Hillstone Networks, Inc.

云·界CloudEdge虚拟防火墙部署手册

Version 5.5R3

目录

目录 1
介绍 1
文档内容 1
目标读者 1
产品列表 1
虚拟防火墙的功能 1
许可证 3
许可证机制 3
平台类许可证 3
功能服务类许可证 3
申请许可证 4
安装许可证 4
在阿里云上部署CloudEdge 6
准备工作 6
部署虚拟防火墙 6
第一步：购买vFW镜像并创建ECS实例 6
第二步：查看vFW初始配置 7
第三步：购买并申请License软件 8
第四步：从外网访问vFW 9
使用SSH2远程登录vFW： 9
使用HTTP远程登录vFW： 10

介绍

山石网科的虚拟防火墙产品，简称为CloudEdge（Virtual Firewall），是一个纯软件形态的产品，是运行在虚拟机上的StoneOS系统。

文档内容

本手册介绍如何将CloudEdge虚拟防火墙部署到阿里云环境中。本文仅讲述安装防火墙和初始的联网操作，StoneOS系统本身的功能将不做讲解。

如果您需要了解StoneOS系统的详细功能，请参考StoneOS的相关文档（点击此处）。

目标读者

本文的目标读者为企业的网络管理员或对山石网科虚拟化感兴趣的读者。

产品列表

CloudEdge系列虚拟防火墙共包含两款产品：SG-6000-VM01和SG-6000-VM02，他们的性能和参数列表如下：

性能参数	SG6000-VM01	SG6000-VM02
内核（最低/最高）	1/1	2/2
内存（GB）	1 GB	2 GB
防火墙吞吐量（1518 Bytes ）	2 Gbps	4 Gbps
最大会话	100 K	500 K
每秒新建会话	10 K	20 K
IPS吞吐量（1280 Bytes）	200 Mbps	400 Mbps
接口最大数	10 x virtual NICs	10 x virtual NICs
IPSec VPN 隧道最大数/隧道接口最大数	50	500
SSL VPN用户数（默认/最大）	5/50	5/250
安全域最大数量	16（包括8个预定义安全域）	16（包括8个预定义安全域）
策略规则最大数量	1000	1000
地址簿对象最大数量	512	512

虚拟防火墙的功能

CloudEdge支持以下防火墙功能：

- 基本防火墙（策略、安全域、NAT等基础防火墙功能）
- 应用识别
- 攻击防护（AD）
- 入侵防御（IPS）
- VPN（IPSec VPN、SSL VPN）
- 用户管理
- 访问控制
- 高可用性（HA）

- LLB负载均衡
- 管理功能
- 日志
- 统计集
- iQoS

许可证

CloudEdge虚拟防火墙产品的性能，由许可证的控制。只有购买并安装了相应的许可证，才能使产品达到其标称的数值。购买许可证，请与销售人员联系。

许可证机制

与Hillstone Networks, Inc.的硬件防火墙产品类似，虚拟防火墙的许可证机制也分为平台许可证和功能服务类许可证。平台许可证是功能服务类许可证运行的基础。

注意: 如果您在公有云平台上购买的防火墙是内置许可证（full license）的版本，那么您无需额外购买许可证，也无需安装许可证，即可获得以下许可证所代表的所有功能。

平台类许可证

- **平台试用许可证（Platform Trial）**
  安装平台试用许可证后，支持的功能和性能与正式许可证相同，但是使用期限较短。具体可用时长，根据申请时协议决定。
  到期后， 已有的配置不能修改，若设备重启，防火墙恢复到默认许可证（default）控制的状态，受限的性能将重新受限。
- **平台正式许可证（Platform Base）**
  设备正式销售后，可以安装平台正式许可证。正式许可证提供基础防火墙功能和VPN功能，并且防火墙性能可达到标称数值。
  到期后，设备恢复到默认许可证的状态，此后设备仍可正常使用，但不能升级到期后的OS版本。
- **默认许可证（Default ）**
  虚拟防火墙预装了一个免费的默认许可证（default license），无需申请。该许可证长期有效。
  使用默认许可证，系统功能的种类与使用正式许可证相同，只是性能受限，如下：
  - 防火墙吞吐（1518 Bytes）：100 Mbps
  - 防火墙吞吐（64 Bytes）：10 Mbps
  - 最大会话： 1 K
  - 每秒新建会话：1 K
  - IPSec 吞吐量 512 包： 0
  - IPSec VPN 隧道数：0
  - SSL VPN用户数：0
  - 最大策略数量：50
  - 最大地址簿数量：100

功能服务类许可证

只有购买并安装了各个功能服务类许可证，用户才能使用相应的功能，并能够获取特征库更新。

- **SSL VPN 许可证**
  授权SSL VPN的最大接入数量。多个SSL VPN许可证可以叠加允许接入用户的最大数量。没有单独的使用期限，过期时间与vFW所使用的平台许可证相同。
- **QoS许可证**

开启QoS功能。 没有单独的使用期限，过期时间与vFW所使用的平台许可证相同。

- **入侵防御（IPS）许可证**
  提供入侵防御功能和IPS特征库升级。 具有单独的使用期限。过期后，不能升级IPS特征库，入侵防御功能正常使用。
- **APP DB 许可证**
  提供APP库升级功能。APP DB许可证不需要单独申请，随平台许可证一同发放，有效期也同平台类许可证。 过期后，不能升级APP特征库。

注意: URL DB功能和边界流量过滤（PTF）功能在界面上可见，但这两个功能暂时不生效，后续版本将支持。

注意: 除了上面列出的许可证外，硬件防火墙所支持的其他许可证，包括VSYS许可证、病毒过滤（AV）许可证、提供高级威胁防护和异常行为分析的StoneShield许可证，虚拟防火墙暂不支持。

申请许可证

申请许可证，需要登录StoneOS系统。

部署好虚拟防火墙后，访问StoneOS的WebUI界面，然后按照以下步骤生成许可证申请：

1. 登录StoneOS系统。
2. 选择“系统 > 许可证”，进入许可证页面。
3. 在“许可证申请”中，填写生成许可证请求所需要的信息。
4. 点击“生成”，出现一串代码。
5. 将生成的代码发送给销售人员，由其获取许可证再返回给您。

安装许可证

获得许可证后，用户需要将其装载到设备上使其生效。安装许可证，请按照以下步骤进行操作：

1. 选择“系统 > 许可证”，进入许可证页面。
2. **在“许可证申请”中，用户可根据需要，以下以下两种方式中的一种导入许可证。**
   - 上传许可证文件：选中“上传许可证文件”单选按钮，点击“浏览”按钮，并且选中许可证文件（许可证为纯文本.txt文件）。
   - 手动输入：选中“手动输入”单选按钮，然后将许可证字符串内容粘贴到文本框中。
3. 点击“确定”按钮保存所做配置。
4. 选择“系统 > 设备管理”，然后点击<设置及操作>标签页。
5. 点击“重启设备”，然后在提示对话框点击“确定”。
6. 等待系统重启。启动后，许可证将生效。

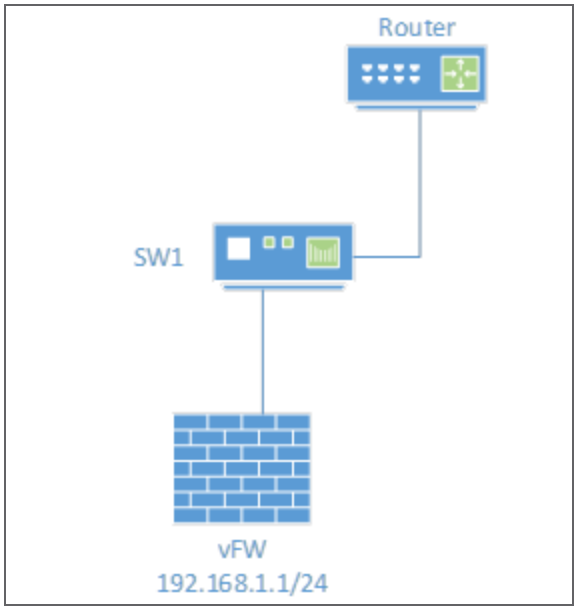
注意: 如果您在非公有云平台上购买CloudEdge系列防火墙，请联系山石网科的销售人员获取USB key 和《虚拟许可证管理系统vLMS使用手册》。

在阿里云上部署CloudEdge

准备工作

- 创建如下VPC：
  - VPC：192.168.0.0/16
  - Subnet 0：192.168.1.0/24
- 创建安全组，并配置安全组规则

部署虚拟防火墙后，网络拓扑为：



部署虚拟防火墙

虚拟防火墙（vFW）将作为一个ECS实例安装在VPC中。安装完成后，您将：

- 拥有一个运行中的虚拟StoneOS系统
- 能够访问防火墙的CLI和WebUI界面

第一步：购买vFW镜像并创建ECS实例

1. 登录阿里云·云市场并搜索“山石网科”关键字。根据您的实际需求，在搜索结果列表中选择“山石网科虚拟化下一代防火墙（IPSEC/SSL/L2TP VPN）双核专业版“等虚拟防火墙。
   标注“IO优化”的版本，只能在勾选“I/O优化实例”的虚拟机上运行。 未标注“IO优化”的版本，只能在未勾选“I/O优化实例”的虚拟机上运行。

2. 在虚拟防火墙页面中，查看产品详情等信息。如需购买，请点击页面右侧的“立即购买”。
3. 选择ECS实例所在的地域和镜像版本。
4. 在<推荐配置>部分选择ECS实例的规格。
   阿里云平台推荐的ECS配置有可能会出现与镜像规格不匹配的情况，这会导致ECS实例创建后无法获取到IP地址的问题，请尽量通过“选择更多配置“来自定义选择ECS配置。

5. 在<I/O优化>部分配置ECS实例是否支持I/O优化。
   如果ECS实例规格分为支持I/O优化和不支持I/O优化两种情况，此处将显示“I/O优化实例”复选框。
6. 在<安全组名称>部分选择ECS实例所属的安全组。如需从外网访问vFW，此安全组需包含从公网到内网入方向的允许规则。
7. 在<网络类型>部分选择“专有网络”。
8. 依次在<公网带宽>、<带宽>、<系统盘>、<数据盘>、<付费方式>和<购买时长>部分完成配置。
9. 在<密码>部分配置vFW的登录密码。
10. 页面右侧显示当前配置信息，点击“立即购买”，并在<确认订单>页点击“去开通”。
11. 完成支付后，等待片刻，ECS实例即可创建成功。

第二步：查看vFW初始配置

1. 创建vFW的ECS实例后，vFW自启动。
2. 在阿里云的管理控制台中，点击“产品与服务 > 云服务器ECS”。在云服务器ECS的实例列表页，找到此vFW的ECS实例。
3. 点击“更多”，在弹出菜单中选择“连接管理终端”。
   阿里云会提供登录管理终端的初始密码，请牢记此密码。
4. 在弹出的对话框中输入初始密码。
   如需修改密码，请点击“修改管理终端密码”。
5. 在CLI页面中输入登录名和密码。登录名为hillstone，密码是用户创建此ECS实例时指定的密码。
   默认情况下，vFW的接口eth0/0可通过DHCP自动获取IP地址，并可以设置默认路由。用户可使用**show interface**命令和**show ip route**命令查看。

```
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 - SYMC, 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
================================================================================
```

6. 执行**show version**命令，查看并记录设备的S/N号。

第三步：购买并申请License软件

此步骤仅适用于BYOL类型的产品，按需付费类型产品请忽略此步骤。

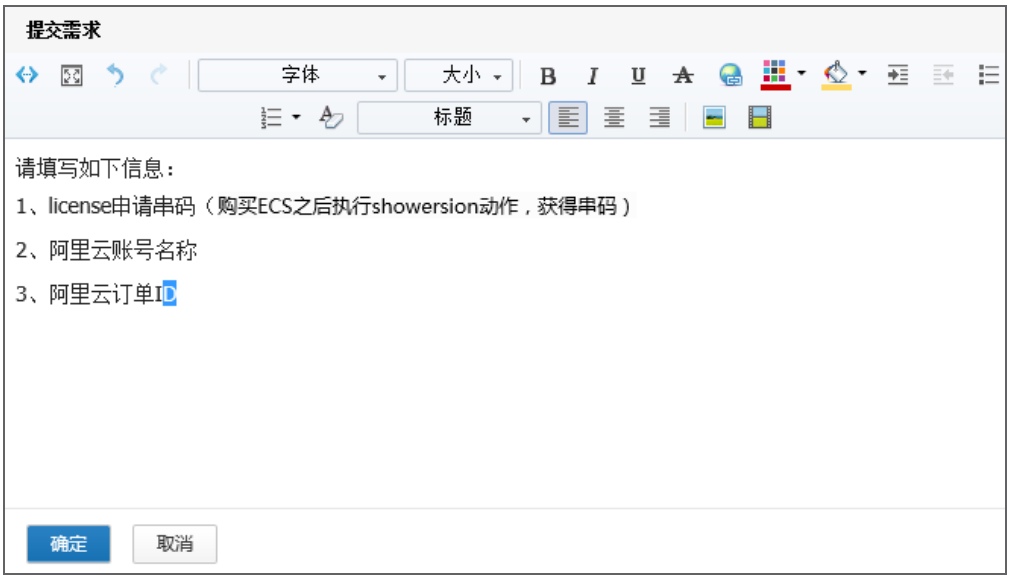
购买BYOL类型的产品并支付完成后，还需要购买山石网科虚拟化下一代防火墙License软件并安装，才能保证虚拟防火墙在阿里云上正常使用。

1. 在阿里云·云市场主页面搜索“山石网科”关键字。根据您已购买的镜像产品型号和规格，在搜索结果列表中选择相应型号的虚拟防火墙License。
   License软件分为专业版、基础版和旗舰版。
2. 在虚拟防火墙License页面中，查看软件详情。在页面右侧选择规格和订购周期后，点击“立即购买”。
3. 在<确认订单>页点击“去支付”并完成支付。
4. 在阿里云·云市场主页面右上角点击“管理我的服务”。

5. 在<已购买的服务>页面，点击刚才购买的license后面的“服务监管”来申请license。

6. 在<服务管理>页面点击“提交需求”按钮。

7. 在<提交需求>页面的文本域内填写S/N号、阿里云账号名称和阿里云订单ID，点击“确定”。



8. 请联系山石网科的客服人员来获取license软件。
将license软件安装到vFW中，请参见"安装许可证" 在第4页

9. 如果license软件安装成功，请进入阿里云·云市场的<服务管理>页面点击“确认”。
至此，您已经完成了license软件的申请流程。

第四步：从外网访问vFW

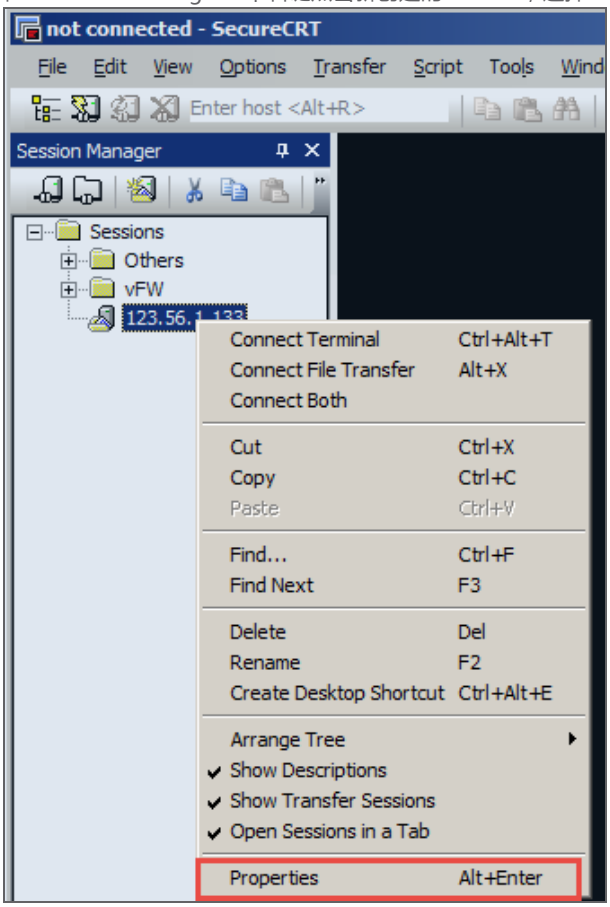
如需从外网访问vFW，ECS所安全组需包含从公网到内网入方向的允许规则。

使用SSH2远程登录vFW：

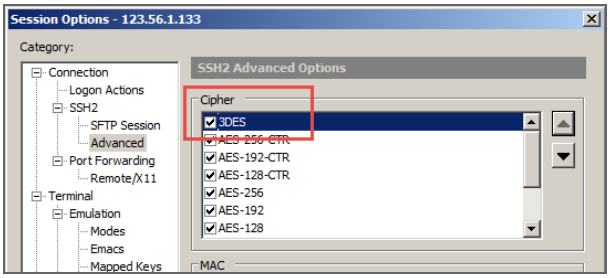
注意: 从外网通过SecureCRT等工具使用SSH2进行远程管理时，需要将连接对应的加密算法进行调整，需要将3DES调整到首位。否则，将无法连接且提示如下信息：Invalid packet header. This probably indicates a problem with key exchange or encryption.

1. 打开远程终端登录软件。以SecureCRT为例。
2. 点击“File > Quick Connect”。在“Protocol”下拉菜单中选择“SSH2”。
3. 在“Hostname”中输入弹性公网IP。
4. 点击“Connect”。

5. 在“Session Manager”中右键点击新创建的Session，选择“Properties”。



6. 在弹出菜单中的“Advanced”选项中，将“3DES”算法上移到顶。



7. 点击“OK”。
8. 连接此Session。
9. 输入用户名hillstone，按回车键。
10. 输入密码。此密码为创建vFW的ECS实例指定的密码。按回车键，即可登录。

使用HTTP远程登录vFW：

1. 打开浏览器，输入vFW的弹性公网IP。
2. 在登录页面输入用户名hillstone。

3. 输入密码。此密码为创建vFW的ECS实例指定的密码。
4. 按回车键，即可登录。