Deploying Vyatta vRouter Firewall OpenStack Plugin

This guide describes how to install Vyatta vRouter Firewall OpenStack plugin on Ubuntu 12.0.4 LTS server with OpenStack Icehouse release

BROCADE

OpenStack Server Requirements

Server with Ubuntu 12.04 LTS and KVM

- OpenStack Icehouse installation
- Two network interfaces – For management and external networks
- OpenvSwitch installation

Vyatta vRouter L3 Plugin Installation

Vyatta vRouter firewall plugin uses vRouters configured through L3 plugin. Please follow the setup instructions from L3 plugin deployment guide first.

Vyatta vRouter Firewall Plugin Installation

Vyatta vRouter firewall plugin package file: vyatta_fw_daisy_plugin.tar.gz

- Unpack plugin package file using the command:

```
tar –xvf vyatta_fw_daisy_plugin.tar.gz
```

- Copy plugin files to OpenStack installation using the commands:

```
sudo cp –r ./vyatta_fw_plugin/agents/*
/opt/stack/neutron/neutron/services/firewall/agents/

sudo cp –r ./vyatta_fw_plugin/drivers/*
/opt/stack/neutron/neutron/services/firewall/drivers/

sudo cp ./vyatta_fw_plugin/vyatta-l3-agent /usr/local/bin/
```

- Copy plugin config file to OpenStack installation using the command:

```
sudo cp ./vyatta_fw_plugin/fwaas_driver.ini /etc/neutron/
```

- Configure the Vyatta vRouter firewall plugin in /etc/neutron/neutron.conf file:

```
service_plugins =
neutron.plugins.brocade.vyatta.vrouter_neutron_plugin.VyattaVRouterPlug
in,neutron.services.firewall.fwaas_plugin.FirewallPlugin
```

- Set the below configuration in /etc/neutron/l3_agent.ini file:

```
l3_agent_manager =
neutron.services.firewall.agents.vyatta.vyatta_router.VyattaL3NATAgentW
ithStateReport

external_network_bridge = br-ext

interface_driver = neutron.agent.linux.interface.OVSInterfaceDriver

gateway_external_network_id = <UUID of external network>
```

- Comment the default l3 agent configuration and set the below configuration in stack-screenrc file (in devstack directory):

```
screen -t q-l3 bash

#stuff "cd /opt/stack/neutron && python /usr/local/bin/neutron-l3-agent
--log-file=/opt/stack/logs/devstack/q-l3.log --config-file
/etc/neutron/neutron.conf --config-file=/etc/neutron/l3_agent.ini --
config-file /etc/neutron/fwaas_driver.ini^M"

stuff "cd /opt/stack/neutron && python /usr/local/bin/vyatta-l3-agent -
-log-file=/opt/stack/logs/devstack/q-l3.log --config-file
/etc/neutron/neutron.conf --config-file /etc/neutron/l3_agent.ini --
config-file /etc/neutron/plugins/ml2/ml2_conf.ini --config-file
/etc/neutron/plugins/brocade/vyatta/vrouter.ini --config-file
/etc/neutron/fwaas_driver.ini^M"
```

- Add the below line in localrc file along with other enable_services:

```
enable_service q-fwaas
```

TESTING THE FUNCTIONALITY

Restart Openstack for the configurations to take effect. If you are using devstack, run the following commands:

```
./unstack.sh
sudo ovs-vsctl add-br br-int
./rejoin-stack.sh
sudo service apache2 restart
```

Create firewall policy, rules and firewall using the below commands from devstack directory:

```
source openrc admin admin
neutron firewall-policy-create MyPolicy

# Below rule will block the pings from internal network to external network
neutron firewall-rule-create --name MyRule --protocol icmp --action deny

neutron firewall-policy-insert-rule MyPolicy MyRule
neutron firewall-create --name MyFirewall MyPolicy
```

When a tenant router is created and a router interface is added, Vyatta vRouter firewall plugin will add the firewall rules to the tenant routers.

Only one firewall instance can be created for each tenant. The Firewall can be visualized as having two zones, trusted and untrusted. All the 'internal' interfaces of Neutron router is treated as trusted. The interface connected to 'external network' is treated as untrusted.

The firewall policy is applied on traffic ingressing/egressing interfaces on the trusted zone. This implies that policy will be applied for traffic passing from: trusted to untrusted zones and untrusted to trusted zones.