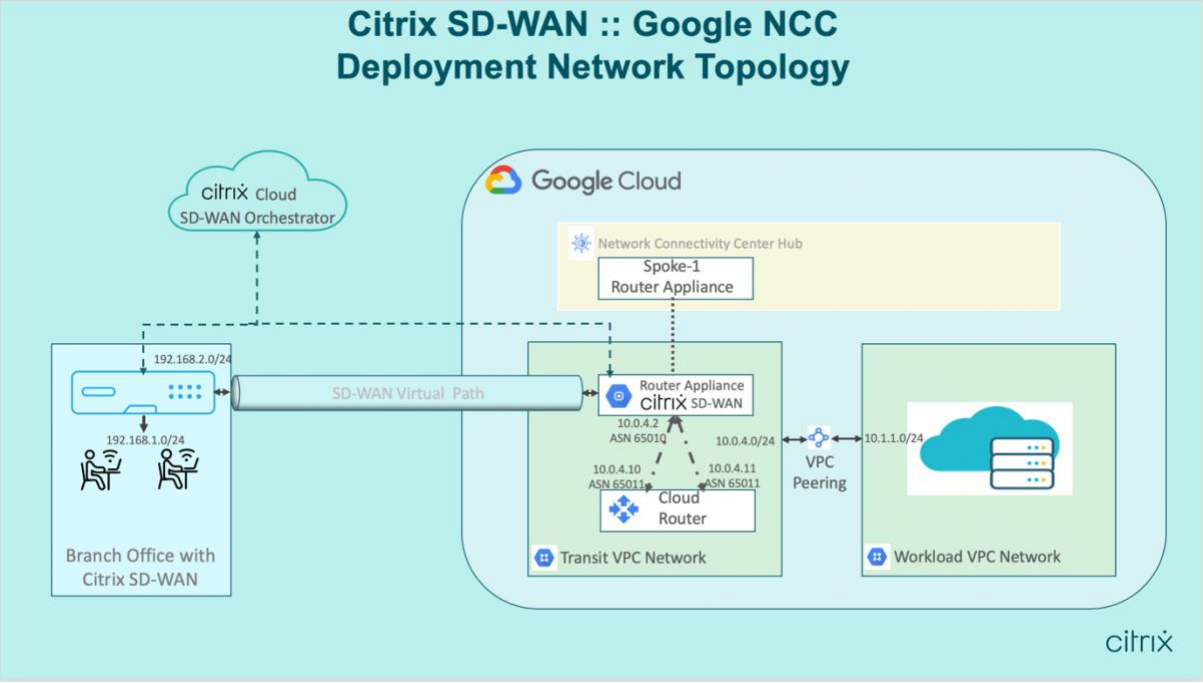
Citrix SD-WAN for Google Network Connectivity Center: Deployment Guide

Google Network Connectivity Center (NCC) provides a mechanism for enterprises to connect On-premises, Virtual Private Clouds (VPCs) on Google Cloud, and other enterprise networks and manage them as spokes to a centralized logical hub on Google Cloud.

Citrix SD-WAN's integration with Google NCC provides a fast, secure and resilient on-ramp for organizations to connect and migrate data from their branch offices, remote sites and on-premise networks to Google Cloud. In addition, enterprises can now leverage Google's high-speed internet backbone to connect to workloads as well as other branch offices.

The guide below describes the configuration and procedure to integrate Citrix SD-WAN with Google NCC, and achieve *branch-to-cloud* connectivity.

Reference Architecture



Pre-Requisites

Before going into the Procedure section, please ensure the following.

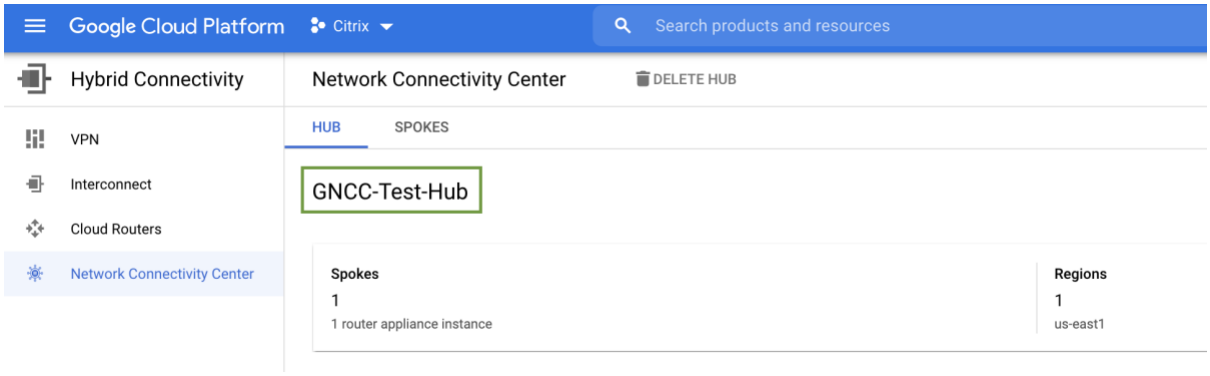
1. You have Citrix Cloud and Google Cloud accounts.
2. You have onboarded the Citrix Orchestrator service.
3. You have an SD-WAN VPX license to run on the cloud.

Procedure

1. **Create Network Connectivity Center Hub**

- Create Network Connectivity Center Hub using **gcloud CLI** as shown below using Google Cloud shell Terminal. The gcloud command-line is a tool to create and manage Google Cloud resources. You can run it in the cloud console by clicking on “Activate Cloud Shell”.

[redacted]~ *(citrix-master-project)$ gcloud alpha network-connectivity hubs create GNCC-Test-Hub*
Create request issued for: [GNCC-Test-Hub]
Waiting for operation [projects/citrix-master-project/locations/global/operations/operation-1632139937989-5cc6c313a4389-1306d426-957f557f] to c
omplete...done.
Created hub [GNCC-Test-Hub].
[redacted]~ *(citrix-master-project)$*



- The hub can also be created in the UI by navigating to “Hybrid Connectivity > **Network Connectivity Center** > Hub” section (as shown in the screenshot above).

2. **Create SD-WAN instance (Router Appliance)**

- Create SD-WAN Instance on Google Cloud Platform by going through https://docs.citrix.com/en-us/citrix-sd-wan-platforms/vpx-models/vpx-se/install-sd-wan-vpx-gcp.html

- Check the SD-WAN instance (Router Appliance) running status on Google cloud platform as shown below.

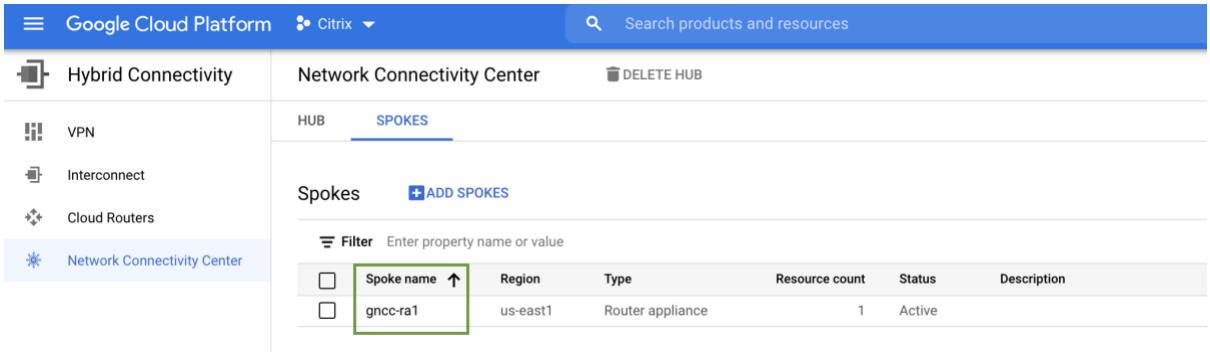
[redacted]~ *(citrix-master-project)$ gcloud compute instances list --filter="zone us-east1-b"*
NAME: ***citrix-sdwan-instance***
ZONE: us-east1-b
MACHINE_TYPE: n1-standard-4
PREEMPTIBLE:

*INTERNAL_IP: 10.142.15.196,**10.0.4.2**,10.0.3.2*
EXTERNAL_IP: 34.139.71.108,35.231.153.54
STATUS: RUNNING
NAME: gncc-workload-windows-server
ZONE: us-east1-b
MACHINE_TYPE: e2-micro
PREEMPTIBLE:
INTERNAL_IP: 10.1.1.2
EXTERNAL_IP: 34.75.89.26
STATUS: RUNNING
[redacted]*~ (citrix-master-project)$*

3. Add Router Appliance as Spoke to NCC Hub

- Configure the Router Appliance(Citrix SD-WAN) as a Spoke to the NCC Hub using gcloud CLI as shown below using Google Cloud shell Terminal.

[redacted]*~ (citrix-master-project)$ gcloud alpha network-connectivity spokes create **gncc-ra1** --hub=https://networkconnectivity.googleapis.com/v1alpha1/projects/839919413162/locations/global/hubs/**GNCC-Test-Hub** --router-appliance=instance=https://www.googleapis.com/compute/v1alpha1/projects/839919413162/zones/us-east1-b/instances/**citrix-sdwan-instance**,ip=**10.0.4.2** --region=us-east1*
*Create request issued for: [**gncc-ra1**]*
Waiting for operation [projects/citrix-master-project/locations/us-east1/operations/operation-1632140692974-5cc6c5e3a6d26-42115463-dd6f98fd] to complete...done.
Created spoke [gncc-ra1].
[redacted]*~ (citrix-master-project)$*



- Alternatively, the Spoke can be attached to the Hub in the UI by going to “Hybrid Connectivity > Network Connectivity Center > Spoke” section as shown in the screenshot above.

4. Create Cloud Router

- Create the Cloud Router using gcloud CLI as shown below using Google Cloud shell Terminal.
  As part of this we need to take care of configuring the appropriate BGP ASN Number.

[redacted]~ *(citrix-master-project)$ gcloud beta compute routers create* ***gncc-cr*** *--region us-east1 --network* ***gncc-sdwan-lan --asn 65011***
Creating router [gncc-cr]...done.
NAME: ***gncc-cr***
REGION: us-east1
NETWORK: ***gncc-sdwan-lan***
[redacted]~ *(citrix-master-project)$*

5. Add Interfaces to Cloud Router

- The Cloud Router can be configured with two network Interfaces. This is to provide Redundancy.

- Use the "--redundant-interface" option while creating the second interface.

[redacted]~ *(citrix-master-project)$ gcloud beta compute routers add-interface* ***gncc-cr*** *--interface-name=****gncc-cr-0*** *--subnetwork=****gncc-sdwan-lan-subnet*** *--region=us-east1 --ip-address=****10.0.4.10***
Updated [https://www.googleapis.com/compute/beta/projects/citrix-master-project/regions/us-east1/routers/gncc-cr].
[redacted]~ *(citrix-master-project)$*
[redacted]~ *(citrix-master-project)$*
[redacted]~ *(citrix-master-project)$ gcloud beta compute routers add-interface gncc-cr --interface-name=****gncc-cr-1 --redundant-interface=gncc-cr-0*** *--subnetwork=gncc-sdwan-lan-subnet --region=us-east1 --ip-address=****10.0.4.11***
Updated [https://www.googleapis.com/compute/beta/projects/citrix-master-project/regions/us-east1/routers/gncc-cr].
[redacted]~ *(citrix-master-project)$*
[redacted]~ *(citrix-master-project)$*

Note 1: **We cannot have these two interfaces as part of different subnetworks.**

Note 2: **The Cloud Router interface information is not accessible on the GCP console. You can use the gcloud CLI's as shown below.**

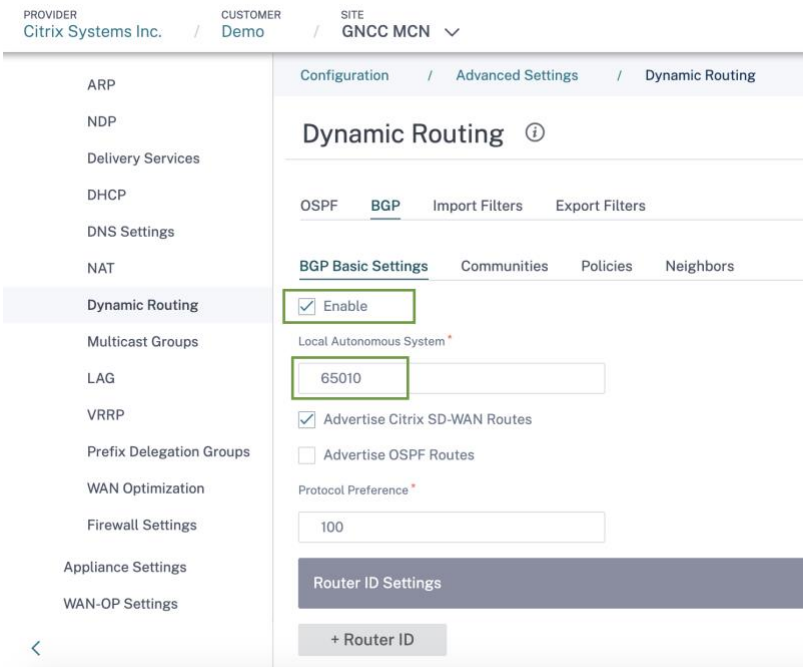
[redacted]~ *(citrix-master-project)$ gcloud beta compute routers describe gncc-cr --region us-east1*

----
interfaces:
- ipRange: 10.0.4.10/24
name: gncc-cr-0

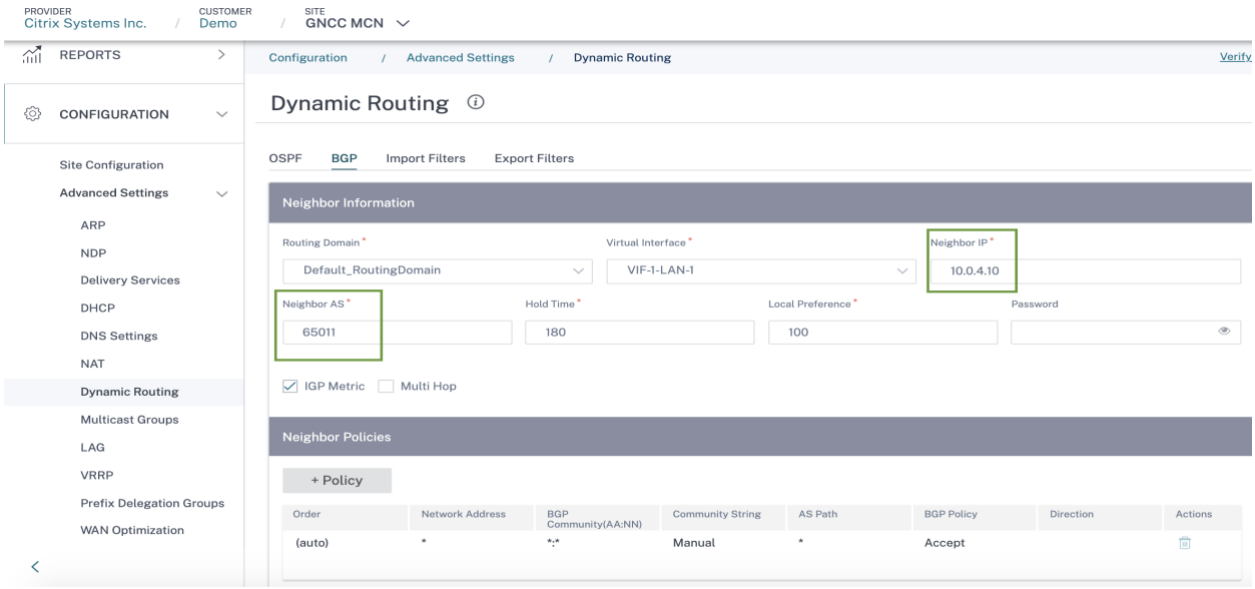
privateIpAddress: 10.0.4.10
redundantInterface: gncc-cr-1
subnetwork: https://www.googleapis.com/compute/beta/projects/citrix-master-project/regions/us-east1/subnetworks/gncc-sdwan-lan-subnet
- ipRange: 10.0.4.11/24
name: gncc-cr-1
privateIpAddress: 10.0.4.11
redundantInterface: gncc-cr-0
subnetwork: https://www.googleapis.com/compute/beta/projects/citrix-master-project/regions/us-east1/subnetworks/gncc-sdwan-lan-subnet
kind: compute#router
name: gncc-cr
network: https://www.googleapis.com/compute/beta/projects/citrix-master-project/global/networks/gncc-sdwan-lan
region: https://www.googleapis.com/compute/beta/projects/citrix-master-project/regions/us-east1
selfLink: https://www.googleapis.com/compute/beta/projects/citrix-master-project/regions/us-east1/routers/gncc-cr
[redacted]*~ (citrix-master-project)$*

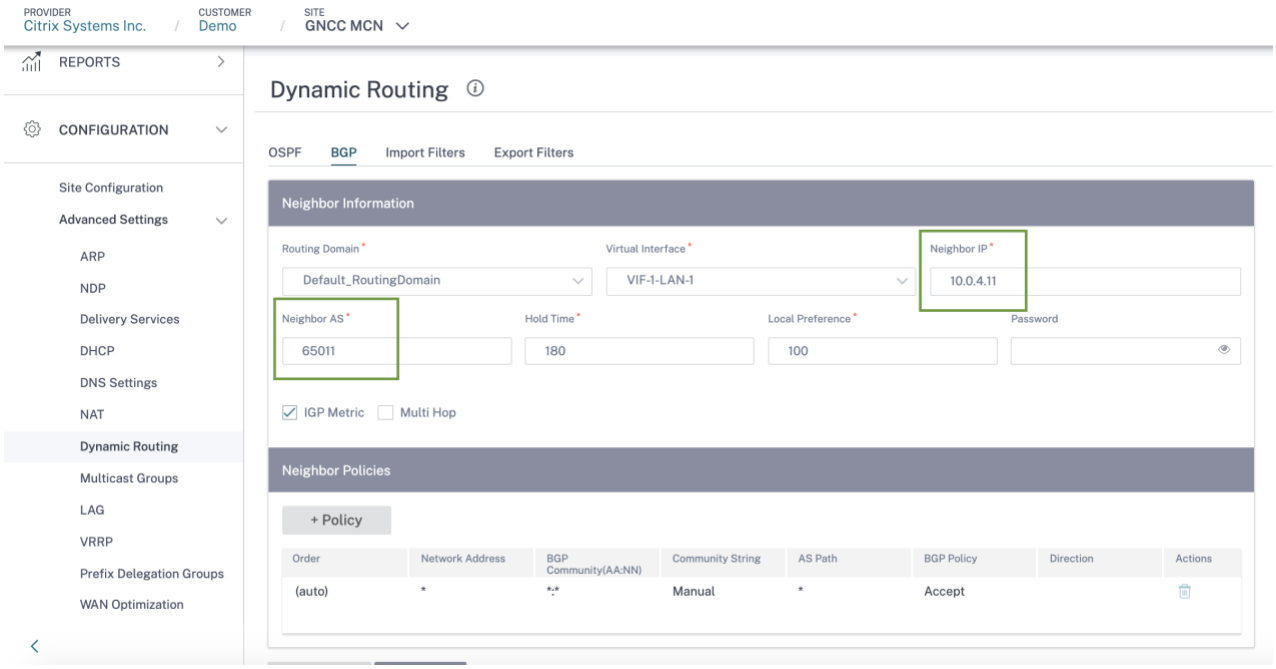
6. Configure BGP on SD-WAN Appliance (Router Appliance)

- Enable BGP on SD-WAN Router appliance as shown below.

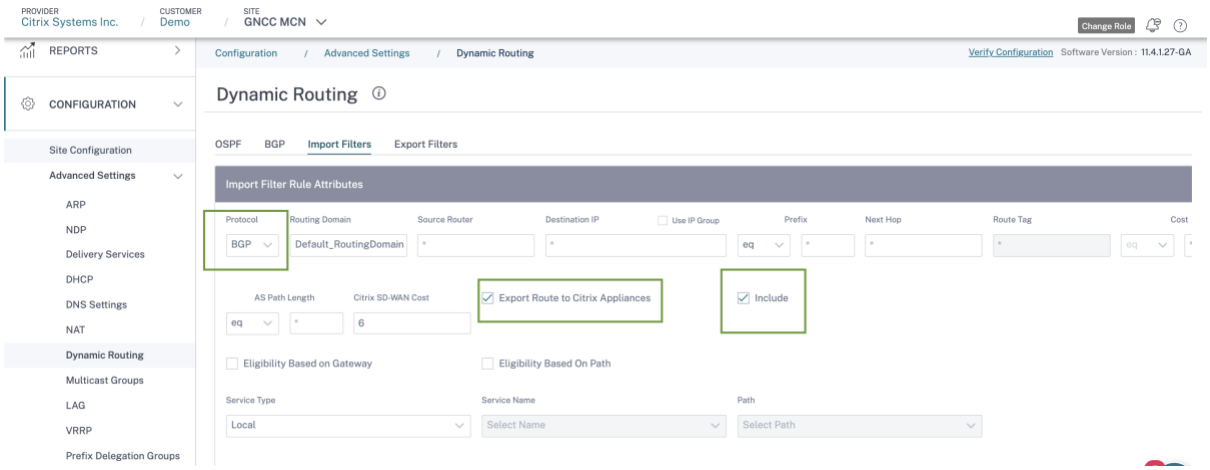


- Configure two BGP Peers pointing to two separate interfaces (10.0.4.10 and 10.0.4.11) of the Cloud Router as show below.





- Configure Import filters to import BGP learnt routes from the Cloud Router onto the SD-WAN routing table (see snapshot below).



7. Add BGP Peer to Cloud Router

- Add BGP Peer to Cloud Router using gcloud CLI as shown below using Google Cloud shell Terminal.

- Add BGP Peer using interface “gncc-cr-0”

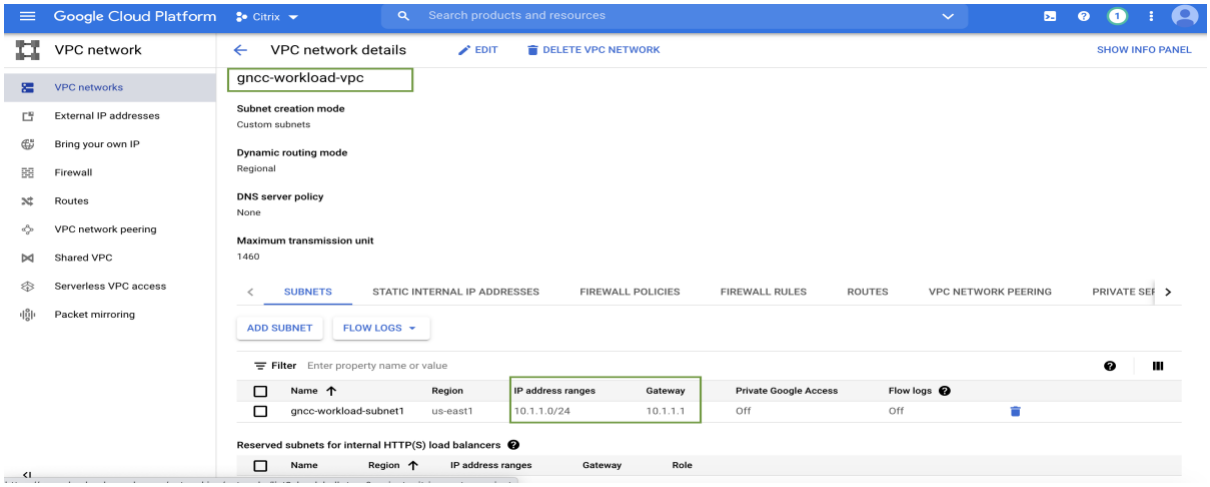
  *gcloud beta compute routers add-bgp-peer gncc-cr --peer-name **gncc-ra1-peer1** --interface=**gncc-cr-0** --peer-ip-address=**10.0.4.2** --peer-asn=**65010** --instance=citrix-sdwan-instance --instance-zone=us-east1-b --region=us-east1*

- Add BGP Peer using interface “gncc-cr-1”

  *gcloud beta compute routers add-bgp-peer gncc-cr --peer-name **gncc-ra1-peer2** --interface=**gncc-cr-1** --peer-ip-address=**10.0.4.2** --peer-asn=**65010** --instance=citrix-sdwan-instance --instance-zone=us-east1-b --region=us-east1*

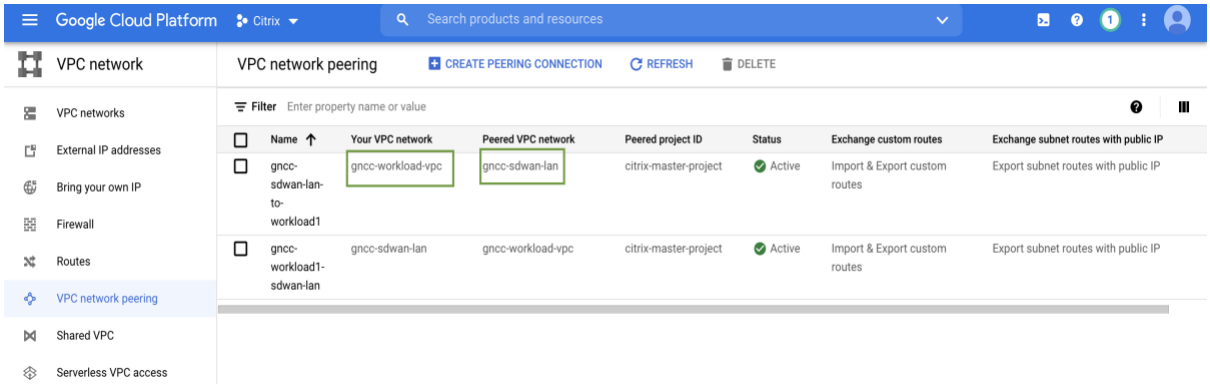
8. Add Workload VPC and Peer with Transit VPC

- Add workload VPC (10.1.1.0/24), host a windows server and run a HTTP server on that machine.



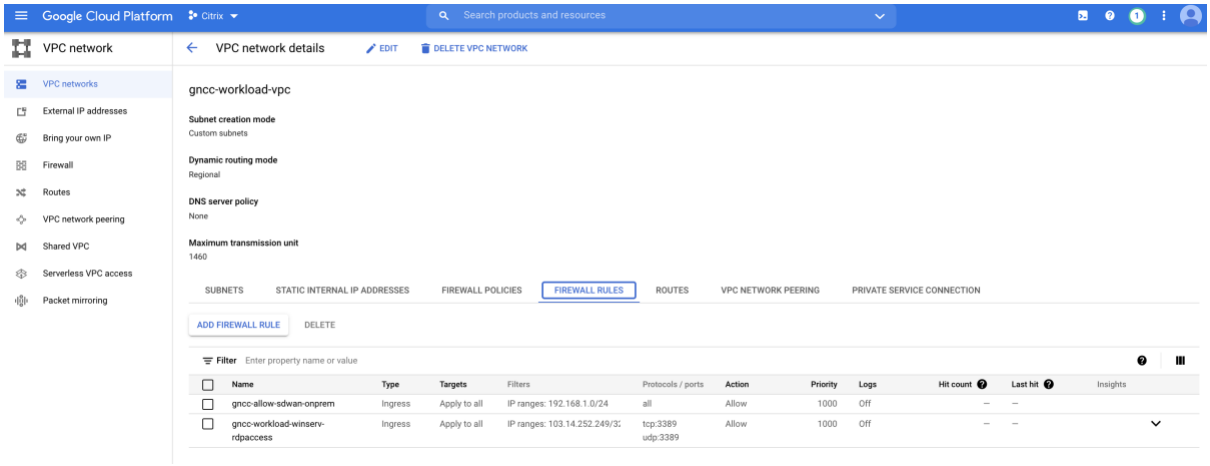
9. Add Workload VPC and Peer with Transit VPC

- Configure VPC peering between Work Load VPC and Transit VPC (Cloud Router/Router Appliance VPC).

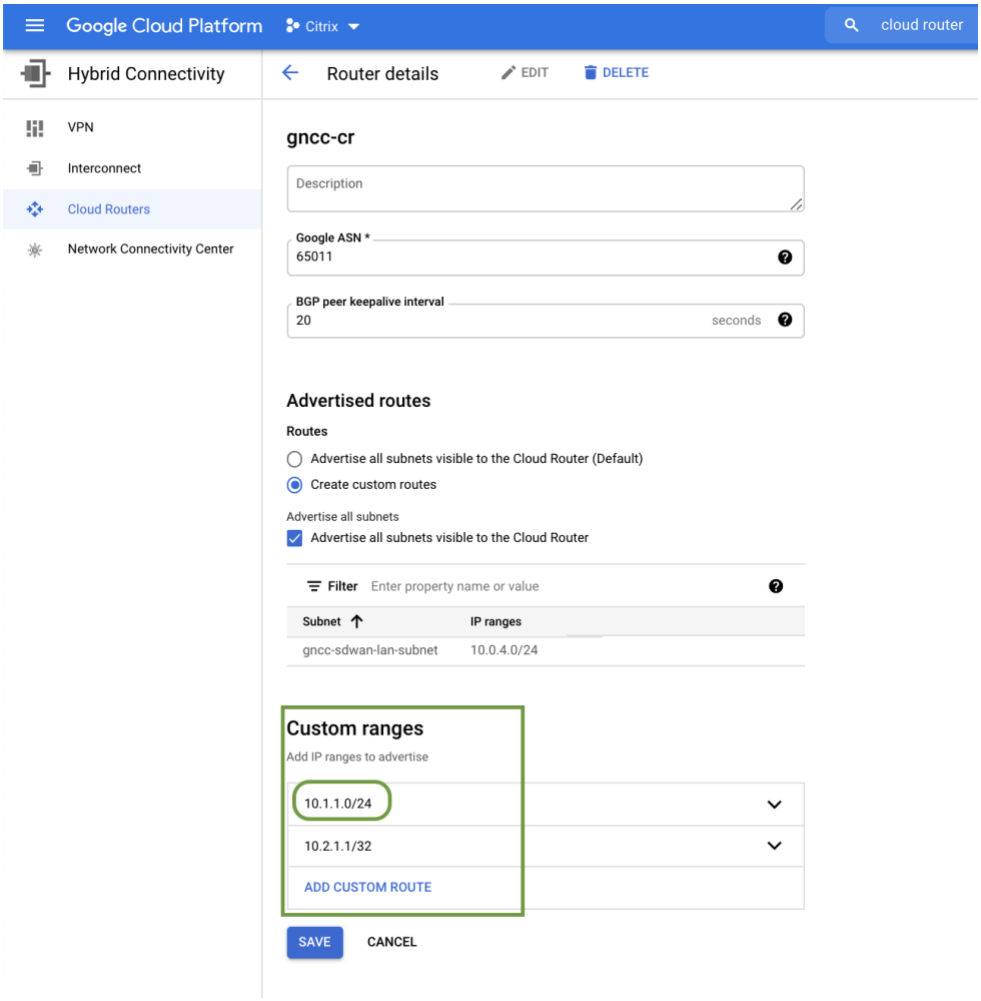


- Configure Firewall policies to allow inbound traffic from the On-prem branch network, and associate to Workload VPC.

- Also configure Firewall policy to allow RDP access to the Windows server hosted.



Note: In order for the Cloud router to advertise workload VPC networks to SD-WAN BGP peer, we need to add custom routes on the Cloud router at the moment. (**This will eventually be automated**).



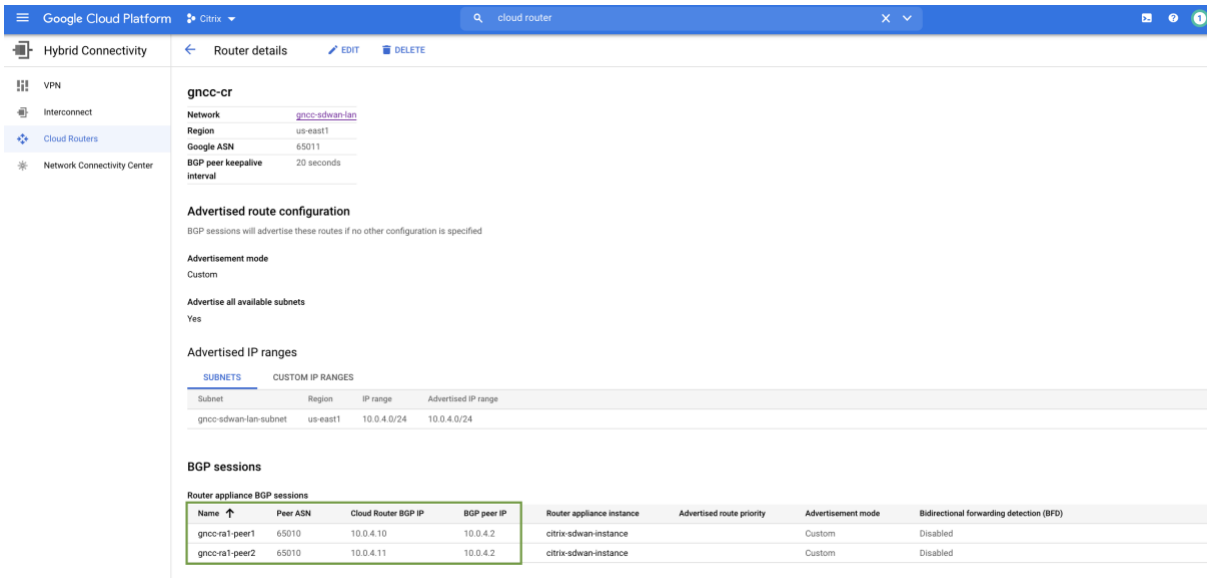
10. Monitor BGP Peering and Routes on the Cloud Router

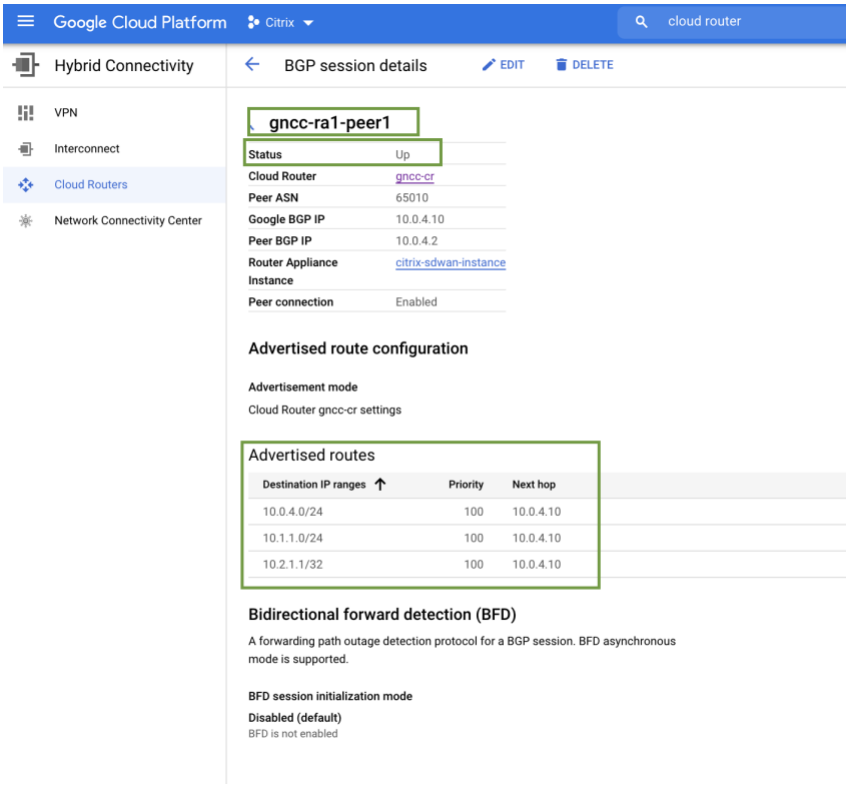
- Validation on GCP: On GCP, we can check for the networks advertised using the CLI input mentioned below.

[redacted]~ *(citrix-master-project)$ gcloud beta compute routers describe gncc-cr --region us-east1*

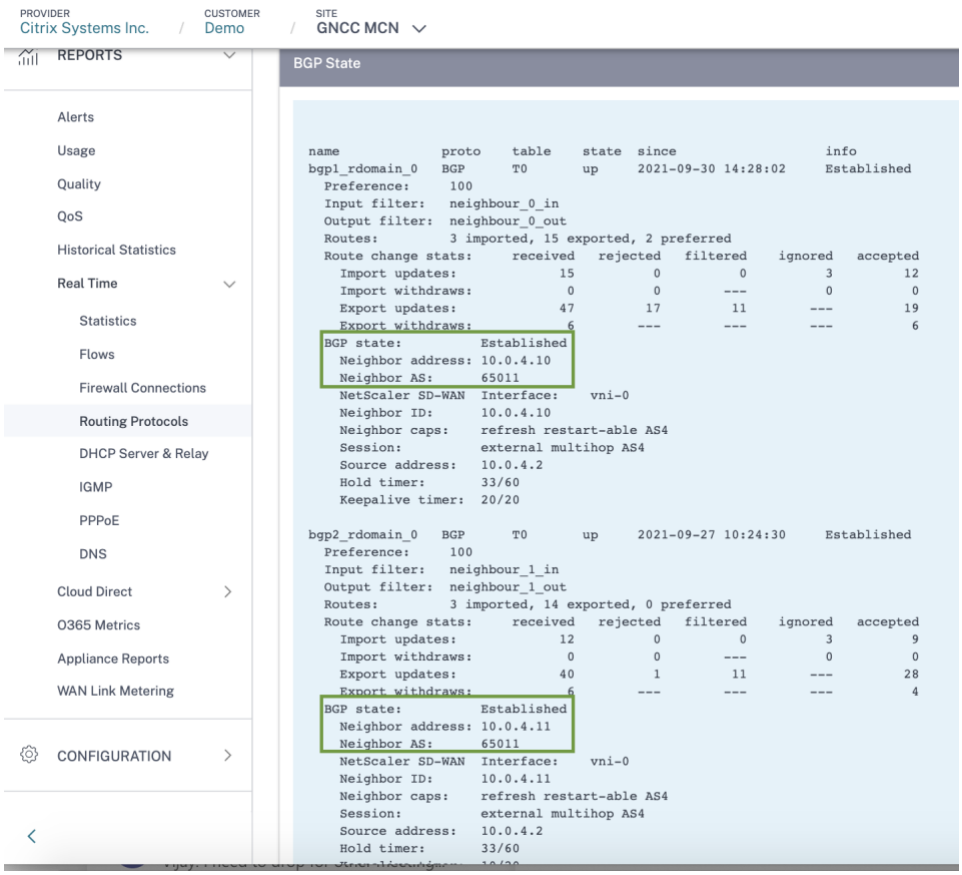
```
bgp:
  advertiseMode: CUSTOM
  advertisedGroups:
  - ALL_SUBNETS
  advertisedIpRanges:
  - description: ''
    range: 10.1.1.0/24
  - description: ''
    range: 10.2.1.1/32
  asn: 65011
  keepaliveInterval: 20
bgpPeers:
- bfd:
    minReceiveInterval: 1000
    minTransmitInterval: 1000
    multiplier: 5
    sessionInitializationMode: DISABLED
  enable: 'TRUE'
  interfaceName: gncc-cr-0
  ipAddress: 10.0.4.10
  name: gncc-ra1-peer1
  ..................
  ..........................
```

- **Validation on GCP:** BGP Peer status and networks advertised can also be checked as shown below.

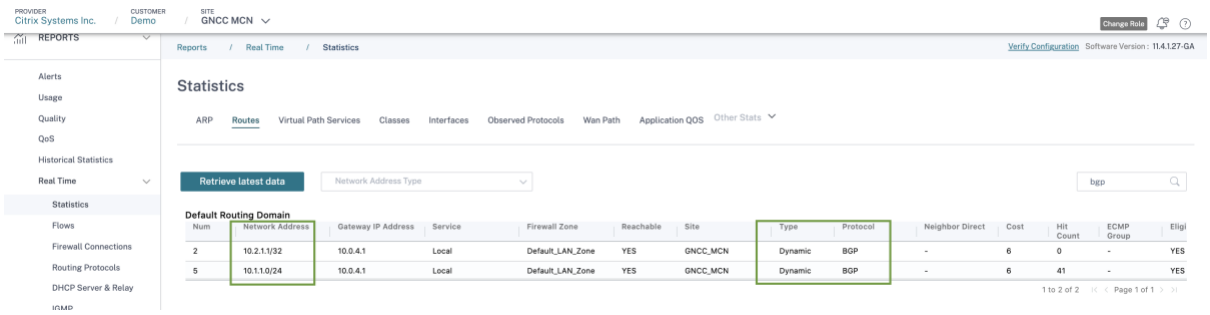




- **Validation on Citrix SD-WAN (Router Appliance):** We can validate the BGP status on Citrix SD-WAN as shown below.

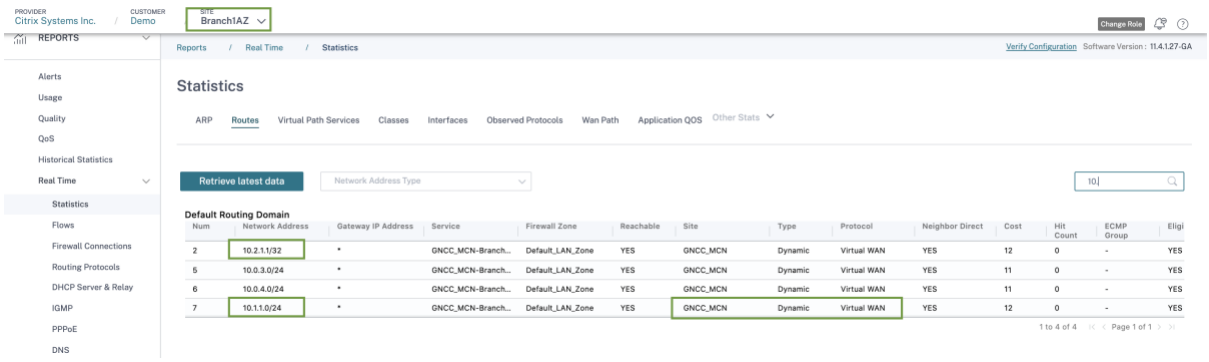


- Routes learnt over BGP can be seen as shown below.



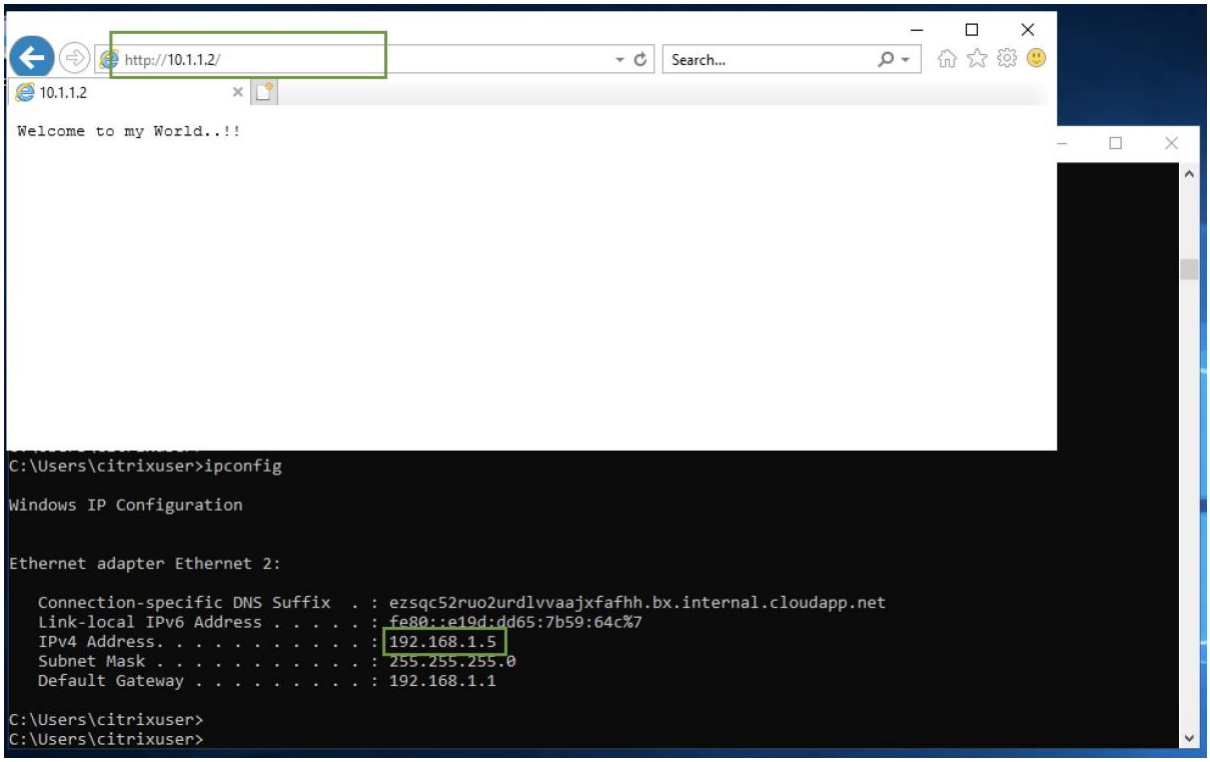
- **Validation on Citrix SD-WAN OnPrem Branch:** GCP Workload VPC networks that are learnt by the Router Appliance (SD-WAN appliance on GCP) will be sent to the on-prem and other connected SD-WAN sites over the SD-WAN overlay network.

- The same routes can be validated on the on-prem SD-WAN branch site as shown below.



11. Access services on the Workload VPC from the On-prem site

- Since we are able to learn the Workload VPC network on the on-prem site, try accessing the http application from the Branch LAN Host. You should be able to access.



- We can monitor the same connection in the *Firewall connections* section of the branch site where we can expect the Source IP to be the LAN network of Branch SD-WAN and the Destination IP address to be the Workload server IP.