Hillstone Networks, Inc.

CloudEdge Deployment Guide

Version 5.5R3P1

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://docs.hillstonenet.com.

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-5.5R3P1-EN-V4.0-2016/10/19

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 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 Alibaba Cloud platform, the administrator should be familiar with the concept of 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 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 and function 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

- **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. When platform trial license expires, the system will not be allowed to configure if it is not restarted; if it is restarted, the system will restore to the status which the it only has a default license.

- **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, CloudEdge will use Default License. The system can be normally functioning, but cannot upgraded to higher version.

- **Default License**

  CloudEdge has a built-in free default license. The default license is eternally valid.

  CloudEdge using the default license provides the same features as Platform Base License, but capacities are restricted.

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.

- **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:** URL DB function and Perimeter Traffic Filtering (PTF) function can be seen in StoneOS, but they are not available for the moment. Future versions will support the two functions.

> **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.

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.

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.
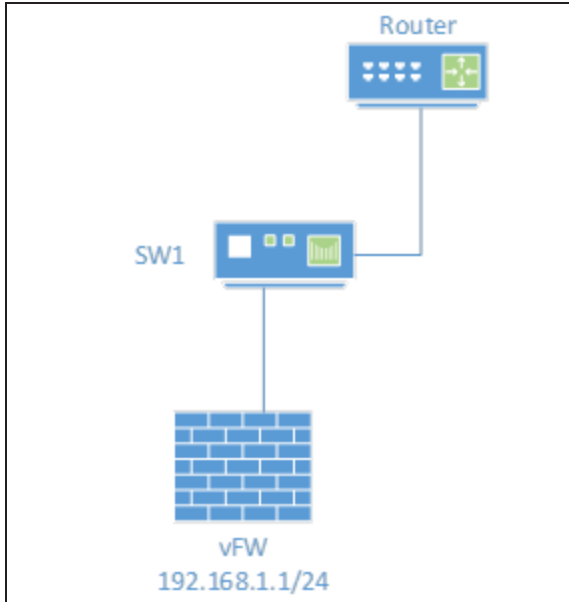
To install a license:

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 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 5
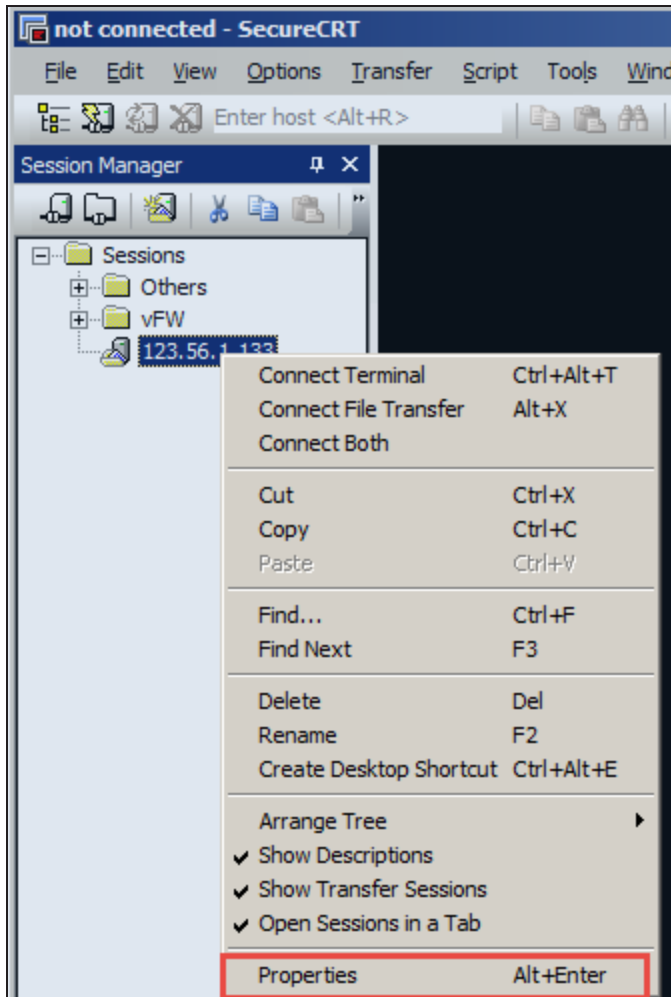
Step 5: Visit the vFW

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.
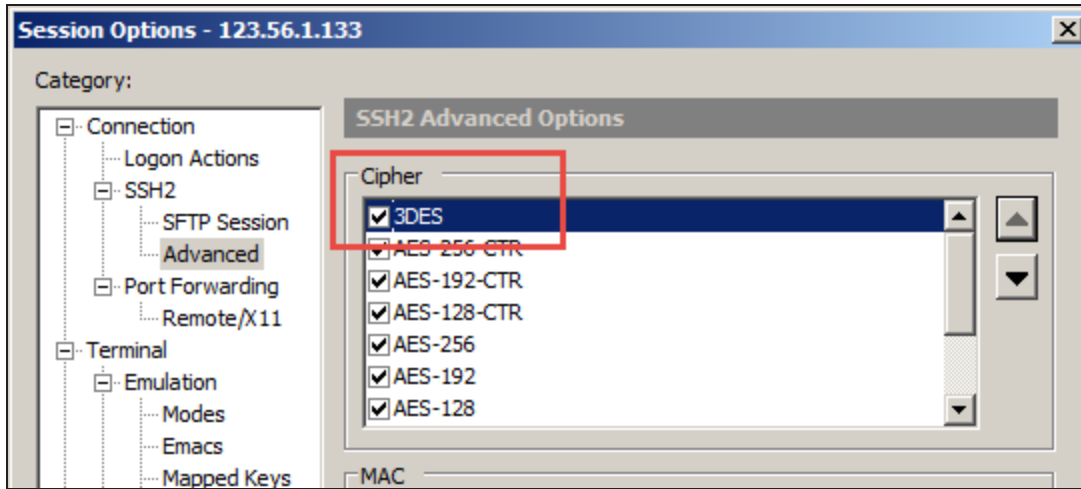
To Login vFW via SSH2

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.