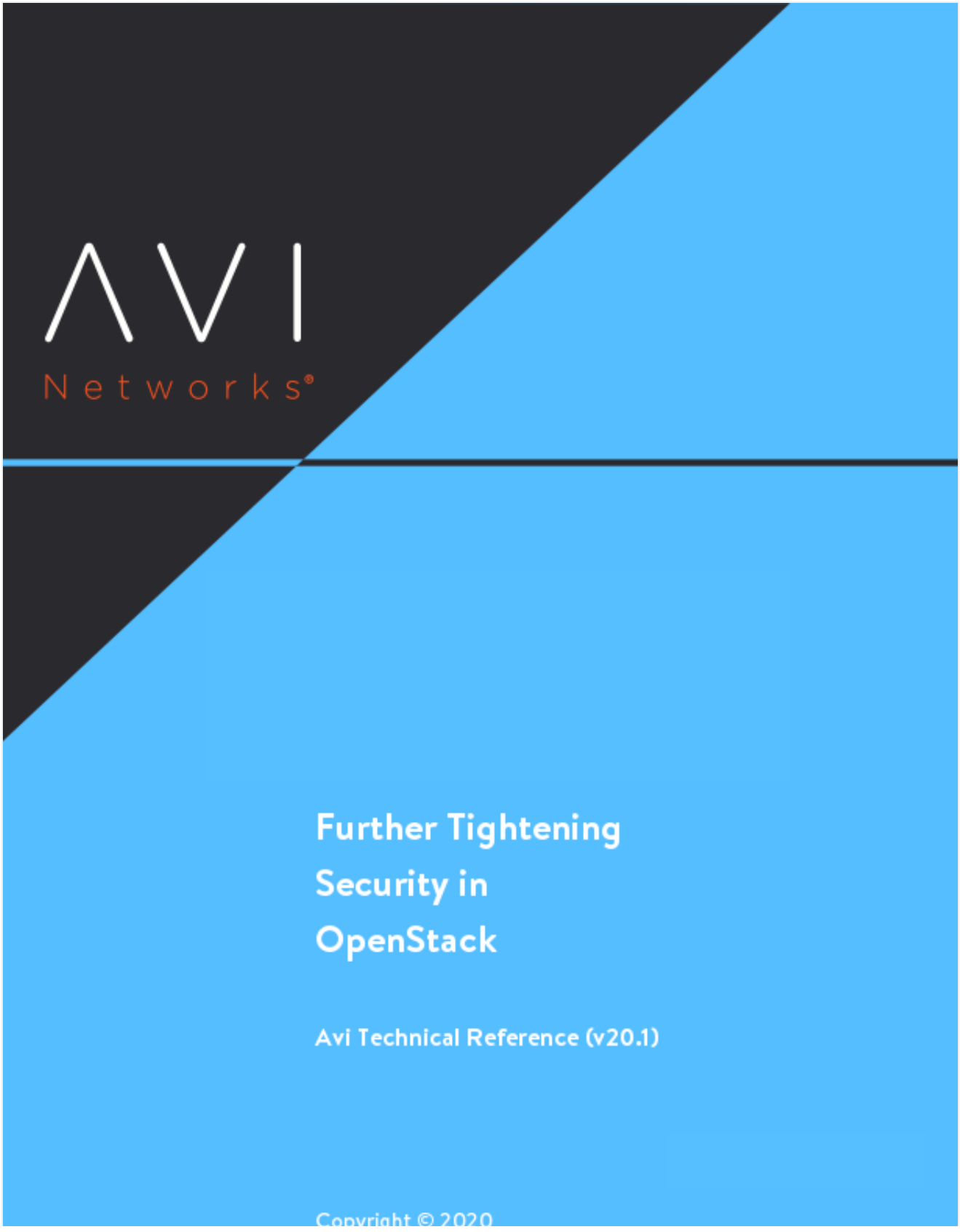

Further Tightening Security in OpenStack

Avi Technical Reference (v20.1)

Further Tightening Security in OpenStack

view online

Overview

By default, the Avi Controller managed Security Group (SG) associated with an Avi SE will have rules to allow both TCP port 22 (SSH) and all ICMP ingress traffic. This is useful during troubleshooting scenarios for Avi Support personnel to directly SSH into the Avi SE. In certain customer environments, it may be required to further lock down TCP port 22. This article shows how to use the Avi cloud's `wildcard_access` configuration flag to achieve this extra measure of security.

After showing the detail case for each type of cloud, we will show the CLI sequence by which to take action.

Default Case in OpenStack

```
root@node-17:~# neutron security-group-list
+--------------------------------------+--------------------------------------------+-------------------------------
| id                                   | name                                       | security_group_rules
+--------------------------------------+--------------------------------------------+-------------------------------
| e1e3f96e-cc9d-4fd4-bb01-4db9480621d8 | avi-se-3cf0f25c-8b25-4b6c-94db-ab59ae8f2f23 | egress, IPv4
|                                      |                                            | egress, IPv6
|                                      |                                            | ingress, IPv4, 22/tcp, remote_ip
|                                      |                                            | ingress, IPv4, icmp, remote_ip_p
+--------------------------------------+--------------------------------------------+-------------------------------
```

Disabling Port 22 Wildcard Access

The below somewhat abbreviated CLI command sequence first reveals that the `wildcard_access` configuration setting is set to True, the default. Subsequent commands change it to False.

Note: The change takes effect only for newly created SEs.

```
[admin:10-10-22-142]: > configure cloud avi-os
Updating an existing object. Currently, the object is:
+--------------------------+-----------------------------------------+
| Field                    | Value                                   |
+--------------------------+-----------------------------------------+
| uuid                     | cloud-c62d3177-ca44-4565-a167-62d783a34be9 |
| name                     | avi-os                                  |
| vtype                    | CLOUD_OPENSTACK                         |
| openstack_configuration  |                                         |
|   username               | admin                                   |
|   security_groups        | True                                    |
|   auth_url               | http://10.10.22.23:5000/v2.0            |
|   wildcard_access        | True                                    |

...  DETAILS OMITTED ...
```

```
| tenant_ref                | admin                                      |
+---------------------------+--------------------------------------------+
[admin:10-10-22-142]: cloud:openstack_configuration>
[admin:10-10-22-142]: cloud:openstack_configuration> no wildcard_access
[admin:10-10-22-142]: cloud:openstack_configuration> save
[admin:10-10-22-142]: cloud> save
[admin:10-10-22-142]: cloud> save
+---------------------------+--------------------------------------------+
| Field                     | Value                                      |
+---------------------------+--------------------------------------------+
| uuid                      | cloud-c62d3177-ca44-4565-a167-62d783a34be9 |
| name                      | avi-os                                     |
| vtype                     | CLOUD_OPENSTACK                            |
| openstack_configuration   |                                            |
|   username                | admin                                      |
|   security_groups         | True                                       |
|   auth_url                | http://10.10.22.23:5000/v2.0               |
|   wildcard_access         | False                                      |
...
| tenant_ref                | admin                                      |
+---------------------------+--------------------------------------------+
```

Confirming Security Has Been Tightened (OpenStack Case)

```
root@node-17:~# neutron security-group-list
+--------------------------------------+--------------------------------------------+--------------------------------
| id                                   | name                                       | security_group_rules
+--------------------------------------+--------------------------------------------+--------------------------------
| fafaf765-9d88-42d0-ae48-76b839177b52 | avi-se-095fa798-d643-4a7b-849b-910e33421f11 | egress, IPv4
|                                      |                                            | egress, IPv6
|                                      |                                            | ingress, IPv4, icmp, remote_ip_p
+--------------------------------------+--------------------------------------------+--------------------------------
```