Hillstone Networks, Inc.

云·界NFV服务链编排指导手册

目录

介绍

本手册介绍山石云·界NFV自动化编排部署的方法及VNFD（Virtualised Network Function Descriptor）和SFC（Service Function Chain）模版的介绍。本文仅讲述编排方法及模板注释，关于Openstack、NFV相关基础知识以及StoneOS系统功能不做讲解。

关于NFV

NFV(Network Function Virtualization，网络功能虚拟化），主要利用虚拟化技术实现软硬件解耦合和功能抽象。NFV方案通过提前编排各个VNF（Virtual Network Feature）网元和自动化授权业务的方式，帮助用户实现业务流程的自动化部署，从而提升了新业务的开展和调整速度。在云计算网络中使用NFV, 需要引入NFV管理器, 用于配置、监视以及管理NFV的生命周期。Tacker是OpenStack的一个子项目，作为一款开源的NFV管理器，用于管理NFV的生命周期。更多Tacker资料请点击此处。

关于山石云·界

云·界是山石网科的一款虚拟防火墙产品，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。如果您需要了解StoneOS系统的详细功能，请参考StoneOS的用户手册（点击此处）。

云·界NFV方案通过编写VNFD（Virtualised Network Function Descriptor）模板和SFC（Service Function Chain）模版的方式，来实现自动化的编排部署。

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产品感兴趣的读者。用户需要相应地熟悉Openstack、NFV及虚拟化相关知识。本手册以读者已经掌握Openstack、NFV及虚拟化知识为前提，将只介绍编排方法及VNFD和SFC模板内容。

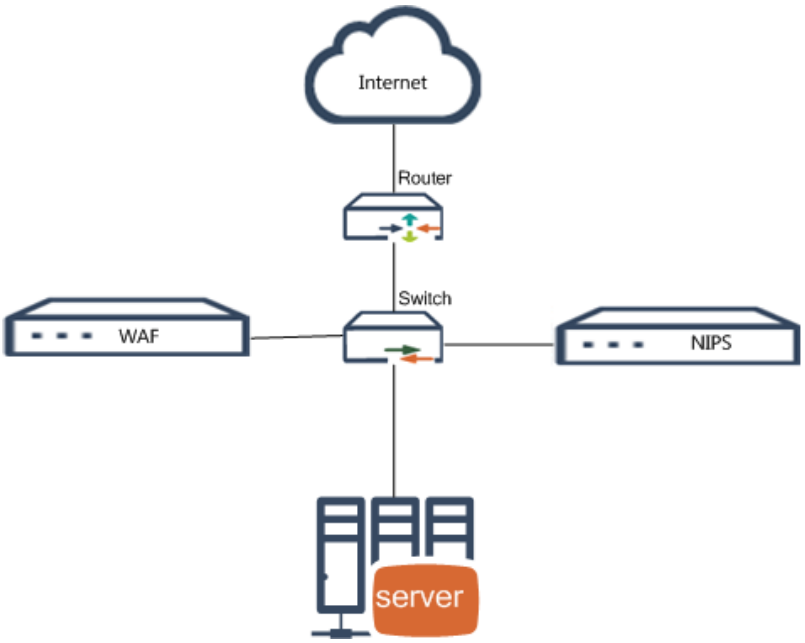
内容导读

本手册主要包含以下内容：

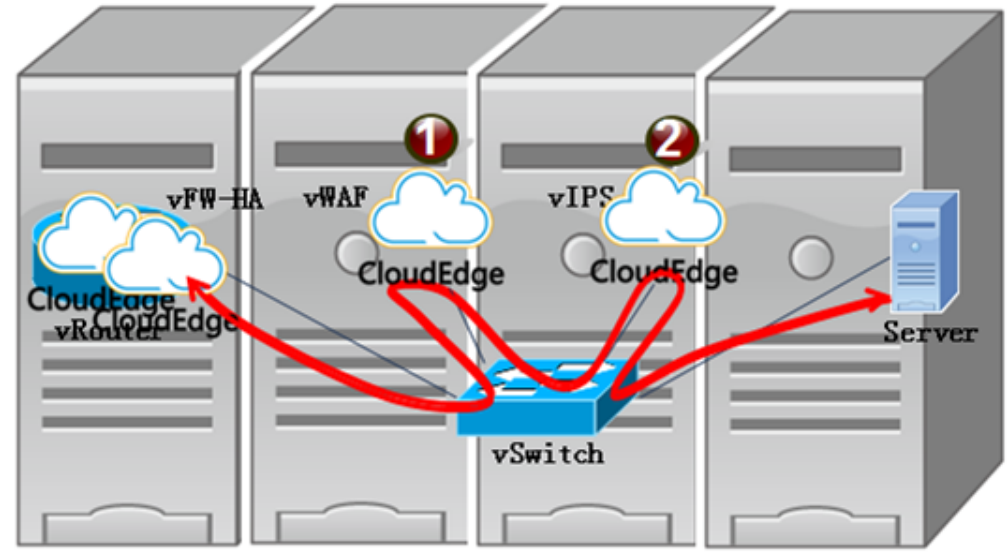
云·界NFV典型案例

本案例介绍云·界产品基于SDN+NFV的服务链编排方法。

如下图所示，某公司内网部署有一台服务器为外网用户提供服务，同时部署山石网科的WAF和NIPS设备对服务器进行安全防护，最终通过网关连接到互联网。



如下图所示，山石云·界基于SDN+NFV对上述业务场景编排的服务链。编排完成后，访问服务器的请求通过vFW-HA网关后，将继续经过vWAF和vIPS进行检查过滤，最终到达服务器，从而保障服务器的安全性。



预置配置：

在Openstack上部署完成山石云·界虚拟防护墙，具体部署方法请参照附录一。部署完成后，Openstack上须配置以下内容：

- 管理员>系统>镜像：配置有“vfw”云·界镜像，注意与模板中的相应名称一致。
- 管理员>系统>云主机类型：配置有“vfw”云主机类型名称，注意与模板中的相应名称一致。
- 管理员>系统>网络：配置完成上述场景的各个网络。具体网段请根据用户实际规划的IP网段为准，注意与模板中的相应名称一致。

配置步骤：

步骤一：编写vFW-HA模板，编写方法参见HA模板及注释。

步骤二：登录OpenStack，上传vFW-HA模板。

- 选择**NFV>VNF MANAGEMENT>VNF Catalog**，点击“**+Onboard VNF**”,打开**OnBoard VNF**对话框。
- 配置名称为“vfw-ha”，选择VNFD-HA模板文件，点击**OnBoard VNF**按钮。

步骤三：启用VNF。

- 选择**NFV>VNF MANAGEMENT>VNF Manager**，点击“**+ DeployVNF**”,打开**Deploy VNF**对话框。
- 配置VNF Name为“vfw-ha”，VNF Catalog Name选择步骤二配置的模板"vfw-ha"，点击**Deploy VNF**按钮。
- 配置成功后，VNF的状态将显示为ACTIVE。

步骤四：重复步骤一～步骤三，完成vWAF和vIPS的模板和启用。

注意：配置VNF Name分别为“waf”和”ips“，注意与服务链模板中的相应名称一致。

- vWAF模板及注释。
- vIPS模板及注释。

步骤五：编写sfc服务链模板，编写方法参见服务链编排模板及注释。

步骤六：登录OpenStack，上传sfc服务链模板。

- 选择**NFV>NFV ORCHEEATIONSTR>VNFFG Catalog**，点击“**+Onboard VNFFG**”,打开**OnBoard VNFFG**对话框。
- 配置名称为“sfc”，选择sfc模板文件进行上传。

步骤七：启用sfc服务链。

- 选择**NFV>NFV ORCHEEATIONSTR>VNFFG Manager**，点击“**+ Deploy VNFFG**”,打开**Deploy VNFFG**对话框。
- 配置VNF Name为“SFC”，VNF Catalog Name选择步骤二配置的模板"sfc"，点击**Deploy VNFFG**按钮。
- 配置成功后，VNFFG的状态将显示为ACTIVE。

至此完成NFV的配置。

HA模板及注释

tosca_definitions_version: tosca_simple_profile_for_nfv_1_0_0

description: vfw-ha example

metadata:

template_name: sample-vnfd-userdata

topology_template:

node_templates:

VDU1: ***//配置山石云·界虚拟机实例:VDU1。***

type: tosca.nodes.nfv.VDU.Tacker

properties:

image: vfw ***//指定山石云·界镜像名称，与【OpenStack-管理员>系统>镜像】中的镜像“名称”对应，用户须提前配置。***

flavor: vfw ***//指定云主机类型，与【OpenStack-管理员>系统>云主机类型】中的“云主机类型名称”对应，用户须提前配置。***

availability_zone: nova

mgmt_driver: noop

config: |

user_data_format: RAW

user_data: |

#cloud-config ***//山石云·界虚拟机的业务配置起始提示标识，表示从“#cloud-config”开始配置安全业务。本模板从此处开始进行业务的初始配置。***

chpasswd:。

list:

hillstone: Hillstone@123 ***//为hillstone账号初始化密码。***

runcmd: ***//开始配置云·界虚拟防火墙的业务命令。***

- interface ethernet0/0 ***//开始配置接口相关信息，如配置IP地址、安全域等，用户可根据业务需要灵活进行配置。具体配置方法请参考StoneOS的用户手册（点击此处）。***

- no ip address dhcp

- ip address dhcp

- exit

- interface ethernet0/2

- zone trust

- ip address 10.0.2.1/24

- manage ping

- exit

- interface ethernet0/3

- local

- zone untrust

- ip address dhcp setroute

- manage ssh

- manage https
- exit ***//至此完成接口相关配置，如上完成对 ethernet0/1 ~ ethernet0/3的配置。***
- ip vrouter trust-vr ***//开始配置NAT相关信息，具体配置方法请参考StoneOS的用户手册（点击此处）***。
- dnatrule from any to 10.90.3.82/32 service any trans-to 10.0.2.9/32
- snatrule from 10.0.2.0/24 to any service any eif ethernet0/3 trans-to 10.90.3.82/32 mode dynamicport
- exit ***//至此完成NAT相关配置，如上完成目的NAT和源NAT策略的配置。***
- rule from any to any service any permit ***//开始配置安全策略规则。具体配置方法请参考StoneOS的用户手册（点击此处）***
- track track
- interface ethernet0/2 weight 255
- exit ***//至此完成安全策略规则相配置。***
- ha group 0 ***//开始配置HA高可靠性。具体配置方法请参考StoneOS的用户手册（点击此处）***
- priority 50
- preempt 1
- monitor track track
- exit
- ha link interface ethernet0/1
- ha link ip 10.0.1.11/24
- ha cluster 1 node 0
- end ***//至此完成HA高可靠性配置。***

CP11: ***//配置山石云·界虚拟机实例的网卡。***
type: tosca.nodes.nfv.CP.Tacker
properties:
management: true
requirements:
- virtualLink:
node: VL1 ***//指定网卡所属的网络为VL1。关于VL1，下文有相关配置。***
- virtualBinding:
node: VDU1 ***//指定网卡所属虚拟机实例VDU1。***

CP12: ***//配置山石云·界虚拟机实例的第二个网卡。***
type: tosca.nodes.nfv.CP.Tacker
properties:
management: true
ip_address: 10.0.1.11 ***//指定网卡的静态IP。用户可根据实际组网情况配置或修改此IP。***
anti_spoofing_protection: false ***//指定网卡收发报文时，将不被检查接口的IP和MAC。***
requirements:
- virtualLink:
node: VL2
- virtualBinding:
node: VDU1

CP13: ***//配置山石云·界虚拟机实例的第三个网卡。相关注释请参考CP11、CP12。***

type: tosca.nodes.nfv.CP.Tacker

properties:

management: true

ip_address: 10.0.2.11

anti_spoofing_protection: false

requirements:

- virtualLink:

node: VL3

- virtualBinding:

node: VDU1

CP14: ***//配置山石云·界虚拟机实例的第四个网卡。相关注释请参考CP11、CP12。***

type: tosca.nodes.nfv.CP.Tacker

properties:

management: true

ip_address: 10.90.3.83

anti_spoofing_protection: false

requirements:

- virtualLink:

node: VL4

- virtualBinding:

node: VDU1

VDU2: ***//配置山石云·界虚拟机实例:VDU2，相关注释请参考VDU1。***

type: tosca.nodes.nfv.VDU.Tacker

properties:

image: vfw

flavor: vfw

availability_zone: nova

mgmt_driver: noop

config: |

user_data_format: RAW

user_data: |

#cloud-config

chpasswd:

list:

hillstone: Hillstone@123

runcmd:

- interface ethernet0/0

- no ip address dhcp

- ip address dhcp
- exit
- interface ethernet0/3
- local
- zone untrust
- ip address dhcp setroute
- manage ssh
- manage https
- exit
- track track
- interface ethernet0/2 weight 255
- exit
- ha group 0
- priority 100
- preempt 1
- monitor track track
- exit
- ha link interface ethernet0/1
- ha link ip 10.0.1.12/24
- ha cluster 1 node 1
- end

CP21:
type: tosca.nodes.nfv.CP.Tacker
properties:
management: true
requirements:
- virtualLink:
node: VL1
- virtualBinding:
node: VDU2

CP22:
type: tosca.nodes.nfv.CP.Tacker
properties:
management: true
ip_address: 10.0.1.12
anti_spoofing_protection: false
requirements:
- virtualLink:
node: VL2

- virtualBinding:
node: VDU2
CP23:
type: tosca.nodes.nfv.CP.Tacker
properties:
management: true
ip_address: 10.0.2.12
anti_spoofing_protection: false
requirements:
- virtualLink:
node: VL3
- virtualBinding:
node: VDU2
CP24:
type: tosca.nodes.nfv.CP.Tacker
properties:
management: true
ip_address: 10.90.3.84
anti_spoofing_protection: false
requirements:
- virtualLink:
node: VL4
- virtualBinding:
node: VDU2
VDU1 ***//配置山石云·界虚拟机实例:VDU1***。
type: tosca.nodes.nfv.VL
properties:
network_name: vfw-mgt ***//指定网络名称，与【OpenStack-管理员>系统>网络】中的“网络名称”对应，用户须提前配置。***
VL2: ***//配置网络实例VL2。***
type: tosca.nodes.nfv.VL
properties:
network_name: vfw-ha
vendor: Tacker
VL3: ***//配置网络实例VL3。***
type: tosca.nodes.nfv.VL
properties:
network_name: web
vendor: Tacker
VL4: ***//配置网络实例VL4。***

type: tosca.nodes.nfv.VL
properties:
network_name: ext
vendor: Tacker

vWAF模板及注释

tosca_definitions_version: tosca_simple_profile_for_nfv_1_0_0

description: waf example

metadata:

template_name: sample-tosca-vnfd

topology_template:

node_templates:

VDU1 ***//配置山石云·界虚拟机实例:VDU1。***

type: tosca.nodes.nfv.VDU.Tacker

properties:

image: vfw ***//指定山石云·界镜像名称，与【OpenStack-管理员>系统>镜像】中的镜像“名称”对应，用户须提前配置。***

flavor: vfw ***//指定山石云·界镜像虚拟机的云主机类型，与【OpenStack-管理员>系统>云主机类型】中的“云主机类型名称”对应，用户须提前配置。***

availability_zone: nova

mgmt_driver: noop

config: |

user_data_format: RAW

user_data: |

#cloud-config ***//山石云·界虚拟机的业务配置起始提示标识，表示从“#cloud-config”开始配置安全业务。本模板从此处开始进行业务的初始配置。***

chpasswd:

list:

hillstone: Hillstone@123 ***//为hillstone账号初始化密码。***

runcmd: ***//开始配置vWAF虚拟防火墙的业务命令。***

- ips sigset waf_http template http ***//开始配置vWAF虚拟防火墙的IPS Profile，如下开启SQL注入检查并记录日志。具体配置方法请参考StoneOS的用户手册***（点击此处）。

- web-server default

- sql-injection-check enable sensitive low action log-only ***//开启SQL注入检查并记录日志。***

- exit

- exit

- ips profile waf

- sigset waf_http

- exit ***//至此完成IPS Profile-开启SQL注入检查并记录日志的相关配置。***

- av-profile av ***//开始配置vWAF虚拟防火墙的病毒过滤Profile，如下开启对.pe和.rar文件的病毒过滤并记录日志。具体配置方法请参考StoneOS的用户手册***（点击此处）。

- protocol-type http action log-only ***//开启HTTP协议的病毒过滤功能并记录日志。***

- file-type pe ***//开启对.pe文件的病毒过滤。***

- file-type rar ***//开启对.pe文件的病毒过滤。***

- exit ***//至此完成病毒过滤Profile-开启对.pe和.rar文件的病毒过滤并记录日志的相关配置。***
- rule id 1 from any to any service any permit ***//开始配置策略规则。具体配置方法请参考StoneOS的用户手册（点击此处）。***
- rule id 1
- ips waf ***//配置策略规则引用IPS profile。***
- av av ***//配置策略规则引用病毒过滤 profile。***
- exit ***//至此完成策略规则的配置。***
- interface ethernet0/0 ***//开始配置接口相关信息，如配置IP地址、安全域等，用户可根据业务需要灵活进行配置。具体配置方法请参考StoneOS的用户手册（点击此处）***
- no ip address dhcp
- ip address dhcp
- exit
- interface ethernet0/1
- zone trust
- ip address dhcp
- no reverse-route
- exit
- interface ethernet0/2
- zone untrust
- ip address dhcp setroute
- manage https
- exit ***//至此完成接口相关配置，如上完成对 ethernet0/1 ~ ethernet0/2的配置。***
- exec av signature update ***//更新病毒特征库。***
- end

CP11: ***//配置山石云·界虚拟机实例的网卡。***

type: tosca.nodes.nfv.CP.Tacker

properties:

management: true

requirements:

- virtualLink:

node: VL11 ***//指定网卡所属的网络为VL1。关于VL1，下文有相关配置。***

- virtualBinding:

node: VDU1 ***//指定网卡所属虚拟机实例VDU1。***

CP12: ***//配置山石云·界虚拟机实例的第二个网卡。***

type: tosca.nodes.nfv.CP.Tacker

properties:

management: true

anti_spoofing_protection: false ***//指定网卡收发报文时，将不被检查接口的IP和MAC。***

requirements:

- virtualLink:

node: VL12

- virtualBinding:

node: VDU1

CP13: ***//配置山石云·界虚拟机实例的第三个网卡。***

type: tosca.nodes.nfv.CP.Tacker

properties:

management: true

ip_address: 10.90.3.85 ***//指定网卡的静态IP。用户可根据实际组网情况配置或修改此IP。***

requirements:

- virtualLink:

node: VL13

- virtualBinding:

node: VDU1

VL11:***//配置网络实例VL11。***

type: tosca.nodes.nfv.VL

properties:

network_name: vfw-mgt ***//指定网络名称，与【OpenStack-管理员>系统>网络】中的“网络名称”对应，用户须提前配置。***

vendor: Tacker

VL12: ***//配置网络实例VL12。***

type: tosca.nodes.nfv.VL

properties:

network_name: web

vendor: Tacker

VL13: ***//配置网络实例VL13。***

type: tosca.nodes.nfv.VL

properties:

network_name: ext

vendor: Tacker

vIPS模板及注释

tosca_definitions_version: tosca_simple_profile_for_nfv_1_0_0

description: ips example

metadata:

template_name: sample-tosca-vnfd

topology_template:

node_templates:

VDU2: ***//配置山石云·界虚拟机实例:VDU2。***

type: tosca.nodes.nfv.VDU.Tacker

properties:

image: vfw ***//指定山石云·界镜像名称，与【OpenStack-管理员>系统>镜像】中的镜像“名称”对应，用户须提前配置。***

flavor: vfw ***//指定智能云·界镜像虚拟机的云主机类型，与【OpenStack-管理员>系统>云主机类型】中的“云主机类型名称”对应，用户须提前配置。***

availability_zone: nova

mgmt_driver: noop

config: |

user_data_format: RAW

user_data: |

#cloud-config ***//山石云·界虚拟机的业务配置起始提示标识，表示从“#cloud-config”开始配置安全业务。本模板从此处开始进行业务的初始配置。***

chpasswd:

list:

hillstone: Hillstone@123 ***//为hillstone账号初始化密码。***

runcmd: ***//开始配置vIPS虚拟防火墙的业务命令。***

- rule id 1 from any to any service any permit ***//开始配置策略规则。具体配置方法请参考StoneOS的用户手册（点击此处）。***

- rule id 1

- ips predef_loose ***//配置策略规则引用预定义的“predef_loose” IPS profile。***

- exit ***//至此完成策略规则的配置。***

- interface ethernet0/0 ***//开始配置接口相关信息，如配置IP地址、安全域等，用户可根据业务需要灵活进行配置。具体配置方法请参考StoneOS的用户手册（点击此处）***

- no ip address dhcp

- ip address dhcp

- exit

- interface ethernet0/1

- zone trust

- ip address dhcp

- no reverse-route

- exit

- interface ethernet0/2
- zone untrust
- ip address dhcp setroute
- manage https
- exit ***//至此完成接口相关配置，如上完成对 ethernet0/1 ~ ethernet0/2的配置。***
- *exec ips signature update* ***//更新IPS特征库。***
- end

CP21: ***//配置山石云·界虚拟机实例的网卡。***
type: tosca.nodes.nfv.CP.Tacker
properties:
management: true
requirements:
- virtualLink:
node: VL21 ***//指定网卡所属的网络为VL21。关于VL21，下文有相关配置。***
- virtualBinding:
node: VDU2 ***//指定网卡所属虚拟机实例VDU2。***
CP22: ***//配置山石云·界虚拟机实例的第二个网卡。***
type: tosca.nodes.nfv.CP.Tacker
properties:
management: true
anti_spoofing_protection: false ***//指定网卡收发报文时，将不被检查接口的IP和MAC。***
requirements:
- virtualLink:
node: VL22
- virtualBinding:
node: VDU2
CP23: ***//配置山石云·界虚拟机实例的第三个网卡。***
type: tosca.nodes.nfv.CP.Tacker
properties:
management: true
ip_address: 10.90.3.86 ***//指定网卡的静态IP。用户可根据实际组网情况配置或修改此IP。***
requirements:
- virtualLink:
node: VL23
- virtualBinding:
node: VDU2
VL21: ***配置网络实例VL21。***
type: tosca.nodes.nfv.VL
properties:

network_name: vfw-mgt ***//指定网络名称，与【OpenStack-管理员>系统>网络】中的“网络名称”对应，用户须提前配置。***

vendor: Tacker

VL22: ***配置网络实例VL22。***

type: tosca.nodes.nfv.VL

properties:

network_name: web

vendor: Tacker

VL23: ***配置网络实例VL23。***

type: tosca.nodes.nfv.VL

properties:

network_name: ext

vendor: Tacker

服务链编排模板及注释

tosca_definitions_version: tosca_simple_profile_for_nfv_1_0_0

description: Sample VNFFG template

topology_template:

description: Sample VNFFG template

node_templates:

Forwarding_path1: ***//指定服务链路径名称。***

type: tosca.nodes.nfv.FP.Tacker

description: creates path (gateway->waf->ips->server)

properties:

id: 51 ***//配置服务链模板ID号。注意不能与其他服务链模板id相同。***

policy:

type: ACL

criteria:

- network_src_port_id: db945b9f-4e4a-4161-925a-cf6208159001 ***//指定流量入口的端口ID，与【OpenStack-管理员>系统>网络】中的端口“ID”对应，用户须对应入口的IP进行对应查找。***

- destination_port_range: 80-80 ***//指定目的端口的区间范围。***

- ip_proto: 6 ***//指定IP协议号。***

- ip_dst_prefix: 10.0.2.9/32 ***//指定服务链的最终目的地址及网络掩码，如本案例中为服务器的目的NAT地址。***

path: ***//开始配置服务链的路径。***

- forwarder: waf ***//指定服务链的第一跳的VNF实例。注意与【OpenStack-NFV>VNF MANAGEMENT>VNF Manager】中的“VNF Name”对应。***

capability: CP12 ***//指定服务链的第一跳是VNF:waf的第二个网卡。***

- forwarder: ips ***//指定服务链的第二跳的VNF实例。注意与【OpenStack-NFV>VNF MANAGEMENT>VNF Manager】中的“VNF Name”对应。***

capability: CP22 ***//指定服务链的第二跳VNF:ips的第二个网卡。***

groups:

VNFFG1:

type: tosca.groups.nfv.VNFFG

description: ext to server

properties:

vendor: tacker

version: 1.0

number_of_endpoints: 5

dependent_virtual_link: [VL12,VL22] ***//指定服务链经过的两个网络分别为VNF:waf的VL12和VNF:ips的VL22。***

connection_point: [CP12,CP22] ***//指定服务链经过的两跳的网卡分别为VNF:waf的CP12和VNF:ips的CP22。***

constituent_vnfs: [waf,ips] ***//指定VNF实例的名称，注意与【OpenStack-NFV>VNF MANAGEMENT>VNF Manager】中的“VNF Name”对应***

members: [Forwarding_path1] ***//指定服务链的名称***。

附录一 在Openstack上部署CloudEdge

系统要求

在Openstack上部署山石网科的虚拟防火墙，需要宿主机满足以下要求。

- 支持Intel VT 或者 AMD-V
- 至少能够分配2个虚拟网卡
- 64位CPU，CPU能虚拟两个内核
- Linux操作系统（推荐使用Ubuntu 14.04版本）
- 已经安装Openstack（icehouse版本），及其组件Horizon，Nova，Neutron，Glance和Cinder。（Openstack的安装方法按照 http://docs.openstack.org/icehouse/install-guide/install/apt/content/ ）

安装步骤

步骤一：导入镜像文件

1. 输入以下命令，对话框自动打开，选取防火墙的系统文件，将其上传到您的Linux终端的根目录中。
   rz。
2. 输入以下命令，将防火墙系统文件导入到Openstack中作为一个镜像。
   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	将文件导入到Openstack中。
--name=*image-name*	自定义镜像名称。
--property	镜像文件的属性。
hw_vif_model=virtio	限定网卡的类型定义为virtio。
--disk-format=iso	导入文件的格式为iso。
--container-format=bare	指不对镜像做封装。
--is-public=true	对所有租户可见。
vfw_iso	虚拟防火墙系统文件的全名，包括后缀名.iso。

例如，创建名为“image-vfw”的镜像，输入命令：
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
返回结果如下：

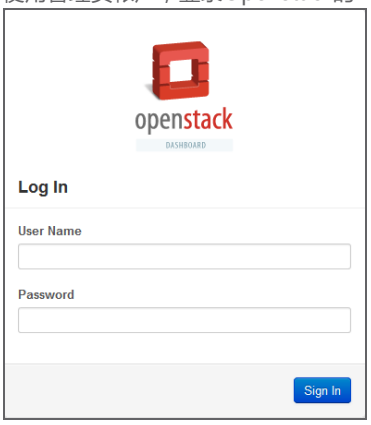
```
+--------------------------+--------------------------------------+
| Property                 | Value                                |
+--------------------------+--------------------------------------+
| Property 'hw_vif_model'  | virtio                               |
| checksum                 | 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                                 |
+--------------------------+--------------------------------------+
```

步骤二：创建云主机类型（Flavor）

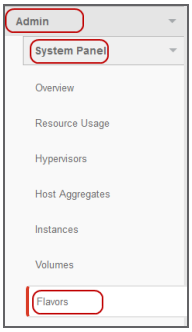
一般情况下，非管理员不能直接修改实例的属性参数（例如内核、内存等信息），只有通过将实例与一个云主机类型（Flavor）绑定，才能继承云主机类型的属性。

使用管理员账户，创建云主机类型：

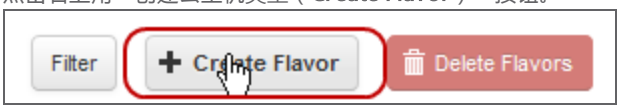
1. 使用管理员帐户，登录Openstack的Web管理界面。



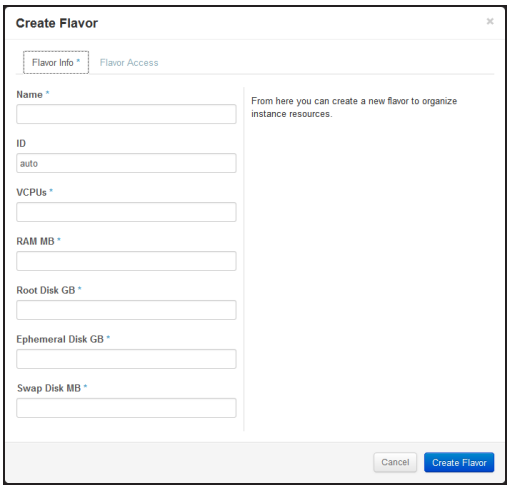
2. 从左侧导航栏选择 “管理员> 系统面板> 云主机类型（**Admin > System Panel > Flavors**）” 。



3. 点击右上角“创建云主机类型（**Create Flavor**）”按钮。



4. 在弹出的<创建云主机类型>对话框，进行设置。



在<云主机类型信息>标签页设置基本信息。

Name	自定义云主机名称。
ID	ID号码由Openstack自动生成。
VCPUs	指定该主机的CPU虚拟内核的数量。对于VM01型号的虚拟防火墙，内核数量指定为1；VM02型号的虚拟防火墙，内核数量为2。
RAM MB	主机的内存大小，单位为MB。对于VM01型号的虚拟防火墙，内存最小值为1024MB；对于VM02，内存最小值为2048MB。
Root Disk	指定根磁盘分区所需容量。单位为GB。建议根磁盘最小值为2 GB。
Ephemeral Disk	临时磁盘大小。单位为GB，使用默认值（0），表示不使用临时磁盘。
Swap Disk	指定交换空间大小。单位为MB，使用默认值（0），不需要使用交换空间。

5. 点击右下角“创建云主机类型（**Create Flavor**）”按钮，完成配置。

步骤三：创建云硬盘

云硬盘用于存储CloudEdge虚拟防火墙的配置文件和许可证。如果不设置云硬盘，虚拟防火墙重启后，防火墙的系统配置将丢失，除非通过配置文件的导入导出功能做过手动备份，否则在没有存储硬盘的情况下，防火墙不能恢复重启前的配置。

虚拟防火墙需要最小为2048 MB的云硬盘作为存储硬盘。

下面步骤介绍如何创建存储硬盘。

1. 创建一个磁盘文件。
   `dd if=/dev/null of=`*`diskname`* **`seek=`***`block_num`* **`bs=`***`bs_size`*

`dd if=/dev/null`	将/dev/null作为初始化文件的设备。
`of=<`*`diskname`*	为磁盘文件命名。
`seek=`*`block_num`*	指定区块数量。

bs=*bs_size*	设定读入/输出的区块的大小。建议设定每一个区块为1M。

例如，创建一个名为“test”的2G磁盘文件：

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

2. 输入以下命令，格式化磁盘文件，使其成为可用的存储硬盘。

mke2fs -t ext4 -qF <*diskname*

mke2fs -t ext4 -qF	将磁盘文件格式化为ext4格式。
diskname	被格式化的磁盘文件的名称，上一步创建的磁盘文件。

例如，将上述的test磁盘文件格式化：

mke2fs -t ext4 -qF <test

3. 将格式化的磁盘作为镜像文件导入到Openstack。

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

glance image-create	在Openstack中创建一个镜像。
--disk-format raw	指定磁盘格式为RAW。
--container-format bare	指定不为磁盘进行封装。
--name *image-name*	
< *diskname*	上一步中的磁盘文件名称。

例如，将上述名为“test”磁盘作为镜像文件导入，作为名为“image1”的镜像：

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

返回的结果如下：

```
+------------------+--------------------------------------+
| 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. 输入以下命令，将镜像文件转换为云硬盘：

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*	创建存储，为存储命名。display-那么为
--image-id $(glance image-list | awk '/*vfw-flash-image***/{print $2}')**	通过glance命令查找到上一步中的磁盘文件对应的ID号码，将该磁盘文件作为云硬盘。
size-num	硬盘的容量大小，默认单位为GB。要求最小值设为2，表示2 GB硬盘。

例如，将上述名为“image1”镜像文件转为容量为2 GB的云硬盘，命名为“volumetest”：

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

步骤四：创建网络

Openstack的网络服务为Openstack云部署提供了可扩展的网络连接服务，通过Openstack的WebUI界面，就可以实现网络的创建和修改。

由于不同用户的组网需求不同，且创建网络属于Openstack的基础操作，本文档不再描述如何创建网络，请参考Openstack的帮助文档中有关创建网络的章节（http://docs.openstack.org/user-guide/content/dashboard_create_networks.html）

步骤五：启动实例

输入以下命令，创建虚拟防火墙。

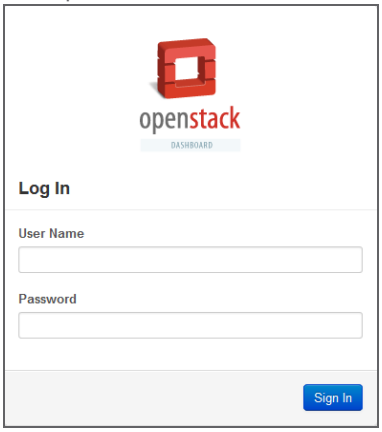
```
nova boot --image image-name --flavor flavor-name --nic net-id=$(neutron net-list | awk '/net1-name/{print $2}') --nic net-id=$(neutron net-list | awk '/net2-name/{print $2}') --nic net-id=$(neutron net-list | awk '/net3-name/{print $2}') --block-device-mapping vdb=$(cinder list | awk '/ volume-name/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

nova boot	启动命令。
--image *image-name*	指定启动防火墙时，要启动的镜像。*image-name*为虚拟防火墙系统文件的镜像名称。
--flavor *flavor-name*	指定云主机类型（flavor）。
--nic net-id=$(neutron net-list | awk '/*net-name***/{print $2}')**	为防火墙连接网络。*net-name*是网络名称。 根据组网规划，重复输入该命令可连接多个网络。
--block-device-mapping vdb=$(cinder list | awk '/ *volume-name***/ {print $2}'):volume::False**	指定云硬盘的名称。
instance-name	自定义实例名称。

访问CloudEdge虚拟防火墙

完成上一步的创建实例后，按照以下步骤访问防火墙：

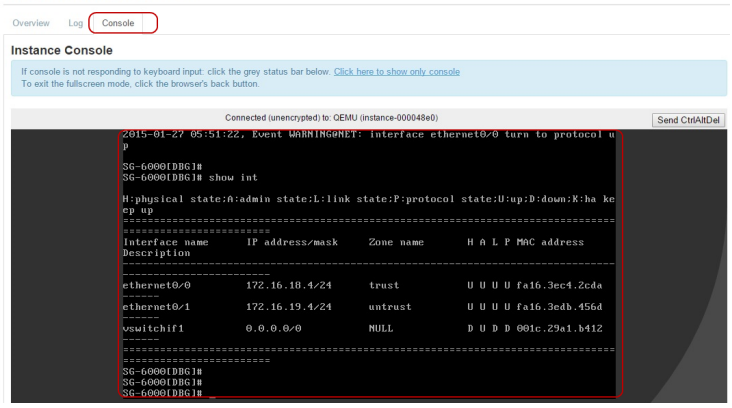
1. 登录Openstack的Web管理界面。



2. 使用以下方法中的一种：
   - 如果您使用普通用户身份登录，从左侧导航栏，选择“项目 > Compute > 实例”。
   - 如果您使用管理员身份登录，从左侧导航栏选择 “管理员> 系统面板> 实例 “。

3. 在列表中，点击虚拟防火墙的名称。

4. 在跳转的界面中，点击“控制台（**Console**）”，即可在嵌入的命令行界面中访问虚拟防火墙。



5. 关于如何操作防火墙，参考StoneOS的用户手册（点击此处）。