OpenStack Study 발표

Chapter 6. Managing Security Groups

Topics

- A brief introduction to iptables
- Creating and managing security groups
- Demonstrating how security groups leverage iptables
- Disabling port security

Security groups in OpenStack

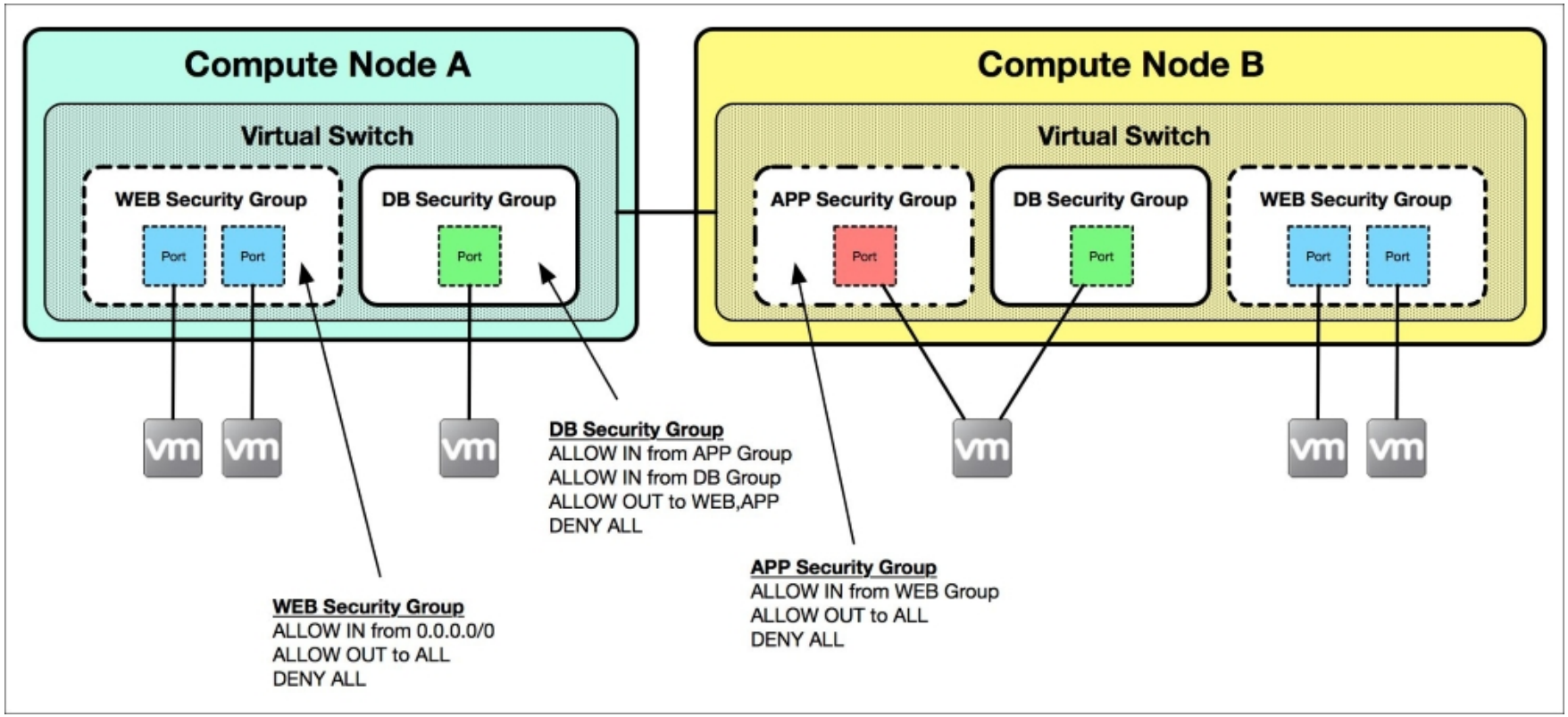
- Security group이란?
  - Instance가 주고 받을 수 있는 트래픽의 종류를 제한하는 network access rule의 모음
  - 레퍼런스 아키텍트에서, security group rule은 compute node가 호스팅하는 instance에 iptables 로 변환되어 적용됨
  - 각각의 tenant는 tenant내에서만 사용자가 수정할 수 있는 default security group 제공
  - Neutron은 security group rule을 생성, 수정, 적용, 삭제를 할수 있는 API 제공

Security groups in OpenStack

- Instance에 security group을 적용하는 여러 방법이 있음
  - (예제) 비슷한 기능이나 역할의 instance를 하나의 security group으로 놓을 수 있음
  - Security group은 IPv4, IPv6 호스트, 네트워트에 Security group자기 자신만큼 참조할 수 있음
  - 특정 호스트, 네트워크 보다는 특정 security group의 rule만 참조할 수 있어, 사용자가 개별 주소를 별도로 지정하지 않아도 됨
  - Neutron은 DB 정보를 기반으로 호스트에 자동으로 filtering rule을 적용

Security groups in OpenStack

- 아래의 그림과 같이, compute node에 Virtual Switch port별로 security group을 적용할 수 있음.

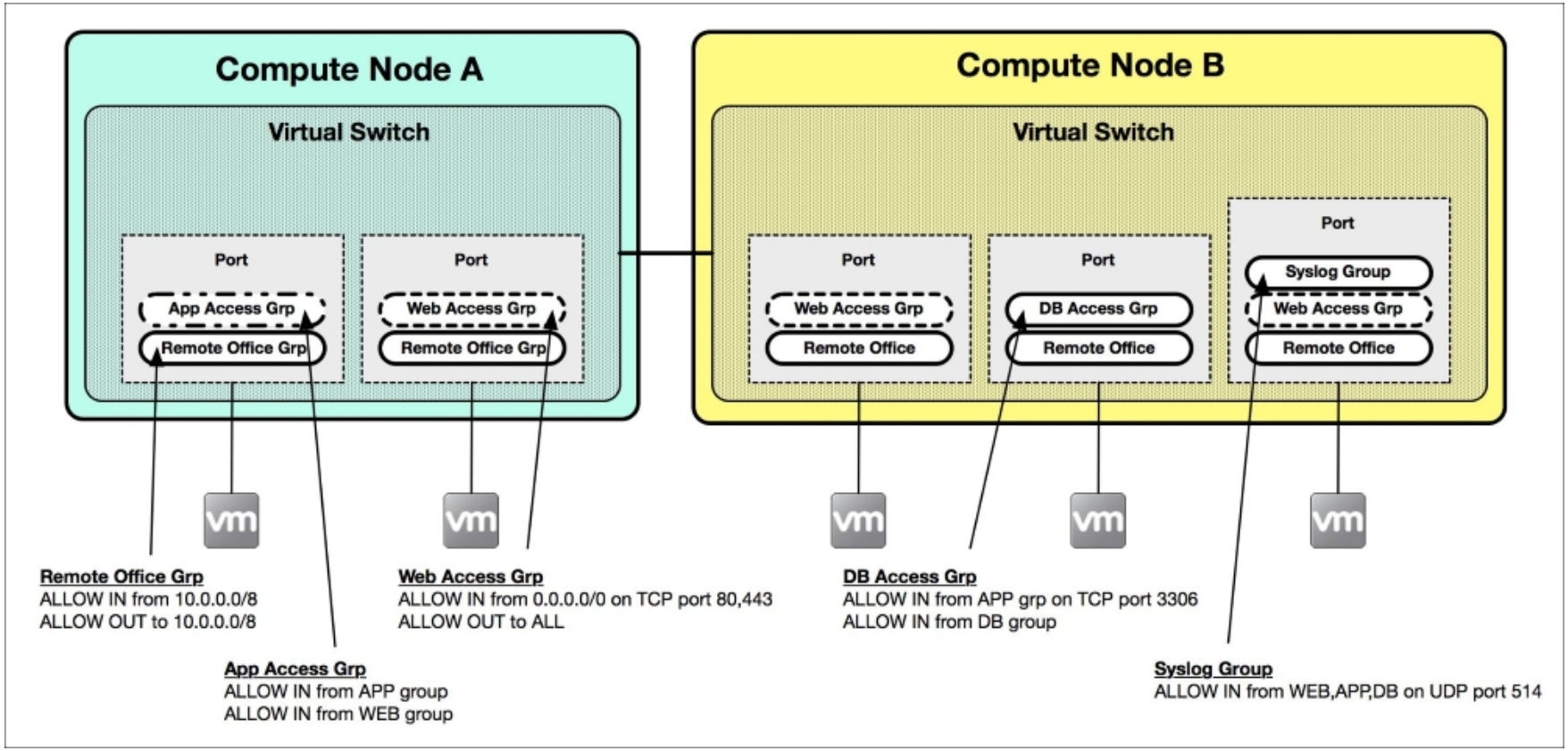


Security groups in OpenStack

- 위의 구성도에서 Virtual Switch에는 3개의 Security Group(WEB, DB, APP)이 설정
- Security Group의 rule 변경이 생기면, compute node에 해당되는 iptables rule이 자동으로 변경
- 사용자는 특정 instance port에 적용될 security group을 지정(정의) 할수 있음.

Security groups in OpenStack

- 포트마다 접속이 허용되는 traffic을 분류하는 security goup의 사용 예



Security groups in OpenStack

- Neutron이 포트 생성하면, security group을 설정하지 않으면, default security group 적용
- Default security group은 instance로 유입되는 ingress traffic 차단(drop), 외부접속 egress traffic은 허용(allow)
- 참고로, standard rule은 모든 instance에 IP, DHCP, MAC Address spoofing에 대해서 금지
- Security gruop이 Neutron포트에 적용되면, Neutron은 security group rule이 대응되는 compute node에서 호스팅하는 instance에 iptable rule로 변환

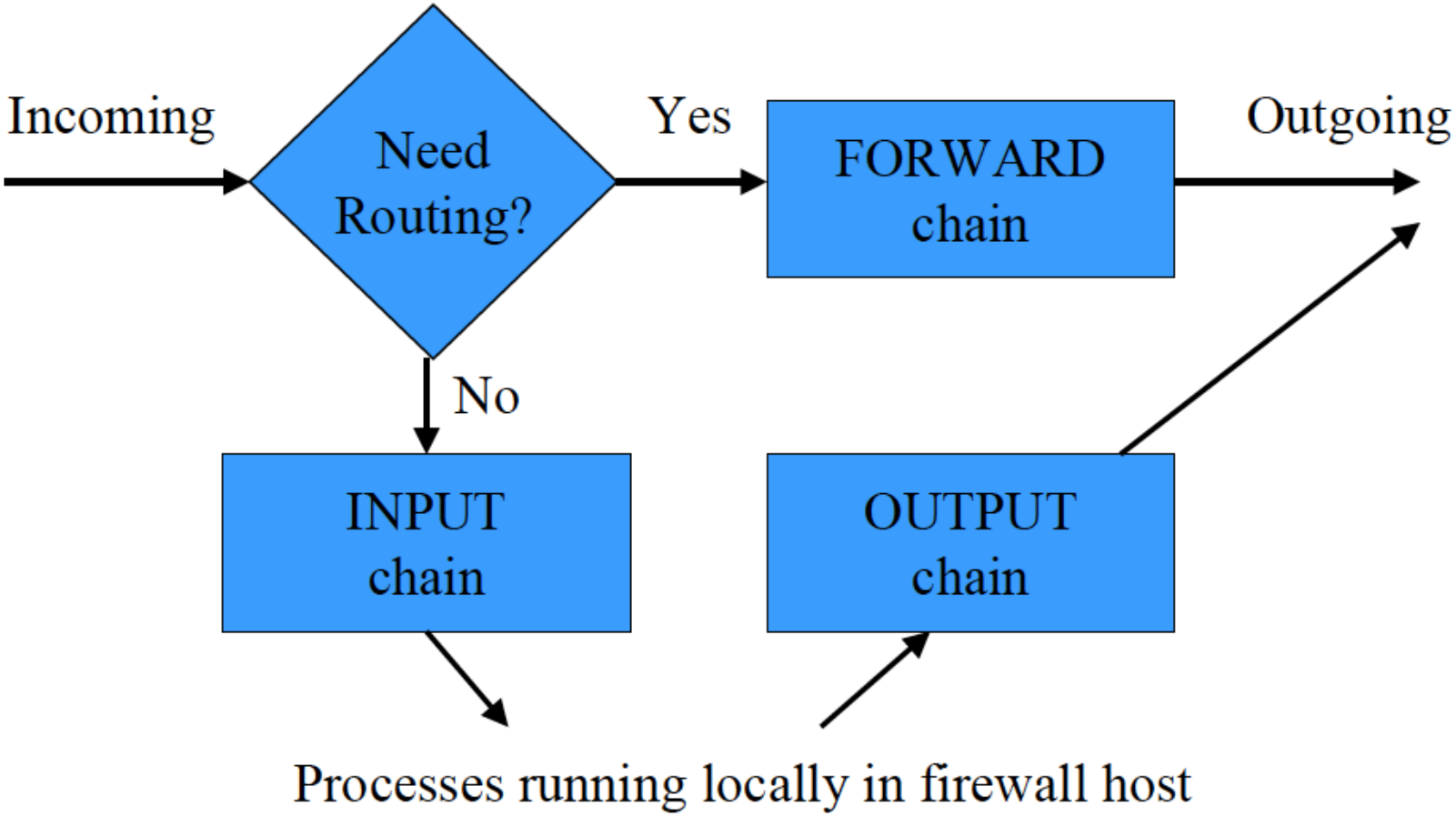
An introduction to iptables

- iptables은 linux에 내장된 방화벽
- 시스템 관리자는사전에 정의된 정책체인(chanin of rules)으로 패킷을 어떻게 처리할지 지정
- 주요 table
  - Raw : 다른 table이 사용전 패킷 분류 하는 default table. Security group, FWaaS에서는 사용안함
  - Filter : filter packet
  - NAT : used for network address translation
  - Mangle : 특정 packet에 대한 alteration. Security group, FWaaS에서는 사용안함

An introduction to iptables

- 5가지 default chains
- PREROUTING: Packets will enter this chain before a routing decision is made. This chain is not used for security group rules but for the floating IP functionality within a router namespace. The PREROUTING chain is used by the raw, mangle, and NAT tables.
- INPUT: This is used when a packet is to be locally delivered to the host machine. The INPUT chain is used by the mangle and filter tables.
- FORWARD: All packets that are routed and not used for local delivery will traverse this chain. The

An introduction to iptables



An introduction to iptables

- Possible verdicts include:
-
- ACCEPT: The packet is accepted and sent to the application for processing
- DROP: The packet is dropped silently
- REJECT: The packet is dropped and an error message is sent to the sender
- LOG: the packet details are logged
- DNAT: This rewrites the destination IP of the packet
- SNAT: This rewrites the source IP of the packet
- RETURN: This returns the processing to the calling chain

An introduction to iptables

- The ACCEPT, DROP, and REJECT verdicts are often used by the filter table. Common rule criteria include:
-
- -p <protocol>: This matches protocols such as TCP, UDP, ICMP, and more
- -s <ip_addr>: This matches the source IP address
- -d <ip_addr>: This matches the destination IP address
- --sport: This matches the source port
- --dport: This matches the destination port
- -i <interface>: This matches the interface from

An introduction to iptables

- 과거 release에선 모든 security group참조시 모든 source, dest. 주소 및 포트에 대해서 수많은 iptable이 생성됨.
- Juno 부터 ipset extension을 통해 iptable을 줄임

```
ipset -N webset iphash
ipset -A webset 1.1.1.1
ipset -A webset 2.2.2.2
ipset -A webset 3.3.3.3
ipset -A webset 4.4.4.4
iptables -A INPUT -p tcp -m set --match-set webset dst --dport 80 -j ACCEPT
```

Working with security groups

- Neutron CLI
- security-group-create
- security-group-delete
- security-group-list
- security-group-rule-create
- security-group-rule-delete
- security-group-rule-list
- security-group-rule-show
- security-group-show
- security-group-update

Implementing security group rules

- Neutron에서 security-group-list
- 현재 설정된 list 확인
-
-

```
root@controller01:~# neutron security-group-list
+--------------------------------------+-------------+-------------------------------+
| id                                   | name        | description                   |
+--------------------------------------+-------------+-------------------------------+
| 4decc566-7bd7-40bb-bd73-731a7a83f334 | default     | Default security group        |
| 60ca9b2c-dc87-40c7-a5ff-5e5037b08c56 | default     | Default security group        |
| b009d622-4a05-4ff1-a870-a3e9f22ff7b6 | WEB_SERVERS | Security group for web servers |
| c0c27f3d-cab1-4b2e-ad63-0339b3510d2f | default     | Default security group        |
+--------------------------------------+-------------+-------------------------------+
```

Implementing security group rules

- WEB_SERVERS Security group 생성 예제
-

```
root@controller01:~# neutron security-group-rule-create --protocol tcp --port-range-min 80 \
> --port-range-max 80 --remote-ip-prefix 0.0.0.0/0 WEB_SERVERS
Created a new security_group_rule:
+-------------------+--------------------------------------+
| Field             | Value                                |
+-------------------+--------------------------------------+
| direction         | ingress                              |
| ethertype         | IPv4                                 |
| id                | 74e11bbb-19df-40cc-a84d-6c2a4fb7a10c |
| port_range_max    | 80                                   |
| port_range_min    | 80                                   |
| protocol          | tcp                                  |
| remote_group_id   |                                      |
| remote_ip_prefix  | 0.0.0.0/0                            |
| security_group_id | b009d622-4a05-4ff1-a870-a3e9f22ff7b6 |
| tenant_id         | 65ff4cf1a04846f1ab2bc1ff0efb1090     |
+-------------------+--------------------------------------+

root@controller01:~# neutron security-group-rule-create --protocol tcp --port-range-min 443 \
> --port-range-max 443 --remote-ip-prefix 0.0.0.0/0 WEB_SERVERS
Created a new security_group_rule:
+-------------------+--------------------------------------+
| Field             | Value                                |
+-------------------+--------------------------------------+
| direction         | ingress                              |
| ethertype         | IPv4                                 |
| id                | 0a7c00ef-5f65-4729-bdc5-34ff976f0927 |
| port_range_max    | 443                                  |
| port_range_min    | 443                                  |
| protocol          | tcp                                  |
| remote_group_id   |                                      |
| remote_ip_prefix  | 0.0.0.0/0                            |
| security_group_id | b009d622-4a05-4ff1-a870-a3e9f22ff7b6 |
| tenant_id         | 65ff4cf1a04846f1ab2bc1ff0efb1090     |
+-------------------+--------------------------------------+
```

Implementing security group rules

- port-update command 사용하여 port에 security group 적용 예제

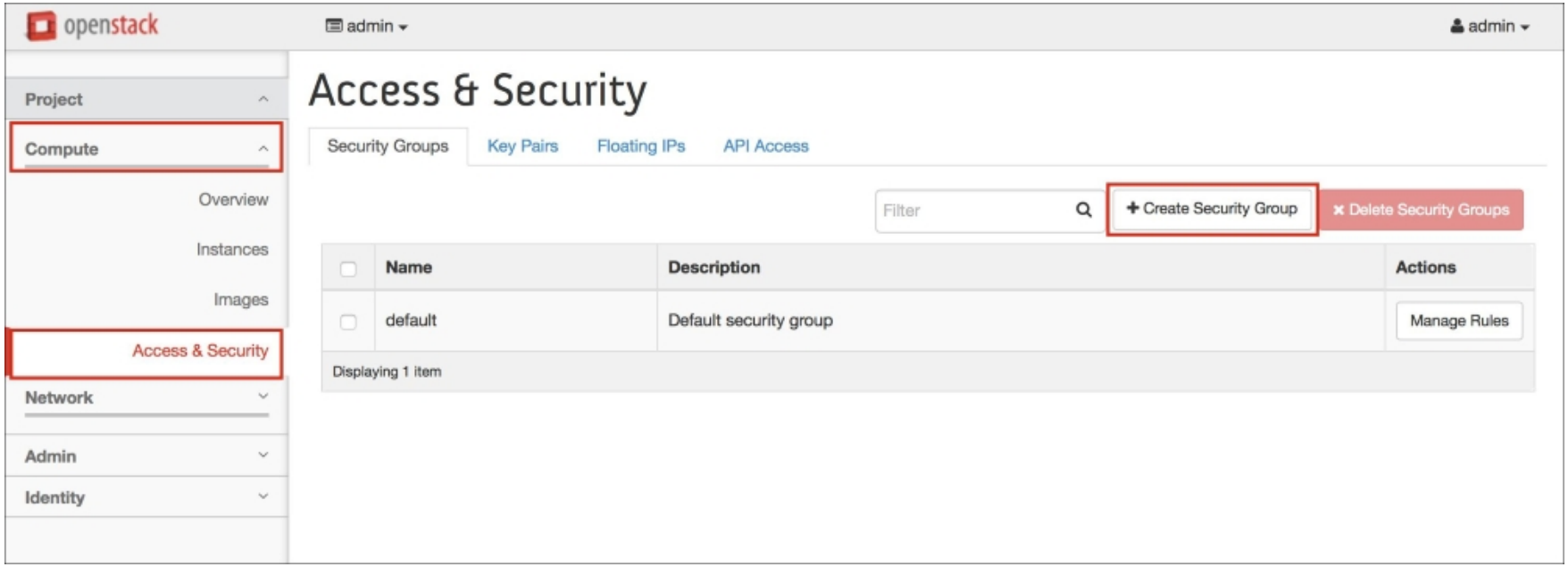
```
root@controller01:~# nova list
+--------------------------------------+------+--------+------------+-------------+--------------------+
| ID                                   | Name | Status | Task State | Power State | Networks           |
+--------------------------------------+------+--------+------------+-------------+--------------------+
| d92fea06-d71e-4009-bf87-d3dfcfc03333 | WEB1 | ACTIVE | -          | Running     | WEB_NET=10.30.0.3 |
+--------------------------------------+------+--------+------------+-------------+--------------------+

root@controller01:~# neutron port-list --device-id=d92fea06-d71e-4009-bf87-d3dfcfc03333 -c id
+--------------------------------------+
| id                                   |
+--------------------------------------+
| 6d7340c8-b1af-4cf0-b393-916a32acb18b |
+--------------------------------------+

root@controller01:~# neutron port-update 6d7340c8-b1af-4cf0-b393-916a32acb18b --security-group WEB_SERVERS
Updated port: 6d7340c8-b1af-4cf0-b393-916a32acb18b

root@controller01:~# neutron port-show 6d7340c8-b1af-4cf0-b393-916a32acb18b
+-----------------------+-------------------------------------------------------------------------------------+
| Field                 | Value                                                                               |
+-----------------------+-------------------------------------------------------------------------------------+
| admin_state_up        | True                                                                                |
| allowed_address_pairs |                                                                                     |
| binding:host_id       | compute02.learningneutron.com                                                       |
| binding:profile       | {}                                                                                  |
| binding:vif_details   | {"port_filter": true}                                                               |
| binding:vif_type      | bridge                                                                              |
| binding:vnic_type     | normal                                                                              |
| device_id             | d92fea06-d71e-4009-bf87-d3dfcfc03333                                                |
| device_owner          | compute:None                                                                        |
| extra_dhcp_opts       |                                                                                     |
| fixed_ips             | {"subnet_id": "d5cbbcb6-f039-4364-b1db-0392cd232dd9", "ip_address": "10.30.0.3"}   |
| id                    | 6d7340c8-b1af-4cf0-b393-916a32acb18b                                                |
| mac_address           | fa:16:3e:a4:c3:f9                                                                   |
| name                  |                                                                                     |
| network_id            | ebea7ab6-93f3-45db-b44a-bf284bac54ac                                                |
| security_groups       | b009d622-4a05-4ff1-a870-a3e9f22ff7b6                                                |
| status                | ACTIVE                                                                              |
| tenant_id             | 65ff4cf1a04846f1ab2bc1ff0efb1090                                                    |
+-----------------------+-------------------------------------------------------------------------------------+
```

Implementing security group rules

```
# Generated by iptables-save v1.4.21 on Tue Oct 27 17:35:56 2015
*filter
:INPUT ACCEPT [44:3963]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [33:4099]
:neutron-filter-top - [0:0]
:neutron-linuxbri-FORWARD - [0:0]
:neutron-linuxbri-INPUT - [0:0]
:neutron-linuxbri-OUTPUT - [0:0]
:neutron-linuxbri-i6d7340c8-b - [0:0]
:neutron-linuxbri-local - [0:0]
:neutron-linuxbri-o6d7340c8-b - [0:0]
:neutron-linuxbri-s6d7340c8-b - [0:0]
:neutron-linuxbri-sg-chain - [0:0]
:neutron-linuxbri-sg-fallback - [0:0]
-A INPUT -j neutron-linuxbri-INPUT
-A FORWARD -j neutron-filter-top
-A FORWARD -j neutron-linuxbri-FORWARD
-A OUTPUT -j neutron-filter-top
-A OUTPUT -j neutron-linuxbri-OUTPUT
-A neutron-filter-top -j neutron-linuxbri-local
-A neutron-linuxbri-FORWARD -m physdev --physdev-out tap6d7340c8-b1 --physdev-is-bridged  -j neutron-linuxbri-sg-chain
-A neutron-linuxbri-FORWARD -m physdev --physdev-in tap6d7340c8-b1 --physdev-is-bridged  -j neutron-linuxbri-sg-chain
-A neutron-linuxbri-INPUT -m physdev --physdev-in tap6d7340c8-b1 --physdev-is-bridged  -j neutron-linuxbri-o6d7340c8-b
-A neutron-linuxbri-i6d7340c8-b -m state --state INVALID -j DROP
-A neutron-linuxbri-i6d7340c8-b -m state --state RELATED,ESTABLISHED -j RETURN
-A neutron-linuxbri-i6d7340c8-b -s 10.30.0.2/32 -p udp -m udp --sport 67 --dport 68 -j RETURN
-A neutron-linuxbri-i6d7340c8-b -p tcp -m tcp --dport 443 -j RETURN
-A neutron-linuxbri-i6d7340c8-b -p tcp -m tcp --dport 80 -j RETURN
-A neutron-linuxbri-i6d7340c8-b -m comment --comment "Send unmatched traffic to the fallback chain." -j neutron-linuxbri-sg-fallback
-A neutron-linuxbri-o6d7340c8-b -p udp -m udp --sport 68 --dport 67 -m comment --comment "Allow DHCP client traffic." -j RETURN
-A neutron-linuxbri-o6d7340c8-b -j neutron-linuxbri-s6d7340c8-b
-A neutron-linuxbri-o6d7340c8-b -p udp -m udp --sport 67 --dport 68 -m comment --comment "Prevent DHCP Spoofing by VM." -j DROP
-A neutron-linuxbri-o6d7340c8-b -m state --state INVALID -j DROP
-A neutron-linuxbri-o6d7340c8-b -m state --state RELATED,ESTABLISHED -j RETURN
-A neutron-linuxbri-o6d7340c8-b -j RETURN
-A neutron-linuxbri-o6d7340c8-b -m comment --comment "Send unmatched traffic to the fallback chain." -j neutron-linuxbri-sg-fallback
-A neutron-linuxbri-s6d7340c8-b -s 10.30.0.3/32 -m mac --mac-source FA:16:3E:A4:C3:F9 -j RETURN
-A neutron-linuxbri-s6d7340c8-b -m comment --comment "Drop traffic without an IP/MAC allow rule." -j DROP
-A neutron-linuxbri-sg-chain -m physdev --physdev-out tap6d7340c8-b1 --physdev-is-bridged -j neutron-linuxbri-i6d7340c8-b
-A neutron-linuxbri-sg-chain -m physdev --physdev-in tap6d7340c8-b1 --physdev-is-bridged -j neutron-linuxbri-o6d7340c8-b
-A neutron-linuxbri-sg-chain -j ACCEPT
-A neutron-linuxbri-sg-fallback -m comment --comment "Default drop rule for unmatched traffic." -j DROP
COMMIT
# Completed on Tue Oct 27 17:35:56 2015
```

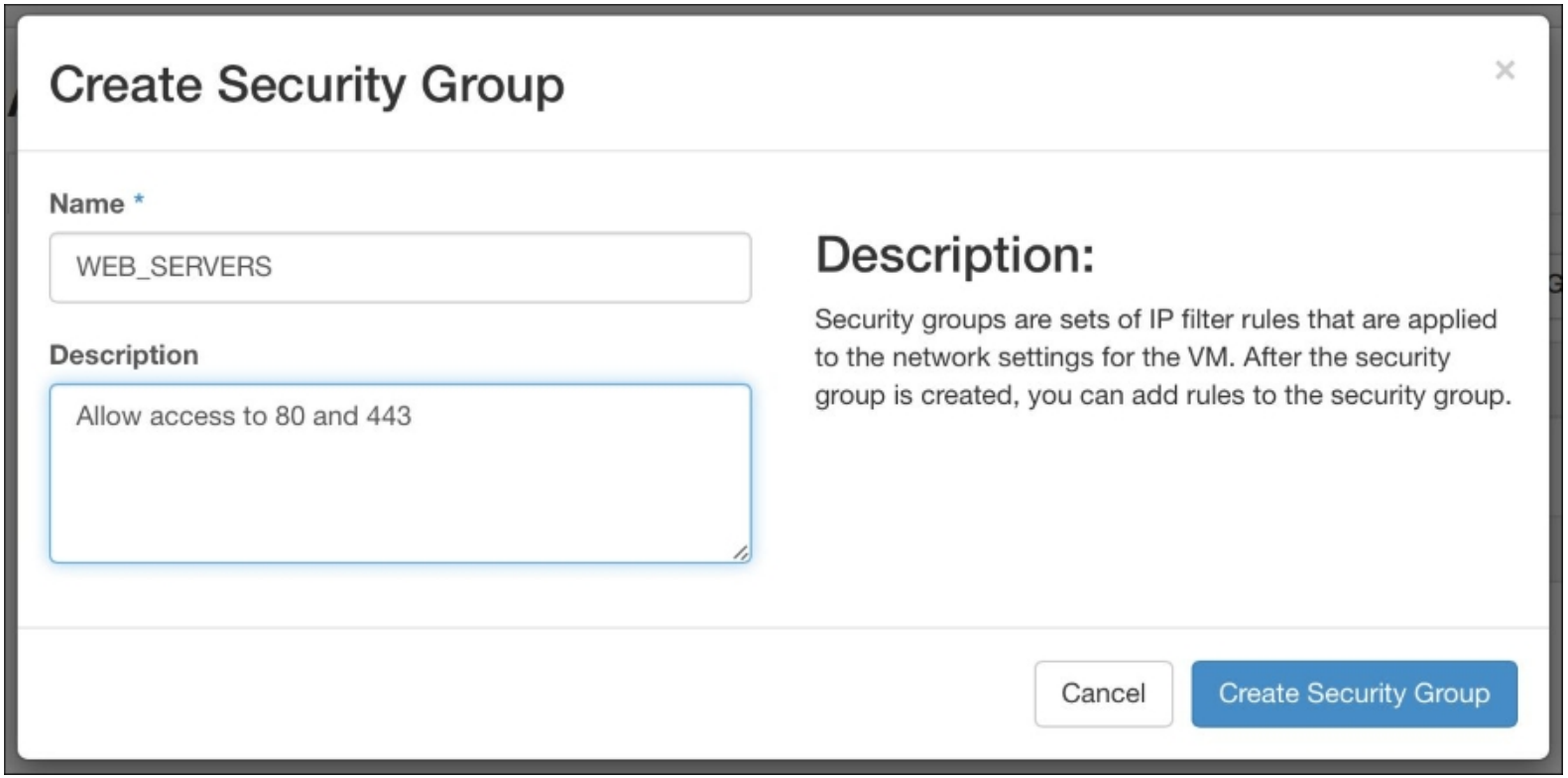
Working with security groups in the dashboard

- Access & Security section under the Compute tab:



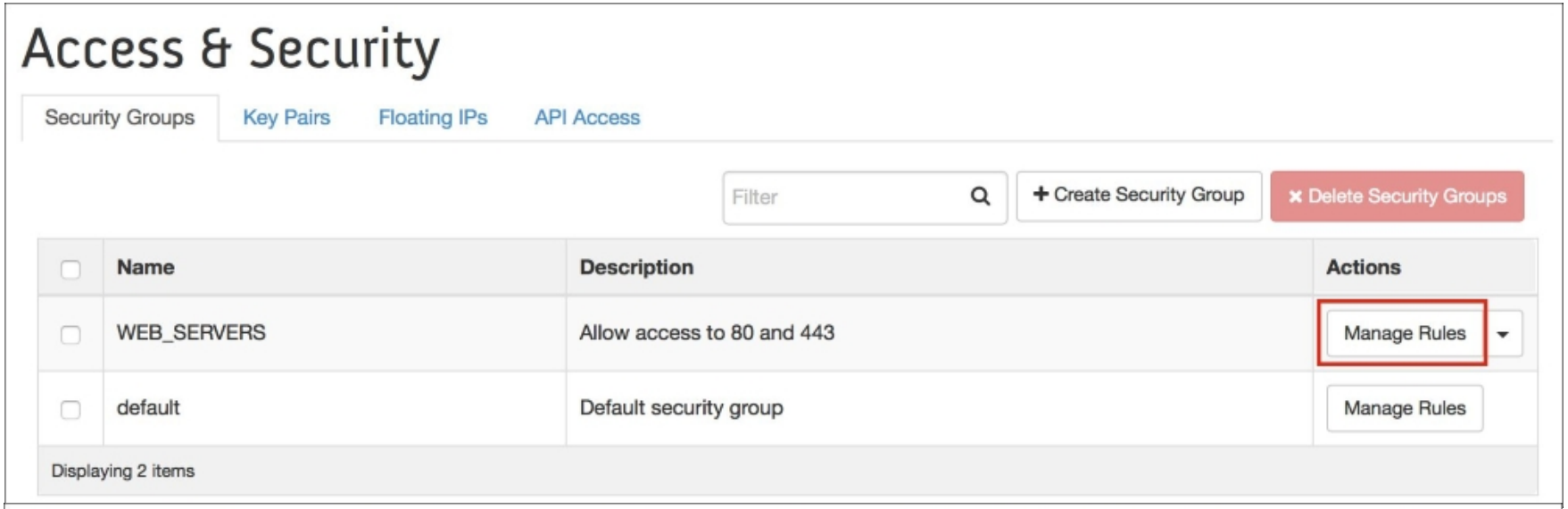
Working with security groups in the dashboard

- Creating a security group



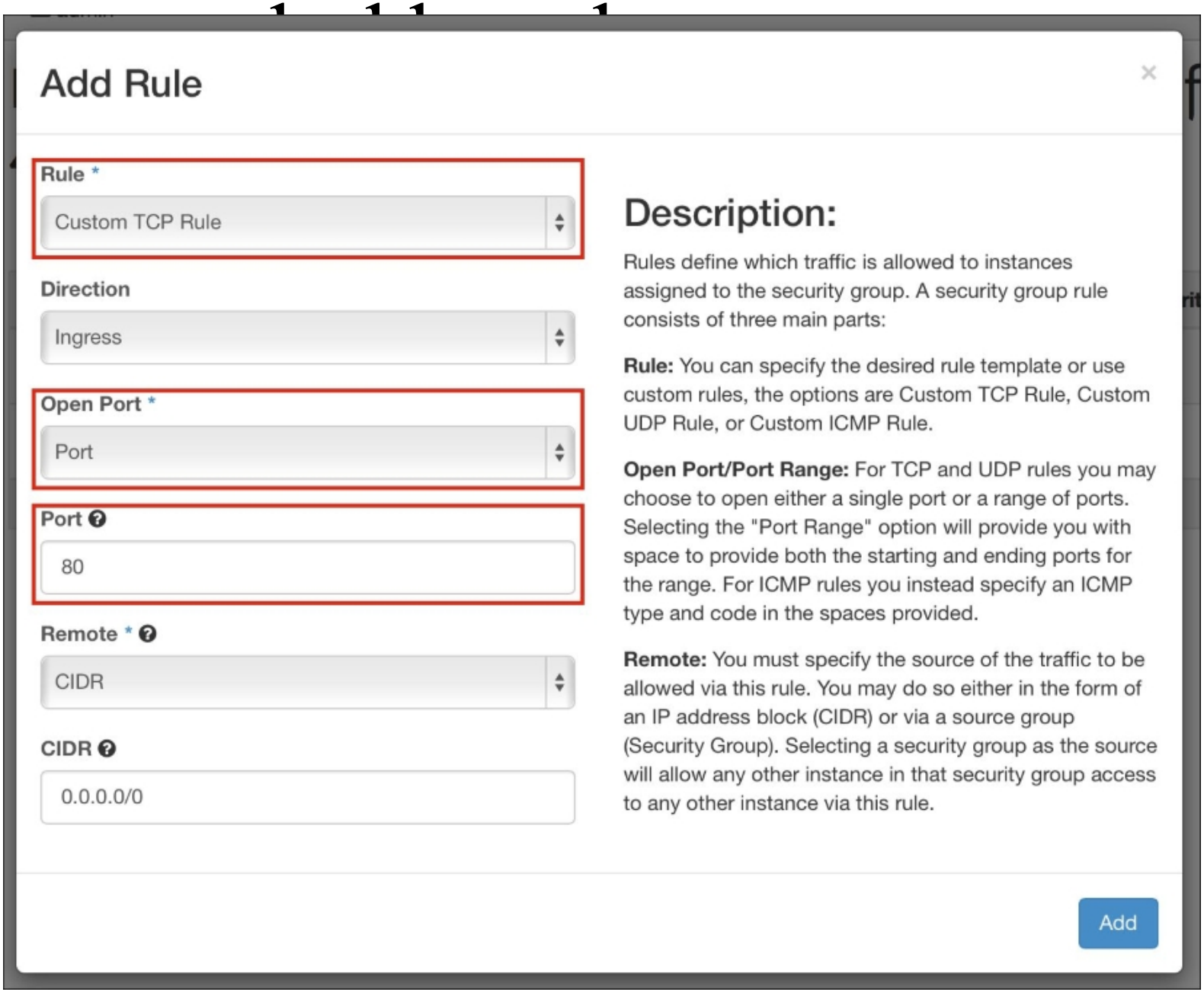
Working with security groups in the dashboard

- Managing security group rules



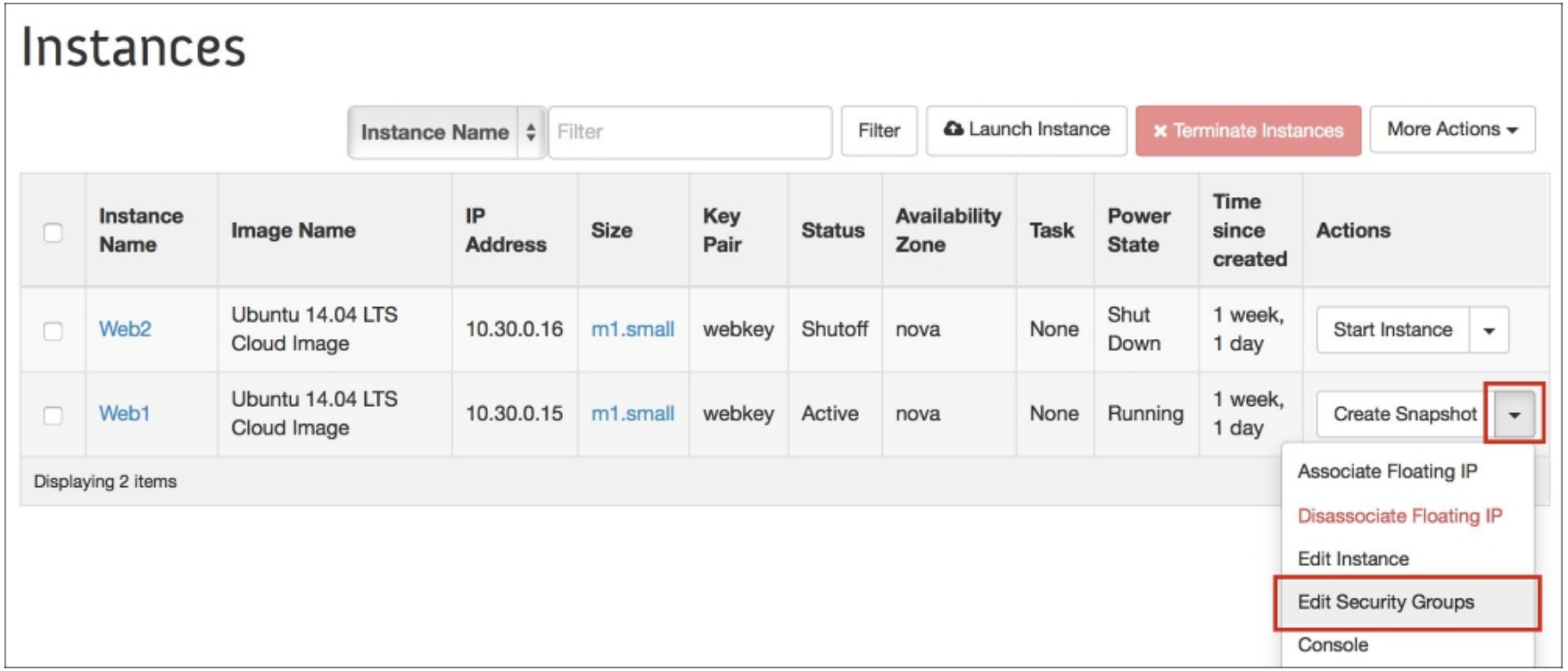
Working with security groups in the

- Managing security group rules



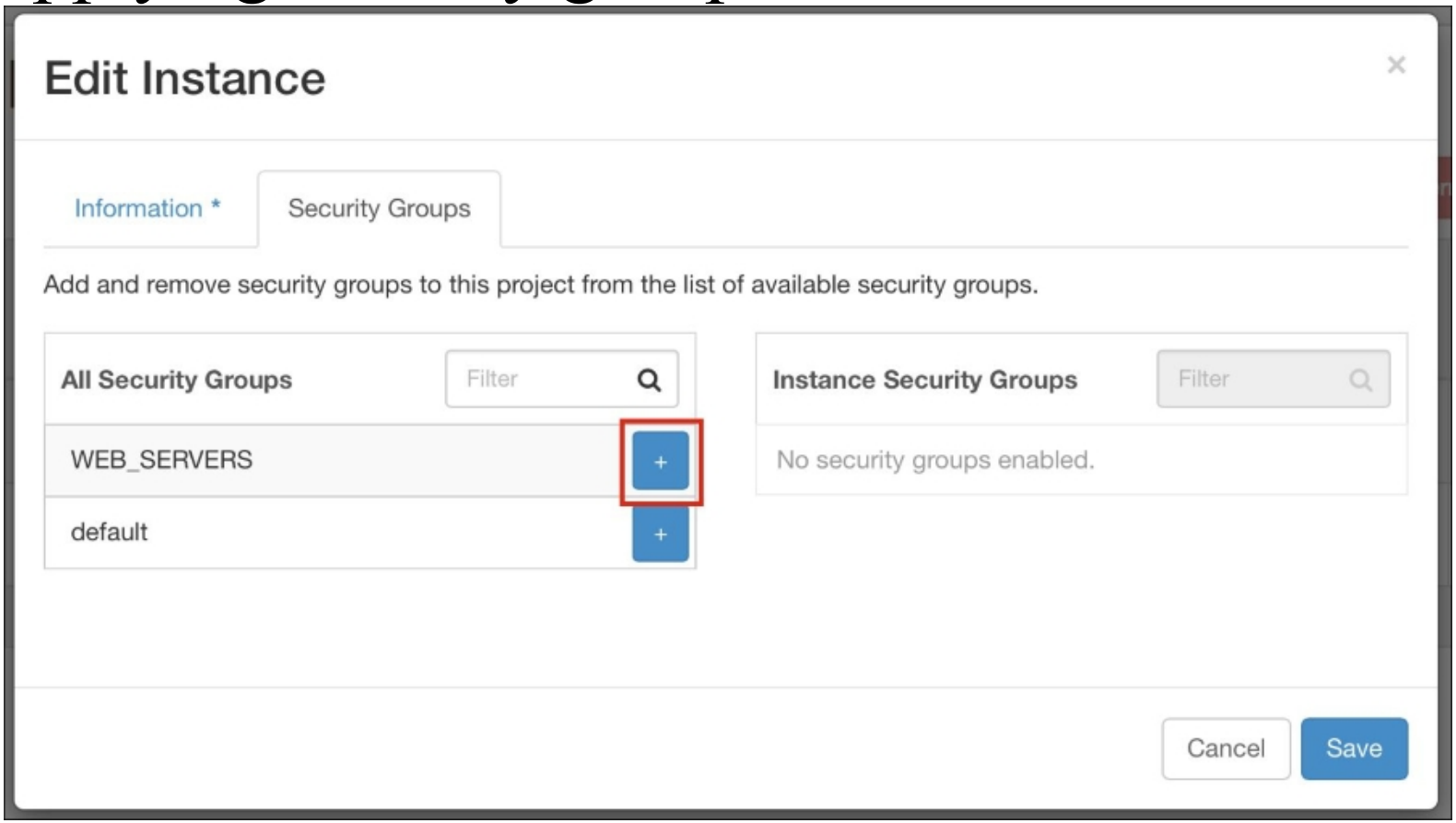
Working with security groups in the dashboard

- Applying security groups to instances



Working with security groups in the dashboard

- Applying security groups to instances



Working with security groups in the dashboard

- Applying security groups to instances