Maidenhead Bridge

Cloud Security Connector Multiplex for Azure

Enabling Gigabit speeds to Zscaler for Azure customers

Administrator Guide

Version 3.1

(July 2021)

Table of Contents

1 Introduction

The Cloud Security Connector Multiplex (CSC Mux) for Azure is a Virtual Machine appliance that connects internal Azure resources to Zscaler Cloud Security Services at Gigabit Speeds.

The CSC Mux for Azure comes with all configurations required. After launching the CSC Mux from the Azure Marketplace using the ARM template provided, your only task is to put your VPN Credentials and select the Zscaler nodes you want to connect or let the CSC Mux discover the Zscaler nodes automatically.

Simple to install and not further management is required.

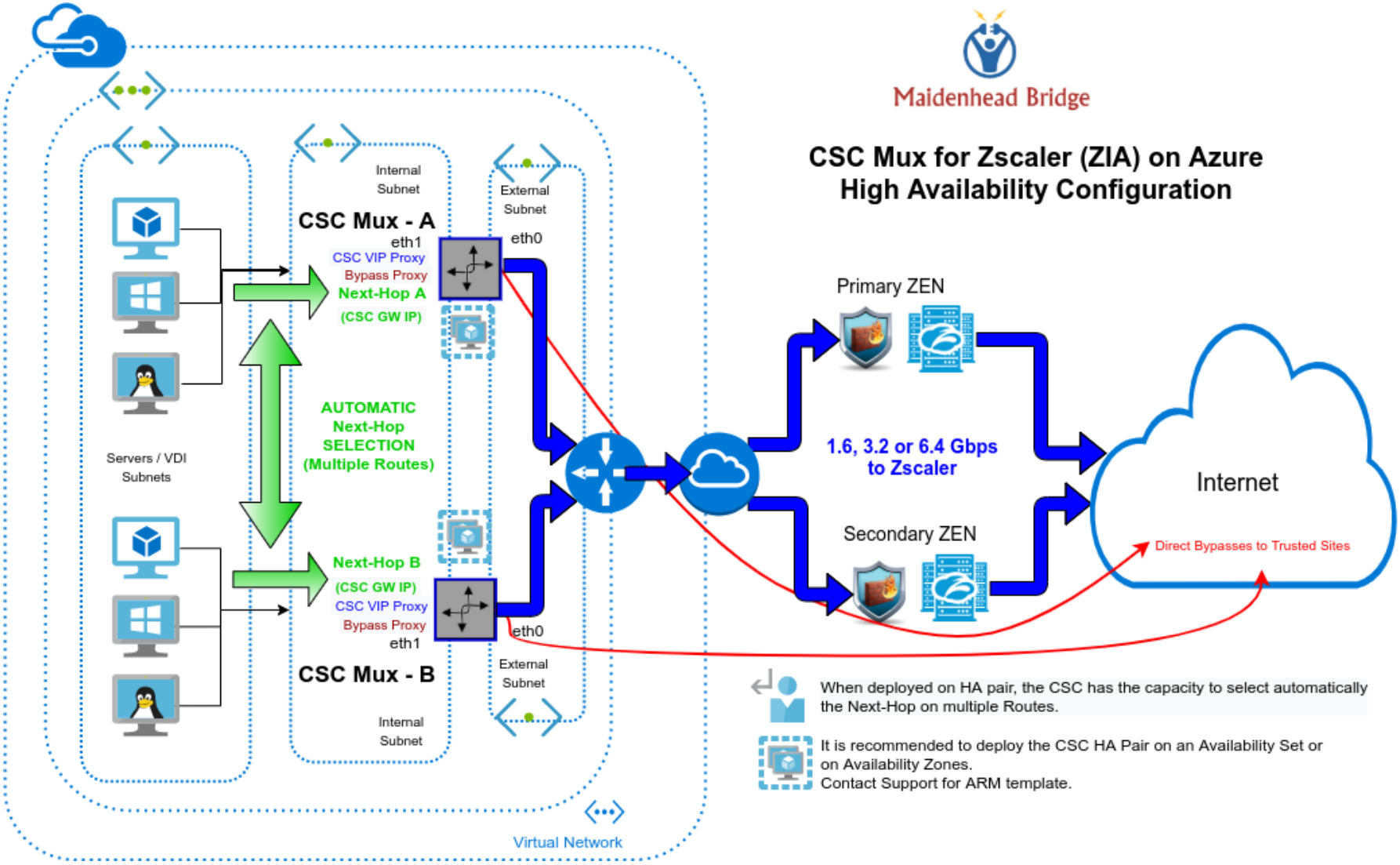
All Zscaler functionalities are available: Cloud Firewall and Web Security. Internal IPs are completely visible on the Zscaler Console.

In addition to this, the CSC Mux provides an easy way to manage direct bypasses to trusted sites.

2 Key benefits of the CSC Multiplex for Azure

- Solves the limitation of speed to Zscaler when using IPsec tunnels.
- Enables to connect any Azure internal resources to Zscaler Cloud Security Services at Gigabit speeds: 1.6 Gbps (CSC Mux 1.6G) or 3.2 Gbps (CSC Mux 3.2G).
- When configured as High Availability pair, you can duplicate your capacity for Web Traffic to 3.2 Gbps (CSC Mux 1.6G) or 6.4 Gbps (CSC Mux 3.2G).
- The deployment of the CSC Mux is automated using ARM templates.
- Easy Configuration: Insert your VPN Credentials and select the Zscaler Nodes.
- Full tunnel redundancy and balancing.
- High Availability via automatic Route configuration and redundant proxies.
- The CSC Mux comes with all parametrization required for Azure and Zscaler with the optimal values according to Zscaler Best practices.
- With the CSC Mux, you can use all Zscaler ZIA functionalities: Firewall and Web Security.
- Complete visibility of internal IPs.
- The CSC Mux provides an easy way to manage direct bypasses to trusted sites using your public IP.
- No operational burden for Administrators.
- The CSC Mux provides an outstanding value for money. The CSC Mux is multiple devices: a Load Balancer, a Firewall, a VPN Concentrator, a Router and a Proxy.

3 The CSC MUX on the Azure architecture



3.1 What problem the CSC Multiplex solves?

GRE tunnels are the recommended method to forward traffic to Zscaler, but Azure cloud doesn't support GRE (Generic Router Encapsulation) packets.

From: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-faq

What protocols can I use within VNets?

You can use TCP, UDP, and ICMP TCP/IP protocols within VNets. Unicast is supported within VNets, with the exception of Dynamic Host Configuration Protocol (DHCP) via Unicast (source port UDP/68 / destination port UDP/67) and UDP source port 65330 which is reserved for the host. Multicast, broadcast, IP-in-IP encapsulated packets, and Generic Routing Encapsulation (GRE) packets are blocked within VNets.

IPsec tunnels to Zscaler can go up to 400 Mbps only. If you need more bandwidth to Zscaler, you need to aggregate multiple tunnels to Zscaler from different Public IPs, as this article says:

From: https://help.zscaler.com/zia/configuring-ipsec-vpn-tunnel

Zscaler IPSec tunnels support a limit of 400 Mbps for each public source IP address. If your organization wants to forward more than 400 Mbps of traffic, Zscaler recommends configuring more IPSec VPN tunnels with different public source IP addresses. For example, if your organization forwards 800 Mbps of traffic, you can configure two primary VPN tunnels and two backup VPN tunnels. If your organization forwards 1200 Mbps of traffic, you can configure three primary VPN tunnels and three backup VPN tunnels.

Suppose you want to create a setup of Gigabits per second to Zscaler with discrete elements. In that case, you will find that is not possible in most cases or extremely expensive. You will need to implement and configure several components: Firewall, Load balancers, Routers, VPN Concentrators, Etc.

The CSC Multiplex has everything ready to work. You don't need to worry about the complexity of the solution.

The CSC Multiplex provides connectivity to all ports and protocols to Zscaler without restrictions and interacts with the Azure fabric to provide High Availability.

Your only task is to input the IPsec VPN credential.

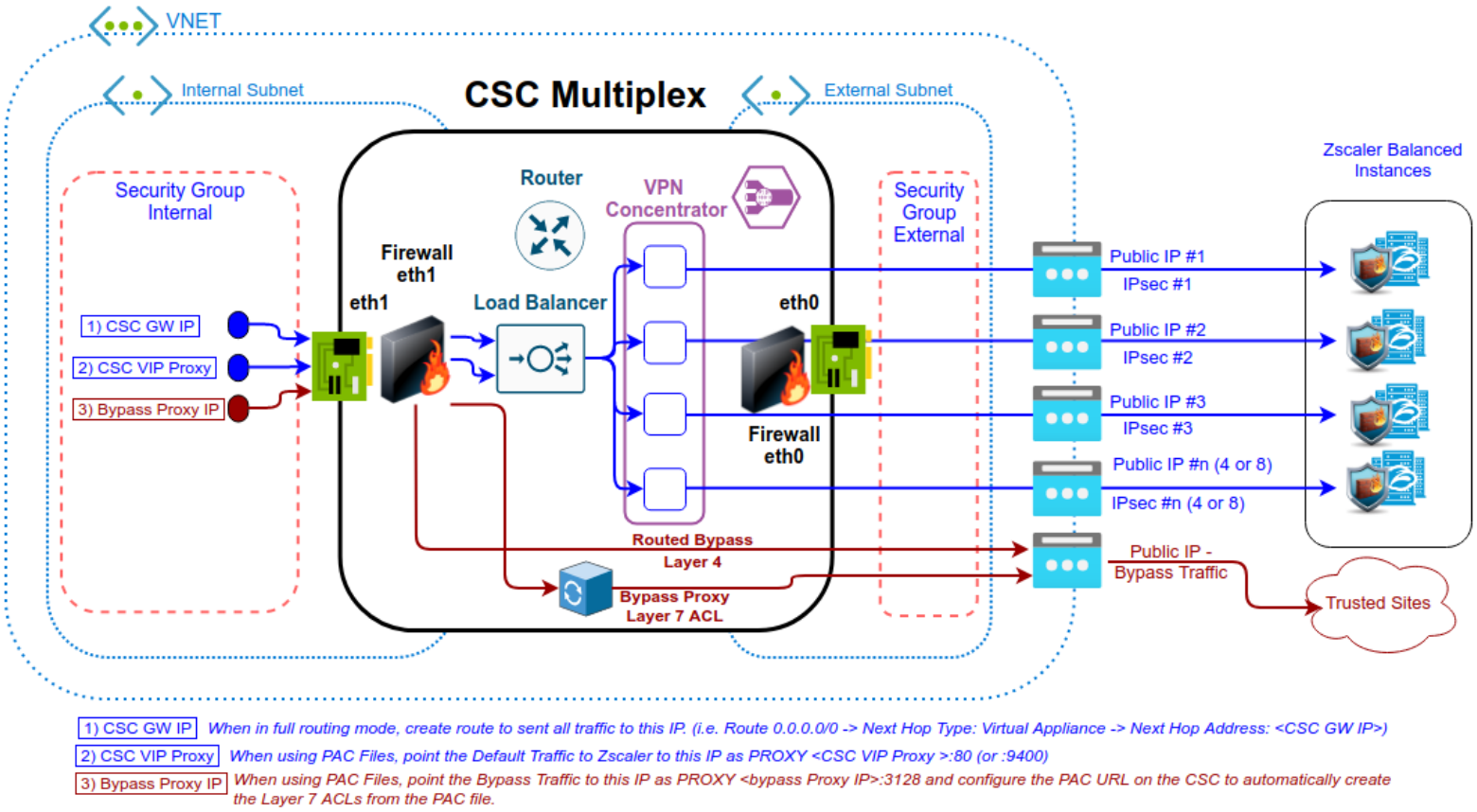
Problem solved. You can overcome the limitation of IPsec tunnels to Zscaler quickly and reach speeds up to 6.4 Gbps.

3.2 What does the CSC Multiplex do?

The CSC Multiplex does the job of multiple devices: Firewall, Load Balancer, VPN Concentrator, Router and Proxy and there are two models:

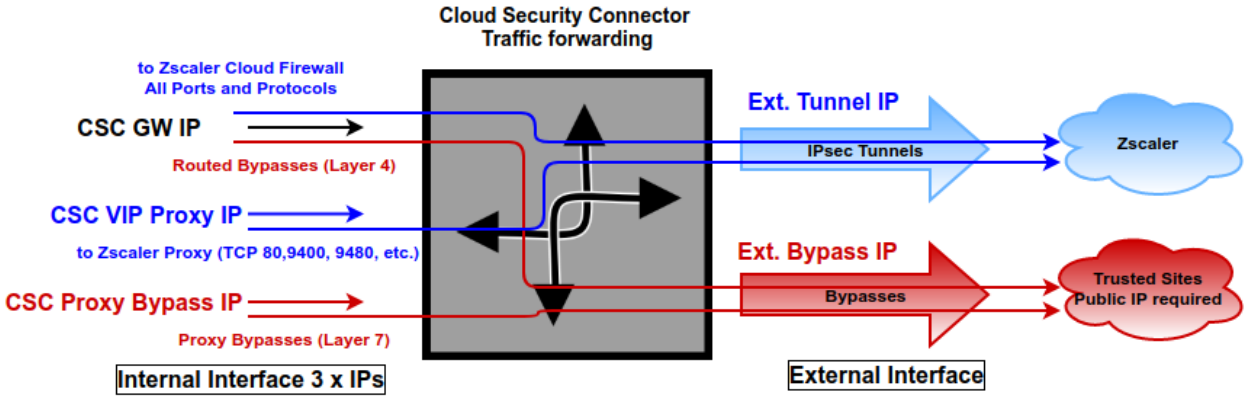
1. CSC Mux 1.6 Gbps: This model aggregates 4 x IPsec Tunnels.
2. CSC Mux 3.2 Gbps: This model aggregates 8 x IPsec Tunnels.

The following diagram shows the internal architecture of the CSC Multiplex:



3.3 Traffic forwarding with CSC Mux

The following image show the traffic forwarding when using the CSC Mux. In blue, traffic to Zscaler. In red, bypass traffic to Trusted sites via your Public IP.



The function of each IP is the follwing:

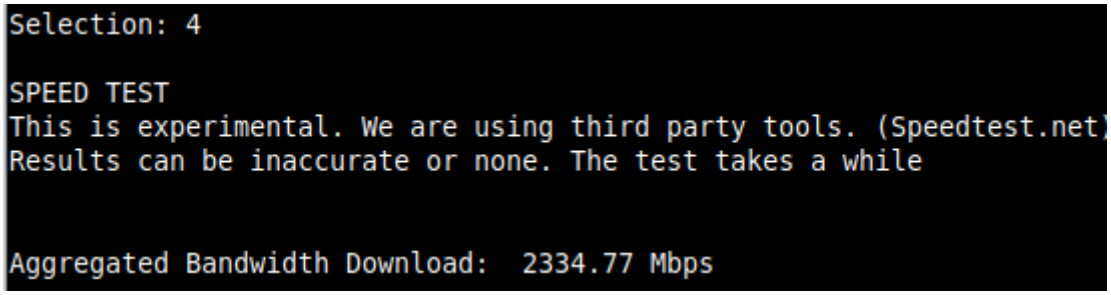
IP	Type	Function
CSC GW	Gateway	Used as Gateway for traffic to Zscaler and bypasses using "Routed Bypass" (Layer 4) functionality.
CSC Vip Proxy	Proxy	Used as Proxy for traffic to Zscaler.
CSC Proxy Bypass	Proxy	User as Proxy for bypasses using "Proxy Bypass" (Layer 7) functionality.

Section 3.5.1 provides a Real Case Scenario showing the use of each IP.

3.4 The CSC Multiplex in action

3.4.1 Speed Test with CSC Mux 1.6 Gbps

The following image is showing a CSC Mux 1.6 Gbps when running a Speed Test simultaneously on all 4 x IPsec tunnels:

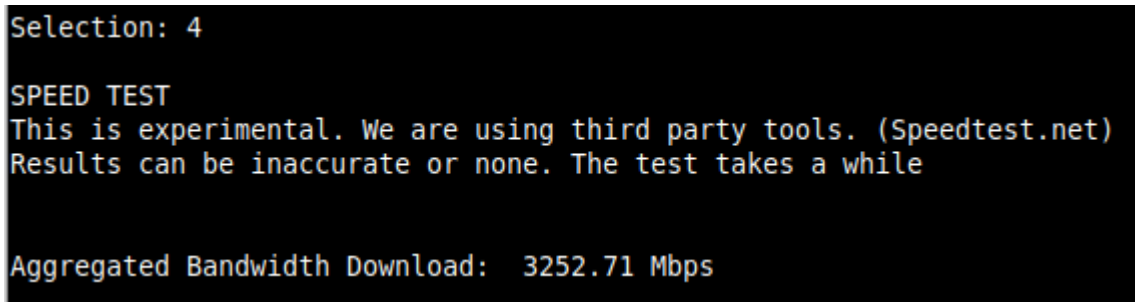


The aggregate bandwidth is 2334.77 Mbps (2.3 Gbps)

Note: During short periods, speeds can go more than 1.6 Gbps, but Zscaler will rate limit each tunnel to a maximum of 400 Mbps (4 x 400Mbps = 1.6 Gbps)

3.4.2 Speed Test with CSC Mux 3.2 Gbps

The following image is showing a CSC Mux 3.2 Gbps when running a Speed Test simultaneously on all 8 x IPsec tunnels:



The aggregate bandwidth is 3252.71 Mbps (~ 3.2 Gbps)

3.5 CSC deployed as High Availability pair (HA pair)

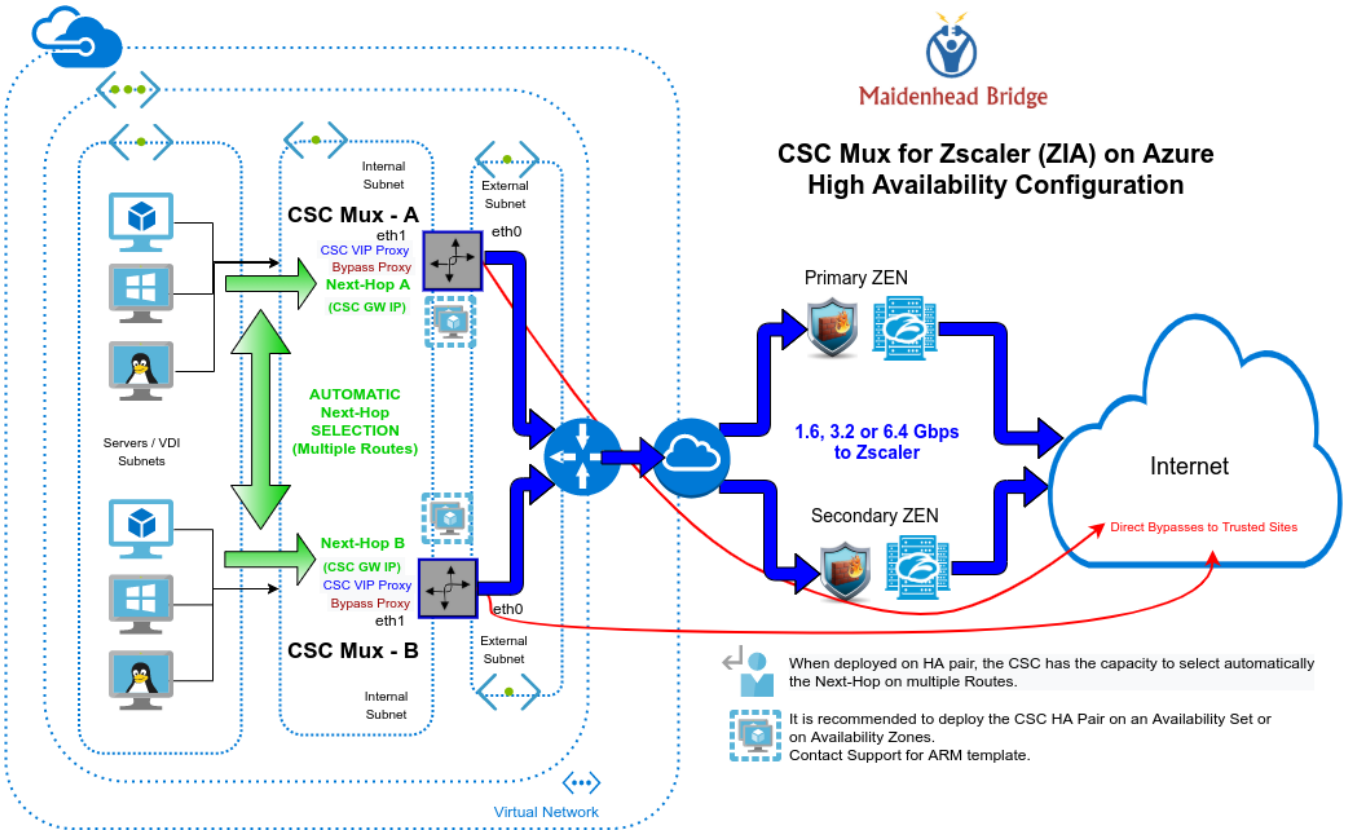
The most common scenario is to deploy the CSC Mux in a HA pair on Availability Set or Availability Zones.

When deployed as HA pair, the CSC can control the next-Hop on multiple routes. In addition to this, you can use both simultaneously for Web Traffic and achieve 6.4 Gbps to Zscaler.

3.5.1 Real Case Scenario: Routing, Explicit Proxy and PAC files.

The diagram below is a current customer with the following requirements:

1. Send all ports and protocols to Zscaler and reach Trusted Sites using your Public IP (Routed Bypass - Layer 4).
2. To provide redundancy to servers that do not support PAC files. Only Explicit Proxy (Single IP) can be configured and reach Trusted Sites using your Public IP (Routed Bypass).
3. To provide the maximum bandwidth available to Virtual Desktops (or any device that can use PAC file) using both CSC simultaneously for Web Traffic and reach Trusted Sites using your Public IP. (Routed Bypass - Layer 4 or Proxy Bypass - Layer 7).



To achieve this objective, we deployed a CSC Mux on HA pair.

3.5.1.1 Routing and Explicit proxy: Solving requirements 1 and 2

To solve the requirements 1) and 2), the CSC Mux on HA pair will manage the Routes on the Routing Tables to select the best exit to Zscaler.

In the case of 1) the CSC Mux Hair Par will control de default routes Next-Hop to Zscaler for the server farm.

Default Route to Internet → 0.0.0.0/0

All traffic to Zscaler:

Routes

Search routes

Name	Address prefix	Next hop
CSC-Zscaler-Default	0.0.0.0/0	172.31.200.17

In the case of 2), we are going to use the Zscaler Global Proxy IP as Explicit Proxy on the servers.

You can use any of this values:

Zscaler Global ZEN IP addresses → 185.46.212.88/32, 185.46.212.89/32, 185.46.212.90/32, 185.46.212.91/32, 185.46.212.92/32, 185.46.212.93/32, 185.46.212.97/32, 185.46.212.98/32.

The CSC Mux HA pair will control this routes to Zscaler Global ZEN IP address.

To Zscaler Global ZENs:

Routes

Search routes

Name	Address prefix	Next hop
server-farm-1	185.46.212.88/32	172.31.200.17

The CSC on the HA Pair will manage the Next Hop this this Address Prefix: 185.46.212.88/32

IMPORTANT: The Next-Hop IP is the CSC GW IP.

3.5.1.2 Case 1, 2 and 3: Routed Bypasses - Layer 4

Routed Bypasses works in a similar way to an outbound Azure Security Group. You can create rules per Source IP, Destination IP, Protocol (UDP / TCP) and destination port.

The configuration file for Routed Bypasses is a JSON file with the following format:

```
{
  "routedBypassRules": [
    {
      "description": "O365 Login URLs 1",
      "ipProtocol": "tcp",
      "sourceCirdIp": "0.0.0.0/0",
      "destinationCirdIp": "20.190.128.0/18",
      "fromPort": "80",
      "toPort": "80"
    },
    {
      "description": "O365 Login URLs 2",
      "ipProtocol": "tcp",
      "sourceCirdIp": "0.0.0.0/0",
      "destinationCirdIp": "20.190.128.0/18",
      "fromPort": "443",
      "toPort": "443"
    },
    {
      "description": "O365 Login URLs 3",
      "ipProtocol": "tcp",
      "sourceCirdIp": "0.0.0.0/0",
      "destinationCirdIp": "40.126.0.0/18",
      "fromPort": "80",
      "toPort": "80"
    },
    {
      "description": "portquiz.net",
      "ipProtocol": "tcp",
      "sourceCirdIp": "0.0.0.0/0",
      "destinationCirdIp": "52.47.209.216/32",
      "fromPort": "80",
      "toPort": "80"
    },
    {
      "description": "O365 Login URLs 4",
      "ipProtocol": "tcp",
      "sourceCirdIp": "0.0.0.0/0",
      "destinationCirdIp": "40.126.0.0/18",
      "fromPort": "443",
      "toPort": "443"
    },
    {
      "description": "Skype and Teams UDP 1",
      "ipProtocol": "udp",
      "sourceCirdIp": "0.0.0.0/0",
      "destinationCirdIp": "13.107.64.0/18",
      "fromPort": "3478",
      "toPort": "3481"
    },
    {
      "description": "Skype and Teams UDP 2",
      "ipProtocol": "udp",
      "sourceCirdIp": "0.0.0.0/0",
      "destinationCirdIp": "52.112.0.0/14",
      "fromPort": "3478",
      "toPort": "3481"
    },
    {
      "description": "Skype and Teams UDP 3",
      "ipProtocol": "udp",
      "sourceCirdIp": "0.0.0.0/0",
      "destinationCirdIp": "52.120.0.0/14",
      "fromPort": "3478",
      "toPort": "3481"
    }
  ]
}
```

To configure Routed Bypasses on the CSC, you paste the JSON file directly via the SSH console or configure an URL from where the CSC can retrieve the JSON file. You can create an object on a Blob container and configure the URL of the object on the CSC.

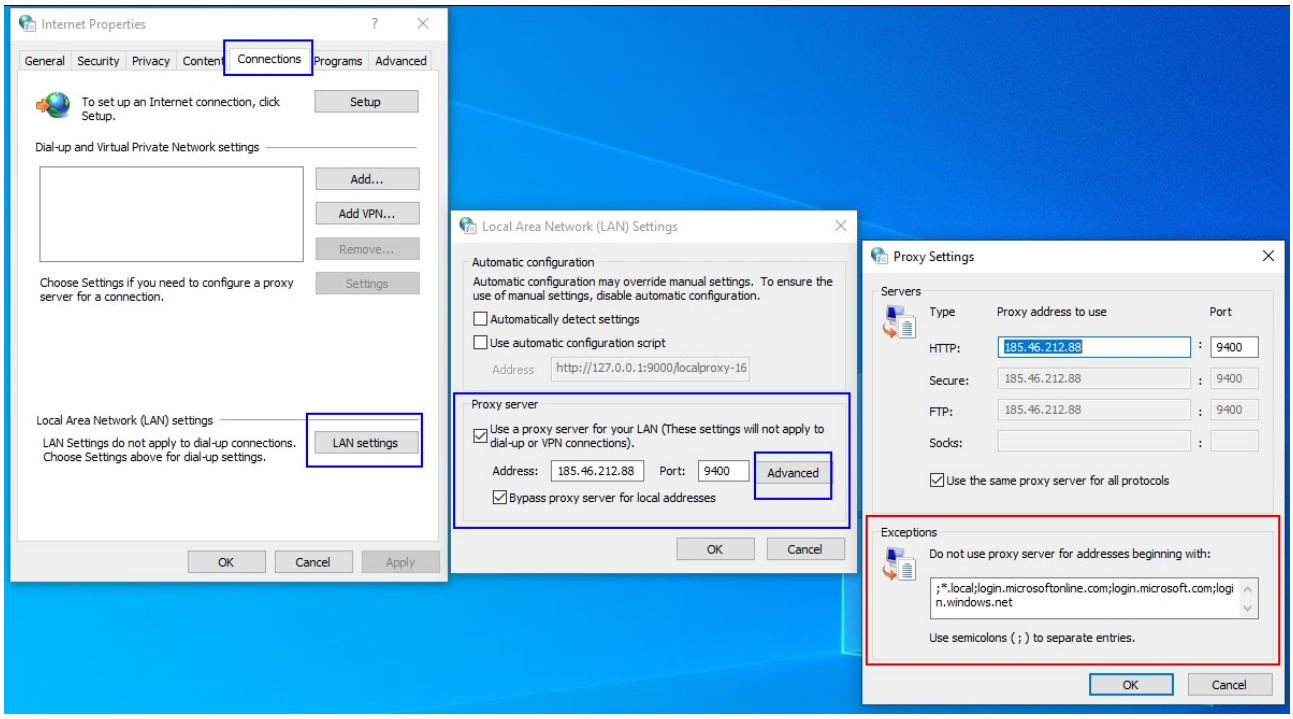
Routed Bypasses for Case 1 - Sending all ports and protocols via the CSC GW.

In this case, there is nothing to configure on the internal devices. The rules of Routed Bypass will inspect any traffic routed by the CSC GW IP. You can bypass any TCP or UDP traffic from Zscaler, for example, O365 Authentication URLs for Conditional Access rules and MFA, and Skype UDP real-time traffic.

Routed Bypasses for Case 2 - Servers with Explicit Proxy

In this case, the traffic sent via the Routed Bypass is configured on "Exceptions" (Windows) or "no_proxy" (Linux). Here is an example for each one.

Windows:



Linux (Ubuntu):

Dynamic setting:

```
export http_proxy="http://185.46.212.88:9400"
export ftp_proxy="http://185.46.212.88:9400"
export https_proxy="http://185.46.212.88:9400"
export no_proxy=localhost,127.0.0.0/8,10.0.0.0/8,172.16.0.0/12,192.168.0.0/16,*.local, login.microsoftonline.com, login.microsoft.com, login.windows.net
```

Remove Dynamic Settings:

```
unset http_proxy
unset ftp_proxy
unset https_proxy
unset no_proxy
```

Make settings permanent:

```
sudo nano /etc/environment
```

```
http_proxy="http://185.46.212.88:9400"
ftp_proxy="http://185.46.212.88:9400"
https_proxy="http://185.46.212.88:9400"
no_proxy=localhost,127.0.0.0/8,10.0.0.0/8,172.16.0.0/12,192.168.0.0/16,*.local,login.microsoftonline.com,login.microsoft.com,login.windows.net
```

Routed Bypasses for Case 3 - Devices with PAC files.

In this case, you need to create a section on the PAC file to send "DIRECT" the traffic via the Routed Bypass.

For example:

```
// Routed Bypass for O365 Login destinations: 20.190.128.0/18 and 40.126.0.0/18
if ((isInNet(host, "20.190.128.0", "255.255.192.0") ||
        isInNet(host, "40.126.0.0", "255.255.192.0"))) {
    return "DIRECT";
}
```

In the following section, we are talking about all options when using PAC files.

3.5.1.3 PAC files: Solving requirements Case 3

In Case 3, the Virtual Desktops are capable of being configured with PAC files. Due to both CSCs on the HA pair are active simultaneously, we can duplicate the bandwidth to Zscaler, achieving maximum throughput. In addition to this, using the Bypass functionality of the CSCs, it is possible to reach Trusted Sites via your Public IP and not Zscaler's IPs.

The CSC allows "Routed Bypasses" (Layer 4) and "Proxy Bypasses" (Layer 7).

As shown in previous pictures, the CSC has 3 Internal IPs:

CSC GW IP	Default Gateway for Routed traffic - On the PAC file, anything with "return DIRECT" will travel via this GW.
CSC VIP Proxy	Proxy to Zscaler.
CSC Bypass Proxy	Proxy for "Proxy Bypass" traffic.

PAC File for Virtual Desktops:

The following PAC file shows how to achieve 6.4 Gbps using the CSC Mux 3.2 Gbps as HA pair.

```
function FindProxyForURL(url, host) {
   // ==========================================================
   // Section 1: Zscaler standard PAC values

   var privateIP = /^(0|10|127|192\.168|172\.1[6789]|172\.2[0-9]|172\.3[01]|169\.254|192\.88\.99)\.[0-9.]+$/;
   var resolved_ip = dnsResolve(host);

   /* Don't send non-FQDN or private IP auths to us */
   if (isPlainHostName(host) || isInNet(resolved_ip, "192.0.2.0", "255.255.255.0") || privateIP.test(resolved_ip))
      return "DIRECT";

   /* FTP goes directly */
   if (url.substring(0, 4) == "ftp:")
      return "DIRECT";

   /* test with ZPA */
   if (isInNet(resolved_ip, "100.64.0.0", "255.255.0.0"))
      return "DIRECT";

   // ==========================================================
   // Section 2: Routed Bypass: Destination IPs / Networks going "DIRECT"
   // Routed Bypass for O365 Login destinations: 20.190.128.0/18 and 40.126.0.0/18
   if ((isInNet(host, "20.190.128.0", "255.255.192.0") ||
      isInNet(host, "40.126.0.0", "255.255.192.0"))) {
   return "DIRECT";
   }

   // ==========================================================
   // Section 3: Load Balancing: 2 x Cloud Security Connectors Multiplex 3.2 Gbps
   // Azure to Zscaler: 6.4 Gbps

   // Get NIC IP address
   nicIp = myIpAddress();

   // Assigning values to "tozscaler" and "bypass"
   if (isInNet(nicIp, "0.0.0.0", "0.0.0.1")) {
      var tozscaler = "PROXY csc1vip:80; PROXY csc2vip:80";
      var bypass = "PROXY csc1bypass:3128; PROXY csc2bypass:3128";
   }

   if (isInNet(nicIp, "0.0.0.1", "0.0.0.1")) {
      var tozscaler = "PROXY csc2vip:80; PROXY csc1vip:80";
      var bypass = "PROXY csc2bypass:3128; PROXY csc1bypass:3128";
   }

   // ==========================================================
   // Section 4: Proxy Bypass via Cloud Security Connectors

   // Proxy Bypass via CSC Public IPs (Examples)
   // Okta Domains (for Location Rules)
   if ((shExpMatch(host, "*.okta.com")) ||
      (shExpMatch(host, "*.oktacdn.com")) ||
```

```
        (shExpMatch(host, "*.okta-emea.com")) ||
        // Trusted Sites
        (shExpMatch(host, "trusted.domain.com")) ||
        (shExpMatch(host, "trusted2.domain.com")) ||
        (shExpMatch(host, "*.trusted-domain.com")) ||
        // O365 Domains for ConditionalAccess
        (shExpMatch(host, "login.microsoftonline.com")) ||
        (shExpMatch(host, "login.microsoft.com")) ||
        (shExpMatch(host, "login.windows.net")) ||
        // IP / Port test page
        (shExpMatch(host, "portquiz.net"))) {
        return bypass
    }

    // ==========================================================
    // Section 5: Default Traffic

    /* Default Traffic Forwarding. Forwarding to Zen on port 80, but you can use port 9400 also */
    return tozscaler
}
```

Sections Explained:

Section 1:	Zscaler Standard PAC values to: Do not send Private IPs to Zscaler or ZPA or FTP traffic.
Section 2:	Shows Destinations IP / Networks sent DIRECT that you want to reach using your Public IP using Routed Bypasses. (L4)
Section 3:	Section 2 does the load balancing between both CSC on the HA pair. As you can see, we are reading the source IP of the VDI (nicIp = myIpAddress();), and we are load balancing by odd/even IP, using different primary/secondary cscvip and cscbypass for odd/even IPs.
Section 4:	Section 4 shows examples of URLs to bypass from Zscaler to reach the destination website with your Public IP. Examples of required URLs for OKTA (for Location rules) and O365 (for Conditional Access) are shown. One common use of these examples is not asking for MFA (Multi-factor Authentication) for VDIs.
Section 5:	Default traffic will go via Zscaler.

Proxy Bypass: PAC file for the CSCs

The Proxy Bypass functionality of the CSC blocks all domains by default. You need to configure which domains (wildcards are accepted) you want to allow.

To make this simple, the CSC is capable of reading PAC files. Your only task is to create a PAC file for the CSC (copying and pasting section 3 of VDI's PAC file) and to configure the PAC file URL on each CSC.

Here is the example of the PAC file for the CSC Routed Bypass functionality:

```
function FindProxyForURL(url, host) {
   // This value of bypass on the PAC file for the CSC can be any.
   // We need to assigned a value just to pass the "Validation" of the PAC on Zscaler console.
   var bypass = "PROXY 1.1.1.1:3128; PROXY 2.2.2.2:3128";

   // ==========================================================
   // Section 3: Bypass via Cloud Security Connectors

   // Bypass via CSC Public IPs (Examples)
   // Okta Domains (for Location Rules)
   if ((shExpMatch(host, "*.okta.com")) ||
      (shExpMatch(host, "*.oktacdn.com")) ||
      (shExpMatch(host, "*.okta-emea.com")) ||
      // Trusted Sites
      (shExpMatch(host, "trusted.domain.com")) ||
      (shExpMatch(host, "trusted2.domain.com")) ||
      (shExpMatch(host, "*.trusted-domain.com")) ||
      // O365 Domains for ConditionalAccess
      (shExpMatch(host, "login.microsoftonline.com")) ||
      (shExpMatch(host, "login.microsoft.com")) ||
      (shExpMatch(host, "login.windows.net")) ||
      // IP / Port test page
      (shExpMatch(host, "portquiz.net"))) {
      return bypass
      }

return bypass

}
```

4 Deploy the Cloud Security Connector

4.1 Prerequisites

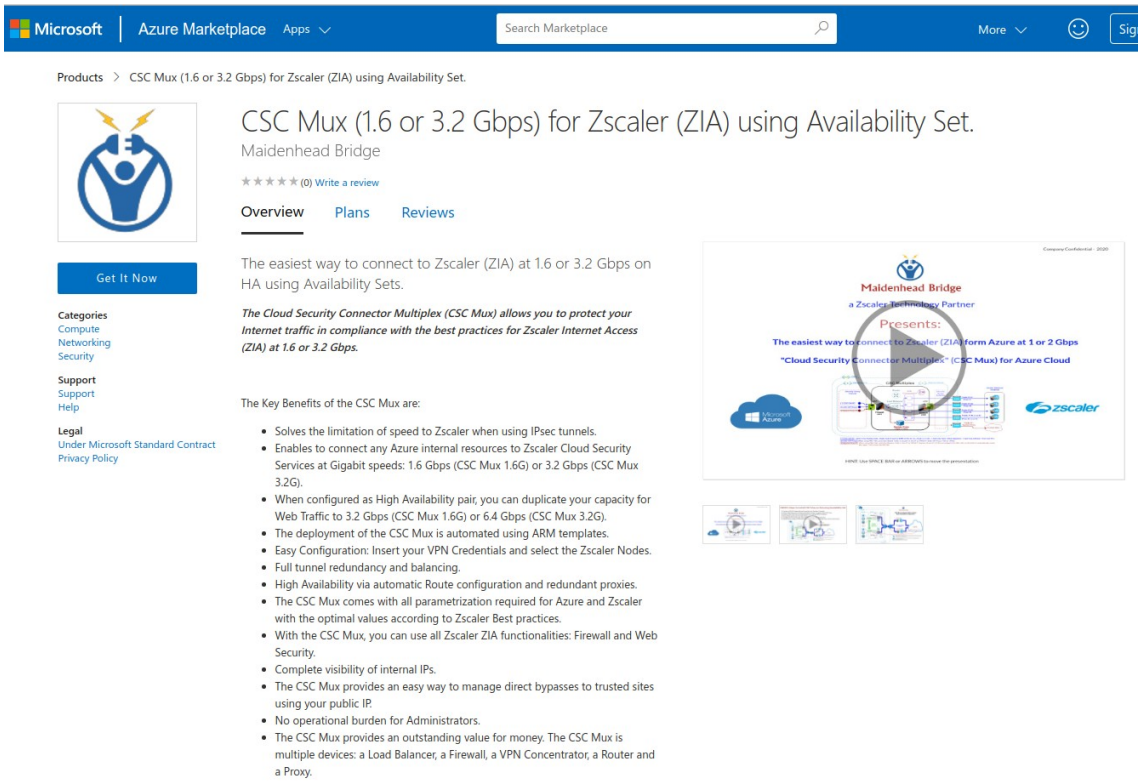
Before launching the CSC, you need to have these elements ready:

1. **(Optional) SSH Key:** If you want to access the CSC using SSH keys. If not, you can use a password during the installation.
2. **Virtual Network**
3. **External Subnet:** The External Subnet must be on the same Virtual Network as the Internal Subnet.
4. **Internal Subnet:** The Internal Subnet must be on the same Virtual Network as the External Subnet.

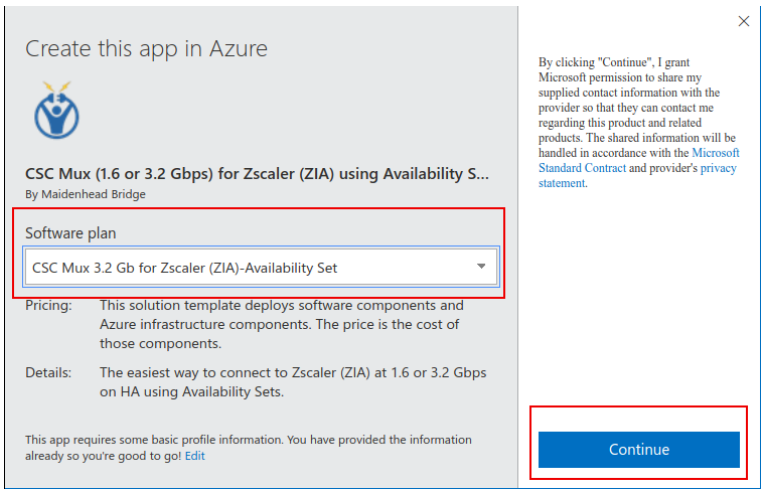
4.2 Launching the CSC from Azure Marketplace using Availability Sets

- Search for Maidenhead Bridge on the Azure Marketplace and select the offer:

CSC Mux (1.6 or 3.2 Gbps) for Zscaler (ZIA) using Availability Set

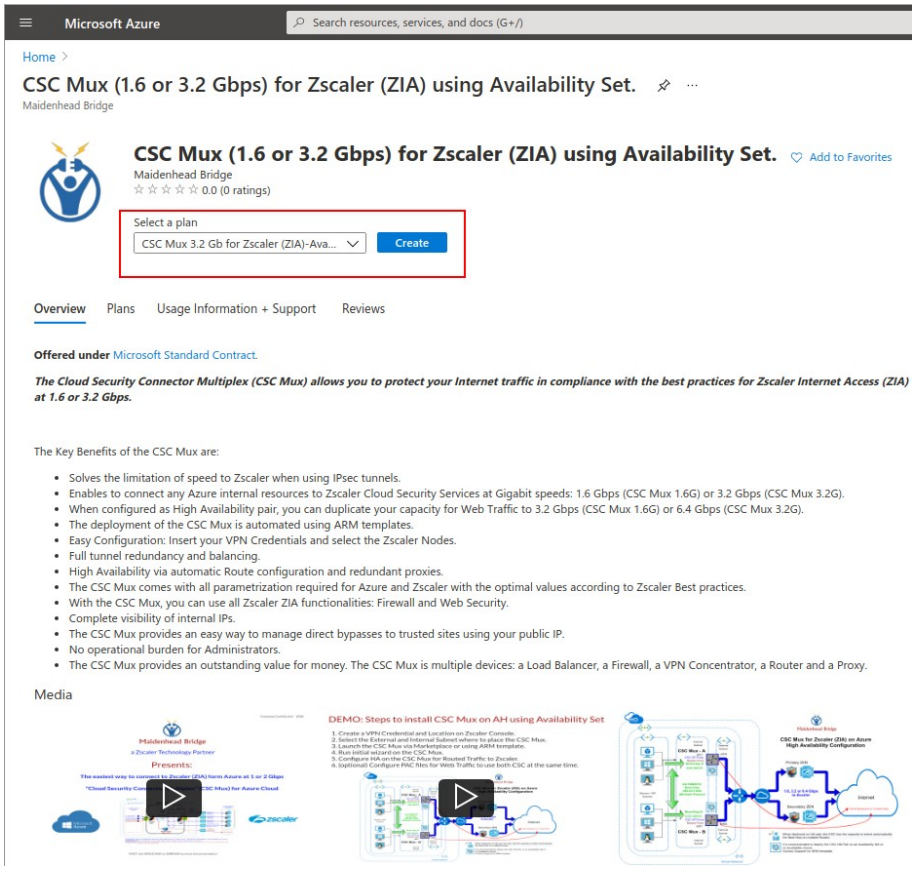


- Click "GET IT NOW" and select the Plan (1.6 Gbps or 3.2 Gbps)

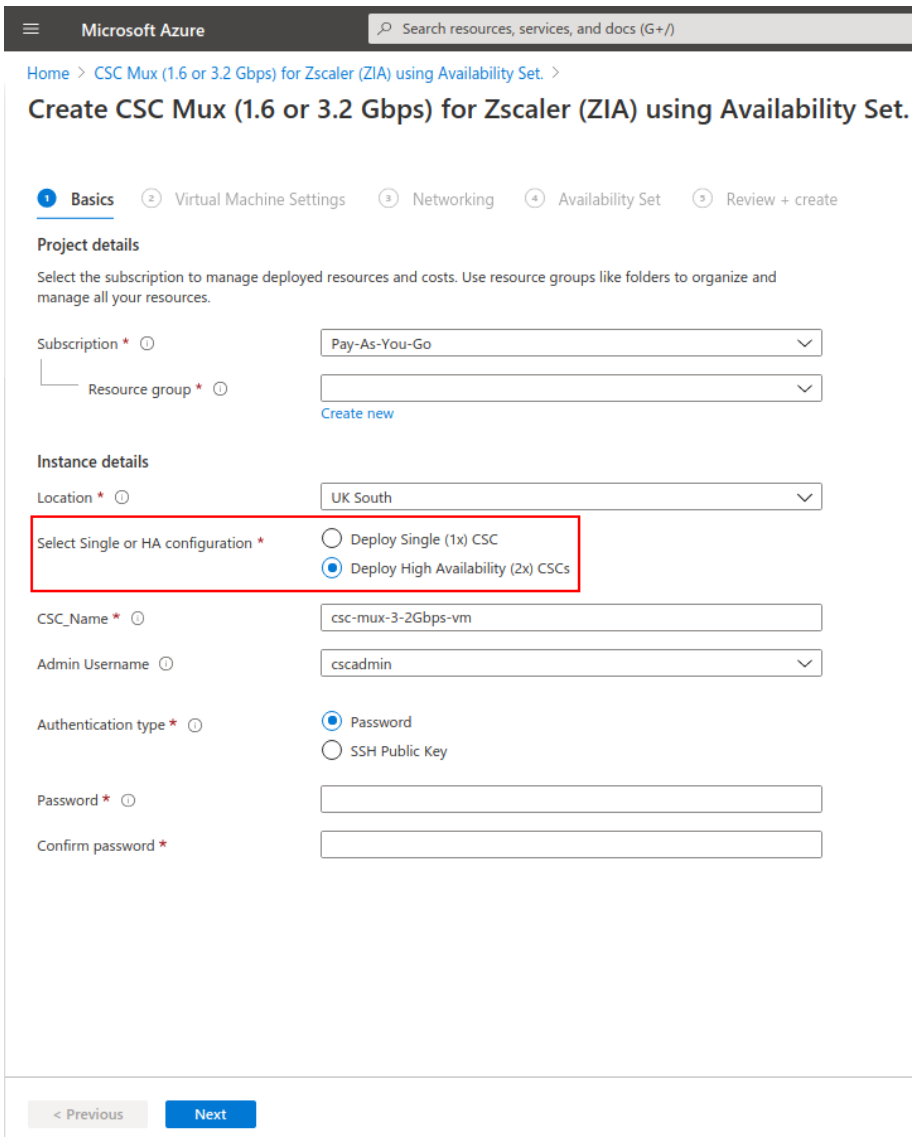


- Click "Continue"

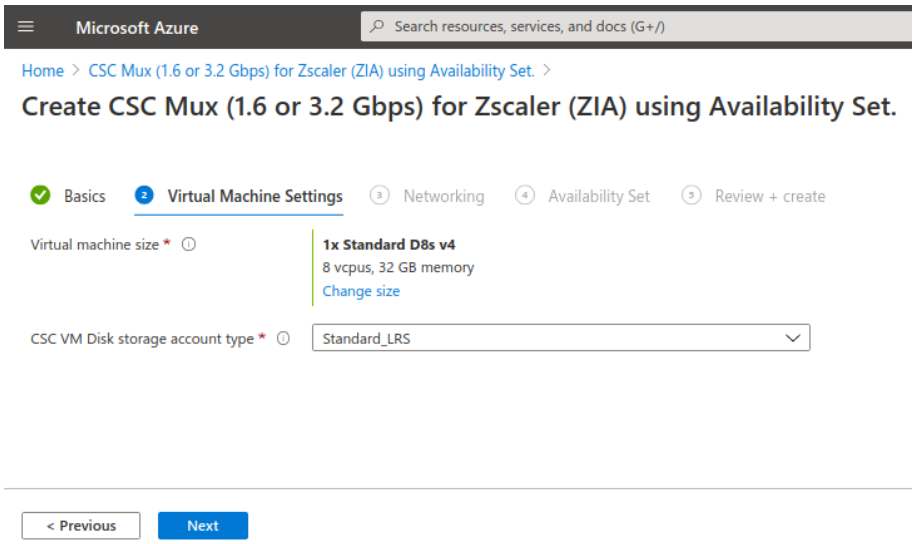
Important: You will be redirected to the Azure Portal. Please, double-check the section "Select plan."



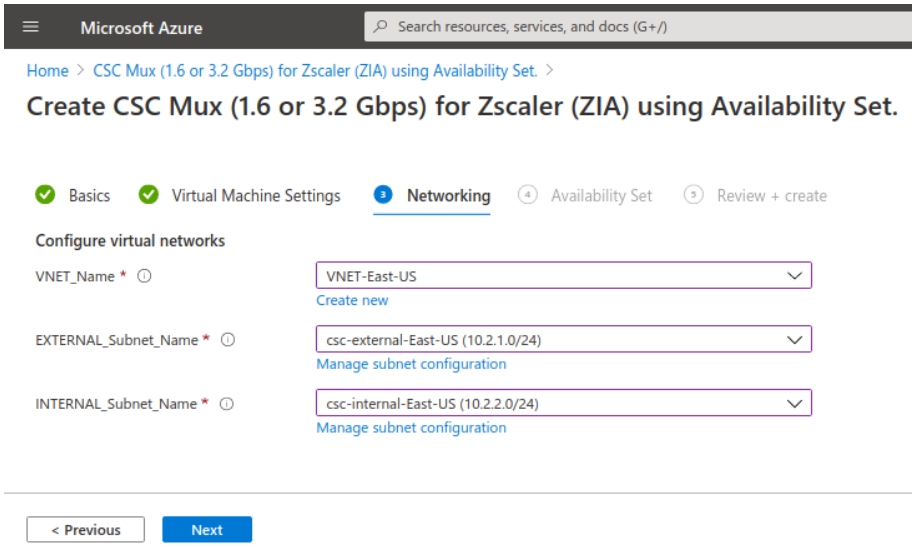
- Click "Create"



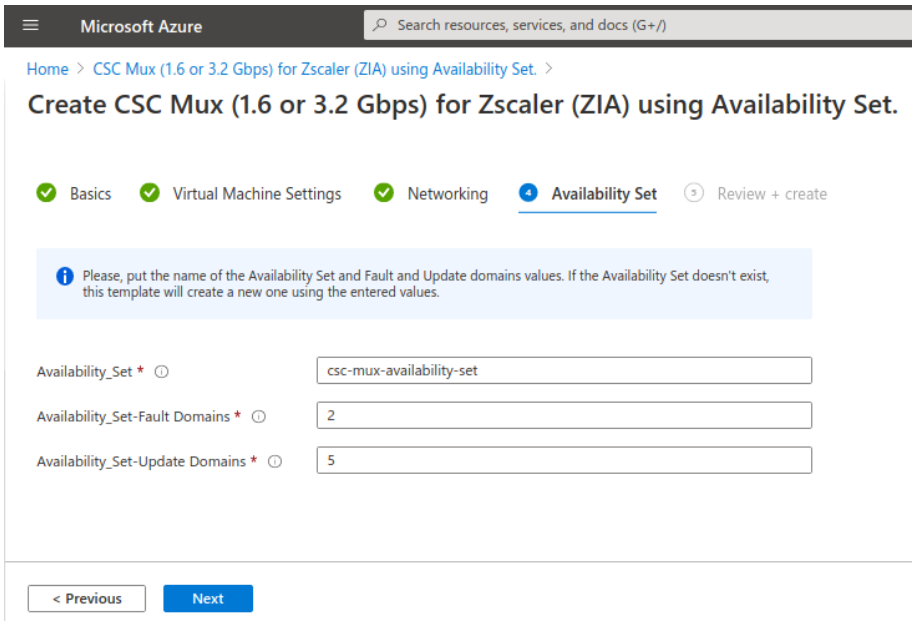
- Fill in the requested values. We recommend launching two to provide High Availability using Availability Sets.
- Click "Next"



- Select the Virtual Machine size and Storage. We recommend using the Virtual Machine Size suggested. If you want to change the values, take into account the minimum requirements:
  - CSC Mux 1.6 Gbps requires 2 x Cores, 4GB RAM and Accelerated Networking.
  - CSC Mux 2.6 Gbps requires 4 x Cores, 8GB RAM and Accelerated Networking.
- Click "Next"

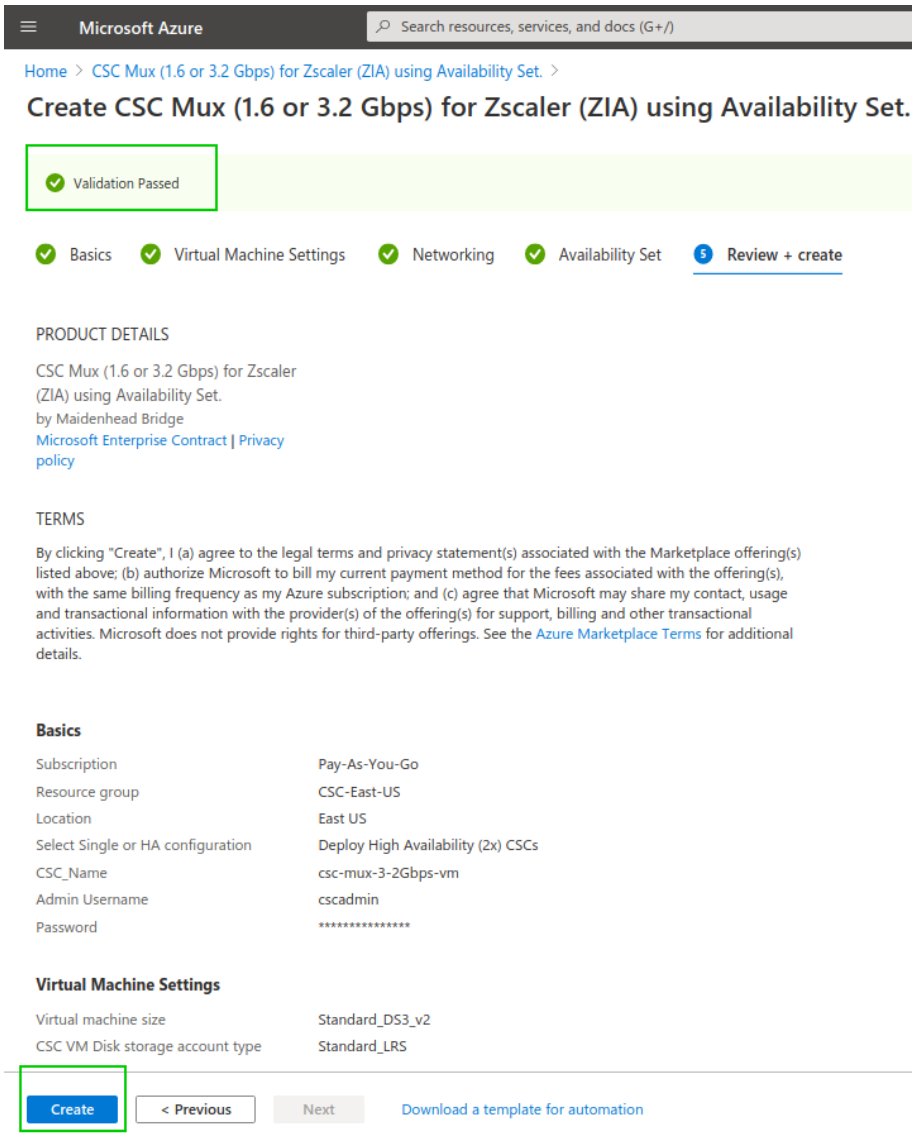


- Select the Virtual Network Name (VNET_Name) and the External and Internal Subnet to place the CSC Mux.
- Click "Next"

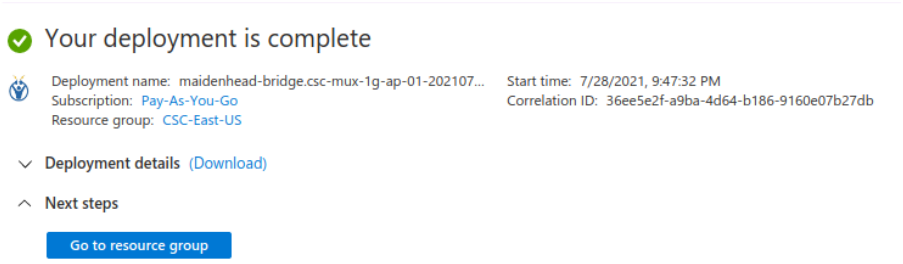


- Input the name of the Availability Set and Domain and Default values.
- Click "Next".
- wait for "Validation Passed"

Note: The most common reason why the Validation can fail is because the Quota Limits on Core and/or Public IPs. Here information how to increase your Quotas: https://docs.microsoft.com/en-us/azure/azure-portal/supportability/per-vm-quota-requests



- Click Create and wait for "Your deployment is complete"



- Click "Go to resource group"
- Done!

Next Steps:

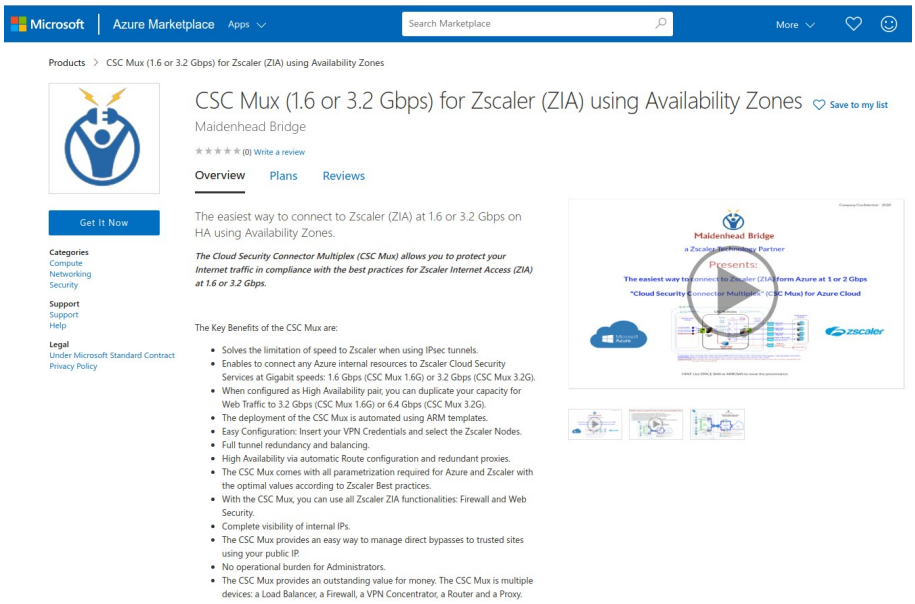
- On your Zscaler console, create:
    - VPN Credentials
    - Location using the VPN Credentials.
- On your Azure Console, select the Virtual Machines created and find the IP of the Internal Interface (<vmname>**-eth1**)
    - SSH the CSC (**cscadmin**@<IP Eth1>) and follow the Initial Wizard Menu. You will be asked for the VPN Credentials to select the Zscaler nodes Primary and Secondary, Etc.
    - After running the initial wizard, the CSC will be ready for Production.

*Important: The username to access the CSC is: "**cscadmin**"*

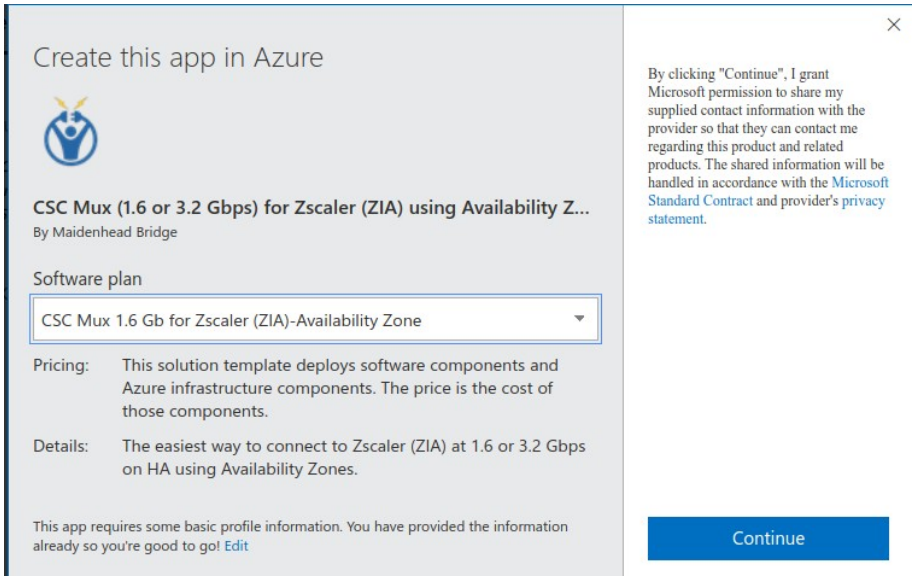
4.3 Launching the CSC from Azure Marketplace using Availability Zones

- Search for Maidenhead Bridge on the Azure Marketplace and select the offer:

CSC Mux (1.6 or 3.2 Gbps) for Zscaler (ZIA) using Availability Zones



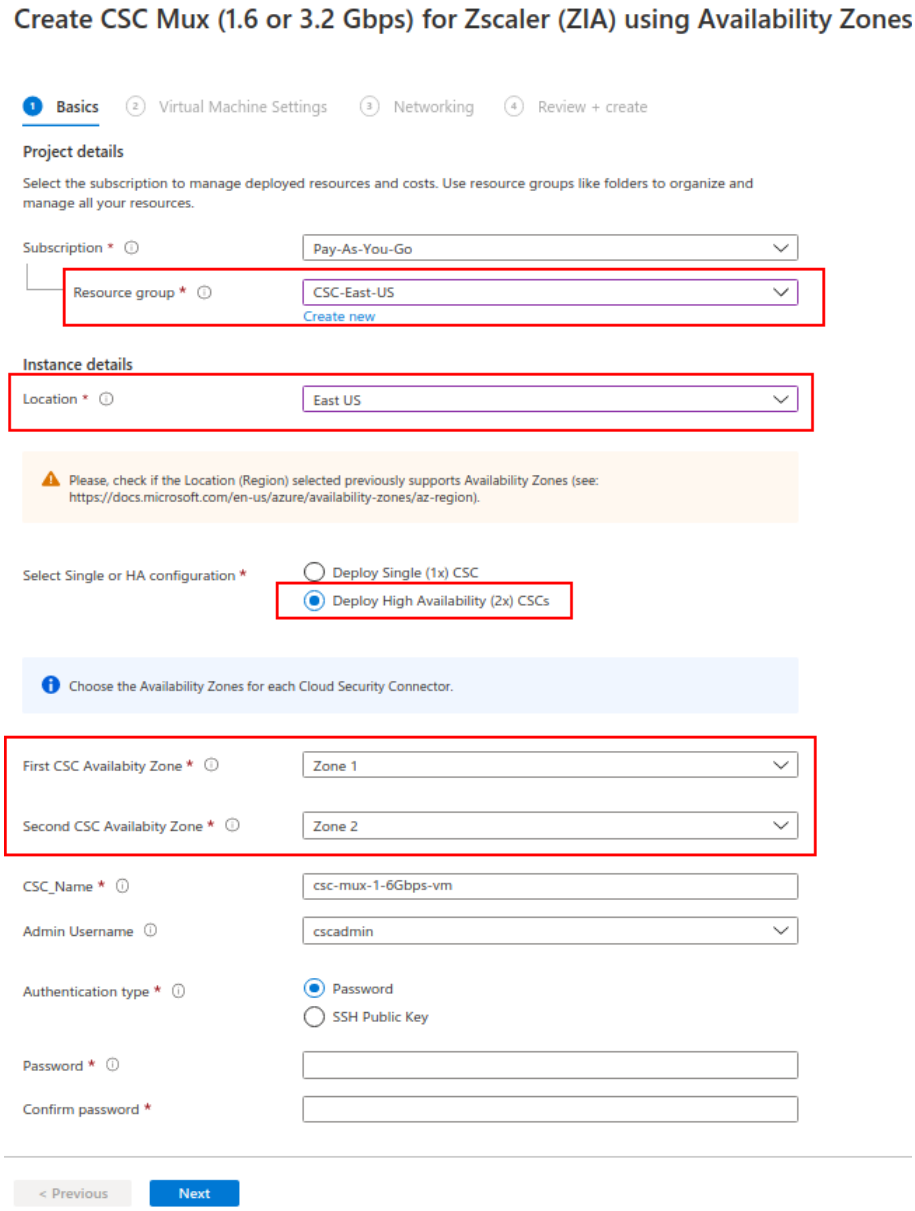
- Click "GET IT NOW" and select the Plan (1.6 Gbps or 3.2 Gbps)



- Click "Continue"

Important: You will be redirected to the Azure Portal. Please, double check the section "Select plan"

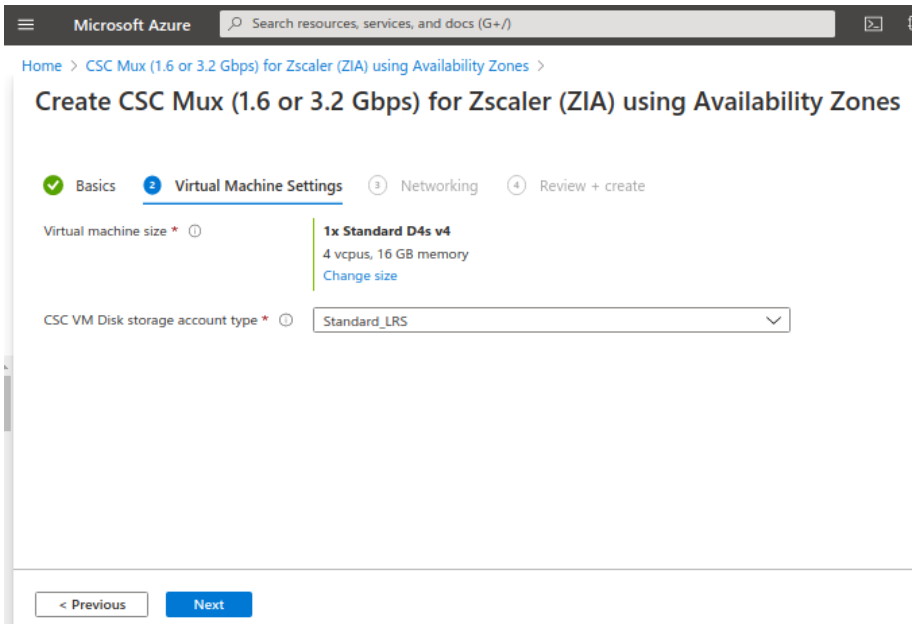
- Click "Create"



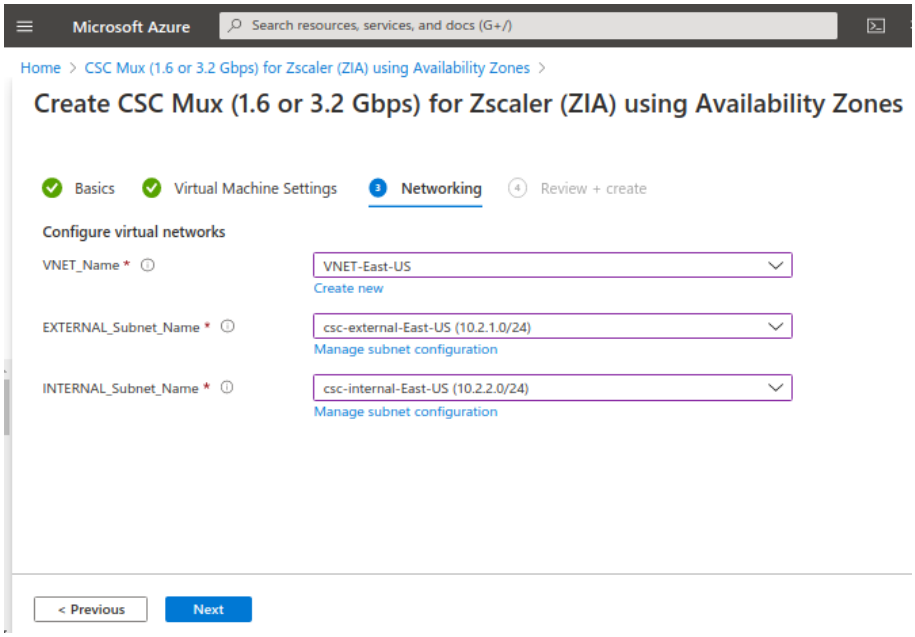
- Fill the values requested.

Note 1: Check of the Location (Region) supports Availability Zones. See: https://docs.microsoft.com/en-us/azure/availability-zones/az-region

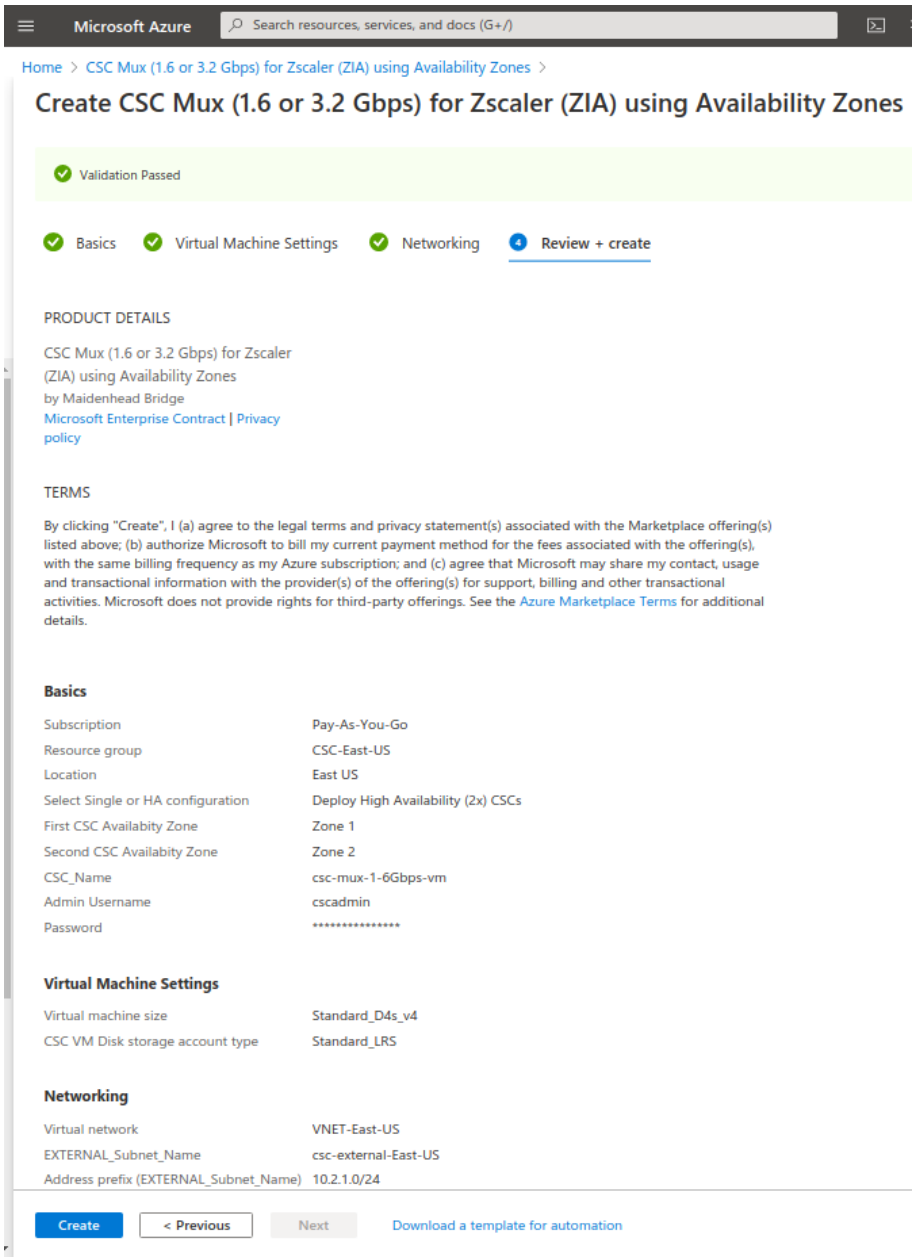
- Click "Next"



- Select the Virtual Machine size and Storage. We recommend using the Virtual Machine Size suggested. If you want to change the values, take into account the following:
  - CSC Mux 1.6 Gbps requires 2 x Cores, 4GB RAM and Accelerated Networking.
  - CSC Mux 3.2 Gbps requires 4 x Cores, 8GB RAM and Accelerated Networking.
- Click "Next"



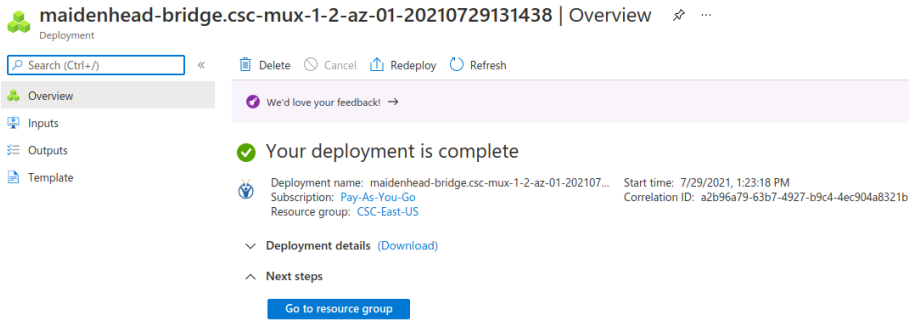
- Select the Virtual Network Name (VNET_Name) and the External and Internal Subnet where to place the CSC Mux.
- Click "Next"



- wait for "Validation Passed"

Note: The most common reason why the Validation can fail is Quota Limits on Core and Public IPs. Here is information on how to increase your Quotas: https://docs.microsoft.com/en-us/azure/azure-portal/supportability/per-vm-quota-requests

- Click Create and wait for "Your deployment is complete"



- Click "Go to resource group"
- Done!

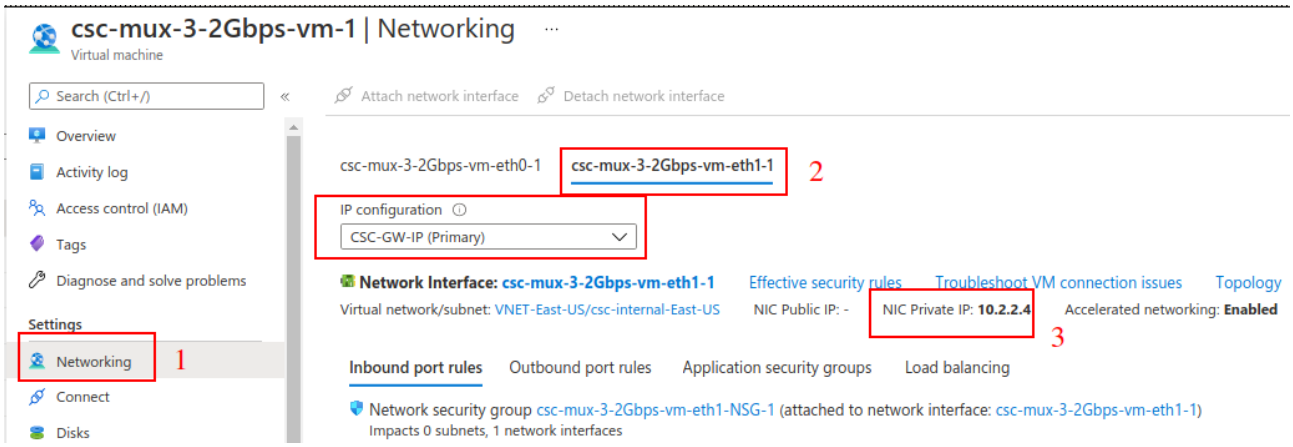
Next Steps:

- On your Zscaler console, create:
  - VPN Credentials
  - Location using the VPN Credentials.
- On your Azure Console, select the Virtual Machines created and find the IP of the Internal Interface (<vmname>**-eth1**)
  - SSH the CSC (**cscadmin**@<IP Eth1>) and follow the Initial Wizard Menu. You will be asked for the VPN Credentials to select the Zscaler nodes Primary and Secondary, Etc.
  - After running the initial wizard, the CSC will be ready for Production.

*Important: The username to access the CSC is: "**cscadmin**"*

5 Accessing for the first time to your CSC

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

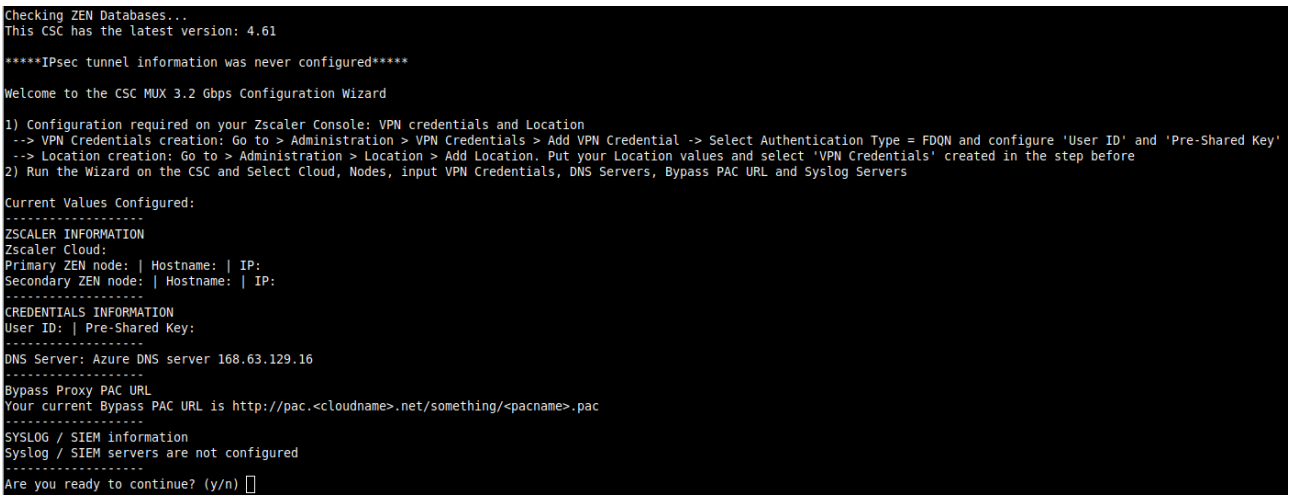


2. In this example, "NIC Private IP" is: 10.2.2.4

3. From a machine inside the Virtual Network, ssh the CSC using the Key, like:

ssh -i <keyname.pem> cscadmin@<eth1 Private IP> or ssh cscadmin@<eth1 Private IP> if using password.

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



```
Checking ZEN Databases...
This CSC has the latest version: 4.61

*****IPsec tunnel information was never configured*****

Welcome to the CSC MUX 3.2 Gbps Configuration Wizard

1) Configuration required on your Zscaler Console: VPN credentials and Location
 --> VPN Credentials creation: Go to > Administration > VPN Credentials > Add VPN Credential -> Select Authentication Type = FDQN and configure 'User ID' and 'Pre-Shared Key'
 --> Location creation: Go to > Administration > Location > Add Location. Put your Location values and select 'VPN Credentials' created in the step before
2) Run the Wizard on the CSC and Select Cloud, Nodes, input VPN Credentials, DNS Servers, Bypass PAC URL and Syslog Servers

Current Values Configured:
-------------------
ZSCALER INFORMATION
Zscaler Cloud:
Primary ZEN node: | Hostname: | IP:
Secondary ZEN node: | Hostname: | IP:
-------------------
CREDENTIALS INFORMATION
User ID: | Pre-Shared Key:
-------------------
DNS Server: Azure DNS server 168.63.129.16
-------------------
Bypass Proxy PAC URL
Your current Bypass PAC URL is http://pac.<cloudname>.net/something/<pacname>.pac
-------------------
SYSLOG / SIEM information
Syslog / SIEM servers are not configured
-------------------
Are you ready to continue? (y/n)
```

4. Your CSC is ready for the initial configuration. Just follow the instructions of the Configuration Wizard.

6 Initial Wizard Configuration

Please, follow these instructions to run the initial configuration of the CSC for Azure:

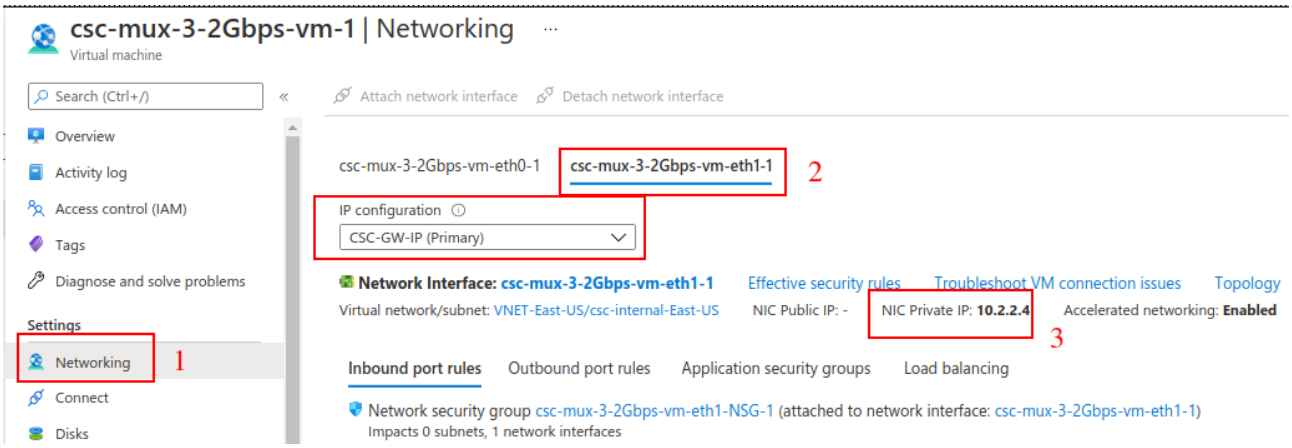
6.1 Short Version

Configuration required on your Zscaler Console: VPN credentials and Location

1. VPN Credentials creation: Go to > Administration > VPN Credentials > Add VPN Credential -> Select Authentication Type = FDQN and configure 'User ID' and 'Pre-Shared Key'
2. Location creation: Go to > Administration > Location > Add Location. Put your Location values and select 'VPN Credentials' created in the step before
3. Run the Wizard. Insert the values. Confirm and reboot.
4. Done!

6.2 Long Version (with Example)

In this example, the CSC GW IP is 10.2.2.4



After doing an SSH to the CSC Mux, the initial wizard appear.

In this example:

Username: cscadmin (use always "cscadmin")

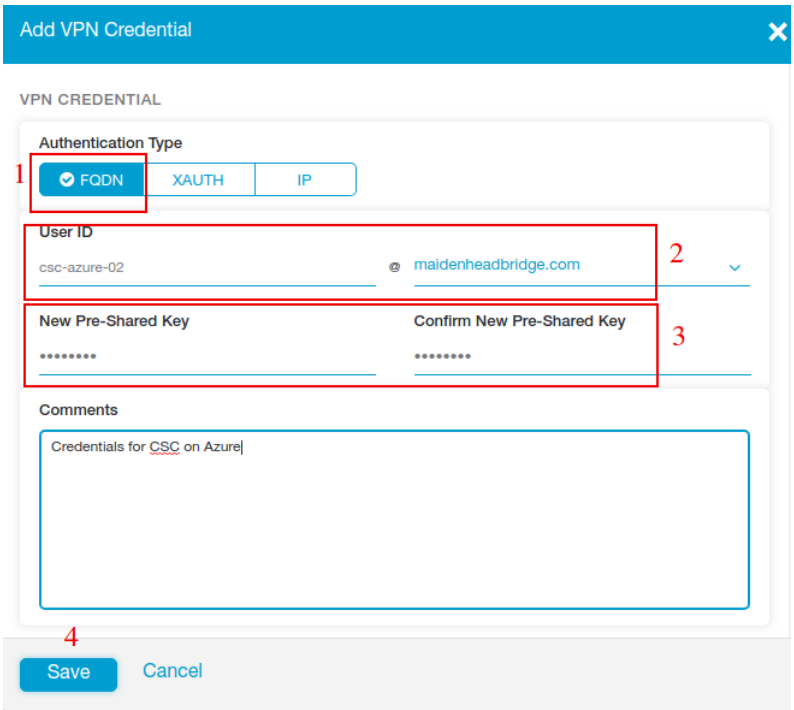
CSC IP: 10.2.2.4

$ ssh *cscadmin@10.2.2.4*
(Please, wait 2 minutes after power on or reboot to SSH the CSC.)

```
Checking ZEN Databases...
This CSC has the latest version: 4.61

*****IPsec tunnel information was never configured*****

Welcome to the CSC MUX 3.2 Gbps Configuration Wizard

1) Configuration required on your Zscaler Console: VPN credentials and Location
 --> VPN Credentials creation: Go to > Administration > VPN Credentials > Add VPN Credential -> Select Authentication Type = FDQN and configure 'User ID' and 'Pre-Shared Key'
 --> Location creation: Go to > Administration > Location > Add Location. Put your Location values and select 'VPN Credentials' created in the step before
2) Run the Wizard on the CSC and Select Cloud, Nodes, input VPN Credentials, DNS Servers, Bypass PAC URL and Syslog Servers

Current Values Configured:
-------------------
ZSCALER INFORMATION
Zscaler Cloud:
Primary ZEN node: | Hostname: | IP:
Secondary ZEN node: | Hostname: | IP:
-------------------
CREDENTIALS INFORMATION
User ID: | Pre-Shared Key:
-------------------
DNS Server: Azure DNS server 168.63.129.16
-------------------
Bypass Proxy PAC URL
Your current Bypass PAC URL is http://pac.<cloudname>.net/something/<pacname>.pac
-------------------
SYSLOG / SIEM information
Syslog / SIEM servers are not configured
-------------------
Are you ready to continue? (y/n)
```

6.2.1 VPN Credential creation.

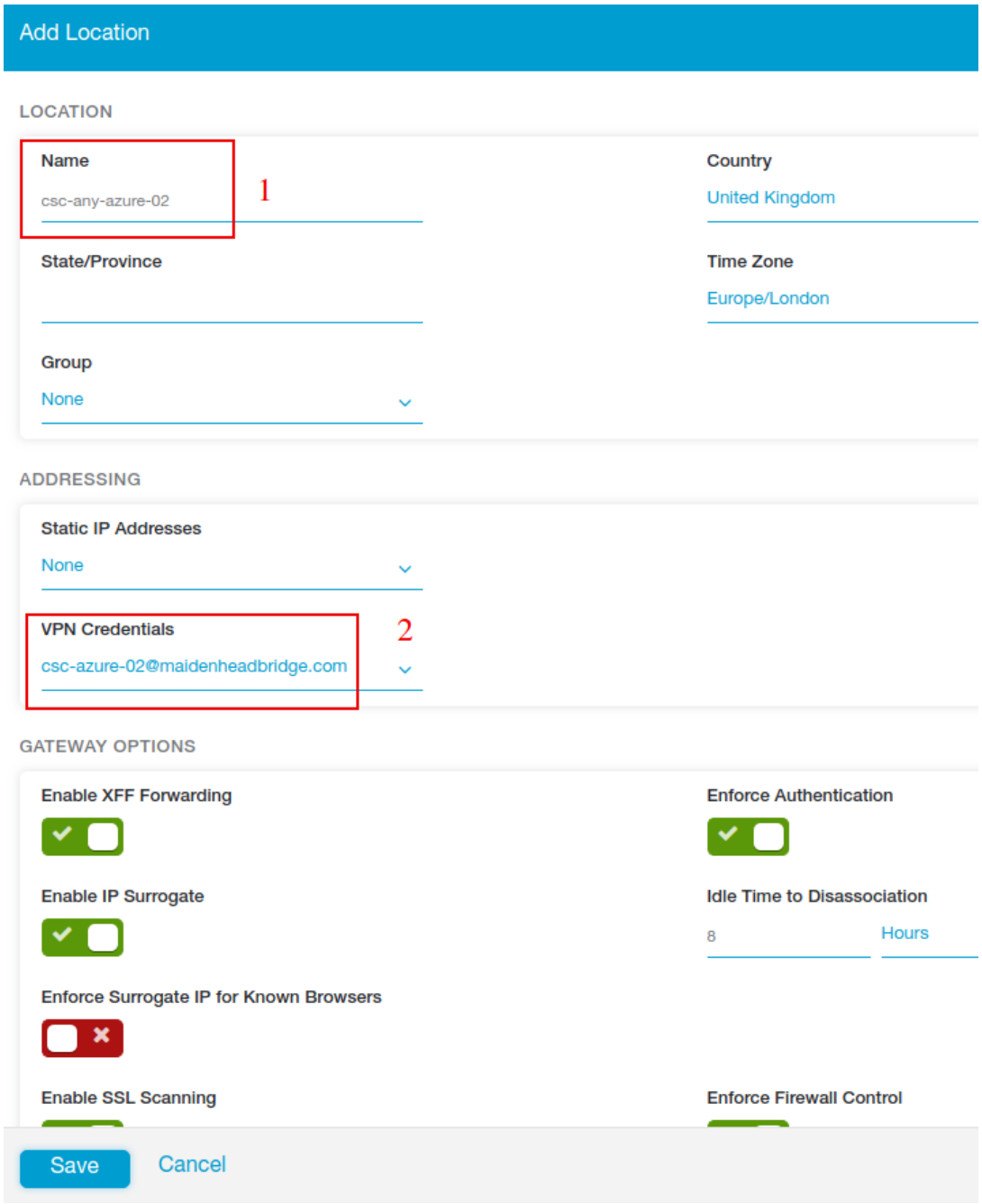
Go to > Administration > VPN Credentials > Add VPN Credential -> Select Authentication Type = FDQN and configure ‘User ID’ and ‘Pre-Shared Key’



Click “Save” and “Activation”

6.2.2 Create the Location on the Zscaler Console

Location creation: Go to > Administration > Location > Add Location. Put your Location values and select 'VPN Credentials' created in the step before.



Fill other values on the Location, click “Save” and “Activate”

6.2.3 Run the Wizard

The initial values are empty.

```
Current Values Configured:
-------------------
ZSCALER INFORMATION
Zscaler Cloud:
Primary ZEN node: | Hostname: | IP:
Secondary ZEN node: | Hostname: | IP:
-------------------
CREDENTIALS INFORMATION
User ID: | Pre-Shared Key:
-------------------
DNS Server: Azure DNS server 168.63.129.16
-------------------
Bypass Proxy PAC URL
Your current Bypass PAC URL is http://pac.<cloudname>.net/something/<pacname>.pac
-------------------
SYSLOG / SIEM information
Syslog / SIEM servers are not configured
-------------------
Are you ready to continue? (y/n) y
-------------------
ZSCALER INFORMATION

You current Zscaler Cloud and Nodes are:

Zscaler Cloud:
Primary ZEN node: | Hostname: | IP:
Secondary ZEN node: | Hostname: | IP:

Do you want to change these values? (y/n)
```

1. Select your cloud:

```
-------------------------------
Please, select your Cloud

1) zscalerthree
2) zscloud
3) zscalertwo
4) zscaler
5) zscalerone
6) zscalerbeta
7) Not in the list? Input Manually
8) Quit
Enter your choice:
```

2. Select the Nodes: Auto or Manual. Selecting Auto, the CSC Mux will detect the nearest Zscaler ZEN nodes. Selecting Manual allows you to choose the Zscaler ZEN nodes you want as Primary and Secondary.

```
-----------------------------
Please, select Manual or Auto Node Selection

1) Manual
2) Auto
3) Quit
Enter your choice: 1

-----------------------------
Please, select your Primary Node on 'zscalerthree'
Nodes marked with (-NRU) may be Not Ready for Use. Check http://ips.zscalerthree.net

1) EMEA,Amsterdam                10) EMEA,LagosII                 19) EMEA,ParisII_2               28) Americas,DallasII            37) Americas,TorontoIII          46) APAC,NewDelhiI
2) EMEA,AmsterdamII              11) EMEA,LondonIII               20) EMEA,RouenI                  29) Americas,DenverIII           38) Americas,VancouverI          47) APAC,OsakaI
3) EMEA,BrusselsII               12) EMEA,MadridIII               21) EMEA,StockholmIII            30) Americas,LosAngeles          39) Americas,WashingtonDC_2      48) APAC,SeoulI
4) EMEA,CopenhagenII             13) EMEA,ManchesterI             22) EMEA,TelAviv                 31) Americas,MiamiIII            40) APAC,Auckland                49) APAC,Shanghai
5) EMEA,DubaiI                   14) EMEA,MilanIII                23) EMEA,ViennaI                 32) Americas,NewYorkIII          41) APAC,Beijing                 50) APAC,SingaporeIV
6) EMEA,FrankfurtIV              15) EMEA,MoscowIII               24) EMEA,WarsawII                33) Americas,NuevoLaredoI        42) APAC,ChennaiII               51) APAC,SydneyIII
7) EMEA,FrankfurtIV_2            16) EMEA,MunichI                 25) EMEA,Zurich                  34) Americas,SanFranciscoIV_2    43) APAC,HongKongIII             52) APAC,TokyoIV
8) EMEA,JohannesburgII           17) EMEA,OsloII                  26) Americas,AtlantaII           35) Americas,SaoPauloIV          44) APAC,MelbourneII             53) Not in the list? Input Manually
9) EMEA,JohannesburgIII          18) EMEA,ParisII                 27) Americas,Chicago_2           36) Americas,Seattle             45) APAC,MumbaiVI                54) Quit
Enter your choice: 39

-----------------------------
Please, select your Secondary Node on 'zscalerthree'
Nodes marked with (-NRU) may be Not Ready for Use. Check http://ips.zscalerthree.net

1) EMEA,Amsterdam                10) EMEA,LagosII                 19) EMEA,ParisII_2               28) Americas,DallasII            37) Americas,TorontoIII          46) APAC,NewDelhiI
2) EMEA,AmsterdamII              11) EMEA,LondonIII               20) EMEA,RouenI                  29) Americas,DenverIII           38) Americas,VancouverI          47) APAC,OsakaI
3) EMEA,BrusselsII               12) EMEA,MadridIII               21) EMEA,StockholmIII            30) Americas,LosAngeles          39) Americas,WashingtonDC_2      48) APAC,SeoulI
4) EMEA,CopenhagenII             13) EMEA,ManchesterI             22) EMEA,TelAviv                 31) Americas,MiamiIII            40) APAC,Auckland                49) APAC,Shanghai
5) EMEA,DubaiI                   14) EMEA,MilanIII                23) EMEA,ViennaI                 32) Americas,NewYorkIII          41) APAC,Beijing                 50) APAC,SingaporeIV
6) EMEA,FrankfurtIV              15) EMEA,MoscowIII               24) EMEA,WarsawII                33) Americas,NuevoLaredoI        42) APAC,ChennaiII               51) APAC,SydneyIII
7) EMEA,FrankfurtIV_2            16) EMEA,MunichI                 25) EMEA,Zurich                  34) Americas,SanFranciscoIV_2    43) APAC,HongKongIII             52) APAC,TokyoIV
8) EMEA,JohannesburgII           17) EMEA,OsloII                  26) Americas,AtlantaII           35) Americas,SaoPauloIV          44) APAC,MelbourneII             53) Not in the list? Input Manually
9) EMEA,JohannesburgIII          18) EMEA,ParisII                 27) Americas,Chicago_2           36) Americas,Seattle             45) APAC,MumbaiVI                54) Quit
Enter your choice: 32
```

After Primary and Secondary are selected, the following screen appears:

```
-------------------------------
You have chosen the following:

Cloudname: zscalerthree
Primary node: WashingtonDC_2 (was1-2-vpn.zscalerthree.net)
Secondary Node: NewYorkIII (nyc3-vpn.zscalerthree.net)
-------------------------------
```

3. Enter your VPN Credentials

```
--------------------
CREDENTIALS INFORMATION

You current VPN Credentials are:

User ID: | Pre-Shared Key:

Do you want to change these values? (y/n) y

Please, ingress VPN Credentials (Email and Pre Shared Key)

Email:csc-azure-02@maidenheadbridge.com   1

Pre Shared Key:                           2
Do you want to display the Pre Shared Key? (y/n)? y
PSK = 12345678
```

4. Enter DNS values. You can use Azure DNS or setup your own DNS servers

```
-------------------
DNS Configuration

You are using Azure DNS server 168.63.129.16

Do you want to change the DNS servers? (y/n) y

Do you want to use Azure DNS 168.63.129.16? (y/n)n

Primary DNS Server (IP): 1.1.1.1
Secondary DNS Server (IP): 8.8.8.8
-------------------
```

5. Enter Bypass PAC URL if you are using Bypass Proxy functionality.

```
-------------------
Bypass Proxy Configuration
Your current Bypass PAC URL is http://pac.<cloudname>.net/something/<pacname>.pac

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

Please, input Bypass PAC URL
Bypass PAC URL:http://pac.zscalerthree.net/8FM8NgF7NMFq/csc-azure-bypass.pac

Your current Bypass PAC URL is: http://pac.zscalerthree.net/8FM8NgF7NMFq/csc-azure-bypass.pac

Do you want to refresh Bypass List? (y/n)? y

This is your current Bypass List

.okta.com
.oktacdn.com
.okta-emea.com
login.mydomain.com
login.microsoftonline.com
login.microsoft.com
login.windows.net
portquiz.net


Do you want apply changes? (y/n)? y

Bypass List updated sucessfully
```

6. Enter Syslog / SIEM information

```
--------------------
Syslog / SIEM Configuration

Your current Syslog / SIEM configuration is:

Syslog / SIEM servers are not configured

Do you want to change Syslog / SIEM Servers values?

1) Yes
2) No
3) Reset default values
Enter your choice: 1

Primary Syslog Server (IP): 10.2.3.4
(Optional) Do you want to configure a Secondary Syslog Server (y/n)n
Please enter Syslog TCP port: 514
```

7. The wizard will ask to confirm the values. Verify and confirm. The CSC will reboot.

```
Please confirm this values:
-------------------
Cloudname: zscalerthree
Primary node: WashingtonDC_2 (was1-2-vpn.zscalerthree.net)
Secondary Node: NewYorkIII (nyc3-vpn.zscalerthree.net)
-------------------
VPN Credentials
User ID: csc-azure-02@maidenheadbridge.com | Pre-Shared Key: 12345678
-------------------
DNS Servers: 1.1.1.1 ; 8.8.8.8
-------------------
Bypass Proxy PAC URL
Your current Bypass PAC URL is http://pac.zscalerthree.net/8FM8NgF7NMFq/csc-azure-bypass.pac
-------------------
Primary Syslog / SIEM server IP: 10.2.3.4
Syslog / SIEM TCP port IP: 514
-------------------
Do you want to implement this values? (y/n)?y

Validating Configuration

Your Cloud is: zscalerthree

Checking Node WashingtonDC_2 hostname was1-2-vpn.zscalerthree.net
Hostname was1-2-vpn.zscalerthree.net has IP 165.225.8.35
Node WashingtonDC_2 is Alive

Checking Node NewYorkIII hostname nyc3-vpn.zscalerthree.net
Hostname nyc3-vpn.zscalerthree.net has IP 165.225.38.52
Node NewYorkIII is Alive

Are this values correct? (y/n)? (answering 'y' will reboot the CSC):y
The system will be configured and rebooted
Connection to 10.2.2.4 closed by remote host.
Connection to 10.2.2.4 closed.
```

Done! Your CSC Mux is ready for production.

7 Cloud Security Connector Admin Console:

The CSC Mux Console simplifies admin tasks and keeps simple operations. It shows what is essential for function and troubleshooting.

Accessing the console via SSH, you will receive the Admin Console.

```
ssh cscadmin@10.2.2.4
```

```
Maidenhead Bridge

Cloud Security Connector MUX - Admin Console

Name : csc-mux-3-2Gbps-vm-1
Azure Region : eastus

Please select an option by typing its number

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

CSC Admin tasks
5) AWS SSM Agent (Register or De-Register)
6) Reserved for future use
7) Change Timezone

Proxy Bypass
8) View Current Proxy Bypass List
9) Configure Proxy Bypass List

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

Log Information
12) View Current Month
13) View Last 6 Months

Configuration Wizards
14) Change Cloud, Nodes, VPN Credentials, DNS, Syslog and more
15) Switch Tunnels - Primary / Secondary
16) High Availability changing Route/s
17) Update ZEN Nodes Database

e) Exit

Selection:
```

The Main Sections are:

- Monitoring Tasks: Check statuses and obtain all values configured, see Interfaces traffic in real-time, do MyTraceRoute test to Zscaler ZEN Nodes and check speed using SpeedTest.
- CSC Admin Tasks: To register the CSC Mux on AWS Systems Manager for remote monitoring and select timezone.
- Proxy Bypass: View and configure Proxy Bypass (Layer 7) functionality.
- Routed Bypass: View and configure Routed Bypass (Layer 4) functionality.
- Configuration Wizard: Run the initial wizard, switch tunnels, configure High Availability and update ZEN nodes databases.

7.1 Monitoring Tasks

7.1.1 Show Configuration and Status

This menu Shows all configuration and all Status.

```
Selection: 1

GENERAL INFORMATION
Name: csc-mux-3-2Gbps-vm-1
Location: eastus | SubscriptionId: ffde02fb-c38f-45fb-9e31-89e5303be5f1 | vmSize: Standard_DS3_v2
CSC date: Thu 29 Jul 08:02:51 UTC 2021
Soft version: 3.1 | CSC Model: CSC MUX 3.2 Gbps for Azure

INTERFACES INFORMATION
External: Tunnel IPs (eth0): 10.2.1.13-[14,15,16,17,18,19,20]/24 | Bypass Proxy Egress IP 10.2.1.21 | Network Gateway: 10.2.1.1
Internal: CSC GW IP (eth1): 10.2.2.4/24 | Network Gateway: 10.2.2.1

TRAFFIC REDIRECTION Options
To Zscaler: VIP Proxy: 10.2.2.5:80 (or :9400) | Route all traffic via CSC GW IP | Zscaler Global Proxies (port 80/9400) via CSC GW IP
Direct to Internet: Bypass Proxy: 10.2.2.6:3128 | Zscaler Global Proxies (port 3128) via CSC GW IP

PUBLIC IP Address INFORMATION
IPsec tunnels Public IP: 52.188.172.172, 52.249.199.73, 52.188.173.117, 52.188.168.157, 52.249.198.134, 52.249.199.83, 52.249.199.8, 52.249.193.190
Bypass Proxy Public IP: 52.249.199.74

DNS INFORMATION
DNS Server (1): 1.1.1.1 is Alive
DNS Server (2): 8.8.8.8 is Alive

ZSCALER INFORMATION
Zscaler Cloud:  zscalerthree
Primary ZEN node: WashingtonDC_2 | Hostname: was1-2-vpn.zscalerthree.net | IP: 165.225.8.35 is Alive
Secondary ZEN node: NewYorkIII | Hostname: nyc3-vpn.zscalerthree.net | IP: 165.225.38.52 is Alive
```

```
LOAD BALANCING INFORMATION
Last change: Thu 29 Jul 07:48:57 UTC 2021
(UP)   Ztun1 is active, using primary.
(UP)   Ztun2 is active, using primary.
(UP)   Ztun3 is active, using primary.
(UP)   Ztun4 is active, using primary.
(UP)   Ztun5 is active, using primary.
(UP)   Ztun6 is active, using primary.
(UP)   Ztun7 is active, using primary.
(UP)   Ztun8 is active, using primary.

IPSEC INFORMATION
Ztun1 connected to: WashingtonDC_2, IPsec uptime uptime: 15 minutes, since Jul 29 07:47:05 2021, Last Security Association: ESTABLISHED 15 minutes ago
Ztun2 connected to: WashingtonDC_2, IPsec uptime uptime: 15 minutes, since Jul 29 07:47:05 2021, Last Security Association: ESTABLISHED 15 minutes ago
Ztun3 connected to: WashingtonDC_2, IPsec uptime uptime: 15 minutes, since Jul 29 07:47:05 2021, Last Security Association: ESTABLISHED 15 minutes ago
Ztun4 connected to: WashingtonDC_2, IPsec uptime uptime: 15 minutes, since Jul 29 07:47:05 2021, Last Security Association: ESTABLISHED 15 minutes ago
Ztun5 connected to: WashingtonDC_2, IPsec uptime uptime: 15 minutes, since Jul 29 07:47:05 2021, Last Security Association: ESTABLISHED 15 minutes ago
Ztun6 connected to: WashingtonDC_2, IPsec uptime uptime: 15 minutes, since Jul 29 07:47:05 2021, Last Security Association: ESTABLISHED 15 minutes ago
Ztun7 connected to: WashingtonDC_2, IPsec uptime uptime: 15 minutes, since Jul 29 07:47:05 2021, Last Security Association: ESTABLISHED 15 minutes ago
Ztun8 connected to: WashingtonDC_2, IPsec uptime uptime: 15 minutes, since Jul 29 07:47:05 2021, Last Security Association: ESTABLISHED 15 minutes ago
```

```
CREDENTIALS INFORMATION
Username: csc-azure-02@maidenheadbridge.com | PSK: Not shown. Please, read it from 'Configuration Wizards' Menu

http://ip.zscaler.com INFORMATION
Ztun1 Node: Washington DC in the zscalerthree.net cloud. ZEN Instance IP: 165.225.8.244, via Public IP: 52.188.172.172
Ztun2 Node: Washington DC in the zscalerthree.net cloud. ZEN Instance IP: 165.225.9.7, via Public IP: 52.249.199.73
Ztun3 Node: Washington DC in the zscalerthree.net cloud. ZEN Instance IP: 136.226.51.2, via Public IP: 52.188.173.117
Ztun4 Node: Washington DC in the zscalerthree.net cloud. ZEN Instance IP: 136.226.51.19, via Public IP: 52.188.168.157
Ztun5 Node: Washington DC in the zscalerthree.net cloud. ZEN Instance IP: 165.225.9.24, via Public IP: 52.249.198.134
Ztun6 Node: Washington DC in the zscalerthree.net cloud. ZEN Instance IP: 165.225.9.5, via Public IP: 52.249.199.83
Ztun7 Node: Washington DC in the zscalerthree.net cloud. ZEN Instance IP: 165.225.9.12, via Public IP: 52.249.199.8
Ztun8 Node: Washington DC in the zscalerthree.net cloud. ZEN Instance IP: 136.226.51.8, via Public IP: 52.249.193.190

BYPASS PROXY - EGRESS INTERFACE STATUS
Bypass Proxy Egress Interface 10.2.1.21 can reach test page (http://pac.zscalerthree.net)

ROUTED BYPASS
*** Routed Bypass URL is not configured ***
No Routed Bypass Rules are configured
Manual Routed Bypass Rules configured: 0

AWS SSM AGENT
AWS SSM Agent is not registered

SYSLOG INFORMATION
SYSLOG Server (1) IP: 10.2.3.4 is Alive
SYSLOG Server (2) IP is not configured
SYSLOG TCP Port: 514

HIGH AVAILABILITY Information
The HA service in NOT Active

Press ENTER to continue
```

7.1.1.1 GENERAL INFORMATION

This section contains general information about the Virtual Machine. To be used for troubleshooting purposes if needed.

```
GENERAL INFORMATION
Name: csc-mux-3-2Gbps-vm-1
Location: eastus | SubscriptionId: ffde02fb-c38f-45fb-9e31-89e5303be5f1 | vmSize: Standard_DS3_v2
CSC date: Thu 29 Jul 08:02:51 UTC 2021
Soft version: 3.1 | CSC Model: CSC MUX 3.2 Gbps for Azure
```

7.1.1.2 INTERFACES INFORMATION

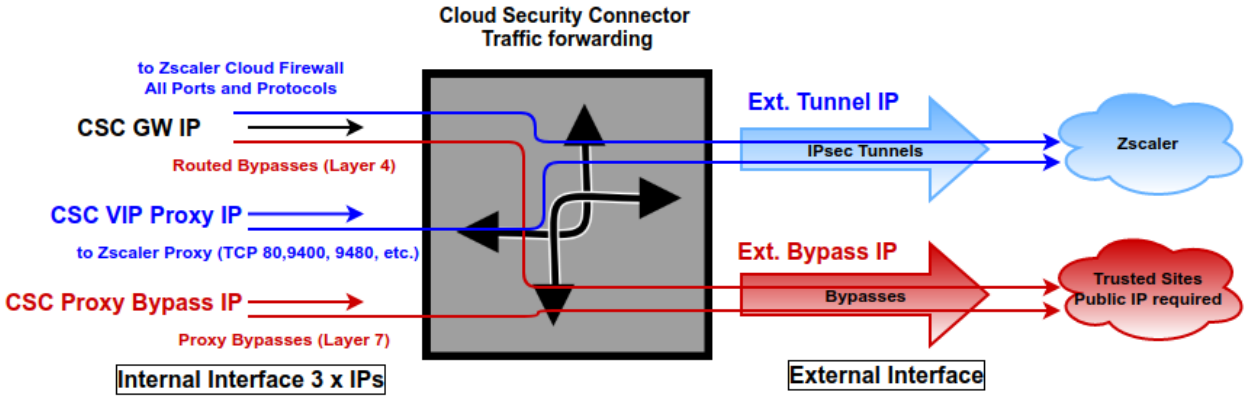
This section contains the interfaces information: IPs and Gateways.

```
INTERFACES INFORMATION
External: Tunnel IPs (eth0): 10.2.1.13-[14,15,16,17,18,19,20]/24 | Bypass Proxy Egress IP 10.2.1.21 | Network Gateway: 10.2.1.1
Internal: CSC GW IP (eth1): 10.2.2.4/24 | Network Gateway: 10.2.2.1
```

7.1.1.3 TRAFFIC REDIRECTION Options

```
TRAFFIC REDIRECTION Options
To Zscaler: VIP Proxy: 10.2.2.5:80 (or :9400) | Route all traffic via CSC GW IP | Zscaler Global Proxies (port 80/9400) via CSC GW IP
Direct to Internet: Bypass Proxy: 10.2.2.6:3128 | Zscaler Global Proxies (port 3128) via CSC GW IP
```

The objective of the Cloud Security Connectors of Maidenhead Bridge is to provide a simple architecture, 100% proven that works, to connect to Zscaler that covers all possible scenarios.



The function of each IP is the follwing:

IP	Type	Function
CSC GW	Gateway	Used as Gateway for traffic to Zscaler and bypasses using "Routed Bypass" (Layer 4) functionality.
CSC Vip Proxy	Proxy	Used as Proxy for traffic to Zscaler.
CSC Proxy Bypass	Proxy	User as Proxy for bypasses using "Proxy Bypass" (Layer 7) functionality.

Section 3.5.1 provides a Real Case Scenario showing the use of each IP.

Note:

The CSC Mux for Azure accepts the option using the Zscaler Global Proxies to send traffic to Zscaler Cloud and via the Proxy Bypass.

Your task is to route the Zscaler Global Proxies IPs via the CSC GW IP and to create a return statement on your PAC file like:

*Traffic to Zscaler → return "PROXY 185.46.212.88:**80**"; (you can use port 9400 as well)*
*Traffic via Bypass Proxy → return "PROXY 185.46.212.88:**3128**";*

List of Zscaler Global Proxies:

185.46.212.88	*185.46.212.89*	*185.46.212.90*	*185.46.212.91*
185.46.212.92	*185.46.212.93*	*185.46.212.97*	*185.46.212.98*

7.1.1.4 PUBLIC IP Address INFORMATION

This section displays the Public IPs in use for the tunnels and for the bypass functionality.

```
PUBLIC IP Address INFORMATION
IPsec tunnels Public IP: 52.188.172.172, 52.249.199.73, 52.188.173.117, 52.188.168.157, 52.249.198.134, 52.249.199.83, 52.249.199.8, 52.249.193.190
Bypass Proxy Public IP: 52.249.199.74
```

Note: *Public IP information is not available when the CSC Mux is deployed using Availability Zones due to a limitation of the Azure Cloud when providing the information via instance metadata.*

7.1.1.5 DNS INFORMATION

This section displays the DNS server information. You can use the default DNS server from Azure or set up your DNS servers.

```
DNS INFORMATION
DNS Server (1): 1.1.1.1 is Alive
DNS Server (2): 8.8.8.8 is Alive
```

7.1.1.6 ZSCALER INFORMATION

This section shows the Cloud and Nodes in use and if they are reachable or not.

```
ZSCALER INFORMATION
Zscaler Cloud:  zscalerthree
Primary ZEN node: WashingtonDC_2 | Hostname: was1-2-vpn.zscalerthree.net | IP: 165.225.8.35 is Alive
Secondary ZEN node: NewYorkIII | Hostname: nyc3-vpn.zscalerthree.net | IP: 165.225.38.52 is Alive
```

7.1.1.7 LOAD BALANCING INFORMATION

This section shows the tunnels currently load balanced. The Load Balancer works in the following way:

- Tunnels connected to a Primary Node have priority over tunnels connected to a Secondary Node.
- Only groups tunnels to Primary Nodes or Secondary Nodes.

The following screenshot shows the Load Balancing information of a CSC Mux 3.2 Gbps:

```
LOAD BALANCING INFORMATION
Last change: Thu 29 Jul 07:48:57 UTC 2021
(UP)   Ztun1 is active, using primary.
(UP)   Ztun2 is active, using primary.
(UP)   Ztun3 is active, using primary.
(UP)   Ztun4 is active, using primary.
(UP)   Ztun5 is active, using primary.
(UP)   Ztun6 is active, using primary.
(UP)   Ztun7 is active, using primary.
(UP)   Ztun8 is active, using primary.
```

7.1.1.8 IPSEC INFORMATION

This section shows the Node Active, IPsec uptime and last Security Association for each tunnel.

```
IPSEC INFORMATION
Ztun1 connected to: WashingtonDC_2, IPsec uptime uptime: 15 minutes, since Jul 29 07:47:05 2021, Last Security Association: ESTABLISHED 15 minutes ago
Ztun2 connected to: WashingtonDC_2, IPsec uptime uptime: 15 minutes, since Jul 29 07:47:05 2021, Last Security Association: ESTABLISHED 15 minutes ago
Ztun3 connected to: WashingtonDC_2, IPsec uptime uptime: 15 minutes, since Jul 29 07:47:05 2021, Last Security Association: ESTABLISHED 15 minutes ago
Ztun4 connected to: WashingtonDC_2, IPsec uptime uptime: 15 minutes, since Jul 29 07:47:05 2021, Last Security Association: ESTABLISHED 15 minutes ago
Ztun5 connected to: WashingtonDC_2, IPsec uptime uptime: 15 minutes, since Jul 29 07:47:05 2021, Last Security Association: ESTABLISHED 15 minutes ago
Ztun6 connected to: WashingtonDC_2, IPsec uptime uptime: 15 minutes, since Jul 29 07:47:05 2021, Last Security Association: ESTABLISHED 15 minutes ago
Ztun7 connected to: WashingtonDC_2, IPsec uptime uptime: 15 minutes, since Jul 29 07:47:05 2021, Last Security Association: ESTABLISHED 15 minutes ago
Ztun8 connected to: WashingtonDC_2, IPsec uptime uptime: 15 minutes, since Jul 29 07:47:05 2021, Last Security Association: ESTABLISHED 15 minutes ago
```

7.1.1.9 CREDENTIALS INFORMATION

This section shows the User ID in use:

```
CREDENTIALS INFORMATION
Username: csc-azure-02@maidenheadbridge.com | PSK: Not shown. Please, read it from 'Configuration Wizards' Menu
```

7.1.1.10 http://ip.zscaler.com INFORMATION

Zscaler recommends checking the page http://ip.zscaler.com to validate that you are using Zscaler and see Zscaler Node connected, Cloud and IP address. The CSC does this test for you on each tunnel.

```
http://ip.zscaler.com INFORMATION
Ztun1 Node: Washington DC in the zscalerthree.net cloud. ZEN Instance IP: 165.225.8.244, via Public IP: 52.188.172.172
Ztun2 Node: Washington DC in the zscalerthree.net cloud. ZEN Instance IP: 165.225.9.7, via Public IP: 52.249.199.73
Ztun3 Node: Washington DC in the zscalerthree.net cloud. ZEN Instance IP: 136.226.51.2, via Public IP: 52.188.173.117
Ztun4 Node: Washington DC in the zscalerthree.net cloud. ZEN Instance IP: 136.226.51.19, via Public IP: 52.188.168.157
Ztun5 Node: Washington DC in the zscalerthree.net cloud. ZEN Instance IP: 165.225.9.24, via Public IP: 52.249.198.134
Ztun6 Node: Washington DC in the zscalerthree.net cloud. ZEN Instance IP: 165.225.9.5, via Public IP: 52.249.199.83
Ztun7 Node: Washington DC in the zscalerthree.net cloud. ZEN Instance IP: 165.225.9.12, via Public IP: 52.249.199.8
Ztun8 Node: Washington DC in the zscalerthree.net cloud. ZEN Instance IP: 136.226.51.8, via Public IP: 52.249.193.190
```

7.1.1.11 BYPASS PROXY – EGRESS INTERFACE STATUS

This section validates if the Bypass Proxy can access the internet directly going to http://pac.<cloudname>.net

```
BYPASS PROXY - EGRESS INTERFACE STATUS
Bypass Proxy Egress Interface 10.2.1.21 can reach test page (http://pac.zscalerthree.net)
```

7.1.1.12 ROUTED BYPASS

This section shows the configuration of the Routed Bypass.

```
ROUTED BYPASS
*** Routed Bypass URL is not configured ***
No Routed Bypass Rules are configured
Manual Routed Bypass Rules configured: 0
```

7.1.1.13 AWS SSM AGENT

This section shows the status of the AWS SSM Agent.

```
AWS SSM AGENT
AWS SSM Agent is not registered
```

7.1.1.14 SYSLOG INFORMATION

This section shows the Syslog Servers configured and TCP port.

```
SYSLOG INFORMATION
SYSLOG Server (1) IP: 10.2.3.4 is Alive
SYSLOG Server (2) IP is not configured
SYSLOG TCP Port: 514
```

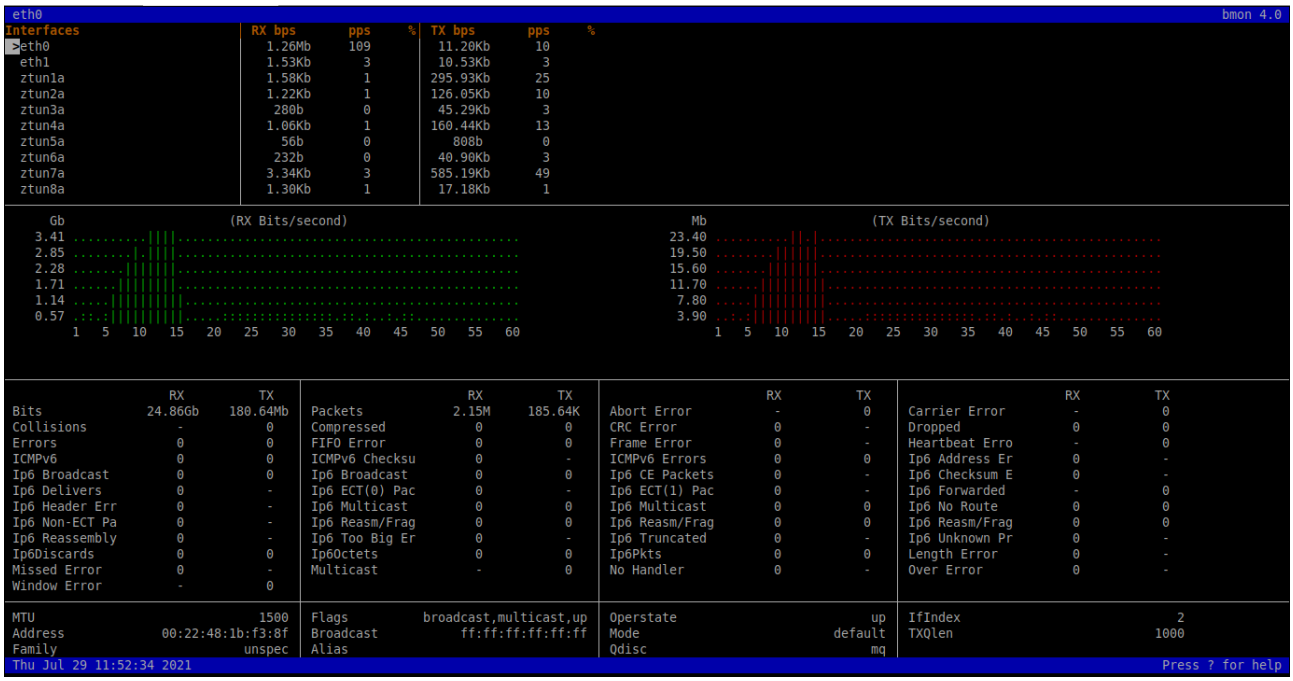
7.1.1.15 HIGH AVAILABILITY Information

This section shows the status and configuration of the High Availability. It offers all Routes under the management of the CSC pair and the current “Next-Hop” in use

```
HIGH AVAILABILITY Information
The HA service in NOT Active
```

7.1.2 Show Interfaces Traffic

You can use this section to see the traffic in real-time on each ethernet interface and tunnel.



7.1.3 Traceroute and Latency Test

This test checks the quality of the Internet path between you location and Zscaler, hop by hop. This is very useful to check if there is any packet loss at some hop.

This test does 10 probes DIRECT to Primary / Secondary ZEN and a Reverse test via Ztun1 to Ztun1 Public IP.

Notes:

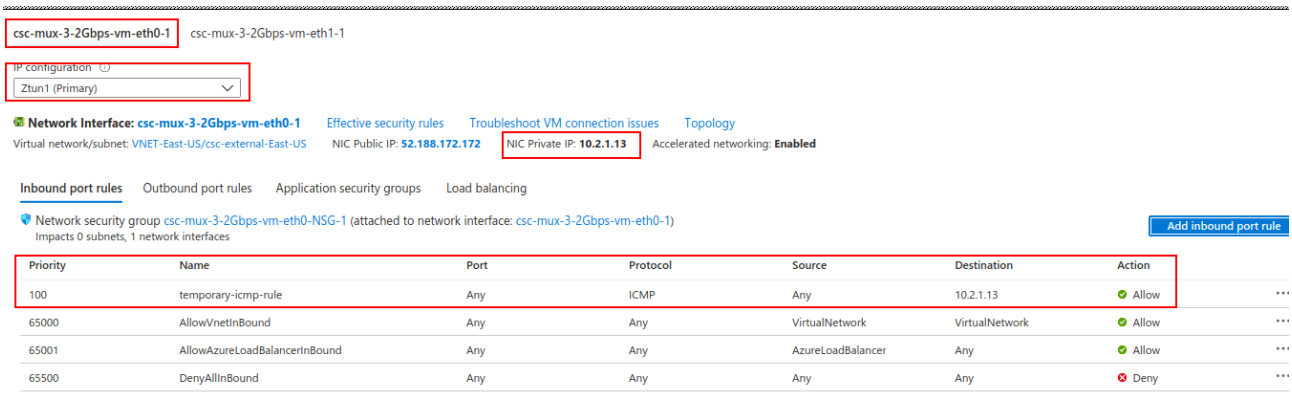
- IMPORTANT: It is required to allow ICMP Time exceeded (type 11) on the Inbound rule of the Security Group of eth0 to destination IP: 10.2.1.13 (← This IP is Ztun1)

  Without this security rule added, you will not able to see the results of middle hops.

- When the Ztun1 is UP, a Reverse Path test from the active ZEN to Ztun1 Public IP is performed

- Max Hops is equal 30. This test can take a while.

Here the temporary "Inbound port rule" required.



MTR results:

```
My TraceRoute (MTR) Test Report
This test does 10 probes DIRECT to Primary / Secondary ZEN and a Reverse test via Ztun1 to Ztun1 Public IP
Notes:
- IMPORTANT: It is required to allow ICMP Time exceeded (type 11) on the Inbound rule of the Security Group of eth0 to destination IP: 10.2.1.13
  Without this security rule added, you will not able to see the results of middle hops.
- When the Ztun1 is UP, a Reverse Path test from the active ZEN to Ztun1 Public IP is performed
- Max Hops is equal 30. This test can take a while

Testing Primary ZEN: WashingtonDC_2 : was1-2-vpn.zscalerthree.net > 165.225.8.35
Start: 2021-07-29T10:09:44+0000
HOST: csc-mux-3-2Gbps-vm-1                                          Loss%   Snt   Last   Avg  Best  Wrst StDev
  1. AS???    ???                                                   100.0    10    0.0   0.0   0.0   0.0   0.0
  2. AS???    ???                                                   100.0    10    0.0   0.0   0.0   0.0   0.0
  3. AS???    ???                                                   100.0    10    0.0   0.0   0.0   0.0   0.0
  4. AS???    ???                                                   100.0    10    0.0   0.0   0.0   0.0   0.0
  5. AS???    ???                                                   100.0    10    0.0   0.0   0.0   0.0   0.0
  6. AS???    ???                                                   100.0    10    0.0   0.0   0.0   0.0   0.0
  7. AS8075   be-166-0.ibr04.bl20.ntwk.msn.net (104.44.32.46)        0.0%    10    3.6  18.5   2.3  87.1  27.3
  8. AS8075   ae162-0.icr02.bl20.ntwk.msn.net (104.44.21.234)        0.0%    10    1.8   2.3   1.8   3.0   0.4
  9. AS8075   ae55-0.ash-96cbe-1b.ntwk.msn.net (104.44.238.132)      0.0%    10    1.7   2.1   1.5   6.6   1.6
 10. AS???    eqix-was1-r1.zscaler9.net (206.126.236.212)            0.0%    10    2.0   1.9   1.8   2.0   0.1
 11. AS22616  165.225.8.35                                           0.0%    10    2.2   2.4   1.8   5.6   1.2

Testing Secondary ZEN: NewYorkIII : nyc3-vpn.zscalerthree.net > 165.225.38.52
Start: 2021-07-29T10:09:59+0000
HOST: csc-mux-3-2Gbps-vm-1                                          Loss%   Snt   Last   Avg  Best  Wrst StDev
  1. AS???    ???                                                   100.0    10    0.0   0.0   0.0   0.0   0.0
  2. AS???    ???                                                   100.0    10    0.0   0.0   0.0   0.0   0.0
  3. AS???    ???                                                   100.0    10    0.0   0.0   0.0   0.0   0.0
  4. AS???    ???                                                   100.0    10    0.0   0.0   0.0   0.0   0.0
  5. AS???    ???                                                   100.0    10    0.0   0.0   0.0   0.0   0.0
  6. AS???    ???                                                   100.0    10    0.0   0.0   0.0   0.0   0.0
  7. AS8075   be-142-0.ibr03.bl20.ntwk.msn.net (104.44.21.225)      0.0%    10    8.6   8.4   8.1   9.2   0.3
  8. AS8075   be-8-0.ibr01.nyc30.ntwk.msn.net (104.44.19.195)       0.0%    10    7.9   8.3   7.9   8.8   0.3
  9. AS8075   ae22-0.ear03.nyc30.ntwk.msn.net (104.44.32.111)       0.0%    10   10.9   8.6   7.3  13.2   1.9
 10. AS8075   ae21-0.nyc-96cbe-1a.ntwk.msn.net (104.44.24.44)       0.0%    10    7.0   8.2   7.0  17.7   3.3
 11. AS???    eqix-ny5.zscaler.com (198.32.118.225)                 0.0%    10    7.2   7.3   7.2   7.4   0.1
 12. AS22616  165.225.38.52                                          0.0%    10    7.7   7.7   7.5   7.9   0.1


Reverse path from: WashingtonDC_2 to your Public IP: 52.188.172.172
Start: 2021-07-29T10:10:15+0000
HOST: csc-mux-3-2Gbps-vm-1                                          Loss%   Snt   Last   Avg  Best  Wrst StDev
  1. AS???    ???                                                   100.0    10    0.0   0.0   0.0   0.0   0.0
  2. AS22616  165.225.9.19                                          0.0%    10    4.0   4.2   2.0   8.1   1.9
  3. AS22616  165.225.8.3                                           0.0%    10    2.9   5.2   2.9  10.3   2.1
  4. AS???    8075-dc2-ix.equinix.com (206.126.236.148)             0.0%    10   11.6   9.7   4.1  21.7   5.3
  5. AS8075   ae55-0.icr02.bl20.ntwk.msn.net (104.44.238.133)       0.0%    10    6.6   6.6   4.0   9.7   1.7
  6. AS8075   be-162-0.ibr04.bl20.ntwk.msn.net (104.44.21.235)      0.0%    10    4.4  25.0   4.3 128.2  43.8
  7. AS8075   ae160-0.icr01.bl20.ntwk.msn.net (104.44.22.210)       0.0%    10   20.9   8.3   3.4  20.9   5.1
  8. AS???    ???                                                   100.0    10    0.0   0.0   0.0   0.0   0.0
```

After the test is done, please, delete the temporary ICMP inbound rule created.

7.1.4 SPEED TEST

This test is experimental because we use third-party tools (speedtest.net), but it works fine in most cases.

This test runs on all tunnels simultaneously and returns the sum of the download speed of all tunnels.

```
Selection: 4

SPEED TEST
This is experimental. We are using third party tools. (Speedtest.net)
Results can be inaccurate or none. The test takes a while


Aggregated Bandwidth Download:  3074.83 Mbps
```

This test was done on a CSC Mux 3.2 Gbps.

Note 1: May be will be required to add the ".speedtest.net" on your SSL Exemption list on your Zscaler console.

Note 2: Zscaler imposes a "soft limit" of 400 Mbps on ipsec tunnels.

7.2 CSC Admin Tasks

```
CSC Admin tasks
5) AWS SSM Agent (Register or De-Register)
6) Reserved for future use
7) Change Timezone
```

5. AWS SSM Agent (Register or De-Register)

6. Reserved for future use.

7. Change Timezone: In case if needed, you can select your Timezone here.

7.2.1 AWS SSM Agent (Register / De-Register)

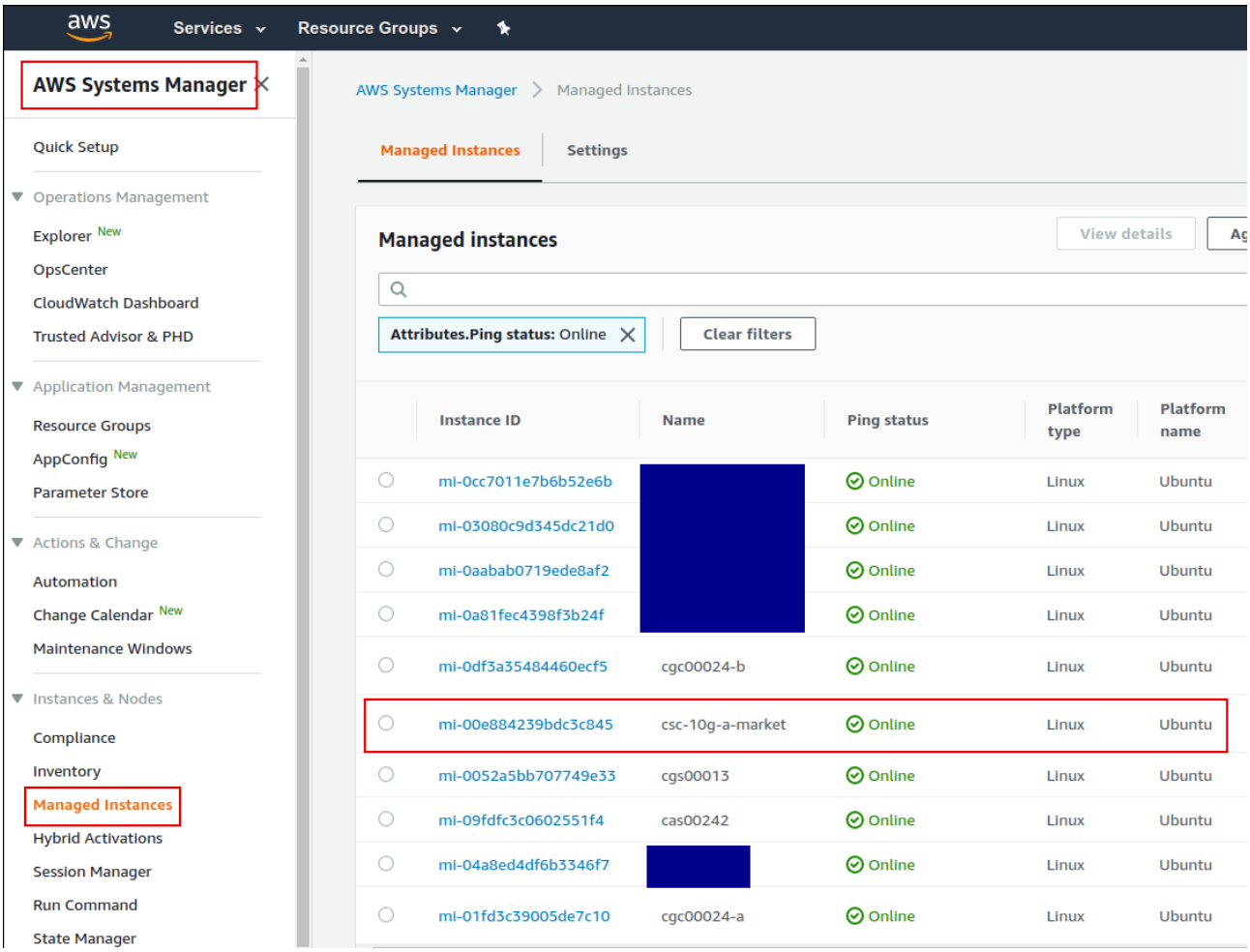
The CSC AWS has installed the AWS SSM Agent that allows you to check remotely the status of the CSC via "AWS Systems Manager" and "Run Commands".

Note: You can learn more about "Run Commands" on Appendix B

Important (**): It is advisable to manage all CSC (for Hyper-V, AWS, KVM, Vmware, Azure, Gcloud) from the same AWS availability zone.

Important (**): Azure Cloud has a function to "Run Commands".

AWS Systems Manager:

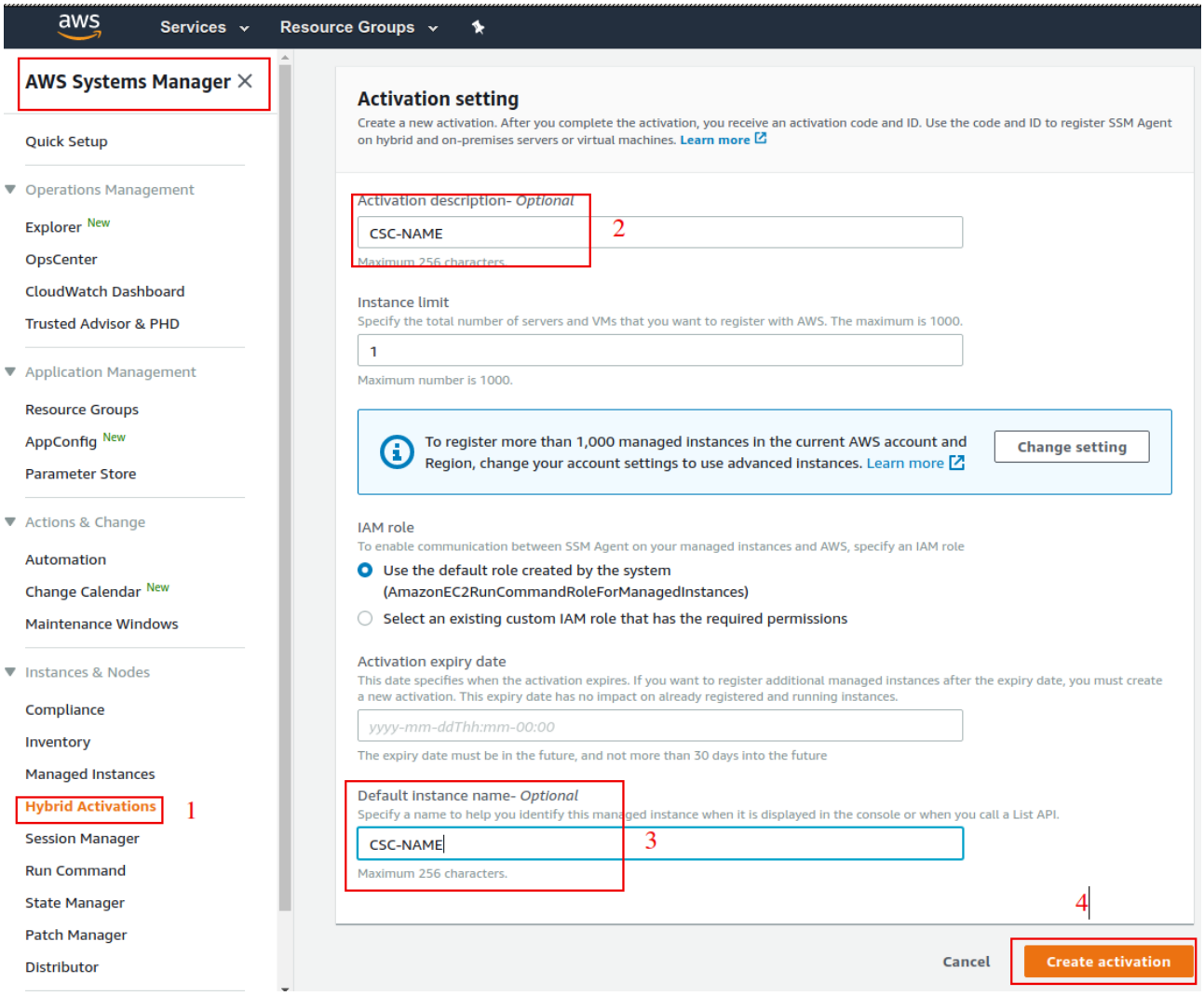


Please, note that in this example, the availability zone is eu-west-1. Check your availability Zone when doing this.

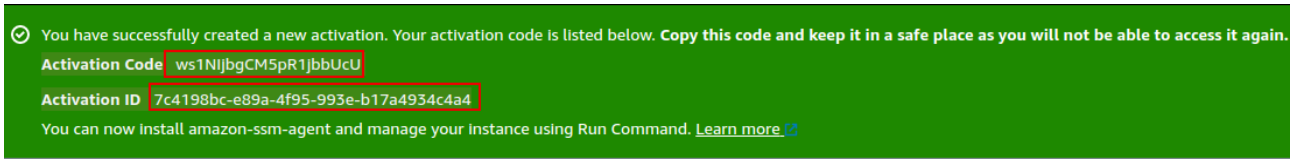
The steps required to register the AWS SSM Agent are two:

1. From your EC2 Console (** in the zone selected for management), go to AWS Systems Manager > Hybrid Activations > Create an activation.

Note: We recommend creating an Activation per CSC and on “Default instance name” to put the name of the CSC instance (or CSC ID o or the name of your “Location” for easy identification)



When you click “Create an Activation” you will receive the following information:



Please, keep copying these values in a safe place. You will need this to register the AWS SSM client on the CSC..

2. From the CSC Admin Tasks Menu, select “5) AWS SSM Agent (Register or De-Register)”. You will be asked for the Activation Code, Activation ID and AWS Region to register the

CSC. (Check your AWS URL https://eu-west-1.console.aws.amazon.com/ec2/v2/home?region=**eu-west-1**#)

```
Do you want to Register (start) the AWS SSM Agent (y/n) y
Please, ingress Activation Code, Activation ID and Region (example: eu-west-1)
Activation Code :2C9+dZ9+DYYCnp6lXaZh
Activation ID :a2317499-ca3c-4574-860d-92d587911fa3
Region :eu-west-1

AWS SSM Agent is active (running) since Thu 2019-02-07 12:15:12 UTC; 37ms ago
Registration values: {"ManagedInstanceID":"mi-0b5653473976667f0","Region":"eu-west-1"}

Press ENTER to continue
```

Done! You have now the CSC integrated with AWS Systems Manager with the instance-id “mi-xxxxxxxxx” (mi-0b5653473976667f0” in this case).

7.2.1.1 Checking the status of the AWS SSM agent

The “Show Configuration and Status” Menu shows the status of the AWS SSM agent.

```
AWS SSM AGENT
AWS SSM Agent is active (running) since Thu 2019-02-07 12:15:12 UTC; 7min ago
Registration values: {"ManagedInstanceID":"mi-0b5653473976667f0","Region":"eu-west-1"}
```

7.2.2 Change Timezone

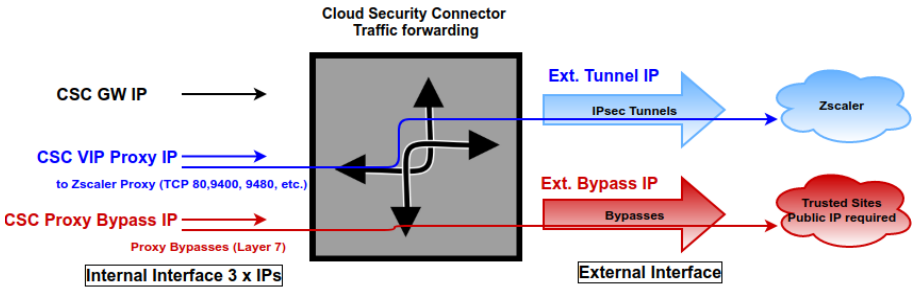
You can select the Time Zone in this section.

7.3 Bypass Proxy

When using PAC files, the Bypass Proxy allows you to connect certain domains direct to the Internet. By default, all domains are blocked, and you need to insert the domains that you want to allow to go direct.

```
Proxy Bypass
8) View Current Proxy Bypass List
9) Configure Proxy Bypass List
```

7.3.1 Proxy Bypass - Traffic Flow



7.3.2 View Current Proxy Bypass List

This commands shows the current domains and subdomains allows to go direct to Internet. By default the list is “blank” blocking all traffic.

```
Selection: 8

This is the list of current Domains configured:

.okta.com
.oktacdn.com
.okta-emea.com
login.mydomain.com
login.microsoftonline.com
login.microsoft.com
login.windows.net
portquiz.net
```

7.3.3 Configure Proxy Bypass List

In order to configure the Bypass List you have two options:

```
Selection: 9

Please, select method to configure Proxy Bypass List

1) Auto - Proxy Bypass PAC URL
2) Manual
3) Quit
Enter your choice:
```

7.3.3.1 Auto – Proxy Bypass PAC URL

Auto–Proxy Bypass PAC URL is the recommended method to use. You need to create a “Proxy Bypass PAC file” on your Zscaler console. The CSC will read the “Proxy Bypass List” from the “Proxy Bypass PAC file”.

By default, the CSC has configured this PAC URL:

*http://pac.<**yourcloudname**>.net/**something**/<pacname>.pac*

** You can change this URL via console menu. You can use an internal URL if you want.*

The “Proxy Bypass PAC file” idea is to act as a central repository of all Layer 7 bypasses required. Moreover, if you manage the CSCs using AWS, you can update all CSCs in your network doing one AWS Run Command.

Example of “Proxy Bypass PAC file”

```
function FindProxyForURL(url, host) {
      var bypassproxy="PROXY 1.1.1.1:3128; PROXY 2.2.2.2:3128";

// ==========================================================
   // Section 3: Bypass via Cloud Security Connectors

   // Bypass via CSC Public IPs (Examples)
      // Okta Domains (for Location Rules)
   if ((shExpMatch(host, "*.okta.com")) ||
      (shExpMatch(host, "*.oktacdn.com")) ||
      (shExpMatch(host, "*.okta-emea.com")) ||
      (shExpMatch(host, "login.mydomain.com")) ||
      // O365 Domains for ConditionalAccess
      (shExpMatch(host, "login.microsoftonline.com")) ||
      (shExpMatch(host, "login.microsoft.com")) ||
      (shExpMatch(host, "login.windows.net")) ||
      // IP / Port test page
      (shExpMatch(host, "portquiz.net"))) {
      return bypassproxy
   }
// ==========================================================
   return bypassproxy
}
```

Note 1: It is mandatory to use this function and format. Feel free to add lines but don't change the format. We recommend to start filling the first line and the last line. Use middle lines for copy/paste.

Note 2: The Bypass Proxy port is 3128

7.3.3.2 Example Using Proxy Bypass

Scenario: It is required to send Okta and O365 Authentication URLs via the customer's public IP and no Zscaler IPs.

Requirements:

1. Create the "Proxy Bypass PAC" with the list of domains you want to bypass on your Zscaler console. Copy the URL.

<u>Proxy Bypass PAC on Zscaler Console:</u>

PAC FILE CONTENTS

```
1  function FindProxyForURL(url, host) {
2          var bypassproxy="PROXY 1.1.1.1:3128; PROXY 2.2.2.2:3128";
3
4  // ==========================================================
5      // Section 3: Bypass via Cloud Security Connectors
6
7      // Bypass via CSC Public IPs (Examples)
8          // Okta Domains (for Location Rules)
9      if ((shExpMatch(host, "*.okta.com")) ||
10         (shExpMatch(host, "*.oktacdn.com")) ||
11         (shExpMatch(host, "*.okta-emea.com")) ||
12         (shExpMatch(host, "login.mydomain.com")) ||
13         // O365 Domains for ConditionalAccess
14         (shExpMatch(host, "login.microsoftonline.com")) ||
15         (shExpMatch(host, "login.microsoft.com")) ||
16         (shExpMatch(host, "login.windows.net")) ||
17         // IP / Port test page
18         (shExpMatch(host, "portquiz.net"))) {
19         return bypassproxy
20     }
21 // ==========================================================
22     return bypassproxy
   }
```

Note: The line "var bypassproxy = "PROXY 1.1.1.1:3128; PROXY 2.2.2.2:3128";" is doing nothing here. You can leave as is on the Proxy Bypass PAC, but you need to correct the production PAC values.

Bypass PAC URL on this example

http://pac.zscalerthree.net/maidenheadbridge.com/bypass.pac

2. Configure the URL of the "Proxy Bypass PAC" on each CSC and refresh the list.

```
Selection: 9

Please, select method to configure Proxy Bypass List

1) Auto - Proxy Bypass PAC URL                                  1
2) Manual
3) Quit
Enter your choice: 1

Please, select method to configure Proxy Bypass List

1) Configure Proxy Bypass PAC URL and/or Update Proxy Bypasses  2
2) See PAC Proxy Bypass Example
3) Quit
Enter your choice: 1
Proxy Bypass Configuration

Your current Proxy Bypass PAC URL is

Do you want to change the Proxy Bypass PAC URL?                 3
1) Yes
2) No
Enter your choice: 1

Please, input Proxy Bypass PAC URL
Bypass PAC URL:http://pac.zscalerthree.net/maidenheadbridge.com/bypass.pac   4

Your current Proxy Bypass PAC URL is: http://pac.zscalerthree.net/maidenheadbridge.com/bypass.pac

Do you want to refresh Proxy Bypass List?                       5
1) Yes
2) No
Enter your choice: 1

This is your current Proxy Bypass List

.okta.com
.oktacdn.com
.okta-emea.com
login.mydomain.com
login.microsoftonline.com
login.microsoft.com
login.windows.net
portquiz.net

Do you want apply changes?                                      6
1) Yes
2) No
Enter your choice: 1

Proxy Bypass List updated sucessfully.                          7
```

3. Check your VIP Proxy and Bypass Proxy using "Show Configuration and Status" on the CSC.

```
TRAFFIC REDIRECTION Options
To Zscaler: VIP Proxy: 172.31.200.87:80 (or :9400) | Route all traffic via CSC GW IP | Zscaler Global Proxies (port 80/9400) via CSC GW IP
Direct to Internet: Bypass Proxy: 172.31.200.66:3128 | Zscaler Global Proxies (port 3128) via CSC GW IP
```

4. Create your production PAC file and Copy/Paste section 3 for Proxy Bypasses, and put the correct values for variables "tozscaler" and "bypassproxy"

```
function FindProxyForURL(url, host) {
   // ==========================================================
   // Section 1: Zscaler standard PAC values

   var privateIP = /^(0|10|127|192\.168|172\.1[6789]|172\.2[0-9]|172\.3[01]|169\.254|192\.88\.99)\.[0-9.]+$/;
   var resolved_ip = dnsResolve(host);

   /* Don't send non-FQDN or private IP auths to us */
   if (isPlainHostName(host) || isInNet(resolved_ip, "192.0.2.0", "255.255.255.0") || privateIP.test(resolved_ip))
      return "DIRECT";

   /* FTP goes directly */
   if (url.substring(0, 4) == "ftp:")
      return "DIRECT";

   /* test with ZPA */
   if (isInNet(resolved_ip, "100.64.0.0", "255.255.0.0"))
      return "DIRECT";

   // ==========================================================
   // Section 2: Assigning values to "tozscaler" and "bypassproxy"
   //

   // CSC VIP
   var tozscaler = "PROXY 172.31.200.87:80";
   // CSC Proxy Bypass
   var bypassproxy = "PROXY 172.31.200.66:3128";

   // ==========================================================
   // Section 3: Bypass via Cloud Security Connectors

   // Bypass via CSC Public IPs (Examples)
   // Okta Domains (for Location Rules)
   if ((shExpMatch(host, "*.okta.com")) ||
      (shExpMatch(host, "*.oktacdn.com")) ||
      (shExpMatch(host, "*.okta-emea.com")) ||
      (shExpMatch(host, "login.mydomain.com")) ||
      // O365 Domains for ConditionalAccess
      (shExpMatch(host, "login.microsoftonline.com")) ||
      (shExpMatch(host, "login.microsoft.com")) ||
      (shExpMatch(host, "login.windows.net")) ||
      // IP / Port test page
      (shExpMatch(host, "portquiz.net"))) {
      return bypassproxy
   }
   // ==========================================================
   // Section 4: Default Traffic

   /* Default Traffic Forwarding. Forwarding to Zen on port 80, but you can use port 9400 also */
   return tozscaler
}
```

Production PAC file URL on this example

http://pac.zscalerthree.net/maidenheadbridge.com/production.pac

5. Checking traffic “tozscaler” and “bypass” using CURL command:

CURL command is available on Linux and Win10. You can check the traffic “tozscaler” or “proxy bypass” using the following commands:

Traffic “tozscaler”

Put the values of the VIP Proxy on “--proxy”

In this example:

Linux:

```
curl -s --proxy http://172.31.200.87:80 ip.zscaler.com | grep You
```

Win 10:

curl -s --proxy http://172.31.200.87:80 ip.zscaler.com | findstr You

Result expected:

```
<div class="headline">You are accessing the Internet via Zscaler Cloud: Washington DC in the zscalerthree.net cloud.</div>
<div class="details" style="margin-top: 20px">Your request is arriving at this server from the IP address <span class="detailOutput">165.225.48.118</span></div>
<div class="details">Your Gateway IP Address is <span class="detailOutput">54.163.234.160<</span></div>
```

Proxy Bypass Traffic:

We are testing the website “portquiz.net” to check that the Bypass works. The page “portquiz.net” returns your public IP and TCP port. Please, note this is a third-party tool, and sometimes it takes a long to answer or is unresponsive.

In this example:

Linux:

curl -s --proxy http://172.31.200.66:3128 portquiz.net

Win 10:

curl -s --proxy http://172.31.200.66:3128 portquiz.net

Result expected:

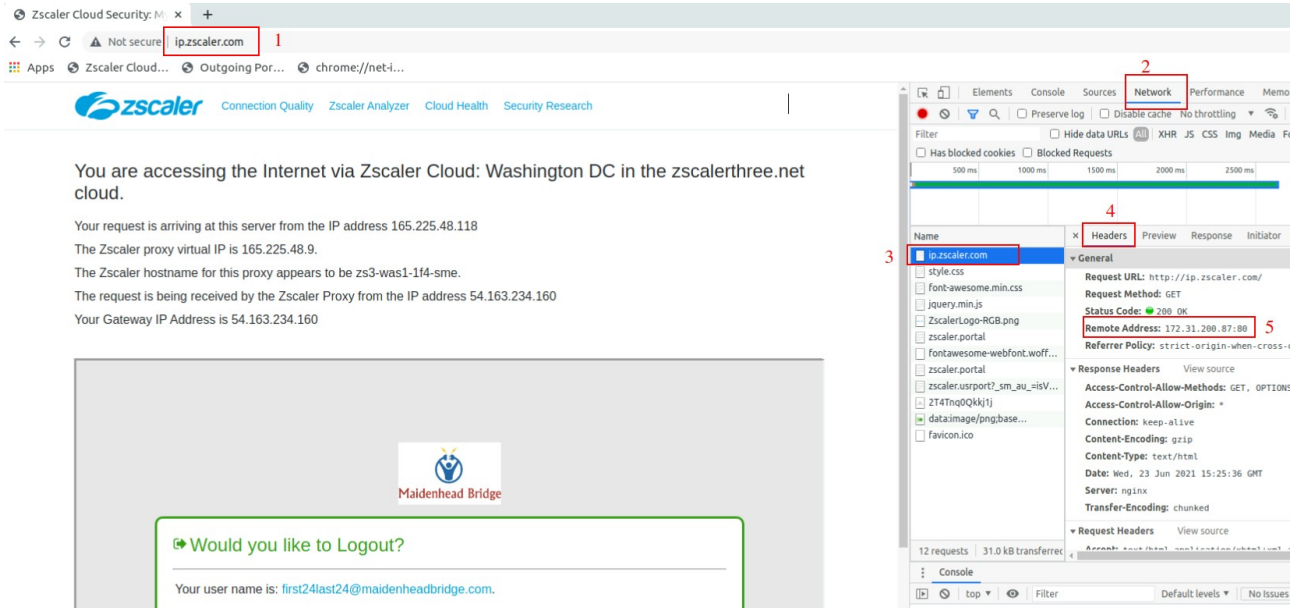
Port 80 test successful!
Your IP: **18.204.121.250**

6. Checking traffic “tozscaler” and “bypass” using Browser command:

Please, setup the Browser proxy using the production PAC URL. In our example is: http://pac.zscalerthree.net/maidenheadbridge.com/production.pac

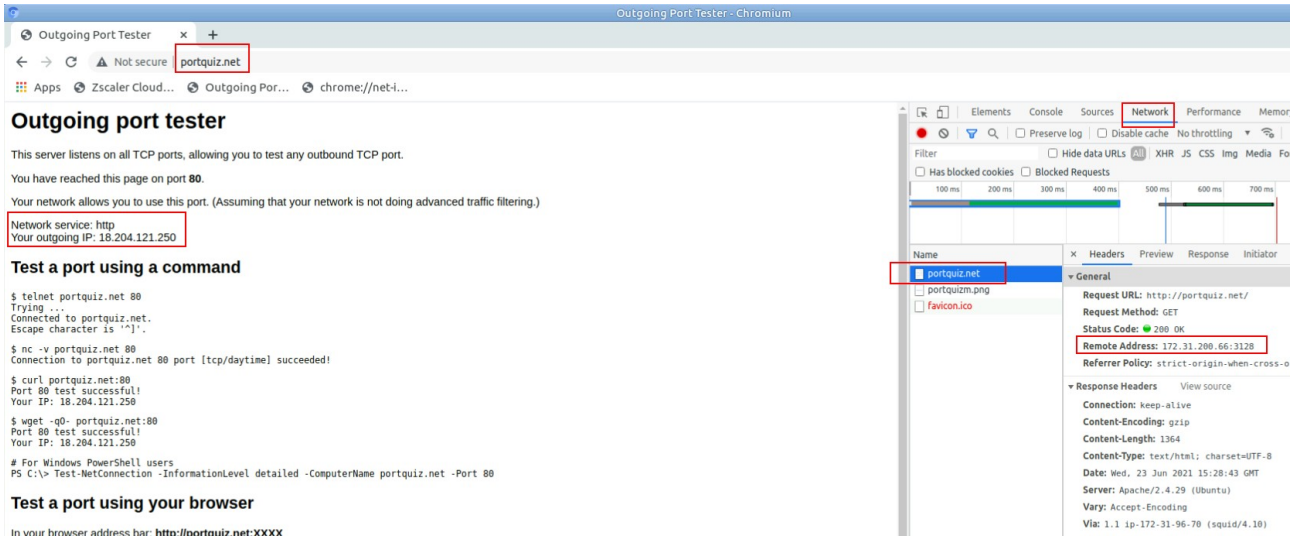
Traffic “tozscaler”

Go to page: ip.zscaler.com and using Chrome Developer tools check the proxy in use:



Proxy Bypass Traffic

Using our example, we are going to http://portquiz.net and using Chrome Developer tools check the proxy in use:



7.3.3.3 Manual

If you want to update manually your Proxy Bypass list, follow this steps.

1. Select Option 2)

```
1) Auto - Proxy Bypass PAC URL
2) Manual
3) Quit
Enter your choice: 2

Please, read the instructions carefully:

You are going to edit the list using NANO editor

The following formats are accepted:

Full Domains:  'www.example.com'
Wildcard for subdomains: '.example.com' - This will allow all subdomains of example.com

To save, press CTRL-X and 'Yes'

Paid attention to ERROR messages if any. ERRORs must be corrected before to continue

Do you want to continue? (y/n)?
```

2. Input “y”

```
  GNU nano 4.8                          domains                          Modified
.okta.com
.oktacdn.com
.okta-emea.com
login.mydomain.com
login.microsoftonline.com
login.microsoft.com
login.windows.net
portquiz.net
manualAdded.com

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     M-U Undo
^X Exit        ^R Read File   ^\ Replace     ^U Paste Text  ^T To Spell    ^_ Go To Line  M-E Redo
```

3. Add / Delete / Modify your full domains and subdomains
4. Please, CTL+X and “Yes” (and after next prompt Enter) to Save
5. The modified Bypass List will be displayed.

```
This is your current Proxy Bypass List

.okta.com
.oktacdn.com
.okta-emea.com
login.mydomain.com
login.microsoftonline.com
login.microsoft.com
login.windows.net
portquiz.net
manualAdded.com


Do you want apply changes?
1) Yes
2) No
Enter your choice:
```

6. Apply Changes Yes or No. If “1” you will receive the following message:

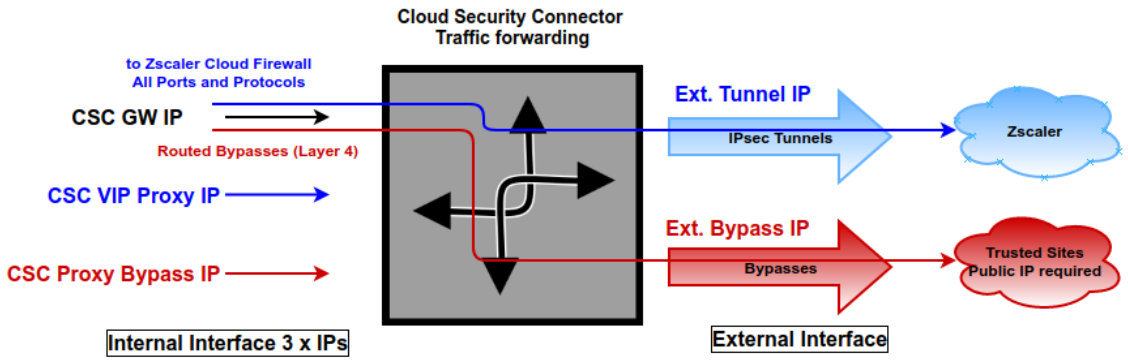
```
Do you want apply changes?
1) Yes
2) No
Enter your choice: 1

Proxy Bypass List updated sucessfully.
```

7.4 Routed Bypass

When routing all traffic via the CSC GW IP, the Routed Bypass functionality allows you to connect specific destinations (IP/Subnet) direct to the Internet, using your Public IP. By default, all destinations will travel via the tunnels to Zscaler. If you want to bypass the tunnel, you need to create a Routed Bypass Rule.

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

7.4.1 Routed Bypass - Traffic Flow



7.4.2 View Current Routed Bypass List

You can select to view the Routed Bypass Rules in Compact format or JSON.

```
Selection: 10

Please, Select 'Compact' or 'Json' format
1) Compact
2) Json
3) Quit
Enter your choice:
```

7.4.2.1 Compact

```
Current Values configured are:

Index: 0, Protocol: tcp, SourceIP: 0.0.0.0/0, DestinationIP: 20.190.128.0/18, FromPort: 80, To Port: 80, Description: "O365 Login URLs 1"
Index: 1, Protocol: tcp, SourceIP: 0.0.0.0/0, DestinationIP: 20.190.128.0/18, FromPort: 443, To Port: 443, Description: "O365 Login URLs 2"
Index: 2, Protocol: tcp, SourceIP: 0.0.0.0/0, DestinationIP: 40.126.0.0/18, FromPort: 80, To Port: 80, Description: "O365 Login URLs 3"
Index: 3, Protocol: tcp, SourceIP: 0.0.0.0/0, DestinationIP: 52.47.209.216/32, FromPort: 80, To Port: 80, Description: "portquiz.net"
Index: 4, Protocol: tcp, SourceIP: 0.0.0.0/0, DestinationIP: 40.126.0.0/18, FromPort: 443, To Port: 443, Description: "O365 Login URLs 4"
Index: 5, Protocol: udp, SourceIP: 0.0.0.0/0, DestinationIP: 13.107.64.0/18, FromPort: 3478, To Port: 3481, Description: "Skype and Teams UDP 1"
Index: 6, Protocol: udp, SourceIP: 0.0.0.0/0, DestinationIP: 52.112.0.0/14, FromPort: 3478, To Port: 3481, Description: "Skype and Teams UDP 2"
Index: 7, Protocol: udp, SourceIP: 0.0.0.0/0, DestinationIP: 52.120.0.0/14, FromPort: 3478, To Port: 3481, Description: "Skype and Teams UDP 3"
```

7.4.2.2 Json

```
Enter your choice: 2

{
  "routedBypassRules": [
    {
      "description": "O365 Login URLs 1",
      "ipProtocol": "tcp",
      "sourceCirdIp": "0.0.0.0/0",
      "destinationCirdIp": "20.190.128.0/18",
      "fromPort": "80",
      "toPort": "80"
    },
    {
      "description": "O365 Login URLs 2",
      "ipProtocol": "tcp",
      "sourceCirdIp": "0.0.0.0/0",
      "destinationCirdIp": "20.190.128.0/18",
      "fromPort": "443",
      "toPort": "443"
    },
    {
      "description": "O365 Login URLs 3",
      "ipProtocol": "tcp",
      "sourceCirdIp": "0.0.0.0/0",
      "destinationCirdIp": "40.126.0.0/18",
      "fromPort": "80",
      "toPort": "80"
    },
    {
      "description": "portquiz.net",
      "ipProtocol": "tcp",
      "sourceCirdIp": "0.0.0.0/0",
      "destinationCirdIp": "52.47.209.216/32",
      "fromPort": "80",
      "toPort": "80"
    },
    {
      "description": "O365 Login URLs 4",
      "ipProtocol": "tcp",
      "sourceCirdIp": "0.0.0.0/0",
      "destinationCirdIp": "40.126.0.0/18",
      "fromPort": "443",
      "toPort": "443"
    },
    {
      "description": "Skype and Teams UDP 1",
      "ipProtocol": "udp",
      "sourceCirdIp": "0.0.0.0/0",
      "destinationCirdIp": "13.107.64.0/18",
      "fromPort": "3478",
      "toPort": "3481"
    },
    {
      "description": "Skype and Teams UDP 2",
      "ipProtocol": "udp",
      "sourceCirdIp": "0.0.0.0/0",
      "destinationCirdIp": "52.112.0.0/14",
      "fromPort": "3478",
      "toPort": "3481"
    },
    {
      "description": "Skype and Teams UDP 3",
      "ipProtocol": "udp",
      "sourceCirdIp": "0.0.0.0/0",
      "destinationCirdIp": "52.120.0.0/14",
      "fromPort": "3478",
      "toPort": "3481"
    }
  ]
}

Press ENTER to continue
```

7.4.3 Configure Routed Bypass List

There are two methods to configure the Routed Bypass List: Routed Bypass URL and Manual. The recommended method is to use Routed Bypass URL.

```
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:
```

7.4.3.1 Routed Bypass URL

Routed Bypass URL is the recommended method. Create an AWS bucket or Azure Blob and place your JSON file on it. Here an example:
https://csc-gre-aws.s3.amazonaws.com/routedBypassRulesFile.json

```
Enter your choice: 1

Your Routed Bypass URL configured is: https://csc-gre-aws.s3.amazonaws.com/routedBypassRulesFile.json

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

Please, input Routed Bypass URL
Routed Bypass URL: https://csc-gre-aws.s3.amazonaws.com/routedBypassRulesFile.json

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

Routed Bypass JSON file imported successfully


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: tcp, SourceIP: 0.0.0.0/0, DestinationIP: 20.190.128.0/18, FromPort: 80, To Port: 80, Description: "O365 Login URLs 1"
Index: 1, Protocol: tcp, SourceIP: 0.0.0.0/0, DestinationIP: 20.190.128.0/18, FromPort: 443, To Port: 443, Description: "O365 Login URLs 2"
Index: 2, Protocol: tcp, SourceIP: 0.0.0.0/0, DestinationIP: 40.126.0.0/18, FromPort: 80, To Port: 80, Description: "O365 Login URLs 3"
Index: 3, Protocol: tcp, SourceIP: 0.0.0.0/0, DestinationIP: 52.47.209.216/32, FromPort: 80, To Port: 80, Description: "portquiz.net"
Index: 4, Protocol: tcp, SourceIP: 0.0.0.0/0, DestinationIP: 40.126.0.0/18, FromPort: 443, To Port: 443, Description: "O365 Login URLs 4"
Index: 5, Protocol: udp, SourceIP: 0.0.0.0/0, DestinationIP: 13.107.64.0/18, FromPort: 3478, To Port: 3481, Description: "Skype and Teams UDP 1"
Index: 6, Protocol: udp, SourceIP: 0.0.0.0/0, DestinationIP: 52.112.0.0/14, FromPort: 3478, To Port: 3481, Description: "Skype and Teams UDP 2"
Index: 7, Protocol: udp, SourceIP: 0.0.0.0/0, DestinationIP: 52.120.0.0/14, FromPort: 3478, To Port: 3481, Description: "Skype and Teams UDP 3"

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

(Index: 0) Rule "O365 Login URLs 1" was created succesfully.
(Index: 1) Rule "O365 Login URLs 2" was created succesfully.
(Index: 2) Rule "O365 Login URLs 3" was created succesfully.
(Index: 3) Rule "portquiz.net" was created succesfully.
(Index: 4) Rule "O365 Login URLs 4" was created succesfully.
(Index: 5) Rule "Skype and Teams UDP 1" was created succesfully.
(Index: 6) Rule "Skype and Teams UDP 2" was created succesfully.
(Index: 7) Rule "Skype and Teams UDP 3" was created succesfully.

Routed Bypass List updated succesfully.

Press ENTER to continue
```

7.4.3.2 Manual (Paste Routed Bypass JSON file)

Another option to configure Routed Bypass Rules is to paste the JSON file using the following menu:

```
Enter your choice: 2


WARNING: Manual Configuration will remove the Bypass Routed URL if configured.

Do you want to paste the Routed Bypass Rules JSON File?
1) Yes
2) No
Enter your choice: 1

Please, paste Routed Bypass JSON File and press 'Enter' if required.

NOTE: If the json file has errors, it is possible that the script will hang. Press '}' and 'Enter' to end the operation.

Routed Bypass JSON file:
```

and paste the JSON file. The JSON file will be displayed, and if no errors are found, you can apply the changes:

```
        },
        {
            "description": "Skype and Teams UDP 3",
            "ipProtocol": "udp",
            "sourceCirdIp": "0.0.0.0/0",
            "destinationCirdIp": "52.120.0.0/14",
            "fromPort": "3478",
            "toPort": "3481"
        }
    ]
}

Routed Bypass JSON file imported successfully


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: tcp, SourceIP: 0.0.0.0/0, DestinationIP: 20.190.128.0/18, FromPort: 80, To Port: 80, Description: "O365 Login URLs 1"
Index: 1, Protocol: tcp, SourceIP: 0.0.0.0/0, DestinationIP: 20.190.128.0/18, FromPort: 443, To Port: 443, Description: "O365 Login URLs 2"
Index: 2, Protocol: tcp, SourceIP: 0.0.0.0/0, DestinationIP: 40.126.0.0/18, FromPort: 80, To Port: 80, Description: "O365 Login URLs 3"
Index: 3, Protocol: tcp, SourceIP: 0.0.0.0/0, DestinationIP: 52.47.209.216/32, FromPort: 80, To Port: 80, Description: "portquiz.net"
Index: 4, Protocol: tcp, SourceIP: 0.0.0.0/0, DestinationIP: 40.126.0.0/18, FromPort: 443, To Port: 443, Description: "O365 Login URLs 4"
Index: 5, Protocol: udp, SourceIP: 0.0.0.0/0, DestinationIP: 13.107.64.0/18, FromPort: 3478, To Port: 3481, Description: "Skype and Teams UDP 1"
Index: 6, Protocol: udp, SourceIP: 0.0.0.0/0, DestinationIP: 52.112.0.0/14, FromPort: 3478, To Port: 3481, Description: "Skype and Teams UDP 2"
Index: 7, Protocol: udp, SourceIP: 0.0.0.0/0, DestinationIP: 52.120.0.0/14, FromPort: 3478, To Port: 3481, Description: "Skype and Teams UDP 3"

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

(Index: 0) Rule "O365 Login URLs 1" was created succesfully.
(Index: 1) Rule "O365 Login URLs 2" was created succesfully.
(Index: 2) Rule "O365 Login URLs 3" was created succesfully.
(Index: 3) Rule "portquiz.net" was created succesfully.
(Index: 4) Rule "O365 Login URLs 4" was created succesfully.
(Index: 5) Rule "Skype and Teams UDP 1" was created succesfully.
(Index: 6) Rule "Skype and Teams UDP 2" was created succesfully.
(Index: 7) Rule "Skype and Teams UDP 3" was created succesfully.

Routed Bypass List updated succesfully.

Press ENTER to continue
```

7.5 Log Information

This section shows the logs for Tunnels, Load Balancer, Etc.

```
Log Information
12) View Current Month
13) View Last 6 Months
```

You can see the current month or last six months.

```
Selection: 12

Current Month (July 2021) Logs for csc-mux-3-2Gbps-vm-1

Jul 28 20:50:19 root: (MHB-CSC)(DOWN) Load Balancer: All Ztunnels are inactive since: Wed 28 Jul 20:50:19 UTC 2021
Jul 28 20:50:20 root: (MHB-CSC)(INFO) Routed Bypass Rules JSON file integrity is OK
Jul 28 20:50:21 root: (MHB-CSC)(UP) CSC Mux 3.2 Gbps for Azure was powered ON: Wed 28 Jul 20:50:21 UTC 2021
Jul 29 06:41:52 root: (MHB-CSC)(DOWN) Load Balancer: All Ztunnels are inactive since: Thu 29 Jul 06:41:52 UTC 2021
Jul 29 06:41:53 root: (MHB-CSC)(INFO) Routed Bypass Rules JSON file integrity is OK
Jul 29 06:41:54 root: (MHB-CSC)(UP) CSC Mux 3.2 Gbps for Azure was powered ON: Thu 29 Jul 06:41:54 UTC 2021
Jul 29 07:46:55 root: (MHB-CSC)(DOWN) Load Balancer: All Ztunnels are inactive since: Thu 29 Jul 07:46:55 UTC 2021
Jul 29 07:46:56 root: (MHB-CSC)(INFO) Routed Bypass Rules JSON file integrity is OK
Jul 29 07:46:56 root: (MHB-CSC)(UP) CSC Mux 3.2 Gbps for Azure was powered ON: Thu 29 Jul 07:46:56 UTC 2021
Jul 29 07:47:25 root: (MHB-CSC)(UP) IPsec: Primary tunnel on Ztun3 is active since Thu 29 Jul 07:47:25 UTC 2021
Jul 29 07:47:25 root: (MHB-CSC)(UP) IPsec: Primary tunnel on Ztun7 is active since Thu 29 Jul 07:47:25 UTC 2021
Jul 29 07:47:25 root: (MHB-CSC)(UP) IPsec: Primary tunnel on Ztun4 is active since Thu 29 Jul 07:47:25 UTC 2021
Jul 29 07:47:25 root: (MHB-CSC)(UP) IPsec: Primary tunnel on Ztun6 is active since Thu 29 Jul 07:47:25 UTC 2021
Jul 29 07:47:25 root: (MHB-CSC)(UP) IPsec: Primary tunnel on Ztun8 is active since Thu 29 Jul 07:47:25 UTC 2021
Jul 29 07:47:25 root: (MHB-CSC)(UP) IPsec: Primary tunnel on Ztun2 is active since Thu 29 Jul 07:47:25 UTC 2021
Jul 29 07:47:25 root: (MHB-CSC)(UP) IPsec: Primary tunnel on Ztun5 is active since Thu 29 Jul 07:47:25 UTC 2021
Jul 29 07:47:25 root: (MHB-CSC)(UP) IPsec: Primary tunnel on Ztun1 is active since Thu 29 Jul 07:47:25 UTC 2021
Jul 29 07:47:56 root: (MHB-CSC)(UP) Load Balancer: Balanced tunnels change on: Thu 29 Jul 07:47:56 UTC 2021
Jul 29 07:47:56 root: (MHB-CSC)(DOWN) Load Balancer: Ztun1 is NO active since: Thu 29 Jul 07:47:56 UTC 2021
Jul 29 07:47:56 root: (MHB-CSC)(UP) Load Balancer: Ztun2 is active since: Thu 29 Jul 07:47:56 UTC 2021 using primary node
Jul 29 07:47:56 root: (MHB-CSC)(UP) Load Balancer: Ztun3 is active since: Thu 29 Jul 07:47:56 UTC 2021 using primary node
Jul 29 07:47:56 root: (MHB-CSC)(UP) Load Balancer: Ztun4 is active since: Thu 29 Jul 07:47:56 UTC 2021 using primary node
Jul 29 07:47:56 root: (MHB-CSC)(UP) Load Balancer: Ztun5 is active since: Thu 29 Jul 07:47:56 UTC 2021 using primary node
Jul 29 07:47:56 root: (MHB-CSC)(UP) Load Balancer: Ztun6 is active since: Thu 29 Jul 07:47:56 UTC 2021 using primary node
Jul 29 07:47:56 root: (MHB-CSC)(UP) Load Balancer: Ztun7 is active since: Thu 29 Jul 07:47:56 UTC 2021 using primary node
Jul 29 07:47:56 root: (MHB-CSC)(UP) Load Balancer: Ztun8 is active since: Thu 29 Jul 07:47:56 UTC 2021 using primary node
Jul 29 07:48:57 root: (MHB-CSC)(UP) Load Balancer: Balanced tunnels change on: Thu 29 Jul 07:48:57 UTC 2021
Jul 29 07:48:57 root: (MHB-CSC)(UP) Load Balancer: Ztun1 is active since: Thu 29 Jul 07:48:57 UTC 2021 using primary node
Jul 29 07:48:57 root: (MHB-CSC)(UP) Load Balancer: Ztun2 is active since: Thu 29 Jul 07:48:57 UTC 2021 using primary node
Jul 29 07:48:57 root: (MHB-CSC)(UP) Load Balancer: Ztun3 is active since: Thu 29 Jul 07:48:57 UTC 2021 using primary node
Jul 29 07:48:57 root: (MHB-CSC)(UP) Load Balancer: Ztun4 is active since: Thu 29 Jul 07:48:57 UTC 2021 using primary node
Jul 29 07:48:57 root: (MHB-CSC)(UP) Load Balancer: Ztun5 is active since: Thu 29 Jul 07:48:57 UTC 2021 using primary node
Jul 29 07:48:57 root: (MHB-CSC)(UP) Load Balancer: Ztun6 is active since: Thu 29 Jul 07:48:57 UTC 2021 using primary node
Jul 29 07:48:57 root: (MHB-CSC)(UP) Load Balancer: Ztun7 is active since: Thu 29 Jul 07:48:57 UTC 2021 using primary node
Jul 29 07:48:57 root: (MHB-CSC)(UP) Load Balancer: Ztun8 is active since: Thu 29 Jul 07:48:57 UTC 2021 using primary node
```

7.6 Configuration Wizards

```
Configuration Wizards
14) Change Cloud, Nodes, VPN Credentials, DNS, Syslog and more
15) Switch Tunnels - Primary / Secondary
16) High Availability changing Route/s
17) Update ZEN Nodes Database
```

7.6.1 Change Cloud, Nodes, VPN Credentials, DNS, Syslog and more

In this section, you can run the initial configuration wizard to change Cloud & Zscaler Nodes, VPN Credentials, DNS servers, Bypass URL and Syslog Servers.

```
Selection: 14

Welcome to the CSC MUX 3.2 Gbps Configuration Wizard

1) Configuration required on your Zscaler Console: VPN credentials and Location
 --> VPN Credentials creation: Go to > Administration > VPN Credentials > Add VPN Credential -> Select Authentication Type = FDQN and configure 'User ID' and 'Pre-Shared Key'
 --> Location creation: Go to > Administration > Location > Add Location. Put your Location values and select 'VPN Credentials' created in the step before
2) Run the Wizard on the CSC and Select Cloud, Nodes, input VPN Credentials, DNS Servers, Bypass PAC URL and Syslog Servers

Current Values Configured:
-------------------
ZSCALER INFORMATION
Zscaler Cloud:  zscalerthree
Primary ZEN node: WashingtonDC_2 | Hostname: was1-2-vpn.zscalerthree.net | IP: 165.225.8.35
Secondary ZEN node: NewYorkIII | Hostname: nyc3-vpn.zscalerthree.net | IP: 165.225.38.52
-------------------
CREDENTIALS INFORMATION
User ID: csc-azure-02@maidenheadbridge.com | Pre-Shared Key: <Run the Wizard to see it>
-------------------
DNS Servers: 1.1.1.1 ; 8.8.8.8
-------------------
Bypass Proxy PAC URL
Your current Bypass PAC URL is http://pac.zscalerthree.net/8FM8NgF7NMFq/csc-azure-bypass.pac
-------------------
SYSLOG / SIEM information
Primary Syslog / SIEM IP: 10.2.3.4
Secondary Syslog / SIEM IP: Not configured
Syslog / SIEM TCP port: 514
-------------------
Are you ready to continue? (y/n)
```

Details of configuration on Chapter 6.

7.6.2 Switch Tunnels - Primary / Secondary

In case you want to switch the Primary / Secondary tunnel you can do it from this menu.

```
Selection: 15
-------------------
ZSCALER INFORMATION

You current Zscaler Cloud and Nodes are:

Zscaler Cloud:  zscalerthree
Primary ZEN node: WashingtonDC_2 | Hostname: was1-2-vpn.zscalerthree.net | IP: 165.225.8.35
Secondary ZEN node: NewYorkIII | Hostname: nyc3-vpn.zscalerthree.net | IP: 165.225.38.52

Do you want to switch these values? (y/n) y


Validating Configuration

Your Cloud is: zscalerthree

Checking NEW Primary Node NewYorkIII hostname nyc3-vpn.zscalerthree.net
Hostname nyc3-vpn.zscalerthree.net has IP 165.225.38.52
Node NewYorkIII is Alive

Checking NEW Secondary Node WashingtonDC_2 hostname was1-2-vpn.zscalerthree.net
Hostname was1-2-vpn.zscalerthree.net has IP 165.225.8.35
Node WashingtonDC_2 is Alive

Are this values correct? (y/n)? (answering 'y' will reboot the CSC):
```

7.6.3 High Availability changing Route/s

```
Selection: 14

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

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

Recommended: Use the same Resource Group for both CSCs and Route Tables. This is to avoid permission problems with IAM roles.

The following instructions are considering that all resources are on the same Resource Group:

1) Deploy a pair of CSCs with the following conditions:
   1.1) There is connectivity each other via their internal interfaces.
   1.2) On each CSC VM, go to Identity -> System Assigned and Turn ON status. (and Save).
2) Go to Resource Group -> Access Control (IAM) and Click '+ Add'
   2.1) Select 'Add role assignment'
   2.2) Input the following values:
      -> Role: Contributor
      -> Assign Access to: Virtual Machine
      -> Select: <Select both CSC's VMs> (and Save)
3) Create (or move) the Route Tables inside the same Resouce Group than the CSCs.
   3.1) Go to Routes (inside the Route Table) and create the Routes that will be controlled by the CSC HA group:
      -> Route name: <any name you want>
      -> Address prefix: <Subnet/Mask>
            Examples: 0.0.0.0/0 (if you want to send all traffic via Zscaler) or 185.46.212.88/32 (when using PAC files and/or Explicit Proxy
      -> Next hop type: Virtual Appliance
      -> Next hop address: <Input GW (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

How it works:

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

---------------------

The HA service is:  active (running) since Fri 2020-05-15 11:08:32 UTC; 21h ago

Identity Type: SystemAssigned

Current values configured are:

Route/s (Qty)= 3
Route 1: myroute (Route Table=csc-rt-1, Resource Group=Development)
Route 2: server-farm-1 (Route Table=csc-rt-for-servers, Resource Group=Development)
Route 3: CSC-Zscaler-Default (Route Table=Csc-Routing-table, Resource Group=Development)

Computer Name of other CSC in the pair: csc-v-2-0-B (Resource Group=Development)

Do you want to change this values?

1) Yes
2) No
3) Restart HA Service
4) Reset to default values
Enter your choice:
```

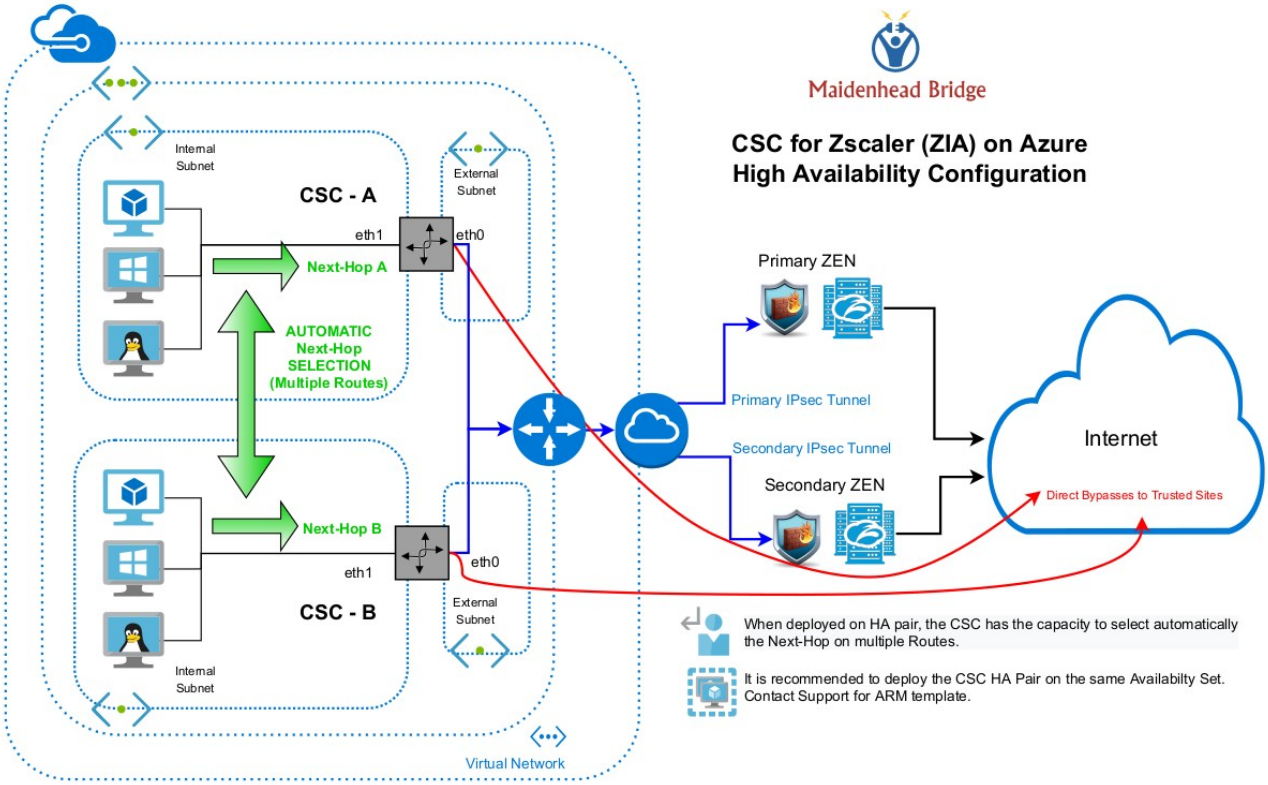
See Appendix A for a detailed configuration with examples.

8 Appendix A: High Availability to Zscaler using CSCs

8.1 Introduction:

When deployed on HA pair, the CSC has the capability to manage the “Next-Hop” of the route/s configured.

There is no limit of the amount of routes that can be configured. This allows to manipulate routes to Zscaler on more than one Route-Table.



8.2 Pre-requisites

The help provided on by the Configuration Wizard contains the pre-requisites:

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

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

Recommended: Use the same Resource Group for both CSCs and Route Tables. This is to avoid permission problems
with IAM roles.

The following instructions are considering that all resources are on the same Resource Group:

1) Deploy a pair of CSCs with the following conditions:
  1.1) There is connectivity each other via their internal interfaces.
  1.2) On each CSC VM, go to Identity -> System Assigned and Turn ON status. (and Save).
2) Go to Resource Group -> Access Control (IAM) and Click '+ Add'
  2.1) Select 'Add role assignment'
  2.2) Input the following values:
    -> Role: Contributor
    -> Assign Access to: Virtual Machine
    -> Select: <Select both CSC's VMs> (and Save)
3) Create (or move) the Route Tables inside the same Resouce Group than the CSCs.
  3.1) Go to Routes (inside the Route Table) and create the Routes that will be controlled by the CSC HA group:
    -> Route name: <any name you want>
    -> Address prefix: <Subnet/Mask>
        Examples: 0.0.0.0/0 (if you want to send all traffic via Zscaler) or 185.46.212.88/32 (when using PAC files
and/or Explicit Proxy)
    -> Next hop type: Virtual Appliance
    -> Next hop address: <Input GW (eth1, first IP) of any CSC>
  3.2) Go to Subnets and associate the Subnet with the Route Table.


How it works:

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

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

8.3 Configuration example:

8.3.1 Route Information

In this example, we are going to put under control of the CSC HA pair two routes:

1. **Route: CSC-Zscaler-Default** (Route Table=Csc-Routing-table, Resource Group=Development): This route has destination (Address Prefix): 0.0.0.0/0 and belongs to a route-table with subnets associated to Virtual Desktops. In this case, I want to send all traffic to Zscaler.

Routes

Search routes

Name	Address prefix	Next hop
CSC-Zscaler-Default	0.0.0.0/0	172.31.200.17

2. **Route: server-farm-1** (Route Table=csc-rt-for-servers, Resource Group=Development): This route has destination (Address Prefix): 185.46.212.88/32 and belongs to a route-table with subnets associated to Servers. In this case, I want to send only Web traffic setting the Proxy IP: 185.46.212.88 (Zscaler Global Proxy).

Routes

Search routes

Name	Address prefix	Next hop
server-farm-1	185.46.212.88/32	172.31.200.17

8.3.2 CSC Information

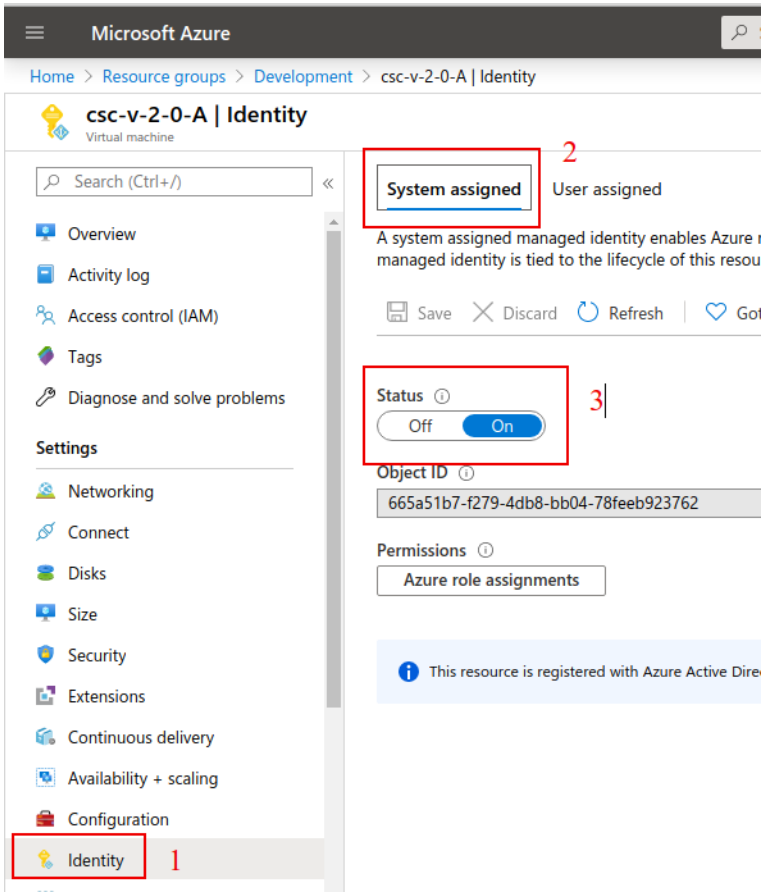
We need to obtain the “Computer Name” and Resource Group of each CSC on the pair. In this example will be:

- csc-v-2-0-A
- csc-v-2-0-B

csc-v-2-0-A	Virtual machine
csc-v-2-0-B	Virtual machine

8.3.3 Identity

On each CSC, Go to: Identity → System Assigned and turn ON status:

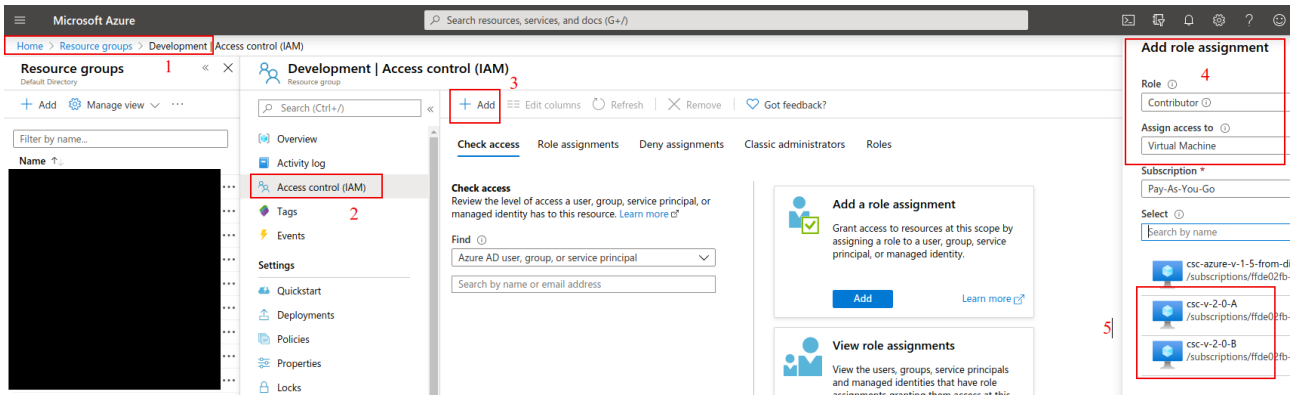


8.3.4 IAM Role

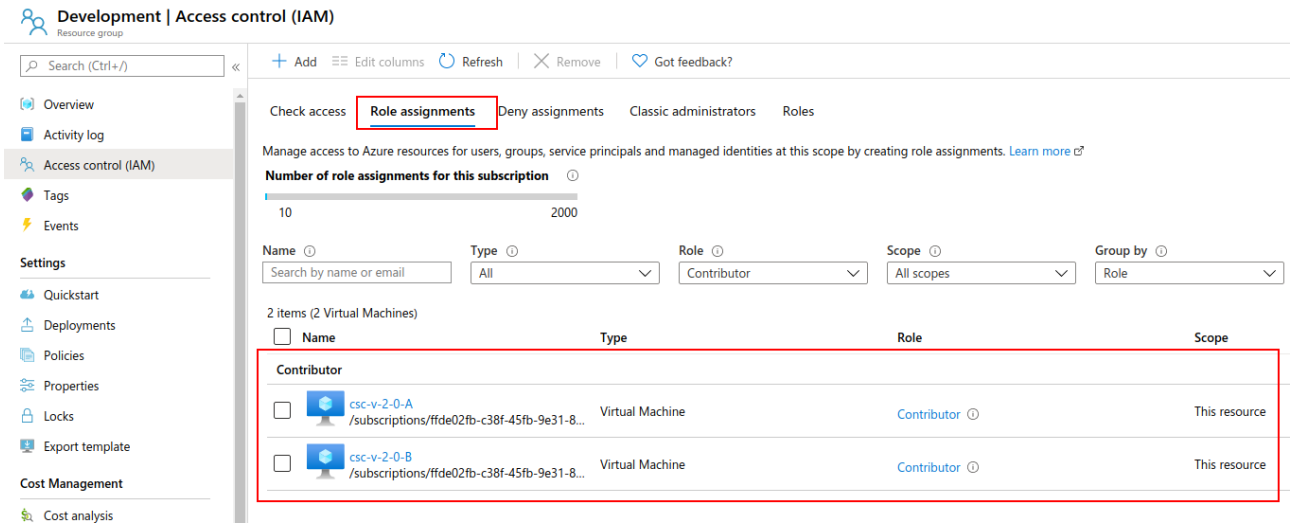
Note: In this example, the VMs and Route Tables are under the same Resource Group. For this reason, I am going to enable the IAM Role to the Resource Group and the IAM Role will be inherited.
If you have the Route Tables on different Resource Group, please, apply the proper permissions.

Go to:

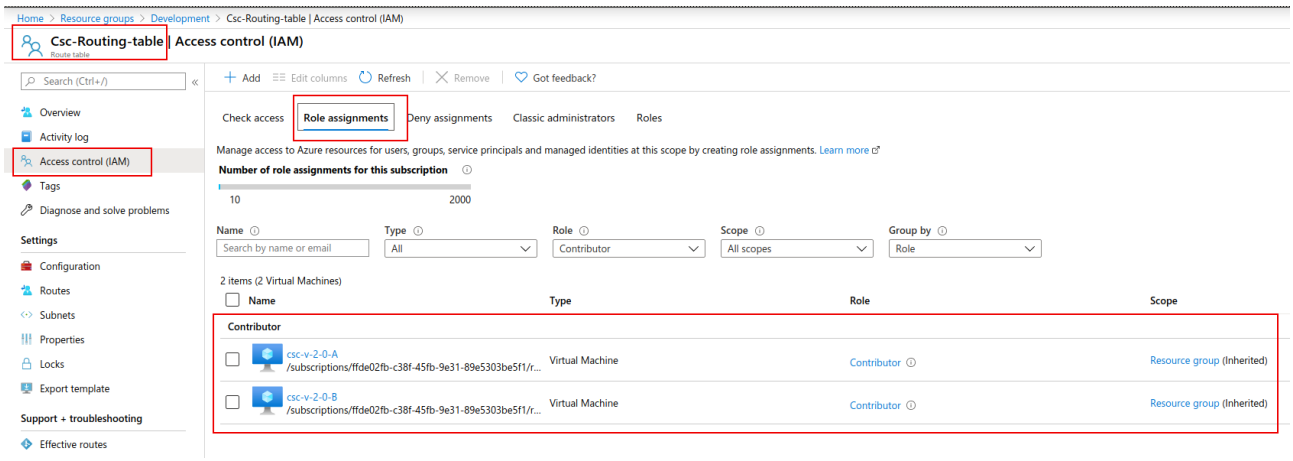
1. Resource Group
2. Access control (IAM)
3. Click “Add”
4. Add role assignment:
   - 4.1. Role: Contributor
   - 4.2. Assign Role to: Virtual Machine.
5. Select the CSCs



Now, Check Roles assignments:



and, when checking the Route Table → Access Control → Role assignments:



You can see that the CSCs are able to manage this Route Table.

8.4 Running the configuration wizard

Enter the Route (Route-tables / Resource Group) values and other CSC Computer Name (+Resource Group)

```
Do you want to change this values?

1) Yes
2) No
3) Restart HA Service
4) Reset to default values
Enter your choice: 1

Identity Type: SystemAssigned        The Wizard checks Identity

Please, input the Route/s values:

Route Name= CSC-Zscaler-Default      Enter your first ROUTE
Route Table= Csc-Routing-table
Resource Group= Development

Do you want to add another Route? (y/n)? y

Route Name= server-farm-1            Add next ROUTE
Route Table= csc-rt-for-servers
Resource Group= Development

Do you want to add another Route? (y/n)? n

Please, input values of other CSC in the pair
                                     Put "Other CSC" Computer Name
Computer Name= csc-v-2-0-B
Resource Group= Development

Values to configure are:
                                     Confirm values to configure
Route/s (Qty)=2
Route 1: CSC-Zscaler-Default (Route Table=Csc-Routing-table, Resource Group=Development)
Route 2: server-farm-1 (Route Table=csc-rt-for-servers, Resource Group=Development)

Computer Name of other CSC in the pair: csc-v-2-0-B (Resource Group=Development)

Do you want to apply changes? (y/n)? y

CSC HA is : active (running) since Sat 2020-05-16 20:38:25 UTC; 27ms ago
```

Now, do the same on the Other CSC.

Finally, check the status of the HA using “Show Configuration and Status” menu.

```
HIGH AVAILABILITY Information
The HA service is:  active (running) since Sat 2020-05-16 20:38:25 UTC; 1h 28min ago
Identity Type: SystemAssigned
Route to Zscaler using Next Hop: 172.31.200.14 of VM: csc-v-2-0-A (this CSC)
Current values configured are:
   Route/s (Qty)= 2
      Route 1: CSC-Zscaler-Default (Route Table=Csc-Routing-table, Resource Group=Development)
      Route 2: server-farm-1 (Route Table=csc-rt-for-servers, Resource Group=Development)
   Computer Name of other CSC in the pair: csc-v-2-0-B (Resource Group=Development)
```

9 Appendix B – AWS Systems Manager “Run Commands” to monitor the CSC

The easiest and cheapest way to manage the Cloud Security Connectors is to use AWS Systems Manager. AWS official documentation is available here: https://aws.amazon.com/systems-manager/.

With AWS Systems Manager, you can manage the CSC remotely. To do it, you need to create "Documents" in advance. "Documents" are a series of commands used by the "Run Command" functionality.

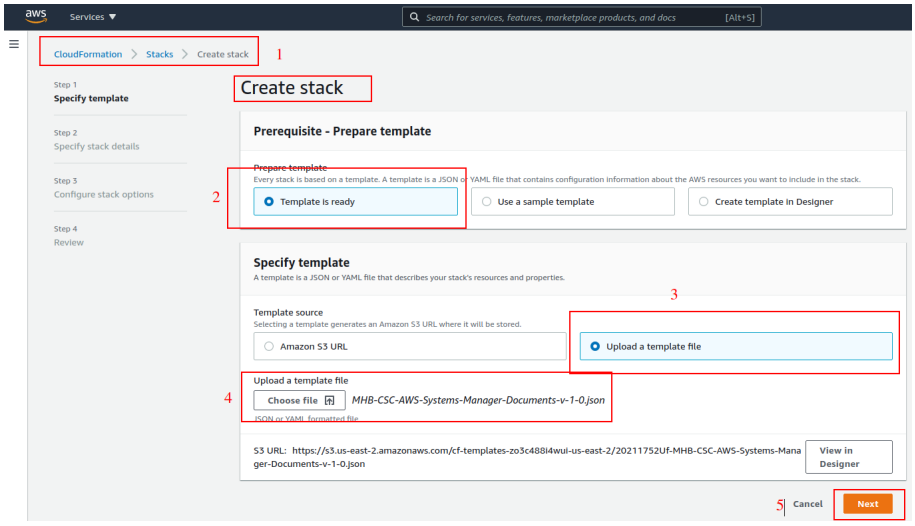
This section explains how to create the "Documents" and how to "Run Commands".

9.1 AWS Systems Manager: Create Documents

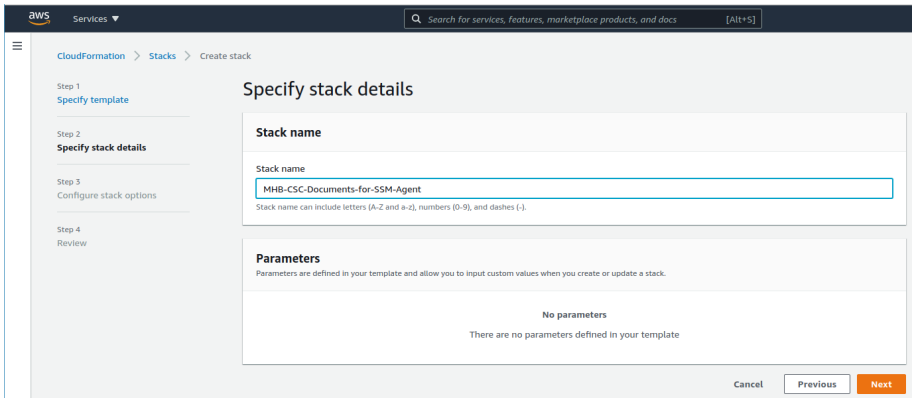
We provide a CloudFormation template to create all "Documents" in one shot.

Steps:

1. Download the CloudFormation template from: https://maidenheadbridge.freshdesk.com/support/solutions/folders/33000214143
2. Deploy Stack. Go to Cloudformation → Create Stack

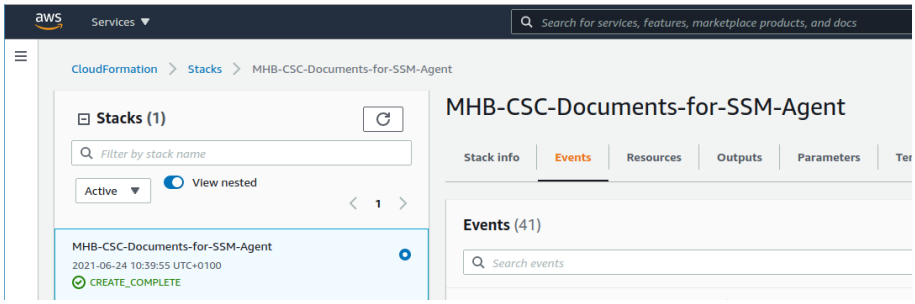


Click "Next" and put a name to the Stack.

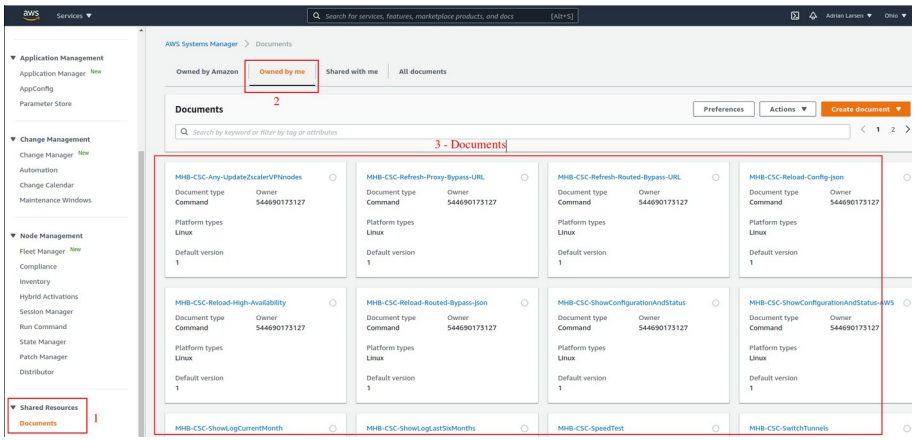


Click "Next", "Next" and "Create Stack".

Wait for the Stack to complete.



3. Check the Documents created on AWS Systems Manager. Go to Systems Manager.



9.2 Run Commands

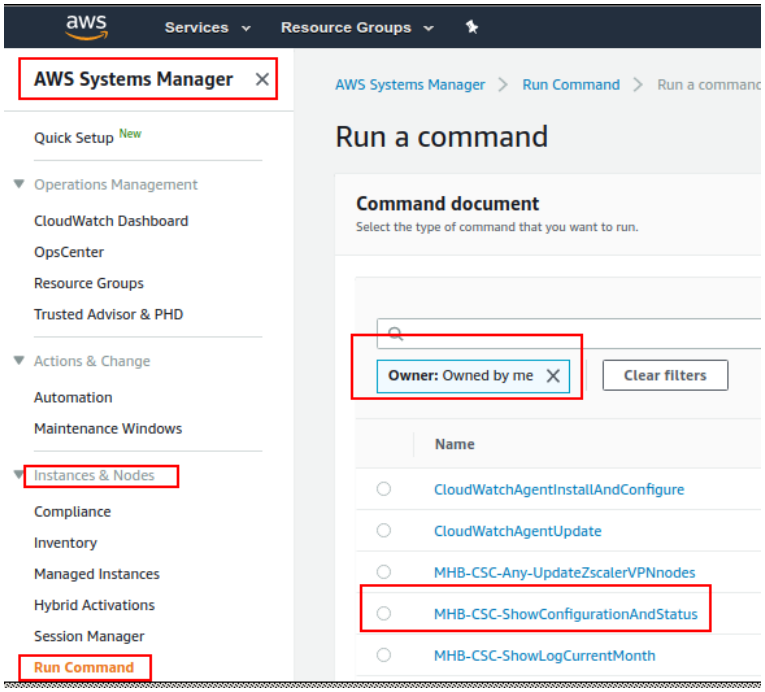
After you created the Documents, you are ready to Run Commands on the CSC.

You can see the results of the operation on the “Output” section or to store the results on a S3 Buckets for further inspection.

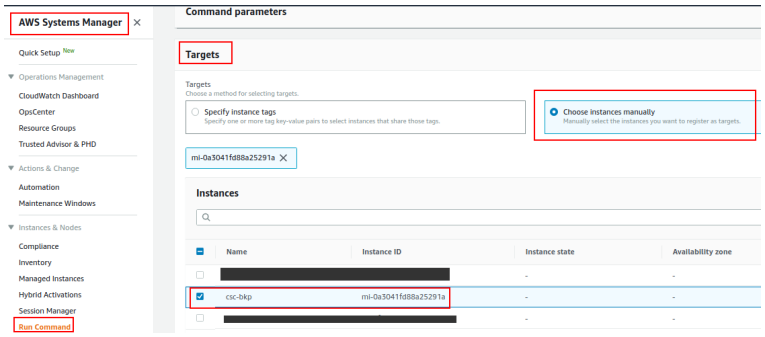
To Run Commands go to: AWS Systems Manager → Instances & Nodes → Run Command

Here an example of Running: MHB-CSC-ShowConfigurationAndStatus

1. Run a Command
2. Select the Document created (Tip: Select “Owned by me”)

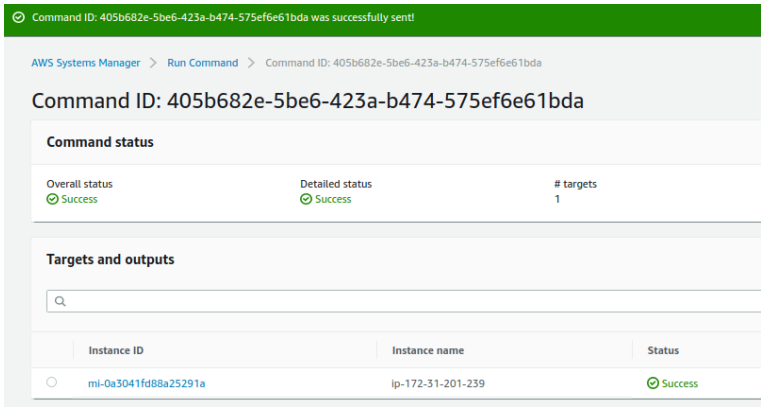


3. Scroll down and Select the Instances
4. We are selecting only one instance, but you can select as much as you want.

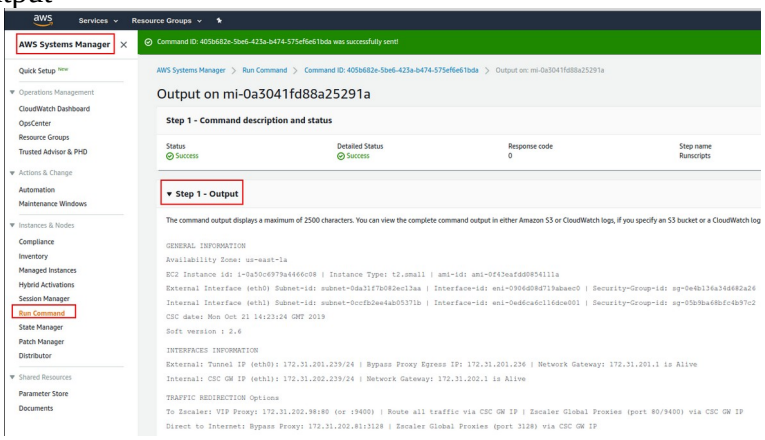


5. Click Run

Next Screen is:



6. Click “Instance ID” (mi-0a3041fd88a25291a)
7. Expand “Output”



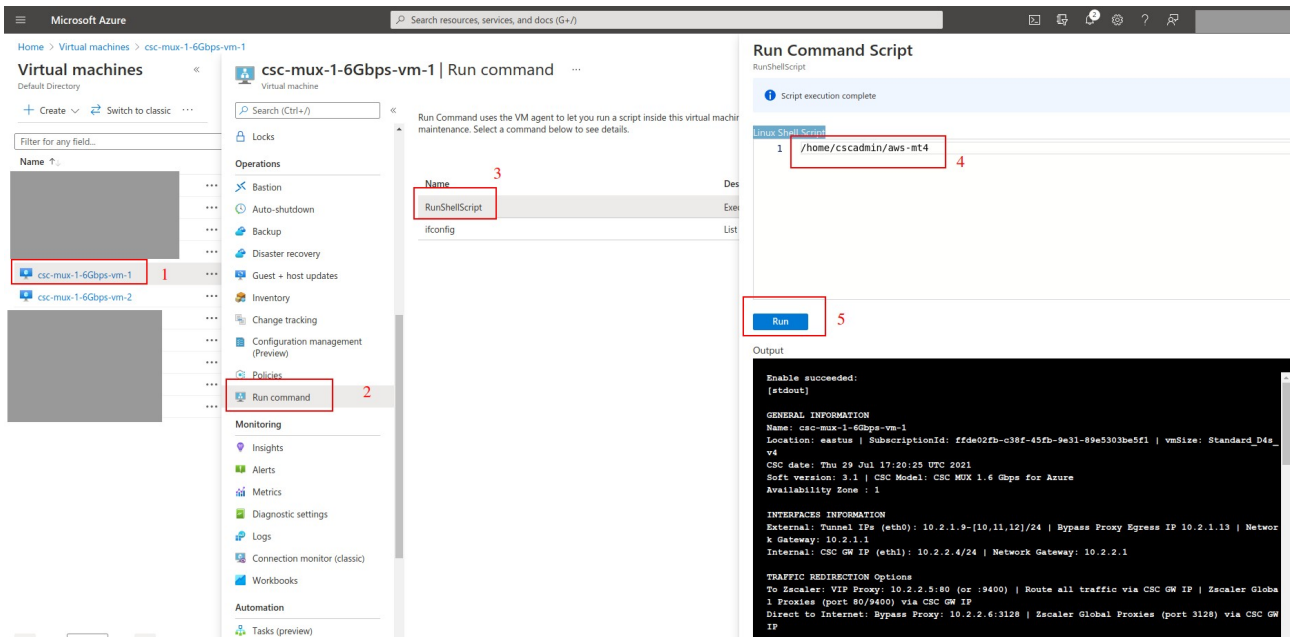
9.3 List of Documents available for "Run Command"

1. "MHB-CSC-ShowConfigurationAndStatus-AWS": Executes "Show Configuration and Status" test on CSCs for AWS with version 2.8 or below.
2. "MHB-CSC-ShowConfigurationAndStatus": Same as above, for all CSC all platforms.
3. "MHB-CSC-Refresh-Proxy-Bypass-URL": Refresh the Proxy Bypass list using the values of the Proxy Bypass PAC file stored in the URL configured.
4. "MHB-CSC-Refresh-Routed-Bypass-URL": Refresh the Routed Bypass list using the values of the JSON file stored in the URL configured.
5. "MHB-CSC-SpeedTest": Performs speedtest.net on the CSC.
6. "MHB-CSC-TraceRouteAndLatencyTest": Performs MyTraceRoute test against the Primary and Secondary ZEN. It also does a Reverse Test from the tunnel active to your Public IP if the tunnel is up.
7. "MHB-CSC-ShowLogCurrentMonth": Shows current month logs.
8. "MHB-CSC-ShowLogLastSixMonths": Shows last six month logs.
9. "MHB-CSC-SwitchTunnels": Switch tunnels.
10. "MHB-CSC-Reload-Config-json": Reloads the values of config.json file.
11. "MHB-CSC-Reload-High-Availability": Reloads the values of highAvailability.json file.
12. "MHB-CSC-Reload-Routed-Bypass-json": Reloads the values of routedBypassRulesFile.json.
13. "MHB-CSC-Any-UpdateZscalerVPNnodes": Updates the VPN node database on IPsec models. Not in use on the CSC for AWS.

10 Appendix C: "Run Commands" using Azure Portal

Similarly to AWS Systems Manager, Azure Portal can "Run Commands" (per VM). The Azure portal doesn't provide a complete management system like AWS Systems Manager, but you can "Run Commands" per VM. "Run Command" is particularly useful if you want to do a quick check and not SSH the CSC. Unfortunately, it is still very buggy and sometimes doesn’t work at all.

Instructions: Select the VM go to Run Command → RunShellScript and on “Linux Shell Script” put the command showed in the below table.



10.1 Table of Commands

Test #	Descritption	Command
1	MHB-CSC-ShowConfigurationAndStatus	/home/cscadmin/aws-mt4
2	MHB-CSC-SpeedTest	/home/cscadmin/aws-mt7
3	MHB-CSC-TraceRouteAndLatencyTest	/home/cscadmin/aws-mt6
4	MHB-CSC-Refresh-Proxy-Bypass-URL	/home/cscadmin/aws-bp-refresh-list
5	MHB-CSC-ShowLogCurrentMonth	/home/cscadmin/aws-l-current-month
6	MHB-CSC-Refresh-Routed-Bypass-URL	/home/cscadmin/aws-refresh-routed-bypass-url
7	MHB-CSC-ShowLogLastSixMonths	/home/cscadmin/aws-l-last-6-months
8	MHB-CSC-Reload-Routed-Bypass-json	/home/cscadmin/aws-reload-routed-bypass-json
9	MHB-CSC-Any-UpdateZscalerVPNnodes	/home/cscadmin/aws-node-region-update

11 Appendix D: Release Notes

11.1 Version 3.1 (July 2021)

Version 3.1 of the CSC Mux for Azure has the following enhancements:

- New! CSC Mux 1.6 Gbps (ex CSC Mux 1G). The CSC Mux with 4 x IPsec tunnels can deliver now 1.6 Gbps.
- New! CSC Mux 3.2 Gbps (ex CSC Mux 2G). The CSC Mux with 8 x IPsec tunnels can deliver now 3.2 Gbps.
- New! Routed Bypass functionality Added. The Routed Bypass allows you to bypass Zscaler for specific destinations when routing all traffic via the CSC Mux using your Public IP.

11.2 Version 3.0 (October 2020)

The CSC Mux for Azure was created merging two existing products: the CSC for Azure + CSC Mux for Vmware/Hyper-V.

This version contains all the features of the CSC for Azure (single) plus the following enhancements:

- The CSC Mux is using Ubuntu 20.04 as base OS
- The CSC Mux 1 Gbps can aggregate 4 x IPsec tunnels to deliver 1 Gbps to Zscaler.
- The CSC Mux 2 Gbps can aggregate 8 x IPsec tunnels to deliver 1 Gbps to Zscaler.
- Speedtest runs in parallel in all tunnels and returns; as a result, the sum of all tests.

12 Appendix E: VM Sizes for CSC Mux 1.6 Gbps and CSC Mux 3.2 Gbps

This Appendix shows the VM Sizes you can use for the CSC Mux 1.6 Gbps and CSC Mux 3.2 Gbps.

CSC Mux 1.6 Gbps: You can use all the VM sizes shown below. Please, note that the ones marked with (*) are not capable of handling 1.6 Gbps
CSC Mux 3.2 Gbps: You can use the VM sizes marked with Yellow. Please, note that the ones marked with (**) are not capable of handling 3.2 Gbps.

12.1 Dv2-series & DSv2-series

URL: https://docs.microsoft.com/en-us/azure/virtual-machines/dv2-dsv2-series

VM Generation Support: Generation 1 and 2
Accelerated Networking: Supported (Requires a minimum of 2 vCPU)

Name	vCPU	Memory	Bandwith (Mbps)
Standard_D2_v2	2	7	1500 (*)
Standard_D3_v2	4	14	3000 (**)
Standard_D4_v2	8	28	6000
Standard_DS2_v2	2	7	1500 (*)
Standard_DS3_v2	4	14	3000 (**)
Standard_DS4_v2	8	28	6000

12.2 Dv3 and Dsv3-series

URL: https://docs.microsoft.com/en-us/azure/virtual-machines/dv3-dsv3-series

VM Generation Support: Generation 1
Accelerated Networking: Supported (Requires a minimum of 4 vCPU)

Name	vCPU	Memory	Bandwith (Mbps)
Standard_D4_v3	4	16	2000
Standard_D8_v3	8	32	4000
Standard_D4s_v3	4	16	2000
Standard_D8s_v3	8	32	4000

12.3 Dav4 and Dasv4-series

URL: https://docs.microsoft.com/en-us/azure/virtual-machines/dav4-dasv4-series

VM Generation Support: Generation 1
Accelerated Networking: Supported (Requires a minimum of 4 vCPU)

Name	vCPU	Memory	Bandwith (Mbps)
Standard_D4a_v4	4	16	1600
Standard_D8a_v4	8	32	3200
Standard_D4as_v4	4	16	1600
Standard_D8as_v4	8	32	3200

12.4 Ddv4 and Ddsv4-series

URL: https://docs.microsoft.com/en-us/azure/virtual-machines/ddv4-ddsv4-series

VM Generation Support: Generation 1 and 2
Accelerated Networking: Supported (Requires a minimum of 4 vCPU)

Name	vCPU	Memory	Bandwith (Mbps)
Standard_D4d_v4	4	16	2000
Standard_D8d_v4	8	32	4000
Standard_D4ds_v4	4	16	2000
Standard_D8ds_v4	8	32	4000

12.5 Dv4 and Dsv4-series

URL: https://docs.microsoft.com/en-us/azure/virtual-machines/dv4-dsv4-series

VM Generation Support: Generation 1 and 2
Accelerated Networking: Supported (Requires a minimum of 4 vCPU)

Name	vCPU	Memory	Bandwith (Mbps)
Standard_D4_v4	4	16	2000
Standard_D8_v4	8	32	4000
Standard_D4s_v4	4	16	2000
Standard_D8s_v4	8	32	4000