

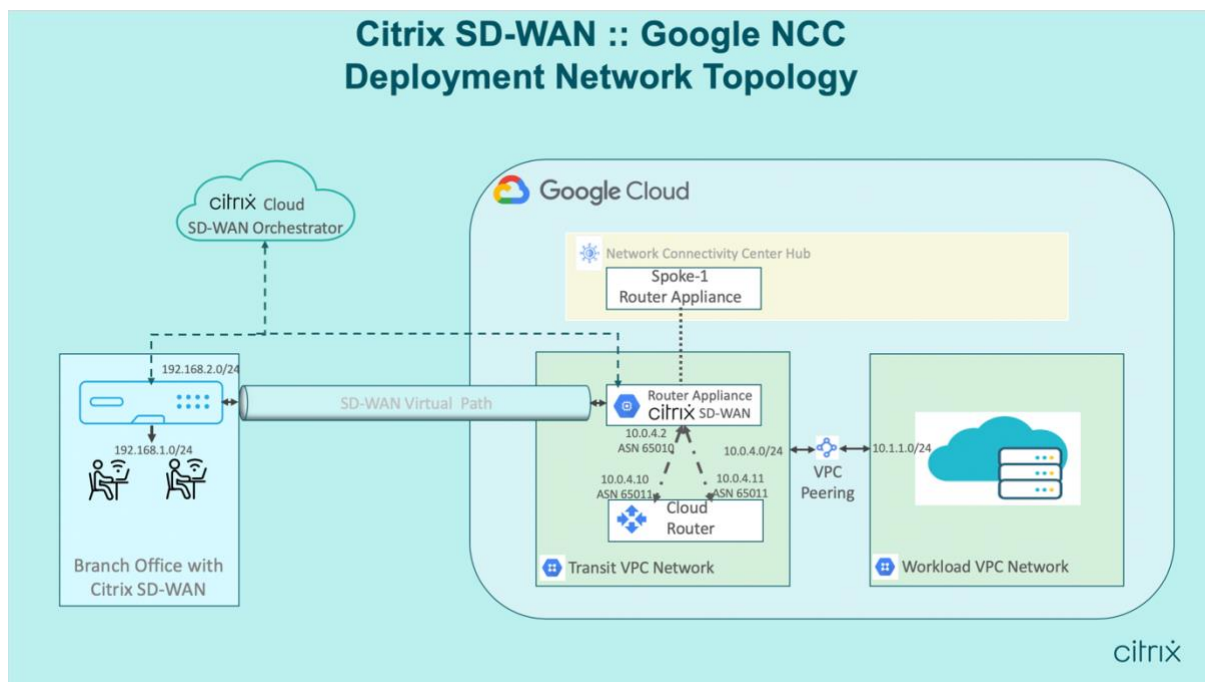
## Citrix SD-WAN for Google Network Connectivity Center: Deployment Guide

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.

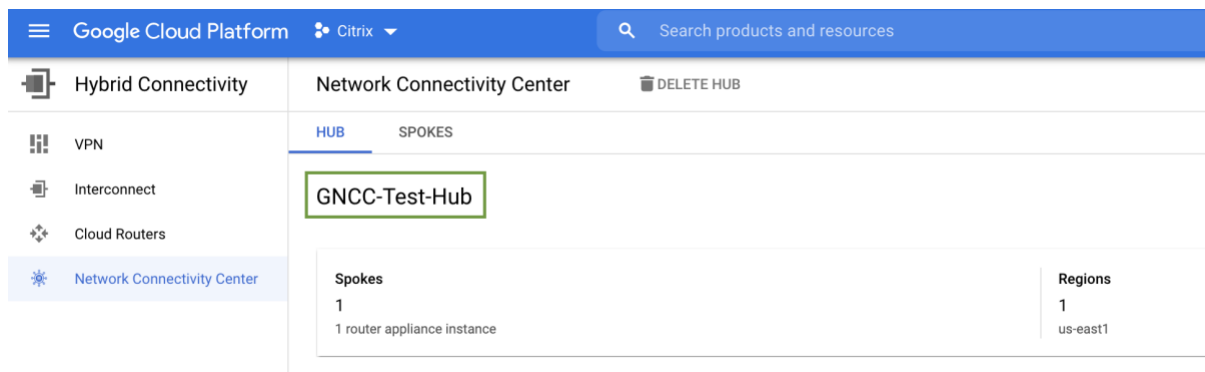
1. You have Citrix Cloud and Google Cloud accounts.
2. You have onboarded the Citrix Orchestrator service.
3. You have an SD-WAN VPX license to run on the cloud.

## 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”.

```
~ (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].
~ (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.

```
~ (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/g
lobal/hubs/GNCC-Test-Hub --router-
appliance=instance=https://www.googleapis.com/compute/v1alpha1/projects/839919413162/z
ones/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)$
```

The screenshot shows the Google Cloud Platform console interface. The left sidebar contains navigation options: Hybrid Connectivity, VPN, Interconnect, Cloud Routers, and Network Connectivity Center (selected). The main content area is titled 'Network Connectivity Center' and includes a 'DELETE HUB' button. Below this, there are tabs for 'HUB' and 'SPOKES', with 'SPOKES' being the active tab. A '+ ADD SPOKES' button is visible. A filter bar is present above a table of spokes. The table has columns for 'Spoke name', 'Region', 'Type', 'Resource count', 'Status', and 'Description'. One spoke is listed: 'gncc-ra1' in the 'us-east1' region, of type 'Router appliance', with a resource count of 1 and an 'Active' status. The 'Spoke name' column header and the 'gncc-ra1' row are highlighted with a green box.

Spoke name	Region	Type	Resource count	Status	Description
gncc-ra1	us-east1	Router appliance	1	Active	

- 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.

```
~ (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
~ (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.

```
~ (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].
~ (citrix-master-project)$
~ (citrix-master-project)$
~ (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].
~ (citrix-master-project)$
~ (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.

```
~ (citrix-master-project)$ gcloud beta compute routers describe
gncc-cr --region us-east1
----
----
interfaces:
- ipRange: 10.0.4.10/24
  name: gncc-cr-0
```



PROVIDER Citrix Systems Inc. / CUSTOMER Demo / SITE GNCC MCN

REPORTS > CONFIGURATION > Dynamic Routing

### Dynamic Routing

OSPF BGP Import Filters Export Filters

**Neighbor Information**

Routing Domain: Default\_RoutingDomain Virtual Interface: VIF-1-LAN-1 Neighbor IP: 10.0.4.10

Neighbor AS: 65011 Hold Time: 180 Local Preference: 100 Password: [ ]

IGP Metric  Multi Hop

**Neighbor Policies**

+ Policy

Order	Network Address	BGP Community(AA:NN)	Community String	AS Path	BGP Policy	Direction	Actions
(auto)	*	*:*	Manual	*	Accept		[ ]

PROVIDER Citrix Systems Inc. / CUSTOMER Demo / SITE GNCC MCN

REPORTS > CONFIGURATION > Dynamic Routing

### Dynamic Routing

OSPF BGP Import Filters Export Filters

**Neighbor Information**

Routing Domain: Default\_RoutingDomain Virtual Interface: VIF-1-LAN-1 Neighbor IP: 10.0.4.11

Neighbor AS: 65011 Hold Time: 180 Local Preference: 100 Password: [ ]

IGP Metric  Multi Hop

**Neighbor Policies**

+ Policy

Order	Network Address	BGP Community(AA:NN)	Community String	AS Path	BGP Policy	Direction	Actions
(auto)	*	*:*	Manual	*	Accept		[ ]

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

PROVIDER Citrix Systems Inc. / CUSTOMER Demo / SITE GNCC MCN

Configuration / Advanced Settings / Dynamic Routing

### Dynamic Routing

OSPF BGP **Import Filters** Export Filters

Import Filter Rule Attributes

Protocol	Routing Domain	Source Router	Destination IP	Use IP Group	Prefix	Next Hop	Route Tag	Cost
BGP	Default_RoutingDomain	*	*	<input type="checkbox"/>	eq	*	*	eq

AS Path Length: eq \* Citrix SD-WAN Cost: 6

Export Route to Citrix Appliances  Include

Eligibility Based on Gateway  Eligibility Based on Path

Service Type: Local Service Name: Select Name Path: Select Path

## 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”

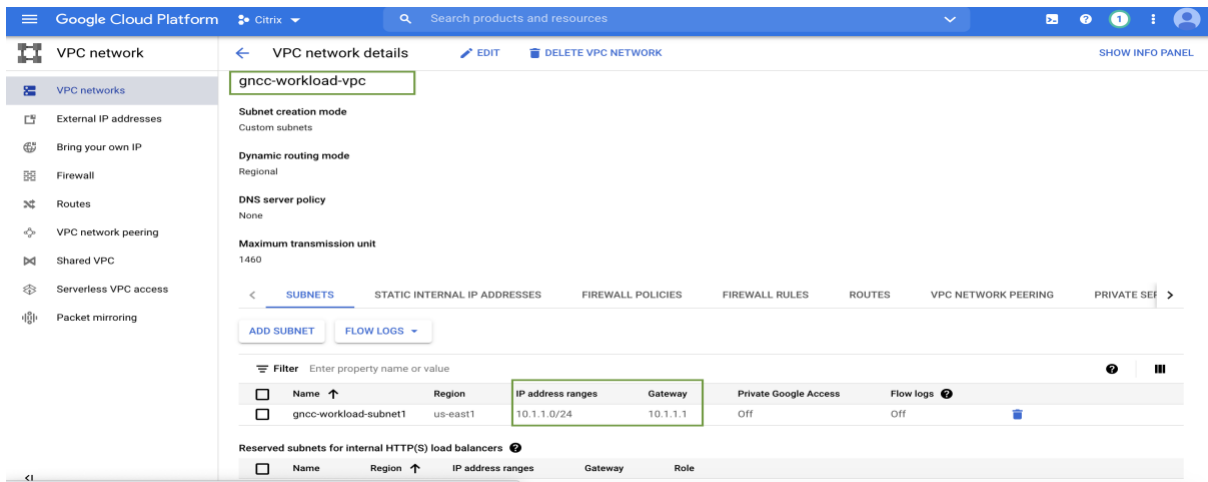
```
gcloud beta compute routers add-bgp-peer gncc-cr --peer-name gncc-ra1-peer1 --
interface=gncc-cr-0 --peer-ip-address=10.0.4.2 --peer-asn=65010 --instance=citrix-sdwan-
instance --instance-zone=us-east1-b --region=us-east1
```

- 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
```

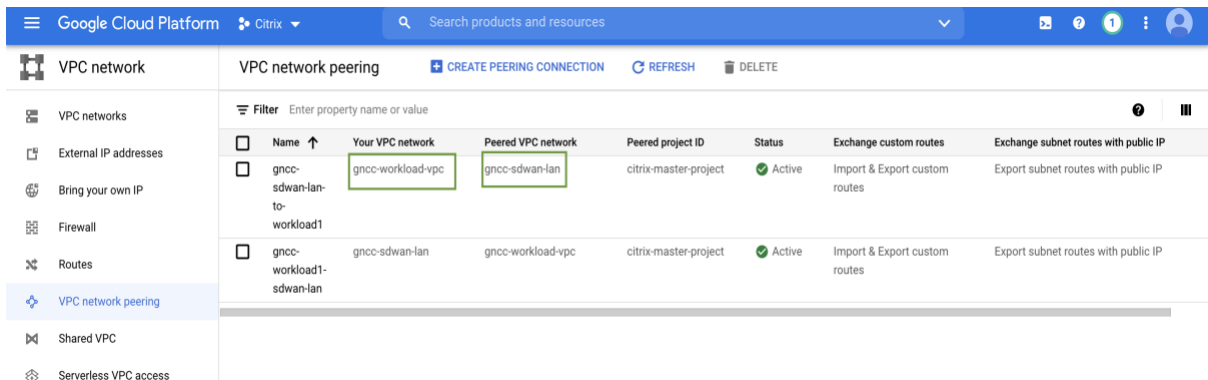
## 8. Add Workload VPC and Peer with Transit VPC

- 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.



Google Cloud Platform | Citrix | Search products and resources

VPC network | VPC network details | EDIT | DELETE VPC NETWORK

gnc-workload-vpc

Subnet creation mode: Custom subnets

Dynamic routing mode: Regional

DNS server policy: None

Maximum transmission unit: 1460

SUBNETS | STATIC INTERNAL IP ADDRESSES | FIREWALL POLICIES | **FIREWALL RULES** | ROUTES | VPC NETWORK PEERING | PRIVATE SERVICE CONNECTION

ADD FIREWALL RULE | DELETE

Filter: Enter property name or value

Name	Type	Targets	Filters	Protocols / ports	Action	Priority	Logs	Hit count	Last hit	Insights
<input type="checkbox"/> gnc-allow-sdwan-onprem	Ingress	Apply to all	IP ranges: 192.168.1.0/24	all	Allow	1000	Off	--	--	
<input type="checkbox"/> gnc-workload-winserv-rdpaccess	Ingress	Apply to all	IP ranges: 103.14.252.249/32	tcp:3389 udp:3389	Allow	1000	Off	--	--	

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).**

Google Cloud Platform | Citrix | cloud router

Hybrid Connectivity | Router details | EDIT | DELETE

gnc-cr

Description:

Google ASN #: 65011

BGP peer keepalive interval: 20 seconds

**Advertised routes**

Routes

Advertise all subnets visible to the Cloud Router (Default)

Create custom routes

Advertise all subnets

Advertise all subnets visible to the Cloud Router

Filter: Enter property name or value

Subnet	IP ranges
gnc-sdwan-lan-subnet	10.0.4.0/24

**Custom ranges**

Add IP ranges to advertise

<input type="text" value="10.1.1.0/24"/>	▼
<input type="text" value="10.2.1.1/32"/>	▼

ADD CUSTOM ROUTE

SAVE | CANCEL

## 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.

```

~ (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.

The screenshot shows the Google Cloud Platform console for a Cloud Router named 'gncc-cr'. The configuration includes:

- Network:** gncc-sdwan-lan
- Region:** us-east1
- Google ASN:** 65011
- BGP peer keepalive interval:** 20 seconds

**Advertised route configuration:**

- Advertisement mode:** Custom
- Advertise all available subnets:** Yes

**Advertised IP ranges:**

Subnet	Region	IP range	Advertised IP range
gncc-sdwan-lan-subnet	us-east1	10.0.4.0/24	10.0.4.0/24

**BGP sessions:**

Name	Peer ASN	Cloud Router BGP IP	BGP peer IP	Router appliance instance	Advertised route priority	Advertisement mode	Bidirectional forwarding detection (BFD)
gncc-ra1-peer1	65010	10.0.4.10	10.0.4.2	citrix-sdwan-instance		Custom	Disabled
gncc-ra1-peer2	65010	10.0.4.11	10.0.4.2	citrix-sdwan-instance		Custom	Disabled

Google Cloud Platform Citrix cloud router

Hybrid Connectivity < BGP session details EDIT DELETE

gncc-ra1-peer1

Status Up

Cloud Router gncc-cr

Peer ASN 65010

Google BGP IP 10.0.4.10

Peer BGP IP 10.0.4.2

Router Appliance Instance citrix-sdwan-instance

Peer connection Enabled

**Advertised route configuration**

Advertisement mode  
Cloud Router gncc-cr settings

**Advertised routes**

Destination IP ranges ↑	Priority	Next hop
10.0.4.0/24	100	10.0.4.10
10.1.1.0/24	100	10.0.4.10
10.2.1.1/32	100	10.0.4.10

**Bidirectional forward detection (BFD)**

A forwarding path outage detection protocol for a BGP session. BFD asynchronous mode is supported.

**BFD session initialization mode**  
Disabled (default)  
BFD is not enabled

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

PROVIDER Citrix Systems Inc. / CUSTOMER Demo / SITE GNCC MCN

REPORTS

- Alerts
- Usage
- Quality
- QoS
- Historical Statistics
- Real Time
  - Statistics
  - Flows
  - Firewall Connections
  - Routing Protocols
  - DHCP Server & Relay
  - IGMP
  - PPPoE
  - DNS
  - Cloud Direct
  - O365 Metrics
  - Appliance Reports
  - WAN Link Metering
- CONFIGURATION

**BGP State**

```

name          proto  table  state  since          info
bgp1_rdomain_0 BGP    T0     up     2021-09-30 14:28:02  Established
Preference:   100
Input filter: neighbour_0_in
Output filter: neighbour_0_out
Routes:       3 imported, 15 exported, 2 preferred
Route change stats: received rejected filtered ignored accepted
Import updates: 15      0      0      3      12
Import withdraws: 0      0      ---    0      0
Export updates: 47     17     11     ---    19
Export withdraws: 6      ---    ---    ---    6
BGP state:    Established
Neighbor address: 10.0.4.10
Neighbor AS:   65011
NetScaler SD-WAN Interface: vni-0
Neighbor ID:   10.0.4.10
Neighbor caps: refresh restart-able AS4
Session:       external multihop AS4
Source address: 10.0.4.2
Hold timer:    33/60
Keepalive timer: 20/20

bgp2_rdomain_0 BGP    T0     up     2021-09-27 10:24:30  Established
Preference:   100
Input filter: neighbour_1_in
Output filter: neighbour_1_out
Routes:       3 imported, 14 exported, 0 preferred
Route change stats: received rejected filtered ignored accepted
Import updates: 12      0      0      3      9
Import withdraws: 0      0      ---    0      0
Export updates: 40     1      11     ---    28
Export withdraws: 6      ---    ---    ---    4
BGP state:    Established
Neighbor address: 10.0.4.11
Neighbor AS:   65011
NetScaler SD-WAN Interface: vni-0
Neighbor ID:   10.0.4.11
Neighbor caps: refresh restart-able AS4
Session:       external multihop AS4
Source address: 10.0.4.2
Hold timer:    33/60
Keepalive timer: 20/20

```

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

The screenshot shows the 'Statistics' page for site 'GNCC\_MCN'. The 'Routes' tab is selected, and a search filter 'bgp' is applied. The table below shows the default routing domain with two BGP routes highlighted in green.

Num	Network Address	Gateway IP Address	Service	Firewall Zone	Reachable	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	ECMP Group	Elig
2	10.2.1/32	10.0.4.1	Local	Default_LAN_Zone	YES	GNCC_MCN	Dynamic	BGP	-	6	0	-	YES
5	10.1.1.0/24	10.0.4.1	Local	Default_LAN_Zone	YES	GNCC_MCN	Dynamic	BGP	-	6	41	-	YES

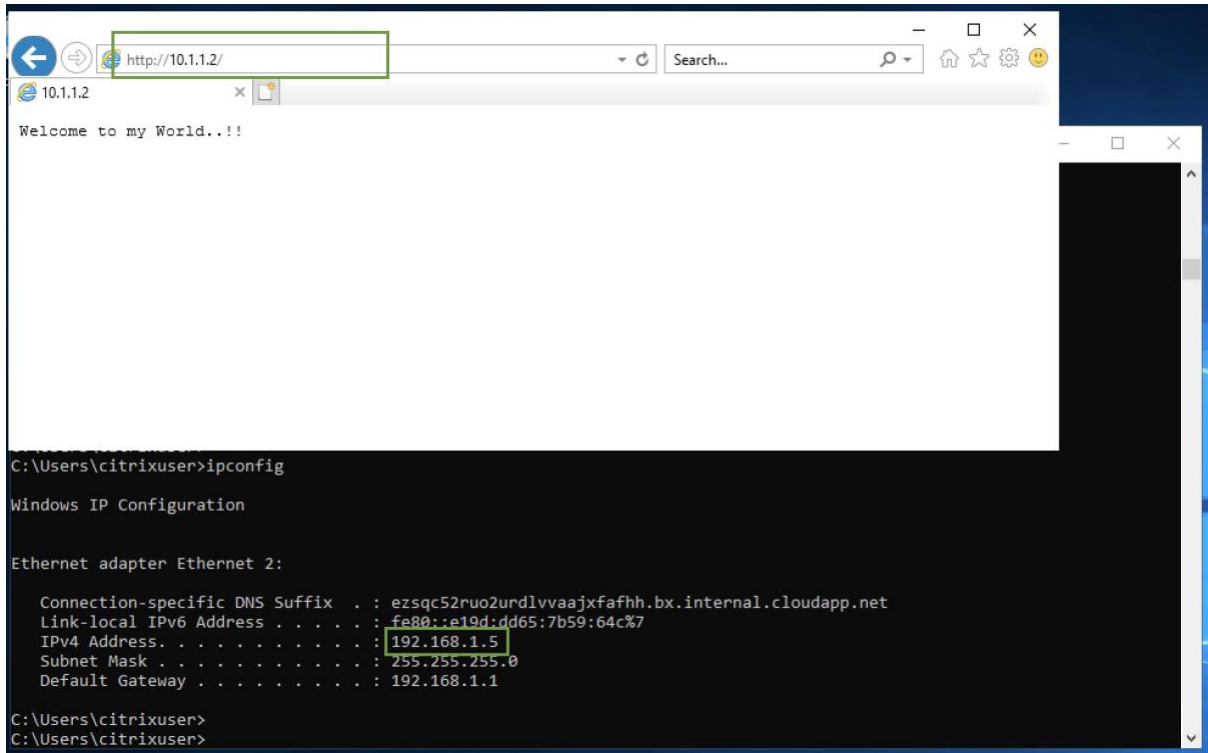
- **Validation on Citrix SD-WAN OnPrem Branch:** GCP Workload VPC networks that are learnt by the Router Appliance (SD-WAN appliance on GCP) will be sent to the on-prem and other connected SD-WAN sites over the SD-WAN overlay network.
- The same routes can be validated on the on-prem SD-WAN branch site as shown below.

The screenshot shows the 'Statistics' page for site 'Branch1AZ'. The 'Routes' tab is selected, and a search filter '10.' is applied. The table below shows the default routing domain with three BGP routes highlighted in green.

Num	Network Address	Gateway IP Address	Service	Firewall Zone	Reachable	Site	Type	Protocol	Neighbor Direct	Cost	Hit Count	ECMP Group	Elig
2	10.2.1/32	*	GNCC_MCN-Branch...	Default_LAN_Zone	YES	GNCC_MCN	Dynamic	Virtual WAN	YES	12	0	-	YES
5	10.0.3.0/24	*	GNCC_MCN-Branch...	Default_LAN_Zone	YES	GNCC_MCN	Dynamic	Virtual WAN	YES	11	0	-	YES
6	10.0.4.0/24	*	GNCC_MCN-Branch...	Default_LAN_Zone	YES	GNCC_MCN	Dynamic	Virtual WAN	YES	11	0	-	YES
7	10.1.1.0/24	*	GNCC_MCN-Branch...	Default_LAN_Zone	YES	GNCC_MCN	Dynamic	Virtual WAN	YES	12	0	-	YES

## 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.

