Maidenhead Bridge

netskope

Cloud Security Connectors for Netskope with PriCPA Azure Cloud Case Study

(CSC for Azure)

Version 1.1

September 2022

Table of Contents

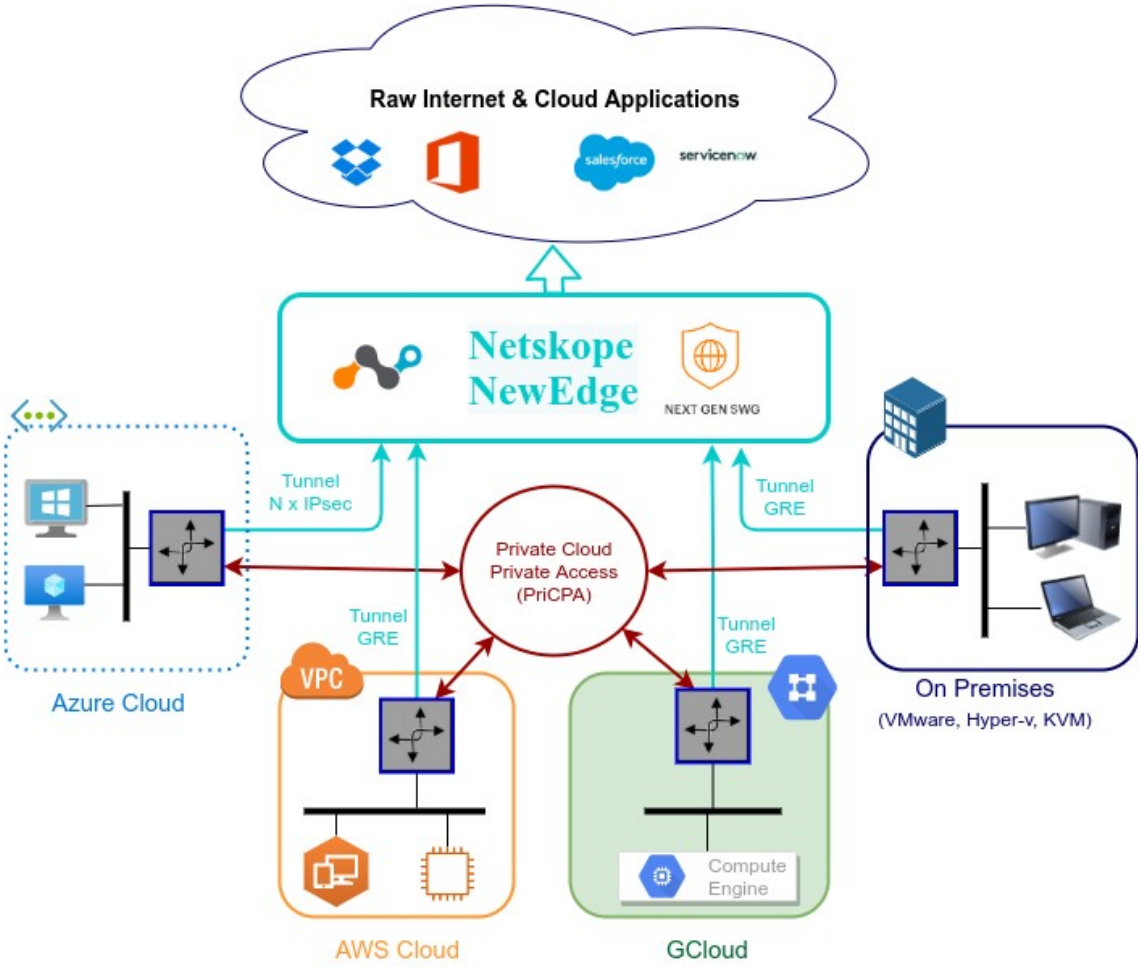
1 About Maidenhead Bridge & Cloud Security Connectors....3
2 Main benefits of using Cloud Security Connectors....4
3 About this Case Study....5
4 Customer requirements....5
5 Network Diagram....6
6 How the solution works....7
7 Detailed Configuration....8
7.1 General Setup....8
7.1.1 Azure Firewall....8
7.1.2 Cloud Security Connector....8
7.2 Subnets, IP Addresses, Gateways, etc....9
7.3 Route Tables....10
7.3.1 Route Table for Private Subnets....10
7.3.2 Route Table for Azure FW Subnet....11
7.3.3 Route Table for CSC Internal Subnet....12
7.3.4 Route Table for CSC External Subnet....13
7.4 Firewalling....14
7.4.1 Azure Firewall....14
7.4.1.1 Inbound Rules:....14
7.4.1.2 Outbound Rules....14
7.4.2 Security Group - External CSC Interface....15
8 Appendix A....16
8.1 Documentation....16
8.2 Creating and Deploying the CSC....16
8.2.1 Prerequisites:....16
8.2.2 Creation and Deployment: Azure Marketplace....16
8.2.3 Configuration required on Netskope Console:....17
8.2.4 Check status....18
8.3 Configuring High Availability....20
8.4 "Routed Bypass" in action....21
8.4.1 Configuration....21
8.4.2 Routed Bypass JSON file explained....23
8.4.2.1 Rules to "Routed Bypass" Non-HTTP Traffic....23
8.4.3 Rules to allow Netskope Agent to reach NewEdge directly....23
8.4.4 Rules to allow MSFT Login URLs (for Conditional Access)....25

1 About Maidenhead Bridge & Cloud Security Connectors

Maidenhead Bridge (MHB) has provided connectivity solutions to Cloud Secure Web Gateways (Now SSE) since 2016.

MHB created a disruptive technology that allows companies to connect to Netskope NewEdge without the requirement of any networking security expertise: The Cloud Security Connector (CSC) for Netskope.

The CSC is a virtual device with the perfect configuration for Netskope that enables easy deployments of the Netskope SSE solution in any customer environment, protecting customers' Public and Private Traffic.



2 Main benefits of using Cloud Security Connectors

- The CSC is a tailored solution with the perfect configuration for Netskope.
- The CSC provides a Reliable, Redundant, High Available, Clean and Scalable connectivity to Netskope NewEdge from AWS, Azure and any HyperVisor.
- Cost savings:
  - ✔ Zero-touch configuration and automated deployment. Any IT professional can implement the CSC. No security networking expertise or Professional Services are required.
  - ✔ Provides encrypted Site-to-Site, Site-to-Cloud and Cloud-to-Cloud connectivity with Zero Trust. Replaces MPLS, VPN Gateways, SD-WAN, Express Routing, etc.
  - ✔ Pay-as-you-go model direct from Cloud Marketplaces. No hidden fees. No BYOL.

3 About this Case Study.

One common scenario on Azure is finding organisations using Azure Firewall that wants to connect to Netskope NewEdge without disrupting or changing the current architecture too much.

Another common scenario is that companies are obligated to use Azure Firewall for compliance purposes or because it is part of the service provided under management for their providers.

This Case Study aims to provide the essential information to deploy and troubleshoot the Cloud Security Connector for Azure when connecting Servers and Virtual Desktops to NewEdge and using Azure Firewall.

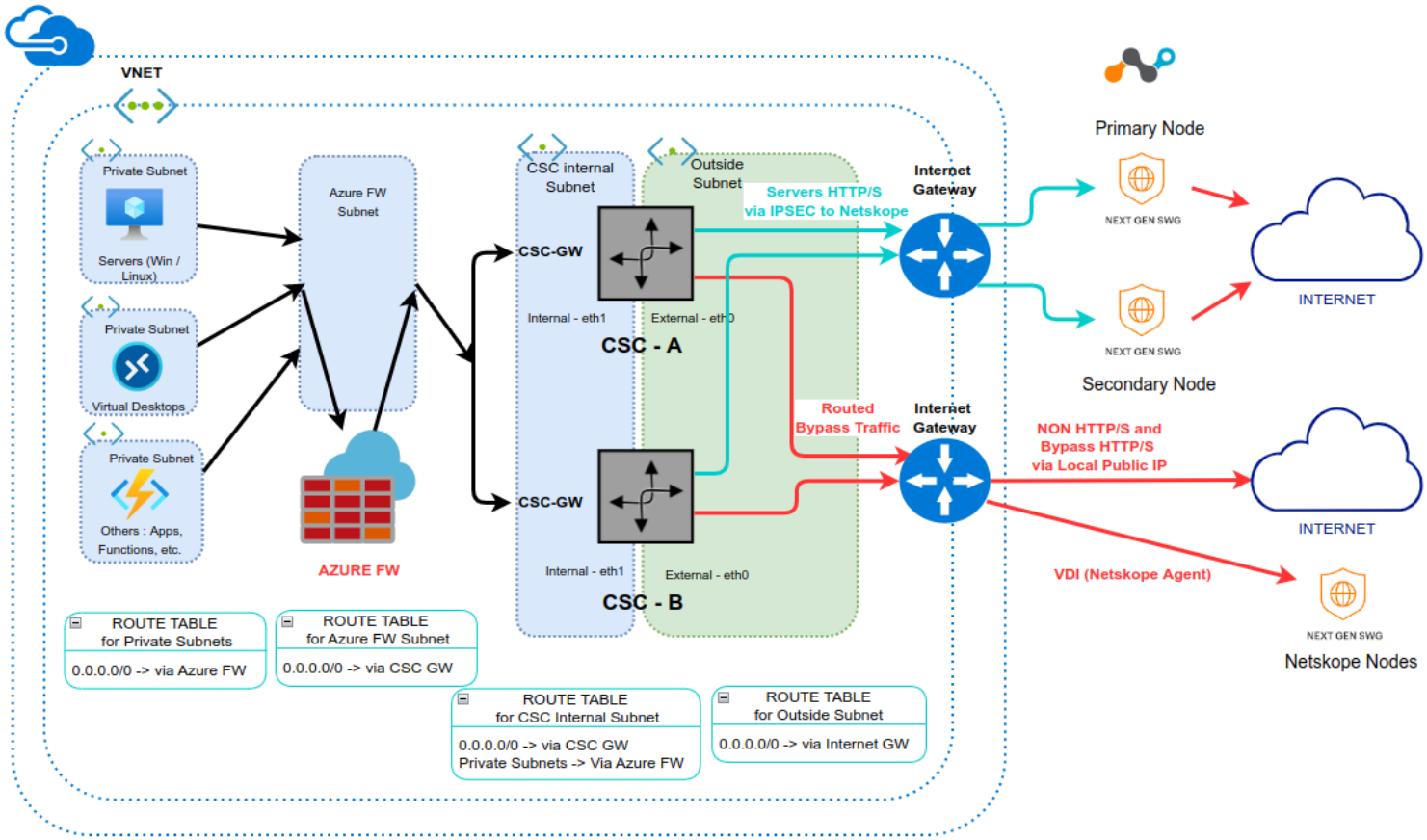
4 Customer requirements.

The customer is an organization with the following traffic steering requirements:

1. Http/s only traffic to NewEdge because the customer has no Cloud Firewall license.
2. Non-Http/s traffic goes directly to the Internet.
3. All traffic must traverse via an Azure Firewall for compliance with local regulators.
4. Authentication exemption for traffic arriving from Server Subnets.
5. The Source IP of the Servers must be visible at NewEdge.
6. Traffic from Servers Subnets will reach NewEdge via IPsec Tunnels at 1 Gbps or more.
7. Virtual Desktops will have the Netskope Client installed and reach NewEdge directly to the Internet and not via the IPsec tunnels.
8. Some Http/s destinations must go direct to the Internet via local Public IP, and not via NewEdge. (i.e. to apply MSFT Conditional Access)

The following Chapter shows how to achieve the customer requirements with the Cloud Security Connector for Netskope.

5 Network Diagram



6 How the solution works

Important note: *The Azure FW has severe limitations on the Source NAT configuration and cannot split traffic to the Internet Source NATed or not Source NATed per Source IP. In this case, we need the Servers' private source IP visible at the Cloud level (no source NAT) and the VDI direct to the Internet (Source Nat applied). The Azure FW is not capable of doing this. For this reason, we send all traffic via the CSC, which has no limitations in this regard.*

This chapter shows how to achieve the customer's requirements, one by one.

1. Http/s only traffic to NewEdge because the customer has no Cloud Firewall license.

After passing via the Azure Firewall, the CSC splits the traffic, sending Http/s from Server Subnets via the IPsec Tunnels and the traffic from VDI Subnets direct to NewEdge Nodes.

2. Non-Http/s traffic goes directly to the Internet.

After passing via the Azure Firewall, the CSC sends all Non-Https/s traffic direct to the Internet.

3. All traffic must traverse via an Azure Firewall for compliance with local regulators.

The default route to the Internet (0.0.0.0/0) for all internal Subnets is the Azure Firewall GW IP.

4. Authentication exemption for traffic arriving from Server Subnets.

On the Netskope console, configure Bypass Settings -> SOURCE IP ADDRESS BYPASS.

5. The Source IP of the Servers must be visible at NewEdge.

The CSC provides full visibility of internal devices IPs at Cloud Level.

6. Traffic from Servers Subnets will reach NewEdge via IPsec Tunnels at 1 Gbps or more.

The CSC Mux 4 aggregates 4 x IPsec tunnels (1 Gbps), and the CSC Mux 8 aggregates 8 x IPsec (2 Gbps)

7. Virtual Desktops will have the Netskope Client installed and reach NewEdge directly to the Internet and not via the IPsec tunnels.

The CSC can split traffic per Source IPs, Destination IPs, Protocol and Port. Therefore, we will create a "routed bypass rule" for the VDI Subnets going to NewEdge Nodes on port 433. This "routed bypass rule" will send the traffic directly via Internet Gateway and not via the IPsec Tunnels.

8. Some Http/s destinations must go direct to the Internet via local Public IP, and not via NewEdge.

Similar than before, we will create a "routed bypass rule" to reach some Http/s destinations directly via the Internet.

7 Detailed Configuration.

This chapter shows the configuration in detail of each component of the solution.

7.1 General Setup

This setup requires the following:

7.1.1 Azure Firewall

Create a Subnet for the Azure Firewall and deploy the Azure Firewall on it.

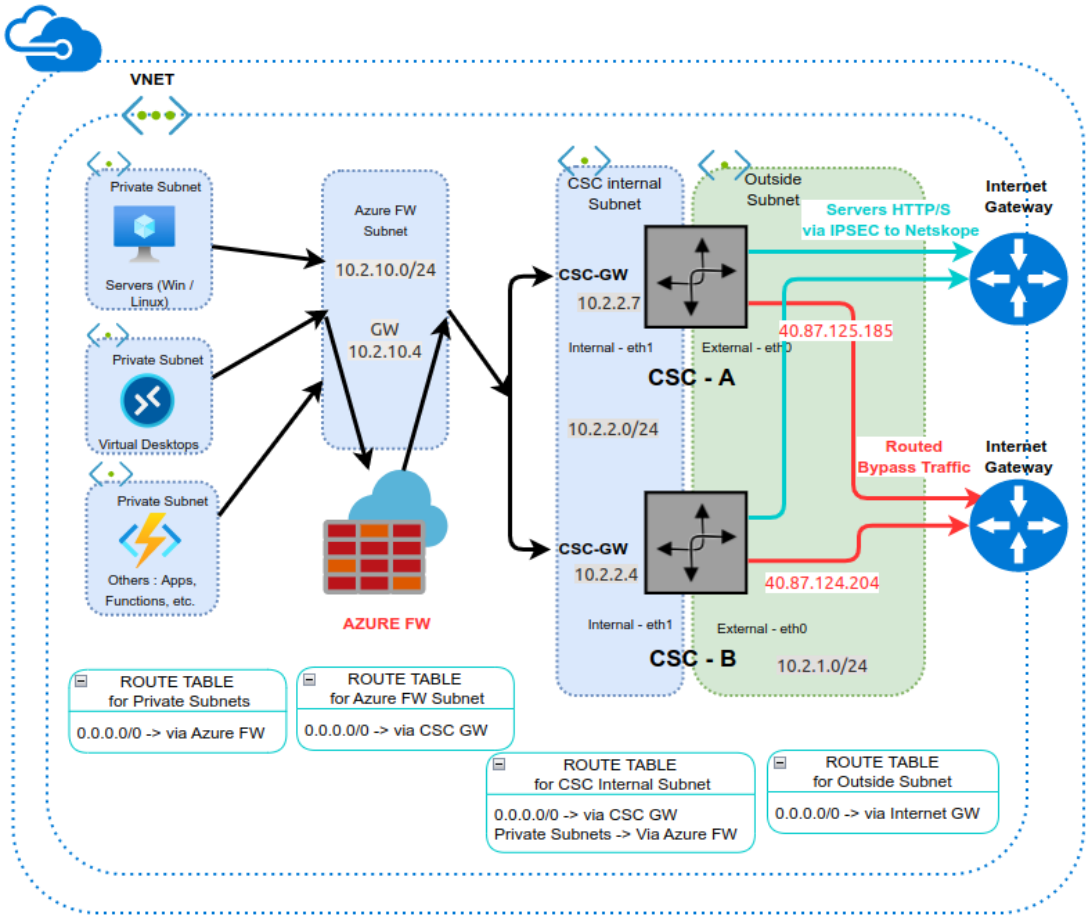
7.1.2 Cloud Security Connector

1. Create 2 subnets for the CSC: Internal and External and deploy a pair of CSCs.
2. Configure the tunnels on the Netskope Console using the CSV file provided by each CSC.
3. Configure High Availability on each CSC adding the routes under the control of the CSC HA Pair.
4. Configure "Routed Bypasses" on each CSC.

Note: See Appendix A for detailed configuration. All steps mentioned above are standard configuration.

7.2 Subnets, IP Addresses, Gateways, etc.

The following network diagram shows the Subnet, IP Addresses, Gateways and bypass public IPs.



Azure Firewall GW IP: 10.2.10.4

CSC-A GW IP: 10.2.2.7

CSC-B GW IP: 10.2.2.4

CSC-A Bypass Public IP: 40.87.125.185

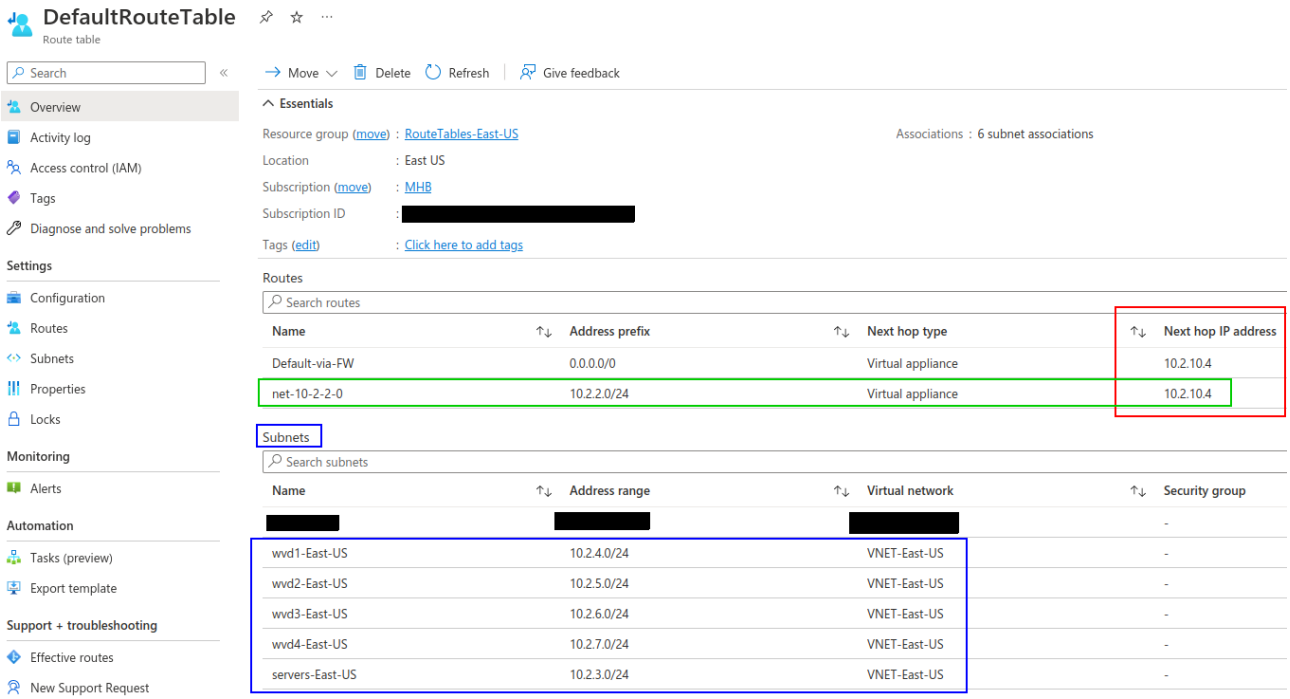
CSC-B Bypass Public IP: 40.87.124.204

7.3 Route Tables

Route tables play an essential role in this design. Please look carefully at the route table applied to each subnet.

7.3.1 Route Table for Private Subnets.

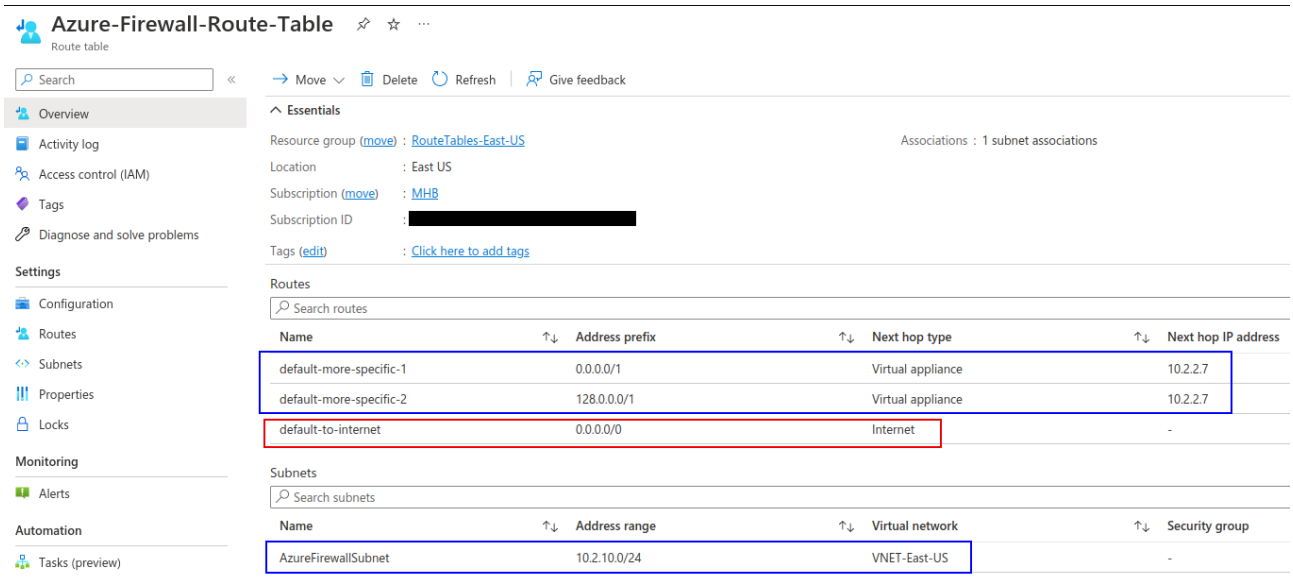
The route table for Private Subnets: Servers, Virtual Desktops, etc.



Important Notes:

- The route to 0.0.0.0/0 has Next-Hop 10.2.10.4 (Azure FW GW IP)
- The route to 10.2.2.0/24 (CSC Internal Subnet) via Next-Hop 10.2.10.4 is required to force any communication from Private Subnets to the CSC Internal Subnet via Azure FW. For example, if you want to SSH the CSCs. This route is needed because Private Subnets and CSC Internal Subnet belong to the same VNET.
- This route table has associated all internal Private Subnets: for Servers and Virtual Desktops.

7.3.2 Route Table for Azure FW Subnet

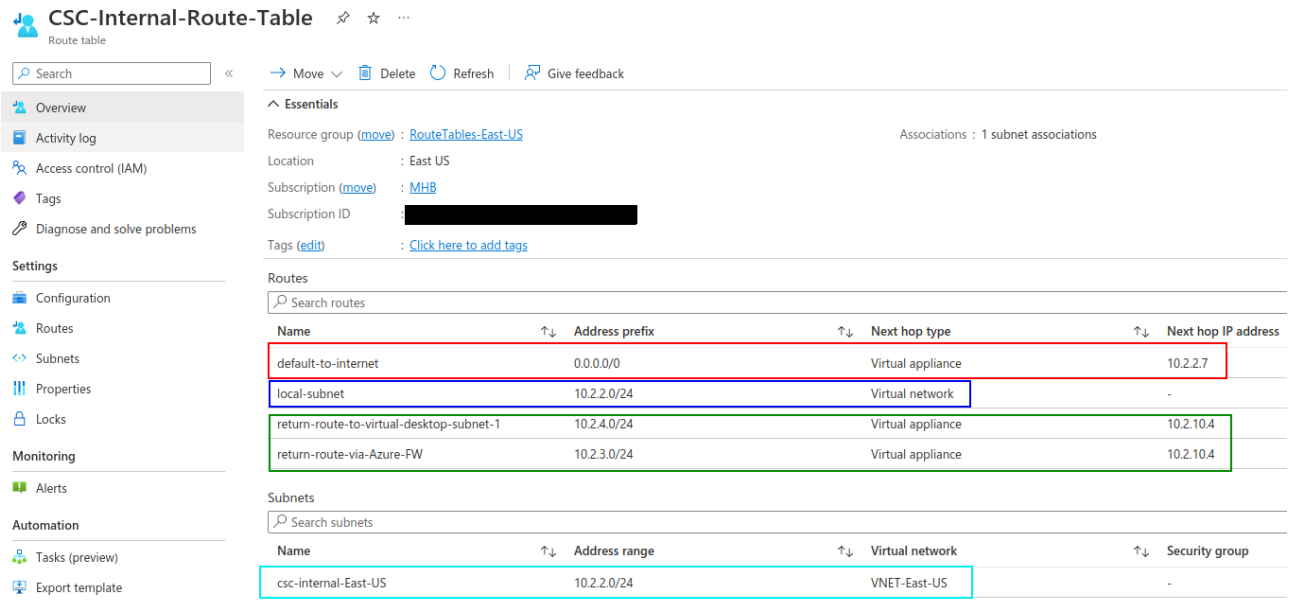


Important Notes:

- Azure FW "Basic Subscription" requires the route 0.0.0.0/0 -> Next hop type -> Internet
- To override the route 0.0.0.0/0, we created two "more specific" routes that also covers all internet address: 0.0.0.0/1 and 128.0.0.0/1, using next-hop IP address: 10.2.2.7 (*) (the CSC GW IP address)
- This route table has associated the Azure Firewall Subnet.

(*) The Next-Hop of routes to destinations 0.0.0.0/1 and 128.0.0.0/1 is controlled by the CSC HA functionality. The Next-Hop will be the active CSC. The value in this example can be 10.2.2.7 or 10.2.2.4

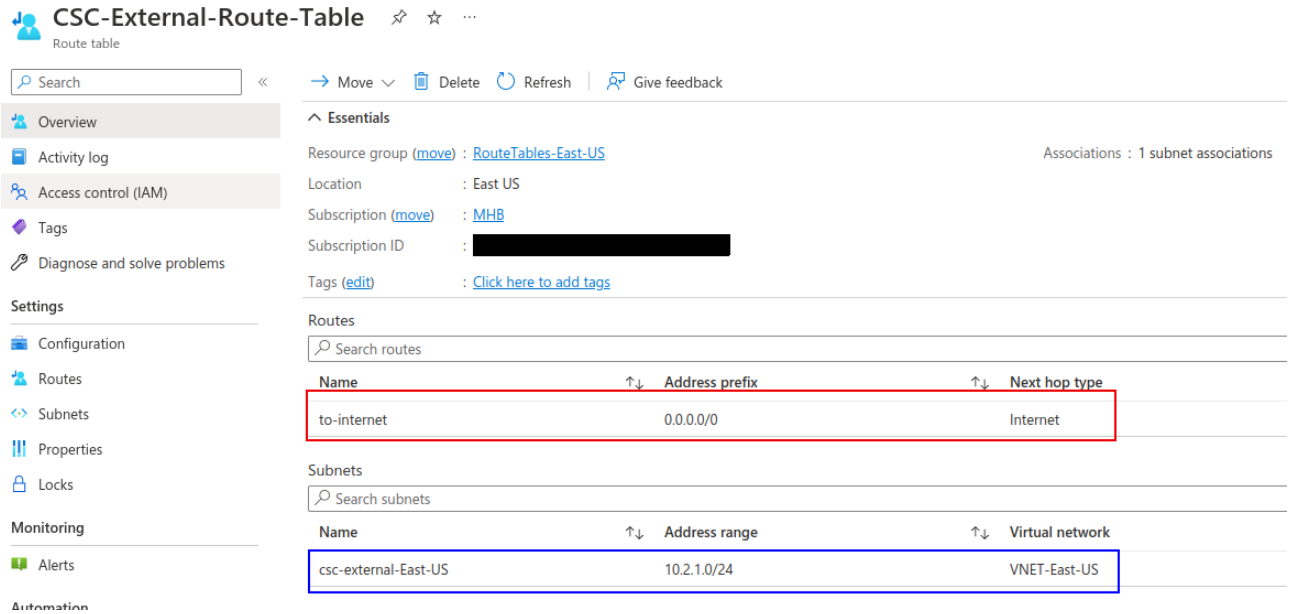
7.3.3 Route Table for CSC Internal Subnet.



Important Notes:

- The route 0.0.0.0/0 via 10.2.2.7 (CSC GW IP) will be controlled by the CSC HA functionality. The value of Next hop IP address will be the CSC GW IP of the CSC active. The value in this example can be 10.2.2.7 or 10.2.2.4
- The route "local-subnet" (10.2.2.0/24) via Virtual Network is required to allow communication between CSC's internal interfaces. This is required by the CSC HA functionality.
- The "return-routes" via 10.2.10.4 (Azure FW GW) are required to force back all traffic to Private Subnets via the Azure FW. Please, include here all internal subnets/mask. Please, do not aggregate subnets (do not use 10.2.0.0/16) if you are using a single VNET.
- Associate this Route Table to the CSC Internal Subnet.

7.3.4 Route Table for CSC External Subnet



Important Notes:

- On the External Subnet, the route for the CSC is to reach the entire Internet via the Internet Gateway: 0.0.0.0/0 -> Internet.

7.4 Firewalling

The design has three layers of Firewalling:

1. Azure Firewall.
2. Cloud Security Connector. The CSC is a Firewall and isolates all traffic from the external to the internal interface. Rules are created automatically. No manual operation is required.
3. Security Group applied to the external interface of the CSC. This Security Group is automatically created when launching the CSC.

7.4.1 Azure Firewall

7.4.1.1 Inbound Rules:

Home > Azure-Firewall-02 | Rules (classic) >

Edit network rule collection ...

Name Inbound-Rules

Priority * 2000

Action * Allow

Rules

IP Addresses

name	Protocol	Source type	Source	Destination type	Destination Addresses	Destination Ports
Ping Syslog	ICMP	IP address	10.2.2.0/24	IP address	10.2.3.4	*
Allow Syslog	TCP	IP address	10.2.2.0/24	IP address	10.2.3.4	514

The Inbound rules required are to allow the CSCs to reach the Syslog servers, that are located on a Private Subnet.

7.4.1.2 Outbound Rules

Home > Azure-Firewall-02 | Rules (classic) >

Edit network rule collection ...

Name Outbound-Rules

Priority * 1000

Action * Allow

Rules

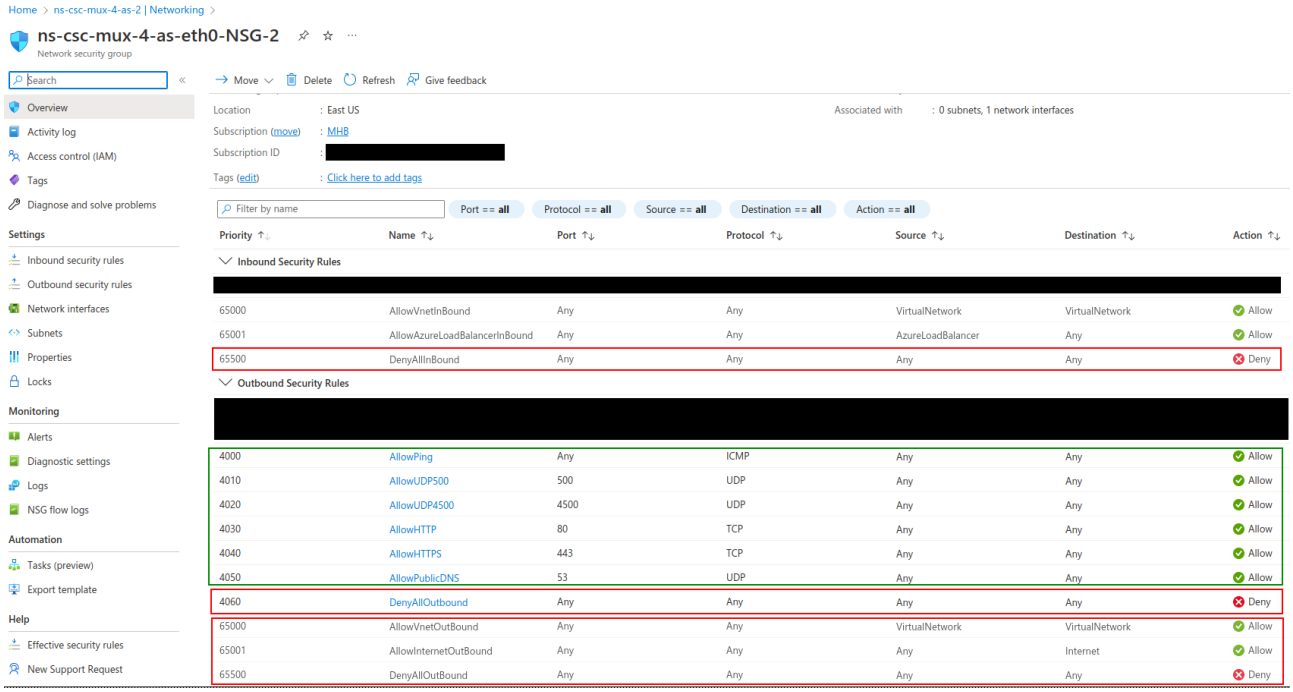
IP Addresses

name	Protocol	Source type	Source	Destination type	Destination Addresses	Destination Ports
WebTraffic	TCP	IP address	10.2.0.0/16	IP address	0.0.0.0/1,128.0.0.0/1	80,443,8081
SSH to CSCs	TCP	IP address	10.2.3.0/24	IP address	10.2.2.0/24	22
Ping	ICMP	IP address	10.2.3.0/24	IP address	10.2.2.0/24	*
Non-HTTP-Traffic	0 selected	IP address	*, 192.168.10.1, 192.168.10.0/24, 192.16...	IP address	*, 192.168.10.1, 192.168.10.0/24, 192.16...	8080, 8080–8090, *

Important Notes:

1. Web traffic to the Internet is allowed on ports 80, 443 (and 8081 in this case).
2. Private Subnet 10.2.3.0/24 can reach CSC internal Subnet for PING and SSH.
3. Non-HTTP-Traffic to be defined.

7.4.2 Security Group - External CSC Interface



Important Notes:

- Inbound: Using default values. Nothing else is required. Everything is blocked.
- Outbound:
  - Rules 4000, 4010 and 4020 are required for the functioning of the IPsec Tunnels to Newedge.
  - Rule 4030, 4040 are for web traffic not sent via the IPsec Tunnels.
  - Rule 4050 is required if the CSC is configured with Public DNS servers, like 8.8.8.8 or 1.1.1.1
  - Rule for Non-HTTP traffic to be defined.
  - Everything else is block via rule 4060.

8 Appendix A

8.1 Documentation

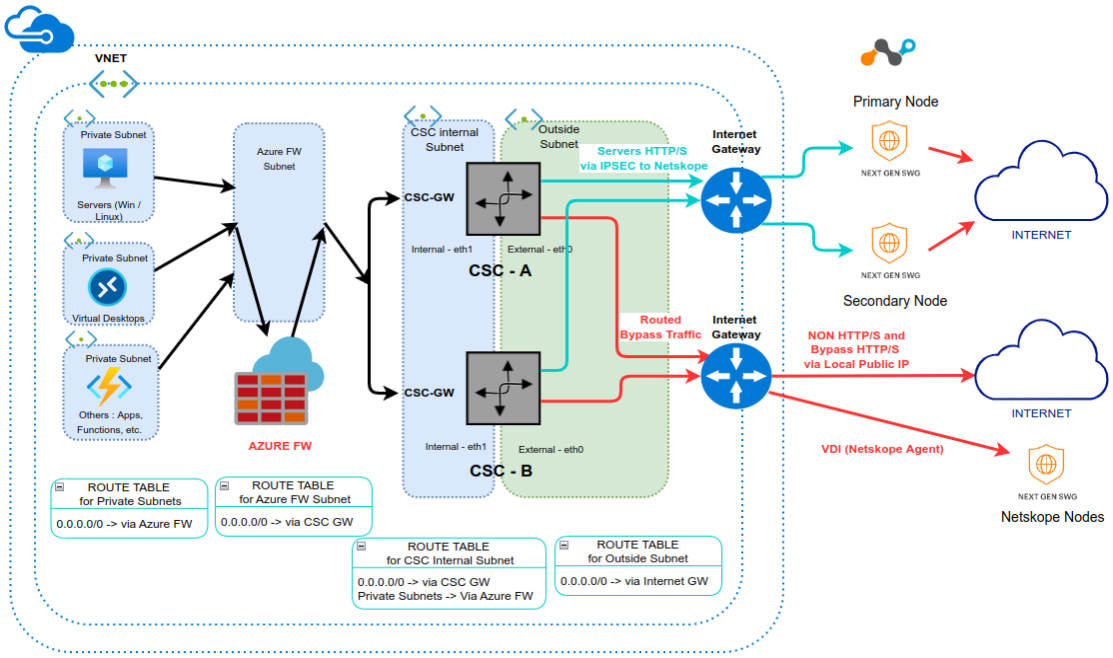
All documentation is available at http://support.maidenheadbridge.com

The specific URL documentation for the CSC for Azure is :
https://maidenheadbridge.freshdesk.com/support/solutions/33000138192

8.2 Creating and Deploying the CSC.

8.2.1 Prerequisites:

- Outside Subnet created and route to allow this subnet to go to internet via Internet. (0.0.0.0/0 -> via Internet)
- CSC Internet Subnet



8.2.2 Creation and Deployment: Azure Marketplace

The simplest way to deploy the CSC Mux 4 or 8 for Netskope on Azure is via Azure Marketplace. Azure Marketplace provides a GUI to the ARM template, making things easy.

Link to Azure Marketplace:

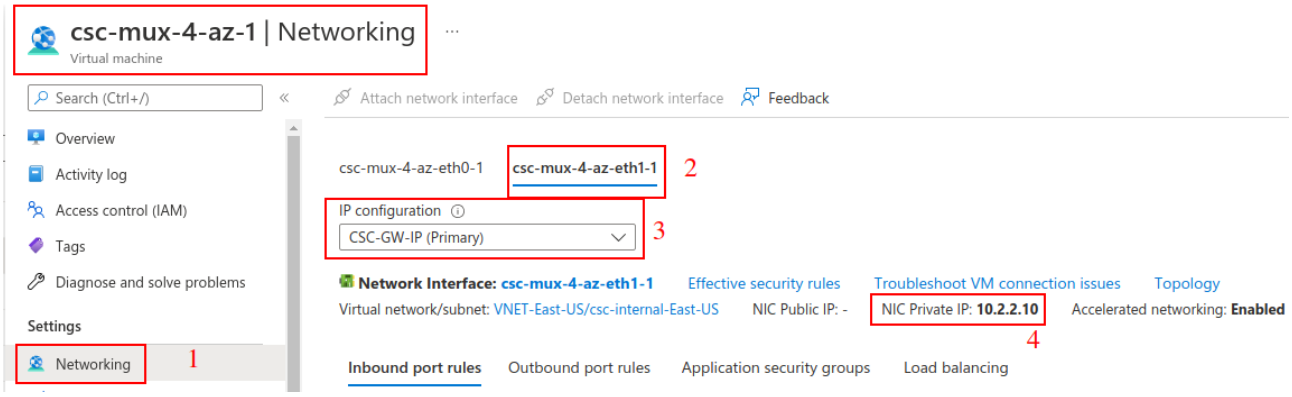
https://azuremarketplace.microsoft.com/en-gb/marketplace/apps/maidenhead-bridge.ns-csc-mux-azure-application?tab=Overview

Via Azure Marketplace, you can deploy the CSC on a Single or High Availability configuration in one shot.

8.2.3 Configuration required on Netskope Console:

In this case, you need to SSH the CSC to obtain the "CSV File" to import on the Netskope Console.

1. Go to your Azure Dashboard → Select the VM created → Networking → eth1 and check "NIC Private IP". (CSC-GW-IP (Primary))



2. In this example, "NIC Private IP" is: 10.2.2.10
3. From a machine inside the Virtual Network, ssh the CSC using username "cscadmin" and key or password:

ssh -i <keyname.pem> cscadmin@<eth1 Private IP>

ssh cscadmin@<eth1 Private IP>

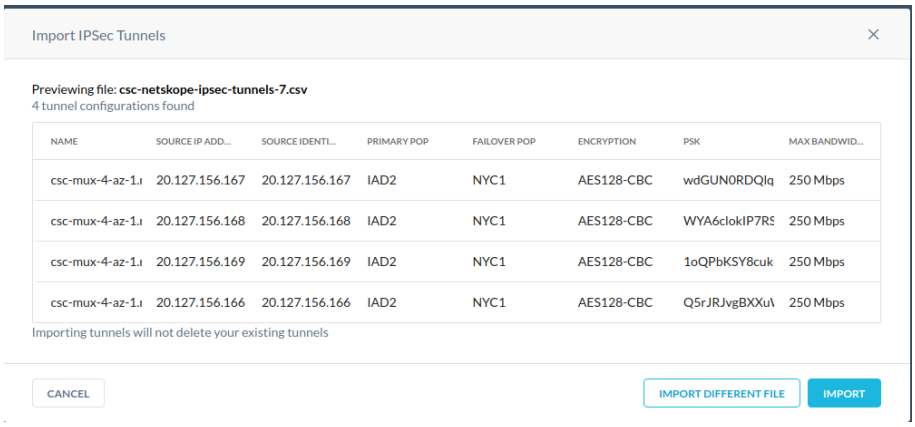
Important: Please, wait 2 minutes before to SSH the CSC to allow all processes to complete.

CSC Mux initial screen shows the tunnel information to import in the Netskope console.

```
Maidenhead Bridge

Cloud Security Connector Mux on Azure for Netskope - Admin Console

On your Netskope console, please go to page: Settings -> Security Cloud Platform -> Traffic Steering Section -> IPSEC and check 'IPSEC Tunnels' to validate you imported the CSV file shown below.

CSV file:
------------------------------------------------------------------------------------------------------------------------------------------------------

tunnel name,source identity,source ip address,primary pop,failover pop,encryption cipher,psk,maximum bandwidth,enabled
csc-mux-4-az-1.nstun1,20.127.156.167,20.127.156.167,IAD2,NYC1,AES128-CBC,wdGUN0RDQlqtFJl0vS8i4QFanXGJUIcF,250,true
csc-mux-4-az-1.nstun2,20.127.156.168,20.127.156.168,IAD2,NYC1,AES128-CBC,WYA6clokIP7RS2bxpqypEdOQVZg0d5NS,250,true
csc-mux-4-az-1.nstun3,20.127.156.169,20.127.156.169,IAD2,NYC1,AES128-CBC,1oQPbKSY8cuk6x5dNMgibnM4u8JyFWZU,250,true
csc-mux-4-az-1.nstun4,20.127.156.166,20.127.156.166,IAD2,NYC1,AES128-CBC,Q5rJRJvgBXXuWnigXPMtUCwpAhk0PDgu,250,true
------------------------------------------------------------------------------------------------------------------------------------------------------

Intructions to Import the CSV file:

        1 - Copy and paste the CSV file's contents on a Text Editor and save it as '<filename>.csv'. Important: Do not add blank lines at the end of the file.
        2 - On your Netskope console, please go to page: Settings -> Security Cloud Platform -> Traffic Steering Section -> IPSEC and click 'IMPORT TUNNELS FROM CSV' and select the CSV file.

Did you 'Import tunnels from CSV' on the Netskope console? Please, confirm.

1) Yes
2) No
Enter your choice:
```

Create a CSV file with this information

4. Copy and paste the CSV file's contents on a Text Editor and save it as '<filename>.csv'. Important: Do not add blank lines at the end of the file.
5. On your Netskope console, please go to page: Settings -> Security Cloud Platform -> Traffic Steering Section -> IPSEC and click "IMPORT TUNNELS FROM CSV" and select the CSV file.



6. Click "IMPORT" and wait a while to see the tunnels up.

8.2.4 Check status

The "Show Configuration and Status" is a complete tool to validate the configuration, checking tunnels to Netskope and connectivity to other devices. (DNS servers, Syslog, Bypass test page, etc.)

```
Monitoring Tasks
1) Show Configuration and Status
2) Show Interfaces Traffic
3) Traceroute and Latency Test
4) Speed Test (Experimental)
```

Check the "Tunnel Section" to verify that all tunnels are UP.

```
NETSKOPE INFORMATION
Tunnels Name:
                NStun1: ns-csc-mux-4-as-2.nstun1
                NStun2: ns-csc-mux-4-as-2.nstun2
                NStun3: ns-csc-mux-4-as-2.nstun3
                NStun4: ns-csc-mux-4-as-2.nstun4
Primary Tunnel:
                Node : US,Washington,IAD2
                Node Public IP: 163.116.146.38 is Alive
                Node Probe: 10.146.6.216
Secondary Tunnel:
                Node : US,NewYork,NYC1
                Node Public IP: 163.116.135.38 is Alive
                Node Probe: 10.135.6.216

LOAD BALANCING INFORMATION
Last change: Mon 19 Sep 23:06:28 UTC 2022
(UP)   NStun1 is active, using primary.
(UP)   NStun2 is active, using primary.
(UP)   NStun3 is active, using primary.
(UP)   NStun4 is active, using primary.

IPSEC INFORMATION
NStun1 connected to: US,Washington,IAD2, IPsec uptime: 2 days, since Sep 19 22:52:32 2022, Last Security Association: ESTABLISHED 4 hours ago
NStun2 connected to: US,Washington,IAD2, IPsec uptime: 2 days, since Sep 19 23:05:18 2022, Last Security Association: ESTABLISHED 4 hours ago
NStun3 connected to: US,Washington,IAD2, IPsec uptime: 2 days, since Sep 19 22:53:03 2022, Last Security Association: ESTABLISHED 4 hours ago
NStun4 connected to: US,Washington,IAD2, IPsec uptime: 2 days, since Sep 19 22:53:13 2022, Last Security Association: ESTABLISHED 4 hours ago

HTTP://WWW.NOTSKOPE.COM PAGE STATUS
NStun1 is connected to 163.116.146.120 Ashburn, United States (IAD2)
NStun2 is connected to 163.116.146.114 Ashburn, United States (IAD2)
NStun3 is connected to 163.116.146.116 Ashburn, United States (IAD2)
NStun4 is connected to 163.116.146.117 Ashburn, United States (IAD2)
```

8.3 Configuring High Availability

NOTE: Detailed step by step configuration at:
https://maidenheadbridge.freshdesk.com/support/solutions/33000138192

1. Go to "Configuration Wizards" and select High Availability Configuration.

```
Configuration Wizards
14) Change Nodes, DNS servers, Syslog and more.
15) Switch Tunnels - Primary / Secondary.
16) Update Netskope Nodes Databases.
17) High Availability configuration.
```

2. Follow the instructions.

```
Selection: 17

This Wizard is for High Availability scenarios when changing Next-Hop on Routes via CSC HA Pair.

---------------------
How to configure:

1) 'Deployment': Deploy a pair of CSCs with the following conditions:
   1.1) There is connectivity each other via their internal interfaces.
   1.2) (Optional, but Recommended) Deploy the CSCs on Availability Zones or Availability Sets.
2) 'Identity': On each CSC VM
   2.1) Go to 'Identity -> System Assigned' and 'Turn ON' status. (and Save).
   2.2) Go to 'Identity -> System Assigned' and click 'Azure role assignments' and add the following Roles:
        -> Role: Contributor, Resource Group: <CSCs VMs Resource Group/s>
        -> Role: Contributor, Resource Group: <Route Tables Resource Group/s>
        -> Role: Network Contributor, Resource Group: <CSC Subnets (VNET) Resource Group>
3) 'Routes'
   3.1) Go to Routes (inside the Route Table) and create the Routes that the CSC HA group will control:
      -> Route name: <any name you want>
      -> Address prefix: <Subnet/Mask>
            Examples: 0.0.0.0/0 (if you want to send all traffic via Netskope) or 163.116.128.80/32 (when using PAC files and/or Explicit Proxy)
      -> Next hop type: Virtual Appliance
      -> Next hop address: <Input CSC-GW-IP (eth1, first IP) of any CSC>
   3.2) Go to Subnets and associate the Subnet with the Route Table.
   3.3) Repeat the process if you want to add more Routes. The CSC HA functionality can manipulate multiple Routes.
4) Obtain the following values and Run the Wizard.
   4.1) Route, Route Table, Resource Group.
   4.2) Computer Name and Resource Group of each CSC.
5) This Wizard will create a JSON file. You can use this JSON file to configure the Other CSC in the pair.

How it works:

The CSCs on the HA pair will automatically select the Next-Hop for the Route/s configured.

---------------------
```

3. Check the status via "Show Configuration and Status" menu.

```
HIGH AVAILABILITY Information
The HA service is:  active (running) since Thu 2022-09-15 16:42:36 UTC; 6 days ago
Identity Type: SystemAssigned
Route to Netskope using Next Hop: 10.2.2.7 of VM: ns-csc-mux-4-as-1 (the other CSC in the pair)
Current values configured are:
   Route/s (Qty)= 3
      Route 1: default-to-internet (Route Table=CSC-Internal-Route-Table, Resource Group=RouteTables-East-US)
      Route 2: default-more-specific-1 (Route Table=Azure-Firewall-Route-Table, Resource Group=RouteTables-East-US)
      Route 3: default-more-specific-2 (Route Table=Azure-Firewall-Route-Table, Resource Group=RouteTables-East-US)
   Computer Name of other CSC in the pair: ns-csc-mux-4-as-1 (Resource Group=CSC-East-US)
Private Access Public IP= 40.87.125.185
```

8.4 "Routed Bypass" in action.

Routed Bypass functionality plays a vital role in this architecture. Routed Bypass allows Non-HTTP traffic, Netskope Agent traffic and MSFT Login destinations to go direct to the Internet and not via the IPsec tunnels.

This section describes how to configure and explains in detail the JSON file.

NOTE: Detailed step by step configuration at:
https://maidenheadbridge.freshdesk.com/support/solutions/33000138192

8.4.1 Configuration

1. Using "Routed Bypass" menu you can insert the "Routed Bypass JSON file" or to configure an URL to download the JSON file from a remote site. (i.e. bucket). We are going to use URL method. The JSON file is stored at this URL:
   https://maidenheadbridge.blob.core.windows.net/documentation/JSON-files-examples/AzureFW_and_CSC_routedBypass_json_Netskope.json

```
Routed Bypass
10) View Current Routed Bypass List
11) Configure Routed Bypass List
```

2. Configure Routed Bypass List.

```
Selection: 11

Please, Select Method:
1) Routed Bypass URL
2) Manual (Paste Routed Bypass Rules JSON File)
3) Reset to Default Values
4) Quit
Enter your choice: 1

*** Routed Bypass URL is not configured ***

Do you want to configure the Routed Bypass URL?
1) Yes
2) No
Enter your choice: 1

Please, input Routed Bypass URL
Routed Bypass URL: https://maidenheadbridge.blob.core.windows.net/documentation/JSON-files-examples/AzureFW_and_CSC_routedBypass_json_Netskope.json

Do you want to refresh the Routed Bypass List?
1) Yes
2) No
Enter your choice: 1

Routed Bypass JSON file imported successfully
```

3. (Optional) Review the List.

```
You can review your values before to apply. Please, Select 'Compact' or 'Json' format.
1) Compact
2) Json
3) No review is needed
Enter your choice: 1

Current Values configured are:

Index: 0, Protocol: icmp, SourceIP: 0.0.0.0/0, DestinationIP: 0.0.0.0/0, FromPort: , To Port: , Description: "Bypass ICMP all"
Index: 1, Protocol: tcp, SourceIP: 0.0.0.0/0, DestinationIP: 0.0.0.0/0, FromPort: 1, To Port: 79, Description: "Bypass TCP Ports I"
Index: 2, Protocol: tcp, SourceIP: 0.0.0.0/0, DestinationIP: 0.0.0.0/0, FromPort: 81, To Port: 442, Description: "Bypass TCP Ports II"
Index: 3, Protocol: tcp, SourceIP: 0.0.0.0/0, DestinationIP: 0.0.0.0/0, FromPort: 444, To Port: 65535, Description: "Bypass TCP Ports III"
Index: 4, Protocol: udp, SourceIP: 0.0.0.0/0, DestinationIP: 0.0.0.0/0, FromPort: 1, To Port: 65535, Description: "Bypass UDP Ports all"
Index: 5, Protocol: tcp, SourceIP: 10.2.9.0/24, DestinationIP: 8.36.116.0/24, FromPort: 443, To Port: 443, Description: "VDI - Netskope Destinations - I"
Index: 6, Protocol: tcp, SourceIP: 10.2.9.0/24, DestinationIP: 8.39.144.0/24, FromPort: 443, To Port: 443, Description: "VDI - Netskope Destinations - II"
Index: 7, Protocol: tcp, SourceIP: 10.2.9.0/24, DestinationIP: 31.186.239.0/24, FromPort: 443, To Port: 443, Description: "VDI - Netskope Destinations - III"
Index: 8, Protocol: tcp, SourceIP: 10.2.9.0/24, DestinationIP: 74.217.93.0/24, FromPort: 443, To Port: 443, Description: "VDI - Netskope Destinations - IV"
Index: 9, Protocol: tcp, SourceIP: 10.2.9.0/24, DestinationIP: 103.219.79.0/24, FromPort: 443, To Port: 443, Description: "VDI - Netskope Destinations - V"
Index: 10, Protocol: tcp, SourceIP: 10.2.9.0/24, DestinationIP: 163.116.128.0/17, FromPort: 443, To Port: 443, Description: "VDI - Netskope Destinations - VI"
Index: 11, Protocol: tcp, SourceIP: 0.0.0.0/0, DestinationIP: 20.190.128.0/18, FromPort: 80, To Port: 80, Description: "MSFT Login - Conditional Access - I"
Index: 12, Protocol: tcp, SourceIP: 0.0.0.0/0, DestinationIP: 20.190.128.0/18, FromPort: 443, To Port: 443, Description: "MSFT Login - Conditional Access - II"
Index: 13, Protocol: tcp, SourceIP: 0.0.0.0/0, DestinationIP: 40.126.0.0/18, FromPort: 80, To Port: 80, Description: "MSFT Login - Conditional Access - III"
Index: 14, Protocol: tcp, SourceIP: 0.0.0.0/0, DestinationIP: 40.126.0.0/18, FromPort: 443, To Port: 443, Description: "MSFT Login - Conditional Access - IV"
```

4. Apply the values.

```
Do you want to apply this values?
1) Yes
2) No
Enter your choice: 1

Routed Bypass - (Index: 0) Rule "Bypass ICMP all" was created succesfully.
Routed Bypass - (Index: 1) Rule "Bypass TCP Ports I" was created succesfully.
Routed Bypass - (Index: 2) Rule "Bypass TCP Ports II" was created succesfully.
Routed Bypass - (Index: 3) Rule "Bypass TCP Ports III" was created succesfully.
Routed Bypass - (Index: 4) Rule "Bypass UDP Ports all" was created succesfully.
Routed Bypass - (Index: 5) Rule "VDI - Netskope Destinations - I" was created succesfully.
Routed Bypass - (Index: 6) Rule "VDI - Netskope Destinations - II" was created succesfully.
Routed Bypass - (Index: 7) Rule "VDI - Netskope Destinations - III" was created succesfully.
Routed Bypass - (Index: 8) Rule "VDI - Netskope Destinations - IV" was created succesfully.
Routed Bypass - (Index: 9) Rule "VDI - Netskope Destinations - V" was created succesfully.
Routed Bypass - (Index: 10) Rule "VDI - Netskope Destinations - VI" was created succesfully.
Routed Bypass - (Index: 11) Rule "MSFT Login - Conditional Access - I" was created succesfully.
Routed Bypass - (Index: 12) Rule "MSFT Login - Conditional Access - II" was created succesfully.
Routed Bypass - (Index: 13) Rule "MSFT Login - Conditional Access - III" was created succesfully.
Routed Bypass - (Index: 14) Rule "MSFT Login - Conditional Access - IV" was created succesfully.

Routed Bypass - Routed Bypass List updated succesfully.
```

8.4.2 Routed Bypass JSON file explained

You can retrieve the JSON file from this URL :
https://maidenheadbridge.blob.core.windows.net/documentation/JSON-files-examples/AzureFW_and_CSC_routedBypass_json_Netskope.json

8.4.2.1 Rules to "Routed Bypass" Non-HTTP Traffic

This section allows to bypass UDP, ICMP and TCP (ports 1-79, 81-442, 443-65535).

```
    {
        "description": "Bypass ICMP all",
        "ipProtocol": "icmp",
        "sourceCirdIp": "0.0.0.0/0",
        "destinationCirdIp": "0.0.0.0/0",
        "fromPort": "",
        "toPort": ""
    },
    {
        "description": "Bypass TCP Ports I",
        "ipProtocol": "tcp",
        "sourceCirdIp": "0.0.0.0/0",
        "destinationCirdIp": "0.0.0.0/0",
        "fromPort": "1",
        "toPort": "79"
    },
    {
        "description": "Bypass TCP Ports II",
        "ipProtocol": "tcp",
        "sourceCirdIp": "0.0.0.0/0",
        "destinationCirdIp": "0.0.0.0/0",
        "fromPort": "81",
        "toPort": "442"
    },
    {
        "description": "Bypass TCP Ports III",
        "ipProtocol": "tcp",
        "sourceCirdIp": "0.0.0.0/0",
        "destinationCirdIp": "0.0.0.0/0",
        "fromPort": "444",
        "toPort": "65535"
    },
    {
        "description": "Bypass UDP Ports all",
        "ipProtocol": "udp",
        "sourceCirdIp": "0.0.0.0/0",
        "destinationCirdIp": "0.0.0.0/0",
        "fromPort": "1",
        "toPort": "65535"
    },
```

8.4.3 Rules to allow Netskope Agent to reach NewEdge directly.

Note: In this case, the Virtual Desktop are on Subnet 10.2.9.0/24.

```
{
    "description": "VDI - Netskope Destinations - I",
    "ipProtocol": "tcp",
    "sourceCirdIp": "10.2.9.0/24",
    "destinationCirdIp": "8.36.116.0/24",
    "fromPort": "443",
    "toPort": "443"
},
{
    "description": "VDI - Netskope Destinations - II",
    "ipProtocol": "tcp",
    "sourceCirdIp": "10.2.9.0/24",
    "destinationCirdIp": "8.39.144.0/24",
    "fromPort": "443",
    "toPort": "443"
},
{
    "description": "VDI - Netskope Destinations - III",
    "ipProtocol": "tcp",
    "sourceCirdIp": "10.2.9.0/24",
    "destinationCirdIp": "31.186.239.0/24",
    "fromPort": "443",
    "toPort": "443"
},
{
    "description": "VDI - Netskope Destinations - IV",
    "ipProtocol": "tcp",
    "sourceCirdIp": "10.2.9.0/24",
    "destinationCirdIp": "74.217.93.0/24",
    "fromPort": "443",
    "toPort": "443"
},
{
    "description": "VDI - Netskope Destinations - V",
    "ipProtocol": "tcp",
    "sourceCirdIp": "10.2.9.0/24",
    "destinationCirdIp": "103.219.79.0/24",
    "fromPort": "443",
    "toPort": "443"
},
{
    "description": "VDI - Netskope Destinations - VI",
    "ipProtocol": "tcp",
    "sourceCirdIp": "10.2.9.0/24",
    "destinationCirdIp": "163.116.128.0/17",
    "fromPort": "443",
    "toPort": "443"
},
```

8.4.4 Rules to allow MSFT Login URLs (for Conditional Access)

Source Information: https://endpoints.office.com/endpoints/worldwide?clientrequestid=b10c5ed1-bad1-445f-b386-b919946339a7

```
{
    "description": "MSFT Login - Conditional Access - I",
    "ipProtocol": "tcp",
    "sourceCirdIp": "0.0.0.0/0",
    "destinationCirdIp": "20.190.128.0/18",
    "fromPort": "80",
    "toPort": "80"
},
{
    "description": "MSFT Login - Conditional Access - II",
    "ipProtocol": "tcp",
    "sourceCirdIp": "0.0.0.0/0",
    "destinationCirdIp": "20.190.128.0/18",
    "fromPort": "443",
    "toPort": "443"
},
{
    "description": "MSFT Login - Conditional Access - III",
    "ipProtocol": "tcp",
    "sourceCirdIp": "0.0.0.0/0",
    "destinationCirdIp": "40.126.0.0/18",
    "fromPort": "80",
    "toPort": "80"
},
{
    "description": "MSFT Login - Conditional Access - IV",
    "ipProtocol": "tcp",
    "sourceCirdIp": "0.0.0.0/0",
    "destinationCirdIp": "40.126.0.0/18",
    "fromPort": "443",
    "toPort": "443"
}
```