Intra-EPG Isolation Enforcement for Cisco ACI Virtual Edge

By default, endpoints with an EPG can communicate with each other without any contracts in place. However, you can isolate endpoints within an EPG from each other. For example, you may want to enforce endpoint isolation within an EPG to prevent a VM with a virus or other problem from affecting other VMs in the EPG.

You can configure isolation on all or none of the endpoints within an application EPG; you cannot configure isolation on some endpoints but not on others.

Isolating endpoints within an EPG does not affect any contracts that enable the endpoints to communicate with endpoints in another EPG.

Note Enforcing intra-EPG Isolation is not supported for the EPG that is associated with Cisco ACI Virtual Edge domains in VLAN mode. If you try to enforce intra-EPG isolation with such an EPG, a fault is triggered.

Note Using intra-EPG isolation on a Cisco ACI Virtual Edge microsegment (uSeg) EPG is not currently supported.

Note Proxy ARP is not supported for Cisco ACI Virtual Edge EPGs using VXLAN encapsulation and on which intra-EPG Isolation is enforced. Therefore, intra-subnet communication is not possible between intra-EPG isolated EPGs even though contracts are in place between those Cisco ACI Virtual Edge EPGs. (VXLAN).

- View Statistics for Isolated Endpoints on Cisco ACI Virtual Edge Under the Virtual Networking Tab, on page 6

Configure Intra-EPG Isolation for Cisco ACI Virtual Edge Using the GUI

Follow this procedure to create an EPG in which the endpoints of the EPG are isolated from each other.

The port that the EPG uses must belong to one of the VM Managers (VMMs).

Note This procedure assumes that you want to isolate endpoints within an EPG when you create the EPG. If you want to isolate endpoints within an existing EPG, select the EPG in Cisco APIC, and in the **Properties** pane, in the **Intra EPG Isolation** area, choose **Enforced**, and then click **SUBMIT**.

Before you begin

Make sure that VXLAN-related configuration is present on the Cisco ACI Virtual Edge VMM domain, particularly a Cisco ACI Virtual Edge fabric-wide multicast address and pool of multicast addresses (one per EPG).

Procedure

Step 1 Log in to Cisco APIC.

Step 2 Choose **Tenants**, expand the folder for the tenant, and then expand the **Application Profiles** folder.

Step 3 Right-click an application profile, and choose **Create Application EPG**.

Step 4 In the **Create Application EPG** dialog box, complete the following steps:

a) In the **Name** field, enter the EPG name.
b) In the **Intra EPG Isolation** area, click **Enforced**.
c) From the **Bridge Domain** drop-down list, choose the bridge domain.
d) Check the **Associate to VM Domain Profiles** check box.
e) Click **Next**.
f) In the **Associate VM Domain Profiles** area, complete the following steps:

- Click the + (plus) icon, and from the **Domain Profile** drop-down list, choose the desired Cisco ACI Virtual Edge VMM domain.
- From the **Switching Mode** drop-down list, choose **AVE**.
- From the **Encap Mode** drop-down list, choose **VXLAN** or **Auto**.

  If you choose **Auto**, make sure that encapsulation mode of the Cisco ACI Virtual Edge VMM domain is VXLAN.
- (Optional) Choose other configuration options appropriate to your setup.

g) Click **Update** and click **Finish**.

What to do next

You can select statistics and view them to help diagnose problems involving the endpoint. See the sections Choose Statistics for Isolated Endpoints on Cisco ACI Virtual Edge Under the Tenants Tab, on page 5 and View Statistics for Isolated Endpoints on Cisco ACI Virtual Edge Under the Tenants Tab, on page 6 in this guide.

Configure Intra-EPG Isolation for Cisco ACI Virtual Edge Using the NX-OS Style CLI

Before you begin

Make sure that VXLAN-related configuration is present on the Cisco ACI Virtual Edge VMM domain, particularly a Cisco ACI Virtual Edge fabric-wide multicast address and pool of multicast addresses (one per EPG).

Procedure

In the CLI, create an intra-EPG isolation EPG:

Example:

```
# Command: show running-config tenant Tenant2 application AP-1 epg EPG-61
  tenant Tenant2
    application AP-1
      epg EPG-61
        bridge-domain member BD-61
        vmware-domain member D-AVE-SITE-2-3
          switching-mode AVE
          encap-mode vxlan
          exit
        isolation enforce            # This enables EPG into isolation mode.
        exit
      exit
    exit
```

What to do next

You can select statistics and view them to help diagnose problems involving the endpoint. See the sections Choose Statistics for Isolated Endpoints on Cisco ACI Virtual Edge Under the Tenants Tab, on page 5 and View Statistics for Isolated Endpoints on Cisco ACI Virtual Edge Under the Tenants Tab, on page 6 in this guide.

Configure Intra-EPG Isolation for Cisco ACI Virtual Edge Using the REST API

Before you begin

Make sure that VXLAN-related configuration is present on the Cisco ACI Virtual Edge VMM domain, particularly a Cisco ACI Virtual Edge fabric-wide multicast address and pool of multicast addresses (one per EPG).

Procedure

Step 1 Send this HTTP POST message to deploy the application using the XML API.

Example:

```
   POST
https://10.197.139.36/api/mo/uni/tn-Tenant2.xml
```

Step 2 For a VMM deployment, include the XML structure in the following example in the body of the POST message.

Example:

```
<fvTenant name="Tenant2" >
  <fvAp name="AP-1">
    <fvAEPg name="EPG-61" pcEnfPref="enforced">
      <!-- pcEnfPref="enforced" ENABLES ISOLATION-->
      <!-- pcEnfPref="unenforced" DISABLES ISOLATION-->
        <fvRsBd tnFvBDName="BD-61" />
        <fvRsDomAtt switchingMode="AVE" encapMode="vxlan" resImedcy="immediate"
tDn="uni/vmmp-VMware/dom-D-AVE-SITE-1-XXIII" >
        </fvRsDomAtt>
    </fvAEPg>
  </fvAp>
</fvTenant>
```

What to do next

You can select statistics and view them to help diagnose problems involving the endpoint. See the sections Choose Statistics for Isolated Endpoints on Cisco ACI Virtual Edge Under the Tenants Tab, on page 5 and View Statistics for Isolated Endpoints on Cisco ACI Virtual Edge Under the Tenants Tab, on page 6 in this guide.

Choose Statistics for Isolated Endpoints on Cisco ACI Virtual Edge

Choose Statistics for Isolated Endpoints on Cisco ACI Virtual Edge Under the Tenants Tab

If you configured intra-EPG isolation on a Cisco ACI Virtual Edge, choose statistics—such as denied connections, received packets, or transmitted multicast packets—for the endpoints. You can then view the statistics.

Procedure

Step 1 Log in to Cisco APIC.

Step 2 Choose **Tenants** > ***tenant***.

Step 3 In the tenant navigation pane, expand the **Application Profiles**, ***profile***, and **Application EPGs** folders, and then choose the EPG containing the endpoint the statistics for which you want to view.

Step 4 In the EPG **Properties** work pane, click the **Operational** tab to display the endpoints in the EPG.

Step 5 Double-click the endpoint.

Step 6 In the **Properties** dialog box for the endpoint, click the **Stats** tab and then click the check icon.

Step 7 In the **Select Stats** dialog box, in the **Available** pane, choose the statistics that you want to view for the endpoint, and then use the right-pointing arrow to move them into the **Selected** pane.

Step 8 Click **Submit**.

Choose Statistics for Isolated Endpoints on Cisco ACI Virtual Edge Under the Virtual Networking Tab

If you configured intra-EPG isolation on a Cisco ACI Virtual Edge, choose statistics—such as denied connections, received packets, or transmitted multicast packets—for the endpoints. You can then view the statistics.

Procedure

Step 1 Log in to Cisco APIC.

Step 2 Choose **Virtual Networking** > **Inventory** > **VMM Domains** > **VMware** > ***VMM domain*** > **Controllers** > ***controller instance name*** > ***DVS-VMM name*** > **Portgroups** > ***EPG name*** > ***Learned Point MAC address (node)*** > **.**

Step 3 Click the **Stats** tab.

Step 4 Click the tab with the check mark.

Step 5 In the **Select Stats** dialog box, click the statistics that you want to view in the **Available** pane, and then click the arrow pointing right to put them in the **Selected** pane.

Step 6 (Optional) Choose a sampling interval.

Step 7 Click **Submit**.

View Statistics for Isolated Endpoints on Cisco ACI Virtual Edge

View Statistics for Isolated Endpoints on Cisco ACI Virtual Edge Under the Tenants Tab

If you configured intra-EPG isolation on a Cisco ACI Virtual Edge, once you have chosen statistics for the endpoints, you can view them.

Before you begin

You must have chosen statistics to view for isolated endpoints. See Choose Statistics for Isolated Endpoints on Cisco ACI Virtual Edge Under the Tenants Tab, on page 5 in this guide for instructions.

Procedure

Step 1 Log in to Cisco APIC.

Step 2 Choose **Tenants** > ***tenant***.

Step 3 In the tenant navigation pane, expand the **Application Profiles**, ***profile***, and **Application EPGs** folders, and then choose the EPG containing the endpoint with statistics that you want to view.

Step 4 In the EPG **Properties** work pane, click the **Operational** tab to display the endpoints in the EPG.

Step 5 Double-click the endpoint with statistics that you want to view.

Step 6 In the **Properties** work pane for the endpoint, click the **Stats** tab.

The work pane displays the statistics that you chose earlier. You can change the view by clicking the table view or chart view icon on the upper left side of the work pane.

View Statistics for Isolated Endpoints on Cisco ACI Virtual Edge Under the Virtual Networking Tab

If you configured intra-EPG isolation on a Cisco ACI Virtual Edge, once you have chosen statistics for the endpoints, you can view them.

Before you begin

You must have chosen statistics to view for isolated endpoints. See Choose Statistics for Isolated Endpoints on Cisco ACI Virtual Edge Under the Tenants Tab, on page 5 in this guide for instructions.

Procedure

Step 1 Log in to Cisco APIC.

Step 2 Choose **Virtual Networking** > **Inventory** > **VMM Domains** > **VMware** > ***VMM name*** > **Controllers** > **controller instance name** > ***DVS-VMM name*** > **Portgroups** > ***EPG name*** > ***Learned Point MAC address (node)***

Step 3 Click the **Stats** tab.

The central pane displays the statistics that you chose earlier. You can change the view by clicking the table view or chart view icon on the upper left side of the work pane.