



# Maidenhead Bridge

## Cloud Security Connector for AWS

Enabling Zscaler for AWS customers

Quick Installation Guide

Version 1.1

(April 2018)

# Table of Contents

1 Introduction.....	3
2 Key benefits of the Cloud Security for AWS.....	3
3 The CSC on the AWS architecture.....	4
4 Deploy the Cloud Security Connector.....	5
4.1 Prerequisites.....	5
4.1.1 Prerequisites EXAMPLE:.....	5
4.2 Launching the CSC from AWS Market.....	6
5 Accessing for first time to your CSC.....	11

# 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.

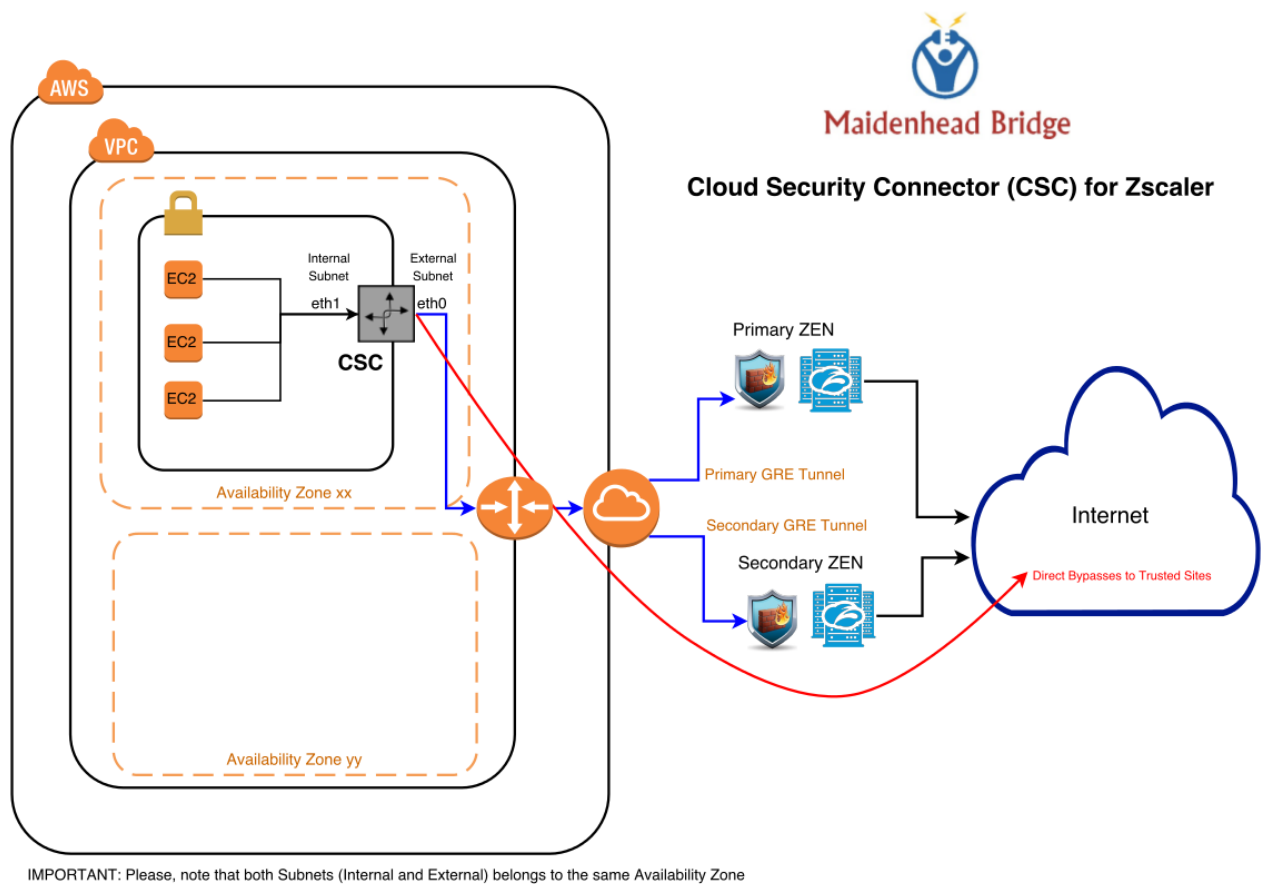
In addition to this, the CSC provides an easy way to manage direct bypasses to trusted sites.

## 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.small, t2.medium, t2.large.

### 3 The CSC on the AWS architecture

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



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.

## 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.

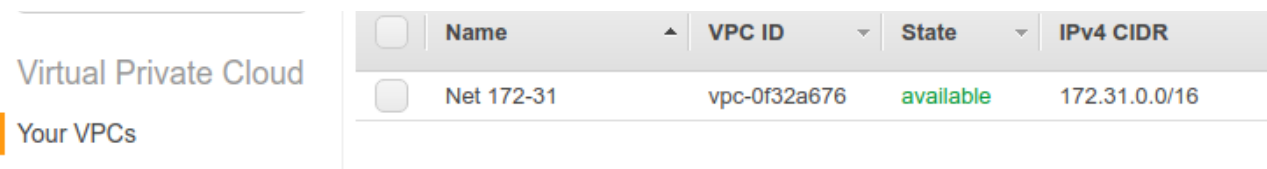
a) Go to your EC2 Dashboard to get the Key Pairs or to create new ones.

1 – SSH Keys : us-east-key



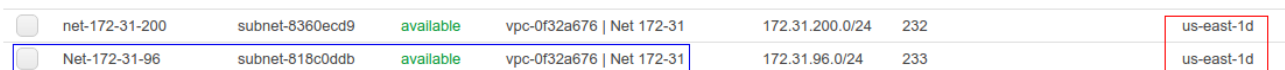
b) Go to your VPC Dashboard, to obtain VPC ID, and Subnets.

2 – VPC ID: vpc-of32a676

A screenshot of the AWS Management Console 'Virtual Private Cloud' page. A table lists subnets. The first row is highlighted with a blue border.


Name	VPC ID	State	IPv4 CIDR
Net 172-31	vpc-of32a676	available	172.31.0.0/16

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

A screenshot of the AWS Management Console 'Subnets' page. A table lists subnets. The row for 'Net-172-31-96' is highlighted with a blue border. The 'Availability Zone' column for this row is highlighted with a red border.

Name	VPC ID	State	IPv4 CIDR	Availability Zone
net-172-31-200	vpc-of32a676   Net 172-31	available	172.31.200.0/24	us-east-1d
Net-172-31-96	vpc-of32a676   Net 172-31	available	172.31.96.0/24	us-east-1d

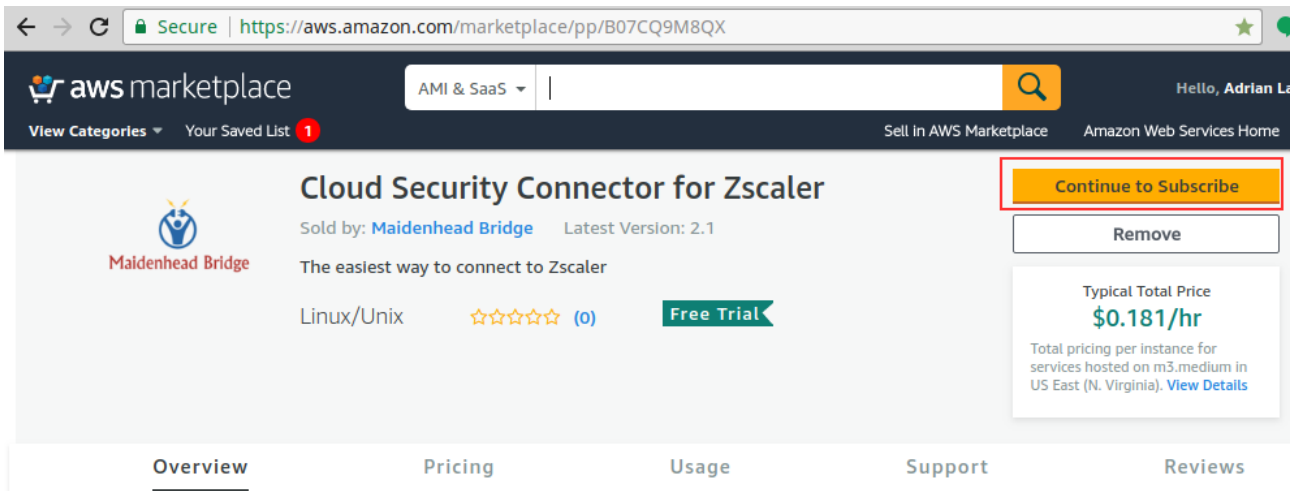
4- Internal Subnet: subnet-8360ecd9 (Note: Availability Zone us-east-1d and VPC ID vpc-of32a676)

A screenshot of the AWS Management Console 'Subnets' page. A table lists subnets. The row for 'net-172-31-200' is highlighted with a blue border. The 'Availability Zone' column for this row is highlighted with a red border.

Name	VPC ID	State	IPv4 CIDR	Availability Zone
net-172-31-200	vpc-of32a676   Net 172-31	available	172.31.200.0/24	us-east-1d
Net-172-31-96	vpc-of32a676   Net 172-31	available	172.31.96.0/24	us-east-1d

## 4.2 Launching the CSC from AWS Market

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



### Product Overview

The Cloud Security Connector will allow to protect your Web traffic in compliance with the best practices for Zscaler Web Services. No manual configuration required: everything is automated with the perfect configuration. Simply ingress your IPs tunnel values.

Version	2.1
Sold by	Maidenhead Bridge
Categories	Security Network Infrastructure
Operating System	Linux/Unix, Ubuntu 16.04.4 LTS (Xenial Xerus)
Fulfillment Methods	CloudFormation Template

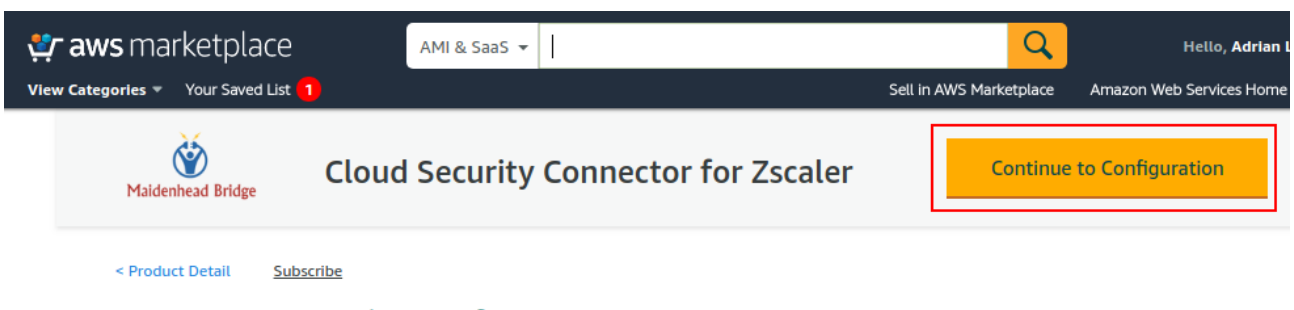
### Highlights

- Easy to install
- Full compliance with Zscaler Best practices
- Easy Bypass functionality

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

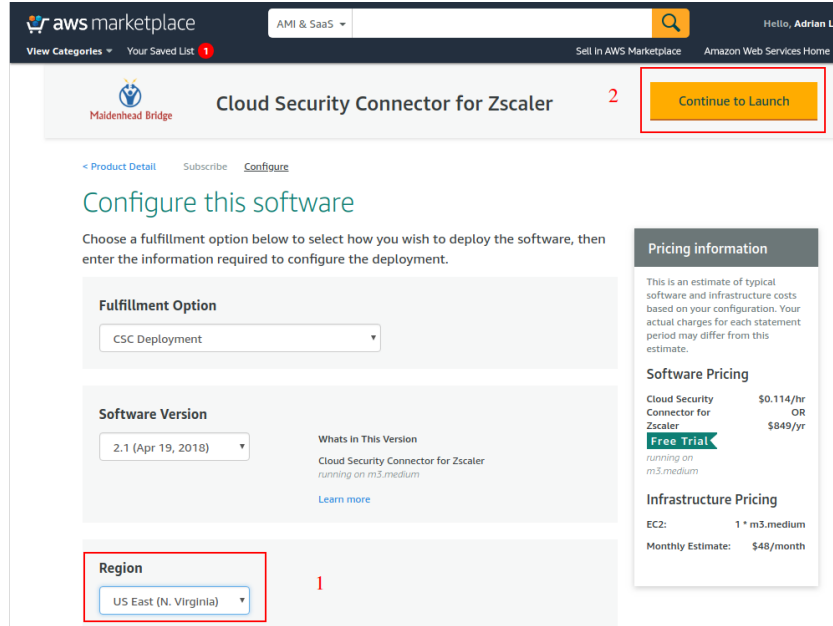
→ Click **“Continue to Subscribe”**

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



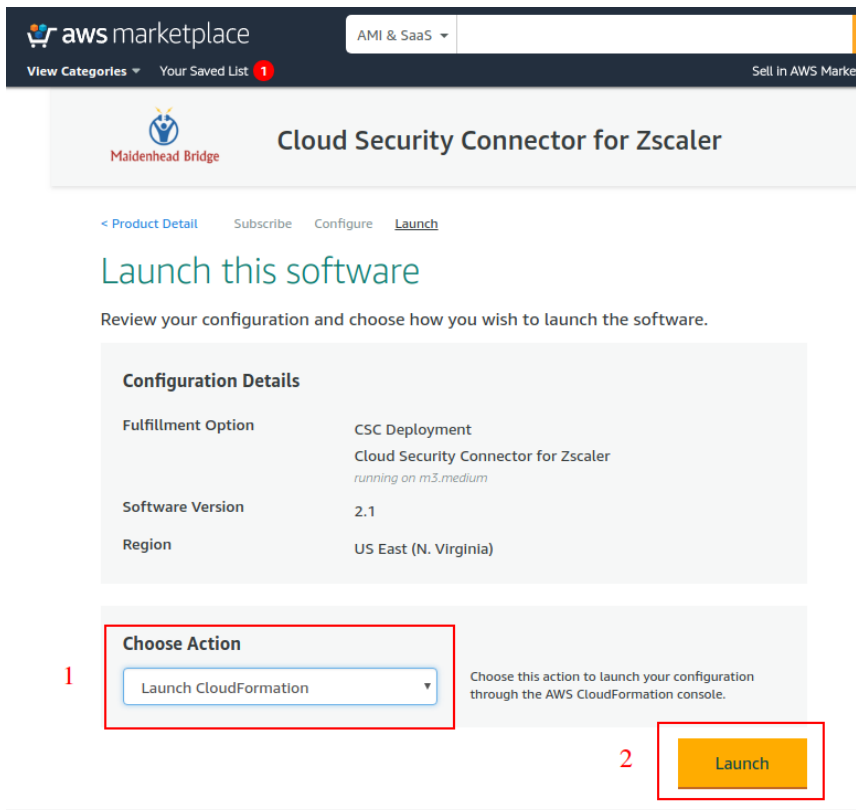
→ Click **“Continue to Configuration”**

### 3. Select “Region”



→ Click “**Continue to Launch**”

### 4. Choose Action: “Launch CloudFormation”



→ Click “**Launch**”

5. At this point, the “Create Stack” screen will appear. (*FYI: Please note the URL used that points to the CloudFormation template*)

The screenshot shows the AWS CloudFormation console's 'Create Stack' page. The breadcrumb navigation at the top indicates the path: CloudFormation > Stacks > Create Stack. The page is divided into a left-hand navigation pane and a main content area. The navigation pane has 'Select Template' selected. The main content area has a sub-header 'Select Template' and a descriptive paragraph. Below this, there are three sections: 'Design a template' with a 'Design template' button; 'Choose a template' with a dropdown menu; and 'Specify an Amazon S3 template URL' with a text input field containing a URL and a 'View/Edit template in Designer' link. At the bottom right, there are 'Cancel' and 'Next' buttons, with the 'Next' button highlighted by a red box.

→ 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 (\*)
- Key Name

**(\*) Important note about CSC and AWS Instance Type:** AWS has not committed bandwidth (Mbps) on Burst instances like t2. The CSC is very light on resources then t2 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 instances and the CSCs:

- t2.small: 200 Mbps to 400 Mbps
- t2.medium: 350 Mbps to 600 Mbps
- t2.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.*



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

## Specify Details

---

Specify a stack name and parameter values. You can use or change the default parameter values, which are defined in t

**Stack name**

## Parameters

---

### Network Configuration

---

**Which VPC should this be deployed to?**    
Select a VPC.

**External Subnet**    
Select an External Subnet (WARNING !! must be the same availability zone than Internal Subnet)

**Internal Subnet**    
Select an Internal Subnet (WARNING !! must be the same availability zone than External Subnet)

### Amazon EC2 Configuration

---

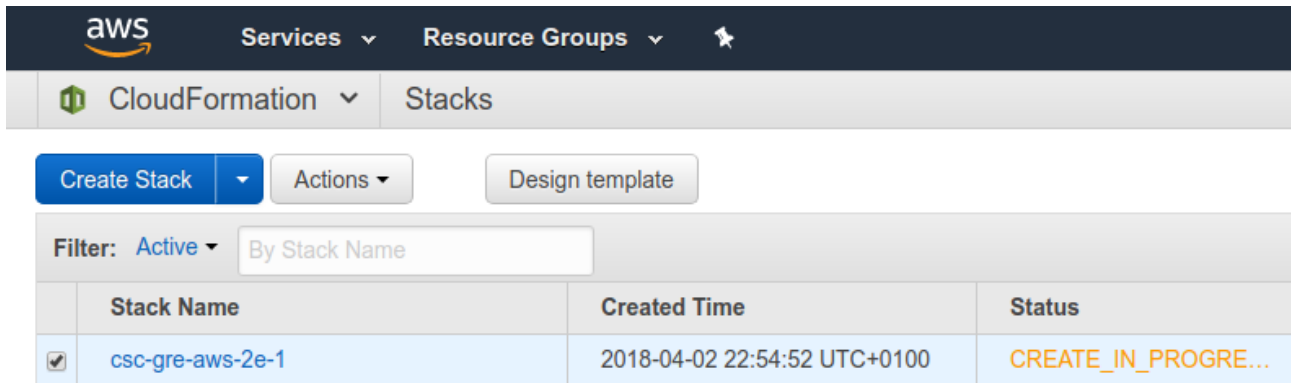
**Name**  The name of the instance

**AWS Instance Type**  Select one of the instance types

**Key Name**    
Key Pair name

- Click **“Next”**
- “Options Section”: Click **“Next”**
- “Review”: Click **“Create”**

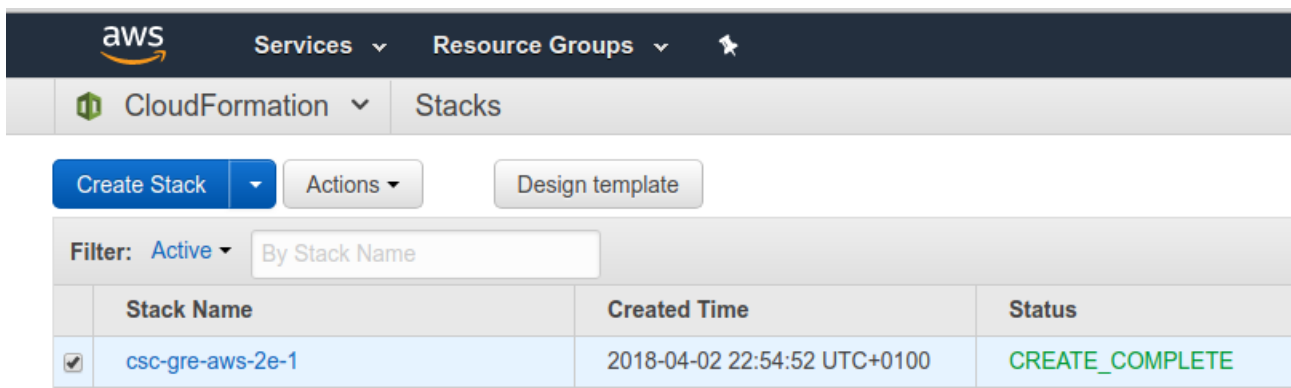
The Stack will show “status” CREATE\_IN\_PROGRESS



The screenshot shows the AWS CloudFormation console. At the top, there are navigation tabs for 'Services' and 'Resource Groups'. Below that, the 'CloudFormation' service is selected, and the 'Stacks' view is active. There are three buttons: 'Create Stack', 'Actions', and 'Design template'. A filter is set to 'Active' and the search is 'By Stack Name'. A table lists one stack:

	Stack Name	Created Time	Status
<input checked="" type="checkbox"/>	csc-gre-aws-2e-1	2018-04-02 22:54:52 UTC+0100	CREATE_IN_PROGRE...

And after a while:



The screenshot shows the AWS CloudFormation console after the stack has finished. The interface is identical to the previous screenshot, but the status of the stack 'csc-gre-aws-2e-1' is now 'CREATE\_COMPLETE'.

	Stack Name	Created Time	Status
<input checked="" type="checkbox"/>	csc-gre-aws-2e-1	2018-04-02 22:54:52 UTC+0100	CREATE_COMPLETE

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.

The screenshot shows the AWS Management Console. On the left, the 'INSTANCES' menu is expanded, and 'Instances' is selected. The main area displays a list of instances. The instance 'csc-gre-aws-2e-1' is highlighted. Below the list, the details for this instance are shown, including its ID, state (running), type (t2.small), and Elastic IP (52.70.55.180). A modal window for 'Network Interface eth1' is open, showing details such as Interface ID, VPC ID, Attachment Status, and Private IP Address (172.31.200.44).

2. On the bottom screen, click “eth1” and take a look of the Private IP address of the eth1. In this example is: 172.31.200.44
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 172.31.200.44`

```
root@ip-172-31-200-163:/home/ubuntu# ssh -i "us-east-key.pem" cscadmin@172.31.200.44
****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: zsccloud, 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 52.70.55.180

Current Values Configured:
-----
Cloudname:
-----
DNS Server: AWS DNS server 169.254.169.253
-----
Tunnel Source IP: 52.70.55.180 (* 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
-----
Are you ready to continue? (y/n) █
```

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

This is the end of the Quick Installation Guide. Please, visit <http://support.maidenheadbridge.com> to download the CSC Administration Guide for more detailed information.