

Cloud Security Connector for AWS

Enabling Zscaler for AWS customers

Administrator Guide

Version 1.3

(August 2017)

CSC for AWS – Admin Guide

Date 05/08/17

Table of Contents

1 Introduction	3
2 The CSC on the AWS architecture	3
3 Key benefits of the Cloud Security for AWS	4
4 Connecting your Subnet to Zscaler Cloud Security	5
4.1 Step 1: Create your VPN credentials and Location on the Zscaler GUI	5
4.1.1 VPN Credentials	5
4.1.2 Location	6
4.2 Step 2: AWS configuration for CSC instance	8
4.2.1 Create you internal subnet (if it does not exist)	8
4.2.2 Create a new "Elastic IP"	8
4.2.3 Create the "Security Groups": Internal and External	9
4.2.3.1 Internal Security Group	.10
4.2.3.2 External Security Group	.10
4.2.4 Create the Network Interfaces: Internal and External	.11
4.2.4.1 Internal Network Interface	.11
4.2.4.2 Disable Source / Destination Check on Internal Interface	.12
4.2.4.3 External Network Interface	.13
4.2.5 Associate the Elastic IP to the External Interface:	.14
4.2.6 Launch the CSC instance:	.14
4.3 Step 3: Configure the CSC	.18
4.3.1 Checking your connection to Zscaler from the CSC	.20
4.3.2 Adding the IPs of the Zscaler Nodes to the Security Group External	.20
5 Using Zscaler from your internal devices	.23
5.1 Create "Route Tables" for Internal Subnet	.23
5.2 Verifying that your reaching Zscaler properly	.25
5.3 Checking Connection Quality	.26
6 Checking full visibility of the transaction on the Zscaler GUI	.27
6.1 Web Logs	.27
6.2 Firewall Logs	.28
7 CSC Monitoring Tasks	.30
7.1 Show Configuration	.30
7.2 Show interfaces traffic	.31
7.3 Show Ipsec Tunnel Status	.32
8 OS Level Administration	.33

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:

Add VPN Credential		>	۲
VPN Credential			^
Authentication Type Path Year FQDN XAUTH			
User ID aws-172-31-48	0	maidenheadbridge.com 👻	
New Pre-Shared Key]	Confirm New Pre-Shared Key	
Comments]		
This is the <u>VPN</u> credential for the <u>Subnet</u> 172-31-4	18 on	AWS	
L			Ŧ
Save Cancel			

In this example the values are:

FDQN (Email) = <u>aws-172-31-48@maidenheadbridge.com</u>

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:

Add Location	
Location	
Name aws-172-31-48	Country Germany
State/Province	Time Zone Europe/Berlin
Addressing	
Public IP Addresses None	
VPN Credentials aws-172-31-48@maidenheadbridge.com	

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.

Gateway Options

Enable XFF Forwarding	Enforce Authentication
Enable IP Surrogate	Idle Time to Disassociation 8 Hours
Enforce Surrogate IP for Known Browsers	4 Hours
Enable SSL Scanning	Enforce Firewall Control
Bandwidth Control	
Enforce Bandwidth Control	
Download (Mbps) 200	Upload (Mbps) 200
Canad	
Save	

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:

Create Subnet			×
Use the CIDR format to spec and /28 netmask. Also, note	cify your subnet's IP address b that a subnet can be the same	lock (e.g., 10.0.0.0/24). N e size as your VPC. An IP	lote that block sizes must be between a /16 netmask Vv6 CIDR block must be a /64 CIDR block.
Name tag	172.31.48.0/24	0	
VPC	vpc-9a6914f2 🔻 🕄		
VPC CIDRs	CIDR	Status	Status Reason
	172.31.0.0/16	associated	
Availability Zone	eu-central-1a 🔻 🛈		
IPv4 CIDR block	172.31.48.0/24		0

Go to your VPC Dashboard > Subnets and "Create Subnet"

🎁 Services 🗸 R	tesource Groups 👻 🕻									
VPC Dashboard	Create Subnet Subnet	Actions v								
Filter by VPC: None	Q Search Subnets and th	eir proj 🗙								
Virtual Private Cloud	Name -	Subnet ID 🗸	State ~	VPC	*	IPv4 CIDR 🗸	Available IPv4 /~	IPv6 CIDR	Availability Zone	•
Your VPCs	172.31.48.0/24	subnet-5a2b2632	available	vpc-9a6914f2		172.31.48.0/24	250		eu-central-1a	
Subnets		subnet-eaeed482	available	vpc-9a6914f2		172.31.16.0/20	4090		eu-central-1a	
Route Tables		subnet-063e324c	available	vpc-9a6914f2		172.31.0.0/20	4091		eu-central-1c	
Internet Gateways		subnet-6b83c411	available	vpc-9a6914f2		172.31.32.0/20	4091		eu-central-1b	

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

VPC Dashboard	Allocate new address	Actions ~
Filter by VPC: None	Q Filter by attributes or sea	arch by keyword
Virtual Private Cloud	Elastic IP	- Allocation ID
Your VPCs	52.59.4.118	eipalloc-9b6655f2
Subnets		
Route Tables		
Internet Gateways		
Egress Only Internet Gateways		
DHCP Options Sets		
Elastic IPs		

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

VPC Dashboard	Allocate new address	Actions v
Filter by VPC: None	Q Filter by attributes or se	arch by keyword
Virtual Private Cloud	Elastic IP	Allocation ID Insta
Your VPCs	52.59.4.118	eipalloc-9b6655f2 i-096
Subnets	35.156.171.226	eipalloc-453b082c -
Route Tables		
Internet Gateways		
Egress Only Internet Gateways		
DHCP Options Sets		
Elastic IPs		

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".

🧊 Services 🗸 R	tesource Groups 🗸 🔭
VPC Dashboard	Create Security Group Actions v
Filter by VPC: None	Filter All security groups V Q Search Security Groups and t X
Virtual Private Cloud	Name tag Group ID Group Name VPC Description
Your VPCs	ubuntu-remote-access sg-66fda20d ubuntu-remote-access vpc-9a6914f2 ubuntu-remote-access
Subnets	LAN-AllowALL sg-6b712f00 LAN-AllowALL vpc-9a6914f2 Allow all traffic
Route Tables	default vpc sg-75eba71e default vpc-9a6914f2 default VPC security group
Internet Gateways	
Egress Only Internet Gateways	
DHCP Options Sets	
Elastic IPs	
Endpoints	sg-6b712f00 LAN-AllowALL
NAT Gateways	
Peering Connections	Summary Inbound Rules Outbound Rules Tags
Security	Edit Type Protocol Port Range Source
Security Groups	ALL Traffic ALL ALL 0.0.0.0/0

And here the detail about "Outbound Rules"

sg-6b712f0	0 LAN-	Allo	WALL				
Summ	ary	In	bound Rules	Outbound	Rules	Tags	
Edit							
Туре	Protoc	ol	Port Range	Destination			
ALL Traffic	ALL		ALL	0.0.0/0			

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

Create Security G	roup		×
Name tag Group name Description VPC	External-CSC-SG External-CSC-SG This group is for the external interface of the vpc-9a6914f2 • ①	0	
		Cancel	Yes, Create

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

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					
Туре ()	Protocol (i)		Port Range (i)	Source (j)	
Custom ICMP Rule - IPv4	Echo Reply		N/A	0.0.0/0	
			_		

6. Select "Outbound Rules" and add the following rules:

	External-CSC-SG	sg-85b4eaee	External-CSC-SG	vpc-9a6914f2	This group is for the external interface of the CSC (e	th0)
Sec	curity Group: sg-85b4eaee			0.0		
D	escription Inbound Outbound	Tags				
	Edit					
	Туре ()	Protocol (i)		Port Range (i)	Destination (i)	
	Custom UDP Rule	UDP		4500	0.0.0.0/0	
	Custom UDP Rule	UDP		500	0.0.0.0/0	
	Custom ICMP Rule - IPv4	Echo Request		N/A	0.0.0.0/0	

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:

Create Netwo	ork In	terface		×
Description	(j)	This is the Internal Network Interface of the CSC]	
Subnet	()	subnet-5a2b2632 eu-central-1a 172.31.48.0/24		
Private IP	(j)	172.31.48.254]	
Security groups	(j)	sg-85b4eaee - External-CSC-SG - This group is for the external interfi- sg-6b712f00 - LAN-AllowALL - Allow all traffic sg-75eba71e - default - default VPC security group sg-66fda20d - ubuntu-remote-access - ubuntu-remote-access		
			Cancel	Yes, Create

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.

	iface-csc-internal	eni-fb872495	subnet-5a2b26	vpc-9a6914f2	eu-central-1a	LAN-AllowALL	This is the Inte	🔵 available	172.31.48.254
--	--------------------	--------------	---------------	--------------	---------------	--------------	------------------	-------------	---------------

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:

Change Source/Dest. Check \times	
Network Interface eni-fb872495 Source/dest. check © Enabled	
Cancel Save	

4. Click "Save"

4.2.4.3 External Network Interface

- 1. Click ""Create Network Interface"
- 2. Fill the fields:

Create Netwo	ork li	nterface		>	<
Description	i	This is the external interface of the CSC			
Subnet	i	subnet-eaeed482* eu-central-1a			
Private IP	(j)	auto assign			
Security groups	(j)	sg-85b4eaee - External-CSC-SG - This group is for the external interfactors sg-6b712f00 - LAN-AllowALL - Allow all traffic sg-75eba71e - default - default VPC security group sg-66fda20d - ubuntu-remote-access - ubuntu-remote-access - vectors - ve			
			Cancel	Yes, Create	

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.

iface-csc-external eni-1585267b subnet-eaeed4... vpc-9a6914f2 eu-central-1a External-CSC-SG

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:

Associate Elastic IP Address	i		×
Select the address you wish to associate with	eni-1585267b		
Address	35.156.171.226	•	
Allow reassociation			(i)
Associate to private IP address	172.31.28.154*	•	(i)
	* denotes the primary private IP address		
		Can	cel Associate Address

3. Click, "Associate Address"

4.2.6 Launch the CSC instance:

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

← → C Secure https://aws.amazon.com	m/marketplace/pp/B074DQ75DC					
^waws marketplace	AMI & SaaS 👻			Q		
View Categories 👻						
	S Maidenberg Bridge	Cloud Security Connector (CSC) for Z old by: Maldenhead Bridge	Iscaler			
	rrademeau bridge v n n	15 Day Free Trial Available - The Cloud Security Connector (CSC) for Zscaler enables AWS customers to protect the instances when surfing the internet using Zscaler Cloud Web Security. The CSC is the perfect configuration for Zscaler and provides redundancy between Zscaler Enforcement Nodes (ZEN) automatically. In minutes you will be able to connect to Zscaler. Simply yo need to add your Zscaler VPN credentials and to select the ZEN Nodes that you want to use.				
	Customer Rating	**** I (0 Customer Reviews)	Continue	You will have an opportunity to review your order before launching or		
	Latest Version	csc-zscaler-aws-04		being charged.		
	Operating System	Linux/Unix, Ubuntu csc-zscaler-aws-04	Pricing Informa	tion		
	Delivery Method	64-bit Amazon Machine Image (AMI) (Read more)	Use the Region dropdow infrastructure pricing inf	n selector to see software and formation for the chosen AWS region.		
	Support	See details below	For Region			
	Highlights	 The easy way to connect to Zscaler 	US East (N. Virgini	a) 🔻		

- 2. Click "Continue"
- 3. Select "Manual Launch"

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

Subscription Term	Applicable Instance Type
 Hourly Annual 	Hourly fee Varies Depends on instance type, reference pricing chart.
5 Solo	oct "Software Version"

✓ Version

 Csc-zscaler-aws-04, released 07/30/2017
 ✓

 Usage Instructions

Note: If you click "Usage Instructions" the following message appears:

Usage Instructions for csc-zscaler-aws-04



The link redirect to this Administrator Guide.

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

Region	ID			
EU (Ireland)	ami-4bi	37dc32	aunch with EC2 Console	
Asia Pacific (Singapore)	ami-44	ea7727 L	aunch with EC2 Console	
Asia Pacific (Sydney)	ami-791	b1ae1a L	aunch with EC2 Console	
EU (Frankfurt)	ami-25	7fd34a L	aunch with EC2 Console	
Asia Pacific (Tokyo)	ami-0e	5dbf68	aunch with EC2 Console	
US East (N. Virginia)	ami-aa(055bd1	aunch with EC2 Console	
South America (Sao Paulo)	ami-8bi	a1d6e7	aunch with EC2 Console	
US West (N. California)	ami-954	4f67f5	Launch with EC2 Console	
US West (Oregon)	ami-8ft	o7adf6	aunch with EC2 Console	
u rity Group vendor recommends usi	ng the follo	owing security	/ group policies. You wil	
elect these settings or co	onfigure you	Ir own when	launching this software	
mection Method	Protocol	Port Range	Source (IP or Group	

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

1. Ch	ose AMI 2. Choose Instance Type 3. Configu	re Instance 4. Add Storag	e 5. Add Tags 6. Configu	re Security Group 7. Review			
Step	2: Choose an Instance Typ	e m4.10xlarge	40	160	EBS only	Yes	10 Gigabit
0	General purpose	m4.16xlarge	64	256	EBS only	Yes	20 Gigabit
	General purpose	m3.medium	1	3.75	1 x 4 (SSD)		Moderate

- 8. Click at the bottom right: "Next: Configure instance details"
- 9. Please, note the following changes:

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Sten	3.	Configure	Instance	Details
Sleb	э.	Connuare	Instance	Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the

Number of instances	()	1	Launch into Auto Scali	ng Group (j)	
Purchasing option	i	Request Spot instances			
Network	i	vpc-9a6914f2 (default)	•	C Create new VPC	
Subnet	(j)	subnet-eaeed482 Default in e 4089 IP Addresses available	u-central-1a 🔹	Create new subnet	
Auto-assign Public IP	(i)	Disable	T		
IAM role	(j)	None	•	C Create new IAM role	
Shutdown behavior	(j)	Stop	•		
Enable termination protection	(j	Protect against accidental te	rmination		
Monitoring	(i)	Enable CloudWatch detailed Additional charges apply.	monitoring		
Tenancy	()	Shared - Run a shared hardwa Additional charges will apply for	re instance •		
▼ Network interfaces ⁽ⁱ⁾					
Device Network Interface	Subnet	Primary IP	Secondary I	P addresses	
eth0 eni-1585267b (iface-c: •	subnet-ea	Auto-assign			
eth1 eni-fb872495 (iface-cs ▼	subnet-5a	Auto-assign		¢	8

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.

1. Choose AMI	2. Choose Instance Type	3. Configure Instance	4. Add Storage	5. Add Tags	6. Configure Security Group	7. Review			
Step 6: Co A security group to reach your inst	s a set of firewall rules that allow	ty Group at control the traffic for y unrestricted access to	our instance. On he HTTP and HT	this page, you TPS ports. You	can add rules to allow specific tr I can create a new security grou	affic to reach you p or select from a	ur instance. For example, if you want to set up an existing one below. Learn more about Am		
	Assign a security gro	oup: OCreate a new se	ecurity group						
		Select an existi	ng security group)					
Security	Group ID	Name			Description				
sg-75eba7	1e	default		d	lefault VPC security group				
sg-85b4ea	ee	External-CSC	SG	Т	his group is for the external inte	rface of the CSC	; (eth0)		
sg-6b712f	0	LAN-AllowALL		Α	Allow all traffic				
sg-66fda20	ld	ubuntu-remote	-access	u	ubuntu-remote-access				
Inbound rules	nbound rules for sg-85b4eaee (Selected security groups: sg-85b4eaee)								
Type (j)		Protoc	ol (j)		Port Range	(j)	Source (j)		
Custom ICMP F	Rule - IPv4	Echo F	eply		N/A		0.0.0/0		

- 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.

eu-central-1a 🥥 running 🔀 Initializing None 🍃 ec2-35-156-171-226.eu... 35.156.171.226

16. Select existing Key Pair or create a new one.

csc-aws-172.31.48.254 i-0a0eaf825b1a4f71d m3.medium

- 17. Launch instance. Go to View instance:
- 18. Put a Name to the CSC. We called csc-aws-172.31.48.254
- Instances

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:

Selection: 2 Select Cloud					
1) Zscloud 2) Zscalerone 3) Zscalertwo 4) Zscalerbeta 5) Zscaler					
Selection:4 You have chosen	: Zscalerbeta				

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 wasl-vpn.zscalerbeta.net Hostname wasl-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



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.

CSC for AWS – Admin Guide

Selection: 4
AWS information
AWS Instance ID: i-0988b04ff2817fd50
AWS Availability Zone: eu-central-la
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:

External-CSC-SG	sg-85b4eaee	External-CSC-S	G vpc-9a6914f2	This group is for the e
dit outbound ru	Iles			×
Type (i)	Protocol (j)	Port Range (j)	Destination (j)	
Custom UDP F •	UDP	4500	Custom • 165.225.72.39/32,104.12	9.194.39/32
Custom UDP F •	UDP	500	Custom T 165.225.72.39/32,104.12	9.194.39/32
Custom ICMP V	Echo Reque: •	N/A	Custom T 165.225.72.39/32,104.12	9.194.39/32
Add Rule IOTE: Any edits made on lepends on that rule to be	existing rules will result in the dropped for a very brief period	edited rule being deleted and a d of time until the new rule can t	new rule created with the new details. This be created.	will cause traffic that

External-CSC-SG	sg-85b4eaee	External-CSC-SG	vpc-9a6914f2	This group is for the extern
Edit inhound rule				~
	5			~
Туре ()	Protocol (i)	Port Range (i)	Source (i)	
Custom ICMP •	Echo Reply 🔻	N/A	Custom • 165.225.72.39/32,104	129.194.39/32
Add Rule				
NOTE: Any edits made on e depends on that rule to be o	existing rules will result in the e dropped for a very brief period of	dited rule being deleted and a r of time until the new rule can be	new rule created with the new details. The created.	nis will cause traffic that
				Cancel Save

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	scurity Group: sg-85b4eaee								
Description Inbound C	Description Inbound Outbound Tags								
Edit									
Туре 🛈	Protocol (j)	Port Range (i)	Destination (j)						
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)
∢ S	ecurity Group: sg-85b4eaee			0.0	
	Description Inbound Outbound	i Tags			
	Edit				
	Type (j)	Protocol (i)		Port Range (j)	Source (j)
	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:



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"

Create Route Tabl	e >	×
A route table specifies how p and your VPN connection.	ackets are forwarded between the subnets within your VPC, the Internet,	
Name tag VPC	<u>csc</u> -internal- <u>gw</u> vpc-9a6914f2 ▼ 1	
	Cancel Yes, Create	

- 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)

rtb-78545310 csc-internal-gw							
Summa	ry Routes	Subnet Associations	Route				
Cancel	Save						
Associate	Subnet	IPv4 CIDR	IPv6 CIDF				
	subnet-063e324c	172.31.0.0/20	-				
	subnet-eaeed482	172.31.16.0/20	-				
	subnet-6b83c411	172.31.32.0/20	-				
	subnet-5a2b2632 172.31	.48.0/24 172.31.48.0/24	-				

- 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:**

rtb-78545310 | csc-internal-gw

	Summary	Routes	Subnet Associations R	oute Propagation	
	Cancel Save	You must f	ix errors before saving.		
	Destination		Target	Status	Propa
1	72.31.0.0/16		local	Active	No
(0.0.0.0/0		A Select a target, or enter a valid resource ID.		No
	Add another route	9	eni-0f47e761 ubuntu-xfce- eni-1585267b iface-csc-ex eni-9f49e9f1 ubuntu-xfce-e eni-fb872495 iface-csc-inte	nt ternal ext ernal	

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

10. Click save.							
Route Tables	csc-internal-gw	rtb-785	45310	1 Subnet	No	vpc-9a6914	4f2
Internet Gateways							
Egress Only Internet Gateways	rtb-78545310 csc-int	ernal-gw					
DHCP Options Sets	Summary	Routes	Subnet Asso	ociations	Route Propage	ation Ta	as
Elastic IPs	Edit				1 5		5
Endpoints	Lun	View:	All rules	•			
NAT Gateways	Destination		Target		Status	Propagated	
Peering Connections	172 31 0 0/16		local		Activo	No	
Security	0.0.0.0/0		eni-fb872495 / i	i-	Active	No	
Network ACLs	010101010		0a0eaf825b1a4	If71d	,		

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

E zs	caler	Connection Quality	Zscaler Analyz	er Cloud Health	Security Researc	ch
You are a zscalerbe	iccessir eta.net (ng this host cloud.	via a Zsca	ler BETA p	proxy hoste	d at Frankfurt
Your request i	s arriving at	this server from t	he IP address 10	5.225.72.149		
The Zscaler p	roxy virtual	IP is 165.225.72.3	38.			
The Zscaler h	ostname foi	this proxy appea	rs to be beta-fra	4a1.		
The request is	being rece	ived by the Zscale	er Proxy from the	Paddress 35.	156.171.226	
Your Gateway	IP Address	is 35.156.171.22	6			
			Maide	nhead	Bridge	
	@ Wo	uld you lik	Maide	nhead ut?	Bridge	
	Fe WC	ould you lik ser name is: firs	Maide e to Logo	nhead ut?	Bridge	
	Ge WC Your u Log	ould you lik ser name is: firs out	Maide e to Logo	nhead ut? enheadbridge	Bridge	

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

1. S	Select Chart T	уре		
	<u>lılı</u>	¢	~	Ħ
		ئ ا	.ogs	
		Apply	Filters	
2. 0	Choose a Tim	eframe		
1	Last 30 Minut	tes: 7/20/2017	7 4:34:08 PM	- 7/2 🔻
3. S	Select Filters			X Clear Filters
	Location			×
	aws-172-3	31-48		•
[Add Filter			-

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

Apply Filters:

Web	Web Insights								
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]

1. \$	Select Chart T	уре		
	<u>lılı</u>	¢	~	
		ه 🕹 ا	_ogs	
		Apply	Filters	
2. (Choose a Tim	eframe		
	Current Day:	7/20/2017 👻		
3. 8	Select Filters			X Clear Filters
	Location			×
	aws-172-3	31-48		•
	Add Filter			-

Apply Filters

Firewall Insights

No.	Logged Time	DNAT Rule Name	User	Location	Client Source IP	Server Destination IP	Rule Name	Network Service	Network
213	Thursday, July 20, 2017 3:59:29 PM	None	first4last4@maidenhea	aws-172-31-48	172.31.48.192	212.58.246.94	Default Firewa	нттр	HTTP
214	Thursday, July 20, 2017 3:59:29 PM	None	first4last4@maidenhea	aws-172-31-48	172.31.48.192	151.101.128.249	Default Firewa	HTTP	HTTP
215	Thursday, July 20, 2017 3:59:29 PM	None	first4last4@maidenhea	aws-172-31-48	172.31.48.192	77.72.116.173	Default Firewa	HTTP	HTTP
216	Thursday, July 20, 2017 3:59:29 PM	None	first4last4@maidenhea	aws-172-31-48	172.31.48.192	37.252.172.53	Default Firewa	HTTP	HTTP
217	Thursday, July 20, 2017 3:59:29 PM	None	first4last4@maidenhea	aws-172-31-48	172.31.48.192	212.58.246.79	Default Firewa	HTTP	BBC

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)

```
Selection: 4

AWS information

AWS Instance ID: i-0988b04ff2817fd50

AWS Availability Zone: eu-central-la

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
```

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

eth1							bmon 3.8
Interfaces		RX bps	pps %	TX bps	pps	%	
lo		0	Θ	Θ	Θ		
qdisc none (n	oqueue)	0	0	0	0		
eth0	fife fact)	940.30K	1B 9.13K	ep18.55M1B	13.38K		
cale quisc none (p	fifo_fast) t by	17 704	10 10 20V	18.55M1B	13.38K		
adisc none (n	fifo fast)	17.70	1D 13.30N	602.11K1B	9.13K		
quise none (p	1110_10307	, v	Ĭ	002.00010	5.150		
MiB	(RX Bytes/	second)				
ult34.050.vSe							
28.38							
22.70			••••••				
17.03	[[[]]						
	!!!!!:						
a an 5.68		25 20	25 40 45	EQ EE	::		
MiB J D	10 15 20	ZD 30 TX Bytes/	55 40 45	50 55	00		
40.33	(IN Bytes/	second				
33.61							
26.88							
20.16		шшіі.					
13.44							
6.72 :::::::	::::	11111111:					
15	10 15 20	25 30	35 40 45	50 55	60		
	RX	тх	2010	RX	ТΧ		- + ×
Bytes	1.37GiB	1.58GiB	Packets	1.36M	1.88	1	
Abort Error		0	Carrier Error		0		
Collisions	-	Θ	Compressed	0	0		Q
CKC Error	0	-	Dropped		0		
Errors Erame Error	0		Heartheat Erro	U	0		
	0	e l	TCMDv6 Errors	- 0	0		
In6 Address Er	0	-	Ip6 Broadcast	0	õ		
Ip6 Broadcast	õ	Θ	Ip6 Delivers	õ	-		
Ip6 Forwarded		Θ	Ip6 Header Err	0			
Ip6 Multicast	Θ	Θ	Ip6 Multicast	Θ	Θ		
Ip6 No Route	Θ	Θ	Ip6 Reasm/Frag	Θ	0		
Ip6 Reasm/Frag	Θ	0	Ip6 Reasm/Frag	Θ	Θ		
Ip6 Reassembly	0		Ip6 Too Big Er	0			
Ip6 Truncated	0	-	Ip6 Unknown Pr	0	-		
IpoDiscards	6	U A	Ipouctets	432B	U		
Missed Error	0		Multicast	0	-		
Over Frror	0		Window Error		0		
					V		
МТО		1500	Flags	broadcast,m	ulticast,u	ıp	
Operstate		ир	IfIndex			3	
Address	02:02:78:b	0:76:09	Broadcast	ff:ff:	ff:ff:ff:f	ff	
Mode		default	TXQlen		100	00	
Family	Policy	unspec	Allas				
Quisc Emi lul 21 14:00	p†1	.To_Tast					Droce 2 for bol-
FII JUL ZI 14:00	. 32 201/						FIESS FIOF NELD

7.3 Show Ipsec Tunnel Status

Selection: 6 Your ZEN Nodes are: primary: Frankfurt IV secondary: Washington DC The Node active is the: primary IPsec uptime: 24 hours, since Jul 20 13:56:56 2017 Last Security Association: ESTABLISHED 4 hours ago, 172.31.28.154[aws-172-31-48@maidenheadbridge.com]...165.225.72.39[165.225.72.39]

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>