Cisco SD-WAN Cloud onRamp for Multicloud using Google Cloud Platform

Prescriptive Deployment Guide

Nov, 2021

© 2020 Cisco and/or its affiliates. All rights reserved.

Contents

© 2020 Cisco and/or its affiliates. All rights reserved.

Introduction

About the Guide

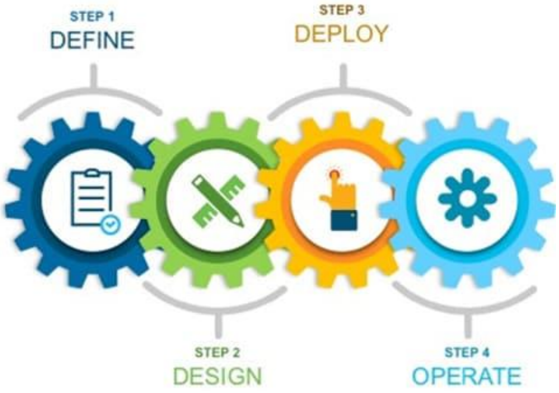
This document discusses the design and deployment of Cisco SD-WAN Cloud onRamp for Multicloud using Google Cloud Platform (GCP). This guide focuses on the design and configuration of the Site to Google Cloud connectivity and the site-to-site connectivity through Google global network. The document includes some of the best practices and steps to instantiate a pair of Cisco Catalyst 8000v instances within a Google cloud gateway(s), association of Google Host VPCs within tags, establishment of Intra-tag communication, mapping of tags to service side VPN along with necessary design and steps to allow the site-to-site communication via the Google Global Network.

This guide assumes that the Cisco SD-WAN controllers are already deployed and integrated into the vManage NMS controller, the WAN Edge devices are deployed, and the Cisco SD-WAN overlay network is successfully established. This guide is written based on the configuration supported in 20.5/17.5 release. Refer to Appendix B to view the device models and software versions used in this deployment and refer to Appendix C for the Catalyst 8000v CLI configuration used in the deployment

This document contains four major sections:

- The Define section introduces the Cisco Cloud onRamp for Multi-cloud feature and explains the overall solution, along with the benefits of deploying it.
- The Design section includes the two use cases covered in the guide, along with the design components and considerations for the successful integration of Cisco SD-WAN and Google Cloud.
- The Deploy section includes all the prerequisites and the necessary steps to associate Google cloud with vManage NMS, along with the steps to deploy vManage device templates for the Catalyst8000v devices to be hosted in Google cloud. The section also includes the steps for the automated deployment of pair of Cisco Catalyst 8000V instances in cloud gateways with their interfaces anchored in three different VPCs to support the two use cases presented within the design section.
- The Operate section explains some of the common monitoring and troubleshooting capabilities available within the Cisco vManage for the Cisco Cloud onRamp for Multi-Cloud feature.

Figure 1. **Implementation Flow**



© 2020 Cisco and/or its affiliates. All rights reserved.

Audience

The audience for this document includes network design engineers, network operations personnel, and cloud operations personnel who wish to establish access from branch site to a service hosted in a VPC in Google Cloud or to connect branches across different regions through the GCP global network.

Define - Cisco Cloud onRamp for Multi-Cloud Introduction

Cisco SD-WAN Interconnection with Multi-Cloud

Network engineers in today's world of enterprise IT are beginning to understand the benefits of multicloud fabric for it offers a premium experience when connecting your branch network to workloads and SaaS applications. Enterprise customers now start to adopt more than one cloud. They choose different cloud platforms to deploy different services based on what works best for them. For example, the front-end service could be placed in AWS, while SQL service is provided by Azure and analytics service from Google Cloud Platform (GCP).

The rest of this guide explains some of the Cisco SD-WAN Google cloud connectivity models using Cisco SD-WAN cloud hub. For details regarding Cisco SD-WAN AWS interconnection, refer to the Cisco Cloud OnRamp for IaaS using AWS guide, and for details regarding Cisco SD-WAN Azure interconnection, refer to the Cisco Cloud OnRamp for IaaS using Azure guide.

About the Solution – Cisco SD-WAN Interconnection with Google Cloud

The Cisco SD-WAN Google cloud integration enables network policies, such as Cisco SD-WAN segmentation, to follow network traffic across the boundary between the enterprise network and Google Cloud, for end-to-end control of security, performance, and quality of experience. With this new integration, customers can extend a single point of orchestration and management for their Cisco SD-WAN network to include the underlay offered by Google Cloud backbone.

Using the Cisco Cloud OnRamp for Multi-Cloud feature, you can associate your Google cloud account with Cisco vManage to bring up a pair of redundant Cisco Catalyst 8000V Edge Software (Cisco Catalyst 8000V) in a Google Cloud Gateway. The services hosted in the Google VPCs are discovered and mapped to the service-side VPNs of the Catalyst 8000v Cisco SD-WAN edge devices. Therefore, allowing your on-premises/ cloud hosted SD-WAN sites to access services hosted within the Google platform. This type of Google cloud connectivity model is referred to as Site-to-Cloud (S2C) connectivity. To enable this form of mapping, a site-to-cloud VPC is automatically provisioned in Google cloud using the Cisco multi-cloud solution.

The Cisco Cloud OnRamp for Multi-Cloud solution also enables you to establish communication between two on-premises branches using your Google platform as the underlay. To enable this traffic flow across two sites through Google cloud, you need to have at least two cloud gateways brought up in different Google cloud regions, each containing a pair of Catalyst8000v devices. A site-to-site VPC (S2S VPC) is automatically brought up in each of the Catalyst 8000v devices hosted between the two separate cloud gateways. The Site-to-Site VPC contains the subnets and firewalls associated with the second WAN tunnel interface labeled as private1. IPsec or GRE tunnels are brought up between the Site-to-Site VPC (S2S VPC) in each Catalyst8000v devices located in the cloud gateways, therefore allowing branch networks located in different regions to communicate with each other through this automated WAN tunnel in GCP Global Network. This type of Google cloud connectivity model is referred to as Site-to-Site (S2S) connectivity.

© 2020 Cisco and/or its affiliates. All rights reserved.

Within the Google Cloud Platform (GCP), the following services are used to interconnect the google resources with the on-premises Cisco SD-WAN network.

Table 1. Google Terminology

Google Terminology	Definition
Google Virtual Private Cloud (VPC)	Google VPC is similar to a traditional network that you operate in your own data center, except that its virtualized within Google Cloud. It is a global resource that consists of a list of regional virtual subnetworks so that each VPC network is logically isolated from each other within the google cloud. Each VPC network implements the following: A virtual firewall to control incoming and outgoing traffic directly on the hypervisor, routes to govern the traffic leaving VM instances/ VPC network and forwarding rules to direct traffic to a google cloud resource in a VPC network.
Service Account Keys	A service account key is essentially a public/private key pair. IAM roles applied against the service account key define the privileges a service account key has. The private key associated to your service account is required to associate your Google Account with vManage. The steps to create private key is explained in the deploy section of this guide.
Network Connectivity Center (NCC)	Network Connectivity Center is a hub-and-spoke model for network connectivity management in Google Cloud, that enables you to connect your on-premises SD-WAN branch and data center networks together by using Google's network as a network for data transfer.
Google Cloud Router	Cloud Router is a fully distributed and managed Google Cloud service that programs custom dynamic routes and scales with your network traffic. The Google cloud routers take care of all the underlay routing within the Google domain.
Google Billing ID	Google Billing ID is a unique number assigned to the organization or an individual that the account is registered to.

Note, all the Google IDs needed for the programmatic sign-in access are explained in depth in the Deploy section, along with the necessary steps.

Benefits of Deploying Cisco Cloud onRamp for Multi-Cloud using Google Cloud Platform

Some of the key benefits of deploying the Cloud onRamp feature includes the following:

Table 2. Benefits of deploying cloud OnRamp for multi-cloud solution

Automated Infrastructure in Public Cloud (Extend SD-WAN)	Cisco SD-WAN Cloud onRamp securely extends Cisco SD-WAN's fabric to public cloud environments through a simplified and automated process. By using Cisco SD-WAN Cloud onRamp, customers can reduce the overall time to deploy and connect branch offices to cloud workloads in minutes. It helps enterprises to significantly increase productivity and avoid error-prone, manual processes.
Policy Control (Policy Framework)	Users can fully utilize Cisco SD-WAN capabilities in the cloud. This allows all on-premises data centers and branch locations which are part of the Cisco SD-WAN fabric to leverage features available both on Cisco SD-WAN vManage and within the cloud provider. Some of the features that can be leveraged on Cisco SD-WAN fabric include:

© 2020 Cisco and/or its affiliates. All rights reserved.

	• Using centralized control policy to redirect critical site to site traffic to traverse through the Google cloud platform, while routing non-critical traffic through SD-WAN overlay network. • Embedded security features such as IPS/IDS, Stateful Firewall, AMP, and URL Filtering to protect and filter data traffic as it leaves the on-premises network to access the Internet cloud.
Reduce OPEX (Cost Effective)	Expenses shift from fixed costs for hardware, software, and data center infrastructure to variable costs based on the usage of compute resources available on Google public cloud.

Design - Cisco Cloud onRamp for Multi-Cloud Use Case and Feature Overview

The design section is organized in the following order:

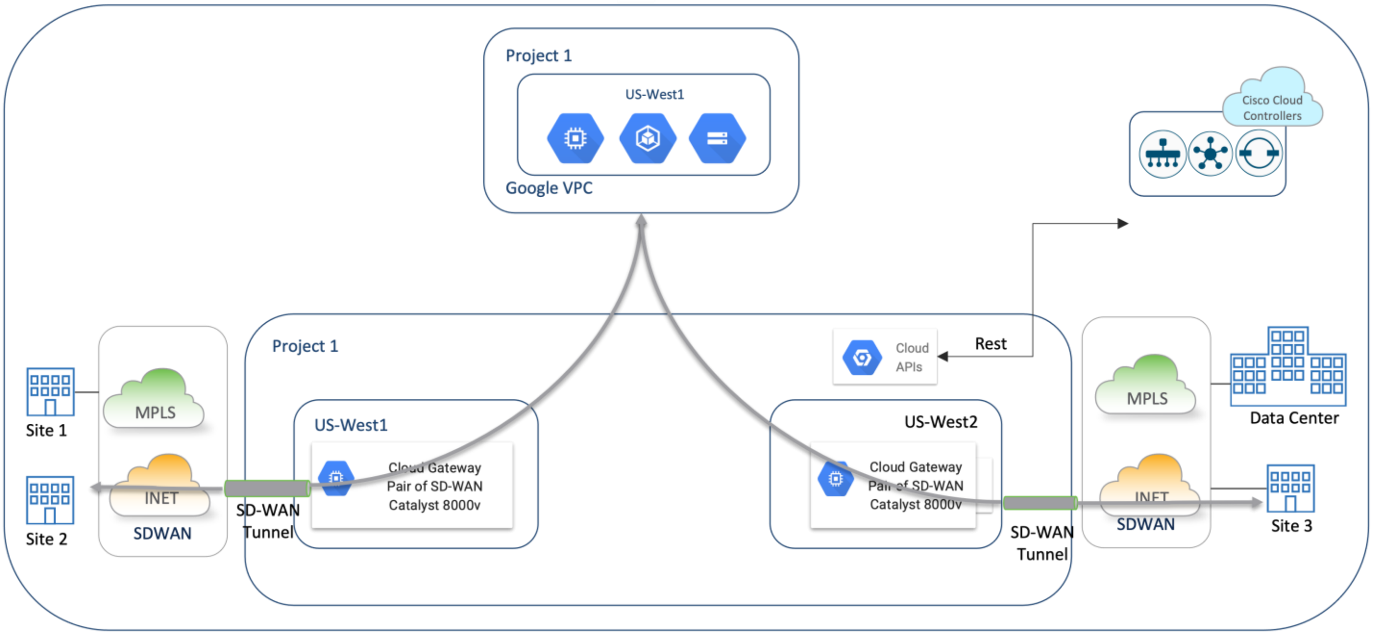
- Cloud Hub Use Case #1 – Site-to-Cloud Connectivity (S2C)
- Cloud Hub Use Case #2 – Site-to-Site Connectivity (S2S) with SDWAN Core
- Design Components and Consideration
  - Supported Platform and Software
  - Preparation of Device Templates
  - Creation and Management of Cloud Gateway
  - Mapping of VPN to Tag
  - Site-to-Cloud Workflow
  - Site-to-Site Workflow

Cloud Hub Use Case #1 – Site-to-Cloud Connectivity (S2C)

In the site-to-cloud use case, Cisco Cloud onRamp automates the backend processes to host a pair of Catalyst 8000v devices as a part of the Cloud Gateway (CGW), through which on-premises branch and data center Cisco SD-WAN Edge devices access Google cloud resources and applications running in a VPC. In this scenario, a branch site, such as site 1 connects to a VPN 0 transport tunnel interface part of the catalyst 8000v device, which connects to your applications hosted in Google VPCs through the Catalyst 8000v service side VPN interface.

© 2020 Cisco and/or its affiliates. All rights reserved.

Figure 2. **Site-to-Cloud Model**

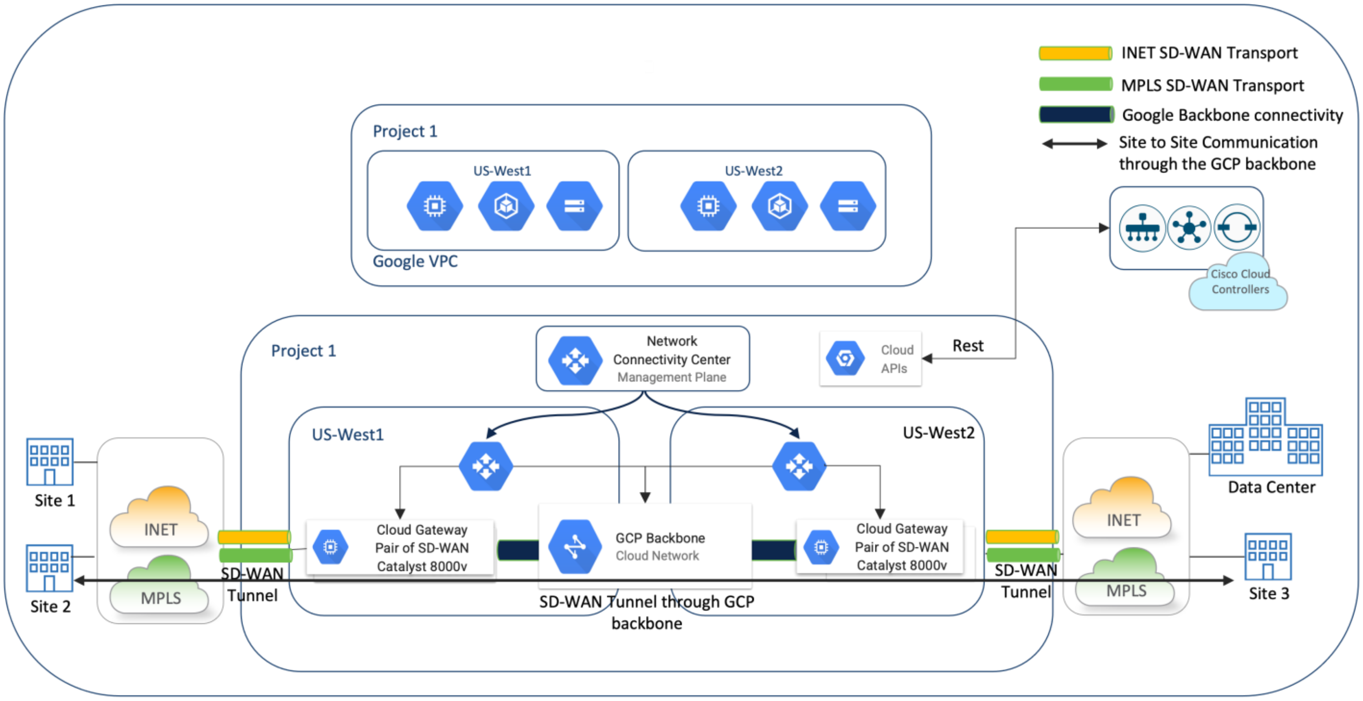


Cloud Hub Use Case #2 – Site to Site Connectivity (S2S) with SDWAN Core

To achieve the site-to-site connectivity, two branches located in different Google Cloud regions are connected through the site-to-site transit VPC or Cloud Gateway in Google Global Network. Within the Google cloud platform, a pair of Catalyst 8000v Edge devices are deployed in a Cloud Gateway (CGW) with a 2nd WAN transport interface in the site-to-site VPC. Similarly, a second set of Catalyst 8000v edge devices are deployed in another Cloud Gateway (CGW) with its 2nd WAN transport interface also part of the same site-to-site VPC. This second transport interface can be either IPsec or GRE encapsulated. The two Cloud Gateways (CGWs) are placed in different Google cloud regions and the Catalyst 8000v devices in each of the CGWs appear as spokes to the Network Connectivity (NCC) hub. The NCC hub acts as a transit within the Google domain to carry data traffic across the IPsec or GRE tunnel via the global Google backbone.

© 2020 Cisco and/or its affiliates. All rights reserved.

Figure 3. **Site-to-Site Model**


INET SD-WAN Transport
MPLS SD-WAN Transport
Google Backbone connectivity
Site to Site Communication through the GCP backbone
Project 1
US-West1
US-West2
Google VPC
Cisco Cloud Controllers
Project 1
Network Connectivity Center Management Plane
Cloud APIs
Rest
US-West1
US-West2
Site 1
Site 2
INET
MPLS
SD-WAN Tunnel
Cloud Gateway Pair of SD-WAN Catalyst 8000v
GCP Backbone Cloud Network
Cloud Gateway Pair of SD-WAN Catalyst 8000v
SD-WAN Tunnel through GCP backbone
SD-WAN Tunnel
INET
MPLS
Data Center
Site 3

Design Components and Consideration

The main building blocks of the Site-to-Cloud (S2C) and Site-to-Site (S2S) design include the bring up of two Cisco Catalyst 8000v SD-WAN routers in each of the Google Cloud Gateways (CGWs). Each of the Catalyst 8000v device contained within these gateways have three gigabit ethernet interfaces. Each interface in the Catalyst 8000v is a part of a different VPC, therefore the design includes the bring up and configuration of the three VPCs – WAN VPC, Site-to-Cloud (S2C) VPC and Site-to-Site (S2S) VPC. Each of these VPCs are explained in detail within the design section.

The design section also focuses on the supported cloud platform/ software and features to be considered while deploying the SD-WAN Google Cloud Integration using Cisco SD-WAN Cloud onRamp for Multi-Cloud feature.

Supported Platforms and Software

Cloud onRamp for Multi-cloud using Google Cloud is supported on Catalyst 8000v SD-WAN router running IOS-XE SD-WAN version 17.5 and above, with the vManage controller running version 20.5 or a higher code.

Preparation of Device Templates

Having noted the software and hardware requirements, the next steps include the design and management of a device template that comprises of a list of feature templates to be associated with a pair of unused Catalyst8000v devices.

To deploy just the Site-to-Cloud use case, you need only a pair of Catalyst 8000v devices deployed in a single Cloud Gateway (CGW).

To deploy the Site-to-Cloud and the Site-to-Site use case, you need at least a two pairs of Catalyst 8000v devices deployed in two different Cloud Gateways (CGWs). The two CGWs containing a pair of Catalyst 8000vs must be deployed in two different Google cloud regions.

© 2020 Cisco and/or its affiliates. All rights reserved.

For ease of use, the GCP device templates are pre-built in the vManage NMS under the default templates tab. The default device template includes all the necessary feature templates required to bring up the WAN Edge devices with both control plane and data plane connections established. While one transport interface is provisioned using the default device template in WAN VPC, the service side VPN interface in the Site-to-Cloud (S2C) VPC and the 2nd WAN transport interface in the Site-to-Site (S2S) VPC is deployed automatically using the Cloud onRamp workflow.

It is upon the creation and deployment of Cloud Gateways (CGWs) in Google cloud that the interfaces and its associated resources required to complete the site-to-cloud and site-to-site use case are deployed.

Creation and Management of Cloud Gateway

A Cloud Gateway (CGW) is simply a pair of Catalyst 8000v devices provisioned in a Google Cloud region. Within the Google cloud platform, CGWs are instantiated in different Google cloud regions based on the global or custom settings entered within the vManage Cloud onRamp setup page.

During the instantiation of a Cloud Gateway containing a pair of Catalyst8000v devices, as mentioned previously, three Google VPCs are created:

WAN VPC: The WAN interface is a part of the WAN VPC. The WAN VPN interface template for the Catalyst 8000v devices is created based on the device template attached to it. Its interface IP address is assigned based on the subnet entered within the CGW global settings. Similarly, the location of the VPC is based on the location in which the CGW is deployed.

Within the Catalyst 8000v, the Gigabit Ethernet 1 or Gig1 interface is part of the WAN VPC and note this is the only interface in the Catalyst 8000v that is assigned a public IP address.

Site-to-Cloud (S2C) VPC: A second VPC is created for the site to cloud use case and associated to the service side VPN interface. The VPC, VPN and the VPN interface details are automatically created and configured based on the region and subnet details entered within the CGW global and custom settings.

The peering between the S2C VPC and host VPC is done based on the BGP offset details entered in the global settings page.

Note, within the Catalyst 8000v, the Gigabit Ethernet 2 or Gig2 interface is part of the S2C VPC.

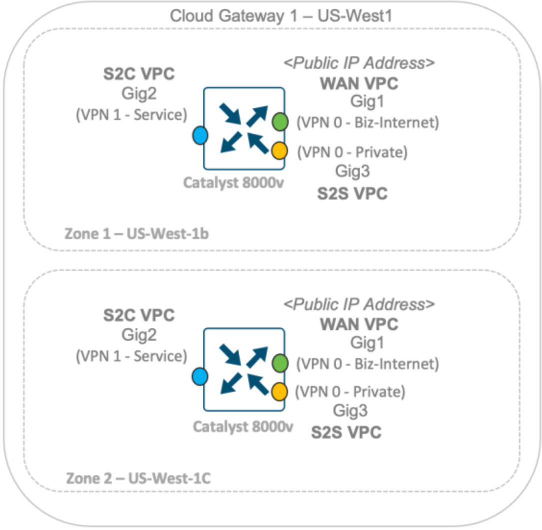
Site-to-Site (S2S) VPC: And finally, a third VPC is created on enabling the site-to-site connectivity within the CGWs global settings. This VPC is associated with a second WAN interface labeled color private1. The VPC, VPN and the VPN interface details are automatically created and configured region and subnet details entered within the CGW global and custom settings.

The BGP routing protocol is used to learn and advertise the underlay routes.

Note, within the Catalyst 8000v, the Gigabit Ethernet 3 or Gig3 interface is part of the S2S VPC.

© 2020 Cisco and/or its affiliates. All rights reserved.

Figure 4. **VPCs created in GCP**



Cloud Gateway Settings

The rest of this section focuses on understanding the Cloud Gateway (CGW) settings required to bring up a pair of Catalyst 8000v devices within the CGWs.

Catalyst 8000v Instance Size: The Catalyst v8000 WAN Edge virtual devices provisioned in google cloud VPC can be of instance type N1-standard-8 and N1-standard-4. Falling under the general-purpose machine category this machine type provides predefined vCPU and memory resources for an instance. The N1-standard-8 machine type provides 8 virtual CPUs and a total of 30GB memory, while the N1-standard-4 machine type provides 4 virtual CPUs and a total of 15GB memory.

Region: Plan the regions wherein your CGWs and its associated resources are to be instantiated. The following link lists out all the regions you can choose to bring up your cloud resources: https://cloud.google.com/compute/docs/regions-zones

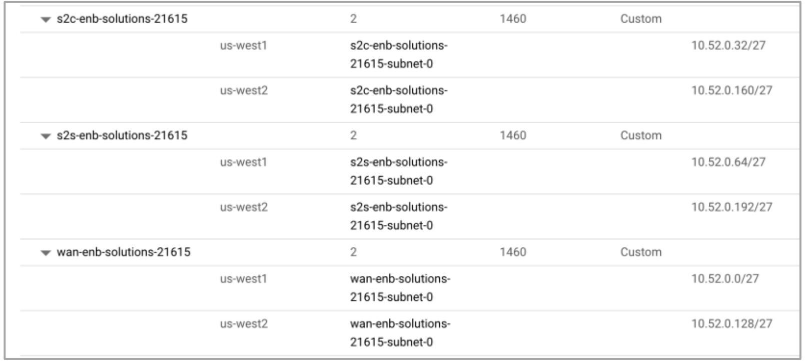
Regions have three or more zones. For example, the us-west1 region denotes a region on the west coast of the United States that has three zones: us-west1-a, us-west1-b, and us-west1-c. During the instantiation of a Cloud Gateway, a pair of Catalyst 8000v devices running 17.5 IOS-XE SD-WAN code are automatically placed in separate zones for redundancy within the chosen region.

CGW Subnet Pool: The subnet pool entered at the time of provisioning your cloud gateways needs to be between the subnet range of /16 to /21. By default, the system allocates /27 per VPC, therefore plan your IP addressing accordingly.

For instance, if the entered subnet pool is 10.52.0.0/16, and you have two Cloud Gateways deployed, one in US-West1 and the other in US-West2 with site-to-site connectivity enabled, then the VPC subnets are assigned subnets in the following order:

© 2020 Cisco and/or its affiliates. All rights reserved.

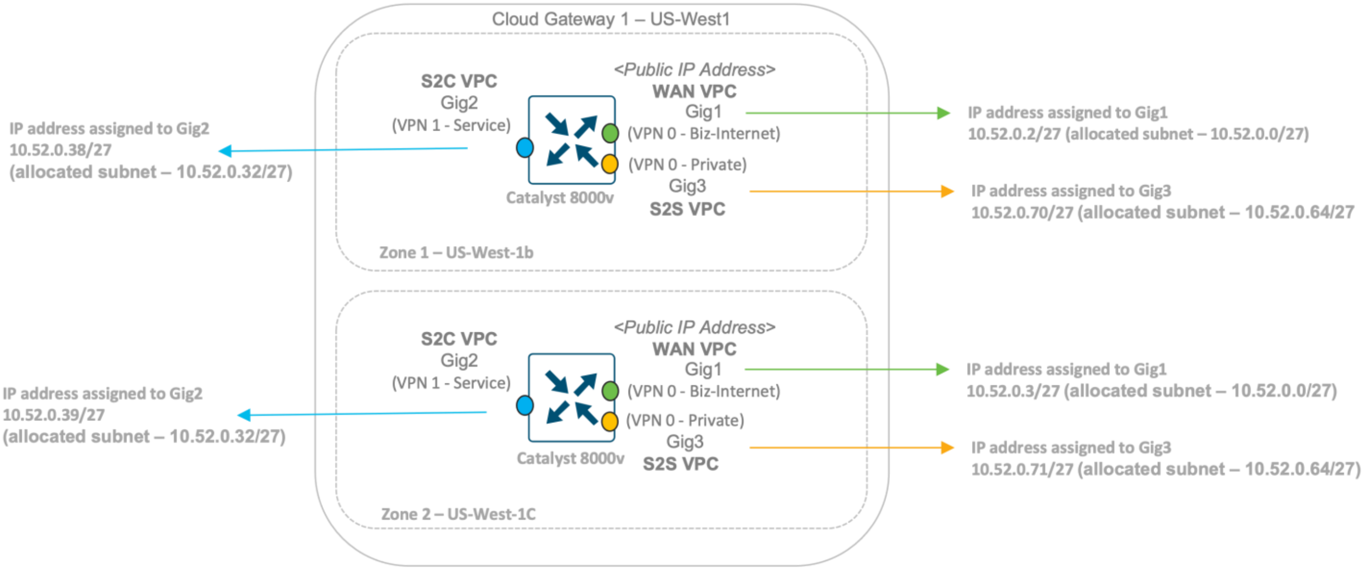
Figure 5. **Subnets in S2S, S2C and WAN VPC**



s2c-enb-solutions-21615		2	1460	Custom	
	us-west1	s2c-enb-solutions-21615-subnet-0			10.52.0.32/27
	us-west2	s2c-enb-solutions-21615-subnet-0			10.52.0.160/27
s2s-enb-solutions-21615		2	1460	Custom	
	us-west1	s2s-enb-solutions-21615-subnet-0			10.52.0.64/27
	us-west2	s2s-enb-solutions-21615-subnet-0			10.52.0.192/27
wan-enb-solutions-21615		2	1460	Custom	
	us-west1	wan-enb-solutions-21615-subnet-0			10.52.0.0/27
	us-west2	wan-enb-solutions-21615-subnet-0			10.52.0.128/27

Based on the subnets listed in the table above, the IP addresses and subnets are assigned to the interfaces part of two Catalyst 8000v devices that belong to the same Cloud Gateway placed in US-West1 in the following way,

Figure 6. **Subnet and IP address distribution in a CGW**



Cloud Gateway 1 – US-West1
S2C VPC
Gig2
(VPN 1 - Service)
<Public IP Address>
WAN VPC
Gig1
(VPN 0 - Biz-Internet)
(VPN 0 - Private)
Gig3
S2S VPC
Catalyst 8000v
IP address assigned to Gig2
10.52.0.38/27
(allocated subnet – 10.52.0.32/27)
IP address assigned to Gig1
10.52.0.2/27 (allocated subnet – 10.52.0.0/27)
IP address assigned to Gig3
10.52.0.70/27 (allocated subnet – 10.52.0.64/27
Zone 1 – US-West-1b
S2C VPC
Gig2
(VPN 1 - Service)
<Public IP Address>
WAN VPC
Gig1
(VPN 0 - Biz-Internet)
(VPN 0 - Private)
Gig3
S2S VPC
Catalyst 8000v
IP address assigned to Gig2
10.52.0.39/27
(allocated subnet – 10.52.0.32/27)
IP address assigned to Gig1
10.52.0.3/27 (allocated subnet – 10.52.0.0/27)
IP address assigned to Gig3
10.52.0.71/27 (allocated subnet – 10.52.0.64/27)
Zone 2 – US-West-1C

The WAN Interface is part of the WAN VPC, wan-enb-solutions-21615 and this interface is assigned one private and one public IP address. The public IP address is used to establish control connections with the Cisco SD-WAN controllers and data plane connections with branch sites.

To establish the site-to-cloud use case, a single service-side VPN is automatically deployed within each Catalyst 8000v. The service-side VPN (VRF 1/ VPN 1) is deployed and associated to the Site-to-Cloud VPC, s2c-enb-solutions-21615.

To establish the site-to-site use case, a second WAN tunnel interface is brought up under the s2s-enb-solutions-21615 VPC.

BGP ASN Offset: As mentioned earlier, the BGP routing protocol is used to learn and advertise the underlay routes.

To establish this peering BGP ASN offset is entered within the settings page. The BGP ASNs entered in the settings are assigned to the resources as given below:

The entered BGP ASN Offset is the number assigned as the BGP ASN for the GCR in Site-to-Cloud VPC.

© 2020 Cisco and/or its affiliates. All rights reserved.

The entered BGP ASN Offset plus one (BGP ASN + 1) is the ASN assigned for GCRs in Site-to-Site VPC.

The entered BGP ASN Offset plus 10 (BGP ASN +10) will be the ASN assigned to the Catalyst8000v devices.

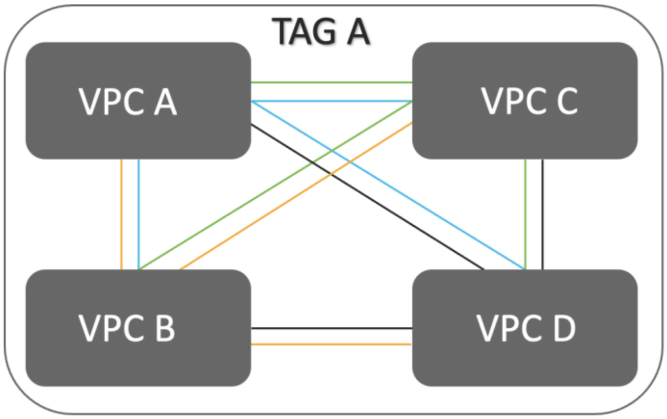
All ASNs must belong to private ASN space i.e. between the ASN range 64250 to 65520. Plan your BGP ASN numbers accordingly.

Intra-Tag Communication: Within the Cloud onRamp workflow, the discovered VPCs are added to a Tag. Tagging allows for the grouping of several VPCs together to treat them as a single unit.

Within the cloud architecture, communication within the same Google VPC network conversation is possible, but to enable communication between multiple VPC's, you can combine them all under one tag and this establishes intra-tag VPN communication. Therefore, this allows Google VPCs that are a part of the same tag to communicate with other. So, in order to achieve intra tag communication between Google VPC's, links are created between different VPC's. The number of links will be N x (N-1) where N is the number of VPC's.

For example, if you have 4 VPCs, VPC A, VPC B, VPC C and VPC D hosted in Google cloud, and they were all added to the same tag A, then the number of links between the VPCs will be, 4 X (4-1) = 12.

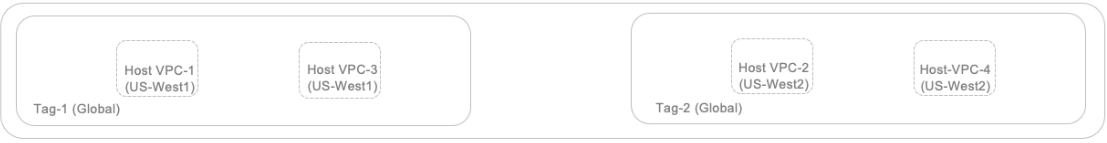
Figure 7. **Tagging Operation**



The intra tag communication is enabled by default, however you can choose to disable this from the global settings.

In this guide, customer hosted VPCs named Host VPC-1 and Host VPC-3 are part of the same tag, Tag 1 and customer hosted VPCs named Host VPC-2 and Host VPC-4 are part of another tag, Tag 2.

Figure 8. **Host VPC to Tag mapping**



Technical Tip
A VPC hosted in Google cloud platform can be a part of tag or removed from an associated tag or moved from one tag to another tag as part of editing of tags. The design for the tagging operation is the same across all cloud types, AWS and Azure included.

© 2020 Cisco and/or its affiliates. All rights reserved.

Site-to-Site Connectivity and Tunnel Encapsulation Type: Enable site-to-site connectivity to deploy the site-to-site use case.

For the site-to-site use case, you need at least two cloud gateways deployed in two different Google cloud regions. Note, only a single Google Cloud Gateway is supported per Google region. Therefore, to establish site-to-site connectivity you need to bring up two Google Cloud Gateway, placed in two different Google cloud regions.

On enabling site-to-site connectivity within each of the cloud gateways, an additional WAN tunnel interface is automatically created and added through the Cloud onRamp workflow with its color automatically set to private1. This interface is associated with the Site-to -Site VPC (s2s-enb-solutions-21615) and is assigned a private IP address. The tunnel type can be of type GRE or IPsec encapsulated and, regardless of the encapsulation type chosen, all data traffic traversing through the Google backbone is encrypted.

Note: All the site-to-site traffic flows through the Google global network only via the private1 color WAN tunnel interface and not through any other WAN interface created on the Catalyst 8000v devices.

Technical Tip
Google recommends using GRE encapsulated tunnels as it provides twice the bandwidth/throughput.

Network Service Tier: Choose one of the GCP network service tiers – Premium or Standard. Premium: Gives users exceptional high performing network experience by using Google's global network costs, while still delivering performance comparable with other cloud providers. The default is Premium. When updated, it will be effective for the next CGW instantiation.

Mapping of VPN to Tag

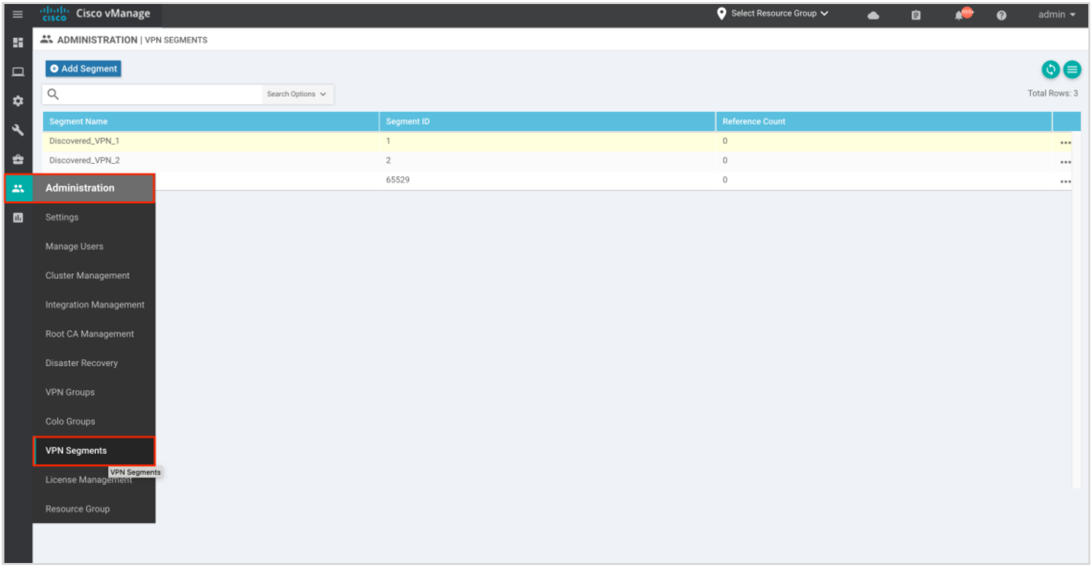
Within the cloud onRamp intent matrix page, you can map a service-side VPN to a tag, or map a tag to tag, or map a tag to a VPN. This type of mapping is referred to as a Forward Mapping.

Since the intent is global in nature, if the mapping intent was entered earlier for a CGW, then when a new CGW gets instantiated in a different region the applicable VPN to Tag mapping gets utilized. So, one does not have to retrigger the mapping on the instantiation of a new CGW. Any mapping operation that comes into play at that time is known as Derived Mapping.

Technical Tip

In the Cloud onRamp workflow, only one tag can be mapped to one Cisco SD-WAN Service side VPN. For example, if VPN 1 to a tag mapping already exists, then another VPN 1 to tag mapping cannot be completed.

Also, note the intent matrix page lists all the service side VPNs known to vManage from the VPN segments page. So, even though your Catalyst 8000v is configured with only one service-side VPN, the intent matrix mapping page may list 1 or more VPNs.



Segment Name	Segment ID	Reference Count
Discovered_VPN_1	1	0
Discovered_VPN_2	2	0
	65529	0

Site-to-Cloud (S2C) VPN to Tag Mapping and Traffic Flow

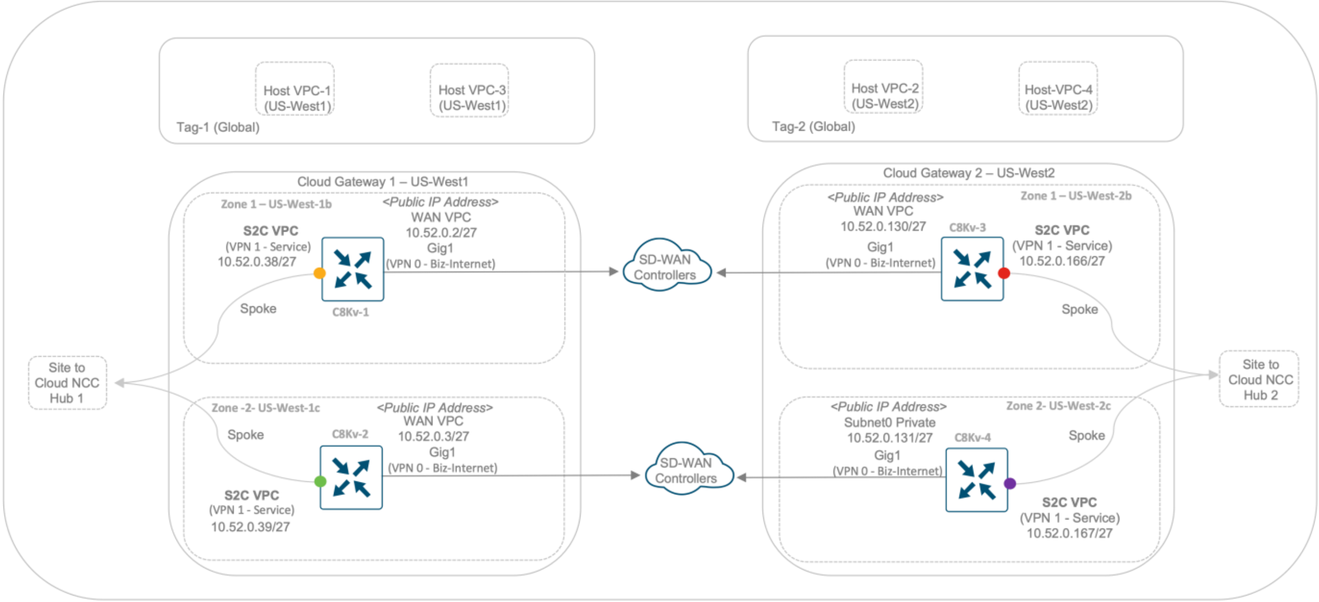
In the following example figure, two CGWs are deployed, one in US-West 1 and the other in the US-West 2 region with each CGW containing a pair of Catalyst 8000v configured with one transport interface in WAN VPC, and one service side interface in Site to cloud VPC.

Now, during the creation of a CGW, an NCC Site-to-Cloud (S2C) hub is automatically created and each Catalyst 8000v router in the CGW connects as a spoke to the Site-to-Cloud (S2C) Hub. The S2C Hub has a global scope while the Cisco SD-WAN CGW Catalyst8000v devices are instantiated at regional level within the project. While the NCC hubs are essentially responsible for inter-region routing using Google's backbone, the S2C Hub does not participate in any inter-region transit and practically not used in any part of the packet transit.

Therefore, the following figure shows two Cloud gateways, each containing a pair of Catalyst 8000v devices that act as spokes to the Site to Cloud NCC Hub. The VPCs placed on the topmost part of the picture are the customer hosted VPCs in Google cloud. In this guide, customer hosted VPCs named Host VPC-1 and Host VPC-3 are part of the same tag, Tag 1 and customer hosted VPCs named Host VPC-2 and Host VPC-4 are part of another tag, Tag 2.

© 2020 Cisco and/or its affiliates. All rights reserved.

Figure 9. **Site to Cloud Design**



The next steps include the mapping of the service side VPN, VPN 1 to the tag, therefore establishing the communication between branch sites with the VPCs part of the global Tag. As a part of this VPN-tag mapping, Google cloud routers are configured in the Google cloud platform within the Site to Cloud VPC which carries the underlay traffic across.

Since we have two Catalyst 8000v devices deployed in each Cloud gateway (total of four Catalyst 8000v routers), an equivalent number of redundant GCRs are also deployed.

In US-West1, two GCRs are deployed with each GCR assigned two private IP addresses. A pair of GCRs located in a Google cloud region are assigned a total of 4 private IP addresses and the BGP ASN offset entered within the global settings is assigned to each of the GCRs in the site to cloud VPC.

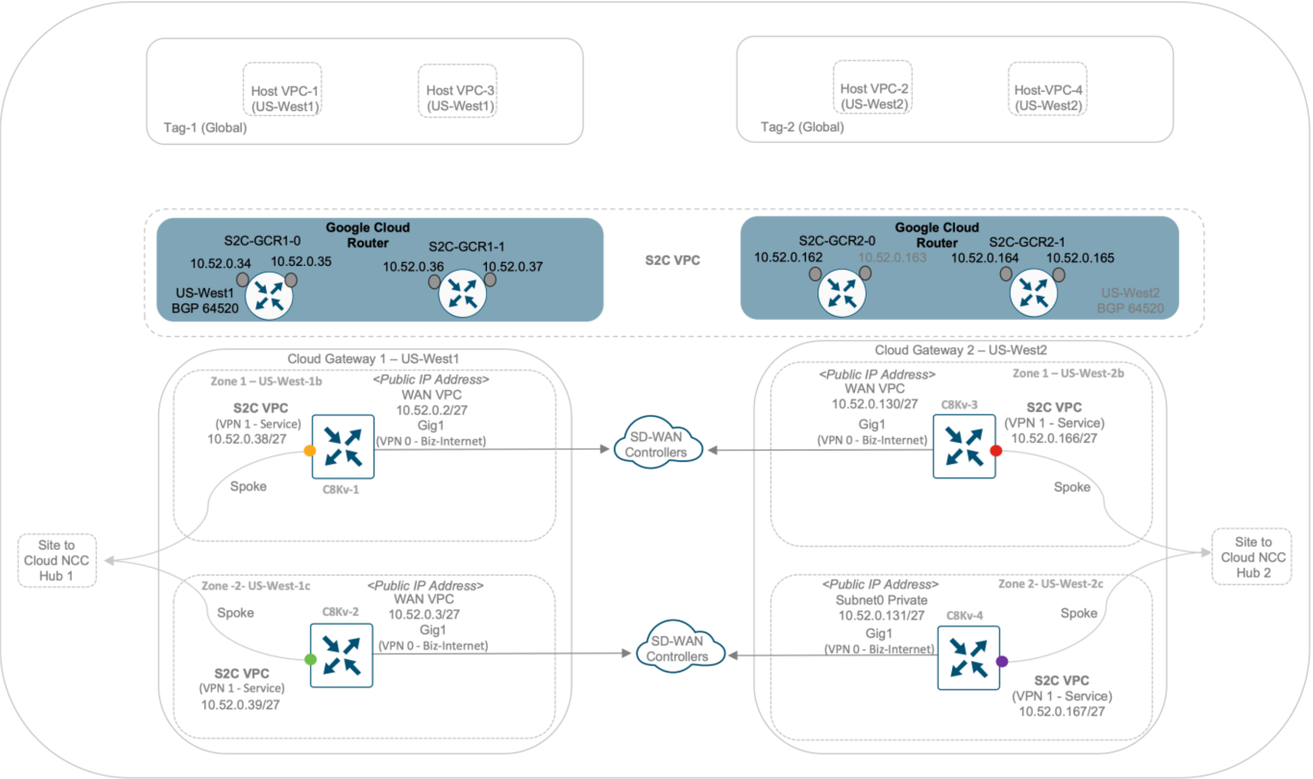
Note: The GCR's are assigned IP addresses based on the IP subnet entered globally or per CGW.

In this guide, the entered BGP ASN Offset is 64520, therefore this BGP ASN Offset is assigned to the GCRs and note each of these GCRs share a common gateway IP address. Note, this gateway IP address is automatically assigned to the GCRs based on the entered subnet. The IP addresses for the first set of the GCRs in the Site to Cloud VPC, range from 10.52.0.34 – 10.52.0.37, therefore IP address 10.52.0.33 is automatically assigned as the gateway IP. Do note, all Google cloud routers are just a conceptual router in the google cloud. The purpose of Cloud Router is to dynamically exchange the routes between two Virtual Private Cloud Networks or Virtual Private Cloud Network and on-premises networks. Cloud Router uses "Border Gateway Protocol" to exchange routing information between the networks. GCRs are not virtual machines or devices that you can log into via telnet or SSH. Similarly, is the gateway IP address too. It is conceptual in nature, and therefore the gateway IP address is not captured in the figures displayed within this guide.

Similarly, part of the tagging operation two redundant GCRs are also automatically provisioned in US-West2 region, with each GCR in that region also assigned a pair of private IP addresses and a BGP ASN (Assigned ASN 64520). This GCR pair also shares a common gateway IP address. The IP addresses for the second set of the GCRs in the Site to Cloud VPC range from 10.52.0.162 – 10.52.0.165, therefore IP address 10.52.0.161 is automatically assigned as the gateway IP.

© 2020 Cisco and/or its affiliates. All rights reserved.

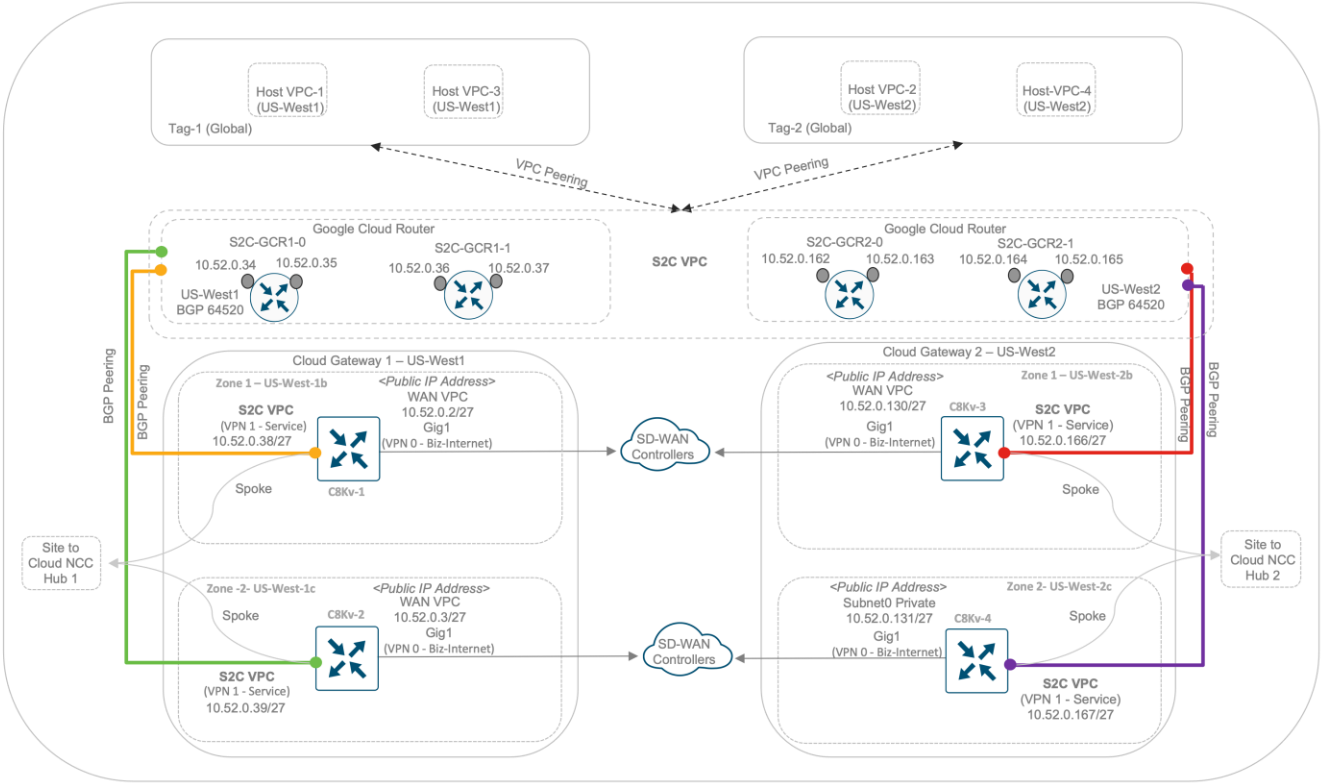
Figure 10. **Google Cloud Routers in S2C VPC**



On mapping a service side VPN 1 or VRF 1 S2C interface to a tag, the Catalyst 8000v devices in each CGW peer with the Google Cloud Routers via its Gig2 interface. As explained in the example figure below, on mapping VPN 1 interface to tags, both the Cat8kv-1 and Cat8kv-2 located in US-West1 forms BGP peers with the Google Cloud Routers (GCR) virtual routers via its service-side private IP addresses and similarly, both the Catalyst8000v routers (Cat8kv-3 and Cat8kv-4) in Cloud Gateway 2 located in US-West2 also peers with the GCRs via its service side VPN 1 private IP addresses - 10.52.0.39 and 10.52.0.167.

© 2020 Cisco and/or its affiliates. All rights reserved.

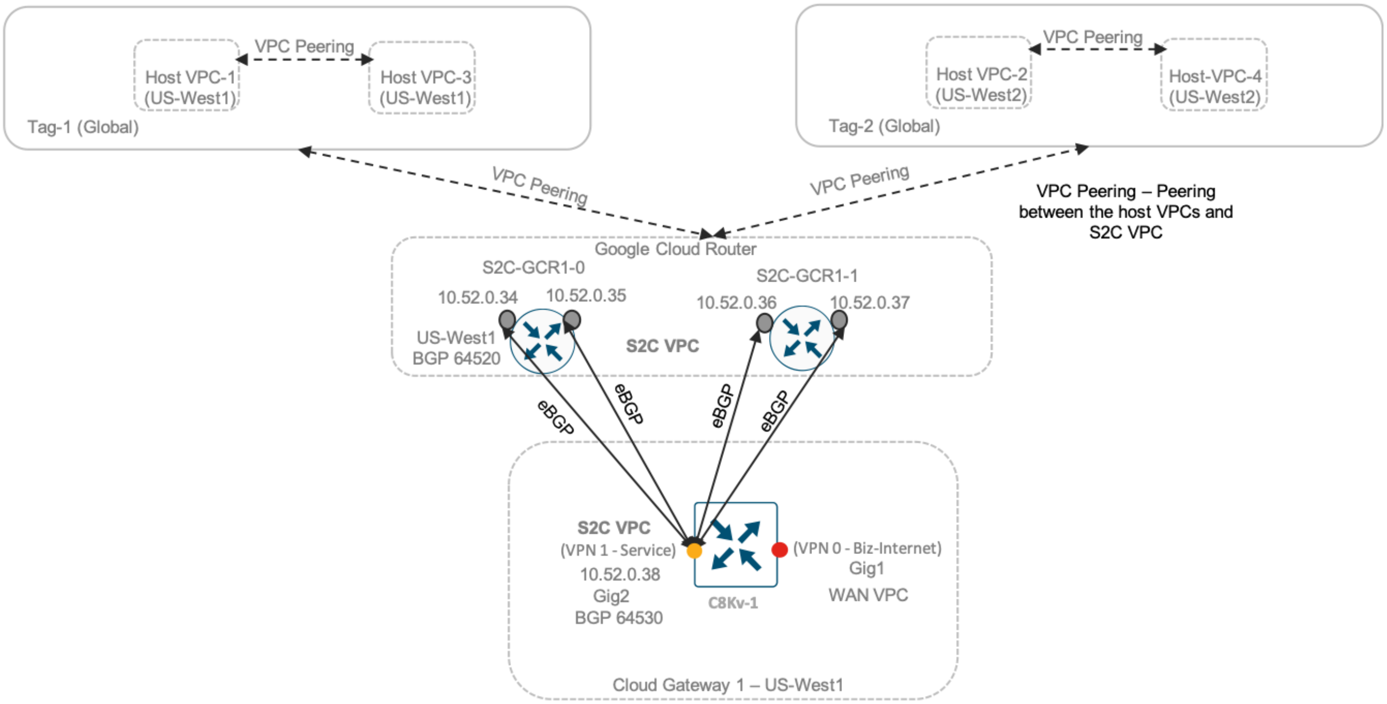
Figure 11. **Site-to-Cloud Workflow**



All Google Cloud Routers (GCRs) act as the underlay routing engine in the Google domain and therefore all Catalyst 8000v routers in the CGWs form four eBGP peers with the GCR IP addresses. The example figure below focuses on the eBGP peering between one of the Catalyst8000v routers and a pair of GCRs. The GCRs advertise the host VPC subnets to the Cat8kv-1 device via eBGP.

© 2020 Cisco and/or its affiliates. All rights reserved.

Figure 12. **BGP Peering in S2C Workflow**



Similarly, each of the Catalyst 8000v devices in each of the Cloud Gateway (CGWs) form 4 eBGP peers with the GCRs (peer with IP 10.52.0.34, 10.52.0.35, 10.52.0.36, 10.52.0.37). Within each Catalyst 8000v device, the learnt BGP routes are advertised to the vSmart controller via OMP. The vSmart controller sends the advertised OMP routes to other Cisco SD-WAN Edge devices. The Catalyst 8000v devices installs the other GCR subnets learnt via OMP and redistributes this into BGP.

The following figure and outputs include the BGP routes learnt by Cat8kv-1. The Cat8kv-1 device installs the second GCR subnet 10.52.0.160/27 learnt via OMP and redistributes this into BGP. For all the relevant CLI outputs from all Catalyst8000v devices, refer to the operate section of this guide.

© 2020 Cisco and/or its affiliates. All rights reserved.

Figure 13. **BGP Peering for two Catalyst8000v Devices**

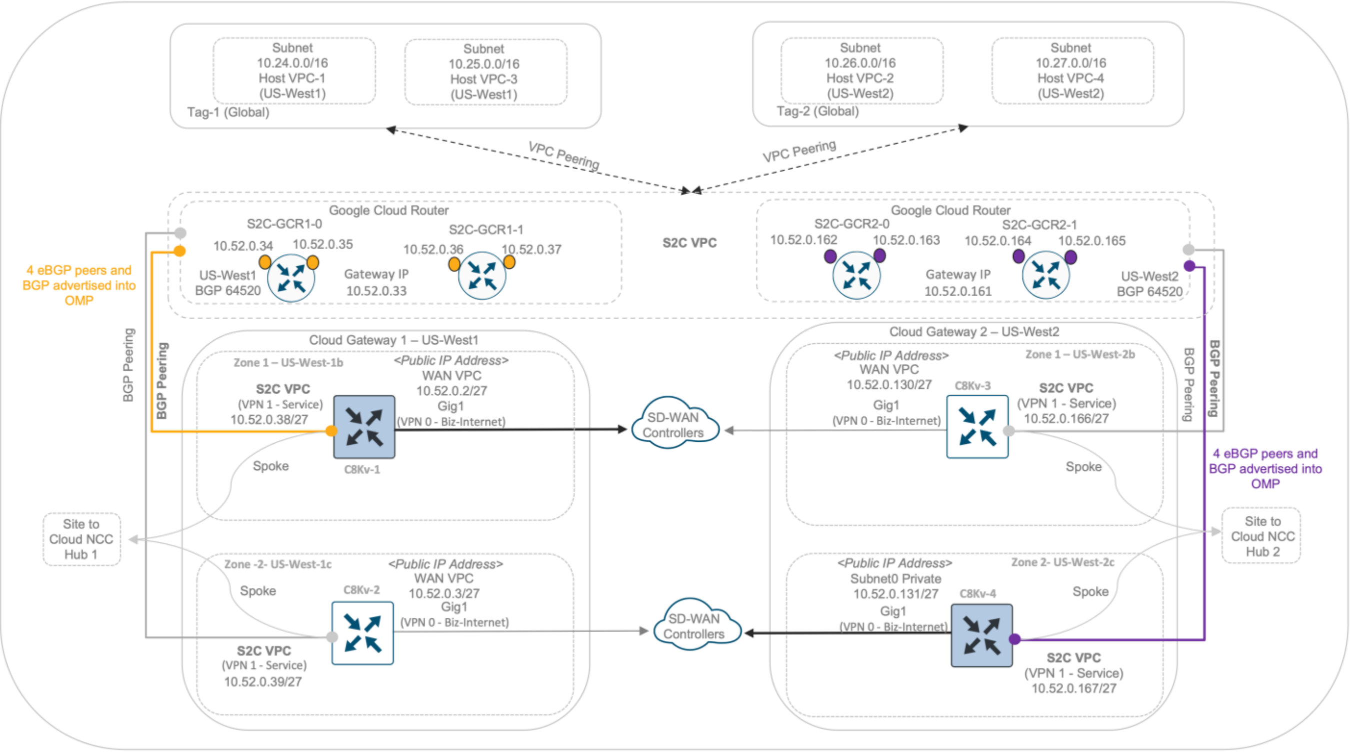
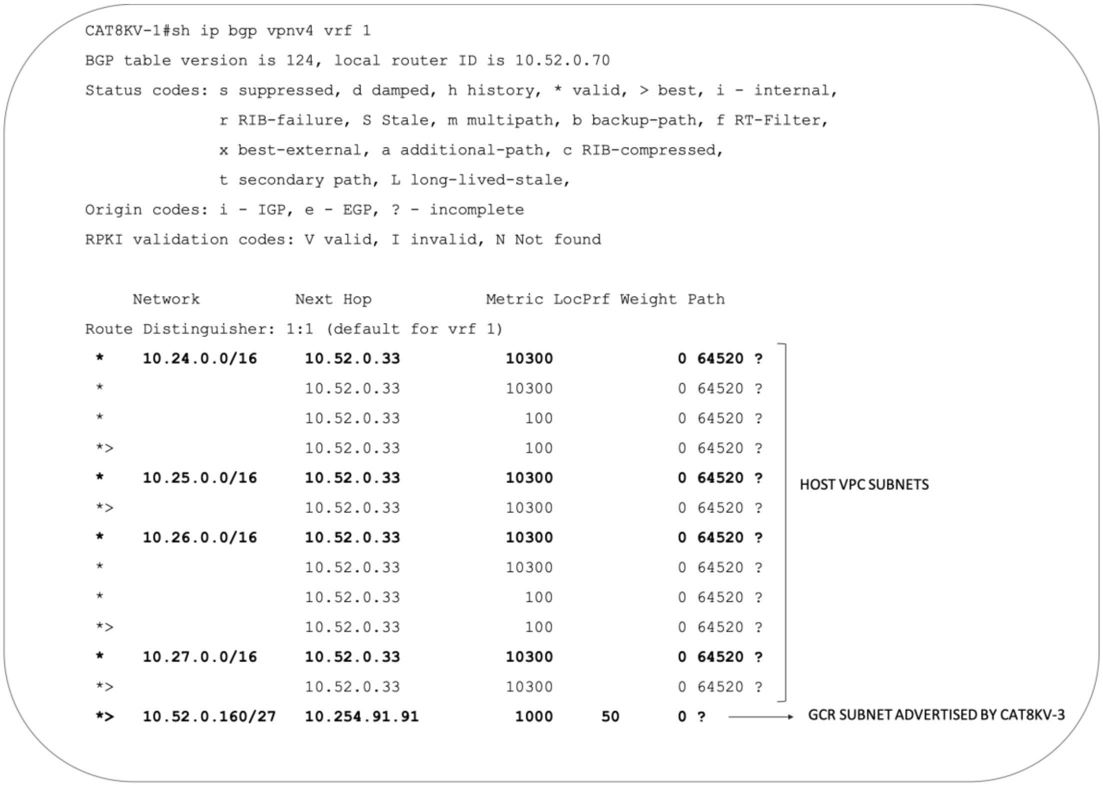


Figure 14. **BGP VPN 1 Routes**



```
CAT8KV-1#sh ip bgp vpnv4 vrf 1
BGP table version is 124, local router ID is 10.52.0.70
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path, L long-lived-stale,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf 1)
 *    10.24.0.0/16     10.52.0.33          10300             0 64520 ?
 *                     10.52.0.33          10300             0 64520 ?
 *                     10.52.0.33            100             0 64520 ?
 *>                    10.52.0.33            100             0 64520 ?
 *    10.25.0.0/16     10.52.0.33          10300             0 64520 ?
 *>                    10.52.0.33          10300             0 64520 ?
 *    10.26.0.0/16     10.52.0.33          10300             0 64520 ?
 *                     10.52.0.33          10300             0 64520 ?
 *                     10.52.0.33            100             0 64520 ?
 *>                    10.52.0.33            100             0 64520 ?
 *    10.27.0.0/16     10.52.0.33          10300             0 64520 ?
 *>                    10.52.0.33          10300             0 64520 ?
 *>   10.52.0.160/27   10.254.91.91         1000     50      0 ?
```

HOST VPC SUBNETS

GCR SUBNET ADVERTISED BY CAT8KV-3

© 2020 Cisco and/or its affiliates. All rights reserved.

All the data plane traffic destined to the applications hosted in Google Cloud from an on-premises SD-WAN branch site, connects to the WAN VPC. This in turn connects to customer hosted Google cloud VPCs through the site to cloud transit VPC.

Note - The term Google cloud hosted VPCs in this guide means either a host VPC, workload or applications VPCs that the customer hosted within Google Cloud.

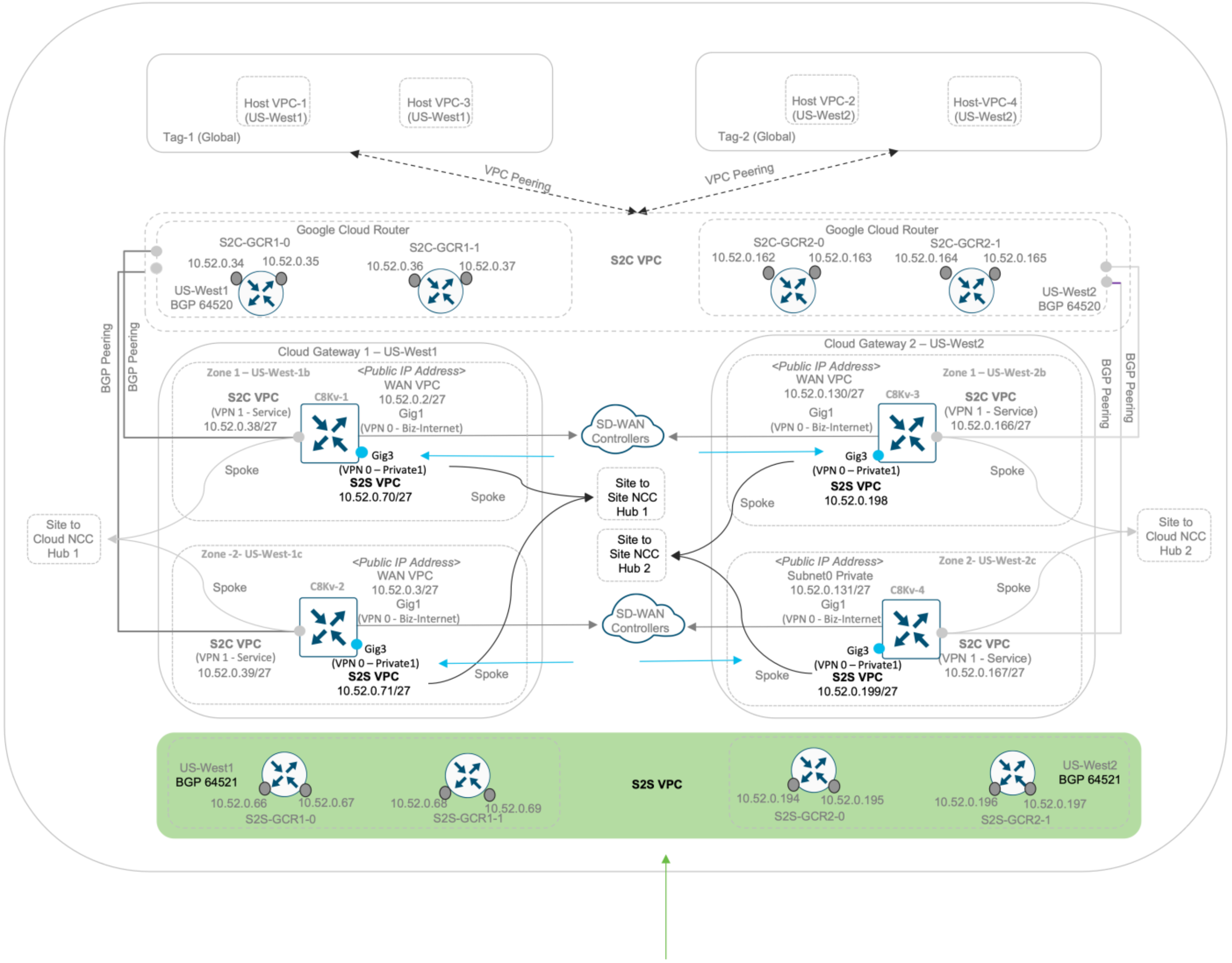
Site-to-Site VPC Workflow

On enabling the site-to-site communication, a Site-to-Site (S2S) VPC is created and within the S2S VPC two pairs of redundant GCRs are created. Within the Catalyst 8000v devices provisioned in the CGWs, a second WAN interface is automatically configured under Interface Gigabit Ethernet 3 with color set to Private1. The tunnel interface can be of type GRE or IPsec with one private IP address assigned to it. This interface receives its subnet and associated firewall details based on resources automatically configured in the S2S VPC.

In the following example figure, we assume that two CGWs are provisioned one in US-West 1 region and the other in US-West 2 region. Within each CGW, site-to-site communication is configured. Therefore, two Google Cloud Routers (GCRs) are deployed in US-West 1 and two Google Cloud Routers (GCRs) are deployed in US-West 2, all a part of the same Site-to-Site VPC (S2S VPC). Within a pair of GCRs, one GCR acts as the primary virtual router and the other acts as the backup. Each Site-to-Site GCR (S2S GCR) is assigned with a BGP ASN, i.e., the entered BGP ASN Offset + 1.

© 2020 Cisco and/or its affiliates. All rights reserved.

Figure 15. **GCRs in S2S VPC**



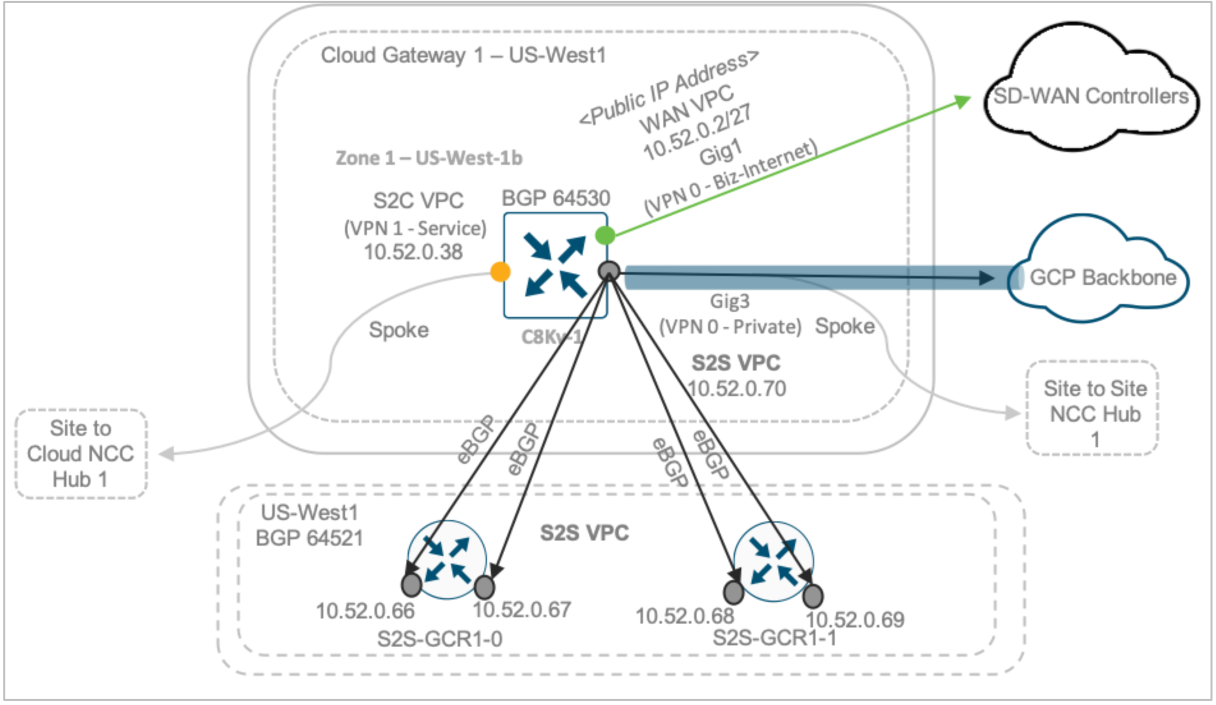
The GCR is the underlying routing engine that acts as a BGP peer in the GCP domain. Therefore, the GCR in the Site-to-Site VPC is programmed for eBGP sessions with the C8kv devices, therefore each C8kv forms BGP neighbors with 4 GCR IPs. The routes advertised through the neighbor include the S2S VPC GCR subnets.

The example figure below explains the BGP peering between one Catalyst8000v device and GCRs. In this deployment, the BGP ASN offset is set to 64520. Therefore, the GCRs are assigned a BGP ASN of 64521 (BGP ASN offset + 1) and Catalyst8000v devices in both the CGWs are assigned BGP ASN of 64530 (BGP ASN offset + 10).

The Catalyst 8000v device learns the GCR subnet from its 4 GCR eBGP neighbors with the next hop set as the GCR gateway IP.

© 2020 Cisco and/or its affiliates. All rights reserved.

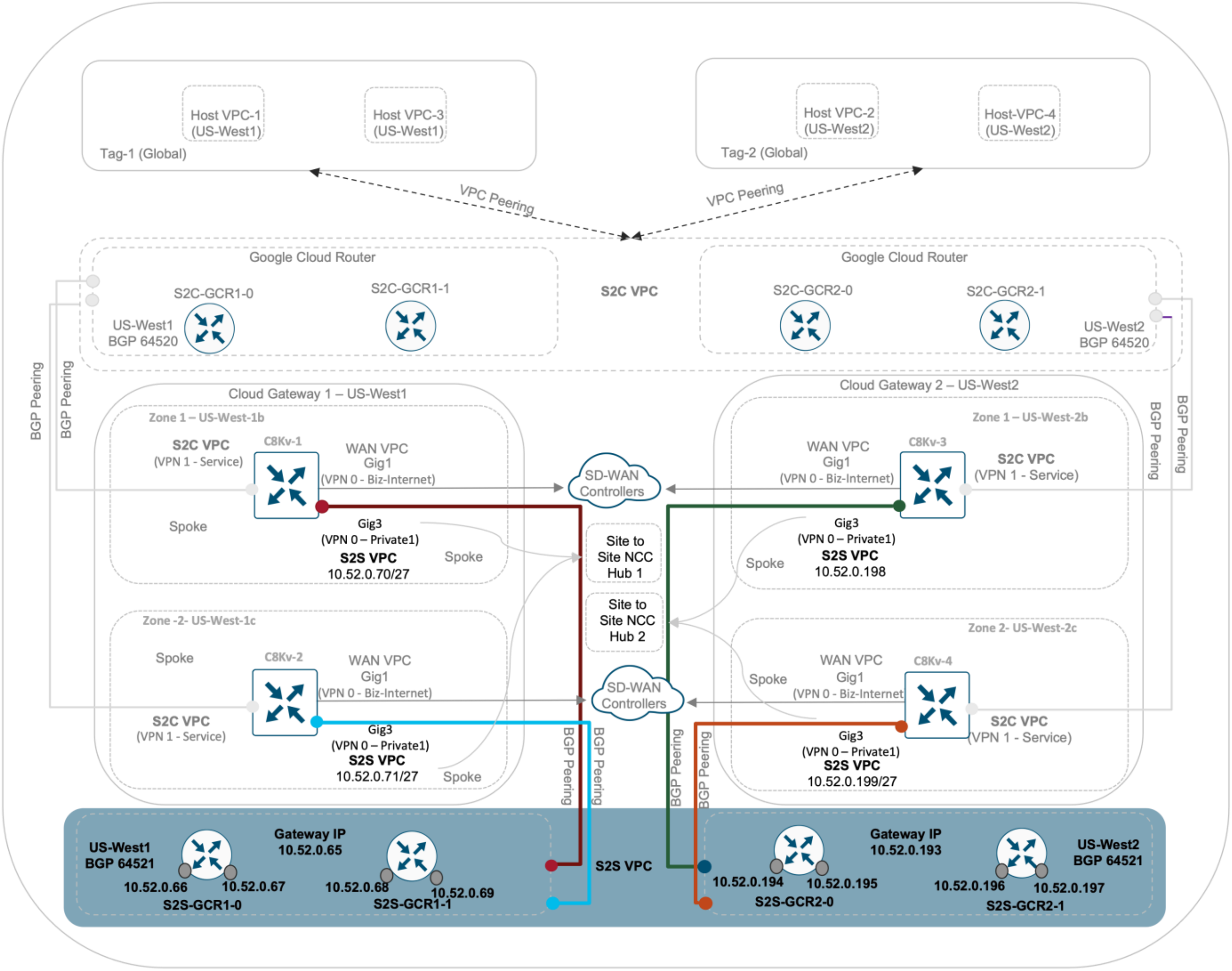
Figure 16. **BGP Peering in S2S VPC**



These neighbors advertise the entire GCR subnet to the Catalyst 8000v. The BGP routes learnt by the Catalyst8000v devices are advertised to the vSmart controller via OMP. The controller sends the advertised OMP routes to other SD-WAN Edge devices, to enable the WAN Edge devices located within on-premises or cloud hosted sites to establish tunnel connectivity with the Catalyst 8000v private link.

© 2020 Cisco and/or its affiliates. All rights reserved.

Figure 17. **GCR Subnet learnt in S2S Workflow**



Within Google Cloud platform, the SD-WAN Cloud Gateway running Catalyst 8000v are modeled as Router Appliances in Google's domain and connect as spokes to the NCC Site to Site Hub. A Hub has a global scope while the SD-WAN CGW VMs are instantiated at regional level within the project. The Hub is responsible for inter-region routing using Google's backbone.

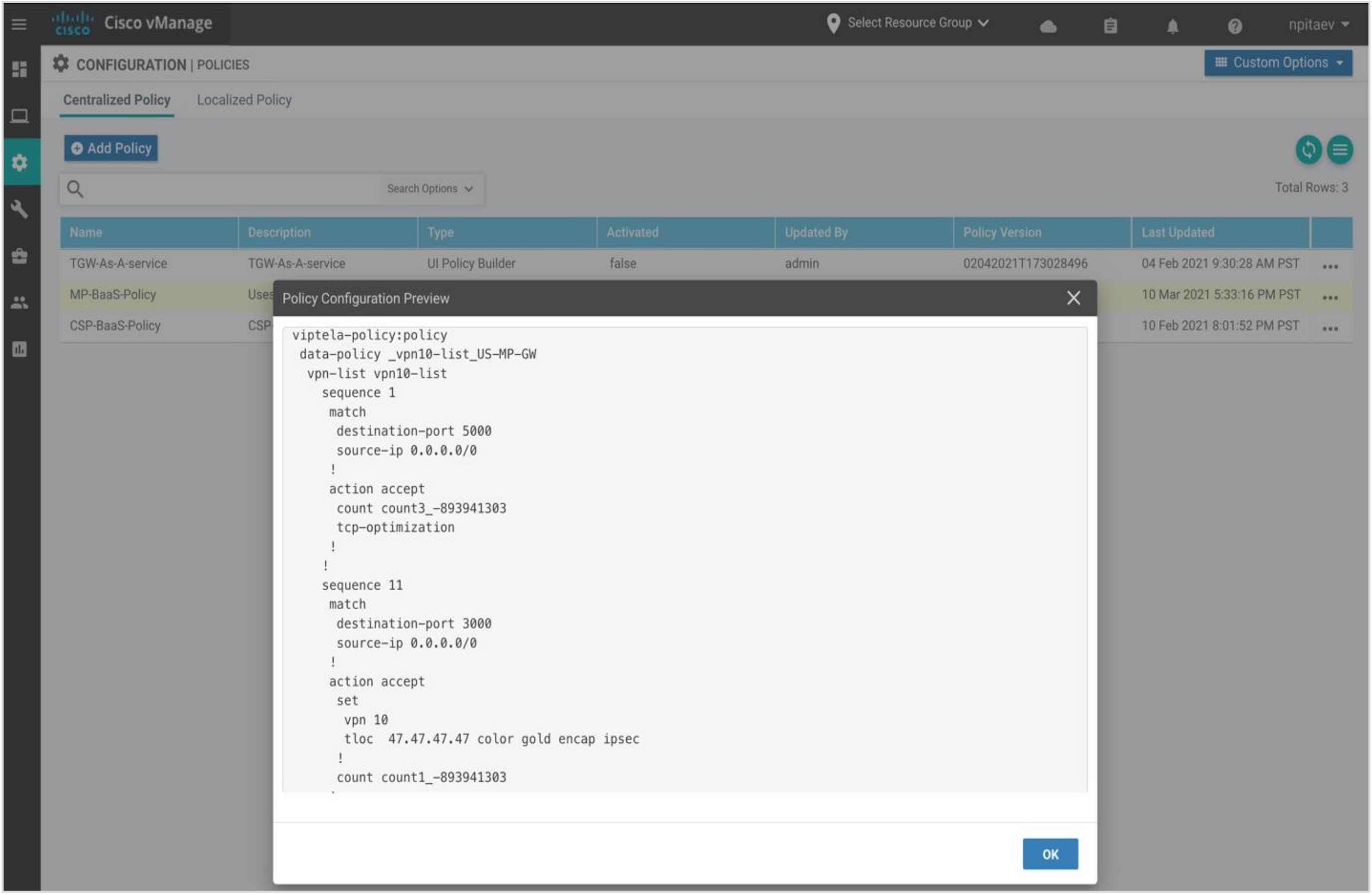
The Catalyst 8000v routers are created in different zones under the same region to meet the fault-tolerance needs. Between the two spokes the hub acts as a transit, therefore it allows for flow of the incoming data traffic through the Google Backbone.

Note: Given a scenario that your on-premises or cloud-hosted sites contain more than one WAN tunnel interface configured, say two WAN interfaces with two different colors assigned to it, MPLS and Private1, and the intent is to send critical traffic over the private link through your GCP global network and non-critical flows over other WAN tunnel links. For such design requirements, a centralized control policy can be configured to redirect traffic based on source IP/ port/ protocol to use the GCP backbone and the remaining non-critical traffic flows to exit via the remaining tunnels.

The following example illustrates a simple SD-WAN control policy, which redirects traffic to GCP using SD-WAN color Gold.

© 2020 Cisco and/or its affiliates. All rights reserved.

Figure 18. **Centralized Data Policy for S2S Workflow**



Name	Description	Type	Activated	Updated By	Policy Version	Last Updated
TGW-As-A-service	TGW-As-A-service	UI Policy Builder	false	admin	02042021T173028496	04 Feb 2021 9:30:28 AM PST
MP-BaaS-Policy	Uses					10 Mar 2021 5:33:16 PM PST
CSP-BaaS-Policy	CSP					10 Feb 2021 8:01:52 PM PST

Policy Configuration Preview

```
viptela-policy:policy
 data-policy _vpn10-list_US-MP-GW
  vpn-list vpn10-list
    sequence 1
     match
      destination-port 5000
      source-ip 0.0.0.0/0
     !
     action accept
      count count3_-893941303
      tcp-optimization
     !
    !
    sequence 11
     match
      destination-port 3000
      source-ip 0.0.0.0/0
     !
     action accept
      set
       vpn 10
       tloc  47.47.47.47 color gold encap ipsec
      !
      count count1_-893941303
```

Please refer to the following Cisco Documentation for more details on SD-WAN Policies: https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/policies/vedge/policies-book/control-policies.html

Limitations and Best Practices

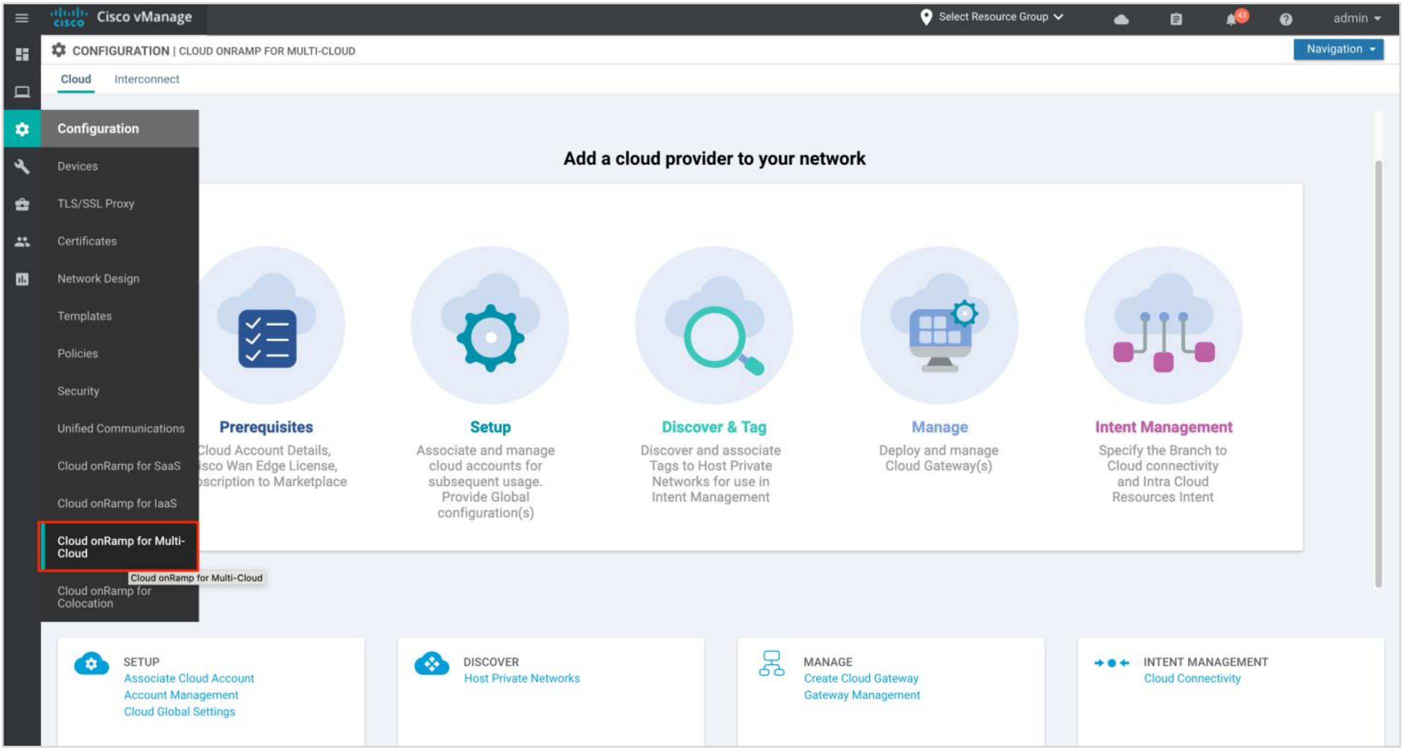
- The default GCP Catalyst 8000v template provisions one interface, that is the transport VPN 0 interface to connect to the public internet and the other two interfaces, that include second WAN transport interface for site-to-site traffic and service side interface for site to cloud traffic are configured at run time through autogenerated configuration.
- At least two free Cisco Catalyst 8000v virtual router UUIDs need to be available in Cisco vManage to bring up one Cloud Gateway.
- Only a maximum of two Catalyst 8000v devices can be deployed in a CGW, and each CGW must be deployed in different regions. The maximum number of CGWs provisioned in Google is based on the number of NCC regions available. Google Network Connectivity Center (NCC) is currently available in the following countries: https://cloud.google.com/network-connectivity/docs/network-connectivity-center/concepts/locations
- The workload VPCs should be set with a CIDR between 10.0.0.0 – 10.255.255.255 (10/8 prefix), 172.16.0.0 – 172.31.255.255 (172.16/12 prefix), and 192.168.0.0 – 192.168.255.255 (192.168/16 prefix)
- Validation checks are placed in the? solution, both at the cloud agent and NMS ports to make sure the CIDR agent is correct.

© 2020 Cisco and/or its affiliates. All rights reserved.

- Intra-VPC peering is enabled through tagging.
- Not all parallel actions are allowed since CGWs are global in nature. Anything after the first CGW is created, the rest of the CGW creations can be done in parallel. A second CGW cannot be created when the first one is being deployed or created. Similarly, deletion of all CGW's except the last one can be done in parallel.

Deploy - Cisco Cloud onRamp for Multi-Cloud using Google Cloud

This section covers the steps to deploy Cisco Cloud onRamp feature using Multi-Cloud.


Cisco vManage
Select Resource Group
admin
CONFIGURATION | CLOUD ONRAMP FOR MULTI-CLOUD
Navigation
Cloud
Interconnect
Configuration
Devices
TLS/SSL Proxy
Certificates
Network Design
Templates
Policies
Security
Unified Communications
Cloud onRamp for SaaS
Cloud onRamp for IaaS
Cloud onRamp for Multi-Cloud
Cloud onRamp for Multi-Cloud
Cloud onRamp for Colocation
Add a cloud provider to your network
Prerequisites
Cloud Account Details, isco Wan Edge License, bscription to Marketplace
Setup
Associate and manage cloud accounts for subsequent usage. Provide Global configuration(s)
Discover & Tag
Discover and associate Tags to Host Private Networks for use in Intent Management
Manage
Deploy and manage Cloud Gateway(s)
Intent Management
Specify the Branch to Cloud connectivity and Intra Cloud Resources Intent
SETUP
Associate Cloud Account
Account Management
Cloud Global Settings
DISCOVER
Host Private Networks
MANAGE
Create Cloud Gateway
Gateway Management
INTENT MANAGEMENT
Cloud Connectivity

Configuration Workflows

- Prerequisites: This workflow includes all the prerequisites to enable and collect APIs, private keys etc. from the Google cloud account, followed by the steps to set up unused Catalyst8000v routers with device templates attached to it.
- Setup: This workflow includes the addition of the Google billing ID and the Google private key credentials within vManage, followed by the successful completion of the global settings required to successfully bring up Cloud Gateways.
- Discover &Tag: This workflow includes the discovery and association of Google Host VPCs to tags. You will use these tags later within the Intent Matrix page, where in you map tags to a service side VPN.
- Manage: This workflow creates and manages Cisco Catalyst 8000v virtual routers acting as cloud gateways. During this step, Cisco vManage will create three Google cloud VPCs, one for the WAN interface, one for the Site-to-Cloud (S2C) use case and the last one for the Site-to-Site (S2S) use case.
- Intent Management: The workflow maps the tags to the service side VPN. This allows on-premise branches to access Google cloud resources through the Site-to-Cloud VPC.

© 2020 Cisco and/or its affiliates. All rights reserved.

Process 1: Prerequisites Part 1 - Google Cloud Prerequisites

The procedures in this section list out the prerequisites to be completed within the Google cloud platform.

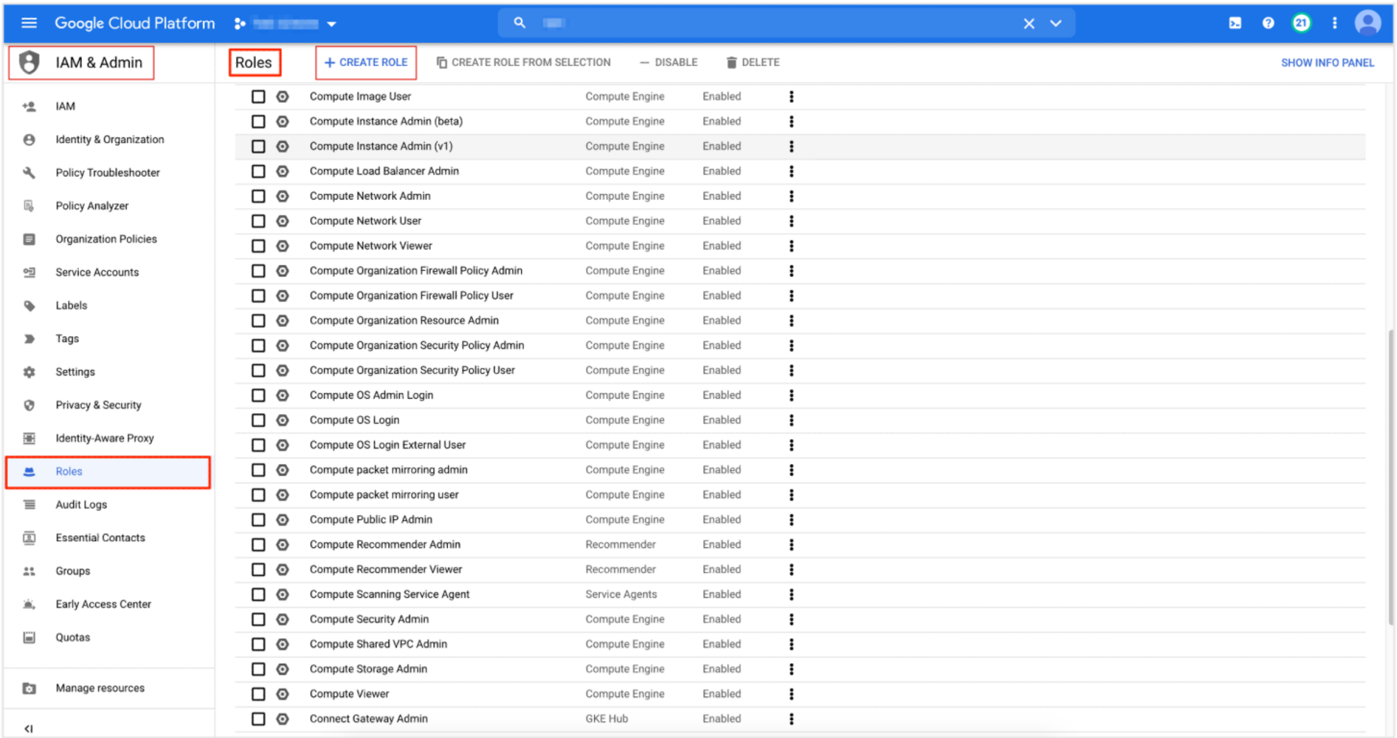
Procedure 1: Google Cloud Subscription

Ensure you have a Google Cloud account subscription as the account details are required to associate your Google cloud account with Cisco vManage.

Step 1. Ensure you have the following roles **Enabled** to your Google account.

- Service Account User
- Compute Instance Admin (v1)
- Compute Network Admin
- Compute Public IP Admin
- Compute Security Admin
- Hub & Spoke Admin
- Spoke Admin

Navigate to **IAM & Admin** > **Roles**, click on **+CREATE ROLE** to enable the required role.



□	Compute Image User	Compute Engine	Enabled	⋮
□	Compute Instance Admin (beta)	Compute Engine	Enabled	⋮
□	Compute Instance Admin (v1)	Compute Engine	Enabled	⋮
□	Compute Load Balancer Admin	Compute Engine	Enabled	⋮
□	Compute Network Admin	Compute Engine	Enabled	⋮
□	Compute Network User	Compute Engine	Enabled	⋮
□	Compute Network Viewer	Compute Engine	Enabled	⋮
□	Compute Organization Firewall Policy Admin	Compute Engine	Enabled	⋮
□	Compute Organization Firewall Policy User	Compute Engine	Enabled	⋮
□	Compute Organization Resource Admin	Compute Engine	Enabled	⋮
□	Compute Organization Security Policy Admin	Compute Engine	Enabled	⋮
□	Compute Organization Security Policy User	Compute Engine	Enabled	⋮
□	Compute OS Admin Login	Compute Engine	Enabled	⋮
□	Compute OS Login	Compute Engine	Enabled	⋮
□	Compute OS Login External User	Compute Engine	Enabled	⋮
□	Compute packet mirroring admin	Compute Engine	Enabled	⋮
□	Compute packet mirroring user	Compute Engine	Enabled	⋮
□	Compute Public IP Admin	Compute Engine	Enabled	⋮
□	Compute Recommender Admin	Recommender	Enabled	⋮
□	Compute Recommender Viewer	Recommender	Enabled	⋮
□	Compute Scanning Service Agent	Service Agents	Enabled	⋮
□	Compute Security Admin	Compute Engine	Enabled	⋮
□	Compute Shared VPC Admin	Compute Engine	Enabled	⋮
□	Compute Storage Admin	Compute Engine	Enabled	⋮
□	Compute Viewer	Compute Engine	Enabled	⋮
□	Connect Gateway Admin	GKE Hub	Enabled	⋮

Procedure 2: Google Cloud API

Within your Google cloud account, the following APIs must be enabled, before you begin with the cloud onRamp workflow.

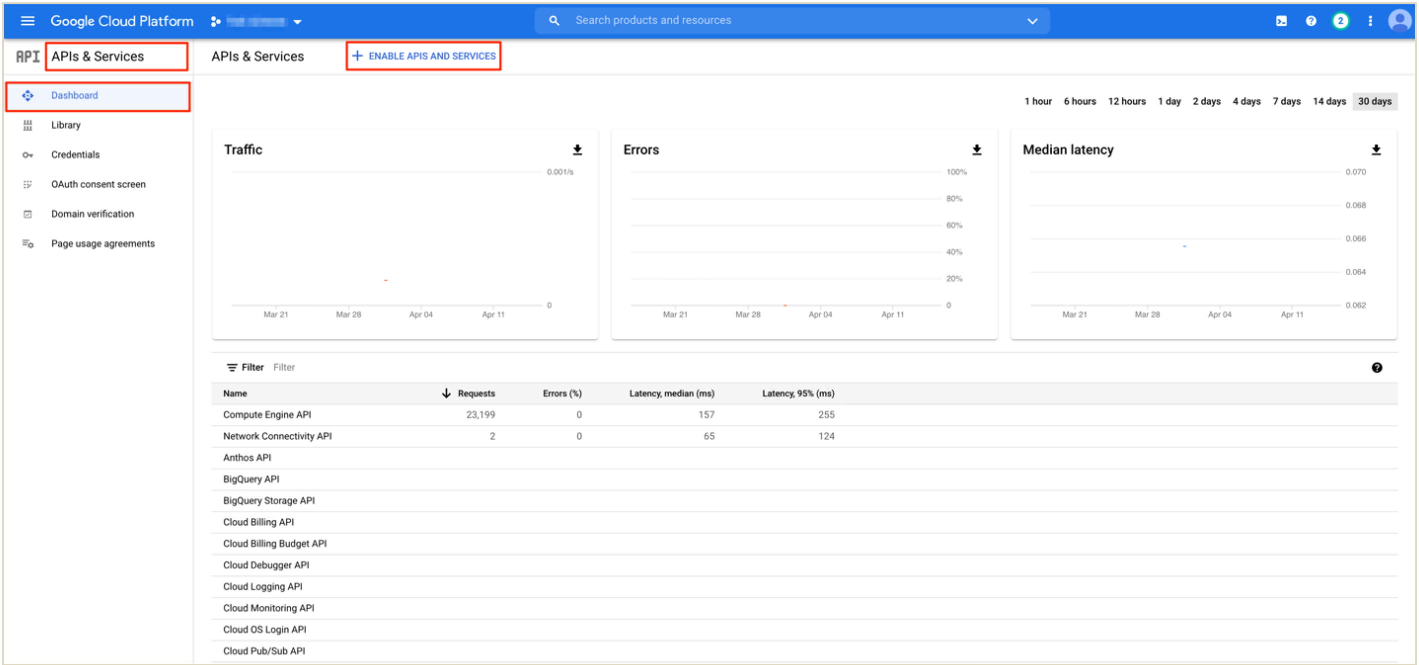
Ensure that following Google Cloud APIs are enabled in the relevant google project:

© 2020 Cisco and/or its affiliates. All rights reserved.

- Compute Engine API: This API is needed to create and run virtual machine, VPCs and firewall rules within the Google Cloud Platform.
- Cloud Billing API: This API is required to manage and validate billing for their Google Cloud Platform projects programmatically. In this guide, we have enabled both the cloud billing budget API and cloud billing API.
- Network Connectivity Center Alpha API: This API is needed to access, create and manage Network Connectivity Center hub and spoke resources.

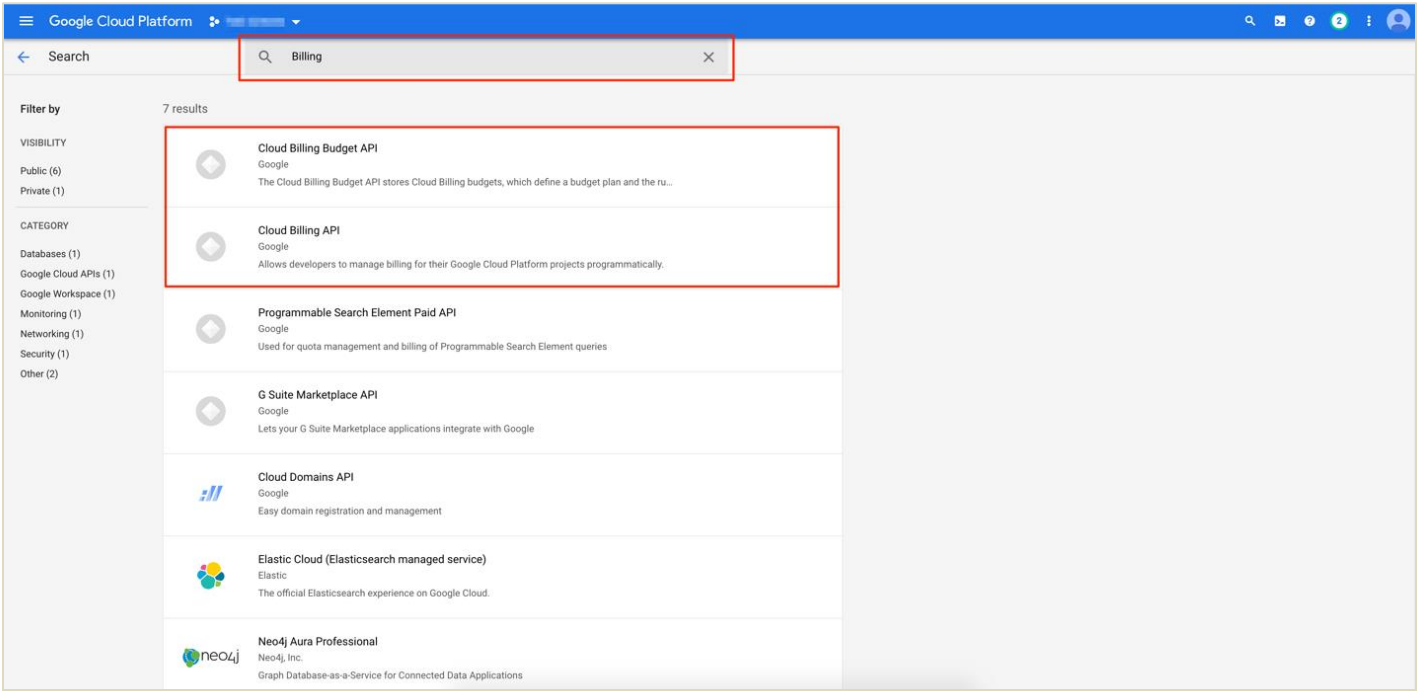
Technical Tip
Your Google Cloud Project must have Network Connectivity Center Alpha APIs enabled. To enable this API, reach out to your Google contact.

Step 1. Navigate to **APIs & Services**. Under Dashboard, click on **+ENABLE APIS AND SERVICES**.



Name	↓ Requests	Errors (%)	Latency, median (ms)	Latency, 95% (ms)
Compute Engine API	23,199	0	157	255
Network Connectivity API	2	0	65	124
Anthos API				
BigQuery API				
BigQuery Storage API				
Cloud Billing API				
Cloud Billing Budget API				
Cloud Debugger API				
Cloud Logging API				
Cloud Monitoring API				
Cloud OS Login API				
Cloud Pub/Sub API				

Step 2. Enter the APIs within the search bar and click **Enable**. The following screenshots display, the APIs enabled in this deployed.



7 results

Cloud Billing Budget API
Google
The Cloud Billing Budget API stores Cloud Billing budgets, which define a budget plan and the ru...

Cloud Billing API
Google
Allows developers to manage billing for their Google Cloud Platform projects programmatically.

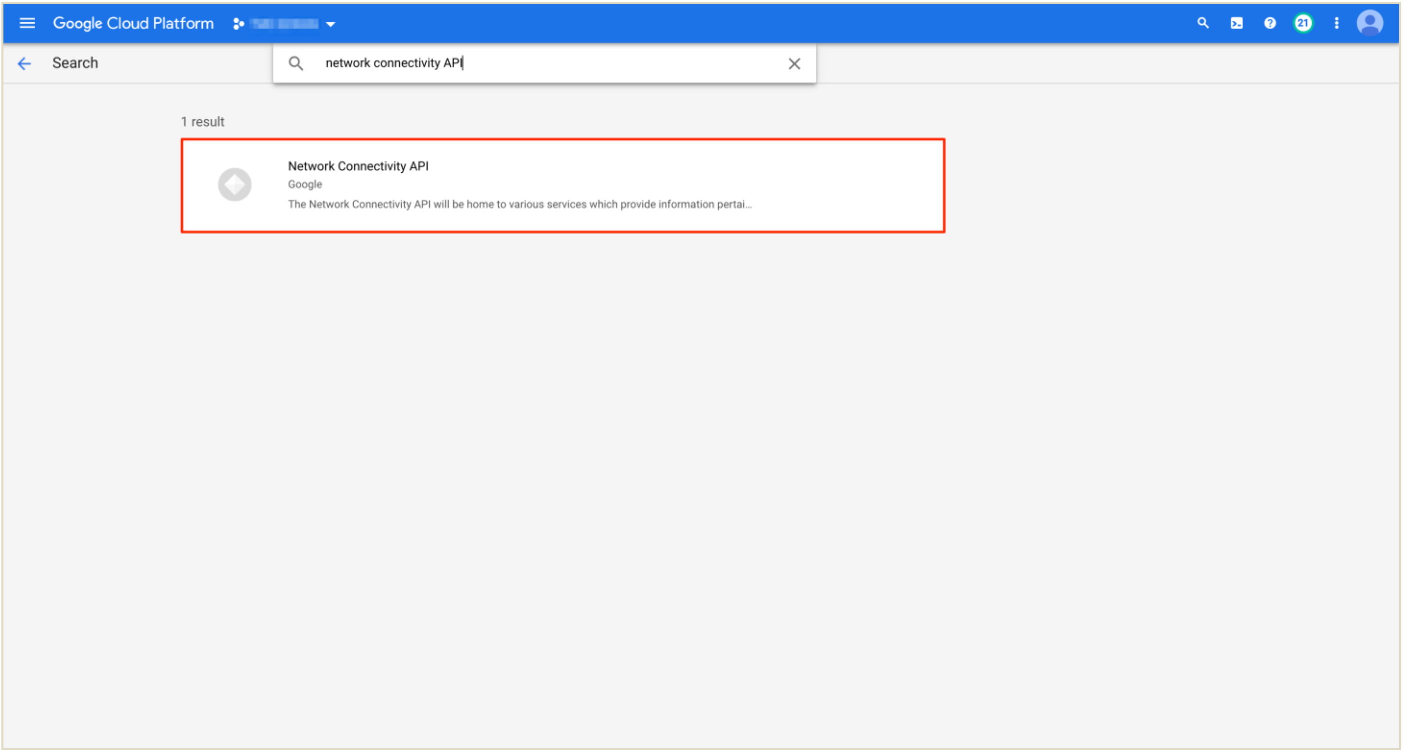
Programmable Search Element Paid API
Google
Used for quota management and billing of Programmable Search Element queries

G Suite Marketplace API
Google
Lets your G Suite Marketplace applications integrate with Google

Cloud Domains API
Google
Easy domain registration and management

Elastic Cloud (Elasticsearch managed service)
Elastic
The official Elasticsearch experience on Google Cloud.

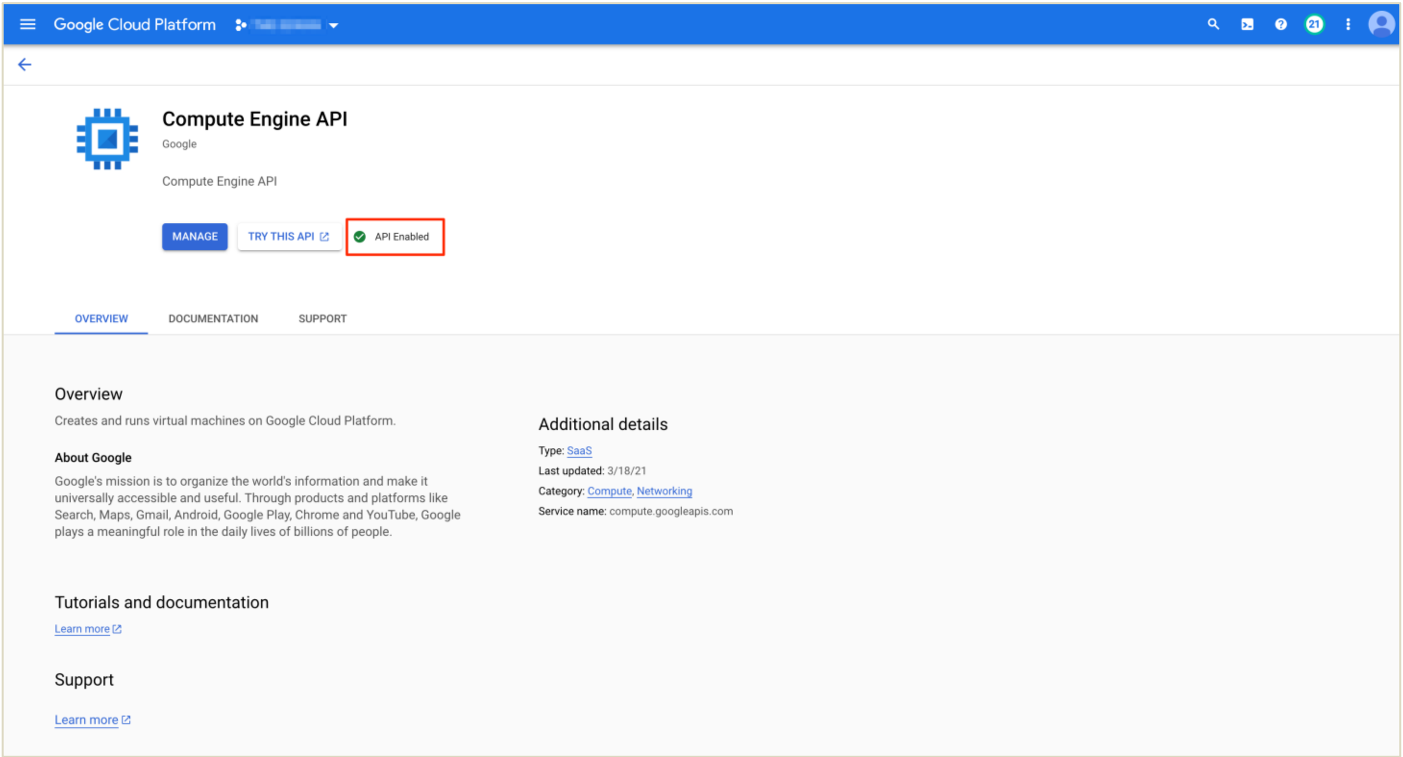
Neo4j Aura Professional
Neo4j, Inc.
Graph Database-as-a-Service for Connected Data Applications



1 result

Network Connectivity API
Google
The Network Connectivity API will be home to various services which provide information pertai...

© 2020 Cisco and/or its affiliates. All rights reserved.



Overview

Creates and runs virtual machines on Google Cloud Platform.

About Google

Google's mission is to organize the world's information and make it universally accessible and useful. Through products and platforms like Search, Maps, Gmail, Android, Google Play, Chrome and YouTube, Google plays a meaningful role in the daily lives of billions of people.

Additional details

Type: SaaS
Last updated: 3/18/21
Category: Compute, Networking
Service name: compute.googleapis.com

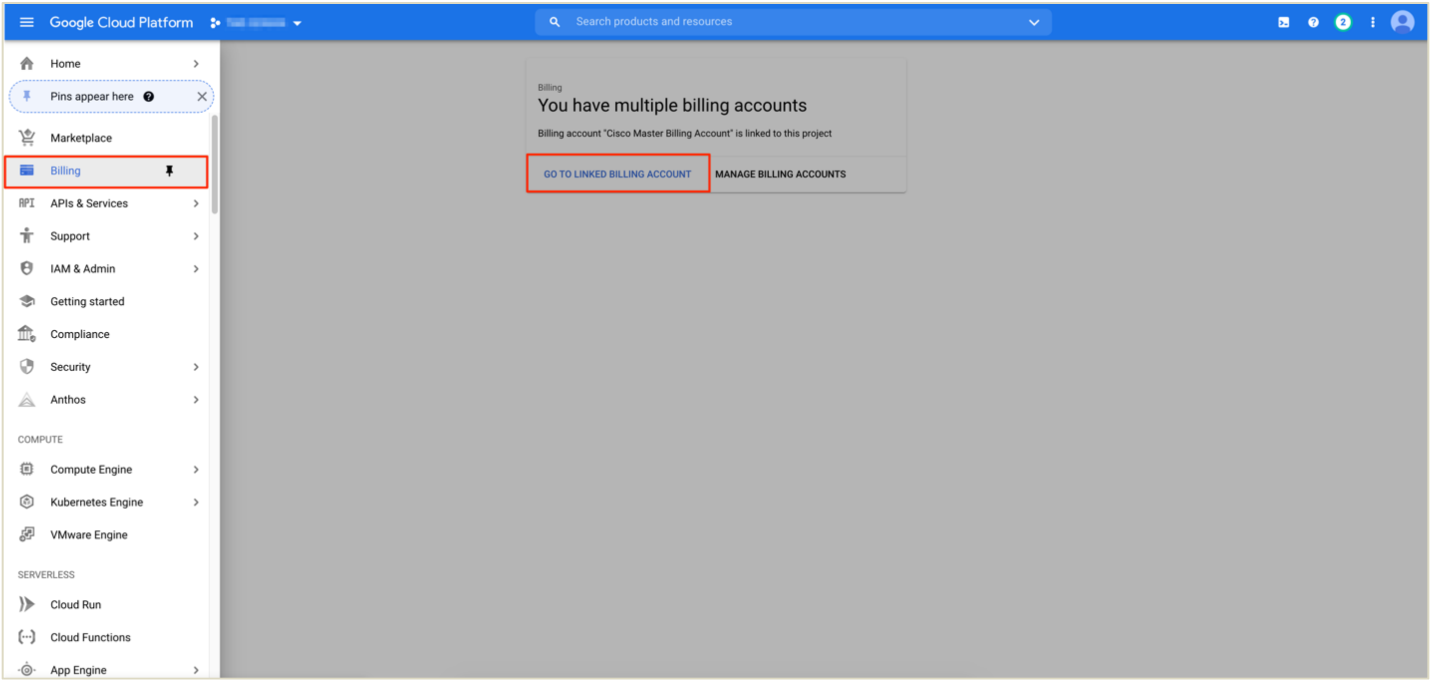
Tutorials and documentation

Learn more

Support

Learn more

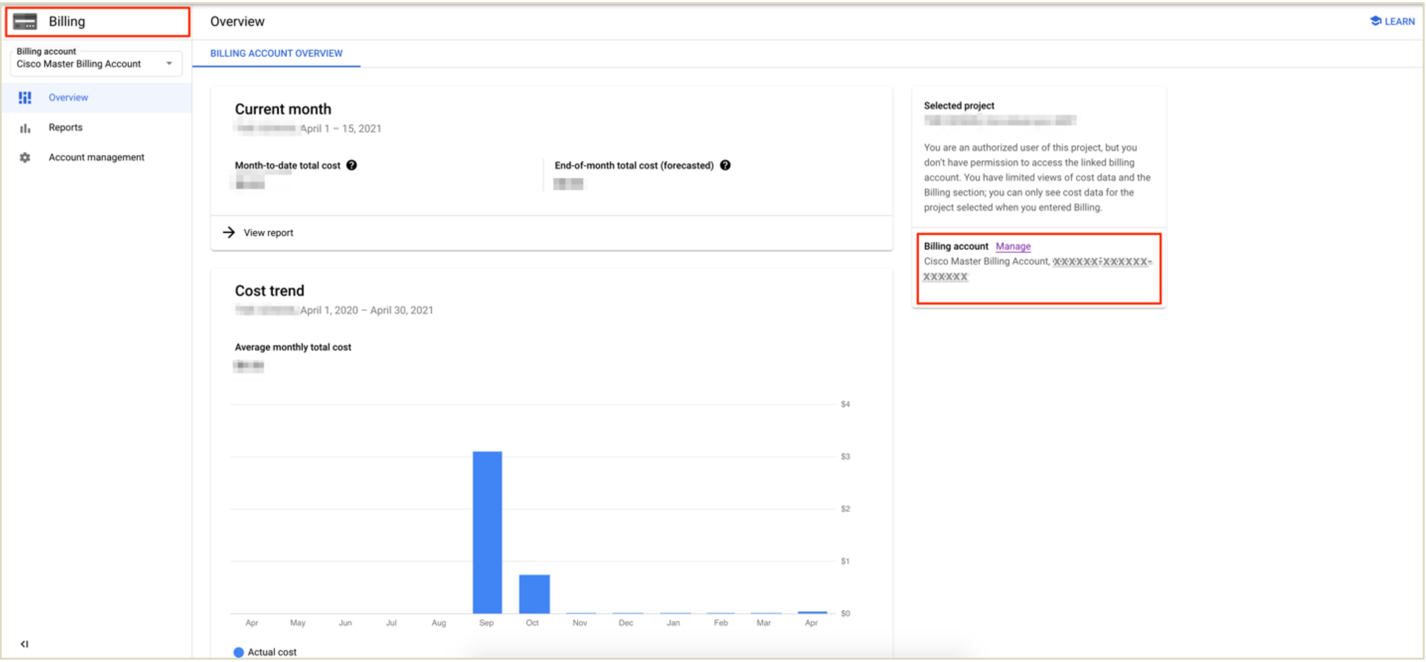
Step 3. While associating your Google Cloud account with your vManage, you can optionally add your Google Cloud billing ID. Navigate to **Google Cloud platform**, click on **Billing** from the hamburger (≡) drop-down menu and click on your **GO TO LINKED BILLING ACCOUNT**.



You have multiple billing accounts

Billing account "Cisco Master Billing Account" is linked to this project

Step 4. Within **Billing**, select **Overview**. On the right side of the screen, you will find your billing account ID. Copy this ID as you need to enter this later while associating your Google Cloud account to your vManage controller.



Billing

Billing account
Cisco Master Billing Account

Overview

Reports

Account management

Overview

LEARN

BILLING ACCOUNT OVERVIEW

Current month

[redacted] April 1 – 15, 2021

Month-to-date total cost

[redacted]

End-of-month total cost (forecasted)

[redacted]

View report

Cost trend

[redacted] April 1, 2020 – April 30, 2021

Average monthly total cost

[redacted]

Selected project

[redacted]

You are an authorized user of this project, but you don't have permission to access the linked billing account. You have limited views of cost data and the Billing section; you can only see cost data for the project selected when you entered Billing.

Billing account Manage

Cisco Master Billing Account, XXXXXX-XXXXXX-XXXXXX

Procedure 3: Service Account and Private Key

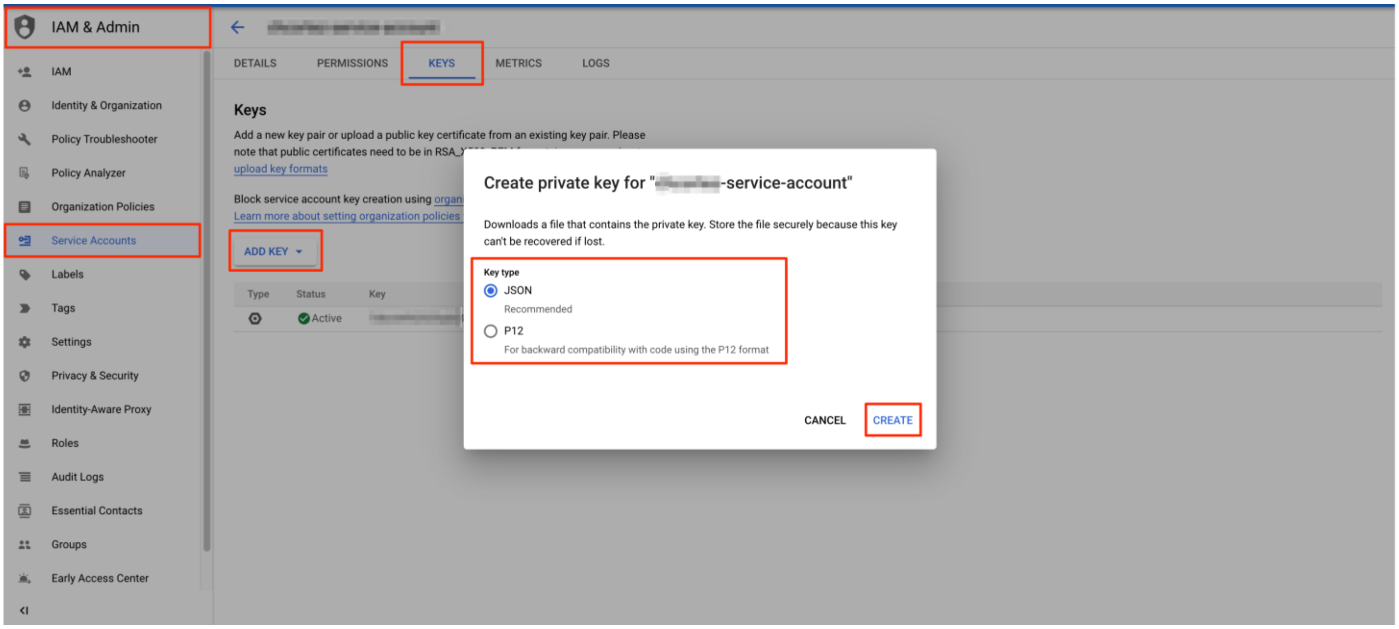
In order to complete all the necessary cloud operations as a part of the cloud onRamp workflow, vManage NMS stores the Google account information in its database. To authenticate and accept the Google Account, vManage NMS uses the service account key method for authentication.

Therefore, if you do not have a service account in Google Cloud Platform defined for this purpose, you will need to create a new one and within the newly created service account a private key must be generated.

Technical Tip
Ensure that you create dedicated service accounts for each project that will have a host VPC.

Step 1. Navigate to **IAM & Admin** > **Service Accounts** and under **Keys**, click **ADD KEYS** and then select "Create new key" from the drop-down menu. to create and associate a new private key to your service account. The private key ID may be in **JSON** or **P12** - REST API formats. The format depends on the method of key generation.

The private key data returned is a base64-encoded string representation of the key. vManage will support both the aforesaid formats as input of the service account key. Once the type is chosen, click **Create.**



Keys

Add a new key pair or upload a public key certificate from an existing key pair. Please note that public certificates need to be in RSA_X509_PEM format. upload key formats

Block service account key creation using organ… Learn more about setting organization policies

Create private key for "[redacted]-service-account"

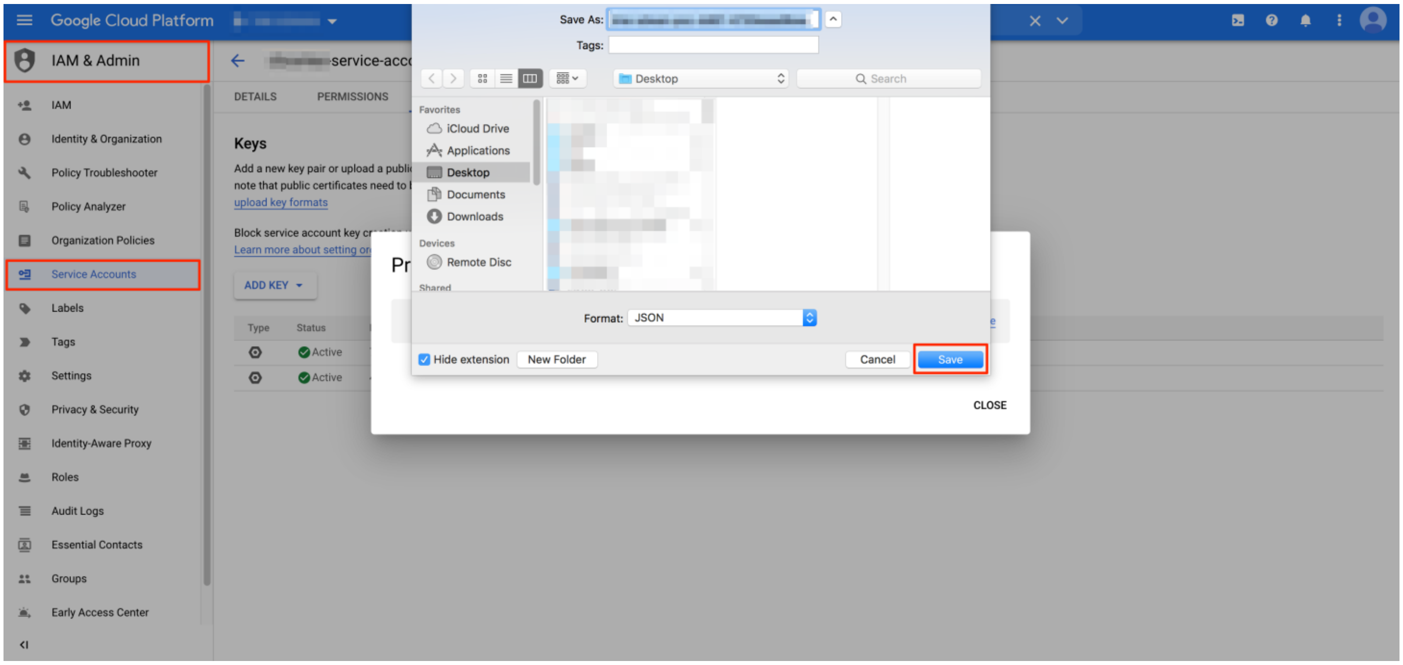
Downloads a file that contains the private key. Store the file securely because this key can't be recovered if lost.

Key type

● JSON
Recommended

○ P12
For backward compatibility with code using the P12 format

Step 2. Download or **Save** your key. This private key will be uploaded to your vManage while associating your Google account in the configuration workflow.



[redacted]service-acc…

Keys

Add a new key pair or upload a publi… note that public certificates need to… upload key formats

Block service account key cr… Learn more about setting or…

Save As: [redacted]

Tags:

Desktop

Format: JSON

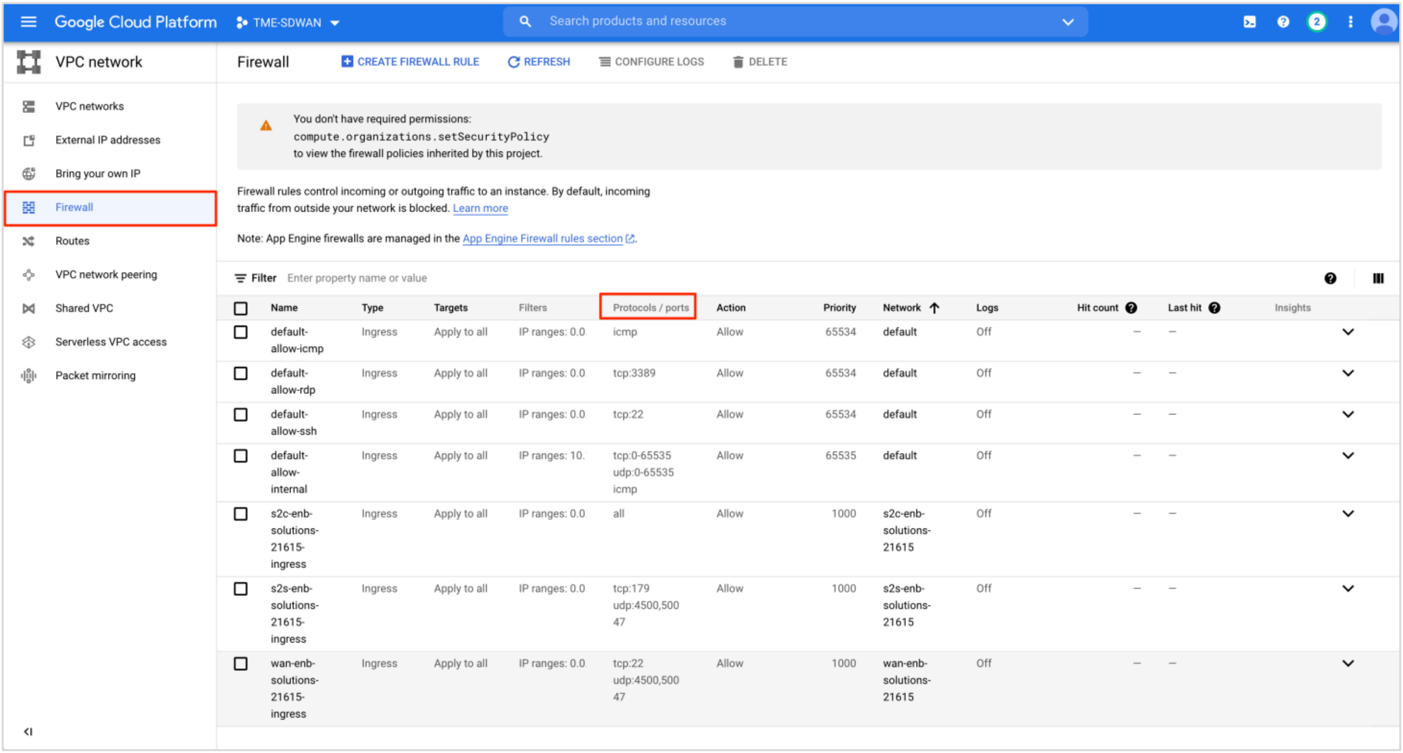
☑ Hide extension

Note, once the key file has been downloaded, the same can be used on multiple vManage/domain controllers without repeating the authorization process for each controller.

Technical Tip
vManage will not allow updates to the credentials data. In order to update, user will have to first deregister the account with vManage and register afresh.

Procedure 4: Firewall Requirements

The following TCP, UDP and ICMP ports are automatically allowed for incoming traffic in Google Cloud upon completion of site-to-cloud and site-to-site workflows and each of the firewall rules are attached to the Site-to-Cloud/ Site-to-Site/ WAN VPCs. In Google Cloud Platform (GCP), all the ports for egress or outgoing traffic are automatically opened. The following example lists out the ingress **Protocols/Ports**, allowed within the Google Cloud firewall rules.



You don't have required permissions:
`compute.organizations.setSecurityPolicy`
to view the firewall policies inherited by this project.

Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. Learn more

Note: App Engine firewalls are managed in the App Engine Firewall rules section.

□	Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Network	Logs	Hit count	Last hit	Insights
□	default-allow-icmp	Ingress	Apply to all	IP ranges: 0.0.	icmp	Allow	65534	default	Off	–	–	
□	default-allow-rdp	Ingress	Apply to all	IP ranges: 0.0.	tcp:3389	Allow	65534	default	Off	–	–	
□	default-allow-ssh	Ingress	Apply to all	IP ranges: 0.0.	tcp:22	Allow	65534	default	Off	–	–	
□	default-allow-internal	Ingress	Apply to all	IP ranges: 10.	tcp:0-65535 udp:0-65535 icmp	Allow	65535	default	Off	–	–	
□	s2c-enb-solutions-21615-ingress	Ingress	Apply to all	IP ranges: 0.0.	all	Allow	1000	s2c-enb-solutions-21615	Off	–	–	
□	s2s-enb-solutions-21615-ingress	Ingress	Apply to all	IP ranges: 0.0.	tcp:179 udp:4500,500 47	Allow	1000	s2s-enb-solutions-21615	Off	–	–	
□	wan-enb-solutions-21615-ingress	Ingress	Apply to all	IP ranges: 0.0.	tcp:22 udp:4500,500 47	Allow	1000	wan-enb-solutions-21615	Off	–	–	

The protocols allowed automatically on WAN VPC,

- TCP: 22
- UDP: 4500, 500

The protocols allowed automatically on S2C VPC,

- ALL

The protocols allowed automatically on S2S VPC,

- TCP: 179
- UDP: 4500, 500

And by default, for all VPCs these ports are allowed,

- TCP: 3389, 22, 0-65535
- UDP: 0-65535
- ICMP

The DTLS control connections to vBond, vSmart and vManage are initiated from the WAN Edge device. Once the control connections are initiated from the WAN Edge device (Catalyst8000v), Google cloud maintains a stateful session to the destination IP/ port/ protocol to complete the authentication process and bring up of the WAN Edge devices. Therefore, no ports need to be manually opened by the user in the Google Firewall to establish control and data plane connections.

However, make sure to open DTLS/TLS ports within the on-premises firewall to establish control and data plane connections with your cloud devices. For details on the ports to be opened, refer to the Cisco SD-WAN Design Guide.

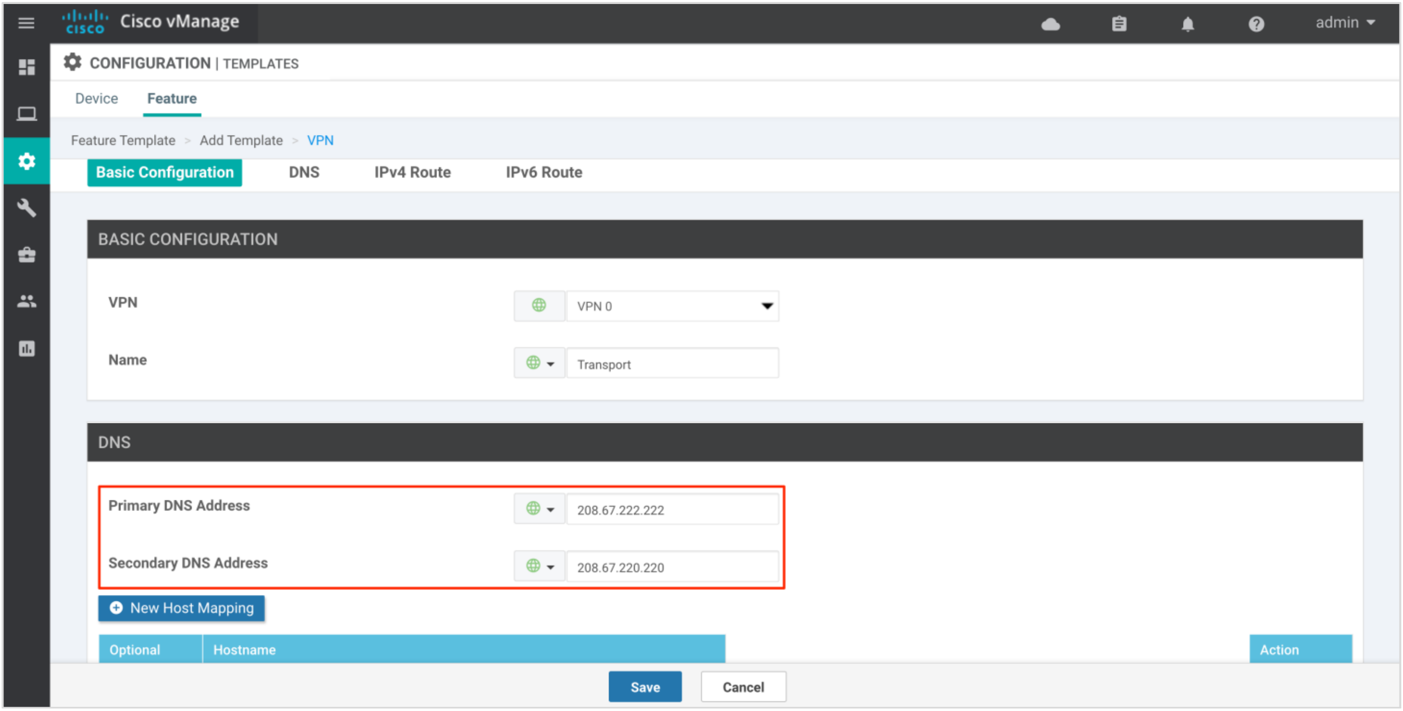
Process 1: Prerequisites - Part 2 - vManage Prerequisites

This section focuses on all the prerequisites within the vManage NMS.

Procedure 1: vManage Internet Access

Step 1. Make sure that your vManage server has access to the Internet and that it has a DNS server configured so that it can reach Google Cloud. To enable the DNS server configuration, you can configure this either within the VPN feature template associated with your vManage device template or via CLI.

Option 1: If your vManage is configured using the vManage device templates, then a DNS server configuration is added in the vManage VPN 0 feature template. To configure a DNS server in vManage VPN 0, enter the IP address of a DNS server and then save the edited feature template.



VPN: VPN 0

Name: Transport

Primary DNS Address: 208.67.222.222

Secondary DNS Address: 208.67.220.220

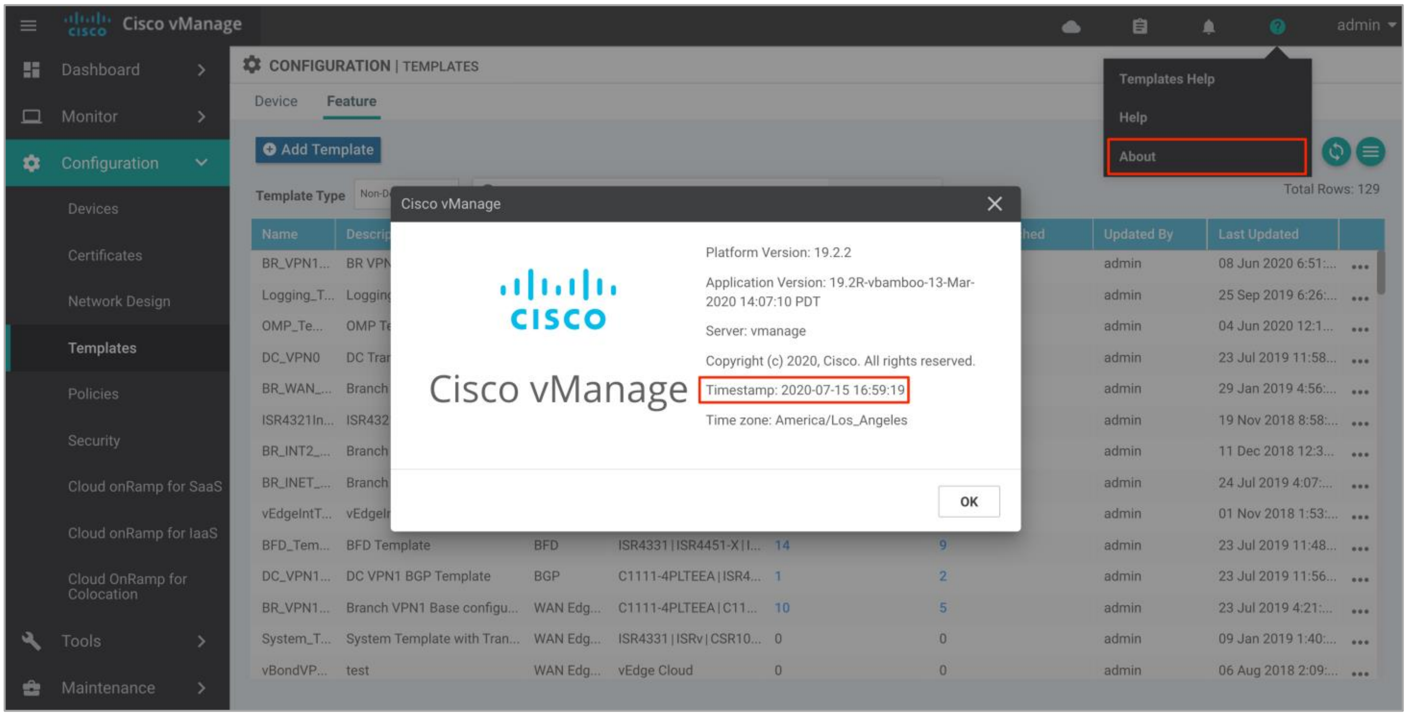
Option 2: If your vManage is configured manually via CLI, then log into the vManage GUI and navigate to **Tools** > **SSH Terminal**. Click on the vManage server from the device group, log in with the admin username and password, and enter the following commands:

```
vManage(config)# vpn 0
vManage(config-vpn-0)# dns 208.67.222.222 primary
vManage(config-vpn-0)# dns 208.67.220.220 secondary
vManage(config-vpn-0)# commit
```

Procedure 2: vManage Time Server Synchronization

Step 1. Ensure that the vManage NMS server is synchronized to the current time. To check the current time, click the Help (?) icon in the top bar of the vManage screen or issue a “show clock” via CLI.

© 2020 Cisco and/or its affiliates. All rights reserved.



Cisco vManage

Platform Version: 19.2.2

Application Version: 19.2R-vbamboo-13-Mar-2020 14:07:10 PDT

Server: vmanage

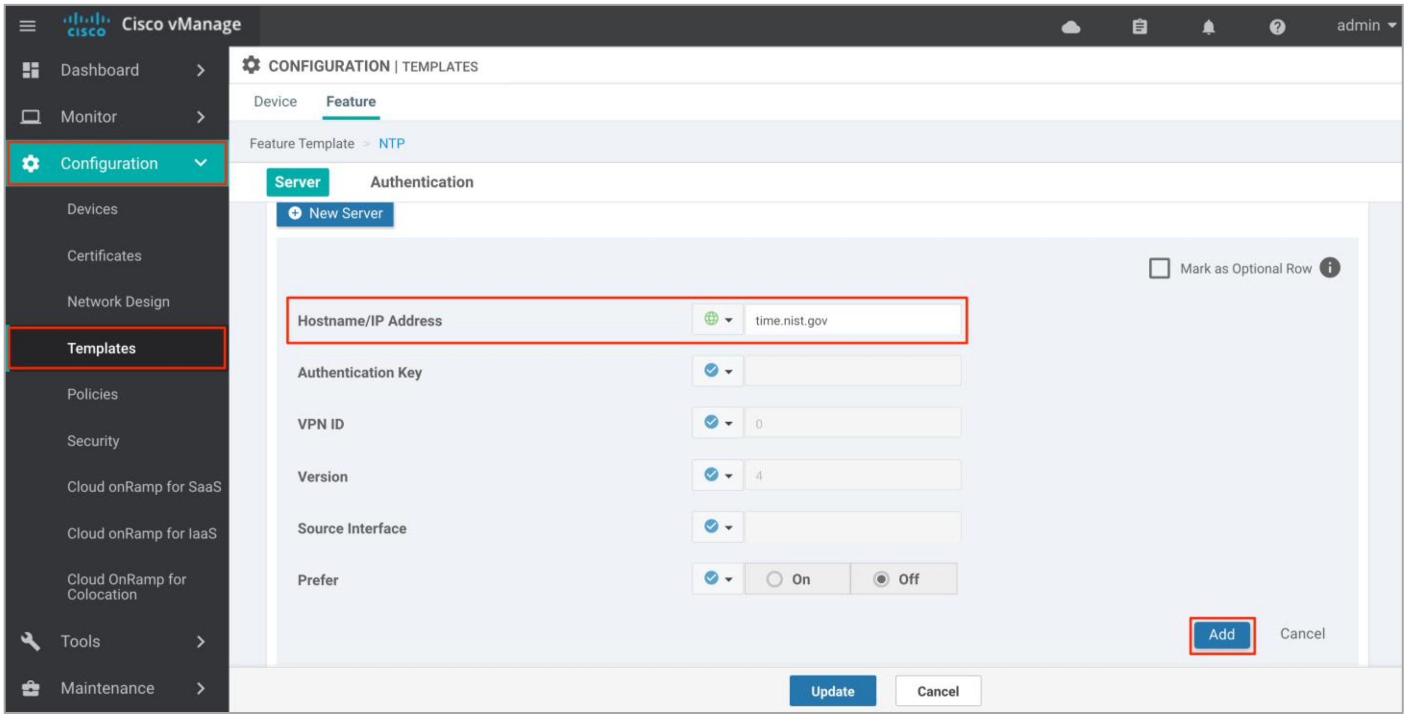
Copyright (c) 2020, Cisco. All rights reserved.

Timestamp: 2020-07-15 16:59:19

Time zone: America/Los_Angeles

Step 2. The Timestamp field shows the current time. If the time mentioned is incorrect, configure the vManage server's time to point to an NTP time server, such as the Google NTP server. To do this, either an NTP feature template can be associated within the vManage device template, or you can configure it manually via CLI.

Option 1: To configure or update the vManage NTP feature template, enter the **Hostname/ IP Address** of an NTP server, and then attach the new or updated feature template within the vManage device template.



Hostname/IP Address: time.nist.gov

Authentication Key:

VPN ID: 0

Version: 4

Source Interface:

Prefer: ○ On ● Off

Option 2: To configure an NTP server via CLI, login to the vManage GUI and navigate to **Tools** > **SSH Terminal.** Click on the vManage server from the device group, log in with the admin username and password, and enter the following commands:

```
vManage# config t
```

```
vManage(config)# system
vManage(config-system)# ntp
vManage(config-ntp)# server time.nist.gov
vManage(config-server-time.nist.gov)# version 4
vManage(config-server-time.nist.gov)# commit
Commit complete.
```

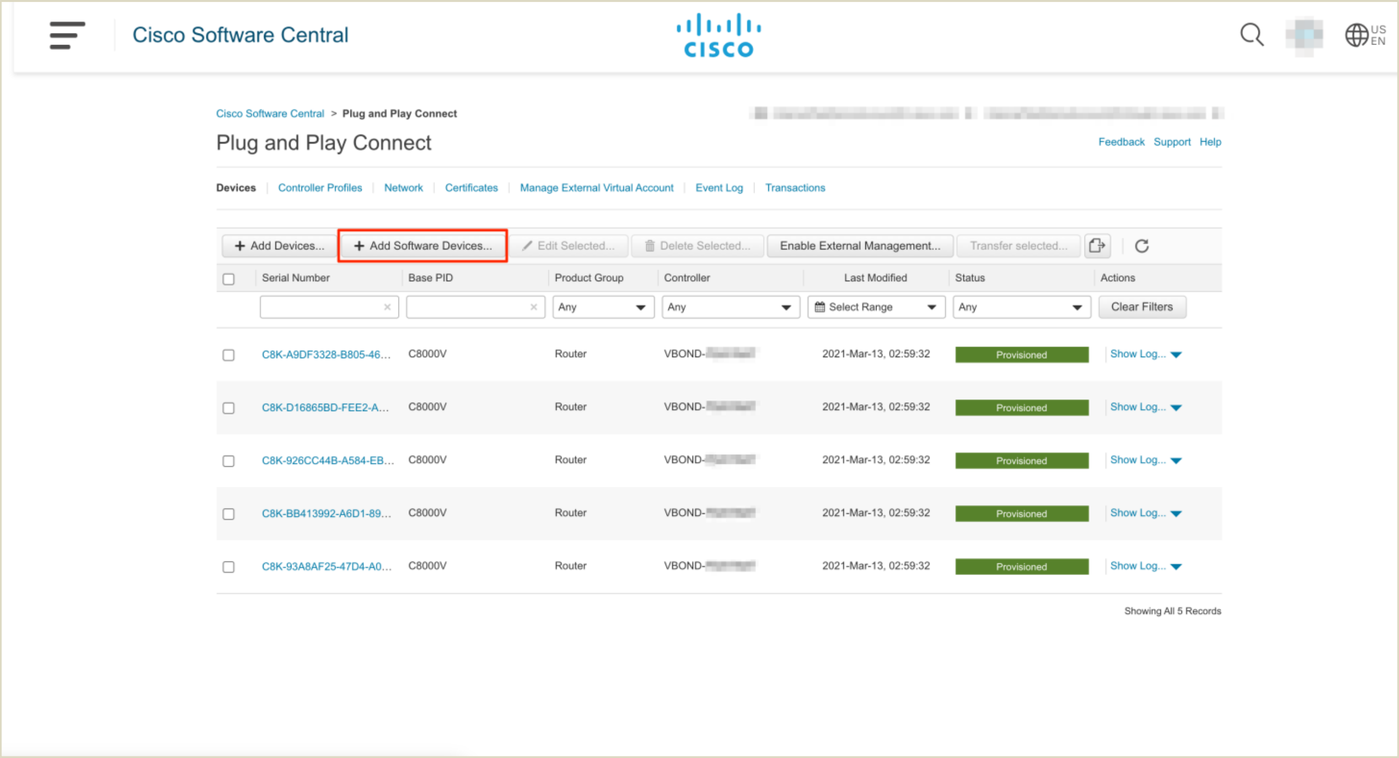
Procedure 2: Verify you have at least four unused Cisco Catalyst 8000v routers in vManage

To complete the site-to-cloud and site-to-site use case, four Catalyst 8000v devices are deployed in Google cloud. Two of the routers are deployed in region 1 and a second pair of devices are deployed in a different region, Region 2. Each of the WAN Edge devices are placed in separate zones (automatically?) for fault-tolerance with high availability.

In this workflow, a pair of unused Catalyst8000v devices are deployed in US-West1 region and a second pair of unused Catalyst8000v devices are deployed in US-West2 region. Therefore, a total of four unused Catalyst8000v devices must be attached to a vManage device template.

Begin by adding Catalyst 8000v routers within your vManage device list.

Step 1. Login to Cisco **Plug and Play portal Connect** via URL **-** https://software.cisco.com/#pnp-devices . Under the **Devices** tab, click **+ Add Software Devices** to add the devices to the portal.



Cisco Software Central
US
EN

Cisco Software Central > Plug and Play Connect [redacted]

Plug and Play Connect

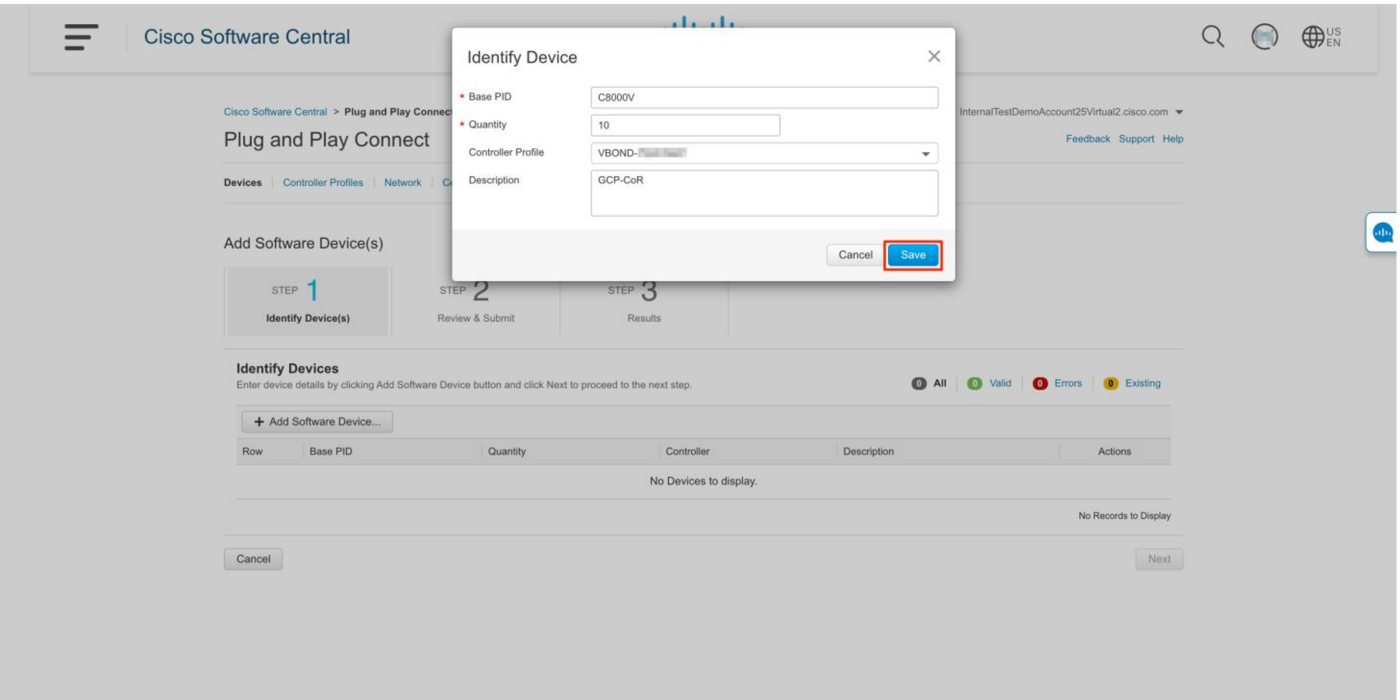
Feedback Support Help
Devices | Controller Profiles | Network | Certificates | Manage External Virtual Account | Event Log | Transactions
+ Add Devices... | + Add Software Devices... | Edit Selected... | Delete Selected... | Enable External Management... | Transfer selected...
Clear Filters

□	Serial Number	Base PID	Product Group	Controller	Last Modified	Status	Actions
			Any	Any	Select Range	Any	Clear Filters
□	C8K-A9DF3328-B805-46...	C8000V	Router	VBOND-[redacted]	2021-Mar-13, 02:59:32	Provisioned	Show Log...
□	C8K-D16865BD-FEE2-A...	C8000V	Router	VBOND-[redacted]	2021-Mar-13, 02:59:32	Provisioned	Show Log...
□	C8K-926CC44B-A584-EB...	C8000V	Router	VBOND-[redacted]	2021-Mar-13, 02:59:32	Provisioned	Show Log...
□	C8K-BB413992-A6D1-89...	C8000V	Router	VBOND-[redacted]	2021-Mar-13, 02:59:32	Provisioned	Show Log...
□	C8K-93A8AF25-47D4-A0...	C8000V	Router	VBOND-[redacted]	2021-Mar-13, 02:59:32	Provisioned	Show Log...

Showing All 5 Records

Step 2. To add Catalyst 8000v devices, enter **Base PID** as **CATALYST 8000V** and **Quantity** as 4 or more, and select your **Controller Profile** from the drop-down option. Click **Save**, then **Next.** then **Submit**. Click **Done**.

© 2020 Cisco and/or its affiliates. All rights reserved.



Cisco Software Central
US
EN
Cisco Software Central > Plug and Play Connec
InternalTestDemoAccount25Virtual2.cisco.com
Feedback Support Help
Devices | Controller Profiles | Network | C
STEP 1 Identify Device(s)
STEP 2 Review & Submit
STEP 3 Results
+ Add Software Device...
Cancel
Next

Plug and Play Connect

Add Software Device(s)

Identify Device

* Base PID: C8000V

* Quantity: 10

Controller Profile: VBOND-[redacted]

Description: GCP-CoR

Cancel Save

Identify Devices

Enter device details by clicking Add Software Device button and click Next to proceed to the next step.

0 All | 0 Valid | 0 Errors | 0 Existing

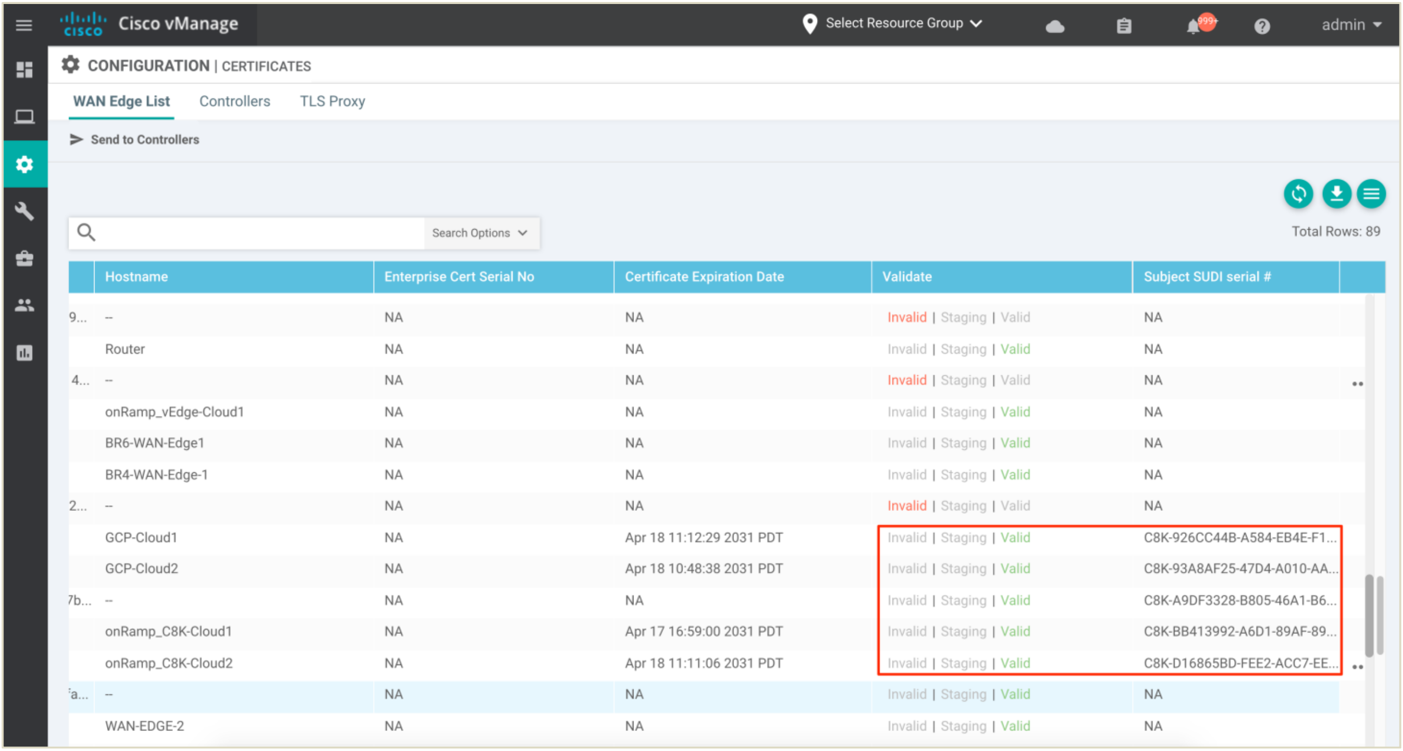
Row	Base PID	Quantity	Controller	Description	Actions

No Devices to display.

No Records to Display

Step 3. Navigate to **Configuration** > **Devices** > **Sync Smart Account** to sync your vManage controllers to the **Cisco Plug and Play** portal. This automatically adds the newly generated devices to the vManage device list.

To add the new devices to your vManage controller manually, within the Plug and Play portal, go to the **Controller Profiles** tab, download the **Provisioning File** available within right side corner of the **Controller Profile** page. Once downloaded, navigate to vManage NMS server and go to **Configuration** > **Devices > Upload WAN Edge List**. Do not forget to click on the checkbox "**Validate the uploaded vEdge List and send to controllers**" before uploading the device list.



CONFIGURATION | CERTIFICATES

WAN Edge List | Controllers | TLS Proxy

Total Rows: 89

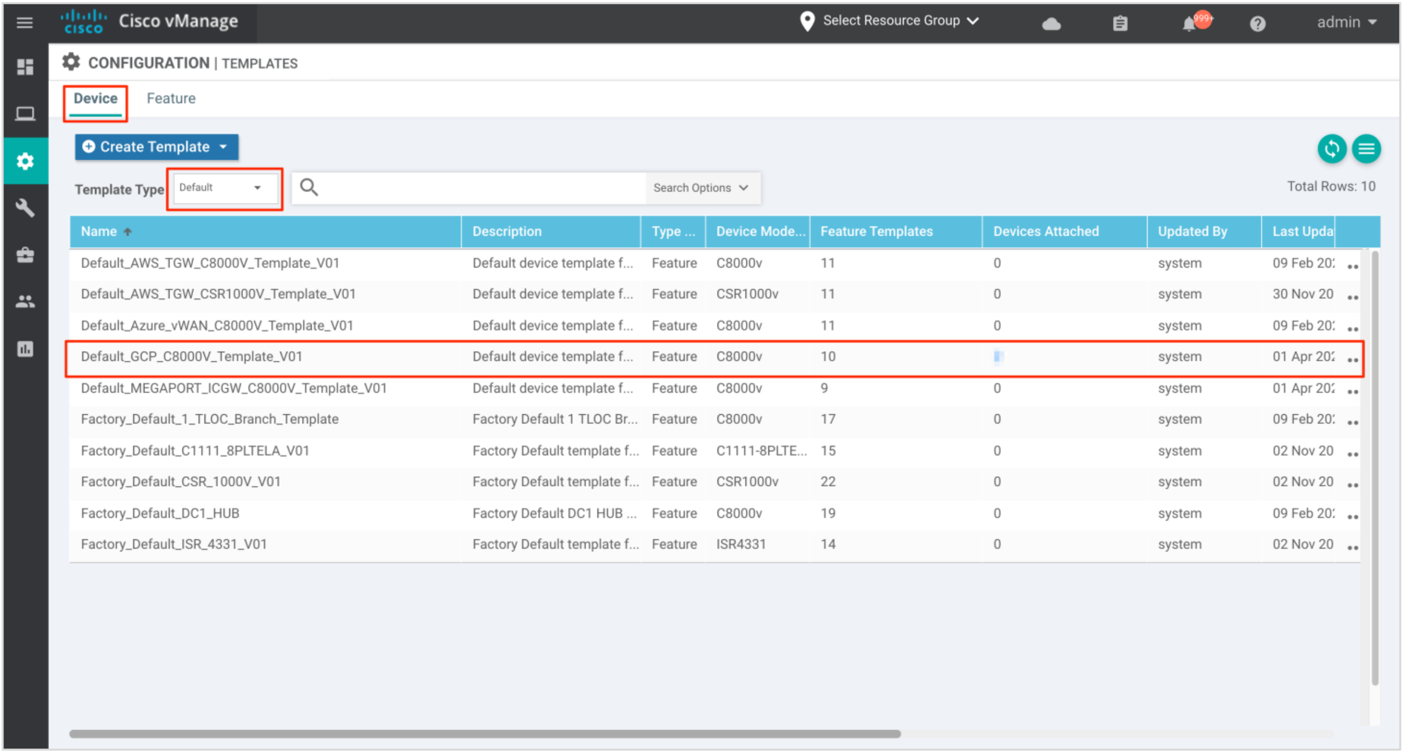
	Hostname	Enterprise Cert Serial No	Certificate Expiration Date	Validate	Subject SUDI serial #
9...	--	NA	NA	Invalid | Staging | Valid	NA
	Router	NA	NA	Invalid | Staging | Valid	NA
4...	--	NA	NA	Invalid | Staging | Valid	NA
	onRamp_vEdge-Cloud1	NA	NA	Invalid | Staging | Valid	NA
	BR6-WAN-Edge1	NA	NA	Invalid | Staging | Valid	NA
	BR4-WAN-Edge-1	NA	NA	Invalid | Staging | Valid	NA
2...	--	NA	NA	Invalid | Staging | Valid	NA
	GCP-Cloud1	NA	Apr 18 11:12:29 2031 PDT	Invalid | Staging | Valid	C8K-926CC44B-A584-EB4E-F1...
	GCP-Cloud2	NA	Apr 18 10:48:38 2031 PDT	Invalid | Staging | Valid	C8K-93A8AF25-47D4-A010-AA...
7b...	--	NA	NA	Invalid | Staging | Valid	C8K-A9DF3328-B805-46A1-B6...
	onRamp_C8K-Cloud1	NA	Apr 17 16:59:00 2031 PDT	Invalid | Staging | Valid	C8K-BB413992-A6D1-89AF-89...
	onRamp_C8K-Cloud2	NA	Apr 18 11:11:06 2031 PDT	Invalid | Staging | Valid	C8K-D16865BD-FEE2-ACC7-EE...
'a...	--	NA	NA	Invalid | Staging | Valid	NA
	WAN-EDGE-2	NA	NA	Invalid | Staging | Valid	NA

© 2020 Cisco and/or its affiliates. All rights reserved.

Step 4. Within the vManage dashboard, navigate to **Configuration** > **Templates** and select the **Device** tab.

Step 5. Find the desired GCP default template (**Default_GCP_CATALYST 8000V_Template_V01**).

An example is shown in the following figure.



Template Type: Default

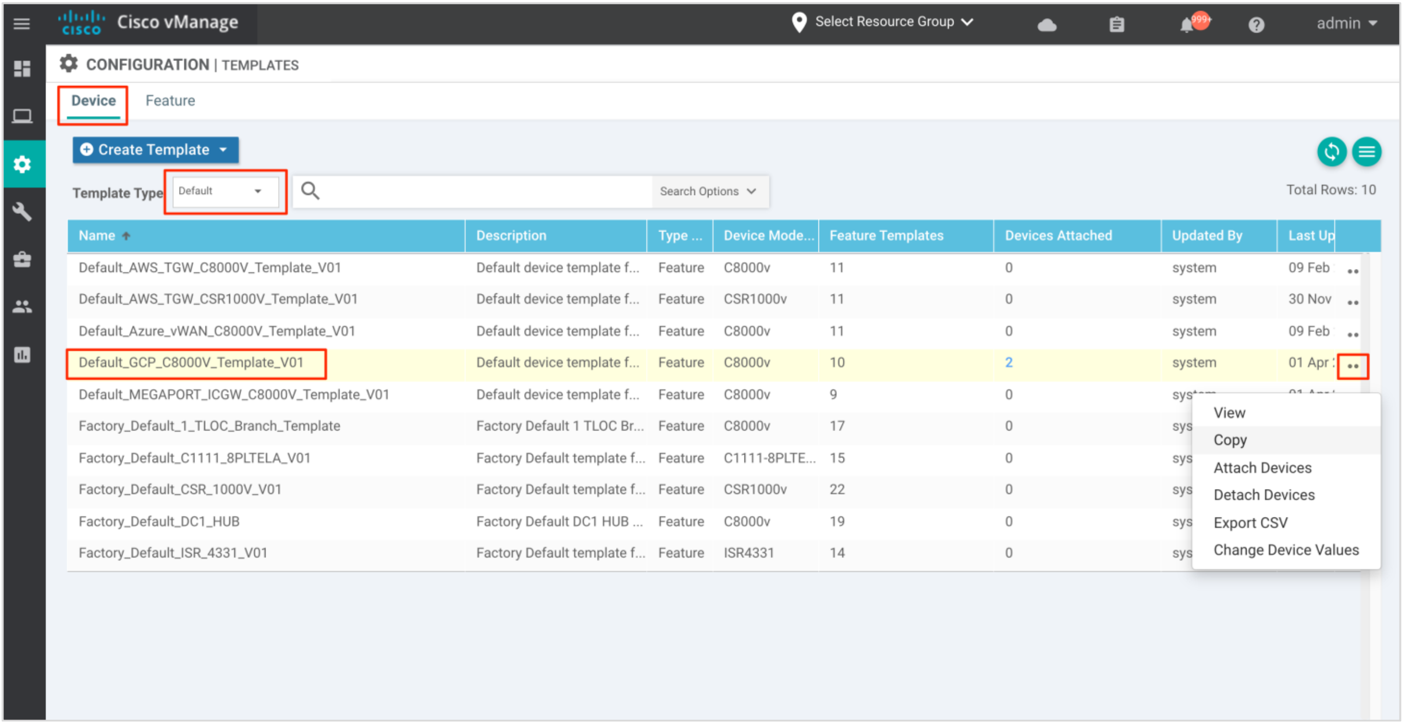
Total Rows: 10

Name	Description	Type ...	Device Mode...	Feature Templates	Devices Attached	Updated By	Last Upda
Default_AWS_TGW_C8000V_Template_V01	Default device template f...	Feature	C8000v	11	0	system	09 Feb 20:
Default_AWS_TGW_CSR1000V_Template_V01	Default device template f...	Feature	CSR1000v	11	0	system	30 Nov 20
Default_Azure_vWAN_C8000V_Template_V01	Default device template f...	Feature	C8000v	11	0	system	09 Feb 20:
Default_GCP_C8000V_Template_V01	Default device template f...	Feature	C8000v	10		system	01 Apr 20:
Default_MEGAPORT_ICGW_C8000V_Template_V01	Default device template f...	Feature	C8000v	9	0	system	01 Apr 20:
Factory_Default_1_TLOC_Branch_Template	Factory Default 1 TLOC Br...	Feature	C8000v	17	0	system	09 Feb 20:
Factory_Default_C1111_8PLTELA_V01	Factory Default template f...	Feature	C1111-8PLTE...	15	0	system	02 Nov 20
Factory_Default_CSR_1000V_V01	Factory Default template f...	Feature	CSR1000v	22	0	system	02 Nov 20
Factory_Default_DC1_HUB	Factory Default DC1 HUB ...	Feature	C8000v	19	0	system	09 Feb 20:
Factory_Default_ISR_4331_V01	Factory Default template f...	Feature	ISR4331	14	0	system	02 Nov 20

Step 6. Within this drop down, you can choose to either **copy** and rename the device template, and later attach devices under the non-default template you've generated or click on attach devices to add devices under the default template. The following screenshot explains the former option.

Click on the three dots **(…)** located on the right side and click **Copy**.

© 2020 Cisco and/or its affiliates. All rights reserved.

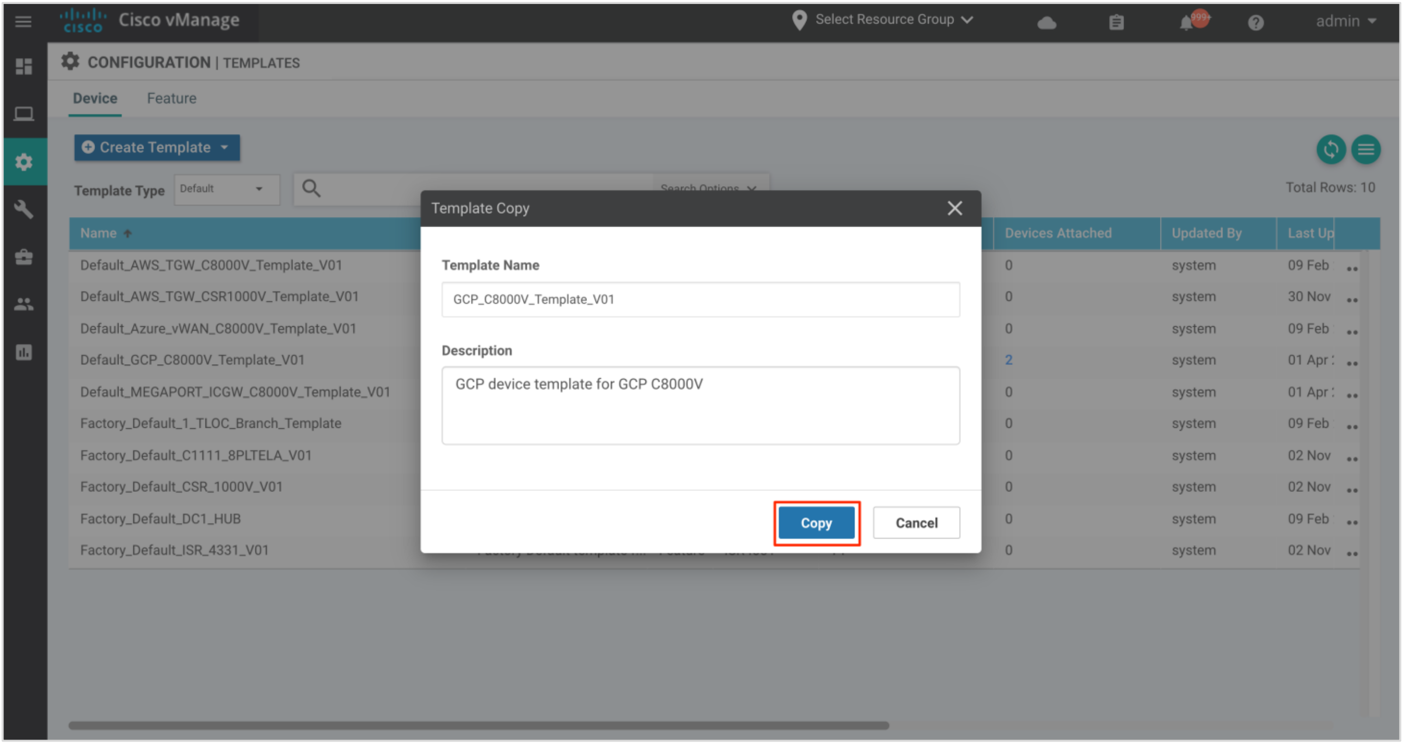


Template Type: Default

Total Rows: 10

Name	Description	Type ...	Device Mode...	Feature Templates	Devices Attached	Updated By	Last Up
Default_AWS_TGW_C8000V_Template_V01	Default device template f...	Feature	C8000v	11	0	system	09 Feb
Default_AWS_TGW_CSR1000V_Template_V01	Default device template f...	Feature	CSR1000v	11	0	system	30 Nov
Default_Azure_vWAN_C8000V_Template_V01	Default device template f...	Feature	C8000v	11	0	system	09 Feb
Default_GCP_C8000V_Template_V01	Default device template f...	Feature	C8000v	10	2	system	01 Apr
Default_MEGAPORT_ICGW_C8000V_Template_V01	Default device template f...	Feature	C8000v	9	0	system	01 Apr
Factory_Default_1_TLOC_Branch_Template	Factory Default 1 TLOC Br...	Feature	C8000v	17	0	sys	
Factory_Default_C1111_8PLTELA_V01	Factory Default template f...	Feature	C1111-8PLTE...	15	0	sys	
Factory_Default_CSR_1000V_V01	Factory Default template f...	Feature	CSR1000v	22	0	sys	
Factory_Default_DC1_HUB	Factory Default DC1 HUB ...	Feature	C8000v	19	0	sys	
Factory_Default_ISR_4331_V01	Factory Default template f...	Feature	ISR4331	14	0	sys	

Step 7. The template is renamed to GCP_CATALYST 8000V_Template_V01 and click **Copy** again.

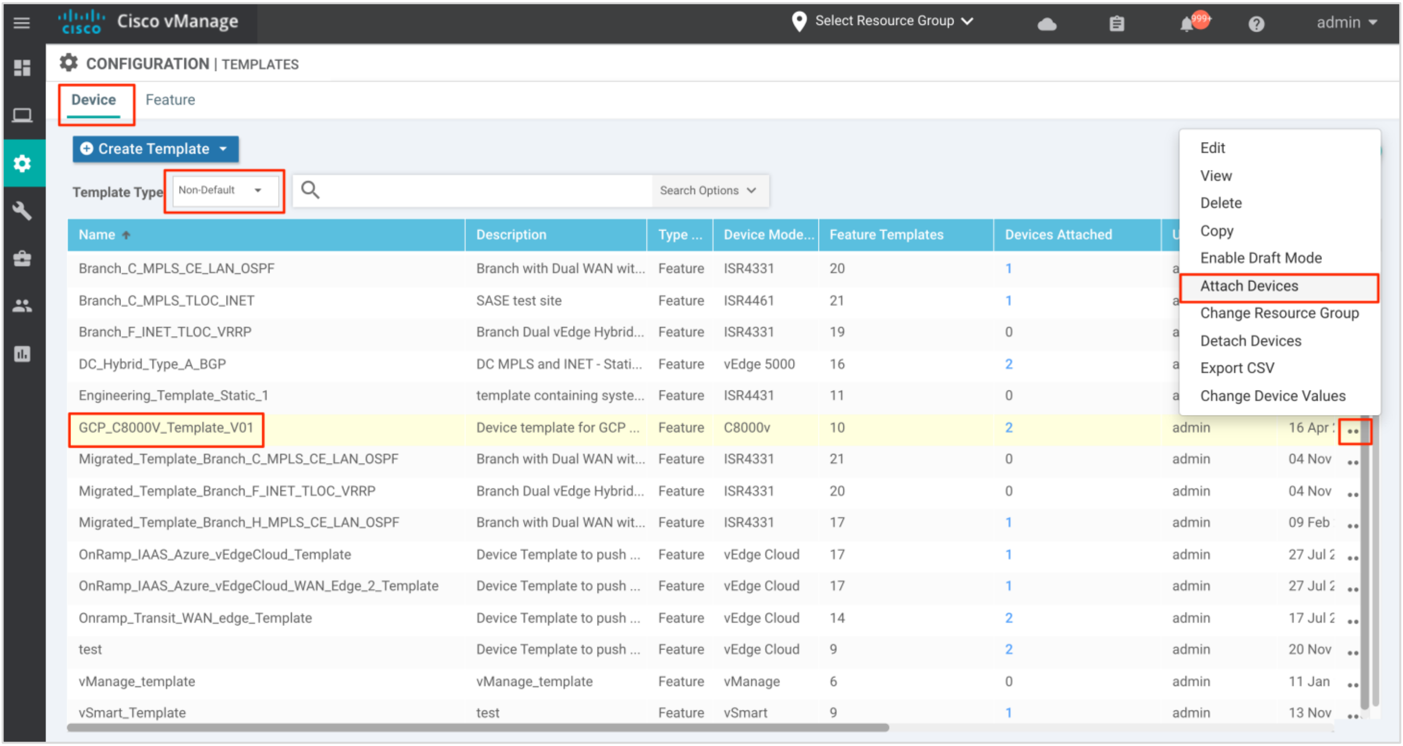


Template Name: GCP_C8000V_Template_V01

Description: GCP device template for GCP C8000V

Step 8. Under the **Device** section, click on the **Template Type** drop-down list and select **Non-Default.** Click on the three dots (**…**) next to the non-default template, **GCP_8000V-Template_V01** and click **Attach Devices.**

© 2020 Cisco and/or its affiliates. All rights reserved.



Template Type: Non-Default

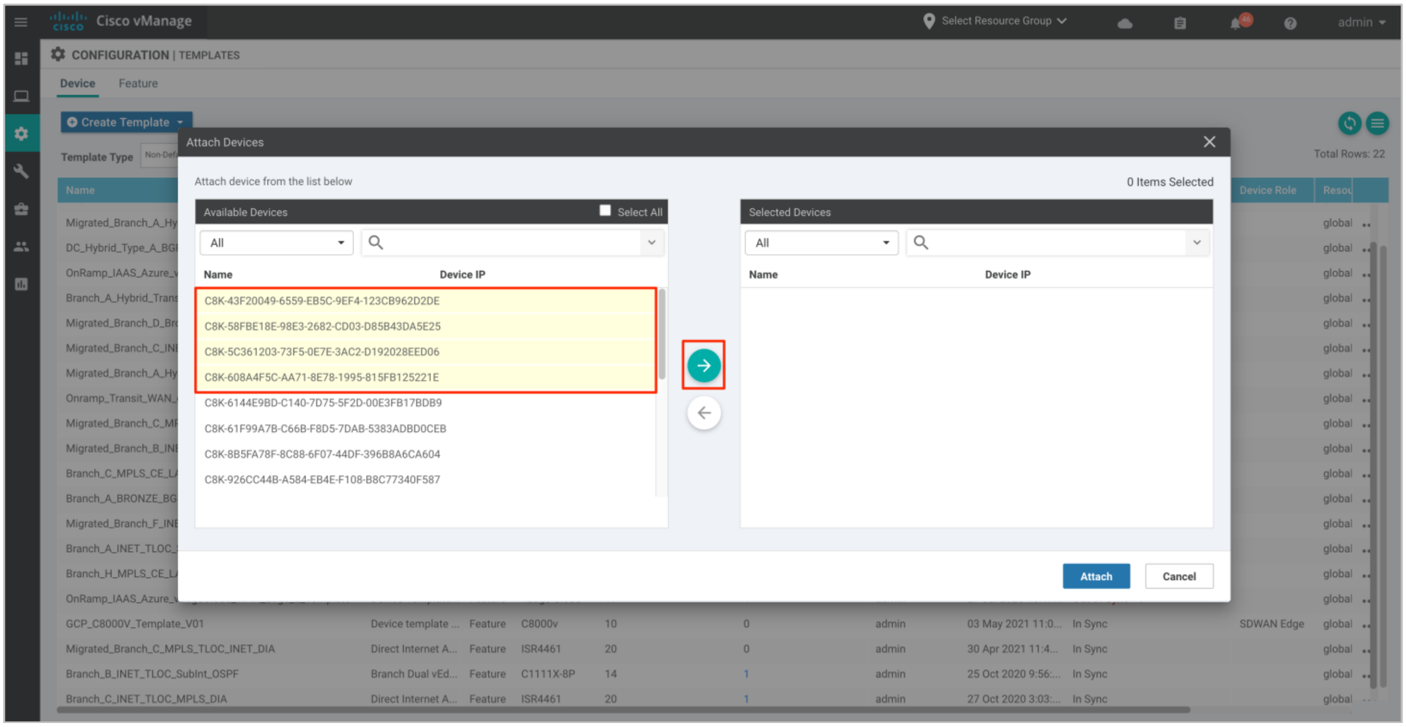
Name	Description	Type ...	Device Mode...	Feature Templates	Devices Attached	U		
Branch_C_MPLS_CE_LAN_OSPF	Branch with Dual WAN wit...	Feature	ISR4331	20	1	a		
Branch_C_MPLS_TLOC_INET	SASE test site	Feature	ISR4461	21	1	a		
Branch_F_INET_TLOC_VRRP	Branch Dual vEdge Hybrid...	Feature	ISR4331	19	0	a		
DC_Hybrid_Type_A_BGP	DC MPLS and INET - Stati...	Feature	vEdge 5000	16	2	a		
Engineering_Template_Static_1	template containing syste...	Feature	ISR4431	11	0	a		
GCP_C8000V_Template_V01	Device template for GCP ...	Feature	C8000v	10	2	admin	16 Apr	•••
Migrated_Template_Branch_C_MPLS_CE_LAN_OSPF	Branch with Dual WAN wit...	Feature	ISR4331	21	0	admin	04 Nov	•••
Migrated_Template_Branch_F_INET_TLOC_VRRP	Branch Dual vEdge Hybrid...	Feature	ISR4331	20	0	admin	04 Nov	•••
Migrated_Template_Branch_H_MPLS_CE_LAN_OSPF	Branch with Dual WAN wit...	Feature	ISR4331	17	1	admin	09 Feb	•••
OnRamp_IAAS_Azure_vEdgeCloud_Template	Device Template to push ...	Feature	vEdge Cloud	17	1	admin	27 Jul 2	•••
OnRamp_IAAS_Azure_vEdgeCloud_WAN_Edge_2_Template	Device Template to push ...	Feature	vEdge Cloud	17	1	admin	27 Jul 2	•••
Onramp_Transit_WAN_edge_Template	Device Template to push ...	Feature	vEdge Cloud	14	2	admin	17 Jul 2	•••
test	Device Template to push ...	Feature	vEdge Cloud	9	2	admin	20 Nov	•••
vManage_template	vManage_template	Feature	vManage	6	0	admin	11 Jan	•••
vSmart_Template	test	Feature	vSmart	9	1	admin	13 Nov	•••

Step 9. A pop-up window listing the available devices to be attached to this configuration will appear. The list of available devices contains either the hostname and IP address of a device if it is known through vManage; or contains the chassis serial number of the devices that have not yet come up on the network and are unknown by vManage. Cisco Catalyst8000v routers are assigned a chassis serial number although there is no physical chassis.

Select the devices you want to apply the configuration template to and select the arrow to move the device from the **Available Devices** box to the **Selected Devices** box.

You can select multiple devices at one time by simply clicking each desired device.

© 2020 Cisco and/or its affiliates. All rights reserved.

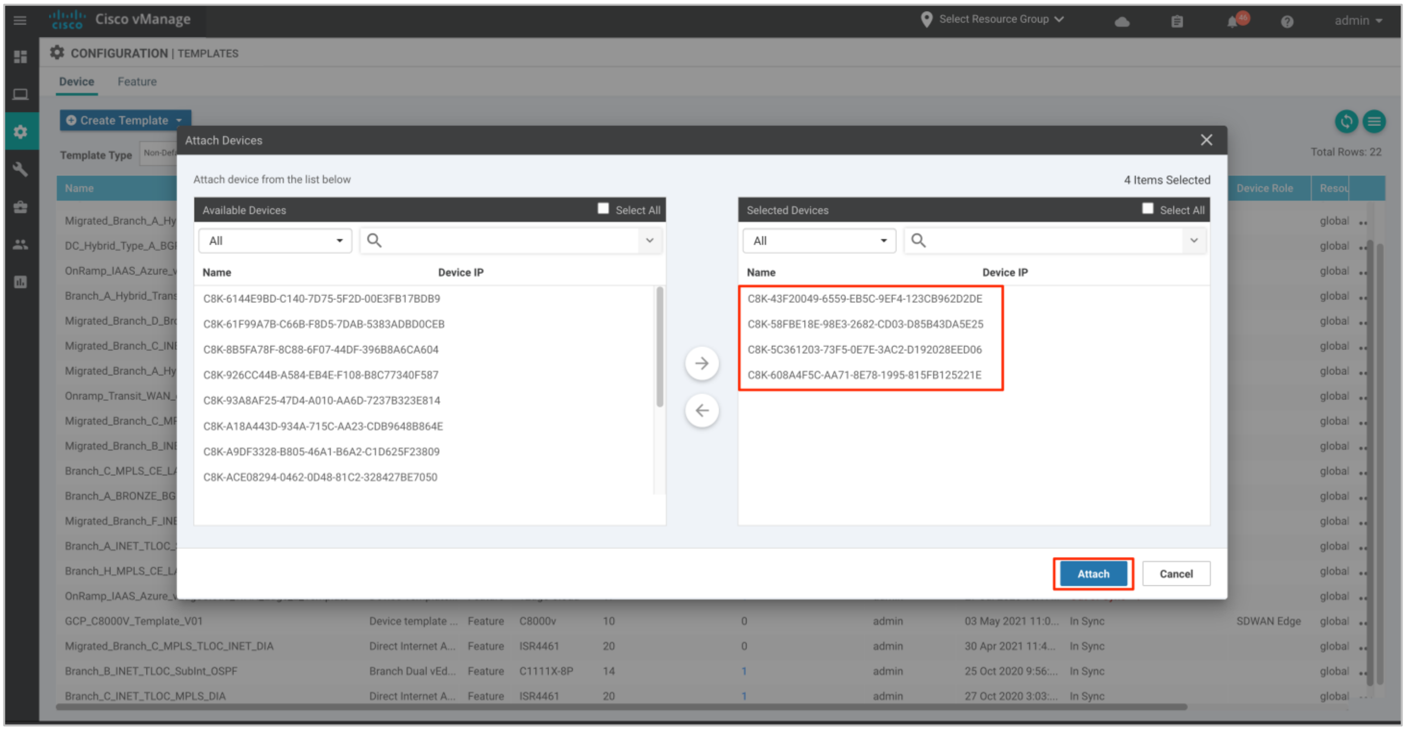


Available Devices:

C8K-43F20049-6559-EB5C-9EF4-123CB962D2DE
C8K-58FBE18E-98E3-2682-CD03-D85B43DA5E25
C8K-5C361203-73F5-0E7E-3AC2-D192028EED06
C8K-608A4F5C-AA71-8E78-1995-815FB125221E
C8K-6144E9BD-C140-7D75-5F2D-00E3FB17BDB9
C8K-61F99A7B-C66B-F8D5-7DAB-5383ADBD0CEB
C8K-8B5FA78F-8C88-6F07-44DF-396B8A6CA604
C8K-926CC44B-A584-EB4E-F108-B8C77340F587

Step 10. Click on the **Attach** button.

A new screen will appear, listing the devices that you have selected.



Available Devices:

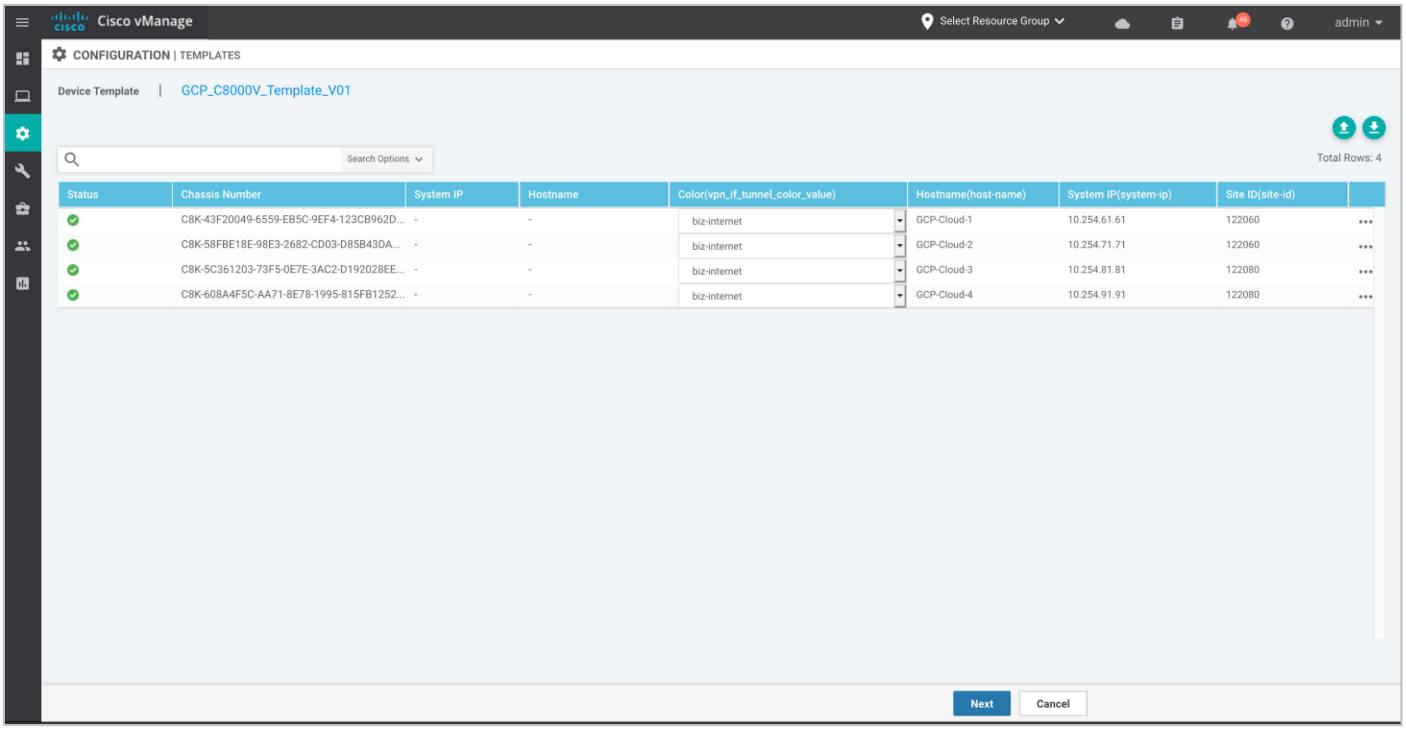
C8K-6144E9BD-C140-7D75-5F2D-00E3FB17BDB9
C8K-61F99A7B-C66B-F8D5-7DAB-5383ADBD0CEB
C8K-8B5FA78F-8C88-6F07-44DF-396B8A6CA604
C8K-926CC44B-A584-EB4E-F108-B8C77340F587
C8K-93A8AF25-47D4-A010-AA6D-7237B323E814
C8K-A18A443D-934A-715C-AA23-CDB9648B864E
C8K-A9DF3328-B805-46A1-B6A2-C1D625F23809
C8K-ACE08294-0462-0D48-81C2-328427BE7050

Selected Devices:

C8K-43F20049-6559-EB5C-9EF4-123CB962D2DE
C8K-58FBE18E-98E3-2682-CD03-D85B43DA5E25
C8K-5C361203-73F5-0E7E-3AC2-D192028EED06
C8K-608A4F5C-AA71-8E78-1995-815FB125221E

Step 11. Click on the three dots (**...**) located to the far right of each device template, and from the drop-down menu select **Edit Device Template** or simply enter the values directly into each of the column.

An example is shown in the following figure.



Device Template | GCP_C8000V_Template_V01

Total Rows: 4

Status	Chassis Number	System IP	Hostname	Color(vpn_if_tunnel_color_value)	Hostname(host-name)	System IP(system-ip)	Site ID(site-id)
✓	C8K-43F20049-6559-EB5C-9EF4-123CB962D...	-	-	biz-internet	GCP-Cloud-1	10.254.61.61	122060
✓	C8K-58FBE18E-98E3-2682-CD03-D85B43DA...	-	-	biz-internet	GCP-Cloud-2	10.254.71.71	122060
✓	C8K-5C361203-73F5-0E7E-3AC2-D192028EE...	-	-	biz-internet	GCP-Cloud-3	10.254.81.81	122080
✓	C8K-608A4F5C-AA71-8E78-1995-815FB1252...	-	-	biz-internet	GCP-Cloud-4	10.254.91.91	122080

Step 12. Fill in the values of the variables in the text boxes.

The following template is deployed on Chassis Number – **C8K-43F20049-6559-EB5C-9EF4-123CB9262D**

Variables	Value
Color (vpn_if_tunnel_color_value)	Biz-Internet
System IP (system-ip)	10.254.61.61
Site ID (site-id)	120060
Hostname (host-name)	GCP-Cloud1

The following template is deployed on Chassis Number – **C8K-58FBE18E-98E3-2682-CD03-D85B43DA**

Variables	Value
Color (vpn_if_tunnel_color_value)	Biz-Internet
System IP (system-ip)	10.254.71.71
Site ID (site-id)	120060
Hostname (host-name)	GCP-Cloud2

The following template is deployed on Chassis Number – **C8K-5C361203-73F5-0E7E-3AC2-D192028EE**

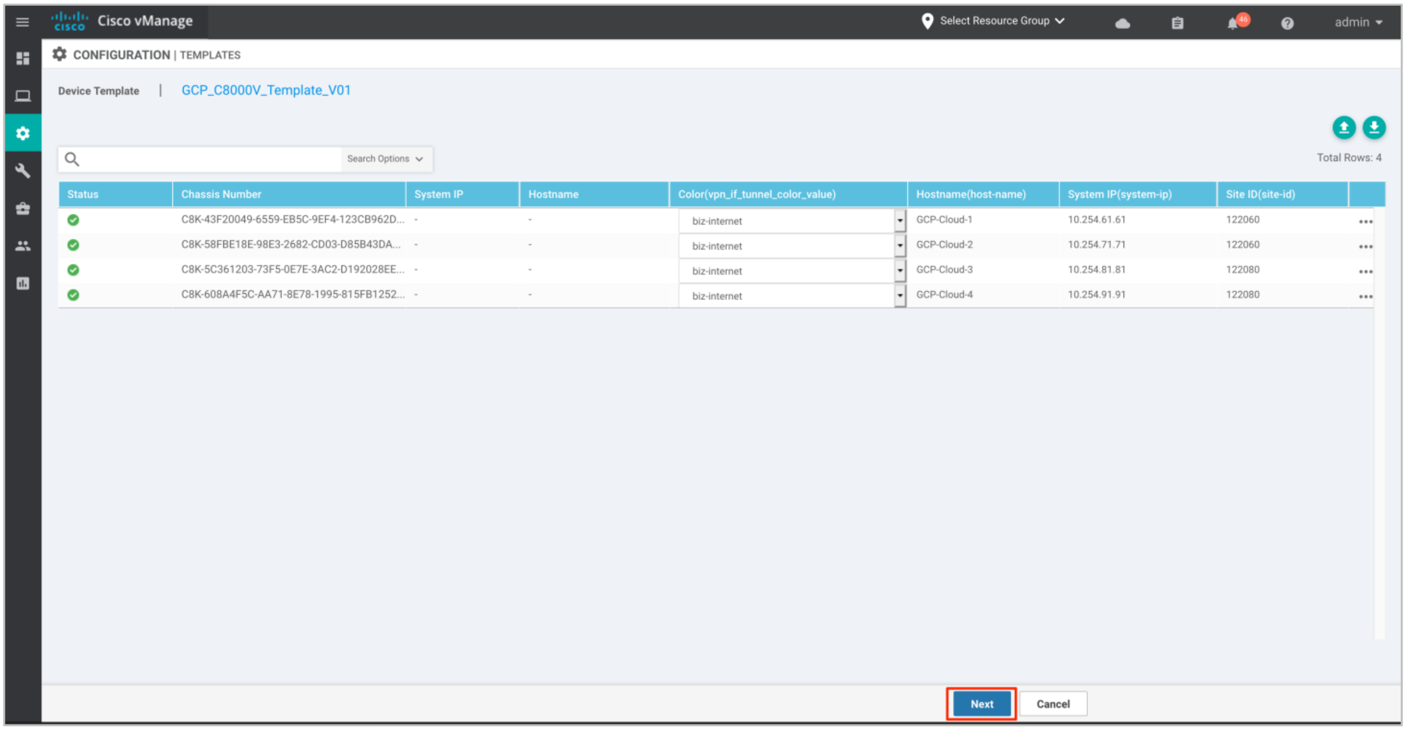
© 2020 Cisco and/or its affiliates. All rights reserved.

Variables	Value
Color (vpn_if_tunnel_color_value)	Biz-Internet
System IP (system-ip)	10.254.81.81
Site ID (site-id)	120080
Hostname (host-name)	GCP-Cloud3

The following template is deployed on Chassis Number – **C8K-608A4F5C-AA71-1995-815FB1252**

Variables	Value
Color (vpn_if_tunnel_color_value)	Biz-Internet
System IP (system-ip)	10.254.91.91
Site ID (site-id)	120080
Hostname (host-name)	GCP-Cloud4

Step 13. Click **Next** to navigate to the final page.



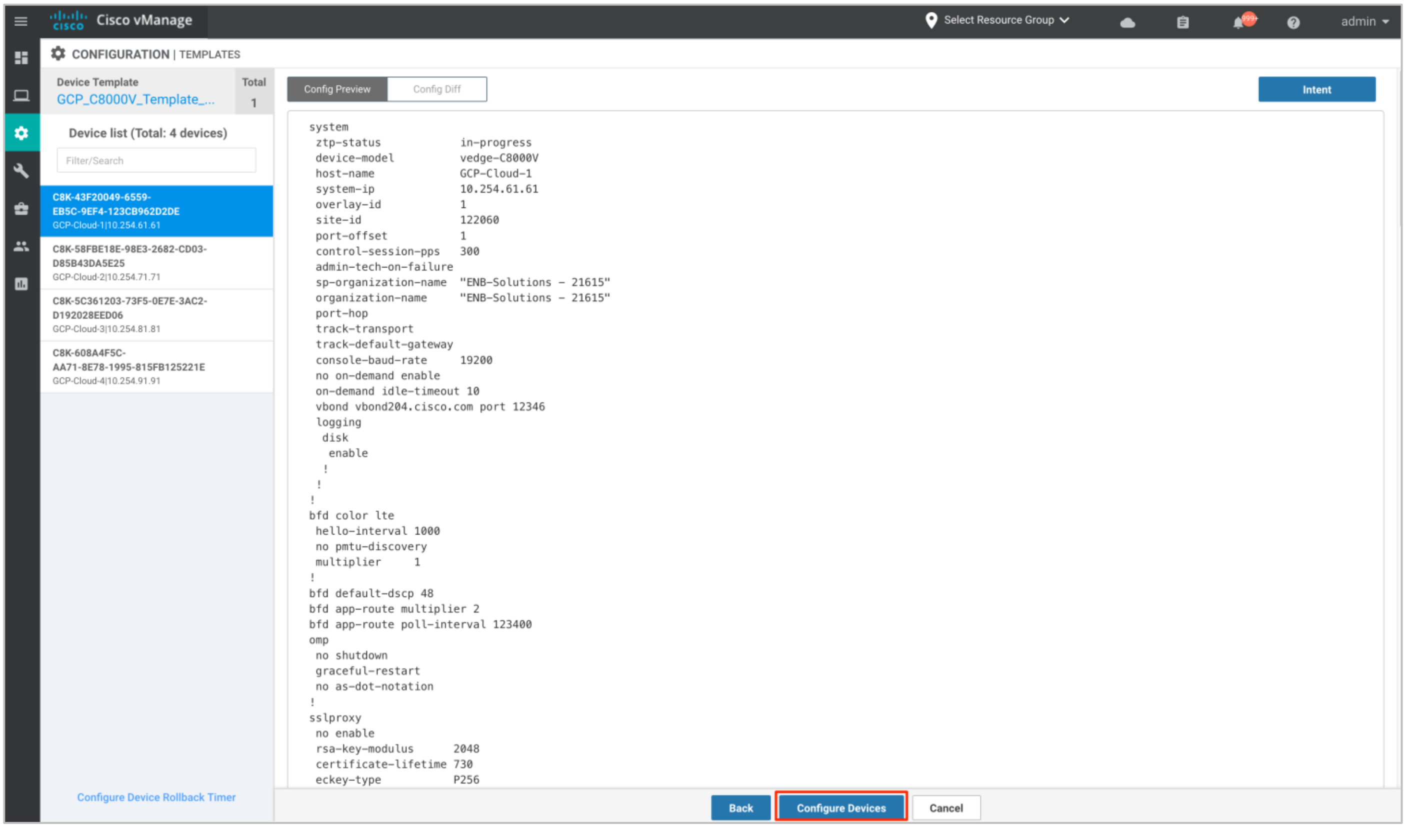
Device Template | GCP_C8000V_Template_V01

Total Rows: 4

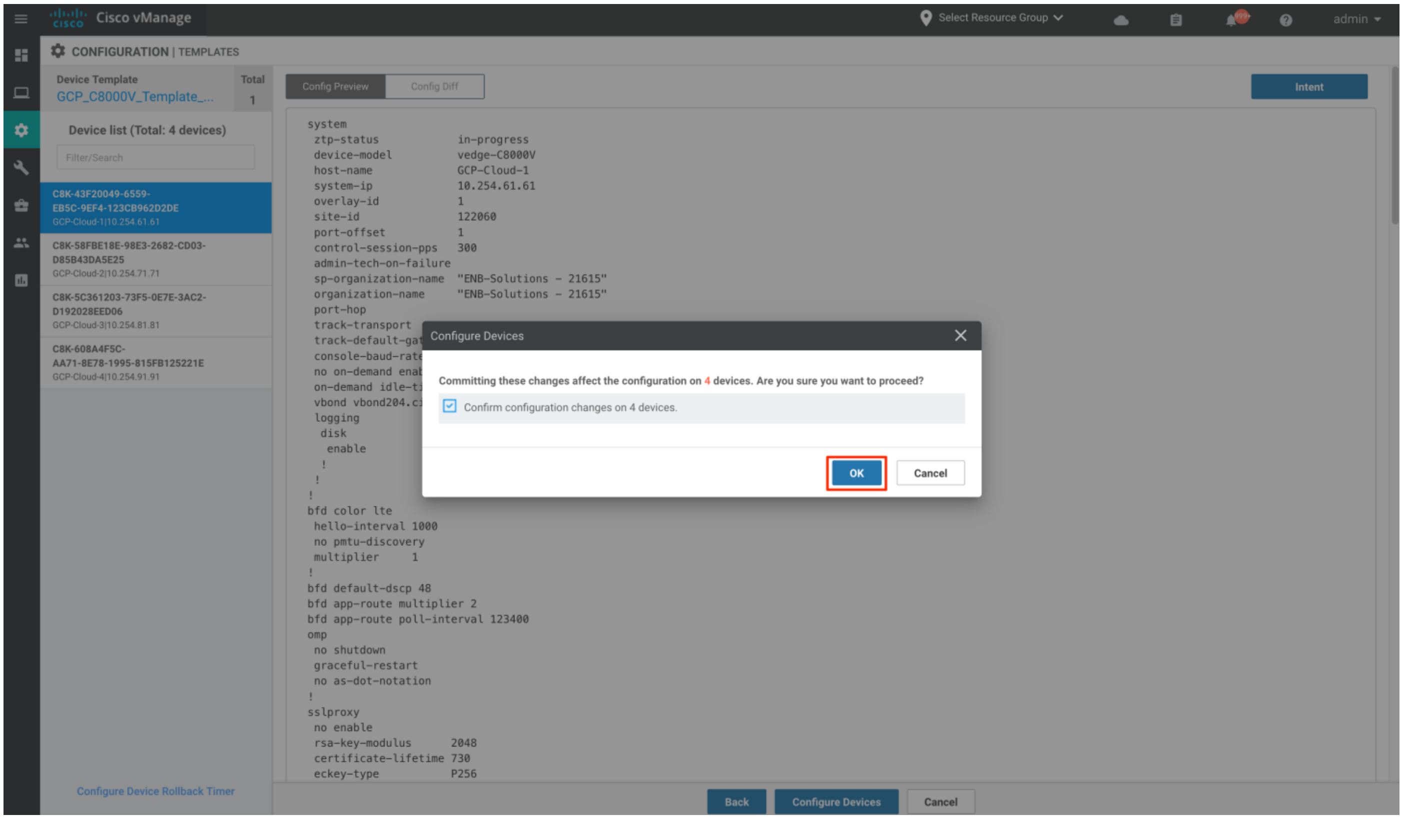
Status	Chassis Number	System IP	Hostname	Color(vpn_if_tunnel_color_value)	Hostname(host-name)	System IP(system-ip)	Site ID(site-id)
✓	C8K-43F20049-6559-EB5C-9EF4-123CB962D...	-	-	biz-internet	GCP-Cloud-1	10.254.61.61	122060
✓	C8K-58FBE18E-98E3-2682-CD03-D85B43DA...	-	-	biz-internet	GCP-Cloud-2	10.254.71.71	122060
✓	C8K-5C361203-73F5-0E7E-3AC2-D192028EE...	-	-	biz-internet	GCP-Cloud-3	10.254.81.81	122080
✓	C8K-608A4F5C-AA71-8E78-1995-815FB1252...	-	-	biz-internet	GCP-Cloud-4	10.254.91.91	122080

Step 14. Preview the configuration and click **Configure Devices**. Then, click **OK** to complete the template creation process.

© 2020 Cisco and/or its affiliates. All rights reserved.



```
system
 ztp-status            in-progress
 device-model          vedge-C8000V
 host-name             GCP-Cloud-1
 system-ip             10.254.61.61
 overlay-id            1
 site-id               122060
 port-offset           1
 control-session-pps   300
 admin-tech-on-failure
 sp-organization-name  "ENB-Solutions - 21615"
 organization-name     "ENB-Solutions - 21615"
 port-hop
 track-transport
 track-default-gateway
 console-baud-rate     19200
 no on-demand enable
 on-demand idle-timeout 10
 vbond vbond204.cisco.com port 12346
 logging
  disk
   enable
  !
 !
!
bfd color lte
 hello-interval 1000
 no pmtu-discovery
 multiplier     1
!
bfd default-dscp 48
bfd app-route multiplier 2
bfd app-route poll-interval 123400
omp
 no shutdown
 graceful-restart
 no as-dot-notation
!
sslproxy
 no enable
 rsa-key-modulus      2048
 certificate-lifetime 730
 eckey-type           P256
```



Committing these changes affect the configuration on 4 devices. Are you sure you want to proceed?

☑ Confirm configuration changes on 4 devices.

```
system
 ztp-status            in-progress
 device-model          vedge-C8000V
 host-name             GCP-Cloud-1
 system-ip             10.254.61.61
 overlay-id            1
 site-id               122060
 port-offset           1
 control-session-pps   300
 admin-tech-on-failure
 sp-organization-name  "ENB-Solutions - 21615"
 organization-name     "ENB-Solutions - 21615"
 port-hop
 track-transport
 track-default-gat
 console-baud-rate
 no on-demand enab
 on-demand idle-ti
 vbond vbond204.ci
 logging
  disk
   enable
  !
 !
!
bfd color lte
 hello-interval 1000
 no pmtu-discovery
 multiplier     1
!
bfd default-dscp 48
bfd app-route multiplier 2
bfd app-route poll-interval 123400
omp
 no shutdown
 graceful-restart
 no as-dot-notation
!
sslproxy
 no enable
 rsa-key-modulus      2048
 certificate-lifetime 730
 eckey-type           P256
```

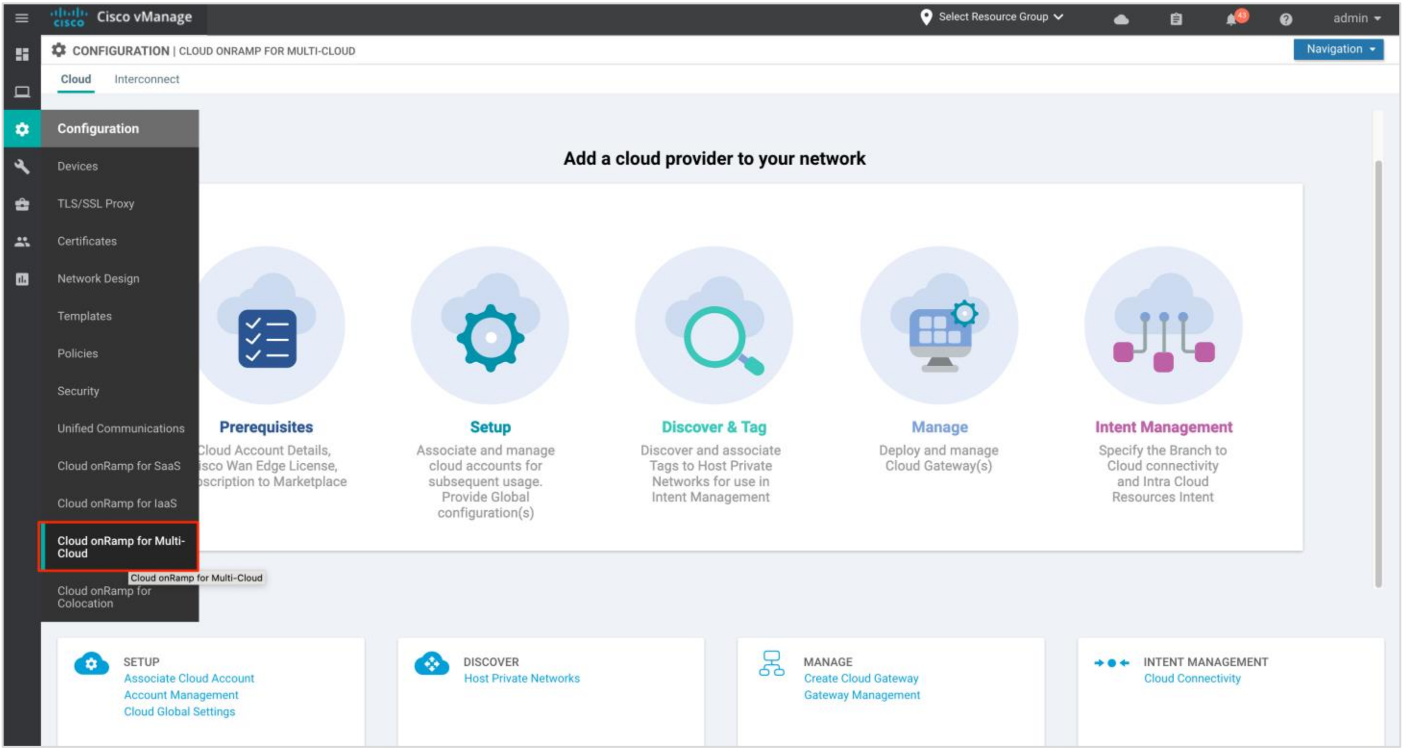
© 2020 Cisco and/or its affiliates. All rights reserved.

Process 2: Setup - Part 1 - Associate Cloud Account

This section discusses the procedures for associating your Google cloud account with Cisco vManage.

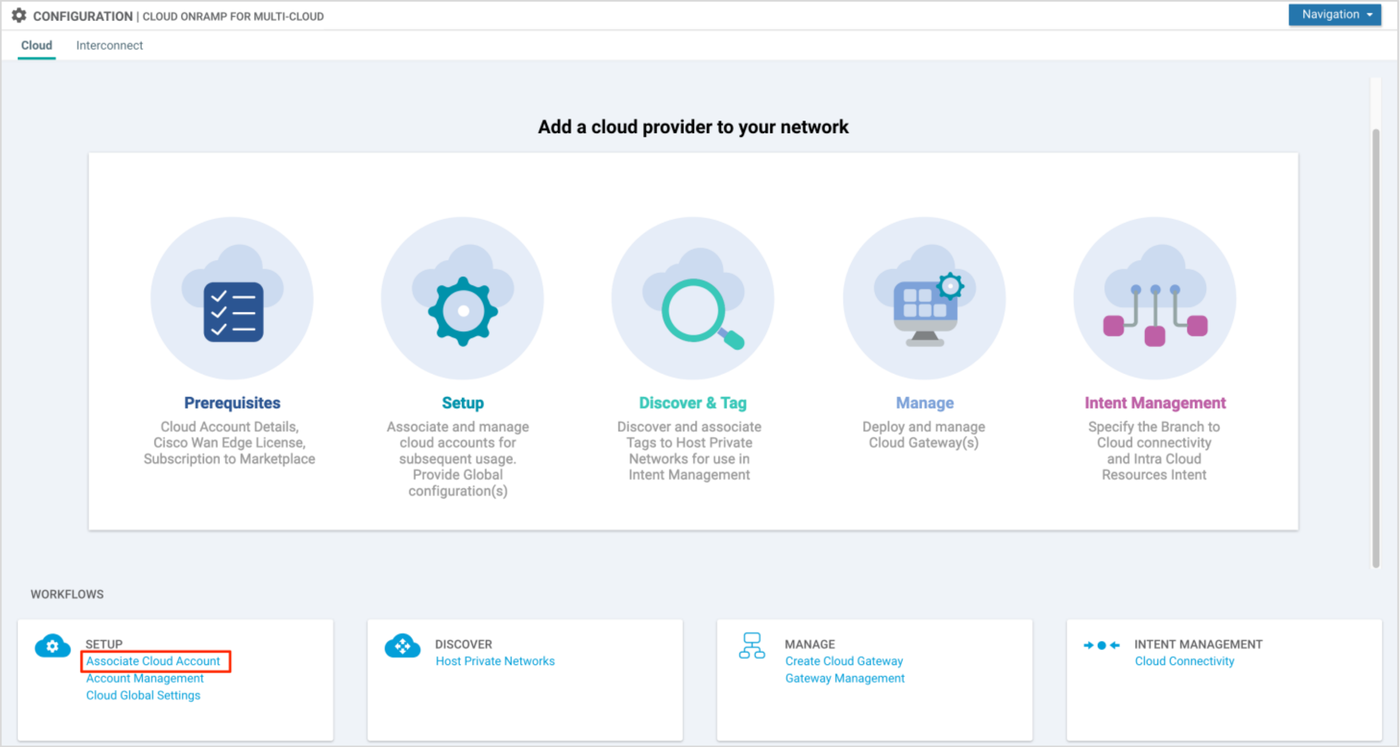
Procedure 1: Login to vManage NMS and Navigate to Cisco Cloud onRamp for Multi-Cloud

Step 1. From the navigation panel on the left side of the screen, select **Configuration > Cloud onRamp for Multi-Cloud.**


Cisco vManage
Select Resource Group
admin
CONFIGURATION | CLOUD ONRAMP FOR MULTI-CLOUD
Navigation
Cloud
Interconnect
Configuration
Devices
TLS/SSL Proxy
Certificates
Network Design
Templates
Policies
Security
Unified Communications
Cloud onRamp for SaaS
Cloud onRamp for IaaS
Cloud onRamp for Multi-Cloud
Cloud onRamp for Multi-Cloud
Cloud onRamp for Colocation
Add a cloud provider to your network
Prerequisites
Cloud Account Details, isco Wan Edge License, bscription to Marketplace
Setup
Associate and manage cloud accounts for subsequent usage. Provide Global configuration(s)
Discover & Tag
Discover and associate Tags to Host Private Networks for use in Intent Management
Manage
Deploy and manage Cloud Gateway(s)
Intent Management
Specify the Branch to Cloud connectivity and Intra Cloud Resources Intent
SETUP
Associate Cloud Account
Account Management
Cloud Global Settings
DISCOVER
Host Private Networks
MANAGE
Create Cloud Gateway
Gateway Management
INTENT MANAGEMENT
Cloud Connectivity

Step 2. Under **Setup**, click **Associate Cloud Account** to associate your Google cloud account with vManage.

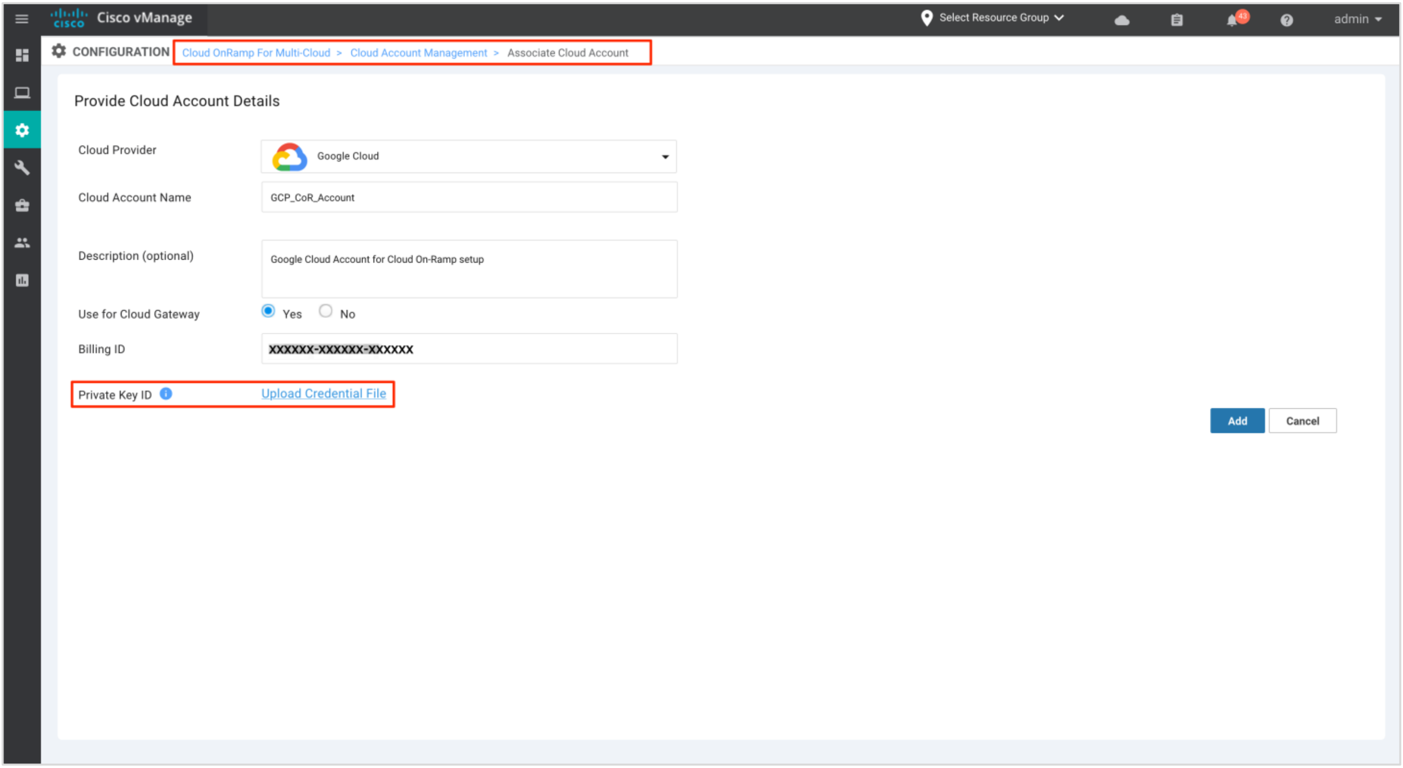
© 2020 Cisco and/or its affiliates. All rights reserved.


CONFIGURATION | CLOUD ONRAMP FOR MULTI-CLOUD
Navigation
Cloud
Interconnect
Add a cloud provider to your network
Prerequisites
Cloud Account Details, Cisco Wan Edge License, Subscription to Marketplace
Setup
Associate and manage cloud accounts for subsequent usage. Provide Global configuration(s)
Discover & Tag
Discover and associate Tags to Host Private Networks for use in Intent Management
Manage
Deploy and manage Cloud Gateway(s)
Intent Management
Specify the Branch to Cloud connectivity and Intra Cloud Resources Intent
WORKFLOWS
SETUP
Associate Cloud Account
Account Management
Cloud Global Settings
DISCOVER
Host Private Networks
MANAGE
Create Cloud Gateway
Gateway Management
INTENT MANAGEMENT
Cloud Connectivity

Step 3. In the **Cloud Provider** field, choose **Google Cloud** from the drop-down list and enter the requested information.

Field	Description
Cloud Account Name	Enter a name for your Google Cloud account.
Description (optional)	Enter a description for the account.
Use for Cloud Gateway	Choose **Yes** to create a cloud gateway in your account. The option **No** is chosen by default.
Billing ID (optional)	Enter the billing ID associated with your Google Cloud service account. If you provide a billing ID, it goes through an automatic billing validation process. Note: This field is visible only if you choose the option **Yes** for the **Use for Cloud Gateway** field
Private Key ID	Click **Upload Credential File** to add your Google service account's private key.

© 2020 Cisco and/or its affiliates. All rights reserved.


Cisco vManage
Select Resource Group
admin
CONFIGURATION
Cloud OnRamp For Multi-Cloud > Cloud Account Management > Associate Cloud Account
Add
Cancel

Provide Cloud Account Details

Cloud Provider: Google Cloud

Cloud Account Name: GCP_CoR_Account

Description (optional): Google Cloud Account for Cloud On-Ramp setup

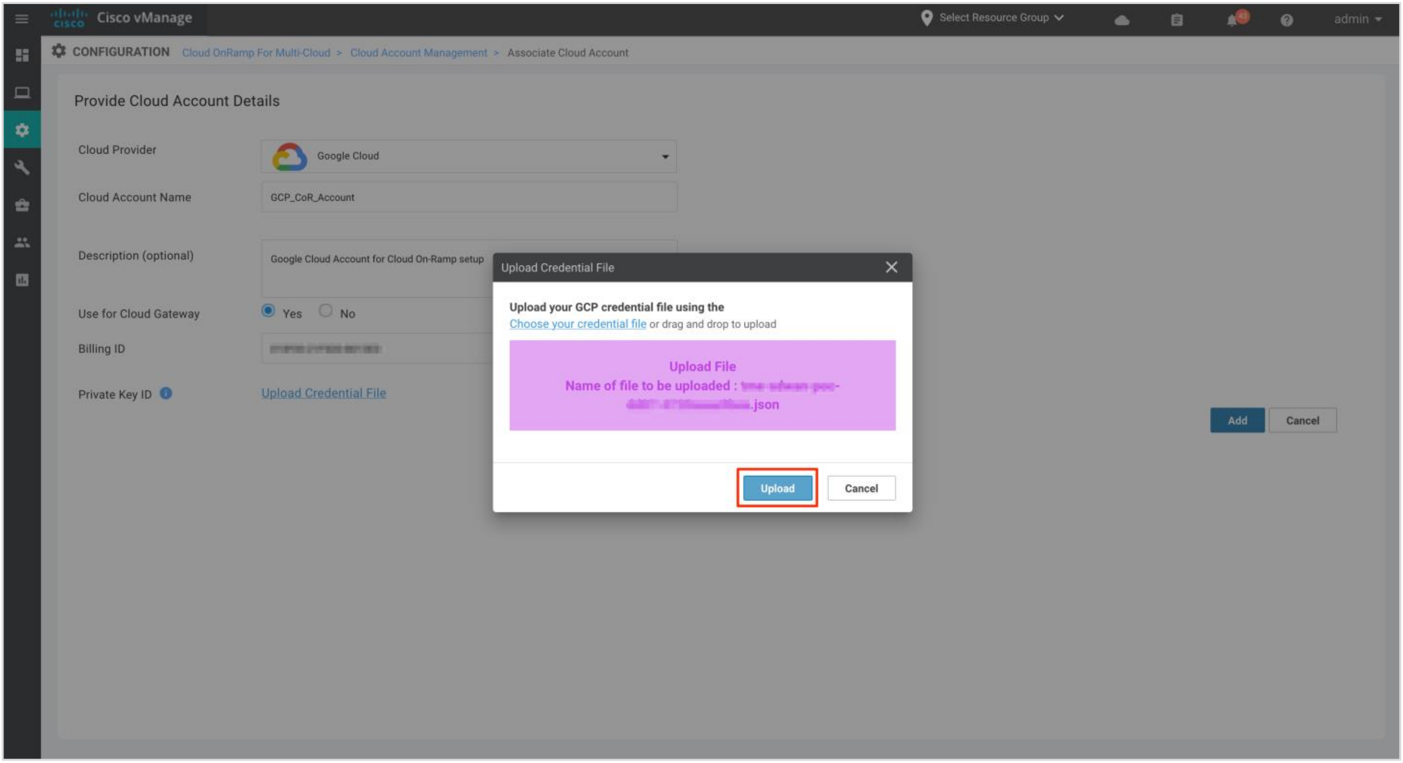
Use for Cloud Gateway: ● Yes ○ No

Billing ID: XXXXXX-XXXXXX-XXXXXX

Private Key ID: Upload Credential File

Step 4. To enter the private key, either drag and drop your Credential File or click on **Upload** to add your private key. vManage will allow user to register GCP service account keys credentials with vManage. The credentials entered will be validated in cloud and used to make GCP cloud calls.

vManage will allow two formats for entering the credentials.



Provide Cloud Account Details

Cloud Provider: Google Cloud

Cloud Account Name: GCP_CoR_Account

Description (optional): Google Cloud Account for Cloud On-Ramp setup

Use for Cloud Gateway: ● Yes ○ No

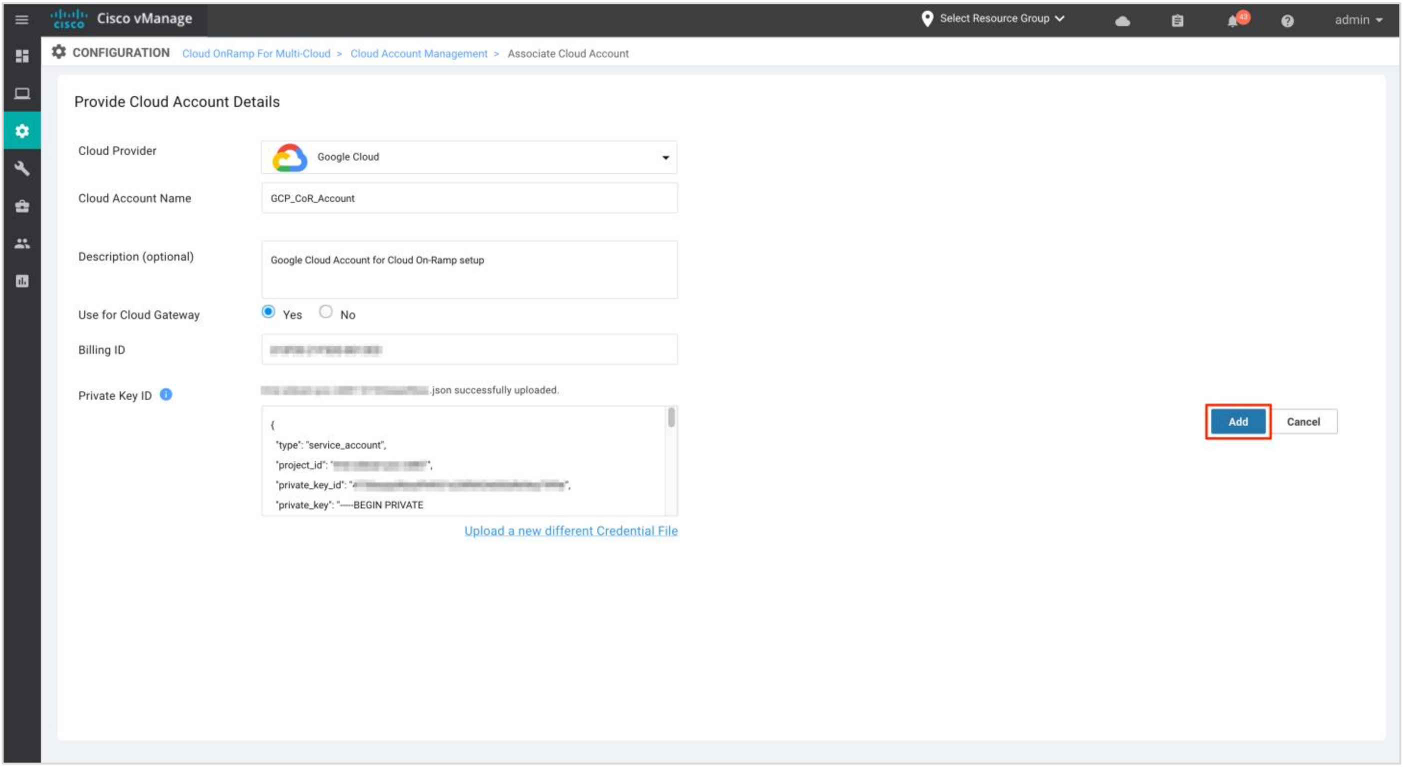
Billing ID: [redacted]

Private Key ID: Upload Credential File

Upload your GCP credential file using the Choose your credential file or drag and drop to upload

Upload File
Name of file to be uploaded : [redacted].json

Step 5. Click **Add** to successfully associate your Google Cloud Account with vManage.


Cisco vManage
Select Resource Group
admin
CONFIGURATION
Cloud OnRamp For Multi-Cloud > Cloud Account Management > Associate Cloud Account

Provide Cloud Account Details

Cloud Provider: Google Cloud

Cloud Account Name: GCP_CoR_Account

Description (optional): Google Cloud Account for Cloud On-Ramp setup

Use for Cloud Gateway: ● Yes ○ No

Billing ID: [redacted]

Private Key ID: [redacted] json successfully uploaded.

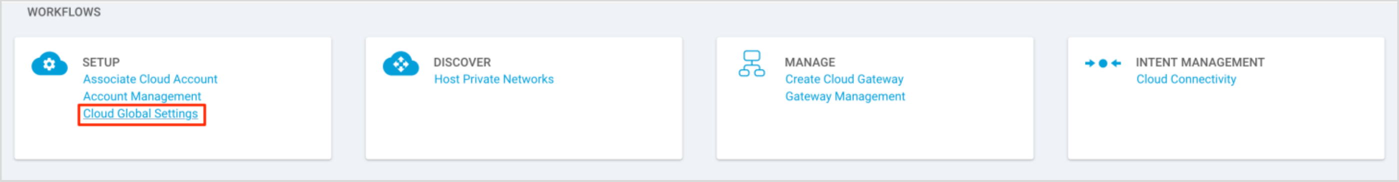
```
{
 "type": "service_account",
 "project_id": "[redacted]",
 "private_key_id": "[redacted]",
 "private_key": "-----BEGIN PRIVATE
```

Upload a new different Credential File
Add
Cancel

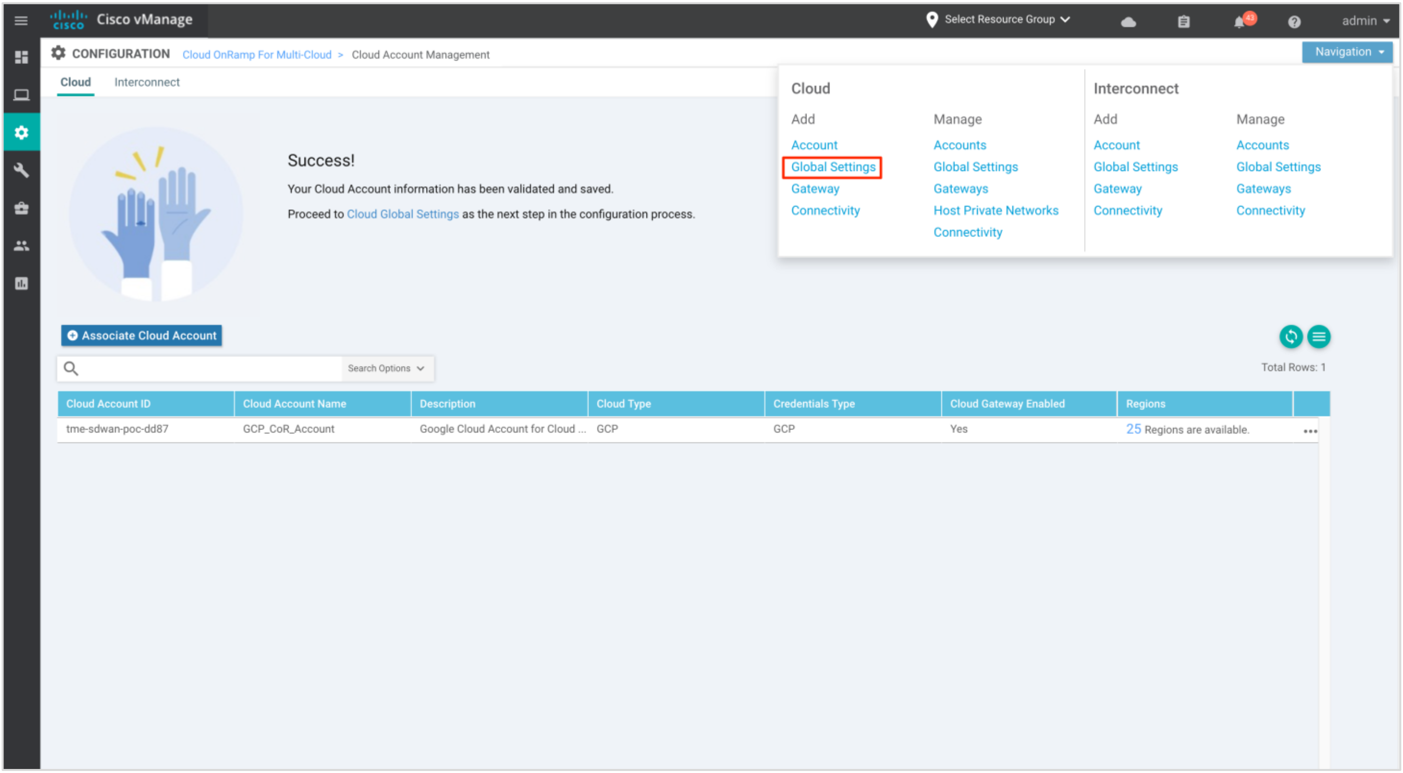
Process 2: Setup – Part 2 – Cloud Global Settings

This section discusses the steps to complete the global settings that includes the configuration items applicable system wide and used by all cloud gateway instantiations.

Step 1. Post account creation, navigate to **Cloud Global Settings.** The cloud global settings include all the global settings that apply to the cloud gateways in Google cloud.



Note: You can navigate to this page from the main page that includes the workflows or click on **Navigation** located on the right corner and select **Global Settings** from the drop down.



Success!

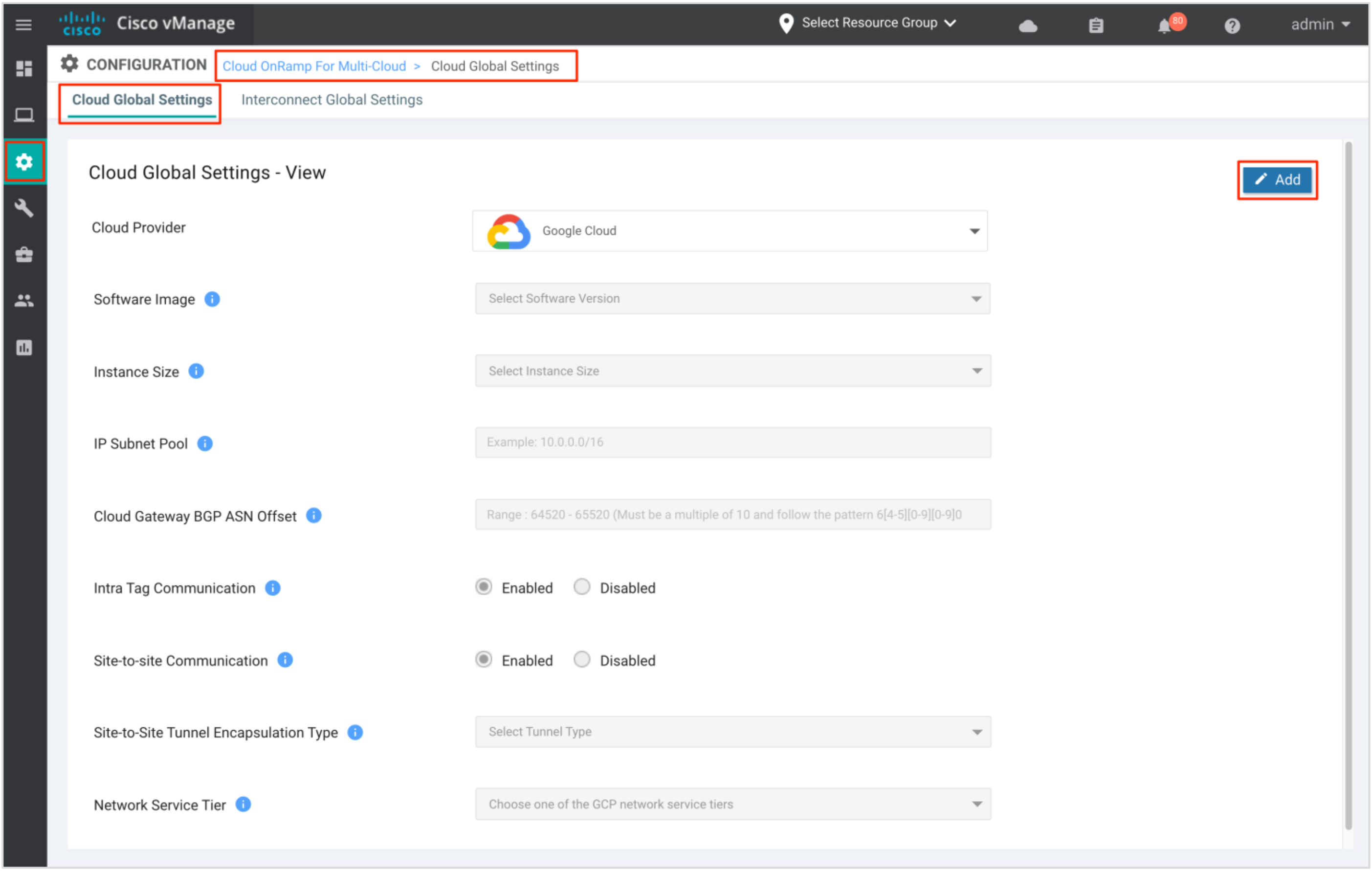
Your Cloud Account information has been validated and saved.

Proceed to Cloud Global Settings as the next step in the configuration process.

Cloud Account ID	Cloud Account Name	Description	Cloud Type	Credentials Type	Cloud Gateway Enabled	Regions
tme-sdwan-poc-dd87	GCP_CoR_Account	Google Cloud Account for Cloud ...	GCP	GCP	Yes	25 Regions are available.

Step 2. In the **Cloud Provider** field, choose **Google Cloud** from the drop-down list and click the **Add** button to add the global cloud gateway settings. If the cloud global settings are already configured, click **Edit** to modify them.

© 2020 Cisco and/or its affiliates. All rights reserved.


Cisco vManage
Select Resource Group
admin
CONFIGURATION
Cloud OnRamp For Multi-Cloud > Cloud Global Settings
Cloud Global Settings
Interconnect Global Settings
Add

Cloud Global Settings - View

Cloud Provider: Google Cloud

Software Image: Select Software Version

Instance Size: Select Instance Size

IP Subnet Pool: Example: 10.0.0.0/16

Cloud Gateway BGP ASN Offset: Range : 64520 - 65520 (Must be a multiple of 10 and follow the pattern 6[4-5][0-9][0-9]0

Intra Tag Communication: ● Enabled ○ Disabled

Site-to-site Communication: ● Enabled ○ Disabled

Site-to-Site Tunnel Encapsulation Type: Select Tunnel Type

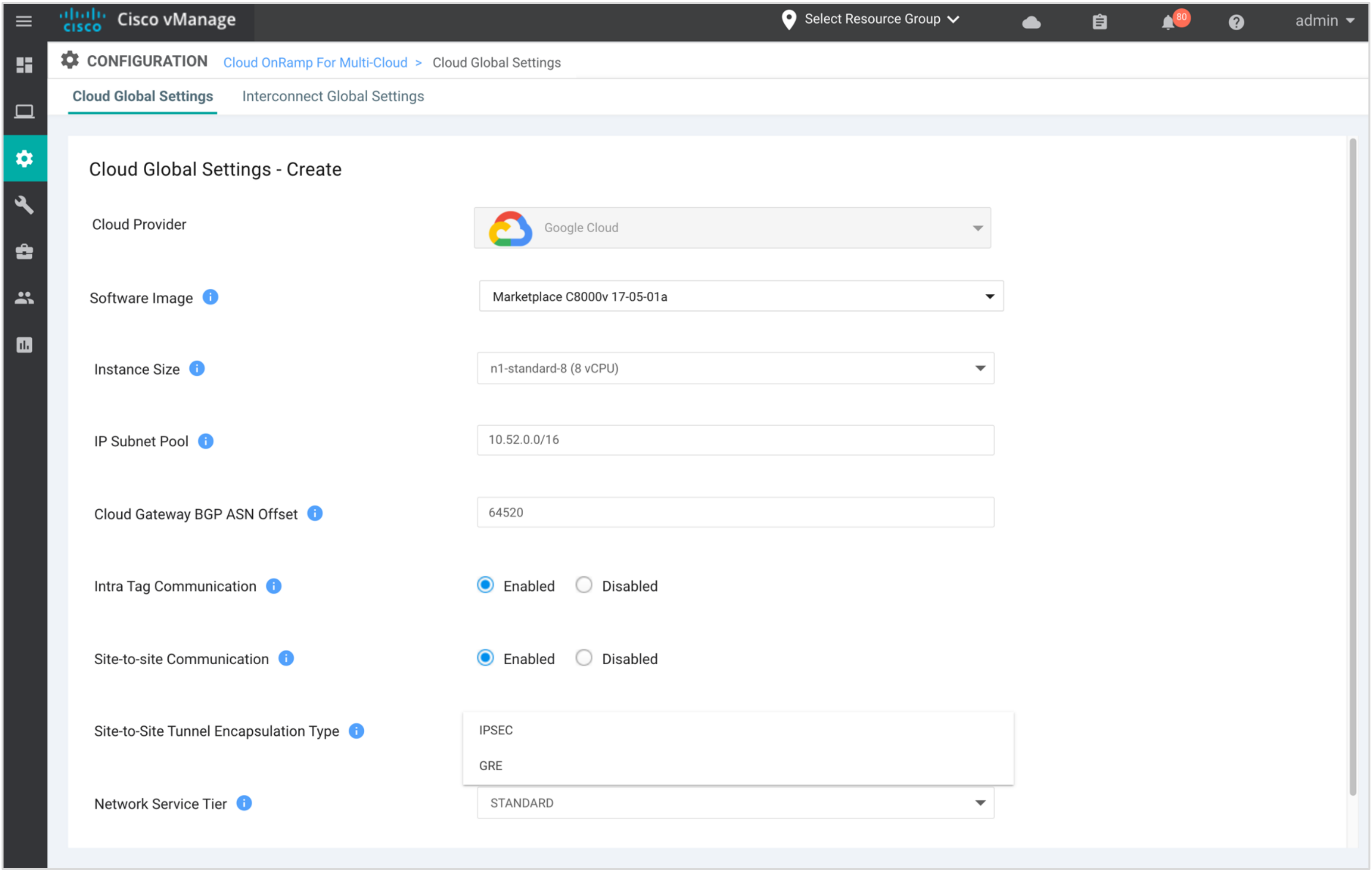
Network Service Tier: Choose one of the GCP network service tiers

Step 3. Enter the following details to the global settings page.

Field	Details
Software Image	Choose the software image that the Cisco Catalyst80000v devices must boot up with in Google Cloud. The drop down includes Marketplace catalyst 8000v 17-04-01a and Marketplace catalyst 8000v 17-05-01a release. In this deployment, the image, Marketplace catalyst 8000v 17-05-01a is selected.
Instance Size	From the drop-down list, choose an instance based on your requirements. The drop down includes the instance sizes C4, N1-Standard-4 and C8, N1-Standard-8 instance type. Machine type N1-standard-4 provides an instance with 4 vCPUs and 15GB of memory, and N1-standard-8 provides an instance with 8 vCPUs and 30GB of memory. Note: the maximum egress bandwidth for the two machine types are different, N1-standard-4 provides 10GBPS vs 16Gbps available in N1-Standard-8 instance type.
IP Subnet Pool	Specify the IP subnet pool for all the Cisco SD-WAN cloud gateway to be deployed in Google Cloud. The subnet pool prefix must be between /16 and /21 subnet. In this deployment, the IP subnet pool is set to 10.52.0.0/16.
Cloud Gateway BGP ASN	Enter a BGP autonomous system number (ASN) between the range 64250 to 65520. • The BGP ASN entered here will be the value for the Google Cloud Routers (GCRs) in the Site-to-Cloud Transit VPC. • The entered BGP ASN plus one will be the ASN for Google Cloud Routers (GCRs) in Site-to-Site Transit VPC. • The entered ASN plus 10 will be the BGP ASN assigned to all your Catt 8000v devices.

© 2020 Cisco and/or its affiliates. All rights reserved.

	All ASNs must belong to the private ASN space.
Intra Tag Communication	Click on either of the radio button to enable or disable communication between the host VPCs part of the same tag.
Site-to-Site Communication	To enable Site-to-Site (S2S) use case select the **Enabled** radio button to establish your site-to-site transit connectivity using Google global network. Otherwise, choose Disabled. In this deployment we have set this to **Enabled** state.
Site-to-Site Tunnel Encapsulation Type	To establish the site to site communication, a second VPN 0 WAN Tunnel interface is created in the Catalyst8000v devices. The tunnel encapsulation type between the two sites can be either of type GRE or IPsec. This tab lists a drop-down that includes both GRE and IPsec encapsulation, choose one or the other. Note: The overall IPsec tunnel bandwidth between the sites cannot go beyond 3 GB, therefore Google recommends the use of GRE as it provides twice the bandwidth/throughput. Also, note regardless of the encapsulation type chosen all data traffic traversing through the Google backbone is encrypted.
Network Service Tier	Choose one of the Google Cloud service tiers. PREMIUM: Provides high-performing network experience using Google global network. STANDARD: Allows control over network costs.

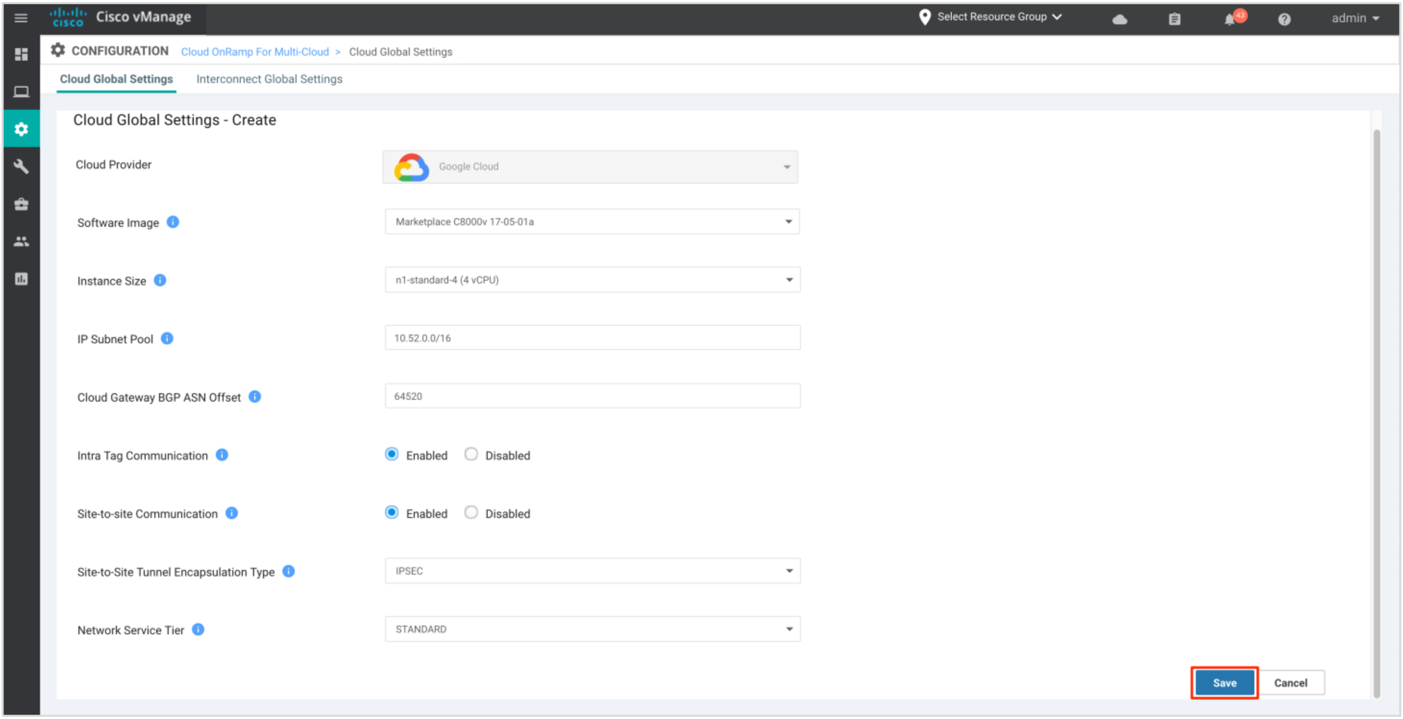

Cisco vManage
Select Resource Group
80
admin
CONFIGURATION
Cloud OnRamp For Multi-Cloud > Cloud Global Settings
Cloud Global Settings
Interconnect Global Settings

Cloud Global Settings - Create

Cloud Provider	Google Cloud
Software Image	Marketplace C8000v 17-05-01a
Instance Size	n1-standard-8 (8 vCPU)
IP Subnet Pool	10.52.0.0/16
Cloud Gateway BGP ASN Offset	64520
Intra Tag Communication	● Enabled ○ Disabled
Site-to-site Communication	● Enabled ○ Disabled
Site-to-Site Tunnel Encapsulation Type	IPSEC GRE
Network Service Tier	STANDARD

Step 4. Click **Save** or **Update** to complete the setup workflow.

© 2020 Cisco and/or its affiliates. All rights reserved.



Cloud Global Settings - Create

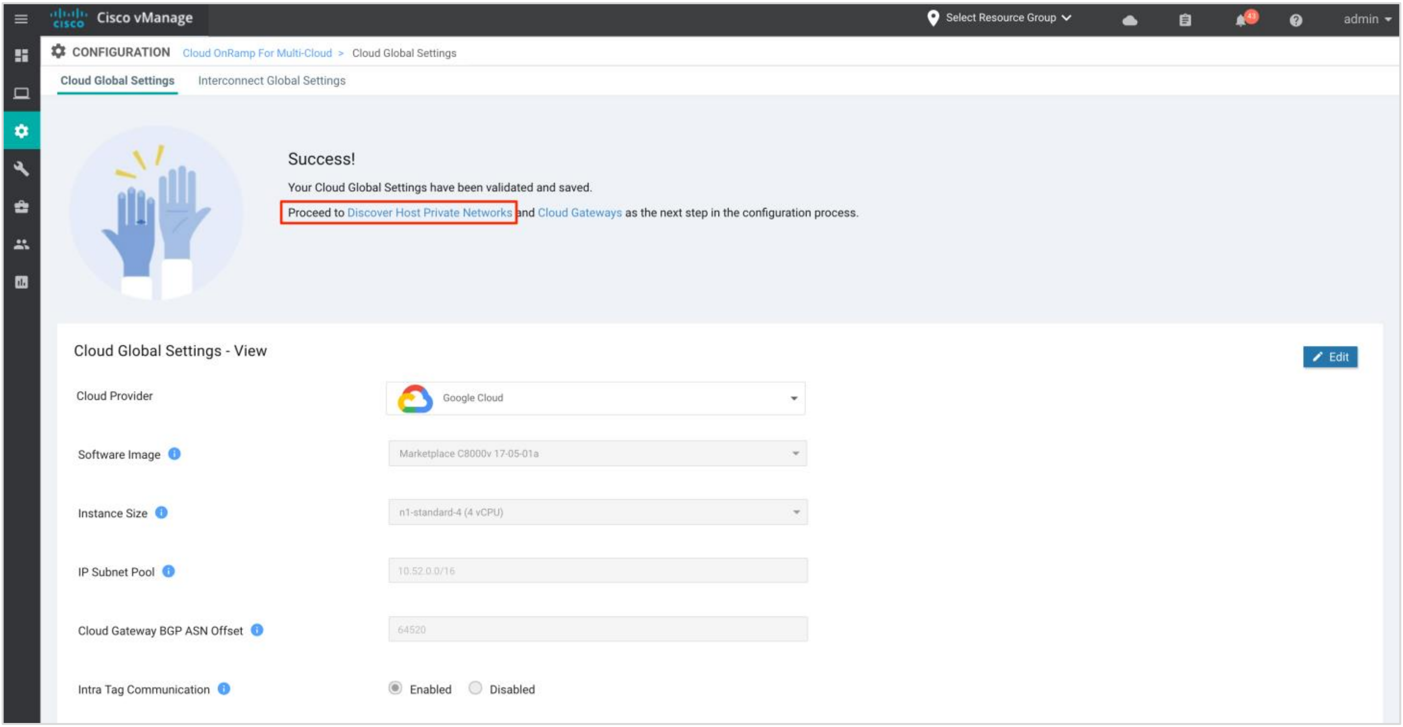
Cloud Provider	Google Cloud
Software Image	Marketplace C8000v 17-05-01a
Instance Size	n1-standard-4 (4 vCPU)
IP Subnet Pool	10.52.0.0/16
Cloud Gateway BGP ASN Offset	64520
Intra Tag Communication	● Enabled ○ Disabled
Site-to-site Communication	● Enabled ○ Disabled
Site-to-Site Tunnel Encapsulation Type	IPSEC
Network Service Tier	STANDARD

Process 3: Discover and Tags - Create Tags for the Discovered Host VPCs

After you associate your Google cloud account with Cisco vManage, you can discover your host VPCs in the regions associated with your Google cloud account. The discovered VPCs are associated to tags and these tags are used later during within Intent matrix to establish connectivity between your Google host VPCs and SD-WAN branch VPNs.

Note: If Intra Tag communication is enabled from the global settings, then all VPCs added within the same tag can communicate with each other.

Step 1. From the success page, click on **Discover Host Private Networks** to associate your host VPCs to tags.


Cisco vManage
Select Resource Group
admin
CONFIGURATION
Cloud OnRamp For Multi-Cloud > Cloud Global Settings
Cloud Global Settings
Interconnect Global Settings
Edit

Success!

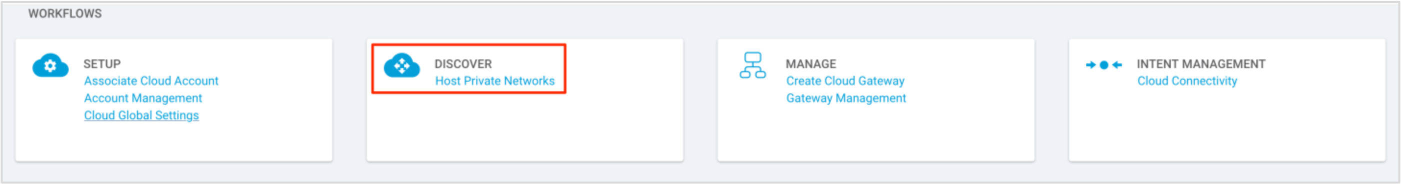
Your Cloud Global Settings have been validated and saved.

Proceed to Discover Host Private Networks and Cloud Gateways as the next step in the configuration process.

Cloud Global Settings - View

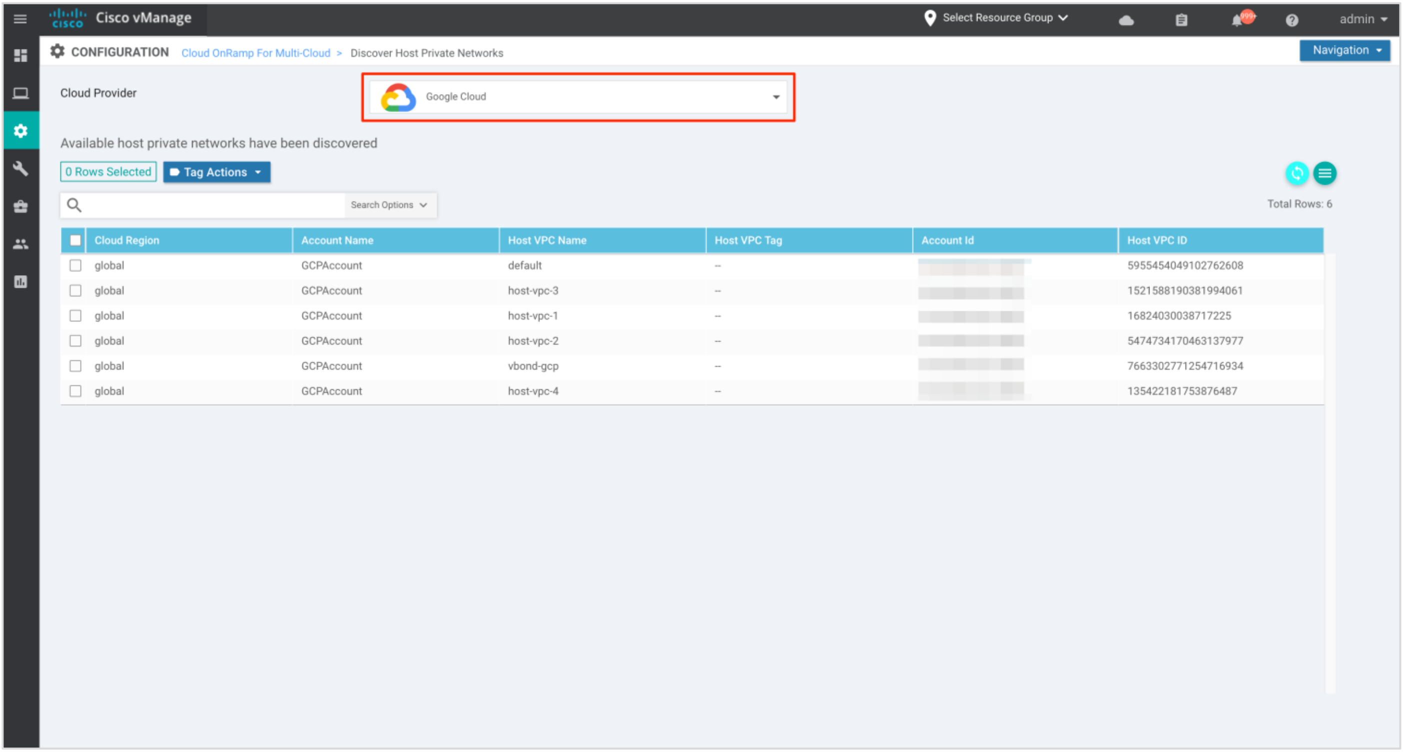
Cloud Provider	Google Cloud
Software Image	Marketplace C8000v 17-05-01a
Instance Size	n1-standard-4 (4 vCPU)
IP Subnet Pool	10.52.0.0/16
Cloud Gateway BGP ASN Offset	64520
Intra Tag Communication	● Enabled ○ Disabled

Note: Alternatively, you can also Discover host VPCs by navigating to main Cloud onRamp multi-cloud page workflow and click **Host Private Networks.**



Step 2. In the **Cloud Provider** field, choose **Google Cloud**. A list of discovered Host VPCs displays in a table with the following columns: **Cloud Region**, **Account Name**, **Host VPC Name**, **Host VPC Tag**, **Account ID**, and **Host VPC ID**.

© 2020 Cisco and/or its affiliates. All rights reserved.



Cisco vManage | Select Resource Group | admin

CONFIGURATION | Cloud OnRamp For Multi-Cloud > Discover Host Private Networks | Navigation

Cloud Provider: Google Cloud

Available host private networks have been discovered

0 Rows Selected | Tag Actions | Search Options | Total Rows: 6

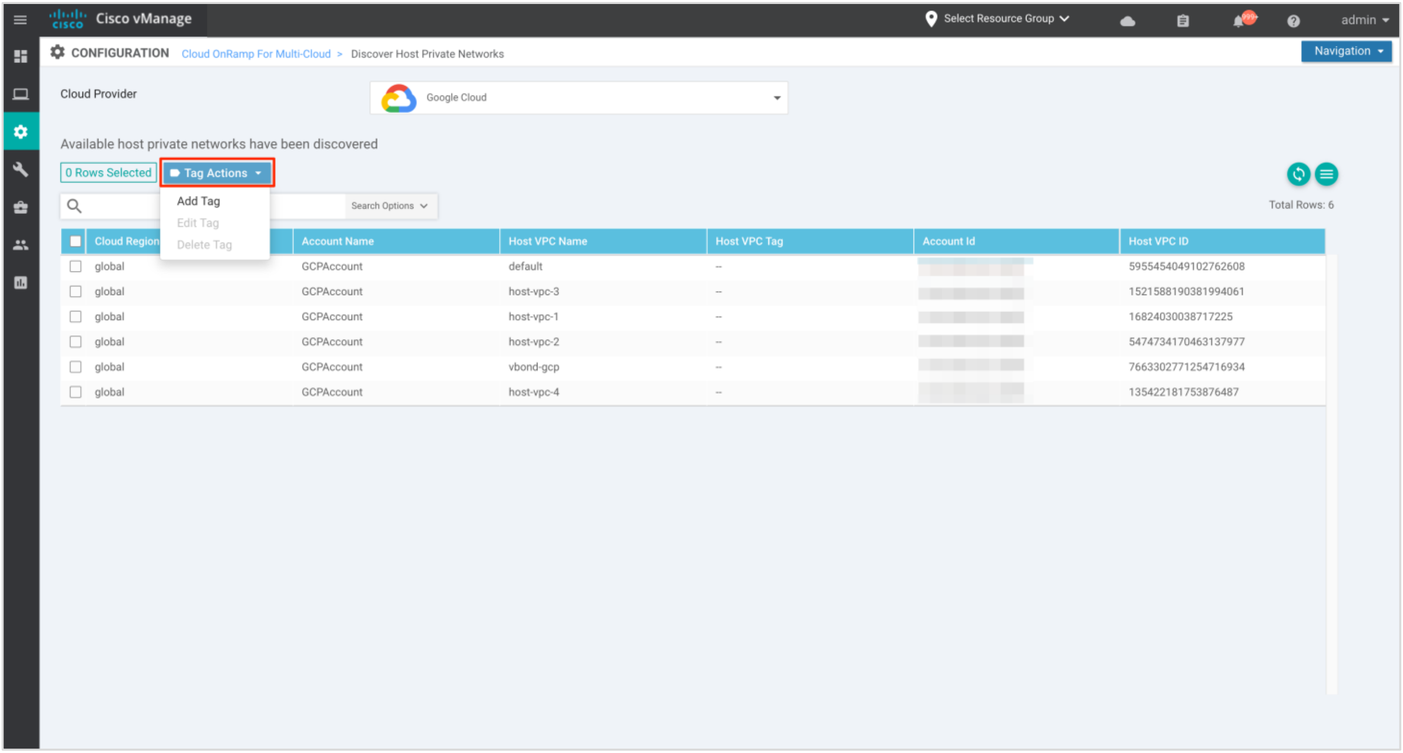
□	Cloud Region	Account Name	Host VPC Name	Host VPC Tag	Account Id	Host VPC ID
□	global	GCPAccount	default	--	[redacted]	5955454049102762608
□	global	GCPAccount	host-vpc-3	--	[redacted]	1521588190381994061
□	global	GCPAccount	host-vpc-1	--	[redacted]	16824030038717225
□	global	GCPAccount	host-vpc-2	--	[redacted]	5474734170463137977
□	global	GCPAccount	vbond-gcp	--	[redacted]	7663302771254716934
□	global	GCPAccount	host-vpc-4	--	[redacted]	135422181753876487

Step 3. Click the **Tag Actions** drop-down list to do any of the following:

Add Tag: Create a tag for a VPC or a group of VPCs.

Edit Tag: Change the selected VPCs for an existing tag.

Delete Tag: Delete the tag for the selected VPC.



Cisco vManage | Select Resource Group | admin

CONFIGURATION | Cloud OnRamp For Multi-Cloud > Discover Host Private Networks | Navigation

Cloud Provider: Google Cloud

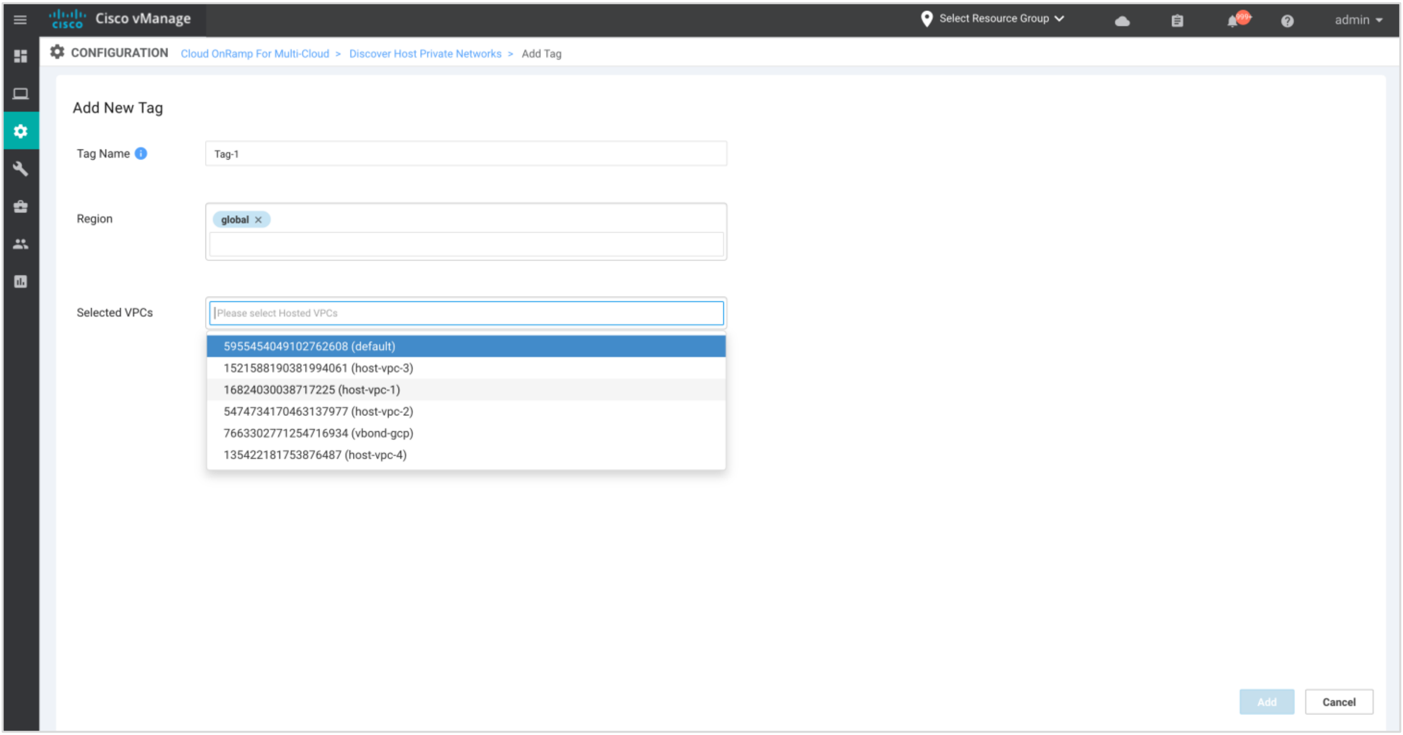
Available host private networks have been discovered

0 Rows Selected | Tag Actions | Search Options | Total Rows: 6

□	Cloud Region	Account Name	Host VPC Name	Host VPC Tag	Account Id	Host VPC ID
□	global	GCPAccount	default	--	[redacted]	5955454049102762608
□	global	GCPAccount	host-vpc-3	--	[redacted]	1521588190381994061
□	global	GCPAccount	host-vpc-1	--	[redacted]	16824030038717225
□	global	GCPAccount	host-vpc-2	--	[redacted]	5474734170463137977
□	global	GCPAccount	vbond-gcp	--	[redacted]	7663302771254716934
□	global	GCPAccount	host-vpc-4	--	[redacted]	135422181753876487

© 2020 Cisco and/or its affiliates. All rights reserved.

Step 4. Under **Add New Tag**, enter a name for the **Tag Name**, set the **Region** as **Global** and choose the host VPCs to be associated with the new tag. You can choose one or more VPCs and associate it to the same tag.



CONFIGURATION Cloud OnRamp For Multi-Cloud > Discover Host Private Networks > Add Tag

Add New Tag

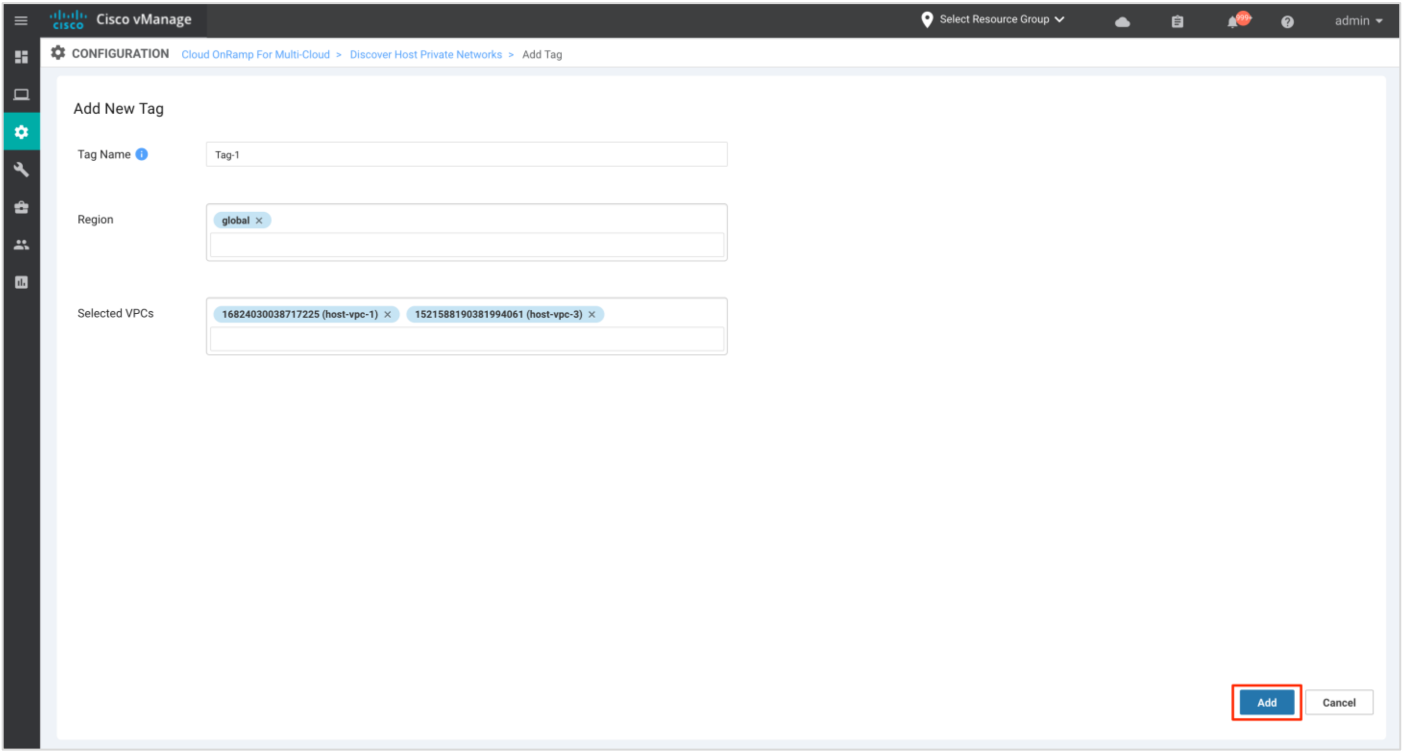
Tag Name Tag-1

Region global

Selected VPCs Please select Hosted VPCs

Cisco vManage
Select Resource Group
admin
5955454049102762608 (default)
1521588190381994061 (host-vpc-3)
16824030038717225 (host-vpc-1)
5474734170463137977 (host-vpc-2)
7663302771254716934 (vbond-gcp)
135422181753876487 (host-vpc-4)
Add
Cancel

Step 5. Click **Add** to create the Tag.



CONFIGURATION Cloud OnRamp For Multi-Cloud > Discover Host Private Networks > Add Tag

Add New Tag

Tag Name Tag-1

Region global

Selected VPCs 16824030038717225 (host-vpc-1) 1521588190381994061 (host-vpc-3)

© 2020 Cisco and/or its affiliates. All rights reserved.

Process 4: Manage – Create Cloud Gateway

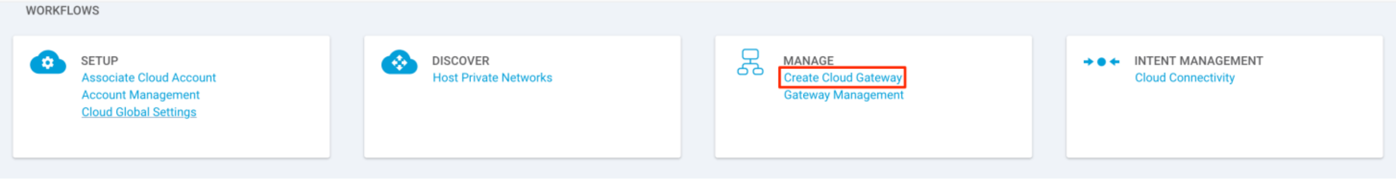
Once the cloud gateway global settings are added and host VPCs are associated to the tags, the next process is to instantiate a pair of Cisco Catalyst 8000V instances within the cloud gateway anchored in the three reserved VPCs –WAN transit VPC, site-to-site transit VPC, and site-to-cloud transit VPC.

Procedure 1: Create and Manage Cloud Gateways

This procedure describes how to create a Cisco SD-WAN cloud gateway with Google Cloud.

Step 1. In Cisco vManage, choose **Configuration** > **Cloud OnRamp for Multi-Cloud**.

Step 2. Under the **Manage** Workflow, click **Create Cloud Gateway**.



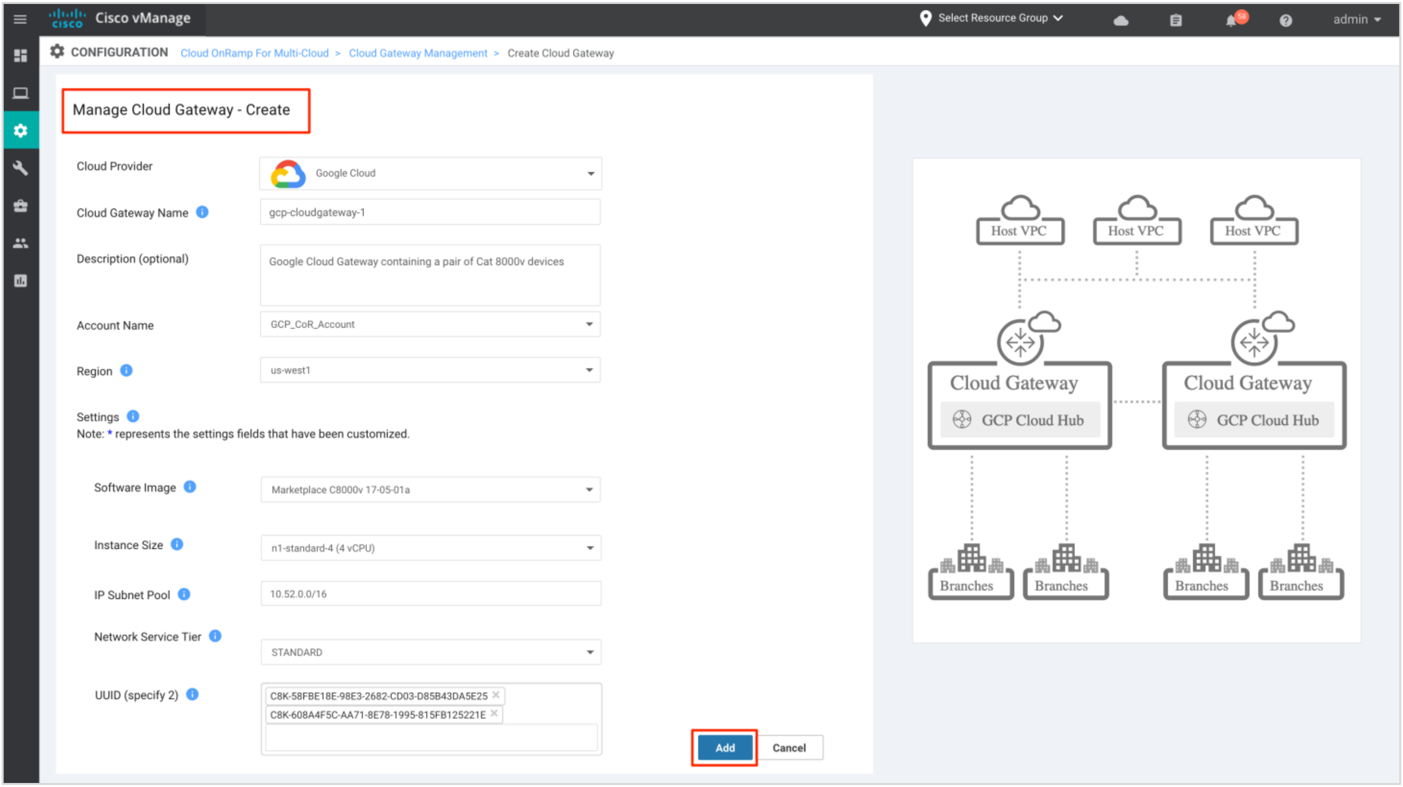
Step 3. Within the Manage Cloud Gateway Page, enter the following details.

Field		Details
Cloud Provider		Choose Google Cloud from the drop-down list
Cloud Gateway Name		Enter a name for your cloud gateway. Ensure that the name is in lowercase letters. See the Google Cloud documentation for information about naming resources and naming convention.
Description (optional)		Enter a description for the new Cloud Gateway (CGW).
Account Name		Choose your Google Cloud account name from the drop-down list.
Region		Choose a Google region from the drop-down list. The cloud gateway containing a pair of Catalyst8000v devices will be hosted in the chosen Google cloud region.
Settings	You can use either the cloud global settings or customize settings for individual Cloud Gateways (CGW) using the fields below.	
	Software Image (optional)	Edit the software image for your Catalyst8000v devices.
	Instance Size (optional)	Edit if needed the instance size for Cisco Catalyst 8000V, based on your requirements.
	IP Subnet Pool (optional)	Edit if needed the IP subnet pool to be used for the Google Cloud WAN VPC. This subnet pool needs prefixes between /16 and /21. The IP subnet pool must not overlap with the IP subnet pool specified in Cloud Global Settings.

© 2020 Cisco and/or its affiliates. All rights reserved.

	Network Service Tier (optional)	Edit the Google Cloud service tiers. PREMIUM: Provides high-performing network experience using Google global network. STANDARD: Allows control over network costs.
	UUID	Choose two Cisco Catalyst 8000V licenses from the drop-down list. These Catalyst8000v devices are deployed in the CGW.

After all the field are defined, Click **Add** to create a Cloud Gateway in Google cloud.



CONFIGURATION Cloud OnRamp For Multi-Cloud > Cloud Gateway Management > Create Cloud Gateway

Manage Cloud Gateway - Create

Cloud Provider	Google Cloud
Cloud Gateway Name	gcp-cloudgateway-1
Description (optional)	Google Cloud Gateway containing a pair of Cat 8000v devices
Account Name	GCP_CoR_Account
Region	us-west1

Settings

Note: * represents the settings fields that have been customized.

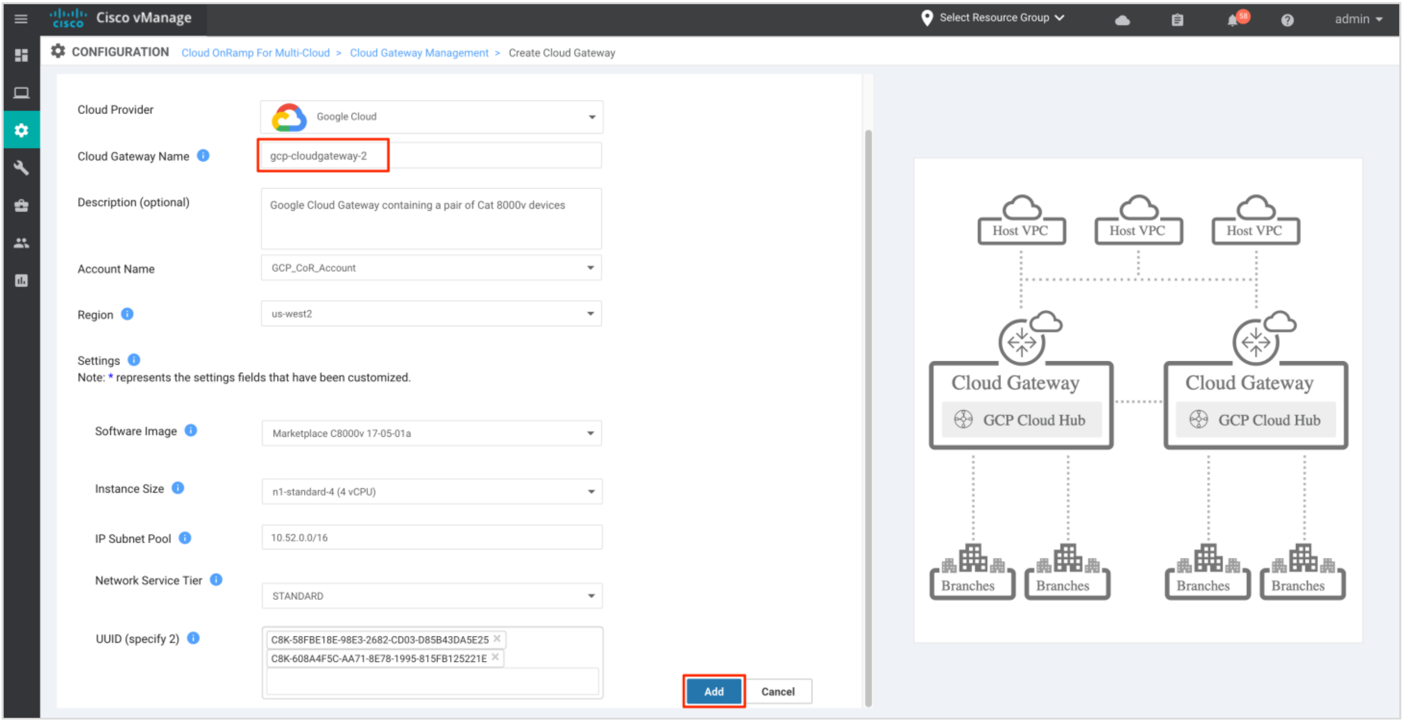
Software Image	Marketplace C8000v 17-05-01a
Instance Size	n1-standard-4 (4 vCPU)
IP Subnet Pool	10.52.0.0/16
Network Service Tier	STANDARD
UUID (specify 2)	C8K-58FBE18E-98E3-2682-CD03-D85B43DA5E25 C8K-608A4F5C-AA71-8E78-1995-815FB125221E

Step 4. For the Site-to-Site (S2S) use case, create a second Cloud Gateway (CGW) in a different Google cloud region. The second Cloud Gateway (CGW) also brings up another pair of Catalyst8000v in a Transit VPC that shares the common CGW resources.

Follow the steps mentioned in the step 3 to create a second cloud gateway.

Note: Only one cloud gateway can be associated in a google region.

© 2020 Cisco and/or its affiliates. All rights reserved.



Cloud Provider: Google Cloud

Cloud Gateway Name: gcp-cloudgateway-2

Description (optional): Google Cloud Gateway containing a pair of Cat 8000v devices

Account Name: GCP_CoR_Account

Region: us-west2

Settings

Note: * represents the settings fields that have been customized.

Software Image: Marketplace C8000v 17-05-01a

Instance Size: n1-standard-4 (4 vCPU)

IP Subnet Pool: 10.52.0.0/16

Network Service Tier: STANDARD

UUID (specify 2): C8K-58FBE18E-98E3-2682-CD03-D85B43DA5E25
C8K-608A4F5C-AA71-8E78-1995-815FB125221E

This process creates the site to cloud and site to site network connectivity (NCC) hubs, along with NCC spokes followed by site to cloud and site to site VPC, the WAN/ site to cloud/ site to site subnets are created, two cloud routers one primary and one redundant are deployed in in S2C and S2S VPC.

This ends the creation of cloud gateway; next mapping changes are identified.

Process 5: Intent Management

Only one service side VPN is created to complete the site to cloud use case. Within the intent Mapping, you can map your tags to the VPN to establish access from your site to the cloud resources.

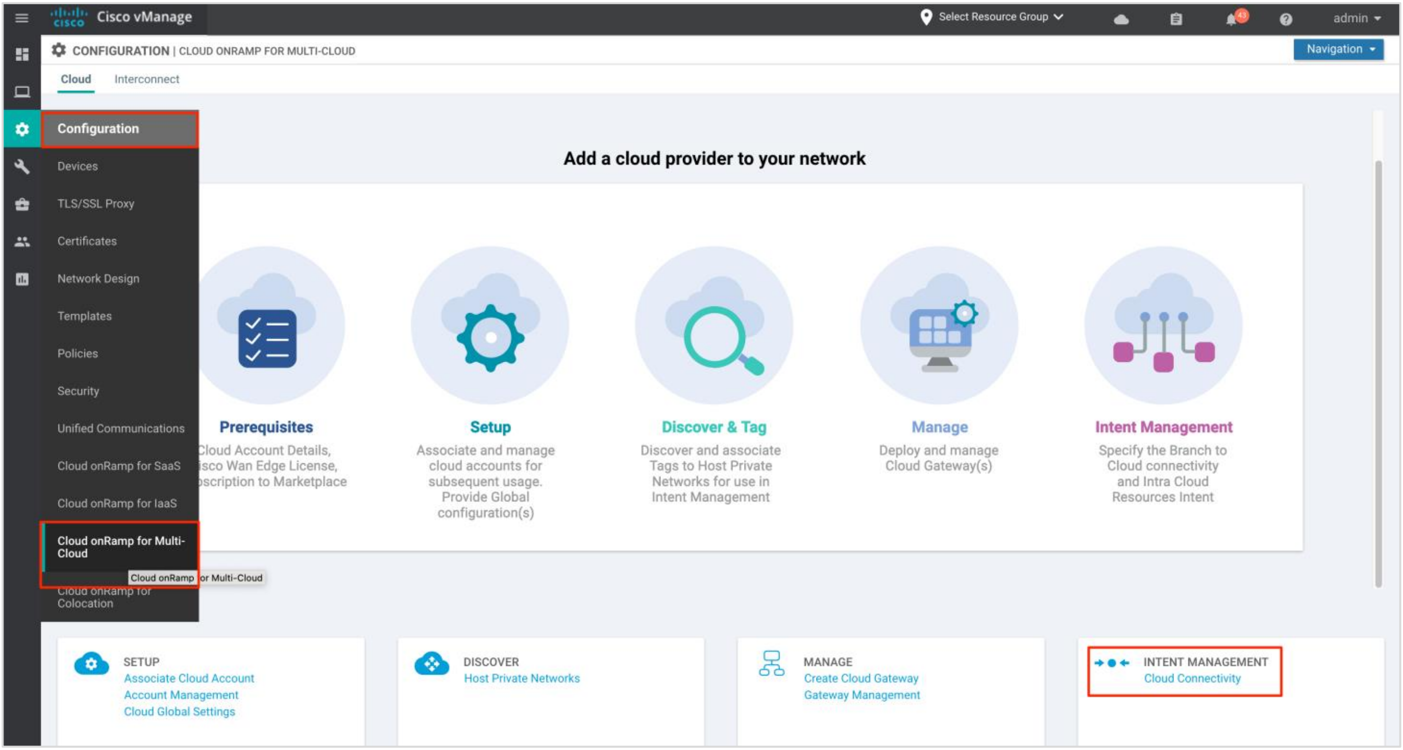
Note: In GCP, as of the 20.5 release you can map your tags to only one VPN.

In this workflow, tag-1 and tag-2 is mapped to VPN 1.

Step 1. Navigate to **Configuration** > **Cloud OnRamp for Multi-Cloud**.

Step 2. Under **Intent Management**, click **Cloud Connectivity**. You can alternatively choose this from the navigation tab on the right.

© 2020 Cisco and/or its affiliates. All rights reserved.



Add a cloud provider to your network

Prerequisites
Cloud Account Details, isco Wan Edge License, bscription to Marketplace

Setup
Associate and manage cloud accounts for subsequent usage. Provide Global configuration(s)

Discover & Tag
Discover and associate Tags to Host Private Networks for use in Intent Management

Manage
Deploy and manage Cloud Gateway(s)

Intent Management
Specify the Branch to Cloud connectivity and Intra Cloud Resources Intent

Step 3. In the **Cloud Provider** field, choose **Google Cloud** from the drop-down list.

The screen displays a connectivity matrix showing source VPNs, and their destinations. The following legend provides information about the status of the intent:

Blue: Intent Defined

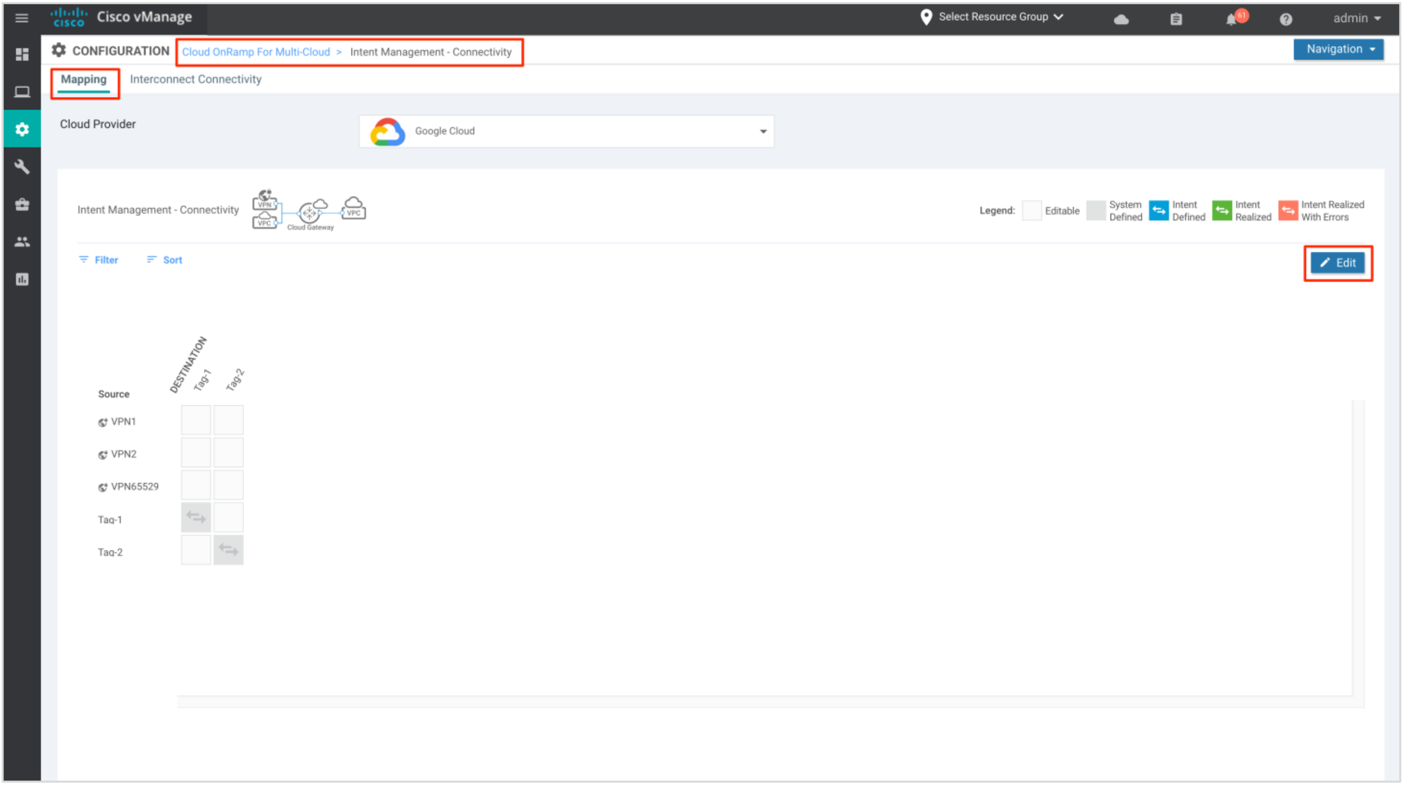
Green: Intent Realized

Red: Intent Realized with Errors

Click any of the cells in the matrix to get a more detailed status information.

Under **Mapping**, define or record a new intent. Click **Edit** to map a VPN to a configured Tag.

© 2020 Cisco and/or its affiliates. All rights reserved.



Cisco vManage — CONFIGURATION — Cloud OnRamp For Multi-Cloud > Intent Management - Connectivity

Mapping | Interconnect Connectivity

Cloud Provider: Google Cloud

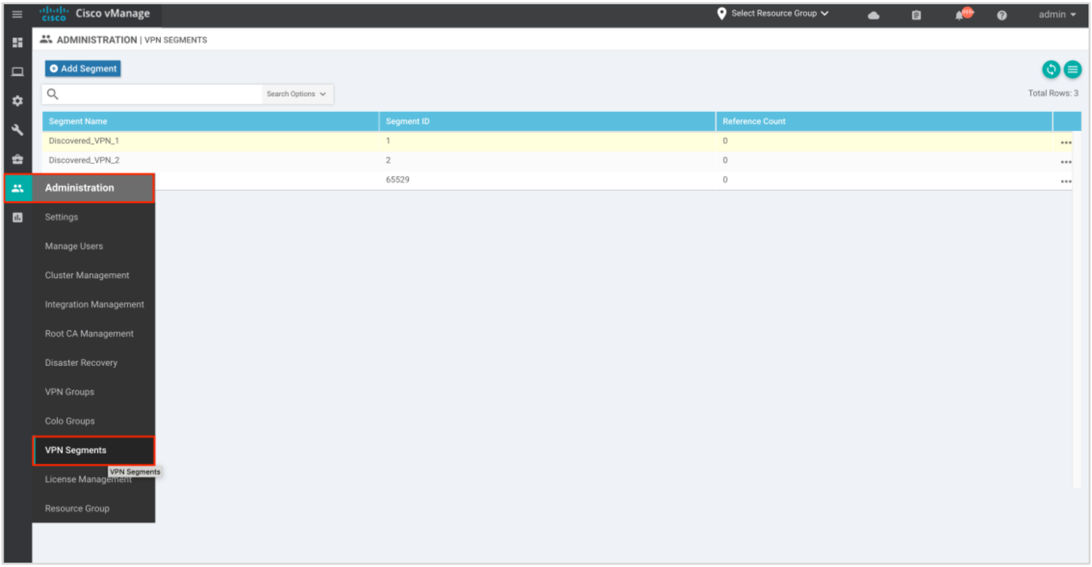
Intent Management - Connectivity

Legend: □ Editable ▨ System Defined 🟦 Intent Defined 🟩 Intent Realized 🟥 Intent Realized With Errors

Source	Tag-1	Tag-2
VPN1		
VPN2		
VPN65529		
Tag-1	▨	
Tag-2		▨

Technical Tip

Within the Intent Management – Connectivity, you might notice one or more VPN as source. The VPN list here is based on the VPN Segments available under Administration tab. Regardless of how many VPNs you view here, through the Google cloud onRamp workflow only one service-side VPN is deployed in each Catalyst 8000v for the site to cloud use case. Therefore, you can map tags to only one VPN.



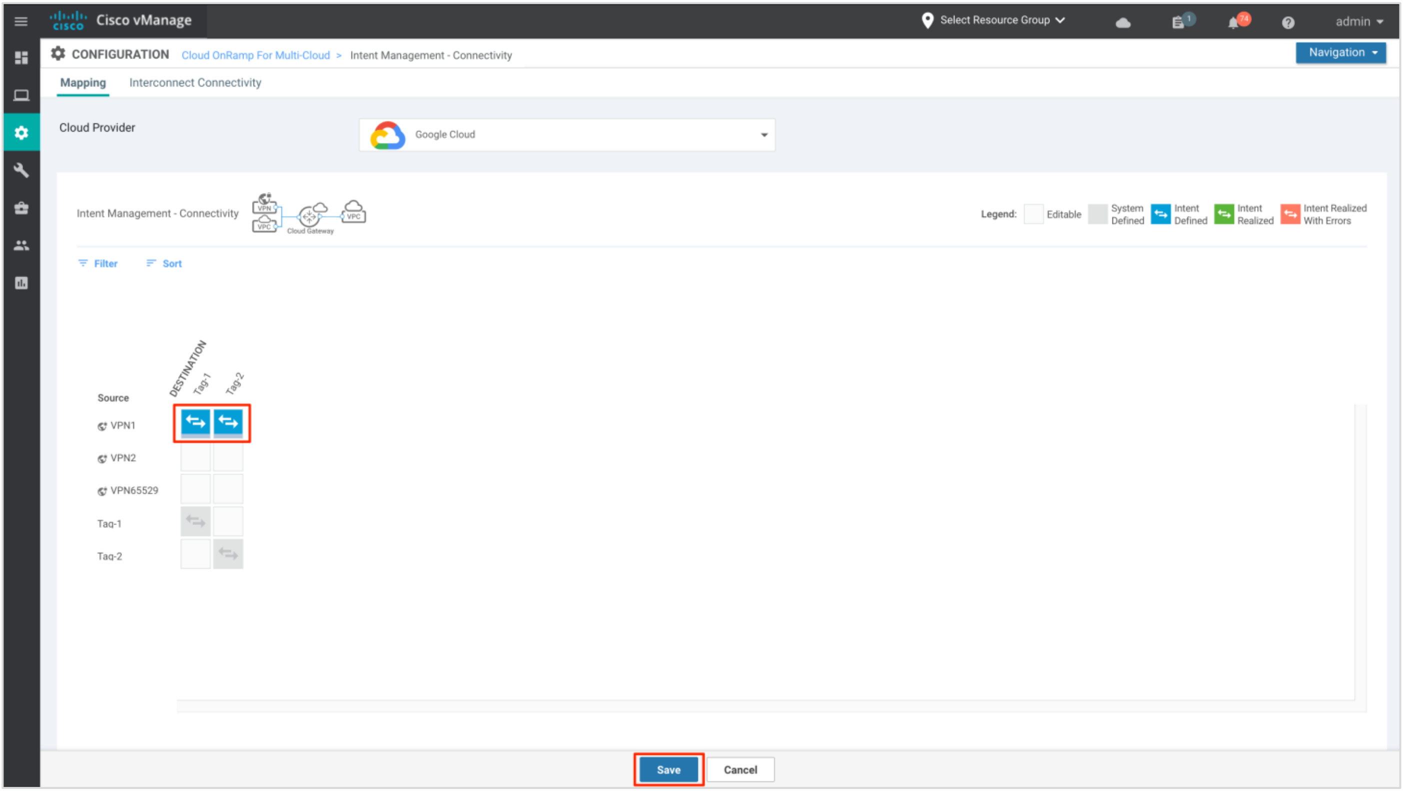
Cisco vManage — ADMINISTRATION | VPN SEGMENTS

Total Rows: 3

Segment Name	Segment ID	Reference Count
Discovered_VPN_1	1	0
Discovered_VPN_2	2	0
	65529	0

© 2020 Cisco and/or its affiliates. All rights reserved.

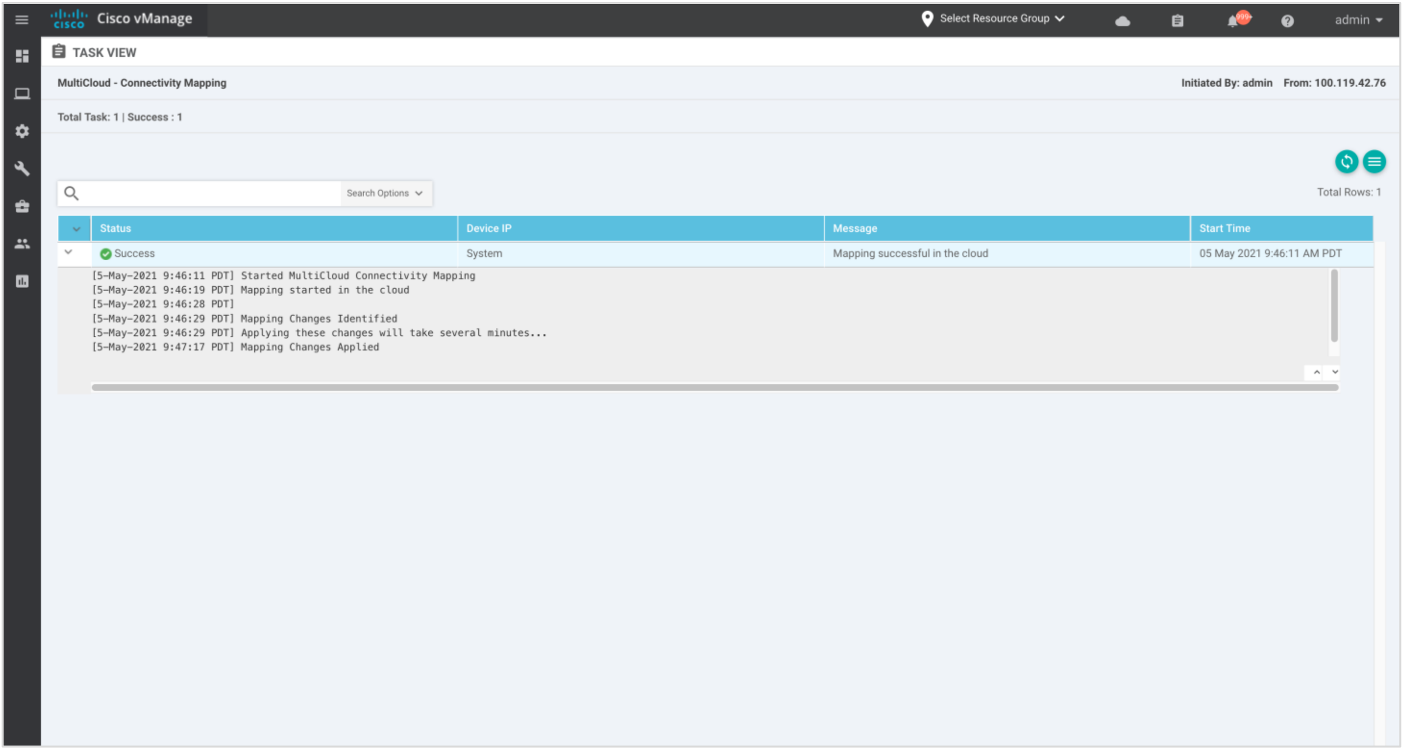
Step 4. Choose the cells that correspond to a VPN and the VPC tags associated with it and click **Save**. In this guide, we are mapping VPN 1 to tag 1 and tag 2 VPC workloads.



Cloud Provider: Google Cloud

Source	DESTINATION Tag-1	Tag-2
VPN1	⇆	⇆
VPN2		
VPN65529		
Tag-1	⇆	
Tag-2		⇆

The following screenshot displays the **TASK VIEW** page upon completion of **Multicloud-Connectivity Mapping**.



MultiCloud - Connectivity Mapping

Initiated By: admin From: 100.119.42.76

Total Task: 1 | Success : 1

Total Rows: 1

Status	Device IP	Message	Start Time
Success	System	Mapping successful in the cloud	05 May 2021 9:46:11 AM PDT

```
[5-May-2021 9:46:11 PDT] Started MultiCloud Connectivity Mapping
[5-May-2021 9:46:19 PDT] Mapping started in the cloud
[5-May-2021 9:46:28 PDT]
[5-May-2021 9:46:29 PDT] Mapping Changes Identified
[5-May-2021 9:46:29 PDT] Applying these changes will take several minutes...
[5-May-2021 9:47:17 PDT] Mapping Changes Applied
```

This completes the Cloud on-Ramp for Multicloud workflow.

Process 6: Deletion of Resources

If you want to delete and clean up resources, which were created by the Cloud onRamp GCP automation, follow the order below.

- Delete NCC Spokes using Google cloud CLI
- Delete NCC Hubs using Google cloud CLI
- Delete GCRs using GCP Console (Hybrid Connectivity -> Cloud Routers page) or CLI
- Delete c8kv VMs using GCP Console or CLI
- Delete VPCs using GCP Console or CLI

Example for Google cloud CLI listing two NCC hubs – the first hub is used for site-to-site and the second hub is for site-to-cloud use case:

```
cloudshell: ~ (gcp)$ gcloud alpha network-connectivity hubs list
[
  {
    "createTime": "2021-03-17T06:01:36.984779764Z",
    "name": "projects/gcp-XXXXX635/locations/global/hubs/s2s-ncc-hub--emo-xxxxx",
    "spokes": [

"https://networkconnectivity.googleapis.com/v1alpha1/projects/53XXXXX3/locations/austra
lia-southeast1/spokes/gc-sydney-cgw1--emo-xxxxx-australia-southeast1-s2s-ncc-spoke",

"https://networkconnectivity.googleapis.com/v1alpha1/projects/5325XXXXX/locations/us-
west2/spokes/gc-uswest-cgw1--emo-xxxxx-us-west2-s2s-ncc-spoke"
    ],
    "state": "ACTIVE",
    "uniqueId": "603ab47a-8979-XXXXX-5XXXX6b9d360e",
    "updateTime": "2021-03-17T06:01:37.281770511Z"
  },
  {
    "createTime": "2021-03-17T05:58:25.072124681Z",
    "name": "projects/gcp-npitaev20XXXX/locations/global/hubs/s2c-ncc-hub--emo-xxxxx",
    "spokes": [

"https://networkconnectivity.googleapis.com/v1alpha1/projects/5325XXXX523/locations/aus
tralia-southeast1/spokes/gc-sydney-cgw1--emo-xxxxx-australia-southeast1-s2c-ncc-spoke",

"https://networkconnectivity.googleapis.com/v1alpha1/projects/5325XXXX6523/locations/us
-west2/spokes/gc-uswest-cgw1--emo-xxxxx-us-west2-s2c-ncc-spoke"
    ],
    "state": "ACTIVE",
    "uniqueId": "4236ce9b-210f-XXXXde-7b566e39f274",
    "updateTime": "2021-03-17T05:58:25.357399310Z"
  }
```

© 2020 Cisco and/or its affiliates. All rights reserved.

]

Operate - Cisco Cloud onRamp for Multi-Cloud Monitoring

Using the vManage GUI, you can monitor, troubleshoot, and manage the Cisco SD-WAN Cloud onRamp for Multi-Cloud using Google Cloud. The 3 main ways to monitor the deployment is as given below:

vManage Cloud onRamp for Multi-Cloud Dashboard: From the vManage Cloud onRamp for Multi-Cloud dashboard you can monitor the connectivity state of the Cloud Gateway (CGW), the mapped tags and host VPCs within those tags.

vManage Monitor Dashboard: From the vManage Monitor dashboard, you can view and gather error logs and interface details for the Catalyst 8000v routers deployed in the CGW.

vManage SSH Dashboard: From the vManage SSH dashboard, you can view the CLI configs and monitor route updates using show commands for all the Catalyst 8000v devices deployed in Google Clouds CGWs.

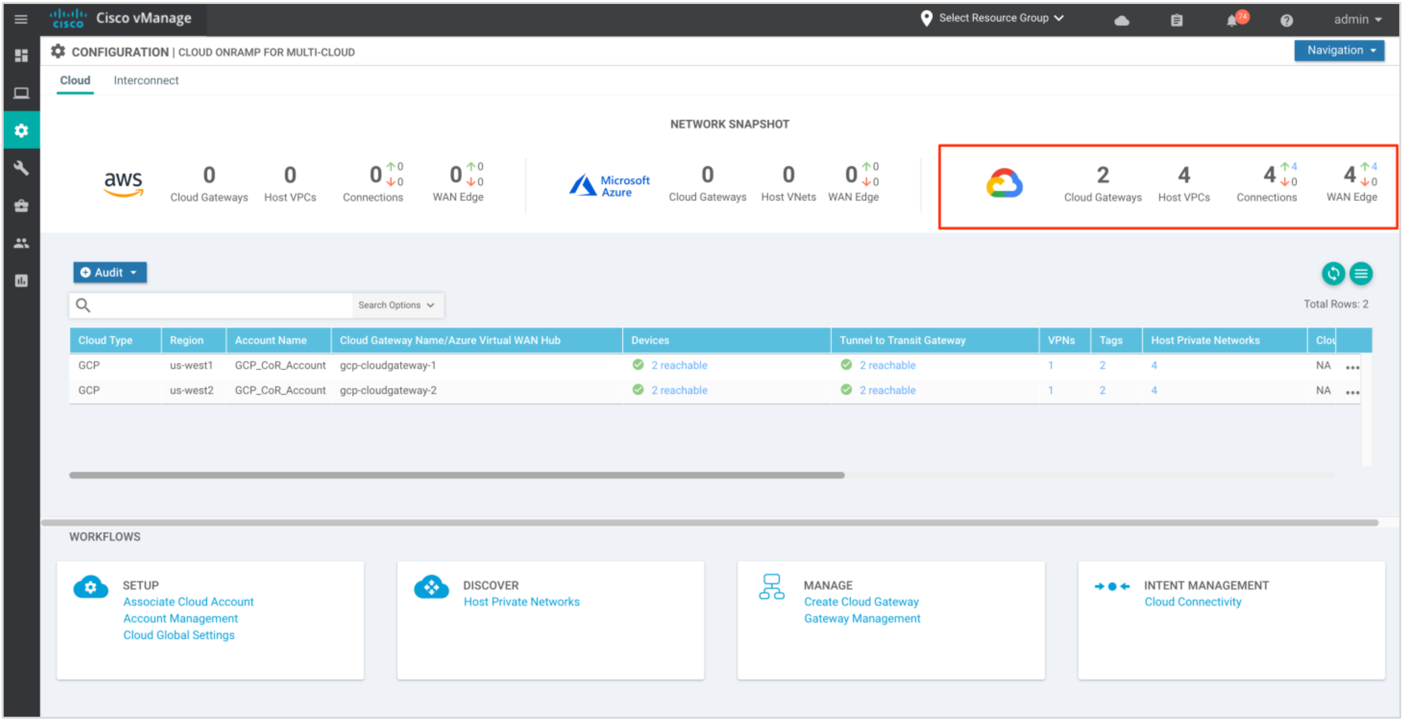
Process 1: vManage Cisco Cloud onRamp for Multi-Cloud Dashboard

Procedure 1: Reachability to Cisco Catalyst 8000v Instances

Verify the bring-up and reachability of the Cisco Catalyst 8000v instances provisioned within the cloud gateway(s).

Step 1. In Cisco vManage, choose **Configuration** > **Cloud onRamp for Multi-Cloud**.

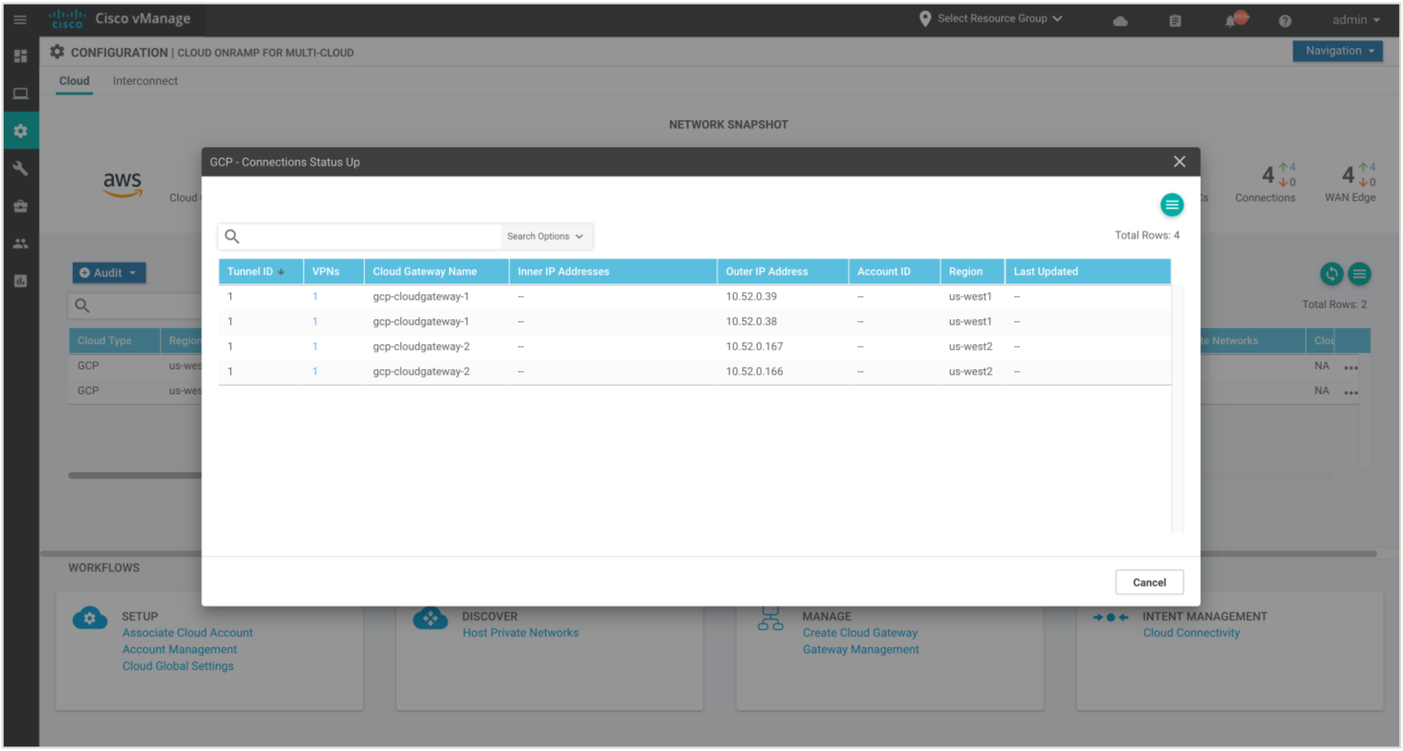
Step 2. Under the **Cloud** section located at the top of the screen, the **Network Snapshot** displays a summary of the cloud gateways deployed, the number of Google host VPCs connected to the Site via Tags, along with its Site-Cloud IP address and VPN label mapped to, finally followed by the status of Catalyst 8000v edge devices brought up to form the cloud gateway.



Cloud Type	Region	Account Name	Cloud Gateway Name/Azure Virtual WAN Hub	Devices	Tunnel to Transit Gateway	VPNs	Tags	Host Private Networks	Clou
GCP	us-west1	GCP_CoR_Account	gcp-cloudgateway-1	✓ 2 reachable	✓ 2 reachable	1	2	4	NA
GCP	us-west2	GCP_CoR_Account	gcp-cloudgateway-2	✓ 2 reachable	✓ 2 reachable	1	2	4	NA

The upward arrow above the section **Connections** indicates the status of the Site-to-Cloud connectivity i.e. the mapping between the site-to-cloud VPN/ VRF to Google host VPC. Click on the arrow to view the number of cloud gateways brought up, along with the VPNs label used to map cloud hosted VPC resources to the service side VPN in the Catalyst 8000v device.

In this design, two cloud gateways are brought up, one in US-West1 and the other in US-West2. Each cloud gateway contains a pair of Catalyst 8000v devices and each device is assigned one service side VPN (VRF 1) for Site-to-Cloud mapping. All Google host VPCs are mapped to VPN 1 and the result of this mapping/connectivity is displayed in the table below. The outer IP address in column five indicate the IP address assigned to the Catalyst 8000v interfaces part of the site-to-cloud VPN/VRF (VRF 1).



GCP - Connections Status Up

Total Rows: 4

Tunnel ID	VPNs	Cloud Gateway Name	Inner IP Addresses	Outer IP Address	Account ID	Region	Last Updated
1	1	gcp-cloudgateway-1	--	10.52.0.39	--	us-west1	--
1	1	gcp-cloudgateway-1	--	10.52.0.38	--	us-west1	--
1	1	gcp-cloudgateway-2	--	10.52.0.167	--	us-west2	--
1	1	gcp-cloudgateway-2	--	10.52.0.166	--	us-west2	--

The upward arrow above the section WAN Edge indicates the reachable WAN Edge devices. Click the arrow to view additional details.

In this deployment, two cloud gateways are deployed each a pair of Catalyst 8000v devices of the following Chassis UUID. The table also lists out the System IP, the name given to each of the cloud gateways along with the Google region in which it is hosted.

Procedure 2: Deployed Google Cloud Resources

Step 1. Another way to monitor the resources deployed through the cloud onramp workflow is by scrolling across the section located at the middle of the Cloud onRamp for multi-cloud dashboard.

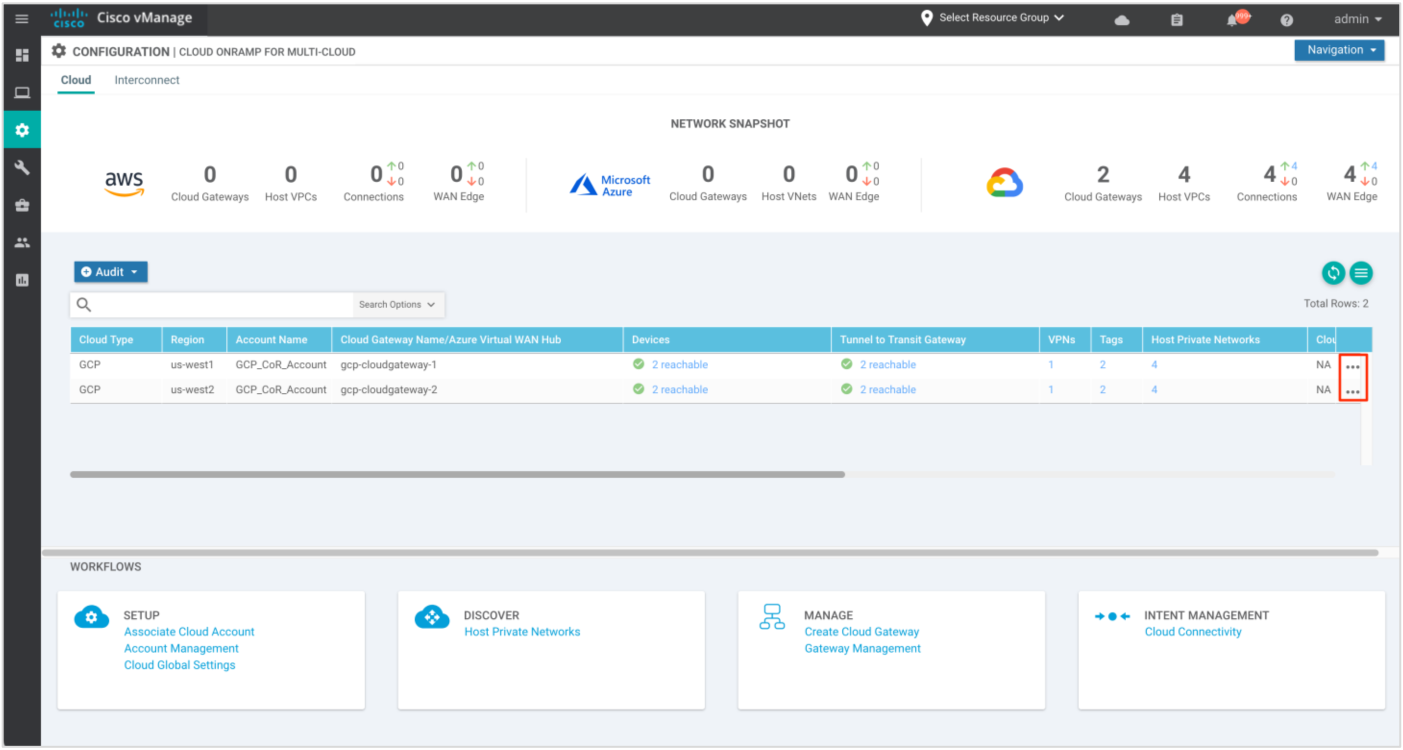
The columns list out the following

- Cloud Type: Lists out the type of cloud deployment, Azure, AWS or Google Cloud platform (GCP)
- Regions: Understand and validate the regions in which your Google cloud gateways are deployed
- Account Name: The name assigned while associating your google account to vManage NMS.
- Cloud Gateway Name: View the name of your cloud gateways deployed in each Google region.
- Device: This column contains a green tick symbol (success) or a red crossed out symbol (failure) to indicate the status of the reachable Catalyst 8000v devices in each of the two cloud gateways.

© 2020 Cisco and/or its affiliates. All rights reserved.

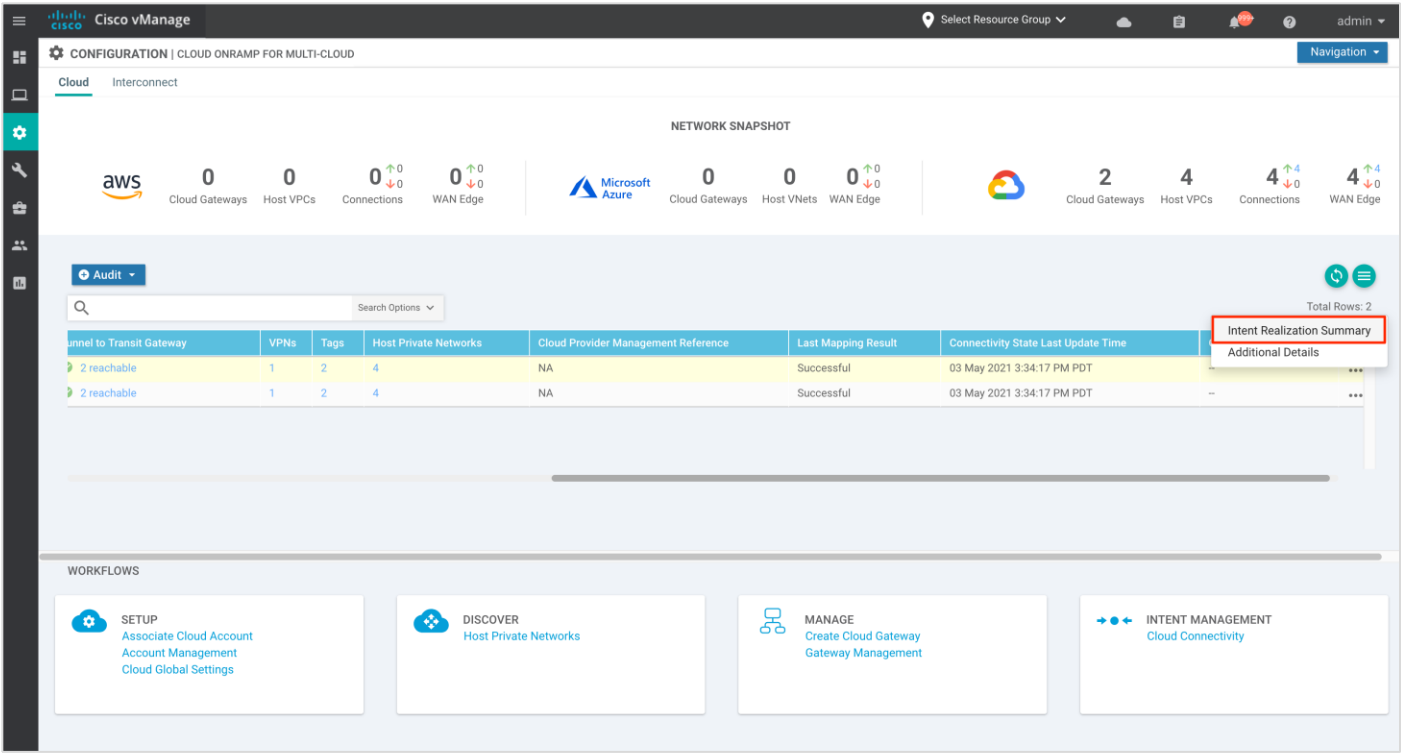
- Tunnel to Transit Gateway: This column indicates the connectivity status between your site-to-cloud service side VPN in Catalyst 8000v to the host VPC mapping.
- VPNs Tags and Host Private Networks: These three columns indicate the VPNs to tag mapping, along with details regarding the host VPCs discovered and attached to each tag.

Step 2. To gather further details regarding the Google cloud resources deployed through the Cloud onRamp workflow, click on the three dots **(…)** located to the right side.

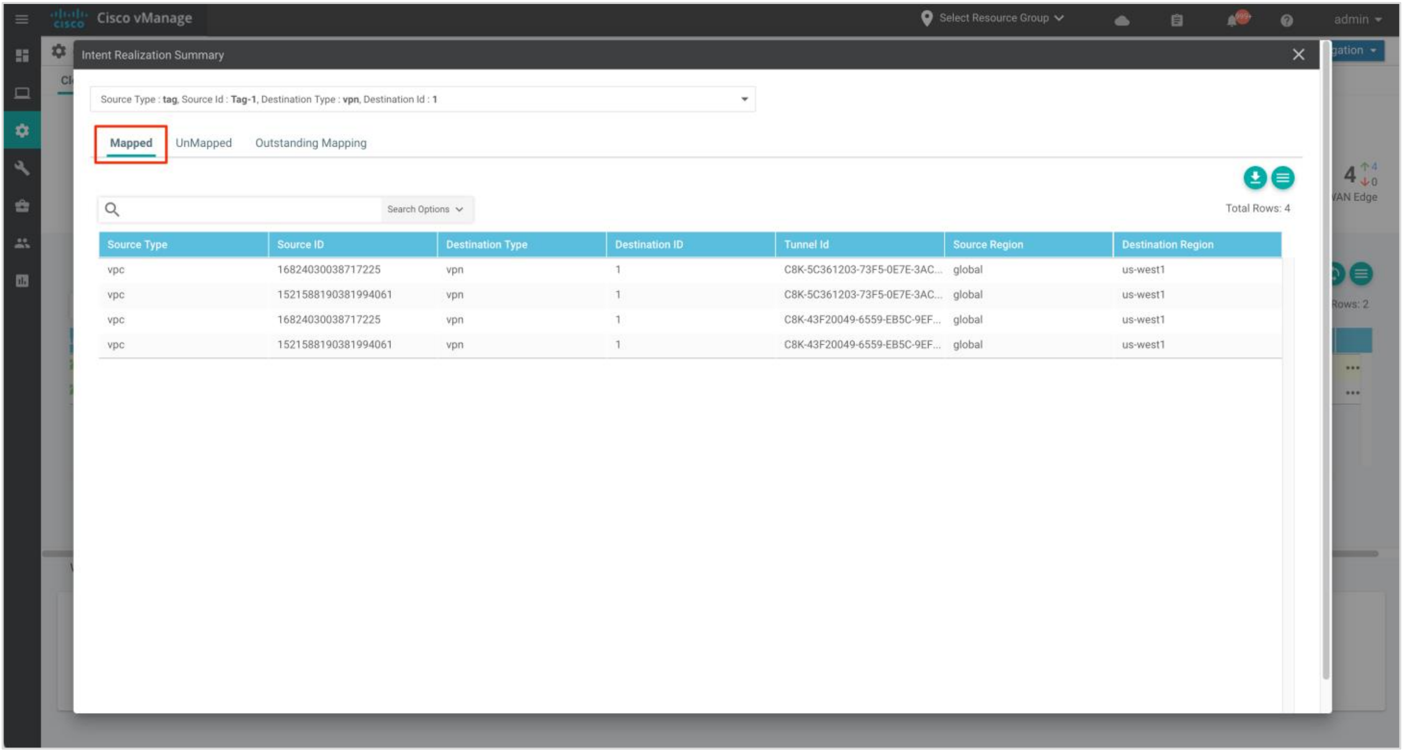


Cloud Type	Region	Account Name	Cloud Gateway Name/Azure Virtual WAN Hub	Devices	Tunnel to Transit Gateway	VPNs	Tags	Host Private Networks	Clou	
GCP	us-west1	GCP_CoR_Account	gcp-cloudgateway-1	✓ 2 reachable	✓ 2 reachable	1	2	4	NA	•••
GCP	us-west2	GCP_CoR_Account	gcp-cloudgateway-2	✓ 2 reachable	✓ 2 reachable	1	2	4	NA	•••

Step 3. Select **Intent Realization Summary** from the drop-down to view the mapped and unmapped host VPCs.



unnel to Transit Gateway	VPNs	Tags	Host Private Networks	Cloud Provider Management Reference	Last Mapping Result	Connectivity State Last Update Time	
2 reachable	1	2	4	NA	Successful	03 May 2021 3:34:17 PM PDT	--
2 reachable	1	2	4	NA	Successful	03 May 2021 3:34:17 PM PDT	--

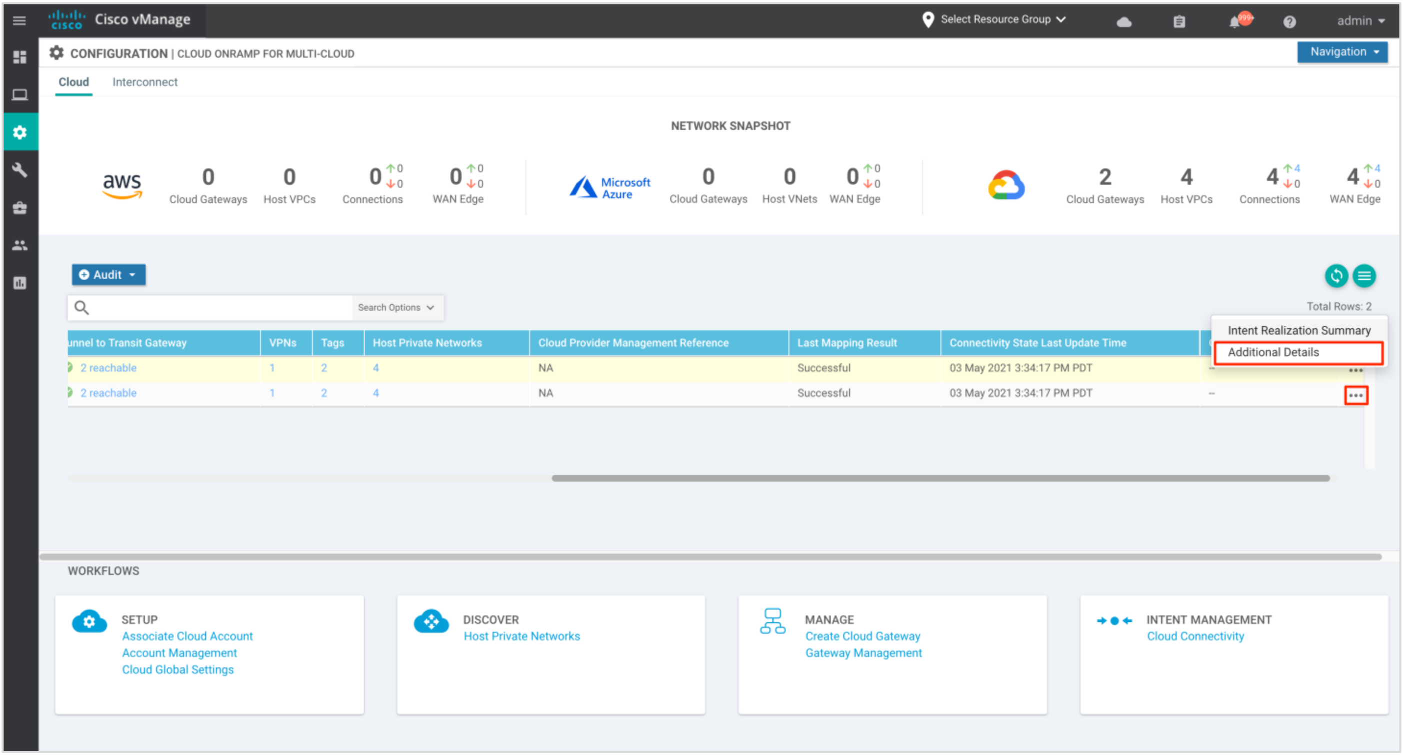


Source Type : **tag**, Source Id : **Tag-1**, Destination Type : **vpn**, Destination Id : **1**

Source Type	Source ID	Destination Type	Destination ID	Tunnel Id	Source Region	Destination Region
vpc	16824030038717225	vpn	1	C8K-5C361203-73F5-0E7E-3AC...	global	us-west1
vpc	1521588190381994061	vpn	1	C8K-5C361203-73F5-0E7E-3AC...	global	us-west1
vpc	16824030038717225	vpn	1	C8K-43F20049-6559-EB5C-9EF...	global	us-west1
vpc	1521588190381994061	vpn	1	C8K-43F20049-6559-EB5C-9EF...	global	us-west1

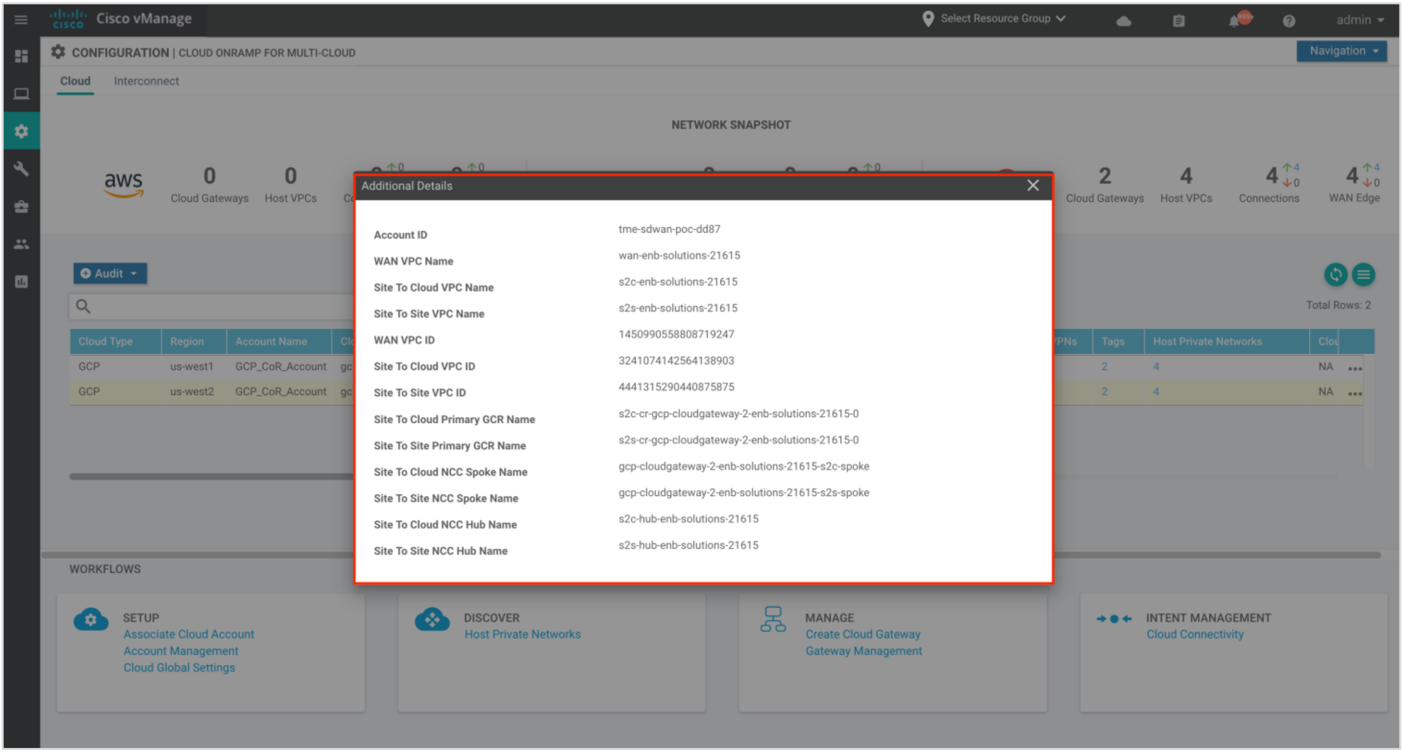
Step 4. To view Google cloud resources deployed through this workflow, select **Additional Details**.

© 2020 Cisco and/or its affiliates. All rights reserved.



unnel to Transit Gateway	VPNs	Tags	Host Private Networks	Cloud Provider Management Reference	Last Mapping Result	Connectivity State Last Update Time		
2 reachable	1	2	4	NA	Successful	03 May 2021 3:34:17 PM PDT	--	•••
2 reachable	1	2	4	NA	Successful	03 May 2021 3:34:17 PM PDT	--	•••

The pop-up window lists out all the google resources deployed through the site to cloud and site to site VPC workflow.



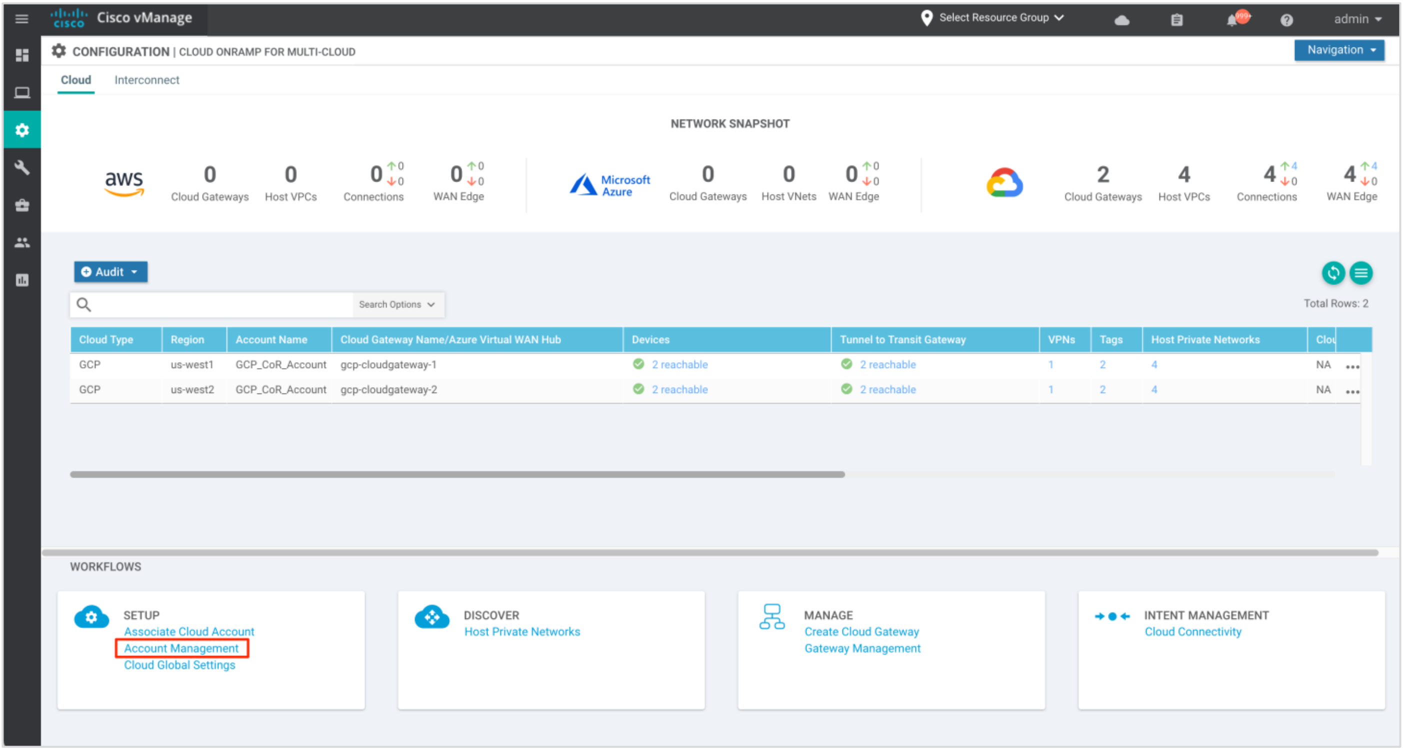
Additional Details

Account ID	tme-sdwan-poc-dd87
WAN VPC Name	wan-enb-solutions-21615
Site To Cloud VPC Name	s2c-enb-solutions-21615
Site To Site VPC Name	s2s-enb-solutions-21615
WAN VPC ID	1450990558808719247
Site To Cloud VPC ID	3241074142564138903
Site To Site VPC ID	4441315290440875875
Site To Cloud Primary GCR Name	s2c-cr-gcp-cloudgateway-2-enb-solutions-21615-0
Site To Site Primary GCR Name	s2s-cr-gcp-cloudgateway-2-enb-solutions-21615-0
Site To Cloud NCC Spoke Name	gcp-cloudgateway-2-enb-solutions-21615-s2c-spoke
Site To Site NCC Spoke Name	gcp-cloudgateway-2-enb-solutions-21615-s2s-spoke
Site To Cloud NCC Hub Name	s2c-hub-enb-solutions-21615
Site To Site NCC Hub Name	s2s-hub-enb-solutions-21615

© 2020 Cisco and/or its affiliates. All rights reserved.

Procedure 3: Manage Google Billing ID and Credentials

Step 1. To view, manage and update the Billing ID and credentials, click **Account Management** under the section **Setup.**



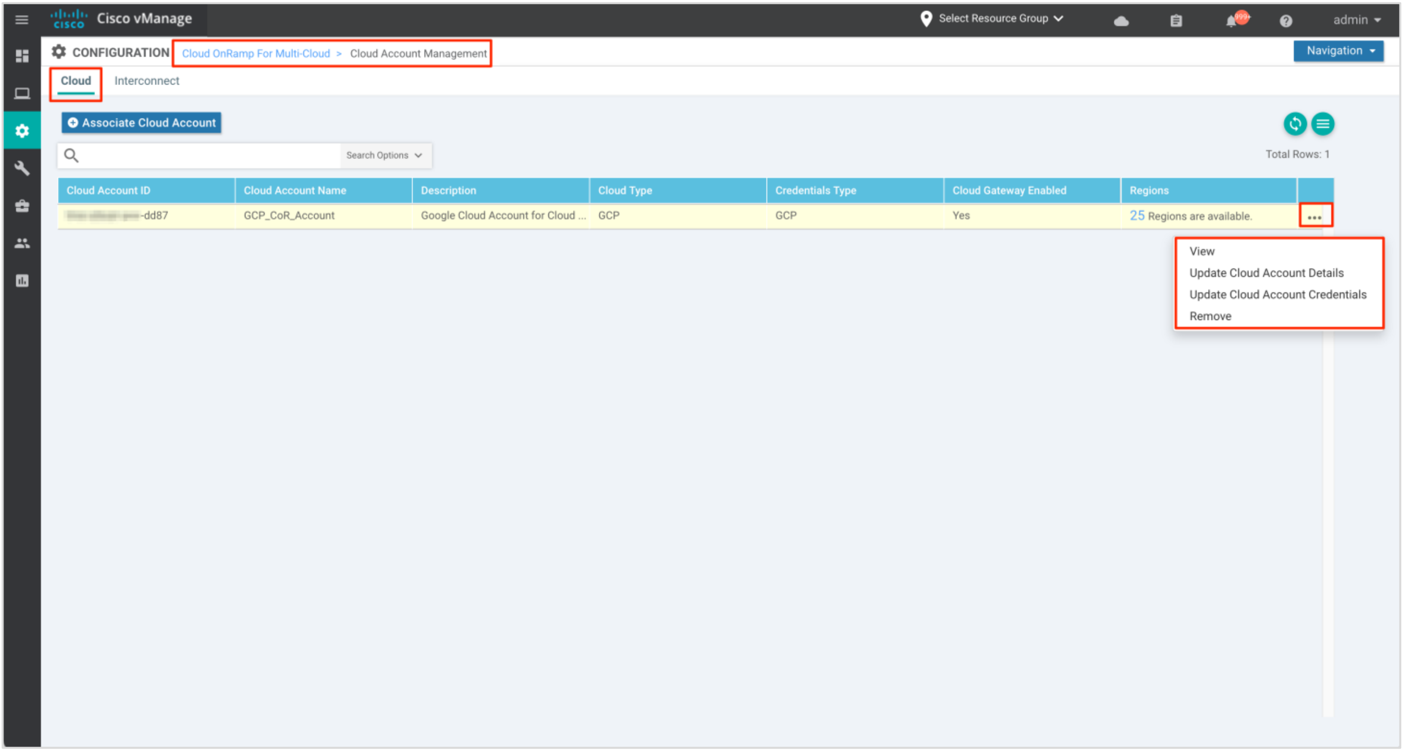
Cloud Type	Region	Account Name	Cloud Gateway Name/Azure Virtual WAN Hub	Devices	Tunnel to Transit Gateway	VPNs	Tags	Host Private Networks	Clou
GCP	us-west1	GCP_CoR_Account	gcp-cloudgateway-1	✓ 2 reachable	✓ 2 reachable	1	2	4	NA •••
GCP	us-west2	GCP_CoR_Account	gcp-cloudgateway-2	✓ 2 reachable	✓ 2 reachable	1	2	4	NA •••

Step 2. Under the section **Cloud**, the Google cloud account details associated with your vManage NMS are listed. To manage the cloud account details, click on the three dots **(…)** located on the right corner.

Select:

- View to manage all the cloud account details.
- Update Cloud Account Details to edit the Billing ID details.
- Update Cloud Account Credentials to update the credentials associated with vManage.
- Remove to delete the Account Details.

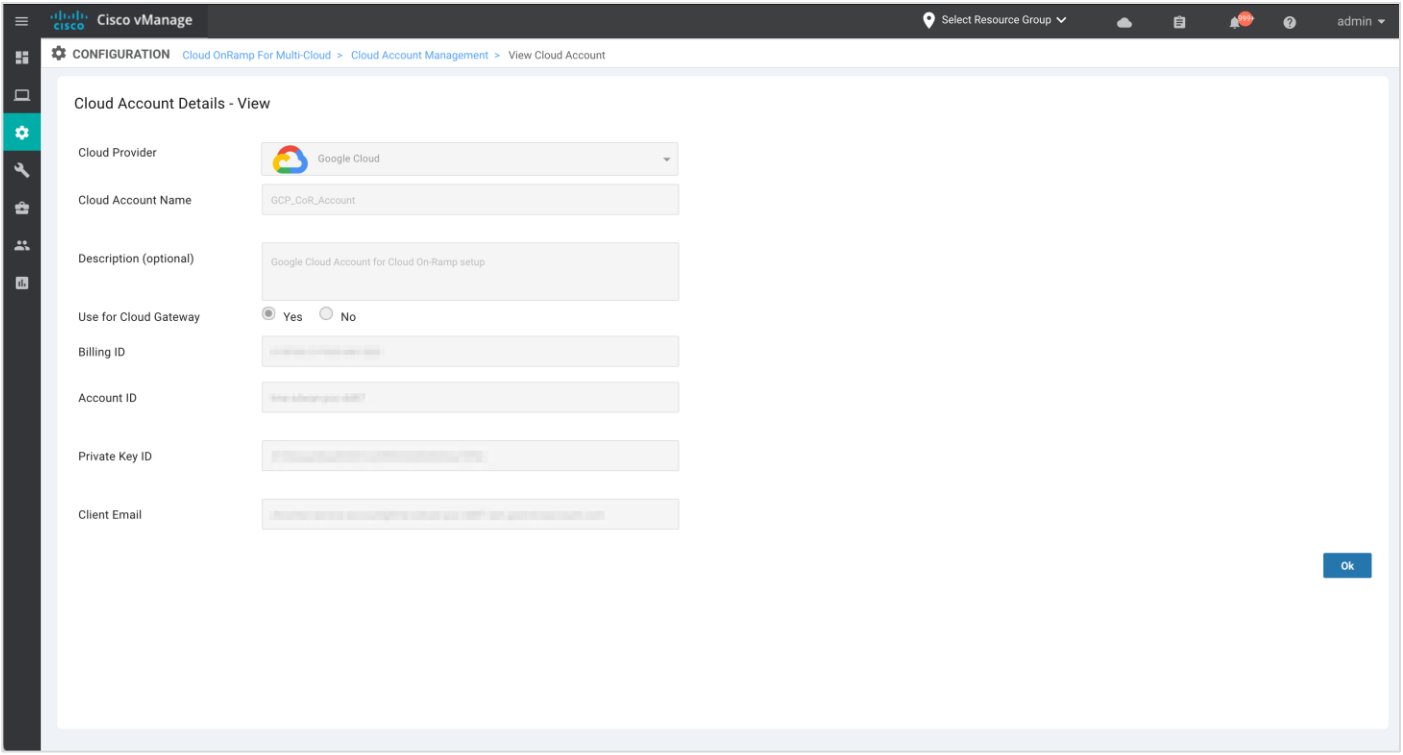
© 2020 Cisco and/or its affiliates. All rights reserved.



Cloud Account ID	Cloud Account Name	Description	Cloud Type	Credentials Type	Cloud Gateway Enabled	Regions	
[redacted]-dd87	GCP_CoR_Account	Google Cloud Account for Cloud ...	GCP	GCP	Yes	25 Regions are available.	...

View
Update Cloud Account Details
Update Cloud Account Credentials
Remove

The example screenshot displays all the entered Cloud Account Details, located under **Cloud onRamp for Multi-Cloud** > **Cloud Account Management** > **View Cloud Account**.


Cisco vManage
Select Resource Group
admin
CONFIGURATION
Cloud OnRamp For Multi-Cloud > Cloud Account Management > View Cloud Account

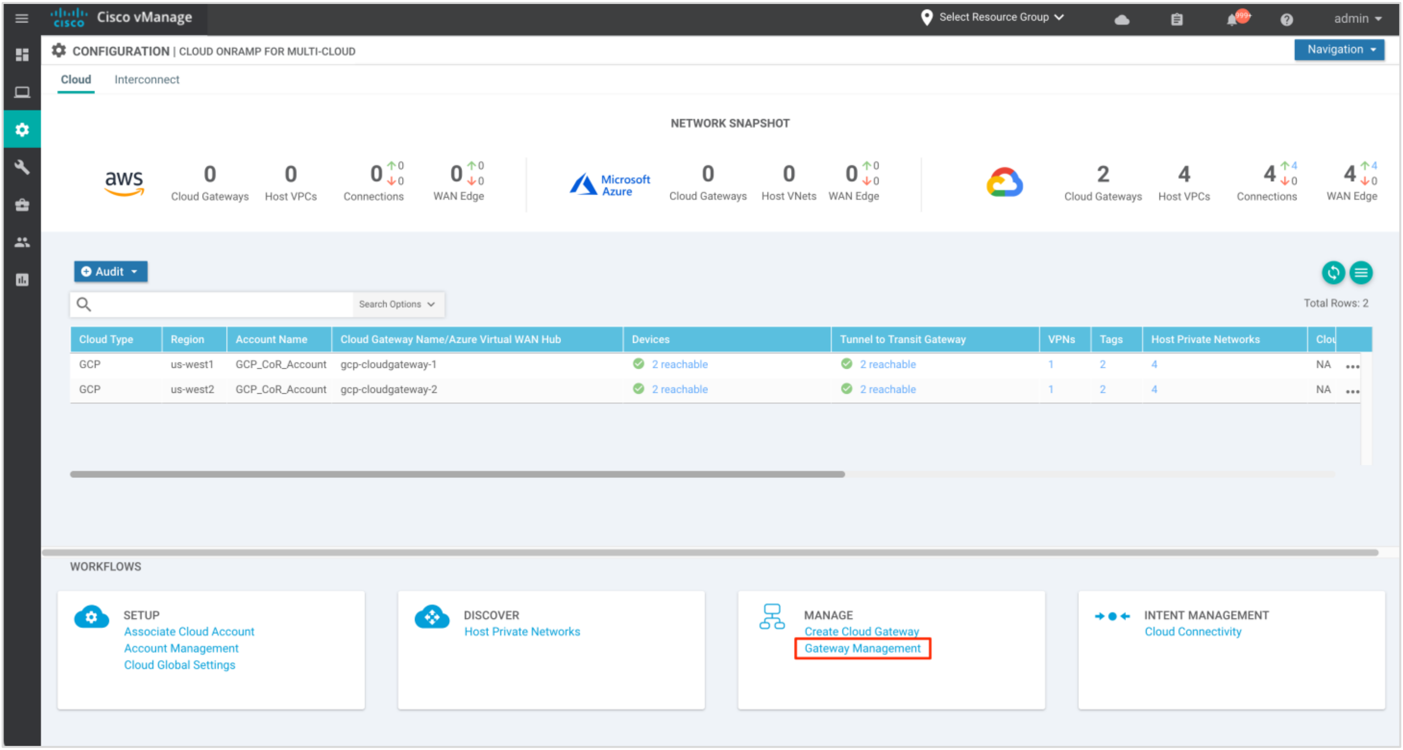
Cloud Account Details - View

Cloud Provider	Google Cloud
Cloud Account Name	GCP_CoR_Account
Description (optional)	Google Cloud Account for Cloud On-Ramp setup
Use for Cloud Gateway	● Yes ○ No
Billing ID	[redacted]
Account ID	[redacted]
Private Key ID	[redacted]
Client Email	[redacted]

Procedure 3: Manage Cloud Global Settings

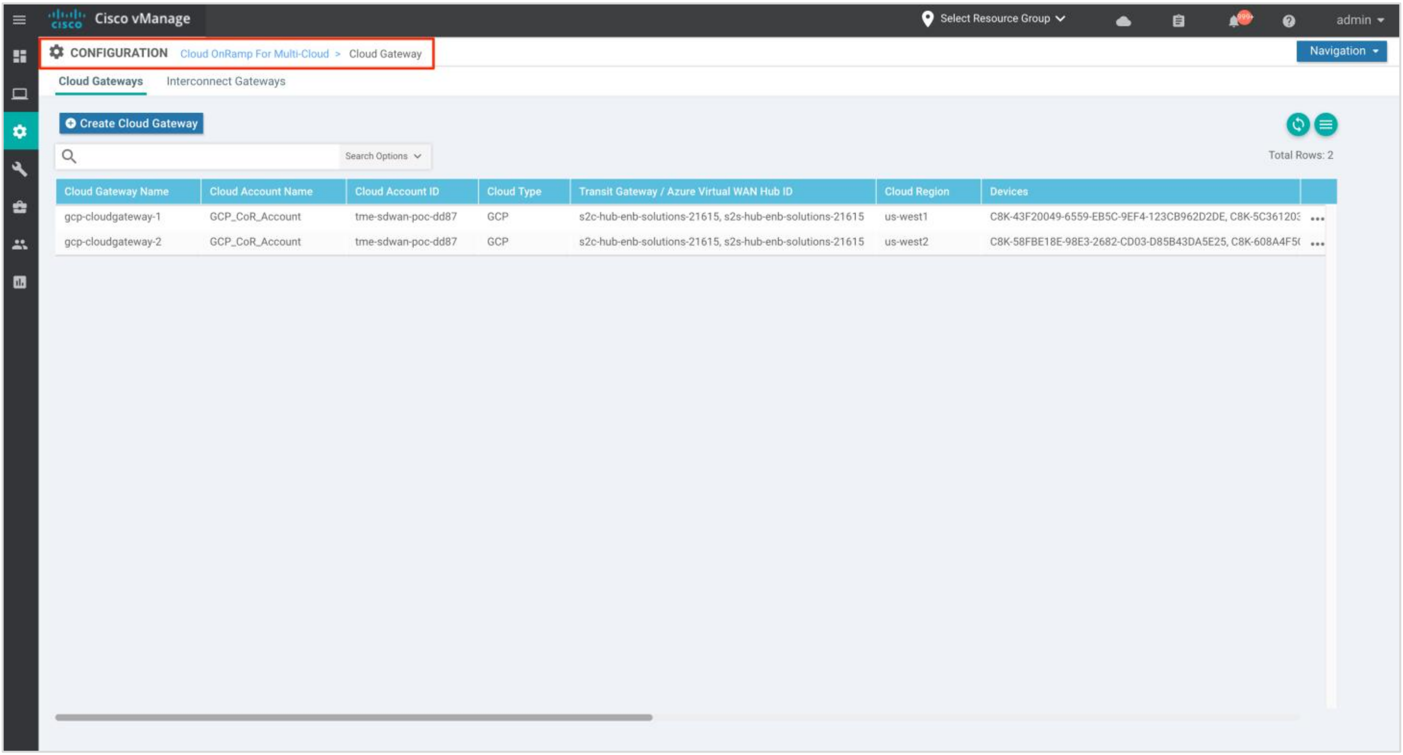
Step 1. To view or delete the Global Cloud Gateway settings. Under **Manage**, click on **Gateway Management**.

© 2020 Cisco and/or its affiliates. All rights reserved.



Cloud Type	Region	Account Name	Cloud Gateway Name/Azure Virtual WAN Hub	Devices	Tunnel to Transit Gateway	VPNs	Tags	Host Private Networks	Clou	
GCP	us-west1	GCP_CoR_Account	gcp-cloudgateway-1	✓ 2 reachable	✓ 2 reachable	1	2	4	NA	...
GCP	us-west2	GCP_CoR_Account	gcp-cloudgateway-2	✓ 2 reachable	✓ 2 reachable	1	2	4	NA	...

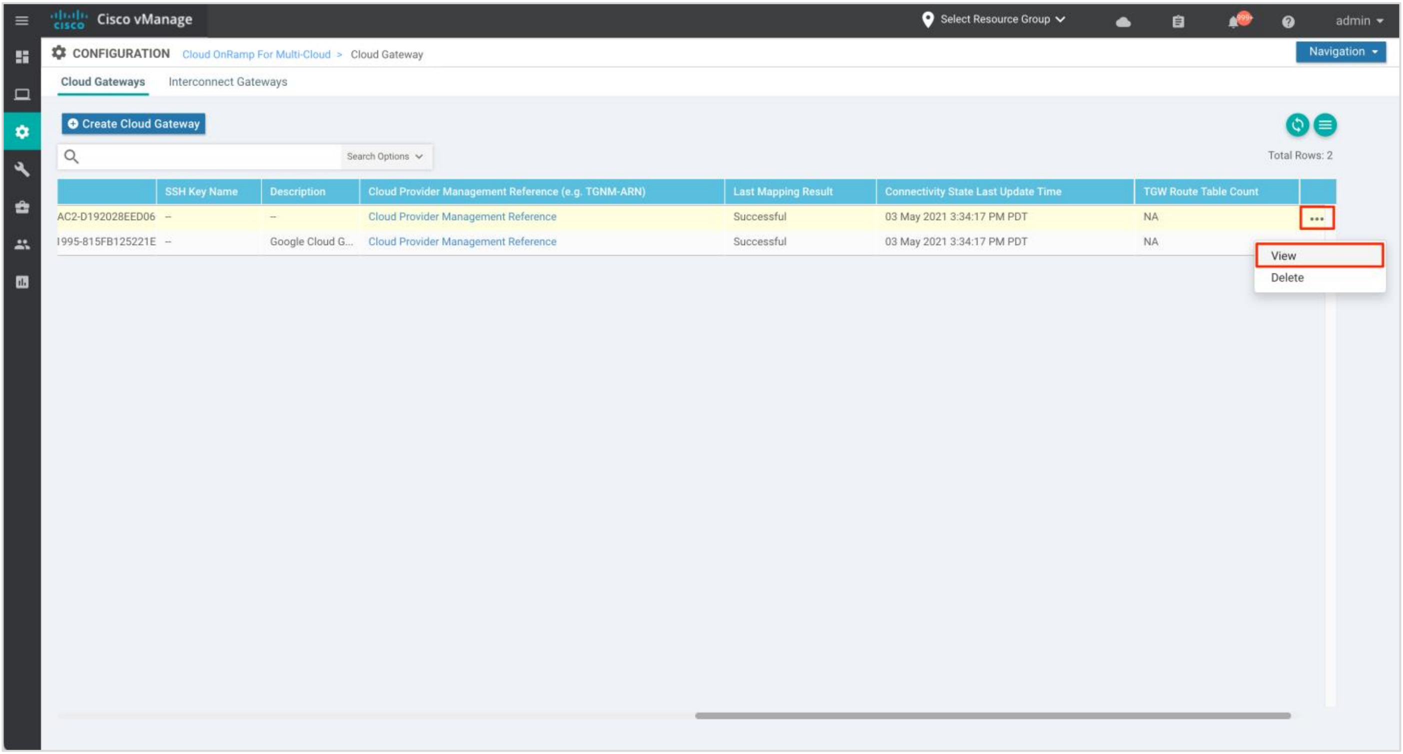
The example screenshot below displays two cloud gateways created through the workflow.



Cloud Gateway Name	Cloud Account Name	Cloud Account ID	Cloud Type	Transit Gateway / Azure Virtual WAN Hub ID	Cloud Region	Devices	
gcp-cloudgateway-1	GCP_CoR_Account	tme-sdwan-poc-dd87	GCP	s2c-hub-enb-solutions-21615, s2s-hub-enb-solutions-21615	us-west1	C8K-43F20049-6559-EB5C-9EF4-123CB962D2DE, C8K-5C36120	...
gcp-cloudgateway-2	GCP_CoR_Account	tme-sdwan-poc-dd87	GCP	s2c-hub-enb-solutions-21615, s2s-hub-enb-solutions-21615	us-west2	C8K-58FBE18E-98E3-2682-CD03-D85B43DA5E25, C8K-608A4F5	...

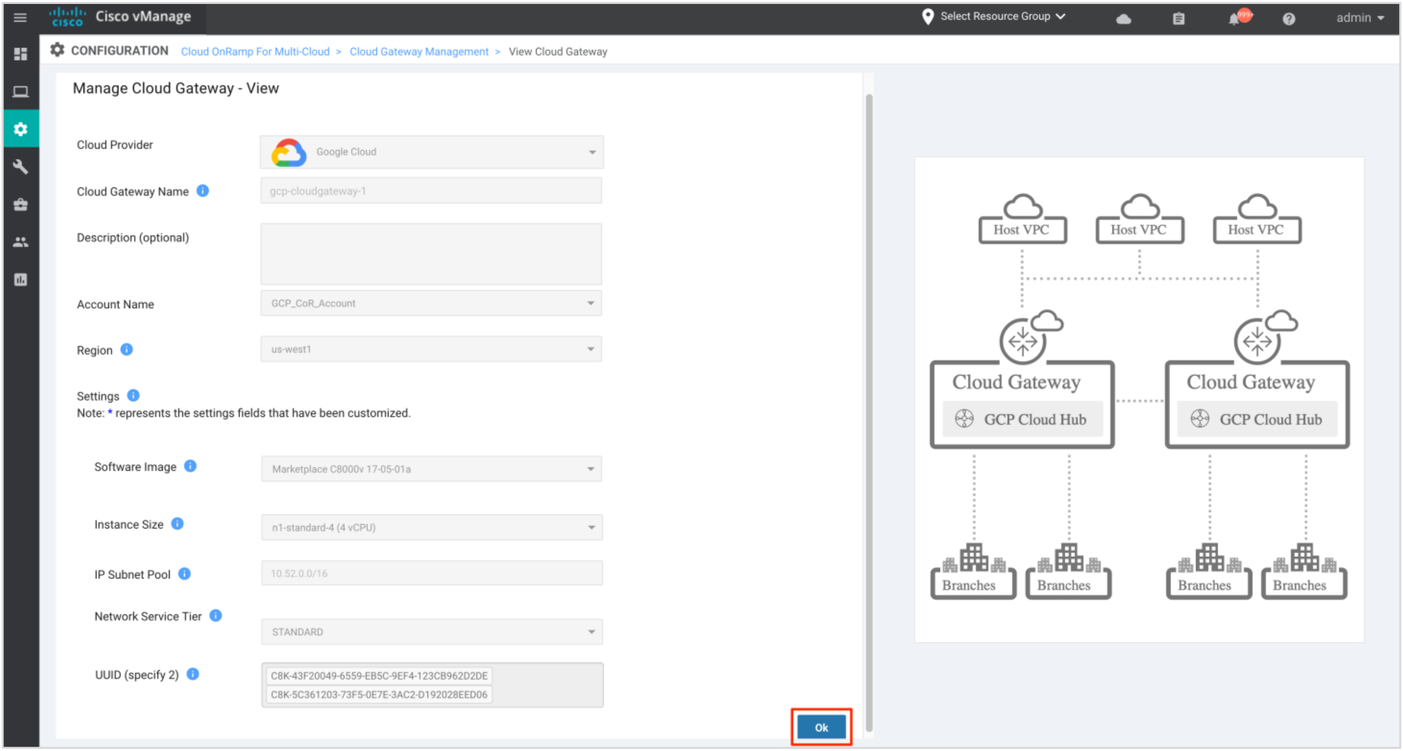
Click on the three dots **(...)** on the right to **View** or **Delete** the cloud gateways.

© 2020 Cisco and/or its affiliates. All rights reserved.



	SSH Key Name	Description	Cloud Provider Management Reference (e.g. TGNM-ARN)	Last Mapping Result	Connectivity State Last Update Time	TGW Route Table Count	
AC2-D192028EED06	--	--	Cloud Provider Management Reference	Successful	03 May 2021 3:34:17 PM PDT	NA	•••
1995-815FB125221E	--	Google Cloud G...	Cloud Provider Management Reference	Successful	03 May 2021 3:34:17 PM PDT	NA	

The example screenshot below displays the details entered within the cloud gateway.



Manage Cloud Gateway - View

Cloud Provider	Google Cloud
Cloud Gateway Name	gcp-cloudgateway-1
Description (optional)	
Account Name	GCP_CoR_Account
Region	us-west1

Settings

Note: * represents the settings fields that have been customized.

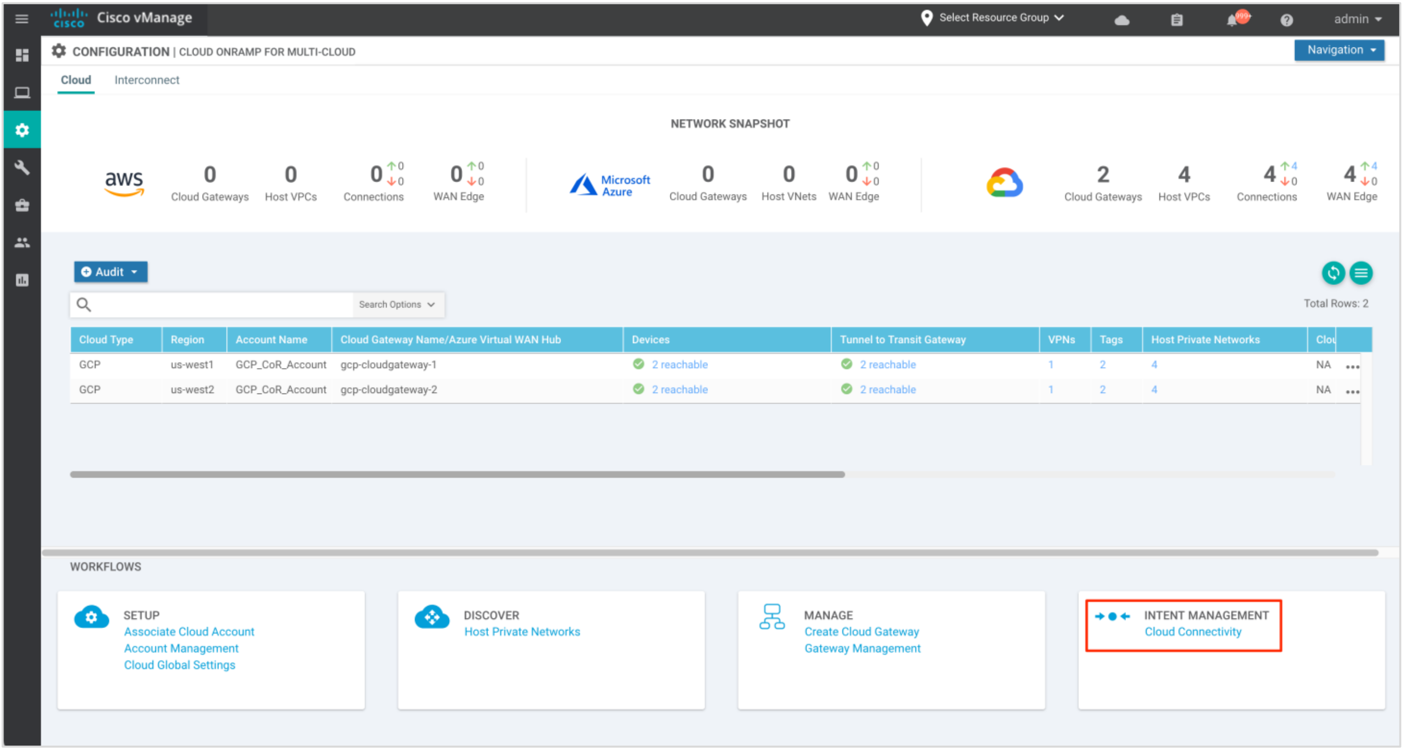
Software Image	Marketplace C8000v 17-05-01a
Instance Size	n1-standard-4 (4 vCPU)
IP Subnet Pool	10.52.0.0/16
Network Service Tier	STANDARD
UUID (specify 2)	C8K-43F20049-6559-EB5C-9EF4-123CB962D2DE C8K-5C361203-73F5-0E7E-3AC2-D192028EED06

Procedure 3: Manage VPN to Tag Mapping

To edit or monitor an existing mapping between your service side VPN and a tag follow the steps below

© 2020 Cisco and/or its affiliates. All rights reserved.

Step 1. Under **Intent Management**, click **Cloud Connectivity** to view and/ or edit the mapping of the host VPCs in Tags to VPN.



CONFIGURATION | CLOUD ONRAMP FOR MULTI-CLOUD

Cloud Interconnect

NETWORK SNAPSHOT

aws: 0 Cloud Gateways, 0 Host VPCs, 0 Connections (↑0 ↓0), 0 WAN Edge (↑0 ↓0)

Microsoft Azure: 0 Cloud Gateways, 0 Host VNets, 0 WAN Edge (↑0 ↓0)

Google Cloud: 2 Cloud Gateways, 4 Host VPCs, 4 Connections (↑4 ↓0), 4 WAN Edge (↑4 ↓0)

Total Rows: 2

Cloud Type	Region	Account Name	Cloud Gateway Name/Azure Virtual WAN Hub	Devices	Tunnel to Transit Gateway	VPNs	Tags	Host Private Networks	Clou
GCP	us-west1	GCP_CoR_Account	gcp-cloudgateway-1	2 reachable	2 reachable	1	2	4	NA
GCP	us-west2	GCP_CoR_Account	gcp-cloudgateway-2	2 reachable	2 reachable	1	2	4	NA

WORKFLOWS

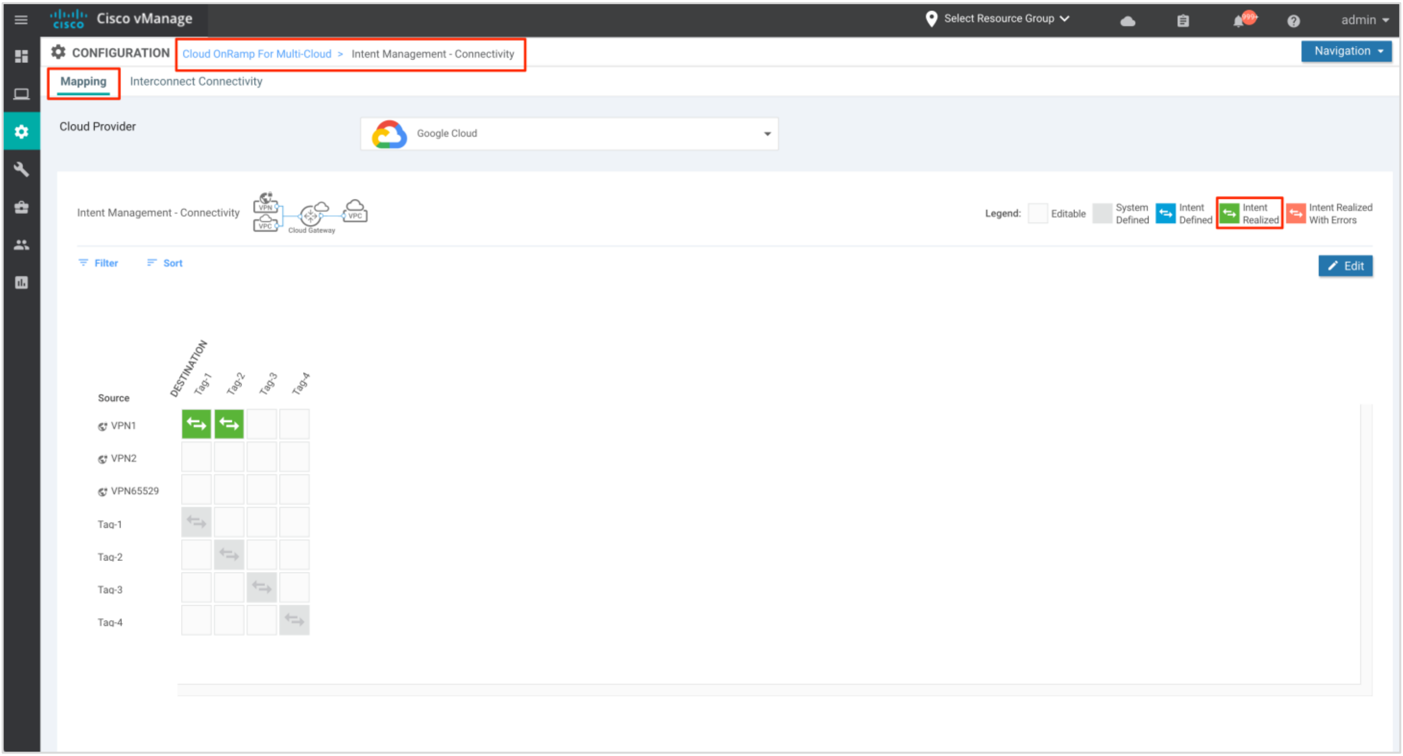
SETUP
Associate Cloud Account
Account Management
Cloud Global Settings

DISCOVER
Host Private Networks

MANAGE
Create Cloud Gateway
Gateway Management

INTENT MANAGEMENT
Cloud Connectivity

Step 2. To associate additional tags that contain host VPCs to VPN, click **Edit** located on the right.



CONFIGURATION Cloud OnRamp For Multi-Cloud > Intent Management - Connectivity

Mapping Interconnect Connectivity

Cloud Provider: Google Cloud

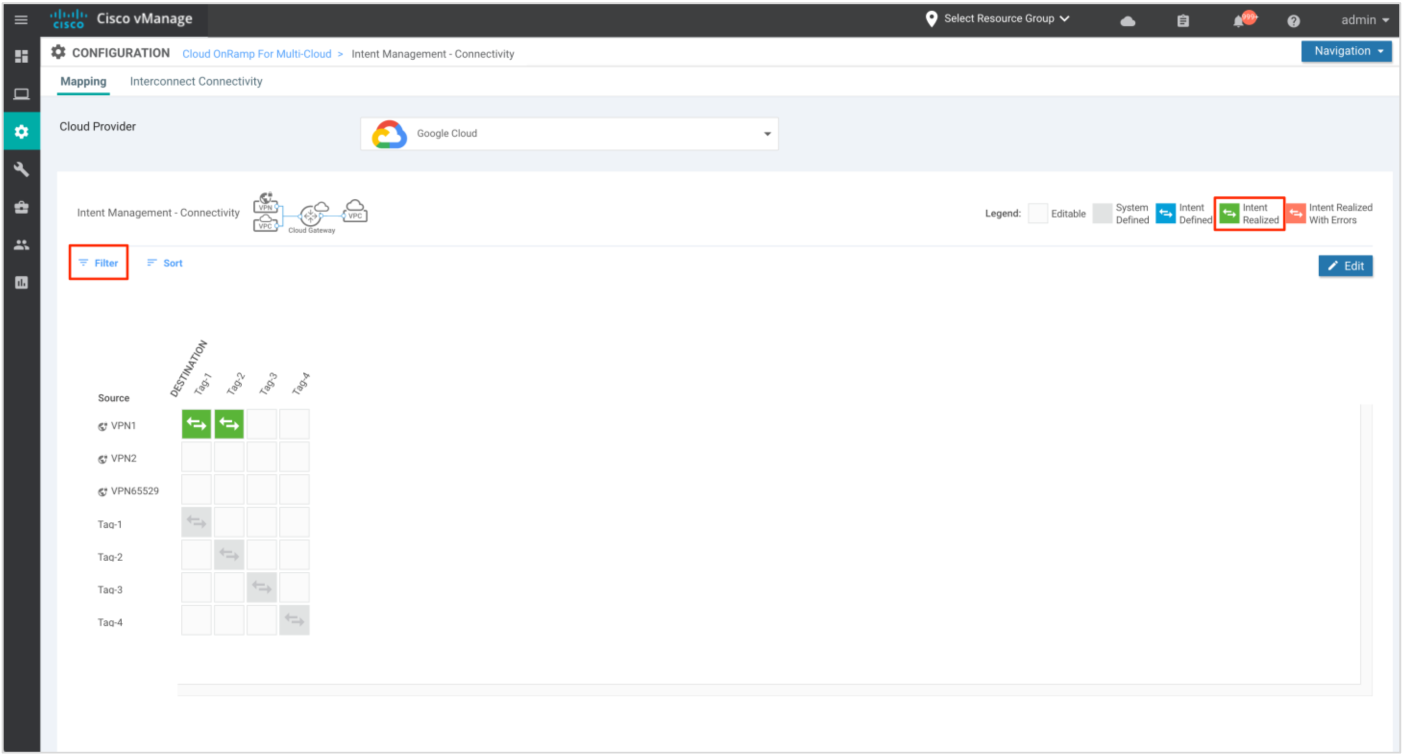
Intent Management - Connectivity

Legend: □ Editable ▨ System Defined 🟦 Intent Defined 🟩 Intent Realized 🟥 Intent Realized With Errors

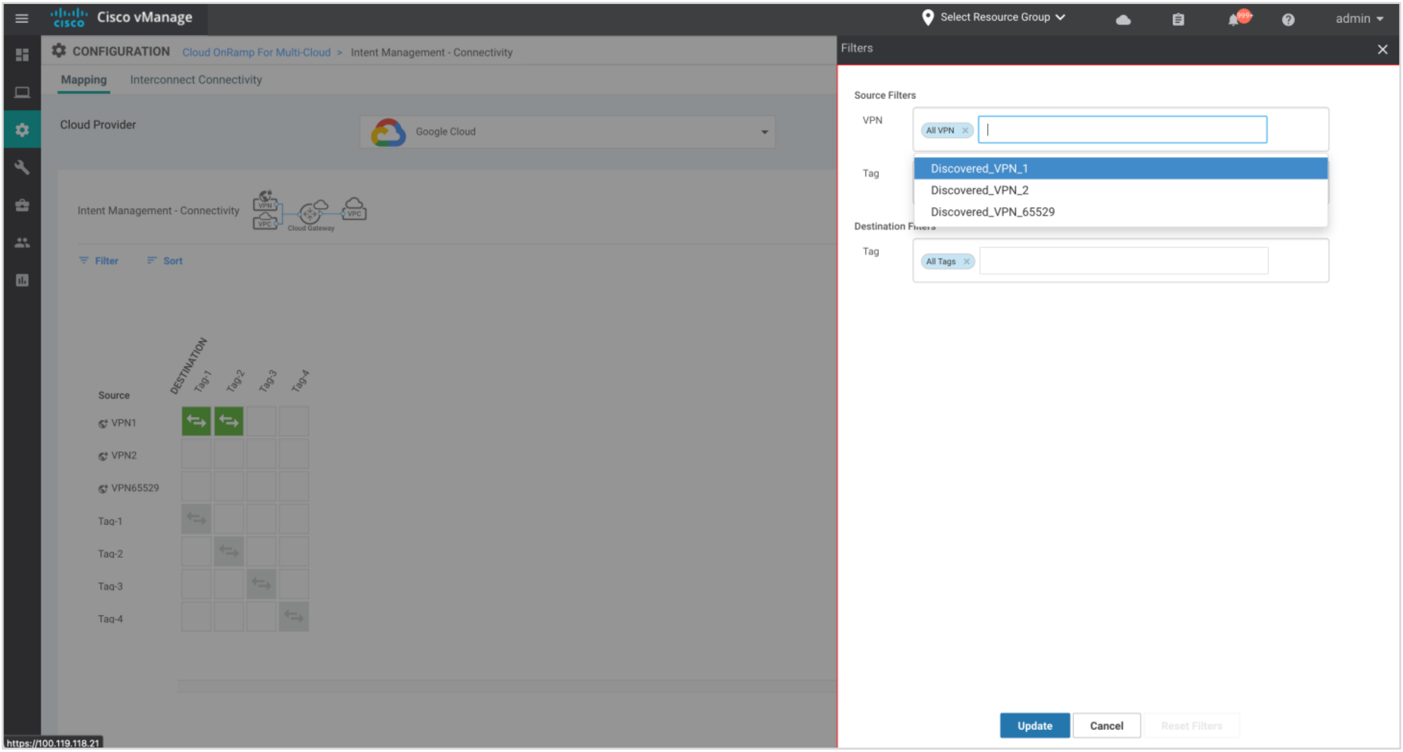
Source \ DESTINATION	Tag-1	Tag-2	Tag-3	Tag-4
VPN1	🟩	🟩		
VPN2				
VPN65529				
Tag-1	▨			
Tag-2		▨		
Tag-3			▨	
Tag-4				▨

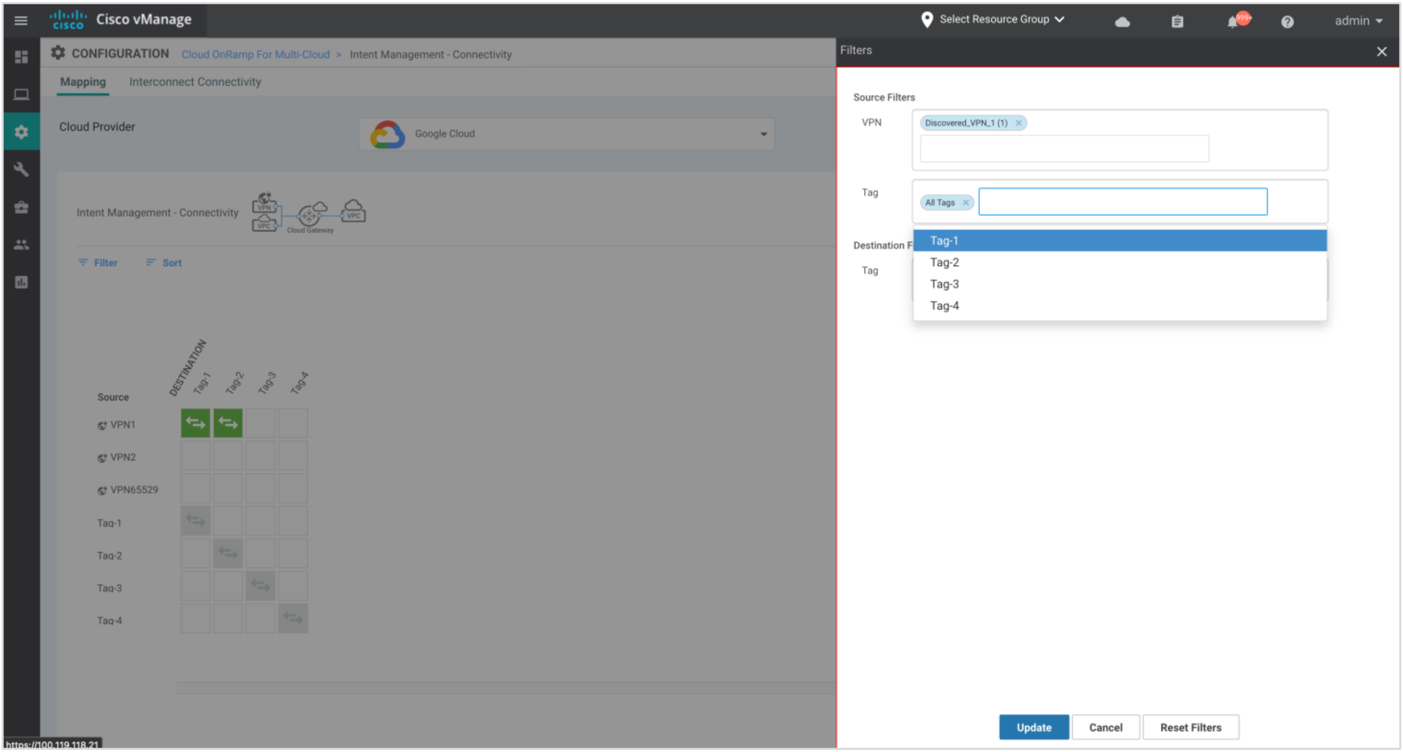
Step 3. Click **Filter** to view the mapping based on a certain source VPN/ Tag and destination Tag.

© 2020 Cisco and/or its affiliates. All rights reserved.



The example screenshots below display the mapping for source VPN 1 and Tag1 mapping.





Cloud Provider: Google Cloud

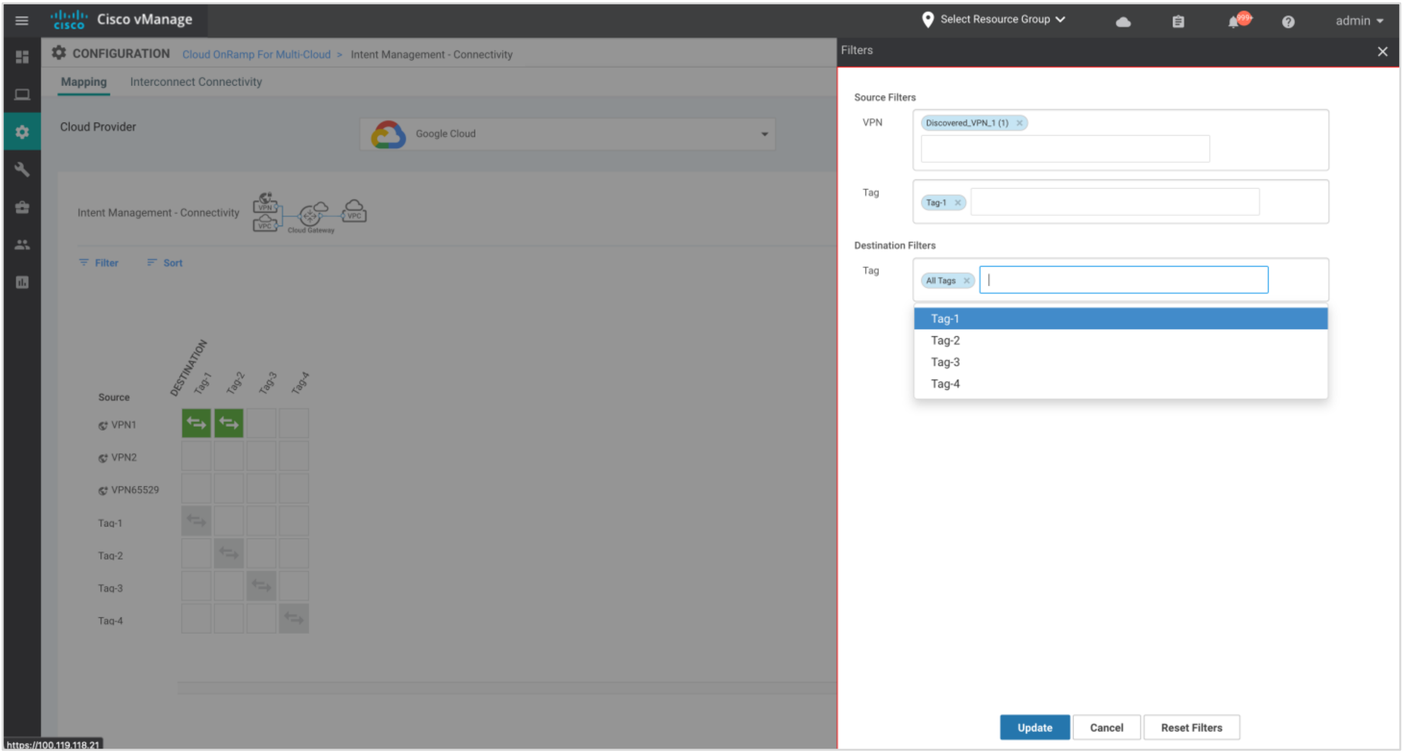
Source Filters

VPN: Discovered_VPN_1 (1)

Tag: All Tags

Destination F

Tag



Cloud Provider: Google Cloud

Source Filters

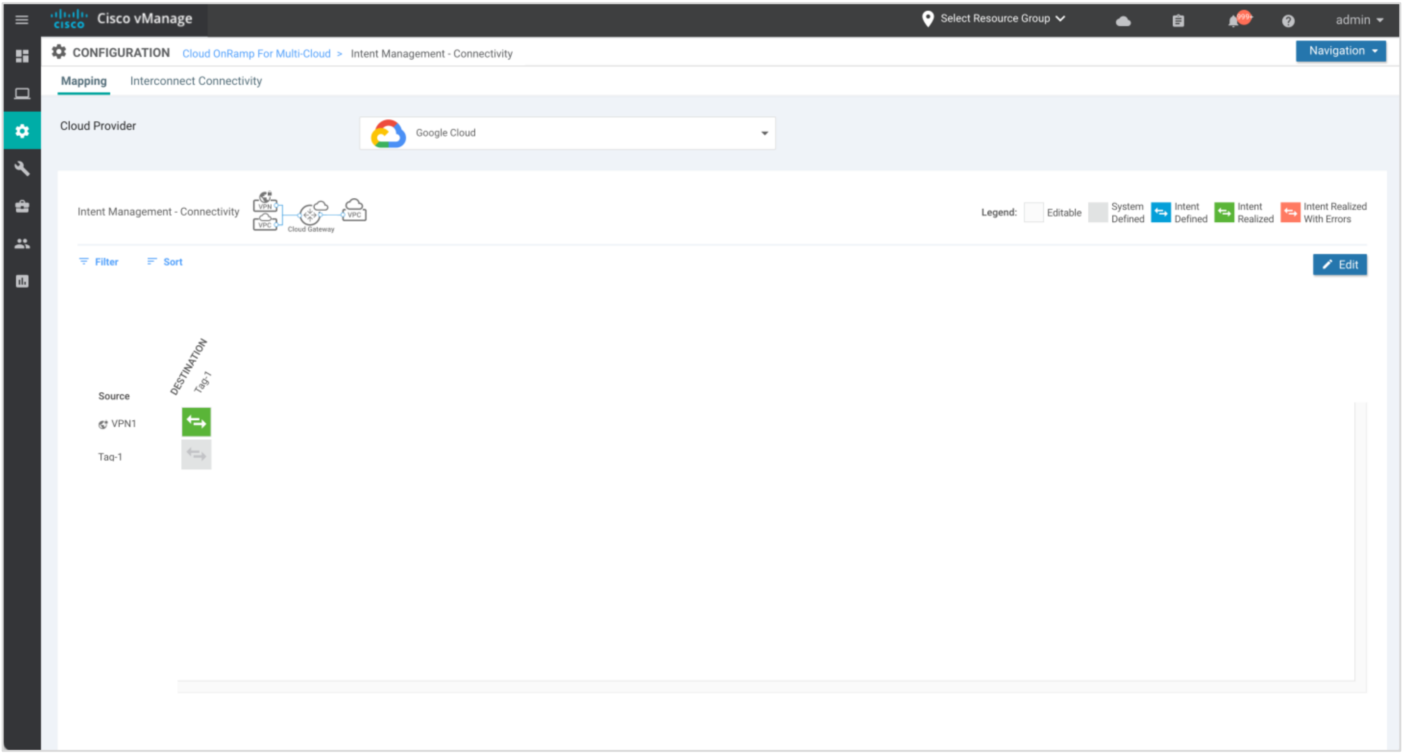
VPN: Discovered_VPN_1 (1)

Tag: Tag-1

Destination Filters

Tag: All Tags

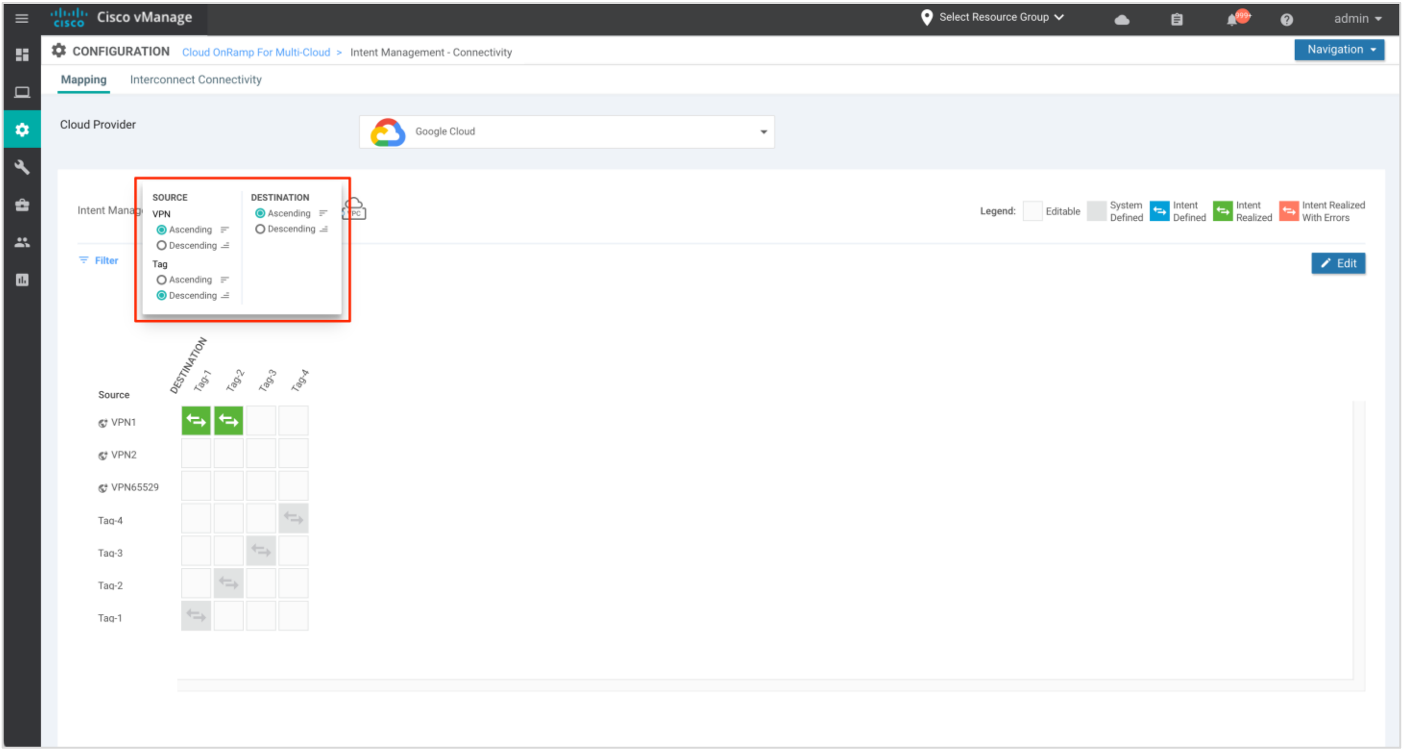
© 2020 Cisco and/or its affiliates. All rights reserved.



Cloud Provider: Google Cloud

Source	Tag-1
VPN1	🟩
Tag-1	▨

Step 4. You can also click on **Sort** to further filter/ arrange the view.



Cloud Provider: Google Cloud

SOURCE
VPN
● Ascending
○ Descending
Tag
○ Ascending
● Descending

DESTINATION
● Ascending
○ Descending

Source	Tag-1	Tag-2	Tag-3	Tag-4
VPN1	🟩	🟩		
VPN2				
VPN65529				
Tag-4				▨
Tag-3			▨	
Tag-2		▨		
Tag-1	▨			

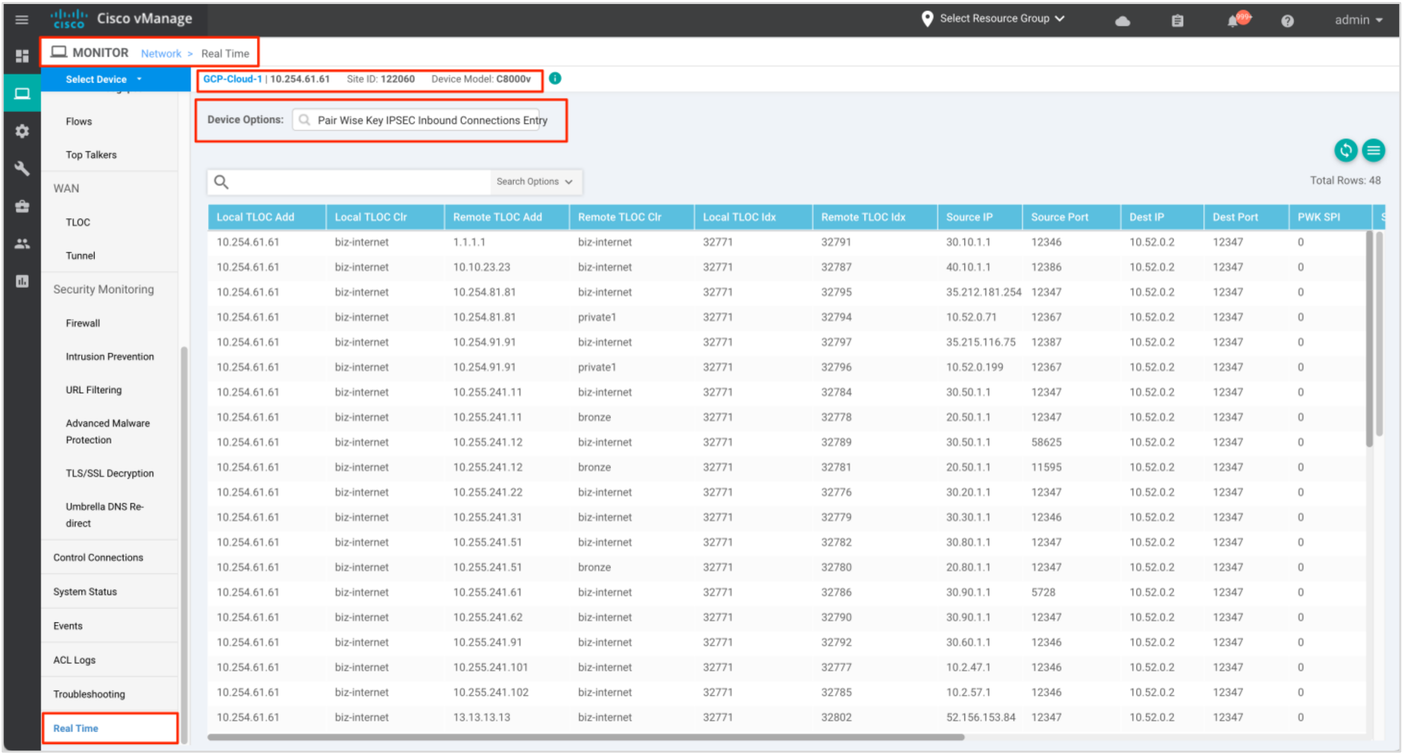
© 2020 Cisco and/or its affiliates. All rights reserved.

Process 2: vManage Monitor Dashboard

Procedure 1: Monitor SD-WAN devices via Monitor tab

Step 1. To monitor both your controllers and WAN Edge devices within the Transit VPC, Navigate to **Monitor** > **Real Time**. The **Device Options** tab lists outputs like logs gathered from the show output.

Some example outputs are added below:

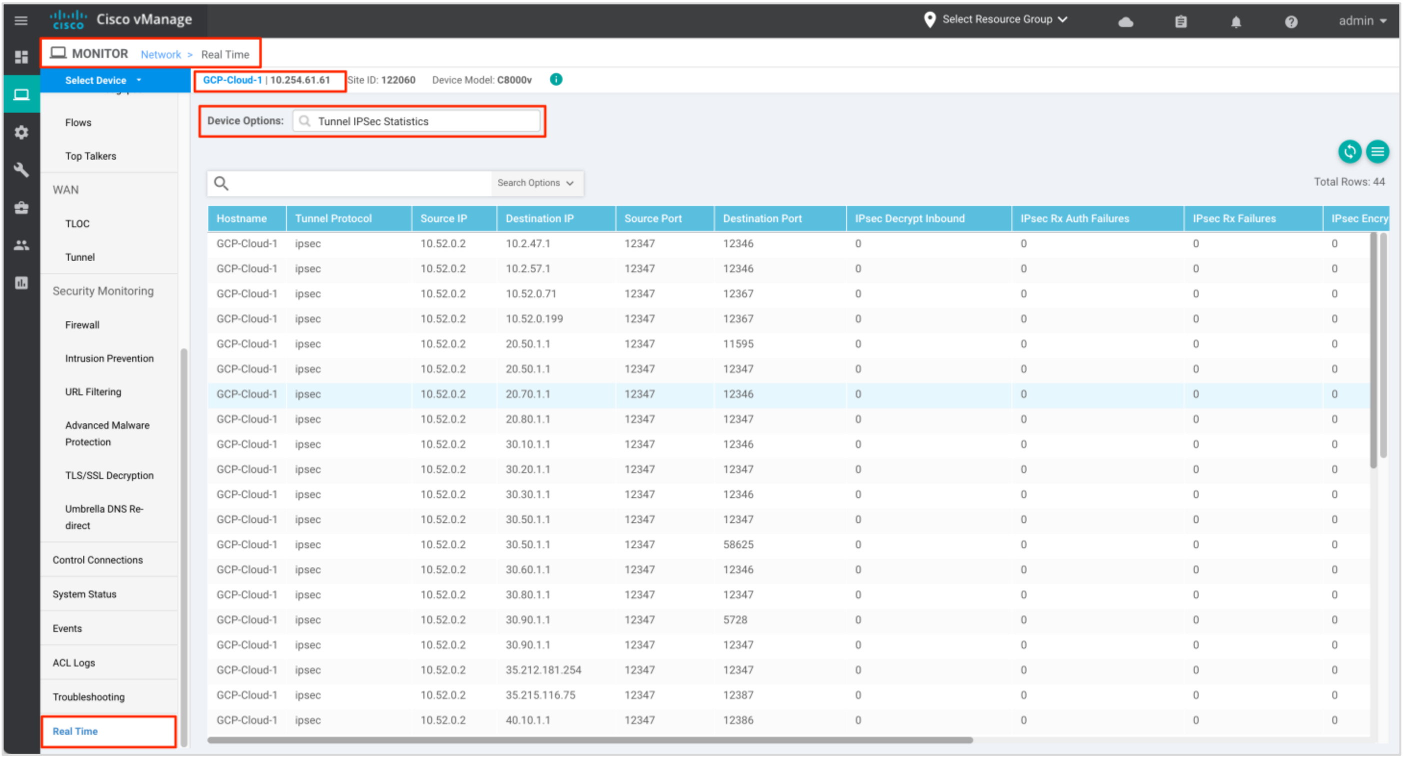


GCP-Cloud-1 | 10.254.61.61 Site ID: 122060 Device Model: C8000v

Device Options: Pair Wise Key IPSEC Inbound Connections Entry

Total Rows: 48

Local TLOC Add	Local TLOC Clr	Remote TLOC Add	Remote TLOC Clr	Local TLOC Idx	Remote TLOC Idx	Source IP	Source Port	Dest IP	Dest Port	PWK SPI
10.254.61.61	biz-internet	1.1.1.1	biz-internet	32771	32791	30.10.1.1	12346	10.52.0.2	12347	0
10.254.61.61	biz-internet	10.10.23.23	biz-internet	32771	32787	40.10.1.1	12386	10.52.0.2	12347	0
10.254.61.61	biz-internet	10.254.81.81	biz-internet	32771	32795	35.212.181.254	12347	10.52.0.2	12347	0
10.254.61.61	biz-internet	10.254.81.81	private1	32771	32794	10.52.0.71	12367	10.52.0.2	12347	0
10.254.61.61	biz-internet	10.254.91.91	biz-internet	32771	32797	35.215.116.75	12387	10.52.0.2	12347	0
10.254.61.61	biz-internet	10.254.91.91	private1	32771	32796	10.52.0.199	12367	10.52.0.2	12347	0
10.254.61.61	biz-internet	10.255.241.11	biz-internet	32771	32784	30.50.1.1	12347	10.52.0.2	12347	0
10.254.61.61	biz-internet	10.255.241.11	bronze	32771	32778	20.50.1.1	12347	10.52.0.2	12347	0
10.254.61.61	biz-internet	10.255.241.12	biz-internet	32771	32789	30.50.1.1	58625	10.52.0.2	12347	0
10.254.61.61	biz-internet	10.255.241.12	bronze	32771	32781	20.50.1.1	11595	10.52.0.2	12347	0
10.254.61.61	biz-internet	10.255.241.22	biz-internet	32771	32776	30.20.1.1	12347	10.52.0.2	12347	0
10.254.61.61	biz-internet	10.255.241.31	biz-internet	32771	32779	30.30.1.1	12346	10.52.0.2	12347	0
10.254.61.61	biz-internet	10.255.241.51	biz-internet	32771	32782	30.80.1.1	12347	10.52.0.2	12347	0
10.254.61.61	biz-internet	10.255.241.51	bronze	32771	32780	20.80.1.1	12347	10.52.0.2	12347	0
10.254.61.61	biz-internet	10.255.241.61	biz-internet	32771	32786	30.90.1.1	5728	10.52.0.2	12347	0
10.254.61.61	biz-internet	10.255.241.62	biz-internet	32771	32790	30.90.1.1	12347	10.52.0.2	12347	0
10.254.61.61	biz-internet	10.255.241.91	biz-internet	32771	32792	30.60.1.1	12346	10.52.0.2	12347	0
10.254.61.61	biz-internet	10.255.241.101	biz-internet	32771	32777	10.2.47.1	12346	10.52.0.2	12347	0
10.254.61.61	biz-internet	10.255.241.102	biz-internet	32771	32785	10.2.57.1	12346	10.52.0.2	12347	0
10.254.61.61	biz-internet	13.13.13.13	biz-internet	32771	32802	52.156.153.84	12347	10.52.0.2	12347	0



GCP-Cloud-1 | 10.254.61.61 Site ID: 122060 Device Model: C8000v

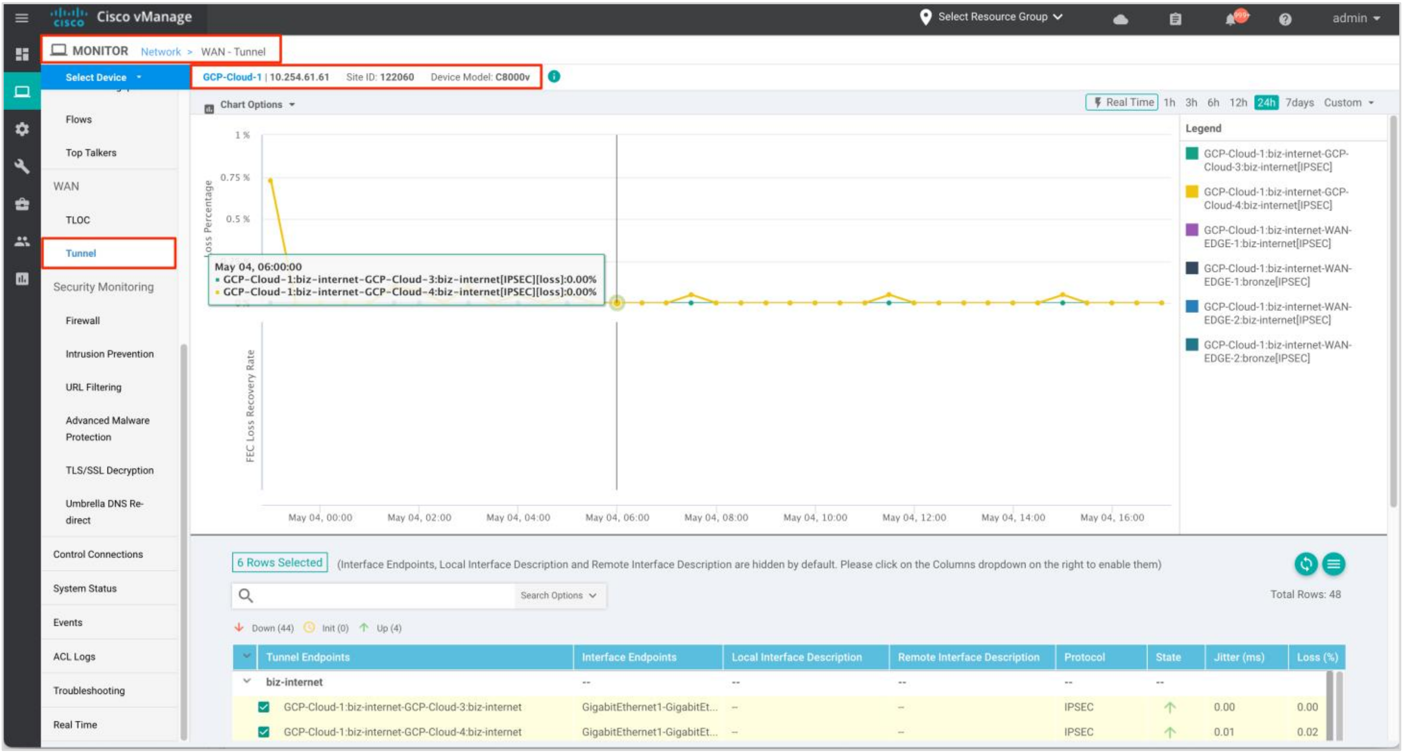
Device Options: Tunnel IPSec Statistics

Total Rows: 44

Hostname	Tunnel Protocol	Source IP	Destination IP	Source Port	Destination Port	IPsec Decrypt Inbound	IPsec Rx Auth Failures	IPsec Rx Failures	IPsec Encry
GCP-Cloud-1	ipsec	10.52.0.2	10.2.47.1	12347	12346	0	0	0	0
GCP-Cloud-1	ipsec	10.52.0.2	10.2.57.1	12347	12346	0	0	0	0
GCP-Cloud-1	ipsec	10.52.0.2	10.52.0.71	12347	12367	0	0	0	0
GCP-Cloud-1	ipsec	10.52.0.2	10.52.0.199	12347	12367	0	0	0	0
GCP-Cloud-1	ipsec	10.52.0.2	20.50.1.1	12347	11595	0	0	0	0
GCP-Cloud-1	ipsec	10.52.0.2	20.50.1.1	12347	12347	0	0	0	0
GCP-Cloud-1	ipsec	10.52.0.2	20.70.1.1	12347	12346	0	0	0	0
GCP-Cloud-1	ipsec	10.52.0.2	20.80.1.1	12347	12347	0	0	0	0
GCP-Cloud-1	ipsec	10.52.0.2	30.10.1.1	12347	12346	0	0	0	0
GCP-Cloud-1	ipsec	10.52.0.2	30.20.1.1	12347	12347	0	0	0	0
GCP-Cloud-1	ipsec	10.52.0.2	30.30.1.1	12347	12346	0	0	0	0
GCP-Cloud-1	ipsec	10.52.0.2	30.50.1.1	12347	12347	0	0	0	0
GCP-Cloud-1	ipsec	10.52.0.2	30.50.1.1	12347	58625	0	0	0	0
GCP-Cloud-1	ipsec	10.52.0.2	30.60.1.1	12347	12346	0	0	0	0
GCP-Cloud-1	ipsec	10.52.0.2	30.80.1.1	12347	12347	0	0	0	0
GCP-Cloud-1	ipsec	10.52.0.2	30.90.1.1	12347	5728	0	0	0	0
GCP-Cloud-1	ipsec	10.52.0.2	30.90.1.1	12347	12347	0	0	0	0
GCP-Cloud-1	ipsec	10.52.0.2	35.212.181.254	12347	12347	0	0	0	0
GCP-Cloud-1	ipsec	10.52.0.2	35.215.116.75	12347	12387	0	0	0	0
GCP-Cloud-1	ipsec	10.52.0.2	40.10.1.1	12347	12386	0	0	0	0

© 2020 Cisco and/or its affiliates. All rights reserved.

Step 2. Navigate to **Monitor** > **Tunnel**, to monitor both your controllers and WAN Edge devices within the Transit VPC.

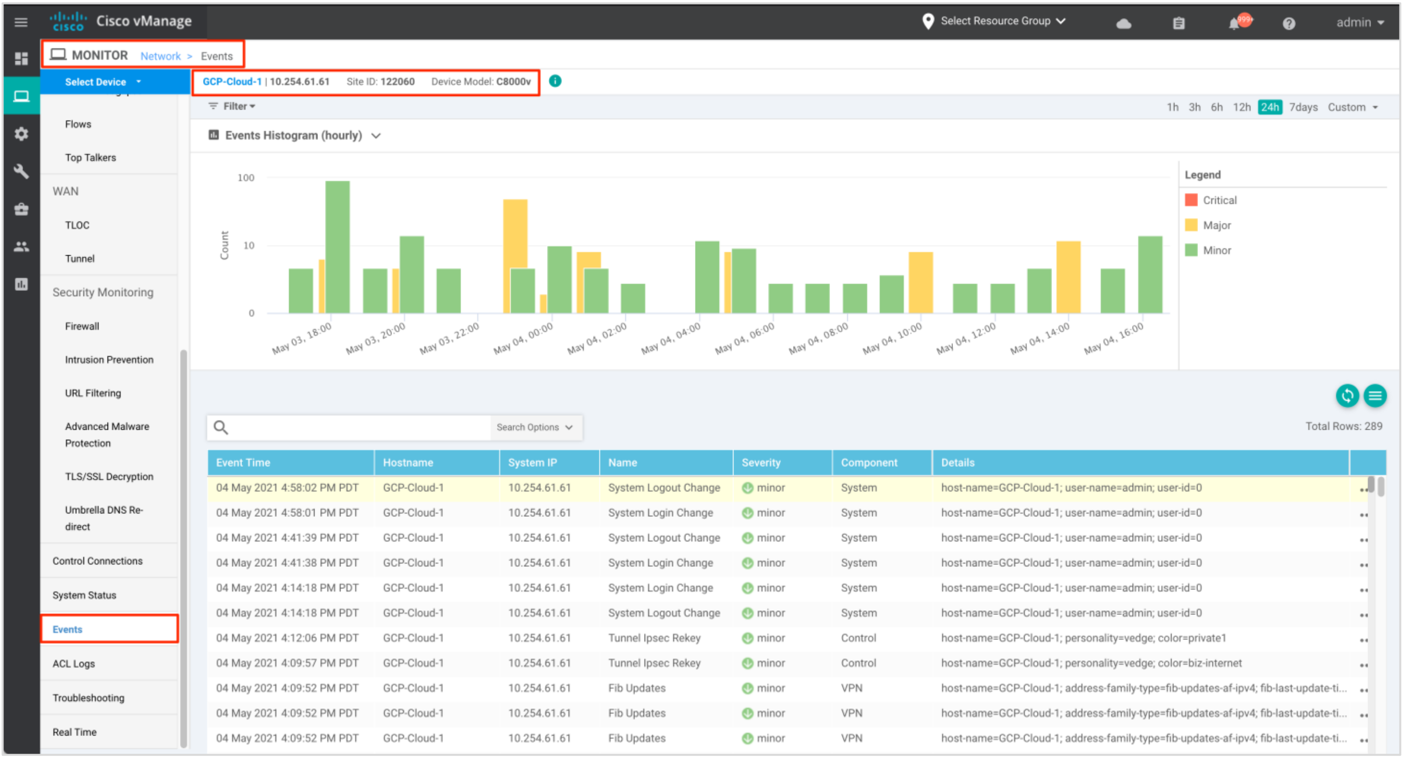

Cisco vManage
Select Resource Group
admin
MONITOR Network > WAN - Tunnel
Select Device
GCP-Cloud-1 | 10.254.61.61 Site ID: 122060 Device Model: C8000v
Flows
Top Talkers
WAN
TLOC
Tunnel
Security Monitoring
Firewall
Intrusion Prevention
URL Filtering
Advanced Malware Protection
TLS/SSL Decryption
Umbrella DNS Re-direct
Control Connections
System Status
Events
ACL Logs
Troubleshooting
Real Time
Chart Options
Real Time 1h 3h 6h 12h 24h 7days Custom
1 %
0.75 %
0.5 %
Loss Percentage
FEC Loss Recovery Rate
May 04, 06:00:00
• GCP-Cloud-1:biz-internet-GCP-Cloud-3:biz-internet[IPSEC][loss]:0.00%
• GCP-Cloud-1:biz-internet-GCP-Cloud-4:biz-internet[IPSEC][loss]:0.00%
May 04, 00:00
May 04, 02:00
May 04, 04:00
May 04, 06:00
May 04, 08:00
May 04, 10:00
May 04, 12:00
May 04, 14:00
May 04, 16:00
Legend
GCP-Cloud-1:biz-internet-GCP-Cloud-3:biz-internet[IPSEC]
GCP-Cloud-1:biz-internet-GCP-Cloud-4:biz-internet[IPSEC]
GCP-Cloud-1:biz-internet-WAN-EDGE-1:biz-internet[IPSEC]
GCP-Cloud-1:biz-internet-WAN-EDGE-1:bronze[IPSEC]
GCP-Cloud-1:biz-internet-WAN-EDGE-2:biz-internet[IPSEC]
GCP-Cloud-1:biz-internet-WAN-EDGE-2:bronze[IPSEC]
Search Options
Down (44) Init (0) Up (4)

6 Rows Selected (Interface Endpoints, Local Interface Description and Remote Interface Description are hidden by default. Please click on the Columns dropdown on the right to enable them)

Total Rows: 48

	Tunnel Endpoints	Interface Endpoints	Local Interface Description	Remote Interface Description	Protocol	State	Jitter (ms)	Loss (%)
	biz-internet	--	--	--	--	--		
☑	GCP-Cloud-1:biz-internet-GCP-Cloud-3:biz-internet	GigabitEthernet1-GigabitEt...	–	–	IPSEC	↑	0.00	0.00
☑	GCP-Cloud-1:biz-internet-GCP-Cloud-4:biz-internet	GigabitEthernet1-GigabitEt...	–	–	IPSEC	↑	0.01	0.02

Step 3. Navigate to **Monitor** > **Events**, to monitor both your controllers and WAN Edge devices within the Transit VPC.



Total Rows: 289

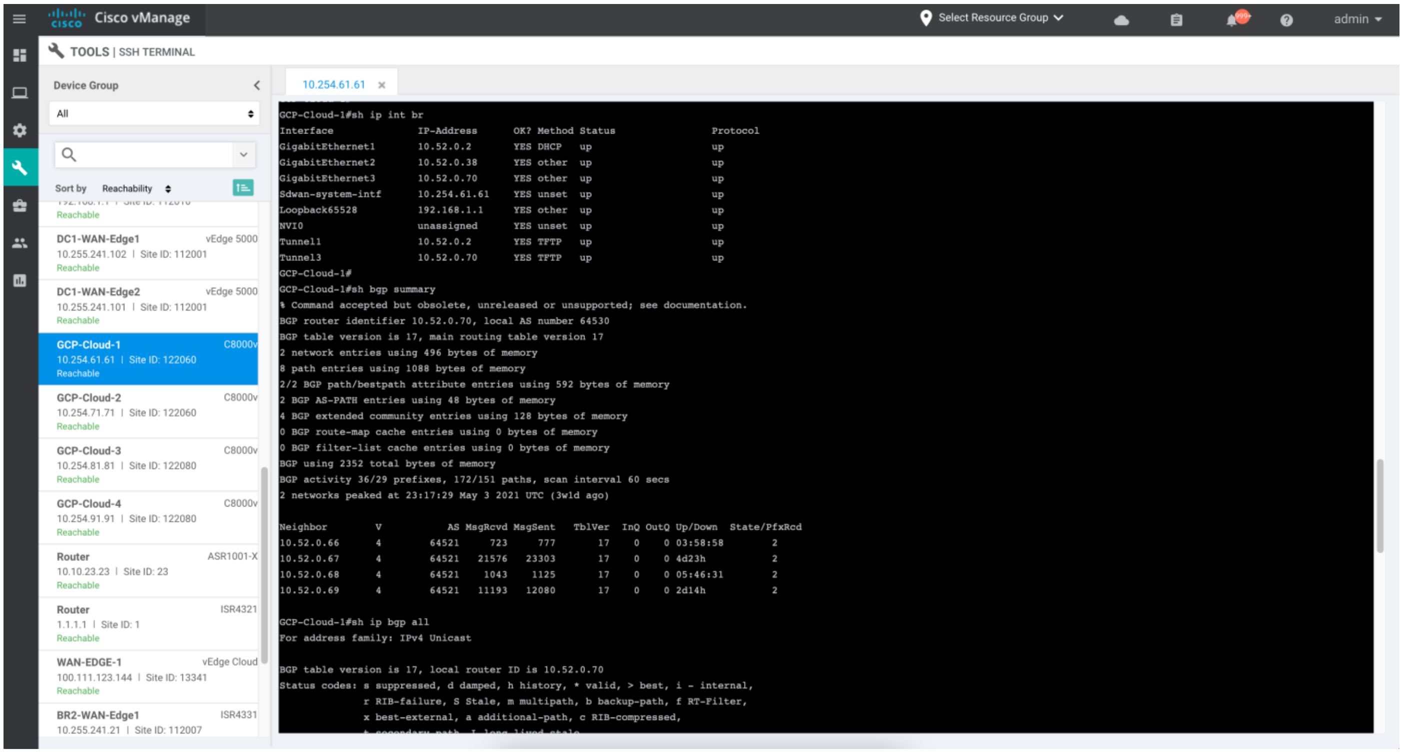
Event Time	Hostname	System IP	Name	Severity	Component	Details
04 May 2021 4:58:02 PM PDT	GCP-Cloud-1	10.254.61.61	System Logout Change	minor	System	host-name=GCP-Cloud-1; user-name=admin; user-id=0
04 May 2021 4:58:01 PM PDT	GCP-Cloud-1	10.254.61.61	System Login Change	minor	System	host-name=GCP-Cloud-1; user-name=admin; user-id=0
04 May 2021 4:41:39 PM PDT	GCP-Cloud-1	10.254.61.61	System Logout Change	minor	System	host-name=GCP-Cloud-1; user-name=admin; user-id=0
04 May 2021 4:41:38 PM PDT	GCP-Cloud-1	10.254.61.61	System Login Change	minor	System	host-name=GCP-Cloud-1; user-name=admin; user-id=0
04 May 2021 4:14:18 PM PDT	GCP-Cloud-1	10.254.61.61	System Login Change	minor	System	host-name=GCP-Cloud-1; user-name=admin; user-id=0
04 May 2021 4:14:18 PM PDT	GCP-Cloud-1	10.254.61.61	System Logout Change	minor	System	host-name=GCP-Cloud-1; user-name=admin; user-id=0
04 May 2021 4:12:06 PM PDT	GCP-Cloud-1	10.254.61.61	Tunnel Ipsec Rekey	minor	Control	host-name=GCP-Cloud-1; personality=vedge; color=private1
04 May 2021 4:09:57 PM PDT	GCP-Cloud-1	10.254.61.61	Tunnel Ipsec Rekey	minor	Control	host-name=GCP-Cloud-1; personality=vedge; color=biz-internet
04 May 2021 4:09:52 PM PDT	GCP-Cloud-1	10.254.61.61	Fib Updates	minor	VPN	host-name=GCP-Cloud-1; address-family-type=fib-updates-af-ipv4; fib-last-update-ti...
04 May 2021 4:09:52 PM PDT	GCP-Cloud-1	10.254.61.61	Fib Updates	minor	VPN	host-name=GCP-Cloud-1; address-family-type=fib-updates-af-ipv4; fib-last-update-ti...
04 May 2021 4:09:52 PM PDT	GCP-Cloud-1	10.254.61.61	Fib Updates	minor	VPN	host-name=GCP-Cloud-1; address-family-type=fib-updates-af-ipv4; fib-last-update-ti...

© 2020 Cisco and/or its affiliates. All rights reserved.

Process 3: vManage SSH Dashboard

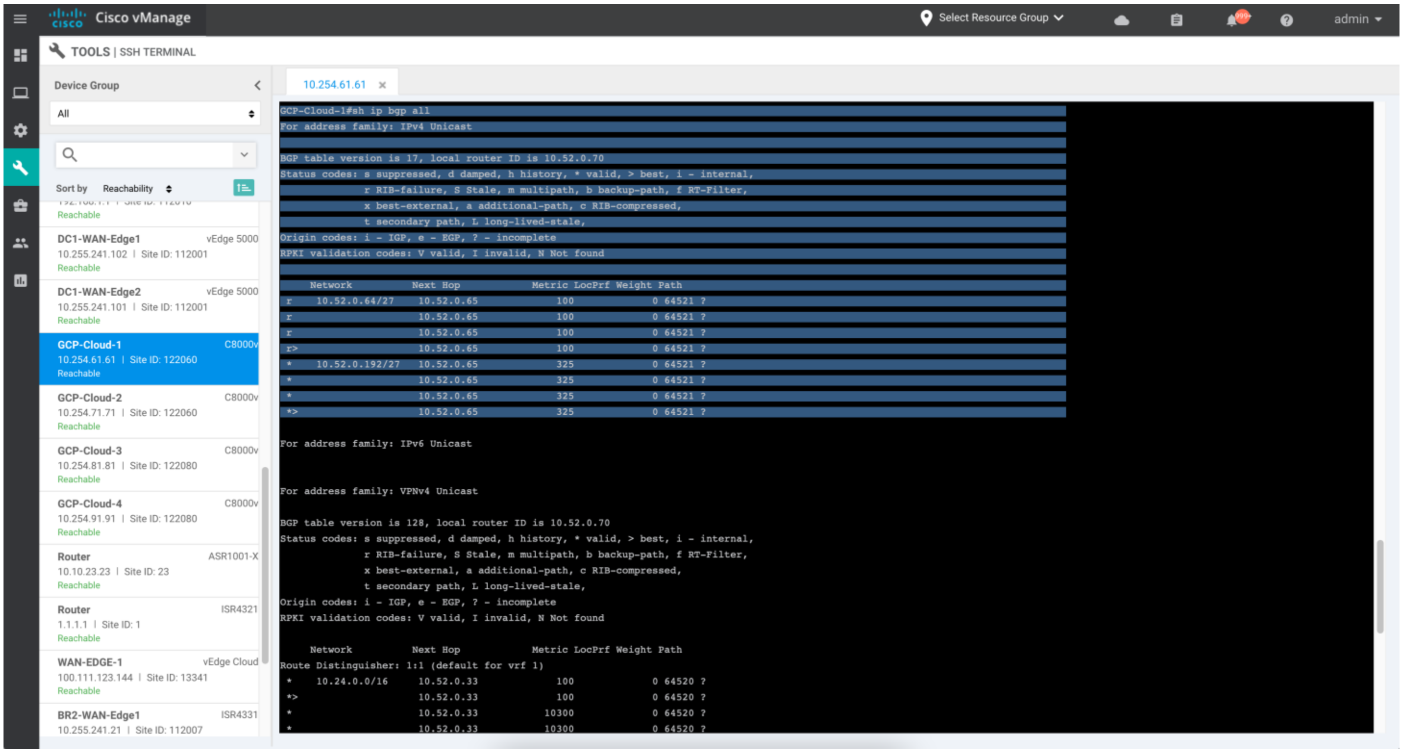
Procedure 1: Monitor Catalyst 8000v devices via CLI

Step 1. To view the IP address and BGP peers in the global routing table, issue the following commands “show ip int br” and “show bgp summary”.



```
GCP-Cloud-1#sh ip int br
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet1       10.52.0.2       YES DHCP   up                    up
GigabitEthernet2       10.52.0.38      YES other  up                    up
GigabitEthernet3       10.52.0.70      YES other  up                    up
Sdwan-system-intf      10.254.61.61    YES unset  up                    up
Loopback65528          192.168.1.1     YES other  up                    up
NVI0                   unassigned      YES unset  up                    up
Tunnel1                10.52.0.2       YES TFTP   up                    up
Tunnel3                10.52.0.70      YES TFTP   up                    up
GCP-Cloud-1#
GCP-Cloud-1#sh bgp summary
% Command accepted but obsolete, unreleased or unsupported; see documentation.
BGP router identifier 10.52.0.70, local AS number 64530
BGP table version is 17, main routing table version 17
2 network entries using 496 bytes of memory
8 path entries using 1088 bytes of memory
2/2 BGP path/bestpath attribute entries using 592 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
4 BGP extended community entries using 128 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 2352 total bytes of memory
BGP activity 36/29 prefixes, 172/151 paths, scan interval 60 secs
2 networks peaked at 23:17:29 May 3 2021 UTC (3w1d ago)

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.52.0.66      4        64521     723     777       17    0    0 03:58:58        2
10.52.0.67      4        64521   21576   23303       17    0    0 4d23h           2
10.52.0.68      4        64521    1043    1125       17    0    0 05:46:31        2
10.52.0.69      4        64521   11193   12080       17    0    0 2d14h           2

GCP-Cloud-1#sh ip bgp all
For address family: IPv4 Unicast

BGP table version is 17, local router ID is 10.52.0.70
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
```

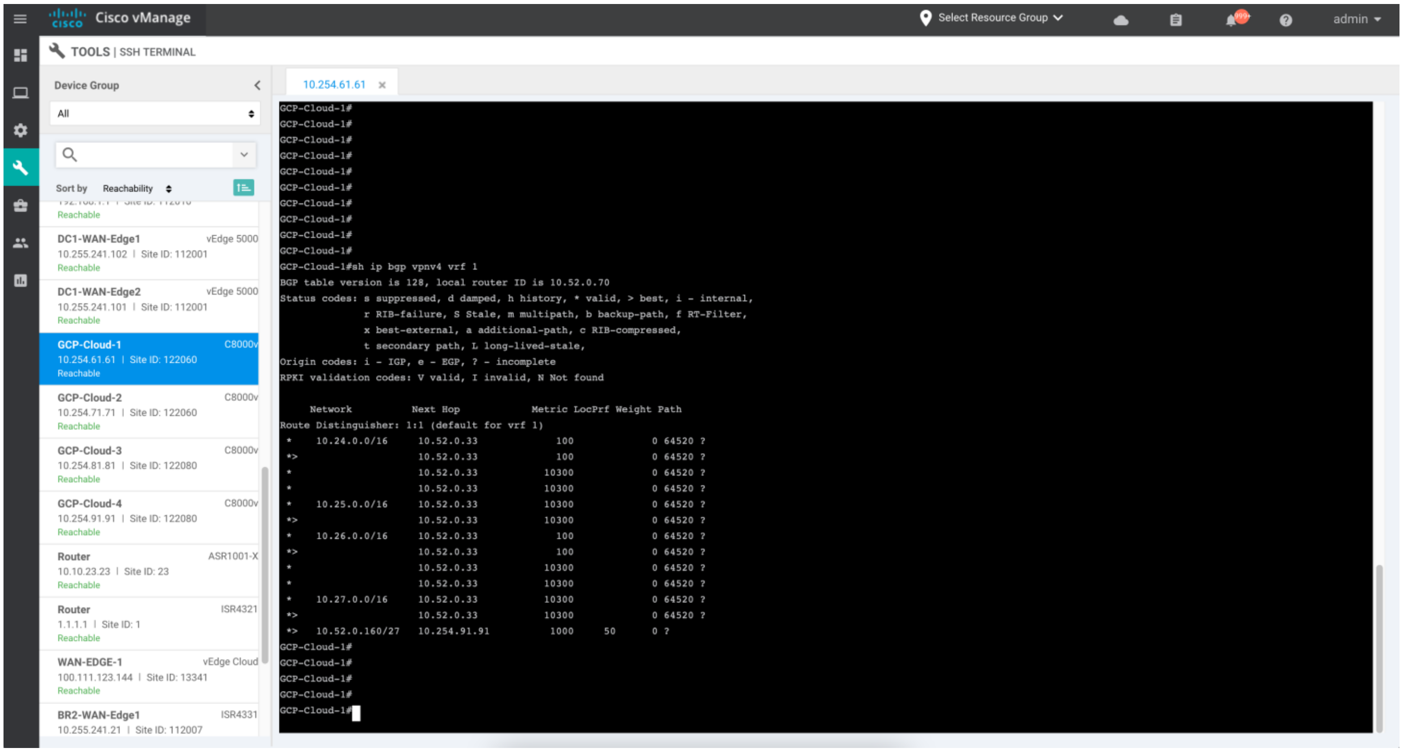
Step 2. To view the BGP routes learnt, enter CLI “show ip bgp all”.



```
GCP-Cloud-1#sh ip bgp all
For address family: IPv4 Unicast

BGP table version is 17, local router ID is 10.52.0.70
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path, L long-lived-stale,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
 r    10.52.0.64/27    10.52.0.65              100             0 64521 ?
 r                     10.52.0.65              100             0 64521 ?
 r                     10.52.0.65              100             0 64521 ?
 r>                    10.52.0.65              100             0 64521 ?
 *    10.52.0.192/27   10.52.0.65              325             0 64521 ?
 *                     10.52.0.65              325             0 64521 ?
 *                     10.52.0.65              325             0 64521 ?
 *>                    10.52.0.65              325             0 64521 ?

For address family: IPv6 Unicast


For address family: VPNv4 Unicast

BGP table version is 128, local router ID is 10.52.0.70
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path, L long-lived-stale,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf 1)
 *    10.24.0.0/16     10.52.0.33              100             0 64520 ?
 *>                    10.52.0.33              100             0 64520 ?
 *                     10.52.0.33            10300             0 64520 ?
 *                     10.52.0.33            10300             0 64520 ?
```

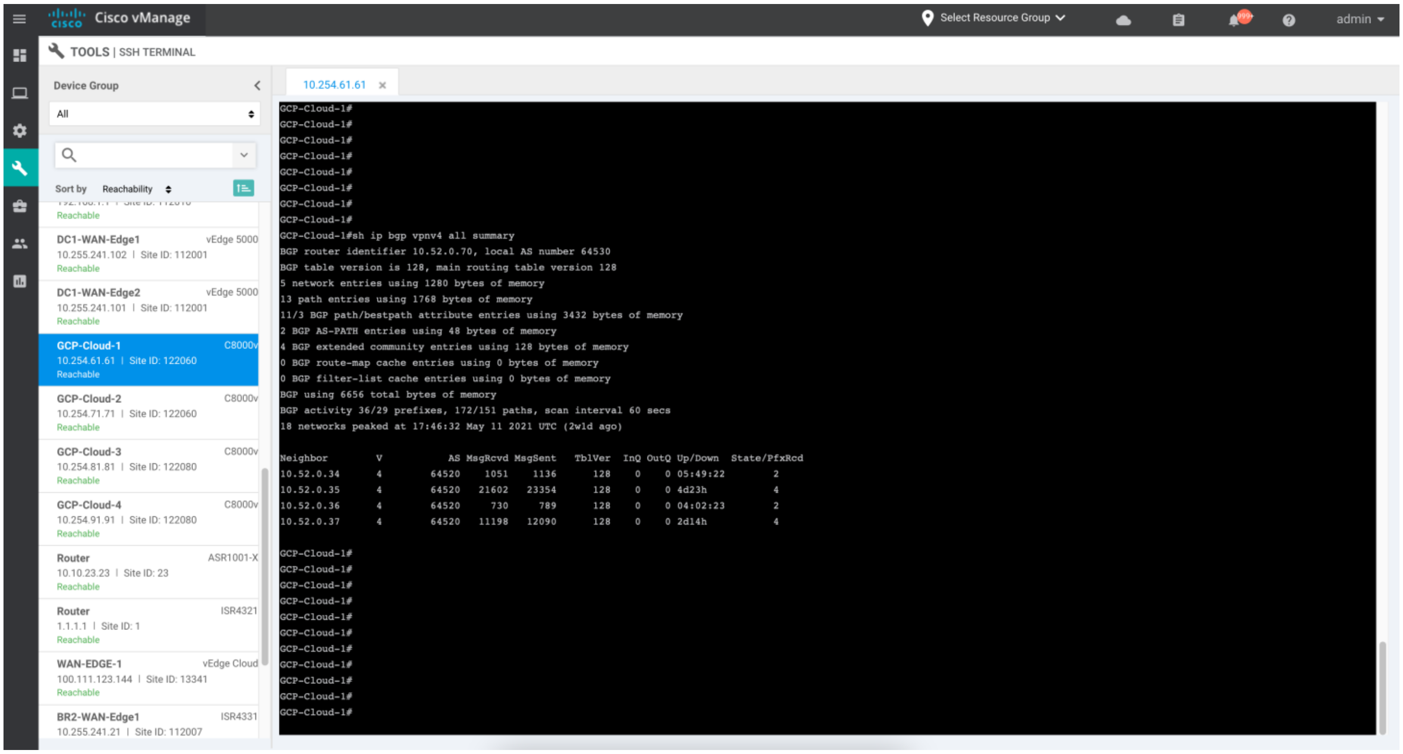
Step 3. To view the BGP routes learnt in VRF 1, issue the following commands “show ip bgp vpnv4 vrf 1”.

© 2020 Cisco and/or its affiliates. All rights reserved.



```
GCP-Cloud-1#
GCP-Cloud-1#
GCP-Cloud-1#
GCP-Cloud-1#
GCP-Cloud-1#
GCP-Cloud-1#
GCP-Cloud-1#
GCP-Cloud-1#
GCP-Cloud-1#
GCP-Cloud-1#
GCP-Cloud-1#sh ip bgp vpnv4 vrf 1
BGP table version is 128, local router ID is 10.52.0.70
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, f RT-Filter,
              x best-external, a additional-path, c RIB-compressed,
              t secondary path, L long-lived-stale,
Origin codes: i - IGP, e - EGP, ? - incomplete
RPKI validation codes: V valid, I invalid, N Not found

     Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf 1)
 *    10.24.0.0/16     10.52.0.33             100             0 64520 ?
 *>                    10.52.0.33             100             0 64520 ?
 *                     10.52.0.33           10300             0 64520 ?
 *                     10.52.0.33           10300             0 64520 ?
 *    10.25.0.0/16     10.52.0.33           10300             0 64520 ?
 *>                    10.52.0.33           10300             0 64520 ?
 *    10.26.0.0/16     10.52.0.33             100             0 64520 ?
 *>                    10.52.0.33             100             0 64520 ?
 *                     10.52.0.33           10300             0 64520 ?
 *                     10.52.0.33           10300             0 64520 ?
 *    10.27.0.0/16     10.52.0.33           10300             0 64520 ?
 *>                    10.52.0.33           10300             0 64520 ?
 *>   10.52.0.160/27   10.254.91.91          1000     50      0 ?
GCP-Cloud-1#
GCP-Cloud-1#
GCP-Cloud-1#
GCP-Cloud-1#
GCP-Cloud-1#
```

Step 4.   To view BGP neighbors learnt within service side, enter CLI "show ip bgp vpvnv4 all summary".



```
GCP-Cloud-1#
GCP-Cloud-1#
GCP-Cloud-1#
GCP-Cloud-1#
GCP-Cloud-1#
GCP-Cloud-1#
GCP-Cloud-1#
GCP-Cloud-1#
GCP-Cloud-1#sh ip bgp vpnv4 all summary
BGP router identifier 10.52.0.70, local AS number 64530
BGP table version is 128, main routing table version 128
5 network entries using 1280 bytes of memory
13 path entries using 1768 bytes of memory
11/3 BGP path/bestpath attribute entries using 3432 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
4 BGP extended community entries using 128 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 6656 total bytes of memory
BGP activity 36/29 prefixes, 172/151 paths, scan interval 60 secs
18 networks peaked at 17:46:32 May 11 2021 UTC (2w1d ago)

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.52.0.34      4        64520    1051    1136      128    0    0 05:49:22        2
10.52.0.35      4        64520   21602   23354      128    0    0 4d23h           4
10.52.0.36      4        64520     730     789      128    0    0 04:02:23        2
10.52.0.37      4        64520   11198   12090      128    0    0 2d14h           4

GCP-Cloud-1#
GCP-Cloud-1#
GCP-Cloud-1#
GCP-Cloud-1#
GCP-Cloud-1#
GCP-Cloud-1#
GCP-Cloud-1#
GCP-Cloud-1#
GCP-Cloud-1#
GCP-Cloud-1#
GCP-Cloud-1#
```

Appendix A: New in this Guide

This guide is new and is not updated from a previous version.

© 2020 Cisco and/or its affiliates. All rights reserved.

Appendix B: Hardware and Software Used for Validation

This guide was validated using the following hardware and software.

Table 3. System Feature Template Settings

Functional Area	Product	Software Version
Cloud	Cisco vManage NMS	20.5
Cloud	Cisco vBond Controller	20.5
Cloud	Cisco vSmart Controller	20.5
Cloud Gateway Devices	Catalyst 8000v	17.5

Appendix C: Catalyst 8000v Configuration

The following section lists out an example Catalyst 8000v configuration.

Cloud Gateway 1 - US-West1

1st Catalyst 8000v in CGW - US-WEST-1

```
system
 system-ip              10.254.61.61
 overlay-id             1
 site-id                122060
 port-offset            1
 control-session-pps    300
 admin-tech-on-failure
 sp-organization-name   "ENB-Solutions - 21615"
 organization-name      "ENB-Solutions - 21615"
 port-hop
 track-transport
 track-default-gateway
 console-baud-rate      19200
 no on-demand enable
 on-demand idle-timeout 10
 vbond vbond204.cisco.com port 12346
!
service tcp-keepalives-in
service tcp-keepalives-out
no service tcp-small-servers
no service udp-small-servers
hostname GCP-Cloud-1
username admin privilege 15 secret 9
$9$3V6L3V6L2VUI2k$ysPnXOdg8RLj9KgMdmfHdSHkdaMmiHzGaUpcqH6pfTo
vrf definition 1
 rd 1:1
```

© 2020 Cisco and/or its affiliates. All rights reserved.

```
 address-family ipv4
  route-target export 64530:1
  route-target import 64530:1
  exit-address-family
 !
 address-family ipv6
  exit-address-family
 !
!
vrf definition Mgmt-intf
 rd 1:512
 address-family ipv4
  route-target export 64530:512
  route-target import 64530:512
  exit-address-family
 !
 address-family ipv6
  exit-address-family
 !
!
ip arp proxy disable
no ip finger
no ip rcmd rcp-enable
no ip rcmd rsh-enable
ip as-path access-list 15 permit ^645[2][0-9]$
ip as-path access-list 25 permit .*
no ip dhcp use class
ip host vbond204.cisco.com 52.156.128.118
ip prefix-list GCP_CSR_PREFIX_LIST_POLICY seq 5 permit 10.52.0.70/32
ip bootp server
no ip source-route
no ip http server
no ip http secure-server
ip nat settings central-policy
cdp run
interface GigabitEthernet1
 no shutdown
 arp timeout 1200
 ip address dhcp client-id GigabitEthernet1
 no ip redirects
 ip dhcp client default-router distance 1
 ip mtu    1500
 load-interval 30
 mtu           1500
 negotiation auto
exit
interface GigabitEthernet2
```

```
 no shutdown
 arp timeout 1200
 vrf forwarding 1
 ip address 10.52.0.38 255.255.255.224
 no ip redirects
 ip mtu    1500
 load-interval 30
 mtu           1500
 negotiation auto
exit
interface GigabitEthernet3
 no shutdown
 arp timeout 1200
 ip address 10.52.0.70 255.255.255.224
 no ip redirects
 ip mtu    1500
 load-interval 30
 mtu           1500
 negotiation auto
exit
interface Tunnel1
 no shutdown
 ip unnumbered GigabitEthernet1
 no ip redirects
 ipv6 unnumbered GigabitEthernet1
 no ipv6 redirects
 tunnel source GigabitEthernet1
 tunnel mode sdwan
exit
interface Tunnel3
 no shutdown
 ip unnumbered GigabitEthernet3
 no ip redirects
 ipv6 unnumbered GigabitEthernet3
 no ipv6 redirects
 tunnel source GigabitEthernet3
 tunnel mode sdwan
exit
route-map GCP_CSR_PREFIX_ROUTE_POLICY permit 10
 match ip address prefix-list GCP_CSR_PREFIX_LIST_POLICY
!
route-map GCP_CSR_PREFIX_ROUTE_POLICY deny 65535
!
route-map GCP_CSR_ROUTE_POLICY deny 1
 match as-path 15
!
route-map GCP_CSR_ROUTE_POLICY permit 11
```

```
 match as-path 25
!
route-map GCP_CSR_ROUTE_POLICY deny 65535
!
clock timezone UTC 0 0
logging persistent size 104857600 filesize 10485760
logging console
aaa authentication login default local
aaa authorization exec default local
aaa server radius dynamic-author
!
router bgp 64530
 bgp log-neighbor-changes
 neighbor 10.52.0.66 remote-as 64521
 neighbor 10.52.0.66 ebgp-multihop 255
 neighbor 10.52.0.67 remote-as 64521
 neighbor 10.52.0.67 ebgp-multihop 255
 neighbor 10.52.0.68 remote-as 64521
 neighbor 10.52.0.68 ebgp-multihop 255
 neighbor 10.52.0.69 remote-as 64521
 neighbor 10.52.0.69 ebgp-multihop 255
 address-family ipv4 unicast vrf 1
  distance bgp 20 200 20
  neighbor 10.52.0.34 remote-as 64520
  neighbor 10.52.0.34 activate
  neighbor 10.52.0.34 ebgp-multihop 255
  neighbor 10.52.0.34 route-map GCP_CSR_ROUTE_POLICY out
  neighbor 10.52.0.34 send-community both
  neighbor 10.52.0.35 remote-as 64520
  neighbor 10.52.0.35 activate
  neighbor 10.52.0.35 ebgp-multihop 255
  neighbor 10.52.0.35 route-map GCP_CSR_ROUTE_POLICY out
  neighbor 10.52.0.35 send-community both
  neighbor 10.52.0.36 remote-as 64520
  neighbor 10.52.0.36 activate
  neighbor 10.52.0.36 ebgp-multihop 255
  neighbor 10.52.0.36 route-map GCP_CSR_ROUTE_POLICY out
  neighbor 10.52.0.36 send-community both
  neighbor 10.52.0.37 remote-as 64520
  neighbor 10.52.0.37 activate
  neighbor 10.52.0.37 ebgp-multihop 255
  neighbor 10.52.0.37 route-map GCP_CSR_ROUTE_POLICY out
  neighbor 10.52.0.37 send-community both
  propagate-aspath
  redistribute omp
  exit-address-family
 !
```

© 2020 Cisco and/or its affiliates. All rights reserved.

```
 address-family ipv4 unicast
  distance bgp 20 200 20
  neighbor 10.52.0.66 activate
  neighbor 10.52.0.66 route-map GCP_CSR_ROUTE_POLICY out
  neighbor 10.52.0.66 send-community both
  neighbor 10.52.0.67 activate
  neighbor 10.52.0.67 route-map GCP_CSR_ROUTE_POLICY out
  neighbor 10.52.0.67 send-community both
  neighbor 10.52.0.68 activate
  neighbor 10.52.0.68 route-map GCP_CSR_ROUTE_POLICY out
  neighbor 10.52.0.68 send-community both
  neighbor 10.52.0.69 activate
  neighbor 10.52.0.69 route-map GCP_CSR_ROUTE_POLICY out
  neighbor 10.52.0.69 send-community both
  redistribute connected
  redistribute connected route-map GCP_CSR_PREFIX_ROUTE_POLICY
  exit-address-family
 !
 timers bgp 60 180
!
snmp-server ifindex persist
line aux 0
 stopbits 1
!
line con 0
 speed    19200
 stopbits 1
!
line vty 0 4
 transport input ssh
!
line vty 5 80
 transport input ssh
!
lldp run
nat64 translation timeout tcp 60
nat64 translation timeout udp 1
sdwan
 interface GigabitEthernet1
  tunnel-interface
   encapsulation ipsec weight 1
   no border
   color biz-internet
   no last-resort-circuit
   no low-bandwidth-link
   no vbond-as-stun-server
   vmanage-connection-preference 5
   port-hop
   carrier                       default
   nat-refresh-interval          5
   hello-interval                1000
   hello-tolerance               12
   allow-service all
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   no allow-service snmp
   no allow-service bfd
  exit
 exit
 interface GigabitEthernet3
  tunnel-interface
   encapsulation ipsec weight 1
   no border
   color private1
   no last-resort-circuit
   no low-bandwidth-link
   max-control-connections       0
   no vbond-as-stun-server
   vmanage-connection-preference 0
   port-hop
   carrier                       default
   nat-refresh-interval          5
   hello-interval                1000
   hello-tolerance               12
   allow-service all
   allow-service bgp
   no allow-service dhcp
   allow-service dns
   allow-service icmp
   allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   no allow-service snmp
```

© 2020 Cisco and/or its affiliates. All rights reserved.

```
   no allow-service bfd
  exit
 exit
 appqoe
  no tcpopt enable
  no dreopt enable
 !
 omp
  no shutdown
  send-path-limit  4
  ecmp-limit       4
  graceful-restart
  no as-dot-notation
  timers
   holdtime               60
   advertisement-interval 1
   graceful-restart-timer 43200
   eor-timer              300
  exit
  address-family ipv4
   advertise bgp
   advertise connected
   advertise static
  !
  address-family ipv6
   advertise bgp
   advertise connected
   advertise static
  !
 !
!
licensing config enable false
licensing config privacy hostname false
licensing config privacy version false
licensing config utility utility-enable false
bfd color lte
 hello-interval 1000
 no pmtu-discovery
 multiplier     1
!
bfd default-dscp 48
bfd app-route multiplier 2
bfd app-route poll-interval 123400
security
 ipsec
  rekey               86400
  replay-window       512
```

© 2020 Cisco and/or its affiliates. All rights reserved.

```
   authentication-type ah-sha1-hmac sha1-hmac
  !
 !
 sslproxy
  no enable
  rsa-key-modulus      2048
  certificate-lifetime 730
  eckey-type           P256
  ca-tp-label          PROXY-SIGNING-CA
  settings expired-certificate  drop
  settings untrusted-certificate drop
  settings unknown-status       drop
  settings certificate-revocation-check none
  settings unsupported-protocol-versions drop
  settings unsupported-cipher-suites drop
  settings failure-mode         close
  settings minimum-tls-ver      TLSv1
  dual-side optimization enable
 !
 policy
  no app-visibility
  no app-visibility-ipv6
  no flow-visibility
  no flow-visibility-ipv6
  no implicit-acl-logging
  log-frequency        1000
 !
```

2nd Catalyst 8000v – CGW US-West-1

```
 system
  system-ip             10.254.71.71
  overlay-id            1
  site-id               122060
  port-offset           1
  control-session-pps   300
  admin-tech-on-failure
  sp-organization-name  "ENB-Solutions - 21615"
  organization-name     "ENB-Solutions - 21615"
  port-hop
  track-transport
  track-default-gateway
  console-baud-rate     19200
  no on-demand enable
  on-demand idle-timeout 10
  vbond vbond204.cisco.com port 12346
 !
```

© 2020 Cisco and/or its affiliates. All rights reserved.

```
service tcp-keepalives-in
service tcp-keepalives-out
no service tcp-small-servers
no service udp-small-servers
hostname GCP-Cloud-2
username admin privilege 15 secret 9
$9$3V6L3V6L2VUI2k$ysPnXOdg8RLj9KgMdmfHdSHkdaMmiHzGaUpcqH6pfTo
vrf definition 1
 rd 1:1
 address-family ipv4
  route-target export 64530:1
  route-target import 64530:1
  exit-address-family
 !
 address-family ipv6
  exit-address-family
 !
!
vrf definition Mgmt-intf
 rd 1:512
 address-family ipv4
  route-target export 64530:512
  route-target import 64530:512
  exit-address-family
 !
 address-family ipv6
  exit-address-family
 !
!
ip arp proxy disable
no ip finger
no ip rcmd rcp-enable
no ip rcmd rsh-enable
ip as-path access-list 15 permit ^645[2][0-9]$
ip as-path access-list 25 permit .*
no ip dhcp use class
ip host vbond204.cisco.com 52.156.128.118
ip prefix-list GCP_CSR_PREFIX_LIST_POLICY seq 5 permit 10.52.0.198/32
ip bootp server
no ip source-route
no ip http server
no ip http secure-server
ip nat settings central-policy
cdp run
interface GigabitEthernet1
 no shutdown
 arp timeout 1200
```

© 2020 Cisco and/or its affiliates. All rights reserved.

```
 ip address dhcp client-id GigabitEthernet1
 no ip redirects
 ip dhcp client default-router distance 1
 ip mtu    1500
 load-interval 30
 mtu           1500
 negotiation auto
exit
interface GigabitEthernet2
 no shutdown
 arp timeout 1200
 vrf forwarding 1
 ip address 10.52.0.166 255.255.255.224
 no ip redirects
 ip mtu    1500
 load-interval 30
 mtu           1500
 negotiation auto
exit
interface GigabitEthernet3
 no shutdown
 arp timeout 1200
 ip address 10.52.0.198 255.255.255.224
 no ip redirects
 ip mtu    1500
 load-interval 30
 mtu           1500
 negotiation auto
exit
interface Tunnel1
 no shutdown
 ip unnumbered GigabitEthernet1
 no ip redirects
 ipv6 unnumbered GigabitEthernet1
 no ipv6 redirects
 tunnel source GigabitEthernet1
 tunnel mode sdwan
exit
interface Tunnel3
 no shutdown
 ip unnumbered GigabitEthernet3
 no ip redirects
 ipv6 unnumbered GigabitEthernet3
 no ipv6 redirects
 tunnel source GigabitEthernet3
 tunnel mode sdwan
exit
```

```
route-map GCP_CSR_PREFIX_ROUTE_POLICY permit 10
 match ip address prefix-list GCP_CSR_PREFIX_LIST_POLICY
!
route-map GCP_CSR_PREFIX_ROUTE_POLICY deny 65535
!
route-map GCP_CSR_ROUTE_POLICY deny 1
 match as-path 15
!
route-map GCP_CSR_ROUTE_POLICY permit 11
 match as-path 25
!
route-map GCP_CSR_ROUTE_POLICY deny 65535
!
clock timezone UTC 0 0
logging persistent size 104857600 filesize 10485760
logging console
aaa authentication login default local
aaa authorization exec default local
aaa server radius dynamic-author
!
router bgp 64530
 bgp log-neighbor-changes
 neighbor 10.52.0.194 remote-as 64521
 neighbor 10.52.0.194 ebgp-multihop 255
 neighbor 10.52.0.195 remote-as 64521
 neighbor 10.52.0.195 ebgp-multihop 255
 neighbor 10.52.0.196 remote-as 64521
 neighbor 10.52.0.196 ebgp-multihop 255
 neighbor 10.52.0.197 remote-as 64521
 neighbor 10.52.0.197 ebgp-multihop 255
 address-family ipv4 unicast vrf 1
  distance bgp 20 200 20
  neighbor 10.52.0.162 remote-as 64520
  neighbor 10.52.0.162 activate
  neighbor 10.52.0.162 ebgp-multihop 255
  neighbor 10.52.0.162 route-map GCP_CSR_ROUTE_POLICY out
  neighbor 10.52.0.162 send-community both
  neighbor 10.52.0.163 remote-as 64520
  neighbor 10.52.0.163 activate
  neighbor 10.52.0.163 ebgp-multihop 255
  neighbor 10.52.0.163 route-map GCP_CSR_ROUTE_POLICY out
  neighbor 10.52.0.163 send-community both
  neighbor 10.52.0.164 remote-as 64520
  neighbor 10.52.0.164 activate
  neighbor 10.52.0.164 ebgp-multihop 255
  neighbor 10.52.0.164 route-map GCP_CSR_ROUTE_POLICY out
  neighbor 10.52.0.164 send-community both
  neighbor 10.52.0.165 remote-as 64520
  neighbor 10.52.0.165 activate
  neighbor 10.52.0.165 ebgp-multihop 255
  neighbor 10.52.0.165 route-map GCP_CSR_ROUTE_POLICY out
  neighbor 10.52.0.165 send-community both
  propagate-aspath
  redistribute omp
  exit-address-family
 !
 address-family ipv4 unicast
  distance bgp 20 200 20
  neighbor 10.52.0.194 activate
  neighbor 10.52.0.194 route-map GCP_CSR_ROUTE_POLICY out
  neighbor 10.52.0.194 send-community both
  neighbor 10.52.0.195 activate
  neighbor 10.52.0.195 route-map GCP_CSR_ROUTE_POLICY out
  neighbor 10.52.0.195 send-community both
  neighbor 10.52.0.196 activate
  neighbor 10.52.0.196 route-map GCP_CSR_ROUTE_POLICY out
  neighbor 10.52.0.196 send-community both
  neighbor 10.52.0.197 activate
  neighbor 10.52.0.197 route-map GCP_CSR_ROUTE_POLICY out
  neighbor 10.52.0.197 send-community both
  redistribute connected
  redistribute connected route-map GCP_CSR_PREFIX_ROUTE_POLICY
  exit-address-family
 !
 timers bgp 60 180
!
snmp-server ifindex persist
line aux 0
 stopbits 1
!
line con 0
 speed    19200
 stopbits 1
!
line vty 0 4
 transport input ssh
!
line vty 5 80
 transport input ssh
!
lldp run
nat64 translation timeout tcp 60
nat64 translation timeout udp 1
sdwan
```

© 2020 Cisco and/or its affiliates. All rights reserved.

```
interface GigabitEthernet1
 tunnel-interface
  encapsulation ipsec weight 1
  no border
  color biz-internet
  no last-resort-circuit
  no low-bandwidth-link
  no vbond-as-stun-server
  vmanage-connection-preference 5
  port-hop
  carrier                       default
  nat-refresh-interval          5
  hello-interval                1000
  hello-tolerance               12
  allow-service all
  no allow-service bgp
  allow-service dhcp
  allow-service dns
  allow-service icmp
  allow-service sshd
  no allow-service netconf
  no allow-service ntp
  no allow-service ospf
  no allow-service stun
  allow-service https
  no allow-service snmp
  no allow-service bfd
 exit
exit
interface GigabitEthernet3
 tunnel-interface
  encapsulation ipsec weight 1
  no border
  color private1
  no last-resort-circuit
  no low-bandwidth-link
  max-control-connections       0
  no vbond-as-stun-server
  vmanage-connection-preference 0
  port-hop
  carrier                       default
  nat-refresh-interval          5
  hello-interval                1000
  hello-tolerance               12
  allow-service all
  allow-service bgp
  no allow-service dhcp
```

```
   allow-service dns
   allow-service icmp
   allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   no allow-service snmp
   no allow-service bfd
  exit
 exit
 appqoe
  no tcpopt enable
  no dreopt enable
 !
 omp
  no shutdown
  send-path-limit  4
  ecmp-limit       4
  graceful-restart
  no as-dot-notation
  timers
   holdtime               60
   advertisement-interval 1
   graceful-restart-timer 43200
   eor-timer              300
  exit
  address-family ipv4
   advertise bgp
   advertise connected
   advertise static
  !
  address-family ipv6
   advertise bgp
   advertise connected
   advertise static
  !
 !
!
licensing config enable false
licensing config privacy hostname false
licensing config privacy version false
licensing config utility utility-enable false
bfd color lte
 hello-interval 1000
 no pmtu-discovery
```

© 2020 Cisco and/or its affiliates. All rights reserved.

```
 multiplier     1
!
bfd default-dscp 48
bfd app-route multiplier 2
bfd app-route poll-interval 123400
security
 ipsec
  rekey               86400
  replay-window       512
  authentication-type ah-sha1-hmac sha1-hmac
 !
!
sslproxy
 no enable
 rsa-key-modulus      2048
 certificate-lifetime 730
 eckey-type           P256
 ca-tp-label          PROXY-SIGNING-CA
 settings expired-certificate  drop
 settings untrusted-certificate drop
 settings unknown-status       drop
 settings certificate-revocation-check none
 settings unsupported-protocol-versions drop
 settings unsupported-cipher-suites drop
 settings failure-mode         close
 settings minimum-tls-ver      TLSv1
 dual-side optimization enable
!
policy
 no app-visibility
 no app-visibility-ipv6
 no flow-visibility
 no flow-visibility-ipv6
 no implicit-acl-logging
 log-frequency        1000
!
```

Cloud Gateway 2 - US-West2

1st Catalyst 8000v - CGW US-West-2

```
system
 system-ip             10.254.81.81
 overlay-id            1
 site-id               122080
 port-offset           1
 control-session-pps   300
 admin-tech-on-failure
 sp-organization-name  "ENB-Solutions - 21615"
```

© 2020 Cisco and/or its affiliates. All rights reserved.

```
 organization-name     "ENB-Solutions - 21615"
 port-hop
 track-transport
 track-default-gateway
 console-baud-rate     19200
 no on-demand enable
 on-demand idle-timeout 10
 vbond vbond204.cisco.com port 12346
!
service tcp-keepalives-in
service tcp-keepalives-out
no service tcp-small-servers
no service udp-small-servers
hostname GCP-Cloud-3
username admin privilege 15 secret 9
$9$3V6L3V6L2VUI2k$ysPnXOdg8RLj9KgMdmfHdSHkdaMmiHzGaUpcqH6pfTo
vrf definition 1
 rd 1:1
 address-family ipv4
  route-target export 64530:1
  route-target import 64530:1
  exit-address-family
 !
 address-family ipv6
  exit-address-family
 !
!
vrf definition Mgmt-intf
 rd 1:512
 address-family ipv4
  route-target export 64530:512
  route-target import 64530:512
  exit-address-family
 !
 address-family ipv6
  exit-address-family
 !
!
ip arp proxy disable
no ip finger
no ip rcmd rcp-enable
no ip rcmd rsh-enable
ip as-path access-list 15 permit ^645[2][0-9]$
ip as-path access-list 25 permit .*
no ip dhcp use class
ip host vbond204.cisco.com 52.156.128.118
ip prefix-list GCP_CSR_PREFIX_LIST_POLICY seq 5 permit 10.52.0.71/32
```

© 2020 Cisco and/or its affiliates. All rights reserved.

```
ip bootp server
no ip source-route
no ip http server
no ip http secure-server
ip nat settings central-policy
cdp run
interface GigabitEthernet1
 no shutdown
 arp timeout 1200
 ip address dhcp client-id GigabitEthernet1
 no ip redirects
 ip dhcp client default-router distance 1
 ip mtu    1500
 load-interval 30
 mtu           1500
 negotiation auto
exit
interface GigabitEthernet2
 no shutdown
 arp timeout 1200
 vrf forwarding 1
 ip address 10.52.0.39 255.255.255.224
 no ip redirects
 ip mtu    1500
 load-interval 30
 mtu           1500
 negotiation auto
exit
interface GigabitEthernet3
 no shutdown
 arp timeout 1200
 ip address 10.52.0.71 255.255.255.224
 no ip redirects
 ip mtu    1500
 load-interval 30
 mtu           1500
 negotiation auto
exit
interface Tunnel1
 no shutdown
 ip unnumbered GigabitEthernet1
 no ip redirects
 ipv6 unnumbered GigabitEthernet1
 no ipv6 redirects
 tunnel source GigabitEthernet1
 tunnel mode sdwan
exit
```

© 2020 Cisco and/or its affiliates. All rights reserved.

```
interface Tunnel3
 no shutdown
 ip unnumbered GigabitEthernet3
 no ip redirects
 ipv6 unnumbered GigabitEthernet3
 no ipv6 redirects
 tunnel source GigabitEthernet3
 tunnel mode sdwan
exit
route-map GCP_CSR_PREFIX_ROUTE_POLICY permit 10
 match ip address prefix-list GCP_CSR_PREFIX_LIST_POLICY
!
route-map GCP_CSR_PREFIX_ROUTE_POLICY deny 65535
!
route-map GCP_CSR_ROUTE_POLICY deny 1
 match as-path 15
!
route-map GCP_CSR_ROUTE_POLICY permit 11
 match as-path 25
!
route-map GCP_CSR_ROUTE_POLICY deny 65535
!
clock timezone UTC 0 0
logging persistent size 104857600 filesize 10485760
logging console
aaa authentication login default local
aaa authorization exec default local
aaa server radius dynamic-author
!
router bgp 64530
 bgp log-neighbor-changes
 neighbor 10.52.0.66 remote-as 64521
 neighbor 10.52.0.66 ebgp-multihop 255
 neighbor 10.52.0.67 remote-as 64521
 neighbor 10.52.0.67 ebgp-multihop 255
 neighbor 10.52.0.68 remote-as 64521
 neighbor 10.52.0.68 ebgp-multihop 255
 neighbor 10.52.0.69 remote-as 64521
 neighbor 10.52.0.69 ebgp-multihop 255
 address-family ipv4 unicast vrf 1
  distance bgp 20 200 20
  neighbor 10.52.0.34 remote-as 64520
  neighbor 10.52.0.34 activate
  neighbor 10.52.0.34 ebgp-multihop 255
  neighbor 10.52.0.34 route-map GCP_CSR_ROUTE_POLICY out
  neighbor 10.52.0.34 send-community both
  neighbor 10.52.0.35 remote-as 64520
  neighbor 10.52.0.35 activate
  neighbor 10.52.0.35 ebgp-multihop 255
  neighbor 10.52.0.35 route-map GCP_CSR_ROUTE_POLICY out
  neighbor 10.52.0.35 send-community both
  neighbor 10.52.0.36 remote-as 64520
  neighbor 10.52.0.36 activate
  neighbor 10.52.0.36 ebgp-multihop 255
  neighbor 10.52.0.36 route-map GCP_CSR_ROUTE_POLICY out
  neighbor 10.52.0.36 send-community both
  neighbor 10.52.0.37 remote-as 64520
  neighbor 10.52.0.37 activate
  neighbor 10.52.0.37 ebgp-multihop 255
  neighbor 10.52.0.37 route-map GCP_CSR_ROUTE_POLICY out
  neighbor 10.52.0.37 send-community both
  propagate-aspath
  redistribute omp
  exit-address-family
 !
 address-family ipv4 unicast
  distance bgp 20 200 20
  neighbor 10.52.0.66 activate
  neighbor 10.52.0.66 route-map GCP_CSR_ROUTE_POLICY out
  neighbor 10.52.0.66 send-community both
  neighbor 10.52.0.67 activate
  neighbor 10.52.0.67 route-map GCP_CSR_ROUTE_POLICY out
  neighbor 10.52.0.67 send-community both
  neighbor 10.52.0.68 activate
  neighbor 10.52.0.68 route-map GCP_CSR_ROUTE_POLICY out
  neighbor 10.52.0.68 send-community both
  neighbor 10.52.0.69 activate
  neighbor 10.52.0.69 route-map GCP_CSR_ROUTE_POLICY out
  neighbor 10.52.0.69 send-community both
  redistribute connected
  redistribute connected route-map GCP_CSR_PREFIX_ROUTE_POLICY
  exit-address-family
 !
 timers bgp 60 180
!
snmp-server ifindex persist
line aux 0
 stopbits 1
!
line con 0
 speed    19200
 stopbits 1
!
line vty 0 4
```

© 2020 Cisco and/or its affiliates. All rights reserved.

```
 transport input ssh
!
line vty 5 80
 transport input ssh
!
lldp run
nat64 translation timeout tcp 60
nat64 translation timeout udp 1
sdwan
 interface GigabitEthernet1
  tunnel-interface
   encapsulation ipsec weight 1
   no border
   color biz-internet
   no last-resort-circuit
   no low-bandwidth-link
   no vbond-as-stun-server
   vmanage-connection-preference 5
   port-hop
   carrier                       default
   nat-refresh-interval          5
   hello-interval                1000
   hello-tolerance               12
   allow-service all
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   no allow-service snmp
   no allow-service bfd
  exit
 exit
 interface GigabitEthernet3
  tunnel-interface
   encapsulation ipsec weight 1
   no border
   color private1
   no last-resort-circuit
   no low-bandwidth-link
   max-control-connections       0
   no vbond-as-stun-server
```

© 2020 Cisco and/or its affiliates. All rights reserved.

```
   vmanage-connection-preference 0
   port-hop
   carrier                       default
   nat-refresh-interval          5
   hello-interval                1000
   hello-tolerance               12
   allow-service all
   allow-service bgp
   no allow-service dhcp
   allow-service dns
   allow-service icmp
   allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   no allow-service snmp
   no allow-service bfd
  exit
 exit
 appqoe
  no tcpopt enable
  no dreopt enable
 !
 omp
  no shutdown
  send-path-limit  4
  ecmp-limit       4
  graceful-restart
  no as-dot-notation
  timers
   holdtime               60
   advertisement-interval 1
   graceful-restart-timer 43200
   eor-timer              300
  exit
  address-family ipv4
   advertise bgp
   advertise connected
   advertise static
  !
  address-family ipv6
   advertise bgp
   advertise connected
   advertise static
  !
```

© 2020 Cisco and/or its affiliates. All rights reserved.

```
 !
!
licensing config enable false
licensing config privacy hostname false
licensing config privacy version false
licensing config utility utility-enable false
bfd color lte
 hello-interval 1000
 no pmtu-discovery
 multiplier     1
!
bfd default-dscp 48
bfd app-route multiplier 2
bfd app-route poll-interval 123400
security
 ipsec
  rekey               86400
  replay-window       512
  authentication-type ah-sha1-hmac sha1-hmac
 !
!
sslproxy
 no enable
 rsa-key-modulus      2048
 certificate-lifetime 730
 eckey-type           P256
 ca-tp-label          PROXY-SIGNING-CA
 settings expired-certificate  drop
 settings untrusted-certificate drop
 settings unknown-status       drop
 settings certificate-revocation-check none
 settings unsupported-protocol-versions drop
 settings unsupported-cipher-suites drop
 settings failure-mode         close
 settings minimum-tls-ver      TLSv1
 dual-side optimization enable
!
policy
 no app-visibility
 no app-visibility-ipv6
 no flow-visibility
 no flow-visibility-ipv6
 no implicit-acl-logging
 log-frequency        1000
!
```

© 2020 Cisco and/or its affiliates. All rights reserved.

2st Catalyst 8000v - CGW US-West-2

```
system
 system-ip             10.254.91.91
 overlay-id            1
 site-id               122080
 port-offset           1
 control-session-pps   300
 admin-tech-on-failure
 sp-organization-name  "ENB-Solutions - 21615"
 organization-name     "ENB-Solutions - 21615"
 port-hop
 track-transport
 track-default-gateway
 console-baud-rate     19200
 no on-demand enable
 on-demand idle-timeout 10
 vbond vbond204.cisco.com port 12346
!
service tcp-keepalives-in
service tcp-keepalives-out
no service tcp-small-servers
no service udp-small-servers
hostname GCP-Cloud-4
username admin privilege 15 secret 9
$9$3V6L3V6L2VUI2k$ysPnXOdg8RLj9KgMdmfHdSHkdaMmiHzGaUpcqH6pfTo
vrf definition 1
 rd 1:1
 address-family ipv4
  route-target export 64530:1
  route-target import 64530:1
  exit-address-family
 !
 address-family ipv6
  exit-address-family
 !
!
vrf definition Mgmt-intf
 rd 1:512
 address-family ipv4
  route-target export 64530:512
  route-target import 64530:512
  exit-address-family
 !
 address-family ipv6
  exit-address-family
 !
!
```

© 2020 Cisco and/or its affiliates. All rights reserved.

```
ip arp proxy disable
no ip finger
no ip rcmd rcp-enable
no ip rcmd rsh-enable
ip as-path access-list 15 permit ^645[2][0-9]$
ip as-path access-list 25 permit .*
no ip dhcp use class
ip host vbond204.cisco.com 52.156.128.118
ip prefix-list GCP_CSR_PREFIX_LIST_POLICY seq 5 permit 10.52.0.199/32
ip bootp server
no ip source-route
no ip http server
no ip http secure-server
ip nat settings central-policy
cdp run
interface GigabitEthernet1
 no shutdown
 arp timeout 1200
 ip address dhcp client-id GigabitEthernet1
 no ip redirects
 ip dhcp client default-router distance 1
 ip mtu    1500
 load-interval 30
 mtu           1500
 negotiation auto
exit
interface GigabitEthernet2
 no shutdown
 arp timeout 1200
 vrf forwarding 1
 ip address 10.52.0.167 255.255.255.224
 no ip redirects
 ip mtu    1500
 load-interval 30
 mtu           1500
 negotiation auto
exit
interface GigabitEthernet3
 no shutdown
 arp timeout 1200
 ip address 10.52.0.199 255.255.255.224
 no ip redirects
 ip mtu    1500
 load-interval 30
 mtu           1500
 negotiation auto
exit
```

© 2020 Cisco and/or its affiliates. All rights reserved.

```
interface Tunnel1
 no shutdown
 ip unnumbered GigabitEthernet1
 no ip redirects
 ipv6 unnumbered GigabitEthernet1
 no ipv6 redirects
 tunnel source GigabitEthernet1
 tunnel mode sdwan
exit
interface Tunnel3
 no shutdown
 ip unnumbered GigabitEthernet3
 no ip redirects
 ipv6 unnumbered GigabitEthernet3
 no ipv6 redirects
 tunnel source GigabitEthernet3
 tunnel mode sdwan
exit
route-map GCP_CSR_PREFIX_ROUTE_POLICY permit 10
 match ip address prefix-list GCP_CSR_PREFIX_LIST_POLICY
!
route-map GCP_CSR_PREFIX_ROUTE_POLICY deny 65535
!
route-map GCP_CSR_ROUTE_POLICY deny 1
 match as-path 15
!
route-map GCP_CSR_ROUTE_POLICY permit 11
 match as-path 25
!
route-map GCP_CSR_ROUTE_POLICY deny 65535
!
clock timezone UTC 0 0
logging persistent size 104857600 filesize 10485760
logging console
aaa authentication login default local
aaa authorization exec default local
aaa server radius dynamic-author
!
router bgp 64530
 bgp log-neighbor-changes
 neighbor 10.52.0.194 remote-as 64521
 neighbor 10.52.0.194 ebgp-multihop 255
 neighbor 10.52.0.195 remote-as 64521
 neighbor 10.52.0.195 ebgp-multihop 255
 neighbor 10.52.0.196 remote-as 64521
 neighbor 10.52.0.196 ebgp-multihop 255
 neighbor 10.52.0.197 remote-as 64521
```

© 2020 Cisco and/or its affiliates. All rights reserved.

```
 neighbor 10.52.0.197 ebgp-multihop 255
 address-family ipv4 unicast vrf 1
  distance bgp 20 200 20
  neighbor 10.52.0.162 remote-as 64520
  neighbor 10.52.0.162 activate
  neighbor 10.52.0.162 ebgp-multihop 255
  neighbor 10.52.0.162 route-map GCP_CSR_ROUTE_POLICY out
  neighbor 10.52.0.162 send-community both
  neighbor 10.52.0.163 remote-as 64520
  neighbor 10.52.0.163 activate
  neighbor 10.52.0.163 ebgp-multihop 255
  neighbor 10.52.0.163 route-map GCP_CSR_ROUTE_POLICY out
  neighbor 10.52.0.163 send-community both
  neighbor 10.52.0.164 remote-as 64520
  neighbor 10.52.0.164 activate
  neighbor 10.52.0.164 ebgp-multihop 255
  neighbor 10.52.0.164 route-map GCP_CSR_ROUTE_POLICY out
  neighbor 10.52.0.164 send-community both
  neighbor 10.52.0.165 remote-as 64520
  neighbor 10.52.0.165 activate
  neighbor 10.52.0.165 ebgp-multihop 255
  neighbor 10.52.0.165 route-map GCP_CSR_ROUTE_POLICY out
  neighbor 10.52.0.165 send-community both
  propagate-aspath
  redistribute omp
  exit-address-family
 !
 address-family ipv4 unicast
  distance bgp 20 200 20
  neighbor 10.52.0.194 activate
  neighbor 10.52.0.194 route-map GCP_CSR_ROUTE_POLICY out
  neighbor 10.52.0.194 send-community both
  neighbor 10.52.0.195 activate
  neighbor 10.52.0.195 route-map GCP_CSR_ROUTE_POLICY out
  neighbor 10.52.0.195 send-community both
  neighbor 10.52.0.196 activate
  neighbor 10.52.0.196 route-map GCP_CSR_ROUTE_POLICY out
  neighbor 10.52.0.196 send-community both
  neighbor 10.52.0.197 activate
  neighbor 10.52.0.197 route-map GCP_CSR_ROUTE_POLICY out
  neighbor 10.52.0.197 send-community both
  redistribute connected
  redistribute connected route-map GCP_CSR_PREFIX_ROUTE_POLICY
  exit-address-family
 !
 timers bgp 60 180
!
```

© 2020 Cisco and/or its affiliates. All rights reserved.

```
snmp-server ifindex persist
line aux 0
 stopbits 1
!
line con 0
 speed    19200
 stopbits 1
!
line vty 0 4
 transport input ssh
!
line vty 5 80
 transport input ssh
!
lldp run
nat64 translation timeout tcp 60
nat64 translation timeout udp 1
sdwan
 interface GigabitEthernet1
  tunnel-interface
   encapsulation ipsec weight 1
   no border
   color biz-internet
   no last-resort-circuit
   no low-bandwidth-link
   no vbond-as-stun-server
   vmanage-connection-preference 5
   port-hop
   carrier                        default
   nat-refresh-interval           5
   hello-interval                 1000
   hello-tolerance                12
   allow-service all
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   allow-service sshd
   no allow-service netconf
   no allow-service ntp
   no allow-service ospf
   no allow-service stun
   allow-service https
   no allow-service snmp
   no allow-service bfd
  exit
 exit
```

© 2020 Cisco and/or its affiliates. All rights reserved.

```
interface GigabitEthernet3
 tunnel-interface
  encapsulation ipsec weight 1
  no border
  color private1
  no last-resort-circuit
  no low-bandwidth-link
  max-control-connections       0
  no vbond-as-stun-server
  vmanage-connection-preference 0
  port-hop
  carrier                       default
  nat-refresh-interval          5
  hello-interval                1000
  hello-tolerance               12
  allow-service all
  allow-service bgp
  no allow-service dhcp
  allow-service dns
  allow-service icmp
  allow-service sshd
  no allow-service netconf
  no allow-service ntp
  no allow-service ospf
  no allow-service stun
  allow-service https
  no allow-service snmp
  no allow-service bfd
 exit
exit
appqoe
 no tcpopt enable
 no dreopt enable
!
omp
 no shutdown
 send-path-limit  4
 ecmp-limit       4
 graceful-restart
 no as-dot-notation
 timers
  holdtime               60
  advertisement-interval 1
  graceful-restart-timer 43200
  eor-timer              300
 exit
 address-family ipv4
```

© 2020 Cisco and/or its affiliates. All rights reserved.

```
   advertise bgp
   advertise connected
   advertise static
  !
  address-family ipv6
   advertise bgp
   advertise connected
   advertise static
  !
 !
!
licensing config enable false
licensing config privacy hostname false
licensing config privacy version false
licensing config utility utility-enable false
bfd color lte
 hello-interval 1000
 no pmtu-discovery
 multiplier     1
!
bfd default-dscp 48
bfd app-route multiplier 2
bfd app-route poll-interval 123400
security
 ipsec
  rekey               86400
  replay-window       512
  authentication-type ah-sha1-hmac sha1-hmac
 !
!
sslproxy
 no enable
 rsa-key-modulus      2048
 certificate-lifetime 730
 eckey-type           P256
 ca-tp-label          PROXY-SIGNING-CA
 settings expired-certificate  drop
 settings untrusted-certificate drop
 settings unknown-status       drop
 settings certificate-revocation-check none
 settings unsupported-protocol-versions drop
 settings unsupported-cipher-suites drop
 settings failure-mode         close
 settings minimum-tls-ver      TLSv1
 dual-side optimization enable
!
policy
```

© 2020 Cisco and/or its affiliates. All rights reserved.

```
 no app-visibility
 no app-visibility-ipv6
 no flow-visibility
 no flow-visibility-ipv6
 no implicit-acl-logging
 log-frequency        1000
!
```

Appendix D: Glossary

VPN	Virtual Private Network
CGW	Cloud Gateway
VPC	Virtual Private Cloud
WAN	Wide Area Network
DNS	Domain Name Server
GW	Gateway
VM	Virtual Machine

Feedback

For comments and suggestions about this guide and related guides, join the discussion on Cisco Community at https://cs.co/en-cvds.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2020 Cisco and/or its affiliates. All rights reserved.