Maidenhead Bridge

Cloud Security Connector for AWS

Enabling Zscaler (ZIA) for AWS customers

Administrator Guide

CSC Version 2.8

April 2020

Table of Contents

1 Introduction

The Cloud Security Connector (CSC) for AWS is an EC2 instance that allows to connect internal AWS resources to Zscaler Cloud Security Services.

The CSC for AWS comes with all configuration required. After launching the CSC from the AWS Market using the CloudFormation template provided, your only task is to put the GRE tunnels IPs.

Simple to install and not further management required.

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

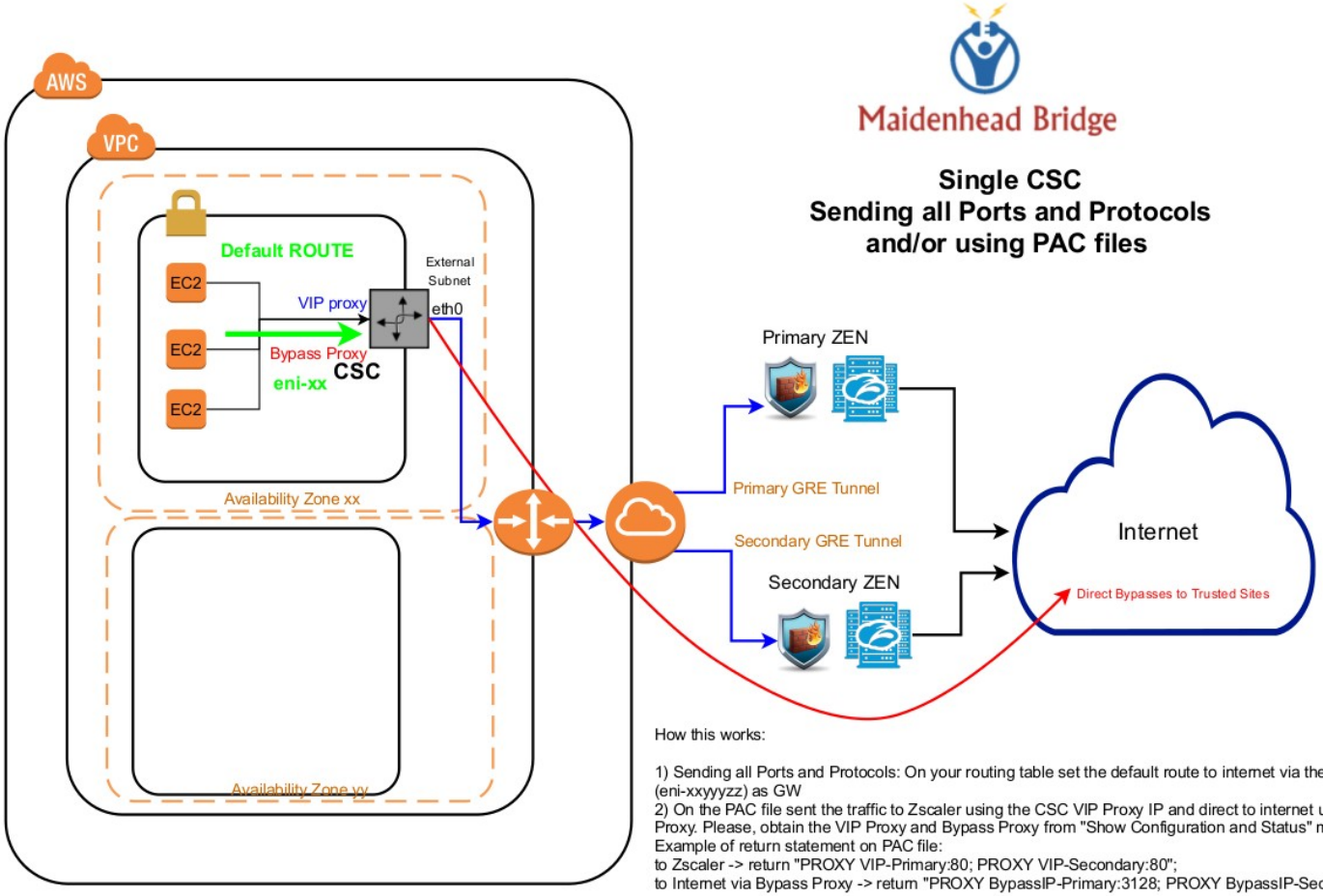
In addition to this, the CSC provides and easy way to manage direct bypasses to trusted sites.

2 Key benefits of the Cloud Security for AWS

- Enables to connect any AWS internal resources to Zscaler Cloud Security Services.
- Automated deployment using CloudFormation template.
- Easy Configuration: Just insert your GRE tunnel IPs
- Full tunnel redundancy.
- All parametrization required for AWS and Zscaler is already configured with the optimal values according Zscaler Best practices.
- All Zscaler functionalities can be used: Firewall and Web Security.
- Full visibility of internal IPs.
- Easy way to do Bypasses to trusted sites.
- No operational burden for Administrators.
- It runs on a cheap AWS instance: t2, t3a and t3 instances.
- Automatic default route selection on multiple Route Tables

3 The CSC on the AWS architecture

3.1 Single CSC – Using Cloud FW and/or PAC files (See Appendix A for details)

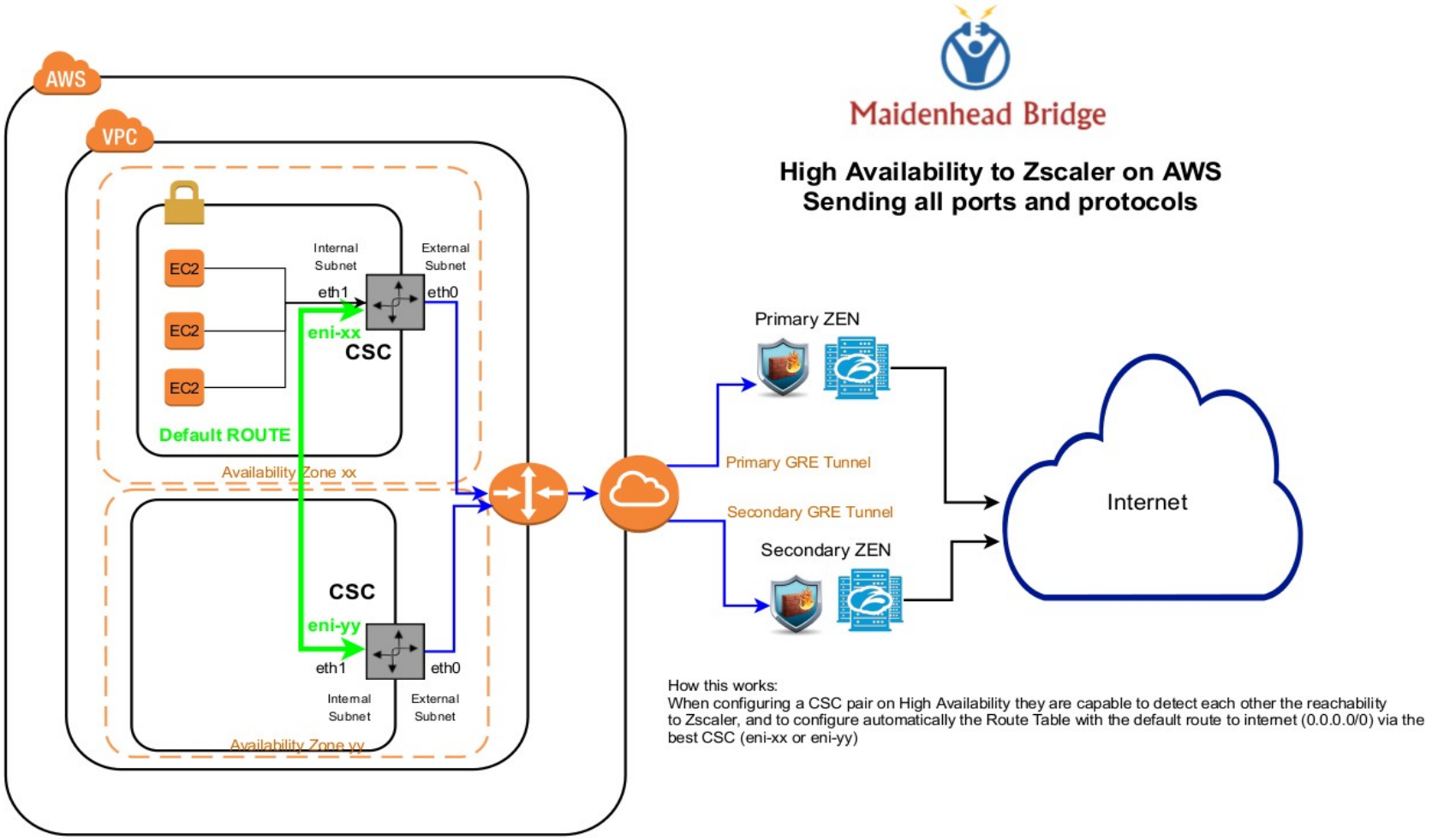


How this works:

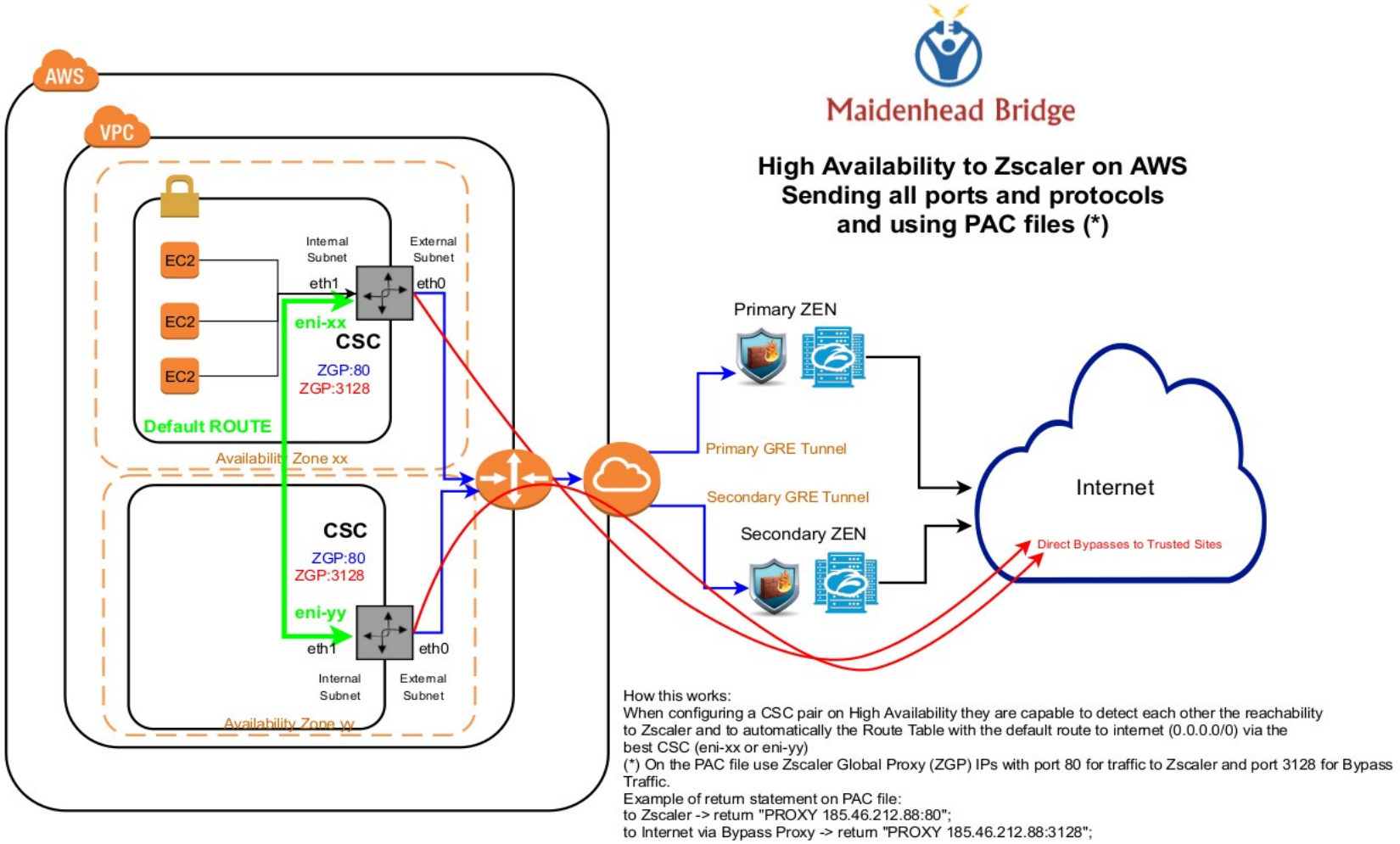
1) Sending all Ports and Protocols: On your routing table set the default route to internet via the CSC Interface-id (eni-xxyyyzz) as GW
2) On the PAC file sent the traffic to Zscaler using the CSC VIP Proxy IP and direct to internet using the Bypass Proxy. Please, obtain the VIP Proxy and Bypass Proxy from "Show Configuration and Status" menu of each CSC.
Example of return statement on PAC file:
to Zscaler -> return "PROXY VIP-Primary:80; PROXY VIP-Secondary:80";
to Internet via Bypass Proxy -> return "PROXY BypassIP-Primary:3128; PROXY BypassIP-Secondary:3128 ";

NOTE: You can use either option 1) or 2) or both at the same time.

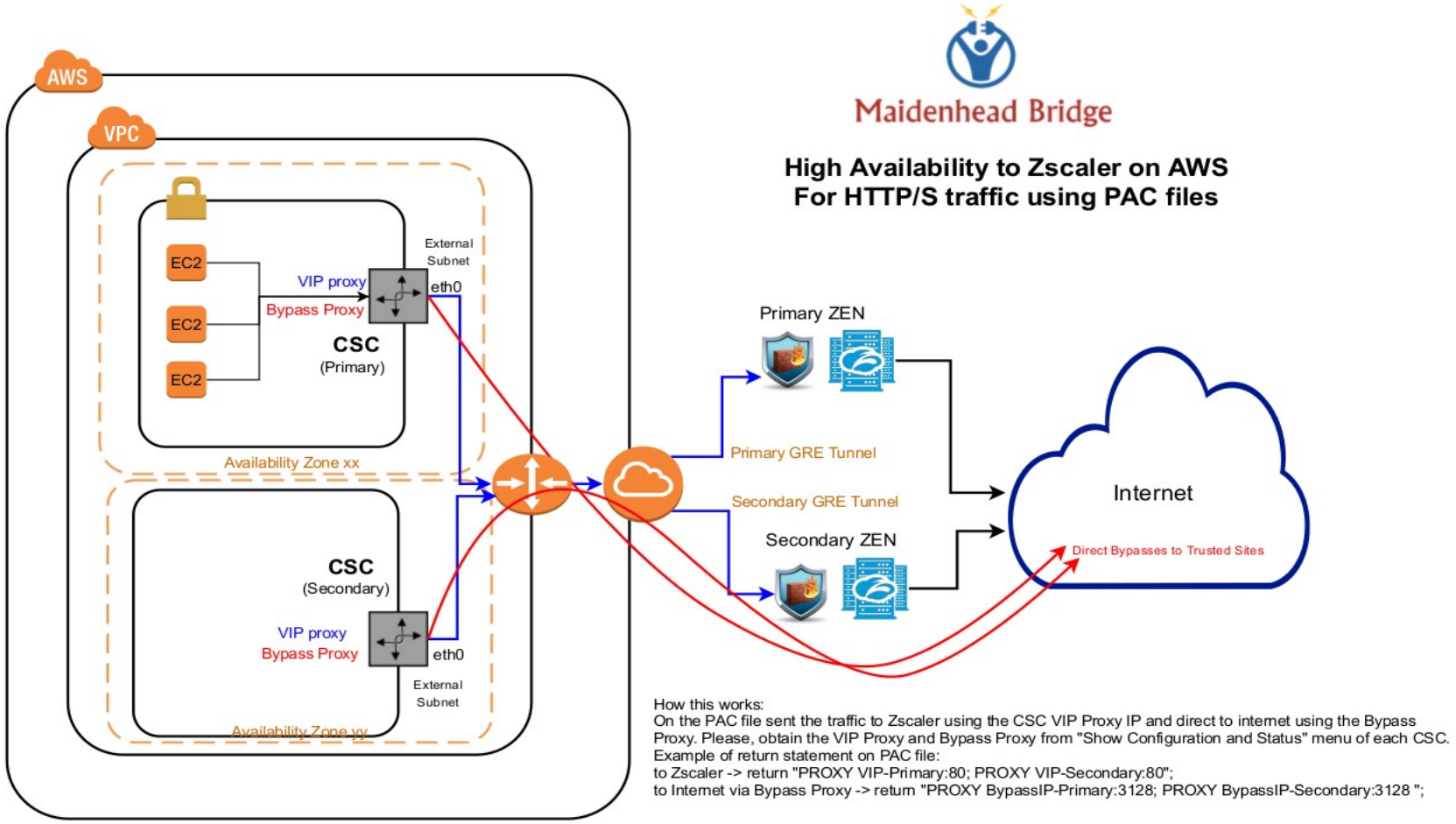
3.2 Redundant CSC – Using Cloud FW (See Appendix A for details)



3.3 Redundant CSC – Using Cloud FW and PAC files (See Appendix A for details)



3.4 Redundant CSC – For Web traffic using PAC files (See Appendix A for details)



4 Deploy the Cloud Security Connector

4.1 Prerequisites

Before to launch the CSC you need to have this elements ready:

1. **SSH Key.** (you can use any ssh key already in use or to create one specific for the CSC)
2. **VPC ID**
3. **External Subnet:** The External Subnet must be on the same VPC and Availability Zone than the Internal Subnet.
4. **Internal Subnet:** The Internal Subnet must be on the same VPC and Availability Zone than the External Subnet.

4.1.1 Prerequisites EXAMPLE:

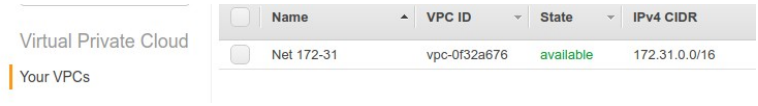
Following an EXAMPLE of prerequisites and how to obtain it.

a) Go to your EC2 Dashboard to get the Key Pairs or to create new ones.

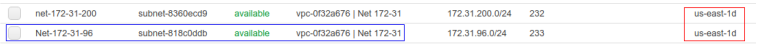
1 – SSH Keys: us-east-key

b) Go to your VPC Dashboard, to obtain VPC ID, and Subnets.

2 – VPC ID: vpc-of32a676



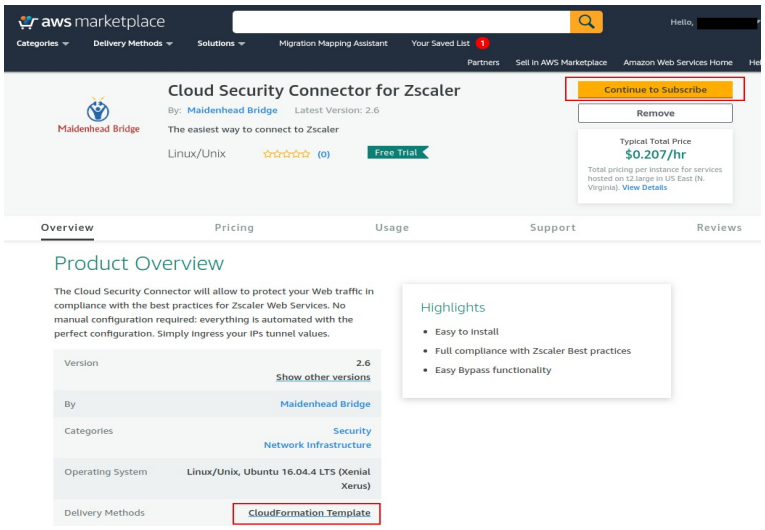
3 – External Subnet: subnet-818c0ddb (Note: Availability Zone us-east-1d and VPC ID vpc-of32a676)



4- Internal Subnet: subnet-8360ecd9 (Note: Availability Zone us-east-1d and VPC ID vpc-of32a676)

4.2 Launching the CSC from AWS Market

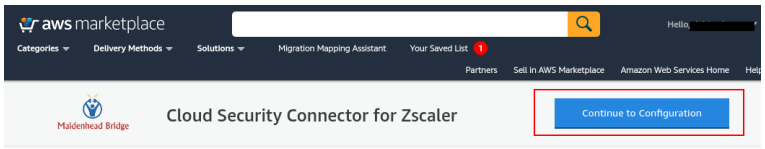
1. Go to the Cloud Security Connector for Zscaler product page at the AWS Market:



Please, note at the bottom that the Fulfilment Method is CloudFormation Template.

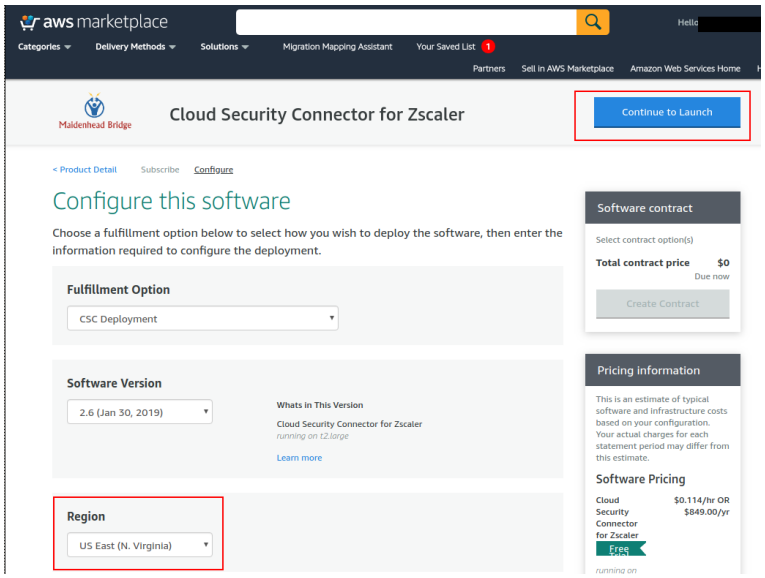
→ Click ***"Continue to Subscribe"***

2. You will be asked to accept the EULA (at the first time), then Continue..



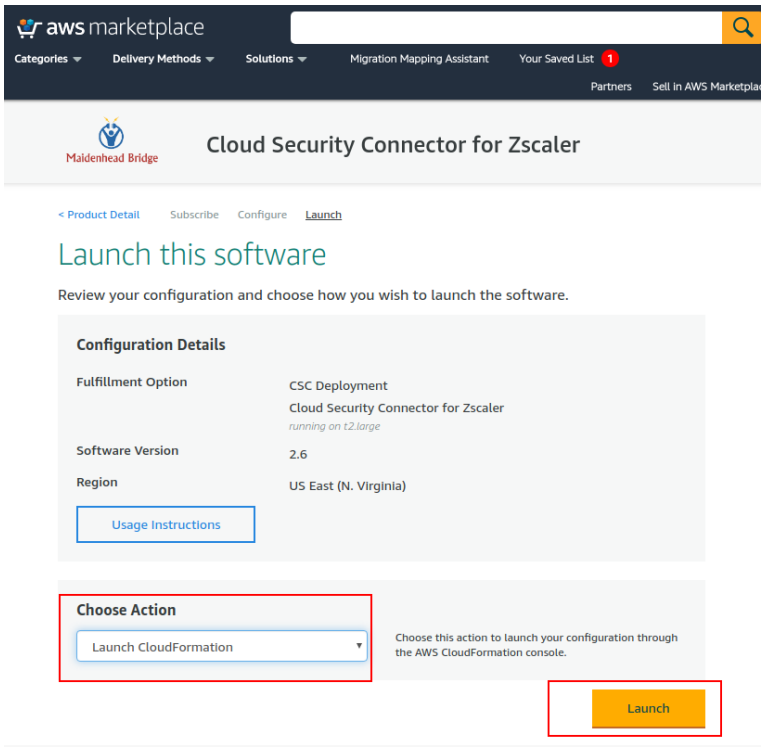
→ Click ***"Continue to Configuration"***

3. Select "Region"



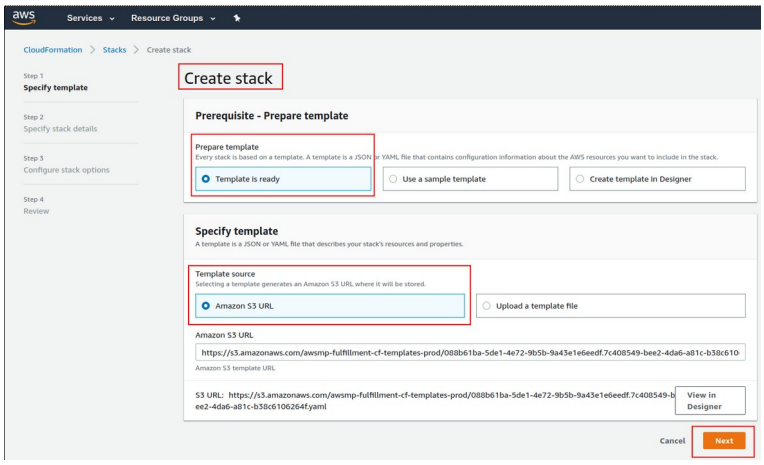
→ Click ***"Continue to Launch"***

4. Choose Action: "Launch CloudFormation"



→ Click ***"Launch"***

5. At this point, the "Create Stack" screen will appear.



→ Click ***"Next"***

6. Specify Details. Please insert here your values:

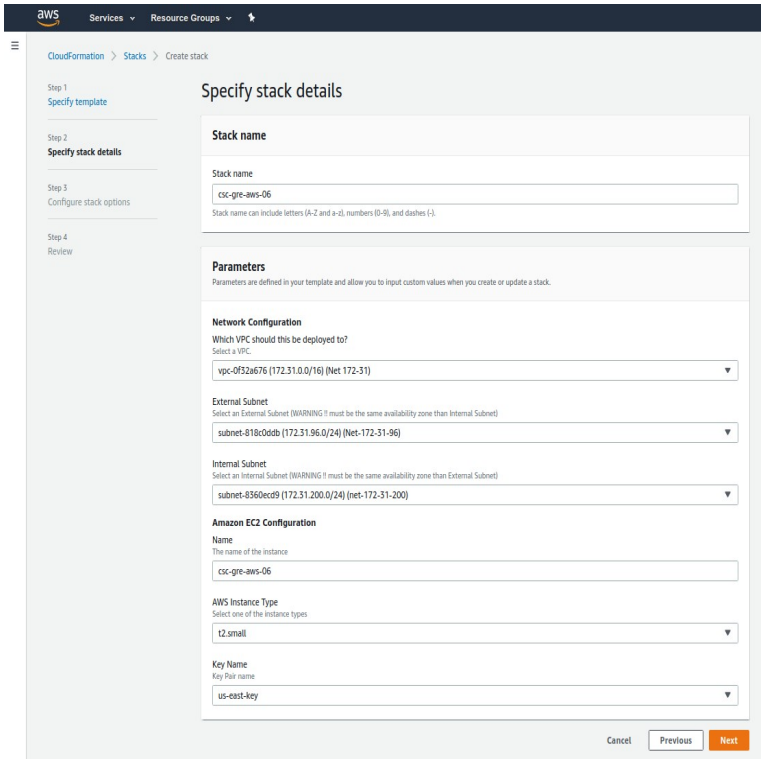
- Stack Name
- VPC
- External Subnet
- Internal Subnet
- Name [of the instance] *(we recommend to use the same name for the stack and the instance for easy visualization)*
- AWS Instance Type: t2.small, t2.medium, t2.large, t3a.small, t3a.medium, t3a.large, t3.small, t3.medium, t3.large, (*)
- Key Name

(*) Important note about CSC and AWS Instance Type: *AWS has not committed bandwidth (Mbps) on Burst instances like t2, t3a or t3. The CSC is very light on resources. This type of instances are good enough in terms of CPU / RAM and Disk requirements. In our tests, we saw the following results in terms of bandwidth performance of t2,t3a,t3 instances and the CSCs:*

- *t(2 or 3a or 3).small: 200 Mbps to 400 Mbps.*
- *t(2 or 3a or 3).medium: 350 Mbps to 600 Mbps.*
- *t(2 or 3a or 3).large: around 850 Mbps.*

This values correspond to the N. Virginia (us-east-1) region. This values can differ region by region. ***Use this as reference only.***
We recommend to use t3a instances. At the moment of writing this document t3a instances performs a little bit better and are cheaper than t2 or t3.

Here the Screenshoot using the values of point 4.1.1 Prerequisites EXAMPLE: (please, use here your own values)

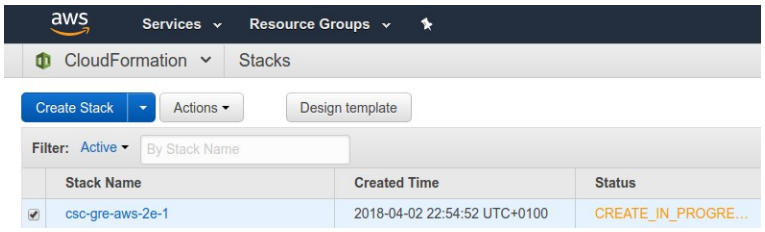


→ Click ***"Next"***

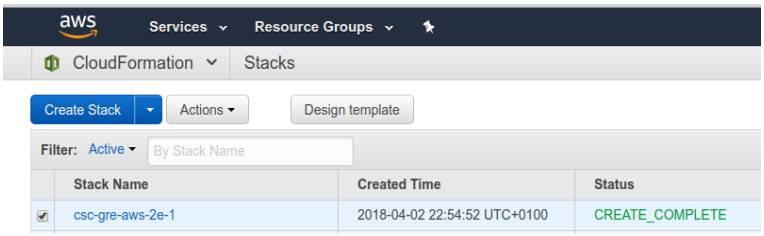
→ "Options Section": Click ***"Next"***

→ "Review": Click ***"Create Stack"***

The Stack will show "status" CREATE_IN_PROGRESS



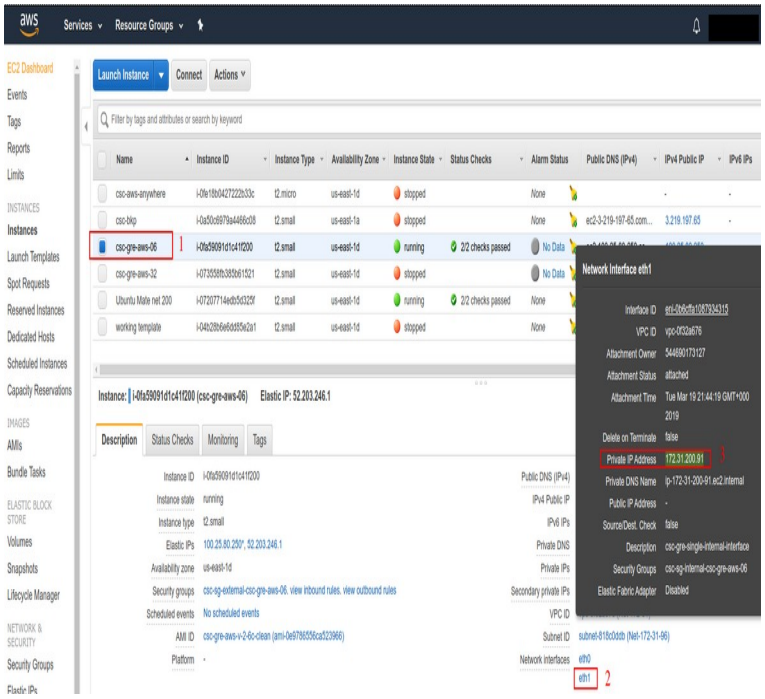
And after a while:



Done! Your CSC is deployed.

5 Accessing for first time to your CSC

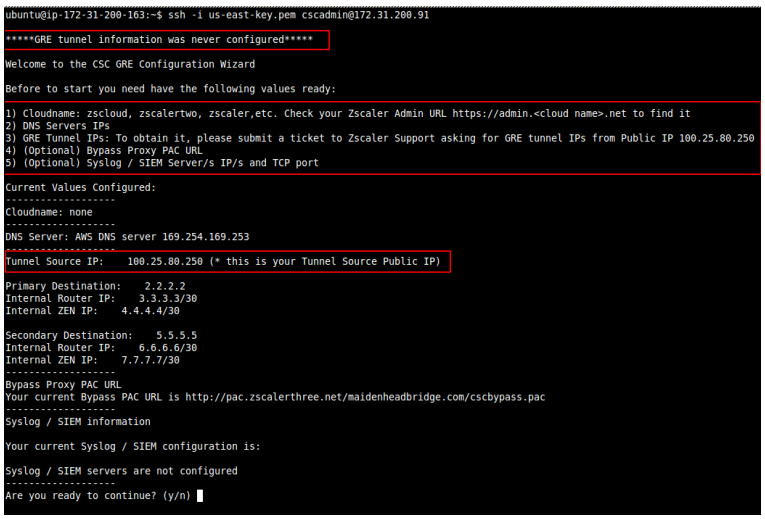
1. Go to your EC2 Dashboard → Instances and select the CSC created.



2. On the bottom screen, click “eth1” and take a look of the Private IP address of the eth1. In this example is: 172.31.200.91
3. From a machine inside the VPC, ssh the CSC using the Key, like:

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

In our example, the value is $ ssh -i us-east-key.pem 172.31.200.91



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

6 Initial Wizard Configuration

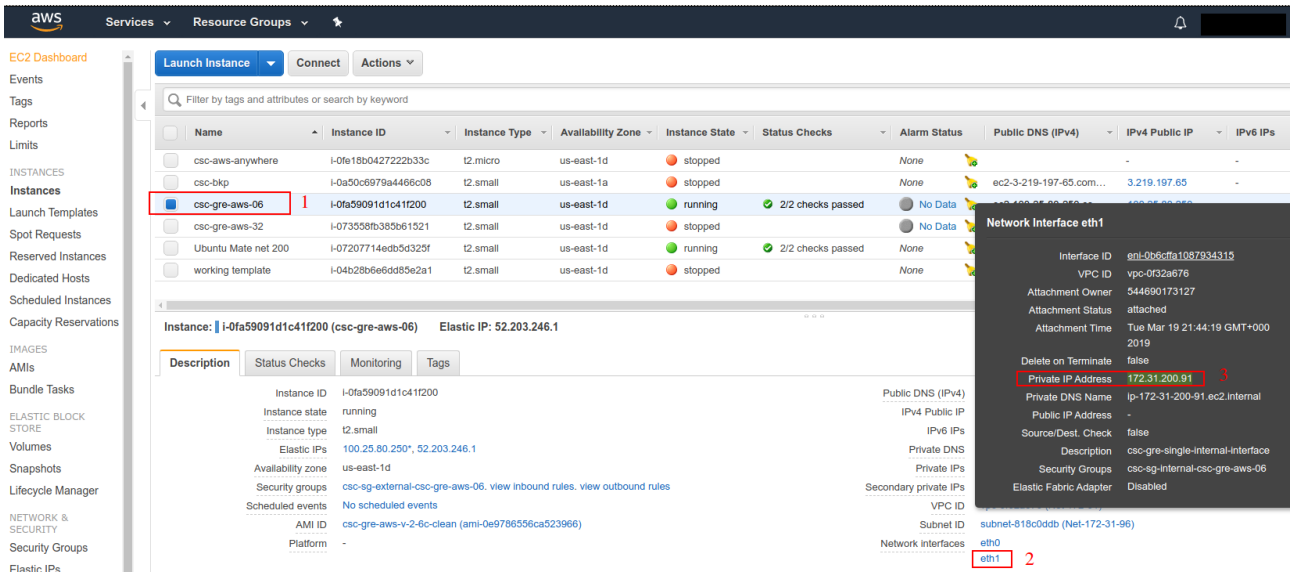
Please, follow this instructions to run the initial configuration of the CSC GRE for AWS:

6.1 Short Version

1. Submit a ticket to Zscaler Support asking for the GRE credentials from: “Tunnel Source IP” showed in the console. Tell the Zscaler Team which is your AWS Datacenter or choose your ZEN nodes using https://ips.<zscaler cloud name>.net/cenr
2. Wait for the response email from Zscaler Support that contains the details of the GRE tunnels IPs.
3. Go to the Zscaler Console and create the “Location”
4. Run the Wizard. Insert the values. Confirm and reboot.
5. Done!

6.2 Long Version (with Example)

In this Example, after the CSC was launched, the values of my CSC are:



The internal IP (eth1) is 172.31.200.91. Doing and SSH from a machine on subnet 172.31.200.0/24 to the CSC, the initial wizard appear.

In this example:

Key Name: us-east-key.pem

Username: cscadmin (use always "cscadmin")

CSC IP: 172.31.200.91

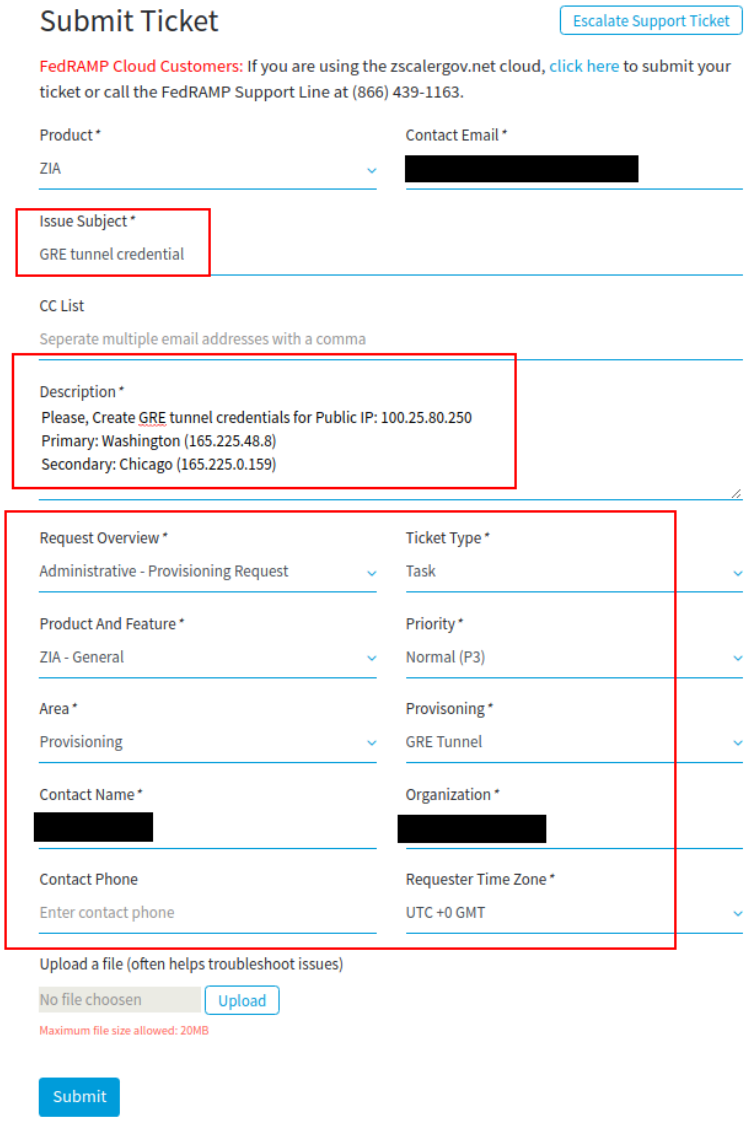
$ ssh -i *us-east-key.pem cscadmin@172.31.200.91*

```
ubuntu@ip-172-31-200-163:~$ ssh -i us-east-key.pem cscadmin@172.31.200.91

*****GRE tunnel information was never configured*****

Welcome to the CSC GRE Configuration Wizard

Before to start you need have the following values ready:

1) Cloudname: zscloud, zscalertwo, zscaler,etc. Check your Zscaler Admin URL https://admin.<cloud name>.net to find it
2) DNS Servers IPs
3) GRE Tunnel IPs: To obtain it, please submit a ticket to Zscaler Support asking for GRE tunnel IPs from Public IP 100.25.80.250
4) (Optional) Bypass Proxy PAC URL
5) (Optional) Syslog / SIEM Server/s IP/s and TCP port

Current Values Configured:
-------------------
Cloudname: none
-------------------
DNS Server: AWS DNS server 169.254.169.253
-------------------
Tunnel Source IP:    100.25.80.250 (* this is your Tunnel Source Public IP)

Primary Destination:    2.2.2.2
Internal Router IP:    3.3.3.3/30
Internal ZEN IP:    4.4.4.4/30

Secondary Destination:    5.5.5.5
Internal Router IP:    6.6.6.6/30
Internal ZEN IP:    7.7.7.7/30
-------------------
Bypass Proxy PAC URL
Your current Bypass PAC URL is http://pac.zscalerthree.net/maidenheadbridge.com/cscbypass.pac
-------------------
Syslog / SIEM information

Your current Syslog / SIEM configuration is:

Syslog / SIEM servers are not configured
-------------------
Are you ready to continue? (y/n)
```

As you can see in this example, the Tunnel Source Public IP is: 100.25.80.250

6.2.1 Submit a ticket to Zscaler Support

From your Zscaler console, Submit a ticket to Zscaler Support asking for the GRE tunnels IPs from the Public IP 100.25.80.250 and Specify your preferred ZEN nodes from https://ips.<cloud name>.net/cenr



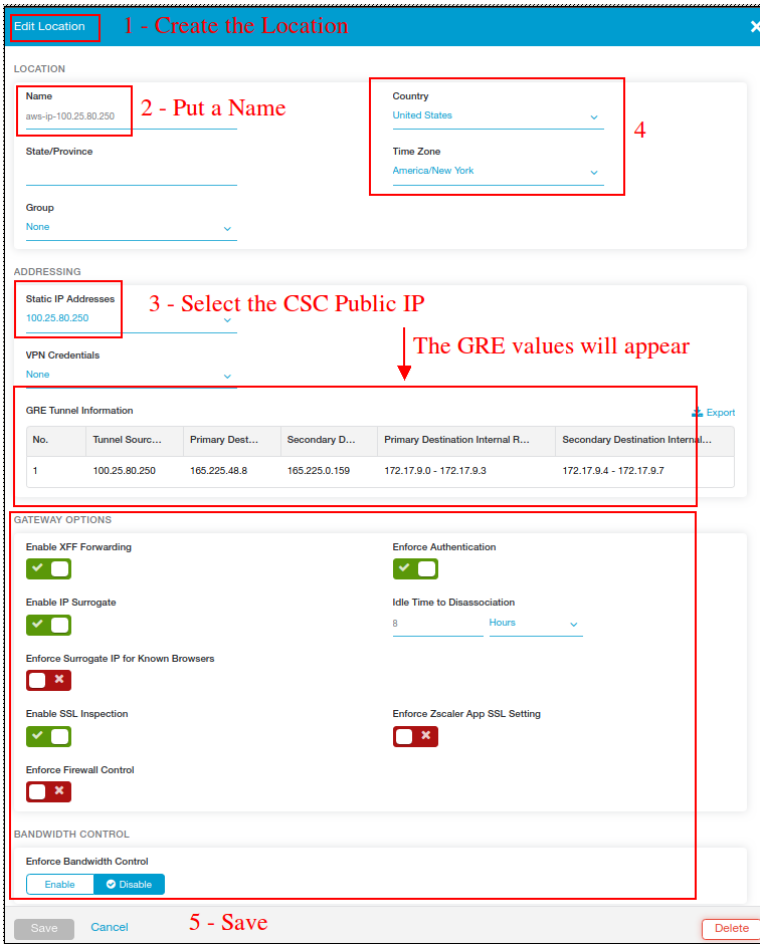
6.2.2 Wait for the email from Zscaler Support

After a while, you will receive an email from Zscaler Support containing the GRE information.

```
--------------------------------------------------------------------------
Tunnel Source IP:    100.25.80.250
Internal Range:  172.17.9.0-172.17.9.7

Primary Destination:    165.225.48.8
Internal Router IP:    172.17.9.1/30
Internal ZEN IP:    172.17.9.2/30

Secondary Destination:    165.225.0.159
Internal Router IP:    172.17.9.5/30
Internal ZEN IP:    172.17.9.6/30
--------------------------------------------------------------------------
```

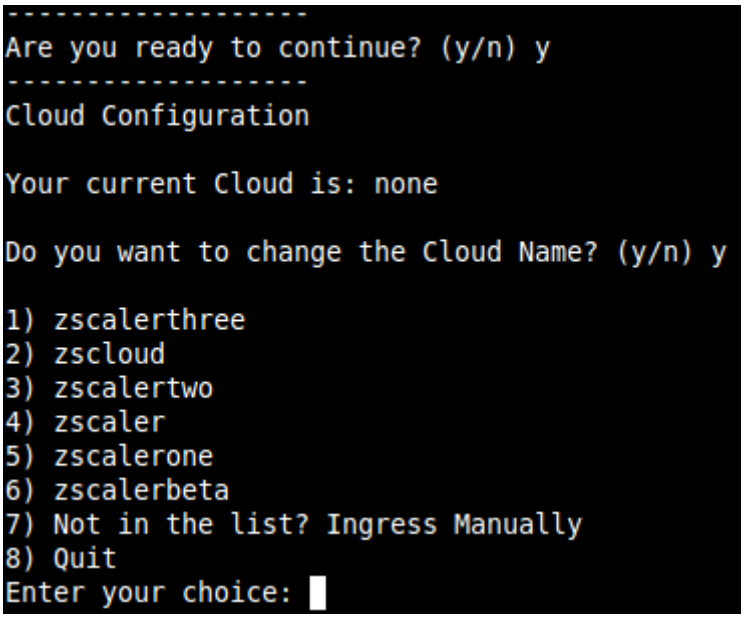
6.2.3 Create the Location on the Zscaler Console

After the email with the GRE tunnel information is received, you can create the Location on the Zscaler Console. Here is the Location of this example:

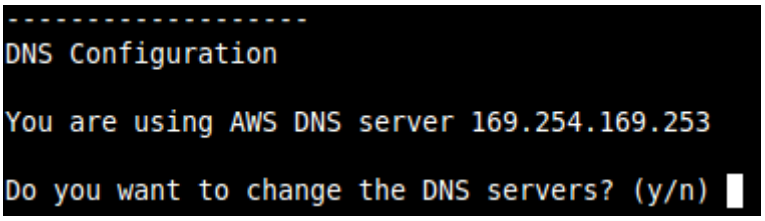


6.2.4 Run the Wizard

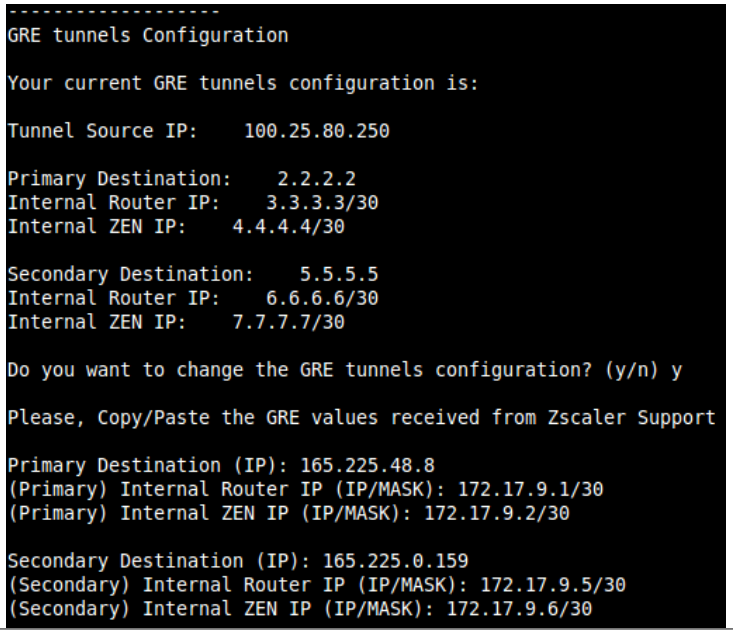
1. Select your cloud



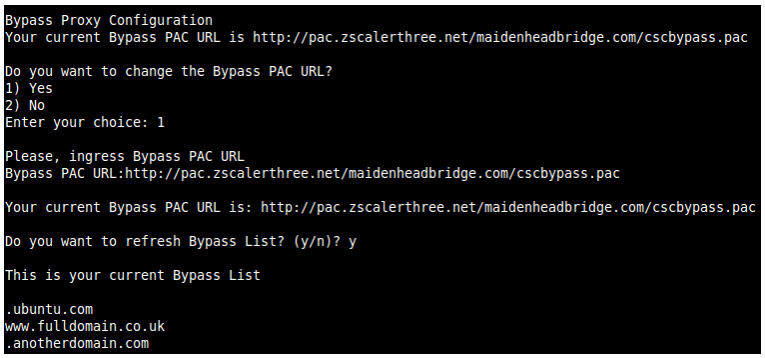
2. Enter your DNS Servers or use AWS DNS server.



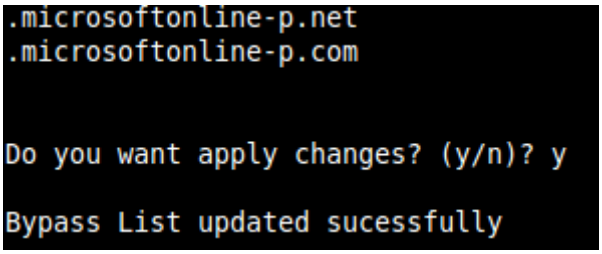
3. Enter the GRE tunnel values received.



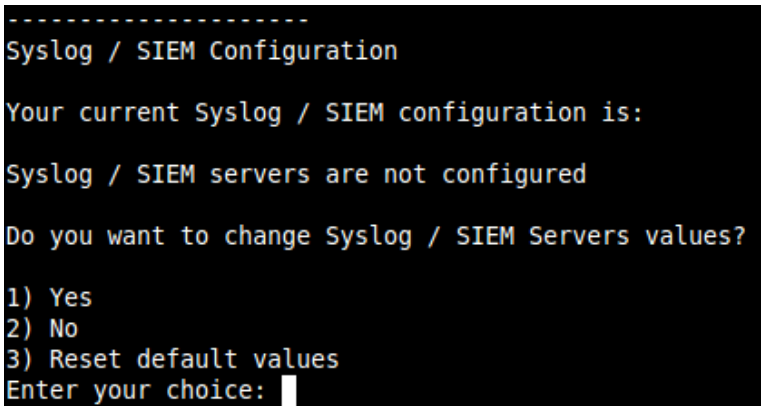
4. (Optional) Enter your Bypass PAC URL. When using the Bypass Proxy functionality, you can insert here the Bypass Proxy URL and to refresh the Bypass List.



(cont.)



5. (Optional) Enter your SIEM server IP and Logs.



6. Finally, check and confirm the values:

```
Please confirm this values:
------------------
Cloudname:  zscalerthree
------------------
DNS Server: AWS DNS server 169.254.169.253
------------------
GRE tunnels IP values:

Tunnel Source IP (IP):  100.25.80.250

Primary Destination:  165.225.48.8
(Primary) Internal Router IP (IP/MASK):  172.17.9.1/30
(Primary) Internal ZEN IP (IP/MASK):  172.17.9.2/30

Secondary Destination:  165.225.0.159
(Secondary) Internal Router IP (IP/MASK):  172.17.9.5/30
(Secondary) Internal ZEN IP (IP/MASK):  172.17.9.6/30
------------------
Bypass Proxy PAC URL
Your current Bypass PAC URL is http://pac.zscalerthree.net/maidenheadbridge.com/cscbypass.pac
------------------
No Syslog / SIEM servers are configured
------------------
Do you want to implement this values? (y/n)? (The CSC will reboot)
```

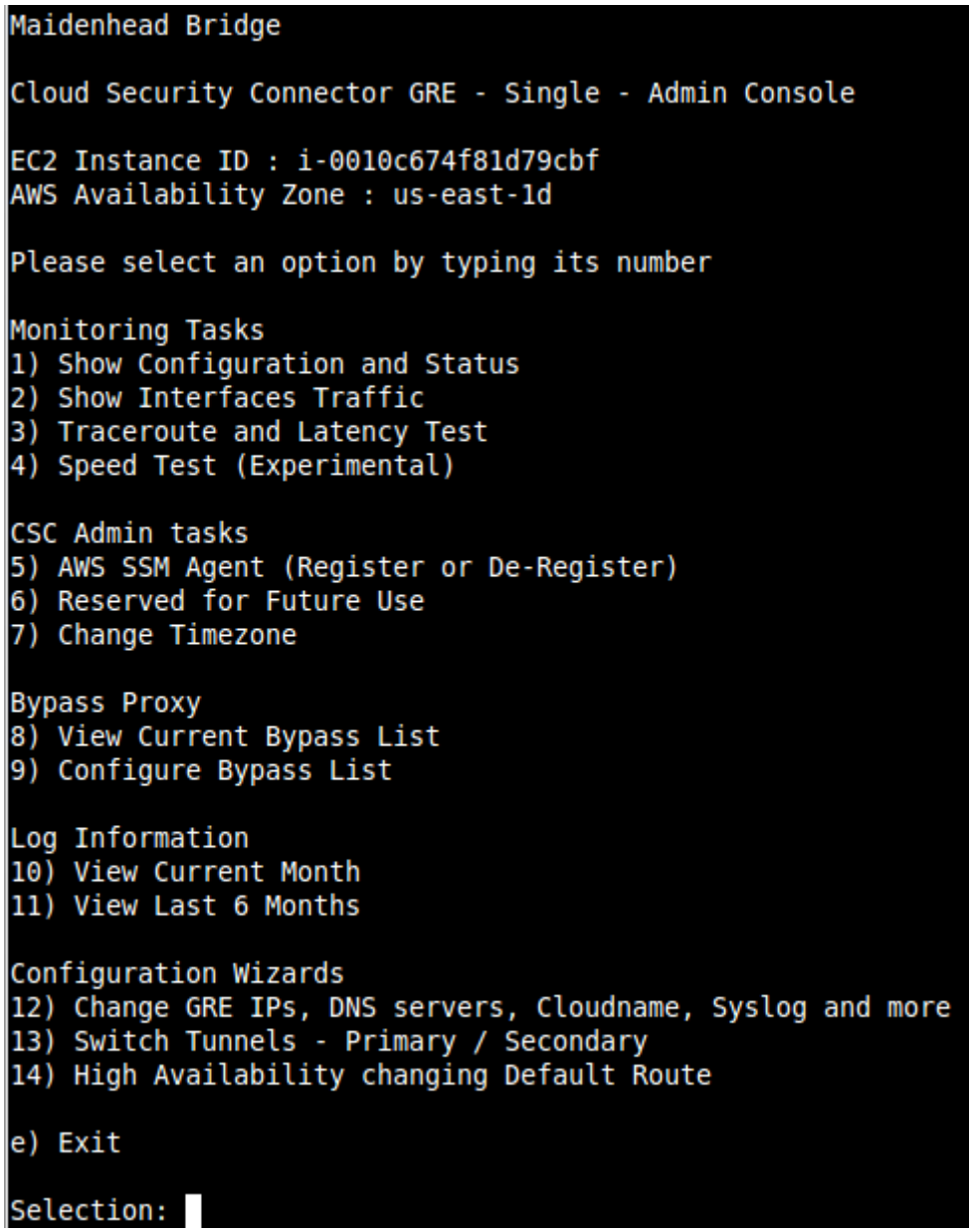
Done! After the reboot, the CSC is ready for Production.

7 The Cloud Security Connector Admin Console:

The CSC SSH Console was created to simplify admin tasks showing what is important to administrators for operation and troubleshooting. In addition to this, all monitoring tasks are able to be done via AWS Console. Simply register the CSC instance on AWS as managed instance and you are ready to manage the CSC using all AWS System Manager tools.

When accessing the console via SSH, you will receive the Admin Console. For example:

```
ssh -i "us-east-key.pem" cscadmin@172.31.200.29
```



The Main Section are:

- Monitoring Tasks: To check statuses, real time traffic, speed, etc.
- CSC Admin Tasks: To register the CSC for AWS management, change password and timezone.
- Bypass Proxy: To manage the Bypass PAC URL or to enter manually the Bypasses.
- Configuration Wizard: To run the initial wizard again, to switch tunnels and configuring HA.

7.1 Monitoring Tasks

7.1.1 Show Configuration and Status

```
GENERAL INFORMATION
Availability Zone: us-east-1d
EC2 Instance id: i-0010c674f81d79cbf | Instance Type: t3a.small | ami-id: ami-0a5a0ceb1b10a090d
External Interface (eth0) Subnet-id: subnet-818c0ddb | Interface-id: eni-088be11799a314217 | Security-Group-id: sg-01aa6d99154e01e8b
Internal Interface (eth1) Subnet-id: subnet-8360ecd9 | Interface-id: eni-033a173aa6e006da9 | Security-Group-id: sg-03343083dc6779f64
CSC date: Tue 25 Feb 03:34:59 EST 2020
Soft version : 2.7

INTERFACES INFORMATION
External: Tunnel IP (eth0): 172.31.96.220/24 | Bypass Proxy Egress IP: 172.31.96.80 | Network Gateway: 172.31.96.1 is Alive
Internal: CSC GW IP (eth1): 172.31.200.29/24 | Network Gateway: 172.31.200.1 is Alive

TRAFFIC REDIRECTION Options
To Zscaler: VIP Proxy: 172.31.200.71:80 (or :9400) | Route all traffic via CSC GW IP | Zscaler Global Proxies (port 80/9400) via CSC GW IP
Direct to Internet: Bypass Proxy: 172.31.200.214:3128 | Zscaler Global Proxies (port 3128) via CSC GW IP

ELASTIC (PUBLIC) IPs INFORMATION
GRE tunnels Public IP: 100.25.80.250
Bypass Proxy Public IP: 3.225.208.27

DNS INFORMATION
Using AWS IP: 169.254.169.253

ZSCALER INFORMATION
Zscaler Cloud:  zscalerthree
GRE tunnels egress Public IP: 100.25.80.250
Primary Tunnel:
               ZEN Public IP: 165.225.48.8
               Tunnel IPs (local/zen): 172.17.9.1 / 172.17.9.2
Secondary Tunnel:
               ZEN Public IP: 165.225.0.159
               Tunnel IPs (local/zen): 172.17.9.5 / 172.17.9.6

TUNNEL STATUS
Primary Tunnel (reachability):
                           Layer 7 Keepalive is: Alive
                           GRE ZEN Tunnel IP is: Alive
Secondary Tunnel (reachability):
                           Layer 7 Keepalive is: Alive
                           GRE ZEN Tunnel IP is: Alive

Tunnel Status: Primary tunnel is active since: Mon 24 Feb 14:11:46 EST 2020

HTTP://IP.ZSCALER.COM PAGE STATUS
You are accessing the Internet via Zscaler Cloud: Washington DC in the zscalerthree.net cloud.
Your Gateway IP Address is 100.25.80.250

BYPASS PROXY - EGRESS INTERFACE STATUS
Bypass Proxy Egress Interface 172.31.96.80 can reach test page (http://pac.zscalerthree.net)

AWS SSM AGENT
AWS SSM Agent is active (running) since Mon 2020-02-24 14:11:02 EST; 13h ago
Registration values: {"ManagedInstanceID":"mi-0dc45c84413312361","Region":"eu-west-1"}

SYSLOG/SIEM Servers Information
Primary Syslog IP: 172.31.200.163
Secondary Syslog IP: Not configured
Syslog TCP port: 514

HIGH AVAILABILITY Information
The HA service is:  active (running) since Mon 2020-02-24 14:11:03 EST; 13h ago
IAM role in use: arn:aws:iam::544690173127:instance-profile/csc-ha-aws-role
The Default Route to Internet is using this Gateway (Target): eni-033a173aa6e006da9 (this CSC)
Current values configured are:
Routing Table ID= rtb-d090c8a8
Instance ID of other CSC in the pair= i-05e327fb84e9bbd91
SNS message ARN= arn:aws:sns:us-east-1:544690173127:AWS-Zscaler-Notification

Press ENTER to continue
```

7.1.1.1 GENERAL INFORMATION

This section contains general information about the instance:

```
GENERAL INFORMATION
Availability Zone: us-east-1d
EC2 Instance id: i-0fa59091d1c41f200 | Instance Type: t2.small | ami-id: ami-0e9786556ca523966
External Interface (eth0) Subnet-id: subnet-818c0ddb | Interface-id: eni-0ec6b2b53d990c2e5 | Security-Group-id: sg-0d2b80c6632946cd9
Internal Interface (eth1) Subnet-id: subnet-8360ecd9 | Interface-id: eni-0b6cffa1087934315 | Security-Group-id: sg-033efd40e740dd848
CSC date: Wed Oct 16 10:49:47 GMT 2019
Soft version : 2.6
```

Important: Please, note the “Interface-id:” value. You will need it if routing traffic via the CSC.

7.1.1.2 INTERFACES INFORMATION

This section contains the interfaces information:

```
INTERFACES INFORMATION
External: Tunnel IP (eth0): 172.31.96.250/24 | Bypass Proxy Egress IP: 172.31.96.193 | Network Gateway: 172.31.96.1 is Alive
Internal: CSC GW IP (eth1): 172.31.200.91/24 | Network Gateway: 172.31.200.1 is Alive
```

7.1.1.3 TRAFFIC REDIRECTION Options

The section contains the information about how to redirect traffic to Zscaler.

```
TRAFFIC REDIRECTION Options
To Zscaler: VIP Proxy: 172.31.200.35:80 (or :9400) | Route all traffic via CSC GW IP | Zscaler Global Proxies (port 80/9400) via CSC GW IP
Direct to Internet: Bypass Proxy: 172.31.200.64:3128 | Zscaler Global Proxies (port 3128) via CSC GW IP
```

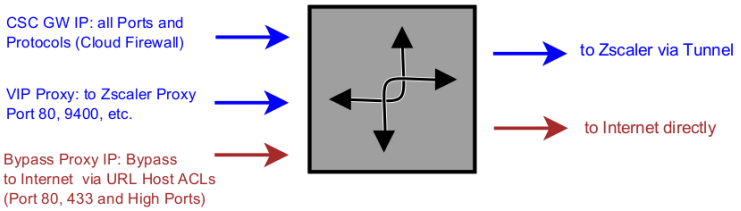
The objective of the Cloud Security Connectors of Maidenhead Bridge is to provide a simple architecture, 100% proven that works, to connect to Zscaler.

Every member of the CSC family follows the principle of “three IPs” on the internal side:

- CSC **GW IP (*)**: To be used as Default Gateway for internal devices behind the CSC redirecting all ports and protocols to Zscaler when using Cloud Firewall.
- **VIP Proxy:** This Virtual IP Proxy translates the packets directly to the Zscaler proxy. To be used when PAC files are implemented or explicit proxy.
- **Bypass Proxy IP:** The Bypass Proxy enables a simple way to do Direct Bypasses to Internet. To be used when PAC files are implemented.

***(*)** On AWS routing tables, the value to use as a GW is the “Interface-id:” (eni-xxyyzz)*

Here an illustration about this:



Important: Please, see Appendix A for detailed information about traffic redirection (with examples)

7.1.1.4 ELASTICP (PUBLIC) IPs INFORMATION

This section shows the Public IP used to initiate the tunnels to Zscaler and the Public IP used for the Bypass Proxy functionality.

In our example:

```
ELASTIC (PUBLIC) IPs INFORMATION
GRE tunnels Public IP: 100.25.80.250
Bypass Proxy Public IP: 52.203.246.1
```

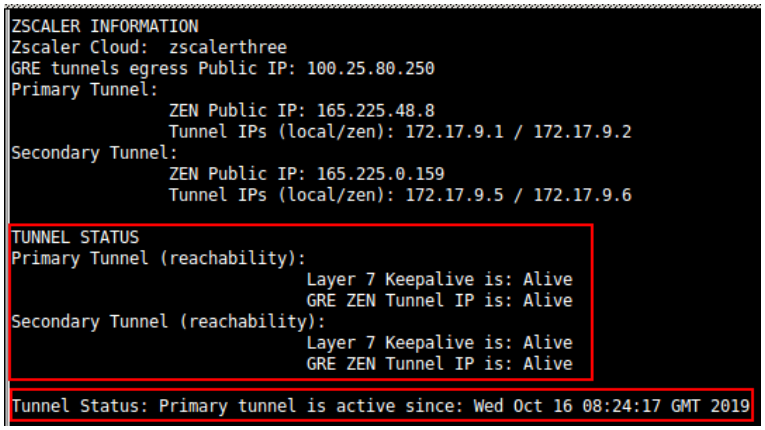
7.1.1.5 DNS INFORMATION

This section displays the DNS information. You can use the default DNS server from AWS or to setup your own DNS servers.

```
DNS INFORMATION
Using AWS IP: 169.254.169.253
```

7.1.1.6 ZSCALER INFORMATION

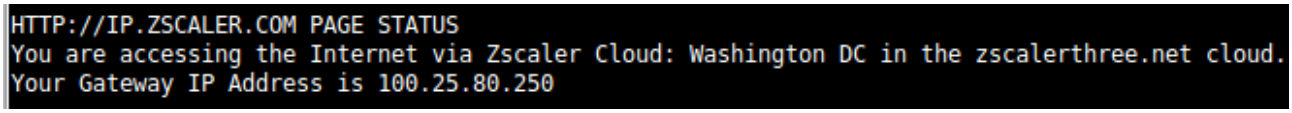
This section shows the GRE tunnel information and Tunnel Status.



Please, pay attention to the reachability of the Keepalives and Tunnels and the Tunnel Status.

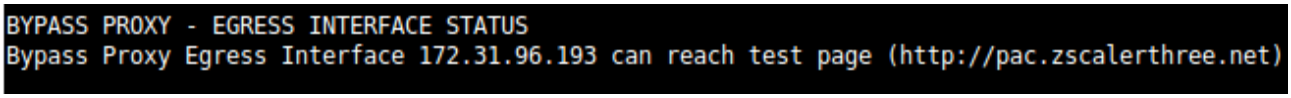
7.1.1.7 HTTP://IP.ZSCALER.COM PAGE STATUS

Zscaler recommend to check the page http://ip.zscaler.com to validate that you are using Zscaler and to see your Zscaler Node, Cloud and IP address. The CSC does this test for you.



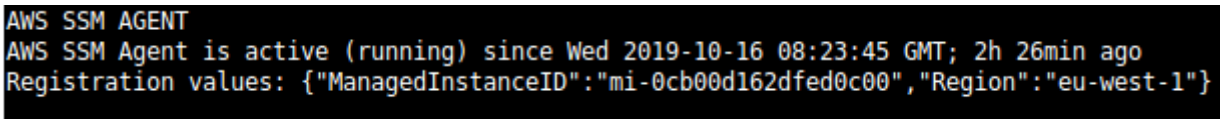
7.1.1.8 BYPASS PROXY – EGRESS INTERFACE STATUS

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



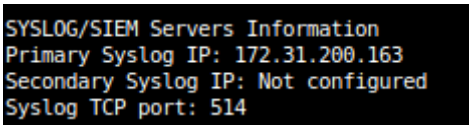
7.1.1.9 AWS SSM AGENT

This section shows the status of the AWS SSM Agent.



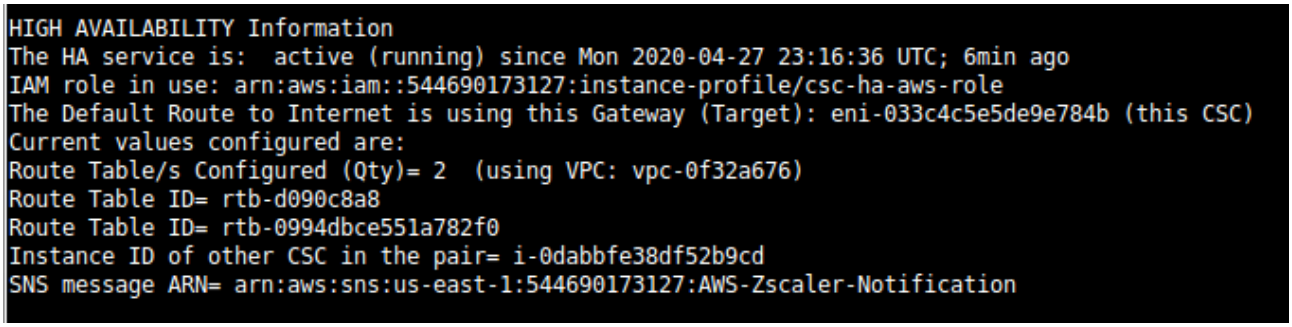
7.1.1.10 SYSLOG/SIEM Servers Information

When configured, this section will show the IP/s and TCP port of your Syslog/SIEM server.



7.1.1.11 HIGH AVAILABILITY Information

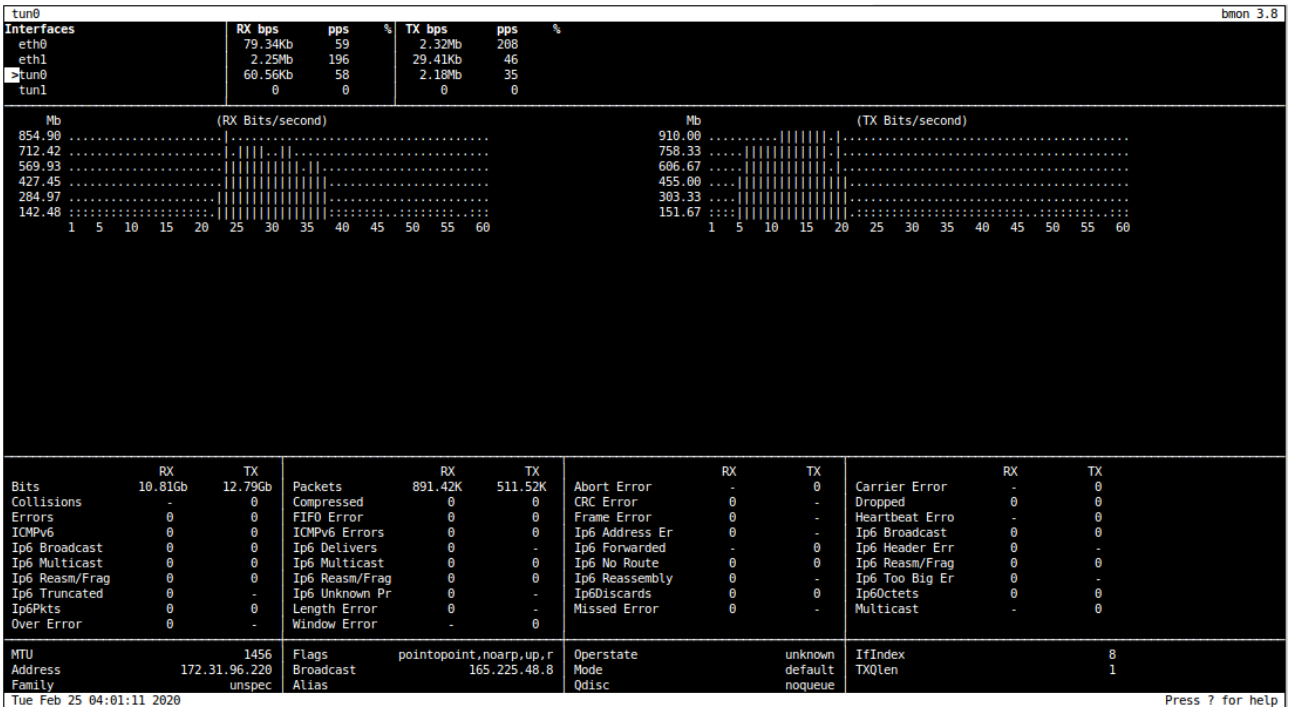
This section all the information when the CSC are configured on HA pair:



- If HA service is active.
- The IAM role in use
- The current “eni-xxyy” that is the default GW to internet for the Route Table/s
- Amount of Route Tables configured and VPC in use.
- The Route table ID/s
- Which is the Instance ID of other CSC on the HA pair.
- The SNS message used for notification.

7.1.2 Show Interfaces Traffic

You can use this section to see the traffic in real time.



7.1.3 Traceroute and Latency Test

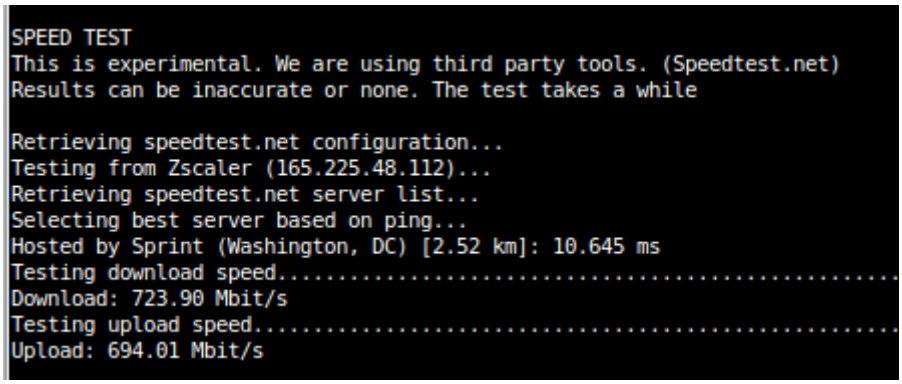
This test can validate the quality of the Internet path between you location and Zscaler. You can run it with tunnels down or up. When the tunnels are up, it does a “Reverse Path” test from your active ZEN node to your location. This is very useful to check if there is any packet loss at some point.

```
My TraceRoute (MTR) Test Report
This test does:
- MTR (TCP/80) DIRECT to the Primary ZEN and Secondary ZEN
- When the tunnel is UP, a MTR Reverse Path test from the active ZEN to your Public IP
NOTE: Max Hops is equal 30. This test can take a while

Testing Primary ZEN
Start: Tue Feb 25 03:44:09 2020
HOST: ip-172-31-96-220             Loss%   Snt   Last   Avg  Best  Wrst StDev
  1.|-- ???                        100.0    10    0.0   0.0   0.0   0.0   0.0
  2.|-- ???                        100.0    10    0.0   0.0   0.0   0.0   0.0
  3.|-- ???                        100.0    10    0.0   0.0   0.0   0.0   0.0
  4.|-- ???                        100.0    10    0.0   0.0   0.0   0.0   0.0
  5.|-- ???                        100.0    10    0.0   0.0   0.0   0.0   0.0
  6.|-- 100.65.13.17                20.0%    10    0.8   4.9   0.3  34.4  11.9
  7.|-- 52.93.28.171                 0.0%    10    1.3   1.1   0.6   1.4   0.0
  8.|-- 100.100.28.58                0.0%    10    1.3   1.2   1.0   1.4   0.0
  9.|-- 100.95.7.112                 0.0%    10    1.1   2.2   1.1   9.5   2.5
 10.|-- 100.100.30.80                0.0%    10    1.5   5.9   1.0  24.5   8.1
 11.|-- 54.239.111.247               0.0%    10    1.1   1.5   1.1   2.1   0.0
 12.|-- 52.93.114.62                 0.0%    10    1.1  10.1   1.1  36.3  12.4
 13.|-- ae14.cr1.dca2.us.zip.zayo.com  0.0%    10    1.7   5.5   1.2  32.1   9.4
 14.|-- ae27.cs1.dca2.us.eth.zayo.com  0.0%    10    1.2   2.0   1.2   3.2   0.3
 15.|-- ae15.cr1.dca2.us.zip.zayo.com  0.0%    10    3.5   4.4   3.2  13.9   3.3
 16.|-- ae27.cs1.dca2.us.eth.zayo.com  0.0%    10    3.2   3.3   2.3   4.0   0.0
 17.|-- ae27.cs1.dca2.us.eth.zayo.com  0.0%    10    3.4  18.9   2.9 106.0  34.8
 18.|-- 64.125.41.157                 0.0%    10  106.0  28.8   2.5 106.1  44.0
 19.|-- 165.225.48.8                  0.0%    10  106.2  99.9   2.5 200.8  49.6

Testing Secondary ZEN
Start: Tue Feb 25 03:44:25 2020
HOST: ip-172-31-96-220                Loss%   Snt   Last   Avg  Best  Wrst StDev
  1.|-- ???                           100.0    10    0.0   0.0   0.0   0.0   0.0
  2.|-- ???                           100.0    10    0.0   0.0   0.0   0.0   0.0
  3.|-- ???                           100.0    10    0.0   0.0   0.0   0.0   0.0
  4.|-- ???                           100.0    10    0.0   0.0   0.0   0.0   0.0
  5.|-- ???                           100.0    10    0.0   0.0   0.0   0.0   0.0
  6.|-- 100.65.14.241                  10.0%    10    0.3   0.4   0.3   0.9   0.0
  7.|-- 52.93.28.179                    0.0%    10    1.0   1.2   0.3   1.7   0.0
  8.|-- 52.93.28.139                   20.0%    10    1.7   1.5   1.0   2.4   0.0
  9.|-- 100.91.177.198                 10.0%    10   22.8  24.2  22.6  31.6   2.8
 10.|-- 100.91.165.30                   0.0%     9   22.8  23.4  22.8  24.1   0.0
 11.|-- 100.91.164.63                   0.0%     9   24.1  23.5  23.0  24.1   0.0
 12.|-- 100.91.198.14                   0.0%     9   23.4  24.8  22.7  36.0   4.2
 13.|-- 100.91.199.57                   0.0%     9   23.4  24.8  23.1  27.9   1.8
 14.|-- 52.93.128.100                   0.0%     9   24.3  24.0  22.9  26.2   0.9
 15.|-- 100.91.189.80                   0.0%     9   23.5  25.0  22.9  36.8   4.4
 16.|-- 100.91.217.65                   0.0%     9   24.2  23.4  22.4  24.2   0.0
 17.|-- 100.91.189.133                  0.0%     9   24.2  24.0  23.1  27.3   1.2
 18.|-- 150.222.212.22                  0.0%     9   23.4  23.7  23.3  24.1   0.0
 19.|-- 54.239.45.24                    0.0%     9   23.7  24.4  22.7  30.5   2.2
 20.|-- 52.93.129.135                   0.0%     9   23.6  24.3  22.8  28.3   1.7
 21.|-- 100.91.29.83                    0.0%     9   25.8  23.7  23.0  25.8   0.7
 22.|-- 64.125.46.75.broadcast.zip.zayo.com  0.0%     9   22.8  24.1  22.8  30.0   2.1
 23.|-- 165.225.0.159                   0.0%     9   25.6  45.5  23.0 134.7  39.6


Reverse path from: 165.225.48.8 to your Public IP: 100.25.80.250
Start: Tue Feb 25 03:44:42 2020
HOST: ip-172-31-96-220              Loss%   Snt   Last   Avg  Best  Wrst StDev
  1.|-- 172.17.9.2                    0.0%    10    3.6   2.9   2.5   3.6   0.0
  2.|-- 165.225.48.3                  0.0%    10    3.1   3.5   2.6   4.5   0.3
  3.|-- ae15-2347.cr0-was1.ip4.gtt.net  0.0%    10    3.8   4.3   2.8   6.5   1.1
  4.|-- et-0-0-61.cr2-was1.ip4.gtt.net  0.0%    10   20.6   7.4   3.3  20.6   6.1
  5.|-- ip4.gtt.net                    0.0%    10    3.3   4.8   3.3  10.9   2.1
  6.|-- ???                          100.0    10    0.0   0.0   0.0   0.0   0.0
  7.|-- ???                          100.0    10    0.0   0.0   0.0   0.0   0.0
  8.|-- 52.93.28.156                   0.0%    10    4.4   7.4   4.4  16.1   3.3
  9.|-- ???                          100.0    10    0.0   0.0   0.0   0.0   0.0
```

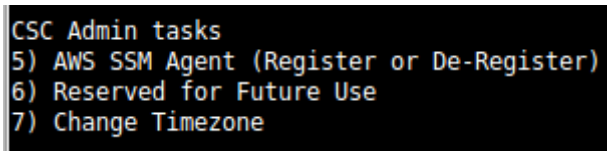
7.1.4 SPEED TEST

This test is experimental due to we are using third party tools (speedtest.net) but it works fine in most cases.

We are using t3a.small instance for the CSC and the download value was 723.90 Mbit/s



7.2 CSC Admin Tasks



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

6. Reserved.

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

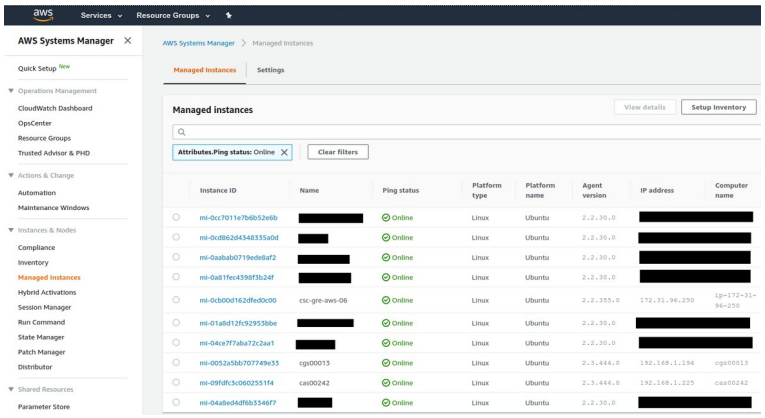
7.2.1 AWS SSM Agent (Register / De-Register)

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

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

Important (**): You can manage the CSC for AWS from ANY AWS Availability Zone. In this example, we have running the CSC for AWS on N. Virginia (us-east-1) but we want to manage it from the Ireland (eu-west-1). It is advisable to manage all CSC (for AWS/Azure/Vmware/Hyper-V) from the same AWS availability zone.

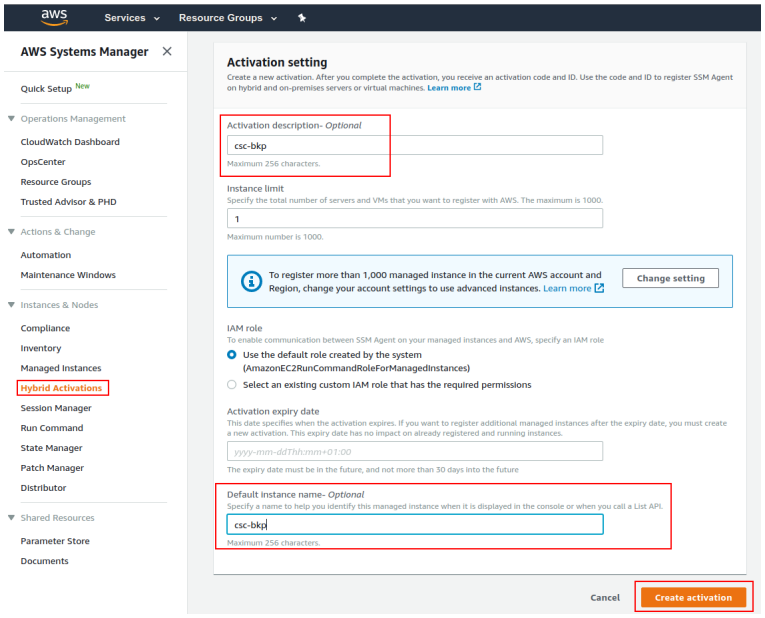
Here is the screenshot of our CSCs under management before to add the CSC for AWS:



Please, note that in this example the availability zone is eu-west-1

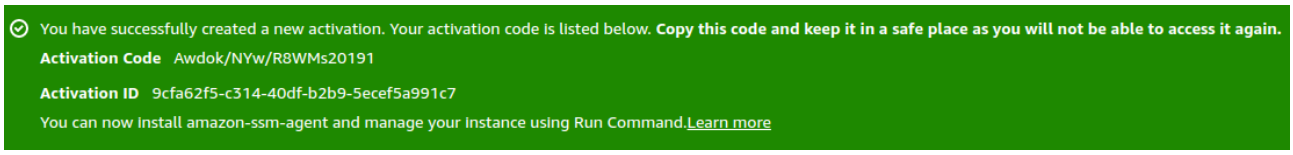
The steps required to register the AWS SSM Agent are two:

1. Go to: AWS Systems Manager -> Hybrid Activations -> click “Create activation”



Note: We recommend to create 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 copy this values on a safe place. You will need this to register the AWS SSM client on the CSC.

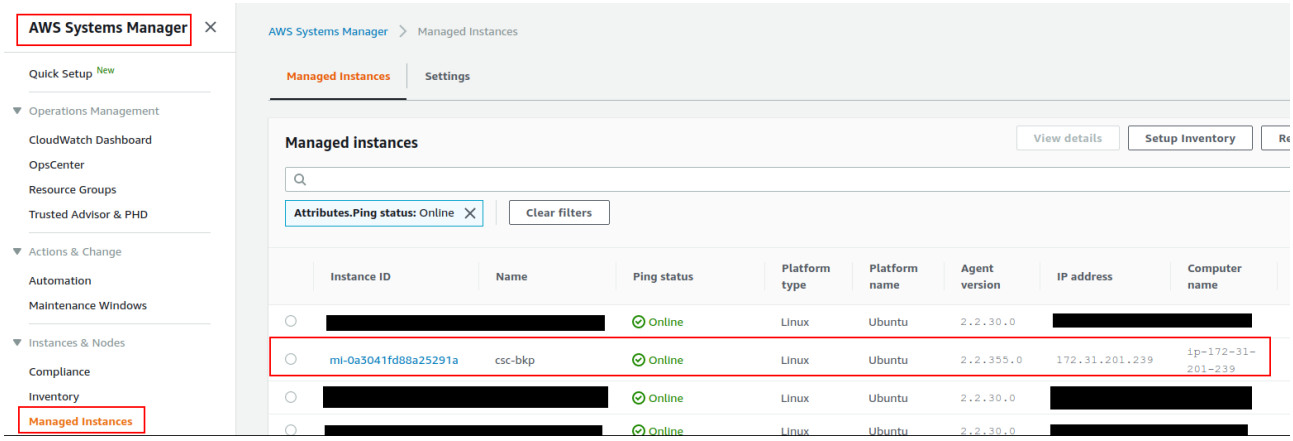
2. From the CSC Admin Tasks Menu, select “5) AWS SSM Agent (Register or De-Register)”. You will asked for the Activation Code, Activation ID and AWS Region where to register the CSC. (Check your AWS URL https://eu-west-1.console.aws.amazon.com/ec2/v2/home?region=**eu-west-1**#)

```
Selection: 5

The SSM Agent is inactive (dead) since Wed 2019-10-16 12:51:23 GMT; 9min ago

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 :Awdok/NYw/R8WMs20191
Activation ID :9cfa62f5-c314-40df-b2b9-5ecef5a991c7
Region :eu-west-1
```

Done! Check now “Show Configuration and Status” :

```
AWS SSM AGENT
AWS SSM Agent is active (running) since Wed 2019-10-16 13:01:21 GMT; 1min 26s ago
Registration values: {"ManagedInstanceID":"mi-0a3041fd88a25291a","Region":"eu-west-1"}
```

Go to AWS Systems Manager → Managed Instances and you will see the new CSC added. (csc-bkp in this case)



7.2.2 Reserved for future use

This menu is reserved for future use.

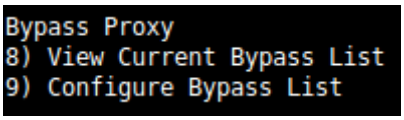
7.2.3 Change Timezone

The CSC automatically takes the time and timezone from the virtual platform but you can change if it is not correct or you want another value.

--- o ---

7.3 Bypass Proxy

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

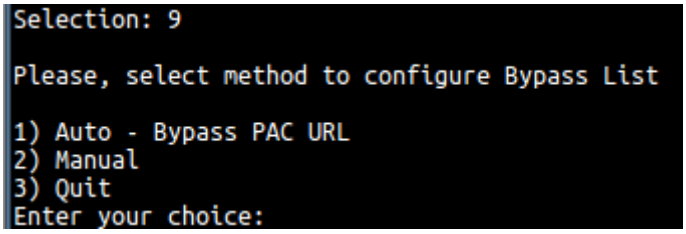


7.3.1 View Current Bypass List

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

7.3.2 Configure Bypass List

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



7.3.2.1 1) Auto – Bypass PAC URL

This is the recommended method to use. You need to create a “Bypass PAC file” on your Zscaler console. The CSC will read the “Bypass List” from the “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 idea of the “Bypass PAC file” is to act a central repository of all bypasses required. Moreover, if you are managing the CSCs using AWS, you can update all CSCs in your network doing one AWS Run Command.

Example of “Bypass PAC file”

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

   //* CSC bypass*/
   if ((shExpMatch(host, "*.firstdomain.com")) ||
      (shExpMatch(host, "www.fulldomain.co.uk")) ||
      (shExpMatch(host, "portquiz.net")) ||
      (shExpMatch(host, "*.salesforce.com")) ||
      (shExpMatch(host, "*.lastdomain.com"))) {
      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

7.3.2.2 Example Using Bypasses

The following example is the case redundant CSCs and bypasses direct to internet.

In this example the redirection method is PAC files only.

Requirements:

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

Bypass PAC on Zscaler Console:

PAC FILE CONTENTS

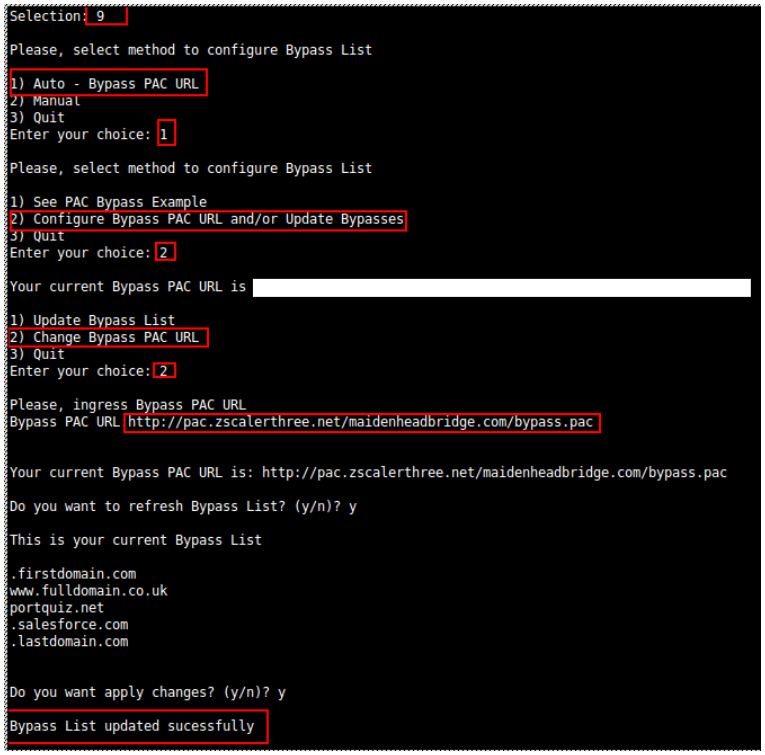
```
function FindProxyForURL(url, host) {
    var bypassproxy = "PROXY 1.1.1.1:3128; PROXY 2.2.2.2:3128";

    //* CSC bypass*/
    if ((shExpMatch(host, "*.firstdomain.com")) ||
        (shExpMatch(host, "www.fulldomain.co.uk")) ||
        (shExpMatch(host, "portquiz.net")) ||
        (shExpMatch(host, "*.salesforce.com")) ||
        (shExpMatch(host, "*.lastdomain.com"))) {
        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 Bypass PAC but you need to put the correct values in the production PAC.

Bypass PAC URL on this example

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

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



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

```
TRAFFIC REDIRECTION Options
To Zscaler: VIP Proxy: 172.31.202.98:80 (or :9400) | Route all traffic via CSC GW IP | Zscaler Global Proxies (port 80/9400) via CSC GW IP
Direct to Internet: Bypass Proxy: 172.31.202.81:3128 | Zscaler Global Proxies (port 3128) via CSC GW IP
```

```
TRAFFIC REDIRECTION Options
To Zscaler: VIP Proxy: 172.31.200.35:80 (or :9400) | Route all traffic via CSC GW IP | Zscaler Global Proxies (port 80/9400) via CSC GW IP
Direct to Internet: Bypass Proxy: 172.31.200.64:3128 | Zscaler Global Proxies (port 3128) via CSC GW IP
```

4. Create your production PAC file and Copy/Paste the section for Bypasses. Put the right values for variables “tozscaler” and “bypassproxy”

```
function FindProxyForURL(url, host) {

   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";

   var tozscaler = "PROXY 172.31.202.98:80; PROXY 172.31.200.35:80";
   var bypassproxy = "PROXY 172.31.202.81:3128; PROXY 172.31.200.64:3128";

   // FTP goes via Zscaler
   if (url.substring(0, 4) == "ftp:")
      return tozscaler

   // Domains to bypass via bypassproxy
   if ((shExpMatch(host, "*.firstdomain.com")) ||
      (shExpMatch(host, "www.fulldomain.co.uk")) ||
      (shExpMatch(host, "portquiz.net")) ||
      (shExpMatch(host, "*.salesforce.com")) ||
      (shExpMatch(host, "*.lastdomain.com"))) {
      return bypassproxy
   }

   // Default Traffic Forwarding to Zscaler
   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 “bypass” using the following commands:

Traffic “tozscaler”

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

In this example:

Linux:

curl -s --proxy http://172.31.202.98:80 ip.zscaler.com | grep You

Win 10:

curl -s --proxy http://172.19.0.195:80 ip.zscaler.com | findstr You

Result expected:

You are accessing the Internet via Zscaler Cloud: Washington DC in the zscalerthree.net cloud.
Your request is arriving at this server from the IP address 165.225.9.6
Your Gateway IP Address is **3.219.197.65**

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 is takes long to answer or is unresponsive.

In this example:

Linux:

curl -s --proxy http://172.31.202.81:3128 portquiz.net

Win 10:

curl -s --proxy http://172.31.202.81:3128 portquiz.net

Result expected:

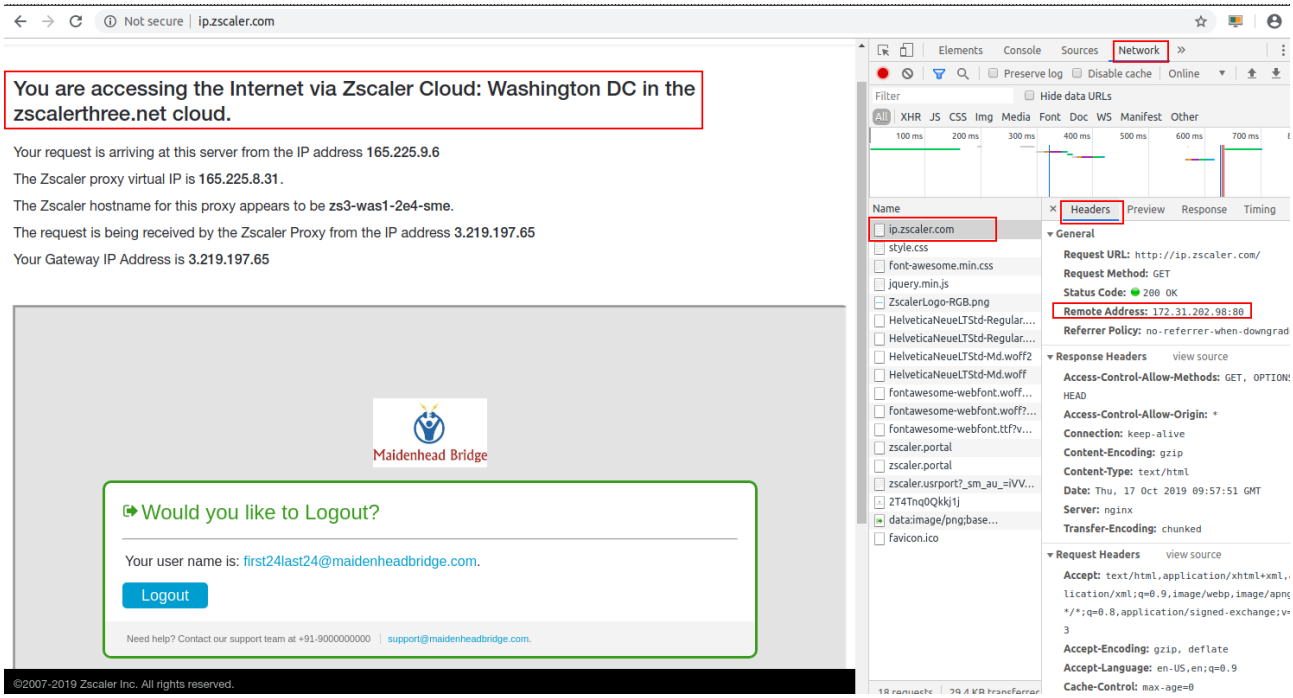
Port 80 test successful!
Your IP: 3.231.138.134

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

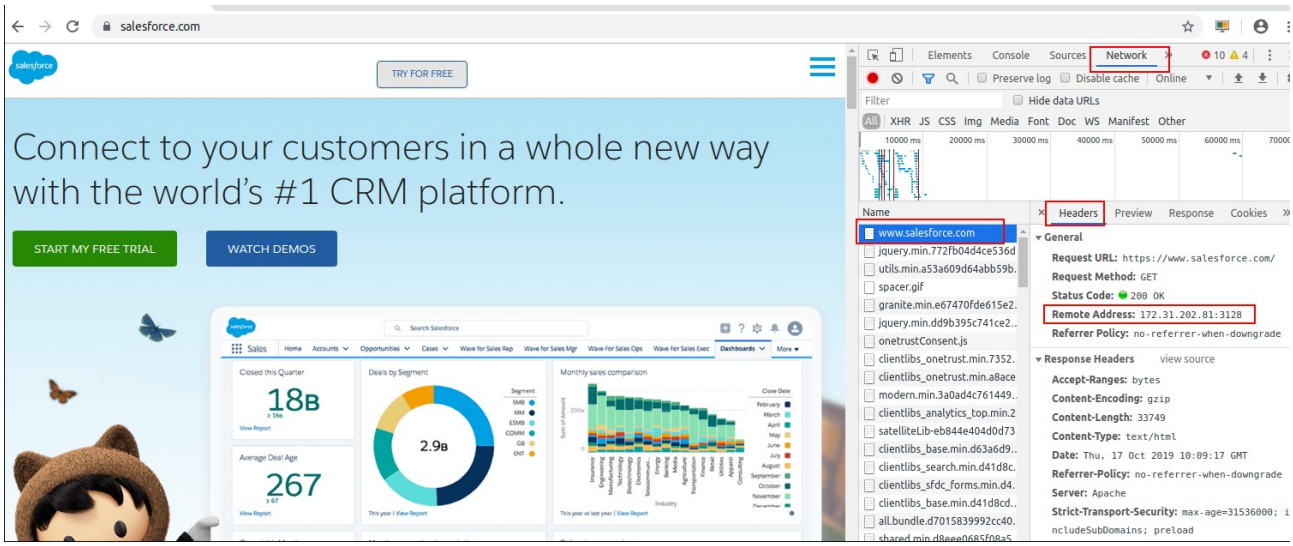
Traffic “tozscaler”

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



Bypass Traffic

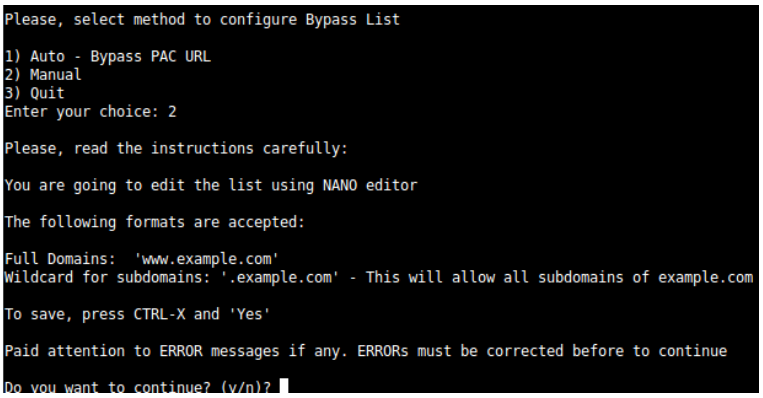
Using our example, we are going to http://www.salesforce.com and using Chrome Developer tools check the proxy in use:



7.3.2.3 2) Manual

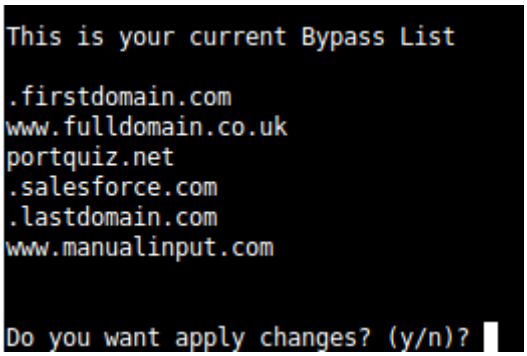
If you want to update manually your bypass list, follow this steps

1. Select Option 2)



2. Ingress “y”

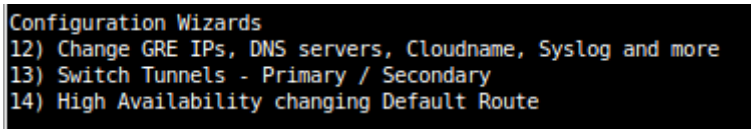
3. Add / Delete / Modify your full domains and subdomains
4. Please, CTL+X and “Yes” (and after next prompt Enter) to Save
5. The modified Bypass List will be displayed.



6. Apply Changes (y) or discard (n). If “y” you will receive the following message
7. Bypass List update successfully.

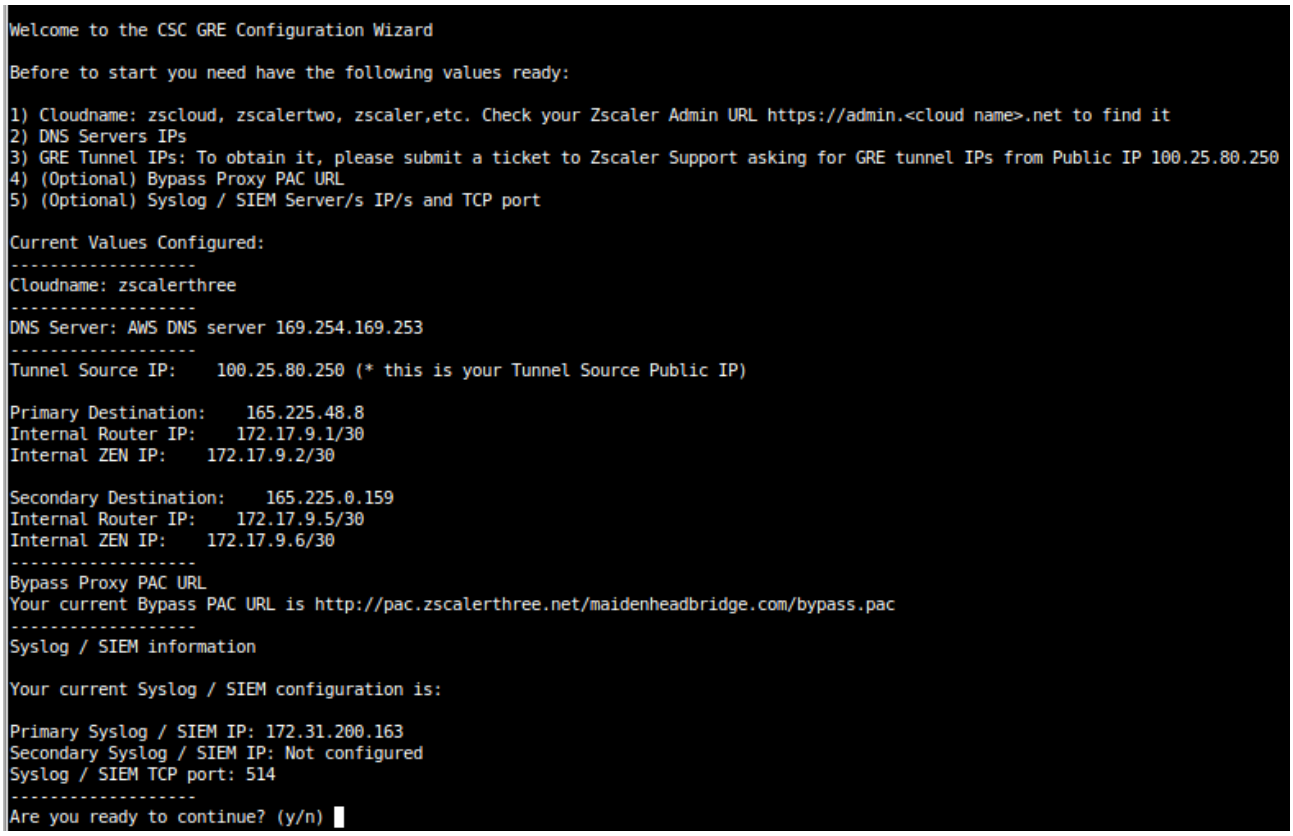
7.4 Configuration Wizards

In this section you can run the initial configuration wizard to change GRE IPs, DNS servers and/or Cloud Name, an easy way to Switch tunnels and to configure High Availability.



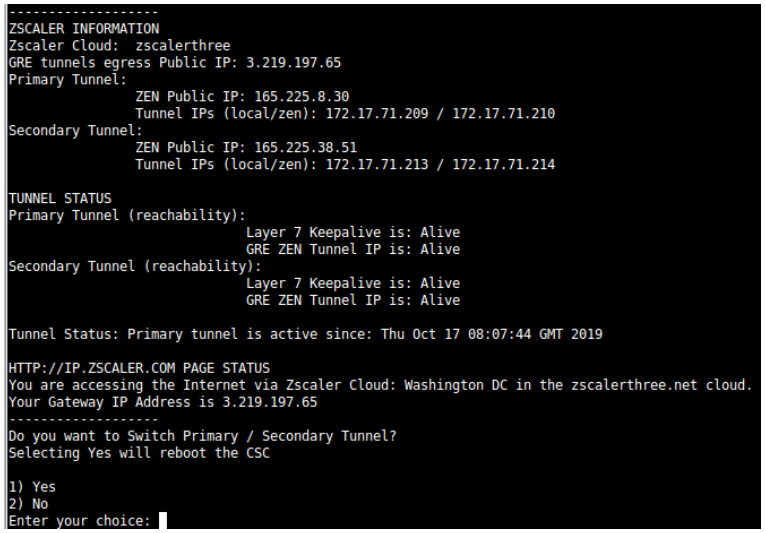
7.4.1 12) Change GRE IPs, DNS servers, Cloudname, Syslog and more

This is the same than the initial configuration Wizard explained at the beginning of this manual.



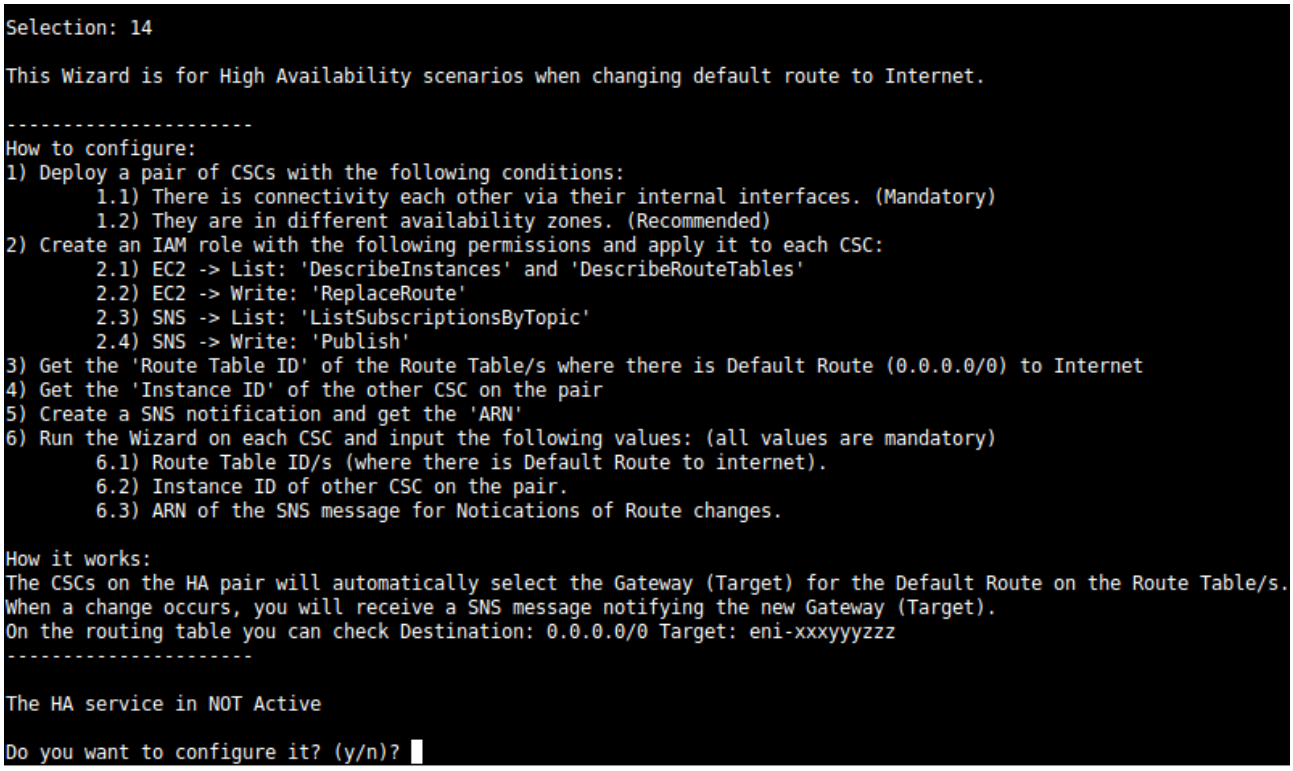
7.4.2 13) Switch Tunnels - Primary / Secondary

This section shows your current settings and statuses and allows to switch tunnels



7.4.3 14) High Availability changing Default Route

In this section you can configure the CSC on HA pair to manage automatically the default route to Internet.



Help provided:

How to configure:

1) Deploy a pair of CSCs with the following conditions:

    1.1) There is connectivity each other via their internal interfaces. (Mandatory)

    1.2) They are in different availability zones. (Recommended)

2) Create an IAM role with the following permissions and apply it to each CSC:

    2.1) EC2 -> List: 'DescribeInstances' and 'DescribeRouteTables'

    2.2) EC2 -> Write: 'ReplaceRoute'

    2.3) SNS -> List: 'ListSubscriptionsByTopic'

    2.4) SNS -> Write: 'Publish'

3) Get the 'Route Table ID' of the Route Table/s where there is Default Route (0.0.0.0/0) to Internet

4) Get the 'Instance ID' of the other CSC on the pair

5) Create a SNS notification and get the 'ARN'

6) Run the Wizard on each CSC and input the following values: (all values are mandatory)

6.1) Route Table ID/s (where there is Default Route to internet).

6.2) Instance ID of other CSC on the pair.

6.3) ARN of the SNS message for Notications of Route changes.

How it works:

The CSCs on the HA pair will automatically select the Gateway (Target) for the Default Route on the Route Table/s.

When a change occurs, you will receive a SNS message notifying the new Gateway (Target).

On the routing table you can check Destination: 0.0.0.0/0 Target: eni-xxxyyyzzz

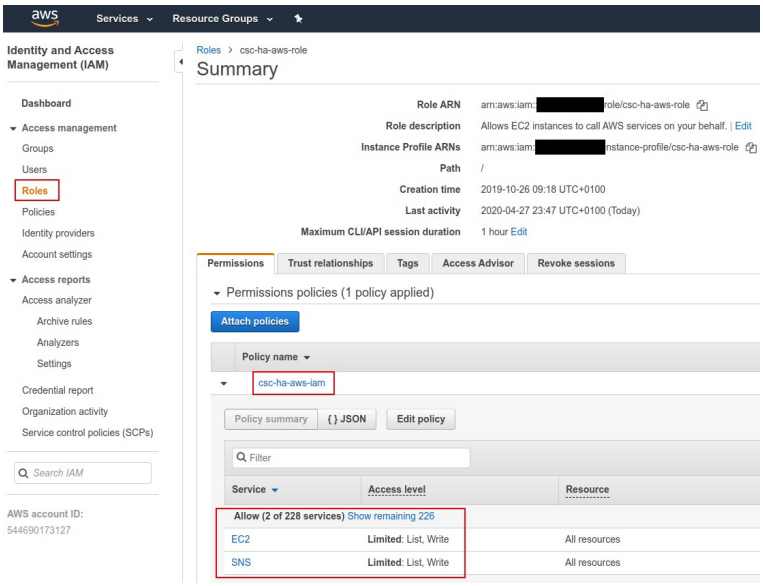
7.4.3.1 High Availability configuration on detail

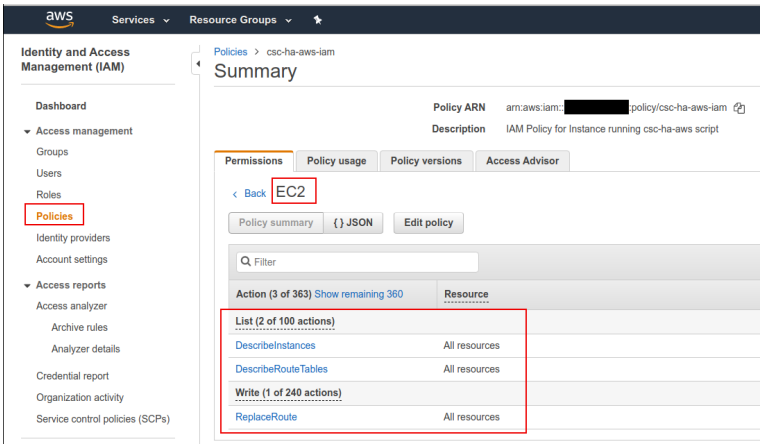
1. **Deploy a pair of CSC on the different availability zones.**

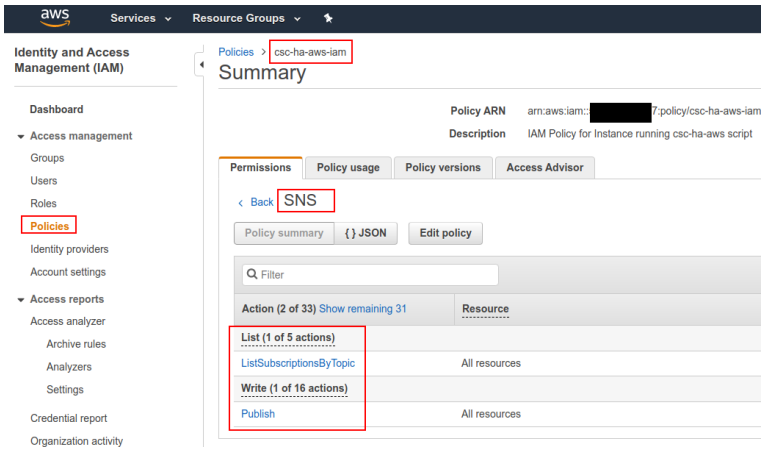
Name	Instance ID	Instance Type	Availability Zone
csc-gre-aws-v-2-7c-1	i-0010c674f81d79cbf	t3a.small	us-east-1d
csc-gre-aws-v-2-7c-2	i-05e327fb84e9bbd91	t3a.small	us-east-1a

2. **Create an IAM role with the following policies:**

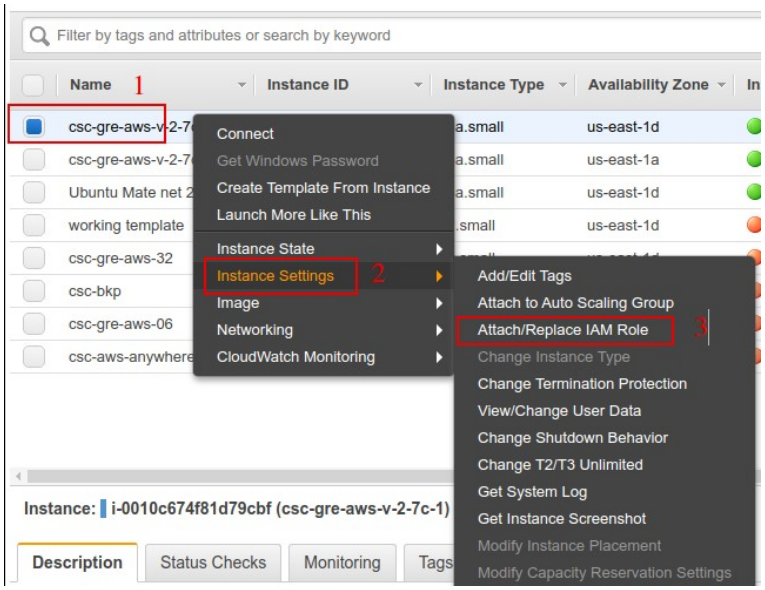
EC2 → List: 'DescribeInstances' and 'DescribeRouteTables'
EC2 → Write: 'ReplaceRoute'
SNS -> List: 'ListSubscriptionsByTopic'
SNS → Write: 'Publish'

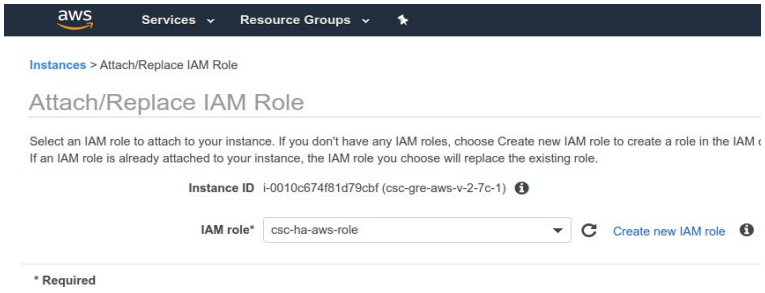

Services
Resource Groups
Identity and Access Management (IAM)
Dashboard
Access management
Groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Service control policies (SCPs)
Search IAM
AWS account ID:
544690173127
Roles > csc-ha-aws-role
Summary
Role ARN
arn:aws:iam:[redacted]role/csc-ha-aws-role
Role description
Allows EC2 instances to call AWS services on your behalf. | Edit
Instance Profile ARNs
arn:aws:iam:[redacted]instance-profile/csc-ha-aws-role
Path
/
Creation time
2019-10-26 09:18 UTC+0100
Last activity
2020-04-27 23:47 UTC+0100 (Today)
Maximum CLI/API session duration
1 hour Edit
Permissions
Trust relationships
Tags
Access Advisor
Revoke sessions
Permissions policies (1 policy applied)
Attach policies
Policy name
csc-ha-aws-iam
Policy summary
{ } JSON
Edit policy
Filter
Service
Access level
Resource
Allow (2 of 228 services) Show remaining 226
EC2
Limited: List, Write
All resources
SNS
Limited: List, Write
All resources


Services
Resource Groups
Identity and Access Management (IAM)
Dashboard
Access management
Groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzer details
Credential report
Organization activity
Service control policies (SCPs)
Policies > csc-ha-aws-iam
Summary
Policy ARN
arn:aws:iam::[redacted]policy/csc-ha-aws-iam
Description
IAM Policy for Instance running csc-ha-aws script
Permissions
Policy usage
Policy versions
Access Advisor
Back
EC2
Policy summary
{ } JSON
Edit policy
Filter
Action (3 of 363) Show remaining 360
Resource
List (2 of 100 actions)
DescribeInstances
All resources
DescribeRouteTables
All resources
Write (1 of 240 actions)
ReplaceRoute
All resources

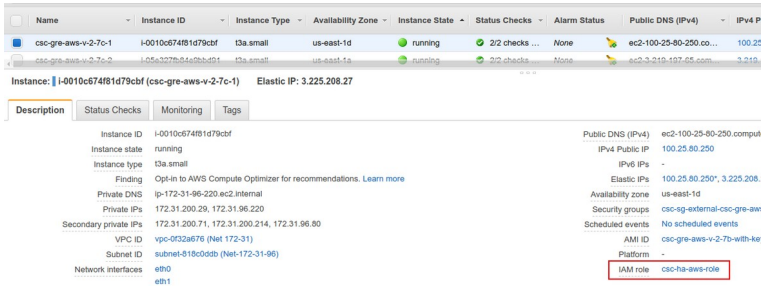

Services
Resource Groups
Identity and Access Management (IAM)
Dashboard
Access management
Groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
Organization activity
Policies > csc-ha-aws-iam
Summary
Policy ARN
arn:aws:iam::[redacted]7:policy/csc-ha-aws-iam
Description
IAM Policy for Instance running csc-ha-aws script
Permissions
Policy usage
Policy versions
Access Advisor
Back
SNS
Policy summary
{ } JSON
Edit policy
Filter
Action (2 of 33) Show remaining 31
Resource
List (1 of 5 actions)
ListSubscriptionsByTopic
All resources
Write (1 of 16 actions)
Publish
All resources

3. Apply the IAM roles to each CSC on the pair.





Check the IAM role is assigned:

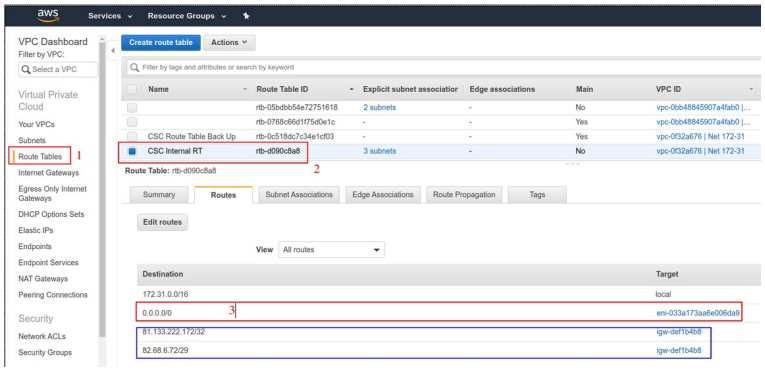


Attached the role to the other CSC on the pair as well.

4. Obtain your Route Table ID:

Note: You can add multiple Route Table ID on this version 2.8

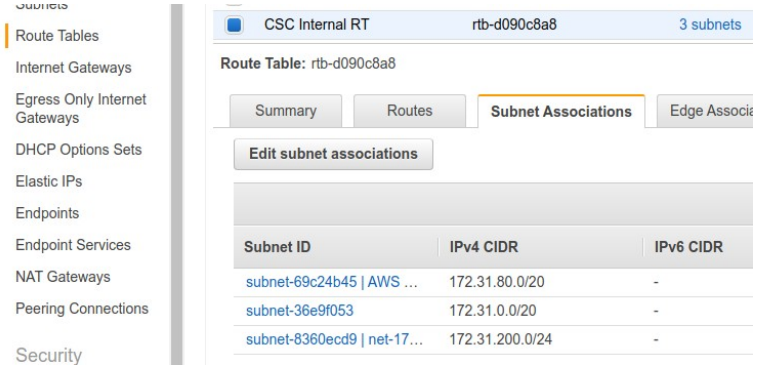
Go to VPC → Route Tables and get your table ID



Note 1: The CSC pair will modify the default route (0.0.0.0/0)"Target", setting the "eni-xxyy" values. Other Destination will remain untouched.

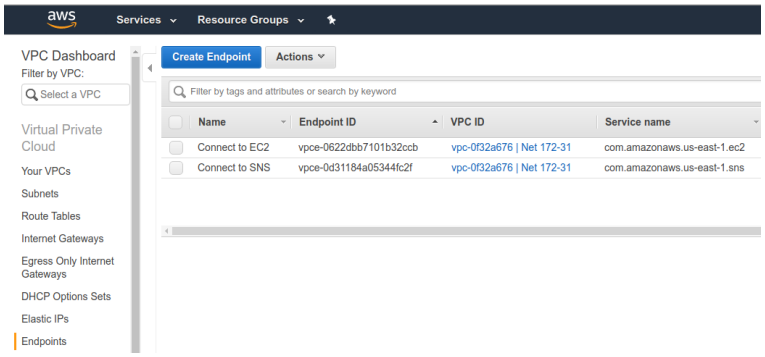
Note 2: We sure to add other destinations, like your internal subnets or your public IPs via the proper "Target" in order to do not loose connectivity to the VPC.

Apply the Subnet Associations to the Routing Table:



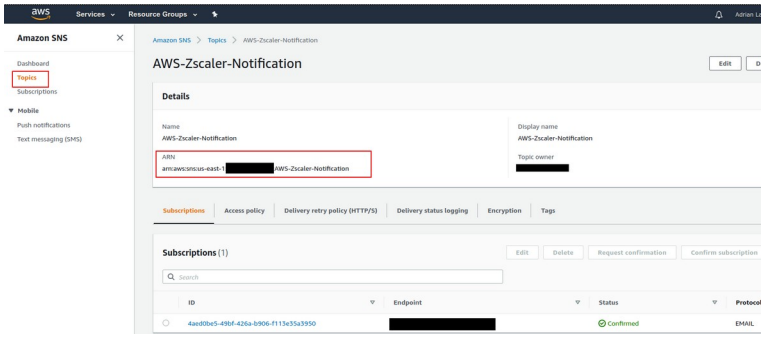
5. Create "Endpoints" to AWS services (EC2, SNS, S3, etc)

When changing the default route to internet via Zscaler you potentially will lost contact with some AWS services. For the CSC on the pair is mandatory to create two endpoints: to EC2 and SNS. Please, note that you may require to add some more for your services.



6. **Create SNS message for Alerts.**

Obtain the ARN



7. **Finally Run the HA Wizard on each CSC**

```
Do you want to configure it? (y/n)? y

IAM role in use: arn:aws:iam::544690173127:instance-profile/csc-ha-aws-role

Please, input the following values
Route Table ID= rtb-d090c8a8
Do you want to add another Route Table ID? (y/n)? y
Route Table ID= rtb-0994dbce551a782f0
Do you want to add another Route Table ID? (y/n)? n
Instance ID of other CSC in the pair= i-0dabbfe38df52b9cd
SNS message ARN= arn:aws:sns:us-east-1:544690173127:AWS-Zscaler-Notification

Values to configure are:

Routing Tables=2
Routing Table ID= rtb-d090c8a8
Routing Table ID= rtb-0994dbce551a782f0
Instance ID of other CSC in the pair= i-0dabbfe38df52b9cd
SNS message ARN= arn:aws:sns:us-east-1:544690173127:AWS-Zscaler-Notification

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

CSC HA is : active (running) since Mon 2020-04-27 23:16:36 UTC; 28ms ago
```

Done!

8. Notifications from CSC on HA

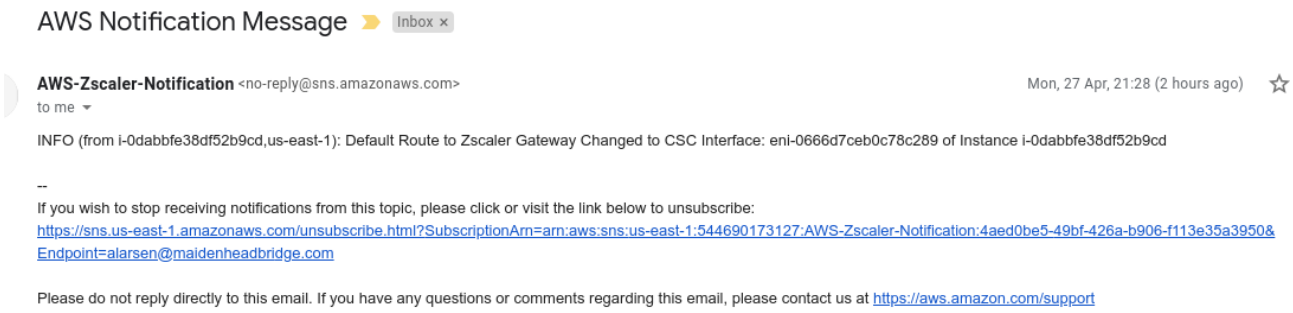
Each CSC on the pair will send notifications when:

→ There is no connectivity at all with Zscaler. No CSC is able to reach Zscaler.

→ At power up the CSC will notify the current “eni-xxyy” used as default GW to internet

→ On routing change, the CSCs will notify the changes.

Example of notifications:



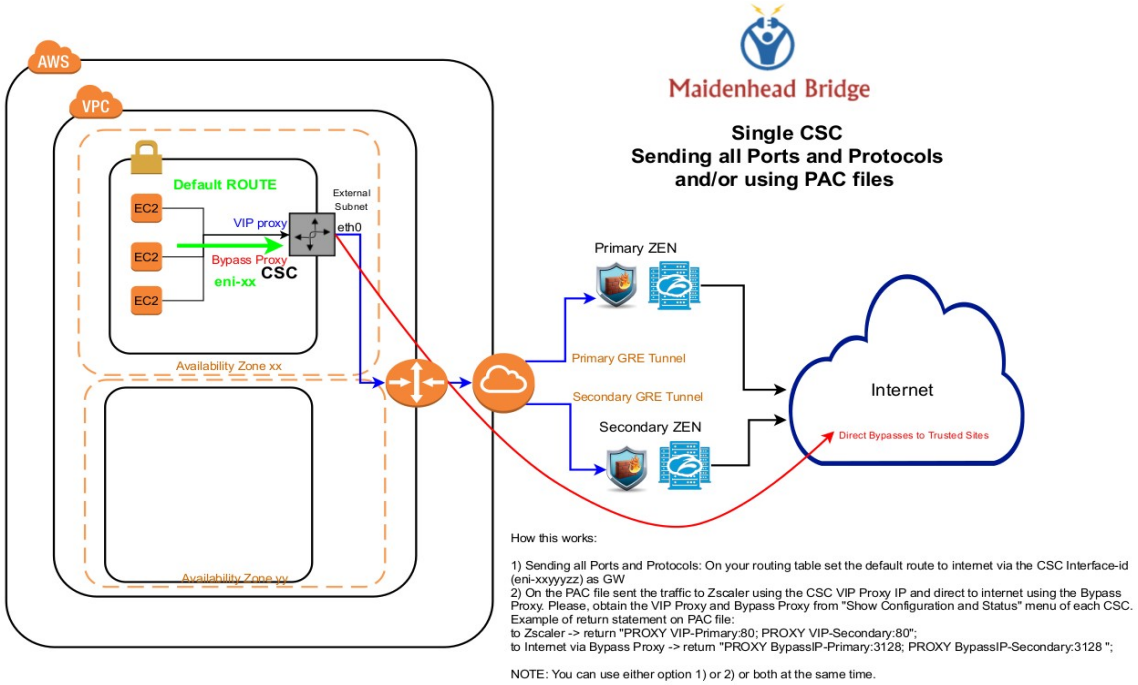
Also, Logs are generated:

```
Apr 27 23:17:40 root: (MHB-CSC)(INFO) Default Route to Zscaler using CSC Interface: eni-033c4c5e5de9e784b of Instance i-027f6d85b46cb4b2b
```

8 Appendix A – Traffic Redirection Examples

8.1 Single CSC – Using Cloud FW and/or PAC files

8.1.1 Network Diagram



8.1.2 Traffic Redirection

8.1.2.1 Using Cloud FW – All ports and protocols to Zscaler

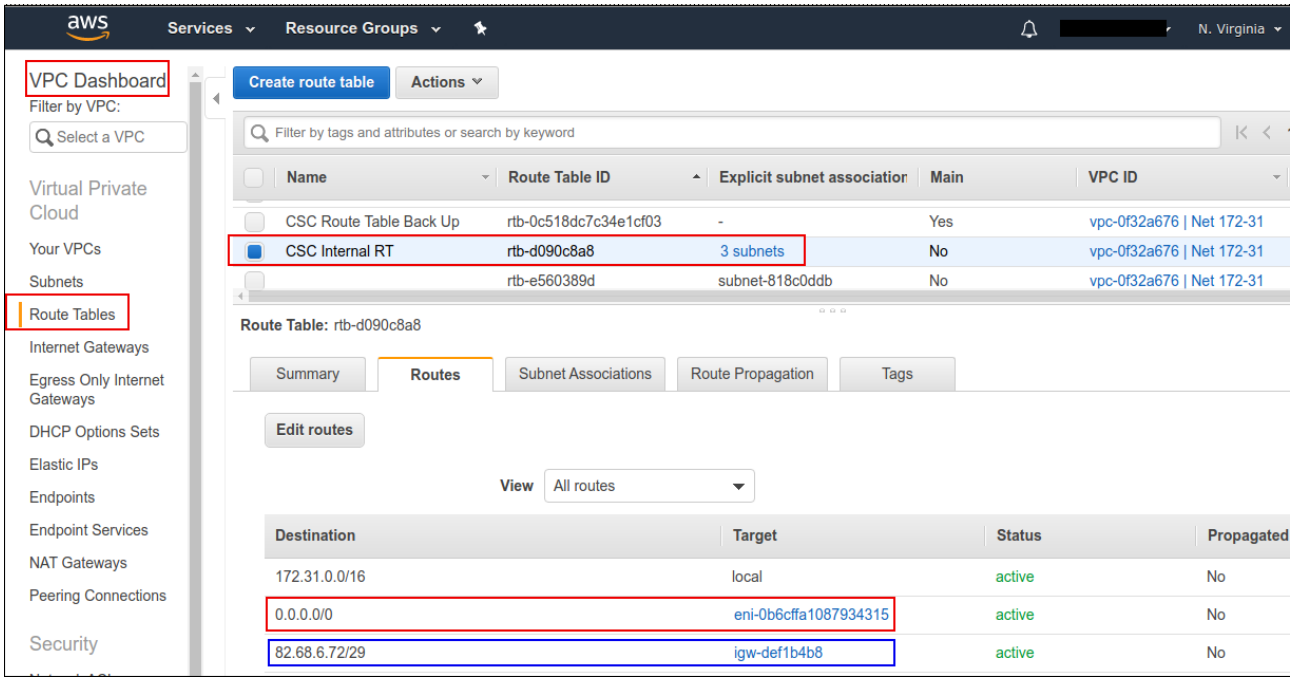
Important: This method provides no redundancy. Later on this guide we show examples with high availability,

1. Deploy a CSC on your VPC
2. Check “Show Configuration and Status” to obtain the “Interface-Id:” of eth1

```
GENERAL INFORMATION
Availability Zone: us-east-1d
EC2 Instance id: i-0fa59091d1c41f200 | Instance Type: t2.small | ami-id: ami-0e9786556ca523966
External Interface (eth0) Subnet-id: subnet-818c0ddb | Interface-id: eni-0ec6b2b53d990c2e5 | Security-Group-id: sg-0d2b80c6632946cd9
Internal Interface (eth1) Subnet-id: subnet-8360ecd9 | Interface-id: eni-0b6cffa1087934315 | Security-Group-id: sg-033efd40e740dd848
CSC date: Thu Oct 17 08:29:11 GMT 2019
Soft version : 2.6
```

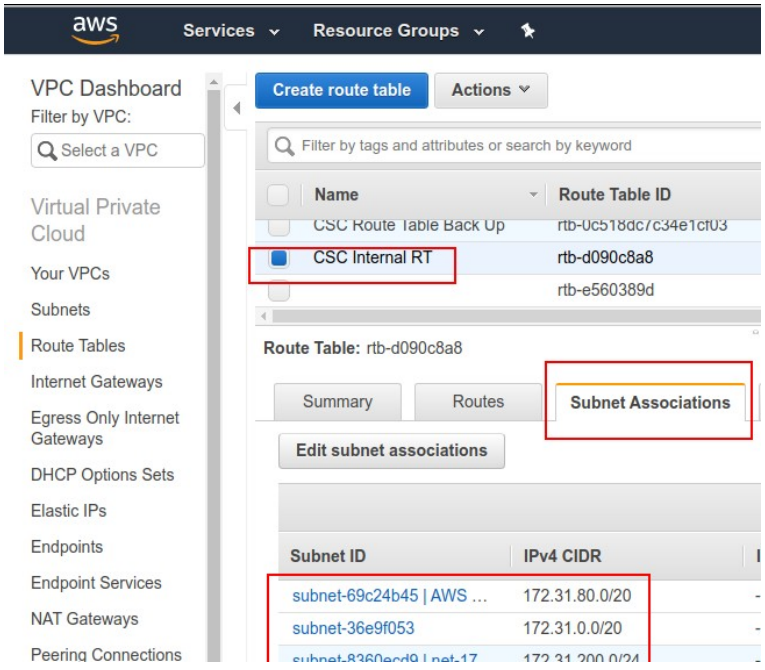
In this example the value is: eni-0b6cffa1087934315

3. Create a Route table with a route 0.0.0.0/0 → Target (GW): eni-xxyyzz



Note: When creating the route for 0.0.0.0/0 take care of creating another route for your remote access to the subnet if necessary. In this example, the IP: 82.68.6.72/29 is our public IPs to access to instances behind the CSC.

4. Associate the Subnets to the Route Table

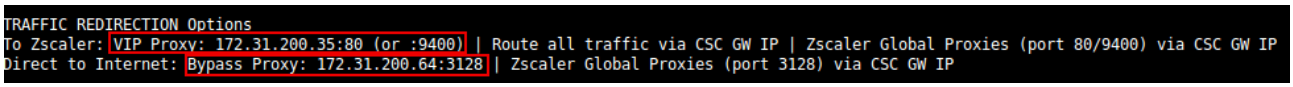


5. Done. All traffic will go via the CSC.

8.1.2.2 Using PAC files only (*)

(*) Important: This method forwards only Web Traffic to Zscaler. (HTTP, HTTPS, FTP) due to the default GW to the internet is not the CSC. In the next example we will show a combination of both redirection methods: all port and protocols and PAC files at the same time.

1. Deploy a CSC on your VPC
2. Check Check “Show Configuration and Status” to obtain the “VIP Proxy” and “Bypass Proxy” IPs.



In this example the values are:

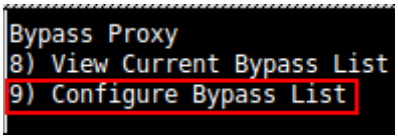
VIP Proxy: 172.31.200.35:80

Bypass Proxy: 172.31.200.64:3128

3. (Optional) Create a “Bypass Proxy PAC” file or manual entry the domains to Bypass. Here an example.

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

   //* CSC bypass*/
   if ((shExpMatch(host, "*.firstdomain.com")) ||
      (shExpMatch(host, "www.fulldomain.co.uk")) ||
      (shExpMatch(host, "portquiz.net")) ||
      (shExpMatch(host, "*.salesforce.com")) ||
      (shExpMatch(host, "*.lastdomain.com"))) {
      return bypassproxy
   }
}
```

Get the URL of the Bypass PAC and configure it on the CSC and refresh the list using Menu 9)



4. Create a “Production PAC”

In the example below you can see that variables “tozscaler” and “bypassproxy” are with the values of VIP Proxy and Bypass Proxy respectively. Also, due to the default route is via the AWS Internet Gateway, it is possible to use the ZEN nodes (or DIRECT) as backup method if the CSC is turned off.

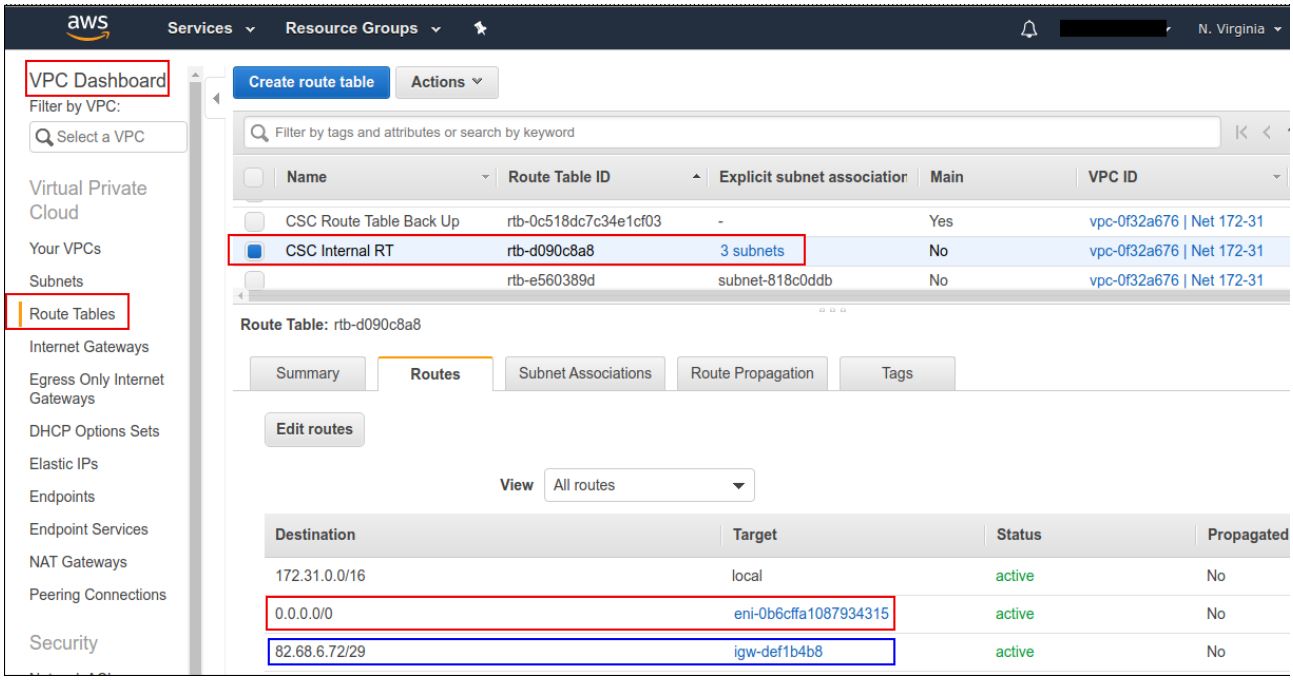
```
function FindProxyForURL(url, host) {

   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";

   var tozscaler = "PROXY 172.31.200.35:80; PROXY ${GATEWAY}:80; PROXY ${SECONDARY_GATEWAY}:80; DIRECT";
   var bypassproxy = "PROXY 172.31.200.64:3128; DIRECT";

   // FTP goes via Zscaler
   if (url.substring(0, 4) == "ftp:")
      return tozscaler

   // Domains to bypass via bypassproxy
   if ((shExpMatch(host, "*.firstdomain.com")) ||
      (shExpMatch(host, "www.fulldomain.co.uk")) ||
      (shExpMatch(host, "portquiz.net")) ||
      (shExpMatch(host, "*.salesforce.com")) ||
      (shExpMatch(host, "*.lastdomain.com"))) {
      return bypassproxy
   }

   // Default Traffic Forwarding to Zscaler
   return tozscaler
}
```

8.1.2.3 Using Cloud FW & PAC Files at the same time

There are cases where you need to do bypasses for certain instances but not for all. In this case, you can setup a PAC file on this particular instances for this purpose. In your production PAC file the variables “tozscaler” and “bypassproxy” will be:

```
var tozscaler = "PROXY 172.31.200.35:80";
var bypassproxy = "PROXY 172.31.200.64:3128";
```

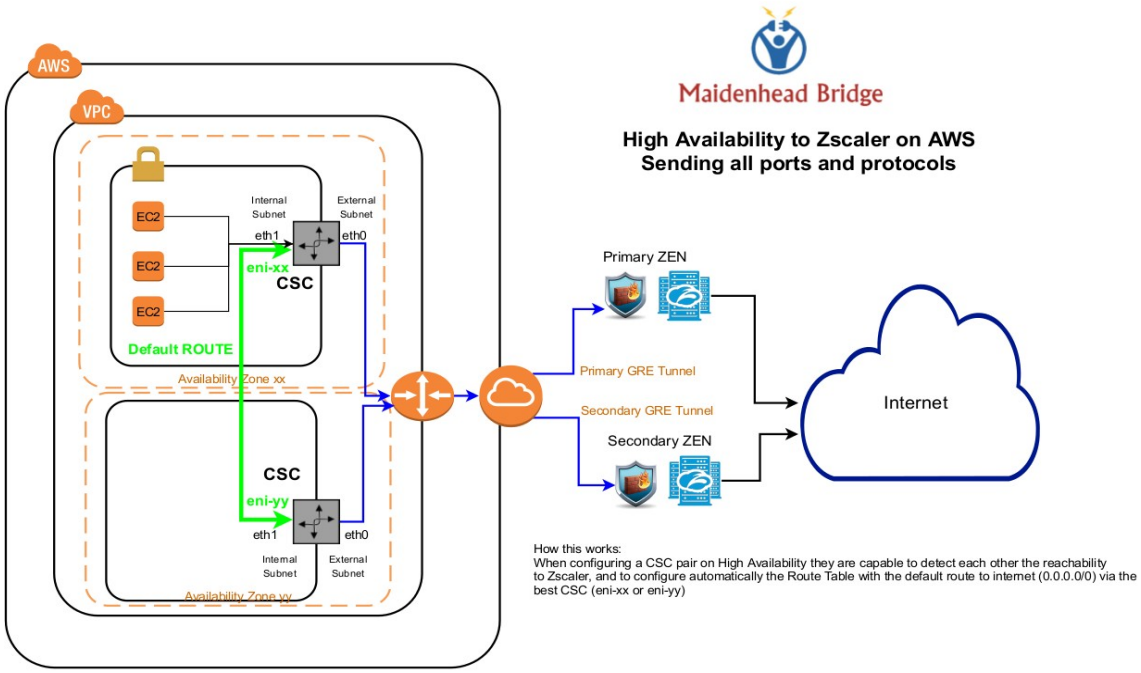
And your routing table like previous example:



Combining this two methods you are able to send all ports and protocols to Zscaler and also to use the bypass capacity of the CSC.

8.2 Redundant CSC – Using Cloud FW

8.2.1 Network Diagram

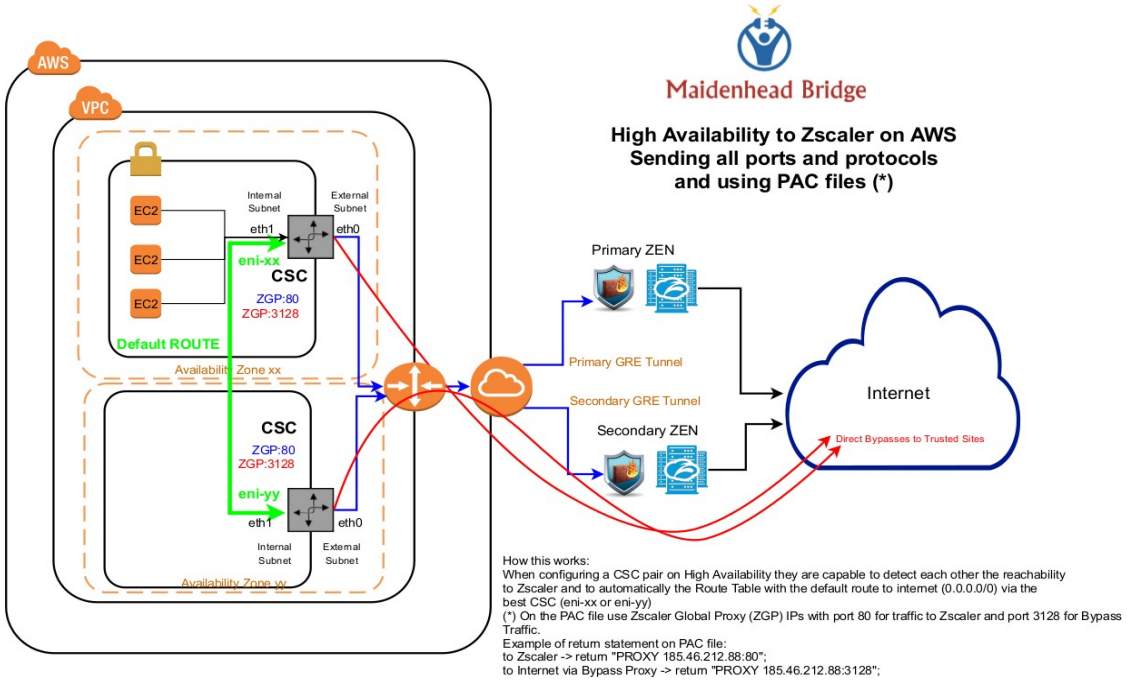


The network diagram shows 2 x CSC on different availability zones with the tunnels to Zscaler up and running.

In order to select which CSC to use, simply follow run the HA wizard (Menu 14). See section: 7.4.3 of this manual.

8.3 Redundant CSC – Using Cloud FW and PAC files

8.3.1 Network Diagram



8.3.2 Traffic Redirection

8.3.2.1 Using Cloud FW (Sending all ports and protocols)

Idem than before. Run Menu 14 (High Availability changing Default Route) on the CSC. Instructions on section 7.4.3

8.3.2.2 and Using PAC files

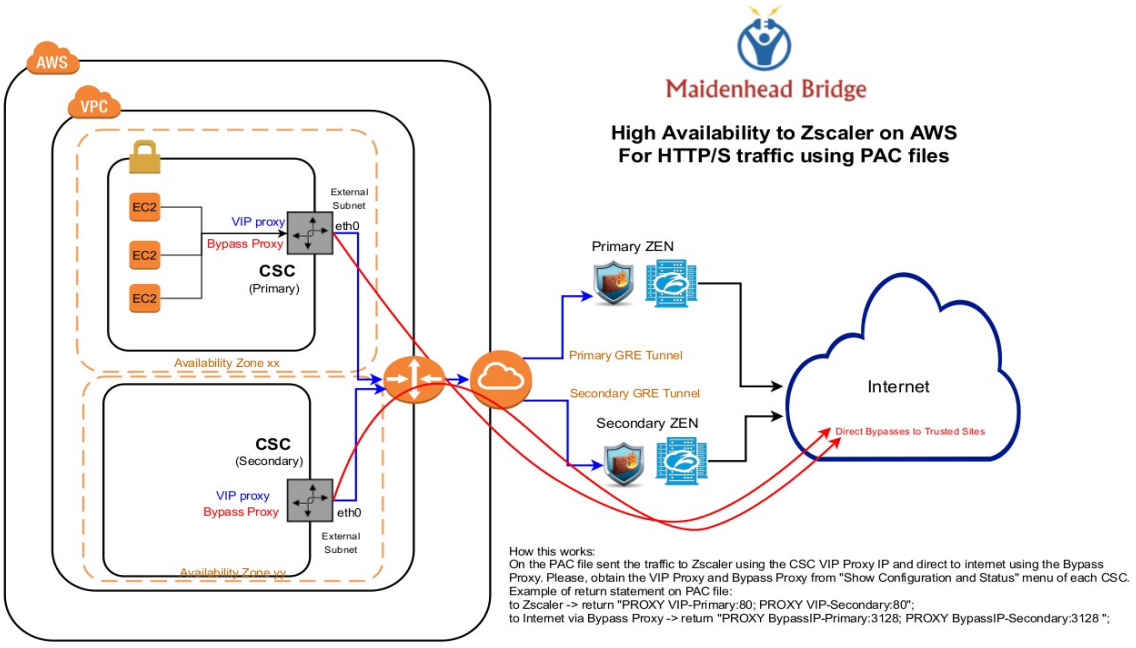
There are situation where you need to use the PAC files on specific machines due to you want to use the Bypass Proxy capacity. In this case, you need to create the PAC files as shown on 8.1.1.2 but your variables “tozscaler” and “bypassproxy” will be using the Zscaler Global Proxies:

```
var tozscaler = "PROXY 185.46.212.88:80; DIRECT";
var bypassproxy = "PROXY 185.46.212.88:3128; DIRECT";
```

```
TRAFFIC REDIRECTION Options
To Zscaler: VIP Proxy: 172.31.200.35:80 (or :9400) | Route all traffic via CSC GW IP | Zscaler Global Proxies (port 80/9400) via CSC GW IP
Direct to Internet: Bypass Proxy: 172.31.200.64:3128 | Zscaler Global Proxies (port 3128) via CSC GW IP
```

8.4 Redundant CSC – For Web traffic using PAC files

8.4.1 Network Diagram

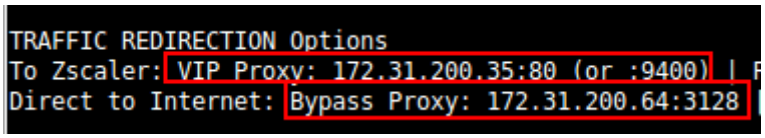


8.4.2 Traffic Redirection: Using PAC files (Primay / Secondary Proxy)

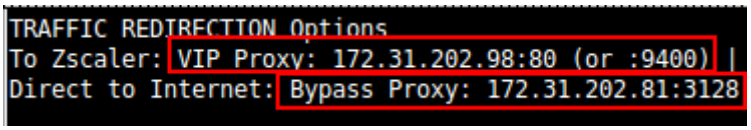
In some situation you may want to send Web Traffic Only. In this case, you need to create the PAC files as shown on 8.1.1.2 but your variables “tozscaler” and “bypassproxy” will be using the “Vip Proxy” and “Bypass Proxy” of each CSC. Using the example values:

```
var tozscaler = "PROXY 172.31.200.35:80; PROXY 172.31.202.98:80; DIRECT";
var bypassproxy = "PROXY 172.31.200.64:3128, PROXY 172.31.202.81:3128; DIRECT";
```

CSC a



CSC b



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

When you have your CSC registered on AWS as “managed instance” you can execute the “Monitoring Tasks” and also to “Update Bypass List”. This is particular important if you have several CSCs.

9.1 AWS Systems Manager: Documents

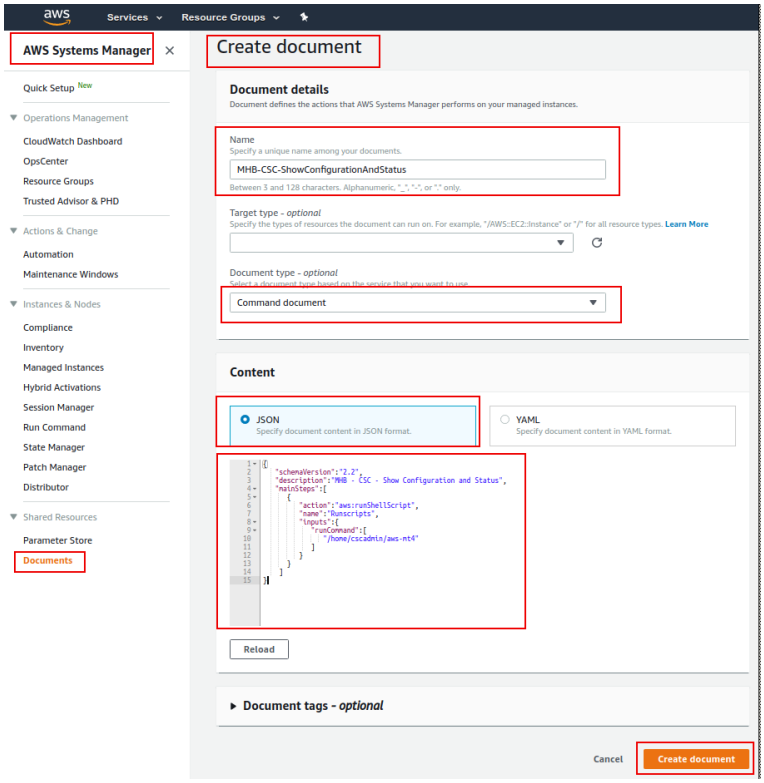
In order to execute “Run Commands” you need to have “Documents” created. “Documents” contains a series of commands to execute. For simplicity purposes, we provide the “Documents” required for the operations of the CSC.

You can create Documents for CSC, Copying/Pasting the information that follows.

9.1.1 Creating a Document

From AWS Systems Manager > Shared Resources > Documents → Click “Create Document”

Put the “Name”, “Document Type” = Command and fill “Content”



Click “Create Document”

9.1.2 List of Documents

Please, create the “Documents” using this values:

Name	MHB-CSC-ShowConfigurationAndStatus-AWS

Content	{
	"schemaVersion":"2.2",
	"description":"MHB - CSC - Show Configuration and Status",
	"mainSteps":[
	{
	"action":"aws:runShellScript",
	"name":"Runscripts",
	"inputs":{
	"runCommand":[
	"sudo -u ubuntu /home/cscadmin/aws-mt4"
	]
	}
	}
	]
	}

Name	MHB-CSC-SpeedTest

Content	{
	"schemaVersion":"2.2",
	"description":"MHB - CSC - Speed Test",
	"mainSteps":[
	{
	"action":"aws:runShellScript",
	"name":"Runscripts",
	"inputs":{
	"runCommand":[
	"/home/cscadmin/aws-mt7"
	]
	}
	}
	]
	}

Name	MHB-CSC-TraceRouteAndLatencyTest

Content	{
	"schemaVersion":"2.2",
	"description":"MHB - CSC - TraceRoute and Latency Test",
	"mainSteps":[
	{
	"action":"aws:runShellScript",
	"name":"Runscripts",
	"inputs":{
	"runCommand":[
	"/home/cscadmin/aws-mt6"
	]
	}
	}
	]
	}

Name	MHB-CSC-UpdateBypassList

Content	{
	"schemaVersion":"2.2",
	"description":"MHB - CSC - Update Bypass List",
	"mainSteps":[
	{
	"action":"aws:runShellScript",
	"name":"Runscripts",
	"inputs":{
	"runCommand":[
	"/home/cscadmin/aws-bp-refresh-list"
	]
	}
	}
	]
	}

Name	MHB-CSC-ShowLogCurrentMonth

Content	{
	"schemaVersion": "2.2",
	"description": "MHB - CSC - Show Log Current Month",
	"mainSteps": [
	{
	"action": "aws:runShellScript",
	"name": "Runscripts",
	"inputs": {
	"runCommand": [
	"/home/cscadmin/aws-l-current-month"
	]
	}
	}
	]
	}

Name	MHB-CSC-ShowLogCurrentMonth-2500Characters

Content	{
	"schemaVersion": "2.2",
	"description": "MHB - CSC - Show Log Current Month - (last 2500 characters)",
	"mainSteps": [
	{
	"action": "aws:runShellScript",
	"name": "Runscripts",
	"inputs": {
	"runCommand": [
	"/home/cscadmin/aws-l-current-month-2500"
	]
	}
	}
	]
	}

Name	MHB-CSC-ShowLogLastSixMonths

Content	{
	"schemaVersion": "2.2",
	"description": "MHB - CSC - Show Log Last Six Months",
	"mainSteps": [
	{
	"action": "aws:runShellScript",
	"name": "Runscripts",
	"inputs": {
	"runCommand": [
	"/home/cscadmin/aws-l-last-6-months"
	]
	}
	}
	]
	}

Name	MHB-CSC-SwitchTunnels

Content	{
	"schemaVersion": "2.2",
	"description": "MHB - CSC – Switch Tunnels",
	"mainSteps": [
	{
	"action": "aws:runShellScript",
	"name": "Runscripts",
	"inputs": {
	"runCommand": [
	"/home/cscadmin/aws-tun-switch"
	]
	}
	}
	]
	}

Name	MHB-CSC-ShowHA

Content	{
	"schemaVersion": "2.2",
	"description": "MHB - CSC - Show HA",
	"mainSteps": [
	{
	"action": "aws:runShellScript",
	"name": "Runscripts",
	"inputs": {
	"runCommand": [
	"sudo -u ubuntu /home/cscadmin/aws-mt4 | tail -8"
	]
	}
	}
	]
	}

9.1.3 Run Commands

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

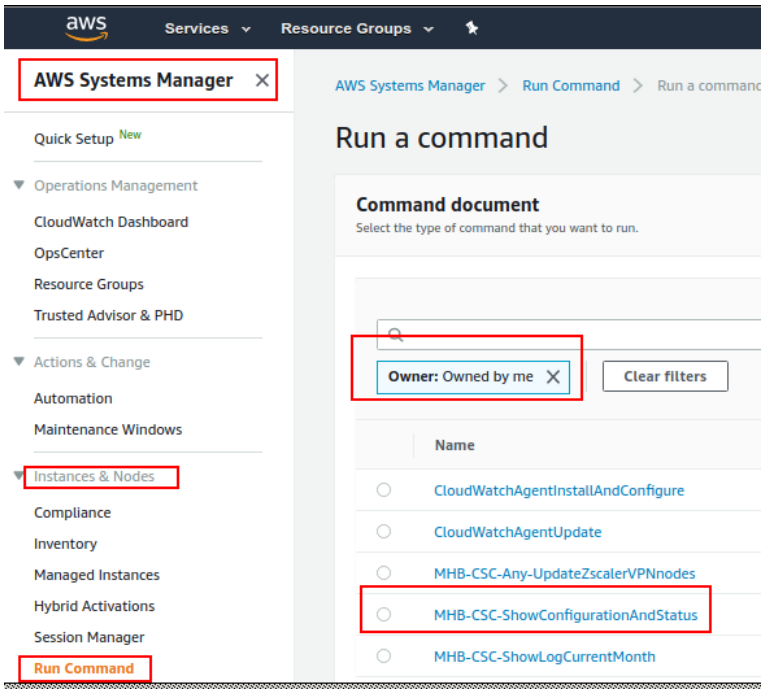
You can see the results of the operation on the “Output” section or to store the results on a S3 Buckets for further inspection.

Note: The “Output” Section allows only 2500 characters. The Traceroute and Latency Test uses more than 2500. We recommend to store this command on a S3 bucket directly.

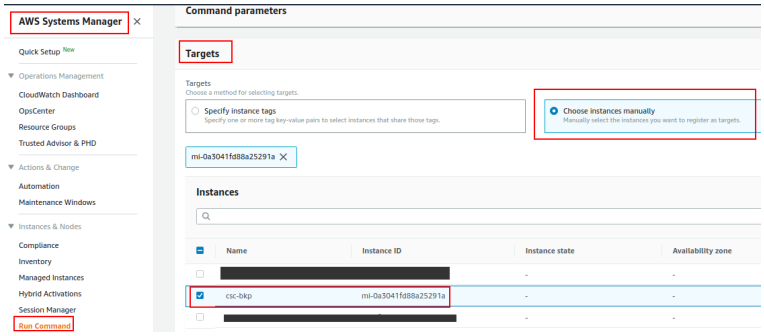
To Run Commands go to: AWS Systems Manager > Instances & Nodes > Run Command

Here an example of Running: MHB-CSC-ShowConfigurationAndStatus

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

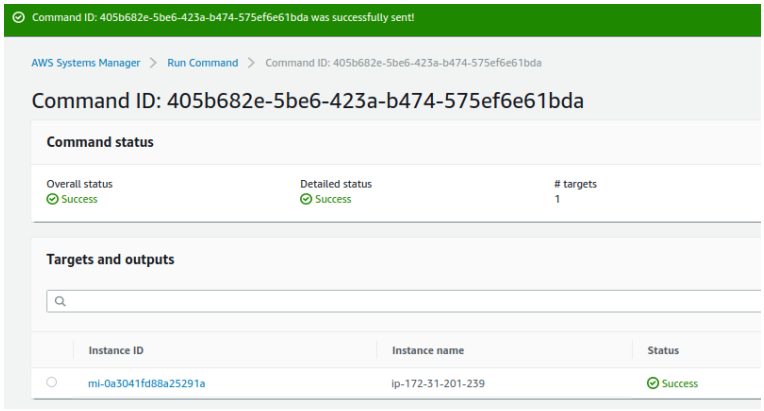


3. Scroll down and Select the Instances
4. We are selecting only one instance, but you can select as much as you want.

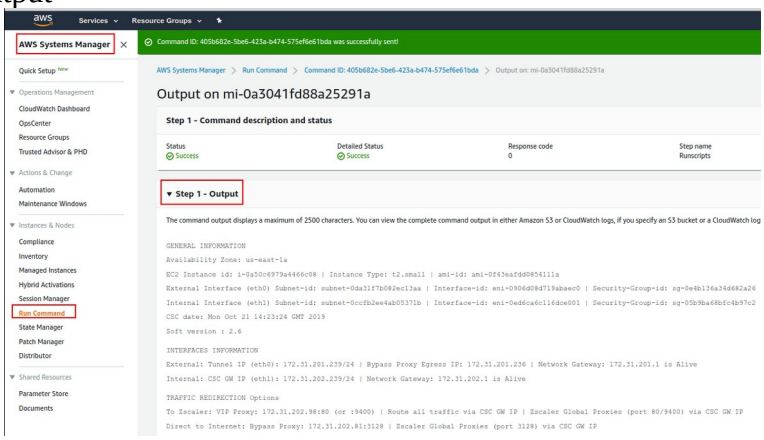


5. Click Run

Next Screen is:



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



10 Appendix C: Release Notes

10.1 Version 2.8

The version 2.8 comes with the following enhancements:

1. New! You can configure multiple Route Tables on High Availability.
2. New! OS base system is Ubuntu 18.04.4 LTS (bionic).
3. Updated “Configuration and Status” Menu.
4. Forced route to AWS DNS via eth1.

10.2 Version 2.7

The version 2.7 comes with the following enhancements:

5. New! “High Availability changing default route”. Now, you can configure a pair of CSC on High Availability to manipulate automatically the default route to internet via Zscaler.
6. Updated “Configuration and Status” Menu.
7. MTR (MyTraceRoute Test) now runs directly via TCP/80 to the ZEN Primary and Secondary. This avoid to enable incoming ICMP rules on security groups.

10.3 Version 2.6

The version 2.6 comes with the following enhancements:

1. Added to Wizard Configuration menu: From the Wizard you can change the Syslog Servers in addition to GRE tunnel IPs, DNS Servers and Bypass PAC URL.
2. New! Switch tunnels configuration wizard. In some circumstances, customers asked us an easy way to switch tunnels Primary / Secondary. Now is possible to do with a single command.
3. Logs to Syslog server. On version 2.6 you can setup one or two Syslog servers where to send the information about Tunnel Status.
4. Updated “Configuration and Status” Menu.