



# Custom Security Groups in OpenStack and AWS Clouds

Avi Technical Reference (v18.1)

Copyright © 2018

# Custom Security Groups in OpenStack and AWS Clouds [view online](#)

By default, the Avi Controller creates and manages a single security group (SG) for an Avi Service Engine. This SG manages the ingress/egress rules for the SE's management- and data-plane traffic. In certain customer environments, it may be required to provide custom SGs to be also be associated with the Avi SEs' management- and/or data-plane vNICs. Starting with release 17.1.3, this requirement can be satisfied. This article shows how to use the Avi SE group's `custom_securitygroups_mgmt` and `custom_securitygroups_data` configuration flags to achieve this extra flexibility in OpenStack and AWS clouds, via the Avi UI and Avi CLI.

## OpenStack Cloud

### Without any custom security group configuration

```
[root@sivacos ~(keystone_admin)]# nova show a2354abc-0455-440b-ac0b-0b0e50bc66d2
+-----+
| Property          | Value
+-----+
...
| avimgmt network   | 172.24.16.4
| description       | Avi-se-pyhlh
| id                | a2354abc-0455-440b-ac0b-0b0e50bc66d2
| image             | Avi-SE-17.1.4-9000-cloud-15190a62-e284-4033-8800-70c27c452bad-cluster-143b2840-19b6-409d-918d
| metadata          | {"AVICNTRL": "10.10.22.44", ..."AVISG_UUID": "bccf43ca-e98d-483b-9bff-43ab5e8970f3", ...}
| name              | Avi-se-pyhlh
| private network   | 10.0.0.10
| security_groups   | avi-se-a2354abc-0455-440b-ac0b-0b0e50bc66d2
| status            | ACTIVE
| tenant_id         | a6d878c0f7db40bf91ed1226e720460a
| xfrontend network| 192.168.10.13
+-----+

[root@sivacos ~(keystone_admin)]# neutron port-show 9427350d-31d9-42d2-a2e5-53bef1e52475
+-----+
| Field             | Value
+-----+
| device_id         | a2354abc-0455-440b-ac0b-0b0e50bc66d2
| device_owner      | compute:None
| fixed_ips         | {"subnet_id": "a178c1f1-5cce-4f0a-ac1a-8277e26b085e", "ip_address": "172.24.16.4"}
| id                | 9427350d-31d9-42d2-a2e5-53bef1e52475
| mac_address       | fa:16:3e:1d:ba:21
| name              | Avi-Mgmt:cluster-143b2840-19b6-409d-918d-d92edc98b2e1:cloud-15190a62-e284-4033-8800-70c27c452
| network_id        | 27bd1f64-5a50-4189-98db-3265809ac71a
| security_groups   | bccf43ca-e98d-483b-9bff-43ab5e8970f3
| status            | ACTIVE
| tenant_id         | a6d878c0f7db40bf91ed1226e720460a
...
+-----+
```

```
[root@sivacos ~(keystone_admin)]# neutron port-show 747d4110-c4d2-443e-8ee0-373702b4f4ec
+-----+
| Field          | Value
+-----+
| device_id      | a2354abc-0455-440b-ac0b-0b0e50bc66d2
| device_owner   | compute:None
| fixed_ips      | {"subnet_id": "4e010951-eb90-43af-9bad-e578f1ac2f77", "ip_address": "10.0.0.10"}
| id             | 747d4110-c4d2-443e-8ee0-373702b4f4ec
| mac_address    | fa:16:3e:fa:bd:ec
| name           | Avi-Data:cluster-143b2840-19b6-409d-918d-d92edc98b2e1:cloud-15190a62-e284-4033-8800-70c27c452
| network_id     | a6669299-dccb-40a9-a0d2-4608aaa79c0
| security_groups | bccf43ca-e98d-483b-9bff-43ab5e8970f3
| status         | ACTIVE
| tenant_id      | a6d878c0f7db40bf91ed1226e720460a
...
+-----+

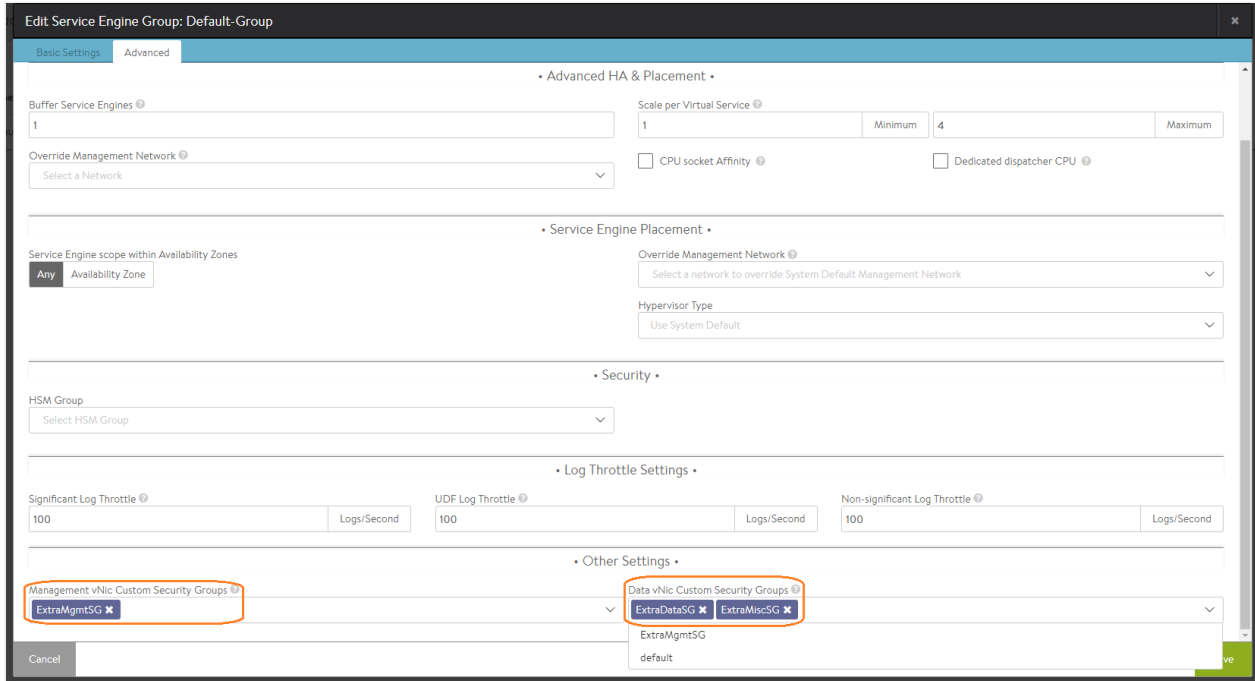
[root@sivacos ~(keystone_admin)]# neutron port-show 16414cce-7eaf-4d58-bdb5-fa8169a4a8e2
+-----+
| Field          | Value
+-----+
| device_id      | a2354abc-0455-440b-ac0b-0b0e50bc66d2
| device_owner   | compute:None
| fixed_ips      | {"subnet_id": "5b0d022b-33a2-42d9-873b-814ac2726e13", "ip_address": "192.168.10.13"}
| id             | 16414cce-7eaf-4d58-bdb5-fa8169a4a8e2
| mac_address    | fa:16:3e:91:a3:24
| name           | Avi-Data:cluster-143b2840-19b6-409d-918d-d92edc98b2e1:cloud-15190a62-e284-4033-8800-70c27c452
| network_id     | d36521da-8810-457e-95e5-a350143e61a4
| security_groups | bccf43ca-e98d-483b-9bff-43ab5e8970f3
| status         | ACTIVE
| tenant_id      | a6d878c0f7db40bf91ed1226e720460a
...
+-----+
```

**Custom security-group configuration via the Avi CLI:**

```
[admin:10-10-22-44]: > configure serviceenginegroup Default-Group
[admin:10-10-22-44]: serviceenginegroup> custom_securitygroups_mgmt 30fe49a4-ee31-43a9-9235-e23d59e392b3
[admin:10-10-22-44]: serviceenginegroup> custom_securitygroups_data 2aba00a7-8b20-45d4-88f3-64b901b9e363
[admin:10-10-22-44]: serviceenginegroup> custom_securitygroups_data adcf99de-46d0-44e2-8f3b-037804f725f0
[admin:10-10-22-44]: serviceenginegroup> save
+-----+
| Field          | Value
+-----+
...
| custom_securitygroups_mgmt[1] | 30fe49a4-ee31-43a9-9235-e23d59e392b3 |
| custom_securitygroups_data[1] | 2aba00a7-8b20-45d4-88f3-64b901b9e363 |
| custom_securitygroups_data[2] | adcf99de-46d0-44e2-8f3b-037804f725f0 |
+-----+
```

## Custom security-group configuration via the Avi UI

Navigate to Applications -> Infrastructure -> Service Engine Group and invoke the SE group editor. Select the appropriate named custom security groups for the management vNIC and the data vNIC.



## **Resulting custom security group configuration**

**As viewed from the OpenStack UI**

# Avi-se-yynxn

---

Overview
Log
Console
Action Log

---

<b>Name</b>	Avi-se-yynxn
<b>ID</b>	6f6abba9-c4e5-4c26-a3aa-f87b02d62419
<b>Status</b>	Active
<b>Availability Zone</b>	nova
<b>Created</b>	July 20, 2017, 12:18 a.m.
<b>Time Since Created</b>	53 minutes
<b>Host</b>	sivacos.110

---

### Specs

<b>Flavor Name</b>	m1.small
<b>Flavor ID</b>	2
<b>RAM</b>	2GB
<b>VCPUs</b>	1 VCPU
<b>Disk</b>	20GB

---

### IP Addresses

<b>Avimgmt</b>	172.24.16.9
<b>Xfrontend</b>	192.168.10.6
<b>Private</b>	10.0.0.6

---

### Security Groups

<b>ExtraDataSG</b>	<ul style="list-style-type: none"> <li>ALLOW IPv4 8888/tcp from 9458b260-173a</li> <li>ALLOW IPv6 to ::/0</li> <li>ALLOW IPv4 80/tcp from ExtraDataSG</li> <li>ALLOW IPv4 to 0.0.0.0/0</li> </ul>
<b>ExtraMgmtSG</b>	<ul style="list-style-type: none"> <li>ALLOW IPv4 9999/tcp from 0.0.0.0/0</li> <li>ALLOW IPv4 to 0.0.0.0/0</li> <li>ALLOW IPv6 to ::/0</li> </ul>
<b>avi-se-6f6abba9-c4e5-4...</b>	<ul style="list-style-type: none"> <li>ALLOW IPv4 22/tcp from 0.0.0.0/0</li> <li>ALLOW IPv4 icmp from 0.0.0.0/0</li> <li>ALLOW IPv4 to 0.0.0.0/0</li> <li>ALLOW IPv4 80/tcp from 0.0.0.0/0</li> <li>ALLOW IPv6 to ::/0</li> </ul>
<b>ExtraMiscSG</b>	<ul style="list-style-type: none"> <li>ALLOW IPv4 to 0.0.0.0/0</li> <li>ALLOW IPv6 to ::/0</li> </ul>

**As viewed from the OpenStack CLI**

```
[root@sivacos ~(keystone_admin)]# nova show 6f6abba9-c4e5-4c26-a3aa-f87b02d62419
+-----+
| Property          | Value
+-----+
...
| avimgmt network   | 172.24.16.9
| description       | Avi-se-yynxn
| id                | 6f6abba9-c4e5-4c26-a3aa-f87b02d62419
| image             | Avi-SE-17.1.4-9000-cloud-15190a62-e284-4033-8800-70c27c452bad-cluster-143b2840-19b6-409d-918c
| metadata          | {"AVICNTRL": "10.10.22.44", "AVISG_UUID": "3d13ee89-5069-4dd2-a505-b6d7032bea9e", ..}
| name              | Avi-se-yynxn
| private network   | 10.0.0.6
| security_groups   | ExtraDataSG, ExtraMgmtSG, ExtraMiscSG, avi-se-6f6abba9-c4e5-4c26-a3aa-f87b02d62419
| status            | ACTIVE
| tenant_id         | a6d878c0f7db40bf91ed1226e720460a
| xfrontend network | 192.168.10.6
+-----+

[root@sivacos ~(keystone_admin)]# neutron port-show 51783401-f174-4240-93df-028564aeb54b
+-----+
| Field             | Value
+-----+
| device_id         | 6f6abba9-c4e5-4c26-a3aa-f87b02d62419
| device_owner      | compute:None
| fixed_ips         | {"subnet_id": "5b0d022b-33a2-42d9-873b-814ac2726e13", "ip_address": "192.168.10.6"}
| id                | 51783401-f174-4240-93df-028564aeb54b
| mac_address       | fa:16:3e:50:7a:73
| name              | Avi-Data:cluster-143b2840-19b6-409d-918d-d92edc98b2e1:cloud-15190a62-e284-4033-8800-70c27c452
| network_id        | d36521da-8810-457e-95e5-a350143e61a4
| security_groups   | 2aba00a7-8b20-45d4-88f3-64b901b9e363
|                   | 3d13ee89-5069-4dd2-a505-b6d7032bea9e
|                   | adcf99de-46d0-44e2-8f3b-037804f725f0
| status            | ACTIVE
| tenant_id         | a6d878c0f7db40bf91ed1226e720460a
...
+-----+

[root@sivacos ~(keystone_admin)]# neutron port-show 69bb1115-7e1d-474d-97b7-178d25a2dbe6
+-----+
| Field             | Value
+-----+
| device_id         | 6f6abba9-c4e5-4c26-a3aa-f87b02d62419
| device_owner      | compute:None
| fixed_ips         | {"subnet_id": "4e010951-eb90-43af-9bad-e578f1ac2f77", "ip_address": "10.0.0.6"}
| id                | 69bb1115-7e1d-474d-97b7-178d25a2dbe6
| mac_address       | fa:16:3e:91:92:38
| name              | Avi-Data:cluster-143b2840-19b6-409d-918d-d92edc98b2e1:cloud-15190a62-e284-4033-8800-70c27c452
| network_id        | a6669299-dccb-40a9-a0d2-4608aaea79c0
```

```

| security_groups      | 2aba00a7-8b20-45d4-88f3-64b901b9e363
|                     | 3d13ee89-5069-4dd2-a505-b6d7032bea9e
|                     | adcf99de-46d0-44e2-8f3b-037804f725f0
| status              | ACTIVE
| tenant_id           | a6d878c0f7db40bf91ed1226e720460a
...
+-----+
[root@sivacos ~(keystone_admin)]# neutron port-show ca8c572e-f430-4176-87e0-780c81e82b91
+-----+
| Field                | Value
+-----+
| device_id            | 6f6abba9-c4e5-4c26-a3aa-f87b02d62419
| device_owner        | compute:None
| fixed_ips            | {"subnet_id": "a178clf1-5cce-4f0a-ac1a-8277e26b085e", "ip_address": "172.24.16.9"}
| id                  | ca8c572e-f430-4176-87e0-780c81e82b91
| mac_address         | fa:16:3e:c2:42:d1
| name                | Avi-Mgmt:cluster-143b2840-19b6-409d-918d-d92edc98b2e1:cloud-15190a62-e284-4033-8800-70c27c452
| network_id          | 27bd1f64-5a50-4189-98db-3265809ac71a
| security_groups     | 30fe49a4-ee31-43a9-9235-e23d59e392b3
|                     | 3d13ee89-5069-4dd2-a505-b6d7032bea9e
| status              | ACTIVE
| tenant_id           | a6d878c0f7db40bf91ed1226e720460a
...
+-----+

```

## AWS Cloud

### Without any custom security group configuration

The screenshot shows the AWS console for an instance named 'i-04cd0bdb7c8d3da61'. The instance is running in the 'us-west-2a' availability zone. A table titled 'Security Groups associated with i-04cd0bdb7c8d3da61' is highlighted, showing the following rules:

Ports	Protocol	Source	Security Group ID	Status
80	tcp	0.0.0.0/0	avi-se-db7e1ed2-6ce6-11e7-ad6e-005056b05c4a	✓
22	tcp	0.0.0.0/0	avi-se-db7e1ed2-6ce6-11e7-ad6e-005056b05c4a	✓
All	All	10.144.0.0/16	avi-se-db7e1ed2-6ce6-11e7-ad6e-005056b05c4a	✓
All	All	10.144.0.0/16	avi-se-db7e1ed2-6ce6-11e7-ad6e-005056b05c4a	✓
All	63	10.144.0.0/16	avi-se-db7e1ed2-6ce6-11e7-ad6e-005056b05c4a	✓
-1	icmp	0.0.0.0/0	avi-se-db7e1ed2-6ce6-11e7-ad6e-005056b05c4a	✓

Network interface eth0 details:

- Interface ID: ent-83e238af
- VPC ID: vpc-1929957c
- Attachment Owner: 13928485014
- Attachment Status: attached
- Attachment Time: Wed Jul 19 18:00:44 GMT-700 2017
- Delete on Terminate: true
- Private IP Address: 10.144.10.68
- Private DNS Name: ip-10-144-10-68.us-west-2.compute.internal
- Elastic IP Address: -
- Source/Dest. Check: false
- Description: Avi-Mgmt
- Security Groups: avi-se-db7e1ed2-6ce6-11e7-ad6e-005056b05c4a

Network interface eth1 details:

- Interface ID: ent-cae43be6
- VPC ID: vpc-1929957c
- Attachment Owner: 13928485014
- Attachment Status: attached
- Attachment Time: Wed Jul 19 18:04:35 GMT-700 2017
- Delete on Terminate: false
- Private IP Address: 10.144.1.27
- Private DNS Name: ip-10-144-1-27.us-west-2.compute.internal
- Elastic IP Address: -
- Source/Dest. Check: false
- Description: Avi-Data
- Security Groups: avi-se-db7e1ed2-6ce6-11e7-ad6e-005056b05c4a

### Custom security group configuration via the Avi CLI

```

[admin:10-10-22-44]: > configure serviceenginegroup Default-Group
[admin:10-10-22-44]: serviceenginegroup> custom_securitygroups_mgmt sg-5c902726

```

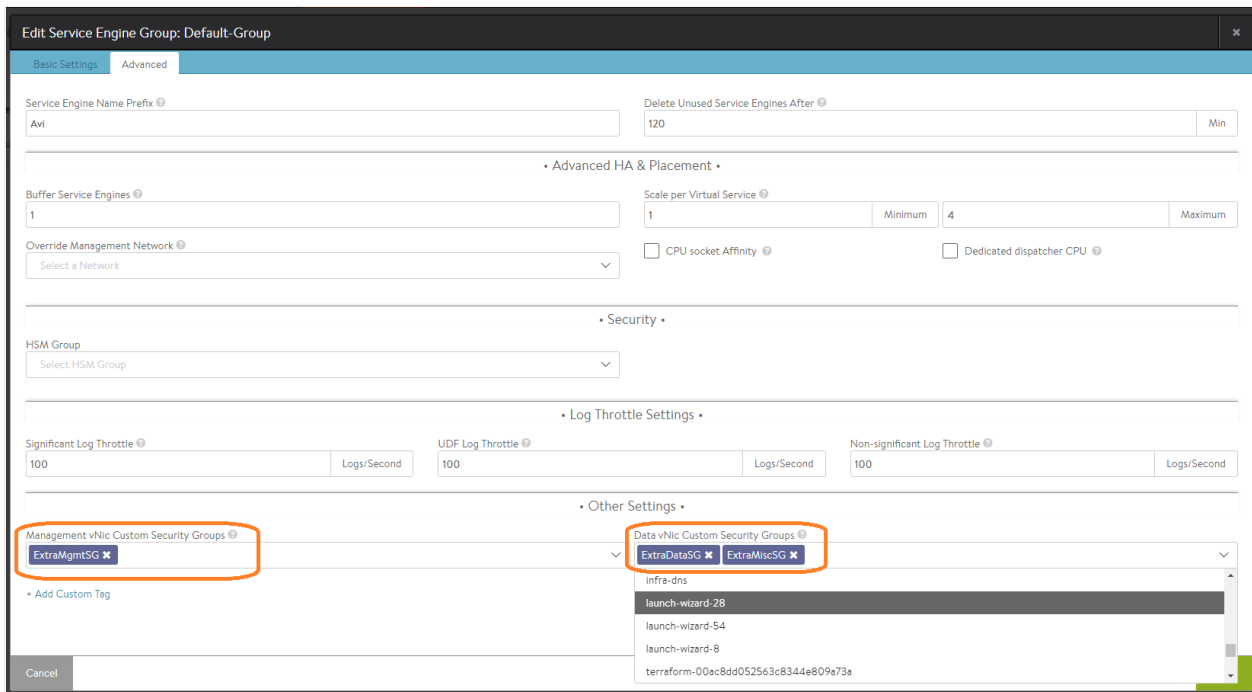


```
[admin:10-10-22-44]: serviceenginegroup> custom_securitygroups_data sg-4b9d2a31
[admin:10-10-22-44]: serviceenginegroup> custom_securitygroups_data sg-b99c2bc3
[admin:10-10-22-44]: serviceenginegroup> save
```

Field	Value
...	
custom_securitygroups_mgmt[1]	sg-5c902726
custom_securitygroups_data[1]	sg-4b9d2a31
custom_securitygroups_data[2]	sg-b99c2bc3

### Custom security-group configuration via the Avi UI

Navigate to Applications -> Infrastructure -> Service Engine Group and invoke the SE group editor. Select the appropriate named custom security groups for the management vNIC and the data vNIC.



### Resulting custom security group configuration as viewed from the AWS UI

Instance: i-041bb268254b6def4 (Avi-se-plybb) Private IP: 10.144.10.178

**Description** | Status Checks | Monitoring | Tags

Instance ID: i-041bb268254b6def4  
 Instance state: running  
 Instance type: t2.micro  
 Elastic IPs: -  
 Availability zone: us-west-2a  
 Security groups: ExtraMgmtSG, avi-se-353d4eb4-6ce9-11e7-ad6e-005056b05c4a  
 Scheduled events: No scheduled events  
 AMI ID: Avi-SE-17.1.4-9000-cloud-d81602db-90ba-45ca-9c84-3765f0c9820-cluster-143b2840-19b6-409d-918d-d92edc98b2e1 (ami-0271687b)  
 Platform: -  
 IAM role: -  
 Key pair name: -  
 Owner: 13928488501  
 Launch time: July 19, 2017  
 Termination protection: False  
 Lifecycle: normal  
 Monitoring: basic  
 Alarm status: None  
 Kernel ID: -  
 RAM disk ID: -

Public DNS (IPv4): -  
 IPv4 Public IP: -  
 IPv6 IPs: -  
 Private DNS: ip-10-144-10-178.us-west-2.com  
 Private IPs: 10.144.10.178, 10.144.1.128  
 Secondary private IPs: 10.144.1.4  
 VPC ID: vpc-19295f7c  
 Subnet ID: subnet-7f8eb81a  
 Network interfaces: eth0, eth1  
 Source/dest. check: False  
 EBS-optimized: False  
 Root device type: ebs  
 Root device: /dev/sda1  
 Block devices: /dev/sda1

**Security Groups associated with i-041bb268254b6def4**

Ports	Protocol	Source	ExtraMgmtSG	avi-se-353d4eb4-6ce9-11e7-ad6e-005056b05c4a
9999	tcp	12.97.16.194/32	✓	✓
80	tcp	0.0.0.0/0	✓	✓
22	tcp	0.0.0.0/0	✓	✓
All	97	10.144.0.0/16	✓	✓
All	73	10.144.0.0/16	✓	✓
All	63	10.144.0.0/16	✓	✓
-1	icmp	0.0.0.0/0	✓	✓

**Network Interface eth0**

Interface ID: eni-1b08d737  
 VPC ID: vpc-19295f7c  
 Attachment Owner: 139284885014  
 Attachment Status: attached  
 Attachment Time: Wed Jul 19 18:17:34 GMT-700 2017  
 Delete on Terminate: true  
 Private IP Address: 10.144.10.178  
 Private DNS Name: ip-10-144-10-178.us-west-2.compute.internal  
 Elastic IP Address: -  
 Source/Dest. Check: false  
 Description: Avi-Mgmt  
 Security Groups: ExtraMgmtSG, avi-se-353d4eb4-6ce9-11e7-ad6e-005056b05c4a

**Network Interface eth1**

Interface ID: eni-a73ee18b  
 VPC ID: vpc-19295f7c  
 Attachment Owner: 139284885014  
 Attachment Status: attached  
 Attachment Time: Wed Jul 19 18:21:41 GMT-700 2017  
 Delete on Terminate: false  
 Private IP Address: 10.144.1.128  
 Private DNS Name: ip-10-144-1-128.us-west-2.compute.internal  
 Elastic IP Address: -  
 Source/Dest. Check: false  
 Description: Avi-Data  
 Security Groups: ExtraDataSG, avi-se-353d4eb4-6ce9-11e7-ad6e-005056b05c4a, ExtraMiscSG

**Network Interface: eni-1b08d737**

Details | Flow Logs | Tags

Network interface ID: eni-1b08d737  
 VPC ID: vpc-19295f7c  
 MAC address: 02:f0:c1:07:25:3e  
 Security groups: avi-se-353d4eb4-6ce9-11e7-ad6e-005056b05c4a, ExtraMgmtSG  
 Status: in-use  
 Private DNS (IPv4): ip-10-144-10-178.us-west-2.com  
 Secondary private IPv4 IPs: -  
 Source/dest. check: false  
 Instance ID: i-041bb268254b6def4  
 Device index: 0  
 Delete on termination: true  
 Allocation ID: -

Subnet ID: subnet-7f8eb81a  
 Availability Zone: us-west-2a  
 Description: Avi-Mgmt  
 Owner ID: 139284885014  
 IPv4 IP: 10.144.10.178  
 Public IP: -  
 IPv6 IPs: -  
 Attachment ID: eni-attach-8200fc59  
 Attachment owner: 139284885014  
 Attachment status: attached  
 Owner ID: -  
 Allocation ID: -

**Security Group Rules**

Ports	Protocol	Source	ExtraMgmtSG	avi-se-353d4eb4-6ce9-11e7-ad6e-005056b05c4a
9999	tcp	12.97.16.194/32	✓	✓
80	tcp	0.0.0.0/0	✓	✓
22	tcp	0.0.0.0/0	✓	✓
All	97	10.144.0.0/16	✓	✓
All	73	10.144.0.0/16	✓	✓
All	63	10.144.0.0/16	✓	✓
-1	icmp	0.0.0.0/0	✓	✓

**Network Interface: eni-a73ee18b**

Details | Flow Logs | Tags

Network interface ID: eni-a73ee18b  
 VPC ID: vpc-19295f7c  
 MAC address: 02:d0:d5:f1:0b:18  
 Security groups: avi-se-353d4eb4-6ce9-11e7-ad6e-005056b05c4a, ExtraDataSG, ExtraMiscSG  
 Status: in-use  
 Private DNS (IPv4): ip-10-144-1-128.us-west-2.com  
 Secondary private IPv4 IPs: 10.144.1.4  
 Source/dest. check: false  
 Instance ID: i-041bb268254b6def4  
 Device index: 1  
 Delete on termination: false  
 Allocation ID: -

Subnet ID: subnet-62f1b707  
 Availability Zone: us-west-2a  
 Description: Avi-Data  
 Owner ID: 139284885014  
 IPv4 IP: 10.144.1.128  
 Public IP: -  
 Attachment ID: eni-attach-17e82f4  
 Attachment owner: 139284885014  
 Attachment status: attached  
 Owner ID: -  
 Allocation ID: -

**Security Group Rules**

Ports	Protocol	Source	ExtraDataSG	avi-se-353d4eb4-6ce9-11e7-ad6e-005056b05c4a	ExtraMiscSG
8888	tcp	10.100.100.0/24	✓	✓	✓
80	tcp	0.0.0.0/0	✓	✓	✓
22	tcp	0.0.0.0/0	✓	✓	✓
All	97	10.144.0.0/16	✓	✓	✓
All	73	10.144.0.0/16	✓	✓	✓
All	63	10.144.0.0/16	✓	✓	✓
-1	icmp	0.0.0.0/0	✓	✓	✓
7777	tcp	0.0.0.0/0, :::0	✓	✓	✓