Security Group and Rules

Security Group Rules

This section describes the Security Group rules we program on AWS with Cisco Catalyst 8000V enabled in home and non-home regions for Cloud Network Controller.

Note The External Network comes from the "cloud formation template during cloud controller launch" and this is the network from which you access Cloud Network Controller or Cisco Catalyst 8000Vs.

Security Group rules created in AWS after the Cloud Network Controller bringup

1. **Security Group**- uni/tn-infra/cloudapp-cloud-infra/cloudepg-controllers

   Purpose- Attached to Cisco Cloud Network Controller management interface.

   Inbound Rules

   a. *Rule 1:* (HTTPS access to Cloud Network Controller)

      Source: External Network

      Destination: Cloud Network Controller

      Protocol- TCP

      Port – 443

   b. *Rule 2:* (Default rule is to allow all traffic within the security group) (This rule will be used for multiple Cloud Network Controllers in the future as a cluster. Currently this rule is not used as there is only one controller NIC is attached to the security group.)

      Source: uni/tn-infra/cloudapp-cloud-infra/cloudepg-controllers

      Destination: Cloud Network Controller

      Protocol- All

      Port- All

c. *Rule 3:* (HTTP access to Cloud Network Controller)

Source: External Network

Destination: Cloud Network Controller

Protocol – TCP

Port – 80

Note This rule is enabled for HTTP access to Cloud Network Controller. HTTP access can be disabled through communication policy in Cloud Network Controller.

d. *Rule 4:*

Source: External Network

Destination: Cloud Network Controller

Protocol – ICMP

Port – All

e. *Rule 5:* (Kafka Rule)

Source: External Network

Destination: Cloud Network Controller

Protocol – TCP

Port – 9095

f. *Rule 6:* (ssh Access to Cloud Network Controller)

Source: External Network

Destination: Cloud Network Controller

Protocol – TCP

Port – 22

Outbound Rules

a. *Rule 1:* (Needed for outbound communication from Cloud Network Controller)

Source: Cloud Network Controller

Destination: 0/0

Protocol- All

Port –All

Note This rule is needed for Cloud Network Controller to access external services like Cisco license server, DNS, NTP.

b. *Rule 2:* (Default rule to allow all traffic within the security group)

Source: Cloud Network Controller

Destination: uni/tn-infra/cloudapp-cloud-infra / cloudepg-controllers

Protocol- All

Port – All

Note This rule is similar to Allow-all inbound rule within the security group as explained above. Currently it is not used.

2. **Security Group**- capic-rCAPICInfra SecurityGroup

   This will be detached from the interface as soon as Cisco Catalyst 8000Vs are deployed and interface will be attached with uni/tn-infra/cloudapp-cloud-infra/cloudepg-controllers-infra-nic with the same set of rules and this security group will be left as is in the cloud.

   Purpose- This security group is attached to Cloud Network Controller infra interface. This will be used for clustering when we support multiple Cloud Network Controller instances.

Note This infra interface is not exposed externally and no elastic IP is attached. All traffic is allowed only within the security group and the VPC. This rule is currenlty not used.

Inbound Rules

a. *Rule 1:*

Source: 0/0

Destination: Cloud Network Controller

Protocol – All

Port – All

Outbound Rules

a. *Rule 1:*

Source: Cloud Network Controller

Destination: 0/0

Protocol – All

Port – All

Rules created for Cloud Network Controller in Home Region Security group- cloudepg-controllers after deploying Cisco Catalyst 8000V in Home and Non Home Region

Note For the **uni/tn-infra/cloudapp-cloud-infra/cloudepg-controllers** security group, the following rules are added in addition to the rules which were deployed during the Cloud Network Controller bringup. These rules are added after deploying Cisco Catalyst 8000V in home and non-home regions. These rules are required for Cloud Network Controller to manage Cisco Catalyst 8000V.

1. **Security Group**- uni/tn-infra/cloudapp-cloud-infra/cloudepg-controllers

   There are no additional Inbound Rules created after Cisco Catalyst 8000V is enabled.

   Outbound Rules

   a. *Rule 1:* (This Rule will be added for each Cisco Catalyst 8000V in non home region.)

   Source: Cloud Network Controller

   Destination: Cisco Catalyst 8000V private IP

   Protocol- TCP

   Port – 22

   b. *Rule 2:* (This Rule will be added per Cisco Catalyst 8000V in each region.)

   Source: Cloud Network Controller

   Destination: /uni/tn-infra/cloudapp-cloud -infra/cloudepg-infra-csr: **< CAT8KV-NAME >**: interface: 3.

   Protocol- All

   Port – All

   c. *Rule 3:* (This Rule will be added for each Cisco Catalyst 8000V in non home region.)

   Source: Cloud Network Controller

   Destination: Cisco Catalyst 8000V private IP

   Protocol- TCP

   Port- 830

   d. *Rule 4:* (This rule is created one per non home region Cisco Catalyst 8000V)

   Source: Cloud Network Controller

   Destination: Non home region Cisco Catalyst 8000V private IP

   Protocol- All

   Port- All

   e. *Rule 5:*

   Source: Cloud Network Controller

   Destination: /uni/tn-infra/cloudapp-cloud-infra/cloudepg-infra -routers

   Protocol- TCP

Port- 830

f. *Rule 6:*

Source: Cloud Network Controller

Destination: /uni/tn-infra/cloudapp-cloud-infra/cloudepg-infra- routers

Protocol- TCP

Port- 22

2. **Security Group**- capic-uni/tn-infra/cloudapp-cloud -infra/ cloudepg-controllers-infra-nic

Purpose- This security group is attached to Cloud Network Controller infra interface.

Note This interface is not exposed externally and no elastic IP is attached. All traffic is allowed only within the security group and the VPC.

Inbound Rules

a. *Rule 1:* (Cloud Network Controller: Default rule)

Source: /uni/tn-infra/cloudapp-cloud-infra/cloudepg-controllers- infra -nic

Destination: Cloud Network Controller

Protocol – All

Port – All

Outbound Rules

a. *Rule 1:*

Source: Cloud Network Controller

Destination: /uni/tn-infra/cloudapp-cloud -infra/cloudepg-controllers-infra-nic

Protocol – All

Port – All

Security Group and rules created in Home Region for Cisco Catalyst 8000V

1. **Security Group**- uni/tn-infra/cloudapp-cloud-infra/cloudepg-infra-routers

Inbound Rules

a. *Rule 1:*

Source: /uni/ tn-infra/cloudapp-cloud-infra/cloudepg-controllers

Destination: Cisco Catalyst 8000V

Protocol – TCP

Port – 22

b. *Rule 2:* (Netconf)

Source: Cloud Network Controller public IP

Destination: Cisco Catalyst 8000V

Protocol- TCP

Port- 830

c. *Rule 3:* (This is created one per non home region Cisco Catalyst 8000V.)

Source: Remote Cisco Catalyst 8000V private IP

Destination: Cisco Catalyst 8000V

Protocol – All

Port- All

d. *Rule 4:*

Source: External Network

Destination: Cisco Catalyst 8000V

Protocol- TCP

Port- 22

e. *Rule 5:*

Source: External Network

Destination: Cisco Catalyst 8000V

Protocol- TCP

Port- 80

f. *Rule 6:*

Source: External Network

Destination: Cisco Catalyst 8000V

Protocol- TCP

Port- 443

g. *Rule 7:*

Source: Cloud Network Controller public IP

Destination: Cisco Catalyst 8000V

Protocol- TCP

Port- 22

h. *Rule 8:*

Source: External Network

Destination: Cisco Catalyst 8000V

Protocol- ICMP

i. *Rule 9:* (This rule is needed to enable communication between the Cisco Catalyst 8000Vs.)

Source: /uni/tn -infra/cloudapp-cloud-infra/cloudepg-infra-routers

Destination: Cisco Catalyst 8000V

Protocol- All

Port- All

j. *Rule 10:*

Source: /uni/tn-infra/cloudapp-cloud-infra/cloudepg-controllers

Destination: Cisco Catalyst 8000V

Protocol- TCP

Port- 830

Outbound Rules

a. *Rule 1:* (This rule is created for two interfaces with private IP per Cisco Catalyst 8000V in non home region.)

Source: Cisco Catalyst 8000V

Destination: Remote (non home region) Cisco Catalyst 8000V private IP

Protocol- All

Port- All

b. *Rule 2:* (This rule is created one per Cisco Catalyst 8000V (both home and non home region) interface 3- Gig4.)

Source: Cisco Catalyst 8000V

Destination: /uni/tn-infra/cloudapp-cloud/-infra/cloudepg-infra-csr: **<CAT8KV_NAME>**: interface: 3

Protocol – All

Port -All

c. *Rule 3:*

Source: Cisco Catalyst 8000V

Destination: /uni/tn-infra/cloudapp-cloud-infra/cloudepg-infra-routers

Protocol- All

Port- All

d. *Rule 4:*

Source: Cisco Catalyst 8000V

Destination: 0.0.0.0/0

Protocol- All

Port- All

e. *Rule 5:* (One rule is created for each gig4 interface private IP address of remote region Cisco Catalyst 8000Vs)

Source: Cisco Catalyst 8000V

Destination: Remote region Cisco Catalyst 8000V Gig4 (Interface-3) private IP

2. **Security Group**- uni/tn-infra/cloudapp-cloud -infra/cloudepg-infra-csr: <**CAT8KV_NAME**_NONHOME>: interface: 2

Note One security group is created per non home region Cisco Catalyst 8000V interface 2. This security group is not being used currently and has been created for future purposes.

Inbound Rules

a. *Rule 1:*(One Per non home region Cisco Catalyst 8000V)

Source: Non home region Cisco Catalyst 8000V Interface 2private IP

Protocol- All

Port – All

b. *Rule 2:* (This is created one per Cisco Catalyst 8000V)

Source: uni/tn-infra /cloudapp -cloud- infra/ cloudepg- infra-csr:**<CAT8KV_NAME>**: interface: 2

Protocol- All

Port- All

3. **Security Group**- uni/tn-dummy/cloudapp-dummy/cloudepg-CAPIC_INTERNAL_EP_SG_DEFAULT

Purpose- Unused security group created in infra. Default security group to place the endpoint until it gets segmented to EPG.

4. **Security Group**- uni/tn-infra/cloudapp-cloud-infra/cloudepg-infra-csr:<**CAT8KV_NAME**>: interface: 3

Note One Security Group is created for each home region Catalyst 8000V interface3 (Gig4). It is attached to the respective local region Cisco Catalyst 8000V interface 3(Gig4).

Inbound Rules

a. *Rule 1:*(There will be 8 such rules)

Source: Private IP of remote Cisco Catalyst 8000V (One per interface in each remote Cisco Catalyst 8000V)

Protocol- All

Port- All

b. *Rule 2:* (This is created one per Cisco Catalyst 8000V)(As there are two Cisco Catalyst 8000Vs per interface, there will be 4 such rules.)

Source: uni/tn-infra /cloudapp -cloud- infra/ cloudepg- infra-csr:**<HOME and NON HOME REGION CAT8KV_NAME>**: interface: 1

Protocol- All

Port- All

c. *Rule 3:* (This is created one per Cisco Catalyst 8000V)(As there are two Cisco Catalyst 8000Vs per interface, there will be 4 such rules.)

Source: /uni/tn-infra/ cloudapp-cloud-infra/cloudepg-infra-csr<<**HOME and NON HOME REGION CAT8KV_NAME>**>: interface: 2

Protocol- All

Port- All

d. *Rule 4:* (This is created one per Cisco Catalyst 8000V)(As there are two Cisco Catalyst 8000Vs per interface, there will be 4 such rules.)

Source: /uni/tn-infra/cloudapp-cloud-infra/cloudepg-infra-csr<<**HOME and NON HOME REGION CAT8KV_NAME>**: interface: 3

Protocol- All

Port- All

e. *Rule 5:*

Source: /uni/tn-infra/cloudapp-cloud-infra/cloudepg-infra-routers

Protocol- All

Port- All

f. *Rule 6:*

Source: /uni/tn-infra/cloudapp-cloud-infra/ cloudepg-controllers

Protocol- All

Port- All

Outbound Rules

a. *Rule 1:*

Destination: External Network

Protocol – All

Port- All

b. *Rule 2:*

Destination: Remote Cisco Catalyst 8000V private IP of Interface 3 (Gig4) (One per Cisco Catalyst 8000V in Non Home Region)

Protocol- All

Port- All

c. *Rule 3:* (Created one per Cisco Catalyst 8000V in both home and non home region)

Source: /uni/tn -infra/ cloudapp -cloud -infra/ cloudepg -infra -csr**:<CAT8KV_NAME >**: interface: 3

Protocol- All

Port- All

5. **Security Group**- uni/tn-infra/cloudapp-cloud-infra/cloudepg-infra-csr:<**CAT8KV_NAME**>: interface: 2 (One per Cisco Catalyst 8000V)

   Inbound Rules

   a. *Rule 1:* (This is created one per Cisco Catalyst 8000V)

      Source: /uni/tn-infra/ cloudapp-cloud-infra/cloudepg- infra-csr:<**CAT8KV_NAME**>:Interface: 2

      Protocol- All

      Port- All

   b. *Rule 2:* (This is created one per remote region Cisco Catalyst 8000V)

      Source: Remote Private IP of Cisco Catalyst 8000V

      Protocol- All

      Port- All

   Outbound Rules

   a. *Rule 1:*

      Destination: Remote Cisco Catalyst 8000V of interface 2 (Gig3) and interface 3 (Gig4) private IP

      Protocol – All

      Port- All

   b. *Rule 2:* (This rule will be added for both home region and non home region Cisco Catalyst 8000Vs.)

      Destination: uni/tn-infra/ cloudapp-cloud -infra/ cloudepg-infra- csr:**<CAT8KV_NAME>**: interface: 2

      Protocol- All

      Port- All

   c. *Rule 3:* (This rule will be added for both home region and non home region Cisco Catalyst 8000Vs.)

      Destination: uni/tn-infra/ cloudapp-cloud -infra/ cloudepg-infra- csr:**<CAT8KV_NAME>**: interface: 3

      Protocol- All

      Port- All

   d. *Rule 4:*

      Destination: 0/0

      Protocol- All

      Port- All

6. **Security Group**- uni/tn-infra/cloudapp-cloud-infra/cloudepg-infra-csr:<**CAT8KV_NAME**>: interface: 1 (One per Cisco Catalyst 8000V)

   Inbound Rules

a. *Rule 1:*(One rule is created for each Cisco Catalyst 8000V Interface 1 including home and non home regions Cisco Catalyst 8000Vs.)

   Source: /uni/tn-infra/ cloudapp-cloud-infra/cloudepg- infra-csr:<**CAT8KV_NAME**>:Interface: 1

   Protocol- All

   Port- All

b. *Rule 2:*(This is created one per remote region Cisco Catalyst 8000V)

   Source: Remote Private IP of remote region Cisco Catalyst 8000V Interface1(Gig2)

   Protocol- All

   Port- All

Outbound Rules

a. *Rule 1:*

   Destination: Remote region Cisco Catalyst 8000V private IP of interface 3 (Gig4) and interface 1 (Gig2)

   Protocol – All

   Port- All

b. *Rule 2:*

   Destination: uni/tn-infra/ cloudapp-cloud -infra/ cloudepg-infra- csr:**<CAT8KV_NAME>**: interface: 1

   Protocol- All

   Port- All

c. *Rule 3:*

   Destination: uni/tn-infra/ cloudapp-cloud -infra/ cloudepg-infra- csr:**<CAT8KV_NAME>**: interface: 3

   Protocol- All

   Port- All

d. *Rule 4:*

   Destination: 0/0

   Protocol- All

   Port- All

In any non-home region Cisco Catalyst 8000V, Security Group and the rules are similar as described in the above section for home region with the following exception- Instead of using security group as destination, some rules would have specific IP address of Cloud Network Controller.

Security Group and Rules