



Intra-EPG Isolation Enforcement and Cisco ACI

This chapter contains the following sections:

- [Intra-EPG Isolation for VMware VDS or Microsoft Hyper-V Virtual Switch, on page 1](#)

Intra-EPG Isolation for VMware VDS or Microsoft Hyper-V Virtual Switch

Intra-EPG Isolation is an option to prevent physical or virtual endpoint devices that are in the same base EPG or microsegmented (uSeg) EPG from communicating with each other. By default, endpoint devices included in the same EPG are allowed to communicate with one another. However, conditions exist in which total isolation of the endpoint devices from one another within an EPG is desirable. For example, you may want to enforce intra-EPG isolation if the endpoint VMs in the same EPG belong to multiple tenants, or to prevent the possible spread of a virus.

A Cisco ACI virtual machine manager (VMM) domain creates an isolated PVLAN port group at the VMware VDS or Microsoft Hyper-V Virtual Switch for each EPG that has intra-EPG isolation enabled. A fabric administrator specifies primary encapsulation or the fabric dynamically specifies primary encapsulation at the time of EPG-to-VMM domain association. When the fabric administrator selects the VLAN-pri and VLAN-sec values statically, the VMM domain validates that the VLAN-pri and VLAN-sec are part of a static block in the domain pool.

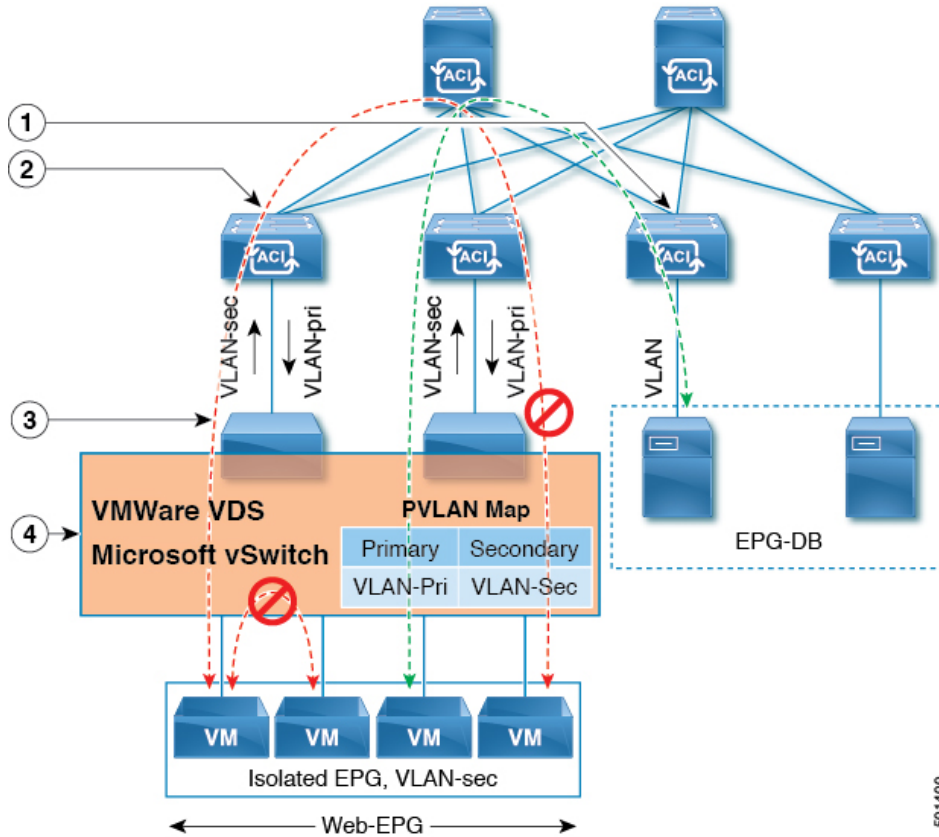


Note When intra-EPG isolation is not enforced, the VLAN-pri value is ignored even if it is specified in the configuration.

VLAN-pri/VLAN-sec pairs for the VMware VDS or Microsoft Hyper-V Virtual Switch are selected per VMM domain during the EPG-to-domain association. The port group created for the intra-EPG isolation EPGs uses the VLAN-sec tagged with type set to `PVLAN`. The VMware VDS or the Microsoft Hyper-V Virtual Switch and fabric swap the VLAN-pri/VLAN-sec encapsulation:

- Communication from the Cisco ACI fabric to the VMware VDS or Microsoft Hyper-V Virtual Switch uses VLAN-pri.
- Communication from the VMware VDS or Microsoft Hyper-V Virtual Switch to the Cisco ACI fabric uses VLAN-sec.

Figure 1: Intra-EPG Isolation for VMware VDS or Microsoft Hyper-V Virtual Switch



Note these details regarding this illustration:

1. EPG-DB sends VLAN traffic to the Cisco ACI leaf switch. The Cisco ACI egress leaf switch encapsulates traffic with a primary VLAN (PVLAN) tag and forwards it to the Web-EPG endpoint.
2. The VMware VDS or Microsoft Hyper-V Virtual Switch sends traffic to the Cisco ACI leaf switch using VLAN-sec. The Cisco ACI leaf switch drops all intra-EPG traffic because isolation is enforced for all intra VLAN-sec traffic within the Web-EPG.
3. The VMware VDS or Microsoft Hyper-V Virtual Switch VLAN-sec uplink to the Cisco ACI Leaf is in isolated trunk mode. The Cisco ACI leaf switch uses VLAN-pri for downlink traffic to the VMware VDS or Microsoft Hyper-V Virtual Switch.
4. The PVLAN map is configured in the VMware VDS or Microsoft Hyper-V Virtual Switch and Cisco ACI leaf switches. VM traffic from WEB-EPG is encapsulated in VLAN-sec. The VMware VDS or Microsoft Hyper-V Virtual Switch denies local intra-WEB EPG VM traffic according to the PVLAN tag. All intra-ESXi host or Microsoft Hyper-V host VM traffic is sent to the Cisco ACI leaf using VLAN-Sec.

Related Topics

For information on configuring intra-EPG isolation in a Cisco ACI Virtual Edge environment, see the chapter "Intra-EPG Isolation Enforcement for Cisco ACI Virtual Edge" in the [Cisco ACI Virtual Edge Configuration Guide](#).

For information on configuring intra-EPG isolation in a Cisco AVS environment, see the chapter "Intra-EPG Isolation Enforcement for Cisco AVS" in the [Cisco Application Virtual Switch Configuration Guide](#).

Configuring Intra-EPG Isolation for VMware VDS or Microsoft Hyper-V Virtual Switch using the GUI

Procedure

- Step 1** Log into Cisco APIC.
- Step 2** Choose **Tenants** > *tenant*.
- Step 3** In the left navigation pane expand the **Application Profiles** folder and appropriate application profile.
- Step 4** Right-click the **Application EPGs** folder and then choose **Create Application EPG**.
- Step 5** In the **Create Application EPG** dialog box, complete the following steps:
- In the **Name** field, add the EPG name.
 - In the **Intra EPG Isolation** area, click **Enforced**.
 - In the **Bridge Domain** field, choose the bridge domain from the drop-down list.
 - Associate the EPG with a bare metal/physical domain interface or with a VM Domain.
 - For the VM Domain case, check the **Associate to VM Domain Profiles** check box.
 - For the bare metal case, check the **Statically Link with Leaves/Paths** check box.
 - Click **Next**.
 - In the **Associated VM Domain Profiles** area, click the + icon.
 - From the **Domain Profile** drop-down list, choose the desired VMM domain.
- For the static case, in the **Port Encap (or Secondary VLAN for Micro-Seg)** field, specify the secondary VLAN, and in the **Primary VLAN for Micro-Seg** field, specify the primary VLAN. If the Encap fields are left blank, values will be allocated dynamically.
- Note** For the static case, a static VLAN must be available in the VLAN pool.
- Step 6** Click **Update** and click **Finish**.
-

