnet： 10.0.1.0/24) in the VPC1. For details, see Adding subnets into VPC. After the creation, the VPC and subnet on the AWS are as follows:

- VPC(VPC1)： 10.0.0.0/16
- Subnet 0 （Internal Subnet1） ： 10.0.2.0/24
- Subnet 1 （External Subnet） ： 10.0.1.0/24
- Web-server IP： 10.0.2.254 , EIP:52.83.163.91

Step 2: Creating EC2 Instances

Create one CloudEdge instance on AWS, and configure network interface 1 as Subnet Subnet1 (External Subnet) : 10.0.1.0/24, network interface 2 as Subnet 0 (Internal Subnet1) : 10.0.2.0/24 . For details , refer to Deploying CloudEdge on AWS.

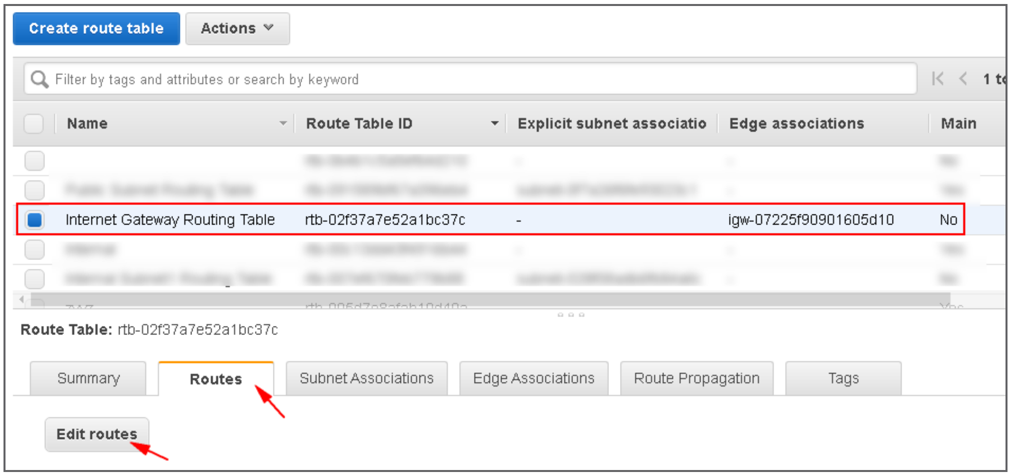
Step 3: Creating and Enabling Internet Gateway

Create an Internet gateway for instances in a VPC to communicate with the Internet. For details, take the following steps:

1. In the VPC Dashboard, select **Internet Gateway**, and click **Create internet gateway**.
2. In the <**Create internet gateway**> page, type the tag "test_IGW".
3. Click **Create** to save the above configurations.
4. In the Internet gateway list, select **the test_IGW** item. Then click the **Actions** drop-down list, select **Attach to VPC**, and select "VPC1" created in step 1 .

Step 4: Creating Internet Gateway Route Table

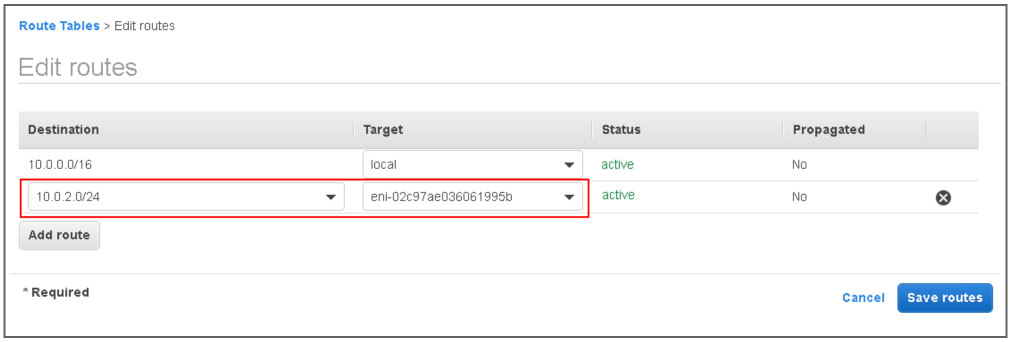
1. In the VPC Dashboard, select **Route Tables**, and click **Create route table** to create "Internet Gateway Routing Table"in the VPC1.
2. In the routing table list, select the **Internet Gateway Routing Table** created in the previous step, then click the <**Routes**> tab at the bottom of the page, and then click the **Edit routes** .



Name	Route Table ID	Explicit subnet associatio	Edge associations	Main
Internet Gateway Routing Table	rtb-02f37a7e52a1bc37c	-	igw-07225f90901605d10	No

Route Table: rtb-02f37a7e52a1bc37c

3. In <**Edit routes**> Page, click **Add route** to add a route whose next hop to subnet 10.0.2.0/24 is the interface 1 (10.0.1.0/24) of CloudEdge .

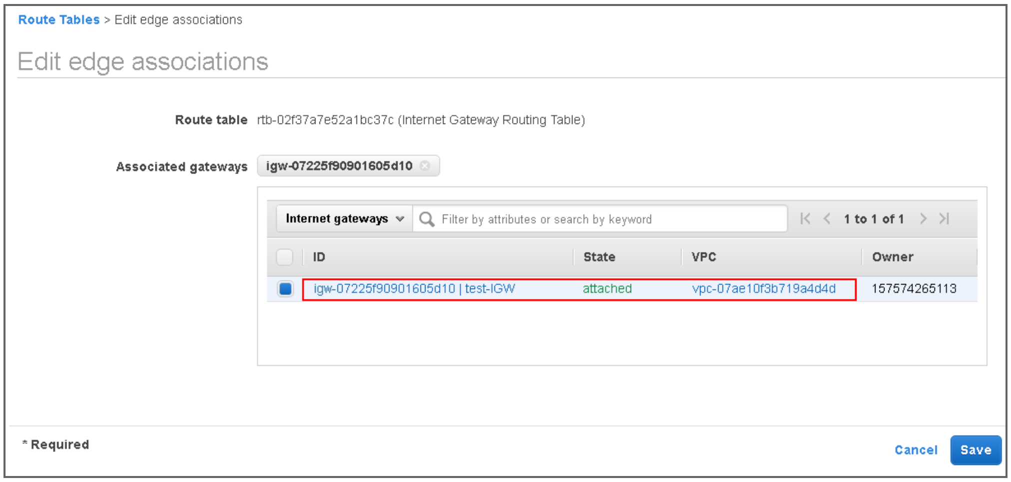


Route Tables > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
10.0.2.0/24	eni-02c97ae036061995b	active	No

4. Click the < **Edge Association** > tab ,and then click the **Edit Edge Association** , then select the created IGW (test-igw) for binding.



Route Tables > Edit edge associations

Edit edge associations

Route table rtb-02f37a7e52a1bc37c (Internet Gateway Routing Table)

Associated gateways igw-07225f90901605d10

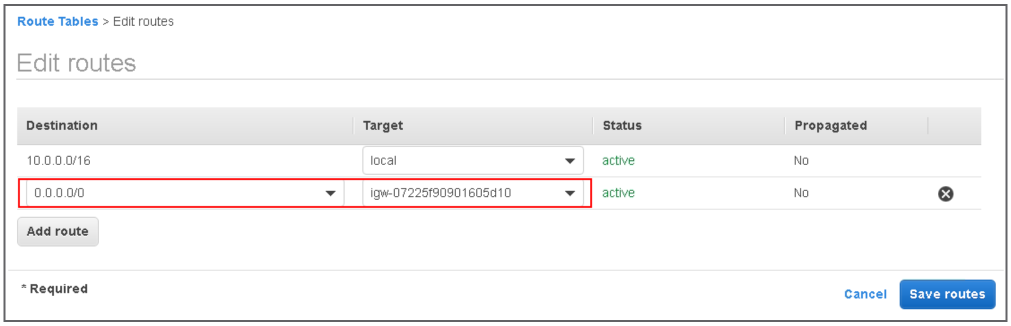
ID	State	VPC	Owner
igw-07225f90901605d10 | test-IGW	attached	vpc-07ae10f3b719a4d4d	157574265113

Step 5: Creating Public Subnet Route Table

1. In the VPC Dashboard, select **Route Tables**. Click **Create route table**, and create " Public Subnet Routing Table" in the VPC1。

2. In the routing table list, select the **Public Subnet Routing Table** created in the previous step, then click the <**Routes**> tab at the bottom of the page, and then click the **Edit routes** .

3. In <**Edit routes**> Page, click **Add route** to add a route whose next hop to subnet 0.0.0.0/0 is the IGW(test_IGW) .

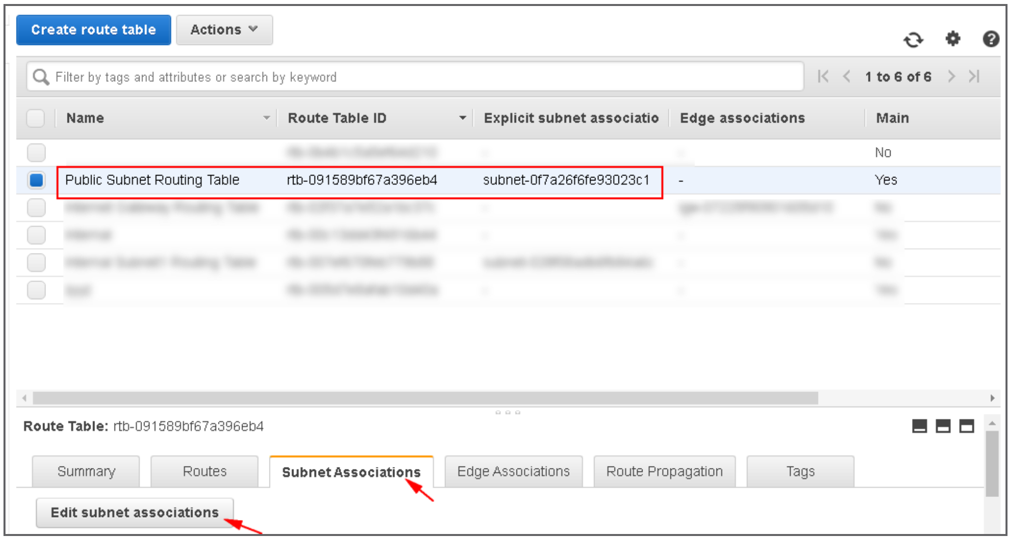


Route Tables > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	igw-07225f90901605d10	active	No

4. Click the < **Subnet Associations**> tab ,and then click the **Edit Subnet Associations** , then select subnet 1 (External Subnet) : 10.0.1.0/24.for binding.



Name	Route Table ID	Explicit subnet associatio	Edge associations	Main
	[redacted]	-	-	No
Public Subnet Routing Table	rtb-091589bf67a396eb4	subnet-0f7a26f6fe93023c1	-	Yes
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Route Table: rtb-091589bf67a396eb4

Step 6: Creating Internal Subnet Route Table

1. In the VPC Dashboard, select **Route Tables**.Click **Create route table**, and create " Internet Gateway Routing Table" in the VPC1。

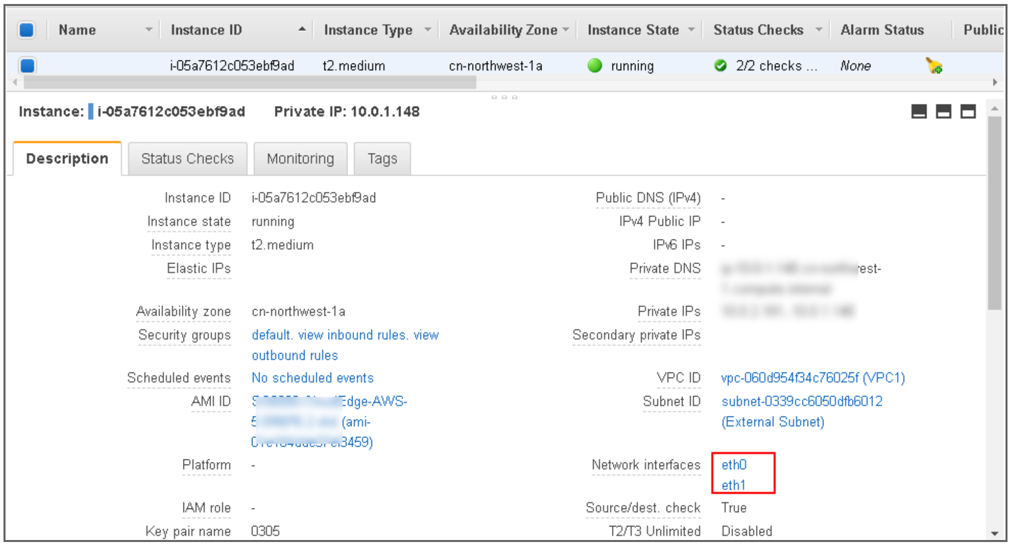
2. In the routing table list, select the i**nternal Gateway Routing Table** created in the previous step, then click the <**Routes**> tab at the bottom of the page, and then click the **Edit routes** .

3. In <**Edit routes**> Page, click **Add route** to add a route whose next hop to subnet 0.0.0.0/0 is the interface 2 (10.0.2.0/24) of CloudEdge

4. Click the < **Subnet Associations**> tab ,and then click the **Edit Subnet Associations** , then select subnet 0 （Internal Subnet1） ： 10.0.2.0/24 for binding.

Step 7: Changing Source/Dest. Check

1. Select the **Services > Compute > EC2**, and in the navigation, select I**NSTANCES > Instances**, and select the CloudEdge instance (test_EC2) created in the step 1, and in the details page below, click the links of network interfaces 1 and 2.



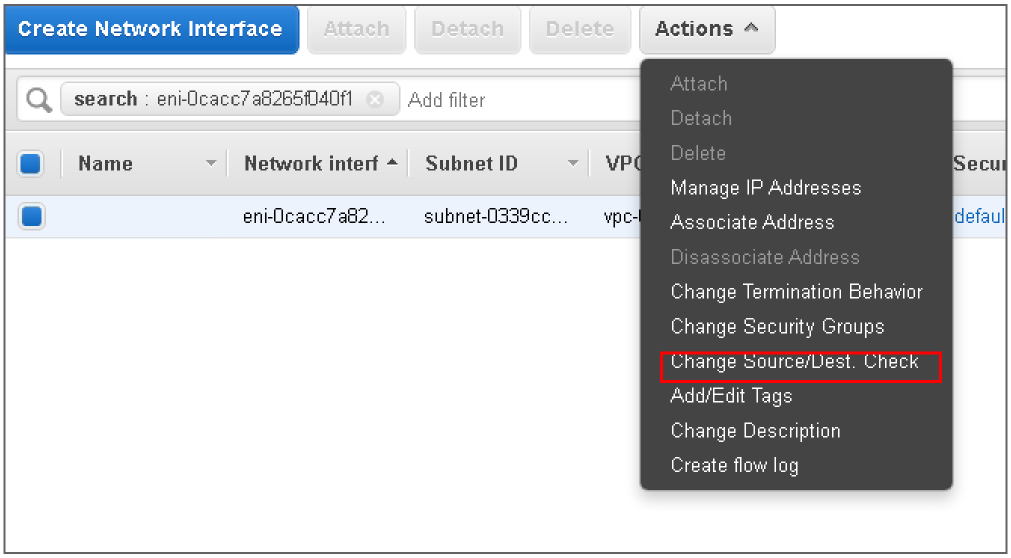
Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public
	i-05a7612c053ebf9ad	t2.medium	cn-northwest-1a	● running	✓ 2/2 checks ...	None	

Instance: i-05a7612c053ebf9ad **Private IP: 10.0.1.148**

Instance ID	i-05a7612c053ebf9ad	Public DNS (IPv4)	-
Instance state	running	IPv4 Public IP	-
Instance type	t2.medium	IPv6 IPs	-
Elastic IPs		Private DNS	[redacted]est- [redacted]
Availability zone	cn-northwest-1a	Private IPs	[redacted]
Security groups	default. view inbound rules. view outbound rules	Secondary private IPs	
Scheduled events	No scheduled events	VPC ID	vpc-060d954f34c76025f (VPC1)
AMI ID	S[redacted]Edge-AWS-5[redacted] (ami-0[redacted]3459)	Subnet ID	subnet-0339cc6050dfb6012 (External Subnet)
Platform	-	Network interfaces	eth0 eth1
IAM role	-	Source/dest. check	True
Key pair name	0305	T2/T3 Unlimited	Disabled

2. Or select **Services > Compute > EC2**, and then in the navigation bar, and select **NETWORK &SECURITY> Network Interfaces**. Find the network interface 1 (subnet 10.0.1.0 / 24) and network interface 2 (subnet 10.0.2.0 / 24) of the CloudEdge instance (test-EC2) created in step 1.

3. Select two network interfaces respectively, and then click **Change Source/Dest. Check** in the "actions" drop-down menu, and then disable the check.



Step 8 : Allocating Elastic IP Addresses

1. In EC2 management console, click **Elastic IPs** from the left navigation.,and allocating elastic IP for CloudEdge instance. For details , refer to "Allocating Elastic IP Addresses" on Page 102

2. In CloudEdge default settings, only the access to eth0. is enabled. So, we will use SSH connection to visit eth0 before we can visit its other ports. For details , refer to Visiting CloudEdge .

Step 9 : Results

At the beginning, you can access the Web UI interface of the CloudEdge through the elastic IP of itself, which is successful; And you can access web server through the elastic IP of the itself, which is unsuccessful. Continue to configure the policy on CloudEdge for result verification :

- After creating a policy on CloudEdge that allows all the released traffic to pass, the Internet users can normally access the web server through elastic IP; And after configuring a policy that prevents the Internet users from accessing the web server, the Internet users can no longer access the web server. It indicates that the incoming traffic can be safely controlled by the CloudEdge.

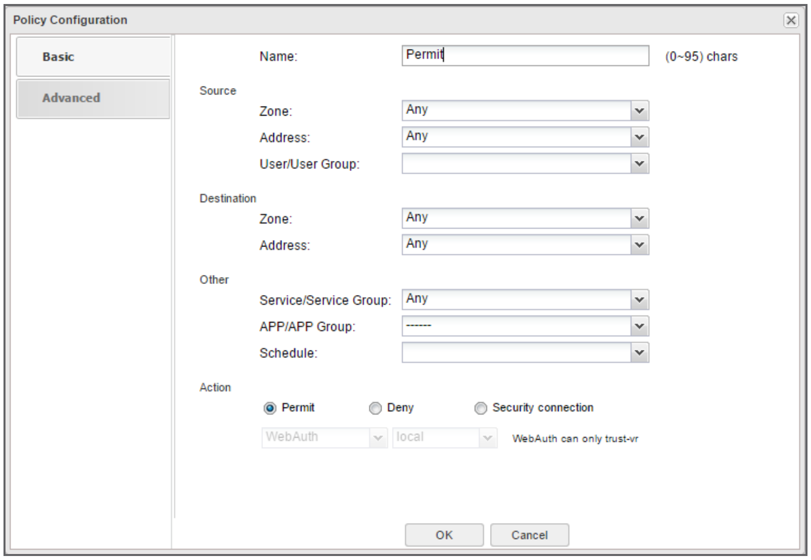
- After creating a policy on CloudEdge that allows all the released traffic to pass, the web address of the extranet can be visited on the web server successfully. And after configuring a policy to prevent the web server VM from accessing the extra-net, the extra-net can be no longer visited on the web server. It indicates that the traffic in the out direction can also be protected by CloudEdge.

> **Notes:** the eth0/1 (belongs to Internal Subnet1of the service network) can not obtain an IP address automatically. Therefore, you need configure a private IP address assigned by the AWS platform for eth0/1 on the CloudEdge Console before verifying the result. You can view the private IP address on the cloud instance details page.

To create a policy rule that allows all traffics from and to all directions:

1. Select **Policy > Security Policy**.

2. Create a security policy that allows all types of traffic (every field is set to **Any**).



Policy Configuration

Name: Permit (0~95) chars

Source

Zone: Any

Address: Any

User/User Group:

Destination

Zone: Any

Address: Any

Other

Service/Service Group: Any

APP/APP Group: ------

Schedule:

Action

● Permit ○ Deny ○ Security connection

WebAuth local WebAuth can only trust-vr

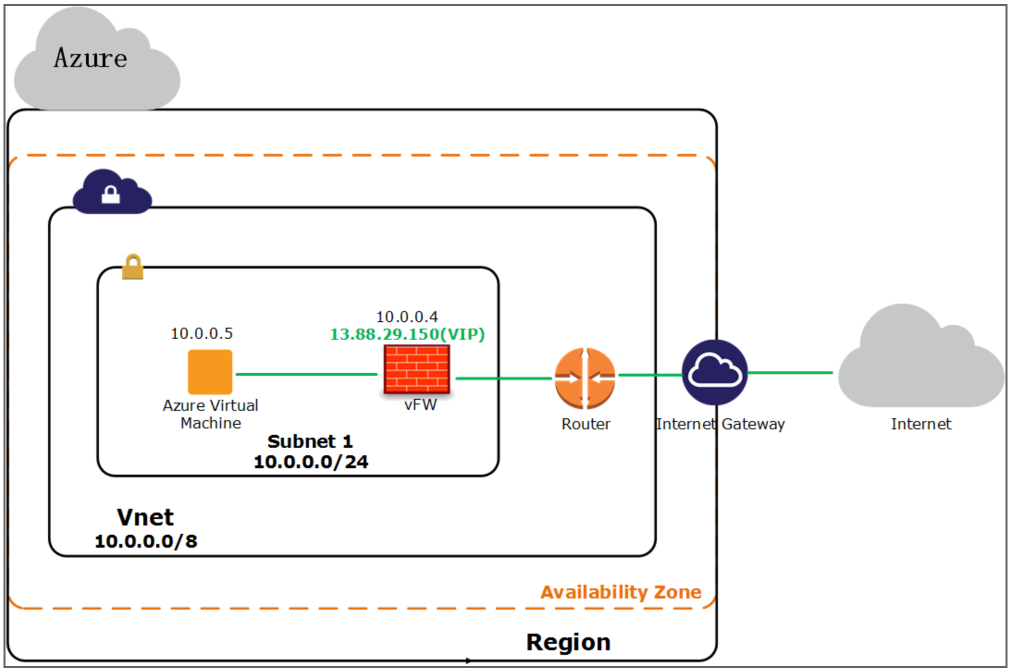
3. Click **OK**.
4. The policy of forbidding Internet users to access web server and web server to access Internet can be configured according to the actual IP address.

About how to use StoneOS, refer to StoneOS related documents (click here).

Deploying CloudEdge on Azure

Typical Scenarios

This guide describes how to deploy CloudEdge virtual firewall (vFW) on Azure as Internet gateway. In this example, CloudEdge is deployed as a router of Azure Vnet(10.0.0.0/8) which contains a subnet (10.0.0.0/24) , and it controls the outbound and inbound traffic of the subnet. The following is the network topology:

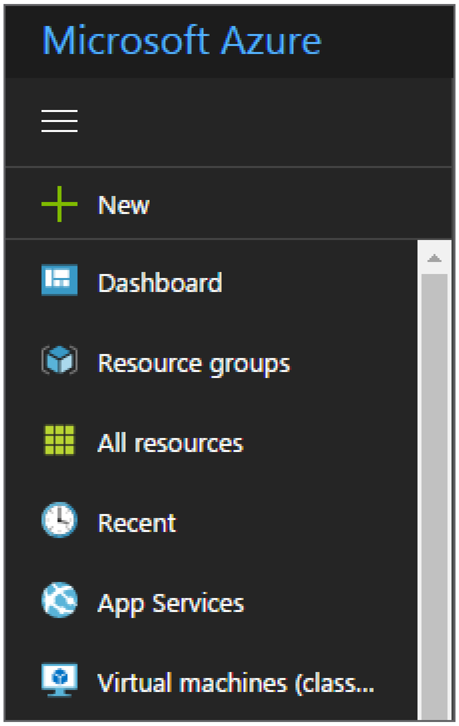


Installing CloudEdge

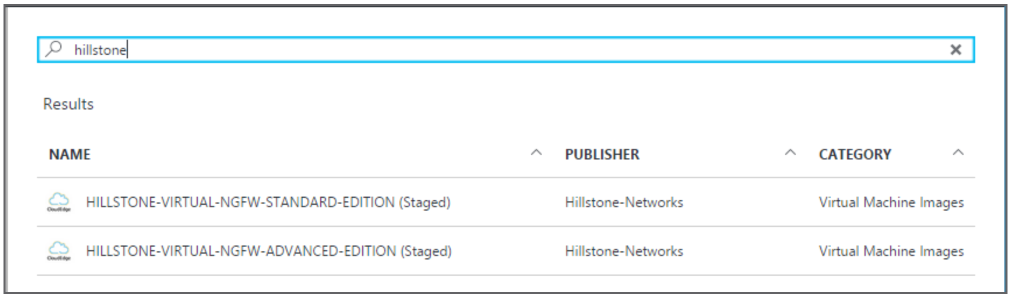
CloudEdge will be running in a virtual machine of the Azure Vnet. After installation, you will have a running virtual StoneOS system which you can visit via CLI and WebUI.

Step 1: Purchasing CloudEdge and Creating a virtual machine

1. Log into Microsoft Azure. Select **Virtual machines** in the left navigation pane, and then click **+New** on the top of the right page.



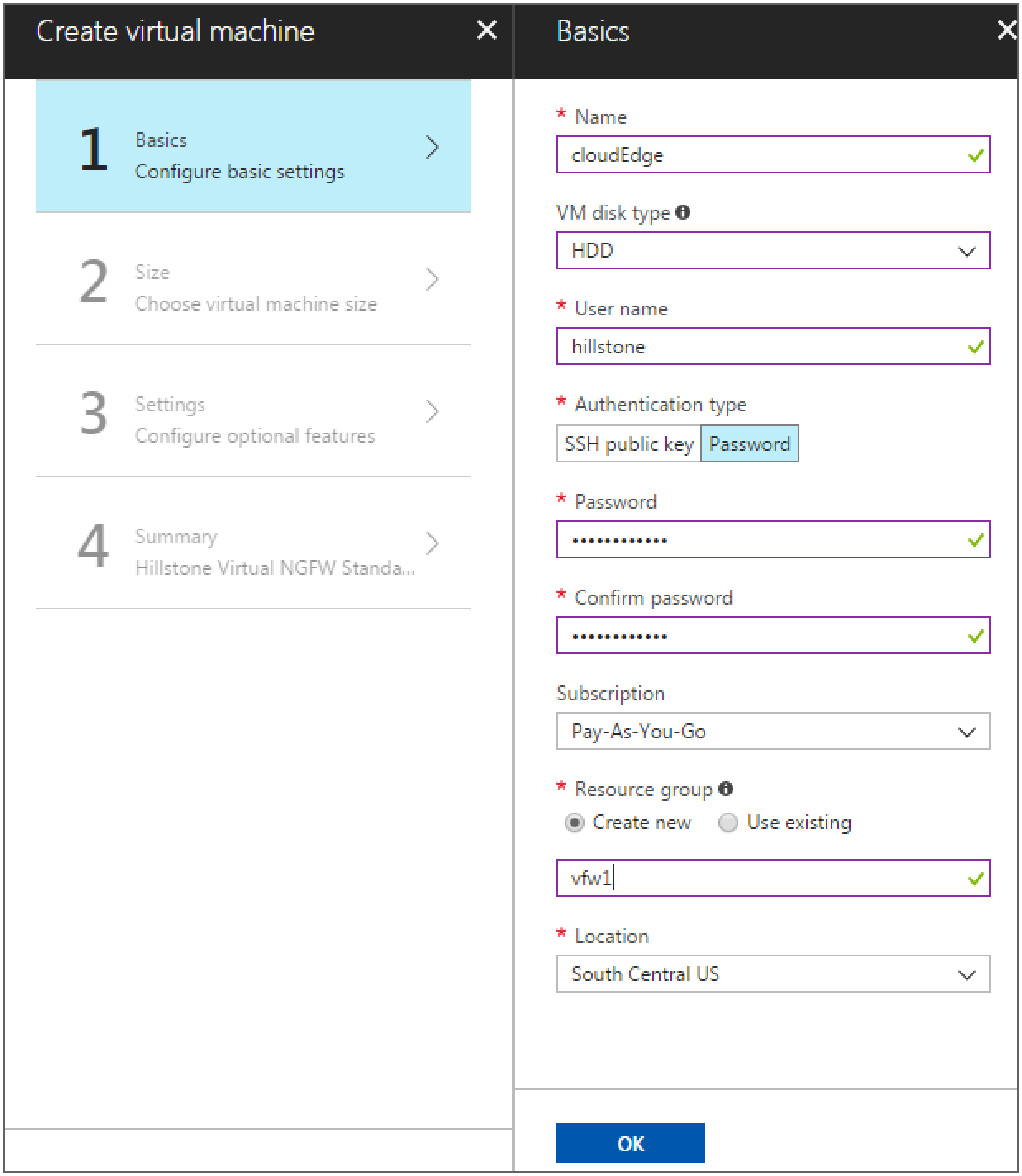
2. Type "hillstone" in the Search box. Select the CloudEdge version you need in the searching results list, and then click **Create** in the pop-up window.


hillstone

Results

NAME	PUBLISHER	CATEGORY
HILLSTONE-VIRTUAL-NGFW-STANDARD-EDITION (Staged)	Hillstone-Networks	Virtual Machine Images
HILLSTONE-VIRTUAL-NGFW-ADVANCED-EDITION (Staged)	Hillstone-Networks	Virtual Machine Images

3. In the Basics page, configure the settings as follows, and then click **OK**.



Create virtual machine
1 Basics
Configure basic settings
2 Size
Choose virtual machine size
3 Settings
Configure optional features
4 Summary
Hillstone Virtual NGFW Standa...
Basics

* Name: cloudEdge

VM disk type: HDD

* User name: hillstone

* Authentication type: SSH public key [✓ Password]

* Password: ••••••••••••

* Confirm password: ••••••••••••

Subscription: Pay-As-You-Go

* Resource group: ● Create new ○ Use existing

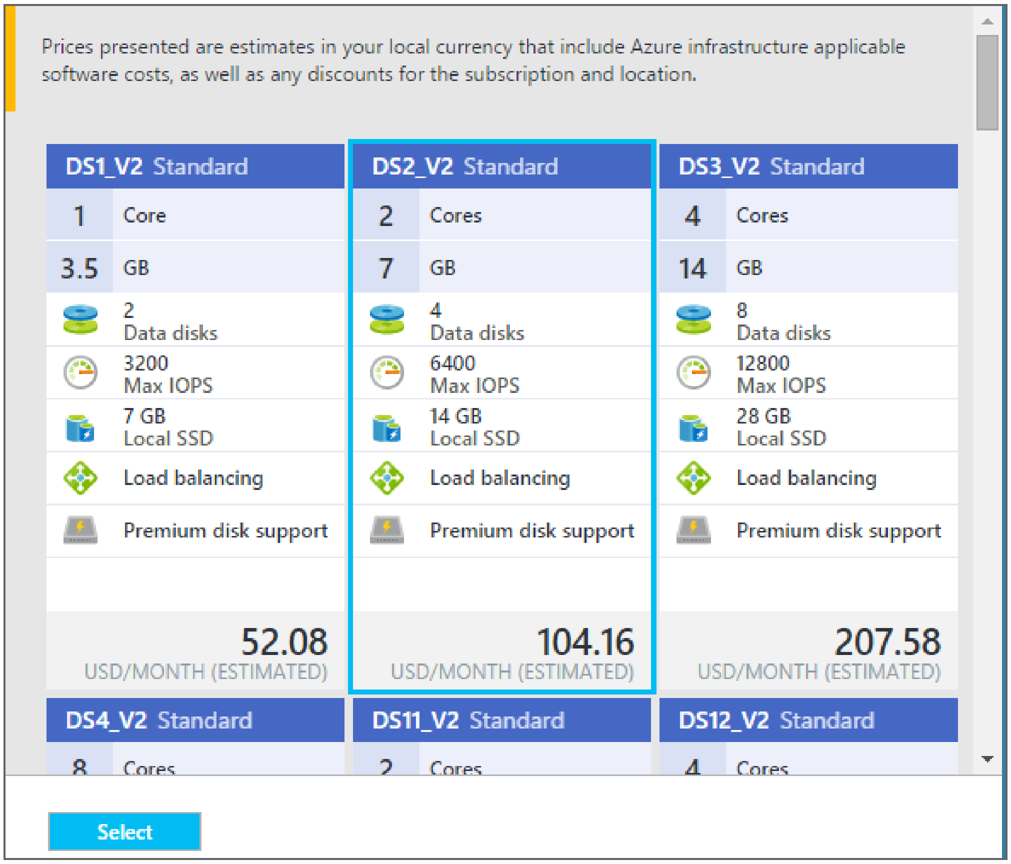
vfw1

* Location: South Central US

Notes:

- If you specify the username as hillstone and change the password, the system will update the password; if the new created username is not hillstone, the system will update the password which belongs to the hillstone user to the new, and a new user will be created, the password will be the same as hillstone user.
- If a resource group has been created , you can use the existing one; otherwise, you can create a new resource group.

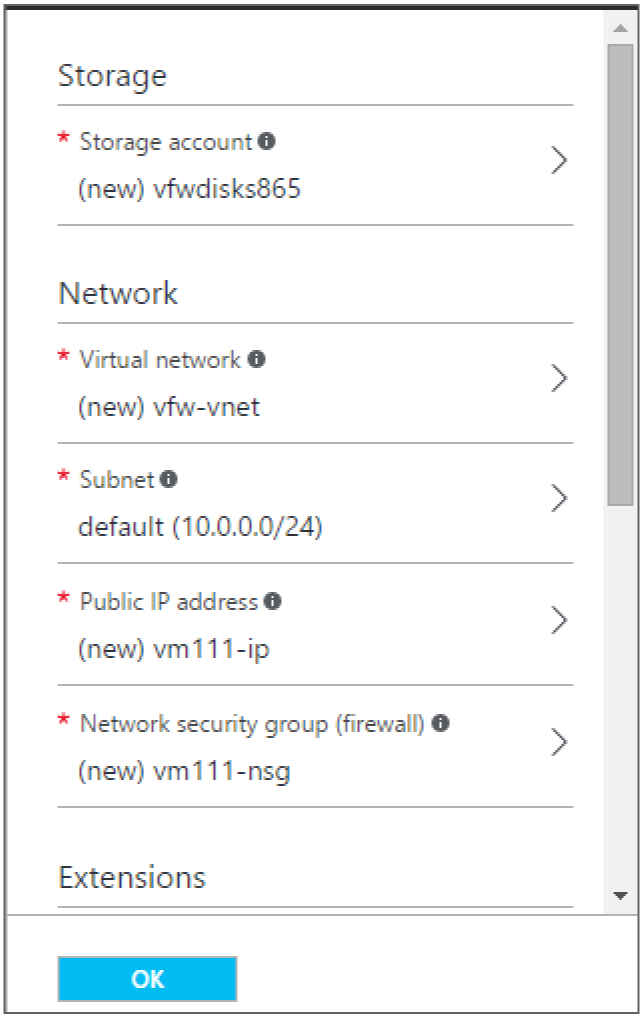
4. In the Size page, choose virtual machine size according to your CloudEdge version, and then click **Select**.



Prices presented are estimates in your local currency that include Azure infrastructure applicable software costs, as well as any discounts for the subscription and location.

DS1_V2 Standard	DS2_V2 Standard	DS3_V2 Standard
1 Core	2 Cores	4 Cores
3.5 GB	7 GB	14 GB
2 Data disks	4 Data disks	8 Data disks
3200 Max IOPS	6400 Max IOPS	12800 Max IOPS
7 GB Local SSD	14 GB Local SSD	28 GB Local SSD
Load balancing	Load balancing	Load balancing
Premium disk support	Premium disk support	Premium disk support
52.08 USD/MONTH (ESTIMATED)	104.16 USD/MONTH (ESTIMATED)	207.58 USD/MONTH (ESTIMATED)
DS4_V2 Standard	**DS11_V2 Standard**	**DS12_V2 Standard**
8 Cores	2 Cores	4 Cores

5. In the Settings page, configure the settings as follows, and then click **OK**.



Storage

* Storage account

(new) vfwdisks865

Network

* Virtual network

(new) vfw-vnet

* Subnet

default (10.0.0.0/24)

* Public IP address

(new) vm111-ip

* Network security group (firewall)

(new) vm111-nsg

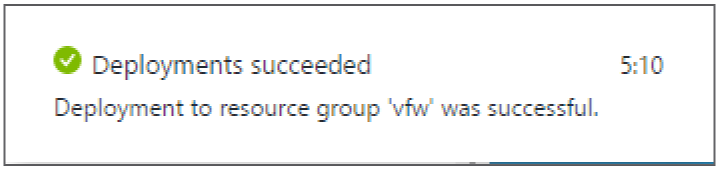
Extensions

The above items will be created or allocated automatically, including storage account, virtual network, public IP address, network security group and diagnostics storage account . If you want to edit them, click > in the right side.

6. Check the detailed configurations in the Summary page, and then click **OK**.

7. Click **Purchase** to pay for the virtual machine in the Buy page.

   After a few minutes, the virtual machine will be deployed successfully.

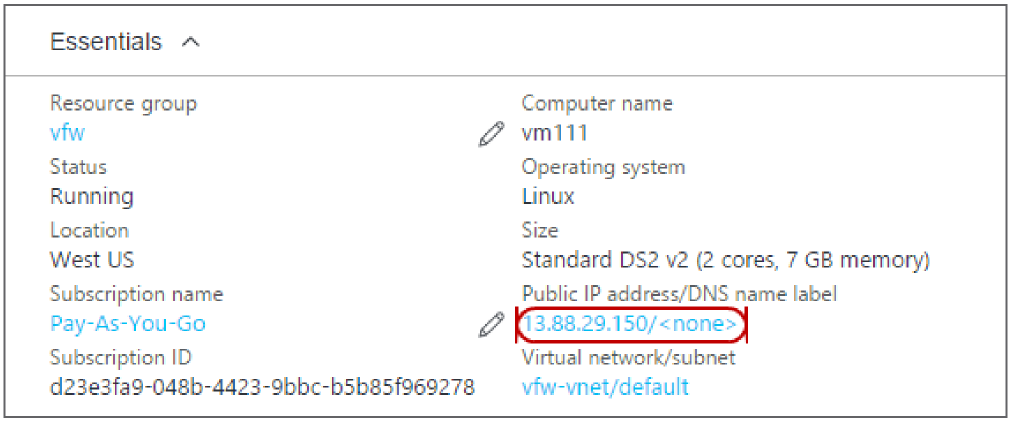


✓ Deployments succeeded 5:10

Deployment to resource group 'vfw' was successful.

Step 2: Viewing Public IP Address

In the pop-up new virtual machine window, you can view the public IP address of CloudEdge in the Essentials tab.



Essentials ^

Resource group
vfw

Status
Running

Location
West US

Subscription name
Pay-As-You-Go

Subscription ID
d23e3fa9-048b-4423-9bbc-b5b85f969278

Computer name
vm111

Operating system
Linux

Size
Standard DS2 v2 (2 cores, 7 GB memory)

Public IP address/DNS name label
13.88.29.150/<none>

Virtual network/subnet
vfw-vnet/default

Step 3: Visiting CloudEdge

After virtual machine is created successfully, CloudEdge will be started automatically.

To Login CloudEdge via SSH2

1. Open a remote terminal login software. We will use SecureCRT as an example.
2. Click **File > Quick Connect** , and then select **SSH2** in Protocol drop-down menu.
3. Enter the public IP address in Hostname text box.

4. Enter username(azure).

5. Click **Connect** to connect this session.

6. Enter password(The new login password). Press the **Enter** key to log in.

To Login CloudEdge via HTTPS

1. Open the browser and enter **https://13.88.29.150** in the address bar.

2. Enter the username(azure) and password(The new login password) on the login page.

3. Press the **Enter** key to log in.

Step 4: Purchasing and Applying for License Software

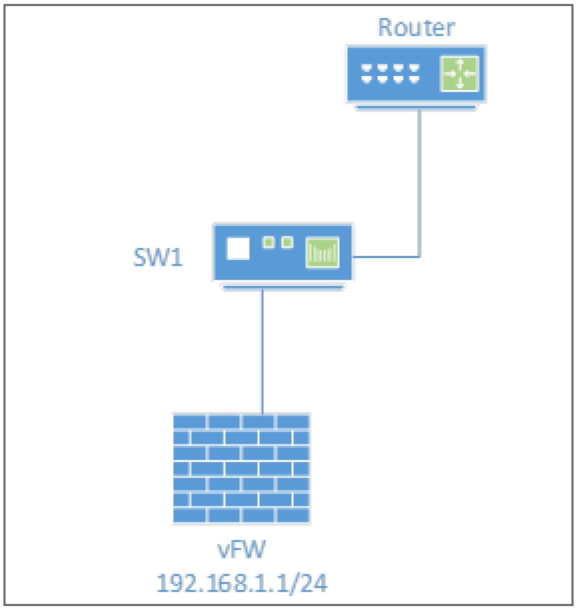
After you purchased CloudEdge, CloudEdge Licenses are also needed, which ensure CloudEdge run normally in Azure. Contact Hillstone salesperson to buy the license you need. To install the license in CloudEdge, see "Installing License" on Page 8

Deploying CloudEdge on Alibaba Cloud

Preparation

- Create an VPC as follows:
  - VPC:192.168.0.0/16
  - Subnet 0： 192.168.1.0/24
- Create a security group, and configure security group rules

After CloudEdge is deployed, the network topology is:



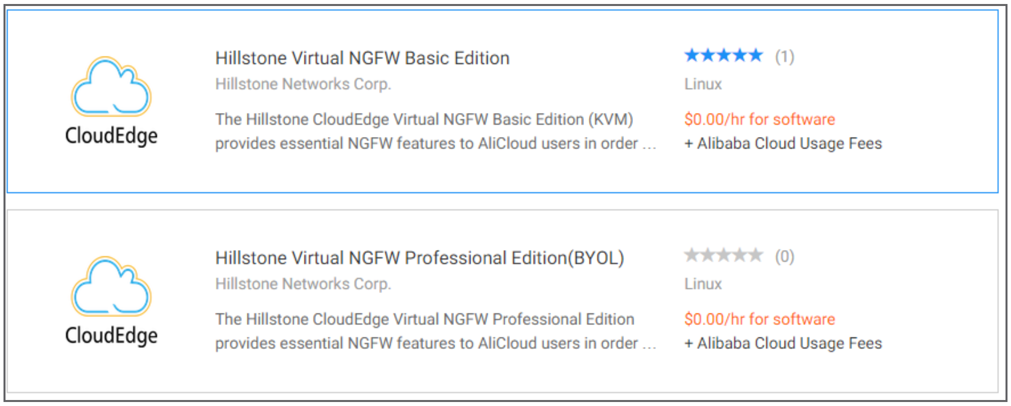
Installing vFW

CloudEdge will be installed with an ECS instance in VPC.

Step 1: Purchase vFW Images and Create an ECS Instance

1. Log into the Alibaba Cloud marketplace, enter a keyword such as "Hillstone" in the search box at the upper-right corner. Select the vFW version you need in the search results list.

   vFW image version includes the following two types: pay-on-demand and BYOL(Buy Your Own License).

   Hillstone Virtual NGFW Basic Edition
   Hillstone Networks Corp.
   The Hillstone CloudEdge Virtual NGFW Basic Edition (KVM) provides essential NGFW features to AliCloud users in order ...
   ★★★★★ (1)
   Linux
   $0.00/hr for software
   + Alibaba Cloud Usage Fees

   Hillstone Virtual NGFW Professional Edition(BYOL)
   Hillstone Networks Corp.
   The Hillstone CloudEdge Virtual NGFW Professional Edition provides essential NGFW features to AliCloud users in order ...
   ☆☆☆☆☆ (0)
   Linux
   $0.00/hr for software
   + Alibaba Cloud Usage Fees

2. Browse the detailed information about the product, then click **Choose Your Plan** to set specification parameter of ECS instance.

3. Click the **Quick Buy** tab.

4. Choose image version in VERSION area, the latest version is recommended.

5. Choose the physical location of the ECS instance in REGION area.

6. Choose the ECS instance type you need in ECS INSTANCE TYPE area, the detailed instance specification will displayed on the right.

7. Select VPC network type in NETWORK area.

   If you don't have a VPC currently, click **Create VPC** below.

8. Click **Agree Terms and Buy Now** to pay for the ECS instance.

   Wait for a moment, ECS instance can be created successfully.

Step 2: View initial configuration of vFW

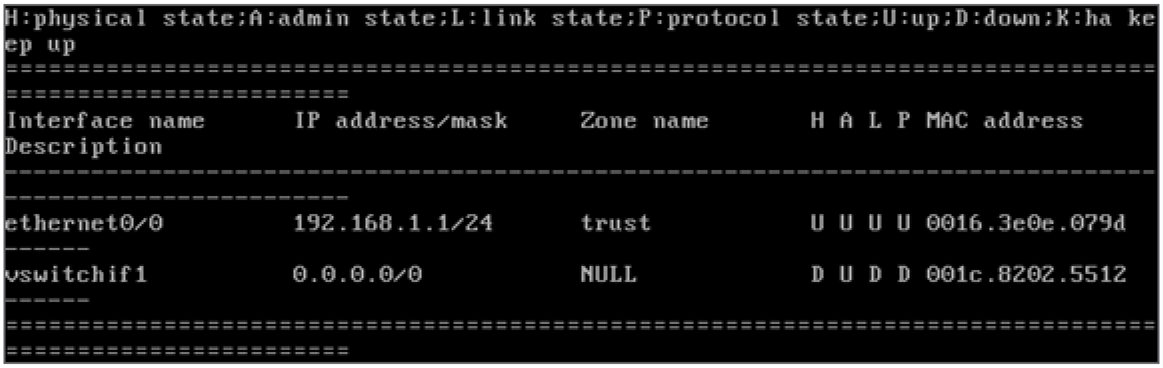
1. After an ECS instance is created successfully, vFW will start automatically.
2. Select **Elastic Compute Service** in the left navigation pane, then click **Instances** item on the left. Instance list will be shown in the right page.
3. Click **More** in Action column of ECS instance which vFW is running in. Then select **Reset Password** to reset the login password of vFW.

   Enter a new login password and confirm password, then click **Submit**. The default login password (hillstone) will be modified so as to enhance the security of the system.
4. Click **More** in Action column of ECS instance which vFW is running in. Then select **Connect to Management Terminal** to login with console.

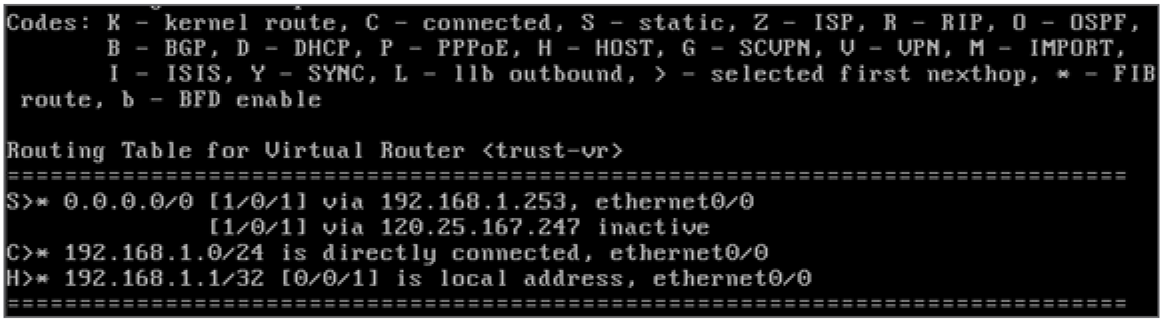
   AlibabaCloud will provide an initial password to login management terminal, make sure keep this password in mind.
5. Enter the initial password in the pop-up dialog box.

   If you need to modify the password, please click **Modify management terminal password**.
6. Enter the default username(hillstone) and new login password in CLI.

   By default, the eth0/0 interface can get the IP address from DHCP server automatically, and the system can get the default route. You can execute the **show interface** command and **show IP route** command to view.



```
H:physical state;A:admin state;L:link state;P:protocol state;U:up;D:down;K:ha ke
ep up
================================================================================
========================
Interface name      IP address/mask     Zone name       H A L P MAC address
Description
--------------------------------------------------------------------------------
------------------------
ethernet0/0         192.168.1.1/24      trust           U U U U 0016.3e0e.079d
------
vswitchif1          0.0.0.0/0           NULL            D U D D 001c.8202.5512
------
================================================================================
========================
```

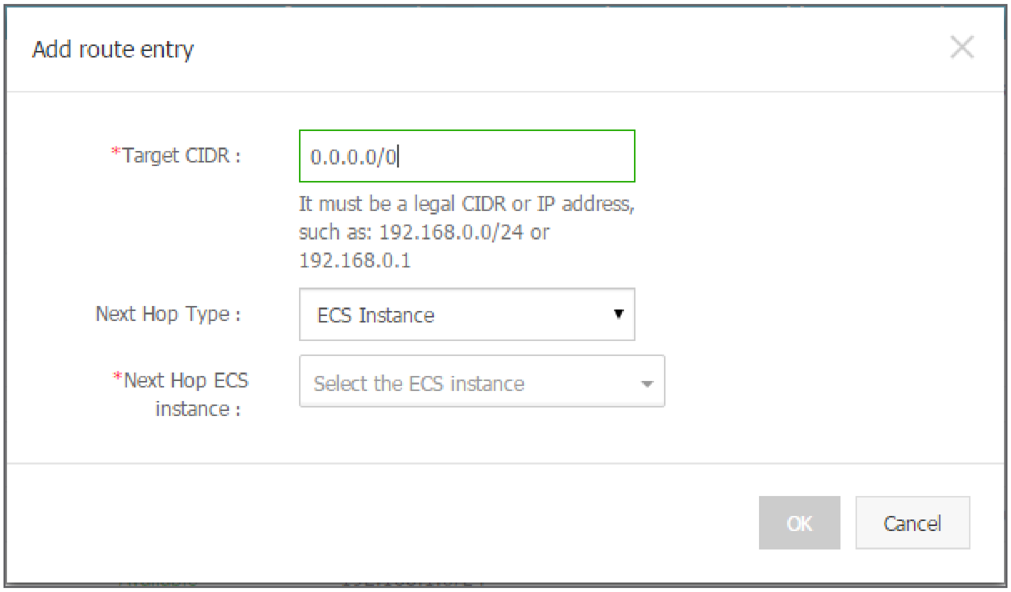


```
Codes: K - kernel route, C - connected, S - static, Z - ISP, R - RIP, O - OSPF,
       B - BGP, D - DHCP, P - PPPoE, H - HOST, G - SCVPN, V - VPN, M - IMPORT,
       I - ISIS, Y - SYNC, L - llb outbound, > - selected first nexthop, * - FIB
 route, b - BFD enable

Routing Table for Virtual Router <trust-vr>
==============================================================================
S>* 0.0.0.0/0 [1/0/1] via 192.168.1.253, ethernet0/0
              [1/0/1] via 120.25.167.247 inactive
C>* 192.168.1.0/24 is directly connected, ethernet0/0
H>* 192.168.1.1/32 [0/0/1] is local address, ethernet0/0
==============================================================================
```

Step 3: Set default route for VPC

1. In the View Console page of Alibaba Cloud, click **Products & Services** at the upper-left corner, then select **Virtual Private Cloud**.
2. Select **VPC** in the left navigation pane, then click **Manage** in Action column of VPC which the vFW belongs to.

3. Select **VRouter** in the left navigation pane, then click **Add route entry** in the upper-right corner of the VRouter info page.



Add route entry

*Target CIDR : 0.0.0.0/0

It must be a legal CIDR or IP address, such as: 192.168.0.0/24 or 192.168.0.1

Next Hop Type : ECS Instance

*Next Hop ECS instance : Select the ECS instance

4. Add a default route entry for VPC, then click **OK**.

   - Target CIDR: Specifies the destination IP address to 0.0.0.0/0.
   - Next Hop Type: Specifies the next hop type to ECS instance.
   - Next Hop ECS Instance: Specifies the ECS Instance which vFW belongs to.

Step 4: Purchase and Apply for License Software

This step is only applicable to the BYOL type of products.

After you purchased BYOL type product, Hillstone next generation virtualization firewall License is also needed, which ensures vFW run normally in Alibaba Cloud. Please contact the Hillstone customer service representatives to get the license software. To install the license software in vFW, see "Installing License" on Page 8

Step 5: Visit the vFW

If you need to visit the vFW from the Internet, the ECS security group should include rules which allow the public network to visit the private network.

To Login vFW via SSH2

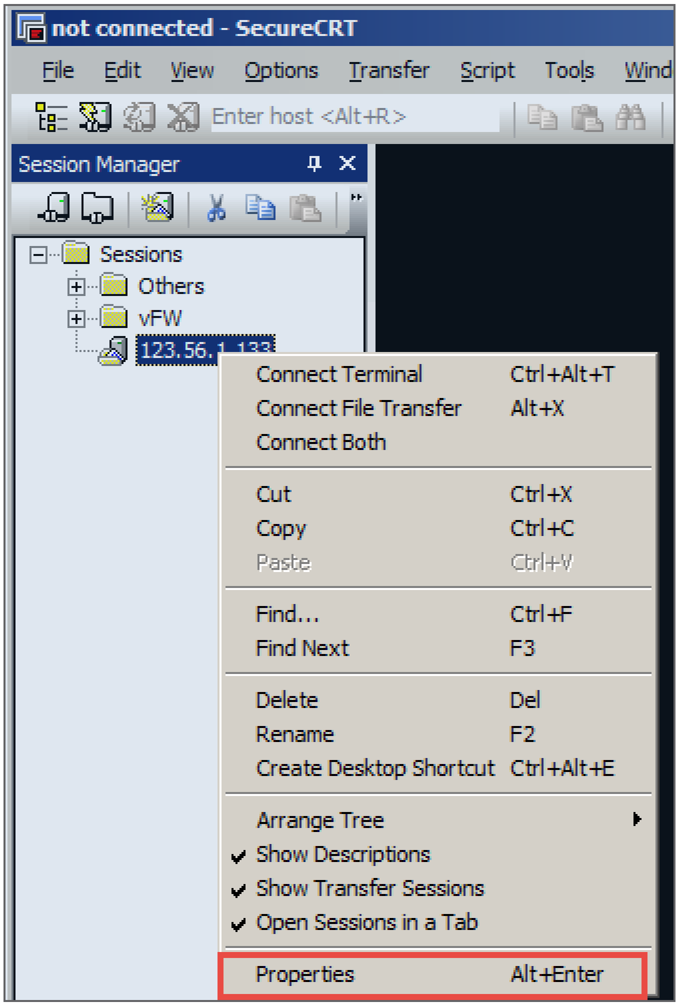
Notes: When you login vFW via SSH2 through SecureCRT or other tools, the 3DES encryption algorithm should be moved to the top. Otherwise, the system will be unable to be connected and the following message will not be prompted: Invalid packet header. This probably indicates a problem with key exchange or encryption.

1. Open the remote terminal login software. We take SecureCRT as an example.

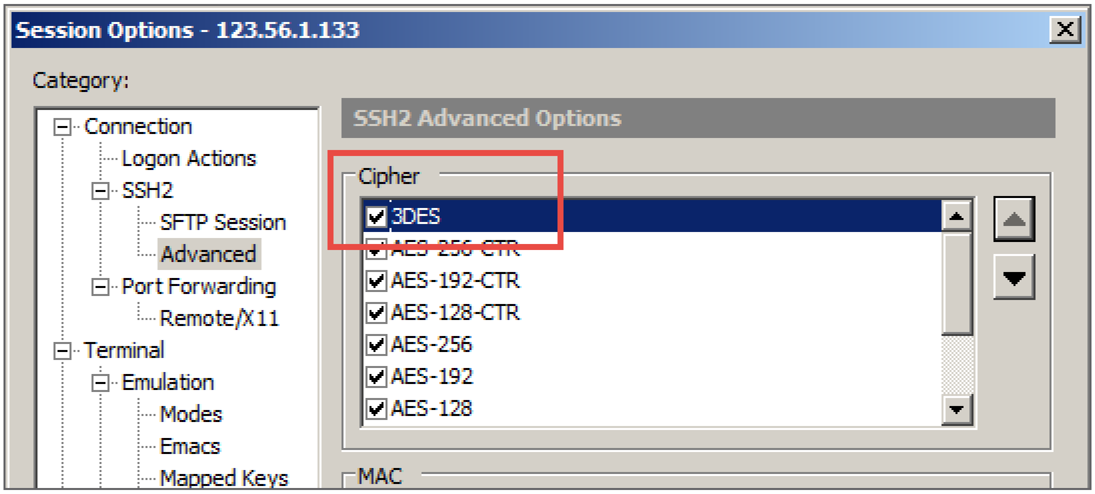
2. Click **File > Quick Connect** , then select **SSH2** in Protocol drop-down menu.

3. Enter the elastic IP address in Hostname text box and click **Connect**.

4. Right-click the new session in Session Manager, then select **Properties**.



5. In the pop-up dialog, select the **Advanced** item on the left, then move the 3DES algorithm to the top.



Cipher

☑ 3DES
☑ AES-256-CTR
☑ AES-192-CTR
☑ AES-128-CTR
☑ AES-256
☑ AES-192
☑ AES-128

6. Click **OK**, and connect this session.

7. Enter username(hillstone) and press the Enter key.

8. Enter password(The new login password). Press the Enter key to log in.

To Login vFW via HTTP

1. Open the browser and enter the elastic IP of vFW.

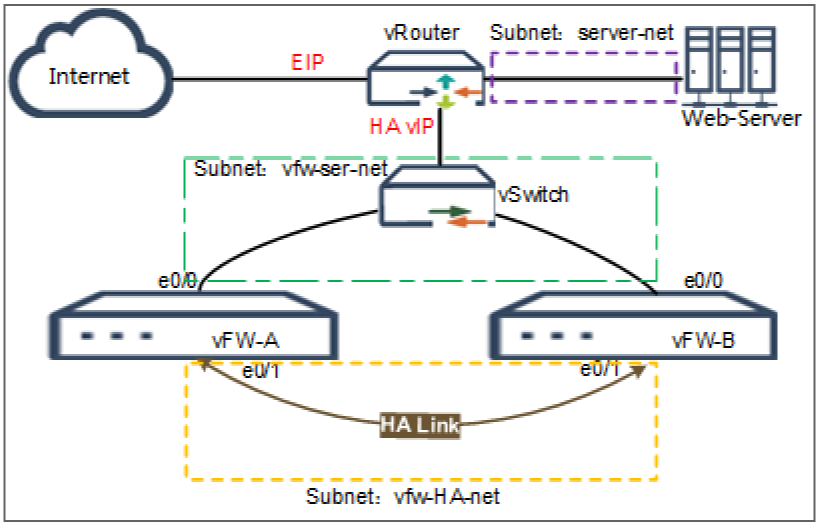
2. Enter the username(hillstone) and password(The new login password) on the login page.

3. Press the Enter key to log in.

Deploying HA Scenarios of CloudEdge via HAVIP on Alibaba Cloud

HA Typical Scenarios

The following topology introduces how to deploy HA scenarios of CloudEdge on Alibaba Cloud. After the deployment, vFW-A will be selected as the master device for forwarding traffic and vFW-B will be selected as the backup device. vFW-A will synchronize its configurations and status data to the backup device vFW-B. When the master device vFW-A failures to forward traffic, the backup device vFW-B will switch to the master device to forward traffic without interrupting user's communication, which can ensure network stability.



According to the topology , you need to configure the followings on Alibaba Cloud:

- 1 Virtual Private Cloud (VPC).
- 3 VSwitches (Subnet). vfw-ser-net and vfw-ha-net subnets, which are used by the CloudEdge instance. (Tips: You need to add another network as HA subnet when creating the CloudEdge instance); subnet for Web-Server: server-net.

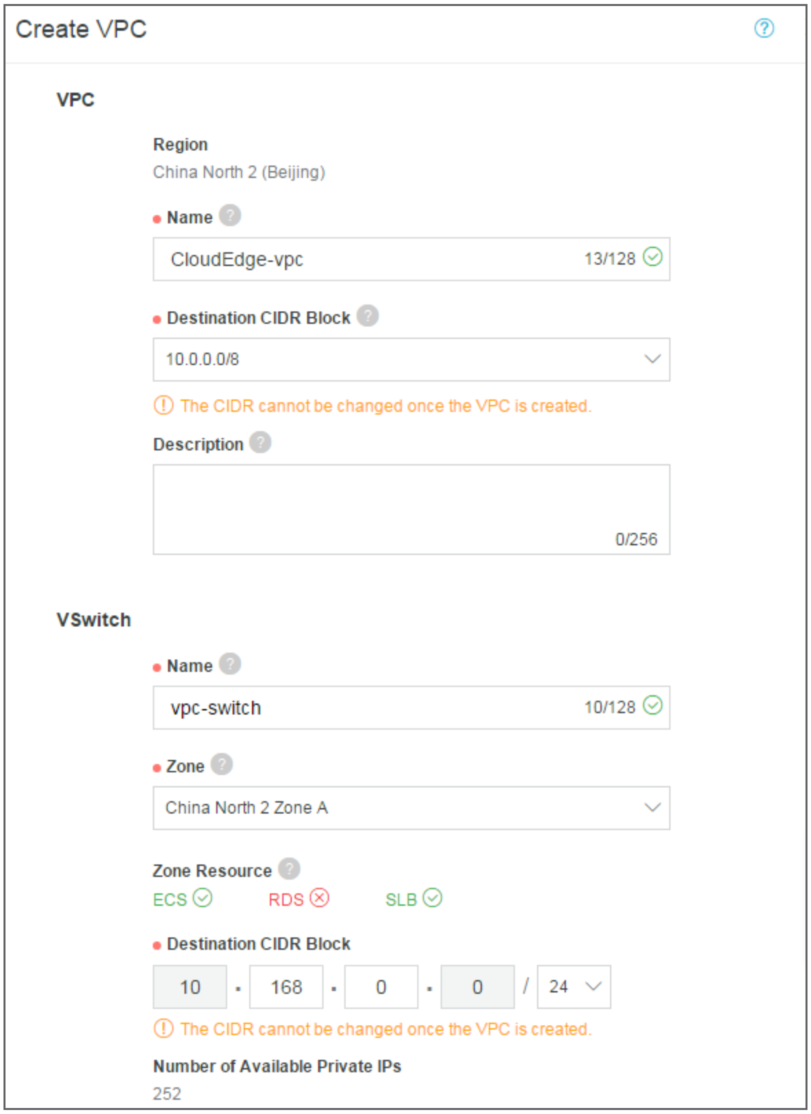
- 3 Elastic Compute Service (ECS) Instances. vFW-A and vFW-B instances for HA deployment; one instance for Web-Server. Three instances need to be on the same VPC.
- 1 Elastic IP（EIP）, which is used to communicate in the Internet.
- 1 HAVIP, which should select the same subnet as the "vfw_ser_net" of the CloudEdge instance.

Deploying HA Scenarios of CloudEdge on Alibaba Cloud

Step 1: Create VPC

1. Log in the Alibaba Cloud , enter the Console page, and select “Virtual Private Cloud >VPC >VPCs” on the left.

2. Click **Create VPC**,and the <Create VPC>dialog box will pop up. Configure as the following example:



Create VPC

VPC

Region
China North 2 (Beijing)

● Name
CloudEdge-vpc 13/128

● Destination CIDR Block
10.0.0.0/8

The CIDR cannot be changed once the VPC is created.

Description
0/256

VSwitch

● Name
vpc-switch 10/128

● Zone
China North 2 Zone A

Zone Resource
ECS ✓ RDS ☒ SLB ✓

● Destination CIDR Block
10 . 168 . 0 . 0 / 24

The CIDR cannot be changed once the VPC is created.

Number of Available Private IPs
252

In the <Create VPC> Dialog Box, Configure the options as follows:

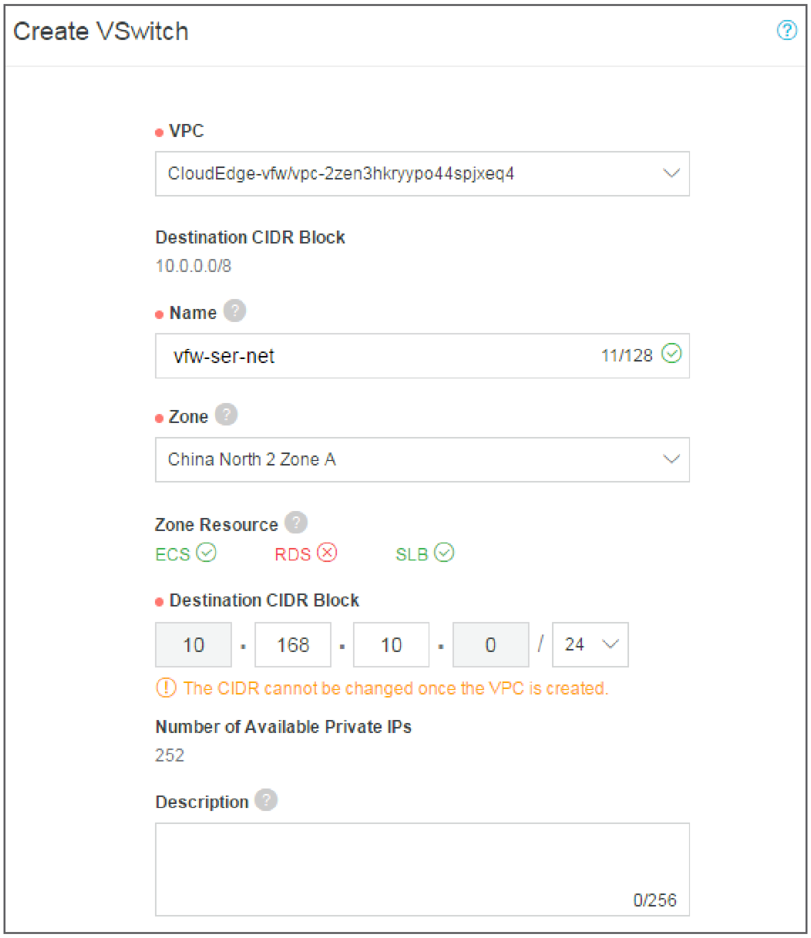
Option	Description
VPC Name	Specifies the name of VPC as "CloudEdge-vpc".
Destination	Specifies **Destination CIDR Block**as 10.0.0.0/8.

Option	Description
CIDR Block	
VSwitch Name	Specifies the name of VSwitch as "vpc-switch".
zone	China North 2 Zone A
Destination CIDR Block	10.168.19.0/24

3. Click **OK**.

Step 2: Create VSwitches

1. Select "Virtual Private Cloud >VPC >VSwitches", click **Create VSwitch** , and the <Create VSwitch>dialog box appears, configure the following options:



Create VSwitch

- VPC

CloudEdge-vfw/vpc-2zen3hkryypo44spjxeq4

Destination CIDR Block

10.0.0.0/8

- Name

vfw-ser-net 11/128

- Zone

China North 2 Zone A

Zone Resource

ECS ✓ RDS ⊗ SLB ✓

- Destination CIDR Block

10 . 168 . 10 . 0 / 24

ⓘ The CIDR cannot be changed once the VPC is created.

Number of Available Private IPs

252

Description

0/256

2. Repeat the above steps to continue configuring the switch **vfw-HA-net** and **server-net**.

   Note: The three switches should be set in the same zone.

Configure these three switches as follows:

Option	Description
vfw-HA-net	
VPC	Select the VPC “CloudEdgLEe-vpc” .
Name	Specifies the name of VSwitch as “vfw-HA-net” .
Zone	China North 2 Zone A

Option	Description
Destination CIDR Block	10.168.1.0/24
vfw-ser-net	
VPC	Select the VPC “CloudEdge-vpc” .
Name	Specifies the name of VSwitch as “vfw-ser-net” 。
Zone	China North 2 Zone A
Destination CIDR Block	10.168.10.0/24
server-net	
VPC	Select the VPC “CloudEdgLEe-vpc” .
Name	Specifies the name of VSwitch with “server-net” 。
Zone	China North 2 Zone A
Destination CIDR Block	10.168.100.0/24

Step 3: Create CloudEdge Instances

1. Create instance vFW-A and instance vFW-B,for HA deployment. For detailed steps, refer to "Deploying CloudEdge on Alibaba Cloud" on Page 155

   Requirements: At least 4 vCPU and 8 GB memory are needed for per instance. To build the HA network for one instance, besides the default network, there should be one more network, which should be choose with the different switch from the default network .

The HA Instances Configuration

Option	Description
vFW-A	
Instance Name	Specifies the name of Instance as "vFW-A".
Instance Type	Select the “ecs.hfc5.xlarge（4-core, 8GB，High Frequency Compute hfc5）” .
Network Interface	Default Network Interface：VPC：CloudEdge-vpc，VSwitch:vfw-ser-net. Add Network Interface：VPC：CloudEdge-vpc，VSwitch:vfw-HA-net.
vFW-B	
Instance Name	Specifies the name of Instance as "vFW-B".
Instance Type	Select “ecs.hfc5.xlarge（4-core, 8GB，High Frequency Compute hfc5）” 。
Network Interface	Default Network Interface：VPC：CloudEdge-vpc，VSwitch:vfw-ser-net。 Add Network Interface：VPC：CloudEdge-vpc，VSwitch:vfw-HA-net。

2. Create instance Web-Server. For detailed steps, refer to "Deploying CloudEdge on Alibaba Cloud" on Page 155.

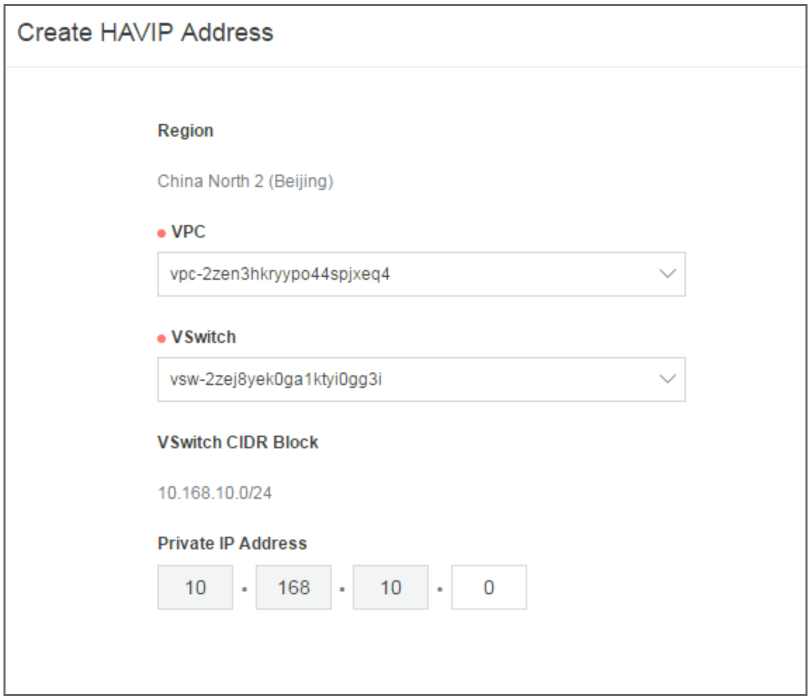
   The network must be selected with the different network from the vFW-A and vFW-B.

Web-server Configuration

Option	Description
Instance Name	Specifies the name of Instance as "Web-Server” .
Instance Type	Select the “ ecs.hfc5.xlarge（4-core, 8GB， High Frequency Compute hfc5） ".You can select flexibly according to actual needs.
Network Interface	Default Network Interface： VPC： CloudEdge-vpc, VSwitch:server-net.

Steps 4: Create HAVIP Address

1. Log in Alibaba Cloud and enter the Console page, and select “ Virtual Private Cloud >HAVIP Addresses ” , click **Create HAVIP Address**, and the <Create HAVIP Address>dialog will pop up.



Create HAVIP Address

Region

China North 2 (Beijing)

VPC

vpc-2zen3hkryypo44spjxeq4

VSwitch

vsw-2zej8yek0ga1ktyi0gg3i

VSwitch CIDR Block

10.168.10.0/24

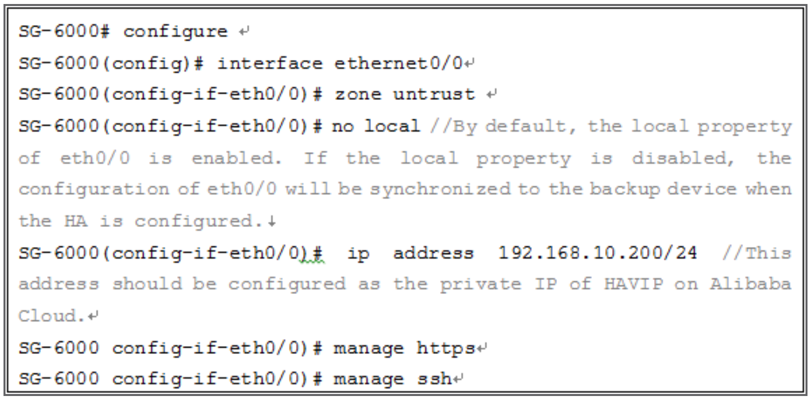
Private IP Address

10 . 168 . 10 . 0

2. Click **OK**. And then click "Manage" in the list and < HAVIP Details>will pop up, bind vFW-A and vFW-B in the binding resource diagram. The EIP shoud be bound so that the the HA device can be visited through the Internet .

Step 5: Configure HA on CloudEdge.

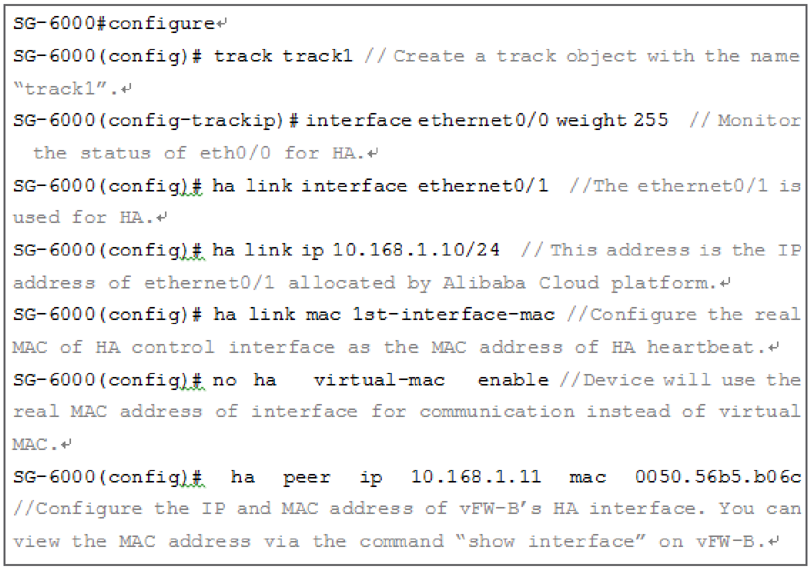
1. Configure the IP address of ethernet0/0 and enable the HTTPS and SSH management on the vFW-A, the master device of HA.



```
SG-6000# configure ↵
SG-6000(config)# interface ethernet0/0↵
SG-6000(config-if-eth0/0)# zone untrust ↵
SG-6000(config-if-eth0/0)# no local //By default, the local property
of eth0/0 is enabled. If the local property is disabled, the
configuration of eth0/0 will be synchronized to the backup device when
the HA is configured.↓
SG-6000(config-if-eth0/0)# ip address 192.168.10.200/24 //This
address should be configured as the private IP of HAVIP on Alibaba
Cloud.↵
SG-6000 config-if-eth0/0)# manage https↵
SG-6000 config-if-eth0/0)# manage ssh↵
```

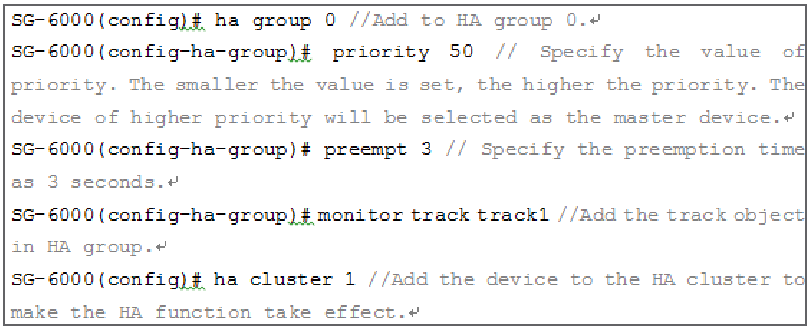
2. On vFW-A,creat a track object to monitor the status of ethernet0/0, Once the interface fails to work, the backup device will take over.At the same time, configure the interface ethernet0/1 for

HA, as well as the related information of IP and MAC.



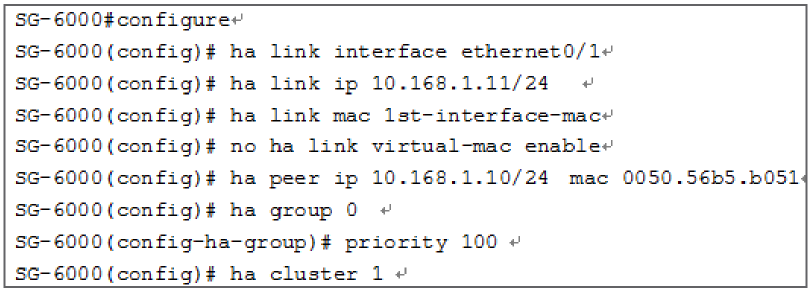
```
SG-6000#configure↵
SG-6000(config)# track track1 // Create a track object with the name
"track1".↵
SG-6000(config-trackip)# interface ethernet0/0 weight 255  // Monitor
  the status of eth0/0 for HA.↵
SG-6000(config)# ha link interface ethernet0/1  //The ethernet0/1 is
used for HA.↵
SG-6000(config)# ha link ip 10.168.1.10/24  // This address is the IP
address of ethernet0/1 allocated by Alibaba Cloud platform.↵
SG-6000(config)# ha link mac 1st-interface-mac //Configure the real
MAC of HA control interface as the MAC address of HA heartbeat.↵
SG-6000(config)# no  ha   virtual-mac   enable //Device will use the
real MAC address of interface for communication instead of virtual
MAC.↵
SG-6000(config)#  ha  peer  ip  10.168.1.11  mac  0050.56b5.b06c
//Configure the IP and MAC address of vFW-B's HA interface. You can
view the MAC address via the command "show interface" on vFW-B.↵
```

3. On the vFW-A,configure the HA group.



```
SG-6000(config)# ha group 0 //Add to HA group 0.↵
SG-6000(config-ha-group)#  priority  50  //  Specify  the  value  of
priority. The smaller the value is set, the higher the priority. The
device of higher priority will be selected as the master device.↵
SG-6000(config-ha-group)# preempt 3 // Specify the preemption time
as 3 seconds.↵
SG-6000(config-ha-group)# monitor track track1 //Add the track object
in HA group.↵
SG-6000(config)# ha cluster 1 //Add the device to the HA cluster to
make the HA function take effect.↵
```

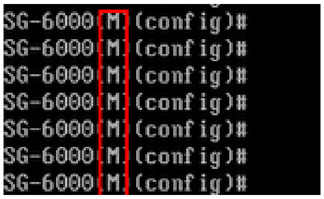
4. Repeat the above steps to configure relevant information on vFW-B.



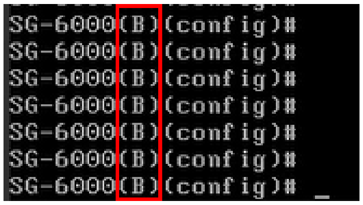
```
SG-6000#configure↵
SG-6000(config)# ha link interface ethernet0/1↵
SG-6000(config)# ha link ip 10.168.1.11/24   ↵
SG-6000(config)# ha link mac 1st-interface-mac↵
SG-6000(config)# no ha link virtual-mac enable↵
SG-6000(config)# ha peer ip 10.168.1.10/24  mac 0050.56b5.b051
SG-6000(config)# ha group 0  ↵
SG-6000(config-ha-group)# priority 100 ↵
SG-6000(config)# ha cluster 1 ↵
```

Step 6: HA Results

After completing the above configuration, the high-priority vFW-A will automatically negotiate to be the master device, and the vFW-B with low priority will become the backup device. The master device and the backup device are marked with the letter "M" and letter "B" respectively in the console.



```
SG-6000(M)(config)#
SG-6000(M)(config)#
SG-6000(M)(config)#
SG-6000(M)(config)#
SG-6000(M)(config)#
SG-6000(M)(config)#
SG-6000(M)(config)#
```



```
SG-6000(B)(config)#
SG-6000(B)(config)#
SG-6000(B)(config)#
SG-6000(B)(config)#
SG-6000(B)(config)#
SG-6000(B)(config)#
SG-6000(B)(config)# _
```

- When the two devices have been successfully negotiated, you only need to configure the master device and the configurations will automatically synchronize to the backup device.
- When vFW-A fails to forward traffic or its ethernet0/0 is disconnected, vFW-B will switch to the main device and start to forward traffic without interrupting user's communication.

Step 7: HA application

To redirect Web-Server traffic to CloudEdge in the HA deployment scenarios, configure as follows:

1. Configure the SNAT rule on the vFW-A, the master device. Change the source address of the traffic in the Web-Server segment to the IP of interface eth0/0, aka HAVIP (high available virtual IP).

   Tips: The Web-Server segment "server-net" set in the Step 2 should be 10.168.100.0/24.

   Command:

   ```
   SG-6000(M)(config-vrouter)# snatrule from 10.168.100.0/24 to
   any service any eif ethernet0/0 trans-to eif-ip mode dynam-
   icport
   ```

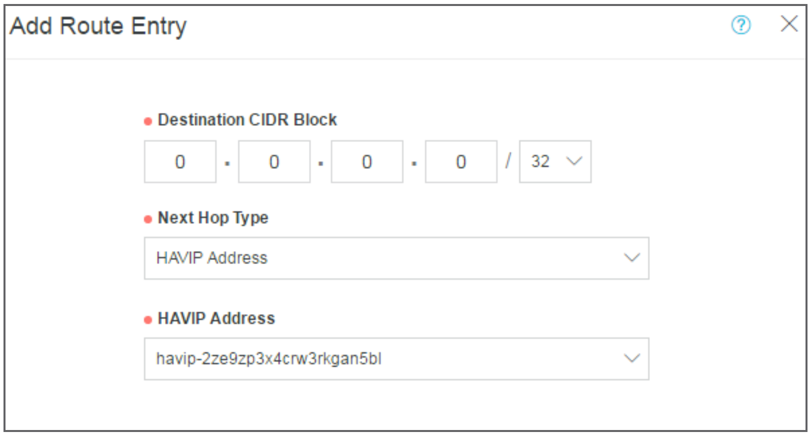
2. Map the SSH traffic whose destination address is HAVIP to the port 22 on the Web-Server.

   Tips: Web-server IP address:10.168.100.113.

   Command:

```
SG-6000(M)(config-vrouter)# dnatrule from any to
10.168.10.200 service ssh trans-to 10.168.100.113
```

3. In the VPC router of Alibaba Cloud platform , add a routing whose destination segment is 0.0.0.0/0 and the next-hop is HAVIP.



Add Route Entry

● Destination CIDR Block

0 . 0 . 0 . 0 / 32

● Next Hop Type

HAVIP Address

● HAVIP Address

havip-2ze9zp3x4crw3rkgan5bl

4. When all configurations have completed, the traffic of the Web-Server segment will be forwarded through the CloudEdge in the HA scenarios, and the CloudEdge will also provide security protection for Web-Server.

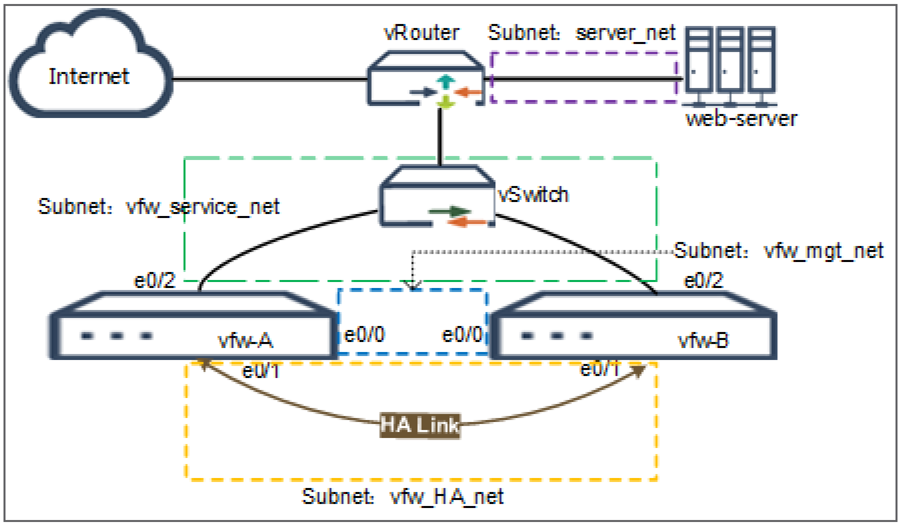
About how to use StoneOS, refer to StoneOS related documents (click here).

Deploying HA Scenarios of CloudEdgevia Secondary Private IP on Alibaba Cloud

HA Typical Scenarios

There is a cloud server web-server (10.0.2.209) on the Alibaba Cloud. You can protect the server by deploying the HA scheme of CloudEdge.The following topology introduces how to deploy HA scenarios of CloudEdge on Alibaba Cloud.

After the deployment, vfw-A will be selected as the master device to protect the web-server and vfw-B will be selected as the backup device. vfw-A will synchronize its configurations and status data to the backup device vfw-B. When the master device vfw-A fails to work, the backup device vfw-B will switch to the master device to protect web-server without interrupting user's communication, which can ensure network stability.



Log in to the AlibabaCloud console (click here) with your Alibaba account. Information of VPC and subnet which web-server belong to are as follows:

- VPC(VPC1):10.0.0.0/16
- Subnet 0 (server_net):10.0.2.0/24
- web-server IP： 10.0.2.209

Create the following subnets, and the VPC which subnets and the web-server belong to should be the same:

- VPC(VPC1)： 10.0.0.0/16
- Subnet 1 （vfw_service_net） ： 10.0.1.0/24
- Subnet 2 （vfw_mgt_net） ： 10.0.10.0/24
- Subnet 3 （vfw_HA_net） ： 10.0.100.0/24

Deployment Steps

Step 1: Creating RAM Roles

Step 2: Creating Switches

Step 3: Creating CloudEdge Instances

Step 4: Adding Elastic Network Interfaces and Configuring Secondary Private IPs

Step 5: Purchasing an Elastic IP and Binding it to an Elastic Network Interface

Step 6: Configuring HA on CloudEdge

Step 7: View HA Results

Step 8: Configure Routing, NAT and Security Policies on CloudEdge

Step 1: Creating RAM Roles

For HA deployment of Cloud Edge, the AccessKey authentication or RAM role authentication is required for accessing to cloud platform API. To avoid exposing an account's AccessKey, it is usuallyauthenticated by a RAM role. For authentication using Accesskey, refer to the Appendix. To create a RAM role, take the following steps:

1. Hover your mouse over the user avatar at the top-right corner, and then click **Access Control** in the pop-up box.
2. Select **Identities > Roles** in the left navigation pane.

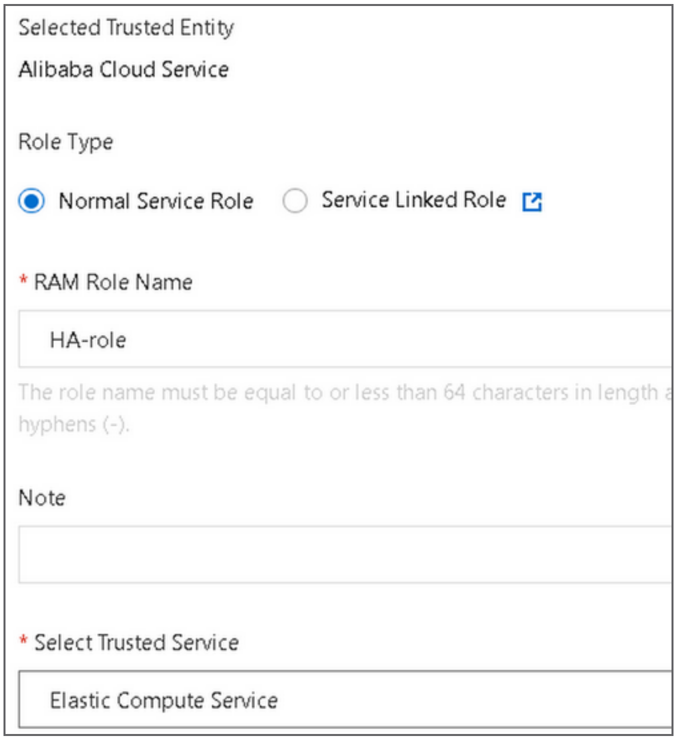
3. Click **Create Role** and configure as follows:

    - Select Role Type: Select **Alibaba Cloud Service**

    - Configure Role: Select **Normal Service Role**

        - RAM Role Name:HA-role

        - Select **Elastic Compute Service**



Selected Trusted Entity

Alibaba Cloud Service

Role Type

● Normal Service Role ○ Service Linked Role

* RAM Role Name

HA-role

The role name must be equal to or less than 64 characters in length a hyphens (-).

Note

* Select Trusted Service

Elastic Compute Service

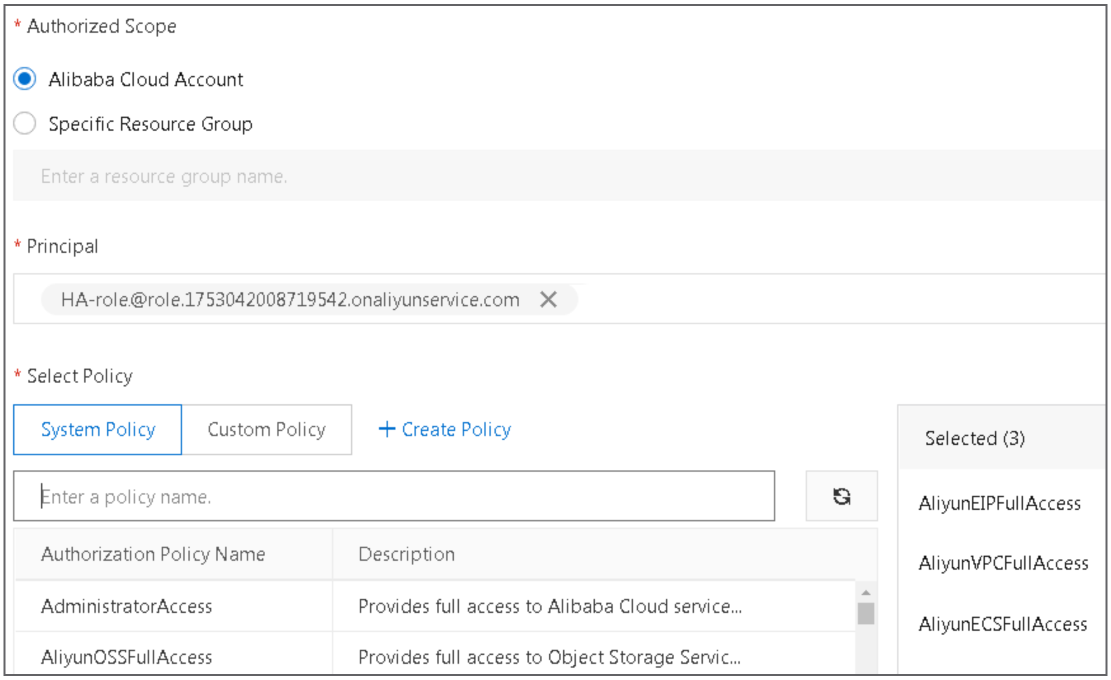
- Click **OK**.

- Click **Add Permissions to RAM Role** and open the <**Add Permissions** >Dialog.

- Autheorized Scope: **Alibaba Cloud Account**

- Principal ： The role created above has been selected .

- Select Policy： Search and select the **System Policy** :AliyunEIPFullAccess、AliyunVPCFullAccess和AliyunECSFullAccess.



* Authorized Scope

● Alibaba Cloud Account

○ Specific Resource Group

Enter a resource group name.

* Principal

HA-role@role.1753042008719542.onaliyunservice.com ✕

* Select Policy

System Policy | Custom Policy | + Create Policy

Enter a policy name.

Authorization Policy Name	Description
AdministratorAccess	Provides full access to Alibaba Cloud service...
AliyunOSSFullAccess	Provides full access to Object Storage Servic...

Selected (3)

AliyunEIPFullAccess

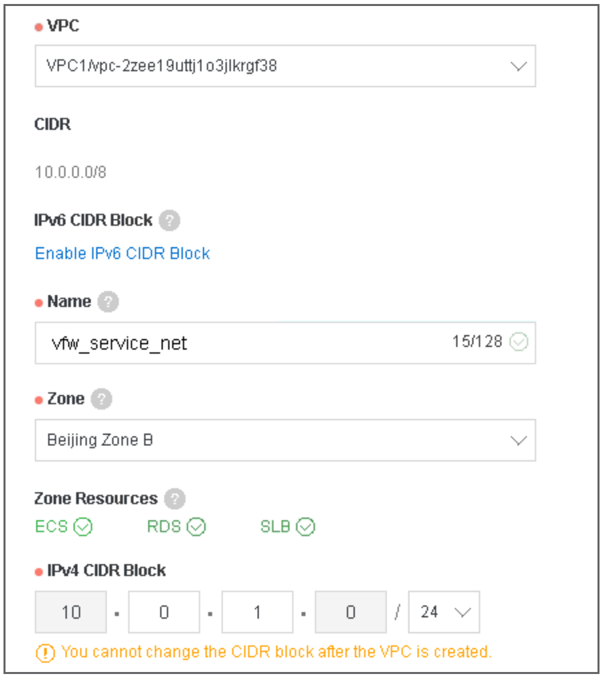
AliyunVPCFullAccess

AliyunECSFullAccess

4. Click OK ,and the RAM role will be referenced directly in subsequent CloudEdge instances.

Step 2: Creating Switches

1. In the left navigation pane, select **Virtual Private Cloud** > **VPC** > **VSwitches**, and then click **Create VSwitch**. The Create VSwitch dialog box will appear. Create a switch named "vfw_service_net", whose subnet is "10.0.1.0/24".



● VPC

VPC1/vpc-2zee19uttj1o3jlkrgf38

CIDR

10.0.0.0/8

IPv6 CIDR Block

Enable IPv6 CIDR Block

● Name

vfw_service_net 15/128

● Zone

Beijing Zone B

Zone Resources

ECS RDS SLB

● IPv4 CIDR Block

10 . 0 . 1 . 0 / 24

You cannot change the CIDR block after the VPC is created.

2. Repeat the above steps to create the switches "vfw_mgt_net" and "vfw_HA_net". **Note:** The three switches should be set in the same zone.

3. Configure the switches as follows:

Option	Description
vfw_mgt_net	
VPC	Select **VPC1**.
Name	Specify the name of the VSwitch as "vfw_mgt_net".
Zone	Shanghai Zone A
Destination CIDR Block	10.0.10.0/24
vfw_HA_net	
VPC	Select **VPC1**.

Option	Description
Name	Specify the name of the VSwitch as "vfw_HA_net".
Zone	Shanghai Zone A
Destination CIDR Block	10.0.100.0/24

Step 3: Creating CloudEdge Instances

1. In the left navigation pane, select **Elastic Compute Service** > **Instances & Images** > **Instances**, and create the two instances vfw-A and vfw-B for HA deployment. For detailed steps, refer to Deploying CloudEdge on Alibaba Cloud.

   Requirements: At least 2 vCPUs and 4 GB memory are required for per instance. For default network interfaces of both instances, you should select the same switch vfw_mgt_net in the same VPC.

2. **Configure the HA Instance as follows:**

Option	Description
vfw-A	
Instance Name	Specify the name as "vfw-A".
Instance Type	Select "ecs.ic5.xlarge (4-core, 4GB, Compute Intensive Type ic5)".
Network Interface	Default Network Interface: VPC: VPC1; VSwitch: vfw_mgt_net. Add Network Interface: VPC: VPC1; VSwitch: vfw_HA_net.

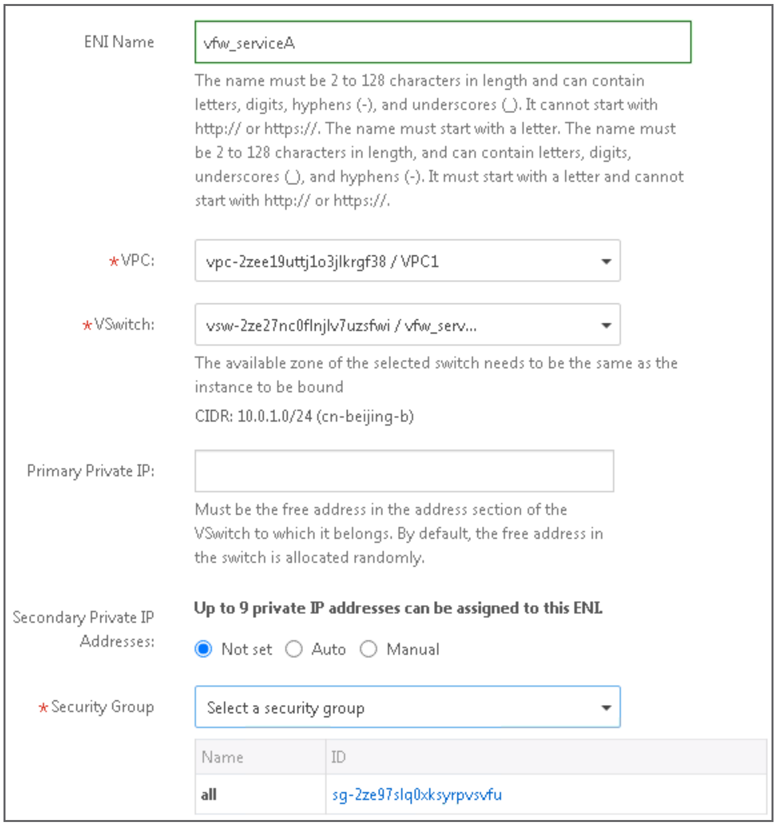
Option	Description
Public IP Address	Select **Assign Public IP Address**, and then the instance will get a public IP address.
Advanced	RAM Role: Select **HA-role**.
vfw-B	
Instance Name	Specify the name as "vfw-B".
Instance Type	Select "ecs.ic5x.large (4-core, 4GB, Compute Intensive Type ic5)".
Network Interface	Default Network Interface: VPC: VPC1; VSwitch: vfw_mgt_net. Add Network Interface: VPC: VPC1; VSwitch: vfw_HA_net.
Advanced	RAM Role: Select **HA-role**.

Step 4: Adding Elastic Network Interfaces and Configuring Secondary Private IPs

1. In the left navigation pane, select **Elastic Compute Service** > **Network and Security** > **ENIs**, and click **Create ENI** to create an elastic network interface "vfw-HA".

   - ENI Name: vfw_serviceA
   - VPC: VPC1
   - VSwitch: vfw_service_net

- Security Group: Select the same security group as the instance.



ENI Name: vfw_serviceA

The name must be 2 to 128 characters in length and can contain letters, digits, hyphens (-), and underscores (_). It cannot start with http:// or https://. The name must start with a letter. The name must be 2 to 128 characters in length, and can contain letters, digits, underscores (_), and hyphens (-). It must start with a letter and cannot start with http:// or https://.

*VPC: vpc-2zee19uttj1o3jlkrgf38 / VPC1

*VSwitch: vsw-2ze27nc0flnjlv7uzsfwi / vfw_serv...

The available zone of the selected switch needs to be the same as the instance to be bound

CIDR: 10.0.1.0/24 (cn-beijing-b)

Primary Private IP:

Must be the free address in the address section of the VSwitch to which it belongs. By default, the free address in the switch is allocated randomly.

Secondary Private IP Addresses: **Up to 9 private IP addresses can be assigned to this ENI.**

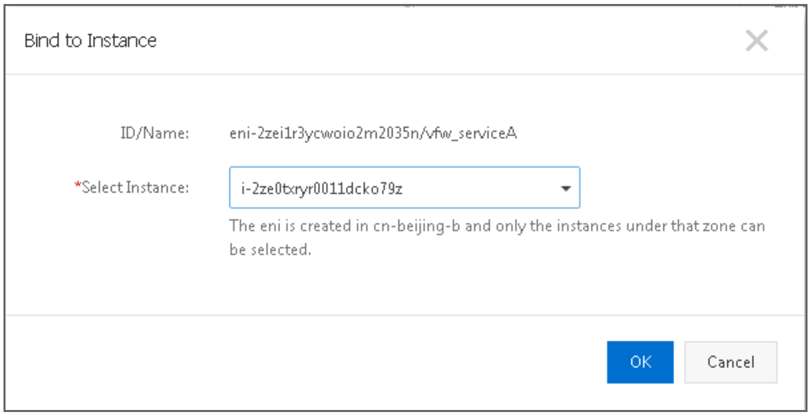
● Not set ○ Auto ○ Manual

*Security Group: Select a security group

Name	ID
all	sg-2ze97slq0xksyrpvsvfu

2. Click **OK**.

3. In the ENI list, click **Bind to Instance** behind the network interface you created, and then select **vfw-A**.



Bind to Instance

ID/Name: eni-2zei1r3ycwoio2m2035n/vfw_serviceA

*Select Instance: i-2ze0txryr0011dcko79z

The eni is created in cn-beijing-b and only the instances under that zone can be selected.

4. Repeat steps 1 and 2 to create another elastic network interface "vfw_serviceB" (VSwitch: vfw_service_net), then bind it to vfw-B.
5. After binding all network interfaces, restart vfw-A and vfw-B.
6. In the ENI list, select the network interface "vfw_service1" of vfw-A, and click **Manage Secondary Private IP Address**. In the pop-up dialog box, click **Assign New IP**, and then configure the secondary private IP address, such as 10.0.1.242.

Step 5: Purchasing an Elastic IP and Binding it to an Elastic Network Interface

1. In the left navigation pane, select **Elastic Compute Service** > **Network and Security** > **EIP**, and click **Create EIP**.
2. After purchasing, select the elastic IP, and click **Bind** at the bottom of the list. In the Bind Elastic IP to Resources dialog box, select the secondary elastic network interface "vfw_serviceA" of vfw-A.
3. Click **OK**.

Step 6: Configuring HA on CloudEdge

1. On the Alibaba cloud platform, view and record information such as the elastic public IP address of vfw_mgt_net of vfw-A and vfw-B, and then log in to the vfw-A via WebUI using the elastic public IP address. For detailed steps, refer to To Login CloudEdge via HTTPS.

2. Disable the reverse routing check for the interface eth0/0 of vfw-A and vfw-B respectively.

```
SG-6000# configure

SG-6000(config)# interface ethernet0/0

SG-6000(config)# dhcp-client route distance 10 ////IP address and default route of eth0/0 are automatically obtained . In this example, routing priority needs to be set as 10.

SG-6000(config-if-eth0/0)# no reverse-route ////Disable the reverse routing checking of eth0/0.
```

3. On the vfw-A, configure secondary private IP to the vfw-Service-net interface (eth0/2 in the example) of CloudEdge. (This configuration can only be set in the master device, which will be synchronized to the backup device after HA is deployed.)

```
SG-6000# configure

SG-6000(config)# interface ethernet0/2

SG-6000(config)#zone untrust

SG-6000(config-if-eth0/2)# ip address 10.0.1.242/24 ////Configure as the secondary private IP address and its mask.

SG-6000(config-if-eth0/2)# manage ping ////Configure the management.

SG-6000(config-if-eth0/2)# manage ssh

SG-6000(config-if-eth0/2)# manage https

SG-6000(config-if-eth0/2)# exit
```

4. Configure host routing and DNS to make vfw-A and vfw-B to communicate with the Alibaba Cloud platform. (This configuration can only be set in the master device, which will be synchronized to the backup device after HA is deployed.)

```
SG-6000# configure
SG-6000# show dns ////View the device's DNS Server address, which is 10.0.0.2 in this example.
SG-6000(config)# ip vrouter trust-vr
SG-6000(config-vrouter)# ip route 0.0.0.0/0 10.0.1.253 ////Configure static routing, next hop is vfw_Service_net gateway IP, and the default is X.X.X.1.
SG-6000(config-vrouter)# ip route 10.0.0.2/32 10.0.10.1 ////The DNS Server address is 10.0.0.2 and the gateway IP of vfw_mgt_net is 10.0.10.1 .
```

5. Configure HA on the master device vfw-A, and configure as follows:

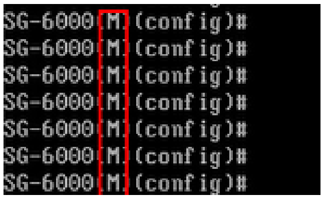
```
SG-6000#configure
SG-6000(config)# track track1 ////Create a track object with the name “track1”.
SG-6000(config-trackip)# interface ethernet0/2 weight 255 ////Configure eth0/2 interface as the HA tracking interface.
SG-6000(config)# ha link interface ethernet0/1 ////Configure eth0/1 interface as the HA link interface.
SG-6000(config)# ha link ip 10.0.100.164/24 ////Configure the IP address for HA negotiation according to the IP assigned to eth0/1 by Alibaba Cloud platform.
SG-6000(config)# ha link mac 1st-interface-mac ////Configure the control interface of HA to use the  real MAC of interface.
SG-6000(config)# no ha virtual-mac enable ////Configure the HA business interface to use the real MAC of interface.
SG-6000(config)# ha peer ip 10.0.100.100 mac 0224.f8f3.e5e2 /////Configure the address of the peer device of HA link interface. The MAC address can be viewed by the command "show interface". (MAC address can be optionally configured.)
SG-6000(config)#ha cloud-deploy havip disable////Disable HAVIP function that Alibaba Cloud provides to deploy HA
SG-6000(config)#ha cloud-deploy platform aliyunSpecify the Cloud platform the CloudEdge were deployed as AliCLoud.
SG-6000(config)# ha group 0 ////Join group HA 0.
SG-6000(config-ha-group)# priority 50 ////Set the priority and the smaller the value, the higher the priority. The device with the higher the priority will be the master device.
SG-6000(config-ha-group)# monitor track track1 ////Add track
SG-6000(config-ha-group)# exit
SG-6000(config)# ha cluster 1 ////Add HA cluster 1.
```

6. On the backup device vfw-B, configure the following information.

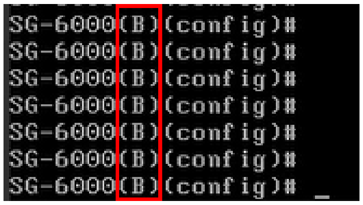
```
SG-6000#configure
SG-6000(config)# ha link interface ethernet0/1
SG-6000(config)# ha link ip 10.0.100.100/24
SG-6000(config)# ha link mac 1st-interface-mac
SG-6000(config)# no ha virtual-mac enable
SG-6000(config)# ha peer ip 10.0.100.164 mac
028e.8f79.700e ////The MAC address configuration is optional.
SG-6000(config)#ha cloud-deploy havip disable////Disable HAVIP function that Alibaba
Cloud provides to deploy HA
SG-6000(config)#ha cloud-deploy platform aliyunSpecify the Cloud platform the
CloudEdge were deployed as AliCLoud.
SG-6000(config)# ha group 0
SG-6000(config-ha-group)# priority 100
SG-6000(config-ha-group)# exit
SG-6000(config)# ha cluster 1 ////It is recommended to add HA
cluster 1 after the status of the master device changes to "M".
```

Step 7: View HA Results

After completing the above configurations, the vfw-A with high priority will be selected as the master device automatically, and the vfw-B with low priority will become the backup device. The master device and the backup device are marked with the letter "M" and letter "B" respectively in the console.



```
SG-6000(M)(config)#
SG-6000(M)(config)#
SG-6000(M)(config)#
SG-6000(M)(config)#
SG-6000(M)(config)#
SG-6000(M)(config)#
SG-6000(M)(config)#
```



```
SG-6000(B)(config)#
SG-6000(B)(config)#
SG-6000(B)(config)#
SG-6000(B)(config)#
SG-6000(B)(config)#
SG-6000(B)(config)#
SG-6000(B)(config)# _
```

- When the two devices have been successfully negotiated, you only need to configure the master device and the configurations will automatically synchronize to the backup device.
- When vfw-A fails to forward traffic or its ethernet0/2 is disconnected, vfw-B will switch to the master device and start to forward traffic without interrupting user's communication.

Step 8: Configure Routing, NAT and Security Policies on CloudEdge

You can configure the web-server's inbound and outbound traffic through the CloudEdge instance in the HA deployment scheme to ensure the high reliability of server's business. The configurations are as follows:

1. Configure the source NAT rule on the master device vfw-A, and the source address of the traffic in the web-server network segment will be to translate into the IP of interface eth0/2, i.e., the secondary private IP: 10.0.1.242.

   Command:

   ```
   SG-6000(M)(config-vrouter)# snatrule from 10.0.2.209/24 to
   any service any eif ethernet0/2 trans-to eif-ip mode dynamicport
   ```

2. Configure the destination NAT rule on the vfw-A, and the destination IP address of the traffic whose destination address is the secondary private IP will be translated into the IP address of web-server 10.0.2.209.

   Command:

   ```
   SG-6000(M)(config-vrouter)# dnatrule from any to 10.0.1.1.242
   service any trans-to 10.0.2.209
   ```

3. Configure a security policy rule on vfw-A that allows all traffic to pass.

   Command:

   ```
   SG-6000(M)(config-policy)# rule from any to any service any
   permit
   ```

4. After the configurations, web-server will not need to be bound with the elastic IP. The intranet address of web-server will be translated to the secondary private IP of the vfw_service_net subnet of CloudEdge through DNA T rules, and Internet users can access the server by accessing the public address of secondary private IP. At the same time, the source IP address of the traffic sent by web-server to Internet will also be translated to the secondary private IP address of CloudEdge through SNAT rules, so as to protect web-server against external attacks.

Results

When the master device vfw-A fails, the backup device vfw-B will automatically switch to the master device. The secondary private IP, routing, information of security policy, source NAT and destination NAT on the original master device will be switched automatically without manual reconfiguration, and the communication will not be affected, thus realizing a high reliable security guarantee for cloud servers.

About how to use StoneOS, refer to StoneOS related documents (click here).

Appendix

If RAM authentication is not used, that is, the RAM role is not bound to CloudEdge instance,you can apply an AccessKey for authentication .

Applying for AccesKey

1. Hover your mouse over the user avatar at the top-right corner, and click **Security Control** in the pop-up box.

2. AccessKey of your cloud account is the secret key to access Alibaba Cloud APIs. It has full permissions of your cloud account, and needs to be verified via the administrator's mobile phone number. You should keep it safe.

3. Click **Create AccessKey**, and then copy and paste the AccessKey ID and Secret for use in subsequent steps.

4. Then perform the configuration in Steps 2 to 9. When configuring HA in Step 7, you need to set the AccessKey ID and Secret commands on the master and backup devices. In global configuration mode, run the following command:
   SG-6000(config)#cloud-deploy accesskeyid XXXXXXXXXXXX accesskeysecret XXXXXXXXXX

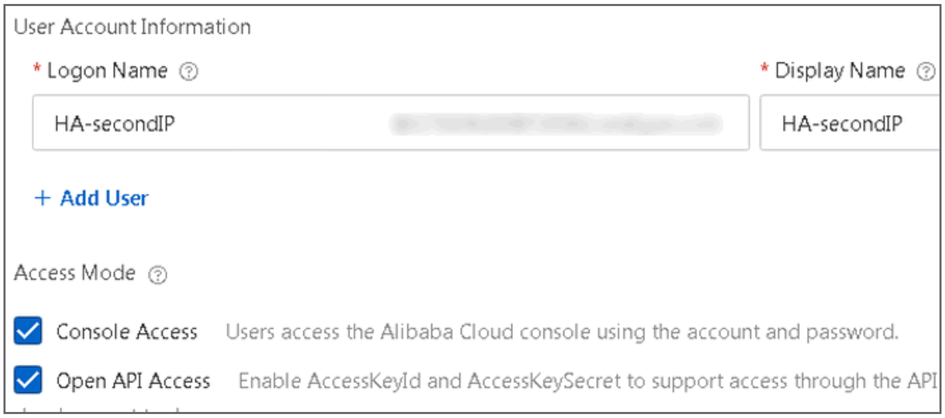
If you do not want to assign all permissions to an AccessKey, you can create an AccessKey using a subuser account and assign the specified permissions to the subuser account. For details , take the following steps:

1. Hover your mouse over the user avatar at the top-right corner, and click **Access Control** in the pop-up box.

2. Select **Idetities** > **Users** and click "**Creater User**".

   - Logon Name : HA-secondIP Display Name:HA-secondIP

   - Access Mode: Select **Console Access** and **Open API Access** .



User Account Information

* Logon Name: HA-secondIP [redacted]

* Display Name: HA-secondIP

Access Mode

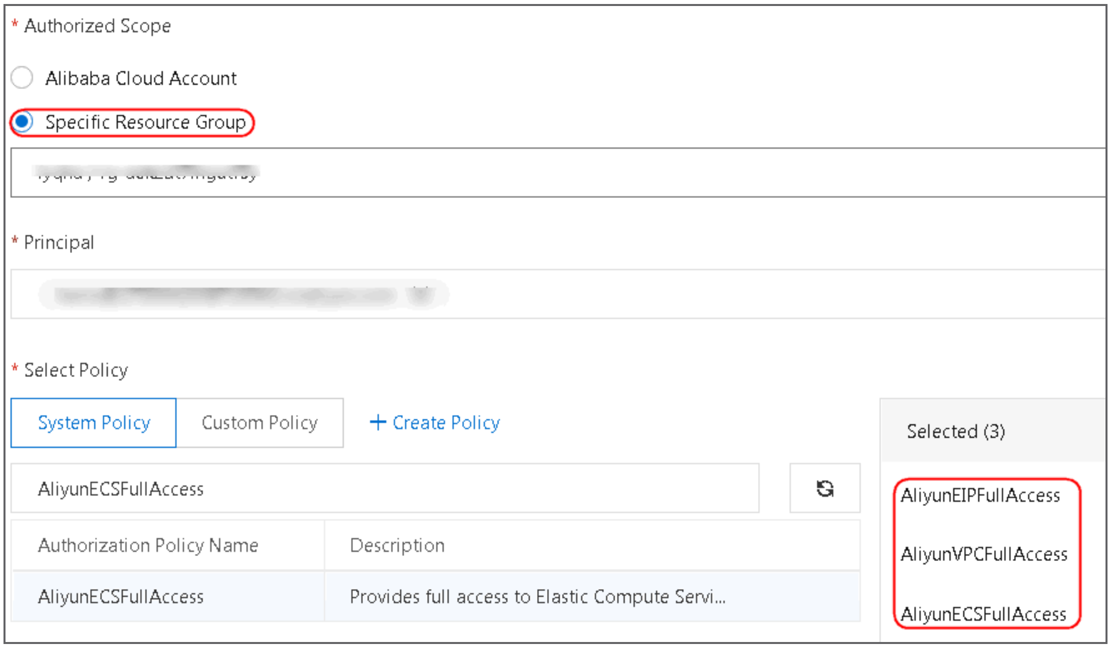
☑ Console Access Users access the Alibaba Cloud console using the account and password.

☑ Open API Access Enable AccessKeyId and AccessKeySecret to support access through the API

3. Click **OK** and complete the SMS verification.

4. In the users list ,find the sub account "HA-secondIP "and click the **Add Permissions** link to open the <Add Permissions>.

   - Authorized Scope : Select "Specific Resource Group "and specify the resource group the vfw-A and vfw-B are located.
   - Select Policy : AliyunEIPFullAccess、 AliyunVPCFullAccess和AliyunECSFullAccess



* Authorized Scope

○ Alibaba Cloud Account

● Specific Resource Group

[redacted]

* Principal

[redacted]

* Select Policy

AliyunECSFullAccess

Authorization Policy Name	Description
AliyunECSFullAccess	Provides full access to Elastic Compute Servi...

Selected (3)

AliyunEIPFullAccess

AliyunVPCFullAccess

AliyunECSFullAccess

   - Click **OK**.

5. In the user list, find the sub account HA-SecondIP, click the user name link to enter the user details page. In the "User AccessKeys " section, click Create AccessKey to create an accesskey, and then copy the AccessKey ID and Secret.

6. Then perform the configuration in Steps 2 to 9. When configuring HA in Step 7, you need to set the AccessKey ID and Secret commands on the master and backup devices. In global configuration mode, run the following command:
   SG-6000(config)#cloud-deploy accesskeyid XXXXXXXXXXXX accesskeysecret

xxxxxxxxx

Deploying CloudEdge on Array AVX

System Requirements

To deploy CloudEdge on an Array AVX platform, the host should meet the following requirements:

- Array AVX has been installed.
- Array AVX has at least 2 CPUs and 2 GB memory.

Installing CloudEdge

CloudEdge will be installed as an instance on Array AVX. After the installation, you can run the virtual StoneOS system, and access the CLI and WebUI of CloudEdge.

Step 1: Importing the Image

1. Log in to Array AVX. Click **VA Image** on the left navigation pane, and then click the **VA Image** tab.

2. On the VA Image page, click ⊕ on the upper-left corner, and the **Import a VA Image** dialog will pop up.

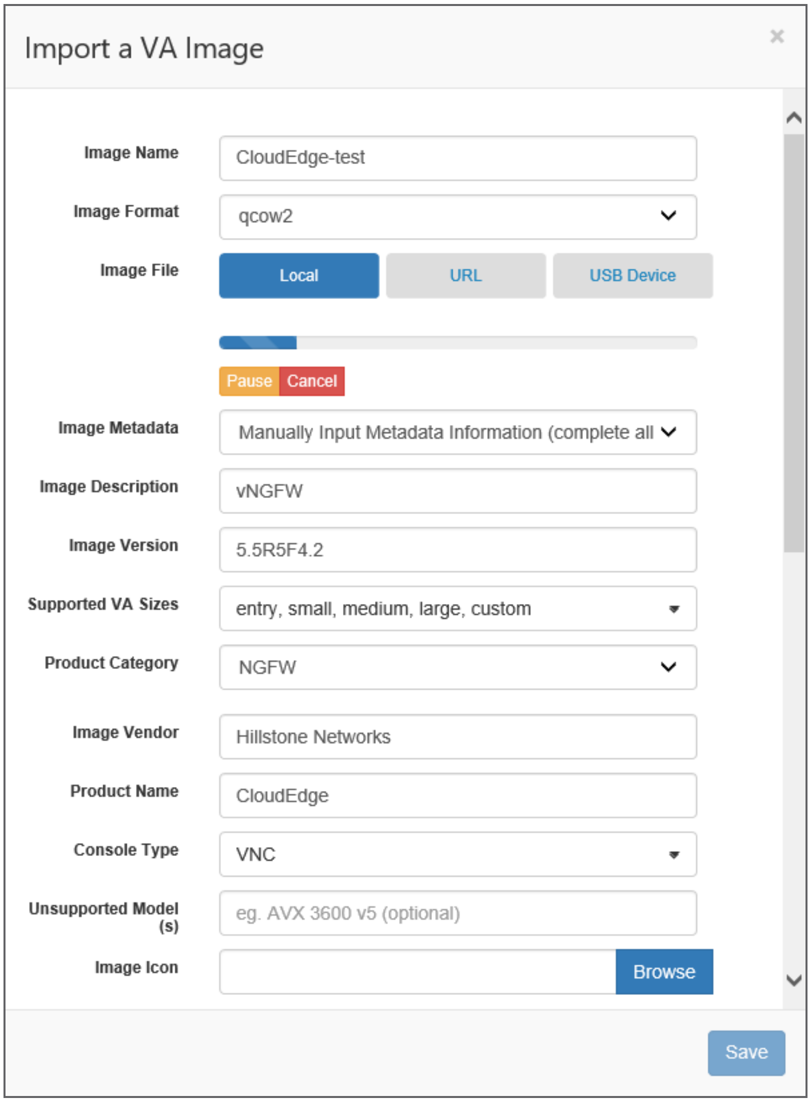


Image Name: CloudEdge-test

Image Format: qcow2

Image File: Local

Image Metadata: Manually Input Metadata Information (complete all

Image Description: vNGFW

Image Version: 5.5R5F4.2

Supported VA Sizes: entry, small, medium, large, custom

Product Category: NGFW

Image Vendor: Hillstone Networks

Product Name: CloudEdge

Console Type: VNC

Unsupported Model (s): eg. AVX 3600 v5 (optional)

Image Icon:

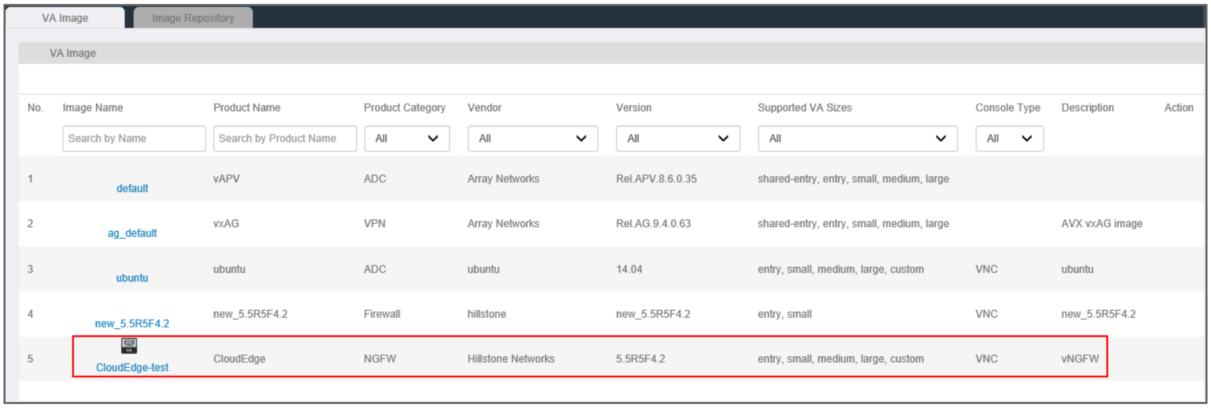
In the Import a VA Image dialog, configure the following options.

Option	Description
Image Name	Enter the image name, such as "CloudEdge-test".
Image Format	Select **qcow2** from the **Image Format** drop-down list.

Option	Description
Image File	Click the **Local** tab, click **Browse**, and select the image file from the local PC. The progress bar of uploading will pop up.
Image Metadata	Select **Manually Input Metadata Information (Complete all fields below)** from the **Image Metadata** drop-down list.
Image Description	Enter the description information of image.
Image Version	Enter the version information of image.
Supported VA Sizes	Select the VM sizes according to requirement, including Large, Medium, Small, Entry and Shared-entry. Since the size selected here will affect the VM size of the CloudEdge instance you create later, you are suggested to select multiple sizes, such as Large, Medium, Small and Entry. The information of CPU and memory is shown as below： • Large: 8 CPUs and 16GB memory. • Medium: 4 CPUs and 8GB memory. • Small: 2 CPUs and 4GB memory. • Entry: 1 CPU and 2GB memory.
Product Category	Select **NGFW** from the **Product Category** drop-down list.
Image Vendor	Enter the image vendor, such as "Hillstone Networks".
Product Name	Enter the product name, such as "CloudEdge".

Option	Description
Console Type	Select **VNC** from the **Console Type** drop-down list.

3. After above configurations, click **Save**. The image file will be imported successfully and displayed in the list.

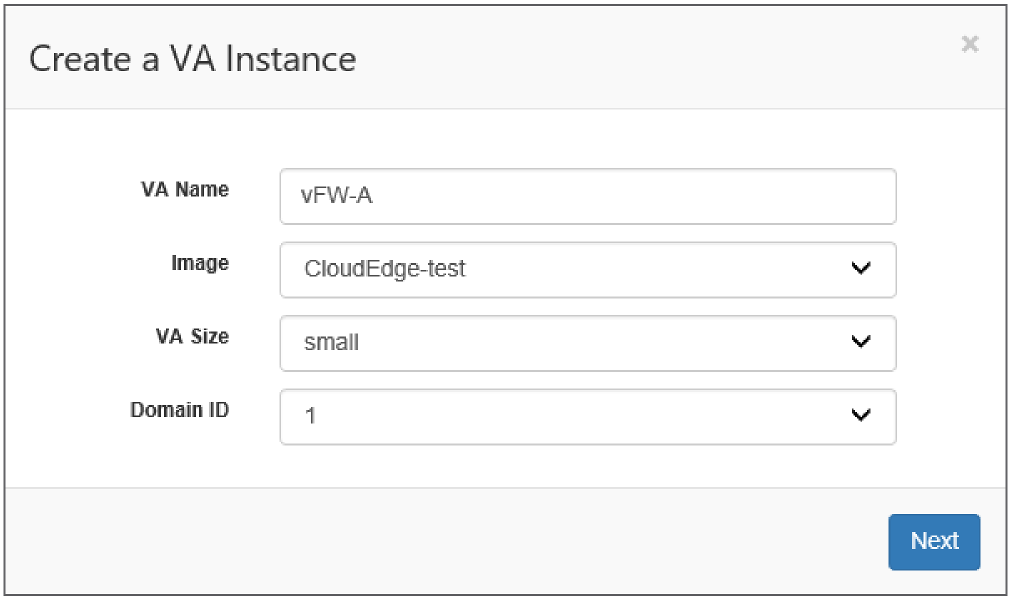


No.	Image Name	Product Name	Product Category	Vendor	Version	Supported VA Sizes	Console Type	Description	Action
	Search by Name	Search by Product Name	All	All	All	All	All		
1	default	vAPV	ADC	Array Networks	Rel.APV.8.6.0.35	shared-entry, entry, small, medium, large			
2	ag_default	vxAG	VPN	Array Networks	Rel.AG.9.4.0.63	shared-entry, entry, small, medium, large		AVX vxAG image	
3	ubuntu	ubuntu	ADC	ubuntu	14.04	entry, small, medium, large, custom	VNC	ubuntu	
4	new_5.5R5F4.2	new_5.5R5F4.2	Firewall	hillstone	new_5.5R5F4.2	entry, small	VNC	new_5.5R5F4.2	
5	CloudEdge-test	CloudEdge	NGFW	Hillstone Networks	5.5R5F4.2	entry, small, medium, large, custom	VNC	vNGFW	

Step2: Creating the Instance

1. Click **VA** on the left navigation pane to enter the VA Management page.

2. Click ⊕ on the upper-left corner, and the **Create a VA Instance** dialog pops up.



Create a VA Instance

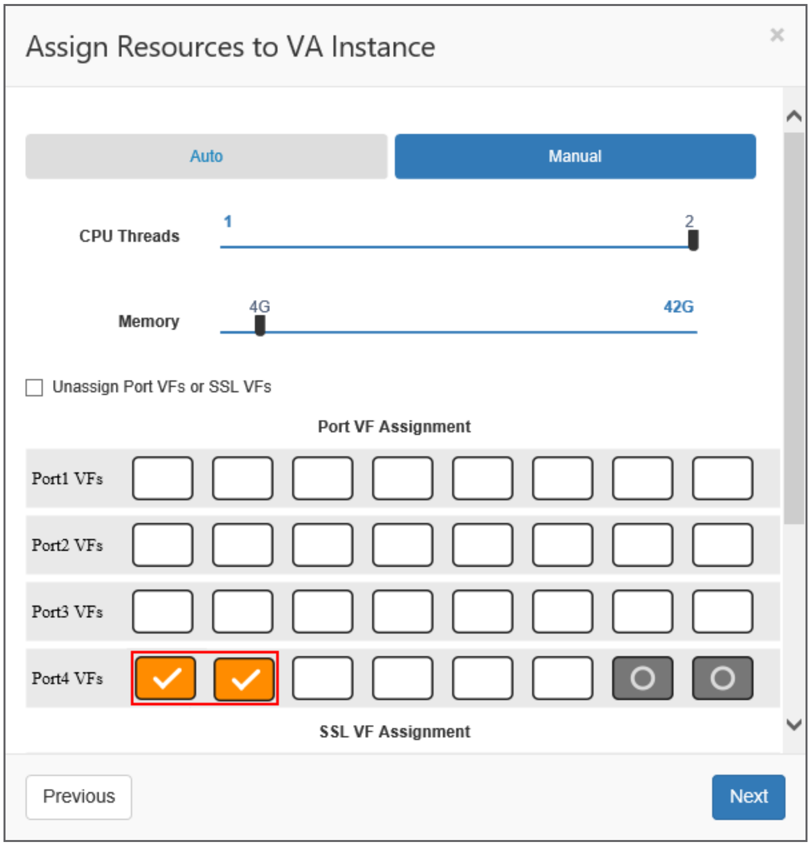
VA Name	vFW-A
Image	CloudEdge-test
VA Size	small
Domain ID	1

3. **In the Create a VA Instance dialog, configure the corresponding options.**

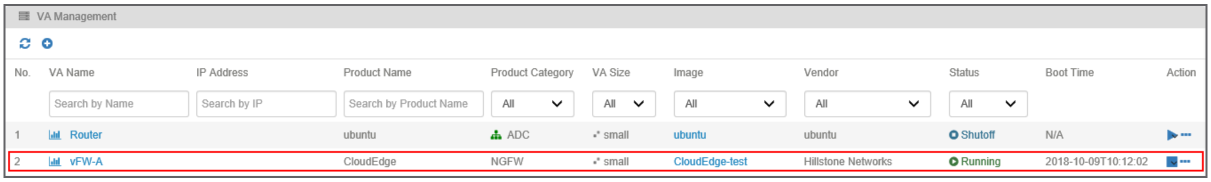
Option	Description
VA Name	Enter the VM name, such as "vFW-A".
Image	Select **CloudEdge-test** from the **Image** drop-down list.
VA Size	Select the VM sizes from the **VA Size** drop-down list, which should meet the standard requirement. The standard requirements of three CloudEdge types are shown as below： • VM-01: 2 CPUs and 2GB memory. • VM-02: 2 CPUs and 4GB memory. • VM-04: 4 CPUs and 8GB memory. You are suggested to select Small, Medium or Large when installing VM-01 and VM-02, and to select Medium or Large when installing VM-04.
Domain ID	Select **1** from the Domain ID drop-down list.

4. Click **Next** to enter the Assign Resources to VA Instance page. Click the **Manual** tab, and assign port VFs for CloudEdge as needed. When you select multiple port VFs, the xethernet interface of CloudEdge will be corresponded according to the selection order. For example, the first selected

port VF will be matched to xethernet0/1.



5. Click **Next** to enter the Confirm VA Instance Configuration page. After you confirm the configurations, click **Save**, and the created instance will be displayed in the list.


VA Management

No.	VA Name	IP Address	Product Name	Product Category	VA Size	Image	Vendor	Status	Boot Time	Action
	Search by Name	Search by IP	Search by Product Name	All	All	All	All	All		
1	Router		ubuntu	ADC	small	ubuntu	ubuntu	Shutoff	N/A	
2	vFW-A		CloudEdge	NGFW	small	CloudEdge-test	Hillstone Networks	Running	2018-10-09T10:12:02	

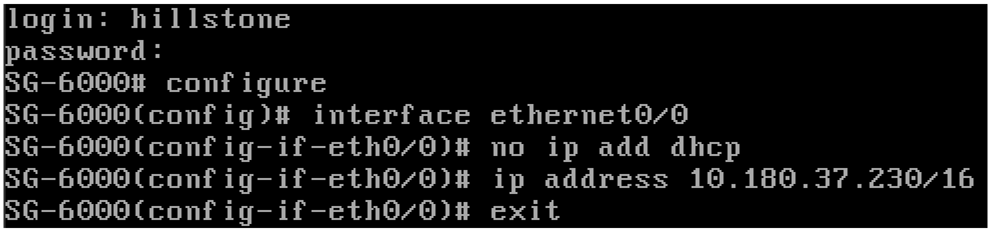
Step 3: Configuring CloudEdge

After you create the CloudEdge instance, ethernet0/0 will be assigned as the management interface. By default, Array AVX will assign IP address for eth0/0 automatically with SSH, HTTPS and Ping enabled. The default route will also be set automatically. If Array AVX cannot provide the DHCP server, you need to configure as below:

1. By default, the created CloudEdge is powered off. Click ▶, and then click ··· when the status of CloudEdge changes to ● Running.

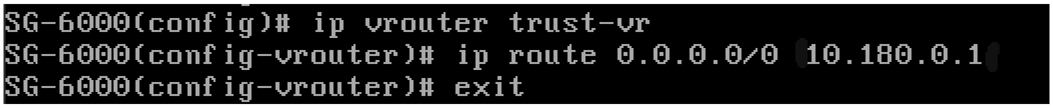
2. Select **>_VNC Console** in the pop-up dialog, and enter the CLI of CloudEdge. Enter the default username and password: hillstone/hillstone.

3. Disable the DHCP function of ethernet0/0 and configure the IP address.



```
login: hillstone
password:
SG-6000# configure
SG-6000(config)# interface ethernet0/0
SG-6000(config-if-eth0/0)# no ip add dhcp
SG-6000(config-if-eth0/0)# ip address 10.180.37.230/16
SG-6000(config-if-eth0/0)# exit
```

4. Configure the static route.



```
SG-6000(config)# ip vrouter trust-vr
SG-6000(config-vrouter)# ip route 0.0.0.0/0 10.180.0.1
SG-6000(config-vrouter)# exit
```

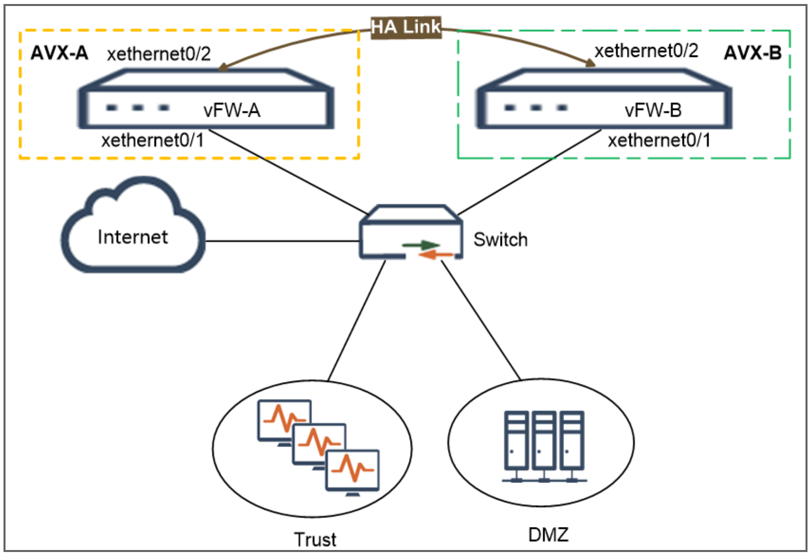
5. After above configurations, you can visit CloudEdge through SSH and HTTPS.

About how to use StoneOS, refer to StoneOS related documents (click here).

Deploying HA Scenarios of CloudEdge on Array AVX

HA Typical Scenarios

The following topology introduces how to deploy HA scenarios of CloudEdge on Array AVX. You should deploy vFW-A on AVX-A, and deploy vFW-B on AVX-B. After the deployment, vFW-A will be selected as the master device to forward traffic and vFW-B will be selected as the backup device. vFW-A will synchronize its configurations and status data to the backup device vFW-B. When the master device vFW-A failures to forward traffic, the backup device vFW-B will switch to the master device to forward traffic without interrupting user's communication, which can ensure network stability.



To deploy CloudEdge on an Array AVX platform, the host should meet the following requirements:

- Two Array AVXs have been installed.
  - Each Array AVX has at least 2 CPUs and 2 GB memory.

Installing CloudEdge

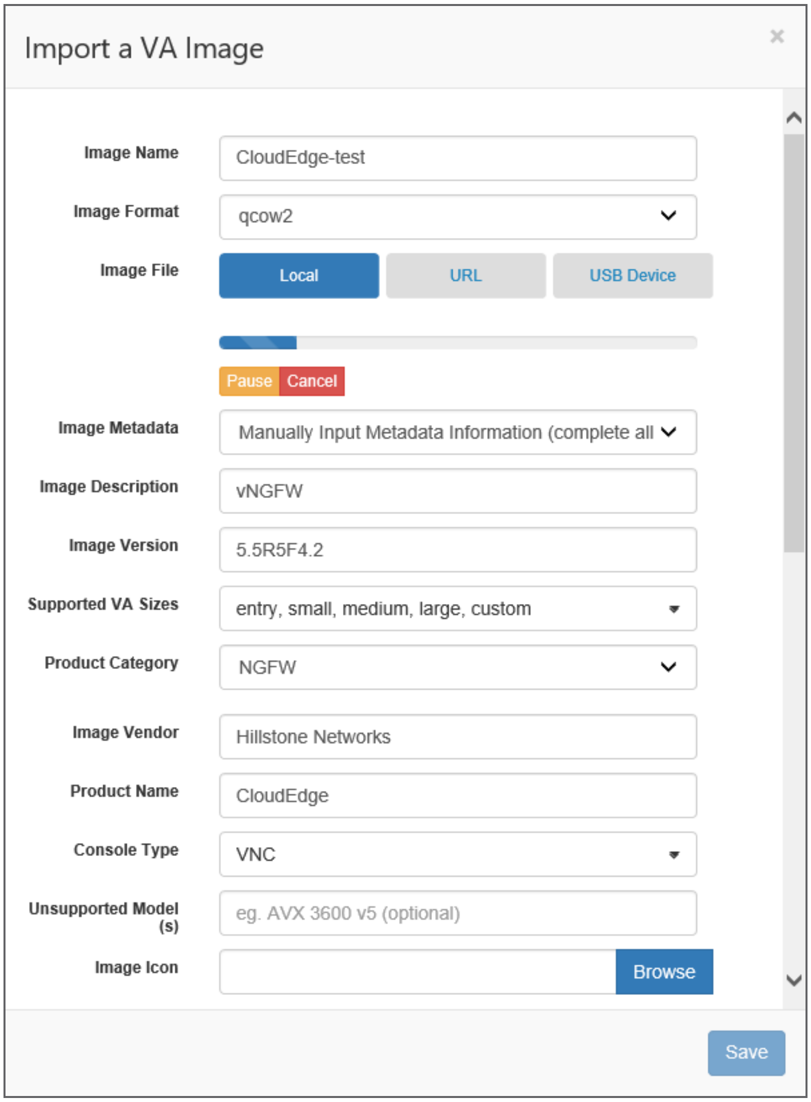
Installing CloudEdge on AVX-A

Step 1: Importing the Image

1. Log in to Array AVX-A.

2. Click **VA Image** on the left navigation pane, and then click the **VA Image** tab.

3. On the VA Image page, click ⊕ on the upper-left corner, and the **Import a VA Image** dialog will pop up.



Import a VA Image

Image Name: CloudEdge-test

Image Format: qcow2

Image File: Local | URL | USB Device

Image Metadata: Manually Input Metadata Information (complete all

Image Description: vNGFW

Image Version: 5.5R5F4.2

Supported VA Sizes: entry, small, medium, large, custom

Product Category: NGFW

Image Vendor: Hillstone Networks

Product Name: CloudEdge

Console Type: VNC

Unsupported Model (s): eg. AVX 3600 v5 (optional)

Image Icon:

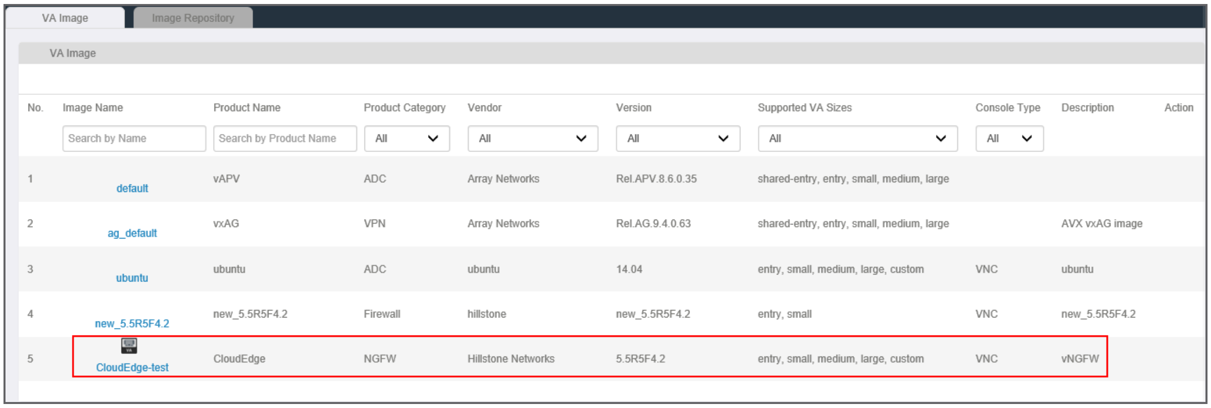
In the Import a VA Image dialog, configure the corresponding options.

Option	Description
Image Name	Enter the image name, such as "CloudEdge-test".
Image Format	Select **qcow2** from the **Image Format** drop-down list.

Option	Description
Image File	Click the **Local** tab, click **Browse**, and select the image file from the local PC. The progress bar of uploading will pop up.
Image Metadata	Select **Manually Input Metadata Information (Complete all fields below)** from the **Image Metadata** drop-down list.
Image Description	Enter the description information of image.
Image Version	Enter the version information of image.
Supported VA Sizes	Select the VM sizes according to requirement, including Large, Medium, Small, Entry and Shared-entry. Since the size selected here will affect the VM size of the CloudEdge instance you create later, you are suggested to select multiple sizes, such as Large, Medium, Small and Entry. The information of CPU and memory is shown as below： • Large: 8 CPUs and 16GB memory. • Medium: 4 CPUs and 8GB memory. • Small: 2 CPUs and 4GB memory. • Entry: 1 CPU and 2GB memory.
Product Category	Select **NGFW** from the **Product Category** drop-down list.
Image Vendor	Enter the image vendor, such as "Hillstone Networks".
Product Name	Enter the product name, such as "CloudEdge".

Option	Description
Console Type	Select **VNC** from the **Console Type** drop-down list.

4. After above configurations, click **Save**. The image file will be imported successfully and displayed in the list.

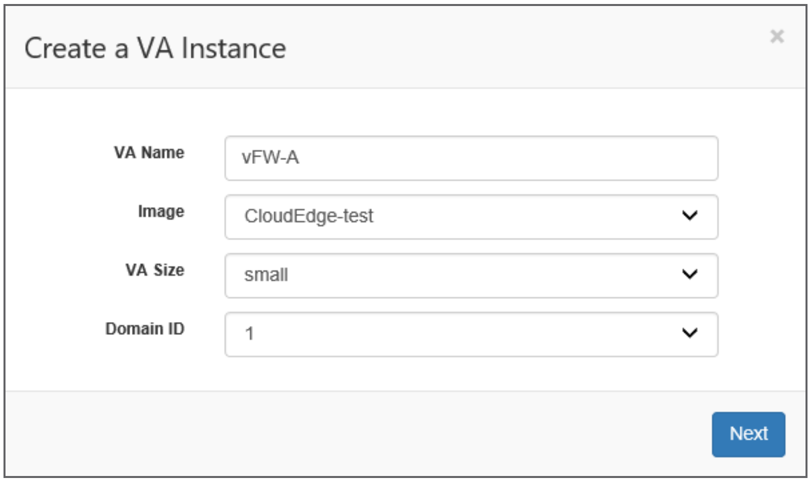


No.	Image Name	Product Name	Product Category	Vendor	Version	Supported VA Sizes	Console Type	Description	Action
	Search by Name	Search by Product Name	All	All	All	All	All		
1	default	vAPV	ADC	Array Networks	Rel.APV.8.6.0.35	shared-entry, entry, small, medium, large			
2	ag_default	vxAG	VPN	Array Networks	Rel.AG.9.4.0.63	shared-entry, entry, small, medium, large		AVX vxAG image	
3	ubuntu	ubuntu	ADC	ubuntu	14.04	entry, small, medium, large, custom	VNC	ubuntu	
4	new_5.5R5F4.2	new_5.5R5F4.2	Firewall	hillstone	new_5.5R5F4.2	entry, small	VNC	new_5.5R5F4.2	
5	CloudEdge-test	CloudEdge	NGFW	Hillstone Networks	5.5R5F4.2	entry, small, medium, large, custom	VNC	vNGFW	

Step 2: Creating the Instance

1. Click **VA** on the left navigation pane to enter the VA Management page.

2. Click ⊕ on the upper-left corner, and the **Create a VA Instance** dialog pops up.



Create a VA Instance

VA Name: vFW-A

Image: CloudEdge-test

VA Size: small

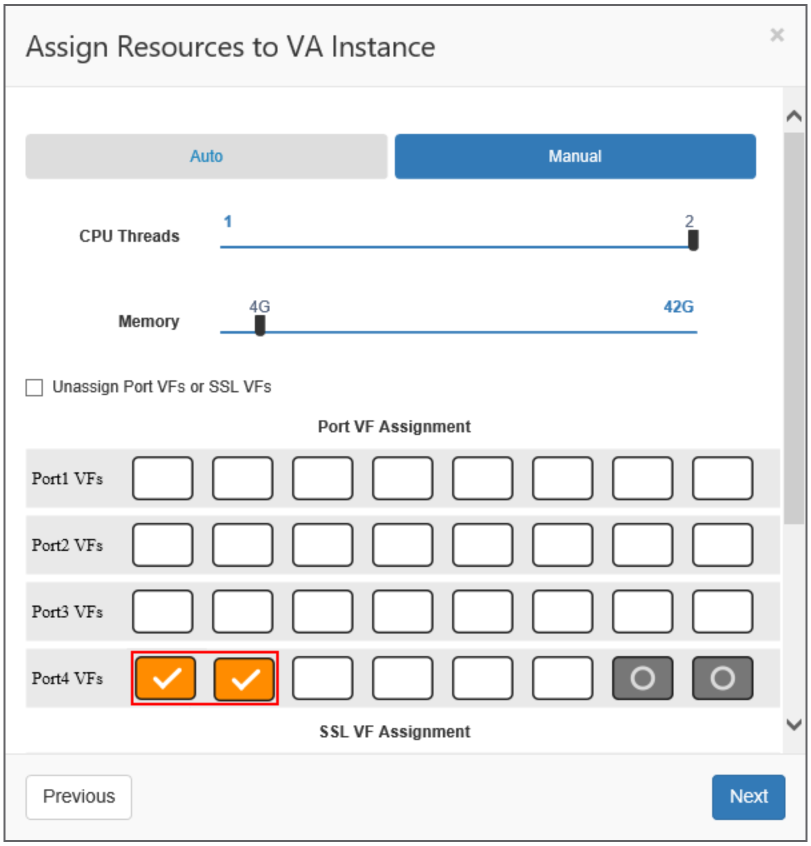
Domain ID: 1

3. In the Create a VA Instance dialog, configure the following options.

Option	Description
VA Name	Enter the VM name, such as "vFW-A".
Image	Select **CloudEdge-test** from the **Image** drop-down list.
VA Size	Select the VM sizes from the **VA Size** drop-down list, which should meet the standard requirement. The standard requirements of three CloudEdge types are shown as below： • VM-01: 2 CPUs and 2GB memory. • VM-02: 2 CPUs and 4GB memory. • VM-04: 4 CPUs and 8GB memory. You are suggested to select Small, Medium or Large when installing VM-01 and VM-02, and to select Medium or Large when installing VM-04.
Domain ID	Select **1** from the **Domain ID** drop-down list.

4. Click **Next** to enter the Assign Resources to VA Instance page. Click the **Manual** tab, and assign port VFs for CloudEdge as needed. When you select multiple port VFs, the xethernet interface of CloudEdge will be matched according to the selection order. For example, the first selected port

VF will be matched to xethernet0/1.



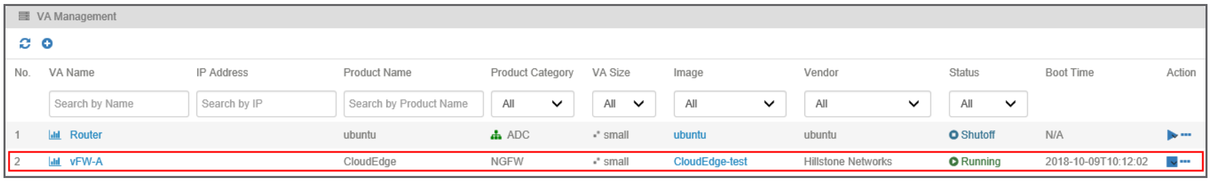
Assign Resources to VA Instance

CPU Threads 1 2

Memory 4G 42G

□ Unassign Port VFs or SSL VFs

5. Click **Next** to enter the Confirm VA Instance Configuration page. After you confirm the configurations, click **Save**, and the created instance will be displayed in the list.



VA Management

No.	VA Name	IP Address	Product Name	Product Category	VA Size	Image	Vendor	Status	Boot Time	Action
	Search by Name	Search by IP	Search by Product Name	All	All	All	All	All		
1	Router		ubuntu	ADC	small	ubuntu	ubuntu	Shutoff	N/A	
2	vFW-A		CloudEdge	NGFW	small	CloudEdge-test	Hillstone Networks	Running	2018-10-09T10:12:02	

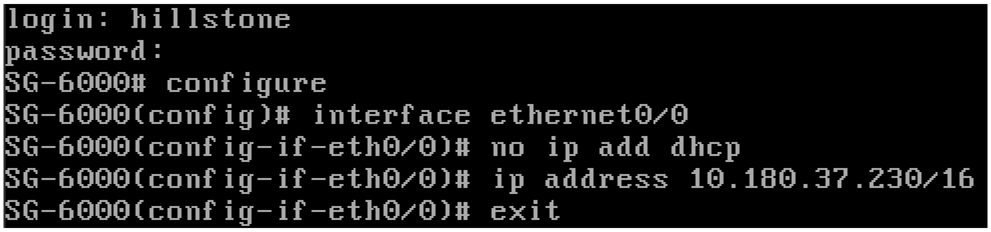
Step 3: Configuring CloudEdge

After you create the CloudEdge instance, ethernet0/0 will be assigned as the management interface. By default, Array AVX will assign IP address for eth0/0 automatically with SSH, HTTPS and Ping enabled. The default route will also be set automatically. If Array AVX cannot provide the DHCP server, you need to configure as below:

1. By default, the created CloudEdge is powered off. Click ▶, and then click ⋯ when the status of CloudEdge changes to ● Running.

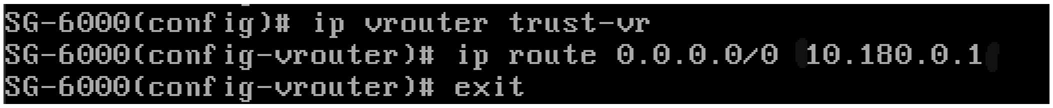
2. Select **>_VNC Console** in the pop-up dialog, and enter the CLI of CloudEdge to enter the default username and password: hillstone/hillstone.

3. Disable the DHCP function of ethernet0/0 and configure the IP address.



```
login: hillstone
password:
SG-6000# configure
SG-6000(config)# interface ethernet0/0
SG-6000(config-if-eth0/0)# no ip add dhcp
SG-6000(config-if-eth0/0)# ip address 10.180.37.230/16
SG-6000(config-if-eth0/0)# exit
```

4. Configure the static route.



```
SG-6000(config)# ip vrouter trust-vr
SG-6000(config-vrouter)# ip route 0.0.0.0/0 10.180.0.1
SG-6000(config-vrouter)# exit
```

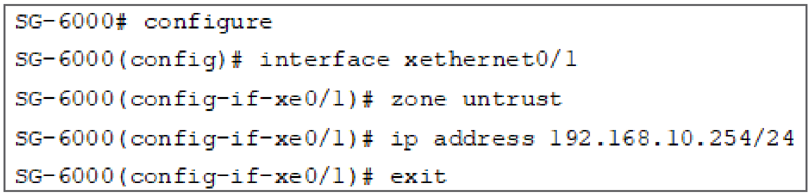
5. After above configurations, you can visit CloudEdge through SSH and HTTPS.

Installing CloudEdge on AVX-B

To install CloudEdge on AVX-B, see Installing CloudEdge on AVX-A.

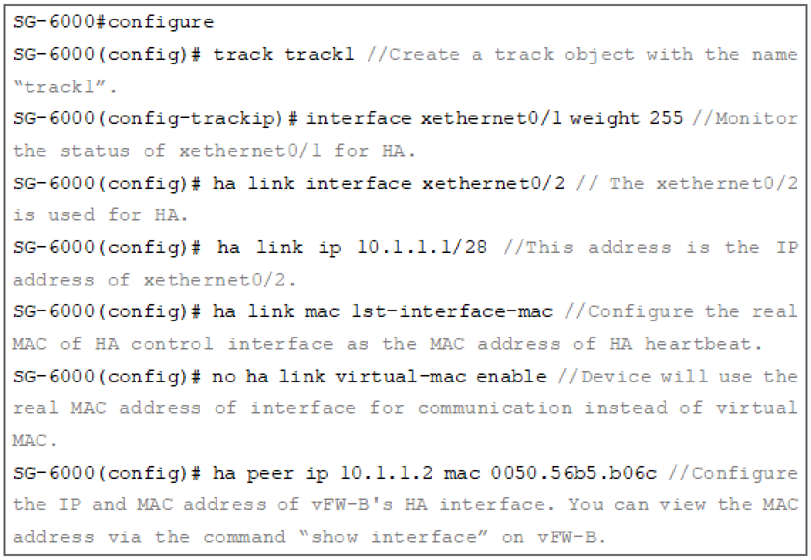
Configuring HA on CloudEdge.

1. Configure the IP address of xethernet0/1 on the vFW-A (the master device of HA).



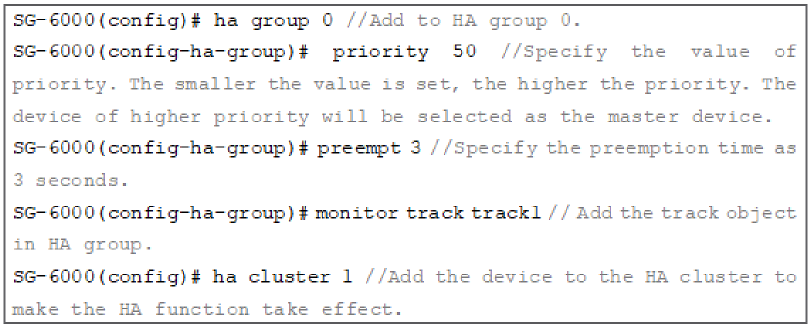
```
SG-6000# configure
SG-6000(config)# interface xethernet0/1
SG-6000(config-if-xe0/1)# zone untrust
SG-6000(config-if-xe0/1)# ip address 192.168.10.254/24
SG-6000(config-if-xe0/1)# exit
```

2. On vFW-A, create a track object to monitor the status of xethernet0/1, Once the interface fails to work, the backup device will take over. At the same time, configure the interface xethernet0/2 for HA, as well as the related information of IP and MAC.



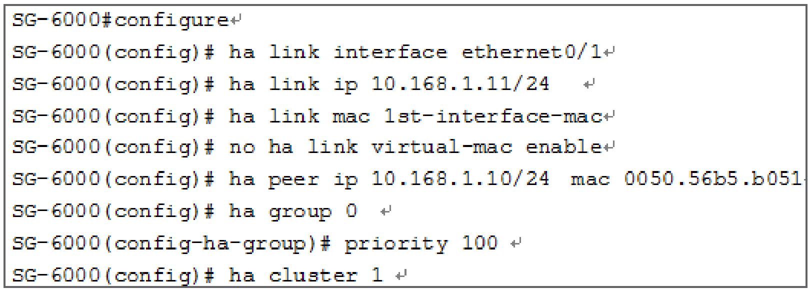
```
SG-6000#configure
SG-6000(config)# track track1 //Create a track object with the name
"track1".
SG-6000(config-trackip)# interface xethernet0/1 weight 255 //Monitor
the status of xethernet0/1 for HA.
SG-6000(config)# ha link interface xethernet0/2 // The xethernet0/2
is used for HA.
SG-6000(config)# ha link ip 10.1.1.1/28 //This address is the IP
address of xethernet0/2.
SG-6000(config)# ha link mac 1st-interface-mac //Configure the real
MAC of HA control interface as the MAC address of HA heartbeat.
SG-6000(config)# no ha link virtual-mac enable //Device will use the
real MAC address of interface for communication instead of virtual
MAC.
SG-6000(config)# ha peer ip 10.1.1.2 mac 0050.56b5.b06c //Configure
the IP and MAC address of vFW-B's HA interface. You can view the MAC
address via the command "show interface" on vFW-B.
```

3. On the vFW-A, configure the HA group.



```
SG-6000(config)# ha group 0 //Add to HA group 0.
SG-6000(config-ha-group)# priority 50 //Specify the value of
priority. The smaller the value is set, the higher the priority. The
device of higher priority will be selected as the master device.
SG-6000(config-ha-group)# preempt 3 //Specify the preemption time as
3 seconds.
SG-6000(config-ha-group)# monitor track track1 // Add the track object
in HA group.
SG-6000(config)# ha cluster 1 //Add the device to the HA cluster to
make the HA function take effect.
```

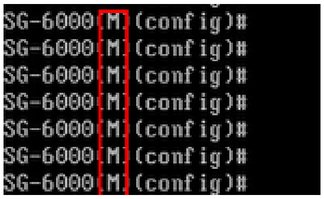
4. Repeat the above steps to configure relevant information on vFW-B.



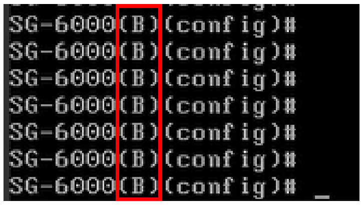
```
SG-6000#configure↵
SG-6000(config)# ha link interface ethernet0/1↵
SG-6000(config)# ha link ip 10.168.1.11/24   ↵
SG-6000(config)# ha link mac 1st-interface-mac↵
SG-6000(config)# no ha link virtual-mac enable↵
SG-6000(config)# ha peer ip 10.168.1.10/24  mac 0050.56b5.b051
SG-6000(config)# ha group 0  ↵
SG-6000(config-ha-group)# priority 100 ↵
SG-6000(config)# ha cluster 1 ↵
```

HA Results

After completing the above configuration, the vFW-A with high priority will automatically negotiate to be the master device, and the vFW-B with low priority will become the backup device. The master device and the backup device are marked with the letter "M" and letter "B" respectively in the console.



```
SG-6000(M)(config)#
SG-6000(M)(config)#
SG-6000(M)(config)#
SG-6000(M)(config)#
SG-6000(M)(config)#
SG-6000(M)(config)#
SG-6000(M)(config)#
```



```
SG-6000(B)(config)#
SG-6000(B)(config)#
SG-6000(B)(config)#
SG-6000(B)(config)#
SG-6000(B)(config)#
SG-6000(B)(config)#
SG-6000(B)(config)# _
```

- When the two devices have been successfully negotiated, you only need to configure the master device and the configurations will automatically synchronize to the backup device.
- When vFW-A fails to forward traffic or its xethernet0/1 is disconnected, vFW-B will switch to the main device and start to forward traffic without interrupting user's communication.

About how to use StoneOS, refer to StoneOS related documents (click here).

DeployingCloudEdge on HuaweiCould

System Requirements

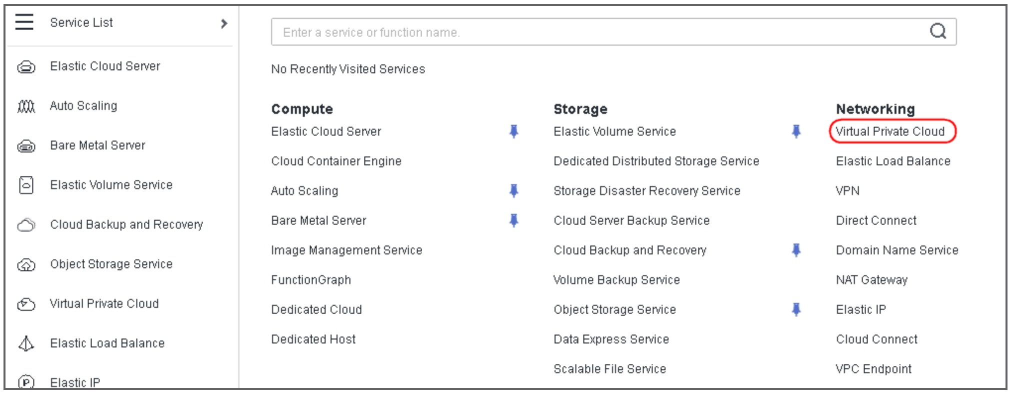
To deploy Hillstone's virtual firewall(vFW) on HuaweiCloud, the host should meet the following requirements:

- CloudEdge virtual machine(VM) requires at least 2 vCPUs, and 2 GB memory. For the specification of product models, see [Product Information](#).
- Subscribe HuaweiCloud.

Installation Steps

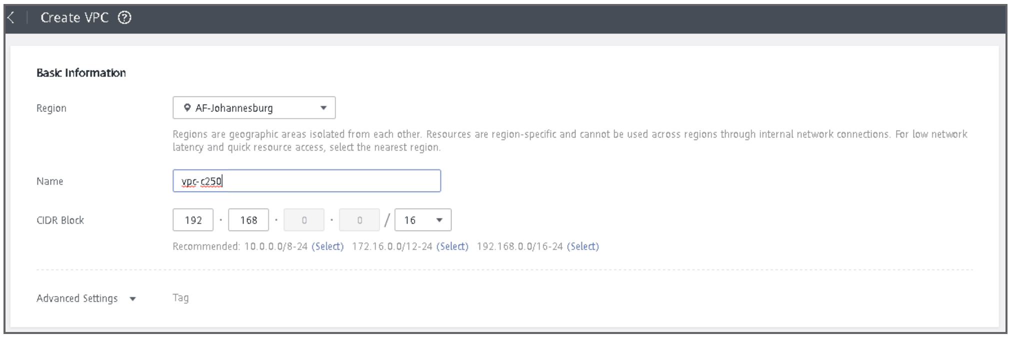
Step 1: Creating a Virtual Private Cloud(VPC)

1. Log in to HuaweiCloud and click **Console**. Hover your mouse over the **Service List** navigation bar and select **Networking** > **Virtual Private Cloud**.



2. On the Virtual Private Cloud page, click Create VPC in the upper-right corner.

3. On the Create VPC page, configure parameters such as the name of the VPC, the CIDR block, and the default subnet. Click **Create Now**.



Basic Information

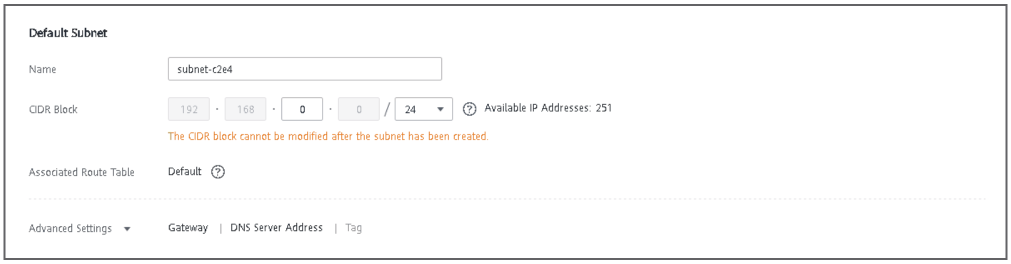
Region: AF-Johannesburg

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region.

Name: vpc-c250

CIDR Block: 192 · 168 · 0 · 0 / 16

Recommended: 10.0.0.0/8-24 (Select) 172.16.0.0/12-24 (Select) 192.168.0.0/16-24 (Select)



Default Subnet

Name: subnet-c2e4

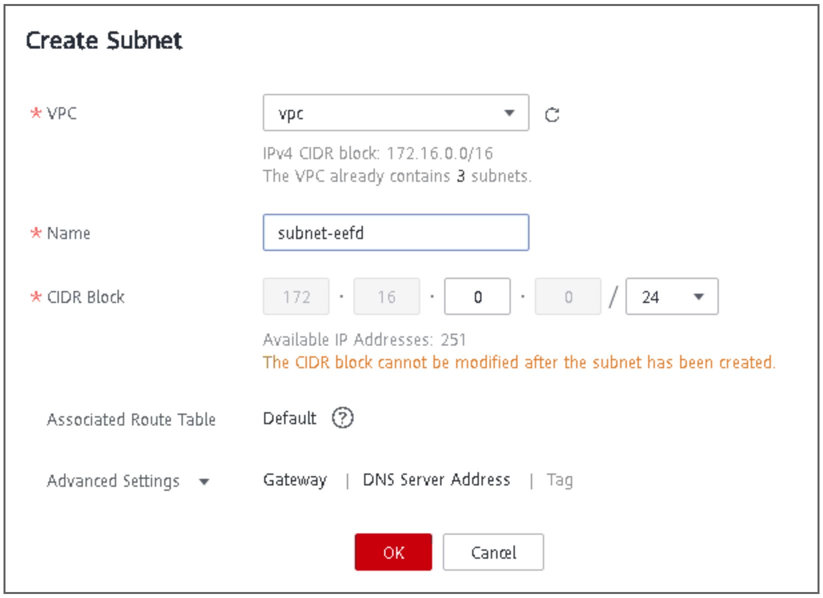
CIDR Block: 192 · 168 · 0 · 0 / 24 Available IP Addresses: 251

The CIDR block cannot be modified after the subnet has been created.

Associated Route Table: Default

4. Wait a few seconds, then you can view the created virtual private cloud on the VPC list.

5. Click **Subnets** in the left **Network Console** column. On the Subnets page, click **Create Subnet** in the upper-right corner to go to the pop-up **Create Subnet** dialog box.



Create Subnet

* VPC: vpc

IPv4 CIDR block: 172.16.0.0/16
The VPC already contains 3 subnets.

* Name: subnet-eefd

* CIDR Block: 172 · 16 · 0 · 0 / 24

Available IP Addresses: 251
The CIDR block cannot be modified after the subnet has been created.

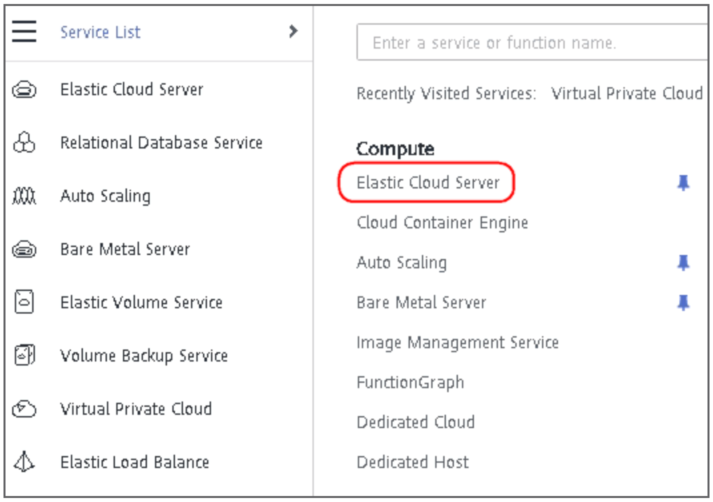
Associated Route Table: Default

On the Create Subnet dialog box, configure the following options.

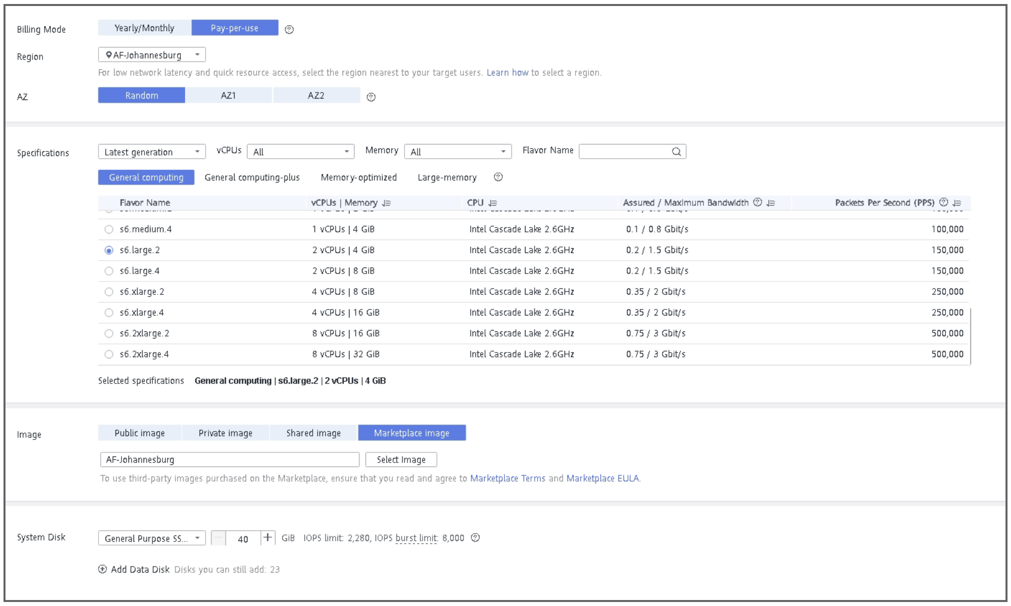
Option	Description
VPC	Specifies the VPC of the subnet.
Name	Specifies the name of the subnet.
IPv4 CIDR Block	Specifies the IPv4 CIDR block, which should be in the available range.
AZ	Specifies the AZ of the subnet.

Step 2: Creating a Cloud Server/ Deploying the CloudEdge

1. Hover your mouse over the **Service List** navigation bar and select **Compute** > **Elastic Cloud Server**.



2. Click Buy ECS in the upper-right corner and configure the following options.



Billing Mode: Yearly/Monthly | **Pay-per-use**

Region: AF-Johannesburg

For low network latency and quick resource access, select the region nearest to your target users. Learn how to select a region.

AZ: **Random** | AZ1 | AZ2

Specifications: Latest generation; vCPUs: All; Memory: All; Flavor Name

General computing | General computing-plus | Memory-optimized | Large-memory

	Flavor Name	vCPUs | Memory	CPU	Assured / Maximum Bandwidth	Packets Per Second (PPS)
○	s6.medium.4	1 vCPUs | 4 GiB	Intel Cascade Lake 2.6GHz	0.1 / 0.8 Gbit/s	100,000
●	s6.large.2	2 vCPUs | 4 GiB	Intel Cascade Lake 2.6GHz	0.2 / 1.5 Gbit/s	150,000
○	s6.large.4	2 vCPUs | 8 GiB	Intel Cascade Lake 2.6GHz	0.2 / 1.5 Gbit/s	150,000
○	s6.xlarge.2	4 vCPUs | 8 GiB	Intel Cascade Lake 2.6GHz	0.35 / 2 Gbit/s	250,000
○	s6.xlarge.4	4 vCPUs | 16 GiB	Intel Cascade Lake 2.6GHz	0.35 / 2 Gbit/s	250,000
○	s6.2xlarge.2	8 vCPUs | 16 GiB	Intel Cascade Lake 2.6GHz	0.75 / 3 Gbit/s	500,000
○	s6.2xlarge.4	8 vCPUs | 32 GiB	Intel Cascade Lake 2.6GHz	0.75 / 3 Gbit/s	500,000

Selected specifications **General computing | s6.large.2 | 2 vCPUs | 4 GiB**

Image: Public image | Private image | Shared image | **Marketplace image**

AF-Johannesburg | Select Image

To use third-party images purchased on the Marketplace, ensure that you read and agree to Marketplace Terms and Marketplace EULA.

System Disk: General Purpose SS... | 40 | GiB IOPS limit: 2,280, IOPS burst limit: 8,000

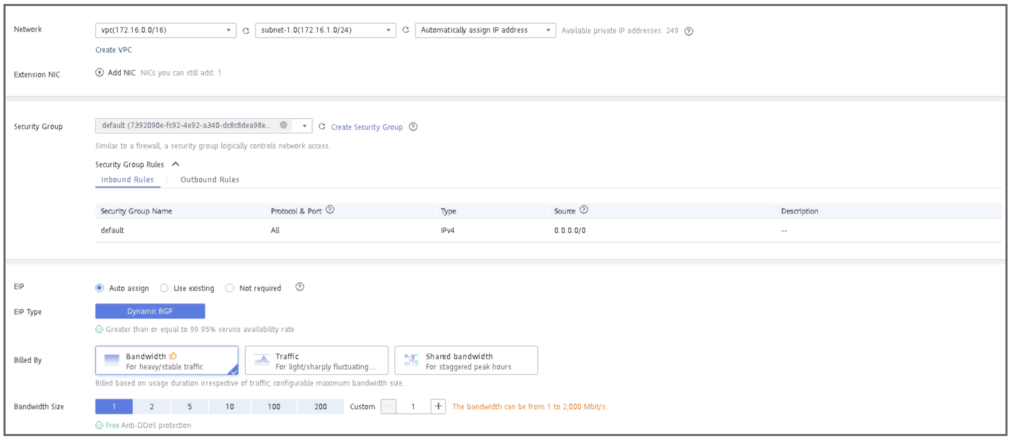
⊕ Add Data Disk Disks you can still add: 23

On the Configure Basic Settings page, configure the following options:

Option	Description
Billing Mode	You can select the billing mode according to your own needs.
Region	Specifies the geographic region of the elastic cloud server. The region specified here should conform to the region of the VPC.
AZ	Specifies the AZ of the elastic cloud server. The AZ specified here should conform to the AZ of the subnet.
CPU Architecture	Select "X86".
Specifications	CloudEdge vFW requires at least 2 vCPUs, 2 GB memory, and a 4 GB hard drive. The **General computing** | s6.large.2 |

Option	Description
	2vCPUs | 4GiB here is used as an example.
Image	Click **Marketplace image** to go to the **Select Marketplace Image** page. Select **Infrastructure Software** > **Security**, and then select "Hillstone CloudEdge Virtual-Firewall (BYOL)". Click **OK**.
System Disk	You can select the system disk according to your own needs. "General Purpose SSD, 40 GiB" is recommended.

3. Click **Next: Configure Network** and configure the following options.



Network: vpc(172.16.0.0/16) | subnet-1.0(172.16.1.0/24) | Automatically assign IP address | Available private IP addresses: 249

Create VPC

Extension NIC: Add NIC NICs you can still add: 1

Security Group: default (7392090e-fc92-4e92-a340-dc8c8dea98e... | Create Security Group

Similar to a firewall, a security group logically controls network access.

Security Group Rules

Inbound Rules | Outbound Rules

Security Group Name	Protocol & Port	Type	Source	Description
default	All	IPv4	0.0.0.0/0	--

EIP: ● Auto assign ○ Use existing ○ Not required

EIP Type: Dynamic BGP

Greater than or equal to 99.95% service availability rate

Billed By: Bandwidth For heavy/stable traffic | Traffic For light/sharply fluctuating ... | Shared bandwidth For staggered peak hours

Billed based on usage duration irrespective of traffic; configurable maximum bandwidth size.

Bandwidth Size: 1 | 2 | 5 | 10 | 100 | 200 | Custom 1 The bandwidth can be from 1 to 2,000 Mbit/s.

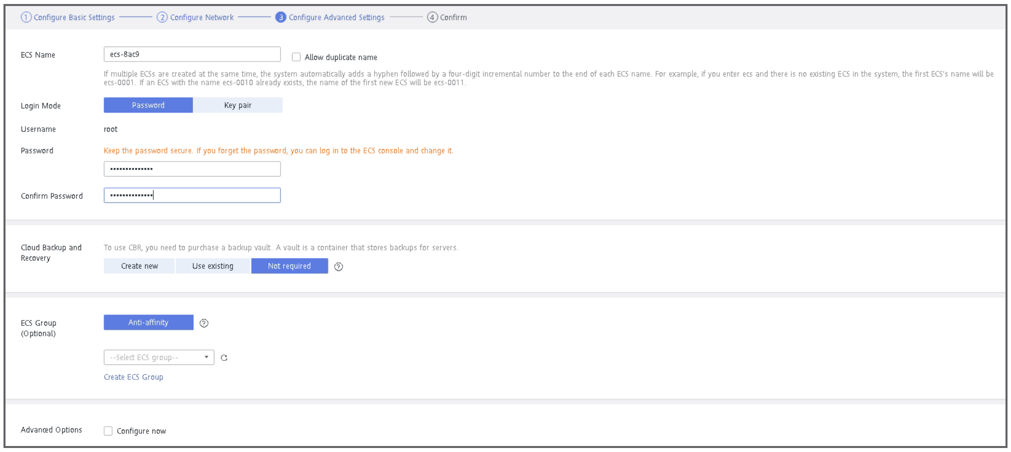
Free Anti-DDoS protection

On the Configure Network page, configure the following options.

Option	Description
Network	Select the VPC and the subnet created in Sept 1, such as "vpc-test" and its subnet.
Security Group	You can select the security group according to your own needs. The security group selected here should be permitted by both inbound and outbound rules.

Option	Description
EIP	You should select **Auto assign** if you need to access CloudEdge from the Internet.
EIP Type	You can select the EIP type according to your own needs. "Static BGP" is used as an example here.
Billed By and Bandwidth Size	You can select the billing method according to your own needs. "Billed by Brandwidth, 1 Mbit/s" is recommended.

4. Click **Next: Configure Advanced Settings** to configure the following options.



ECS Name: ecs-8ac9 ☐ Allow duplicate name

If multiple ECSs are created at the same time, the system automatically adds a hyphen followed by a four-digit incremental number to the end of each ECS name. For example, if you enter ecs and there is no existing ECS in the system, the first ECS's name will be ecs-0001. If an ECS with the name ecs-0010 already exists, the name of the first new ECS will be ecs-0011.

Login Mode: [✓ Password] Key pair

Username: root

Password: Keep the password secure. If you forget the password, you can log in to the ECS console and change it.
••••••••••••••

Confirm Password: ••••••••••••••

Cloud Backup and Recovery: To use CBR, you need to purchase a backup vault. A vault is a container that stores backups for servers.
Create new Use existing [✓ Not required]

ECS Group (Optional): [✓ Anti-affinity]
--Select ECS group--
Create ECS Group

Advanced Options: ☐ Configure now

On the Configure Advanced Settings page, configure the following options.

Option	Description
ECS Name	Specifies the name of the ECS, such as "vfw-test".
Login Mode	You can select the login mode according to your own needs. If you select the password mode, you need to configure and confirm the password according to the password policy.

Option	Description
Cloud Backup and Recovery	You can decide whether to use the Cloud Backup and Recovery service or not.

5. Click **Next: Confirm**. On the **Confirm** page, select "default" for **Enterprise Project** and tick the **I have read and agree to the Image Disclaimer.** check box.

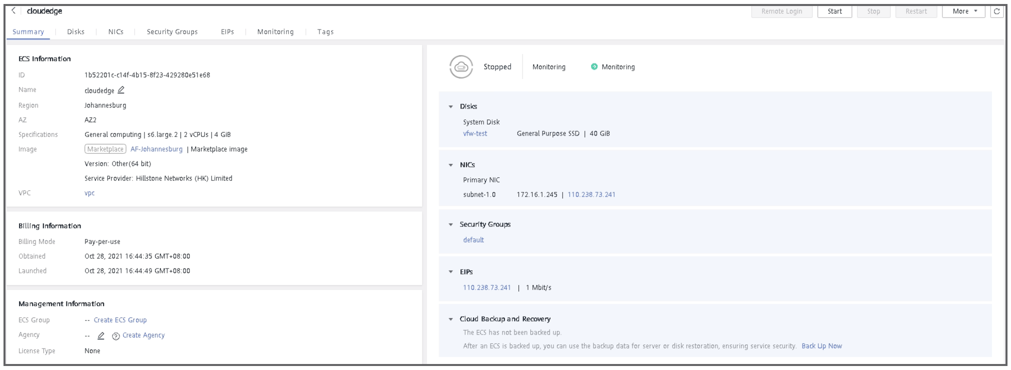
6. Click **Submit**. Click **Pay**. You will see a message indicating that the cloud server is successfully created. That is to say, the deployment of CloudEdge is completed.

Step 3: Accessing CloudEdge

To access the firewall after the creation of the elastic cloud server, take the following steps:

1. Log in to HuaweiCloud and go to the Console page. Select **Cloud Server Console** > **Elastic Cloud Server**.

2. Click the ECS on the ECS list to go to its details page.



ECS Information

ID 1b52201c-c14f-4b15-8f23-429280e51e68

Name cloudedge

Region Johannesburg

AZ AZ2

Specifications General computing | s6.large.2 | 2 vCPUs | 4 GiB

Image Marketplace AF-Johannesburg | Marketplace image

Version: Other(64 bit)

Service Provider: Hillstone Networks (HK) Limited

VPC vpc

Billing Information

Billing Mode Pay-per-use

Obtained Oct 28, 2021 16:44:35 GMT+08:00

Launched Oct 28, 2021 16:44:49 GMT+08:00

Management Information

ECS Group -- Create ECS Group

Agency -- Create Agency

License Type None

Stopped Monitoring Monitoring

Disks

System Disk

vfw-test General Purpose SSD | 40 GiB

NICs

Primary NIC

subnet-1.0 172.16.1.245 | 110.238.73.241

Security Groups

default

EIPs

110.238.73.241 | 1 Mbit/s

Cloud Backup and Recovery

The ECS has not been backed up.

After an ECS is backed up, you can use the backup data for server or disk restoration, ensuring service security. Back Up Now

3. Click **Remote Login** in the upper-right corner to go to the CLI interface of CloudEdge.

Accessing CloudEdge from the Internet

By default, the SSH and HTTPS protocols are enabled. You can access CloudEdge by using the elastic IP bound to the ECS through these two protocols.

Logging in via SSH2

1. Open the remote terminal login software. Here, SecureCRT is taken as an example.
2. Click **File** > **Quick Connect**, and then select SSH2 in Protocol drop-down list.
3. Enter the elastic public IP in the **Hostname** text box.
4. Enter the name of the VPC created in Step 1 in the **Username** text box.
5. Click **Connect**.
6. Enter the password configured in Step 1 and then click **OK** to log in.

Logging in via HTTPS

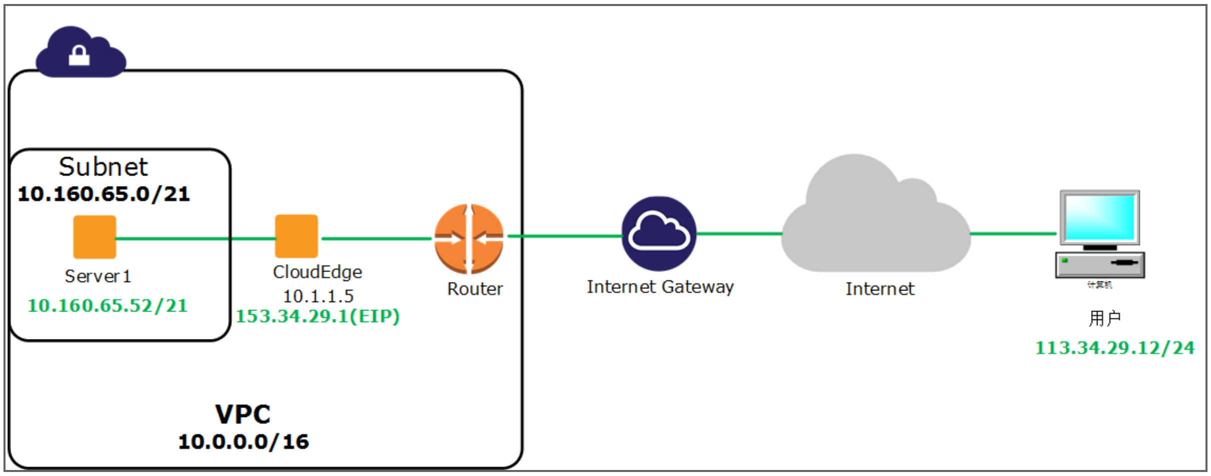
1. Open the browser and enter the https://elastic IP address.
2. Enter the name and password configured in Step 1 on the login page.
3. Press the Enter key to log in.

For more information on the operation of the firewall, see StoneOS User Guide (Click here).

Allowing Remote Users to Access VPC via SSL VPN

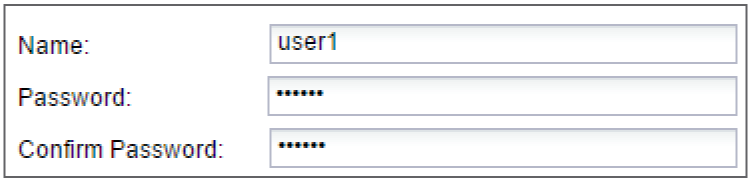
This example shows how to use SSL VPN to provide remote users with access to servers in own VPC.

The topology describes a remote user trying to visit the Server1 within a VPC located in a public cloud platform. Using SSL VPN tunnel, the connection between remote users and server in VPC is encrypted and safe.



Step 1: Creating a User

Select **Object** > **User**. In the Local User tab, under Local Server, click **New** > **User**.



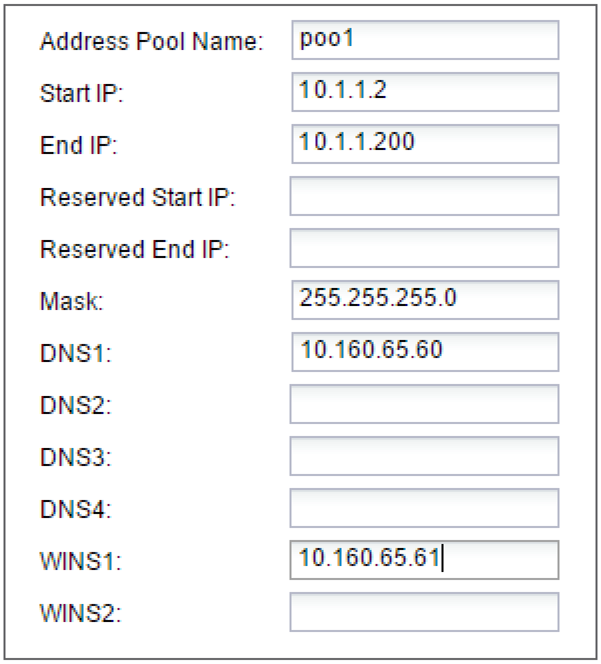
Name:	user1
Password:	••••••
Confirm Password:	••••••

- Name: user1
- Password: 123456
- Confirm Password: 123456

Note: You can choose other types of AAA server to create new users according to your actual requirements.

Step 2: Configuring SCVPN Address Pool

Select **Network > VPN > SSL VPN**, and click **Address Pool**. In the prompt, click **New**.

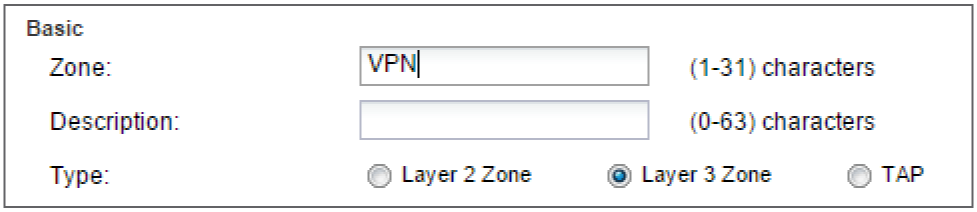


Address Pool Name:	poo1
Start IP:	10.1.1.2
End IP:	10.1.1.200
Reserved Start IP:	
Reserved End IP:	
Mask:	255.255.255.0
DNS1:	10.160.65.60
DNS2:	
DNS3:	
DNS4:	
WINS1:	10.160.65.61
WINS2:	

- Address Pool Name: pool1
- Start IP: 10.1.1.2
- End IP: 10.1.1.200
- Mask: 255.255.255.0
- DNS1: 10.160.65.60
- WINS1: 10.160.65.61

Step 3: Creating Tunnel Interface

Select **Network** > **Zone**, and click **New**.



Basic

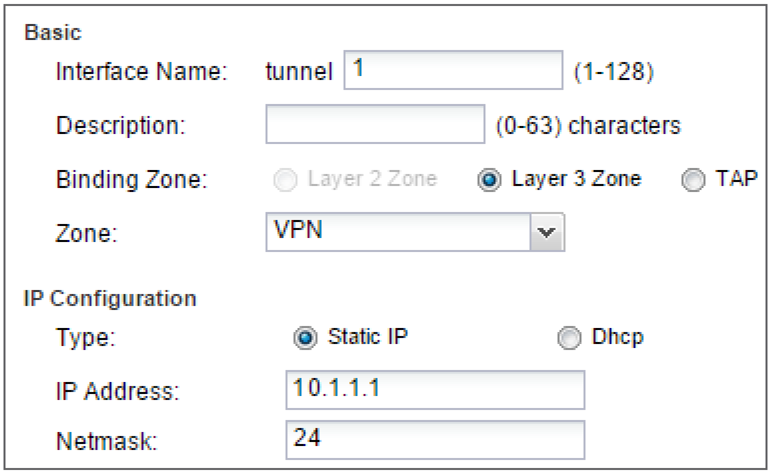
Zone: VPN (1-31) characters

Description: (0-63) characters

Type: ○ Layer 2 Zone ● Layer 3 Zone ○ TAP

- Zone: VPN
- Type: Layer 3 Zone

Select **Network** > **Interface**, and click **New** > **Tunnel Interface**.



Basic

Interface Name: tunnel 1 (1-128)

Description: (0-63) characters

Binding Zone: ○ Layer 2 Zone ● Layer 3 Zone ○ TAP

Zone: VPN

IP Configuration

Type: ● Static IP ○ Dhcp

IP Address: 10.1.1.1

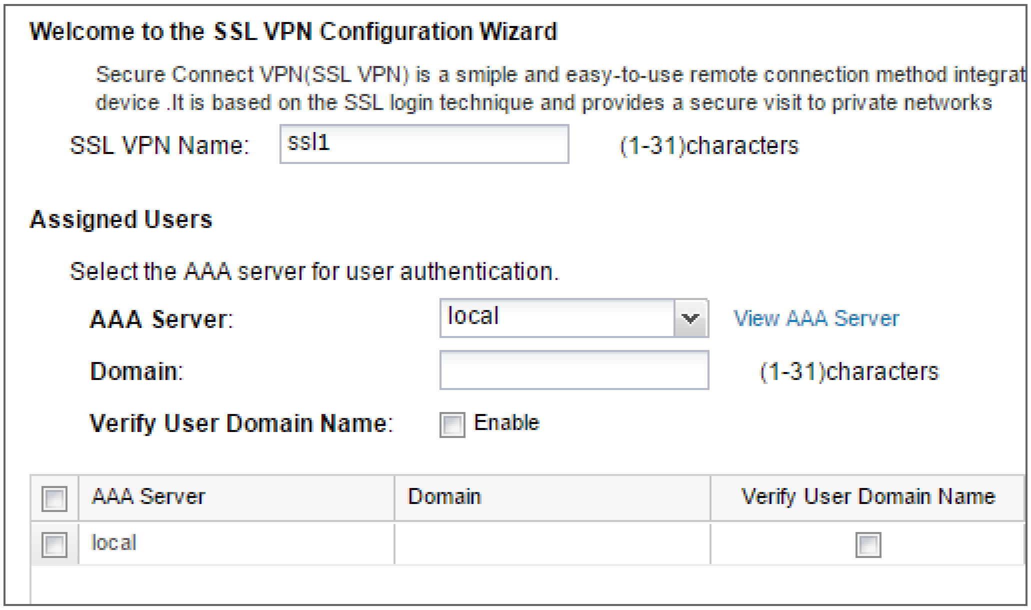
Netmask: 24

- Interface Name: tunnel1
- Binding Zone: Layer 3 Zone
- Zone: VPN
- Type: Static IP
- IP Address: 10.1.1.1
- Netmask: 24

Note: Tunnel interface must be of the same network segment of SSL VPN address pool and not in the pool.

Step 4: Configuring SCVPN

Select **Network** > **VPN** > **SSL VPN**, and click **New**.



Welcome to the SSL VPN Configuration Wizard

Secure Connect VPN(SSL VPN) is a smiple and easy-to-use remote connection method integrat
device .It is based on the SSL login technique and provides a secure visit to private networks

SSL VPN Name: ssl1 (1-31)characters

Assigned Users

Select the AAA server for user authentication.

AAA Server: local View AAA Server

Domain: (1-31)characters

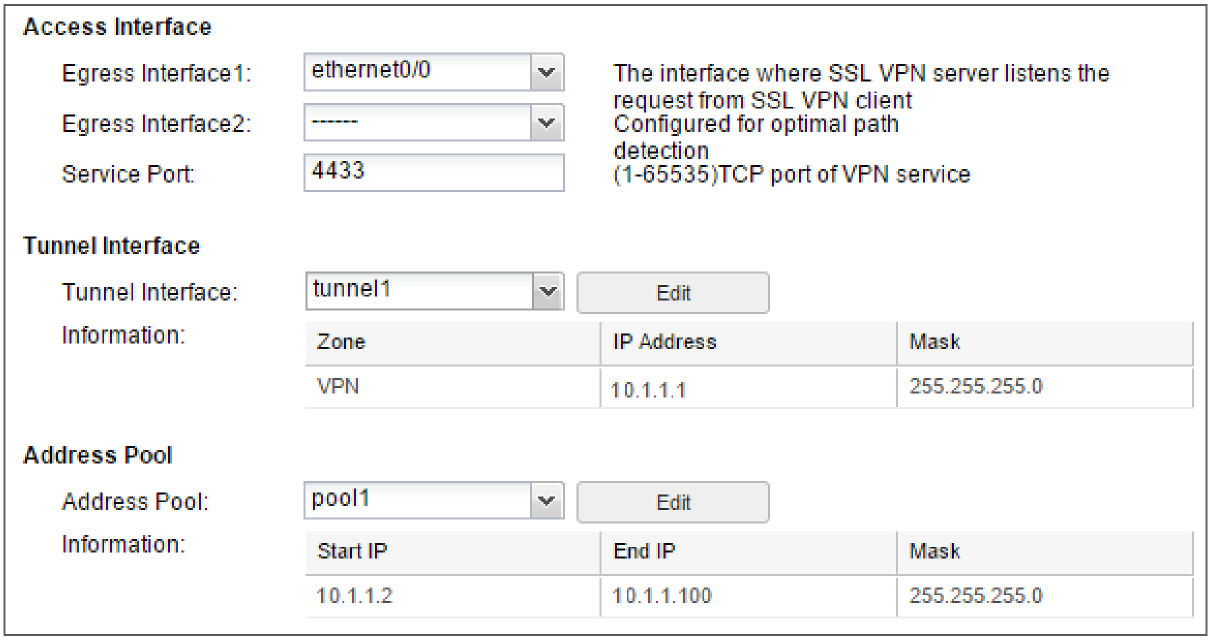
Verify User Domain Name: □ Enable

□	AAA Server	Domain	Verify User Domain Name
□	local		□

In the Name/Access User tab:

- SSL VPN Name: ssl1
- AAA Server: select **local**, and click **Add**

In the Interface tab:



Access Interface

Egress Interface1: ethernet0/0 — The interface where SSL VPN server listens the request from SSL VPN client

Egress Interface2: ------ — Configured for optimal path detection

Service Port: 4433 — (1-65535)TCP port of VPN service

Tunnel Interface

Tunnel Interface: tunnel1

Information:

Zone	IP Address	Mask
VPN	10.1.1.1	255.255.255.0

Address Pool

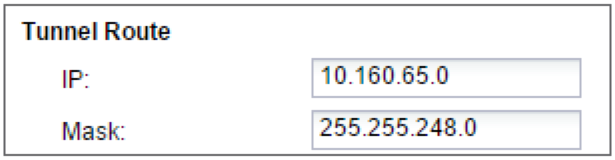
Address Pool: pool1

Information:

Start IP	End IP	Mask
10.1.1.2	10.1.1.100	255.255.255.0

- Egress Interface 1: ethernet0/0
- Service port: 4433
- Tunnel Interface: tunnel1
- Address Pool: pool1

In the Tunnel Route tab:



Tunnel Route

IP: 10.160.65.0

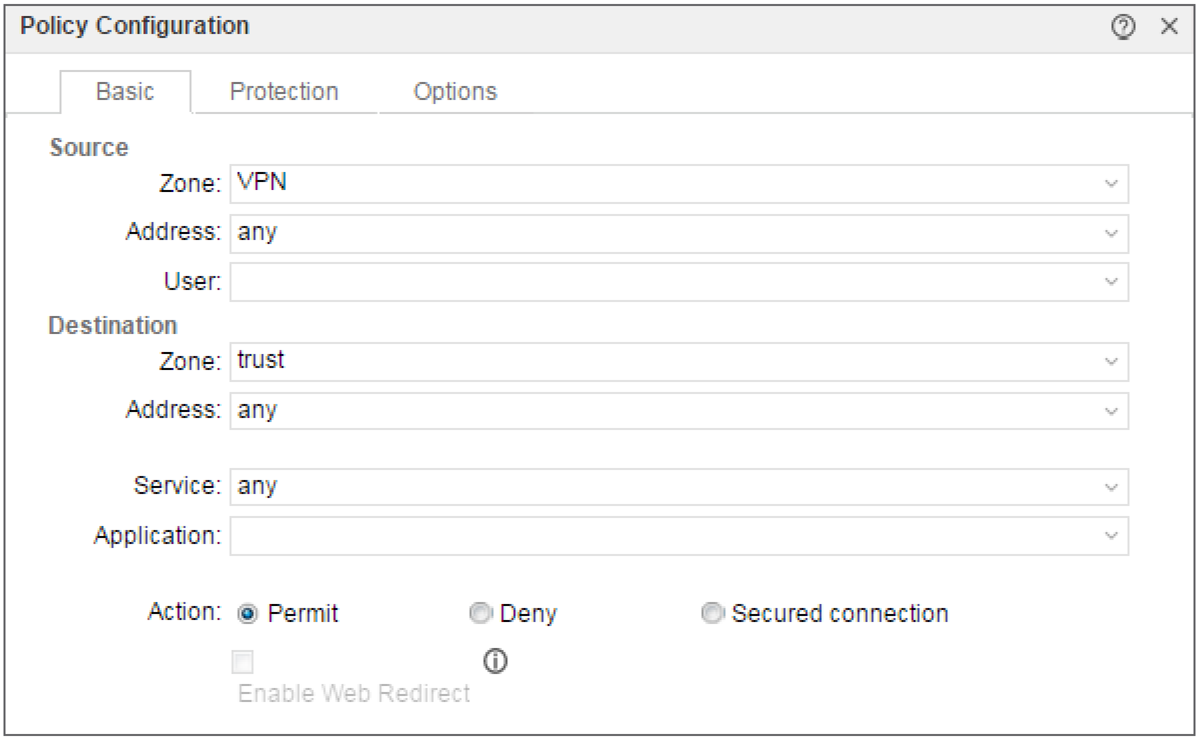
Mask: 255.255.248.0

- IP: 10.160.65.0
- Netmask: 255.255.248.0

Note: Tunnel route must be of the same network segment of internal server ("Server1").

Step 5: Creating Policy from VPN to trust

Select **Policy** > **Security Policy**, and click **New**.



Source

Zone: VPN

Address: any

User:

Destination

Zone: trust

Address: any

Service: any

Application:

Action: ● Permit ○ Deny ○ Secured connection

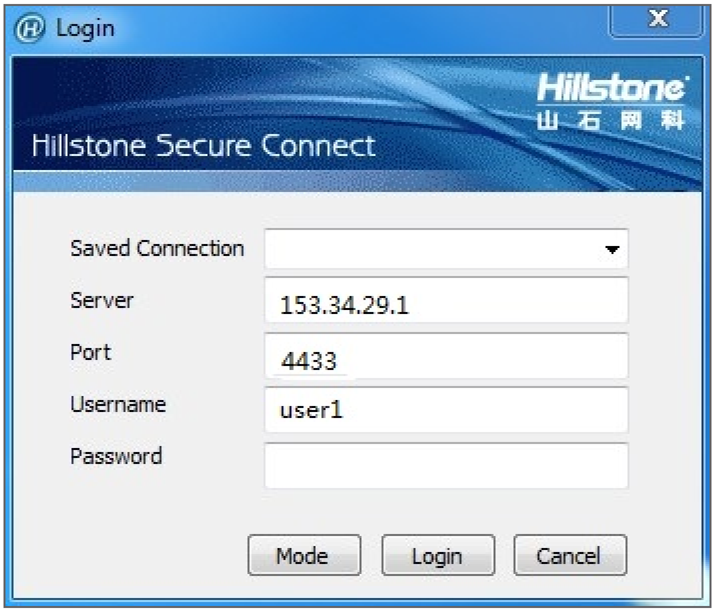
□ Enable Web Redirect

- Source Information
  - Zone: VPN
  - Address: Any
- Destination Information
  - Zone: trust
  - Address: Any
- Other Information
  - Service: Any

- Action: Permit

Step 6: Accessing the Resources in VPC

After configuration, the remote user enters address "https://153.34.29.1:4433" in a browser. The browser will show login page. Enter username and password ("user1" and "123456"), and then click **Login**. The browser will prompt to hint you to download the VPN client. Follow the steps to download and install the scvpn client. The remote user click open the Hillstone Secure Connect client, and enter information below:



Saved Connection

Server 153.34.29.1

Port 4433

Username user1

Password

- Server: 153.34.29.1
- Port: 4433
- Username: user1
- Password: 123456

When the icon in the taskbar becomes green, the client is connected. Then, the remote user can access the Server1 via SSL VPN.