OpenStack 방화벽 서비스 (FWaaS)

2016 OpenStack Neutron Networking Study
Chapter 8 Firewall Service

Li Guohua
Interdisciplinary Computing Lab.
Department of Advanced Technology Fusion
Konkuk University, Seoul, Korea

2016-05-26

Contents

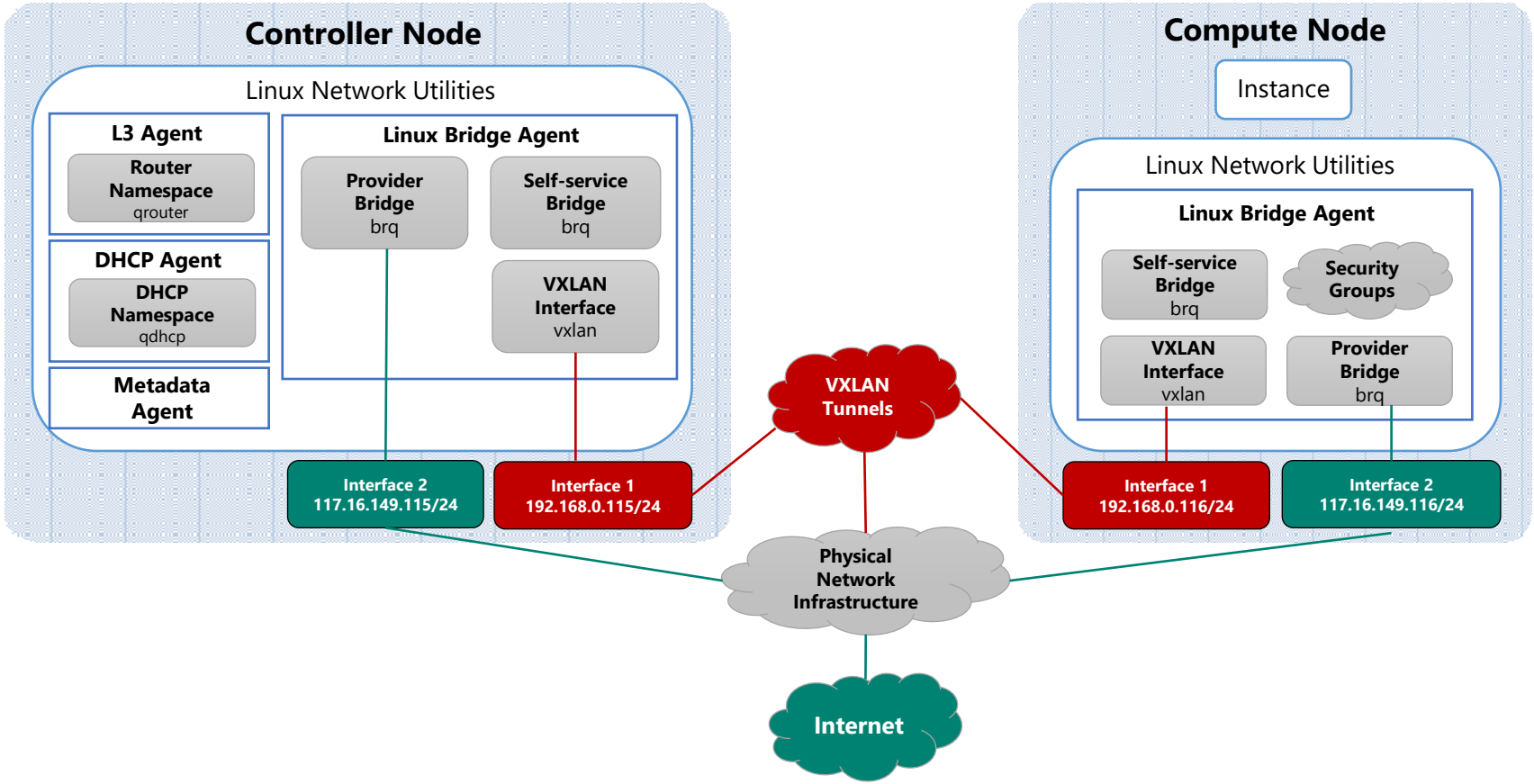
- OpenStack 멀티 노드 테스트베드 구성
- OpenStack Mitaka 설치 이슈
- OpenStack 방화벽 서비스 (FWaaS)
- OpenStack Mitaka with FWaaS 설치 및 설정 이슈

OpenStack Multi-node 테스트베드 구성

테스트베드 구성

Hard/Software Spec	Controller Node	Compute Node
CPU	Intel(R) Core(TM)2 CPU 6320 @ 1.86GHz	Intel(R) Core(TM) i3-2100 CPU @ 3.10GHz
Core	2	4
Memory	4 GB	8 GB
Disk	750 GB	320 GB
OpenStack Mitaka	SQL Database : MariaDB 10.1.12 Message Queue: RabbitMQ Identify Service: memcachd, httpd, Keystone Image Service: Glance Compute Service: Nova Dashboard: Horizon Network Service: Neutron (Neutron-server, Neutron-dhcp-agent, Neutron-l3-agent, Neutron-metadata-agent, Neutron-linuxbridge-agent)	Compute Service: Nova, libvirt Network: Neutron (Neutron-linuxbridge-agent)

Self-Service 네트워크 구성



OpenStack Mitaka 설치 이슈

OpenStack Mitaka Install Issues 1

vi /etc/httpd/conf.d/wsgi-keystone.conf

```
Listen 127.0.0.1:5000
Listen 127.0.0.1:35357

<VirtualHost 127.0.0.1:5000>
    WSGIDaemonProcess keystone-public processes=5 threads=1 user=keystone group=keystone display-name=%{GROUP}
    WSGIProcessGroup keystone-public
    WSGIScriptAlias / /usr/bin/keystone-wsgi-public
    WSGIApplicationGroup %{GLOBAL}
    WSGIPassAuthorization On
    ErrorLogFormat "%{cu}t %M"
    ErrorLog /var/log/httpd/keystone-error.log
    CustomLog /var/log/httpd/keystone-access.log combined

    <Directory /usr/bin>
        Require all granted
    </Directory>
</VirtualHost>

<VirtualHost 127.0.0.1:35357>
    WSGIDaemonProcess keystone-admin processes=5 threads=1 user=keysto
    WSGIProcessGroup keystone-admin
    WSGIScriptAlias / /usr/bin/keystone-wsgi-admin
    WSGIApplicationGroup %{GLOBAL}
    WSGIPassAuthorization On
    ErrorLogFormat "%{cu}t %M"
    ErrorLog /var/log/httpd/keystone-error.log
    CustomLog /var/log/httpd/keystone-access.log combined

    <Directory /usr/bin>
        Require all granted
    </Directory>
</VirtualHost>
```

vi /etc/keystone/keystone.conf

```
# Its value may be silently ignored in the future.
#public_bind_host = 0.0.0.0
public_bind_host = pcontroller
admin_bind_host = controller
# The port number which the public service listens on. (port value)
```

systemctl restart httpd.service
systemctl enable openstack-keystone
systemctl start openstack-keystone

Reference: http://heavenkong.blogspot.kr/2015/08/openstack-kilo-error-openstack-internal.html

OpenStack Mitaka Install Issues 2

OpenStack Server create error HTTP 500 Timeout
(tail -f /var/log/nova/nova-compute.log**)**
Error:
[root@controller ~]# openstack server create --flavor m1.tiny --image cirros --nic net-id=d7eaf8ab-b4aa-4533-89b1-517f2ae2dba4 --security-group default --key-name mykey instance1
Unexpected API Error. Please report this at http://bugs.launchpad.net/nova/ and attach the Nova API log if possible.

Solution:

1. On controller node, add following lines.
vi /etc/nova/nova.conf

```
[DEFAULT]
enabled_apis = osapi_compute,metadata
rpc_backend = rabbit
auth_strategy = keystone
my_ip = 192.168.0.115
use_neutron = True
firewall_driver = nova.virt.firewall.NoopFirewallDriver

network_api_class = nova.network.neutronv2.api.API
security_group_api = neutron
linuxnet_interface_driver = nova.network.linux_net.NeutronLinuxBridgeInterfaceDriver
```

systemctl restart openstack-nova-api

2. On compute node, add two lines.
vi /etc/nova/nova.conf

```
[DEFAULT]
rpc_backend = rabbit
auth_strategy = keystone
my_ip = 192.168.0.116
use_neutron = True
firewall_driver = nova.virt.firewall.NoopFirewallDriver

vif_plugging_is_fatal = False
vif_plugging_timeout = 0
```

systemctl restart openstack-nova-compute

Reference: http://heavenkong.blogspot.kr/2016/04/resolved-mitaka-openstack-server-create.html

OpenStack Mitaka Install Issues 3

Linux Bridge Agent Error out of sync with plugin ! (가상머신이 IP를 할당받지 못하는 경우)

Error:

/var/log/neutron/linuxbridge-agent.log.

INFO **neutron.plugins.ml2.drivers.agent._common_agent** [req-e511876d-fe0c-4def-83ac-a468255d5521 - - - - -] **Linux bridge agent Agent out of sync with plugin!**

2016-04-29 14:13:08.264 27614 INFO neutron.agent.securitygroups_rpc [req-e511876d-fe0c-4def-83ac-a468255d5521 - - - - -] Preparing filters for devices set(['tap5ad39ad4-0d', 'tap026e5c66-46'])

2016-04-29 14:13:08.657 27614 ERROR neutron.plugins.ml2.drivers.agent._common_agent [req-e511876d-fe0c-4def-83ac-a468255d5521 - - - - -] Error in agent loop. Devices info: {'current': set(['tap5ad39ad4-0d', 'tap026e5c66-46']), 'removed': set([]), 'added': set(['tap5ad39ad4-0d', 'tap026e5c66-46']), 'updated': set([])}

... ...

Solution:

On compute node, install ipset, restart neutron-linuxbridge-agent !

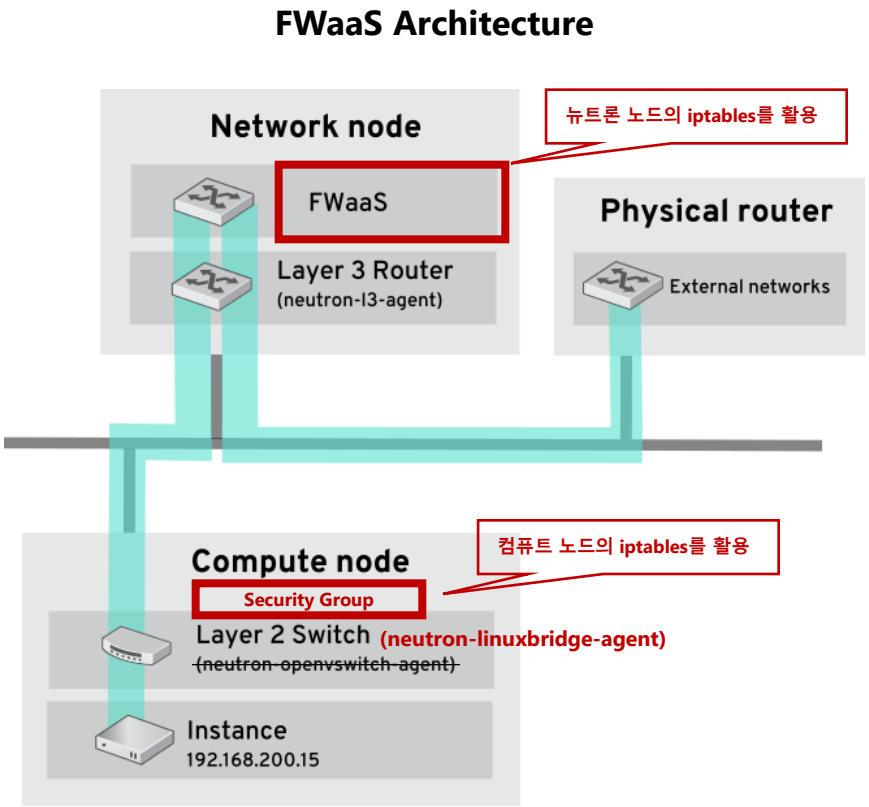
yum install ipset

systemctl restart neutron-linuxbridge-agent

Reference: http://heavenkong.blogspot.kr/2016/04/resolved-mitaka-linux-bridge-agent.html

OpenStack 방화벽 서비스 (FWaaS)

OpenStack 방화벽 서비스 (FWaaS)



FWaaS 는 뉴트론의 확장 기능으로 사용자가 네트워크에 방화벽을 적용할 수 있는 기능을 제공함.

- 뉴트론 라우터에 연결된 테넌트 네트워크로 들어오거나 나가는 트래픽에 대한 방화벽 룰을 적용
- 방화벽 정책을 순서가 정해진 일련의 방화벽 정책 형태로 생성하고 공유
- 방화벽 룰과 정책을 감시(audit)

Reference: https://access.redhat.com/documentation/en/red-hat-enterprise-linux-openstack-platform/7/networking-guide/chapter-16-configure-firewall-as-a-service-fwaas

Neutron에서 FWaaS 드라이버와 플러그인 설정

1. **FWaaS 설치**

   [root@controller ~]# yum install openstack-neutron-fwaas
   [root@controller ~]# yum install python-neutron-fwaas

2. **FWaaS 드라이버 설정**

   [root@controller ~]# vi /etc/neutron/l3_agent.ini
   [fwaas]
   driver = neutron_fwaas.services.firewall.drivers.linux.iptables_fwaas.IptablesFwaasDriver
   enabled = True

   P.S. 드라이버 이름을 모를 경우
   [root@controller ~]# vi /usr/lib/python2.7/site-packages/neutron_fwaas-8.0.0.0b3-py2.7.egg-info/entry_points.txt
   [firewall_drivers]
   neutron.services.firewall.drivers.varmour.varmour_fwaas.vArmourFwaasDriver = neutron_fwaas.services.firewall.drivers.varmour.varmour_fwaas:vArmourFwaasDriver
   neutron.services.firewall.drivers.linux.iptables_fwaas.IptablesFwaasDriver = neutron_fwaas.services.firewall.drivers.linux.iptables_fwaas:IptablesFwaasDriver

Reference: http://heavenkong.blogspot.kr/2016/05/resolved-openstack-mitaka-with-fwaas.html

Neutron에서 FWaaS 드라이버와 플러그인 설정

3. **FWaaS 서비스 플러그인 설정**

root@controller ~]# vi /etc/neutron/neutron.conf
[DEFAULT]
core_plugin = ml2
service_plugins = router, **firewall**
allow_overlapping_ips = True
rpc_backend = rabbit
auth_strategy = keystone

P.S. 플러그인 이름 모를 경우
[root@controller ~]# vi /usr/lib/python2.7/site-packages/neutron-8.0.0.0b4.dev16-py2.7.egg-info/entry_points.txt

[neutron.service_plugins]
firewall = neutron_fwaas.services.firewall.fwaas_plugin:FirewallPlugin
router = neutron.services.l3_router.l3_router_plugin:L3RouterPlugin
… …

4. **neutron-server 와 neutron-l3-agent 서비스 재 시작**
5. **Dashboard 에서 firewall enable 설정** (vi /usr/share/openstack-dashboard/openstack_dashboard/local/local_settings.py)

Reference: http://heavenkong.blogspot.kr/2016/05/resolved-openstack-mitaka-with-fwaas.html

Mitaka with FWaaS 설치 및 설정 이슈

neutron-server 와 neutron-l3-agent restart error!

Error msg:

tail -f /var/log/neutron/server.log

2016-05-25 14:39:04.262 28312 ERROR oslo_messaging.rpc.dispatcher [req-10dfbc37-7e60-4038-bfed-b2504e2e6471 - - - - -] Exception during message handling: (pymysql.err.ProgrammingError) (1146, u"Table 'neutron.firewall_router_associations' doesn't exist") **[SQL: u'SELECT firewall_router_associations.router_id AS firewall_router_associations_router_id \nFROM firewall_router_associations \nWHERE firewall_router_associations.fw_id = %s'] [parameters: (u'2ece652b-5630-49d8-9c04-8af5ce5efa5e',)]**

2016-05-25 14:39:04.262 28312 ERROR oslo_messaging.rpc.dispatcher Traceback (most recent call last):
... ...
2016-05-25 14:39:04.262 28312 TRACE **neutron.api.v2.resource ProgrammingError:**
(ProgrammingError) (1146, "Table 'neutron.firewall_router_associations' doesn't exist**') 'SELECT firewall_router_associations.router_id** AS firewall_router_associations_router_id \nFROM firewall_router_associations \nWHERE firewall_router_associations.router_id IN (%s) AND firewall_router_associations.fw_id IS NOT NULL' ('30d71169-18ff-4c88-8a7b-e0521549c067',)
... ...

Solution:

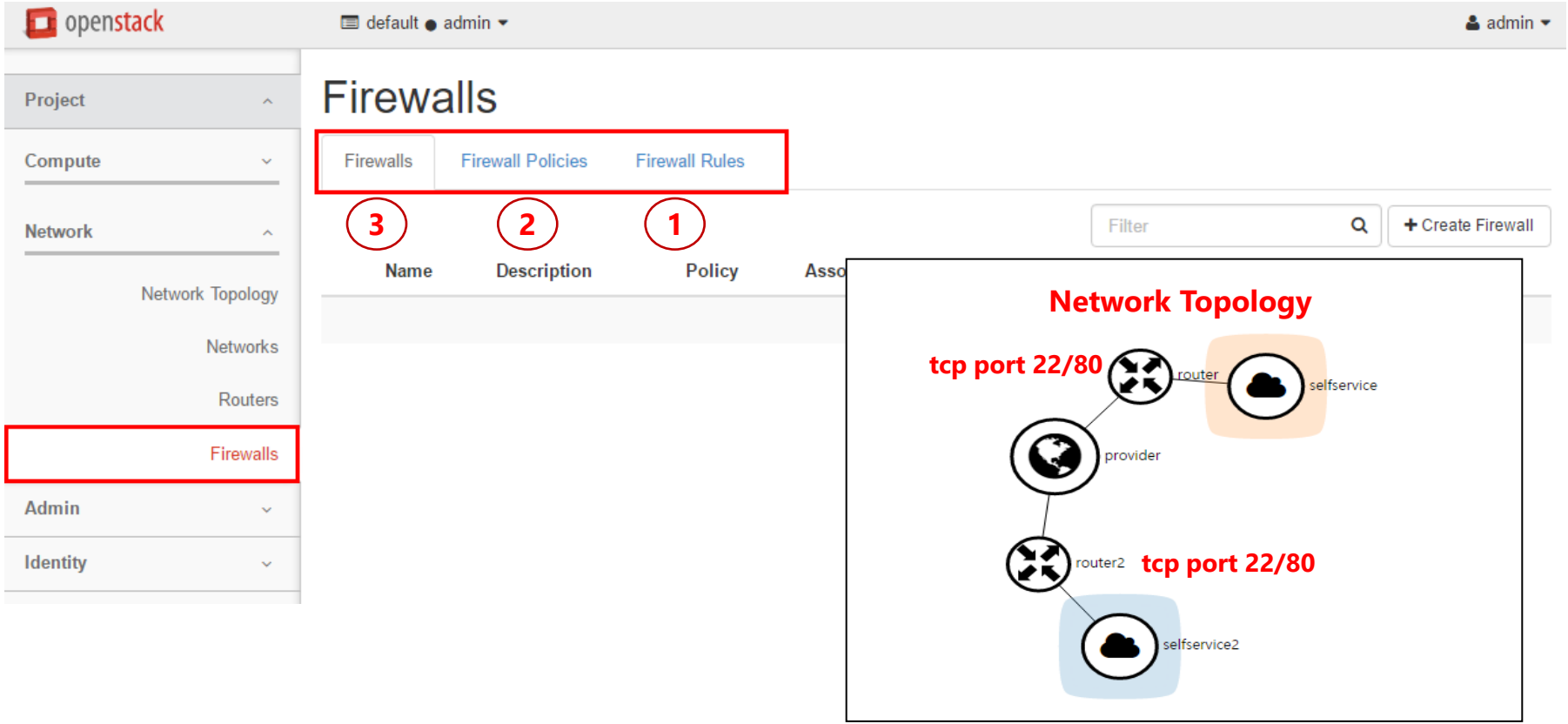
neutron database 업데이트!

[root@controller ~]# neutron-db-manage --config-file /etc/neutron/neutron.conf --config-file /etc/neutron/plugins/ml2/ml2_conf.ini --service fwaas upgrade 540142f314f4

[root@controller ~]# systemctl restart neutron-server neutron-l3-agent

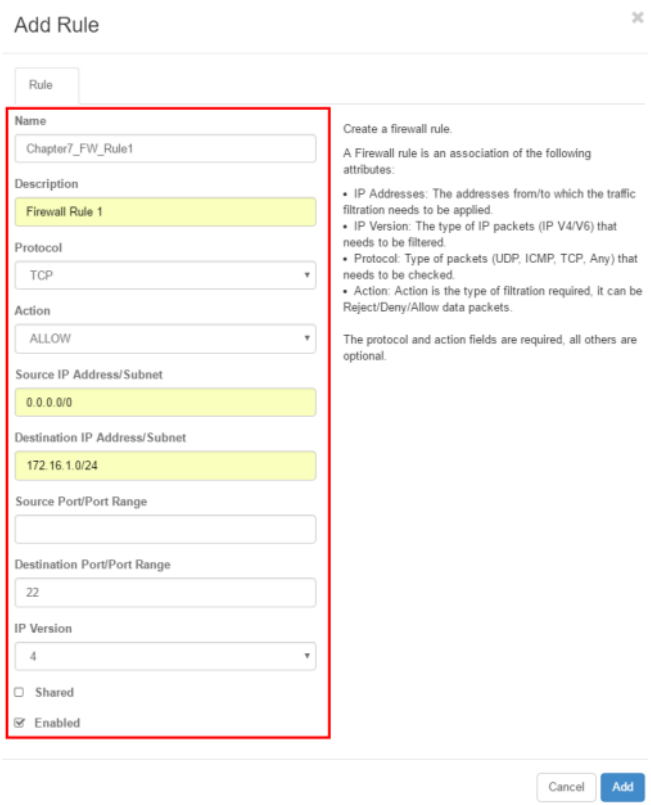
Reference: http://heavenkong.blogspot.kr/2016/05/resolved-openstack-mitaka-with-fwaas.html

Dashboard & CLI Create FWaaS Service



Dashboard & CLI Create FWaaS Service

1 Create Rule



[root@controller ~]# neutron firewall-rule-create --name Chapter7_FW_Rule2 --description "Chapter 7 Rule 2" --source-ip-address 0.0.0.0/0 --destination-ip-address 10.10.10.0/24 --destination-port 22 --protocol tcp --action allow

```
Created a new firewall_rule:
+--------------------------+--------------------------------------+
| Field                    | Value                                |
+--------------------------+--------------------------------------+
| action                   | allow                                |
| description              | Chapter 7 Rule 2                     |
| destination_ip_address   | 10.10.10.0/24                        |
| destination_port         | 22                                   |
| enabled                  | True                                 |
| firewall_policy_id       |                                      |
| id                       | 0f0b28e4-aa1f-47ee-bc30-6317155fb520 |
| ip_version               | 4                                    |
| name                     | Chapter7_FW_Rule2                    |
| position                 |                                      |
| protocol                 | tcp                                  |
| shared                   | False                                |
| source_ip_address        | 0.0.0.0/0                            |
| source_port              |                                      |
| tenant_id                | caa5f23035d7419189810c91e3c17e2c     |
+--------------------------+--------------------------------------+
[root@controller ~]#
```

Rule Command:

firewall-rule-create

firewall-rule-delete

firewall-rule-list

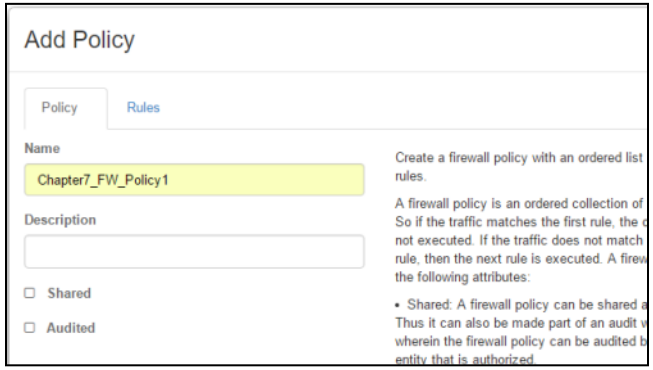
firewall-rule-show

firewall-rule-update

```
[root@controller ~]# neutron firewall-rule-list
+--------------------------------------+------------------+--------------------+-----------------------------+---------+
| id                                   | name             | firewall_policy_id | summary                     | enabled |
+--------------------------------------+------------------+--------------------+-----------------------------+---------+
| 0f0b28e4-aa1f-47ee-bc30-6317155fb520 | Chapter7_FW_Rule2 |                    | TCP,                        | True    |
|                                      |                  |                    |  source: 0.0.0.0/0(none),   |         |
|                                      |                  |                    |  dest: 10.10.10.0/24(22),   |         |
|                                      |                  |                    |  allow                      |         |
| c01011b8-96c7-457d-a2ba-a5f7768bdb3d | Chapter7_FW_Rule1 |                    | TCP,                        | True    |
|                                      |                  |                    |  source: 0.0.0.0/0(none),   |         |
|                                      |                  |                    |  dest: 172.16.1.0/24(22),   |         |
|                                      |                  |                    |  allow                      |         |
+--------------------------------------+------------------+--------------------+-----------------------------+---------+
```

Dashboard & CLI Create FWaaS Service

2 Create Policy (Grouping Rules)



[root@controller ~]# neutron firewall-policy-create --firewall-rules "Chapter7_FW_Rule2 Chapter7_FW_Rule4" --description "Chapter7 Firewall Policy 2" Chapter7_FW_Policy2

```
Created a new firewall_policy:
+----------------+--------------------------------------+
| Field          | Value                                |
+----------------+--------------------------------------+
| audited        | False                                |
| description    | Chapter7 Firewall Policy 2           |
| firewall_rules | 0f0b28e4-aa1f-47ee-bc30-6317155fb520 |
|                | 0bafbdfd-6431-4c30-a6f7-f45db94770fb |
| id             | 7baa4448-5047-4f40-9a47-34da8ad19ea4 |
| name           | Chapter7_FW_Policy2                  |
| shared         | False                                |
| tenant_id      | caa5f23035d7419189810c91e3c17e2c     |
+----------------+--------------------------------------+
```

Policy Command:

firewall-policy-create

firewall-policy-delete

firewall-policy-list

firewall-policy-insert-rule

firewall-policy-remove-rule

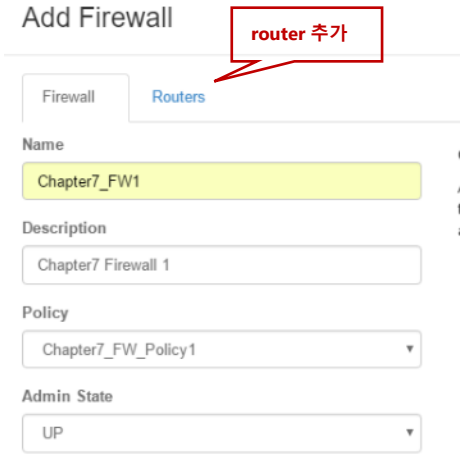
firewall-policy-show

firewall-policy-update

```
[root@controller ~]# neutron firewall-policy-list
+--------------------------------------+--------------------+--------------------------------------+
| id                                   | name               | firewall_rules                       |
+--------------------------------------+--------------------+--------------------------------------+
| 7baa4448-5047-4f40-9a47-34da8ad19ea4 | Chapter7_FW_Policy2 | [0f0b28e4-aa1f-47ee-bc30-6317155fb520, |
|                                      |                    |  0bafbdfd-6431-4c30-a6f7-f45db94770fb] |
| eb45293a-8a30-438e-bacb-b5857d8f332e | Chapter7_FW_Policy1 | [d9df7ef5-7c3f-4df9-851e-8f60bc9ee3d1, |
|                                      |                    |  b6117541-199b-434b-a17e-85dd24b89ee2] |
+--------------------------------------+--------------------+--------------------------------------+
```

Dashboard & CLI Create FWaaS Service

3 **Create Firewall**



[root@controller ~]# neutron firewall-create --name Chapter7_FW2 --router router2 --description "Chapter7 Firewall 2" Chapter7_FW_Policy2

```
Created a new firewall:
+--------------------+--------------------------------------+
| Field              | Value                                |
+--------------------+--------------------------------------+
| admin_state_up     | True                                 |
| description        | Chapter7 Firewall 2                  |
| firewall_policy_id | 7baa4448-5047-4f40-9a47-34da8ad19ea4 |
| id                 | 9625a31e-93ce-4190-8ff3-a70ad62188b7 |
| name               | Chapter7_FW2                         |
| router_ids         | fe3cad2c-3f00-41f8-84c0-69b4c86c067e |
| status             | PENDING_CREATE                       |
| tenant_id          | caa5f23035d7419189810c91e3c17e2c     |
+--------------------+--------------------------------------+
```

Firewall Command:

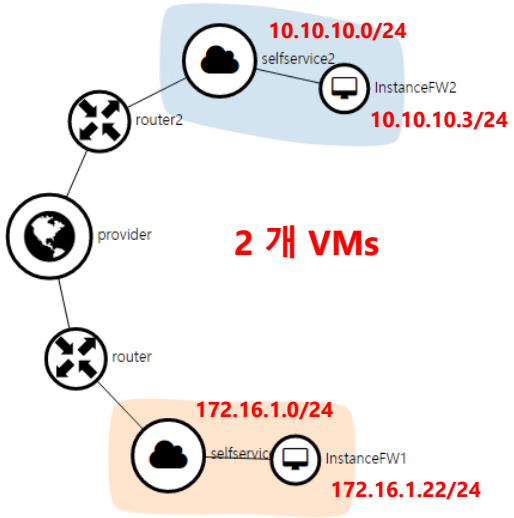
firewall-create

firewall-delete

firewall-list

```
[root@controller ~]# neutron firewall-list
+--------------------------------------+--------------+--------------------------------------+
| id                                   | name         | firewall_policy_id                   |
+--------------------------------------+--------------+--------------------------------------+
| 9625a31e-93ce-4190-8ff3-a70ad62188b7 | Chapter7_FW2 | 7baa4448-5047-4f40-9a47-34da8ad19ea4 |
| def58c7a-bce4-4e05-9180-a39a6cbd8621 | Chapter7_FW1 | eb45293a-8a30-438e-bacb-b5857d8f332e |
+--------------------------------------+--------------+--------------------------------------+
```

Verify FWaaS Service



[root@controller ~]# ip netns
qrouter-fe3cad2c-3f00-41f8-84c0-69b4c86c067e (id: 5)
qdhcp-9656fd6e-71dc-48d7-8dde-cf7390a52ec1 (id: 4)
qrouter-99bc40fa-cfbf-4eea-aa2e-70cbfb2de916 (id: 3)
qdhcp-7893bedf-c7b1-41f1-979f-c46baae0943b (id: 1)
qdhcp-7ce7d700-92e9-40c6-a699-2737a9d0e276 (id: 0)

[root@controller ~]# ip netns exec qrouter-99bc40fa-cfbf-4eea-aa2e-70cbfb2de916 bash
[root@controller ~]# **iptables -L -n -v**

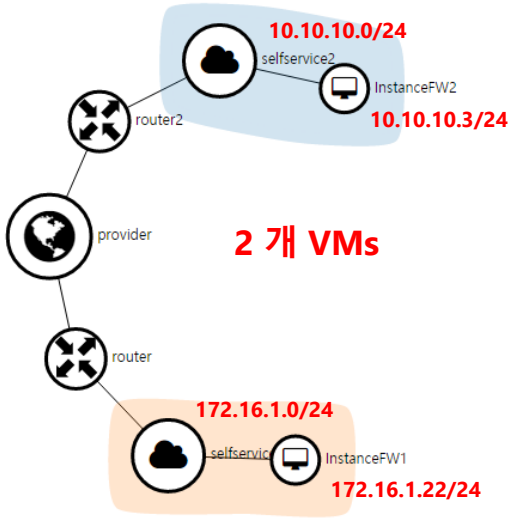
```
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
   14  1150 neutron-filter-top  all  --  *      *       0.0.0.0/0            0.0.0.0/0
   14  1150 neutron-l3-agent-FORWARD  all  --  *      *       0.0.0.0/0            0.0.0.0/0
```

```
Chain neutron-l3-agent-FORWARD (1 references)
 pkts bytes target     prot opt in     out     source               destination
   14  1150 neutron-l3-agent-scope  all  --  *      *       0.0.0.0/0            0.0.0.0/0
    0     0 neutron-l3-agent-iv4def58c7a  all  --  *      qr-+    0.0.0.0/0            0.0.0.0/0
   14  1150 neutron-l3-agent-ov4def58c7a  all  --  qr-+   *       0.0.0.0/0            0.0.0.0/0
    0     0 neutron-l3-agent-fwaas-defau  all  --  *      qr-+    0.0.0.0/0            0.0.0.0/0
   14  1150 neutron-l3-agent-fwaas-defau  all  --  qr-+   *       0.0.0.0/0            0.0.0.0/0
```

```
Chain neutron-l3-agent-iv4def58c7a (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0            state INVALID
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            172.16.1.0/24        tcp dpt:22
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            172.16.1.0/24        tcp dpt:80
```

```
Chain neutron-l3-agent-ov4def58c7a (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0            state INVALID
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0            state RELATED,ESTABLISHED
    0     0 ACCEPT     icmp --  *      *       0.0.0.0/0            0.0.0.0/0
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            172.16.1.0/24        tcp dpt:22
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            172.16.1.0/24        tcp dpt:80
```

Verify FWaaS Service



[root@controller ~]# ip netns
qrouter-fe3cad2c-3f00-41f8-84c0-69b4c86c067e (id: 5)
qdhcp-9656fd6e-71dc-48d7-8dde-cf7390a52ec1 (id: 4)
qrouter-99bc40fa-cfbf-4eea-aa2e-70cbfb2de916 (id: 3)
qdhcp-7893bedf-c7b1-41f1-979f-c46baae0943b (id: 1)
qdhcp-7ce7d700-92e9-40c6-a699-2737a9d0e276 (id: 0)

[root@controller ~]# ip netns exec qrouter-fe3cad2c-3f00-41f8-84c0-69b4c86c067e bash
[root@controller ~]# **iptables -L -n -v**

```
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
 pkts bytes target     prot opt in     out     source               destination
    1   294 neutron-filter-top  all  --  *      *       0.0.0.0/0            0.0.0.0/0
    1   294 neutron-l3-agent-FORWARD  all  --  *      *       0.0.0.0/0            0.0.0.0/0
```

```
Chain neutron-l3-agent-FORWARD (1 references)
 pkts bytes target     prot opt in     out     source               destination
    1   294 neutron-l3-agent-scope  all  --  *      *       0.0.0.0/0            0.0.0.0/0
    0     0 neutron-l3-agent-iv49625a31e  all  --  *      qr-+    0.0.0.0/0            0.0.0.0/0
    0     0 neutron-l3-agent-ov49625a31e  all  --  qr-+   *       0.0.0.0/0            0.0.0.0/0
    0     0 neutron-l3-agent-fwaas-defau  all  --  *      qr-+    0.0.0.0/0            0.0.0.0/0
    0     0 neutron-l3-agent-fwaas-defau  all  --  qr-+   *       0.0.0.0/0            0.0.0.0/0
```

```
Chain neutron-l3-agent-iv49625a31e (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0           state INVALID
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            10.10.10.0/24       tcp dpt:22
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            10.10.10.0/24       tcp dpt:80
```

```
Chain neutron-l3-agent-ov49625a31e (1 references)
 pkts bytes target     prot opt in     out     source               destination
    0     0 DROP       all  --  *      *       0.0.0.0/0            0.0.0.0/0           state INVALID
    0     0 ACCEPT     all  --  *      *       0.0.0.0/0            0.0.0.0/0           state RELATED,ESTABLISHED
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            10.10.10.0/24       tcp dpt:22
    0     0 ACCEPT     tcp  --  *      *       0.0.0.0/0            10.10.10.0/24       tcp dpt:80
```


Thank You