

Cloud Security Connector Anywhere

Enabling Zscaler from Any Location

Administrator Guide

Software Version 4.0

(January 2018)

CSC – Anywhere – Admin Guide

Page 1 of 49

Date 10/01/18

Table of Contents

1 Introduction	4
2 CSC Anywhere – Network diagrams	5
2.1 CSC Anywhere – One Arm – (One Unit)	5
2.2 CSC Anywhere – One Arm – High Availability	5
2.3 CSC Anywhere – Single – (One Unit)	6
2.4 CSC Anywhere – Single – High Availability	6
3 Key benefits of the Cloud Security Anywhere	7
4 Creating the CSC Anywhere	8
4.1 CSC Anywhere – One Arm – IP Addressing	8
4.2 CSC Anywhere – Single – IP Addressing	8
4.3 Filling the Form	9
4.4 CSC files: OVA, VPN Credentials and URL/Bypass PAC example	10
5 Creating the Location on Zscaler GUI.	11
5.1 Import the VPN Credentials	11
5.2 Create the Location on the Zscaler GUI	12
6 Installing the OVA file in your Virtual Platform	13
7 Firewall Requirements	14
7.1 CSC One Arm	14
7.1.1 First Internal IP	14
7.1.2 Third Internal IP	14
7.2 CSC Single	15
7.2.1 First External IP	15
7.2.2 Second External IP	15
8 Powering up the CSC Anywhere	16
8.1 Verifying that your reaching Zscaler properly	18
8.2 Using a PC	18
8.3 Using the "Show Configuration and Status" menu	18
8.4 Checking Connection Quality	19
8.4.1 Using a PC	19
8.4.2 Using "Speed Test" menu	19
9 CSC Anywhere – Admin Console	20
9.1 Zscaler Admin Tasks:	20
9.2 Monitoring Tasks:	20
9.2.1 Show Configuration and Status	21
9.2.1.1 GENERAL INFORMATION	21
9.2.1.2 INTERFACES INFORMATION	21
9.2.1.3 DNS INFORMATION	22
9.2.1.4 ZSCALER INFORMATION	22
9.2.1.5 TUNNEL INFORMATION	23
9.2.1.6 CREDENTIALS INFORMATION	23
9.2.1.7 http://ip.zscaler.com INFORMATION	23
9.2.1.8 AWS SSM Agent	23
9.2.2 Show Interfaces Traffic	24
9.2.3 Traceroute and Latency Test	24
9.2.3.1 Traceroute and Latency Test with the tunnel "Not Active"	25
9.2.3.2 Traceroute and Latency Test with the tunnel "Active"	27
9.3 CSC Admin Tasks	29
9.3.1 AWS SSM Agent (Register / De-Register)	29
0 (0 0)	

9.3.1.1 Checking the status of the AWS SSM agent	31
9.3.2 Change SSH Password	31
9.3.3 Change Timezone	31
9.4 Bypass Proxy	32
9.4.1 View Current Bypass List	32
9.4.2 Configure Bypass List	32
9.4.2.1 1) Auto – Bypass PAC URL	32
9.4.2.2 2) Manual	35
10 Checking full visibility of the transaction on the Zscaler GUI	37
10.1 Web Logs	37
10.2 Firewall Logs	38
11 Troubleshooting	40
11.1 If the tunnels are not connecting	40
11.2 Proxy Bypass	41
11.2.1 How to check if the Proxy Bypass is active?	41
11.2.2 If you added the bypass in the PAC but forgot to update the CSC	41
11.3 PAC file troubleshooting	42
11.3.1 How to check what PAC file URL is applied?	42
11.3.2 How to Check if the Domain destination is using VIP Proxy or Bypass Proxy?	42
12 Maidenhead Bridge Contact Information	45
13 APPENDIX A	46
13.1 Improvements of Version 4.0	46
13.1.1 New! Bypass Proxy functionality	46
13.2 Improvements of Version 3.5	46
13.2.1 New Model: CSC Anywhere One Arm	46
13.2.2 Resilient Algorithm	46
13.3 Improvements of Version 3.2	46
13.3.1 Traceroute and Latency Test	46
13.4 Speed Test (Experimental)	47
13.5 Improvements of Version 3.0	47
13.5.1 One Click Configuration and Status report	47
13.5.2 AWS management	47
13.5.2.1 CSC Anywhere as "Managed Instance" on EC2 console	47
13.5.2.2 Executing "Run Commands" or schedule "Associations" on AWS Console	48
13.5.2.3 Zscaler API ready	49

1 Introduction

The Cloud Security Connector (CSC) Anywhere family allows to connect securely Zscaler Cloud Security Services from any location.

The main purpose of the CSC Anywhere family is simplicity: You don't need to re-architect your network and is a direct replacement of your current Web Security Appliance. You can place the CSC Anywhere on the same network segment that you current appliance and the CSC will redirect the traffic to Zscaler.

No configuration is required. Simply fill a form with your IP address and download the CSC and power it on.

The CSC Anywhere comes with the perfect parameters to work with Zscaler. As soon you lunch the CSC at the location, the CSC will automatically detect the best Zscaler nodes to connect to and will create all tunnels, firewall rules and routing tables that are necessary.

No restrictions: No static IP or public IPs are required. You can run it on any virtual software and hardware version is also available.

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

Simple to install with full management from Amazon AWS. The CSC is a cloud instance running on your premises.

The CSC Anywhere - One Arm is a direct replacement of your web appliance. The simplest way to connect to Zscaler.

The CSC Anywhere – Single is commonly used by Zscaler customers that are using Zscaler Cloud Firewall

2 CSC Anywhere – Network diagrams

2.1 CSC Anywhere – One Arm – (One Unit)



2.2 CSC Anywhere – One Arm – High Availability

CSC - Anywhere - One Arm High Availability - Active Active



2.3 CSC Anywhere – Single – (One Unit)





2.4 CSC Anywhere – Single – High Availability

CSC - Anywhere - Single High Availability - Active Active



3 Key benefits of the Cloud Security Anywhere

- Direct replacement of your current appliance. (One Arm)
- Enables any Location to be connected to Zscaler Cloud Security Services.
- Full tunnel redundancy.
- VIP proxy to direct the traffic to Zscaler.
- Bypass Proxy to send the traffic direct to Internet.
- Easy configuration: After you buy the CSC, you will need to fill a form indicating your IPs and GWs. After the form is submitted, you will receive the OVA file to install.
- All parametrization required for 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.
- Full hardened device.
- Auto selection of Zscaler nodes.
- No static IP required.
- No public IP required.
- All virtual platform supported: Vmware, KVM, Virtual Box, etc.
- Hardware version available if required.
- One click Status and Configuration. This shows 25 values and does 14 checks.
- Amazon AWS management
- Zscaler API Ready
- MTR (MyTraceRoute) test to the Zscaler nodes and in the reverse path as well.
- Speedtest.net integrated
- Works with No default Route Scenarios.
- No changes on your network is required. You can place the internal interface of the CSC on the same subnet than your current Web Security Solution.
- Small OVA instance: 1 CPU, 1 GB RAM, 4 GB Disk

4 Creating the CSC Anywhere

To create the CSC anywhere is very easy. You just need to fill a form with your IP addressing.

Here the network diagram showing the information required:

4.1 CSC Anywhere – One Arm – IP Addressing



4.2 CSC Anywhere – Single – IP Addressing



4.3 Filling the Form

After you buy the CSC Anywhere, you will receive a Welcome Email with the indication about to fill the a form with your data. Here a partial view of the form:



The form is very easy to fill. The values that you need to ingress are:

- 1. Email
- 2. Company Name
- 3. Zscaler Company ID
- 4. Zscaler Cloud Name
- 5. Your domain (for auto-generation of VPN credentials)
- 6. Location Name
- 7. Internal Interface: IP / Bitmask (Note: The CSC uses three consecutive IPs. You need to ingress the first one) and Gateway.
- 8. External Interface (Single model only): IP/Bitmask (Note: The CSC single uses two consecutive IPs) and Gateway.

9. (Optional) DNS Server.

4.4 CSC files: OVA, VPN Credentials and URL/Bypass PAC example.

After you fill the form, you will receive an email containing links to download two files:

- CASxxxxx-vpncredentials.csv (VPN credentials to import)
- CASxxxxx-v-y-z.ova (your Open Virtual Appliance file to install in your virtual infrastructure)
- CASxxxx-url-bypass-pac.txt (Instructions to create the "Bypass PAC" to feed your CSCs Bypass List and contains your Bypass PAC URL already configured on the CSCs)

5 Creating the Location on Zscaler GUI

Two steps are required here: To import the VPN credentials and to create the Location.

5.1 Import the VPN Credentials

- 1. On your Zscaler GUI, go to: Administration > VPN Credentials
- 2. On VPN Credentials, Click "Import VPN Credentials"
- 3. Select the CSV file received: CASxxxxx-vpncredentials.csv

Import VPN Credentials	×
Import VPN Credentials	
CSV File Choose file CAS00016-vpentials.csv	
Import Cancel	

- 4. Click "Import"
- 5. You will see a new FDQN credentials with the format of: CASxxxx@<yourDomain>. In this example the value is:

8	cas00016@maidenheadbridge.com	FQDN

Note: VPN credentials are created automatically in order to simplify the installation. You can create your own VPN credentials and to configure it on the CSC manually if you want.

5.2 Create the Location on the Zscaler GUI

- 1. Go to Administration > Locations
- 2. Click create "Add Location"
- 3. Put Name and other parameters. Select the VPN Credentials imported in the step before.

Edit Location	×
Location	*
Name cas00016	Country United Kingdom
State/Province	Time Zone Europe/London
Addressing	
Public IP Addresses None VPN Credentials cas00016@maidenheadbridge.com	lentials
Gateway Options	
Enable XFF Forwarding	Enforce Authentication
Enable IP Surrogate	Idle Time to Disassociation 2 Hours
Enforce Surrogate IP for Known Browsers	
Enable SSL Scanning	Enforce Firewall Control
Bandwidth Control	
Enforce Bandwidth Control	
Save Cancel	▼ Delete

6 Installing the OVA file in your Virtual Platform.

We are going to show how to install the OVA file on Vmware. The process is very simple. Just follow the defaults values and map the interfaces EXTERNAL and INTERNAL (Single) or only INTERNAL for One Arm.

- 1. Go to vSphere, File > Deploy OVF template
- 2. Select the OVA File:

Source		
<u>OVF Template Details</u>		
Name and Location		
Resource Pool		
Disk Format		
Network Mapping	Deploy from a file or URL	
Ready to Complete	\\VBOXSVR\adrian\csc-any-01\CAS00016-v-2-4.ova	owse
	Enter a URL to download and install the OVF package from the Internet specify a location accessible from your computer, such as a local hard d network share, or a CD/DVD drive.	, or rive, a

- 3. OVF Template Details: Click Next
- 4. Name and Location: Put the Name you want.
- 5. Resource Pool: Place the VM where you want.
- 6. Disk Format: Click Next
- 7. Network Mapping: Please map the interfaces EXTERNAL and INTERNAL to your interfaces. Here an example:

🕝 Deploy OVF Template

Network Mapping

What networks should the deployed template use?

OVF Template Details Name and Location	Map the networks used in this OVF	template to networks in your inventory
<u>Resource Pool</u> Disk Format	Source Networks	Destination Networks
Network Mapping Ready to Complete	INTERNAL	Net-192-168-1-0 Net-172-19-0-0

- 8. Click "Next"
- 9. Click "Finish"

7 Firewall Requirements

The CSC Anywhere requires Outbound stateful rules (or in/out if stateful is not available) to connect to Zscaler.

The CSC Anywhere Single can be connected directly to an Internet Public IP or behind a Firewall (NAT is supported).

The most common scenario is to sit the CSC Anywhere Single behind the Broadband Router / Firewall provided by the Internet Service Provider where all ports mentioned below are, in general, allowed by default.

The CSC Anywhere One Arm is always behind a firewall with private IPs

7.1 CSC One Arm

Here the list of Protocols and Ports required:

7.1.1 First Internal IP

The first IP of the CSC Anywhere One Arm will require the following Firewall rules:

Item	Protocol	Port / Service	Used for:
1	UDP (in/out)	500,4500	IPsec tunnel.
2	TCP (out)	80 (HTTP)	Test pages: <u>http://ip.zscaler.com</u> , speedtest.net
3	TCP (out)	443 (HTTPS)	AWS SSM Agent
4	ICMP (in/out)	Out: echo In: echo-reply, time- exceeded.	Keepalives and Monitoring tests. (ICMP types: echo=type 8, echo-reply=type 0, time-exceeded=type 11)
5	UDP, TCP (in/out)	Out: TCP 53 In / Out: UDP 53	DNS

7.1.2 Third Internal IP

The Third IP is the Bypass Proxy. Outgoing connection direct to internet are initiated from here as well.

Item	Protocol	Port / Service	Used for:
1	ТСР	80 (HTTP)	Web traffic
2	ТСР	443 (HTTPS)	Web traffic encrypted
3	TCP (out)	1024 to 65535	Web sites that are using particular ports, for example: http://www.example.com:8080

7.2 CSC Single

Here the list of Protocols and Ports required:

7.2.1 First External IP

The first IP of the CSC Anywhere Single will required the following Firewall Rules.

Item	Protocol	Port / Service	Used for:
1	UDP (in/out)	500,4500	IPsec tunnel.
2	TCP (out)	80 (HTTP)	Test pages: <u>http://ip.zscaler.com</u> , speedtest.net
3	TCP (out)	443 (HTTPS)	AWS SSM Agent
4	ICMP (in/out)	Out: echo In: echo-reply, time- exceeded.	Keepalives and Monitoring tests. (ICMP types: echo=type 8, echo-reply=type 0, time-exceeded=type 11)
5	UDP, TCP (in/out)	Out: TCP 53 In / Out: UDP 53	DNS

7.2.2 Second External IP

The Second IP is the Egress IP of the Bypass Proxy. Outgoing connections direct to internet are initiated from here.

Item	Protocol	Port / Service	Used for:
1	TCP (out)	80 (HTTP)	Web traffic
2	TCP (out)	443 (HTTPS)	Web traffic encrypted
3	TCP (out)	1024 to 65535	Web sites that are using particular ports, for example: http://www.example.com:8080

8 Powering up the CSC Anywhere

- 1. Power on the Virtual Machine
- 2. Open the Console:

Note: At the first time you power in the CSC, the process of Automatic Zscaler Node selection will happen and the CSC will reboot. This process is very fast.

When prompted, put the following username and password to login on the CSC Console:

Username: cscadmin

Password: maidenheadbridge

Note: You can access the CSC using SSH. Please, SSH the CSC INTERNAL IP and use the same credentials. SSH to the EXTERNAL interface is not allowed.

```
Welcome to Maidenhead Bridge - Cloud Security Connector Anywhere
Last login: Fri Dec 22 14:23:49 2017 from 172.19.0.140
Maidenhead Bridge
Cloud Security Connector Anywhere - Single - Admin Console
Company : Maidenhead Bridge
Location : CASmaidenheadbridge
CSC ID : cas00101
Soft Version : 4.0
Please select an option by typing its number
Zscaler Admin Tasks

    VPN Credentials - View/Configure Email (FDQN) and Pre Shared Key (PSK)

Select Zscaler Cloud and Enforcement Nodes
Confirm Configuration (and Reboot)
Monitoring Tasks
Show Configuration and Status
5) Show Interfaces Traffic
Traceroute and Latency Test
Speed Test (Experimental)
CSC Admin tasks
AWS SSM Agent (Register or De-Register)
9) Change SSH Password
10) Change Timezone
Bypass Proxy
11) View Current Bypass List
12) Configure Bypass List
e) Exit
Selection:
```

3. Select 4) Show Configuration and Status check "TUNNEL INFORMATION".

Selection: 4 GENERAL INFORMATION Company : Maidenhead Bridge Location : CASmaidenheadbridge CSC ID : cas00101 CSC date: Fri 22 Dec 15:00:01 GMT 2017 Soft version : 4.0 INTERFACES INFORMATION External Interface (eth0) IP: 192.168.1.215/24 | External Gateway: 192.168.1.254 is Alive Internal Interface (eth1) IP: 172.19.0.215/24 | Internal Gateway: 172.19.0.200 is Alive VIP Proxy: 172.19.0.216 Bypass Proxy: 172.19.0.217 DNS INFORMATION DNS Server IP: 192.168.1.100 is Not reachable Google DNS 1: 8.8.8.8 is Alive Google DNS 2: 8.8.4.4 is Alive ZSCALER INFORMATION Zscaler Cloud: Zscalerbeta Primary ZEN node: AutoPrimary | Hostname: vpn.zscalerbeta.net | IP: 165.225.72.39 is Alive Secondary ZEN node: AutoSecondary | Hostname: secondary.vpn.zscalerbeta.net | IP: 104.129.194.39 is Alive TUNNEL INFORMATION The Node active is the: AutoPrimary IPsec uptime: 4 hours, since Dec 22 10:41:23 2017 Last Security Association: ESTABLISHED 4 hours ago CREDENTIALS INFORMATION Username: cas00101@maidenheadbridge.com | PSK: Not shown for security reasons. Please, read it from 'VPN Credentials' Menu http://ip.zscaler.com INFORMATION You are accessing this host via a Zscaler BETA proxy hosted at Frankfurt IV in the zscalerbeta.net cloud. Your Gateway IP Address is 82.68.6.78 AWS SSM AGENT AWS SSM Agent is active (running) since Fri 2017-12-22 10:41:20 GMT; 4h 18min ago Registration values: {"ManagedInstanceID":"mi-025e7e0e5b569278a","Region":"eu-west-1"}

- 4. Congratulations! You are connected to Zscaler.
- 5. Now, you can forward your traffic through the CSC using the following methods:
 - PAC file (recommended): Traffic to Zscaler via VIP Proxy, Traffic direct to internet via Bypass Proxy
 - Explicit proxy: via VIP Proxy.
 - All port and protocols: If you are using Zscaler Cloud Firewall, you can use the Internal Interface as your default Gateway to Zscaler and to send all ports and protocols.

8.1 Verifying that your reaching Zscaler properly

8.2 Using a PC

Go to the following page: ip.zscaler.com from your PC

	lew History Bookmarks	Tools Help							ч	En	■))	19:53	3
Zscaler - Cl	Cloud Performan × Zscaler	Cloud Security: My ×	_+		1	1							_
🗧 🧲 🛈 C ip.	p.zscaler.com				C Q Search		쇼	Ê	ŧ	Â		8	-
	Exercise	Connection Quality	Zscaler Analyzer	Cloud Health	Security Research								
≥ . ■	You are access zscalerbeta.ne	sing this host v t cloud.	<i>i</i> ia a Zscaler	BETA pro	oxy hosted at	Frankfurt IV	in tł	ne					
	Your request is arriving	at this server from the	e IP address 165.2	25.72.149									
	The Zscaler proxy virtu	ual IP is 165.225.72.38											
	The Zscaler hostname	for this proxy appears	s to be beta-fra4a1										
	The request is being re	eceived by the Zscaler	Proxy from the IP	address 82.68	.6.78								
	Your Gateway IP Addre	ess is 82.68.6.78											
										_			
6													
-			Maiden	head B	ridge								
1													
	🖙 V	Vould you like t	o Logout?										
				dhaida a ann									
	You	ruser name is: iristatia	asisi @maidennea	abnage.com.									
		ogout											
	Need	help? Contact our support team	at +91-900000000 sup	port@maidenheadbri	idge.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 [82.68.6.78. This is your public IP]
- The name or logo of your organization [Maidenhead Bridge]
- The Username (if Authentication was enabled on the location) [first31last31@maidenheadbridge.com]

8.3 Using the "Show Configuration and Status" menu

This menu also goes to http://ip.zscaler.com .

```
http://ip.zscaler.com INFORMATION
You are accessing this host via a Zscaler BETA proxy hosted at Frankfurt IV in the zscalerbeta.net cloud.
Your Gateway IP Address is 82.68.6.78
```

8.4 Checking Connection Quality

8.4.1 Using a PC

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

800	File Edit View History Bookmarks Tools Help Zscaler-Cloud Performan × Zscaler-Cloud Performan × +			tų.	En	€)) 1	9:56 ╏	\$
0	€ 0 € 165.225.72.156/test 🖾 €] Q. Search	4	Ê	÷	î	v i	≥ ≡	:
					Go t	o ip.zsc	aler.com	F.
	Company™ The Cloud Security Company™							
	Cloud Performance Monitor Test 🕑							l
	This test will measure throughput as observed at application keyer between your machine and ZEN whose IP is displayed below. This session is viaid for a single test of 5 minimum.							l
	ZEN N# 105.25.72.155 ZEN Name beta-frad-3-sme.gateway.zscalerbeta.net Your IP 82.68.6.78							
	Your User Name first31last31@maidenheadbridge.com Current Time 06:55 PM Thursday 12 October 2017 UTC							
a,								
	Test Complete.							
	Download Bandwidth 62.46 Mbps Upload Bandwidth 17.84 Mbps							
	Latency is round trip time of a HTTP request between your machine and ZEN.							
	Download Results							
ľ-								J
0	Copyright ©2007-2016, Zscaler Inc. All rights reserved.							1

IMPORTANT: The limit of Zscaler for IPSEC tunnels is 200 Mbps. If you link is more than 200 Mbps, please use the Cloud Security Connector GRE.

8.4.2 Using "Speed Test" menu

The CSC runs the Speedtest.net (same test that you can run from the Web Page). This function is experimental due to we need to rely on third party tools.

```
SPEED TEST
This is experimental. We are using third party tools. (Speedtest.net)
Results can be inaccurate or none. The test takes a while
Ping: 35.13 ms
Download: 63.89 Mbit/s
Upload: 18.81 Mbit/s
```

9 CSC Anywhere – Admin Console

The Cloud Security Anywhere has an Admin Console that allows to do different tasks. When you access to the Admin Console, the following information appears on top:

```
Welcome to Maidenhead Bridge - Cloud Security Connector Anywhere
Last login: Fri Dec 22 14:23:49 2017 from 172.19.0.140
Maidenhead Bridge
Cloud Security Connector Anywhere - Single - Admin Console
Company : Maidenhead Bridge
Location : CASmaidenheadbridge
CSC ID : cas00101
Soft Version : 4.0
```

And you can select the following tasks:

9.1 Zscaler Admin Tasks:

```
Please select an option by typing its number
Zscaler Admin Tasks
1) VPN Credentials - View/Configure Email (FDQN) and Pre Shared Key (PSK)
2) Select Zscaler Cloud and Enforcement Nodes
3) Confirm Configuration (and Reboot)
```

With Zscaler Admin Tasks you can:

- 1. View / Change the VPN Credentials
- 2. Select manually the Zscaler Cloud and Zscaler nodes that you want to connect.
- 3. Confirm the values 1) and 2) and configure the CSC with this new values. The CSC will reboot.

9.2 Monitoring Tasks:

```
Monitoring Tasks
4) Show Configuration and Status
5) Show Interfaces Traffic
6) Traceroute and Latency Test
7) Speed Test (Experimental)
```

9.2.1 Show Configuration and Status

4. Show Configuration and Status. This menu show all parameters configured on the CSC Anywhere and does several checks.

In total, 25 parameters are showed and 14 checks are done. All in one shot.

```
Selection: 4
GENERAL INFORMATION
Company : Maidenhead Bridge
Location : CASmaidenheadbridge
CSC ID : cas00101
CSC date: Fri 22 Dec 15:12:52 GMT 2017
Soft version : 4.0
INTERFACES INFORMATION
External Interface (eth0) IP: 192.168.1.215/24 | External Gateway: 192.168.1.254 is Alive
Internal Interface (eth1) IP: 172.19.0.215/24 | Internal Gateway: 172.19.0.200 is Alive
VIP Proxy: 172.19.0.216
Bypass Proxy: 172.19.0.217
DNS INFORMATION
DNS Server IP: 192.168.1.100 is Not reachable
Google DNS 1: 8.8.8.8 is Alive
Google DNS 2: 8.8.4.4 is Alive
ZSCALER INFORMATION
Zscaler Cloud: Zscalerbeta
Primary ZEN node: AutoPrimary | Hostname: vpn.zscalerbeta.net | IP: 165.225.72.39 is Alive
Secondary ZEN node: AutoSecondary | Hostname: secondary.vpn.zscalerbeta.net | IP: 104.129.194.39 is Alive
TUNNEL INFORMATION
The Node active is the: AutoPrimary
IPsec uptime: 4 hours, since Dec 22 10:41:23 2017
Last Security Association: ESTABLISHED 4 hours ago
CREDENTIALS INFORMATION
Username: cas00101@maidenheadbridge.com | PSK: Not shown for security reasons. Please, read it from 'VPN Credentials' Menu
http://ip.zscaler.com INFORMATION
You are accessing this host via a Zscaler BETA proxy hosted at Frankfurt IV in the zscalerbeta.net cloud.
Your Gateway IP Address is 82.68.6.78
AWS SSM AGENT
AWS SSM Agent is active (running) since Fri 2017-12-22 10:41:20 GMT; 4h 31min ago
Registration values: {"ManagedInstanceID":"mi-025e7e0e5b569278a","Region":"eu-west-1"}
```

Here the detail of the information provided. Test are marked in *bold*

9.2.1.1 GENERAL INFORMATION

Here is general information about the device.

- Company Name
- Location
- CSC ID
- Soft Version

9.2.1.2 INTERFACES INFORMATION

Interfaces configuration and gateways and test of reachability of the gateways.

• Internal Interface (eth1) IP/Mask

- Internal Gateways IP/Mask
- Internal Gateway reachability: Alive or Not reachable.
- External Interface (eth0) IP/Mask
- External Gateways IP/Mask
- External Gateway reachability: Alive or Not reachable.
- VIP Proxy \rightarrow For traffic to Zscaler Nodes
- Bypass Proxy → For traffic direct to Internet

9.2.1.3 DNS INFORMATION

DNS configuration and reachability. Please, note that the CSC Anywhere has pre-configured the Google DNS as back up.

- Internal DNS IP
- Internal DNS reachability: Alive or Not reachable
- Google DNS 1 IP
- Google DNS 1 reachability: Alive or Not reachable
- Google DNS 2 IP
- Google DNS 2 reachability: Alive or Not reachable

9.2.1.4 ZSCALER INFORMATION

Here the values configured: Cloud and Nodes.

- Zscaler Cloud
- Primary ZEN Node
- Primary ZEN Node Hostname
- Primary ZEN Node IP
- Primary ZEN Node IP reachability: Alive or Not reachable
- Secondary ZEN Node
- Secondary ZEN Node Hostname
- Secondary ZEN Node IP
- Secondary ZEN Node IP reachability: Alive or Not reachable

9.2.1.5 TUNNEL INFORMATION

Here the values that shows where the CSC is connected (Zscaler Node) and the status of the Ipsec connection and the last Security Association.

- The Node Active
- Ipsec Uptime
- Last Security Association

9.2.1.6 CREDENTIALS INFORMATION

VPN Credentials Information. This is useful to check what credentials are in use.

- Username
- PSK Not Shown for Security Reasons. Please, read it from "VPN Credentials" Menu.

9.2.1.7 <u>http://ip.zscaler.com</u> INFORMATION

This test is what Zscaler support always recommends to do to validate that you are effectively using Zscaler. The CSC is going to the page <u>http://ip.zscaler.com</u> and is retrieving the following information:

- The Cloud and Node that you are using when connected. If you are not connected this value is blank.
- Your Gateway IP (this is your public IP in use)

9.2.1.8 AWS SSM Agent

This section shows the Status of the AWS SSM Agent. It helps to identify the CSC managed instance on AWS, showing the instance ID and the region where the CSC was registered.

- AWS SSM Agent is active (running) or dead
- Registration values: Instance ID and region

9.2.2 Show Interfaces Traffic

5. Show Interfaces Traffic: This selection shows the traffic information on all interfaces.

eth0									bmon 3.8
Interfaces		RX bps	pps %	TX bps	pps %				
eth1		3.88M 18.02M	lb 1.08K lb 1.84K	17.60MD 3.61Mb	1K 603				
Mb		(RX Bits/s	econd)		M	b	(TX Bits	/second)	
76.99					. 18.9	9			
64.16					. 15.8	3 6			
38.50					. 9.5	9 9			
25.66					6.3	3			
12.83 ::	[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[[:::::::			3.1	7 : :			
1 5 16	9 15 20	25 30	35 40 45	50 55 60)	1 5 10 15	20 25 3	0 35 40	45 50 55 60
	RX	тх		RX	тх		RX	тх	
Bits	1.88Gb	192.68Mb	Packets	201.00K	133.75K	Abort Error		0	
Carrier Error	-	Θ	Collisions	-	0	Compressed	0	0	
CRC Error	0	-	Dropped Frame Frree	0	0	Errors	Θ	0	
	0	0	TCMPv6 Errors	0	- 0	The Address Er	0	-	
Ip6 Broadcast	0	0	Ip6 Broadcast	0	0	Ip6 Delivers	0		
Ip6 Forwarded	-	0	Ip6 Header Err	õ		Ip6 Multicast	0	0	
Ip6 Multicast	0	Θ	Ip6 No Route	Θ	Θ	Ip6 Reasm/Frag	Θ	Θ	
Ip6 Reasm/Frag	Θ	Θ	Ip6 Reasm/Frag	Θ	Θ	Ip6 Reassembly	Θ		
Ip6 Too Big Er	0	-	Ip6 Truncated	0	-	Ip6 Unknown Pr	0	-	
IpoDiscards	0	Θ	Missed Error	0	0	IDOPKIS Multicast	0	0	
Over Error	0	-	Window Error	-	0	nuccicasc		•	
		1505	5]	h d t					
MIU TfIndex		1500	Address	proadcast, mul		Broadcast	ff.ff. ff .	up ff.ff.ff	
Mode		default	TXOlen	00.00.25	1000	Family		unspec	
Alias		acruate	Qdisc		ofifo fast			anopee	
Fri Dec 22 15:17:3	34 2017								Press ? for help

IMPORTANT:

- Press "q" to quit
- Press "?" for help

9.2.3 Traceroute and Latency Test

This test is particular important to check your internet path to Zscaler nodes and the quality of your link.

This Test does a MTR (MyTraceRoute) Tests to the Primary ZEN, Secondary ZEN, Google DNS and if the tunnel is UP, it check the reverse path from your ZEN active to your public IP (you don't need to open a ticket to Zscaler requesting this any more)

9.2.3.1 Traceroute and Latency Test with the tunnel "Not Active"

If the tunnel is active, the MTR test will run through the tunnel. In some cases, you may want to do this test direct from your Location without the tunnel. In order to do this test, you need to put the tunnel "Not active". The easiest way is to go to the Zscaler console and to change the credentials of the location for some fake values, like:

١	VPN Credentials		
	fakecredential@maidenheadbridge.com	•	

Wait about 3 minutes and check "Show Configuration and Status". You will receive the following result:



Now, we can run the "Traceroute and Latency Test" with the tunnel not active.

Here an example of the test:

Here an example of the test:

Selection: 6 My TraceRoute (MTR) Test Report This test does 10 probes to the Primary ZEN, Secondary ZEN, Google DNS 8.8.8.8 Notes: When the tunnel is UP, this test runs through the tunnel When the tunnel is UP, a Reverse Path test from the active ZEN to your Public IP is performed Max Hops is equal 30. This test can take a while Testing Primary ZEN: AutoPrimary : vpn.zscalerbeta.net > 165.225.72.39 Start: Mon Oct 16 19:10:10 2017 HOST: CAS00027 Loss% Snt Last Avg Best Wrst StDev 0.5 3.7 192.168.1.254 0.0% 10 0.5 0.6 0.7 0.0 2. AS13037 losubs.subs.bng2.th-lon.zen.net.uk (62.3.80.21) 0.0% 4.0 4.0 4.2 0.0 5.2 3.7 3. AS13037 ae1-183.cr2.th-lon.zen.net.uk (62.3.86.82) 0.0% 10 5.3 4.2 6.6 0.7 3. AS13037 ael-183.cr2.th-lon.zen.net.uk (62.3.86.82)
4. AS??? ge-3-3-0.mprl.lhr3.uk.above.net (195.66.236.76)
5. AS6461 ae6.mpr3.lhr3.uk.zip.zayo.com (64.125.21.21)
6. AS6461 ae27.cs1.lhr15.uk.eth.zayo.com (64.125.30.234)
7. AS6461 ae2.cs1.ams10.nl.eth.zayo.com (64.125.29.16)
8. AS6461 ae0.cs1.ams17.nl.eth.zayo.com (64.125.29.81)
9. AS6461 ae2.cs1.fra6.de.eth.zayo.com (64.125.29.58)
10. AS6461 ae27.mprl.fra4.de.zip.zayo.com (64.125.30.255)
11. AS6461 ae27.mprl.fra4.de.zip.zayo.com (64.125.30.255)
12. AS6461 94.31.32.194.IPYX-069051-027-ZY0.zip.zayo.com (94.31.32.194) 4.2 3.4 0.0% 5.2 0.3 0.0% 10 4.4 4.4 3.9 4.9 0.0 14.9 15.3 0.0% 10 14.7 16.7 0.3 15.0 14.6 0.0% 10 14.6 15.2 0.0 17.3 14.9 20.8 0.0% 10 16.7 2.3 0.0% 10 15.4 15.2 14.9 15.8 0.0 15.7 14.7 0.0% 10 15.5 21.1 1.8 16.2 15.2 14.7 14.7 15.3 19.4 0.0% 10 1.8 0.0% 10 14.8 16.9 0.6 13. AS62044 165.225.72.39 0.0% 10 15.0 14.8 14.6 15.0 0.0 Testing Secondary ZEN: AutoSecondary : secondary.vpn.zscalerbeta.net > 104.129.194.39 Start: Mon Oct 16 19:10:28 2017 Avg 0.5 HOST: CAS00027 Last Best Wrst StDev Loss% Snt 0.5 0.5 0.6 1. AS??? 192.168.1.254 0.0% 10 0.0 2. AS13037 losubs.subs.bng2.th-lon.zen.net.uk (62.3.80.21) 3.9 3.9 3.3 4.5 0.0% 10 0.0 3. AS13037 ae1-183.cr2.th-lon.zen.net.uk (62.3.86.82) 7.5 0.0% 10 6.2 4.3 22.0 5.2 3. AS13037 ael-183.cr2.th-lon.zen.net.uk (62.3.86.82)
4. AS??? ge-3-3-0.mpr1.lhr3.uk.above.net (195.66.236.76)
5. AS6461 ae6.mpr3.lhr3.uk.zip.zayo.com (64.125.21.21)
6. AS6461 ae27.cs1.lhr15.uk.eth.zayo.com (64.125.30.234)
7. AS6461 ae5.cs1.dca2.us.eth.zayo.com (64.125.30.247)
9. AS6461 ae3.mpr3.iad1.us.zip.zayo.com (64.125.30.247)
9. AS6461 ae3.mpr3.iad1.us.zip.zayo.com (64.125.31.142)
10. AS6461 208.185.155.194.IPYX-069051-015-ZY0.above.net (208.185.155.194) 0.0% 10 5.1 4.2 3.7 0.0 4.5 4.5 4.3 5.0 0.0% 10 0.0 79.5 79.8 79.5 0.0% 10 79.9 0.0 87.0 79.4 100.4 0.0% 10 83.0 6.7 0.0% 10 78.9 79.2 78.9 79.7 0.0 79.4 82.9 79.2 102.9 0.0% 10 7.9 79.4 79.2 0.0% 10 79.3 79.7 0.0 0.0% 10 79.7 80.2 79.5 85.2 1.6 12. AS22616 104.129.194.39 0.0% 10 79.5 79.6 79.2 80.0 0.0 Testing Google DNS 8.8.8.8 Start: Mon Oct 16 19:10:44 2017 Avg 0.6 HOST: CAS00027 Loss% Snt Last Best Wrst StDev 0.6 0.6 0.7 192.168.1.254 0.0% 10 0.0 2. AS13037 losubs.subs.bng2.th-lon.zen.net.uk (62.3.80.21) 3.9 3.9 4.1 0.0% 10 3.7 0.0 4.3 5.5 4.3 7.0 3. AS13037 ae1-183.cr2.th-lon.zen.net.uk (62.3.86.82) 0.0% 10 0.9 4. AS15169 72.14.223.28 0.0% 10 4.9 4.2 3.9 4.9 0.0 5. AS15169 108.170.246.193 10 5.0 5.6 0.0% 5.1 4.6 0.0 6. AS15169 108.170.233.227 10 6.3 6.0 0.0% 6.3 0.0 7. AS15169 google-public-dns-a.google.com (8.8.8.8) 5.9 5.4 5.9 0.0% 10 5.6 0.0 Reverse Path Test No active tunnel. Reverse Path Test runs only when tunnel is active

9.2.3.2 Traceroute and Latency Test with the tunnel "Active"

When the tunnel is active the test runs from inside the tunnel. This is particular useful to see path from the Zscaler Cloud and to see the Reverse Path from the active node to your Public IP.

First, Check that the tunnel is active from the "Show Configuration and Status" menu.

```
ZSCALER INFORMATION
Zscaler Cloud: zscalerbeta
Primary ZEN node: AutoPrimary | Hostname: vpn.zscalerbeta.net | IP: 165.225.72.39 is Alive
Secondary ZEN node: AutoSecondary | Hostname: secondary.vpn.zscalerbeta.net | IP: 104.129.194.39 is Alive
TUNNEL INFORMATION
The Node active is the: AutoPrimary
IPsec uptime: 32 seconds, since Oct 16 19:18:28 2017
Last Security Association: ESTABLISHED 27 seconds ago
CREDENTIALS INFORMATION
Username: CAS00027@maidenheadbridge.com | PSK: Not shown for security reasons. Please, read it from 'VPN Credentials' Menu
http://ip.zscaler.com INFORMATION
You are accessing this host via a Zscaler BETA proxy hosted at Frankfurt IV in the zscalerbeta.net cloud.
Your Gateway IP Address is 82.68.6.78
```

And run the "Traceroute and Latency Test" after:

Here an example of the test with the tunnel active.

```
Selection: 6
My TraceRoute (MTR) Test Report
This test does 10 probes to the Primary ZEN, Secondary ZEN, Google DNS 8.8.88
Notes:

    When the tunnel is UP, this test runs through the tunnel

  When the tunnel is UP, a Reverse Path test from the active ZEN to your Public IP is performed
 Max Hops is equal 30. This test can take a while
Testing Primary ZEN: AutoPrimary : vpn.zscalerbeta.net > 165.225.72.39
Start: Mon Oct 16 19:22:17 2017
                                               Last Avg Best Wrst StDev
15.6 15.5 15.3 15.6 0.0
HOST: CAS00027
                              Loss%
                                        Snt
  1. AS62044 165.225.72.39 0.0%
                                         10
Testing Secondary ZEN: AutoSecondary : secondary.vpn.zscalerbeta.net > 104.129.194.39
Start: Mon Oct 16 19:22:32 2017
H0ST: CAS00027
                                                                      Loss%
                                                                               Snt
                                                                                      Last
                                                                                              Avg Best Wrst StDev
                                                                                      0.0
                                                                                                    0.0
                                                                                                          0.0
                                                                      100.0
              ???
                                                                                10
                                                                                             0.0
                                                                                                                  0.0
                                                                                            23.9
  2. AS62044 165.225.72.2
                                                                       0.0%
                                                                                10
                                                                                      23.3
                                                                                                   20.2
                                                                                                          29.2
                                                                                                                  3.5
                                                                                                         28.8
  3. AS3257 xe-3-0-7.crl-fra2.ip4.gtt.net (46.33.89.9)
                                                                       0.0%
                                                                                            24.1 16.9
                                                                                10
                                                                                      21.7
                                                                                                                  3.3
 4. AS3257 xe-1-0-5.cr0-was1.ip4.gtt.net (213.254.214.150)
5. AS3257 zscaler-gw.ip4.gtt.net (77.67.68.146)
                                                                       0.0%
                                                                                10
                                                                                   107.0 106.1 101.5 110.3
                                                                                                                  3.0
                                                                                    108.5 109.7 102.7 131.7
                                                                       0.0%
                                                                                10
                                                                                                                  8.5
  6. AS22616 104.129.194.39
                                                                                    103.5 108.3 102.3 121.5
                                                                       0.0%
                                                                                10
                                                                                                                  6.3
Testing Google DNS 8.8.8.8
Start: Mon Oct 16 19:22:47 2017
HOST: CAS00027
                                                              Loss%
                                                                       Snt
                                                                              Last
                                                                                      Avg
                                                                                           Best
                                                                                                 Wrst StDev
  1. AS???
                                                                                            0.0
                                                                                                   0.0
              ???
                                                              100.0
                                                                              0.0
                                                                                     0.0
                                                                                                          0.0
                                                                        10
                                                                                    27.0
  2. AS62044 165.225.72.2
                                                               0.0%
                                                                        10
                                                                              35.6
                                                                                           20.5
                                                                                                  35.6
                                                                                                          5.6
  3. AS??? de-cix.fra.google.com (80.81.192.108)
                                                               0.0%
                                                                        10
                                                                              21.8
                                                                                    25.1
                                                                                           20.4
                                                                                                  30.5
                                                                                                          3.2
                                                                              0.0
                                                                                     0.0
                                                                        10
                                                                                            0.0
                                                                                                   0.0
              ???
                                                              100.0
                                                                                                          0.0
  5. AS15169 216.239.48.93
                                                               0.0%
                                                                        10
                                                                              29.9
                                                                                    25.5
                                                                                           20.4
                                                                                                  32.9
                                                                                                          4.1
  6. AS15169 google-public-dns-a.google.com (8.8.8.8)
                                                                              25.0
                                                                                    25.0
                                                                                           19.2
                                                                                                  35.8
                                                               0.0%
                                                                        10
                                                                                                          4.7
Reverse path from: AutoPrimary to your Public IP: 82.68.6.78
Start: Mon Oct 16 19:23:03 2017
HOST: CAS00027
                                                                        Loss%
                                                                                        Last
                                                                                                Avg
                                                                                                     Best
                                                                                 Snt
                                                                                                            Wrst StDev
                                                                        100.0
                                                                                        0.0
                                                                                               0.0
                                                                                                      0.0
                                                                                                             0.0
                                                                                                                    0.0
                                                                                  10
              ???
  2. AS62044 165.225.72.2
                                                                                               23.0
                                                                         0.0%
                                                                                  10
                                                                                        20.7
                                                                                                     19.6
                                                                                                            26.5
                                                                                                                     2.3
                                                                                        23.4 25.4
  3. AS6461 xe-9-2-1.mpr1.fra4.de.zip.zayo.com (94.31.32.193)
                                                                         0.0%
                                                                                  10
                                                                                                     19.4
                                                                                                            40.5
                                                                                                                     6.1
                                                                                              23.9
  4. AS6461 ae8.mpr1.fra3.de.zip.zayo.com (64.125.26.233)
5. AS6461 ae27.cs1.fra6.de.eth.zayo.com (64.125.31.216)
                                                                                        17.2
                                                                                                     17.2
                                                                         0.0%
                                                                                                            31.4
                                                                                                                    4.6
                                                                         0.0%
                                                                                   10
                                                                                        41.2
                                                                                               39.6
                                                                                                     27.0
                                                                                                            46.3
                                                                                                                    5.6
  6. AS6461 ae2.cs1.ams17.nl.eth.zayo.com (64.125.29.59)
                                                                         0.0%
                                                                                  10
                                                                                        28.8
                                                                                              35.8
                                                                                                     27.6
                                                                                                            52.2
                                                                                                                     8.4
 7. AS6461 ae0.cs1.ams10.nl.eth.zayo.com (64.125.29.80)
8. AS6461 ae2.cs1.lhr15.uk.eth.zayo.com (64.125.29.17)
9. AS6461 ae27.mpr3.lhr3.uk.zip.zayo.com (64.125.30.235)
                                                                         0.0%
                                                                                        34.3 33.8
                                                                                                     26.7
                                                                                                            41.8
                                                                                                                    4.1
                                                                                        34.3
                                                                                               34.3
                                                                         0.0%
                                                                                  10
                                                                                                     27.2
                                                                                                            42.2
                                                                                                                     5.0
                                                                                                     27.5
                                                                         0.0%
                                                                                  10
                                                                                        32.9
                                                                                              31.1
                                                                                                            34.0
                                                                                                                    2.2
 10. AS6461 ae13.mpr1.lhr15.uk.zip.zayo.com (64.125.30.55)
                                                                         0.0%
                                                                                  10
                                                                                        37.3 38.2
                                                                                                     28.5
                                                                                                            64.9
                                                                                                                   12.4
 11. AS??? linx-1.zen.net.uk (195.66.224.158)
12. AS13037 ge-2-0-0-0.cr1.th-lon.zen.net.uk (62.3.80.41)
                                                                                        34.5 33.2
34.0 32.0
                                                                                                     28.1
                                                                         0.0%
                                                                                  10
                                                                                                            37.7
                                                                                                                    2.8
                                                                         0.0%
                                                                                                     27.6
                                                                                                            35.5
                                                                                                                    2.6
                                                                                  10
 13. AS13037 v182.subs.bng2.th-lon.zen.net.uk (62.3.86.81)
                                                                         0.0%
                                                                                  10
                                                                                        45.0
                                                                                              33.8
                                                                                                     28.9
                                                                                                            45.0
                                                                                                                     4.2
 14. AS13037 82-68-6-78.dsl.in-addr.zen.co.uk (82.68.6.78)
                                                                         0.0%
                                                                                  10
                                                                                        38.5 35.1
                                                                                                     30.3
                                                                                                            42.3
                                                                                                                    4.0
```

Please note that the amount of Hops to the tunnel active is one:

Testing Primary ZEN: AutoPr	imary :	vpn.zs	calerb	eta.ne	t > 1	.65.225	.72.39
Start: Mon Oct 16 19:22:17	2017						
H0ST: CAS00027	Loss%	Snt	Last	Avg	Best	Wrst	StDev
1. AS62044 165.225.72.39	0.0%	10	15.6	15.5	15.3	15.6	0.0

And the Reverse Path test is done in this case.

9.3 CSC Admin Tasks



- 6. AWS SSM Agent (Register or De-Register)
- 7. Change SSH Password: Allows to change the password of the CSC.
- 8. Change Timezone: In case if needed, you can select your Timezone here.

9.3.1 AWS SSM Agent (Register / De-Register)

One of the main functionalities added after version 3.0 is that the CSC Anywhere can be integrated with the Amazon Cloud (AWS). The CSC Anywhere is now part of the Cloud.

Amazon AWS offers a Free Tier Account (<u>https://aws.amazon.com/free</u>) with some product free for 1 year and others always free. You need to create or to have an AWS account to manage the CSC Anywhere. AWS allows to manage for free up to 1000 managed instances.

The steps required to add the CSC are two:

1. From your EC2 Console, go to SYSTEMS MANAGER SHARED RESOURCES > Activations > Create an activation

Activations > Create Activation	
Create Activation	
Creating a new activation allows you to gen	erate a code which can be used to register a run command agent on instances. Specify the details below to create a new activation:
Activation description	CAS00027
Instance limit	10
IAM Role Name*	 Use the system created default command execution role (AmazonEC2RunCommandRoleForManagedInstances)
	 Select an existing custom IAM role that has the required permissions
Activation expiry date	2017-11-07T00:00+00:00
Default Instance name	CAS00027

Note: We recommend to create an Activation per CSC and on "Default instance name" to put the name of the CSC ID (CASxxxx) or the name of your "Location" for easy identification.

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

Create Activation

Success You have successfully created a new activation (b4e8d912-223e-421d-8efe-e84da0b10e4b). Your activation code is listed below. Copy this code and keep it in a safe place as you will not be able to access it again. Activation Code VvAO0VjkxHqhls8v/UeF Activation ID b4e8d912-223e-421d-8efe-e84da0b10e4b You can now install amazon-ssm-agent and manage your instance using Run Command. Learn more View result

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 "8) AWS SSM Agent (Register or De-Register)"





You will asked for the Activation

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**#)

Please, ingress Activation Code, Activation ID and Region (example: eu-west-1) Activation Code :VvAO0VjkxHqhls8v/UeF Activation ID :b4e8d912-223e-421d-8efe-e84da0b10e4b Region :eu-west-1

If the AWS SSM agent is registered successfully you will receive the following message:

2017/10/16 18:11:33 Failed to load instance info from vault. RegistrationKey does not exist. 2017-10-16 18:11:48 INFO Successfully registered the instance with AWS SSM using Managed instance-id: mi-0100217713cd99941

Done! You have the CSC integrated with AWS now with the instance-id "mi-xxxxxxx" (mi-0100217713cd99941" in this case).

Go to your EC2 Console (SYSTEMS MANAGER SHARED RESOURCES > Managed Instances) and you will be able to see your CSC registered as an instance:

aws	Services	•	Resource G	roups 🗸 🏷						
indle Tasks	•	Ru	n a command	Create Association	Setup Inventory	Resource Data Syncs	Actions V			
ASTIC BLOCK		Q	Filter by attribute	95						
lumes apshots			Name	Instance ID	Ping status	Platform Type	Platform Na	ne Agent Version	IP Address	Computer Name
TWORK &			CAS00027	mi-010021771	3cd9 🥥 Online	Linux	Ubuntu	2.2.30.0	192.168.1.40	CAS00027

9.3.1.1 Checking the status of the AWS SSM agent

The "Show Configuration and Status" Menu shows the status of the AWS SSM agent at the bottom.

```
AWS SSM AGENT
AWS SSM Agent is active (running) since Mon 2017-10-16 18:11:48 BST; 8min ago
Registration values: {"ManagedInstanceID":"mi-0100217713cd99941","Region":"eu-west-1"}
```

9.3.2 Change SSH Password

From this menu, you can change the SSH Password of the Admin Console.

9.3.3 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.

9.4 Bypass Proxy

The Bypass Proxy allows you to connect certain allowed 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.



Important about domains and wildcards. The CSC uses the same nomenclature than Zscaler, but the PAC files are different. Please not the following examples:

CSC	PAC file					
Www.example.com	Www.example.com					
.example.com	*.example.com					
Important! Be careful not to create an "Open Proxy" setting something like ".com" that will						

allow to pass all domains ending on ".com"

9.4.1 View Current Bypass List

This commands shows the current domains and subdomains allows to go direct to Internet

9.4.2 Configure Bypass List

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



9.4.2.1 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:

<u>http://pac</u>.<yourcloudname>.net/<yourdomain>/cscbypass.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 2.2.2.3128";
    //* CSC bypass*/
    if ((shExpMatch(host, "*.firstdomain.com")) ||
        (shExpMatch(host, "www.fulldomain.co.uk")) ||
        (shExpMatch(host, "*.anotherdomain.com")) ||
        (shExpMatch(host, "*.salesforce.com")) ||
        (shExpMatch(host, "*.lastdomain.com"))){
        return bypassproxy
    }
}
```

Important Note: 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: You can use the lines in **bold** to copy/paste in your production pac file. Please, pay attention to replace 1.1.1.1 and 2.2.2.2 for your real Bypass proxy addresses.

Bypass Proxy on the Zscaler Console:

Edit PAC File	×
PAC File	
Description	PAC File Name
CSC Bypass Proxy	cscbypass.pac
Domain	Obfuscate URL
maldenheadbridge.com 👻	
AC File Contents function FindProxyForURL(url, host) { var bypassproxy=PROXY 10.1.1.3122 /*CCF bypassf/ if (chExpMath(host, **.firstdd (shExpMath(host, **.slesfor (shExpMath(host, **.slesfor (shExpMath(host, **.lastdor) })	; PROXY 10.2.2.2:3128"; main.com")). domain.co.vt*)) domain.com")) uin.com"))){ Verify
Save Cancel	Delete

For example, here is a production pac file with the bypasses added:

Edit PAC File		×
PAC File		
Description	PAC File Name	
pacha	pacha.pac	
Domain	Obfuscate URL	
maldenheadbridge.com	✓	
PAC File Contents		
36 var byDassprox/= PKU 37 var byDassprox/= PKU 39 if ((shExpMatch(host, 40 (shExpMatch(host, 41 (shExpMatch(host, 42 (shExpMatch(host, 43 (shExpMatch(host, 44 return byDassproxy	<pre>[Y 172.19.6.217:3128; PMOX 192.168.1.220:3128; **.firstdomain.co.w")) **ww.fulldomain.co.w")) **.satesforce.com")) **.satesforce.com")) **.lastdomain.co.w"))){ </pre>	•
46 47 48 49 49 50 51 51 51 51 51 51 51 51 51 51	: www.company.com (overwriting b) sentence *.company.com) "www.company.com"))){	Ì.
52 // b) Bypass Internal 53	. domains and subdomains: intranet.company.com, *.mail.company.	
54 if ((shExpMatch(host, 55 (shExpMatch(host, 56 (shExpMatch(host, 57 return "DIRECT"; 58 3	<pre>"intranet.company.com")) "*.company.com")) "*.mail.company.net"))){</pre>	•
59 4	••••••••••••••••••••••••••••••••••••••	
	Verify	
Save Cancel	Delete	•

Important: Proxy Bypass is reachable only on port TCP 3128

Configuration Steps:

1. Select 1) Auto – Bypass PAC URL, you are invited to change the Bypass PAC URL, here an screenshoot:



2. The next step will show the Bypass URL in use and will invite to update the list:

Your current Bypass PAC URL is: http://pac.zscalerbeta.net/maidenheadbridge.com/cscbypass.pac Do you want to refresh Bypass List? (y/n)?



- 3. The CSC retrieves the list of bypasses from the Zscaler cloud
- 4. Press "y" and you will receive a notification or error message.

```
Do you want apply changes? (y/n)? y
Bypass List updated sucessfully
```

5. Verify the list using menu 11)



9.4.2.2 2) Manual

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

1. Select Option 2)



2. Ingress "y"

GNU nano 2.5.3		File:	domains		Modified
.firstdomain.com www.fulldomain.co .anotherdomain.co .salesforce.com .lastdomain.com www.manualentry.c .manualwithsubdom	.uk m om ains.co.uk <mark>.</mark>				
<mark>^G</mark> Get Help <mark>^0</mark> ^X Exit ^R	Write Out Read File	₩ Where Is \ Replace	s <mark>^K</mark> Cut Text <mark>^U</mark> Uncut Text	<mark>^J</mark> Justify <mark>^T</mark> To Spell	^C Cur Pos ^_ Go To Line

- 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:

```
Do you want apply changes? (y/n)? y
Bypass List updated sucessfully
```

10 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.

10.1 Web Logs

Go to Analytics > Web Insights

Click Logs and Filter by Location [cas00016 in this example is the name of the Location]

	¢	~								
📥 Logs										
Apply Filters										
. Choose a Timeframe										
Current Day: 9)/6/2017 🔻									
3. Select Filters			X Clear Filters							
Location			×							
cas00016			-							
Add Filter			•							

Apply Filters:

Web Insights

No.	Logged Time	User	URL	Policy Action	URL Category	Client IP	Server IP
158	Wednesday, September 06, 2017 7:24:20	first1last1@maidenheadbri	www.bbc.co.uk:443	Allowed	News and Media	172.19.0.140	212.58.246.93
159	Wednesday, September 06, 2017 7:24:20	first1last1@maidenheadbri	edigitalsurvey.com:443	Allowed	Professional Services	172.19.0.140	46.236.9.36
160	Wednesday, September 06, 2017 7:24:20	first1last1@maidenheadbri	edigitalsurvey.com:443	Allowed	Professional Services	172.19.0.140	46.236.9.36
161	Wednesday, September 06, 2017 7:24:20	first1last1@maidenheadbri	edigitalsurvey.com:443	Allowed	Professional Services	172.19.0.140	46.236.9.36
162	Wednesday, September 06, 2017 7:24:20	first1last1@maidenheadbri	homepage.files.bbci.co.uk:443	Allowed	News and Media	172.19.0.140	172.227.98.43
163	Wednesday, September 06, 2017 7:24:20	first1last1@maidenheadbri	ssl.bbc.co.uk:443	Allowed	News and Media	172.19.0.140	212.58.244.114
164	Wednesday, September 06, 2017 7:24:20	first1last1@maidenheadbri	search.files.bbci.co.uk:443	Allowed	News and Media	172.19.0.140	172.227.98.43
165	Wednesday, September 06, 2017 7:24:20	first1last1@maidenheadbri	nav.files.bbci.co.uk:443	Allowed	News and Media	172.19.0.140	172.227.98.43
166	Wednesday, September 06, 2017 7:24:20	first1last1@maidenheadbri	static.bbc.co.uk:443	Allowed	News and Media	172.19.0.140	172.227.98.43

As you can see, you have full visibility of the Client IP [172.19.0.140 in this case]

More in detail:

Client IP	Server IP
172.19.0.140	212.58.246.93
172.19.0.140	46.236.9.36
172.19.0.140	46.236.9.36
172.19.0.140	46.236.9.36
172.19.0.140	172.227.98.43

10.2 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 [cas00016 in this example is the name of the Location]

1. Select Chart 7	Гуре						
	¢	~					
	۵ ا	.ogs					
	Apply	Filters					
2. Choose a Timeframe							
Last 1 Minut	e: 9/6/2017 7:4	42:35 AM - 9/	′6/20 v				
3. Select Filters			X Clear Filters				
Location			×				
cas00016	1		-				
Add Filter			-				

Apply Filters

Firewall Insights

No.	Logged Time	DNAT Rule N	User	Location	Client Source IP	Server Destination IP	Rule Name	Network Service	Network A
16	Wednesday, September 06, 2017 7:42:39	None	first1last1@maidenhead	cas00016	172.19.0.140	8.8.4.4	Default Firewa	DNS	DNS
17	Wednesday, September 06, 2017 7:42:42	None	first1last1@maidenhead	cas00016	172.19.0.140	91.190.217.135	Default Firewa	TCP	TCP
18	Wednesday, September 06, 2017 7:42:43	None	first1last1@maidenhead	cas00016	172.19.0.140	157.55.56.164	Default Firewa	TCP	TCP
19	Wednesday, September 06, 2017 7:42:49	None	first1last1@maidenhead	cas00016	172.19.0.140	91.190.217.135	Default Firewa	TCP	TCP
20	Wednesday, September 06, 2017 7:42:56	None	first1last1@maidenhead	cas00016	172.19.0.140	74.125.133.188	Default Firewa	TCP	TCP
21	Wednesday, September 06, 2017 7:43:00	None	first1last1@maidenhead	cas00016	172.19.0.140	91.190.217.135	Default Firewa	TCP	TCP

More in detail:

Client Source IP	Server Destination IP
172.19.0.140	8.8.4.4
172.19.0.140	91.190.217.135
172.19.0.140	157.55.56.164
172.19.0.140	91.190.217.135
172.19.0.140	74.125.133.188
172.19.0.140	91.190.217.135

11 Troubleshooting

11.1 If the tunnels are not connecting

The "Configuration and Status" menu is providing all information required and is doing all checks for you. Start doing this command to verify everything, from configuration to reachability of gateways, DNS and Zscaler nodes.

According our experience, the most common issues are related to this:

- 1. Is the upstream device (broadband router, firewall, etc.) is running properly and NOT blocking PING (echo-request / echo-reply), UDP port 500 and 4500, DNS, HTTP/HTTPS?
- 2. Are Vmware interfaces are properly mapped?

Please, note that the **first interface** is **EXTERNAL** and the **second** is **INTERNAL**.

In this example:

- Network adapter 1 (EXTERNAL interface) is mapped to Net-192-168-1-0.

- Network adapter 2 (INTERNAL interface) is mapped to Net-172-19-0-0.



3. Did you imported the VPN Credentials and created the Location on the Zscaler GUI?

Please, see section 5) Creating the Location on Zscaler GUI on this guide.

4. Are the configuration values correct? Check all values again using "Configuration and Status" menu.

11.2 Proxy Bypass

11.2.1 How to check if the Proxy Bypass is active?

Open a browser, type the IP of your proxy bypass plus (:) proxy port 3128, here the format:

http://<your bypass proxy ip>:3128

For example: <u>http://172.19.0.217:3128/</u>

and you will received the following page:

← → C ③ 172.19.0.217:3128

Cloud Security Connector

Cloud Security Connector (CSC ID: cas00101) says:

Bypass Proxy is active

Generated Sat, 23 Dec 2017 08:25:25 GMT by cas00101

Please, note that the CSC ID is showed in this notification. This helps administrators to identify the CSC in case is needed.

11.2.2 If you added the bypass in the PAC but forgot to update the CSC

In the case the bypass Domain Host is in your production PAC file but not configured on the CSC, the user will received the following message:

← → C ③ www.primerdomain.com
 Cloud Security Connector
 Error Message: The requested URL could not be retrieved
 Cloud Security Connector (CSC ID: cas00101) says:
 The URL <u>http://www.primerdomain.com/</u> you are trying to reach is in your "PAC file Bypass Proxy List" but not configured on the Cloud Security Connector ID: cas00101
 Please, contact your organization IT Team or Help Desk

Generated Sat, 23 Dec 2017 08:32:48 GMT by cas00101

11.3 PAC file troubleshooting

Please, for all this test use "Google Chrome"

11.3.1 How to check what PAC file URL is applied?

Using Google Chrome, go to:

chrome://net-internals/#proxy

You will receive the following screen:

$oldsymbol{\epsilon}$ $ ightarrow$ $oldsymbol{C}$ Chrome $ $	chrome:// net-internals /#proxy								
capturing events (1973)									
Capture									
Import	Re-apply settings								
Proxy	Effective proxy settings								
Events	PAC script: http://pac.zscalerbeta.net/JT5LQFYF015N/pacha.pac								
Timeline									
DNS									

11.3.2 How to Check if the Domain destination is using VIP Proxy or Bypass Proxy?

Using Google Chrome, do the following steps:

- 1. Open in one tab the domain you are looking for. For example: www.salesforce.com
- 2. Open another tab and type: chrome://net-internals/#events
- 3. On the Sort & Filter field (?) type: <domain> & http_stream_job_controller. In this example we are going to put salesforce.com & http_stream_job_controller
- 4. Refresh the page on the tab that contains www.salesforce.com
- 5. Go back to the events tab and click on any event that this HTTP_STREAM_JOB_CONTROLLER and contains the <domain> at the beginning

In the next example, you can see that <u>www.salesforce.com</u> is:

- Matching the CONFIGURED proxy string "PROXY 172.19.0.217:3128;PROXY 192.168.1.220:3128" of the PAC file in use.
 (PROXY_SERVICE_RESOLVED_PROXY_LIST, --> pac_string = "PROXY 172.19.0.217:3128;PROXY 192.168.1.220:3128")
- USING the proxy "PROXY 172.19.0.217:3128" (--> proxy_server = "PROXY 172.19.0.217:3128")

CRM Softw	are & Cloud 🔅	×Ý	Chrome://net-internals// ×				
← → C (Chrome	chro	ome:// net-internals /#events				
capturing eve	ents (18028)					
Capture		(?)	salesforce.com & http_stream_job_c	ontroller	76 of 1096		
Import Proxy			7207 URL_REQUEST	https://v	www.salesforce.com/etc/clientcontext/sfdc-ww	7211: HTTP_STREAM https://www.salesfo	_OB_CONTROLLER prce.com/etc/clientcontext/sfdc-www/content/jcr:content/stores.init.js?path=%2Fcontent%2Fwww%
Events			7211 HTTP_STREAM_JOB_CONTROLL	ER https://v	www.salesforce.com/etc/clientcontext/sfdc-ww	Start Time: 2017-12-2	3 03:23:13:030
Timeline			7221 URL_REQUEST	https://o	dc.ads.linkedin.com/collect/?fmt=gif&pid=543	t=56413 [st=0] -	+HIP_SIREAM_JOB_CONIROLLER [dt=2] > is_preconnect = false
DNS			7224 URL_REQUEST	https://v	www.facebook.com/tr?id=620008638087704&e	t=56413 [st=0]	> url = "https://www.salesforce.com/etc/clientcontext/sfdc-www/content/jcr HTTP STREAM JOB CONTROLLER BOUND
Sockets			7228 URL_REQUEST	https://v	www.facebook.com/tr?id=1424193781160198&	t=56413 [st=0]	> source dependency = 7207 (URL_REQUEST) +PROXY_SERVICE [dt=1]
Alt-Svc			7244 URL_REQUEST	https://g	go.affec.tv/i/5575ca3d95cfa4000ce63d1d	t=56414 [st=1]	+HOST_RESOLVER_IMPL_REQUEST [dt=0]
HTTP/2			7262 URL_REQUEST	https://v	www.facebook.com/tr?id=1424193781160198&		> allow cached response = true
QUIC			7281 URL_REQUEST	https://o	omtr2.partners.salesforce.com/b/ss/salesforcer		> nost = "www.salestorce.com:80" > is_speculative = false Configured
Cache			7285 URL_REQUEST	https://o	d.adroll.com/ipixel/2ZCUYMULN5AQRHP3F45E2	t=56414 [st=1]	HOST_RESOLVER_IMPL_CACHE_HIT > address_list = ["96.43.148.26:80","96.43.149.26:80"]
Modules			7289 URL_REQUEST	https://g	googleads.g.doubleclick.net/pagead/viewthrou	t=56414 [st=1] t=56414 [st=1]	-HOST RESOLVER IMPL REQUEST PROXY SERVICE RESOLVED PROXY LIST
Domain Secu	urity Policy		7293 HTTP_STREAM_JOB_CONTROLL	ER https://o	omtr2.partners.salesforce.com/b/ss/salesforcer	t-56414 [st-1]	> pac_string = "PROXY 172.19.0.217:3128;PROXY 192.168.1.220:3128"
Bandwidth			7295 HTTP_STREAM_JOB_CONTROLL	R https://g	googleads.g.doubleclick.net/pagead/viewthrou	t=56414 [st=1]	HTTP_STREAM_JOB_CONTROLLER_PROXY_SERVER_RESOLVED In use
Prerender			7315 URL_REQUEST	https://p	onapi.invoca.net/1/api/2014-09-01/map_numbe	t=56414 [st=1]	HTTP_STREAM_REQUEST_STARTED_JOB
			7318 HTTP_STREAM_JOB_CONTROLL	R https://p	onapi.invoca.net/1/api/2014-09-01/map_numbe	t=56415 [st=2]	> source_dependency = 7212 (HTTP_STREAM_JOB) -HTTP STREAM JOB CONTROLLER
			TOT UNL DEOLISET	L	1 1 - 4 - 9 - JE., 1 - JE., 15		

In this example, <u>www.salesforce.com</u> is using the Bypass proxy:								
INTERFACES INFORMATION								
External Interface (eth0) IP: 192.168.1.215/24 External Gateway: 192.168.1.254 is Alive								
Internal Interface (eth1) IP: 172.19.0.215/24 Internal Gateway: 172.19.0.200 is Alive								
VIP Proxy: 172.19.0.216								
Bypass Proxy: 172.19.0.217								
Please, remember that Bypass Proxy uses port tcp 3128.								

Example of a domain host that is using the VIP Proxy:

Following the previous steps, we are going to inspect the domain "<u>www.google.co.uk</u>"

G Google	×Y	🗅 ch	rome://net-internals// ×						
← → C Schrome chrome://net-internals/#events									
capturing events (4285)	")								
Capture	(?	goog	le.co.uk & http_stream_job_contro	blier 46 of 2409					
Import		ID	Source Type	Description	8665: HTTP_STREAM_JOB_CONTROLLER https://www.google.co.uk/complete/search?rlient=chrome-omnikgs_ri=chrome-ext-ansg&yssi=t&g=g&oit=1&cn=1&u				
Proxy		8662	URL_REQUEST	https://www.google.co.uk/complete/search?client=chro	Start Time: 2017-12-23 09:57:17.096				
Timeline		8665	HTTP_STREAM_JOB_CONTROLLER	https://www.google.co.uk/complete/search?client=chro	t=1740479 [st= 0] +HTTP_STREAM_JOB_CONTROLLER [dt=127]				
DNS		8673	URL_REQUEST	https://www.google.co.uk/complete/search?client=chro	> url = "https://www.google.co.uk/complete/search?client=chrome-omni				
Sockets		8676	HTTP_STREAM_JOB_CONTROLLER	https://www.google.co.uk/complete/search?client=chre	> source_dependency = 8662 (URL_REQUEST)				
Alt-Svc		8678	URL_REQUEST	https://www.google.co.uk/complete/search?client=chro	t=1740479 [st= 0] +HOST_RESOLVER_IMPL_REQUEST [dt=12]				
HTTP/2		8681	HTTP_STREAM_JOB_CONTROLLER	https://www.google.co.uk/complete/search?client=chre	> allow cached_response = true				
QUIC		8973	URL_REQUEST	https://www.google.co.uk/complete/search/client=chro	> host = "www.googte.co.uk:80" > is speculative = false				
Cache		8983		https://www.google.co.uk/complete/search?client=chr/	t=1740480 [st= 1] HOST RESOLVER IMPL_CREATE_JOB t=1740480 [st= 1] HOST_RESOLVER_IMPL_JOB_ATTACH				
Modules		8986	HTTP STREAM JOB CONTROLLER	https://www.google.co.uk/complete/search?client=chro	t=1740491 [st= 12] -HOST_RESOLVER_IMPL_REQUEST				
Bandwidth		8988	URL_REQUEST	https://www.google.co.uk/complete/search?client=chro	t=1/40492 [st= 13] PROXY_SERVICE_RESOLVED_PROXY_LISI > pac_string = "PROXY_172.19.0.216:80;PROXY_192.168.1.219:80"				
Prerender		8991	HTTP_STREAM_JOB_CONTROLLER	https://www.google.co.uk/complete/search?client=chro	t=1740492 [st= 13] -FROAT SERVICE t=1740492 [st= 13] HTTP_STREAM_JOB_CONTROLLER_PROXY_SERVER_RESOLVED				
		8993	URL_REQUEST	https://www.google.co.uk/complete/search?client=chro	t=1740492 [st= 13] HTTP_STREAM_REQUEST_STARTED_JOB				
		8996	HTTP_STREAM_JOB_CONTROLLER	https://www.google.co.uk/complete/search?client=chro	t=1740606 [st=127] -HTTP_STREAM_JOB_CONTROLLER				

In this case:

• PROXY_SERVICE_RESOLVED_PROXY_LIST

--> pac_string = "PROXY 172.19.0.216:80;PROXY 192.168.1.219:80"

• HTTP_STREAM_JOB_CONTROLLER_PROXY_SERVER_RESOLVED

--> proxy_server = "PROXY 172.19.0.216:80"

In this example, <u>www.google.com</u> is using the VIP proxy: INTERFACES INFORMATION External Interface (eth0) IP: 192.168.1.215/24 | External Gateway: 192.168.1.254 is Alive Internal Interface (eth1) IP: 172.19.0.215/24 | Internal Gateway: 172.19.0.200 is Alive VIP Proxy: 172.19.0.216 Bypass Proxy: 172.19.0.217 Please, remember that VIP Proxy uses port tcp 80 or 9400.

12 Maidenhead Bridge Contact Information

Website: <u>www.maidenheadbridge.com</u>

Sales enquiries: sales@maidenheadbridge.com

Support: <u>http://support.maidenheadbridge.com</u>

13 APPENDIX A

13.1 Improvements of Version 4.0

13.1.1 New! Bypass Proxy functionality

The Bypass Proxy solves the problem when is required to send traffic direct to internet and not via Zscaler ZEN nodes.

The most common case is when destination web site accepts only traffic coming from a specific public IP.

Without the Bypass Proxy, customers where obligated to have an internal proxy or to configure several firewall rules and routes to the destinations required to be bypassed.

The Bypass Proxy simplifies this task: using the Zscaler PAC files servers as repository of your bypasses and automating the task with AWS, you can easily get up to date all your bypasses in all CSC instances.

The Bypass Proxy acts as Web Firewall. It only allows to reach domains hosts defined by the Administrator.

13.2 Improvements of Version 3.5

13.2.1 New Model: CSC Anywhere One Arm

The purpose of the CSC Anywhere One Arm is to provide a direct replacement of the Web Security Appliance installed on premises. The CSC Anywhere One Arm can be placed on the same subnet than the current appliance and the traffic will be redirected to Zscaler directly.

13.2.2 Resilient Algorithm

When returning to the Primary ZEN, Resilient Algorithm checks if the Primary ZEN was stable for 15 minutes before to change nodes.

Timers were adjusted to better support locations with long delays (more than 250 ms) to the ZEN Nodes.

13.3 Improvements of Version 3.2

13.3.1 Traceroute and Latency Test

This test was requested by customers in order to check the quality of the link from the CSC. This allows to check hop-by-hop the quality of the path to Zscaler nodes on the internet.

In addition to this, when the tunnel is active, a Reverse Path check is performed, validating the quality of the path from the Zscaler node to your public IP.

13.4 Speed Test (Experimental)

Another feature requested by customer. Now, you can validate the speed of your internet link from the CSC. We use third party tools to do this. (speedtest.net)

13.5 Improvements of Version 3.0

13.5.1 One Click Configuration and Status report.

There is a new menu on Monitoring tasks: Show Configuration and Status



13.5.2 AWS management

On version 3.0 the CSC Anywhere can be managed from AWS as a "managed instance".

13.5.2.1 CSC Anywhere as "Managed Instance" on EC2 console

Amazon AWS offers on the free account to control up to 1000 managed instances for hybrid environments. The CSC had the AWS SSM pre-installed on the machines. You simply need to register the agent and you will be able to manage the CSC from the AWS Cloud. Here you can see the status of all CSC Anywhere connectors.

C Secure https://eu-west-1.console.aws.amazon.com/ec2/v2/home?region=eu-west-1#ManagedInstances:sort=InstanceId											
aws Service	es 🗸 Resource G	roups 🗸 🍾							<u>م</u> ۸		
Bundle Tasks	Run a command	Create Association Setup	Inventory	Resource Data Syncs A	ctions v						
ELASTIC BLOCK	Q Filter by attribute	95									
Volumes Snapshots	Name	Instance ID	Ping status	Platform Type	Platform Name	Agent Version	IP Address	Computer Name	Association Status		
NETWORK &	CAS00029	mi-027c1440adc7e	Online	Linux	Ubuntu	2.2.24.0	192.168.1.44	CAS00029	Success		
SECURITY	CAS00027	mi-02f0c193846c43	Online	Linux	Ubuntu	2.2.24.0	192.168.1.40	CAS00027	Success		
Security Groups	CAS00031	mi-038783bdee7bd	Online	Linux	Ubuntu	2.2.24.0	192.168.1.48	CAS00031	Success		
Elastic IPs	csc-mgmt	mi-0610b60b7b8bfb	Online	Linux	Debian GNU/Linux	2.0.847.0	192.168.1.252	HQgre73	Success		
Placement Groups	CAS00030	mi-085a6b724b9f8d	Online	Linux	Ubuntu	2.2.24.0	192.168.1.46	CAS00030	Success		
Key Pairs	CAS00032	mi-0dce17139deb5	Online	Linux	Ubuntu	2.2.30.0	192.168.1.32	CAS00032	Success		
Network Interfaces	CAS00028	mi-0df192078ce8a8	Online	Linux	Ubuntu	2.2.24.0	192.168.1.42	CAS00028	Success		
LOAD BALANCING											

13.5.2.2 Executing "Run Commands" or schedule "Associations" on AWS Console

With AWS you can manage the CSC. Here the results of "One Click Configuration and Status Report"



Having the CSC Anywhere as part of the Amazon AWS Cloud is a great achievement. From now, we can have completely remote control of the CSC. Maidenhead Bridge will provide the "Documents" (scripts to execute). On this case, with the AWS Run Commands we are executing the scripts that retrieves the complete configuration and status of the "Location40" (CSC ID: CAS00027)

Note: All management can be done using AWS CLI as well. This allows full Dev Ops automation.

13.5.2.3 Zscaler API ready

Currently Zscaler API is on BETA and not general available, but having the CSC integrated with AWS enables the integration with the Zscaler API.