Maidenhead Bridge

Cloud Security Connector Anywhere

Enabling Zscaler from Any Location

Administrator Guide

Software Version 4.0

(January 2018)

Table of Contents

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.

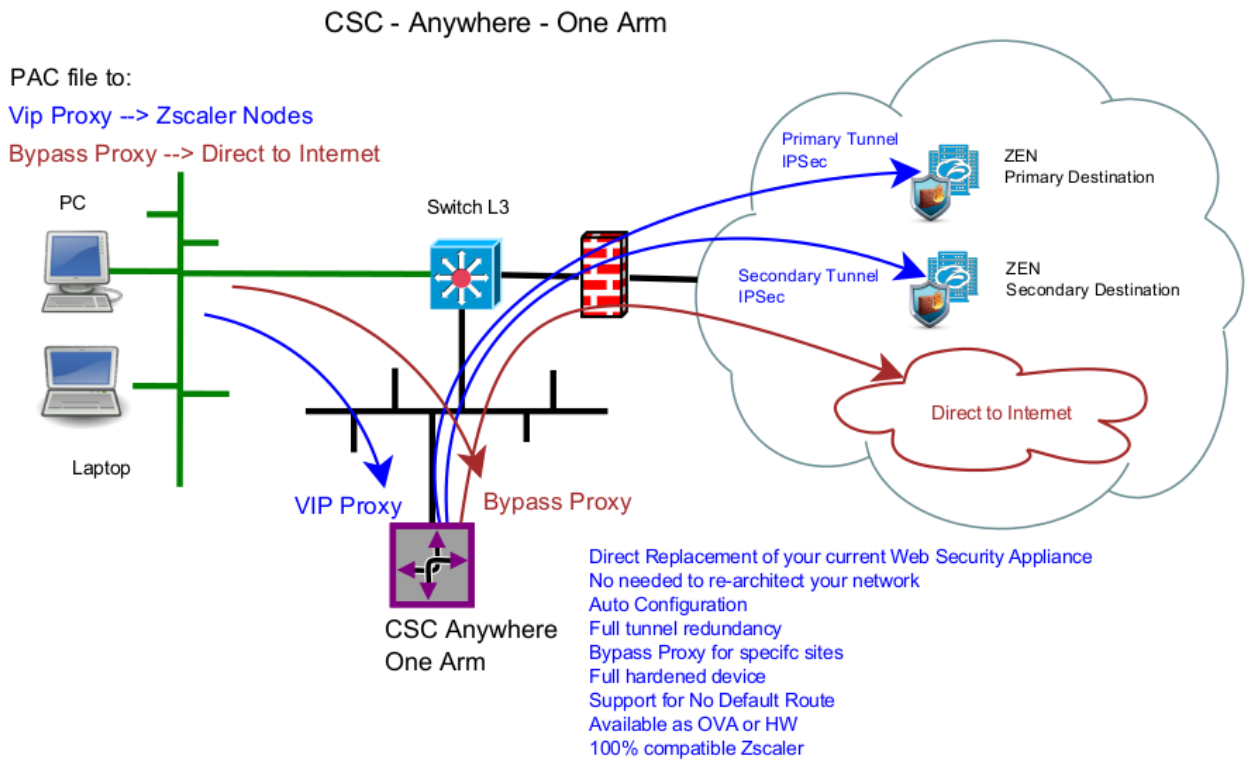
Simple to install with full management from Amazon AWS. The CSC is a cloud instance running on your premises.

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

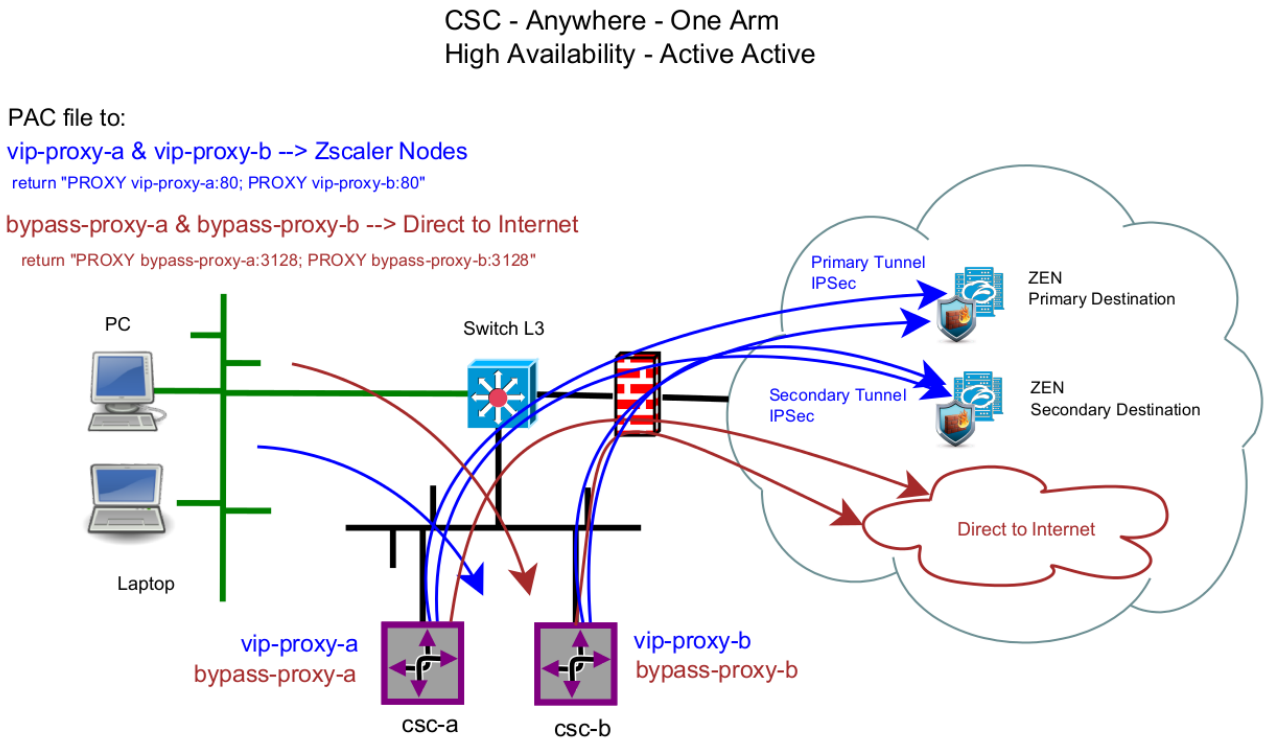
The CSC Anywhere – Single is commonly used by Zscaler customers that are using Zscaler Cloud Firewall

2 CSC Anywhere – Network diagrams

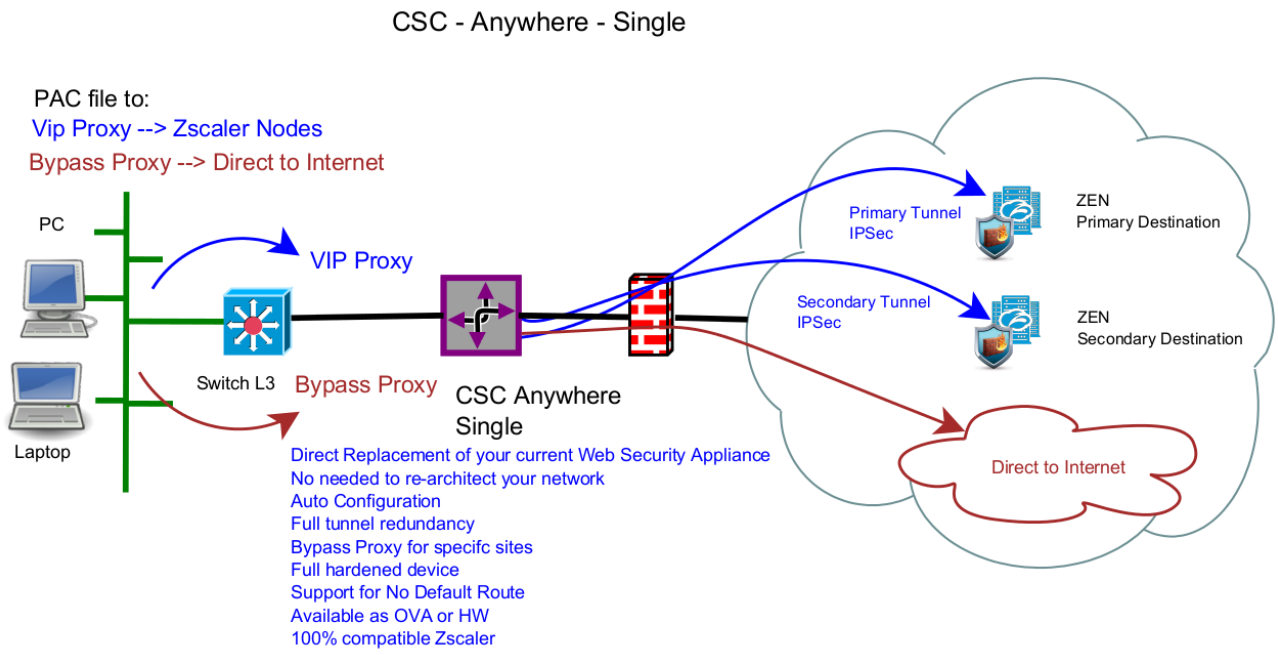
2.1 CSC Anywhere – One Arm – (One Unit)



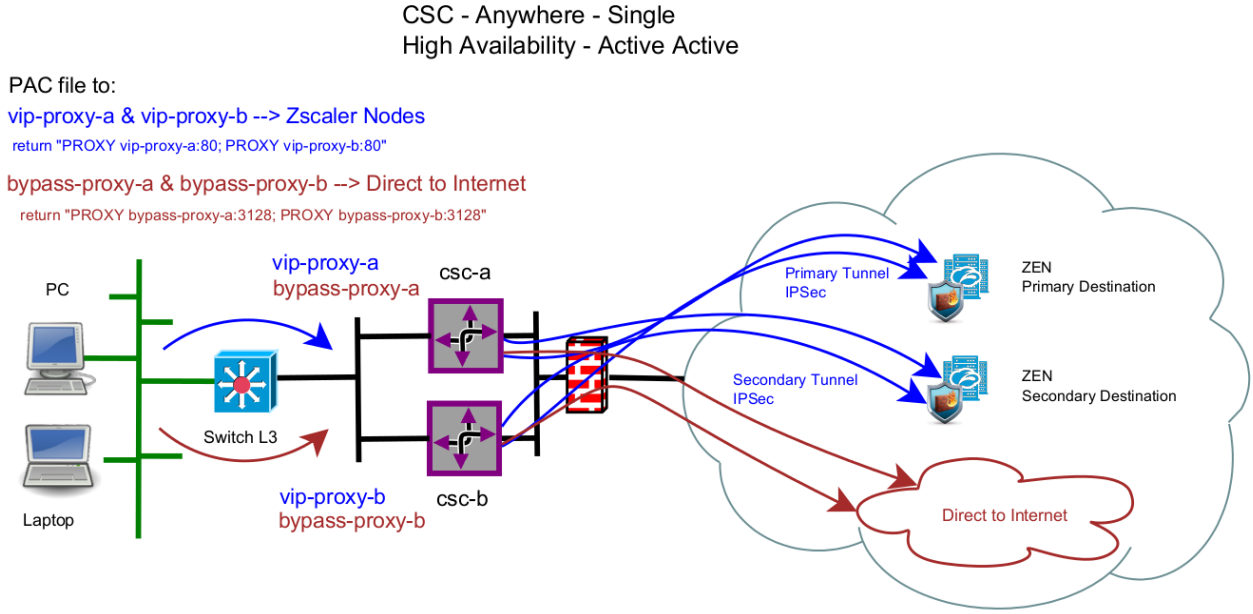
2.2 CSC Anywhere – One Arm – High Availability



2.3 CSC Anywhere – Single – (One Unit)



2.4 CSC Anywhere – Single – High Availability



3 Key benefits of the Cloud Security Anywhere

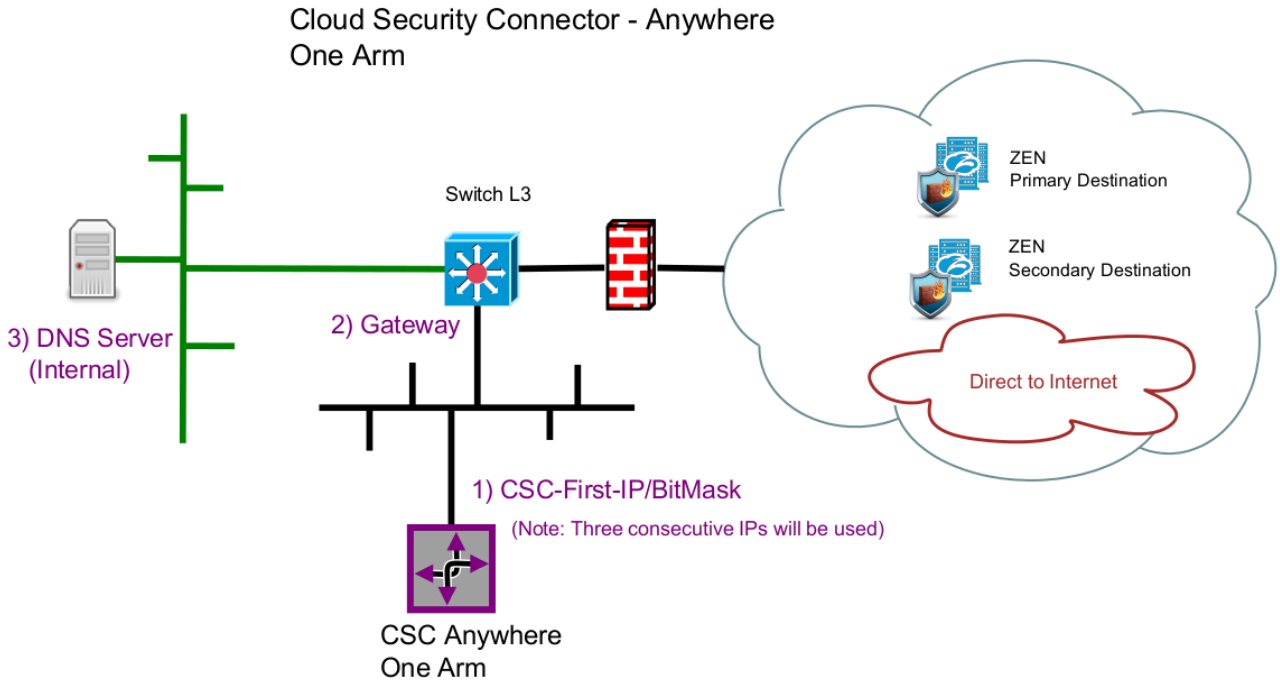
- Direct replacement of your current appliance. (One Arm)
- Enables any Location to be connected to Zscaler Cloud Security Services.
- Full tunnel redundancy.
- VIP proxy to direct the traffic to Zscaler.
- Bypass Proxy to send the traffic direct to Internet.
- Easy configuration: After you buy the CSC, 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

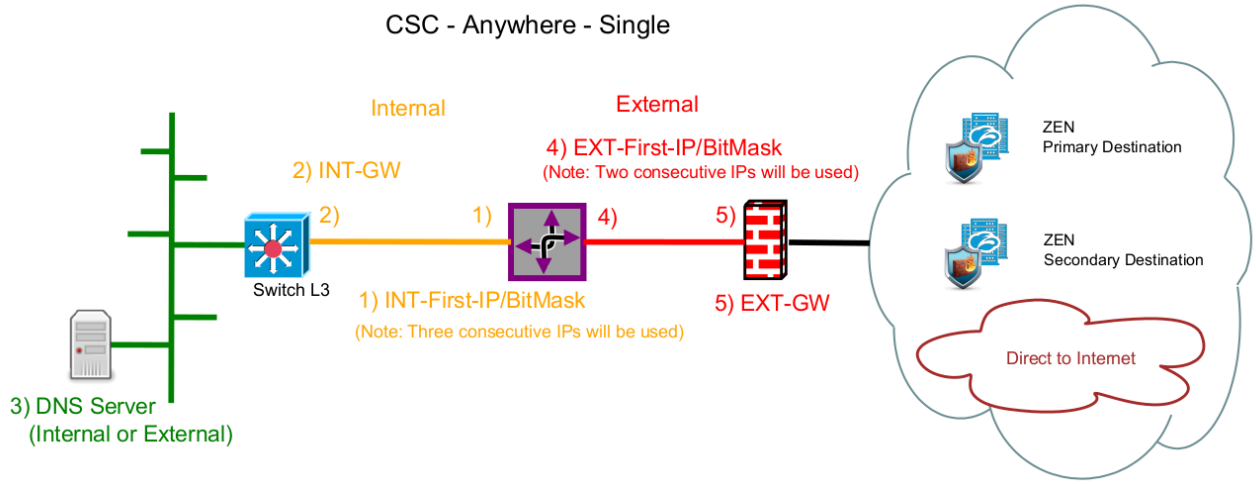
To create the CSC anywhere is very easy. You just need to fill a form with your IP addressing.

Here the network diagram showing the information required:

4.1 CSC Anywhere – One Arm – IP Addressing

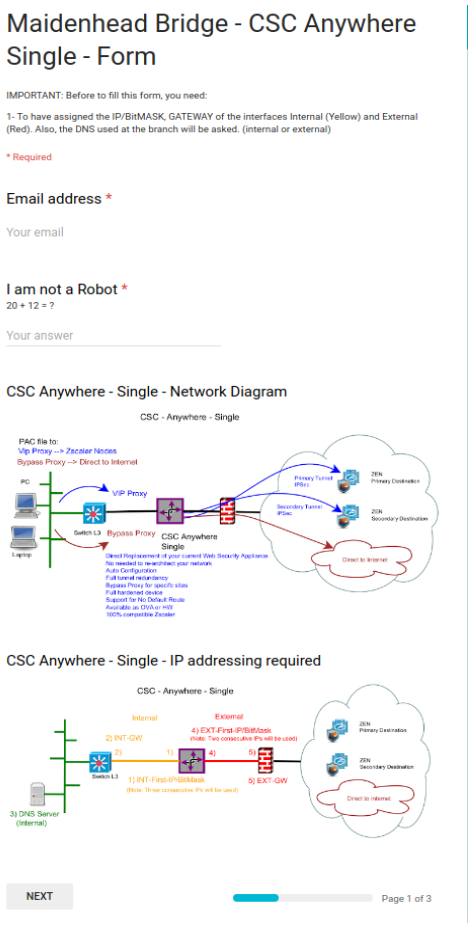


4.2 CSC Anywhere – Single – IP Addressing



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:



Maidenhead Bridge - CSC Anywhere Single - Form

IMPORTANT: Before to fill this form, you need:

1- To have assigned the IP/BitMASK, GATEWAY of the interfaces Internal (Yellow) and External (Red). Also, the DNS used at the branch will be asked. (internal or external)

* Required

Email address *

Your email

I am not a Robot *

20 + 12 = ?

Your answer

CSC Anywhere - Single - Network Diagram

CSC Anywhere - Single - IP addressing required

NEXT

Page 1 of 3

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:

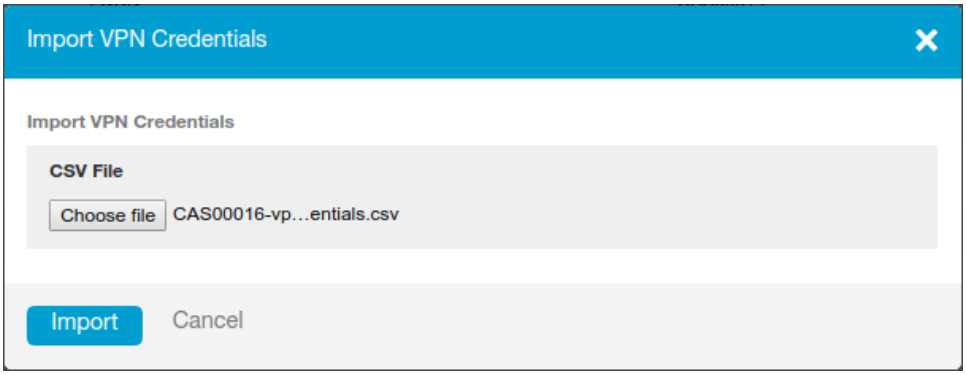
- CASxxxxx-vpncredentials.csv (VPN credentials to import)
- CASxxxxx-v-y-z.ova (your Open Virtual Appliance file to install in your virtual infrastructure)
- CASxxxxx-url-bypass-pac.txt (Instructions to create the “Bypass PAC” to feed your CSCs Bypass List and contains your Bypass PAC URL already configured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

5 Creating the Location on Zscaler GUI

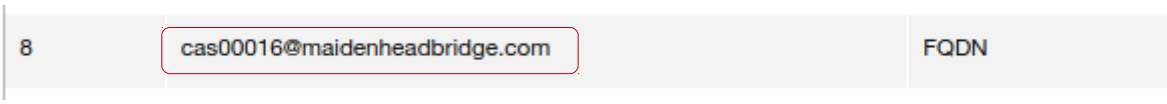
Two steps are required here: To import the VPN credentials and to create the Location.

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



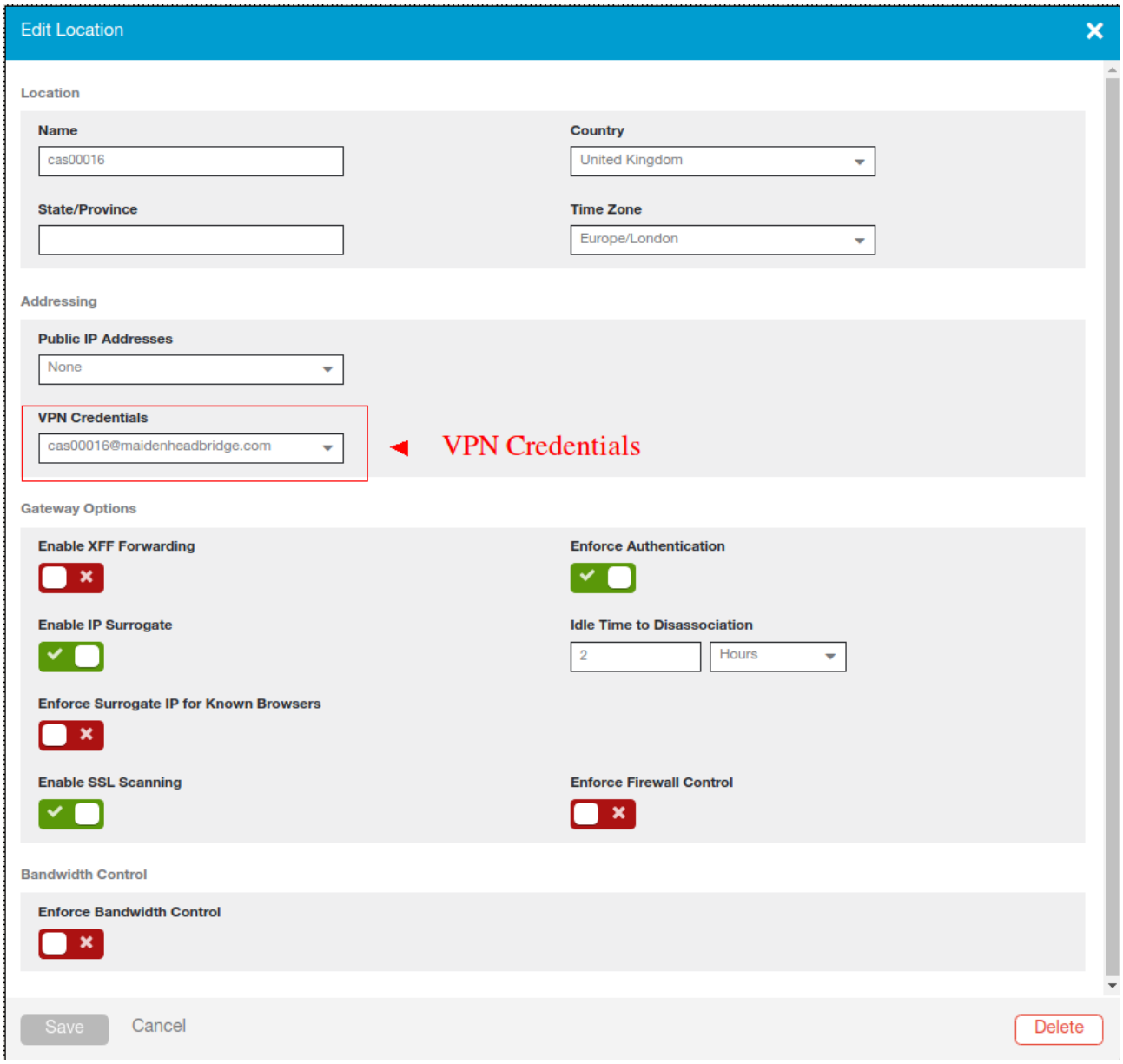
4. Click “Import”
5. You will see a new FDQN credentials with the format of: CASxxxxx@<yourDomain>. In this example the value is:



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

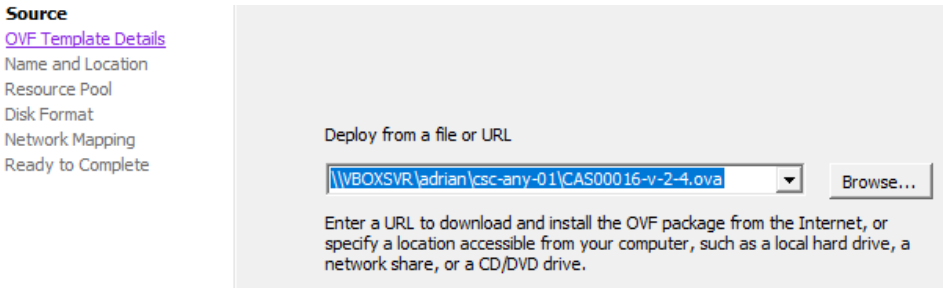
1. Go to Administration > Locations
2. Click create “Add Location”
3. Put Name and other parameters. Select the VPN Credentials imported in the step before.



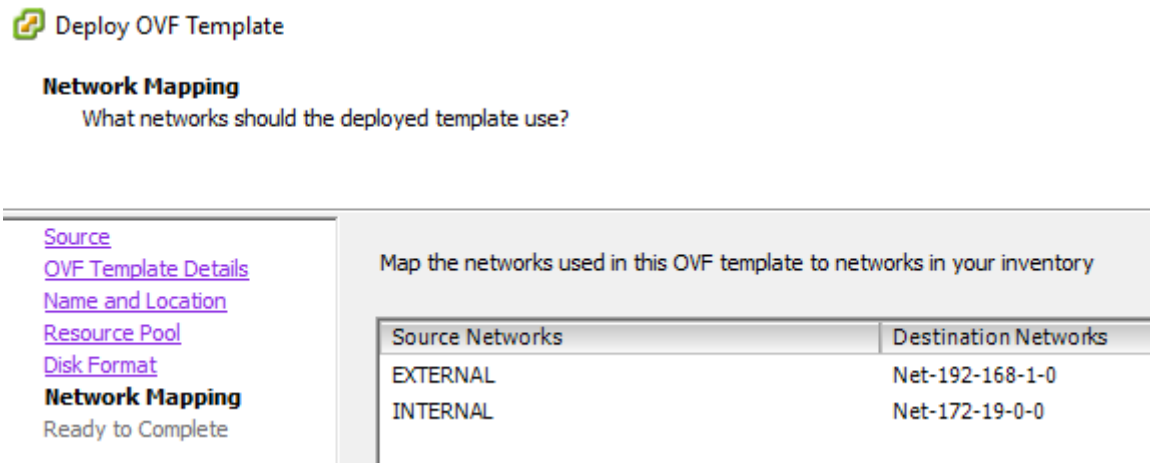
6 Installing the OVA file in your Virtual Platform.

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:



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:**



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: http://ip.zscaler.com , 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	TCP	80 (HTTP)	Web traffic
2	TCP	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: http://ip.zscaler.com , 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
1) VPN Credentials - View/Configure Email (FDQN) and Pre Shared Key (PSK)
2) Select Zscaler Cloud and Enforcement Nodes
3) Confirm Configuration (and Reboot)

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

CSC Admin tasks
8) 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”.

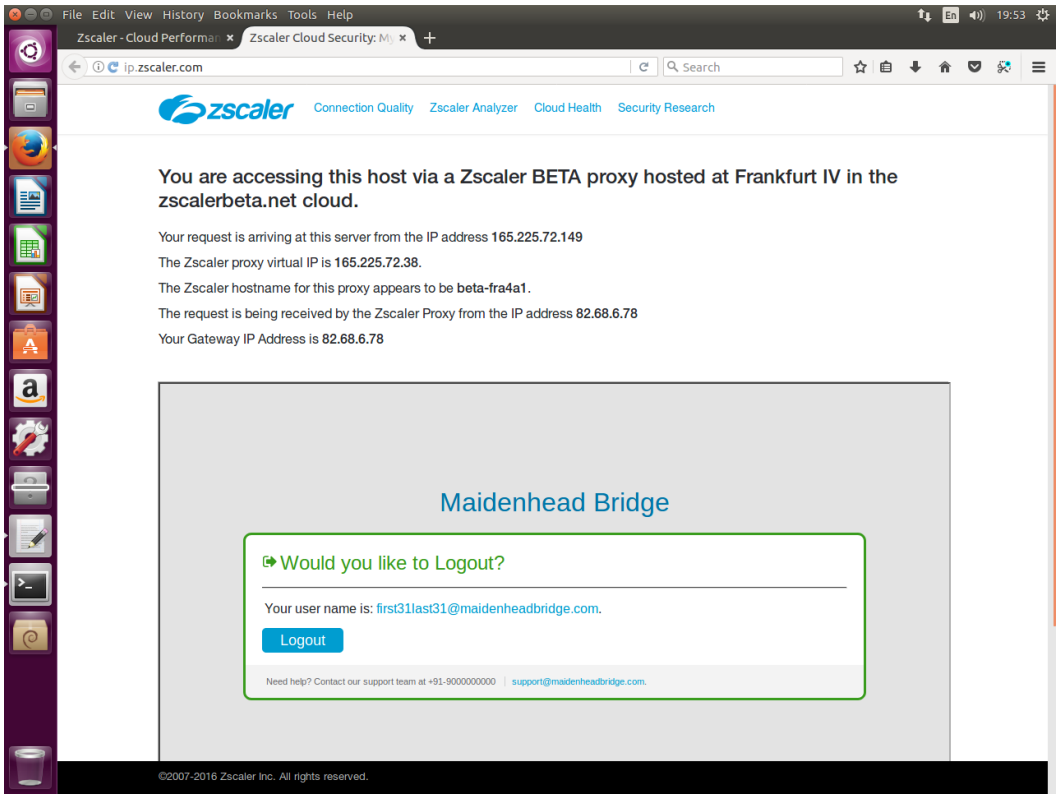
```
Selection: 4

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"}

Press ANY KEY to continue
```

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



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

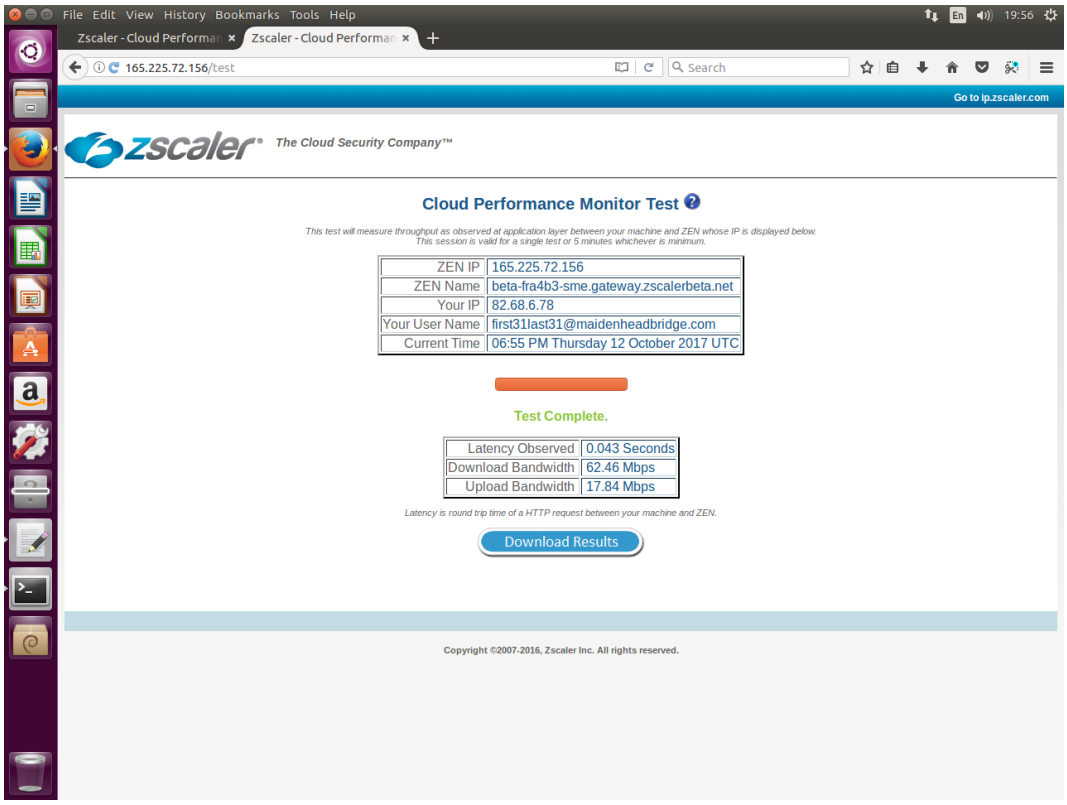
This menu also goes to http://ip.zscaler.com .

```
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”



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 → 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 http://ip.zscaler.com 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 http://ip.zscaler.com 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)***

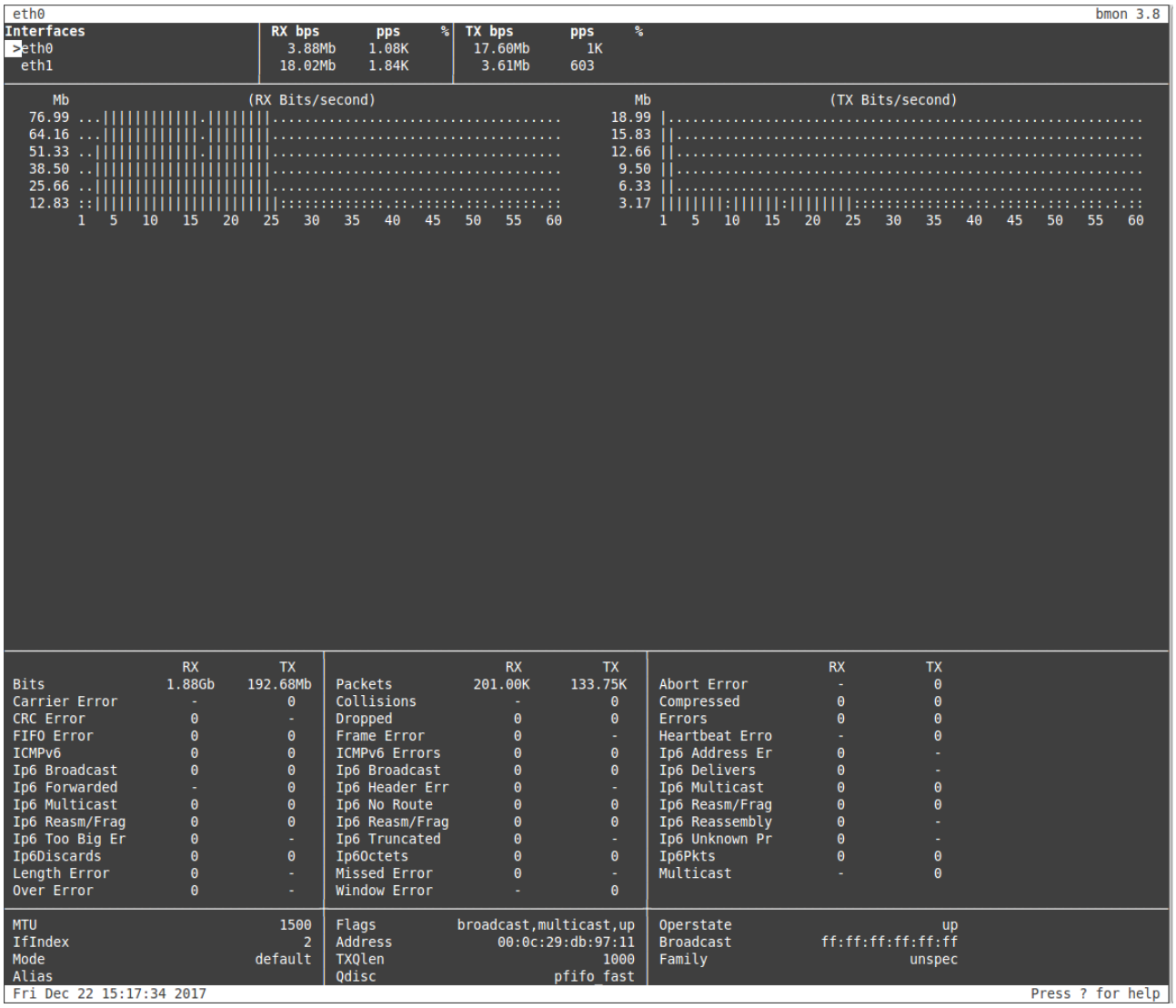
9.2.1.8 AWS SSM Agent

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.



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:

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

```
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
No Active Connections

CREDENTIALS INFORMATION
Username: CAS00027@maidenheadbridge.com | PSK: Not shown for security reasons. Please, read it from 'VPN Credentials' Menu

http://ip.zscaler.com INFORMATION

Your Gateway IP Address is 82.68.6.78
```

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
  1. AS???   192.168.1.254                                               0.0%    10    0.5   0.6   0.5   0.7   0.0
  2. AS13037 losubs.subs.bng2.th-lon.zen.net.uk (62.3.80.21)             0.0%    10    4.0   4.0   3.7   4.2   0.0
  3. AS13037 ae1-183.cr2.th-lon.zen.net.uk (62.3.86.82)                  0.0%    10    5.2   5.3   4.2   6.6   0.7
  4. AS???   ge-3-3-0.mpr1.lhr3.uk.above.net (195.66.236.76)             0.0%    10    3.7   4.2   3.4   5.2   0.3
  5. AS6461  ae6.mpr3.lhr3.uk.zip.zayo.com (64.125.21.21)                0.0%    10    4.4   4.4   3.9   4.9   0.0
  6. AS6461  ae27.cs1.lhr15.uk.eth.zayo.com (64.125.30.234)              0.0%    10   14.9  15.3  14.7  16.7   0.3
  7. AS6461  ae2.cs1.ams10.nl.eth.zayo.com (64.125.29.16)                0.0%    10   14.6  15.0  14.6  15.2   0.0
  8. AS6461  ae0.cs1.ams17.nl.eth.zayo.com (64.125.29.81)                0.0%    10   17.3  16.7  14.9  20.8   2.3
  9. AS6461  ae2.cs1.fra6.de.eth.zayo.com (64.125.29.58)                 0.0%    10   15.4  15.2  14.9  15.8   0.0
 10. AS6461  ae0.cs1.fra9.de.eth.zayo.com (64.125.29.55)                 0.0%    10   15.5  15.7  14.7  21.1   1.8
 11. AS6461  ae27.mpr1.fra4.de.zip.zayo.com (64.125.30.255)              0.0%    10   15.3  16.2  14.7  19.4   1.8
 12. AS6461  94.31.32.194.IPYX-069051-027-ZYO.zip.zayo.com (94.31.32.194) 0.0%    10   14.8  15.2  14.7  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
HOST: CAS00027                                                            Loss%   Snt   Last   Avg  Best  Wrst StDev
  1. AS???   192.168.1.254                                                 0.0%    10    0.5   0.5   0.5   0.6   0.0
  2. AS13037 losubs.subs.bng2.th-lon.zen.net.uk (62.3.80.21)               0.0%    10    3.9   3.9   3.3   4.5   0.0
  3. AS13037 ae1-183.cr2.th-lon.zen.net.uk (62.3.86.82)                    0.0%    10    6.2   7.5   4.3  22.0   5.2
  4. AS???   ge-3-3-0.mpr1.lhr3.uk.above.net (195.66.236.76)               0.0%    10    5.1   4.2   3.7   5.1   0.0
  5. AS6461  ae6.mpr3.lhr3.uk.zip.zayo.com (64.125.21.21)                  0.0%    10    4.5   4.5   4.3   5.0   0.0
  6. AS6461  ae27.cs1.lhr15.uk.eth.zayo.com (64.125.30.234)                0.0%    10   79.5  79.8  79.5  79.9   0.0
  7. AS6461  ae5.cs1.dca2.us.eth.zayo.com (64.125.29.131)                  0.0%    10   87.0  83.0  79.4 100.4   6.7
  8. AS6461  ae27.cr1.dca2.us.zip.zayo.com (64.125.30.247)                 0.0%    10   78.9  79.2  78.9  79.7   0.0
  9. AS6461  ae3.mpr3.iad1.us.zip.zayo.com (64.125.24.10)                  0.0%    10   79.4  82.9  79.2 102.9   7.9
 10. AS6461  ae1.mpr3.iad2.us.zip.zayo.com (64.125.31.142)                 0.0%    10   79.3  79.4  79.2  79.7   0.0
 11. AS6461  208.185.155.194.IPYX-069051-015-ZYO.above.net (208.185.155.194) 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
HOST: CAS00027                                            Loss%   Snt   Last   Avg  Best  Wrst StDev
  1. AS???   192.168.1.254                                 0.0%    10    0.6   0.6   0.6   0.7   0.0
  2. AS13037 losubs.subs.bng2.th-lon.zen.net.uk (62.3.80.21) 0.0%    10    3.9   3.9   3.7   4.1   0.0
  3. AS13037 ae1-183.cr2.th-lon.zen.net.uk (62.3.86.82)    0.0%    10    4.3   5.5   4.3   7.0   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                               0.0%    10    5.1   5.0   4.6   5.6   0.0
  6. AS15169 108.170.233.227                               0.0%    10    6.3   6.0   5.7   6.3   0.0
  7. AS15169 google-public-dns-a.google.com (8.8.8.8)      0.0%    10    5.9   5.6   5.4   5.9   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 8.8.8.8
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 19:22:17 2017
HOST: 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

Testing Secondary ZEN: AutoSecondary : secondary.vpn.zscalerbeta.net >   104.129.194.39
Start: Mon Oct 16 19:22:32 2017
HOST: CAS00027                                                Loss%   Snt   Last   Avg  Best  Wrst StDev
  1. AS???   ???                                              100.0    10    0.0   0.0   0.0   0.0   0.0
  2. AS62044 165.225.72.2                                      0.0%    10   23.3  23.9  20.2  29.2   3.5
  3. AS3257  xe-3-0-7.cr1-fra2.ip4.gtt.net (46.33.89.9)        0.0%    10   21.7  24.1  16.9  28.8   3.3
  4. AS3257  xe-1-0-5.cr0-was1.ip4.gtt.net (213.254.214.150)   0.0%    10  107.0 106.1 101.5 110.3   3.0
  5. AS3257  zscaler-gw.ip4.gtt.net (77.67.68.146)             0.0%    10  108.5 109.7 102.7 131.7   8.5
  6. AS22616 104.129.194.39                                    0.0%    10  103.5 108.3 102.3 121.5   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???   ???                                      100.0    10    0.0   0.0   0.0   0.0   0.0
  2. AS62044 165.225.72.2                               0.0%    10   35.6  27.0  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
  4. AS???   ???                                      100.0    10    0.0   0.0   0.0   0.0   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)   0.0%    10   25.0  25.0  19.2  35.8   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%   Snt   Last   Avg  Best  Wrst StDev
  1. AS???   ???                                                100.0    10    0.0   0.0   0.0   0.0   0.0
  2. AS62044 165.225.72.2                                        0.0%    10   20.7  23.0  19.6  26.5   2.3
  3. AS6461  xe-9-2-1.mpr1.fra4.de.zip.zayo.com (94.31.32.193)   0.0%    10   23.4  25.4  19.4  40.5   6.1
  4. AS6461  ae8.mpr1.fra3.de.zip.zayo.com (64.125.26.233)       0.0%    10   17.2  23.9  17.2  31.4   4.6
  5. AS6461  ae27.cs1.fra6.de.eth.zayo.com (64.125.31.216)       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)        0.0%    10   34.3  33.8  26.7  41.8   4.1
  8. AS6461  ae2.cs1.lhr15.uk.eth.zayo.com (64.125.29.17)        0.0%    10   34.3  34.3  27.2  42.2   5.0
  9. AS6461  ae27.mpr3.lhr3.uk.zip.zayo.com (64.125.30.235)      0.0%    10   32.9  31.1  27.5  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)                  0.0%    10   34.5  33.2  28.1  37.7   2.8
 12. AS13037 ge-2-0-0-0.cr1.th-lon.zen.net.uk (62.3.80.41)       0.0%    10   34.0  32.0  27.6  35.5   2.6
 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

Press ANY KEY to continue
```

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

```
Testing Primary ZEN: AutoPrimary : vpn.zscalerbeta.net >  165.225.72.39
Start: Mon Oct 16 19:22:17 2017
HOST: 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

```
CSC Admin tasks
6) AWS SSM Agent (Register or De-Register)
7) Change SSH Password
8) Change Timezone
```

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.

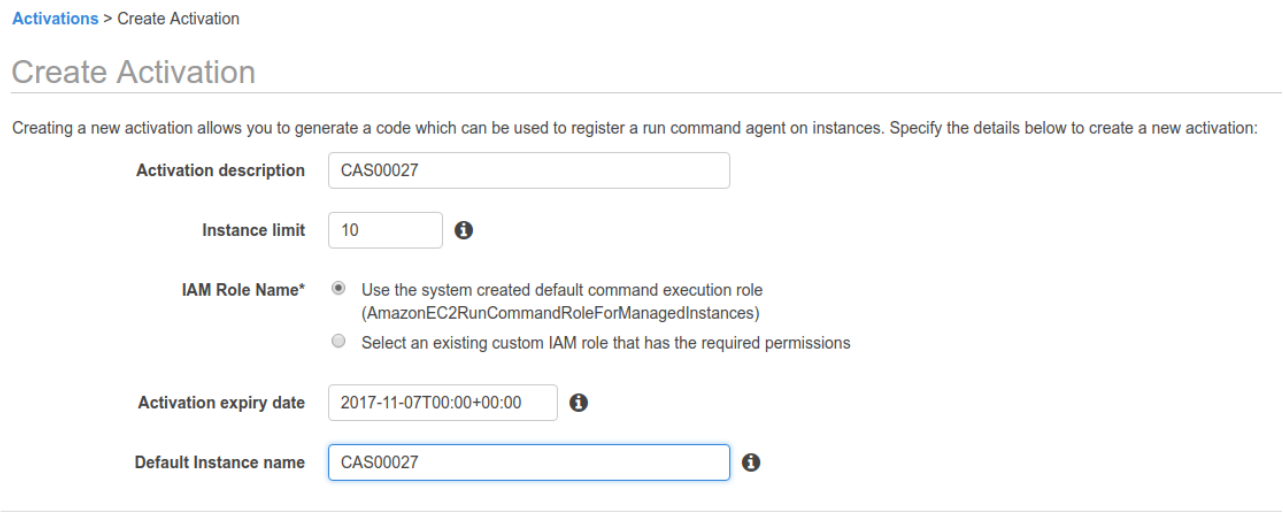
9.3.1 AWS SSM Agent (Register / De-Register)

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 (https://aws.amazon.com/free) 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.

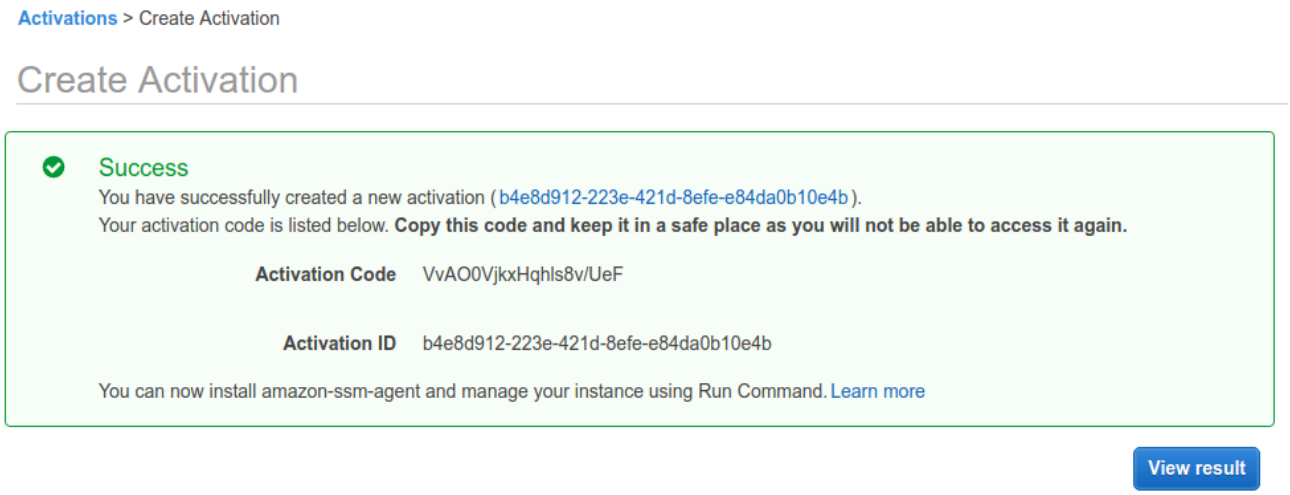
The steps required to add the CSC are two:

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



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

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



Please, keep copy this values on a safe place. You will need this to register the AWS SSM client on the CSC.

2. From the CSC Admin Tasks Menu, select “8) AWS SSM Agent (Register or De-Register)”

```
CSC Admin tasks
8) AWS SSM Agent (Register or De-Register)
9) Change SSH Password
10) Change Timezone
```

```
Selection: 8

The SSM Agent is inactive (dead) since Mon 2017-10-16 17:22:55 BST; 43min ago

Do you want to Register (start) the AWS SSM Agent (y/n)
```

Ingress “y”

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**#)

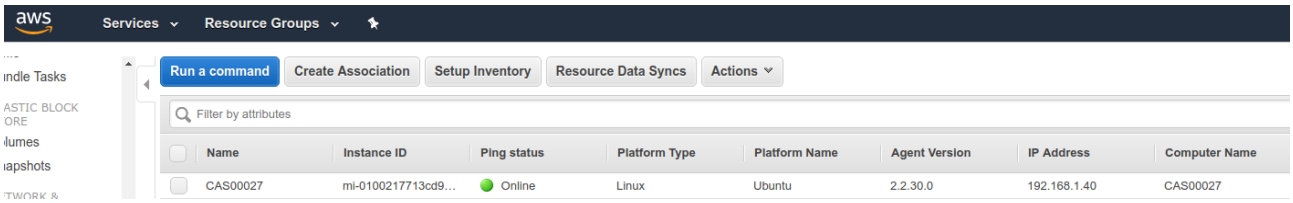
```
Please, ingress Activation Code, Activation ID and Region (example: eu-west-1)
Activation Code :VvAO0VjkxHqhls8v/UeF
Activation ID :b4e8d912-223e-421d-8efe-e84da0b10e4b
Region :eu-west-1
```

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

Press ANY KEY to continue
```

Done! You have the CSC integrated with AWS now with the instance-id “mi-xxxxxxxxx” (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:



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.

```
Bypass Proxy
11) View Current Bypass List
12) Configure Bypass List
```

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:

```
Selection: 12

Please, select method to configure Bypass List

1) Auto - Bypass PAC URL
2) Manual
3) Quit
Enter your choice:
```

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:

*http://pac.<**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.

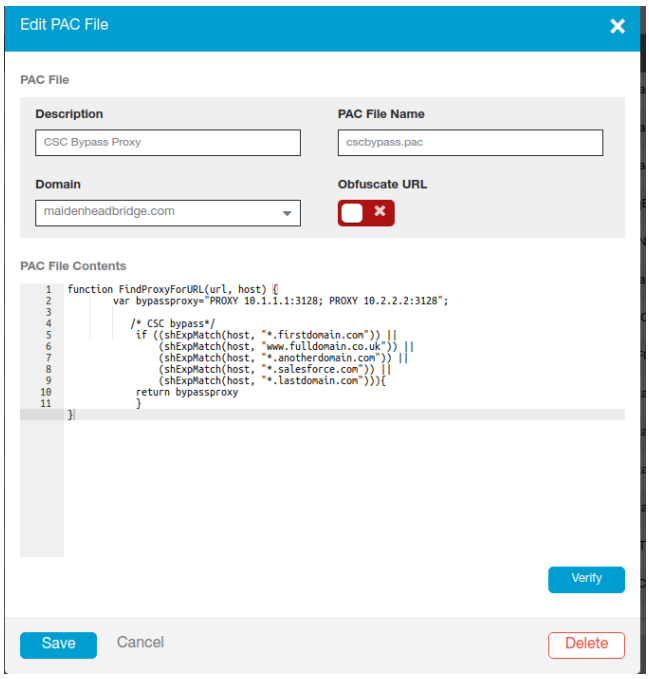
Example of “Bypass PAC file”

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

        //* 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
                }
}
```

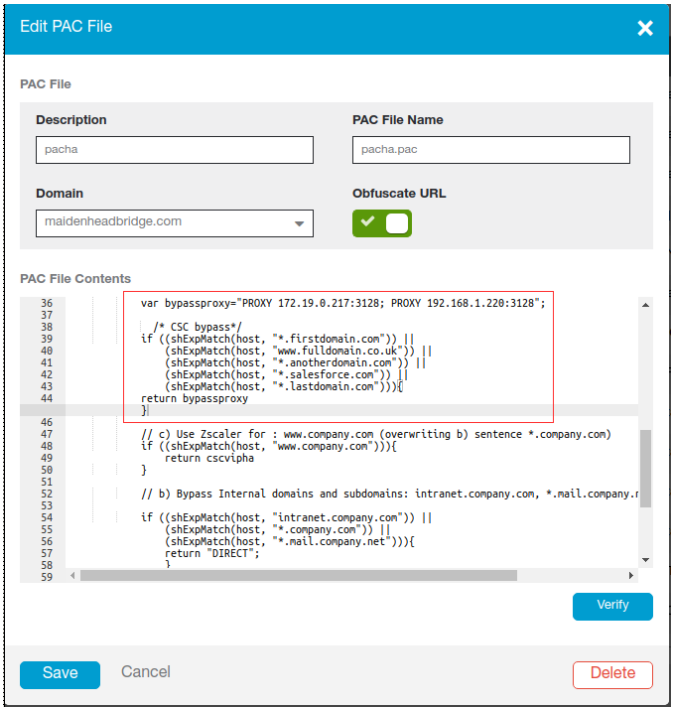
Important Note: It is mandatory to use this function and format. Feel free to add lines but don’t change the format. We recommend to start filling the first line and the last line. Use middle lines for copy/paste.

*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:



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



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:

```
Enter your choice: 1

Current Bypass PAC URL configured is: http://pac.zscalerbeta.net/maidenheadbridge.com/cscbypass.pac

Do you want to change Bypass PAC URL? (y/n)? y

Please, ingress Bypass PAC URL
Bypass PAC URL:http://pac.zscalerbeta.net/maidenheadbridge.com/cscbypass.pac
```

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)?
```

```
Do you want to refresh Bypass List? (y/n)? y

This is your current Bypass List

.firstdomain.com
www.fulldomain.co.uk
.anotherdomain.com
.salesforce.com
.lastdomain.com


Do you want apply changes? (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)

```
This is the list of current Domains configured:

.firstdomain.com
www.fulldomain.co.uk
.anotherdomain.com
.salesforce.com
.lastdomain.com

Press ANY KEY to continue
```

9.4.2.2 2) Manual

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

1. Select Option 2)

```
Enter your choice: 2

Please, read the instructions carefully:

You are going to edit the list using NANO editor

The following formats are accepted:

Full Domains:  'www.example.com'
Wildcard for subdomains: '.example.com' - This will allow all subdomains of example.com

To save, press CTRL-X and 'Yes'

Paid attention to ERROR messages if any. ERRORs must be corrected before to continue

Do you want to continue? (y/n)?
```

2. Ingress “y”

```
  GNU nano 2.5.3                File: domains                          Modified

.firstdomain.com
www.fulldomain.co.uk
.anotherdomain.com
.salesforce.com
.lastdomain.com
www.manualentry.com
.manualwithsubdomains.co.uk

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell    ^_ 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.

```
This is your current Bypass List

.firstdomain.com
www.fulldomain.co.uk
.anotherdomain.com
.salesforce.com
.lastdomain.com
www.manualentry.com
.manualwithsubdomains.co.uk


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

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
```

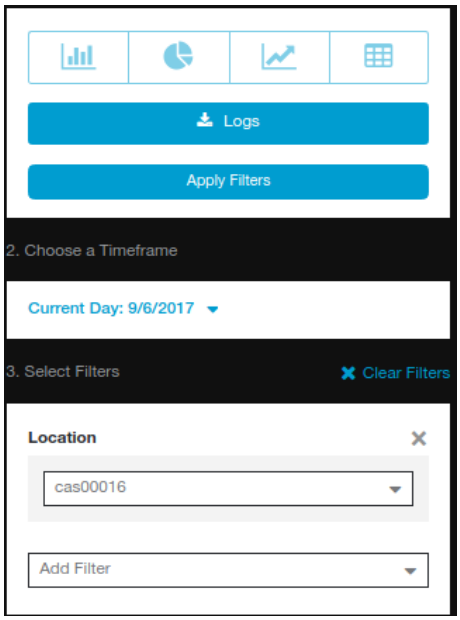
10 Checking full visibility of the transaction on the Zscaler GUI

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]



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:

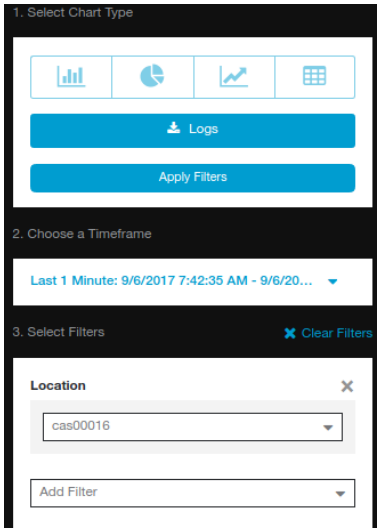
Client IP	Server IP
172.19.0.140	212.58.246.93
172.19.0.140	46.236.9.36
172.19.0.140	46.236.9.36
172.19.0.140	46.236.9.36
172.19.0.140	172.227.98.43

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]



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?***

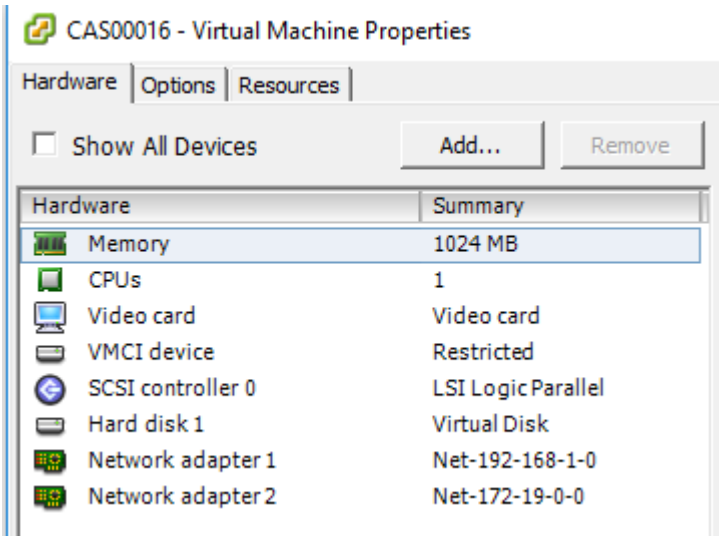
2. ***Are Vmware interfaces are properly mapped?***

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

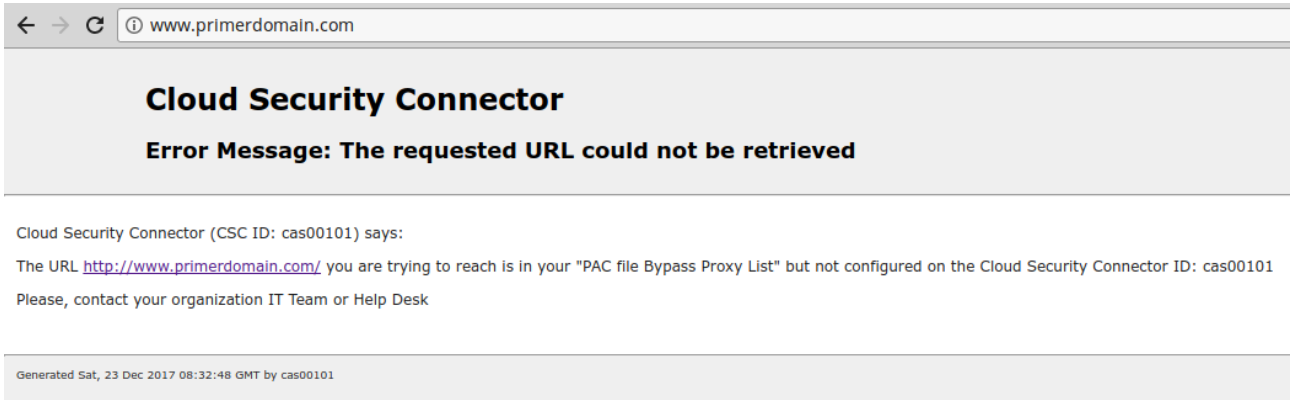
For example: http://172.19.0.217:3128/

and you will received the following page:

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:



11.3 PAC file troubleshooting

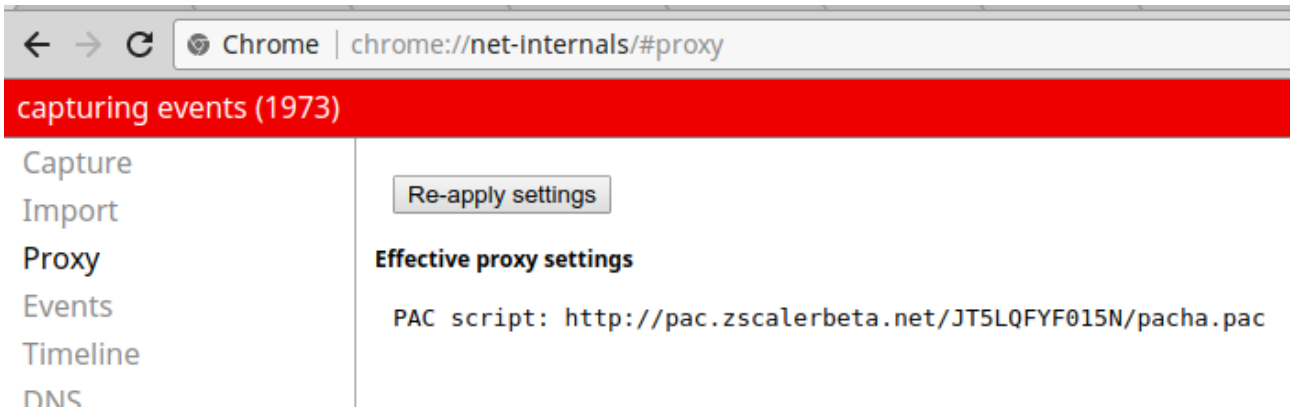
Please, for all this test use “Google Chrome”

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:



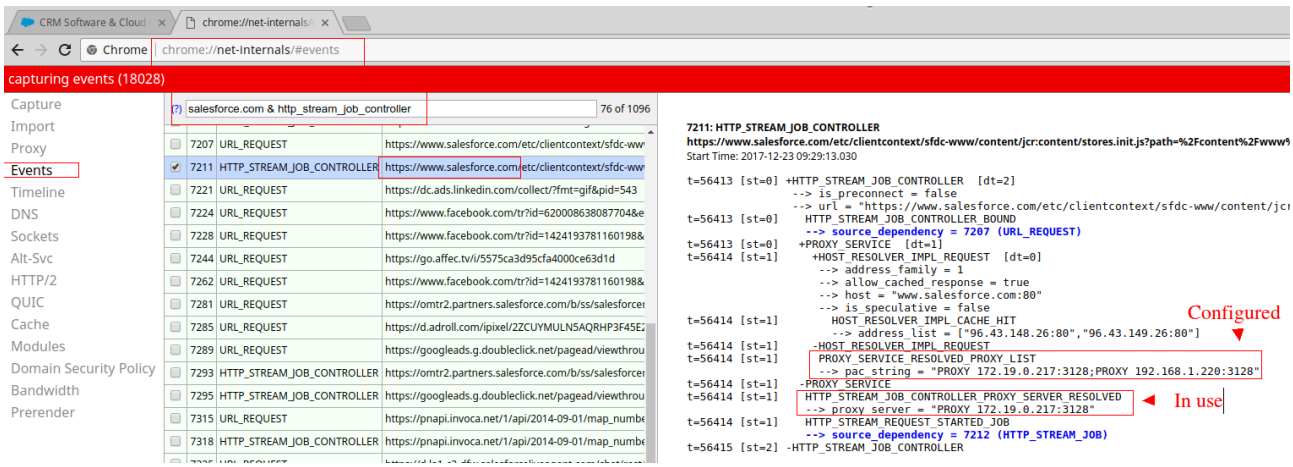
11.3.2 How to Check if the Domain destination is using VIP Proxy or Bypass Proxy?

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 www.salesforce.com 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")



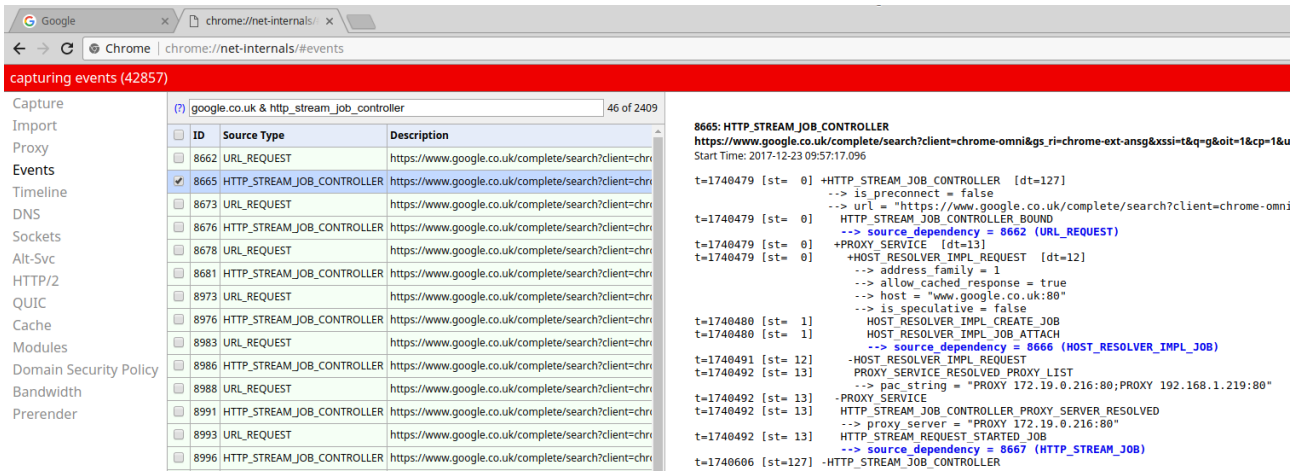
In this example, www.salesforce.com is using the Bypass proxy:

```
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 "www.google.co.uk"



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, www.google.com 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: www.maidenheadbridge.com

Sales enquiries: sales@maidenheadbridge.com

Support: http://support.maidenheadbridge.com

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

```
Monitoring Tasks
4) Show Configuration and Status
5) Show Interfaces Traffic
```

In one click, 25 parameters are showed and 14 tests are performed.

```
Selection: 4

GENERAL INFORMATION
Company : Maidenhead Bridge
Location : Location40
CSC ID : CAS00027
Soft version : 3.0

INTERFACES INFORMATION
Internal Interface (eth1) IP: 172.21.0.40/24 | Internal Gateway: 172.21.0.254 is Alive
External Interface (eth0) IP: 192.168.1.40/24 | External Gateway: 192.168.1.254 is Alive
VIP Proxy: 172.21.0.41

DNS INFORMATION
Internal DNS IP: 192.168.1.254 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: San Francisco IV | Hostname: sunnyvale1-vpn.zscalerbeta.net | IP: 199.168.148.132 is Alive
Secondary ZEN node: Washington DC | Hostname: was1-vpn.zscalerbeta.net | IP: 104.129.194.39 is Alive

TUNNEL INFORMATION
The Node active is the: San Francisco IV
IPsec uptime: 7 hours, since Oct 12 07:28:32 2017
Last Security Association: ESTABLISHED 7 hours ago

CREDENTIALS INFORMATION
Username: CAS00027test@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 San Francisco 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 Thu 2017-10-12 08:42:12 BST; 6h ago
Registration values: {"ManagedInstanceID":"mi-02f0c193846c4366e","Region":"eu-west-1"}
```

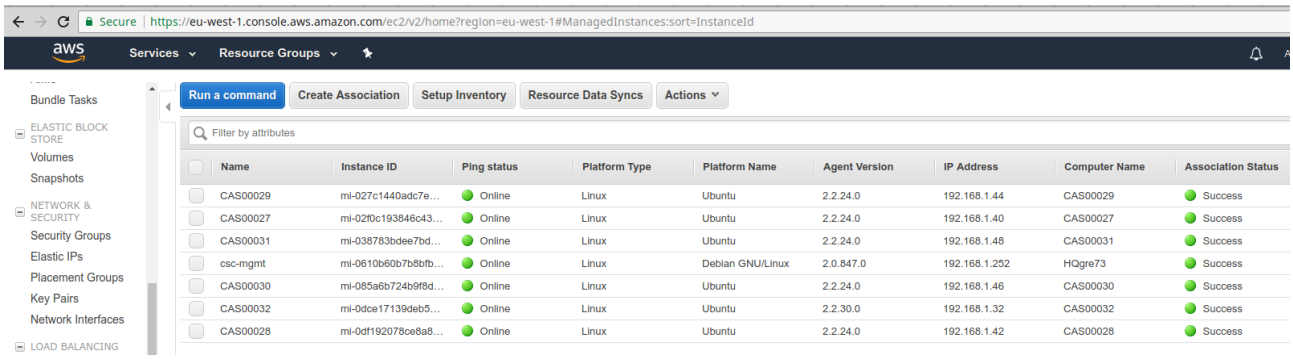
13.5.2 AWS management

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

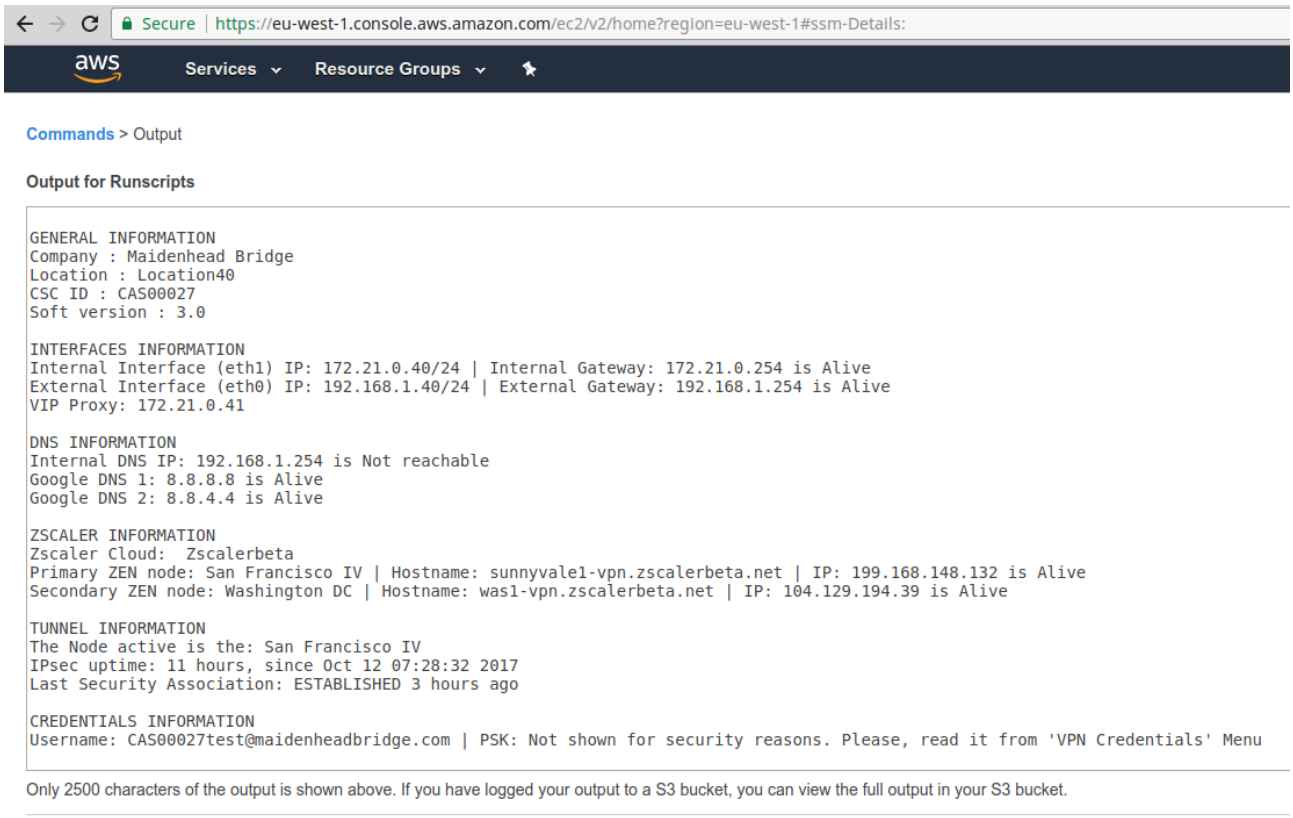
Amazon AWS offers on the free account to control up to 1000 managed instances for hybrid environments. The CSC had the AWS SSM pre-installed on the machines. You simply need to

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.



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.