Security Group Logging

Networking logging tool for ml2/OVN

Elvira García Ruiz

In this presentation….

Security Group Logging

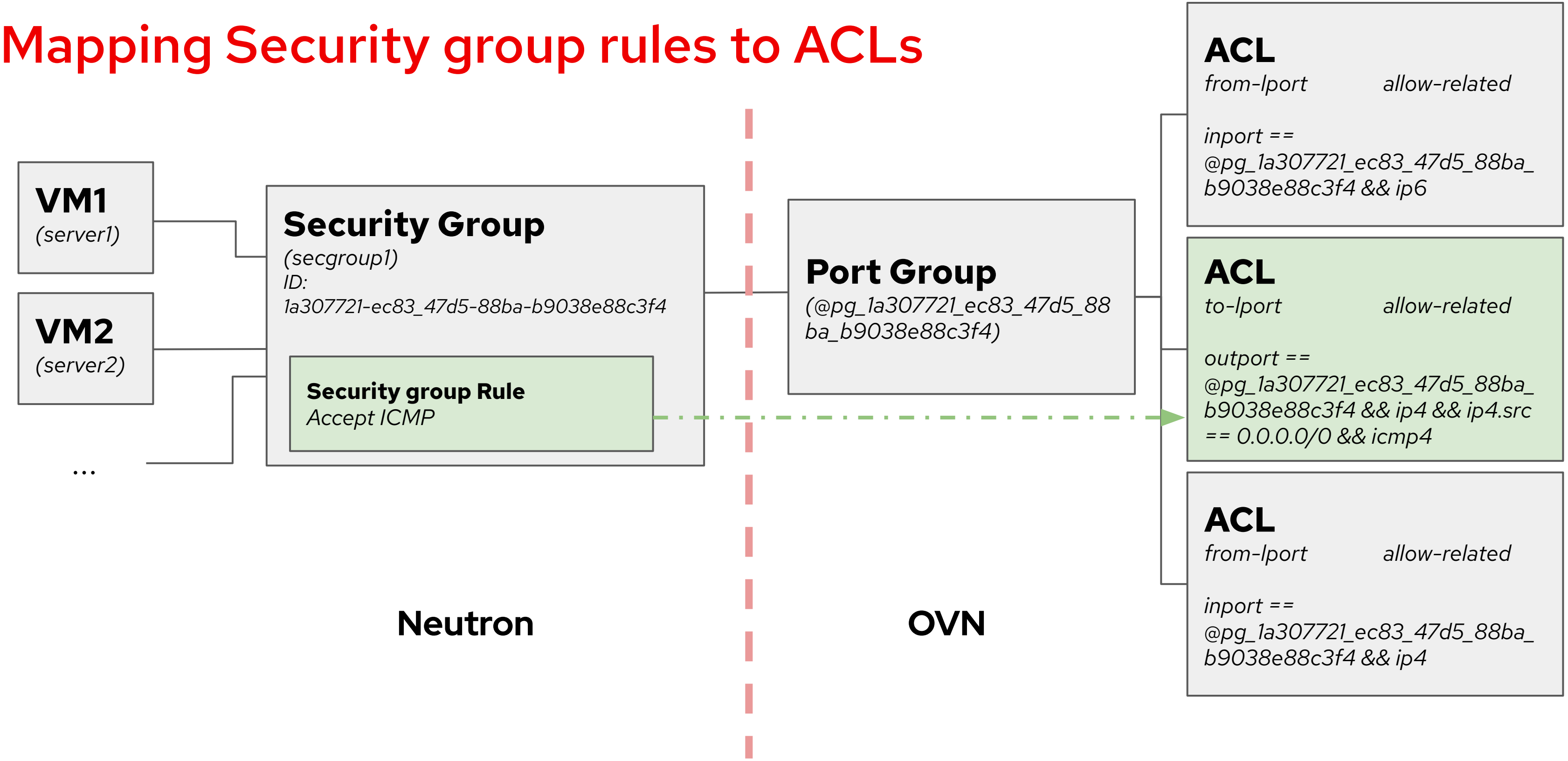
1. Security groups in ml2/OVN
2. What is Security Group Logging?
3. How-to
4. Finding our logs
5. Demo
6. Known limitations

What is a Security Group?

“Collection of network access rules that are used to limit the types of traffic that have access to instances.”

- Neutron denies all traffic incoming and outcoming from ports.
- In ml2/OVN, we control this using OVN Port Groups and Access Control Lists.

Mapping Security group rules to ACLs


VM1
(server1)
VM2
(server2)
...
Security Group
(secgroup1)
ID:
1a307721-ec83_47d5-88ba-b9038e88c3f4
Security group Rule
Accept ICMP
Port Group
(@pg_1a307721_ec83_47d5_88ba_b9038e88c3f4)
ACL
from-lport *allow-related*
inport == @pg_1a307721_ec83_47d5_88ba_b9038e88c3f4 && ip6
ACL
to-lport *allow-related*
outport == @pg_1a307721_ec83_47d5_88ba_b9038e88c3f4 && ip4 && ip4.src == 0.0.0.0/0 && icmp4
ACL
from-lport *allow-related*
inport == @pg_1a307721_ec83_47d5_88ba_b9038e88c3f4 && ip4
Neutron
OVN

Note: Neutron networking is firewalled as a blacklist. This means that by default no traffic will be allowed inside a VM, unless we say otherwise

What does logging have to do with Security Groups?

- Monitoring of networking packets.
- Of packets flowing through ports associated to one or several security groups.
- For stateful and stateless security groups.

Network Logging in ACLs

OVN Northbound DB Access Control List entry:

```
_uuid                  : b910b0d3-d6df-435b-aed5-443d3cf1f8f9
action                 : allow-related
direction              : to-lport
external_ids           : {"neutron:security_group_rule_id"="ae4fb91a-0940-4a51-879e-e0a1067a01ba"}
label                  : 0
log                    : true
match                  : "outport == @pg_1a307721_ec83_47d5_88ba_b9038e88c3f4 && ip4 && ip4.src == 0.0.0.0/0 && icmp4"
meter                  : acl_log_meter
name                   : neutron-e9ebf19c-3d84-49ae-a81e-7a01035a8768  # ID of the SG logging object
options                : {}
priority               : 1002
severity               : info
```

How to set it up

1. If not present, add the **log** plugin to *neutron.conf* in the neutron container in the controller nodes.
    - Remember to restart the network container if you had to change this!

```
[DEFAULT]
...
service_plugins=qos,ovn-router,...,log
...
```

2. Create a network log object with **ACCEPT**, **DROP** or **ALL**
    - You can associate a security group using the `--resource` parameter, if not used it will applied to all security groups.

```
(overcloud) $ openstack network log create --event ACCEPT \
                  --resource-type security_group \
                  --resource secgroup1 netlog_sg1_accept
```

Note: It is not needed to enter the containers of a node to change their neutron.conf. You can make changes in the file located at /var/lib/config-data/puppet-generated/neutron/etc/neutron/neutron.conf and the changes made there will sync with the container neutron.conf after a restart.

How to set it up

3. It is possible to set parameters in *ml2_conf.ini* to tune how we want to log the packets.

```
...
[network_log]
rate_limit=120
burst_limit=30
```

- **Rate limit -** Limit the packet rate of the logs that are sent to the OVN controller. (packets per second)
- **Burst limit -** Increase the packet rate limit by the specified value for a short period of time.

These parameters can be changed using heat templates:

```
NeutronOVNLoggingRateLimit
NeutronOVNLoggingBurstLimit
NeutronOVNLoggingLocalOutputLogBase
```

Finding our logs

- The logs are located at every *ovn-controller.log*

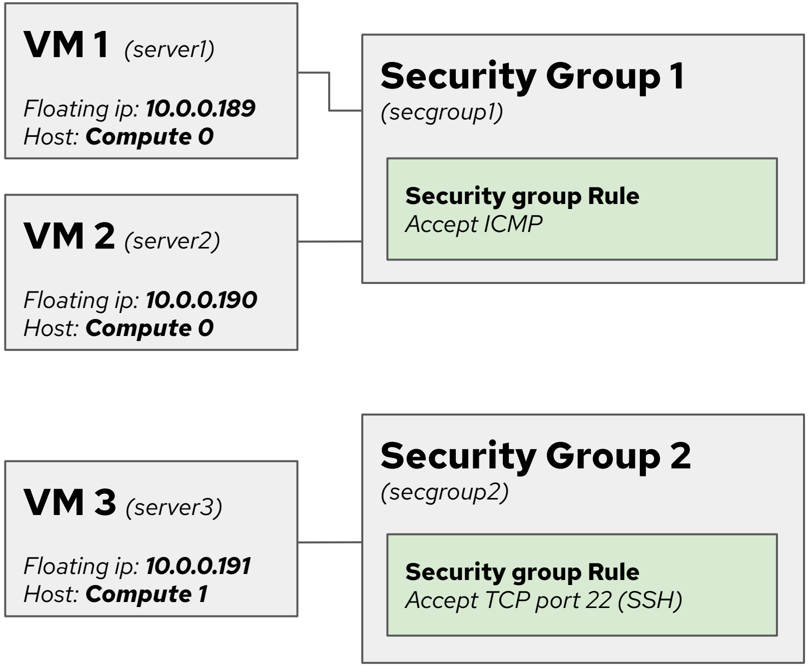
- The logs are **distributed** among the compute nodes. This is because every OVN controller has only the ability to examine packets within the node it is located in.

- Example of a packet logged:
  - Name: `neutron-<security group log object ID>`
  - Verdict, severity and direction for the OVN Controller
  - Packet content

```
2023-01-08T17:57:28.283002425+00:00 stderr F
2023-01-08T17:57:28Z|00094|acl_log(ovn_pinctrl0)|INFO|name="neutron-e9ebf19c-3d84-49ae-a81e-7a01035a8768",
verdict=allow, severity=info, direction=to-lport: icmp, vlan_tci=0x0000, dl_src=fa:16:3e:d3:b4:48,
dl_dst=fa:16:3e:9a:d9:7d, nw_src=10.0.0.67, nw_dst=192.168.100.11, nw_tos=0, nw_ecn=0, nw_ttl=63,
nw_frag=no, icmp_type=8, icmp_code=0
```

Note: If you want to quickly check in which compute node your VMs are located you can use `$ openstack server list --long`
Note 2: Full path to ovn_controller.log in OSP17: `/var/log/containers/stdouts/ovn_controller.log`

Demo



VM 1 *(server1)*

Floating ip: ***10.0.0.189***
Host: ***Compute 0***

VM 2 *(server2)*

Floating ip: ***10.0.0.190***
Host: ***Compute 0***

VM 3 *(server3)*

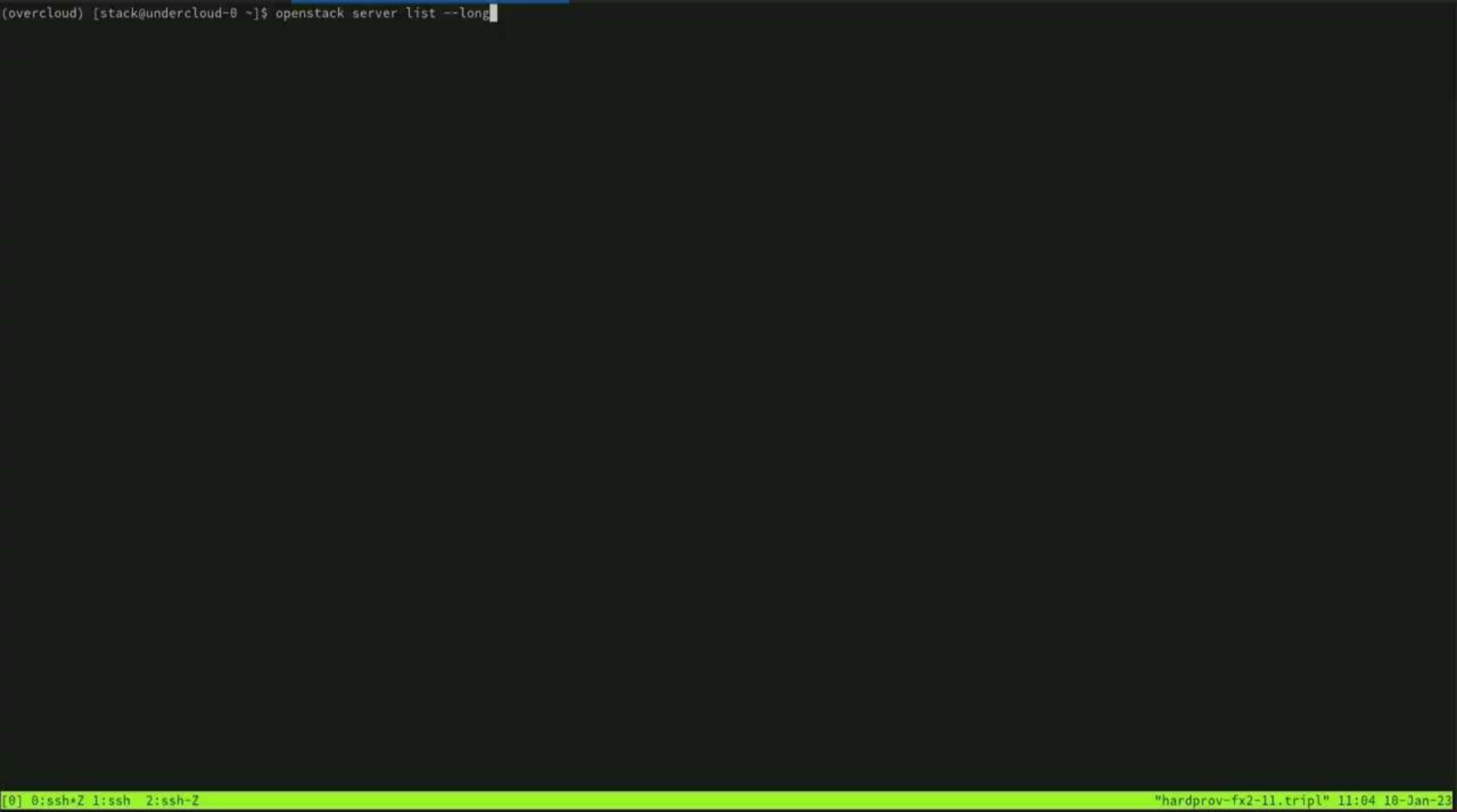
Floating ip: ***10.0.0.191***
Host: ***Compute 1***

Security Group 1
(secgroup1)

Security group Rule
Accept ICMP

Security Group 2
(secgroup2)

Security group Rule
Accept TCP port 22 (SSH)



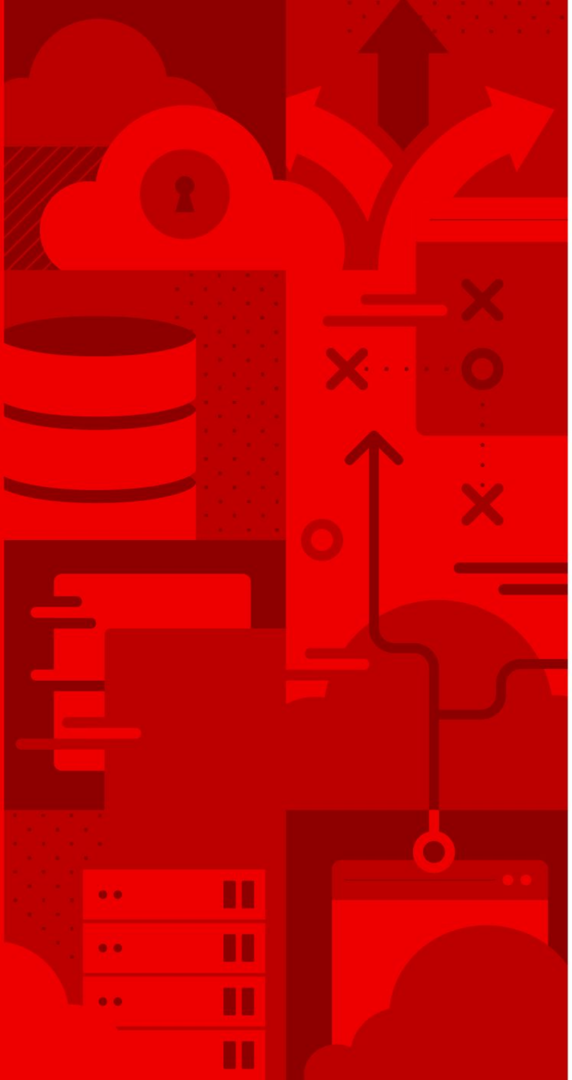
```
(overcloud) [stack@undercloud-0 ~]$ openstack server list --long
```

```
[0] 0:ssh*Z 1:ssh  2:ssh-Z                                                    "hardprov-fx2-11.tripl" 11:04 10-Jan-23
```

Known limitations

- **Logs are distributed.** It is up to the user to decide how to manage and process these logs.
- Using the limit_rate parameter can result in not logging desired packages from certain VMs if there is a noisy neighbour
- **If we choose to log dropped traffic, we will log dropped traffic for every security group** as of today. This will be reflected in the documentation. The reason if this is how security groups are designed. It is not possible to log dropped traffic of only certain security groups because there is not an individual ACL per security group, but a general ACL called *neutron_pg_drop*.

  New ways of implementing security groups are being studied: https://review.opendev.org/c/openstack/neutron/+/839066



Thank you!

linkedin.com/company/red-hat

facebook.com/redhatinc

youtube.com/user/RedHatVideos

twitter.com/RedHat

Red Hat