Maidenhead Bridge

Cloud Security Connector for AWS

Enabling Zscaler for AWS customers

Administrator Guide

Version 1.3

(August 2017)

Table of Contents

1 Introduction

The Cloud Security Connector (CSC) for AWS is an EC2 instance that allows to connect securely any AWS VPC subnet to Zscaler Cloud Security Services.

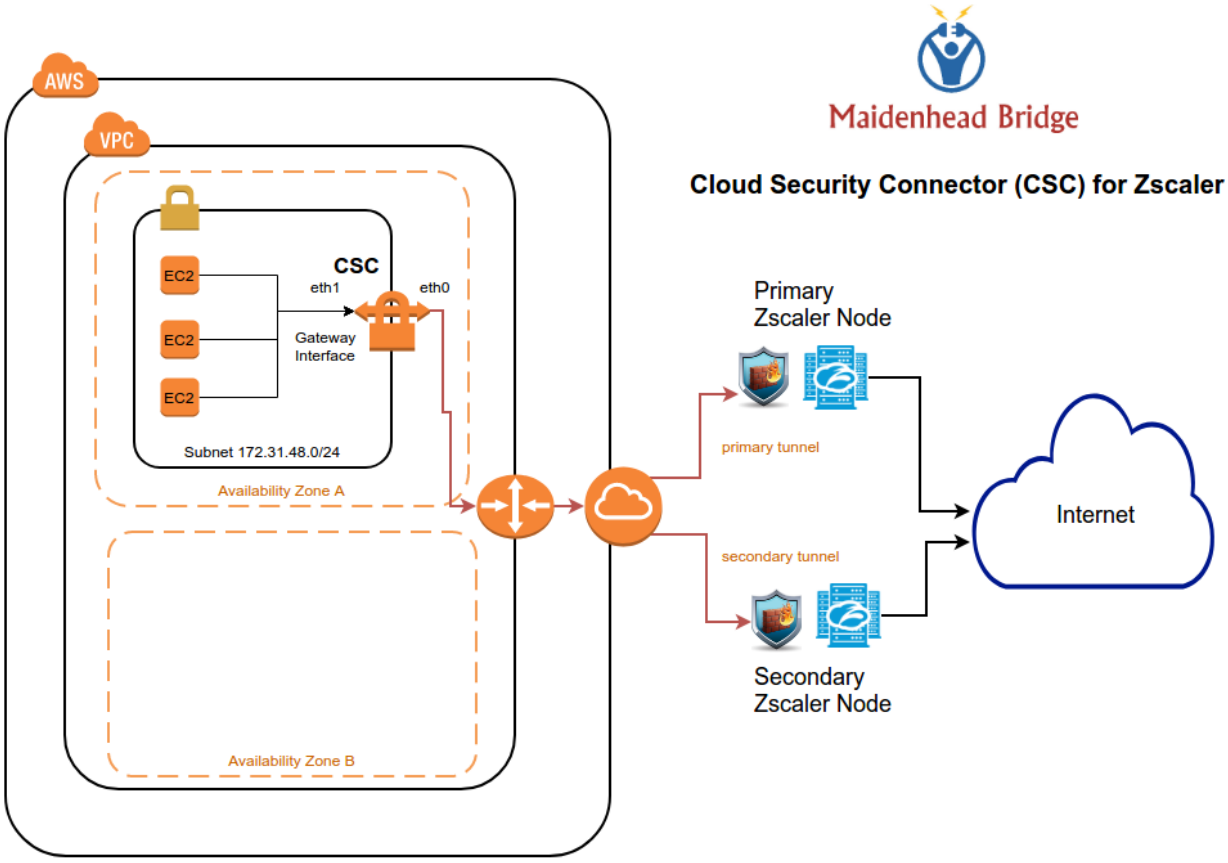
The CSC for AWS comes with all configuration required. You only need to ingress your VPN credentials: FDQN (Email) and Pre Shared Key. In addition to this, you can select the Zscaler nodes primary and secondary or to allow the CSC to select the best nodes automatically.

Simple to install and not further management required. The CSC will inspect the availability of the Zscaler nodes and will connect to the primary or secondary automatically.

All Zscaler functionalities are available. Internal IPs are completely visible on the Zscaler Gui.

2 The CSC on the AWS architecture

The following network diagram shows where the CSC is located inside the AWS architecture:



In this example, the CSC is connecting the Subnet 172.31.48.0/24 to the Zscaler primary and secondary.

As you can see on the image, eth0 is the “external” interface and eth1 the “internal” interface. In the following chapter we are explaining how to create and install the CSC for AWS.

3 Key benefits of the Cloud Security for AWS

- Enables to connect any AWS subnet to Zscaler Cloud Security Services.
- Full tunnel redundancy.
- Easy configuration: Just put your VPN credentials and select your primary and secondary nodes to connect.
- All parametrization required for AWS and Zscaler is already configured with the optimal values.
- All Zscaler functionalities can be used: Firewall and Web Security.
- Full visibility of internal IPs.
- No operational burden for Administrators.
- No configuration required on your Instances. Just create the proper AWS route table and point the GW to the CSC’s interface.
- It runs on a cheap AWS instance: m3.medium

4 Connecting your Subnet to Zscaler Cloud Security

In this chapter, we are going to explain step by step how to connect your AWS to Zscaler Cloud Security.

4.1 Step 1: Create your VPN credentials and Location on the Zscaler GUI.

Go to the Zscaler GUI

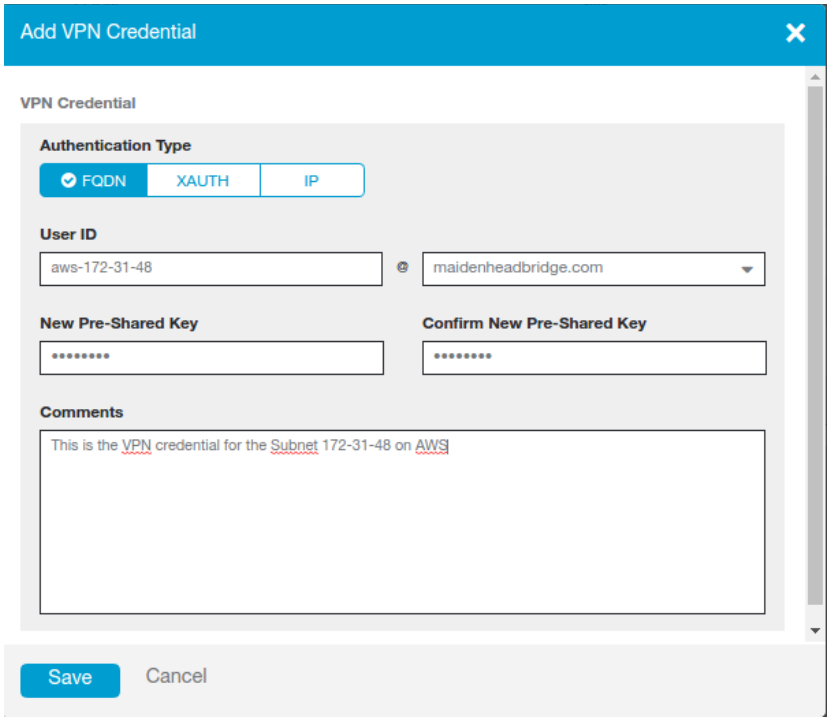
4.1.1 VPN Credentials

From Zscaler Support page: https://help.zscaler.com/zia/how-do-i-add-individual-vpn-credentials

To to add a VPN credential:

1. Go to **Administration** > **Resources** > **VPN Credentials**.
2. Click **Add VPN Credential**.
3. **Authentication Type:** Choose one of the following that will be used to identify the peer, and configure accordingly:
   - FQDN
     - **User ID:** Enter the FQDN of the peer.
     - **New Pre-Shared Key:** Enter a pre-shared key.
     - **Confirm New Pre-Shared Key:** Re-enter the pre-shared key.
     - **Comments:** Optionally, enter additional notes or information. The comments cannot exceed 10,240 characters.

Example on the GUI:



IMPORTANT: This values will be requested to configure the CSC.

In this example the values are:

FDQN (Email) = aws-172-31-48@maidenheadbridge.com

Pre Shared Key (PSK) = 12345678

4.1.2 Location

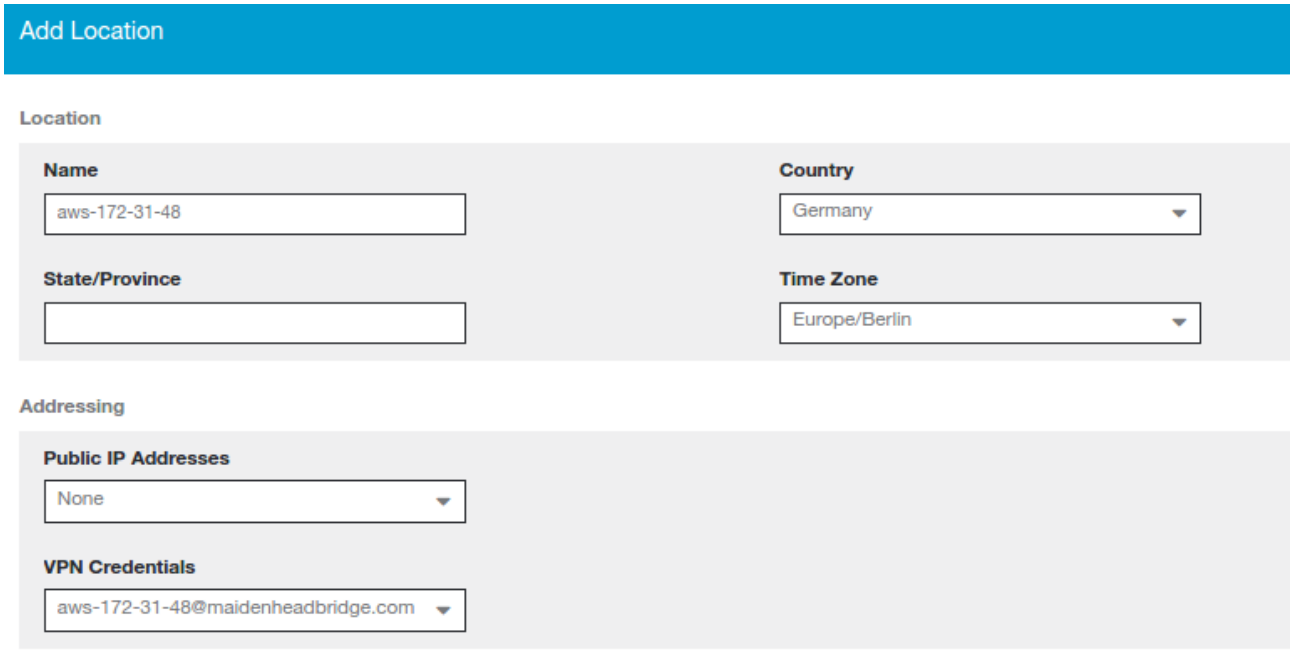
Now, it is time to create the Zscaler “Location” and to associate the VPN credentials to it.

From Zscaler support page: https://help.zscaler.com/zia/how-do-i-configure-ipsec-vpn-tunnels

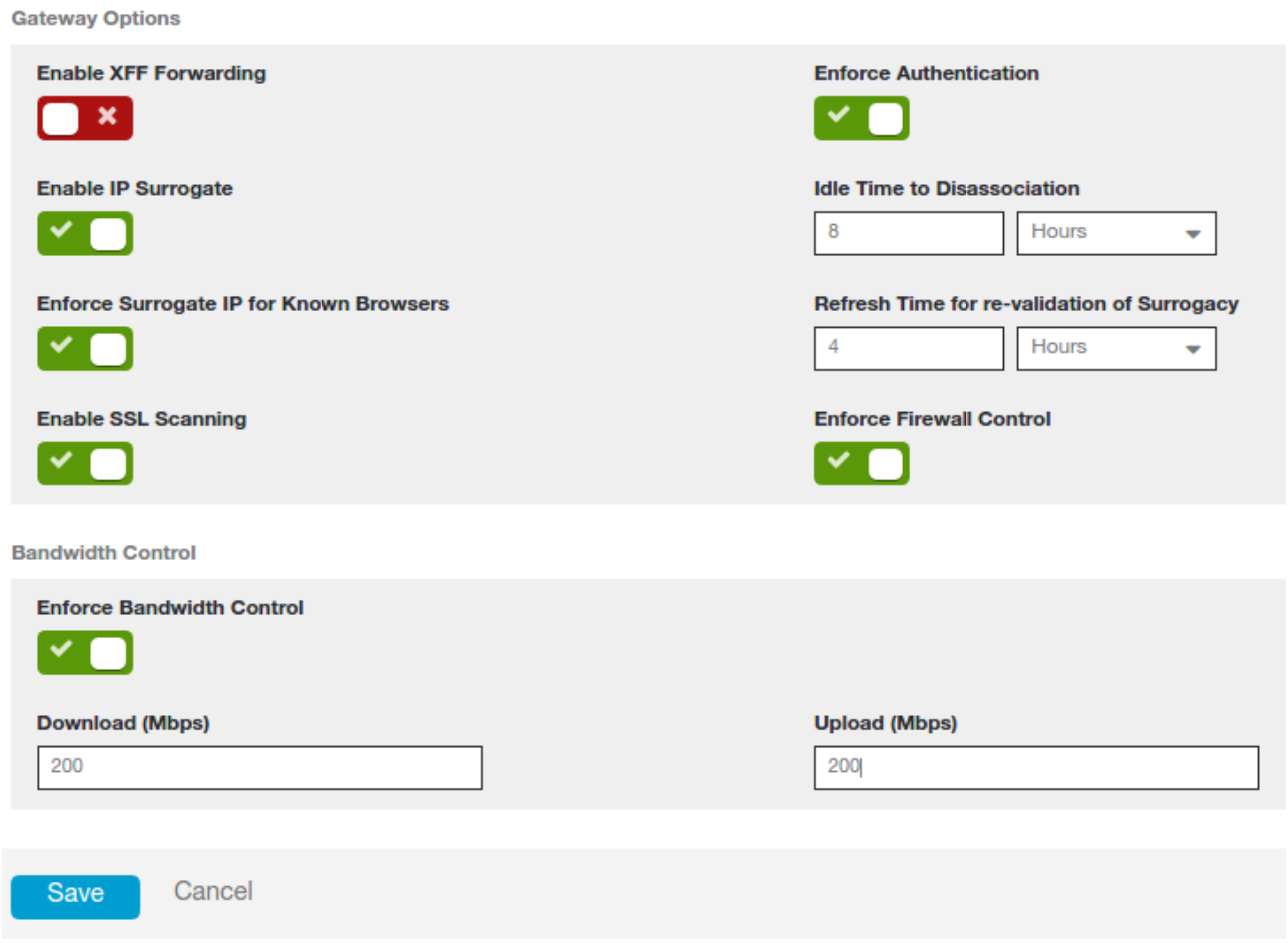
3. Link the VPN credentials to a location.
   Log in to the admin portal and do the following:

   1. Go to **Administration** > **Resources** > **Locations**.
   2. Add or edit a location.
   3. From the **VPN Credentials** menu, choose the IP address or FQDN.
   4. Click **Done** to exit the dialog.
   5. Click **Save** and activate the change.

Example on the GUI:



and add you Gateway options. There is not restriction of functionalities with the CSC. You can use all. In this example, I will enable everything except to XFF.



IMPORTANT: Zscaler has a limit of 200 Mbps per tunnel Ipsec. This is the maximum bandwidth available. This is a limitation of Zscaler and not of the CSC.
Anyway, Zscaler has not limits in the amount of Locations. You can create as much as you want. As design strategy you can group your devices on subnets that will not require more than 200 Mbps and to install a CSC on each one.

IMPORTANT: Check your Zscaler license in order to validate if you have SSL scanning and/or Bandwidth Control available.

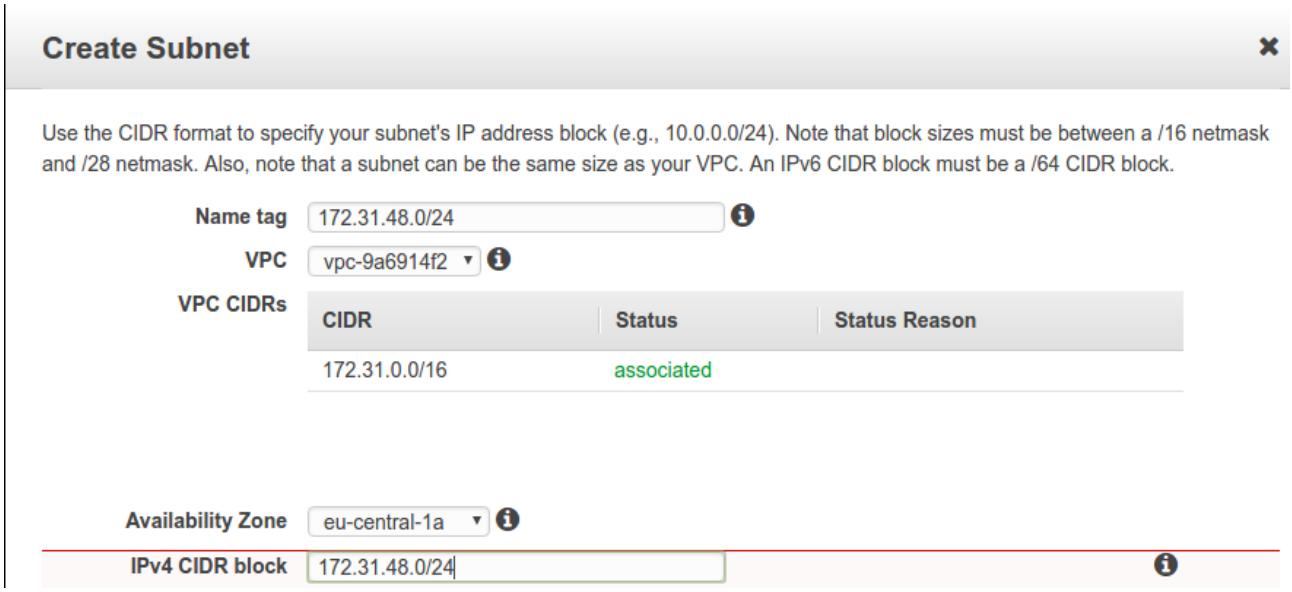
4.2 Step 2: AWS configuration for CSC instance.

Please, review the networks diagram of item 2). We will use it as example. In the network diagram we are going to connect the subnet 172.31.48.0/24 to the Zscaler Cloud Security service.

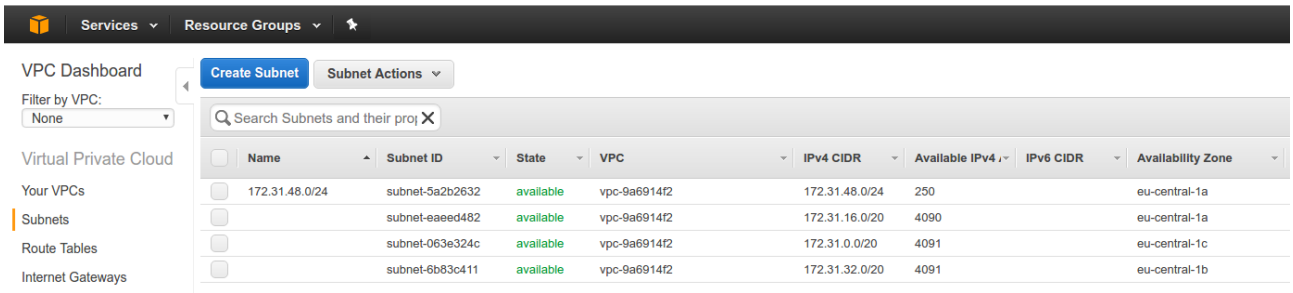
Now, go to Amazon AWS console and follow the next steps.

4.2.1 Create you internal subnet (if it does not exist)

Normally the internal subnet is already created and the instances are running on it, but just in case you are starting from scratch, here is the example:



Go to your VPC Dashboard > Subnets and “Create Subnet”



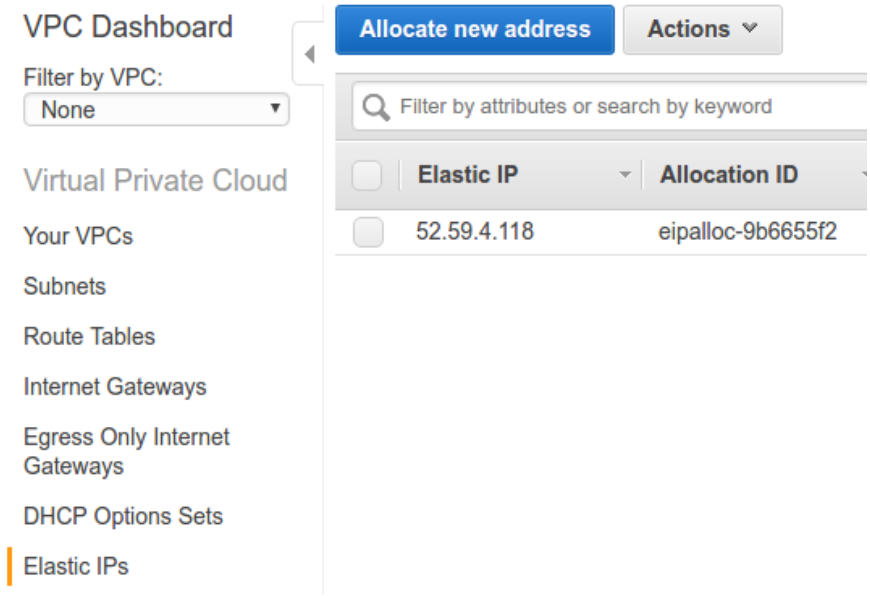
This is my list of Subnets at his point:

IMPORTANT: Please, take a look of the “Availability Zone”. In this case, we are using eu-central-1a. The CSC will have the “internal” (eth1) interface connected to this Subnet (172.31.48.0/24) created and the “external” (eth0) to the 172.31.16.0/20 that is also on the same Availability Zone.

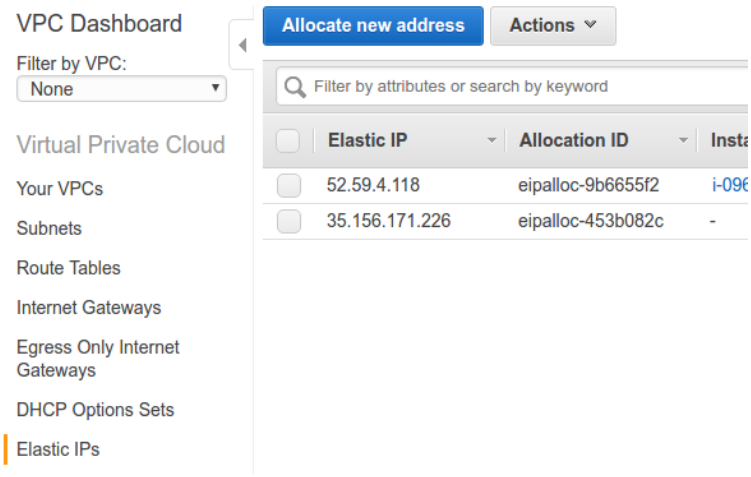
4.2.2 Create a new “Elastic IP”

This Elastic IP will be the public IP associated to the external (etho) interface of the CSC.

Go to you VPC Dashboard > Elastic IP



1. Click “Allocate New Address”
2. Click “Allocate”
3. Click “Close”
4. You will be able to see the new address:



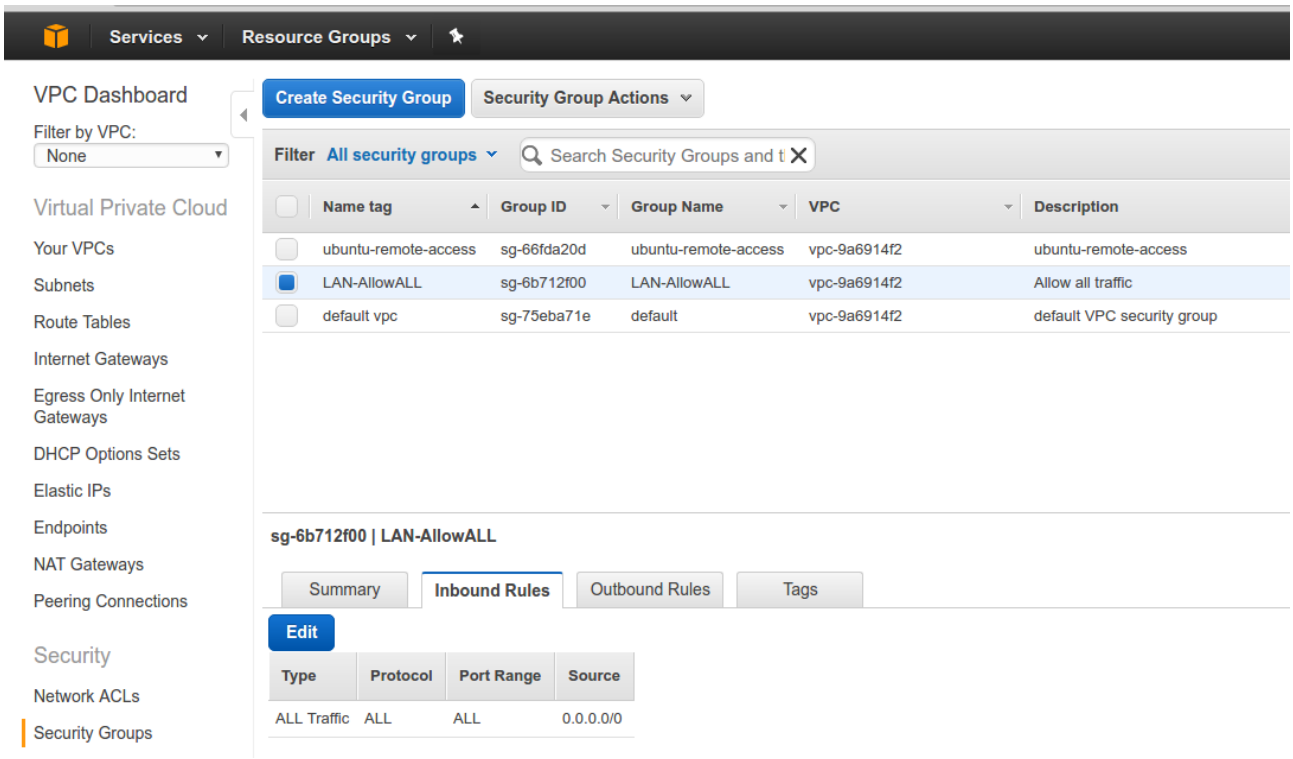
In this case, the address allocated is: 35.156.171.226.

4.2.3 Create the “Security Groups”: Internal and External

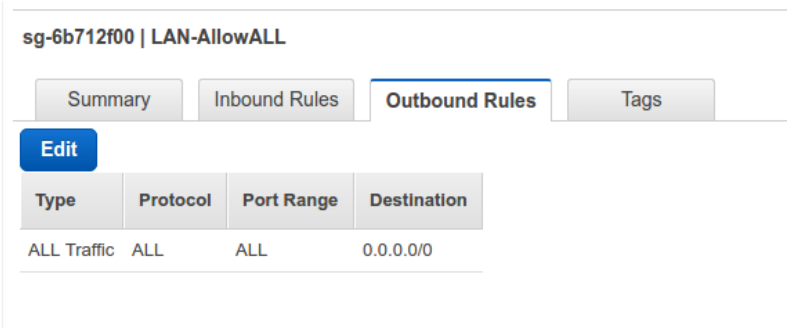
The next task is to create the Security Groups that will be applied to the internal and external interface of the CSC.

4.2.3.1 Internal Security Group

The Internal Security group in this example, allows ALL inbound and outbound communications. It is acting like a “physical LAN segment”.



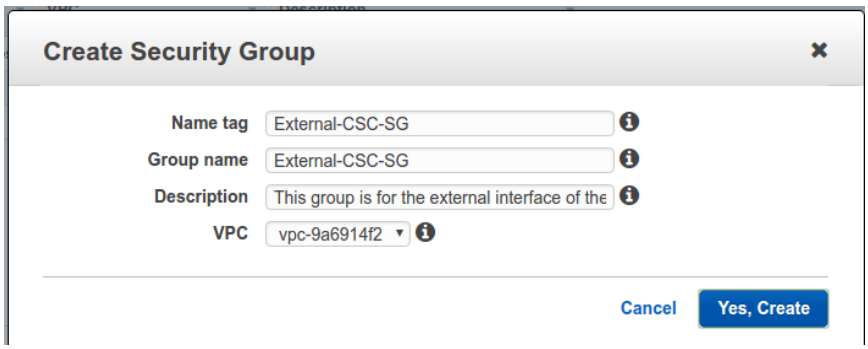
And here the detail about “Outbound Rules”



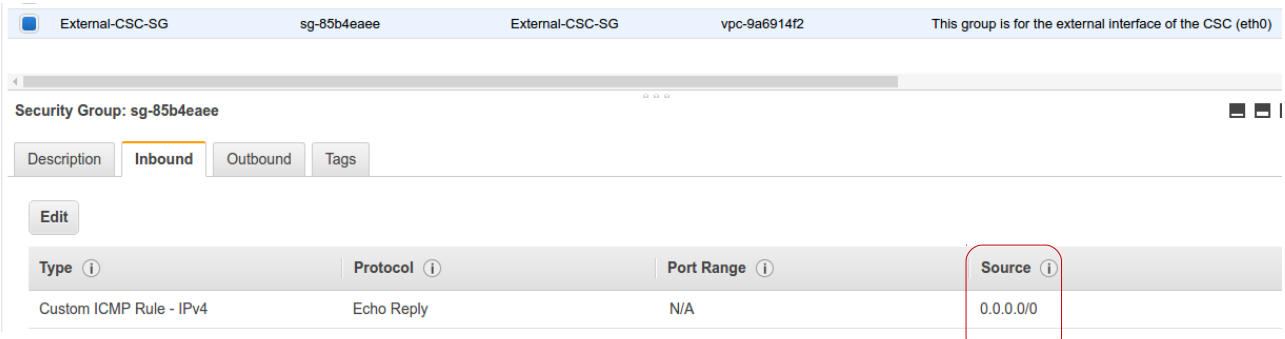
4.2.3.2 External Security Group

This Security Group will be created in order to allow the only communications required by the CSC to the Internet.

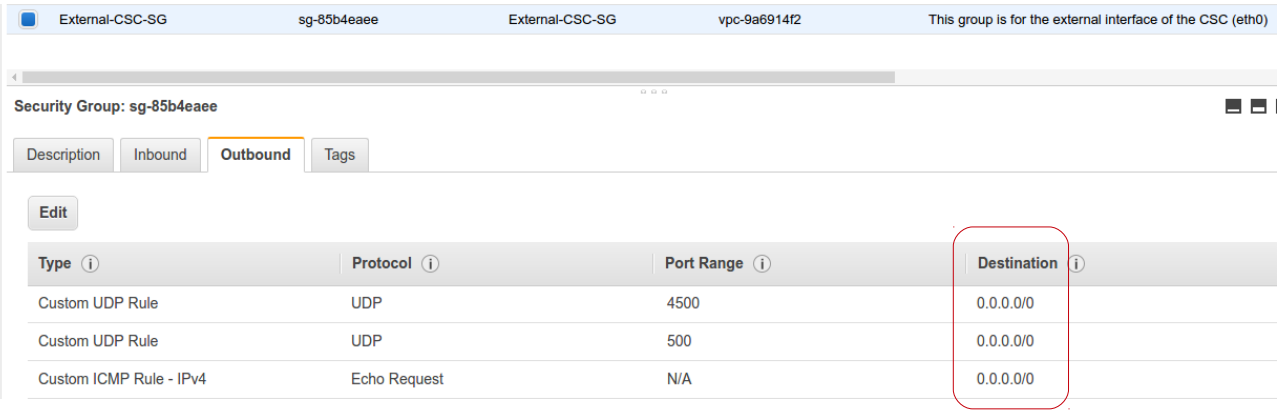
1. Click on “Create a Security Group”
2. Put a name and description



3. Click, “Yes, Create”
4. Select the Group and Edit “Inbound Rules”
5. Add the following rule:



6. Select “Outbound Rules” and add the following rules:



IMPORTANT: We are going to come back later to edit again this rules to specify the Source (Inbound Rules) and Destination (Outbound Rules) after the Zscaler Nodes are selected.

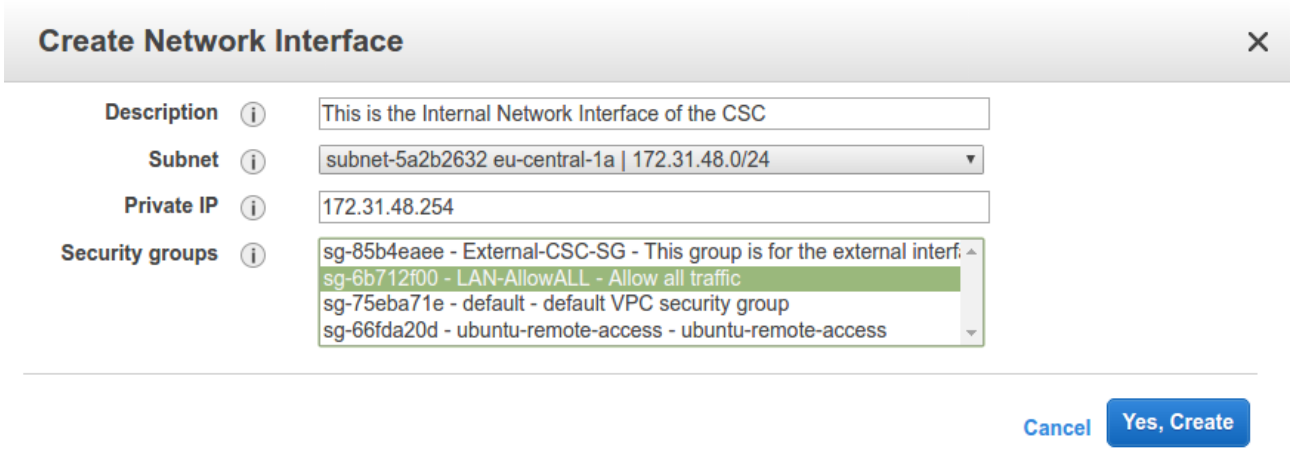
4.2.4 Create the Network Interfaces: Internal and External

The next task is to create the Network interfaces.

4.2.4.1 Internal Network Interface

1. Go to EC2 Dashboard > Network and Security > Network Interfaces

2. Click “Create Network Interface”
3. Fill the fields:

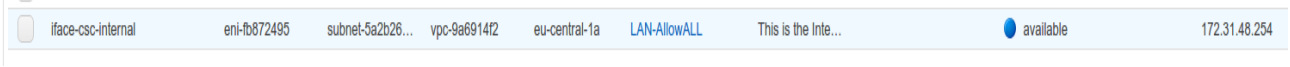


IMPORTANT: Note the following:

- The Subnet selected is the Internal Subnet created on point 4.2.1
- The Private IP can be auto assigned. Due to this will be the Gateway to the Internal Subnet 172.31.48.0/24, we recommend to setup a fix value, like 172.31.48.254 that is available. (the value 172.31.48.1 is reserved by AWS as standard default GW and cannot be used.)
- The Security Group selected is the one created on point 4.2.3.1

IMPORTANT:

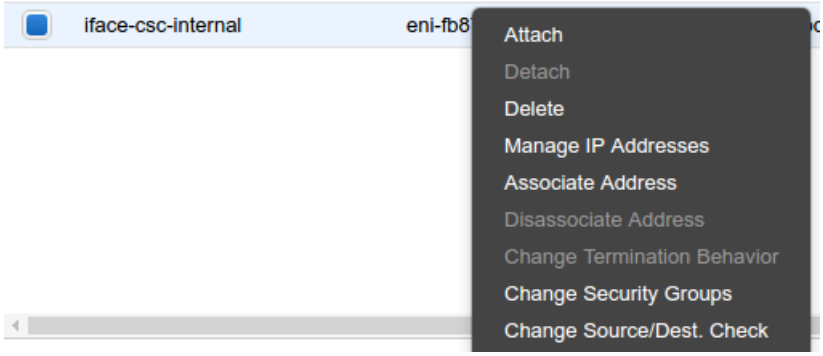
Finally, put a **Name** to this interface.



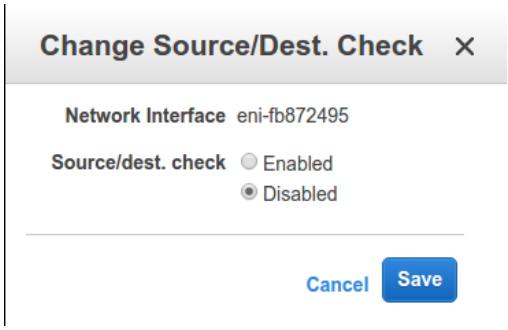
We called it: **iface-csc-internal**

4.2.4.2 Disable Source / Destination Check on Internal Interface

1. Select iface-csc-internal.
2. Right Click and select “Change Source/Dest. Check”



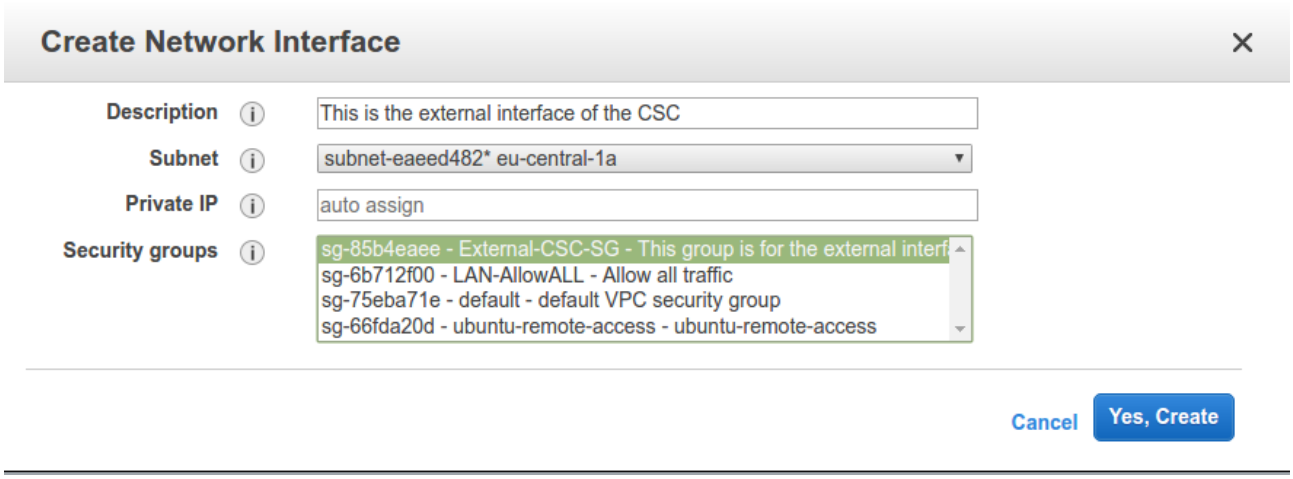
3. Disable Source / Dest. Check:



4. Click “Save”

4.2.4.3 External Network Interface

1. Click ““Create Network Interface”
2. Fill the fields:

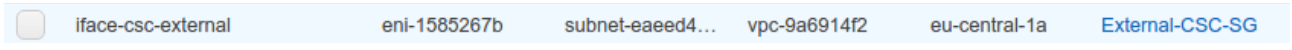


IMPORTANT:

- The subnet selected is the VPC default subnet for Availability Zone: eu-central-1a. Same Availability Zone than our previous created internal interface.
- Leave the IP on “auto assign”
- The Security Group Selected is the External Security Group created on point 4.2.3.2

IMPORTANT:

Finally, put a **Name** to this interface.

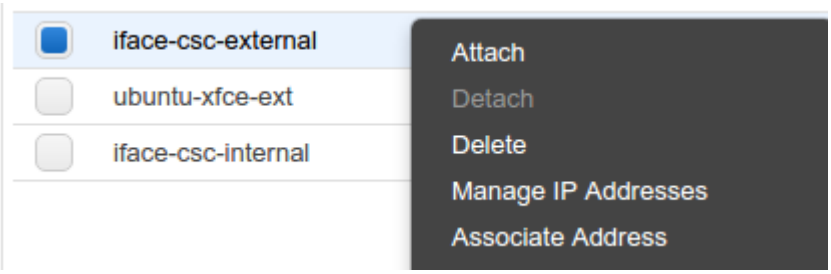


We called it: **iface-csc-external**

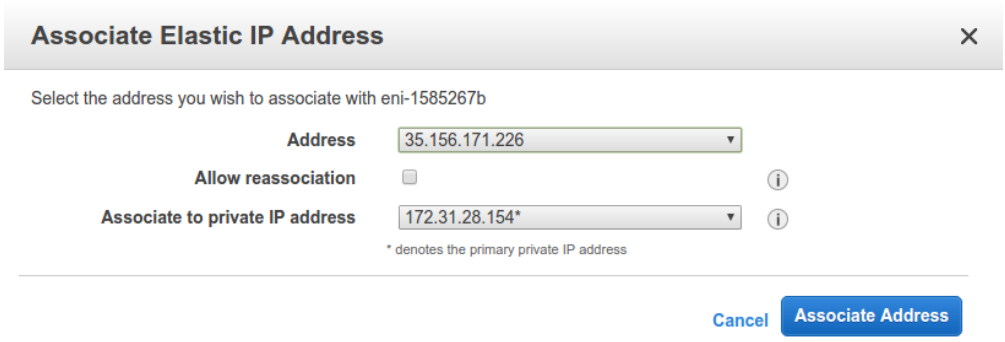
4.2.5 Associate the Elastic IP to the External Interface:

The next task is to associate the recently External Interface create to the Elastic IP created on point 4.2.2

1. Select the interface “iface-csc-external”



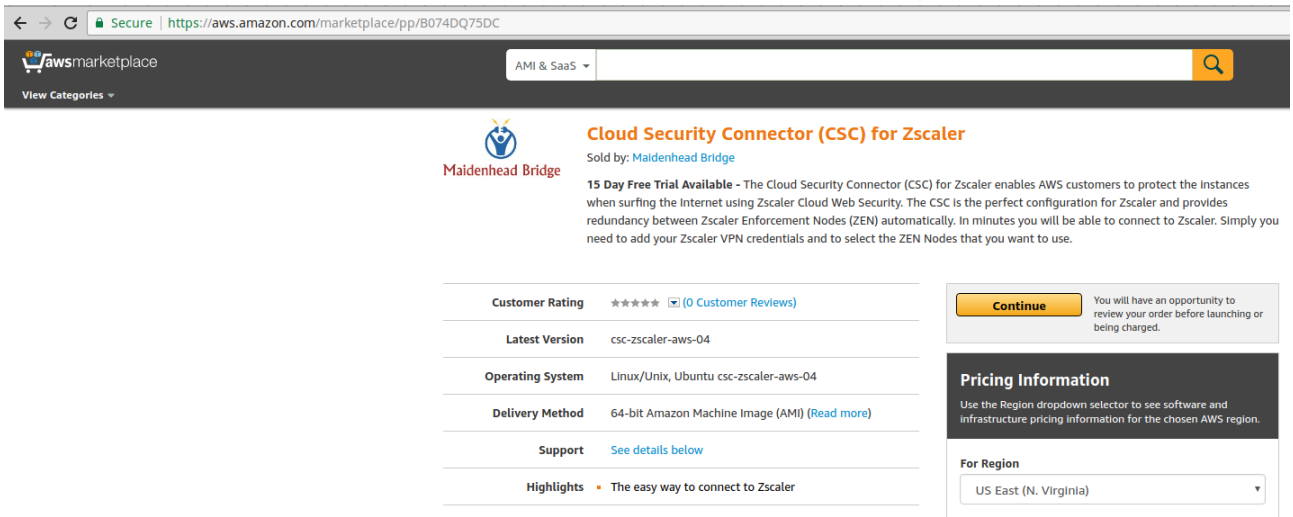
2. Right Click and click : Associate Address. Select the Elastic IP created:



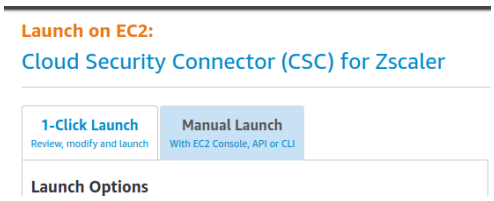
3. Click, “Associate Address”

4.2.6 Launch the CSC instance:

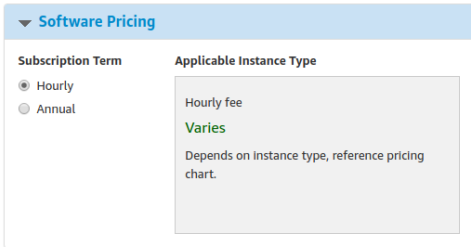
1. Go to the AWS Marketplace and search for Maidenhead Bridge



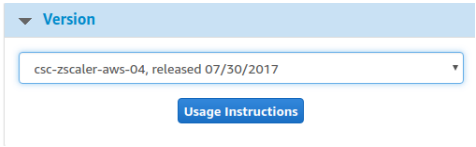
2. Click “Continue”
3. Select “Manual Launch”



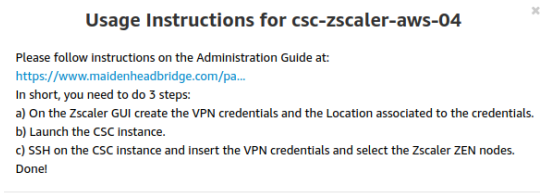
4. Go down the page and select your “Software Pricing” (Hourly or Yearly)



5. Select “Software Version”

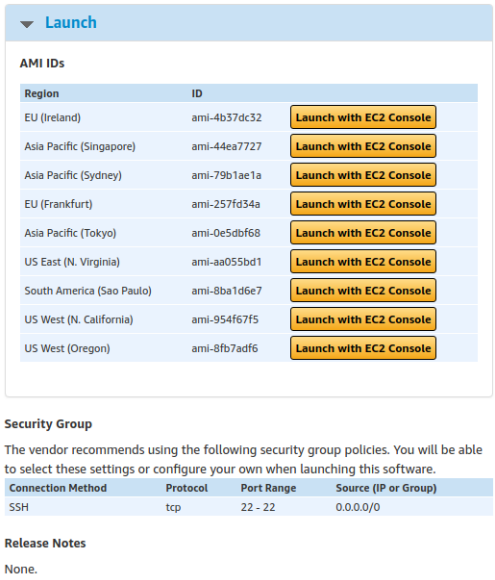


Note: If you click “Usage Instructions” the following message appears:



The link redirect to this Administrator Guide.

6. Select the Region that you want to launch the instance:

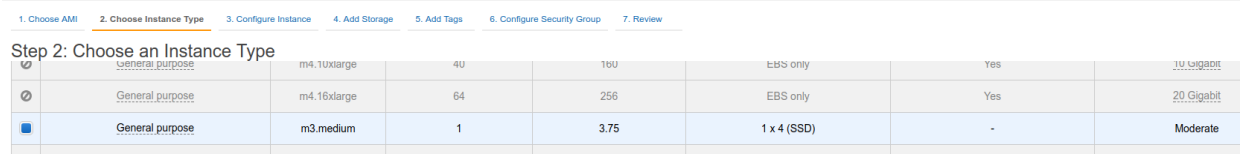


In this example we are going to select EU (Frankfurt)

Note: Leave the Security Group as is. We are going to modify it later.

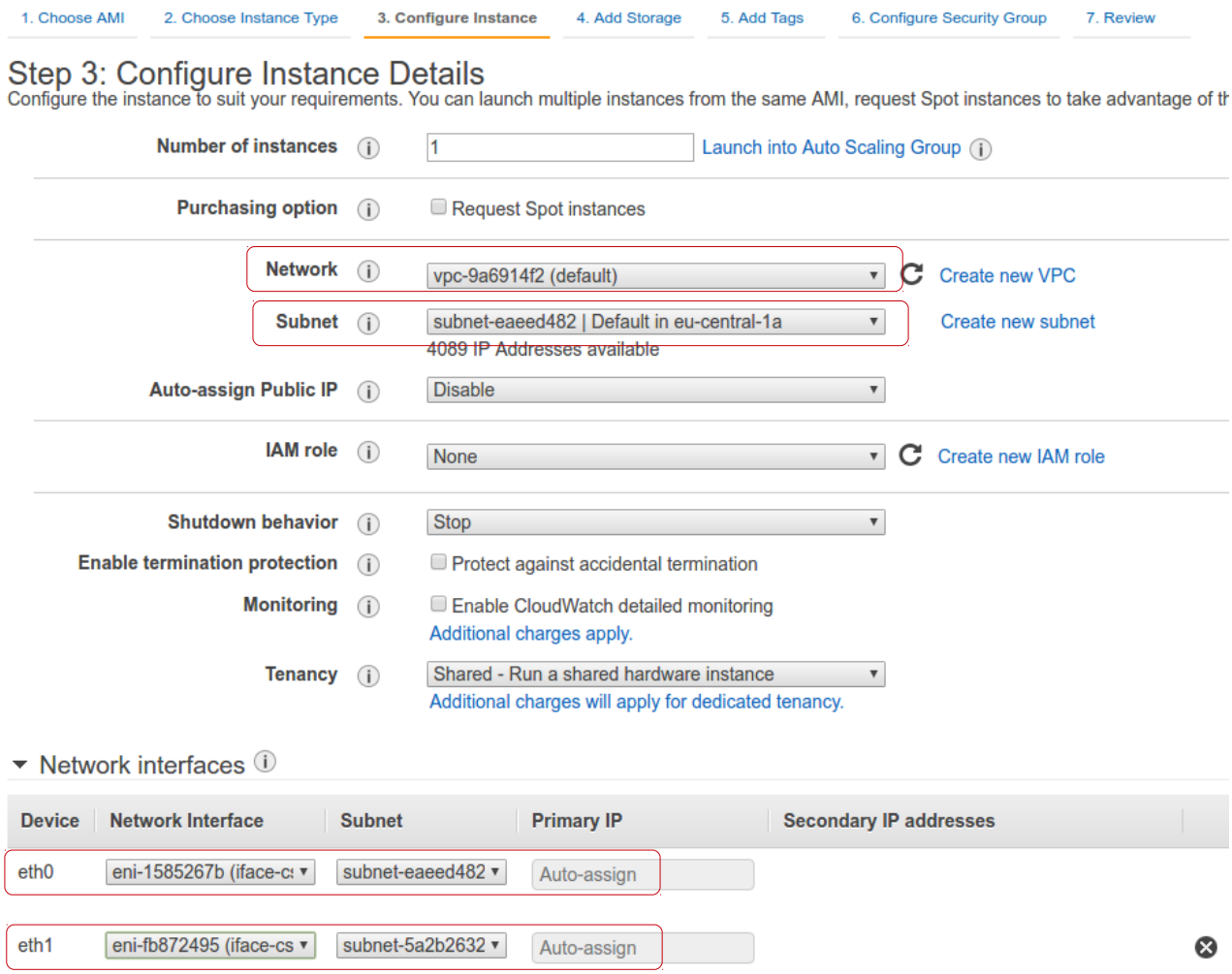
7. Choose Instance type:

The CSC is very frugal in terms of CPU and Memory resources but we need to select an instance type that has “Moderate” network performance. The smallest (and cheaper) one is the m3.medium



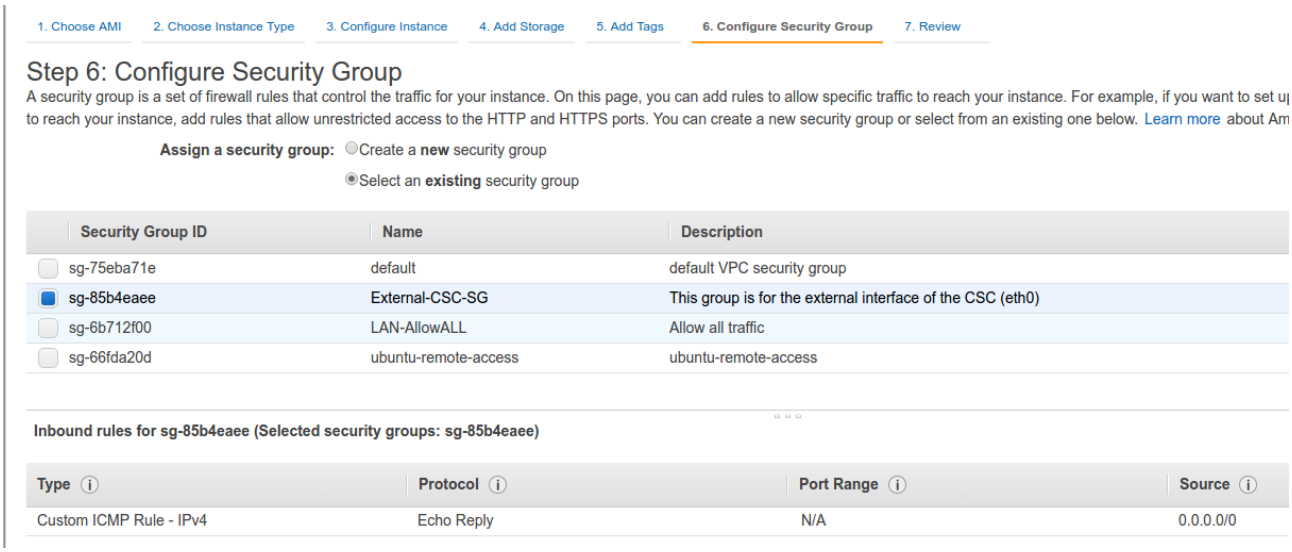
8. Click at the bottom right: “Next: Configure instance details”

9. Please, note the following changes:

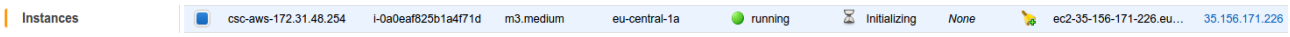


IMPORTANT:
Network: default VPC was selected. Pay attention if you have more than one VPC.
Subnet: This is the default Subnet of the VPC ***(Check the availability Zone selected!!!)***
eth0: the interface iface-csc-external was selected for eth0
eth1: eth1 was added and the iface-csc-internal was selected.

10. Click: Review and Launch.
11. On the next screen you will see that the Security Group is not correct. Please, click on “Edit Security Group”
12. Select existing and click on the External Security Group created.



13. Click review and launch.
14. Note : you will receive a message that not SSH from outside from enabled. The reason of this is because the CSC will be accessed from the internal subnet.
15. Click Launch. (Ignore warning messages about “you are open...” we are going to correct this is next steps.
16. Select existing Key Pair or create a new one.
17. Launch instance. Go to View instance:
18. Put a Name to the CSC. We called csc-aws-172.31.48.254



19. As you can observe, the Elastic IP associated is showed now.

4.3 Step 3: Configure the CSC

The CSC configuration is very easy to do. Just execute step 1, 2 and 3 of the menu: Admin Tasks.

Ssh on to the CSC ***from an internal machine located on the internal subnet*** using your own certificate:

Ssh -i <yourcertificate.pem> **cscadmin**@<eth1 ip>

Note: the default username is "**cscadmin**"

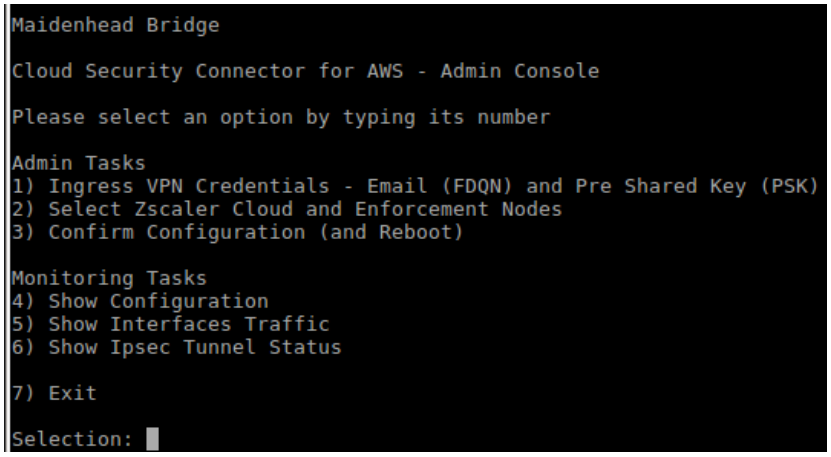
In this example the values are:

eth1 IP: 172.31.48.254

certificate: csc-254.pem

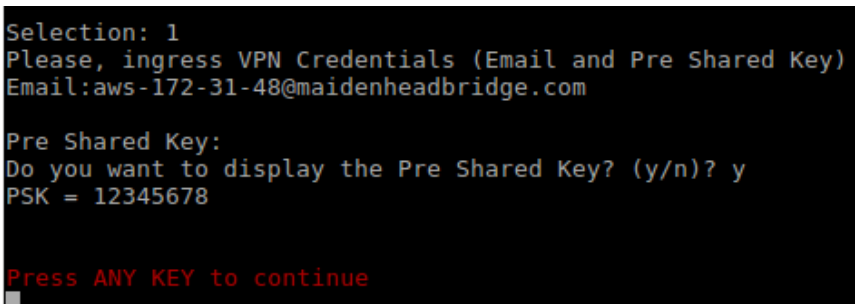
username (always use this): **cscadmin**

SSH command: ssh -i csc-254.pem **cscadmin**@172.31.48.254



1. Select 1) Ingress VPN Credentials - Email (FDQN) and Pre Shared Key (PSK). This are the VPN credentials created on the Zscaler GUI. (point 4.1.1)

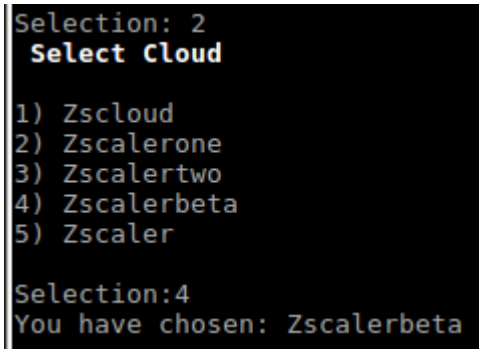
The values on our example are:



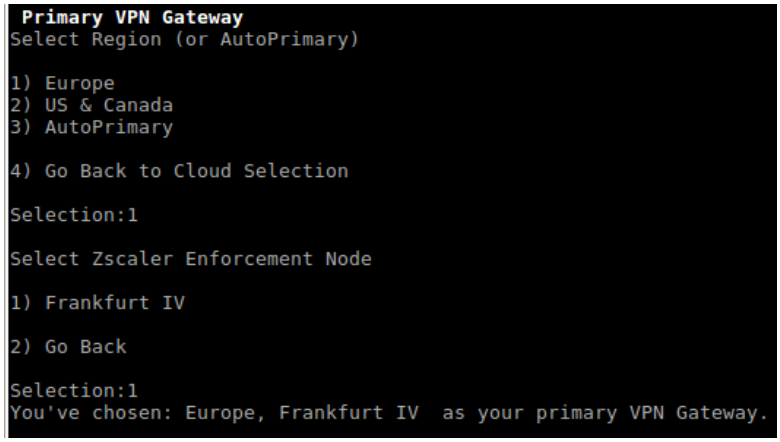
2. Select Zscaler Cloud and Enforcement Nodes

IMPORTANT: After selecting the Zscaler Cloud you can select the nodes manually or automatically. (AutoPrimary / AutoSecondary).

A) Select the Cloud:



B) Select your primary Zscaler Enforcement Node (or AutoPrimary)



C) Select your secondary Zscaler Enforcement Node (or AutoSecondary)

3. Confirm Configuration (and Reboot)

```
Selection: 3

Validating Configuration

Your Cloud is: Zscalerbeta

Checking Node Frankfurt IV hostname fra4-vpn.zscalerbeta.net
Hostname fra4-vpn.zscalerbeta.net has IP 165.225.72.39
Node Frankfurt IV is Alive

Checking Node Washington DC hostname was1-vpn.zscalerbeta.net
Hostname was1-vpn.zscalerbeta.net has IP 104.129.194.39
Node Washington DC is Alive

Your VPN credentials are:

Email: aws-172-31-48@maidenheadbridge.com

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

Are this values correct? (y/n)? y
The system will be configured and rebooted
Connection to 172.31.48.254 closed by remote host.
Connection to 172.31.48.254 closed.
ubuntu@ip-172-31-26-56:~$
```

In this steps we are validating that the nodes selected are alive and the values of the credentials. Ingress “y” if the values are correct and the CSC will be rebooted. If you select “n” you will be redirected to the main menu again.

IMPORTANT: Please, take note of the IPs of the Nodes Selected. (In this example are 165.225.72.39 and 104.129.194.39). This IPs will be configured later on the Security Group External. You can view this IP on menu 4) Show Configuration

4.3.1 Checking your connection to Zscaler from the CSC

After the reboot, SSH again on to the CSC and check that the VPN connection is established, selecting 6) Show Ipsec Tunnel Status

```
Selection: 6

Your ZEN Nodes are:

primary: Frankfurt IV
secondary: Washington DC

The Node active is the: primary

IPsec uptime: 15 seconds, since Jul 20 13:56:57 2017
Last Security Association: ESTABLISHED 12 seconds ago, 172.31.28.154[aws-172-31-48@maidenheadbridge.com]...165.225.72.39[165.225.72.39]

Press ANY KEY to continue
```

Good work! You are connected to Zscaler.

This option shows your nodes primary and secondary, the node active (primary in this case), the uptime of the Ipsec service and the Last Security Association.

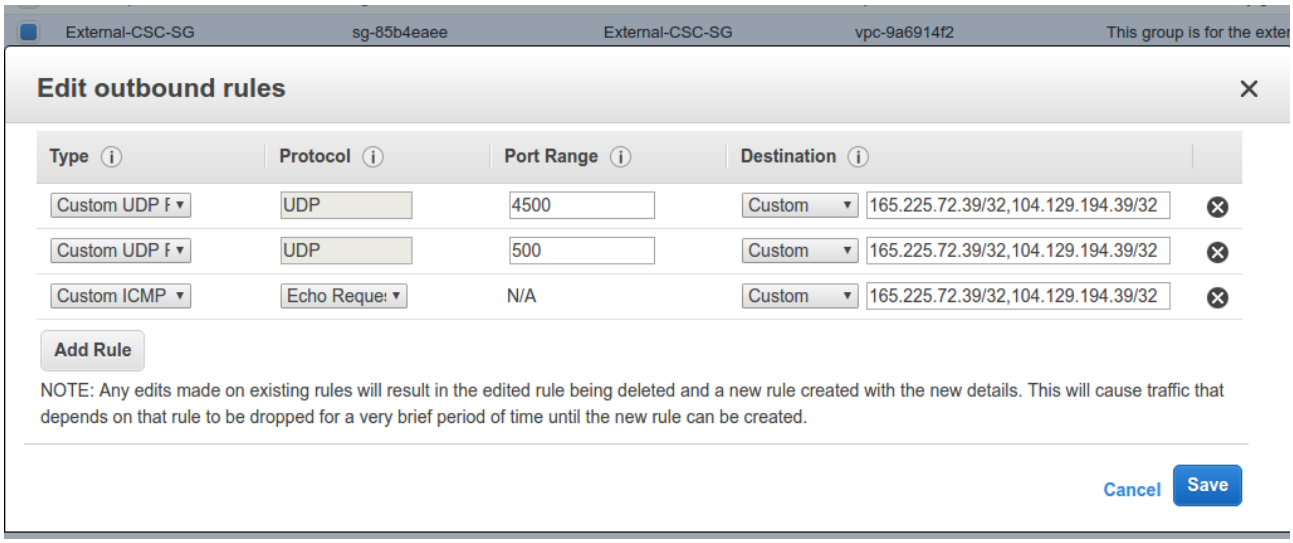
4.3.2 Adding the IPs of the Zscaler Nodes to the Security Group External

On Menu 4) Show Configuration, you can see the IPs of the Zscaler Nodes.

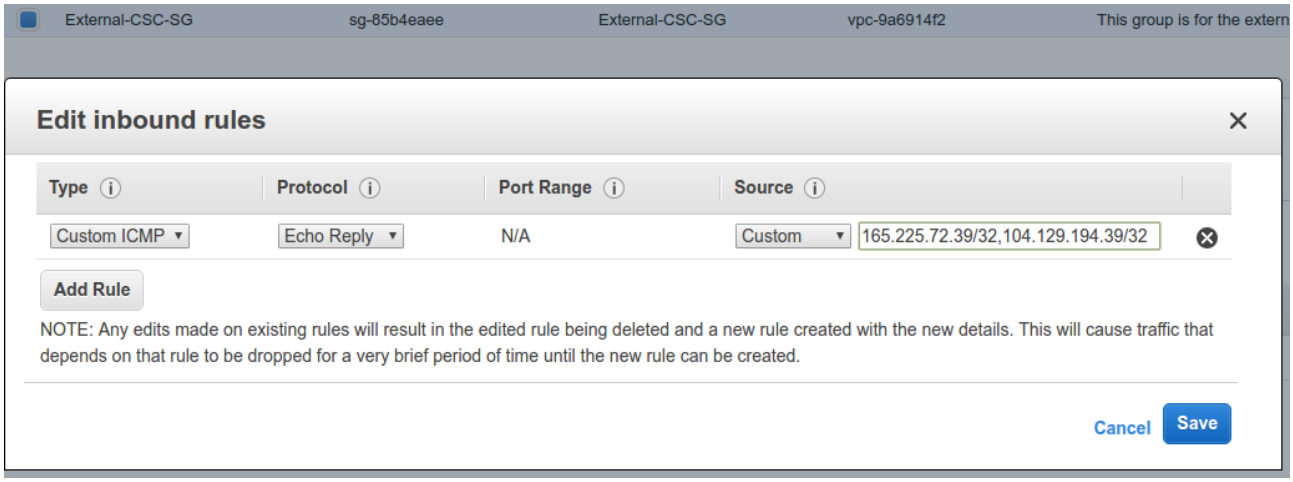
```
Selection: 4

AWS information
AWS Instance ID: i-0988b04ff2817fd50
AWS Availability Zone: eu-central-1a

Zscaler information
Zscaler Cloud:  Zscalerbeta
Primary ZEN node: Frankfurt IV | Hostname: fra4-vpn.zscalerbeta.net | IP: 165.225.72.39
Secondary ZEN node: Washington DC | Hostname: was1-vpn.zscalerbeta.net | IP: 104.129.194.39

Interfaces information
Internal Interface (eth1) IP: 172.31.48.254 | ID: eni-fb872495 | Security Group: LAN-AllowALL
External Interface (eth0) IP: 172.31.28.154 | ID: eni-1585267b | Security Group: External-CSC-SG

VPN Credentials information
Email: aws-172-31-48@maidenheadbridge.com

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

Please, add the Primary ZEN and Secondary ZEN in the Inbound and Outbound rules of the Security Group External

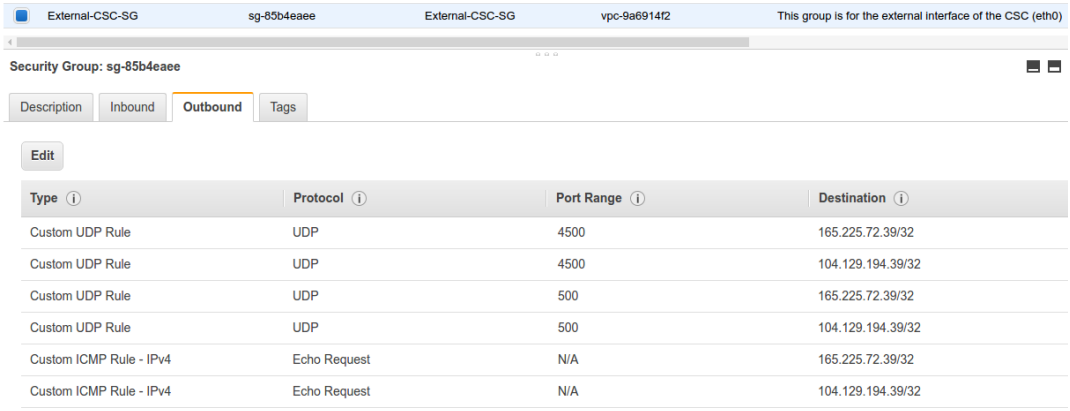
Edit your Inbound and Outbound. Here an example of editing Outbound:



Do the same for Inbound.



Your External-CSC-SG should look like this:



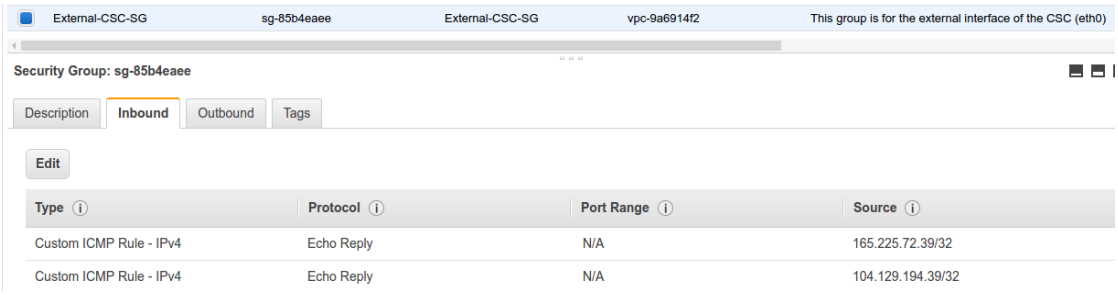
External-CSC-SG | sg-85b4eaee | External-CSC-SG | vpc-9a6914f2 | This group is for the external interface of the CSC (eth0)

Security Group: sg-85b4eaee

Description | Inbound | **Outbound** | Tags

Edit

Type	Protocol	Port Range	Destination
Custom UDP Rule	UDP	4500	165.225.72.39/32
Custom UDP Rule	UDP	4500	104.129.194.39/32
Custom UDP Rule	UDP	500	165.225.72.39/32
Custom UDP Rule	UDP	500	104.129.194.39/32
Custom ICMP Rule - IPv4	Echo Request	N/A	165.225.72.39/32
Custom ICMP Rule - IPv4	Echo Request	N/A	104.129.194.39/32



External-CSC-SG | sg-85b4eaee | External-CSC-SG | vpc-9a6914f2 | This group is for the external interface of the CSC (eth0)

Security Group: sg-85b4eaee

Description | **Inbound** | Outbound | Tags

Edit

Type	Protocol	Port Range	Source
Custom ICMP Rule - IPv4	Echo Reply	N/A	165.225.72.39/32
Custom ICMP Rule - IPv4	Echo Reply	N/A	104.129.194.39/32

and finally check the connectivity to Zscaler again:

```
6) Show Ipsec Tunnel Status

7) Exit

Selection: 6

Your ZEN Nodes are:

primary: Frankfurt IV
secondary: Washington DC

The Node active is the: primary

IPsec uptime: 25 hours, since Jul 20 13:56:56 2017
Last Security Association: ESTABLISHED 5 hours ago, 172.31.28.154[aws-172-31-48@maidenheadbridge.com]...165.225.72.39[165.225.72.39]
```

Done! You are connected to Zscaler!

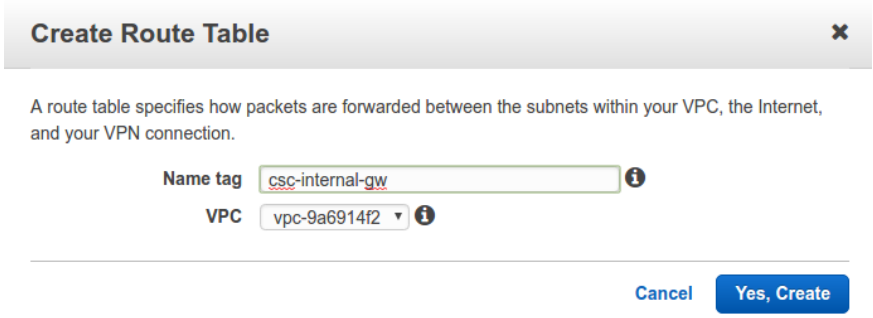
5 Using Zscaler from your internal devices

In this chapter we will setup the CSC as default Gateway and to review some utilities provided by Zscaler to verify that everything is working properly

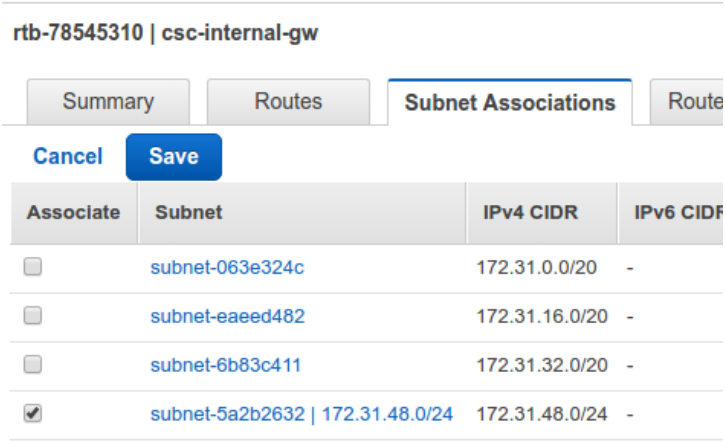
5.1 Create “Route Tables” for Internal Subnet.

We are going to create a Route Table for the Internal Subnet indicating that the default route to internet will have the Internal Interface of the CSC as default Gateway.

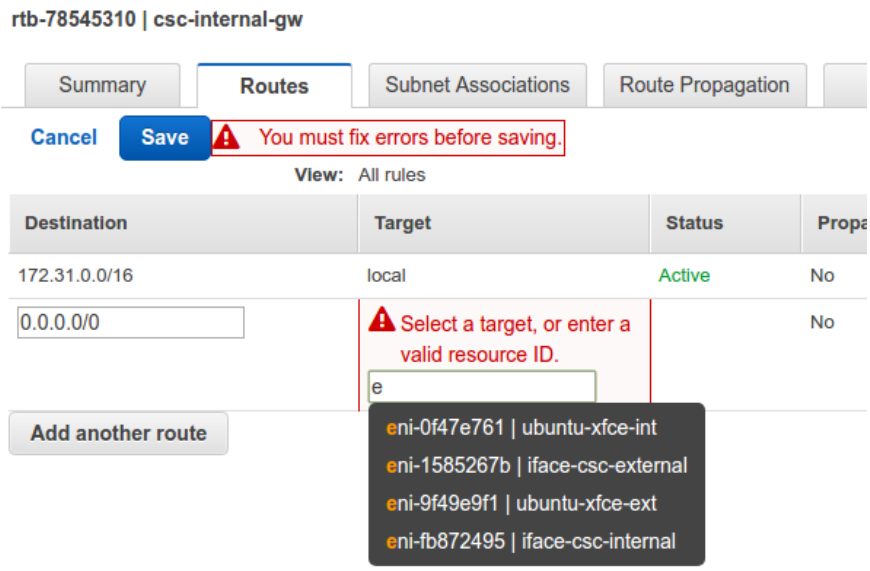
1. Go to VPC Dashboard > Router Tables
2. Click “Create a Route”



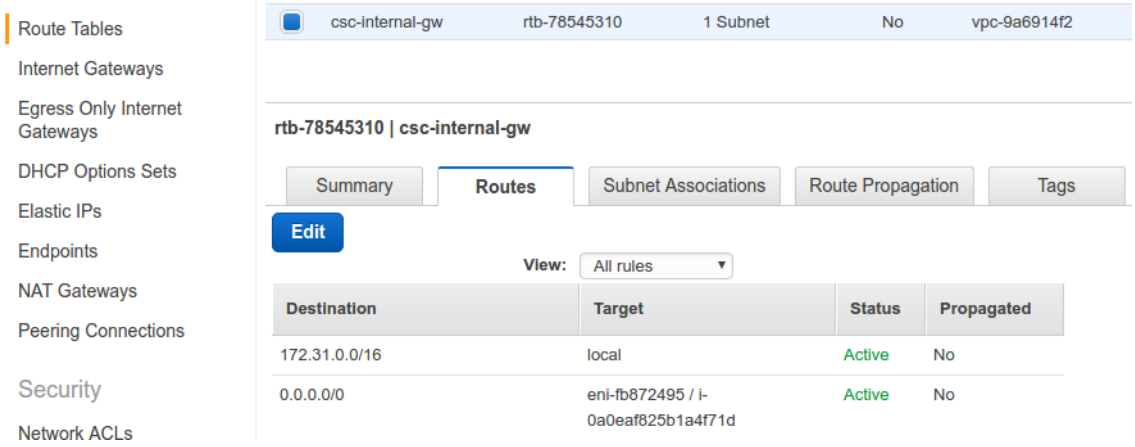
3. Put a Name and click “Yes, Create”
4. Select the Route and click on Subnet Associations > Edit
5. Select the Internal Subnet (172.31.48.0/24 in this example)



6. Save
7. Now, Click “Routes” and “Edit”
8. Click “Add another Route” and add the default route with “Target” the internal interface of the CSC. **TIP: Type “e” and you will be able to see the list of interfaces:**



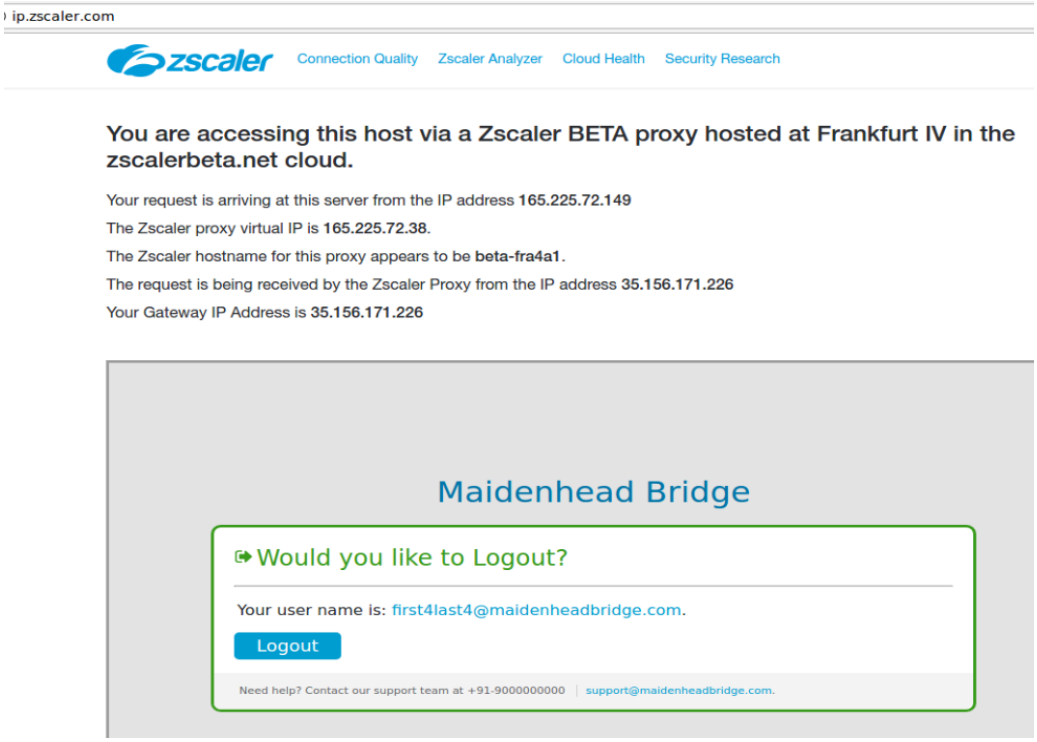
9. Select the Internal Interface. In this example is : eni-fb872495 | iface-csc-internal
10. Click save.



IMPORTANT: To create the Route Table with default route to the interface (eth1) of the CSC is enough in most cases.
Sometimes, it can be required to setup the default gateway pointing to the CSC IP (172.31.48.254 in our example) on the routing table of the **instance**.

5.2 Verifying that your reaching Zscaler properly

Go to the following page: ip.zscaler.com



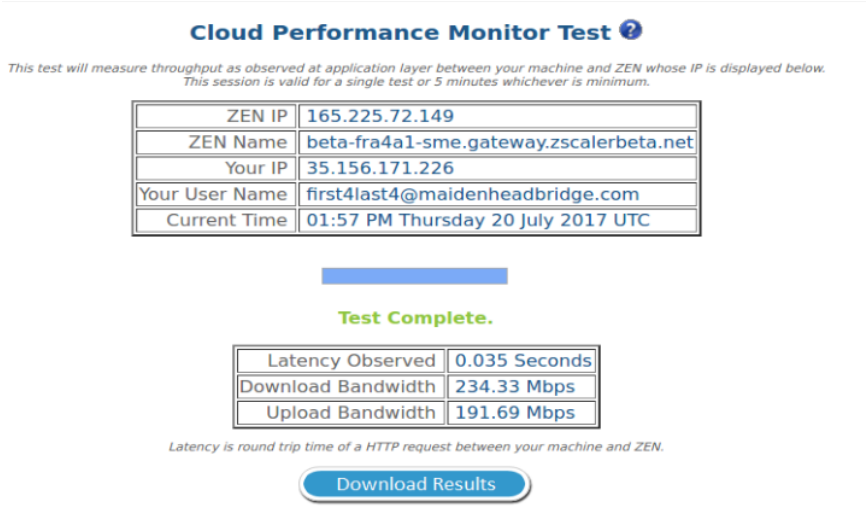
This page shows:

(values of this example between brackets [])

- Cloud name: [Zscaler Beta]
- Node: [Frankfurt]
- Zscaler internal values [165.225.72.149, 165.225.72.38, beta-fra4a1]
- Your Gateway IP addresses [35.156.171.226, this is the Elastic IP associated to the CSC on the external interface (eth0)]
- The name or logo of your organization [Maidenhead Bridge]
- The Username (if Authentication was enabled on the location) [first4last4@maidenheadbridge.com]

5.3 Checking Connection Quality

On the page ip.zscaler.com, click on “Connection Quality” and “Start Test”



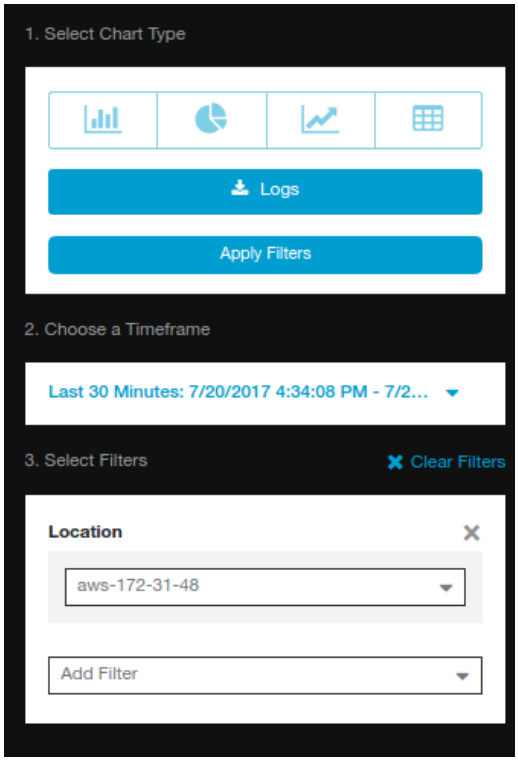
IMPORTANT: You should receive values near 200 Mbps that is the limit of Zscaler for Ipsec tunnels.

6 Checking full visibility of the transaction on the Zscaler GUI

The most important thing when doing tunnels to the Zscaler Cloud is to do not NAT the connections to the cloud. This allows to see the internal IPs on the Zscaler logs. Having visibility of the internal IPs is a must for full Security and Control.

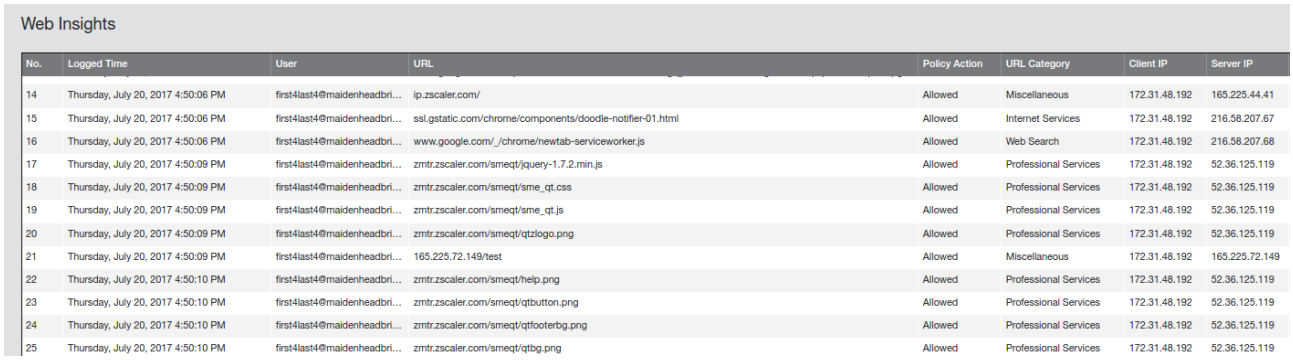
6.1 Web Logs

Go to Analytics > Web Insights



Click Logs and Filter by Location [aws-172-31-48]

Apply Filters:



No.	Logged Time	User	URL	Policy Action	URL Category	Client IP	Server IP
14	Thursday, July 20, 2017 4:50:06 PM	first4last4@maidenheadbri...	ip.zscaler.com/	Allowed	Miscellaneous	172.31.48.192	165.225.44.41
15	Thursday, July 20, 2017 4:50:06 PM	first4last4@maidenheadbri...	ssl.gstatic.com/chrome/components/doodle-notifier-01.html	Allowed	Internet Services	172.31.48.192	216.58.207.67
16	Thursday, July 20, 2017 4:50:06 PM	first4last4@maidenheadbri...	www.google.com/_/chrome/newtab-serviceworker.js	Allowed	Web Search	172.31.48.192	216.58.207.68
17	Thursday, July 20, 2017 4:50:09 PM	first4last4@maidenheadbri...	zmtr.zscaler.com/smeqt/jquery-1.7.2.min.js	Allowed	Professional Services	172.31.48.192	52.36.125.119
18	Thursday, July 20, 2017 4:50:09 PM	first4last4@maidenheadbri...	zmtr.zscaler.com/smeqt/sme_qt.css	Allowed	Professional Services	172.31.48.192	52.36.125.119
19	Thursday, July 20, 2017 4:50:09 PM	first4last4@maidenheadbri...	zmtr.zscaler.com/smeqt/sme_qt.js	Allowed	Professional Services	172.31.48.192	52.36.125.119
20	Thursday, July 20, 2017 4:50:09 PM	first4last4@maidenheadbri...	zmtr.zscaler.com/smeqt/qtzlogo.png	Allowed	Professional Services	172.31.48.192	52.36.125.119
21	Thursday, July 20, 2017 4:50:09 PM	first4last4@maidenheadbri...	165.225.72.149/test	Allowed	Miscellaneous	172.31.48.192	165.225.72.149
22	Thursday, July 20, 2017 4:50:10 PM	first4last4@maidenheadbri...	zmtr.zscaler.com/smeqt/help.png	Allowed	Professional Services	172.31.48.192	52.36.125.119
23	Thursday, July 20, 2017 4:50:10 PM	first4last4@maidenheadbri...	zmtr.zscaler.com/smeqt/qtbutton.png	Allowed	Professional Services	172.31.48.192	52.36.125.119
24	Thursday, July 20, 2017 4:50:10 PM	first4last4@maidenheadbri...	zmtr.zscaler.com/smeqt/qtfooterbg.png	Allowed	Professional Services	172.31.48.192	52.36.125.119
25	Thursday, July 20, 2017 4:50:10 PM	first4last4@maidenheadbri...	zmtr.zscaler.com/smeqt/qtbg.png	Allowed	Professional Services	172.31.48.192	52.36.125.119

As you can see, you have full visibility of the Client IP [172.31.48.192 in this case]

More in detail:

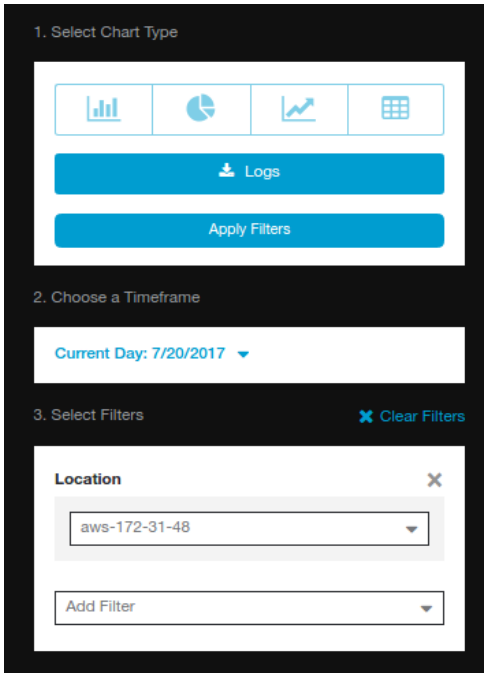
Client IP	Server IP
172.31.48.192	165.225.44.41
172.31.48.192	216.58.207.67
172.31.48.192	216.58.207.68

6.2 Firewall Logs

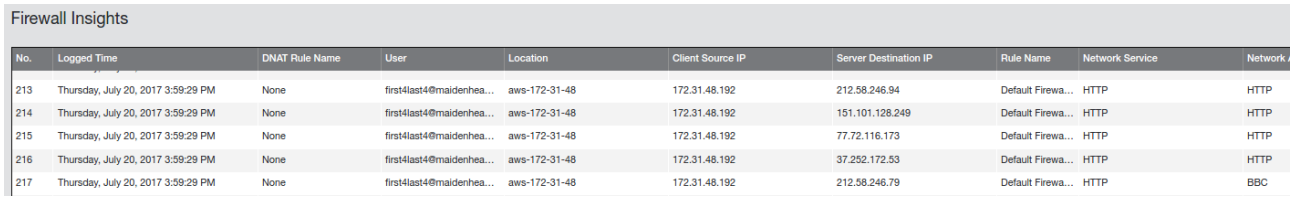
Same than before, with the CSC you will have full visibility on Firewall Logs of your internal IPs.

Go to Analytics > Firewall Insights

Click Logs and Filter by Location [aws-172-31-48]



Apply Filters



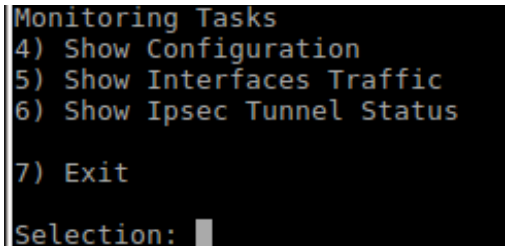
More in detail:

Client Source IP	Server Destination IP
172.31.48.192	212.58.246.94
172.31.48.192	151.101.128.249
172.31.48.192	77.72.116.173
172.31.48.192	37.252.172.53

7 CSC Monitoring Tasks

The CSC doesn't required to be monitored permanently. Despite this, the CSC provides monitoring tasks that will allow to troubleshoot configuration and connectivity if required.

Here the Menu of Monitoring Tasks:



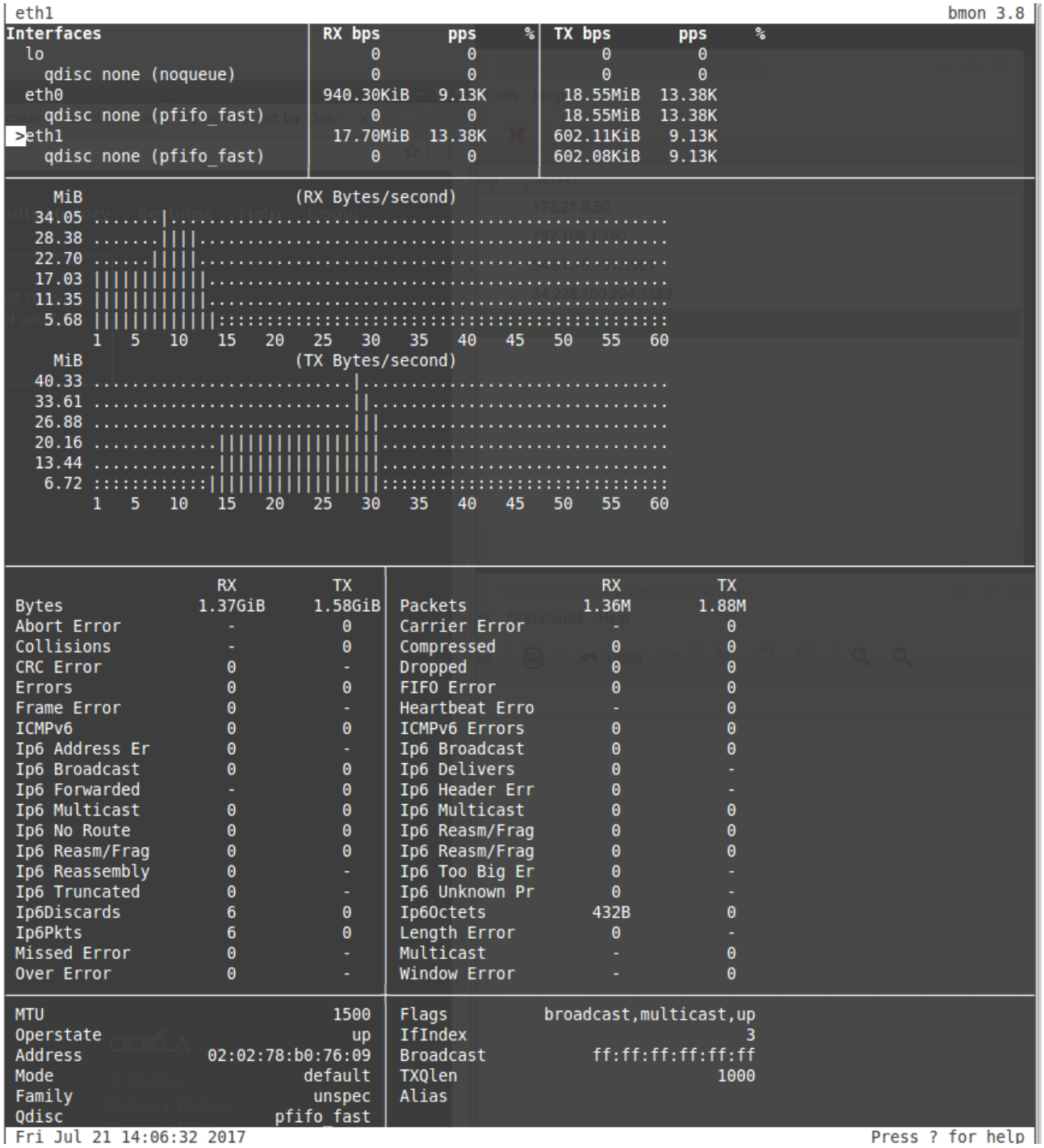
7.1 Show Configuration

This option shows the configuration of the CSC related to AWS, Zscaler Nodes (Hostname | IP), Interfaces (IP | ID | Security Group) and VPN Credentials (Email and Pre Shared Key)

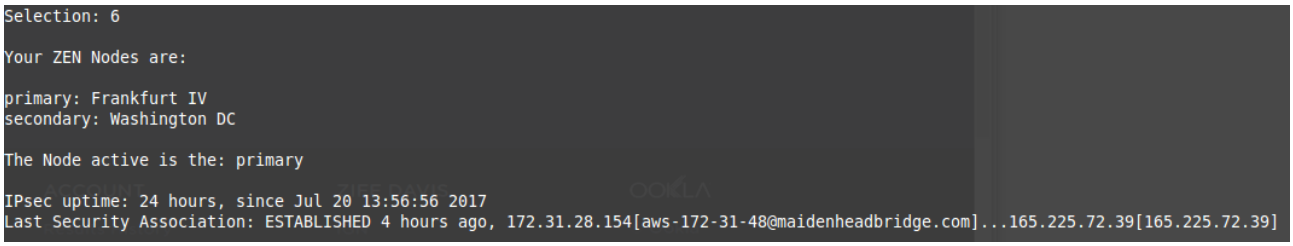
7.2 Show interfaces traffic

With this option you will be able to see how the traffic is on each interface.

IMPORTANT: • Press “q” to quit • Press “?” for help



7.3 Show Ipsec Tunnel Status



This option shows:

- ➔ Your Zen nodes: primary and secondary
- ➔ The Node Active:
- ➔ Ipsec Uptime.
- ➔ Last Security Association

8 OS Level Administration

AWS request that all AMI on the AWS market can be accessed at OS Level. From: AWS Marketplace Seller Guide, (v 3.7 - Last updated May 2, 2017)

> ...”Item 6.2.2:
> *AMIs MUST allow OS-level administration capabilities to allow for compliance requirements, vulnerability updates and log file access. For Linux-based AMIs this is through SSH, and for Windows-based AMIs this is normally through RDP.”...*

If you want to access to the CSC at OS level, simply SSH the machine using the username: csccli (SSH -i <key.pem> csccli@<eth1 IP>). The <key.pem> is the same than for the user: cscadmin

> *Note: You don’t need this username csccli for configuration or monitoring.* ***For configuration and monitoring use the username: cscadmin (SSH -i <key.pem> cscadmin@<eth1 IP>***