Overview

Prerequisites

Before you follow the procedures described in this document, you must have the following basic configuration already completed:

- Nexus Dashboard cluster deployed and ready.

  This is described in detail in *Cisco Nexus Dashboard Deployment Guide* for your release.

- One or more cloud sites onboarded in the Nexus Dashboard.

  This is described in detail in *Cisco Nexus Dashboard User Guide* for your release.

- Nexus Dashboard Orchestrator, Release 3.5(1) or later installed and enabled.

  This is described in detail in *Cisco Nexus Dashboard Orchestrator Deployment Guide* for your release.

- The cloud sites enabled for management in the Orchestrator service and basic infra configuration completed.

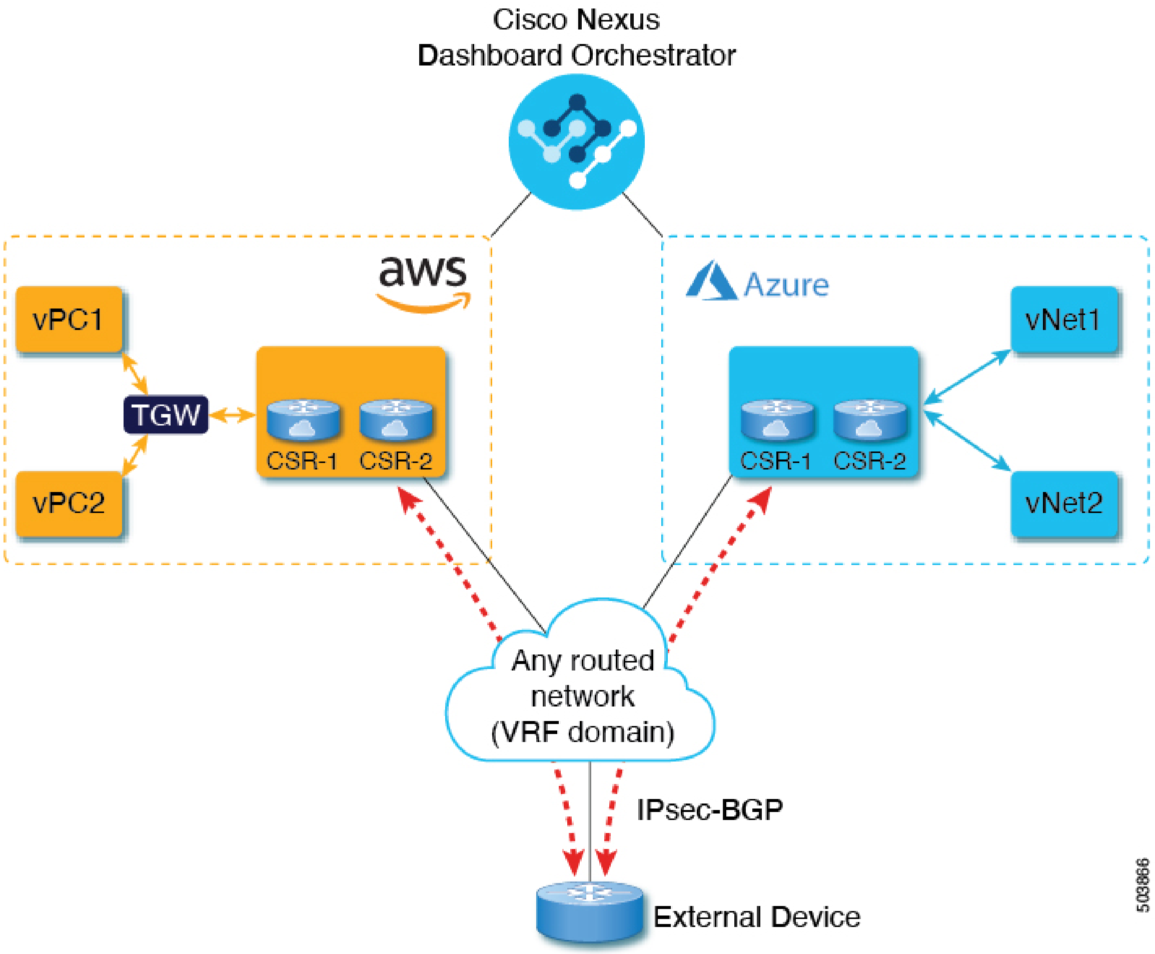
  This is described in detail in *Cisco Nexus Dashboard Orchestrator Configuration Guide for ACI Fabrics* for your release.

BGP IPv4 External Connectivity Overview

As you already know, Nexus Dashboard Orchestrator allows you to configure infrastructure for intersite connectivity between multiple sites. Connectivity is established between any two sites, including the on-premises Cisco ACI and Cloud ACI sites, using BGP-EVPN. This approach however, was not suitable for cases where the deployment domain contains one or more external networks that you want to configure and manage through the Orchestrator.

Beginning with Release 3.5(1), Nexus Dashboard Orchestrator allows you to connect one or more Cisco Cloud ACI sites to one or more external routers, which are outside your Nexus Dashboard Orchestrator domain and not managed by the Orchestrator, but to which you want to establish connectivity from endpoints in your sites.

This connectivity is established by connecting the cloud site's CSRs to the external routers and once the connectivity is established, creating route leak configurations to allow subnets from the external devices to establish connectivity with the cloud site's VRFs. A more detailed configuration workflow is described below and illustrated in the following diagram:



The following terminology is used throughout this document:

- **External devices**—any device that resides outside the Cloud ACI domain and is capable of creating IPsec tunnels and BGP peering to the cloud sites' CSRs.

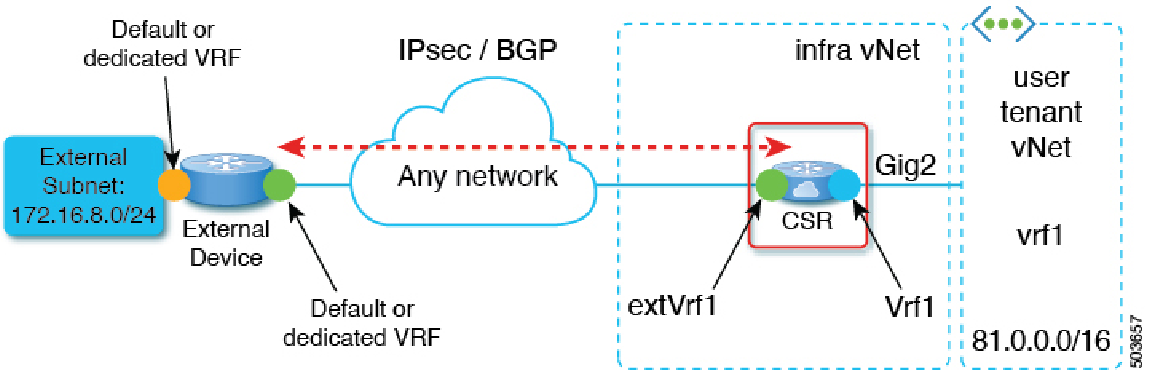
  The existing external connectivity model is extended to provide connectivity from AWS CSRs to any non-ACI external device. BGP IPv4 sessions are created on an external VRF from the infra VPC CSRs to these non-ACI external devices, and inter-VRF routing is set up between the external VRF and the site local VRFs.

- **External VRF**—a unique VRF that does not have any presence in the cloud but is associated with one or more external networks. As opposed to an internal VRF, which is a VRF that is used to host the VPCs and is associated with a cloud context profile, an external VRF is not referred to in any cloud context profile used by Cisco Cloud APIC.

  An external VRF represents an external network that is connected to other cloud sites or to on-premises branch offices. Multiple cloud VRFs can leak routes to an external VRF or can get the routes from an external VRF. When an external network is created on an external VRF, all routes coming from the external devices which are part of the external network are received over the external VRF.

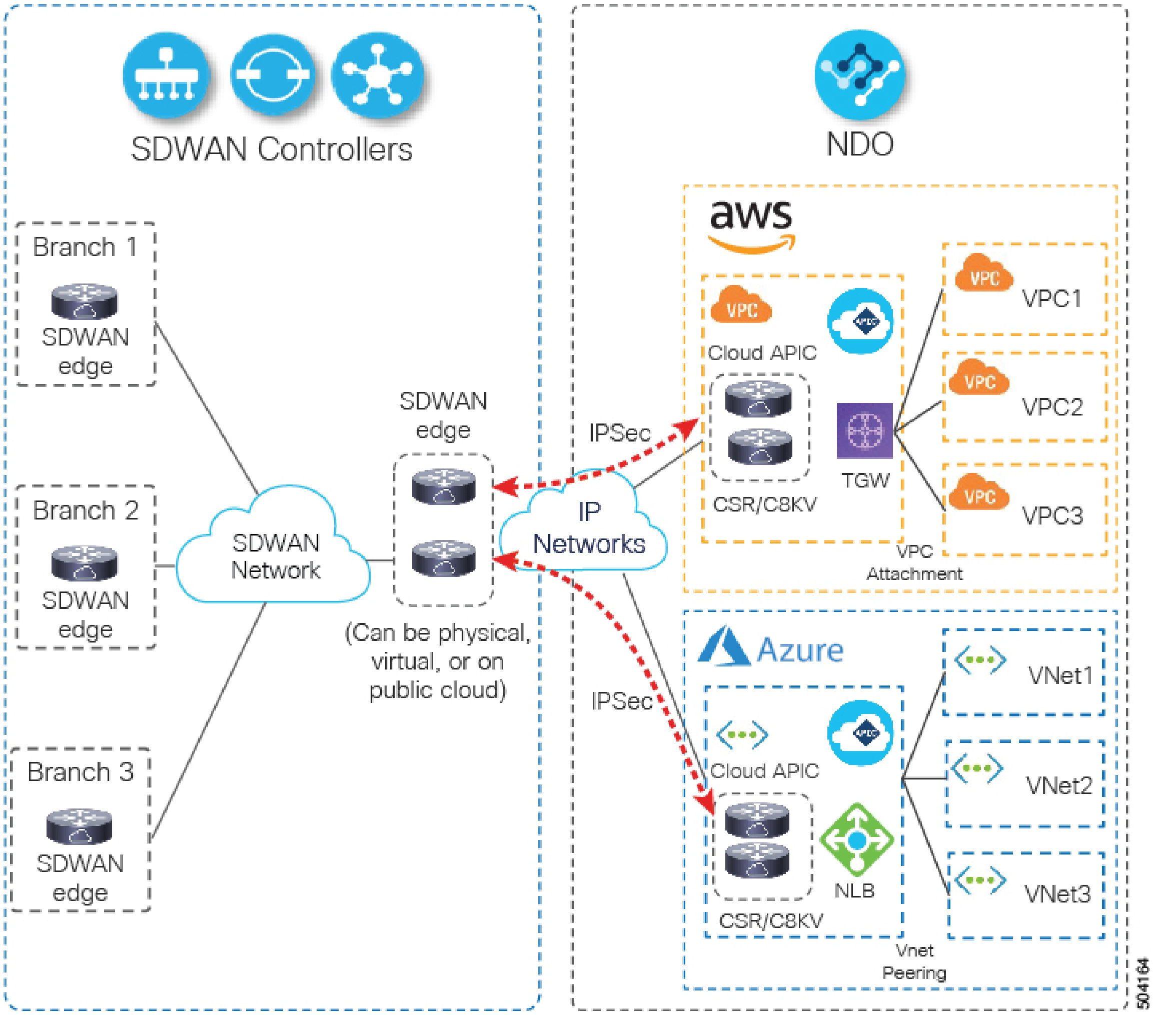
- **Internal VRF**—any cloud VRF where the cloud workloads are deployed and managed by the Cloud APIC.

The following topology diagram and summary describe the connectivity between a cloud VRF and an external destination represented by an external VRF over the IPsec tunnel between the cloud CSR and an external device. While the diagram is Azure-specific, the same principle applies for AWS sites with each cloud site being able to connect to one or more external devices independently. Note that the external connectivity using BGP IPv4 does not change the inter-site connectivity between managed Cloud APIC sites, which continues to use VXLAN EVPN.



- External network to cloud:
  - In external VRF (`extVrf1`), CSR establishes a BGP adjacency to the external device over the IPsec tunnel
  - CSR learns the external subnet (`172.16.8.0/24`) in `extVrf1` through eBGP
  - On CSR, the external subnet (`172.16.8.0/24`) is leaked from `extVrf1` to the user tenant `vrf1`
- Cloud to external network:
  - In `extVrf1`, CSR advertises the cloud prefixes to the external device via BGP

One of the ways this functionality can be used is to establish connectivity between a Cloud ACI fabric and SDWAN as shown in the following diagram, with the SDWAN devices deployed in the Cloud essentially becoming the external routers:



The following sections describe two main use cases for this feature:

- Brand new external connectivity configuration directly from the Nexus Dashboard Orchestrator.

  This is described in Configuring External Connectivity and consists of the following workflow:

  - Creating external VRFs in the cloud site's Infra tenant
  - Providing information about the external devices in the Orchestrator GUI
  - Configuring sites' external connectivity to those devices
  - Deploying infra configuration to the sites, which will allow them to connect to the external devices
  - Deploying configuration to the external devices, which will allow them to connect to the cloud sites' CSRs
  - Configuring route leaking between the external VRF and any existing cloud VRFs in the cloud site
  - Creating an external EPG, which will contain the endpoints in the external network
  - Establishing a contract between the external EPG and an existing cloud EPG associated to a cloud VRF to allow traffic to flow between the cloud endpoints and the external subnets

- Importing existing configuration which was previously configured directly in the Cloud APIC to be managed by the Nexus Dashboard Orchestrator.

  In this case an existing Cloud APIC site with all existing configurations done directly through the Cloud APIC is added to Nexus Dashboard to be managed by Nexus Dashboard Orchestrator. This is described in Importing Existing External Connectivity Configuration and consists of the following workflow:

  - Adding an existing Cloud APIC site to the Nexus Dashboard and enabling the Nexus Dashboard Orchestrator to manage it
  - Importing an existing user tenant from the cloud site
  - Importing an existing external VRF and external EPG
  - Importing an existing cloud VRF and route leak configurations

Guidelines and Limitations

The following guidelines apply when using inter-VRF route leaking between external and cloud VRFs:

- Route leaking must be configured between an internal VRF and the external VRF in both directions.
- You cannot configure "smaller" prefixes to be leaked while a "larger" prefix is already being leaked.

  For example, attempting to add the `10.10.10.0/24` prefix when you already have the `10.10.0.0/16` prefix configured will be rejected. Similarly, if you configure the `0.0.0.0/0` prefix (leak all), no other prefix will be allowed.
- Contracts are not allowed between external EPGs.
- An external VRF cannot be used for creating cloud EPGs.
- An external VRF always belongs to the infra tenant.
- Route leaking is not supported between external VRFs.