Hillstone Networks, Inc.

CloudEdge Deployment Guide

Version 5.5R4

Hillstone Networks, Inc.

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 Networks, Inc.CloudEdge .

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

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

hs-doc@hillstonenet.com

Hillstone Networks, Inc.

www.hillstonenet.com

TWNO: TW-DPL-VFW-EN-5.5R4-EN-V4.0-2017/3/6

Table of Contents

Overview

The virtualization product of Hillstone Networks, Inc. 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, Inc.. 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 two models: SG-6000-VM01 and SG-6000-VM02. 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 3). The required configuration of virtual machine is as listed below:

Configuration	SG6000-VM01	SG6000-VM02
Minimum	1CPU / 1GB memory	2CPU / 2GB memory
Recommended	1CPU / 8GB memory	2CPU / 8GB memory

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

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

CloudEdge licenses are categorized to platform licenses, sub licenses, function licenses and private cloud platform licenses. A platform license is the base to install all other types of licenses.

Note: 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

- **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.

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.

Note:

- Besides the licenses listed above, a hardware platform from Hillstone Networks, Inc. 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.

Private Cloud Platform Licenses

Private cloud platform licenses include platform trial licenses and platform base licenses. To be compatible with CloudEdge licenses for various cloud environments, please install the private cloud platform license first and insert the USB-Key after reboot when you deploy CloudEdge in a private cloud environment. After the installation of the private cloud platform license, the initial SN of the system will be replaced with the SN in the private cloud platform license, so licenses for CloudEdge deployed in non-private cloud environment can be installed in the current system and the priority is higher than that of the private cloud.

When the private cloud platform license expires, the sub license and function license are still valid. However, the relevant functions ares not configurable until the system is restarted.

If private cloud platform license is uninstalled and there is no license for private cloud environment, the SN will be restored to the initial SN after reboot. At the same time, all non-private cloud licenses that has been installed will be invalid.

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.

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.

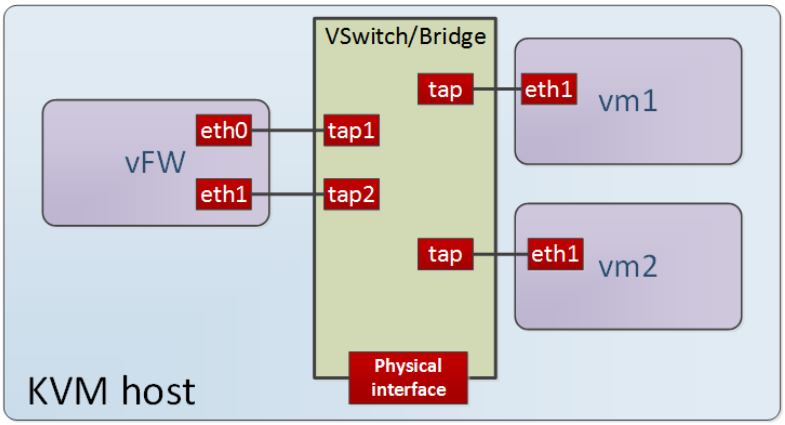
System Requirements

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

- Support Intel VT or AMD-V
- Be able to allocate at least two virtual network cards
- 64 bit CPU which can provide two virtual cores
- Linux system (Ubuntu 14.04 is recommended)
- 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。

Installing vFW on KVM Host

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

Step 1: Acquiring vFW software package

1. Contact salesperson to get the address of downloading vFW KVM software package.
2. The package will include:
   - **vFw script file** (with name "hsvfw"). The script file contains commands that can install, upgrade or restart vFW.
   - **vFW image file** (an .iso file, e.g. SG6000-VFW02-V6-r1230.iso), the vFW system image.
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.

```
hillstone@vfw:~$ rz
rz waiting to receive.
Starting zmodem transfer.  Press Ctrl+C to cancel.
Transferring SG6000-MX_MAIN-VFW02-V6-r1230.iso...
  100%   78180 KB 3127 KB/s 00:00:25       0 Errors
```

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

   ls

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

```
 hillstone@vfw:~$ ls
hsvfw    SG6000-MX_MAIN-VFW02-V6-r1230.iso
```

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

   sudo ./hsvfw install ./*vfw_iso* [**vm01|vm02**] *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_iso*	Define the vFW image name, including suffix ".iso".
vm01 | vm02	Define the vFW model. vm01 represents SG6000-VM01, and vm02 is SG6000-VM02.
vm_name	Specify a name for your vFW.
if_num	Specify how many interfaces in your vFw. You can have 10 interfaces at most.

For instance, the command below will create a vFW named "vfwname" of model SG6000-VM02 with 2 interfaces.

```
hillstone@vfw:~$ sudo ./hsvfw install ./SG6000-VFW00-5.0R0-D0203.iso vm02 vfwname 2
[sudo] password for hillstone:
1+0 records in
1+0 records out
1048576 bytes (1.0 MB) copied, 0.00199942 s, 524 MB/s
Network vfwname-eth0 defined from /var/lib/vfw/vfwname/vfwname-eth0

Network vfwname-eth0 marked as autostarted

Network vfwname-eth0 started

Network vfwname-eth1 defined from /var/lib/vfw/vfwname/vfwname-eth1

Network vfwname-eth1 marked as autostarted

Network vfwname-eth1 started


Starting install...
Creating domain...
error: XDG_RUNTIME_DIR not set in the environment.
Cannot open display:
Run 'virt-viewer --help' to see a full list of available command line options
Domain creation completed. You can restart your domain by running:
  virsh --connect qemu:///system start vfwname
vFW vfwname installed.
  Console access: telnet localhost 7014
  SSH access: ssh hillstone@192.168.144.2
hillstone@vfw:~$
```

6. Linux will print the port number of Console, e.g. 7014 in the example.

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

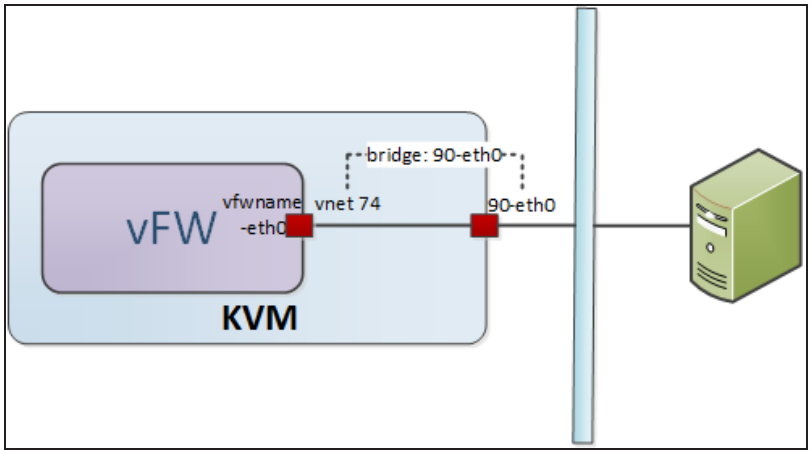
   password: hillstone

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.

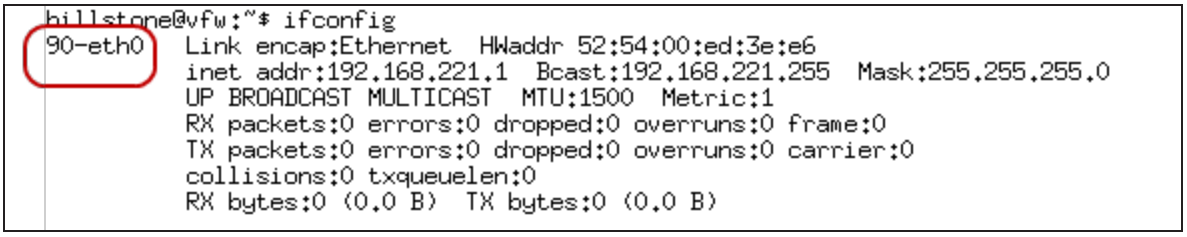
Using the example below, we will introduce how to connect "vnet0" (vFW) to "90-eth0" (a physical interface of KVM host).



Step 1: Viewing interfaces

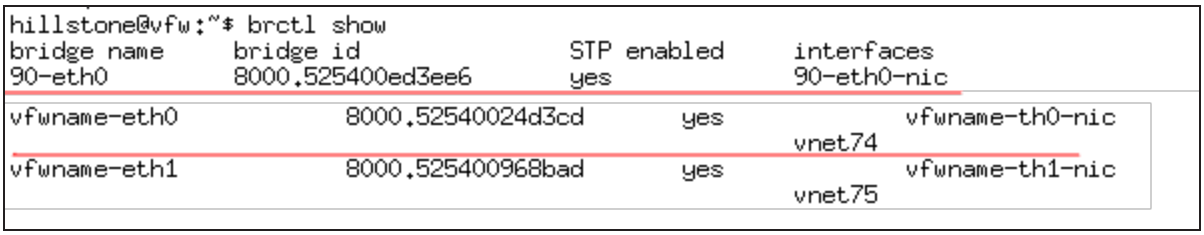
In this example, a physical network (e.g. company's internal network) is connected to the physical interface of KVM host. You may view the interface information of KVM host interface and vFW interfaces.

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



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".



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.

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":

```
hillstone@vfw:~$ ./hsvfw show vfwname
VFW instance: 14
VFW instance name: vfwname
Version: SG6000-VFW00-5.0R0-D0203.iso
Status: running
Console port: 7014
VNC port: :16
Mgmt address: 192.168.144.2
Interface count: 2
Interface detail:
Interface  Type       Source     Model       MAC
-------------------------------------------------------
vnet74     network    vfwname-eth0 virtio      52:54:00:0e:12:00
vnet75     network    vfwname-eth1 virtio      52:54:00:0e:12:01
```

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

Note: 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*.

If your firewall is older than 5.5R1P7.1, you should use the method below to upgrade your system. The target system should also be older than 5.5R1P7.1.

To upgrade a vFW's StoneOS system, use the command:

1. Use command **rz** to upload new image file.
2. Use the following command to start uploading system:

   sudo ./hsvfw upgrade *vm_name* **./***new_vfw_iso*

./hsvfw upgrade	This is the upgrade command in the script.
vm-name	Specify the name of vFW you want to upgrade.
./*new_vfw_iso*	Enter the name of new image file, including suffix ".iso".

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, eth-0/0 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 7)
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).

Deploying CloudEdge on OpenStack

System Requirements

To deploy vFW on an OpenStack platform, the host should meet the following requirements:

- Support Intel VT or AMD-V
- Be able to allocate at least two virtual network cards
- 64 bit CPU which can provide two virtual cores
- Linux system (Ubuntu 14.04 is recommended)
- The Linux system is installed with OpenStack (Icehouse 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/).

Installing vFW on OpenStack Platform

Step 1: Importing image file

1. Use the command to open a dialog box. Browse your PC and select vFW's system file. The system file will be uploaded to the root directory of Linux host.

   rz

2. To save the system file as an OpenStack image file, use the following command:

   glance image-create --name=*image-name* **--property hw_vif_model=virto --disk-format**=iso **--container-form-at=bare --is-public=true <***vfw_iso*

glance image-create	Create an image
--name=*image-name*	Specify a name for the image
--property	Begin defining the image's properties
hw_vif_model=virtio	This indicates the interface model is virtio.
--disk-format=iso	This indicates the imported file format is iso.
--container-format=bare	This indicates there is no container or metadata envelope for the image
--is-public=true	This indicates this image is public to all.
vfw_iso	Enter the name of vFW system file, including suffix .iso.

   For instance, the command below creates a vFW image "image-vfw".

   glance image-create --name=image-vfw --property hw_vif_model=virtio --disk-format=iso --container-form-at=bare --is-public=true <SG6000-MX_MAIN-VFW02-V6-r1230.iso

   This command returns the following results:

```
+--------------------------+--------------------------------------+
| Property                 | Value                                |
+--------------------------+--------------------------------------+
| Property 'hw_vif_model'  | virtio                               |
| checksum                 | a1c764edc703654e230ca04f1b4ddc73     |
| container_format         | bare                                 |
| created_at               | 2015-01-08T08:59:37                  |
| deleted                  | False                                |
| deleted_at               | None                                 |
| disk_format              | iso                                  |
| id                       | 4d1e1c30-4eec-4b67-9072-686a1ac24fd9 |
| is_public                | True                                 |
| min_disk                 | 0                                    |
| min_ram                  | 0                                    |
| name                     | image-vfw                            |
| owner                    | a925cd9e37e0496fb5e535ad4bbf99c4     |
| protected                | False                                |
| size                     | 80056320                             |
| status                   | active                               |
| updated_at               | 2015-01-08T08:59:39                  |
| virtual_size             | None                                 |
+--------------------------+--------------------------------------+
```

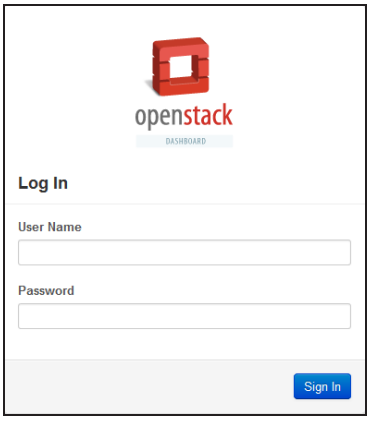
Step 2: Creating a Flavor

Under normal circumstances, a non-admin user cannot change the properties of an instance, including core, memory, etc..

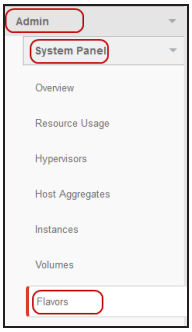
If you want to change an instance, you can change the flavor it belongs to. An instance inherits what its flavor has.

To create a flavor, use admin account and do the following:

1. Login Openstack Web manager with admin account.

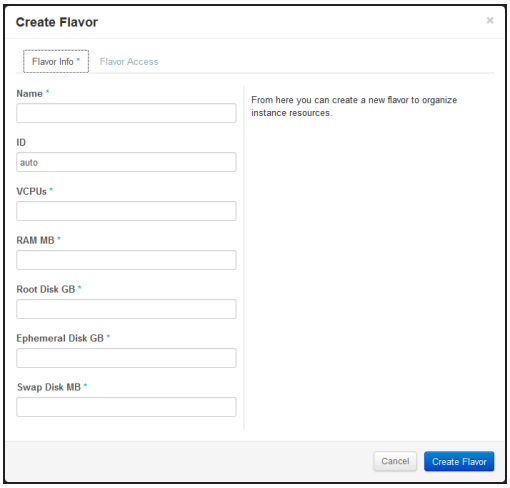


2. From the left navigation, select **Admin > System Panel > Flavors**.



3. Click **Create Flavor** on the top right corner.

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



Enter basic information.

Name	Enter a name for the flavor.
ID	Ignore this. ID is automatically generated by Openstack.
VCPUs	Specify the number of CPU cores. For model VM01, vCPU should be at least 1; for model VM02, vCPU should be at least 2.
RAM MB	Specify the RAM size of the virtual machine. For model VM01, the RAM size should be at least 1024 MB; for model VM02, the size is 2048 at least.

Root Disk	Specify a disk size. The recommended size is at least 2 GB.
Ephemeral Disk	You may ignore this option. No need to use ephemeral disk.
Swap Disk	You may ignore this option. No need to use swap disk.

5. Click **Create Flavor** to finish.

Step 3: Creating a cinder volume

For vFW, a cinder is used to store vFW's configuration files and licenses. If you do not have cinder volume, vFW will lose system configuration after restarting. Without cinder disk, the only way to restore previous configuration is to export and import configuration files.

The cinder disk should be at least 2048 MB.

To create a cinder, use the following steps:

1. Use the command to create a disk:

   dd if=/dev/null of=*diskname* **seek=***block_num* **bs=***bs_size*

dd if=/dev/null	This indicates that "/dev/null" is the device to be used as cinder.
of=<*diskname*	Specify a name for the disk.
seek=*block_num*	Specify how many blocks of the disk.
bs=*bs_size*	Specify the size of each block. It is recommended to use 1 MB block, and create 2048 blocks.

   For instance, this command below creates a disk with name "test".

   dd if=/dev/zero of=<test> seek=2048 bs=1M

2. Use the command to format this disk, so that it can be used as a storage disk.

   mke2fs -t ext4 -qF <*diskname*

mke2fs -t ext4 -qF	Format the disk file to ext4.
diskname	Enter the name of disk created above.

   For instance, this command will format the disk "test".

   mke2fs -t ext4 -qF <test

3. To import the formatted disk into OpenStack:

   glance image-create --disk-format raw **--container-format** bare **--name** *image-name* **<***diskname*

glance image-create	Create an image in OpenStack.
--disk-format raw	Define the disk format as RAW.
--container-format bare	This indicates there is no container or metadata envelope for the image
--name *image-name*	Enter a name for the disk.
<*diskname*	Enter the name of the formatted disk above.

For instance, this command will import the "test" disk and give it a new name "image1" as the image name.

```
glance image-create --disk-format raw --container-format bare --name image1 <test
```

The command will return the following results:

```
+------------------+--------------------------------------+
| Property         | Value                                |
+------------------+--------------------------------------+
| checksum         | d62c4f44d79a2368be3468d6ed0d781f     |
| container_format | bare                                 |
| created_at       | 2015-01-08T07:30:44                  |
| deleted          | False                                |
| deleted_at       | None                                 |
| disk_format      | raw                                  |
| id               | d1385a5c-aa9e-42bf-b82b-17d153470fd1 |
| is_public        | False                                |
| min_disk         | 0                                    |
| min_ram          | 0                                    |
| name             | image1                               |
| owner            | 4280f63e5f6d4ec8a362c8ba2a6e5932     |
| protected        | False                                |
| size             | 2147483648                           |
| status           | active                               |
| updated_at       | 2015-01-08T07:31:35                  |
| virtual_size     | None                                 |
+------------------+--------------------------------------+
```

4. To change the image into a cinder:

```
cinder create --display-name volume-name --image-id $(glance image-list | awk '/vfw-flash-image/{print $2}
') size-num
```

cinder create --display-name *volume-name*	Create a volume and name it.
--image-id $(glance image-list | awk '/*vfw-flash-image***/{print $2}')**	Change the image to a cinder. The glance command in this sentence will look up for the ID of the cinder volume above.
size-num	Specify the size of the cinder. The default unit is GB. The minimum size is 2, which means 2 GB.

For instance, change the image1 to a cinder of size 2 GB, and name it "volumetest":

```
cinder create --display-name volumetest --image-id $(glance image-list | awk '/image1/{print $2}') 2
```

Step 4: Networking vFW

OpenStack provides extensive networking services. Through OpenStack's WebUI manager, a network can be easily created and modified.

To create a network for vFW, please refer to OpenStack help documents (http://docs.openstack.org/user-guide/-content/dashboard_create_networks.html).

Step 5: Starting vFW Instance

To boot vFW instance, use the following command:

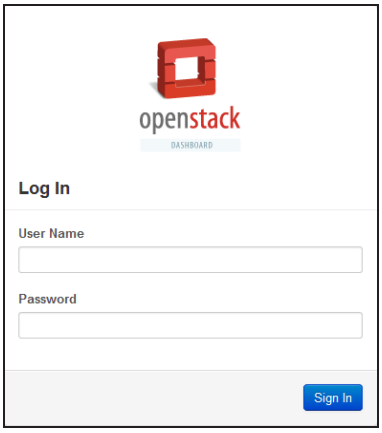
nova boot --image *image-name* **--flavor** *flavor-name* **--nic net-id=$(neutron net-list | awk '/***net1-name***/{print $2}') --nic net-id=$(neutron net-list | awk '/***net2-name***/{print $2}') --nic net-id=$(neutron net-list | awk '/***net3-name***/{print $2}') --block-device-mapping vdb=$(cinder list | awk '/** *volume-name***/ {print $2}'):volume::False** *instance-name*

nova boot	The boot command.
--image *image-name*	Specify the image to start vFW. *image-name* is the vFW image name.
--flavor *flavor-name*	Enter the flavor name.
--nic net-id=$(neutron net-list | awk '/*net-name***/{print $2}')**	This command connects vFW into networks. *net-name* is the network name. Retype this command will connect more networks to vFW.
--block-device-mapping vdb=$(cinder list | awk '/ *volume-name***/ {print $2}'):volume::False**	Enter the cinder name.
instance-name	Specify a name for the vFW instance.

Visiting vFW

After vFW instance is created, follow the steps below to visit vFW:

1. Log in OpenStack.

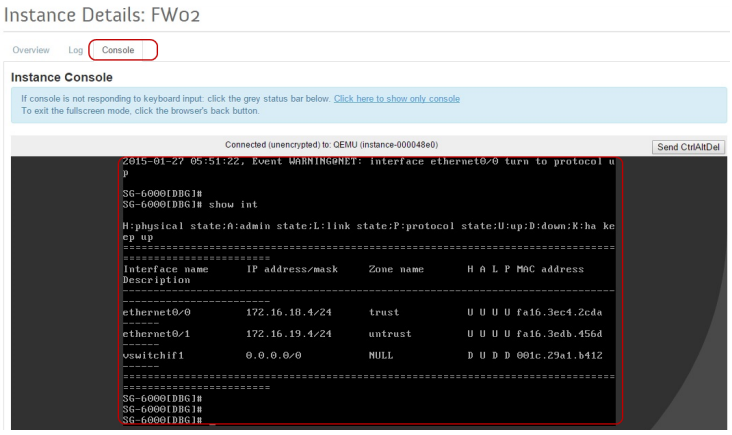


2. Use one of the following steps:

   - If you log in as a normal user, from left navigation, select **Project > Compute > Instances**.
   - If you log in as admin user, from left navigation, select **Admin > System Panel > Instances**.

3. From the list, click the name of vFW.

4. In the new interface, click **Console** and you will be accessed to vFW's StoneOS.



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

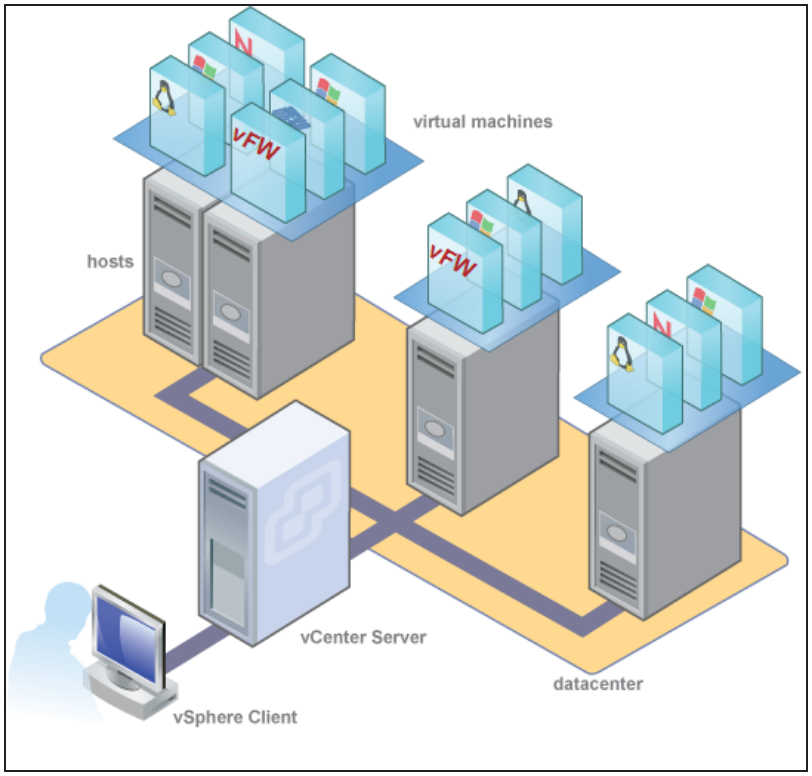
Deploying SG6000-VM on VMware ESXi

CloudEdge is packed in VMDK, ISO 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.
- SG6000-VM01 requires at least 1 vCPU and 1 GB memory; SG6000-VM02 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.

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, ISO file or OVA file(VMDK and OVA file only from 5.5R4). If you deploy vFW for the first time, importing VMDK file or 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.

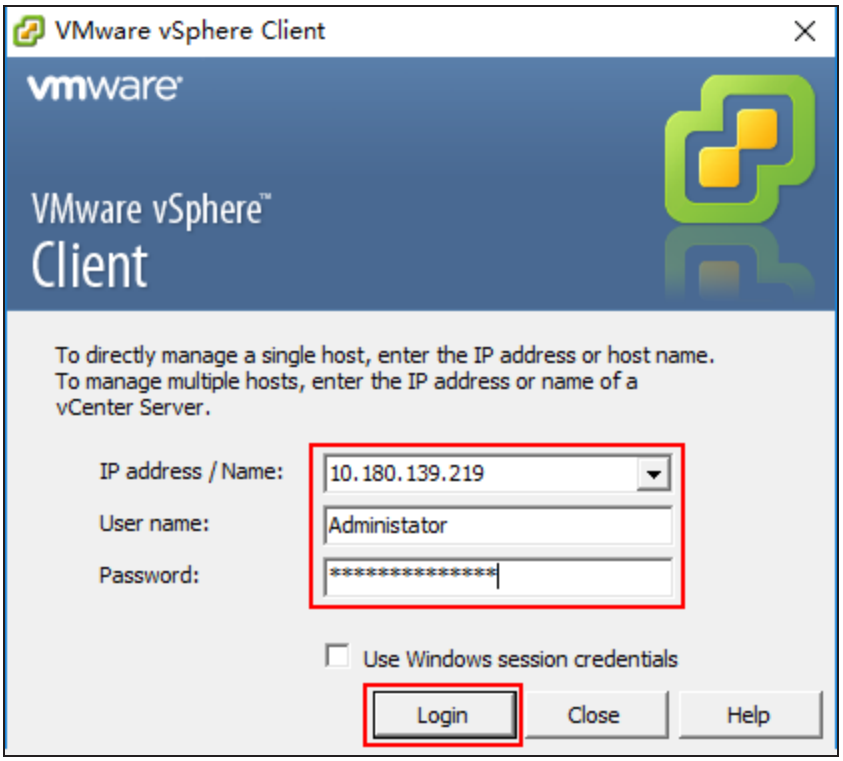
Installing CloudEdge by Importing VMDK

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:

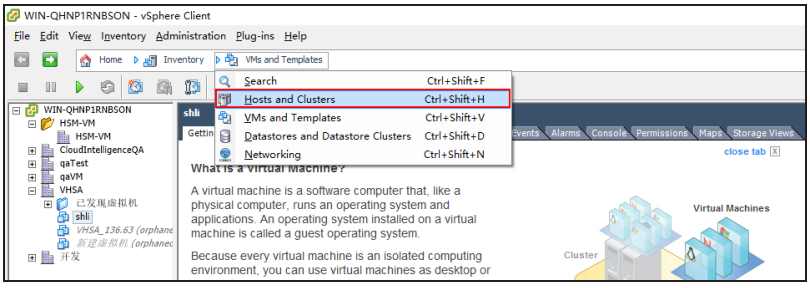
- Step 1: Importing VMDK
- Step 2: Creating a Virtual Machine
- Step 3: Selecting the CloudEdge VMDK File for VM

Step 1: Importing VMDK

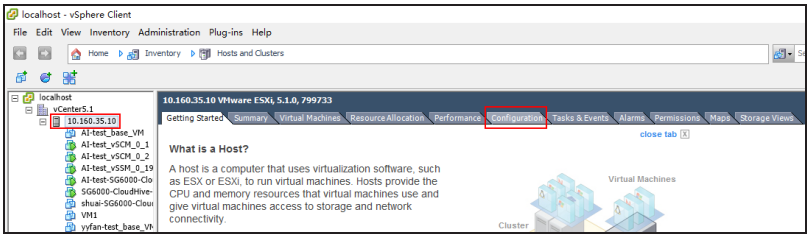
1. Save the CloudEdge VMDK file in your local computer.
2. Double-click the local Sphere Client to enter the login page. In the login page, enter the IP address/Name , username and password of vCenter, and click **Login** to enter the main interface.



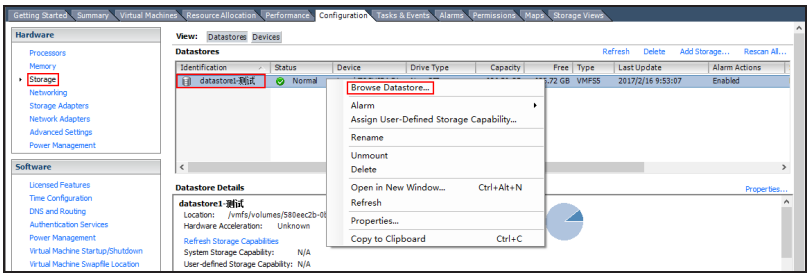
3. In the main interface, select **Home > Inventory > Hosts and Clusters** to enter the Hosts and Clusters page.



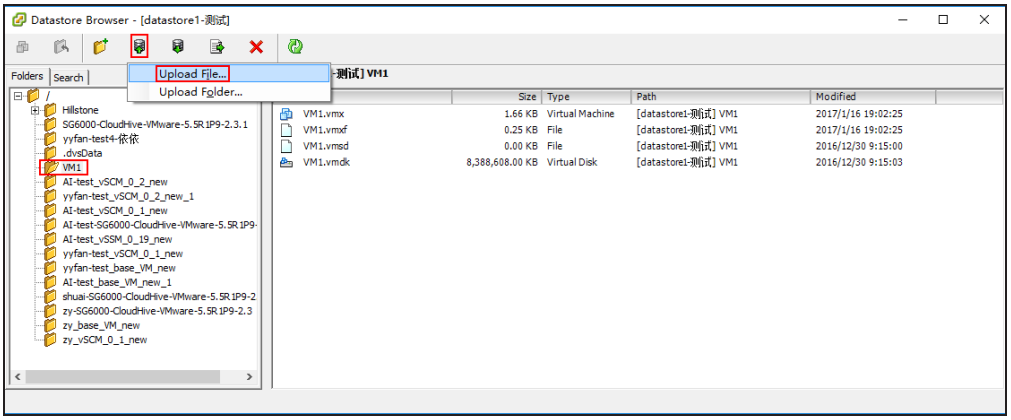
4. In the Hosts and Clusters page, choose the ESXi host which CloudEdge will belong to, and click the **Configuration** tab appears on the right pane to enter the configuration page.



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.

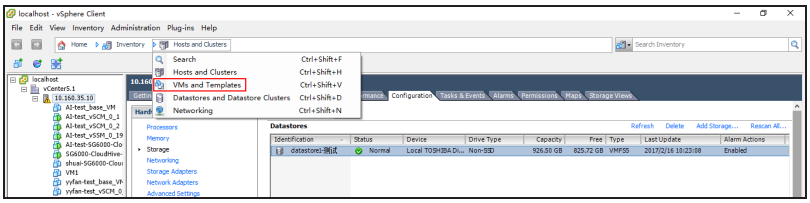


6. In the Datastore Browse page, select the folder to save file and click upload button  . In the drop-down list, click **Upload File** to browse your PC to import CloudEdge's VMDK file to the datastore.

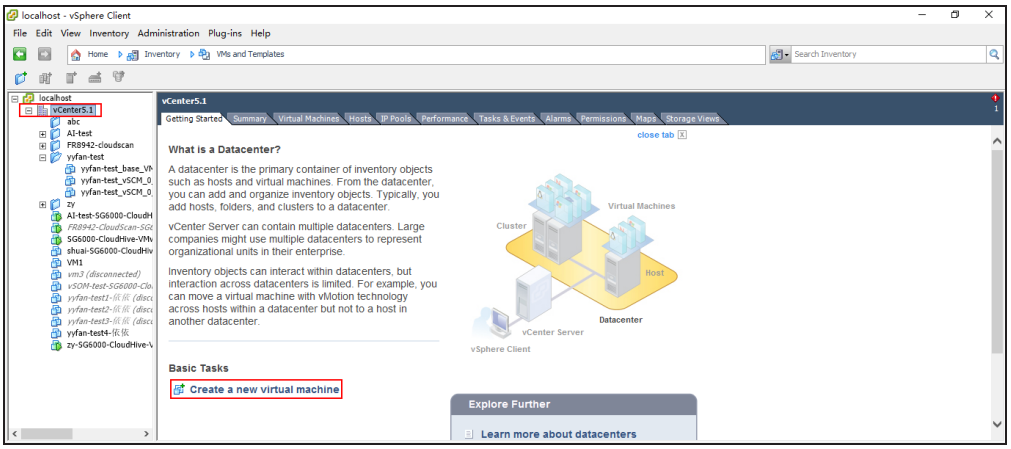


Step 2: Creating a Virtual Machine

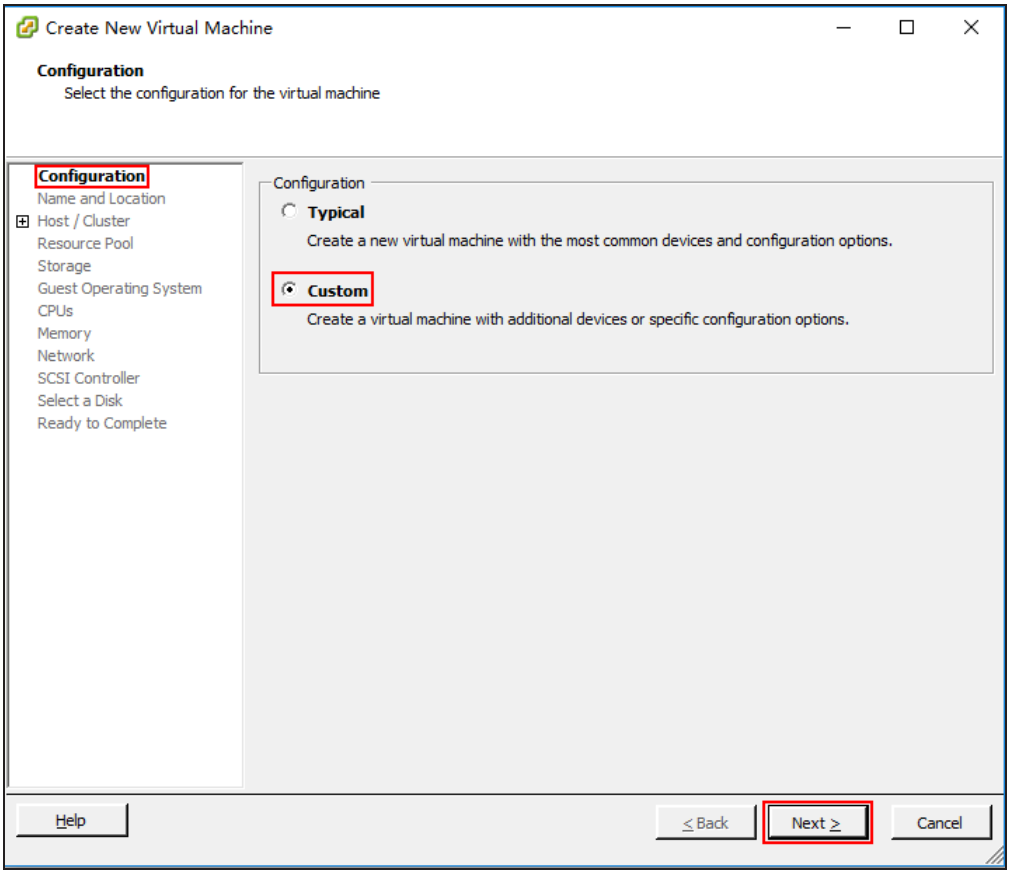
1. In the vSphere Client main interface, select **Home > Inventory > VMs and Templates** to enter the VMs and Templates page.



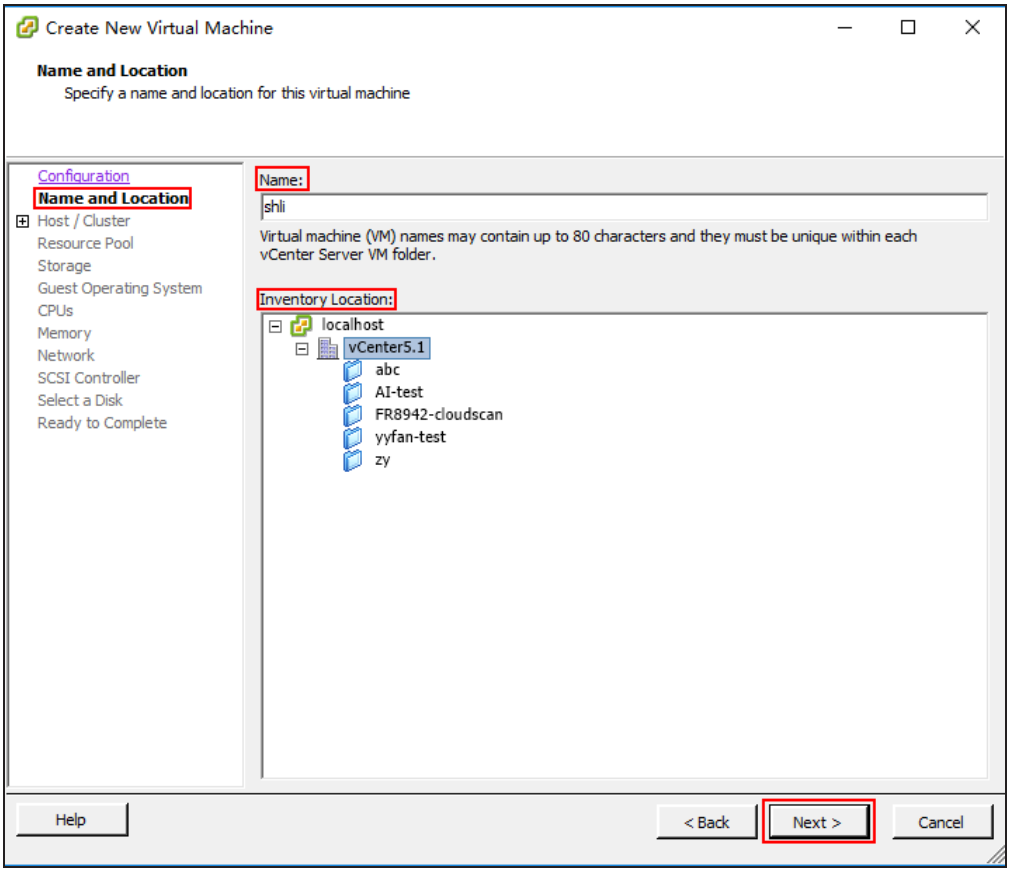
2. In the VMs and Templates page, select a datacenter in the left pane and click **Create a new virtual machine** appears in the right pane. The Create New Virtual Machine wizard pops up.



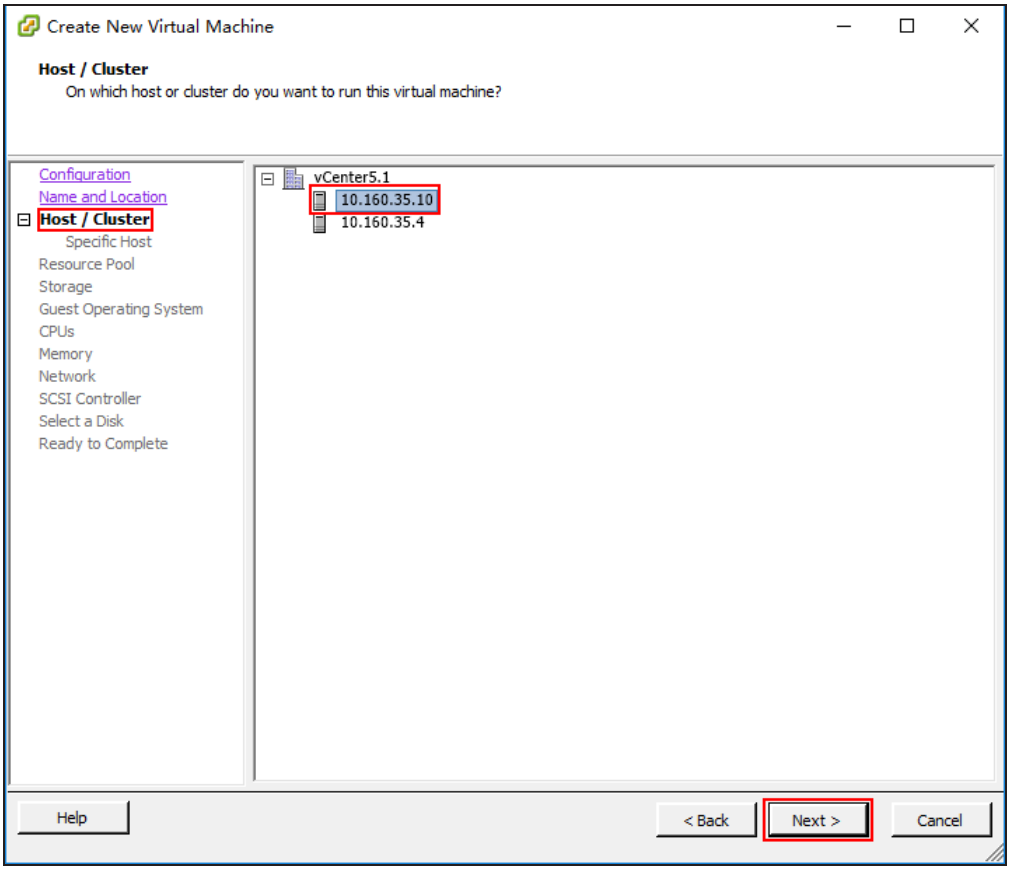
3. In the Create New Virtual Machine wizard, select **Custom** under the **Configuration** tab, and click **Next**.



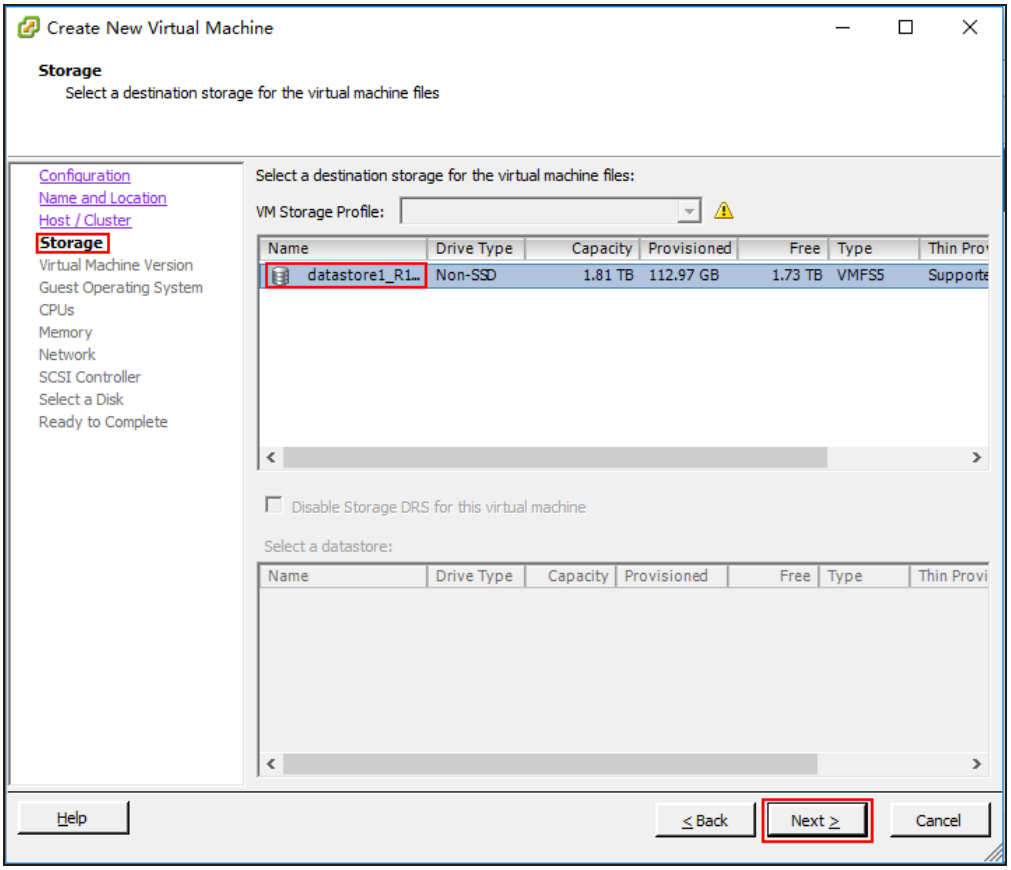
4. Under the **Name and Location** tab, enter a name and select the inventory location for virtual machine , and click **Next**.



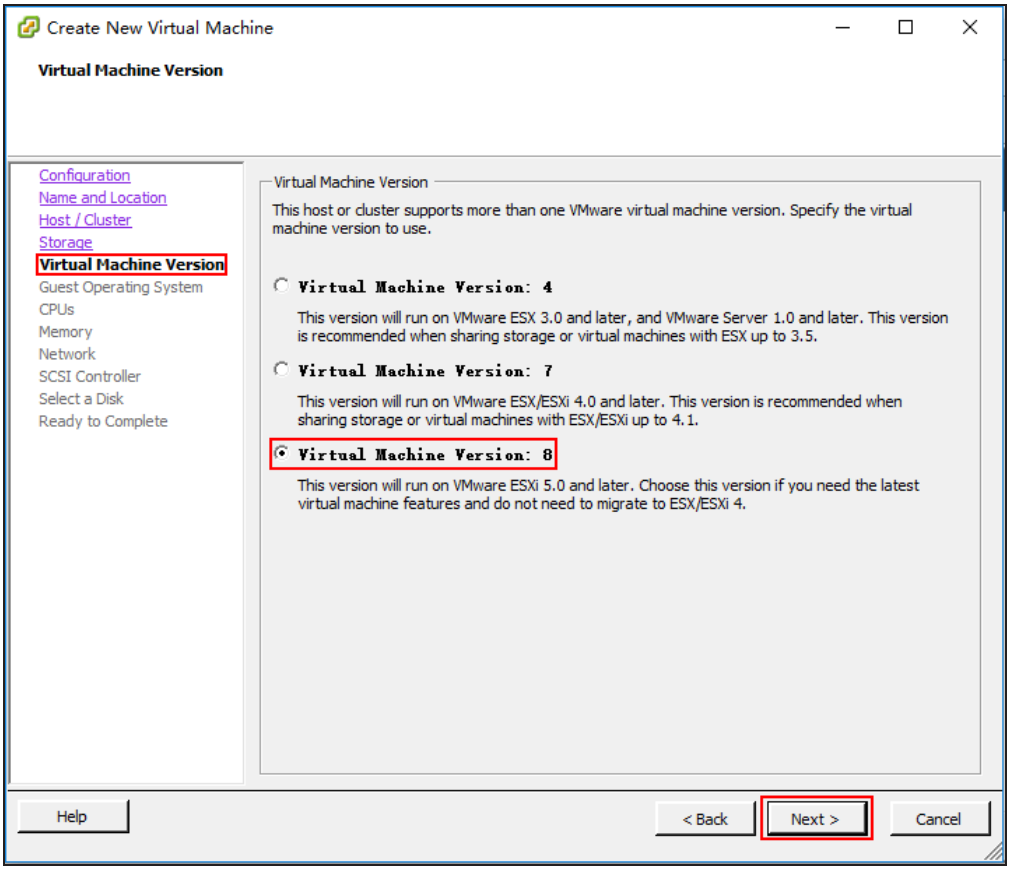
5. Under the **Host/Cluster** tab, select your target ESXi host, and click **Next**.



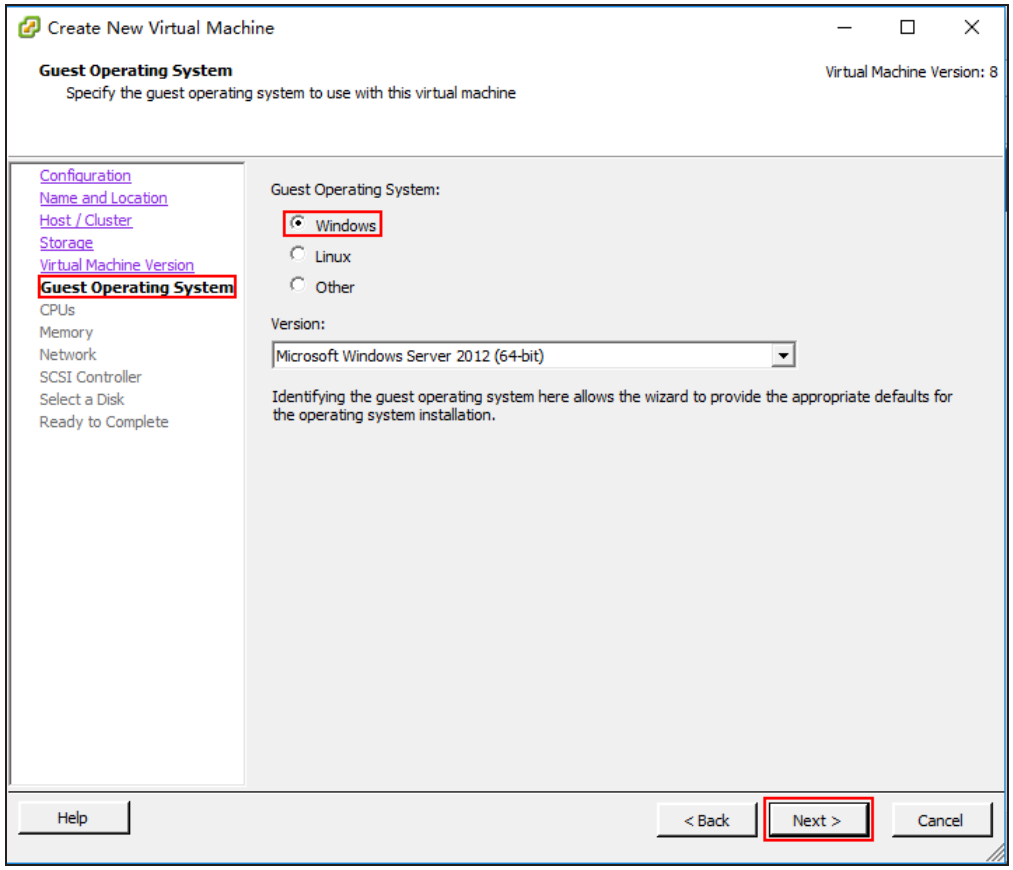
6. Under the **Storage** tab, select a datastore for virtual machine files, and click **Next**.



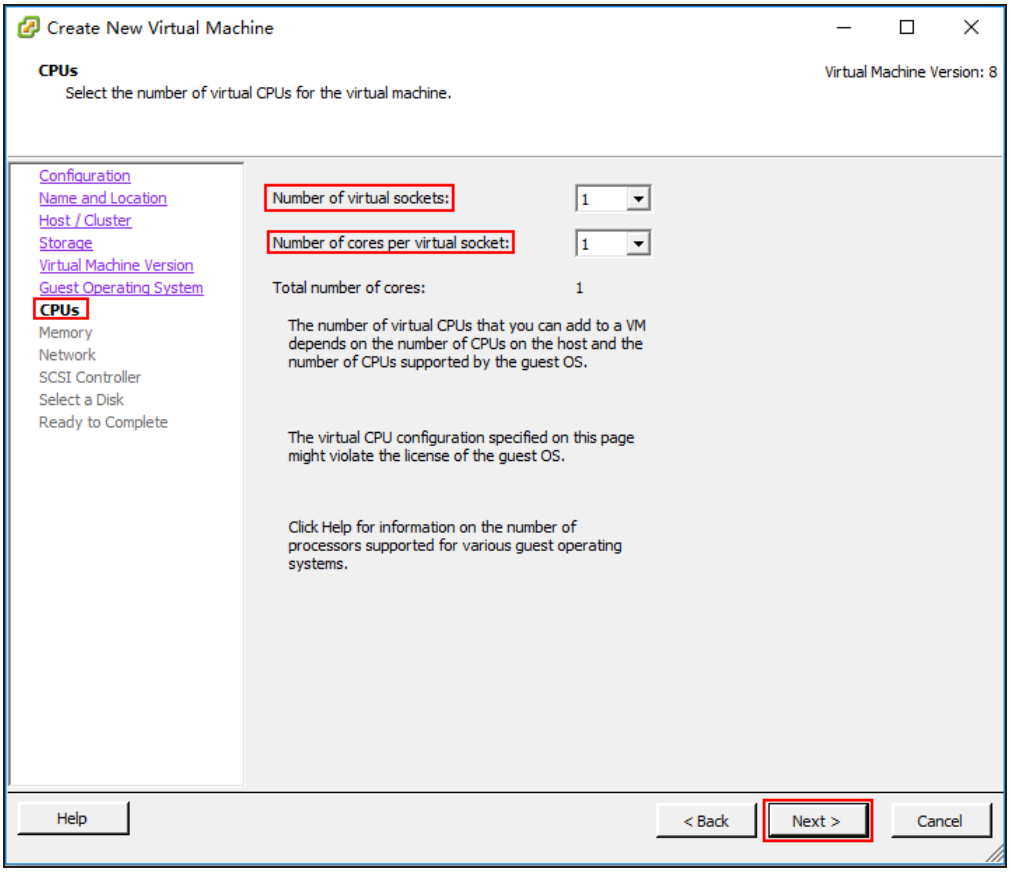
7. Under the **Virtual Machine Version** tab, select **Virtual Machine Version: 8**, and click **Next**.



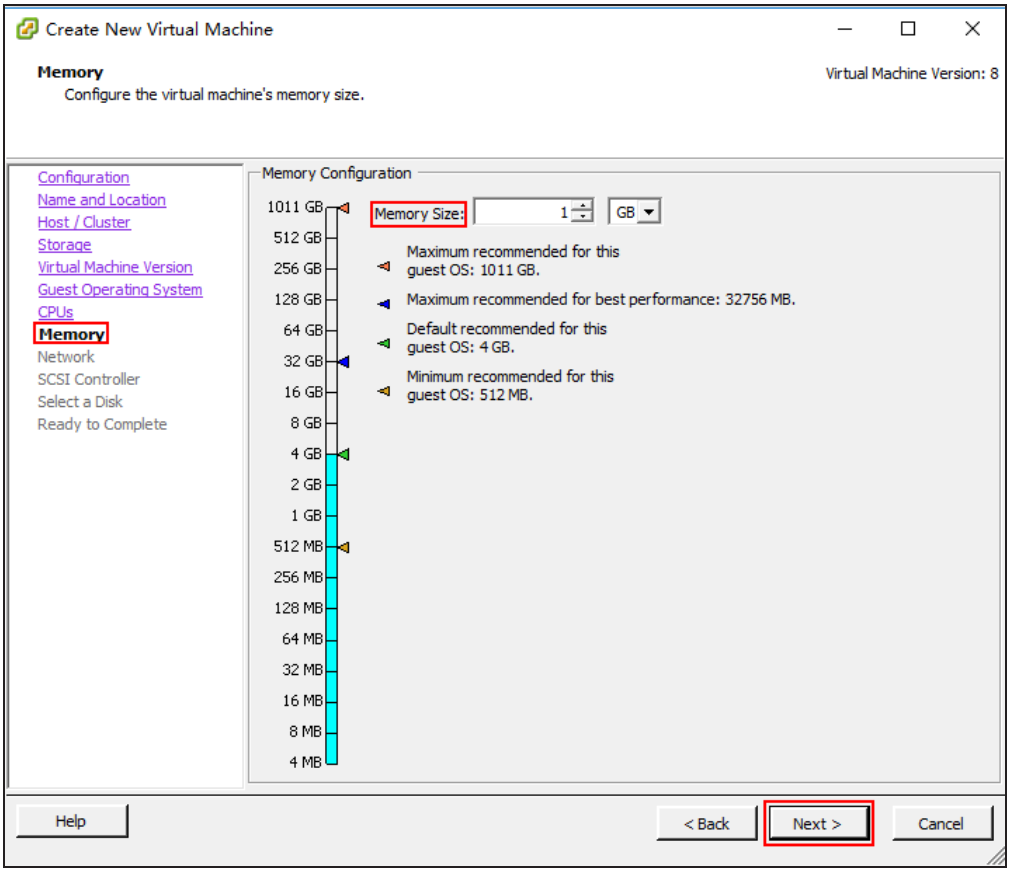
8. Under the **Guest Operating System** tab, select **Windows**, and click **Next**.



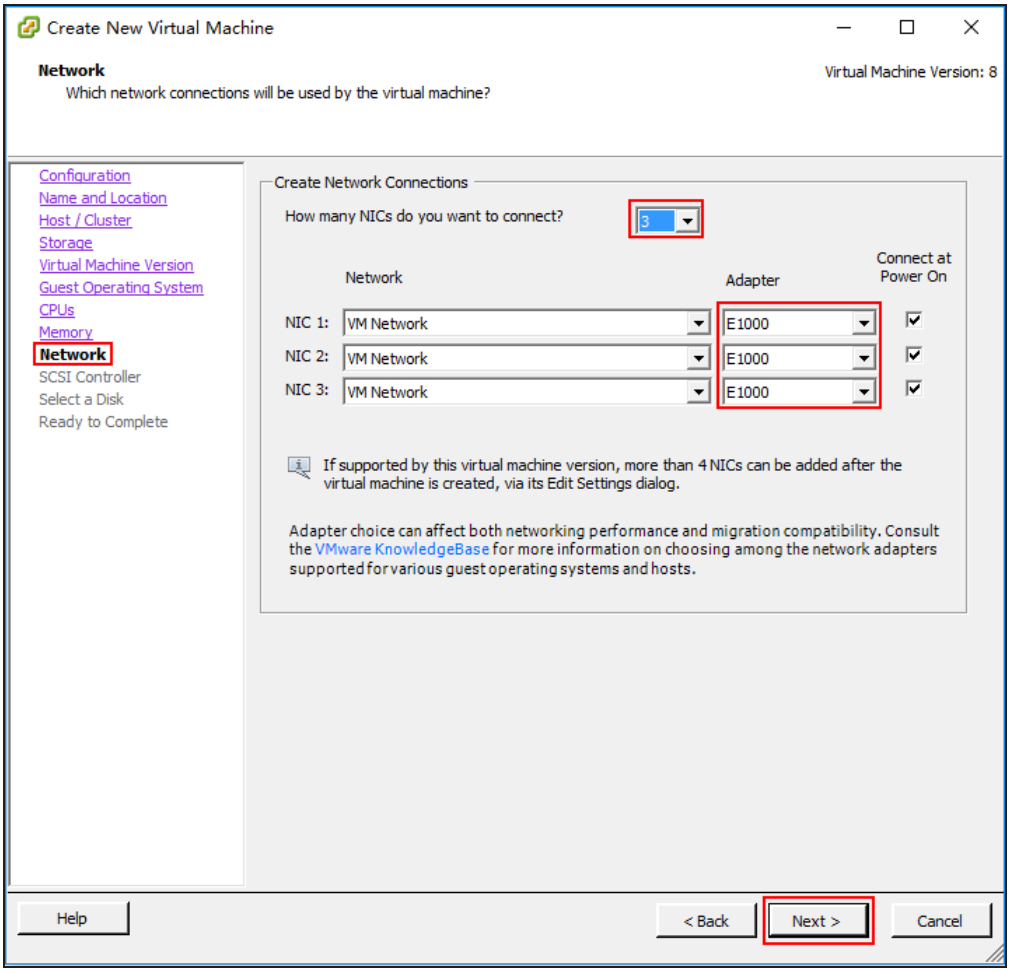
9. Under the **CPUs** tab, apply appropriate value for CPU and core. If you create SG6000-VM01, choose 1 socket and 1 core for each socket; if you create SG6000-VM02, choose 2 sockets and 2 core for each socket. Click **Next**.



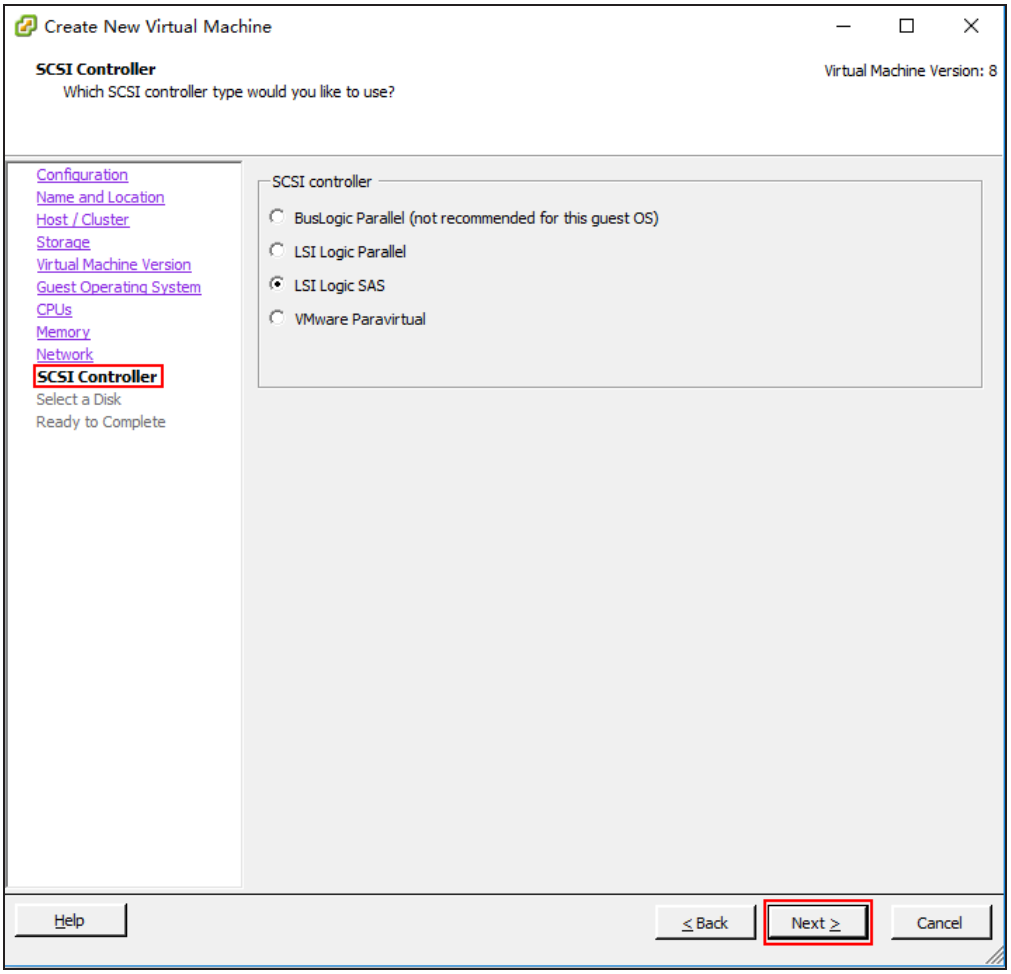
10. Under the **Memory** tab, assign a memory value for CloudEdge . For SG6000-VM01, choose at least 1 GB memory; for SG6000-VM02, choose at least 2 GB memory. Click **Next**.



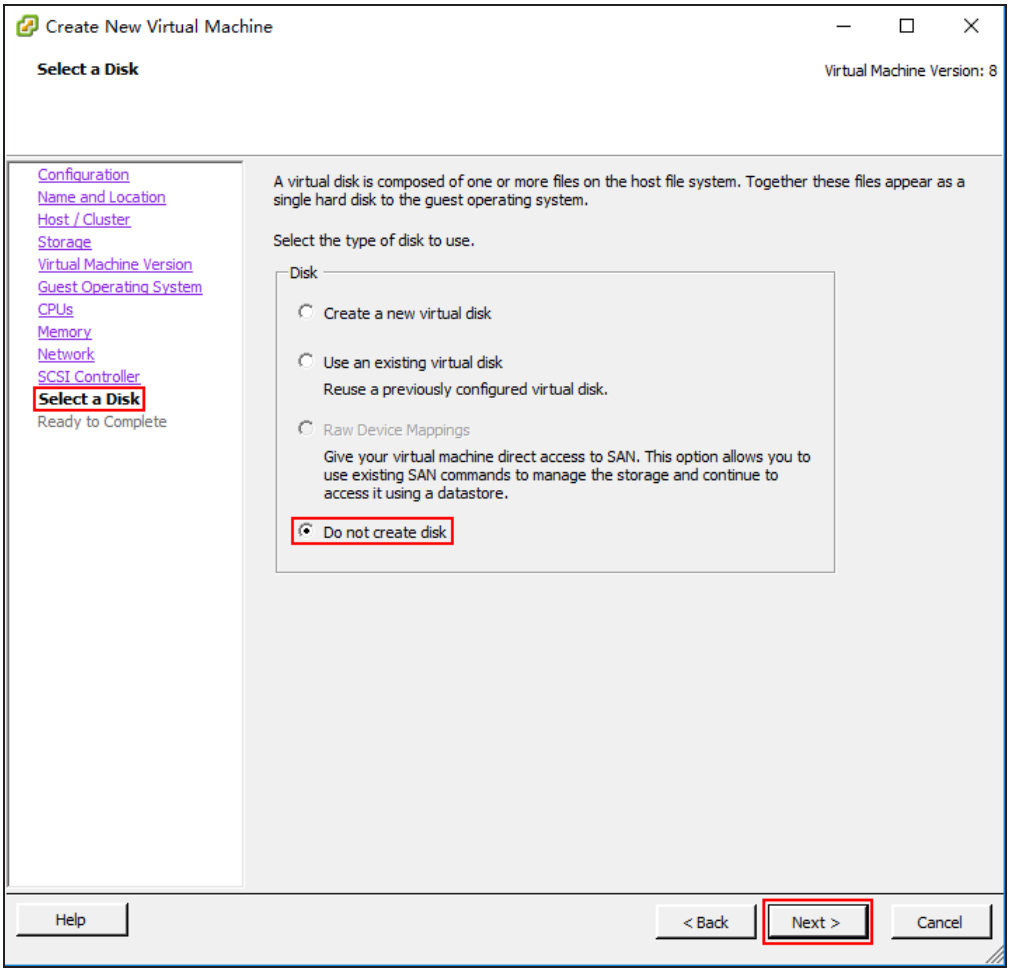
11. Under the **Network** tab, select at least 3 NICs, including management interface, data ingress and data egress. All NIC types should be E1000 or VMNET3. Click **Next**.



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



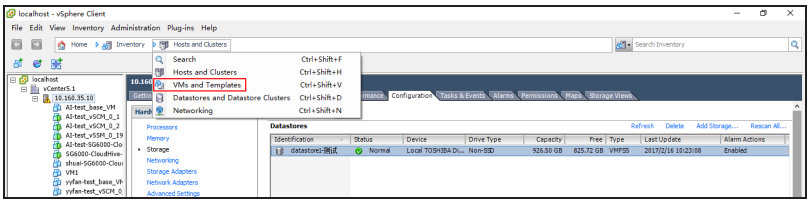
13. Under the **Select a Disk** tab, select **Do not create disk** , and click **Next**.



14. Click **Finish** to complete.

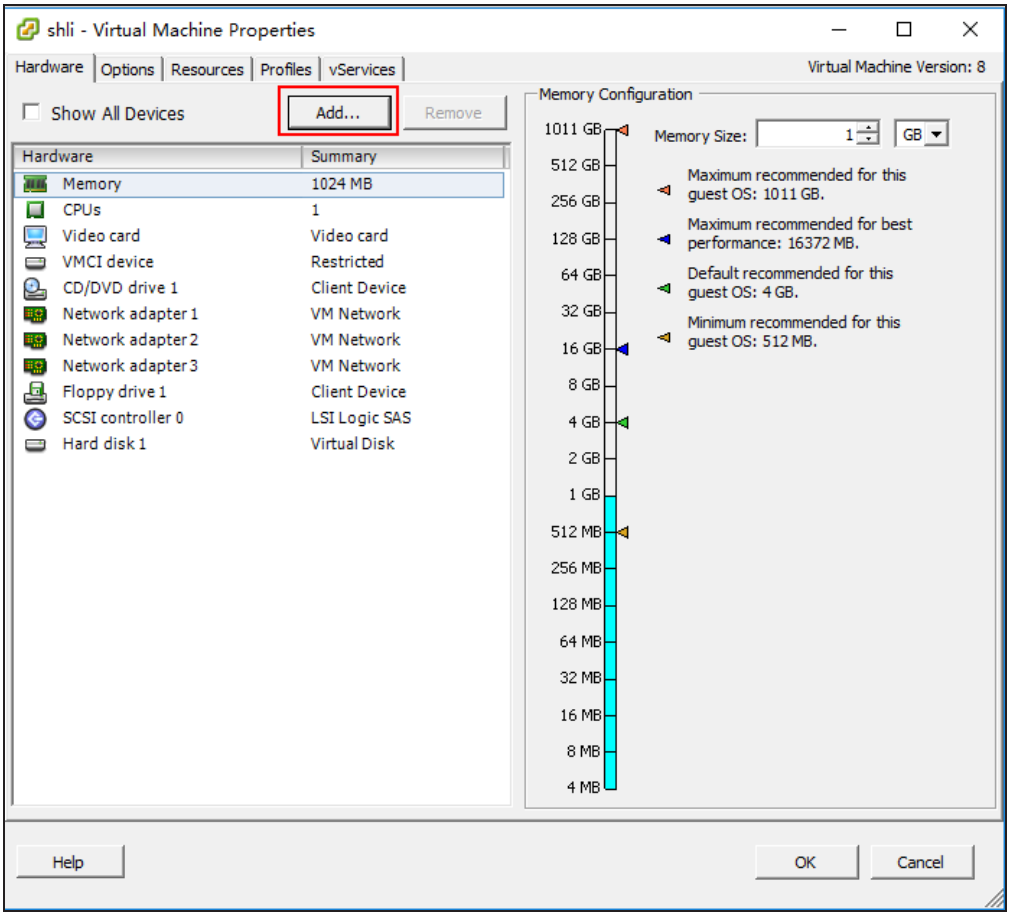
Step 3: Selecting the CloudEdge VMDK File for VM

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

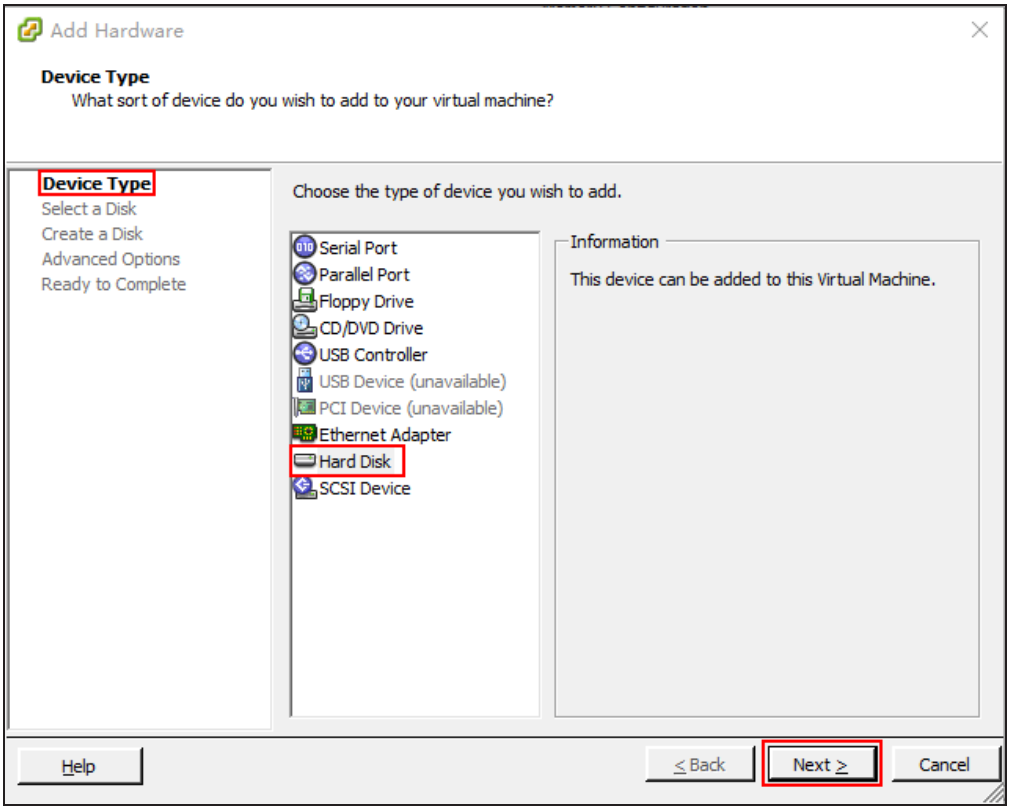


2. In the VMs and Templates page, click the CloudEdge virtual machine created in Step 2, and select **Editing virtual machine settings** appears in the right pane. The **Virtual Machine Properties** dialog pops up.

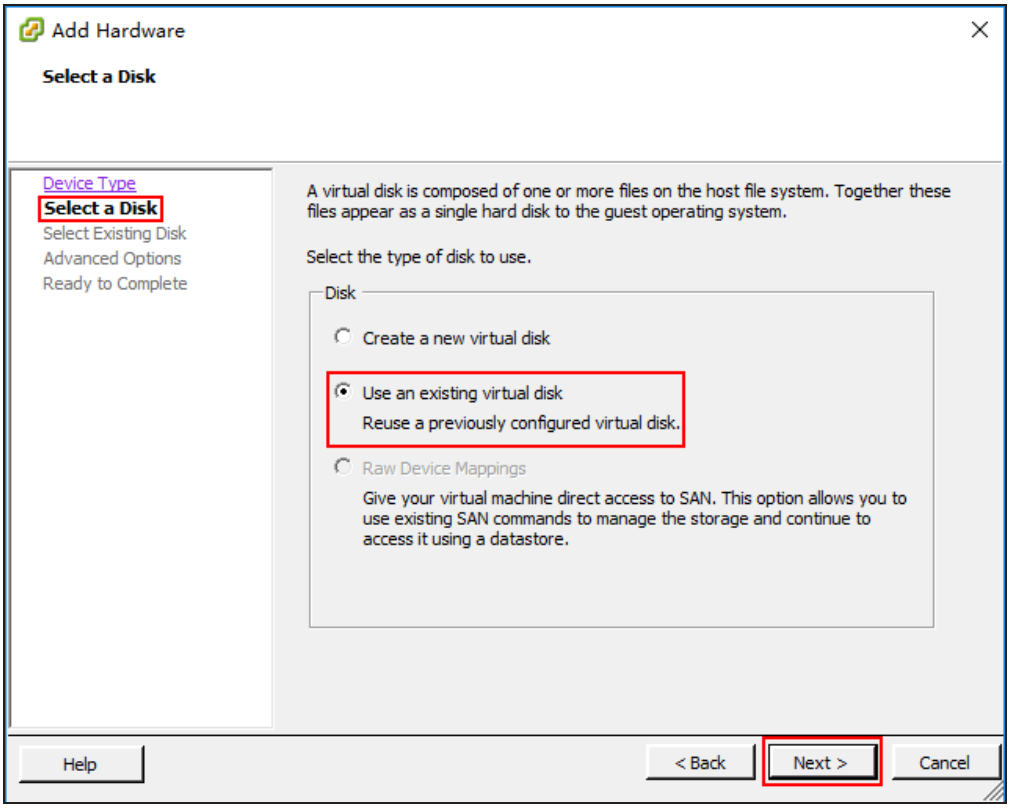
3. In the **Virtual Machine Properties** dialog, click **Add** to enter the Add Hardware wizard.



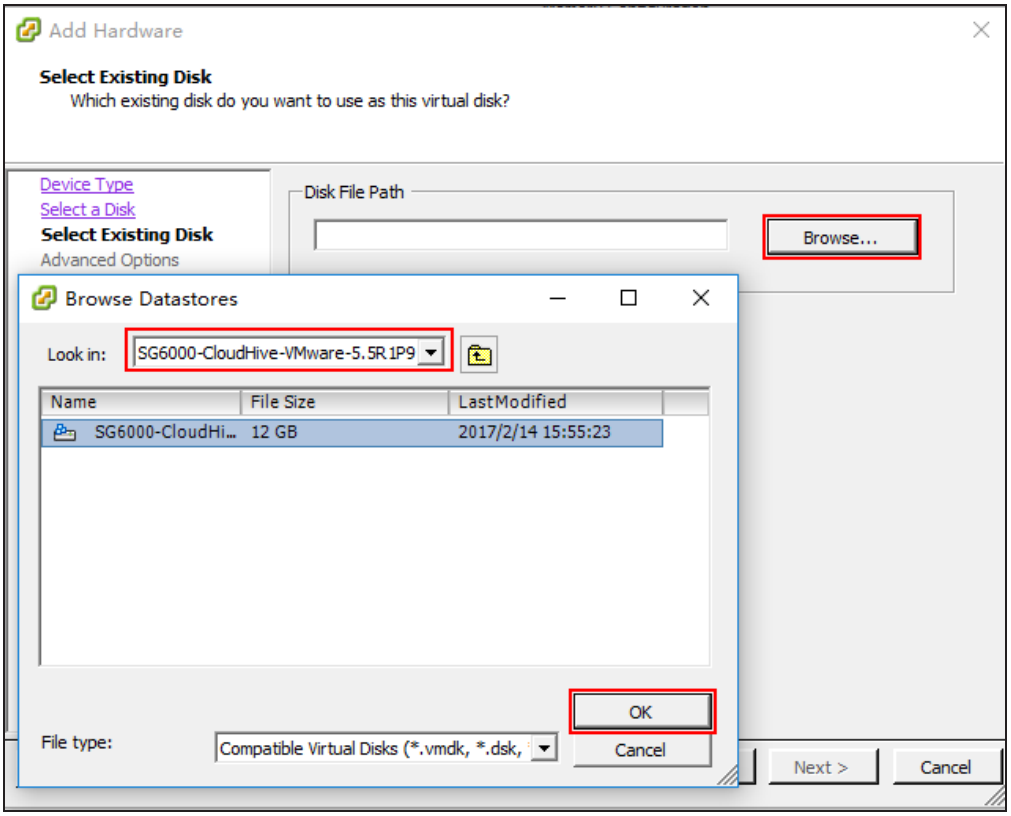
4. In the **Add Hardware** wizard, select **Hard disk** under the **Device Type** tab, and click **Next**.



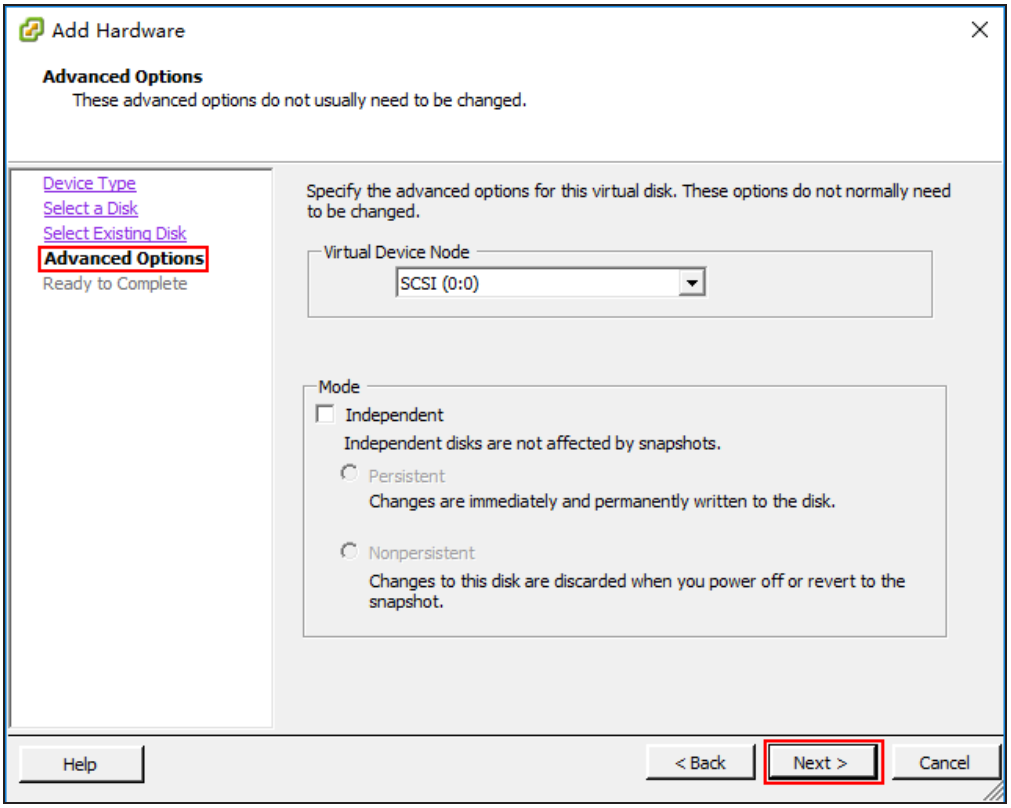
5. Under the **Select a Disk** tab, select **Use an existing virtual disk**, and click **Next**.



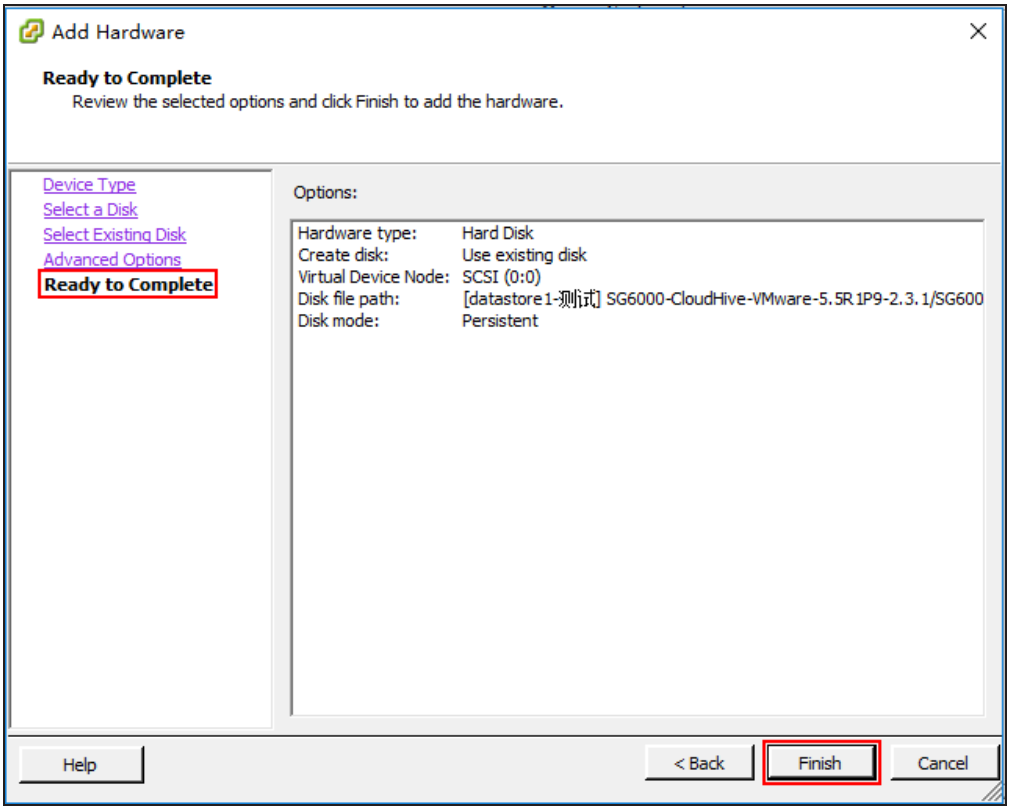
6. Under the **Select Existing Disk** tab, click **Browse** and the **Browse Datastores** dialog pops up. In the **Browse Datastores** dialog, select the VMDK file imported in Step 1, and click **OK**.Then click **Next**.



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



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



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

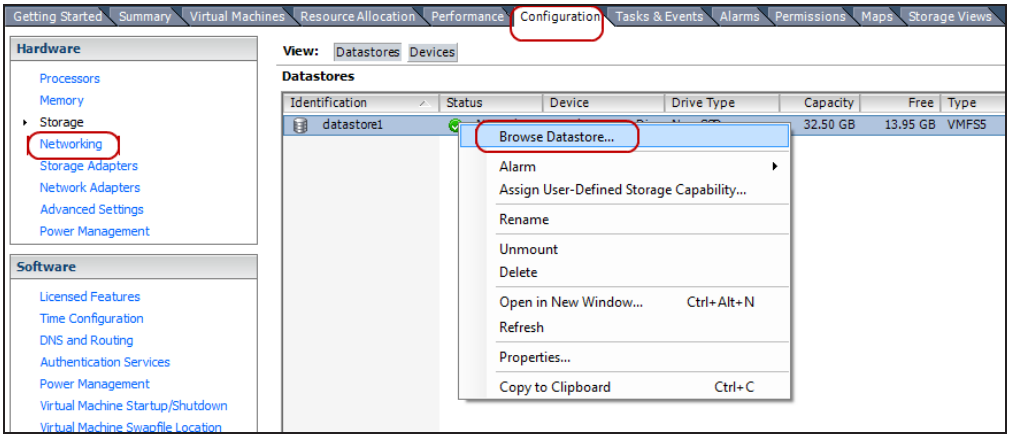
Installing vFW by Importing ISO

Contact Hillstone sales persons to get the trial or official vFW ISO file before installing vFW. .

Step 1: Importing ISO

1. Save the vFW ISO 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. In the main interface, select **Home > Inventory > Hosts and Clusters** to enter the Hosts and Clusters page.
4. Select **Home > Inventory > Hosts and Clusters**, and click the ESXi host which vFW will belong to.
5. In the Hosts and Clusters page, choose the ESXi host which vFW will belong to, and click the **Configuration** tab appears on the right pane to enter the configuration page.

6. 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.



7. 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 vFW's VMDK file to the datastore.

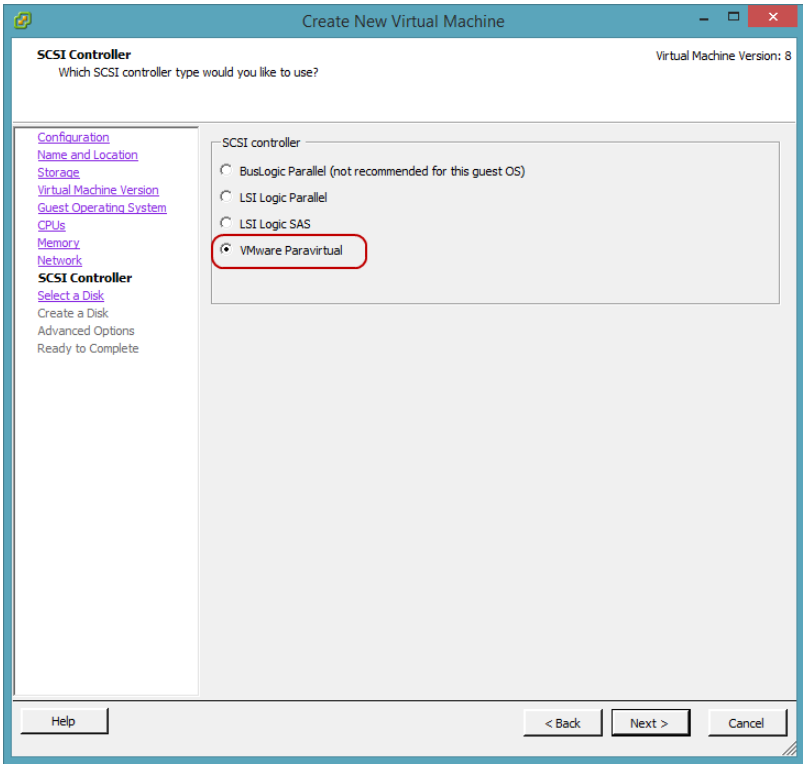
Step 2: Creating a virtual machine

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

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.

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

4. Under the <Host/Cluster> tab, select your target ESXi host, and click **Next**.
5. Under the <Storage> tab, select a datastore for virtual machine files, and click **Next**.
6. Under the <Virtual Machine Version> tab, select **Virtual Machine Version: 8**, and click **Next**.
7. Under <Guest Operating System> tab, select **Windows**, and click **Next**.
8. Under the <CPU> tab, apply appropriate value for CPU and core. If you create SG6000-VM01, assign 1 socket and 1 core for each socket; if you create SG6000-VM02, choose 2 sockets and 2 cores for each socket. Click **Next**.
9. Under the <Memory> tab, assign a memory value for vFW. For SG6000-VM01, choose at least 1 GB memory; for SG6000-VM02, select at least 2 GB memory. Click **Next**.
10. Under the <Network> tab, select 3 NICs. One is management interface, one is data ingress and one is data egress. All NIC types should be E1000 or VMNET3. Click **Next**.
11. Under the <SCSI Controller> tab, keep the default value, or choose **VMware paravirtual**. The default VM disk type is SCSI. As vFW only supports IDE type disk to be startup disk, you will need to change the disk type in the follow-up steps. But, if you don't wish to change disk type, you can choose VMware paravirtual now, and keep the default SCSI disk type, in this way, VMware will be able to read SCSI type disk as startup disk. Click **Next**.



12. Under the <Select a Disk> tab, select **Create a new virtual disk** and click **Next**.

13. Under the <Create a Disk> tab, assign at least 2 GB size for vFW, and click **Next**.

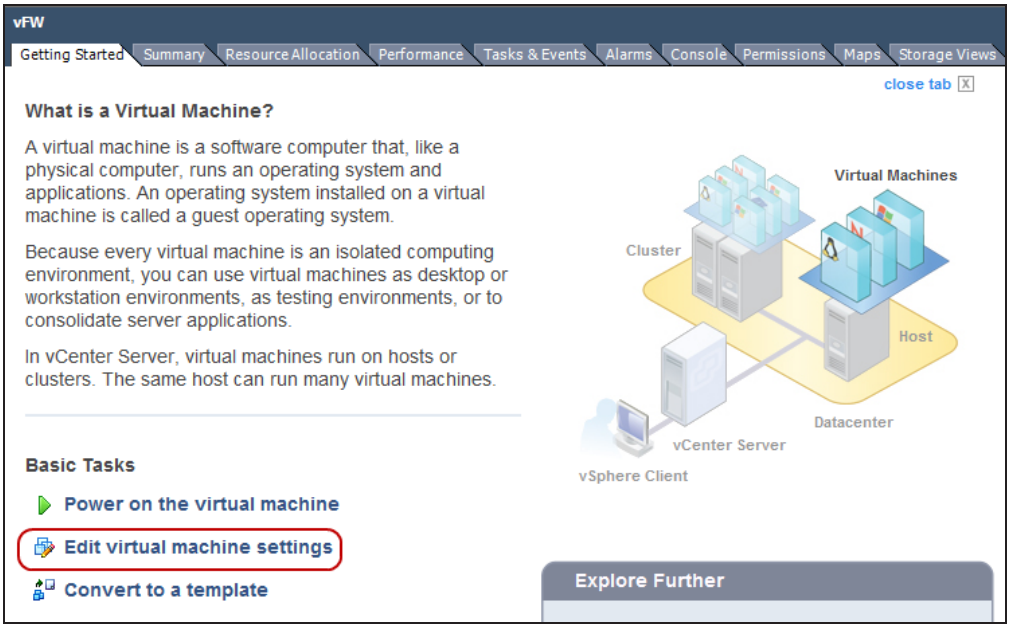
14. Under the <Advanced Options> tab, select **IDE** as virtual device node. IDE is the only disk type that vFW can read when it starts up. However, if you have selected to use VMware paravirutal to start up the disk(see step 11), you can keep the SCSI type for this option, otherwise, you must select IDE. Click **Next**.

15. Click **Finish** to complete.

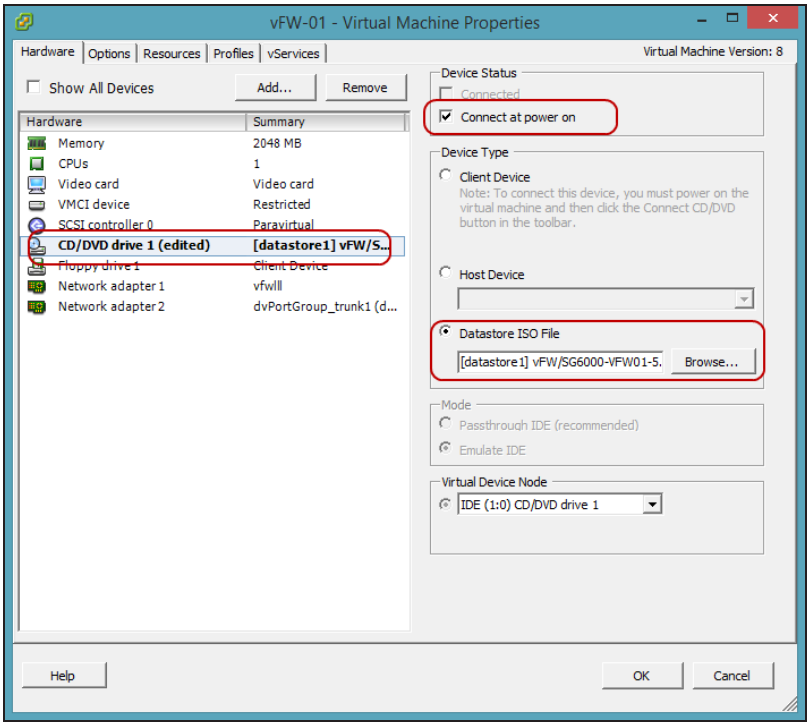
Step 3: Selecting vFW ISO file for VM

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

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



3. In the <Virtual Machine Properties> dialog, select **CD/DVD drive**, and then select **Database ISO file**, click **Browse** to locate the imported ISO file. Also, select **Connect at power on**.



4. Click **OK**.

Step 4: Networking vFW

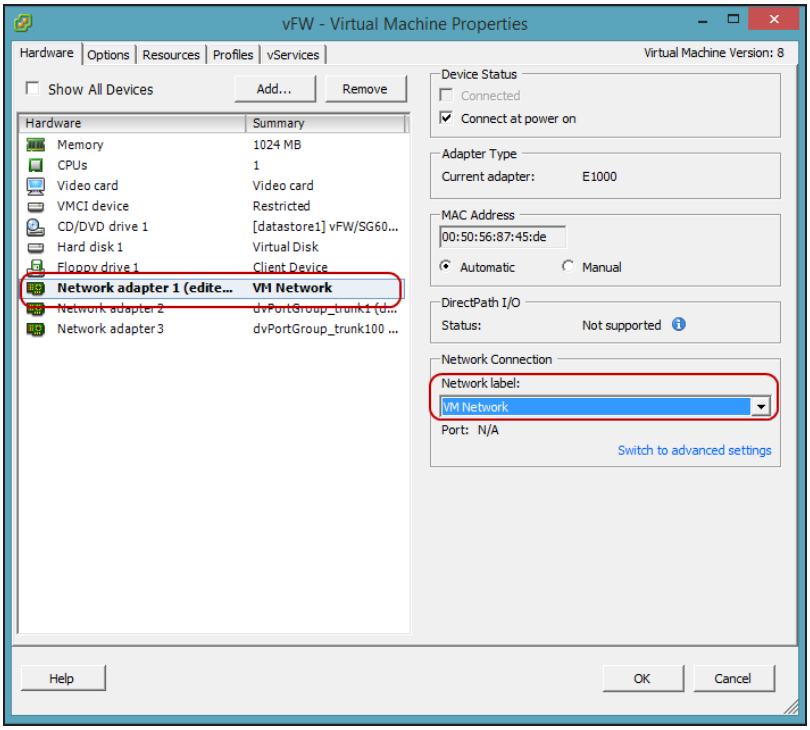
1. In vSphere Client, select **Home > Inventory > Hosts and Clusters**, and from left pane, select the ESXi host which has vFW virtual machine.

2. In the right pane, click the **Configuration** tab, and select **Networking** from left navigation, make sure you are under "vSphere Standard Switch", and click **Add Networking...**.

Note: vSphere Standard Switch (vSS) is usually used for networking a vFW on a single ESXi host. If you design to use vFW for more than one ESXi hosts, you need to select vSphere Distributed Switch (vDS). To

set up vDS, go to **Home > Inventory > Networking** and select your DataCenter, and then you will be able to add or edit vDS networks and its port groups.

3. In the popped <Add Network Wizard> dialog box, select **Virtual Machine**, and click **Next**.
4. Select the vSwitch where vFW's interface belongs, and click **Next**.
5. In the Network Label textbox, enter a name for vFW interface, and you may select a VLAN or none depending on if you want the interface to be in a VLAN or not. Click **Next**.
6. Click **Finish**.
7. Repeat step 2 to step 6 to create more vSwitch ports for vFW's interfaces.
8. Go back to **Home > Inventory > VMs and Templates**, right click vFW virtual machine and select **Edit Settings**.
9. In the <Virtual Machine Properties> dialog box, select a **Network Adapter**, and from the **Network Label** drop-down menu, select the vSwitch port it belongs, then click **OK**.



10. Repeat the step above to assign vSwitch port for each interface of vFW. If your vFW did not have enough interfaces when it was created, you can click **Add** to create more interface.

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.

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.

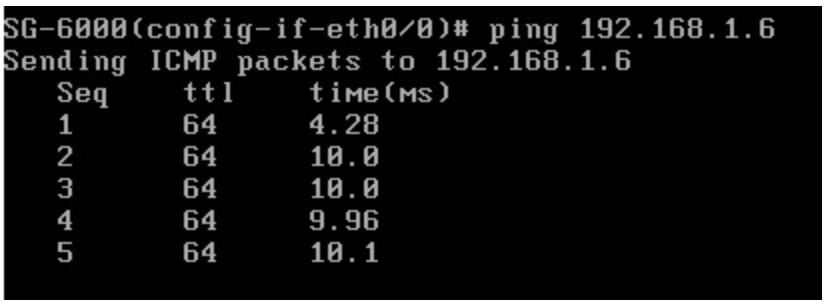
```
SG-6000(config)# ip vrouter trust-vr

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.

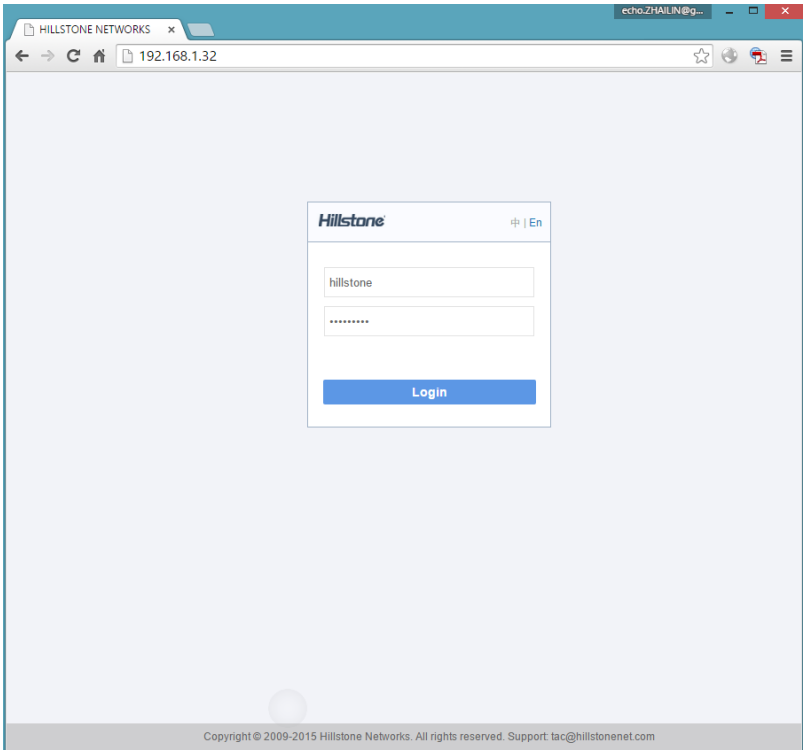
4. Save the settings.

```
SG-6000# save
```

5. Test if the gateway is accessible.



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).



Upgrading StoneOS

Note: 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*.

To upgrade StoneOS to a higher version:

1. Get and save vFW new ISO image in a local directory.
2. Open VMwre vSphere Client, select **Home > Inventory > Hosts and Clusters**, and then click the ESXi host of vFW.
3. Click the **Configuration** tab on the right. From left list, select **Storage**, and then right click datastore, select **Browse Datastore**.

4. In the <Datastore Browser> window, click the upload button "  " and select **Upload File**. Then you find the new ISO image and upload it into datastore.
5. Select **Home > Inventory > VMs and Templates**. From the left navigation, click the vFW VM, and on the right pane, click **Edit virtual machine settings**.
6. In the **Virtual Machine Properties** window, select **CD/DVD drive**, and then click **Datastore ISO file** radio button, click **Browse**. Find and select the uploaded ISO file. Ensure that **Connect at power** on is selected.
7. Click **OK**.
8. Click **Shut down the virtual machine** to power off the VM.
9. Wait for a while. Click **Power on the virtual machine** to restart vFW VM. Since **Connect at power on** is enabled, the VM will load new ISO image. Thus, the firewall system is upgraded.

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.

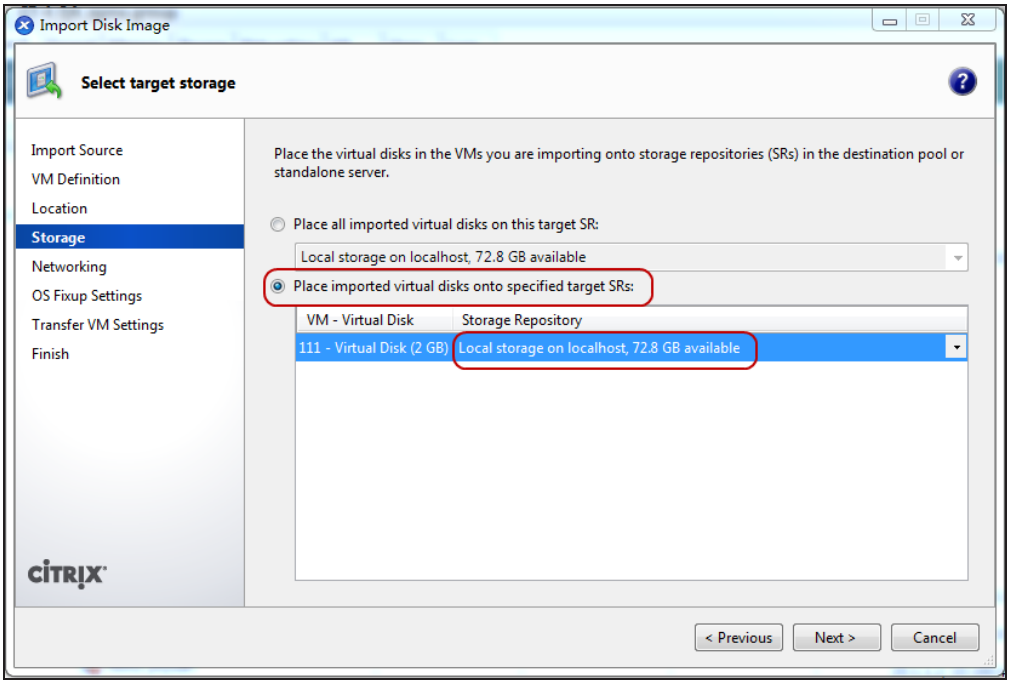
Step 2: Importing the VHD file

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.
   If the model is SG6000-VM01, at least 1 CPU and 1024M memory are needed; if the model is SG6000-VM02, at least 2 CPU and 2048M memory are needed.
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.

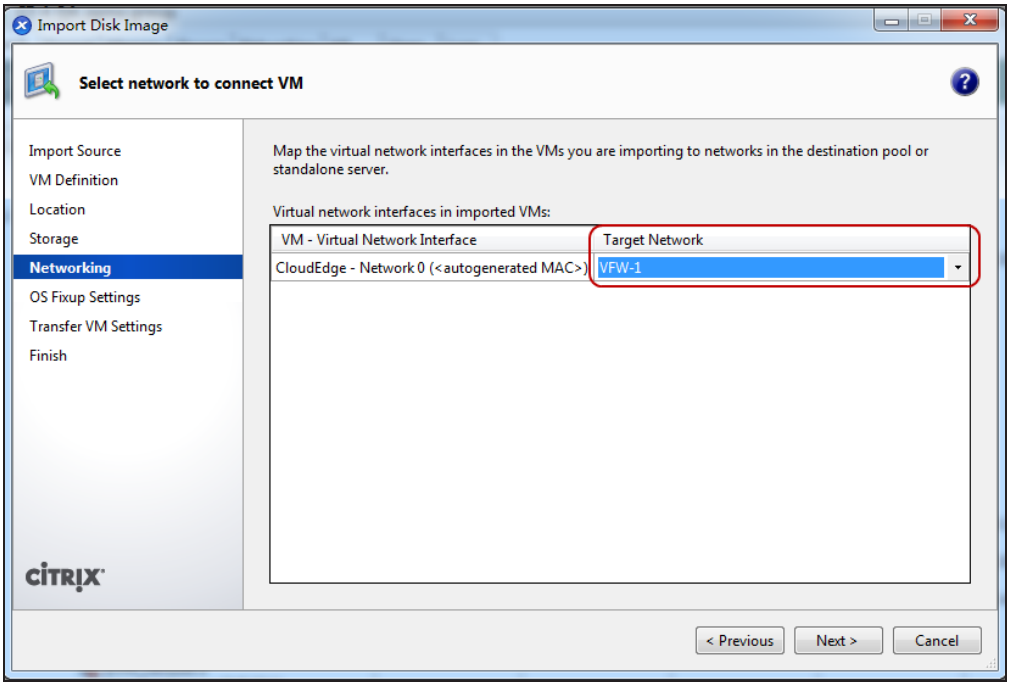
   On the **Storage** page, select a storage repository (SR) where the imported virtual disk will be placed.



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/stan-

dalone server for the new VM's virtual network interface.



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, eth-0/0 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 54
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 AWS

Overview

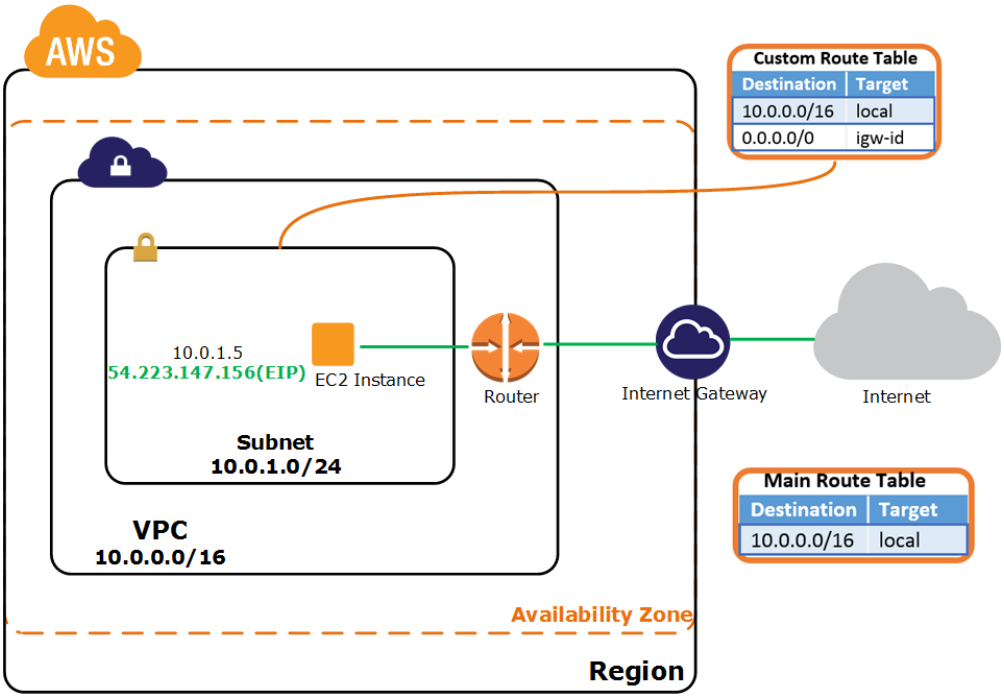
This chapter introduces how to install CloudEdge virtual firewall (abbr. vFW) on Amazon Web Service.

Introduction to AWS

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

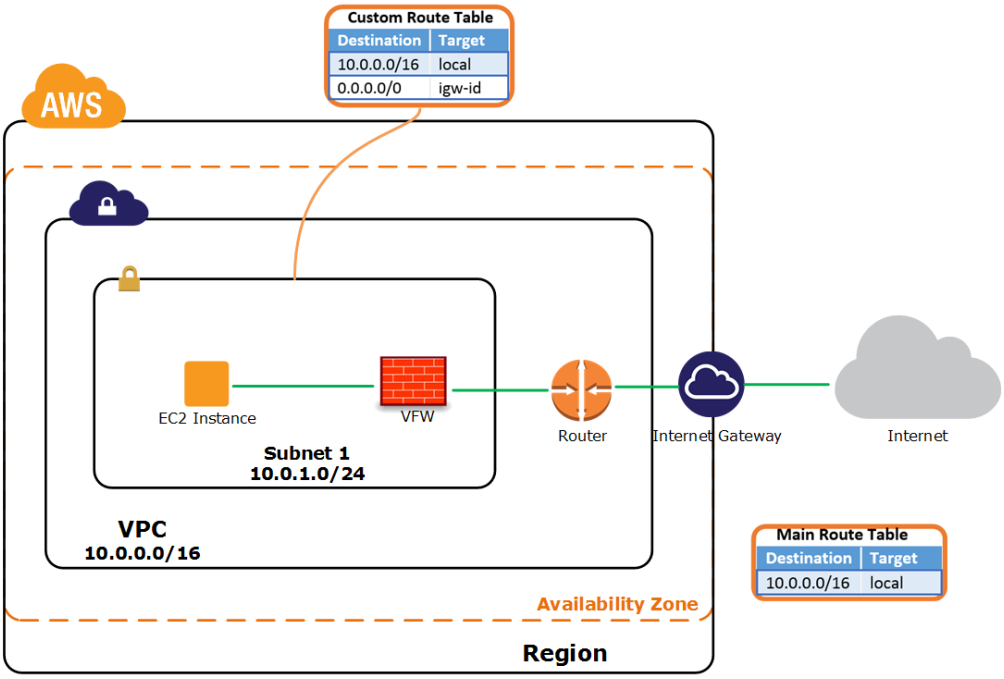
Among all the AWS components, VPC and EC2 are used in deploying vFW.

- 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.



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

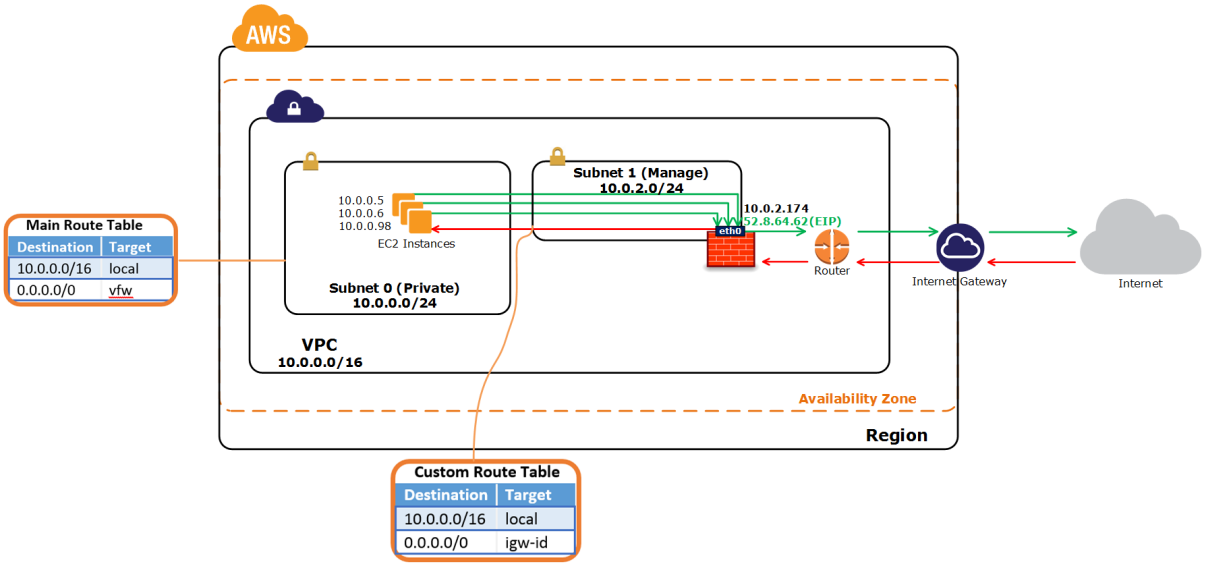
algorithms are supported, including weighted hashing, weighted least-connection and weighted round-robin. The advantage of integrating SLB with the firewall is that the firewall can inspect and analyze all inbound traffic. In the VPC, this means thatCloudEdge can block attack threats hidden in traffic 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.



- **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).

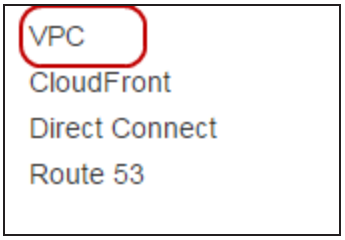
In this guide, we presume that our readers have built a VPC network, and the default subnet, Subnet 0, is named for Manage. The Manage subnet has a default route whose next hop is directed to Internet gateway (IGW). In this chapter, we will introduce to you how to set up a subnet. In the later steps,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

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

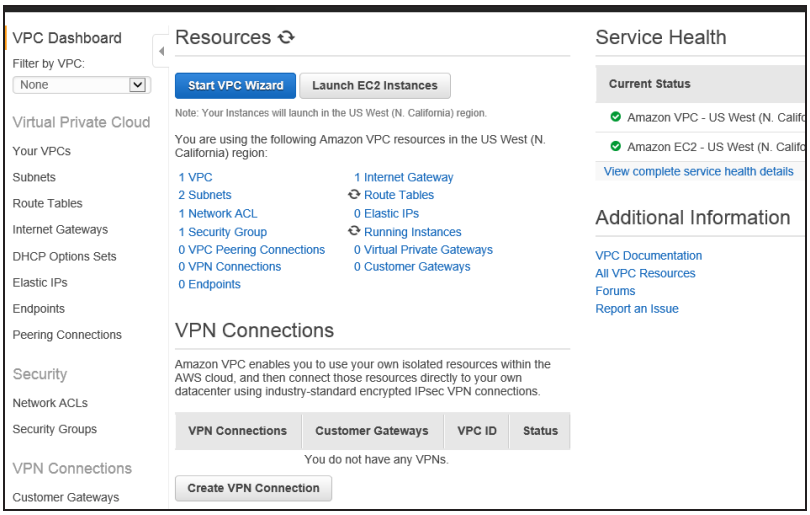
- VPC: 10.0.0.0/16
- Subnet 0 (Manage): 10.0.0.0/24
- Subnet 2 (Public): 10.0.2.0/24

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.



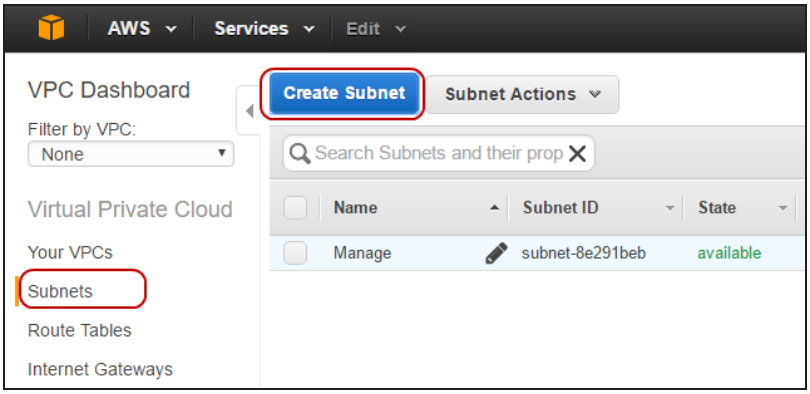
Step 2: Adding Subnets into VPC

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.

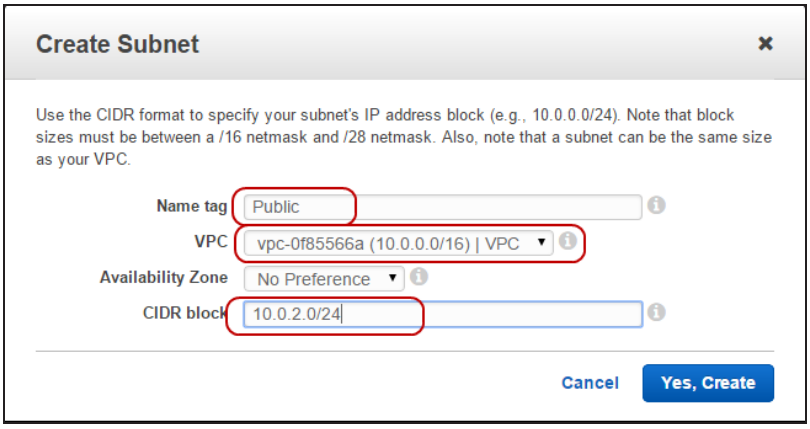
Subnet 0 (Manage) is already created in the step above. Next, in this step, we will introduce how to create a new subnet.

Use the configuration steps below to add a new subnet:

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



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".



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 61), 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:

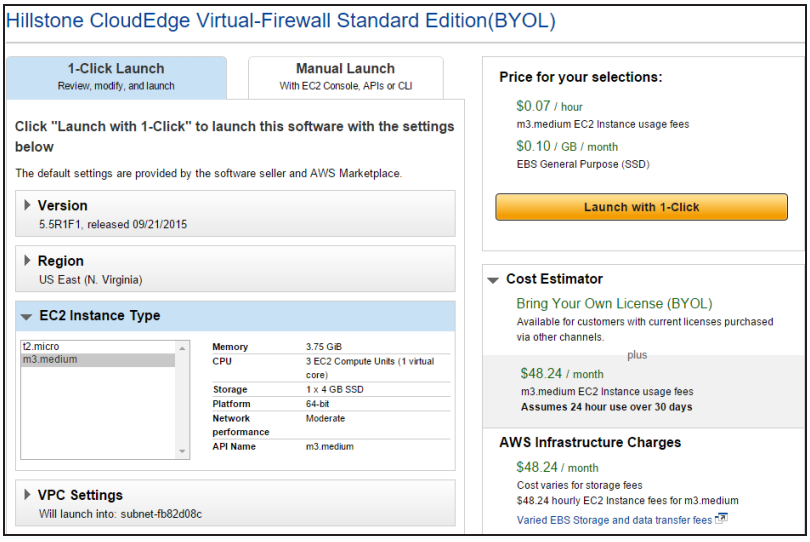
- have a running StoneOS system
- see that interface eth0 has acquired private IP addresses and elastic IP addresses (public)
- be able to visit the CLI and WebUI of StoneOS

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

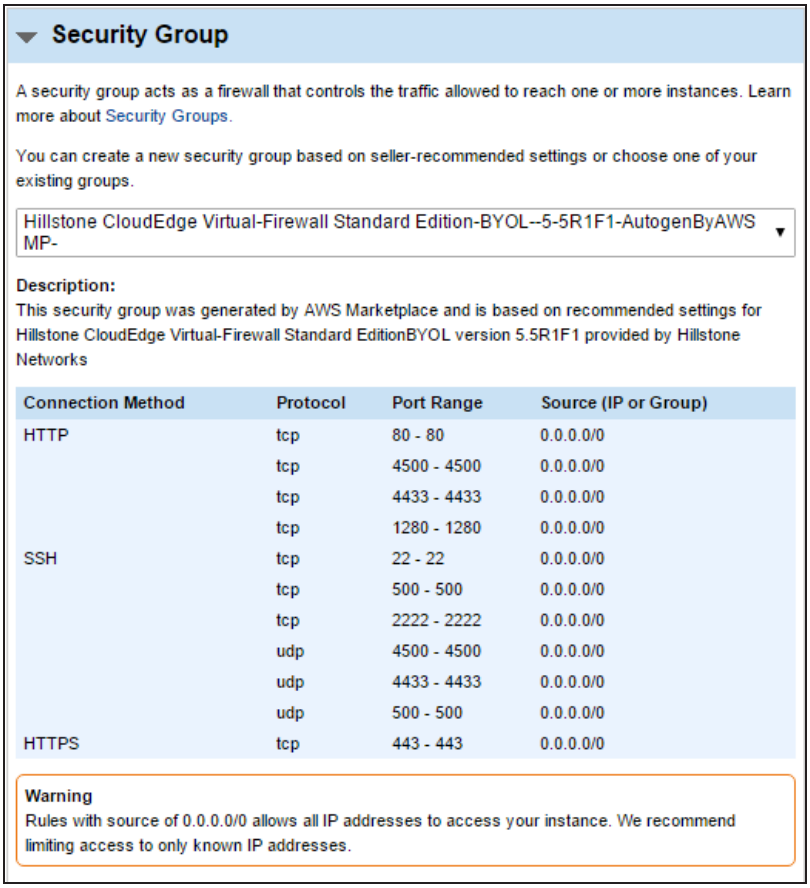
Using 1-Click launching, you will get an instance set up ready for you just with 1 click.

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 VM01 model or VM02 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.

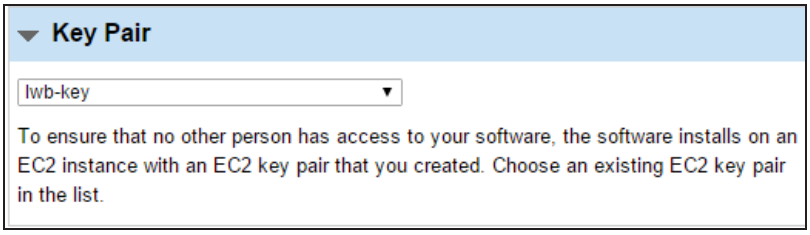


5. Please be noted that you should have already built a VPC for CloudEdge. Select the VPC and subnet. More subnets can also be added later in management console.

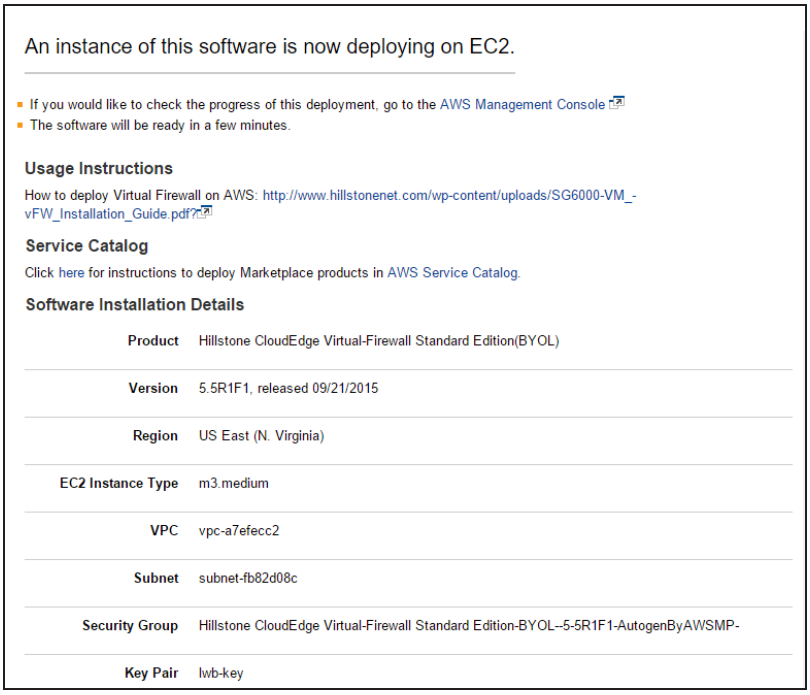
6. For **Security Group**, we recommend you select the existing group with "Hillstone CloudEdge" name on it. The Hillstone security group opens ports to allow all potential communication. Please do not select a security group that does not allow SSH, HTTP or HTTPS connection, which will incur disconnection.



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



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



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

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 VM01 model or VM02 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

If you want SG6000-VM01 model, you shall need an instance of 1 vCPU and 1 GB memory; if you want SG6000-VM02, you shall have an instance of 2 vCPU and 2 GB memory.

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

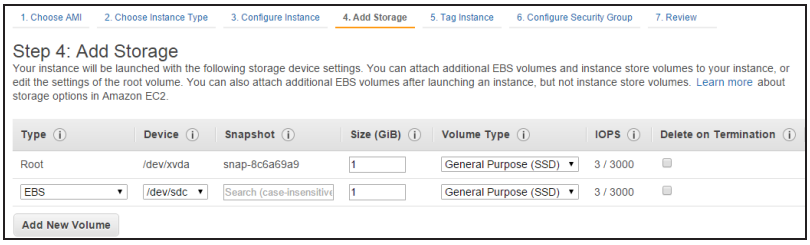
Step 4: Configuring Instance Details

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.



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

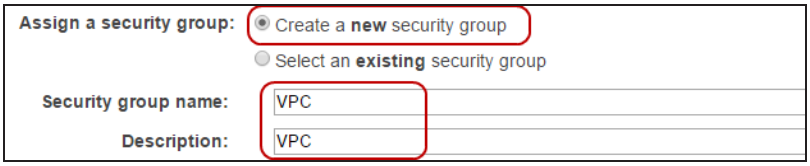
Step 6: Tag Instance

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**.

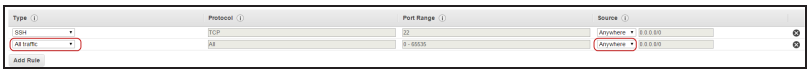
Step 7: Configuring Security Group

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.



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

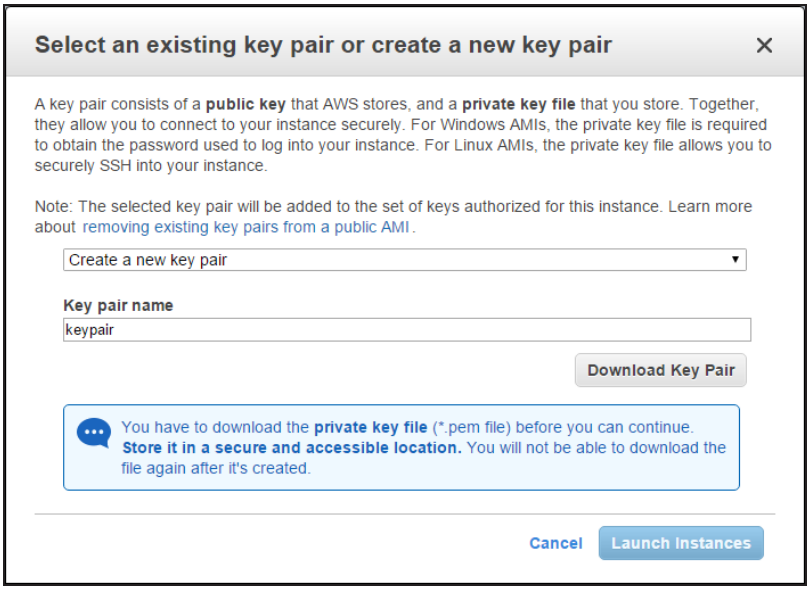


3. Click **Review and Launch**.

Step 8: Launching Instance

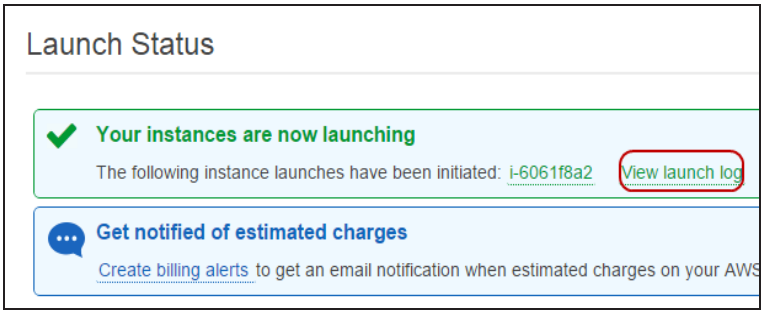
1. On the review page, look at all the configurations and click **Launch**.

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.



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.



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

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.

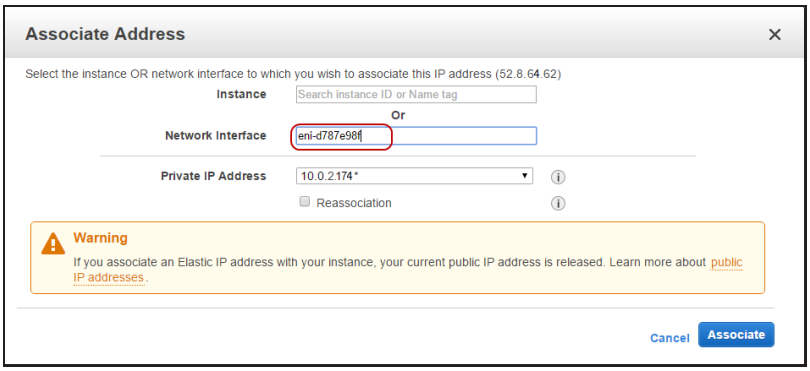
As the DHCP function of eth0 interface is enabled by default, after the virtual firewall is started, the eth0 interface is automatically assigned with a private IP address. We will apply for an elastic IP address for eth0. After that, eth0 interface has a private IP address and public IP address. The 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.

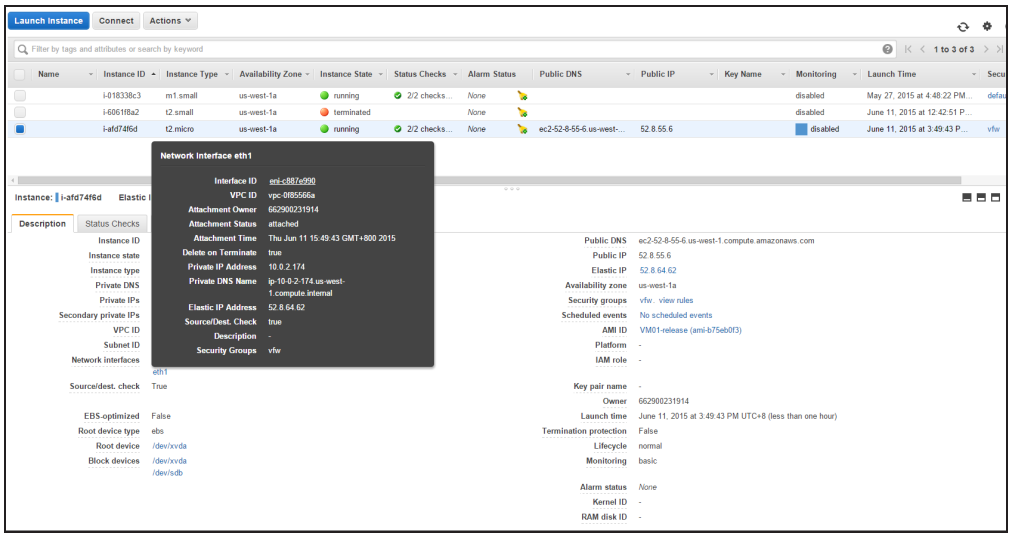
4. Select an EIP, click **Associate Address**. In the prompt, enter the ID of vFW's eth0 (you can find eth0's ID from vFW's instance information). Click **Associate**, this EIP will be the public IP address of vFW's management interface eth0.



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.



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 6

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 PuTTY-gen, 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**.

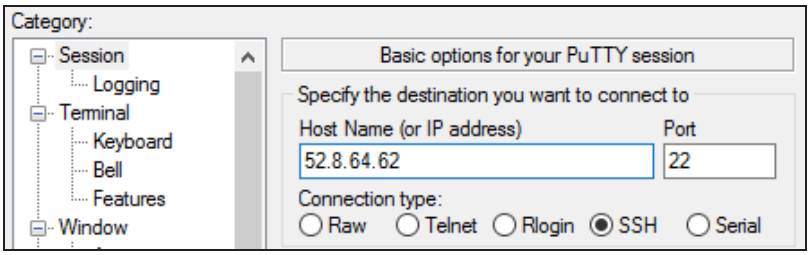
3. Click **Load**. By default, PuTTYgen displays only files with the extension `.ppk`. To locate your `.pem` file, select the option to display files of all types.
4. Browse and select PEM file.
5. Click **Save private key**, and save it (a `.ppk` file) to a secured location on your PC. It will be used 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.

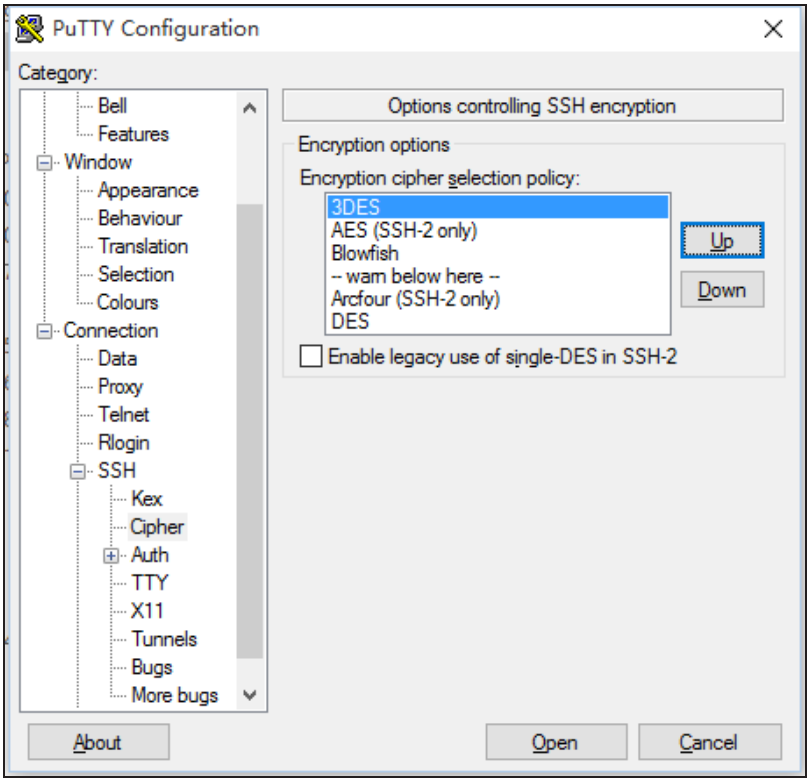
1. Start PuTTY (from the **Start** menu, click **All Programs > PuTTY > PuTTY**).

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

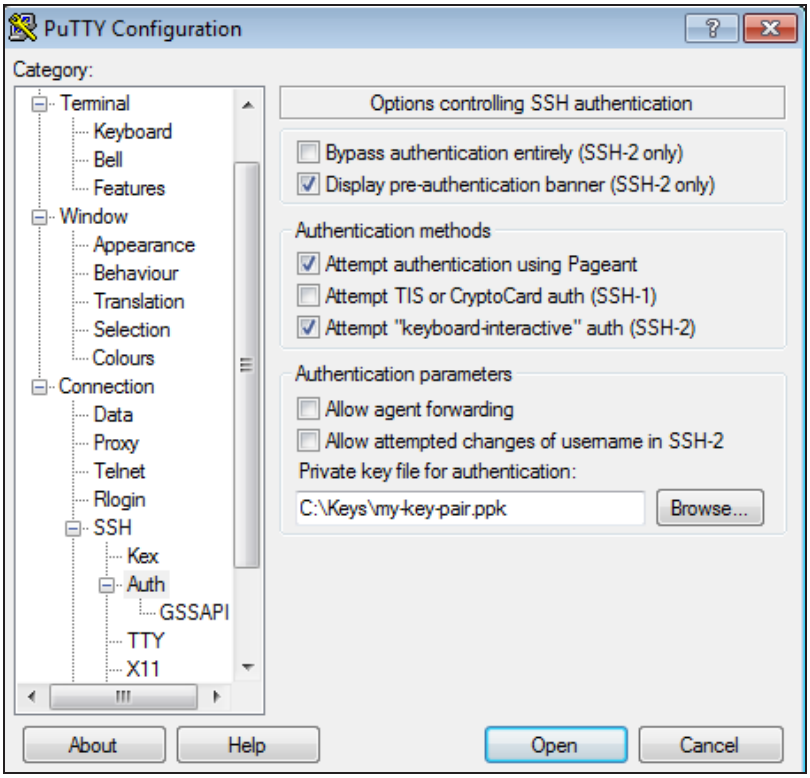


   - In the **Host Name box**, enter instance's public IP (eth0 public address).
   - Under **Connection** type, select **SSH**.
   - Ensure that **Port** is 22.

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

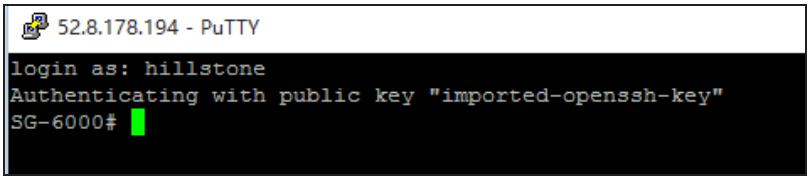


4. In the **Category** pane, expand **Connection > SSH > Auth**. Click Browse, and select the `.ppk` file that was generated for private key pair.



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.

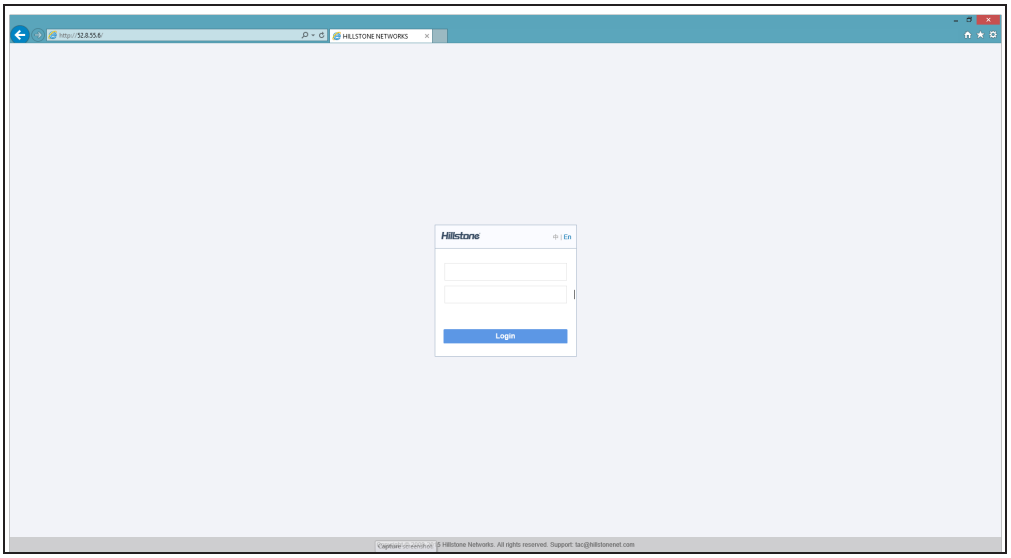


Visiting WebUI of StoneOS

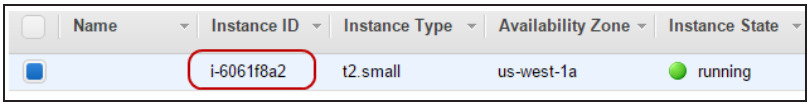
1. In order to enable WebUI access, enter the command below to enable eth0's http protocol first:

```
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.



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

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

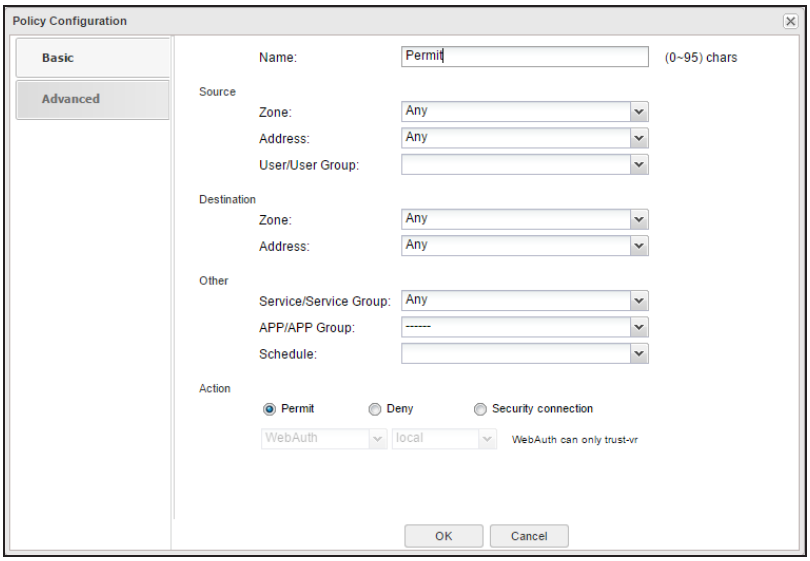
Basic Configurations of StoneOS

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**).



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)

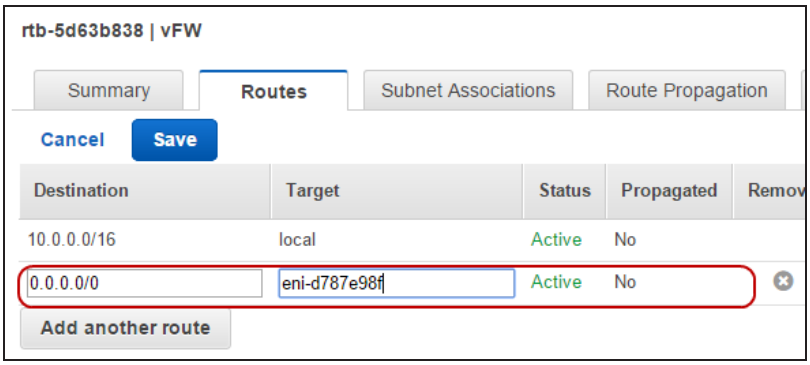
In this section, a Windows 2012 Server virtual machine will be created. This virtual server will be an internal server in a company's private network, and it connects to public network by vFW.

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.

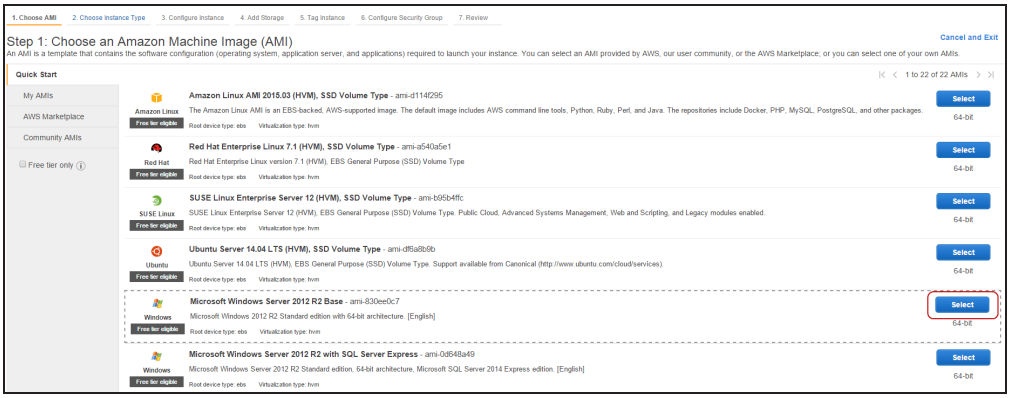


4. Click **Save**.

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**.

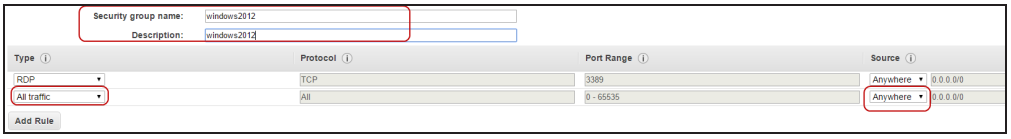


3. Keep the default settings in instance type page, click **Next: Configure Instance Details**.

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.

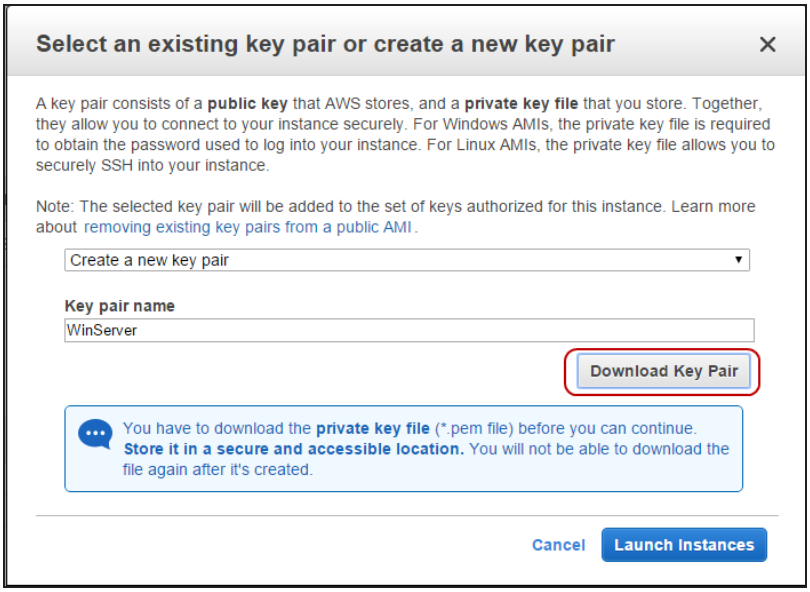
   On this page, add a rule to allow all traffic.



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.

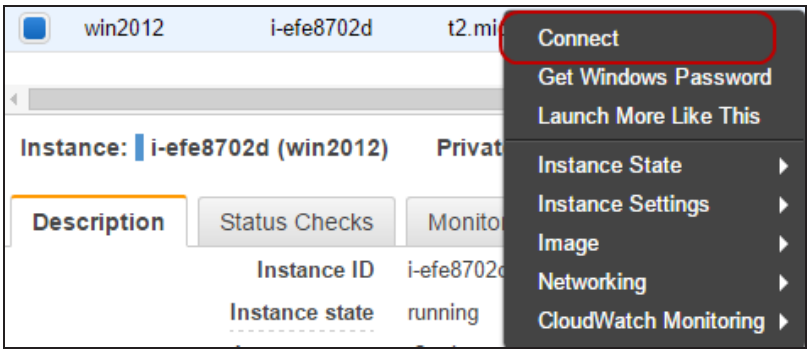


8. Click **Launch Instance**. The Windows EC2 instance will start to boot.

Step 3: Acquiring Password of Test Instance

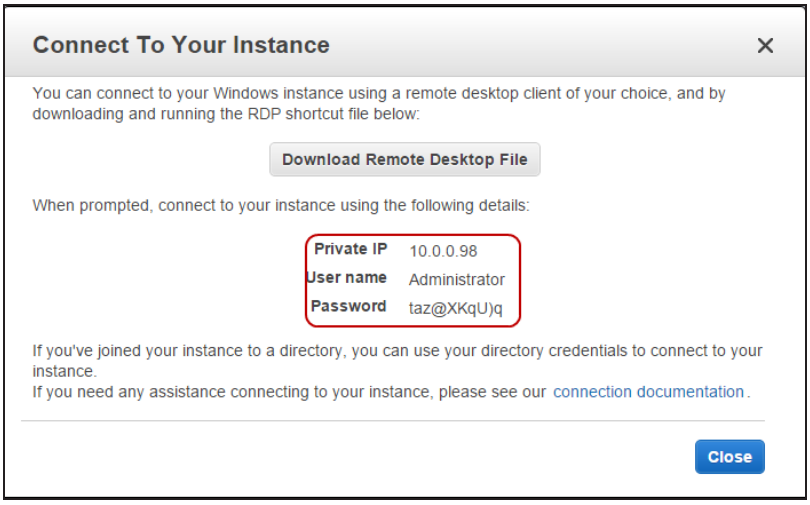
To connect to the test Windows instance, you will use the key pair file.

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



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.



4. Close this dialog.

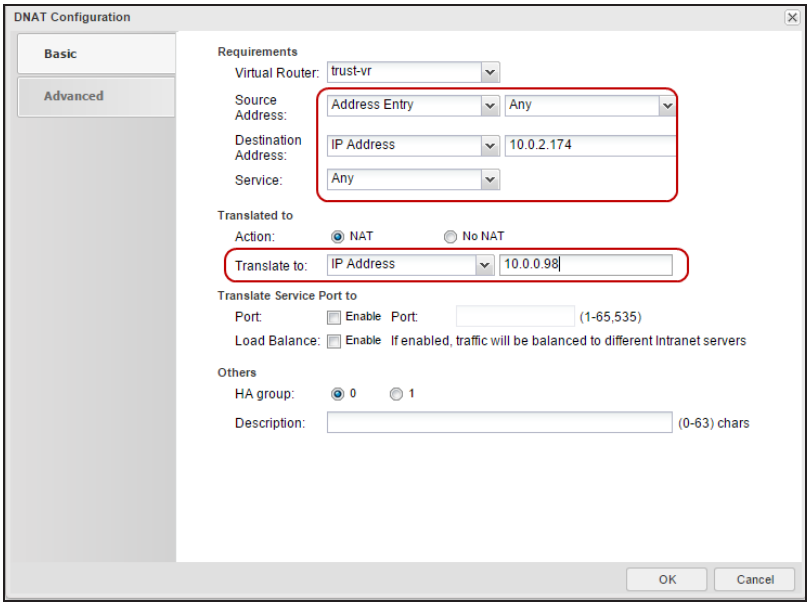
Step 4: Creating a DNAT rule

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.



3. Click **OK**.

Or, you can use the following command in CLI:

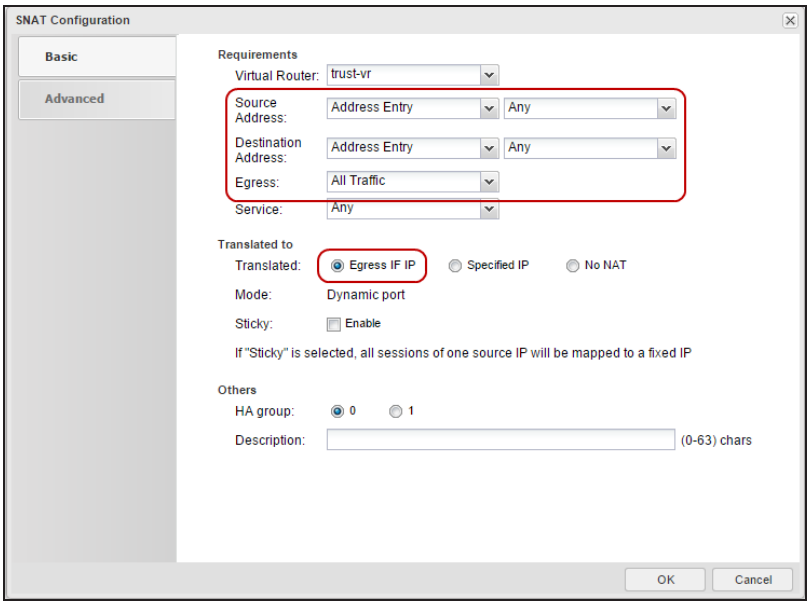
```
SG-6000(config)# ip vrouter trust-vr

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.



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
```

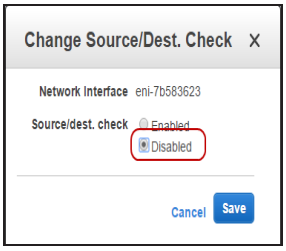
Step 6: Disabling Source/Dest. Check

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**.



Starting Test

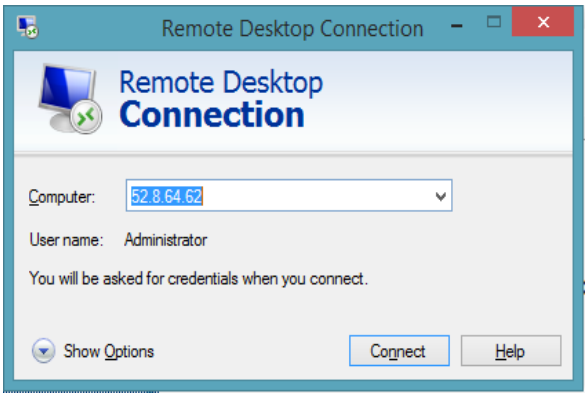
Before testing, make sure your vFW has the following settings:

- A security rule that allows all traffic ("Creating a Policy Rule" on Page 75);
- You have disabled Source/Dest. check for interfaces that connect to IGW ("Installing CloudEdge on AWS" on Page 65);
- A DNAT rule that translates eth0's address to private server's address ("Step 4: Creating a DNAT rule" on Page 80);

Test 1: Visiting Private Server

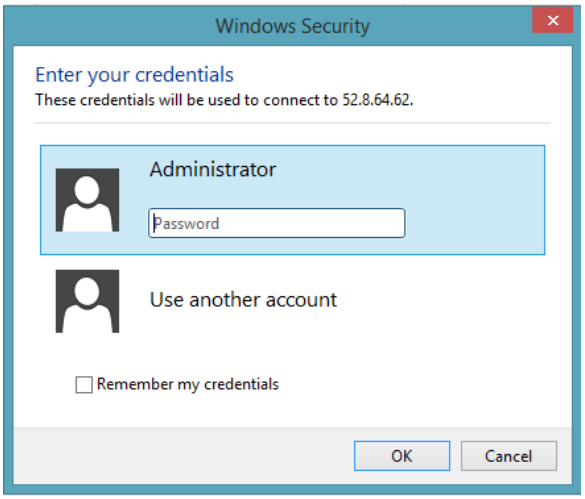
On a PC with Internet connection, you can use remote desktop client to visit private virtual server.

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).



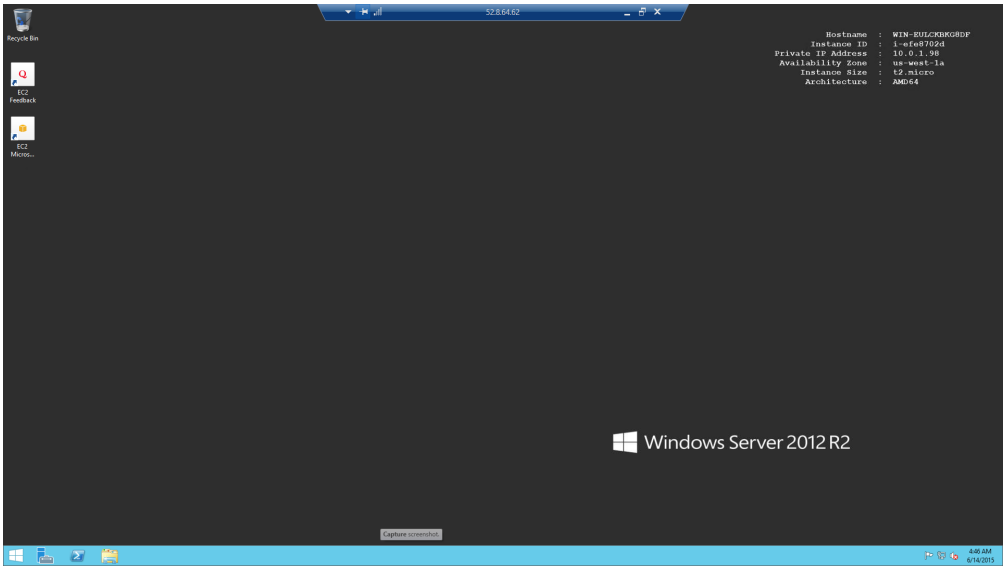
3. Click **Connect**. Copy the encrypted password (you should have already saved the password in text file), and paste the password in the password field. If the system indicates your password is wrong, you may try to manually input the pass-

word.



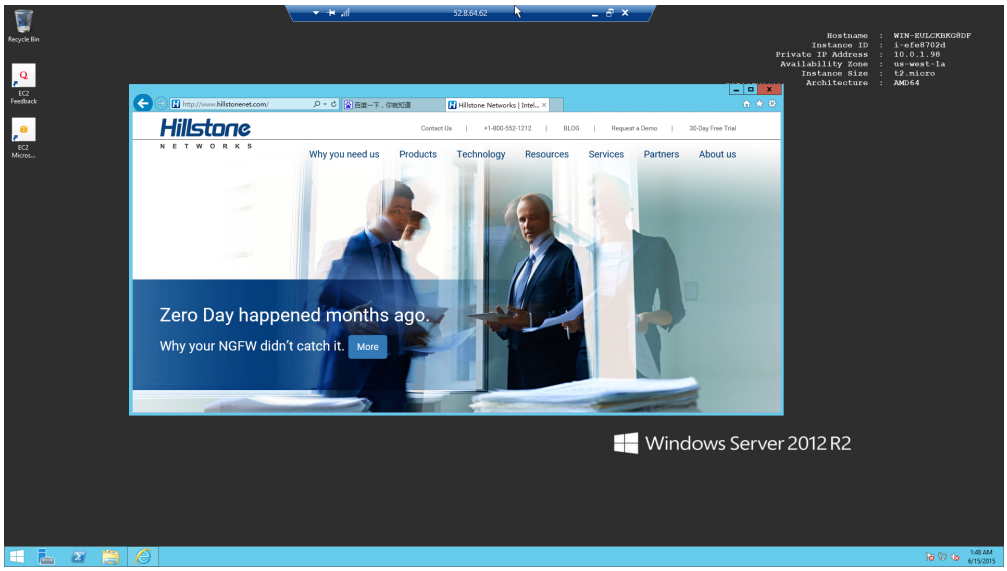
4. In the prompt of certificate warning, click **Yes** to continue.

5. Now you have entered the Windows server system.



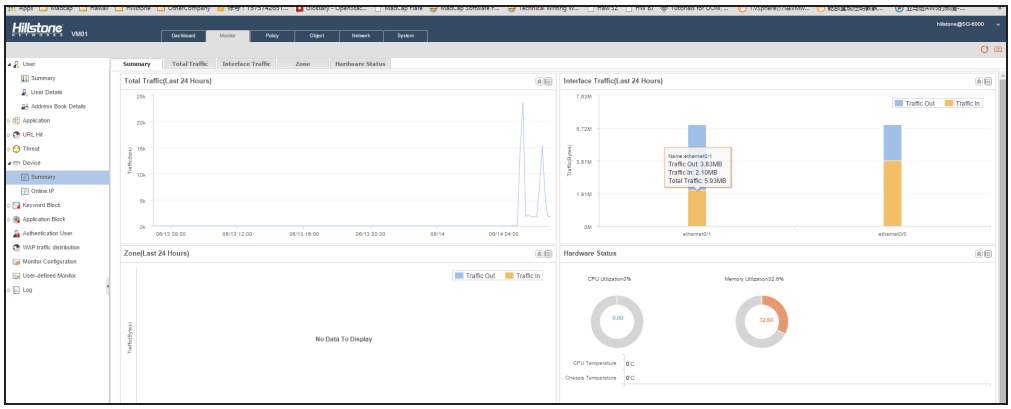
Test 2: Internal Server to Access Internet

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



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.



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.

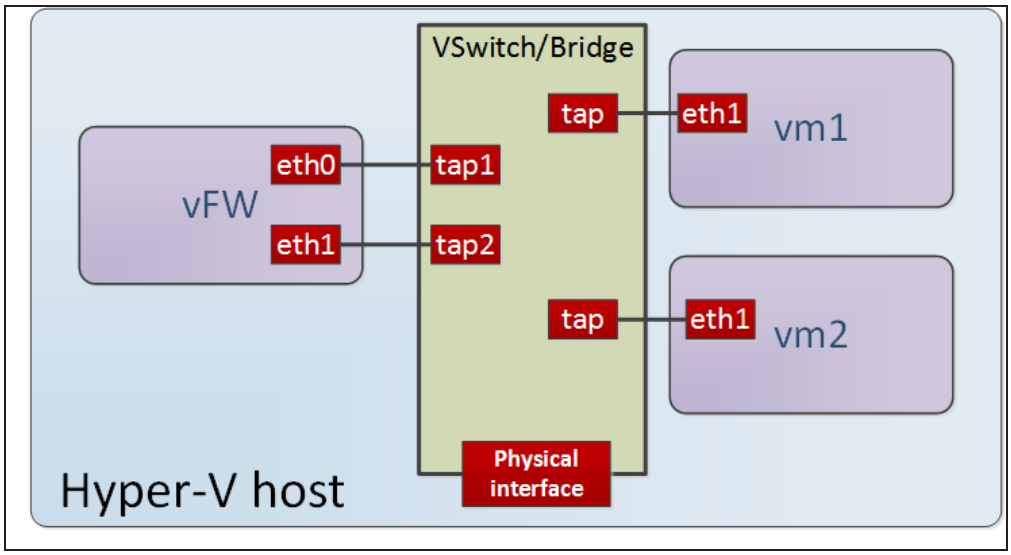
System Requirements

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**.
   For the VM01 model, the minimum memory value is 1024 MB; for VM02 model, the minimum memory value is 2048 MB.
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, eth-0/0 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 86

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).

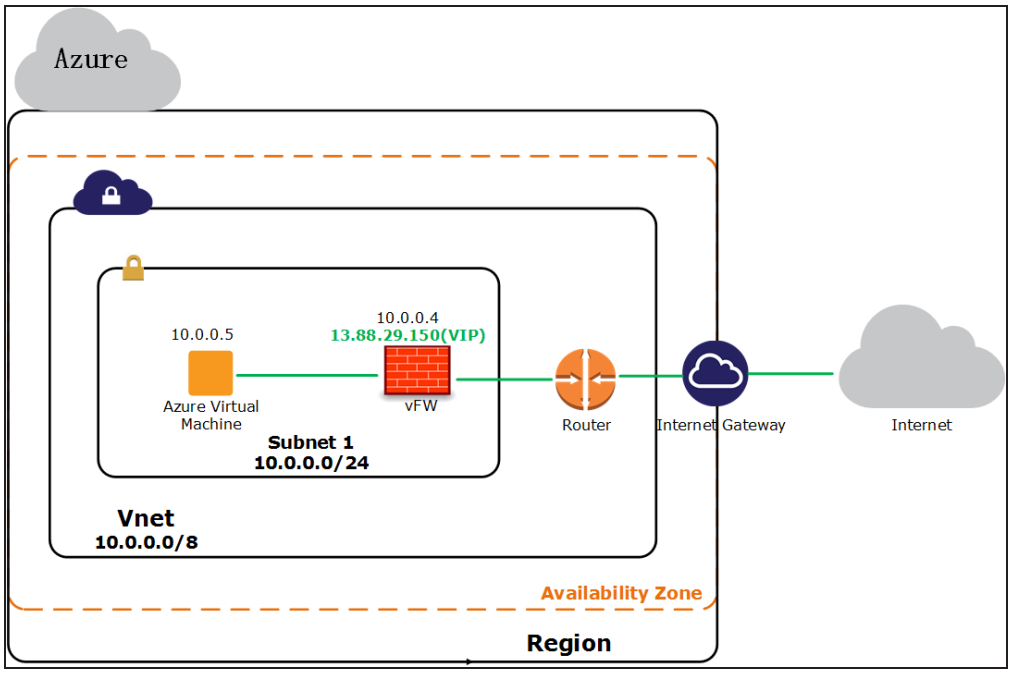
Upgrading vFW

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 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 out-bound and inbound traffic of the subnet. The following is the network topology:

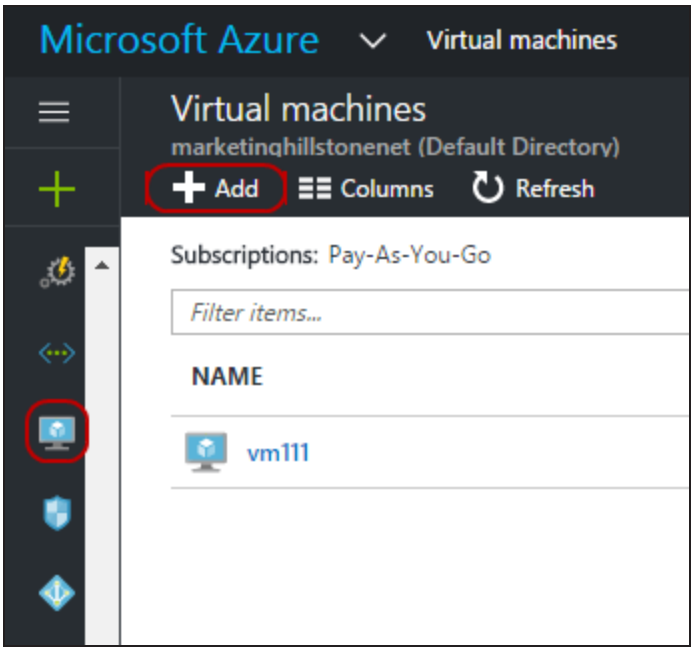


Installing CloudEdge

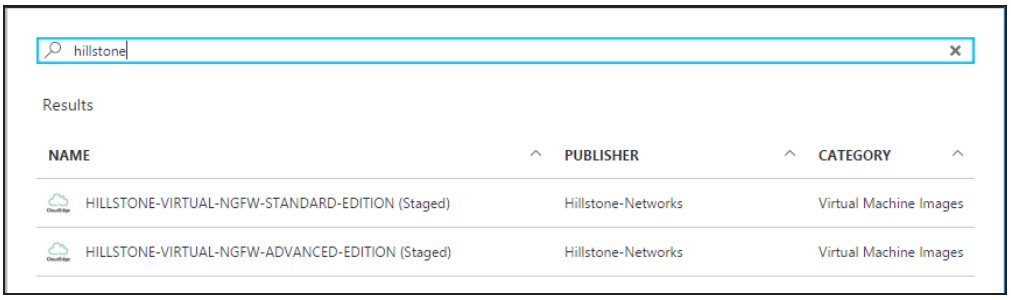
CloudEdge will be running in a virtual machine of the Azure Vnet. After installation, you will have a running virtual StoneOS system which you can visit via CLI and WebUI.

Step 1: Purchasing CloudEdge and Creating a virtual machine

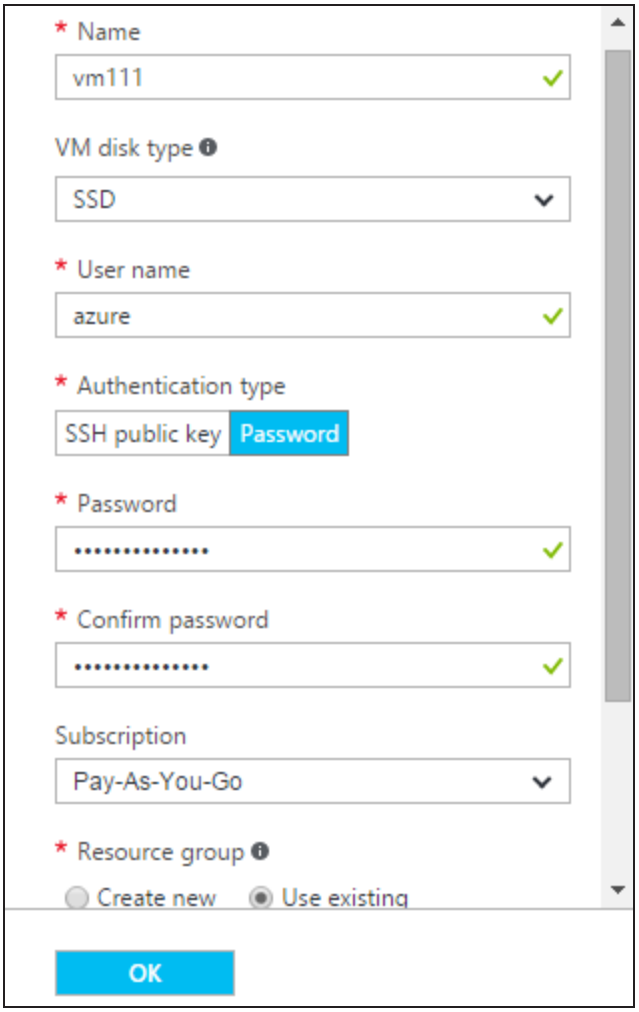
1. Log into Microsoft Azure. Select **Virtual machines** in the left navigation pane, and then click **Add** on the top of the right page.



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.



3. In the Basics page, configure the settings as follows, and then click **OK**.

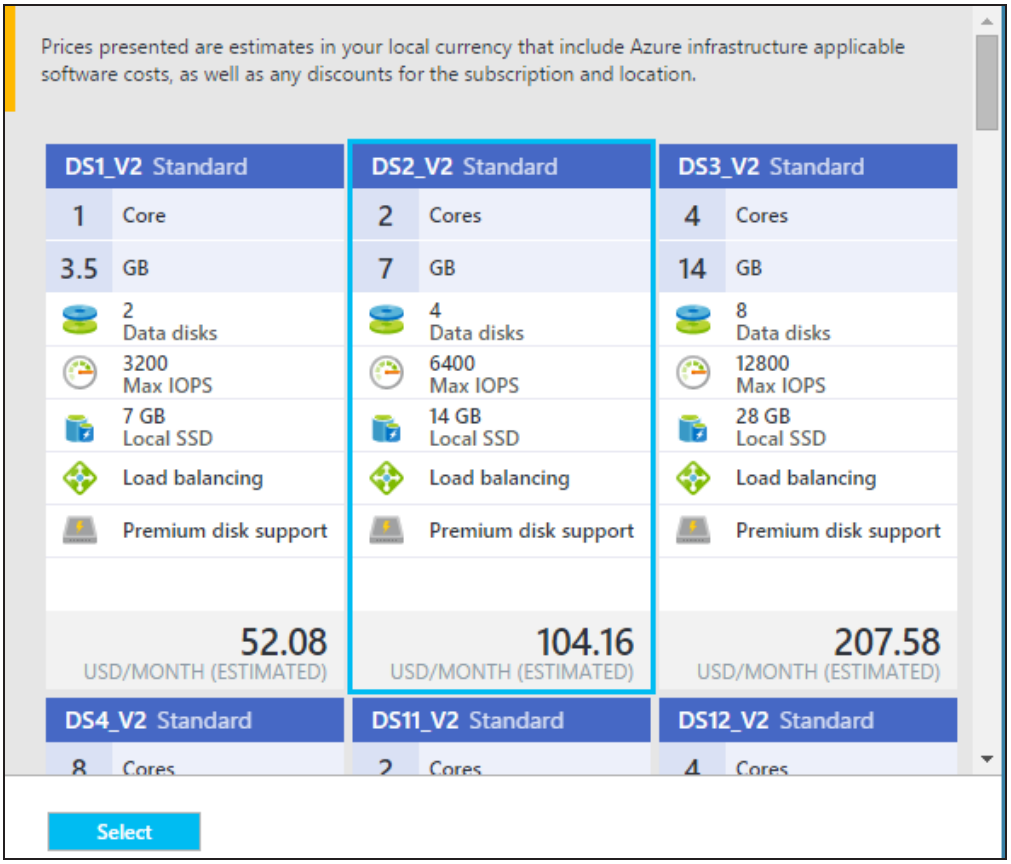


Note:

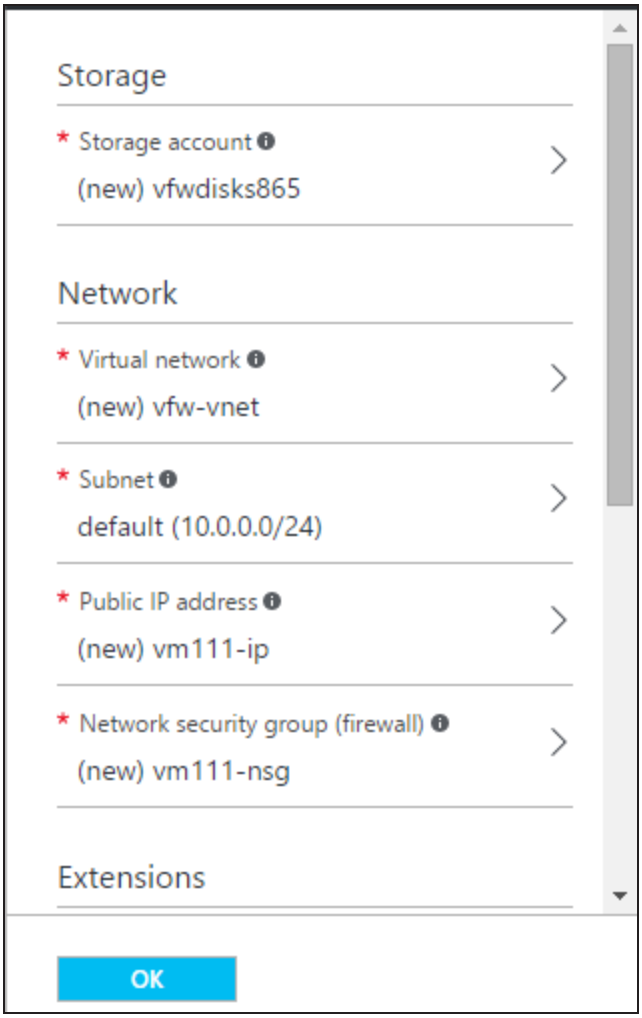
- If you specify the username as hillstone and change the password, the system will update the password; if the new created username is not hillstone, the system will update the password which belongs to the hillstone user to the new, and a new user will be created, the password will be the same as hillstone 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**.



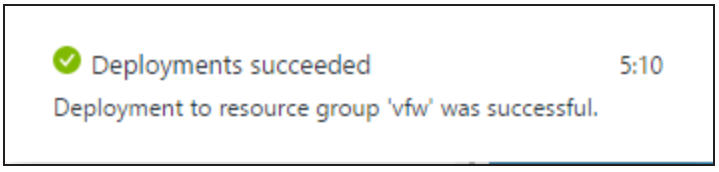
5. In the Settings page, configure the settings as follows, and then click **OK**.



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.

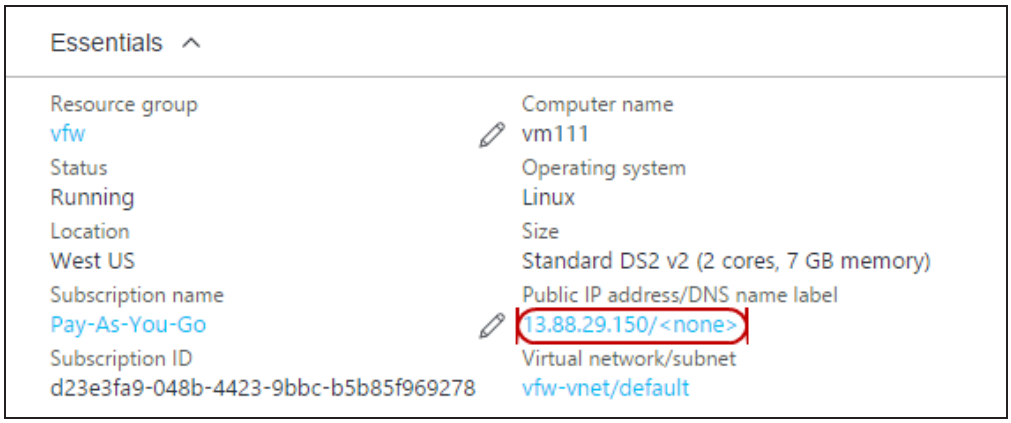
6. Check the detailed configurations in the Summary page, and then click **OK**.

7. Click **Purchase** to pay for the virtual machine in the Buy page.
After a few minutes, the virtual machine will be deployed successfully.



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.



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

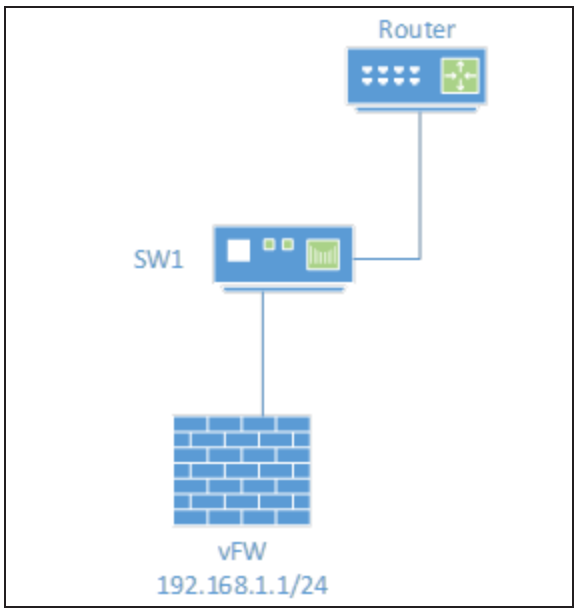
After you purchased CloudEdge, CloudEdge Licenses are also needed, which ensure CloudEdge run normally in Azure. Contact Hillstone salesperson to buy the license you need. To install the license in CloudEdge, see "Installing License" on Page 6

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:



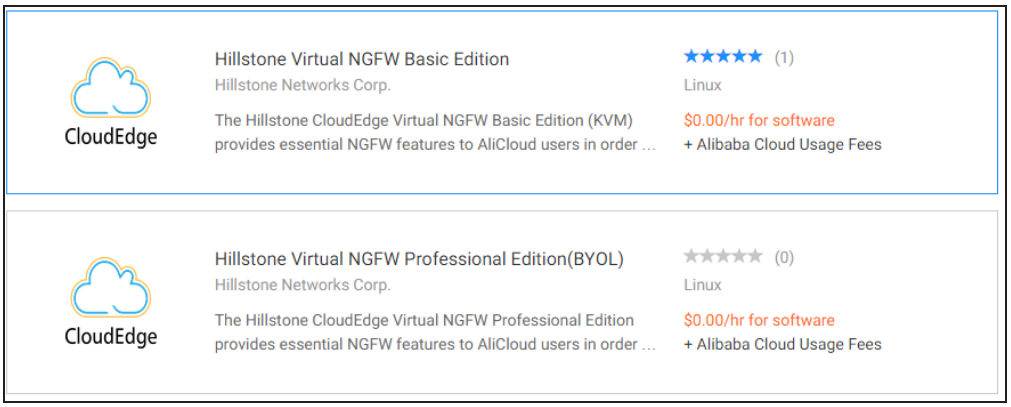
Installing vFW

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).



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

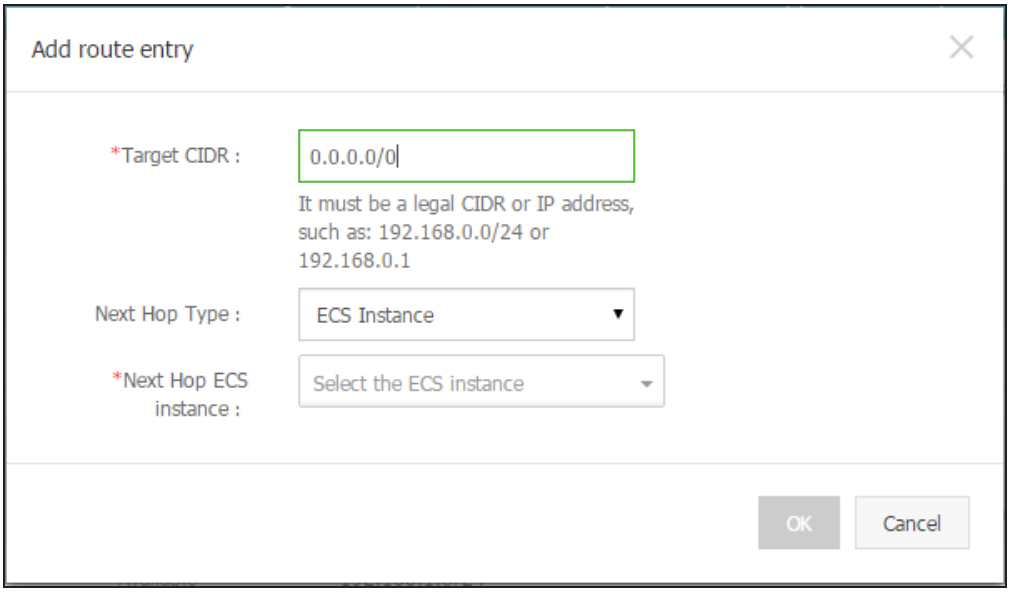
1. After an ECS instance is created successfully, vFW will start automatically.
2. Select **Elastic Compute Service** in the left navigation pane, then click **Instances** item on the left. Instance list will be shown in the right page.
3. Click **More** in Action column of ECS instance which vFW is 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.



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 6

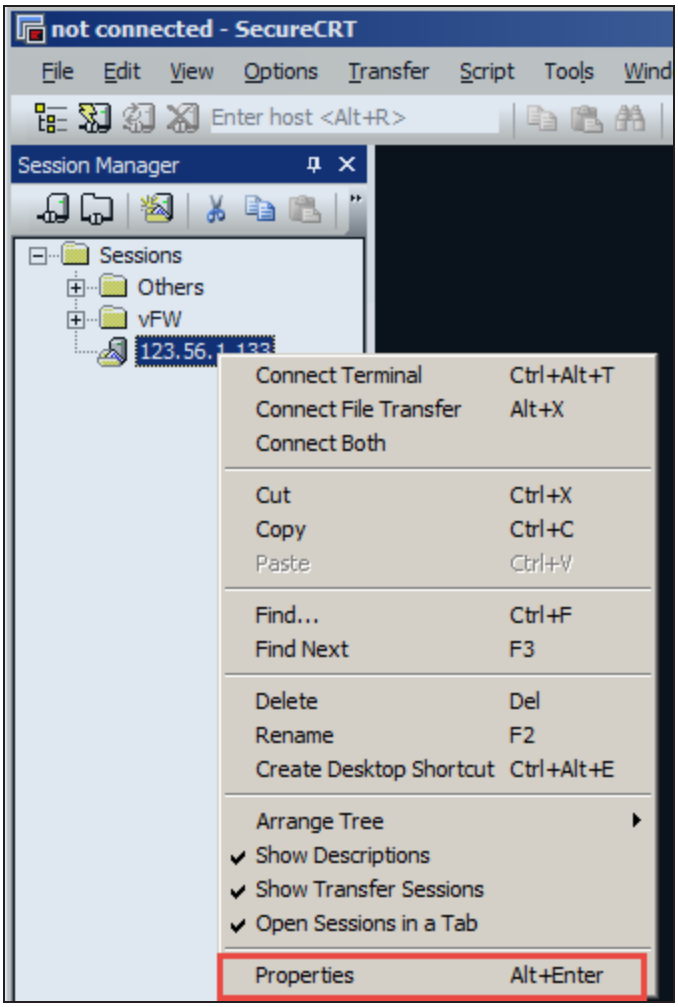
Step 5: Visit the vFW

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.

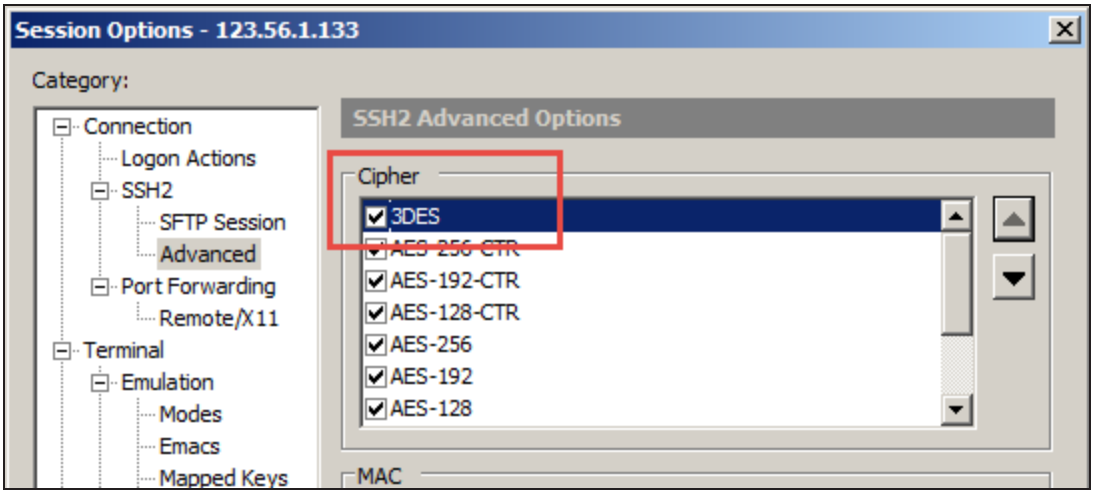
To Login vFW via SSH2

Note: 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.



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.

Change History

You are reading the V4.0 version of this document. The change history is as follows.

Release	Change
Feb, 2015	Initial release. System version 5.5R1. Doc version V1.0.
Jun, 2015	Added installations on VMware ESXi and AWS. System version 5.5R1P1. Doc version V2.0.
Aug, 2015	Added upgrade steps for AWS and VMware; IPS parameters corrected. System Version 5.5R1P1, Doc Version V2.1.
Nov, 2015	Update installations on AWS: private key, AMI and license. System Version 5.5R1T20. Doc Version V2.2.
Nov 26, 2015	AWS: StoneOS UI login password is instance ID. System version is 5.5R1T21. Doc version is V2.3.
Dec 1, 2015	AWS: added browser compatibility notice. System Version is 5.5R1T21. Doc version is V2.4.
Jan 12, 2016	Intro: correct a typo. Doc version is V2.5. System Version is 5.5R1T21.
April 15, 2016	New Feature: support system upgrade via Web UI; support full license image on AWS. OS version 5.5R1P7.1.