Cloud Security Connector
Multiplex GRE

Enabling Zscaler beyond 1 Gbps with Tunnel Aggregation

Administrator Guide

Software Version 1.0

(October 2018)

Table of Contents

1 Introduction

The Cloud Security Connector (CSC) Multiplex GRE allows to connect securely Zscaler Cloud Security Services to more than 1 Gbps.

The main purpose of the CSC Multiplex GRE 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 Multiplex GRE 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.

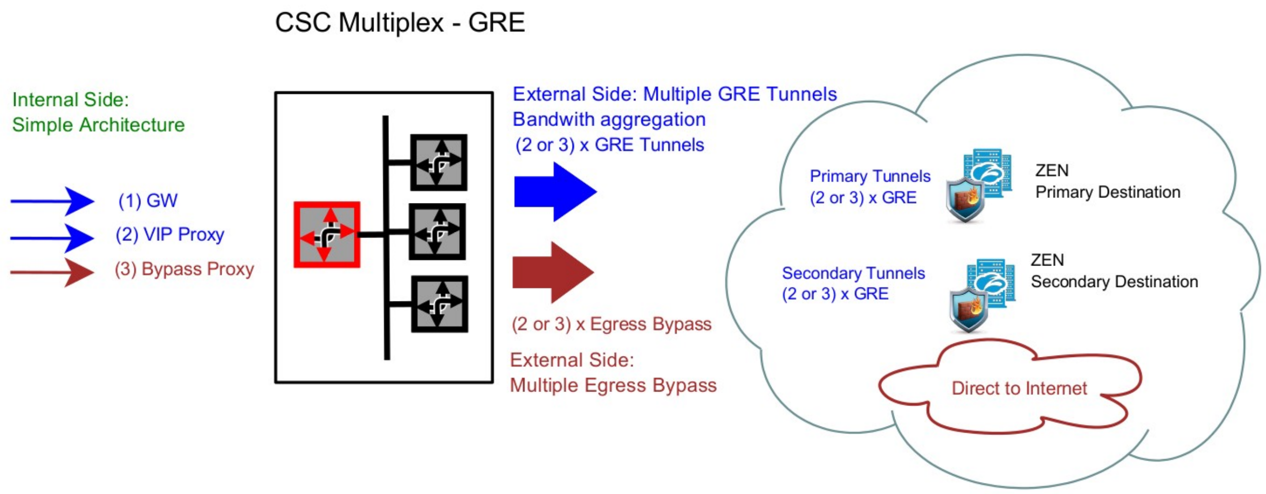
The CSC Multiplex GRE comes with the perfect parameters to work with Zscaler. As soon you lunch the CSC at the location, the CSC will automatically connect to the best Zscaler nodes. The CSC Mutliplex GRE contain the perfect configuration for GRE tunnels, firewall rules and routing tables that are necessary.

No restrictions: 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.

2 CSC Multiplex GRE - Network diagrams



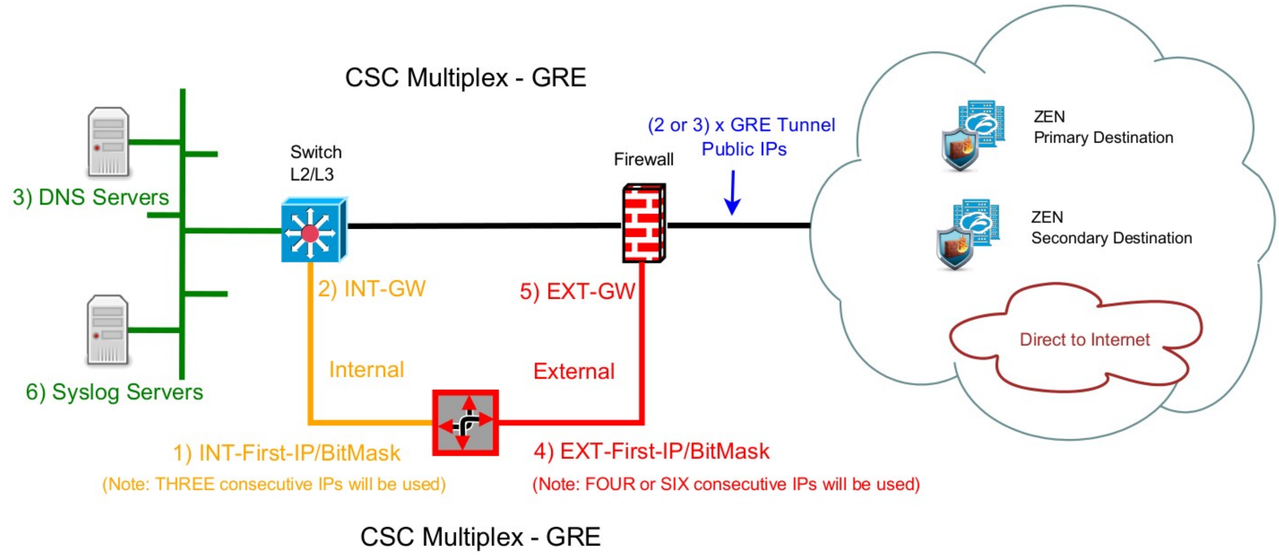
3 Key benefits of the Cloud Security Connector Multiplex GRE

- No Networking knowledge required. No configuration.
- Direct replacement of your current appliance Web Security Appliance.
- Enables any Location to be connected to Zscaler Cloud Security Services to more 1 Gbps.
- Full tunnel redundancy.
- Full use of all bandwidth available at all Internet Links.
- 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.
- Works behind a NAT
- All virtual platform supported: Vmware, Hyper-vV, KVM, Virtual Box, etc.
- Hardware version available if required.
- One click Status and Configuration. This shows all values and does all checks for you in one step.
- Amazon AWS management
- MTR (MyTraceRoute) test to the Zscaler nodes and in the reverse path as well.
- Speedtest.net integrated
- Works with No default Route Scenarios.
- Small OVA instances.

4 Creating the CSC Multiplex GRE

To create the CSC Multiplex GRE is very easy. You just need to fill a form with your IP addressing and the GRE tunnels IPs.

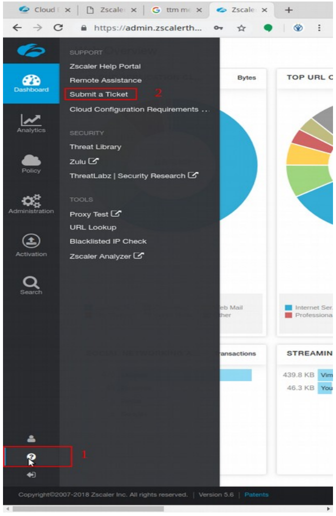
Here the network diagram showing the information required:



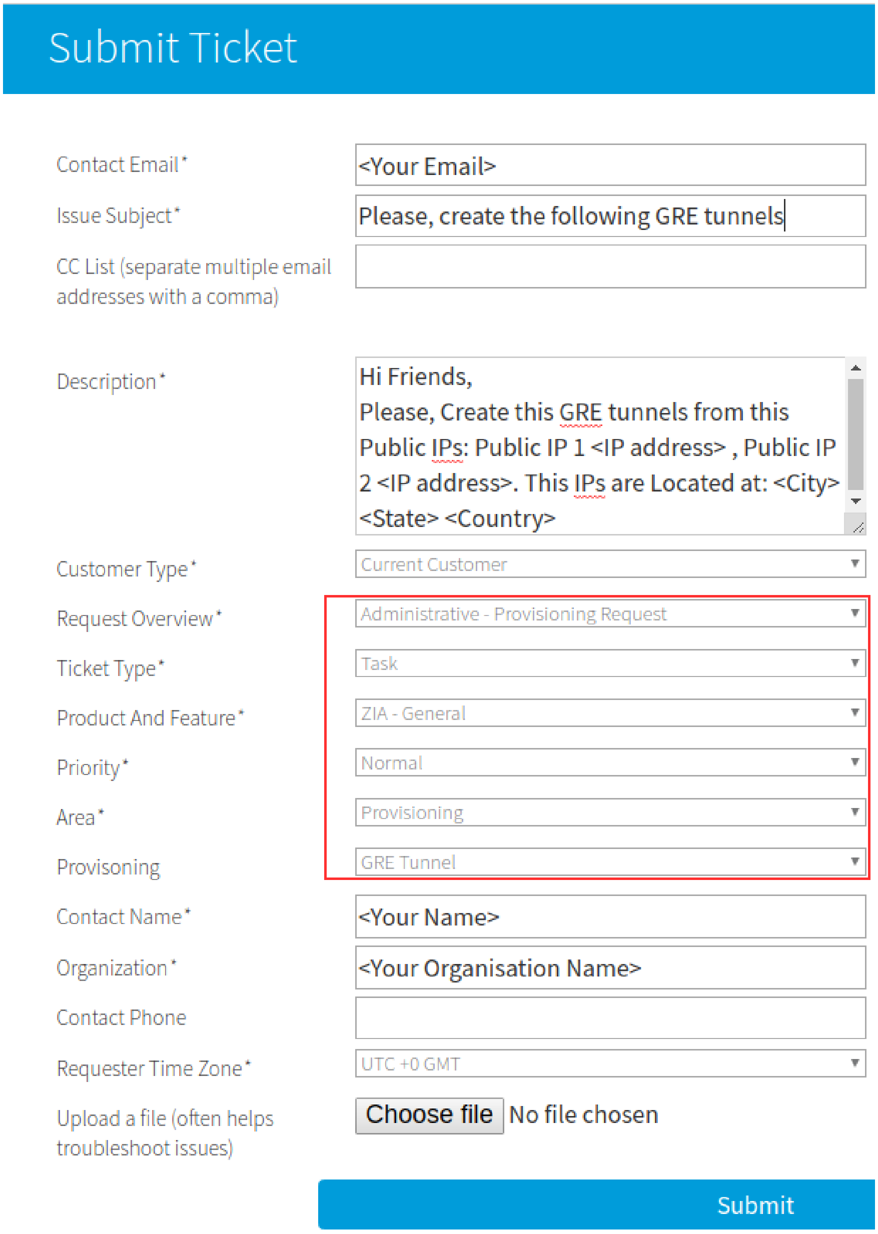
4.1 Submit a ticket to Zscaler Support for GRE Instructions

You will need to submit a ticket to Zscaler to request the GRE tunnels. When submitting a ticket to Zscaler you need to specify the GRE tunnels Public IPs (in blue in the diagram above)

➔ From the GUI, Go to: Help > Submit a Ticket



➔ You will be redirected to the Submit Ticket Page:



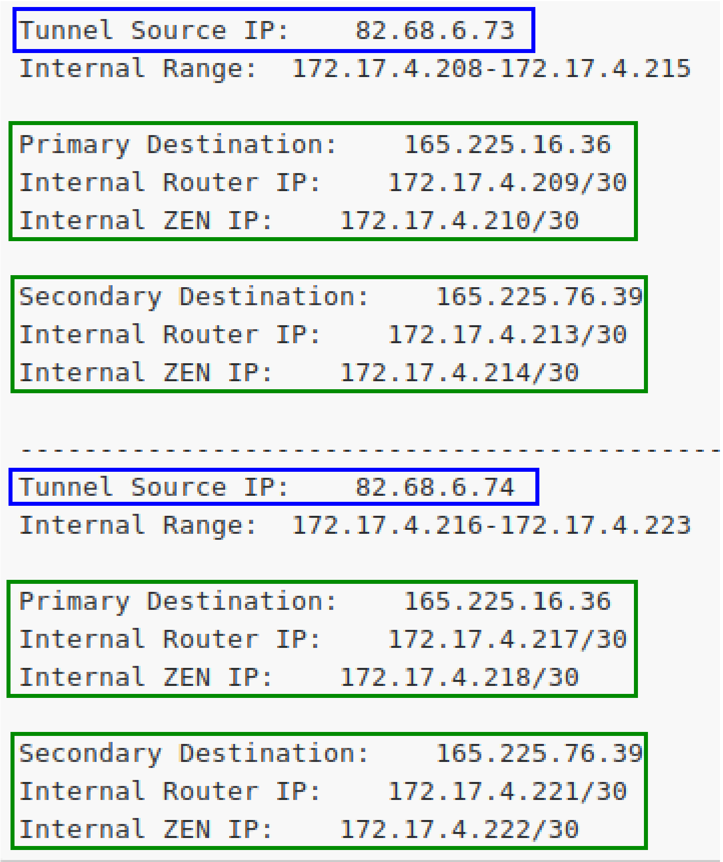
Submit Ticket

Contact Email*	<Your Email>
Issue Subject*	Please, create the following GRE tunnels
CC List (separate multiple email addresses with a comma)	
Description*	Hi Friends, Please, Create this GRE tunnels from this Public IPs: Public IP 1 <IP address> , Public IP 2 <IP address>. This IPs are Located at: <City> <State> <Country>
Customer Type*	Current Customer
Request Overview*	Administrative - Provisioning Request
Ticket Type*	Task
Product And Feature*	ZIA - General
Priority*	Normal
Area*	Provisioning
Provisoning	GRE Tunnel
Contact Name*	<Your Name>
Organization*	<Your Organisation Name>
Contact Phone	
Requester Time Zone*	UTC +0 GMT
Upload a file (often helps troubleshoot issues)	Choose file No file chosen

Where **Public IP 1, Public IP 2 (optional Public IP 3) are the Public IPs of GRE tunnels.**

Important: You need to specify the **<city>, <state>** and **<country>** where the IP is located. This allows Zscaler Support to indicate the best ZEN nodes for your location.

➔ After the ticket is submitted, you will receive an email with the GRE information, like this one:



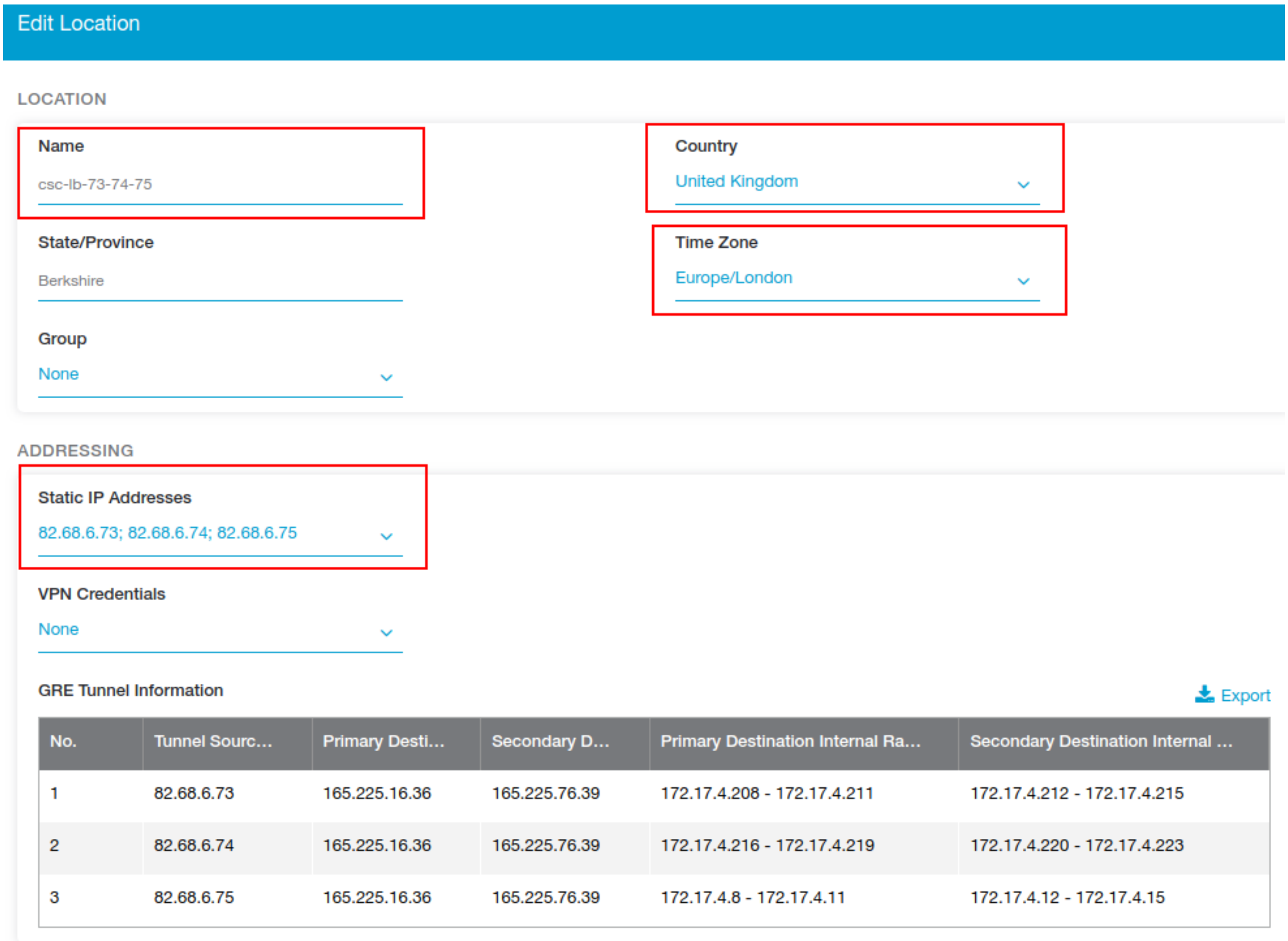
```
Tunnel Source IP:     82.68.6.73
Internal Range:   172.17.4.208-172.17.4.215

Primary Destination:     165.225.16.36
Internal Router IP:     172.17.4.209/30
Internal ZEN IP:     172.17.4.210/30

Secondary Destination:     165.225.76.39
Internal Router IP:     172.17.4.213/30
Internal ZEN IP:     172.17.4.214/30

--------------------------------------------
Tunnel Source IP:     82.68.6.74
Internal Range:   172.17.4.216-172.17.4.223

Primary Destination:     165.225.16.36
Internal Router IP:     172.17.4.217/30
Internal ZEN IP:     172.17.4.218/30

Secondary Destination:     165.225.76.39
Internal Router IP:     172.17.4.221/30
Internal ZEN IP:     172.17.4.222/30
```

Please, note that Tunnel Source IP = <GRE Public IP> and the values remark in green will be requested when filling the “CSC GRE Form”

4.2 Create the Location on Zscaler GUI

On the Zscaler GUI, go to Administration > Location > Add Location

➔ ***Mandatory:*** Put Name, Country and Time Zone. Select all Public IPs requested for the location.



Edit Location

LOCATION

Name: csc-lb-73-74-75

Country: United Kingdom

State/Province: Berkshire

Time Zone: Europe/London

Group: None

ADDRESSING

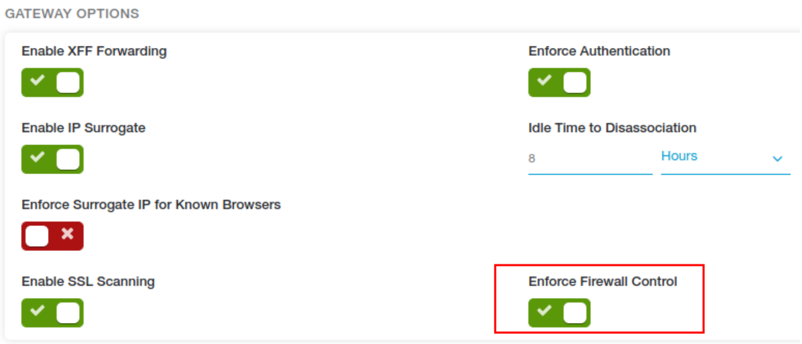
Static IP Addresses: 82.68.6.73; 82.68.6.74; 82.68.6.75

VPN Credentials: None

GRE Tunnel Information

No.	Tunnel Sourc...	Primary Desti...	Secondary D...	Primary Destination Internal Ra...	Secondary Destination Internal ...
1	82.68.6.73	165.225.16.36	165.225.76.39	172.17.4.208 - 172.17.4.211	172.17.4.212 - 172.17.4.215
2	82.68.6.74	165.225.16.36	165.225.76.39	172.17.4.216 - 172.17.4.219	172.17.4.220 - 172.17.4.223
3	82.68.6.75	165.225.16.36	165.225.76.39	172.17.4.8 - 172.17.4.11	172.17.4.12 - 172.17.4.15

➔ ***Optional:*** Select additional options for the Location according your design, like Enforce Authentication, SSL inspection, Surrogate IP, etc.



GATEWAY OPTIONS

Enable XFF Forwarding: ✓

Enforce Authentication: ✓

Enable IP Surrogate: ✓

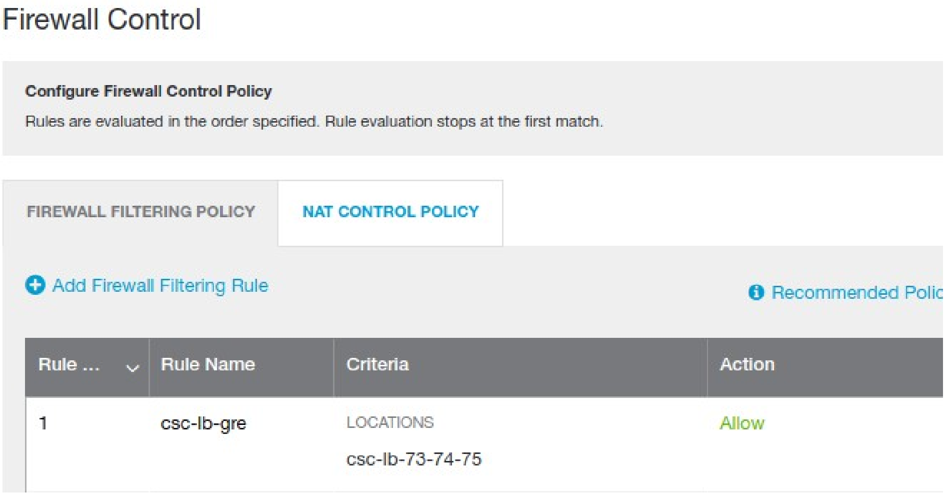
Idle Time to Disassociation: 8 Hours

Enforce Surrogate IP for Known Browsers: ✗

Enable SSL Scanning: ✓

Enforce Firewall Control: ✓

- ➔ **Recommended (1):** Enable "Enforce Firewall Control". This will enforce all traffic to leave the Zscaler Cloud from the same outgoing IP for all tunnels. IMPORTANT: You must create a Firewall Rule for the Location allowing the traffic to go out, like:



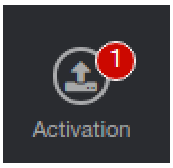
Firewall Control

Configure Firewall Control Policy

Rules are evaluated in the order specified. Rule evaluation stops at the first match.

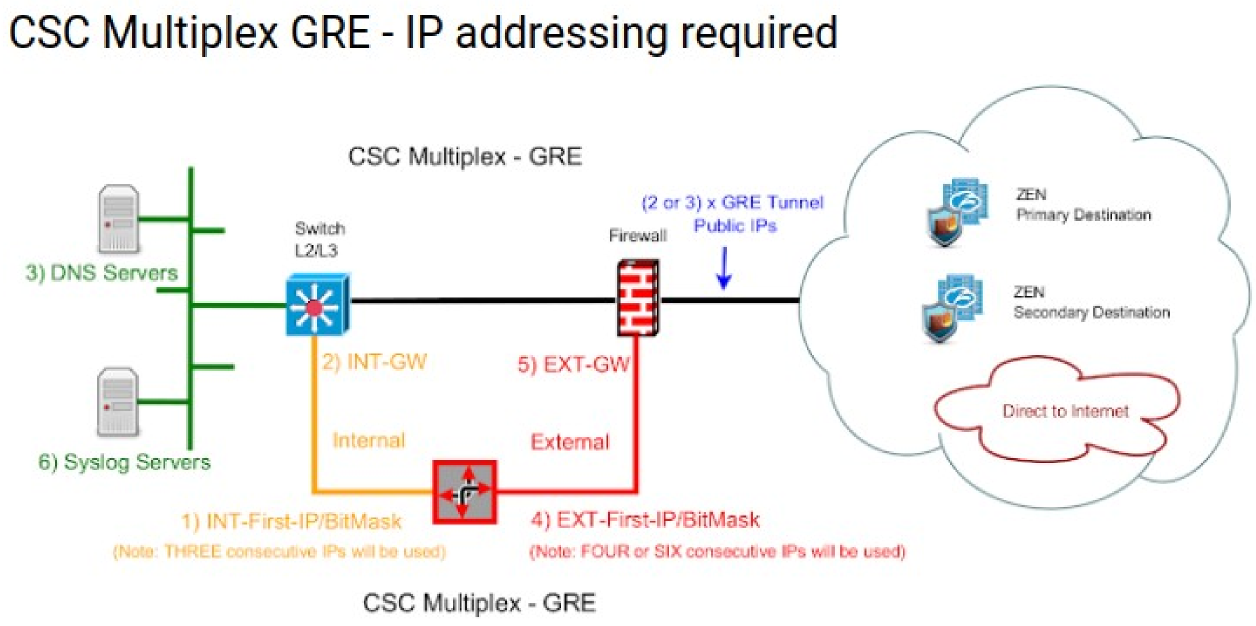
Rule ...	Rule Name	Criteria	Action
1	csc-lb-gre	LOCATIONS csc-lb-73-74-75	Allow

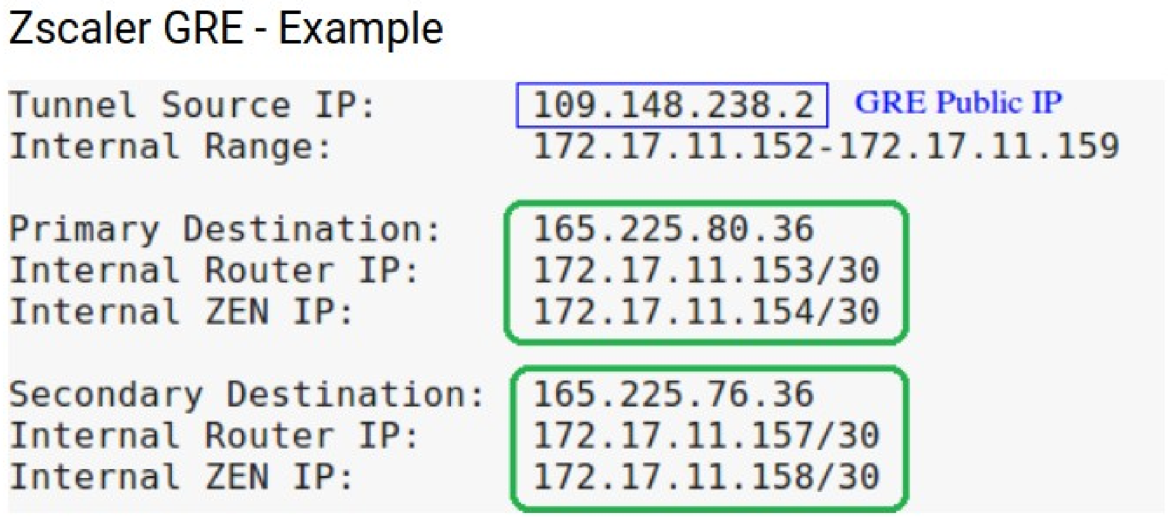
- ➔ Click "Save"
- ➔ and "Activate".



4.3 Filling the Form

After you buy the CSC, 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:





Zscaler GRE - Example

```
Tunnel Source IP:          109.148.238.2  GRE Public IP
Internal Range:            172.17.11.152-172.17.11.159

Primary Destination:       165.225.80.36
Internal Router IP:        172.17.11.153/30
Internal ZEN IP:           172.17.11.154/30

Secondary Destination:     165.225.76.36
Internal Router IP:        172.17.11.157/30
Internal ZEN IP:           172.17.11.158/30
```

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
6. Location Name
7. Internal Interface: First IP / Bitmask (Note: The CSC Multiplex GRE Cluster uses three consecutive IPs. You need to ingress the first one) and Gateway.
8. External Interface First IP/Bitmask (Note: The CSC Multiplex uses four or six consecutive IPs) and Gateway.
9. DNS Servers.
10. Syslog / SIEM Servers (optional)
11. Ingress your GRE tunnel information.

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

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

(a) cmgXXXXX-lb-v-Y-Z.ova : This is the Load Balancer of the CSC Multiplex GRE

(b) cmgXXXXX-1-v-Y-Z.ova: This is the first CSC GRE Single #1

(c) cmgXXXXX-2-v-Y-Z.ova: This is the first CSC GRE Single #2

(d) cmgXXXXX-3-v-Y-Z.ova: This is the first CSC GRE Single #3 (optional)

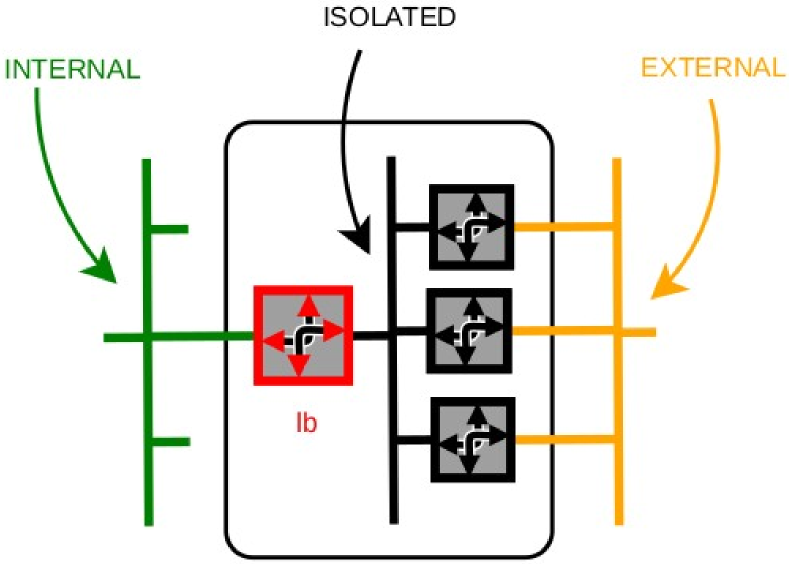
(e) cmgXXXX-url-bypass-pac.txt (Instructions to create the “Bypass PAC” to feed your CSCs Bypass List. It also contains your Bypass PAC URL already configured on the CSCs)

Please, note that the CSC Multiplex GRE is composed of 3 or 4 Virtual Machines. The first virtual machine is the load balancer. The other are the Connectors to Zscaler.

5 Installing the OVA files in your Virtual Platform.

5.1 Networking required on your Virtual Platform

The following diagram shows the Networks "names" used by the CSC Multiplex GRE on the OVA files. When importing the OVA file, you need to map this interfaces name accordingly.



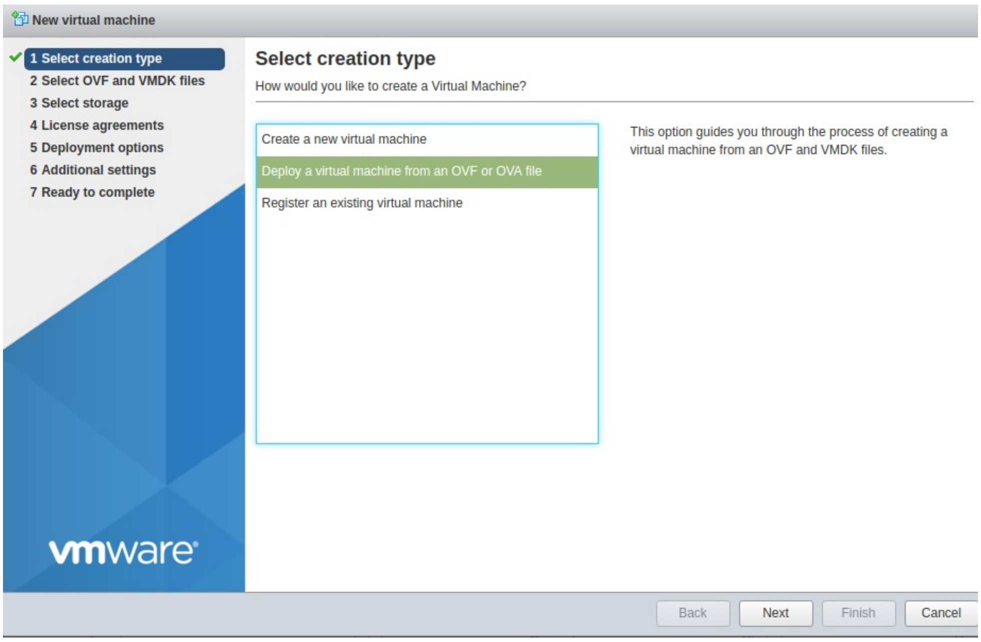
Important: You must create an internal network in your Virtual Platform for the only purpose of the communication between the Load Balancer and the Connectors.
On the CSC VMs, the name of the Network that comes with the OVA file is "ISOLATED"

5.2 Deploying OVF files

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, INTERNAL and ISOLATED accordingly.

5.2.1 Deploying the Load Balancer

1. Go to vSphere, New Machine > Deploy VM from OVF or OVA (on version 5.5 File > Deploy OVF template)



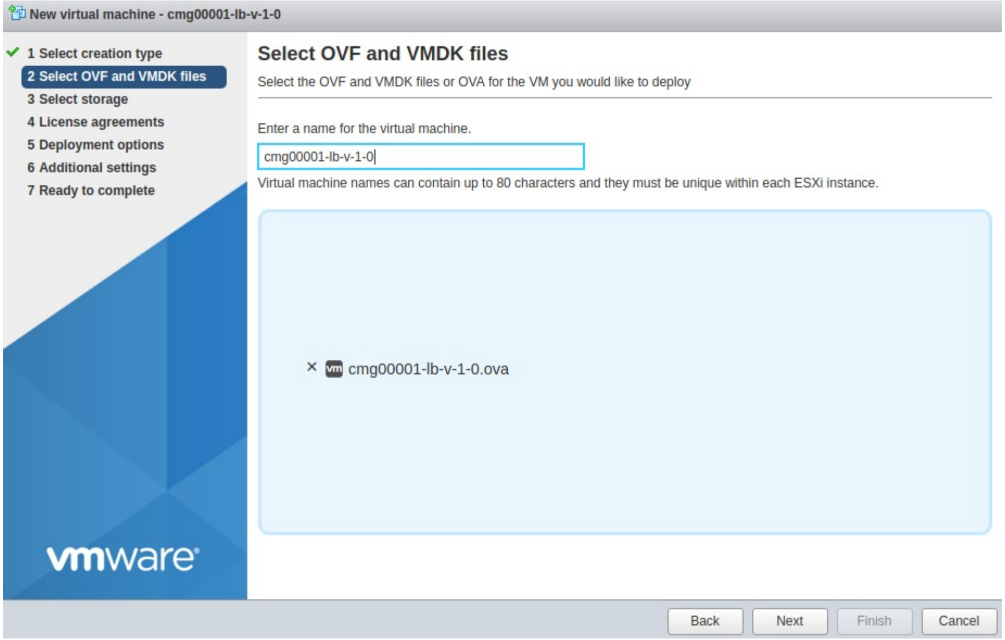
Select creation type

How would you like to create a Virtual Machine?

- Create a new virtual machine
- Deploy a virtual machine from an OVF or OVA file
- Register an existing virtual machine

This option guides you through the process of creating a virtual machine from an OVF and VMDK files.

2. Select the OVA File and put the name for the Load Balancer



Select OVF and VMDK files

Select the OVF and VMDK files or OVA for the VM you would like to deploy

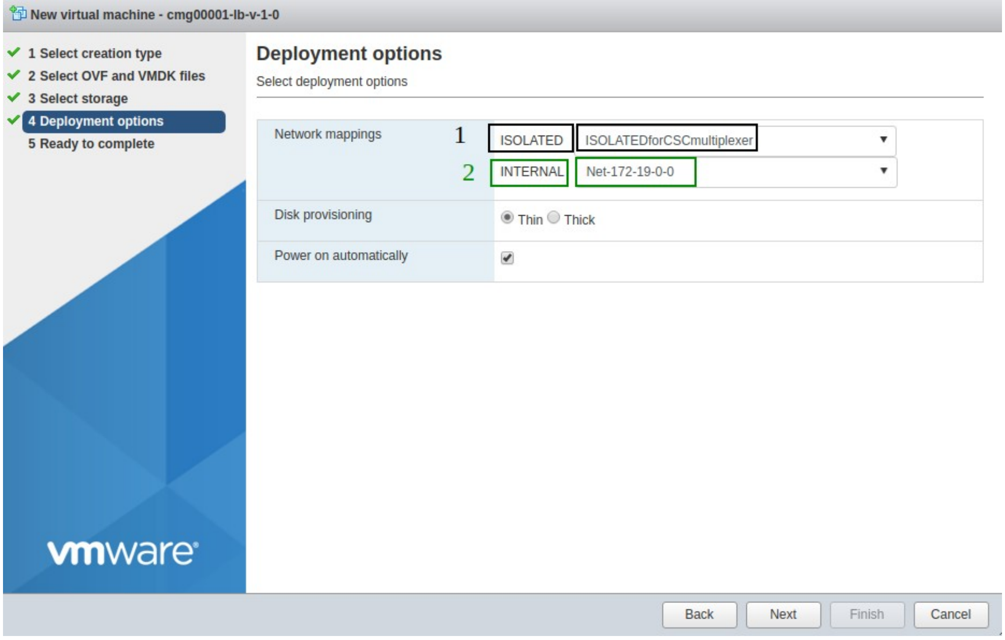
Enter a name for the virtual machine.

cmg00001-lb-v-1-0

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

× cmg00001-lb-v-1-0.ova

3. Select Storage
4. On Deployment Options, map the interfaces INTERNAL and ISOLATED accordingly:



Deployment options

Select deployment options

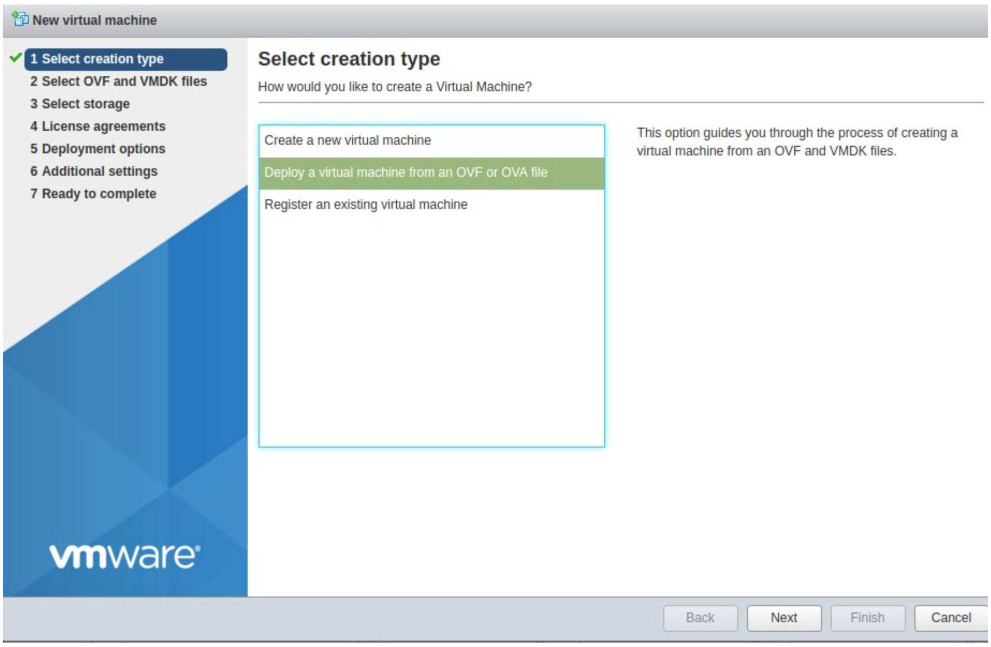
Network mappings	1 ISOLATED	ISOLATEDforCSCmultiplexer
	2 INTERNAL	Net-172-19-0-0
Disk provisioning	● Thin ○ Thick	
Power on automatically	☑	

Note: In this example the “ISOLATED” Network Name was mapped to “ISOLATEDforCSCMultiplexer” and the “INTERNAL” to “Net-172-19-0-0”

5. Click Next > Ready to Complete > Finish

5.2.2 Deploying the CSC GRE Single (2 or 3 depending the model)

1. Go to vSphere, New Machine > Deploy VM from OVF or OVA (on version 5.5 File > Deploy OVF template)



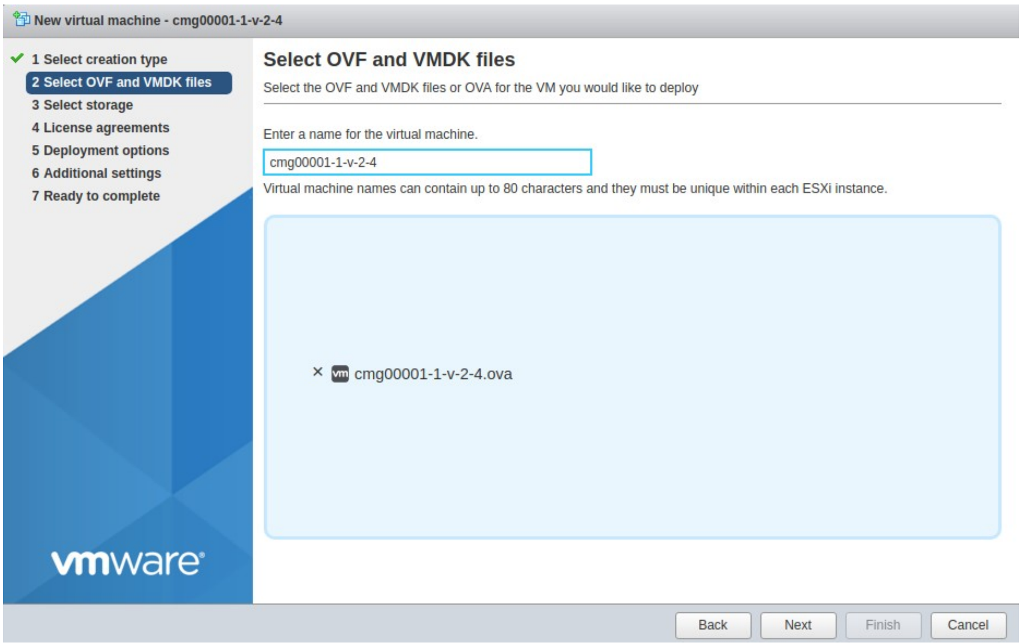
Select creation type

How would you like to create a Virtual Machine?

Selected: Deploy a virtual machine from an OVF or OVA file

This option guides you through the process of creating a virtual machine from an OVF and VMDK files.

2. Select the OVA File and put the name for the CSC



Select OVF and VMDK files

Select the OVF and VMDK files or OVA for the VM you would like to deploy

Enter a name for the virtual machine.

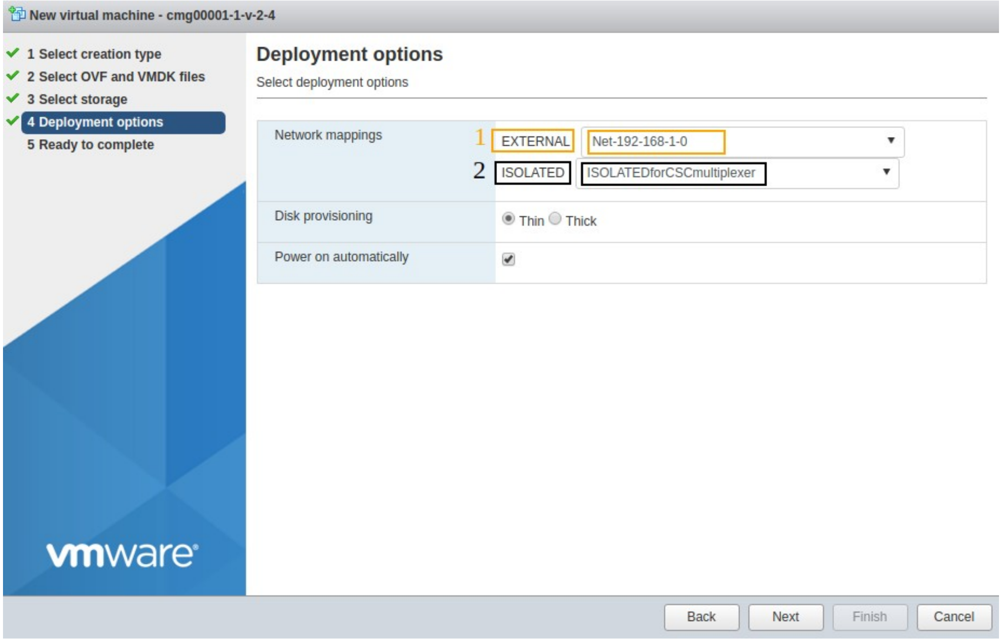
cmg00001-1-v-2-4

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

× cmg00001-1-v-2-4.ova

3. Select Storage

4. On Deployment Options, map the interfaces EXTERNAL and ISOLATED accordingly:



Deployment options

Select deployment options

Network mappings: EXTERNAL — Net-192-168-1-0; ISOLATED — ISOLATEDforCSCmultiplexer

Disk provisioning: ● Thin ○ Thick

Power on automatically: ☑

Note: In this example the “EXTERNAL” to “Net-192-168-1-0” and the “ISOLATED” Network Name was mapped to “ISOLATEDforCSCMultiplexer”.

5. Click Next > Ready to Complete > Finish

IMPORTANT : Repeat the process for CSC #2 (and CSC #3 if available)

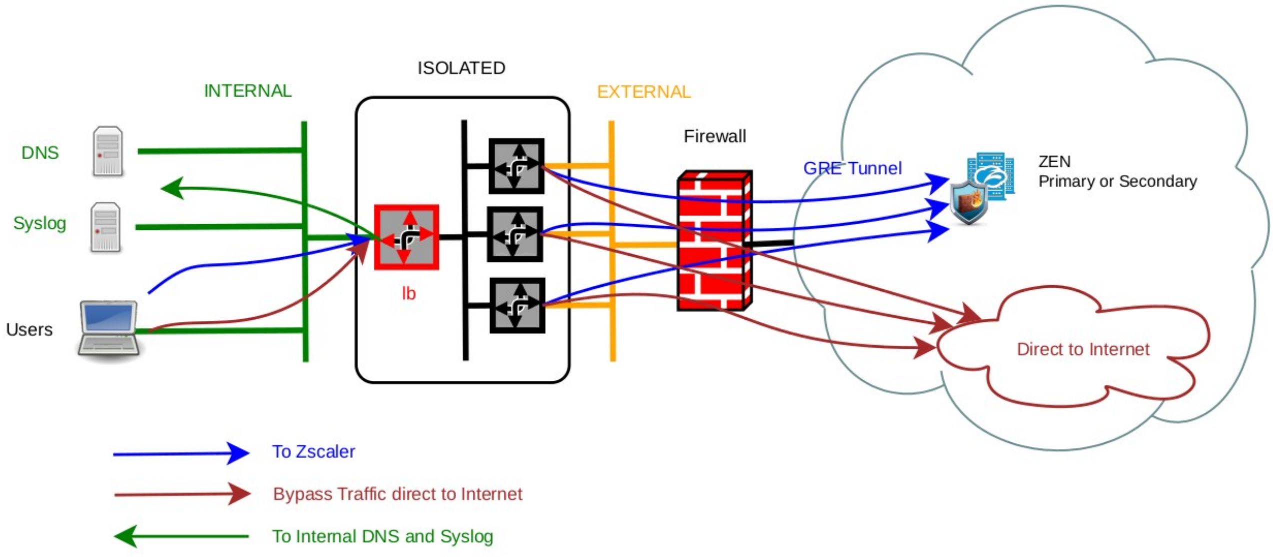
6 Firewall Requirements

The CSC Mutliplex GRE can be connected directly to Internet Public IPs or behind a Firewall (NAT is supported).

The most common scenario is to sit the CSC Multiplex GRE behind a Firewall.

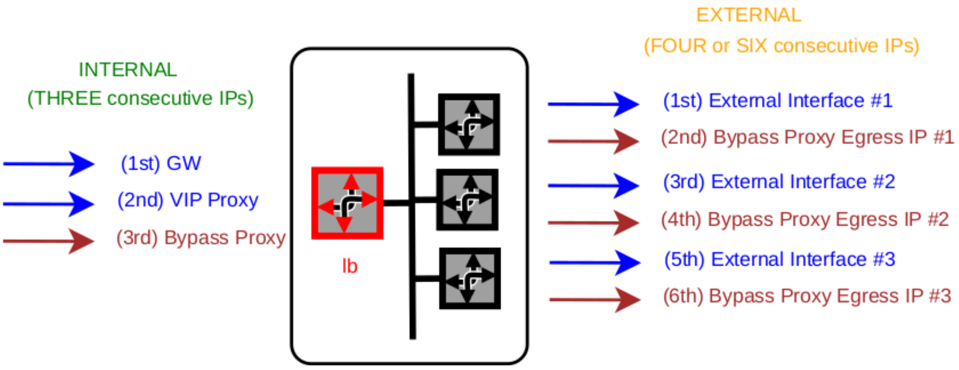
6.1 Traffic Flow

The following diagram shows how the traffic flows when using the CSC Multiplex GRE:



6.2 Internal and External Interfaces IPs

The CSC Multiplex GRE uses 3 x Internal IPs and 4 (or 6) x External IPs. Here a diagram showing the IPs on the CSC Multiplex GRE:


INTERNAL
(THREE consecutive IPs)
(1st) GW
(2nd) VIP Proxy
(3rd) Bypass Proxy
lb
EXTERNAL
(FOUR or SIX consecutive IPs)
(1st) External Interface #1
(2nd) Bypass Proxy Egress IP #1
(3rd) External Interface #2
(4th) Bypass Proxy Egress IP #2
(5th) External Interface #3
(6th) Bypass Proxy Egress IP #3

6.3 External Interface: Firewall Configuration

On the External Interface of the CSC Multiplex GRE, the 1st, 3rd and 5th IPs are used for traffic to Zscaler, keepalives and some particular troubleshooting tests.

The 2nd, 4th and 6th are used for the Bypass Proxy functionality.

6.3.1 NAT Rules

When the CSC Multiplex GRE is behind a firewall, the following NAT rules are required:

Item	**IPs to NAT**	**Public IP to use**	**NAT Type**	**Description**
1	1st, 3rd, 5th	Your Public IP (*)	Static (1:1)	Static NAT is required GRE Protocol 47.
2	2nd, 4th, 6th	Any Public IP available	Hide (N:1)	Used for Bypass Proxy

(*) Some FW will require a dedicated IP when NATing GRE Protocol 47. We recommend to use a dedicated Public IP.

6.3.2 Allow Rules

Item	**Source IP**	**Destination IP**	**Protocol**	**Ports**	**Description**
1	1st, 3rd, 5th	Zscaler ZEN nodes (Primary and Secondary)	GRE (47)	N/A	Allow GRE protocol 47 to Zscaler ZEN Nodes.
2	1st, 3rd, 5th	Zscaler ZEN nodes (Primary and Secondary)	TCP	80	Layer 7 Keepalives to Zscaler Nodes.
3	2nd, 4th, 6th	All Internet	TCP	80, 443 TCP High Ports: 1024 - 65535	Used for Bypass Proxy to reach Internet sites. Port 80 and 433 are mandatory. High Port are optional, but probably required. A lot of Cloud Providers are using High Ports today (SAP for example)
4	1st, 3rd, 5th	Zscaler ZEN nodes (Primary and Secondary) and PAC File Servers	ICMP		Used for testing purposes. Allow ping (echo – echo-reply) and traceroute (“time-exceed”)
5	1st, 3rd, 5th	Public DNS Servers	UDP	53	(Optional). Only needed if you are using Public DNS.

6.4 Internal Interface: Firewall Configuration

In the case you want to apply internal Firewall Rules, here the description of the IP and Ports in use on the CSC Multiplex GRE.

The CSC Multiplex GRE uses 3 Internal IPs. Here the description and purpose of each one:

6.4.1 Gateway IP (1st IP)

The first internal IP of the CSC Multiplex GRE is the Gateway IP. This IP is commonly used in two scenarios:

1. Zscaler Cloud Firewall: You can send all ports and protocols to Zscaler cloud and to use this Internal Cluster IP as default GW to internet.
2. No PAC file scenario: When you don't want to implement PAC files or Explicit proxies on your devices and you want to redirect all HTTP/HTTPS traffic to Zscaler, you can create a rule in your FW redirecting all HTTP/HTTPS to the Internal Cluster IP

Item	Protocol	Port / Service	Used for:
1	All	All	Zscaler Cloud Firewall To forward HTTP/HTTPS traffic (No PAC or Explicit Proxy scenario)

6.4.2 VIP Proxy (2nd IP)

The second internal IP of the CSC Multiplex GRE is the VIP Proxy. The VIP Proxy is a direct connection to Zscaler proxies in the cloud through the GRE tunnels.

The VIP Proxy is used in two scenarios:

1. As a default proxy on the PAC file.
2. As Explicit proxy.

Item	Protocol	Port / Service	Used for:
1	TCP	80 / 9400	Zscaler Web Security proxy

6.4.3 Bypass Proxy (3rd)

The Third internal IP of the CSC Multiplex GRE is the Bypass Proxy. The Bypass Proxy allows to send specific configured URLs direct to the internet.

The Bypass Proxy is used in several scenarios like this ones:

1. When the destination Web Site requires the traffic coming from the local customer IP and not Zscaler.

2. When the customer wants to communicate direct with specific cloud services.
3. When the customer wants to communicate direct with specific trusted partners.
4. Etc.

Item	Protocol	Port / Service	Used for:
1	TCP	3128	Bypass Proxy.

6.4.4 Other traffic IN / OUT to / from internal IPs

Item	Protocol	Port / Service	Description
1	TCP (in)	22	Accepted on 1st and 3rd Internal IP. Used to access to SSH console.
2	UDP (in/out)	53	DNS to Local DNS servers
3	TCP (out)	Defined by the Admin. Typical 514 or 601	Syslog Servers

7 Powering up the CSC Multiplex GRE

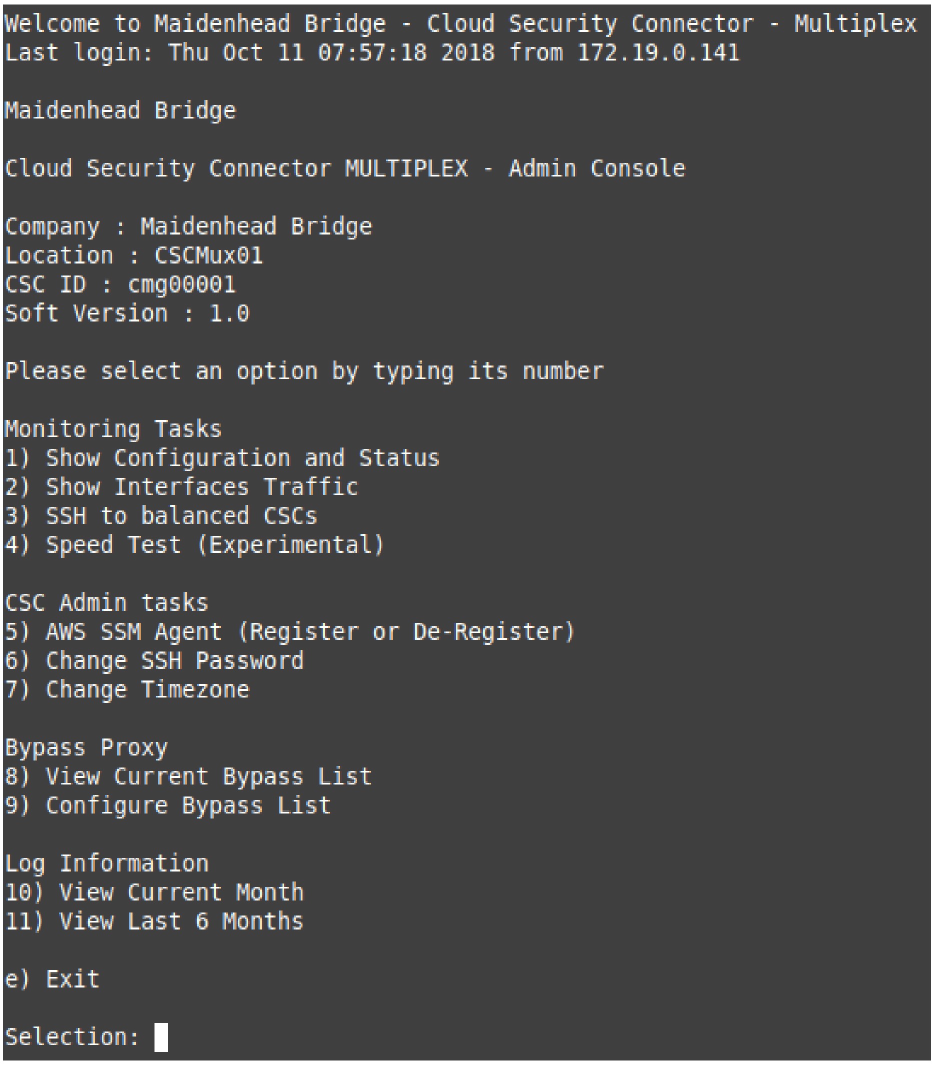
1. Power on the all Virtual Machines. At the first boot, please wait 3 minutes to allow the Load Balancer to acquire all CSC Single.
2. Open the VM Console (or SSH to GW IP)

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

Username: **cscadmin**

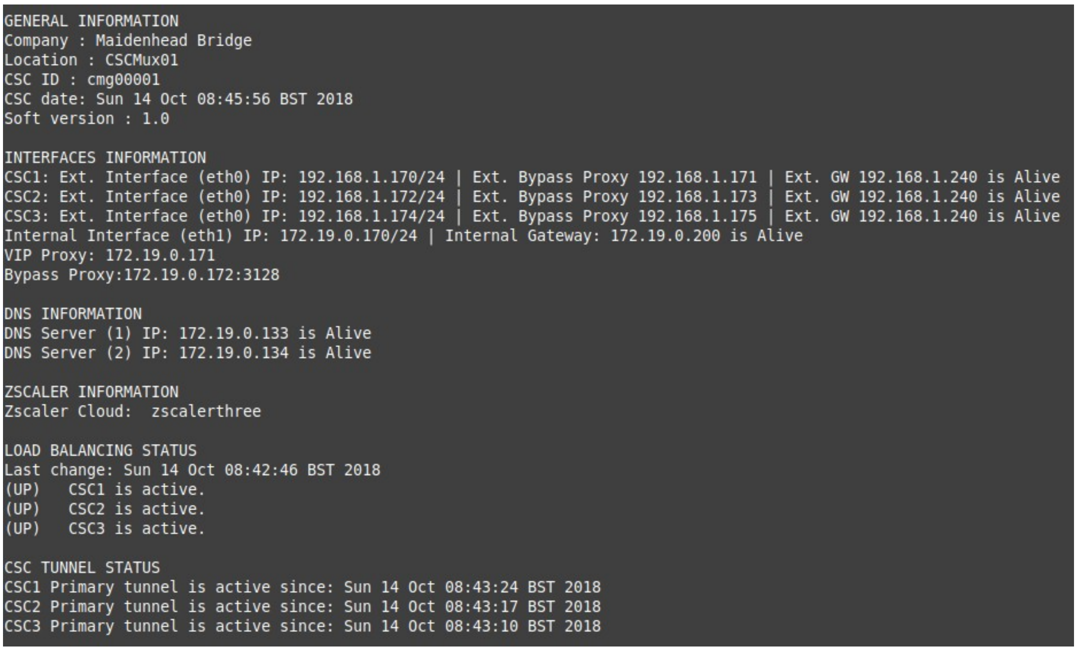
Password: **maidenheadbridge**

Note: SSH to the EXTERNAL interfaces is not allowed.



```
Welcome to Maidenhead Bridge - Cloud Security Connector - Multiplex
Last login: Thu Oct 11 07:57:18 2018 from 172.19.0.141

Maidenhead Bridge

Cloud Security Connector MULTIPLEX - Admin Console

Company : Maidenhead Bridge
Location : CSCMux01
CSC ID : cmg00001
Soft Version : 1.0

Please select an option by typing its number

Monitoring Tasks
1) Show Configuration and Status
2) Show Interfaces Traffic
3) SSH to balanced CSCs
4) Speed Test (Experimental)

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

Bypass Proxy
8) View Current Bypass List
9) Configure Bypass List

Log Information
10) View Current Month
11) View Last 6 Months

e) Exit

Selection: █
```

3. Select 1) Show Configuration and Status check “Load Balancing” and “Tunnel” Status.



```
GENERAL INFORMATION
Company : Maidenhead Bridge
Location : CSCMux01
CSC ID : cmg00001
CSC date: Sun 14 Oct 08:45:56 BST 2018
Soft version : 1.0

INTERFACES INFORMATION
CSC1: Ext. Interface (eth0) IP: 192.168.1.170/24 | Ext. Bypass Proxy 192.168.1.171 | Ext. GW 192.168.1.240 is Alive
CSC2: Ext. Interface (eth0) IP: 192.168.1.172/24 | Ext. Bypass Proxy 192.168.1.173 | Ext. GW 192.168.1.240 is Alive
CSC3: Ext. Interface (eth0) IP: 192.168.1.174/24 | Ext. Bypass Proxy 192.168.1.175 | Ext. GW 192.168.1.240 is Alive
Internal Interface (eth1) IP: 172.19.0.170/24 | Internal Gateway: 172.19.0.200 is Alive
VIP Proxy: 172.19.0.171
Bypass Proxy:172.19.0.172:3128

DNS INFORMATION
DNS Server (1) IP: 172.19.0.133 is Alive
DNS Server (2) IP: 172.19.0.134 is Alive

ZSCALER INFORMATION
Zscaler Cloud:  zscalerthree

LOAD BALANCING STATUS
Last change: Sun 14 Oct 08:42:46 BST 2018
(UP)   CSC1 is active.
(UP)   CSC2 is active.
(UP)   CSC3 is active.

CSC TUNNEL STATUS
CSC1 Primary tunnel is active since: Sun 14 Oct 08:43:24 BST 2018
CSC2 Primary tunnel is active since: Sun 14 Oct 08:43:17 BST 2018
CSC3 Primary tunnel is active since: Sun 14 Oct 08:43:10 BST 2018
```

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 Cluster IP as your default Gateway to Zscaler and to send all ports and protocols.

Take a look of the next section for more details.

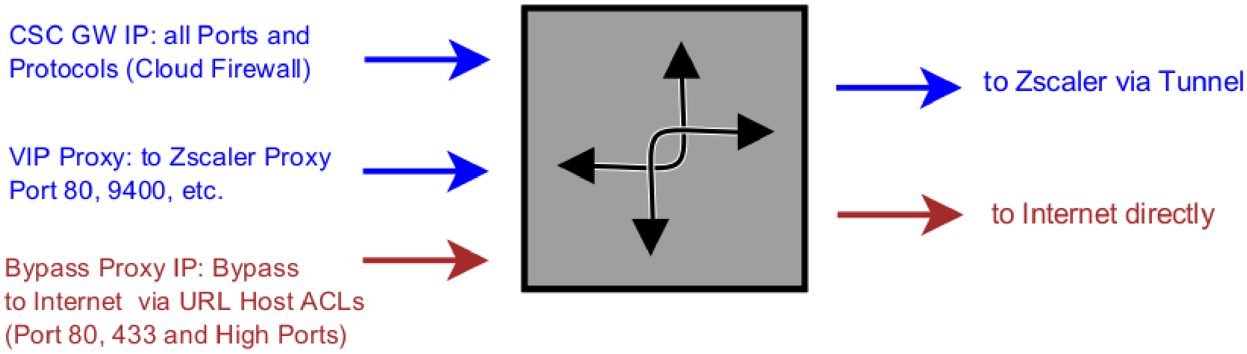
8 How to Redirect traffic to the CSC

The objective of the Cloud Security Connectors of Maidenhead Bridge is to provide a simple architecture, 100% proven that works, to connect to Zscaler.

Every member of the CSC family follows the principle of “three IPs” on the internal side:

- **(1st IP)** CSC **Internal Interface**: To be used as Default Gateway for internal devices behind the CSC redirecting all ports and protocols to Zscaler when using Cloud Firewall.
- **(2nd IP) VIP Proxy:** This Virtual IP Proxy translates the packets directly to the Zscaler proxy. To be used when PAC files are implemented or explicit proxy.
- **(3rd IP) Bypass Proxy:** The Bypass Proxy enables a simple way to do Direct Bypasses to Internet.

Here an illustration about this:


CSC GW IP: all Ports and Protocols (Cloud Firewall)
VIP Proxy: to Zscaler Proxy Port 80, 9400, etc.
Bypass Proxy IP: Bypass to Internet via URL Host ACLs (Port 80, 433 and High Ports)
to Zscaler via Tunnel
to Internet directly

How to Redirect your traffic:

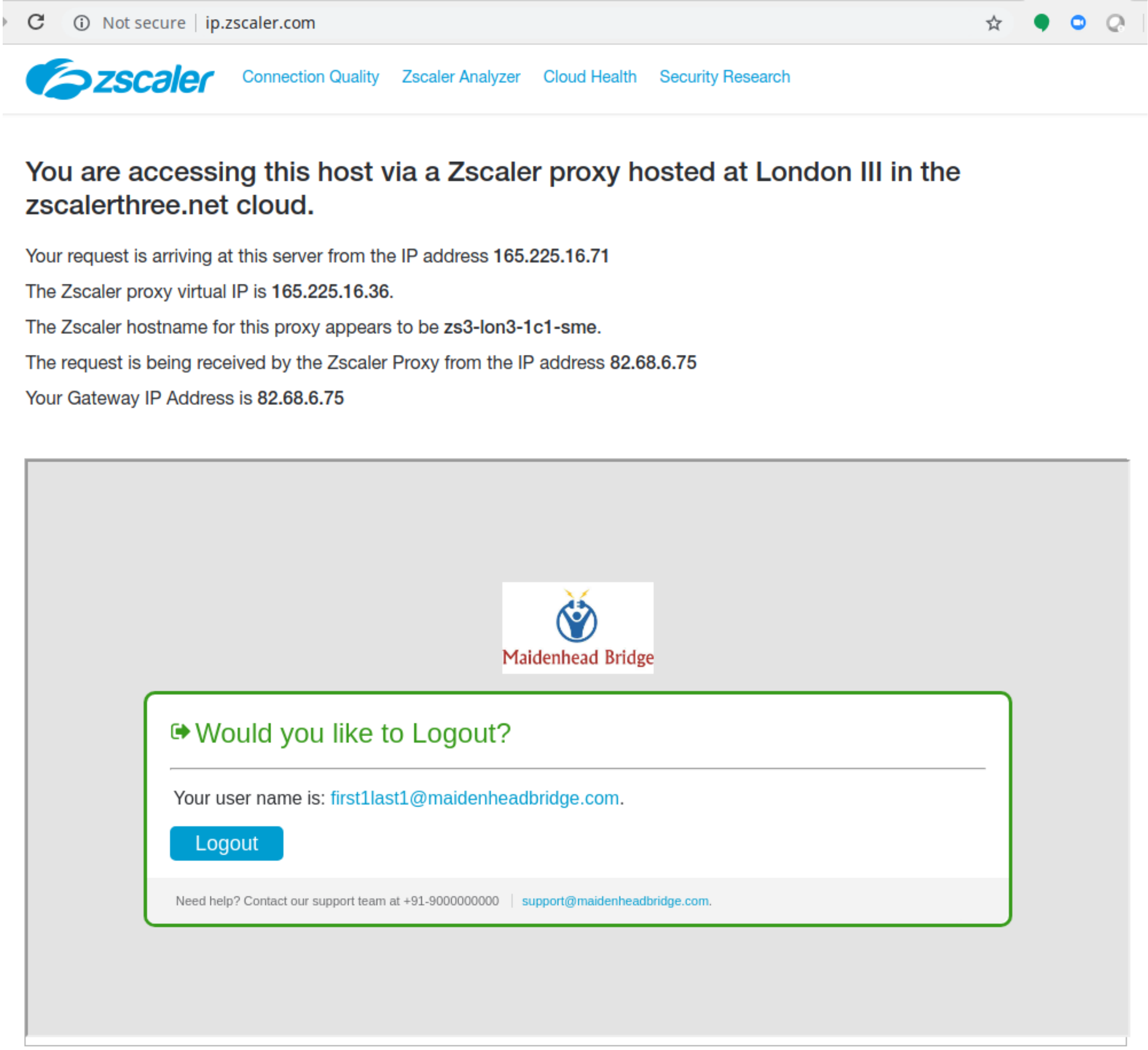
1. Sending all traffic using CSC (Internal Interface) GW IP as default gateway to internet for all internal devices.
2. Using a PAC File: You can download a PAC file Example from here: Click here

Note: The Zscaler recommend method is to use PAC files over GRE tunnels.

8.1 Verifying that your reaching Zscaler.

8.1.1 Using a PC

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



You are accessing this host via a Zscaler proxy hosted at London III in the zscalerthree.net cloud.

Your request is arriving at this server from the IP address **165.225.16.71**

The Zscaler proxy virtual IP is **165.225.16.36**.

The Zscaler hostname for this proxy appears to be **zs3-lon3-1c1-sme**.

The request is being received by the Zscaler Proxy from the IP address **82.68.6.75**

Your Gateway IP Address is **82.68.6.75**

Would you like to Logout?

Your user name is: first1last1@maidenheadbridge.com.

Need help? Contact our support team at +91-9000000000 | support@maidenheadbridge.com.

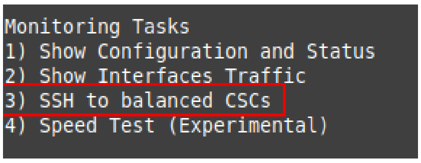
This page shows:

(values of this example between brackets [])

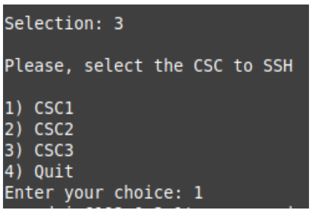
- Cloud name: [Zscaler Three]
- Node: [London III]
- Zscaler internal values [165.225.16.71, 165.225.16.36, zs3-lon3-1c1-sme]
- Your Gateway IP addresses [82.68.6.75. This is your public IP]
- The name or logo of your organization [Maidenhead Bridge]
- The Username (if Authentication was enabled on the location) [first1last1@maidenheadbridge.com]

8.1.2 Using the “Show Configuration and Status” menu of each CSC GRE single.

The CSC Multiplex Console allow you to login to each CSC GRE Single for particular check of statuses of each one:

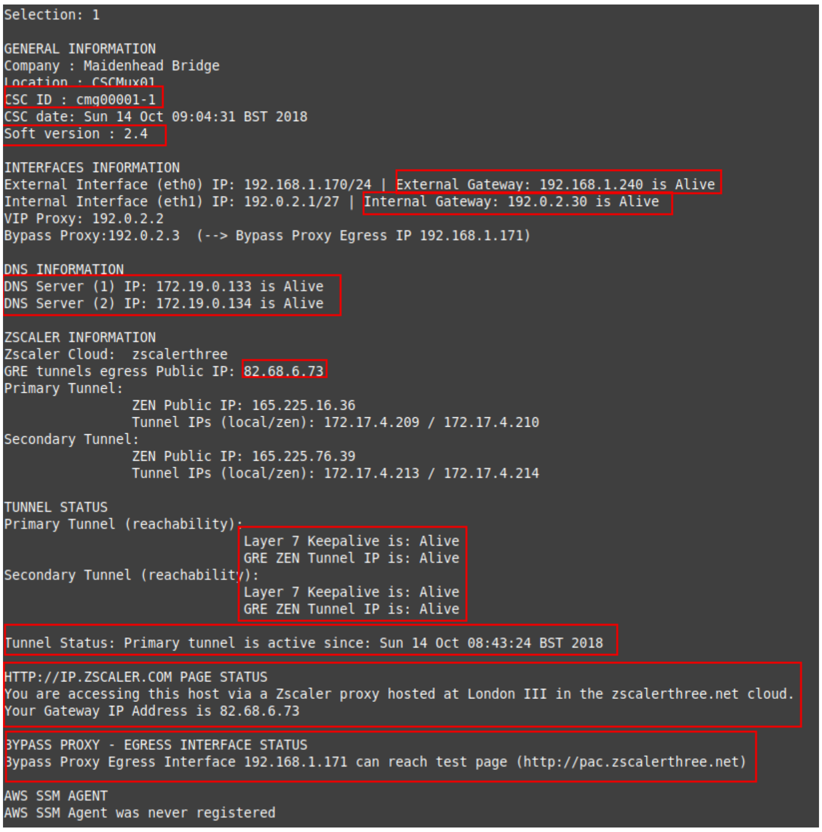


```
Monitoring Tasks
1) Show Configuration and Status
2) Show Interfaces Traffic
3) SSH to balanced CSCs
4) Speed Test (Experimental)
```



```
Selection: 3

Please, select the CSC to SSH

1) CSC1
2) CSC2
3) CSC3
4) Quit
Enter your choice: 1
```

And you can check the status of each one in particular. Here showing CSC1:



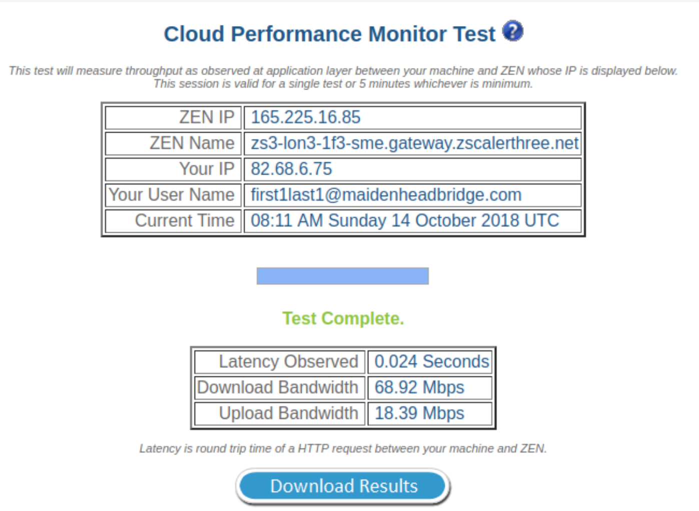
```
Selection: 1

GENERAL INFORMATION
Company : Maidenhead Bridge
Location : CSCMux01
CSC ID : cmg00001-1
CSC date: Sun 14 Oct 09:04:31 BST 2018
Soft version : 2.4

INTERFACES INFORMATION
External Interface (eth0) IP: 192.168.1.170/24 | External Gateway: 192.168.1.240 is Alive
Internal Interface (eth1) IP: 192.0.2.1/27 | Internal Gateway: 192.0.2.30 is Alive
VIP Proxy: 192.0.2.2
Bypass Proxy:192.0.2.3  (--> Bypass Proxy Egress IP 192.168.1.171)

DNS INFORMATION
DNS Server (1) IP: 172.19.0.133 is Alive
DNS Server (2) IP: 172.19.0.134 is Alive

ZSCALER INFORMATION
Zscaler Cloud:  zscalerthree
GRE tunnels egress Public IP: 82.68.6.73
Primary Tunnel:
                ZEN Public IP: 165.225.16.36
                Tunnel IPs (local/zen): 172.17.4.209 / 172.17.4.210
Secondary Tunnel:
                ZEN Public IP: 165.225.76.39
                Tunnel IPs (local/zen): 172.17.4.213 / 172.17.4.214

TUNNEL STATUS
Primary Tunnel (reachability):
                              Layer 7 Keepalive is: Alive
                              GRE ZEN Tunnel IP is: Alive
Secondary Tunnel (reachability):
                              Layer 7 Keepalive is: Alive
                              GRE ZEN Tunnel IP is: Alive

Tunnel Status: Primary tunnel is active since: Sun 14 Oct 08:43:24 BST 2018

HTTP://IP.ZSCALER.COM PAGE STATUS
You are accessing this host via a Zscaler proxy hosted at London III in the zscalerthree.net cloud.
Your Gateway IP Address is 82.68.6.73

3YPASS PROXY - EGRESS INTERFACE STATUS
3ypass Proxy Egress Interface 192.168.1.171 can reach test page (http://pac.zscalerthree.net)

AWS SSM AGENT
AWS SSM Agent was never registered
```

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

8.2 Checking Connection Quality

8.2.1 Using a PC

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



Cloud Performance Monitor Test

This test will measure throughput as observed at application layer between your machine and ZEN whose IP is displayed below. This session is valid for a single test or 5 minutes whichever is minimum.

ZEN IP	165.225.16.85
ZEN Name	zs3-lon3-1f3-sme.gateway.zscalerthree.net
Your IP	82.68.6.75
Your User Name	first1last1@maidenheadbridge.com
Current Time	08:11 AM Sunday 14 October 2018 UTC

Test Complete.

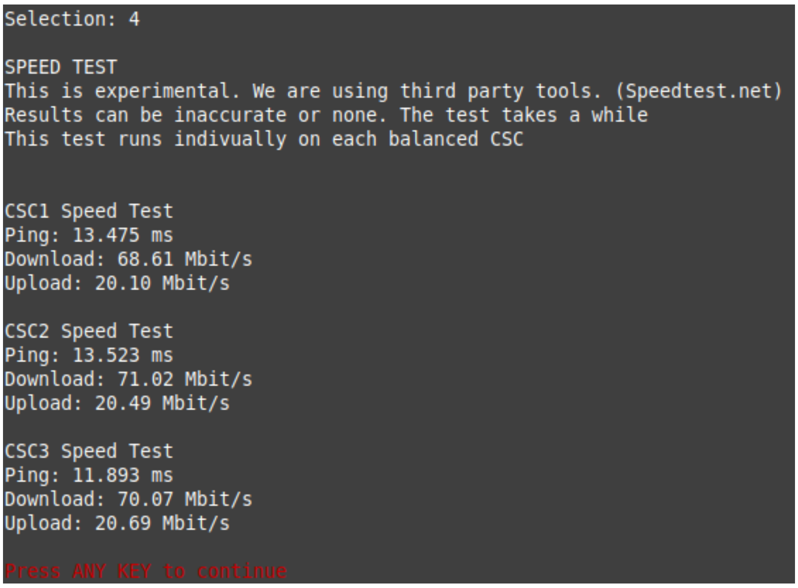
Latency Observed	0.024 Seconds
Download Bandwidth	68.92 Mbps
Upload Bandwidth	18.39 Mbps

Latency is round trip time of a HTTP request between your machine and ZEN.

8.2.2 Using “Speed Test” menu of the CSC Multiplex GRE

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

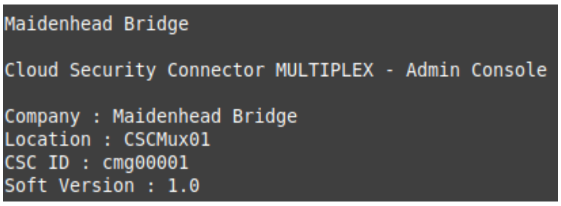
With this tool, you can check the quality of each GRE tunnel individually.



```
Selection: 4

SPEED TEST
This is experimental. We are using third party tools. (Speedtest.net)
Results can be inaccurate or none. The test takes a while
This test runs indivually on each balanced CSC


CSC1 Speed Test
Ping: 13.475 ms
Download: 68.61 Mbit/s
Upload: 20.10 Mbit/s

CSC2 Speed Test
Ping: 13.523 ms
Download: 71.02 Mbit/s
Upload: 20.49 Mbit/s

CSC3 Speed Test
Ping: 11.893 ms
Download: 70.07 Mbit/s
Upload: 20.69 Mbit/s

Press ANY KEY to continue
```

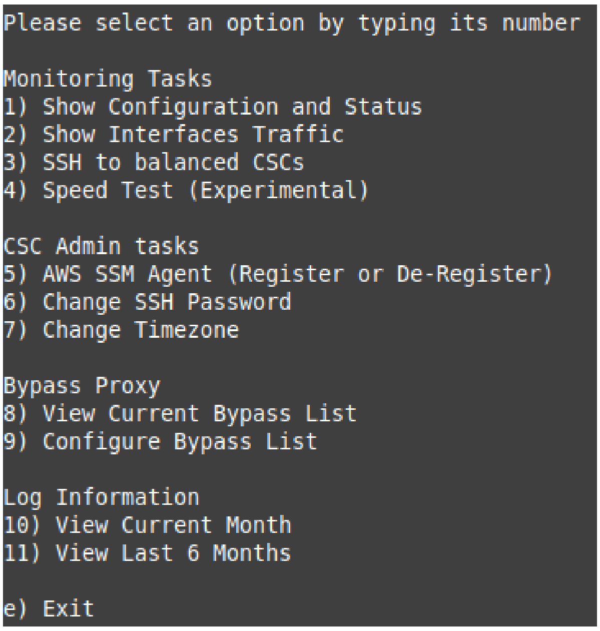
9 CSC Multiplex GRE – Admin Console

The CSC Multiplex GRE has an Admin Console that allows to do different tasks. When you access to the Admin Console, the following information appears on top:



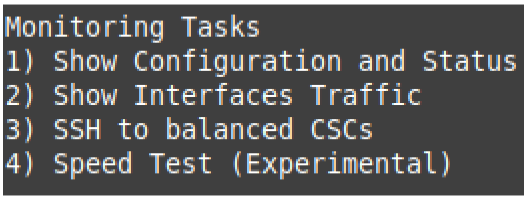
```
Maidenhead Bridge

Cloud Security Connector MULTIPLEX - Admin Console

Company : Maidenhead Bridge
Location : CSCMux01
CSC ID : cmg00001
Soft Version : 1.0
```

And you can select the following items:



```
Please select an option by typing its number

Monitoring Tasks
1) Show Configuration and Status
2) Show Interfaces Traffic
3) SSH to balanced CSCs
4) Speed Test (Experimental)

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

Bypass Proxy
8) View Current Bypass List
9) Configure Bypass List

Log Information
10) View Current Month
11) View Last 6 Months

e) Exit
```

9.1 Monitoring Tasks:

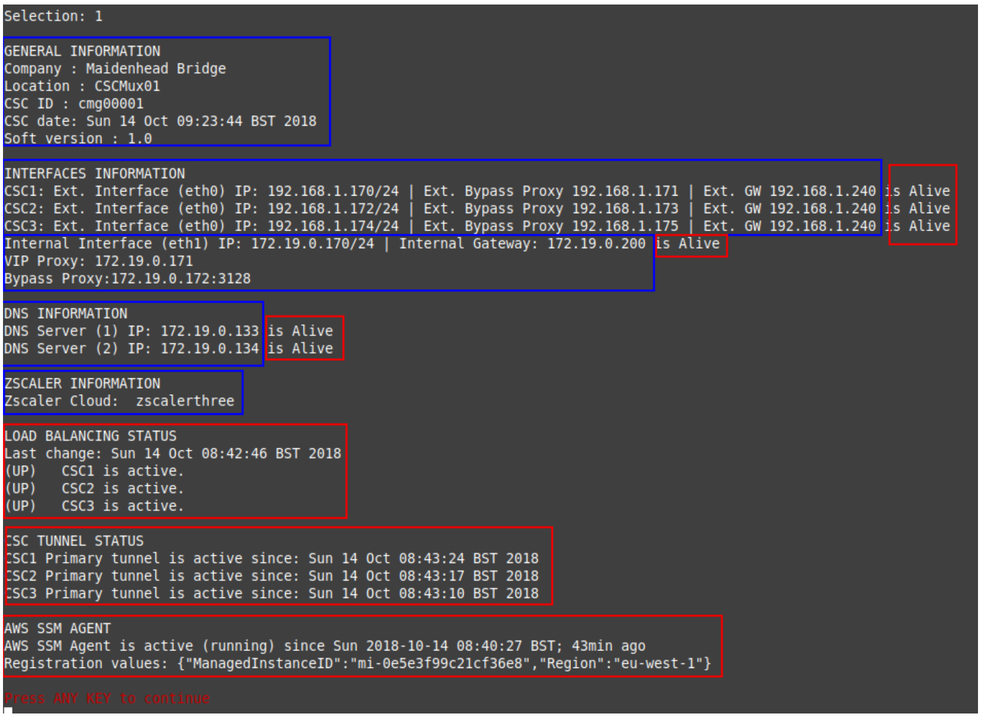


```
Monitoring Tasks
1) Show Configuration and Status
2) Show Interfaces Traffic
3) SSH to balanced CSCs
4) Speed Test (Experimental)
```

9.1.1 Show Configuration and Status

1. Show Configuration and Status. This menu show all parameters configured on the CSC Multiplex GRE and does several checks.

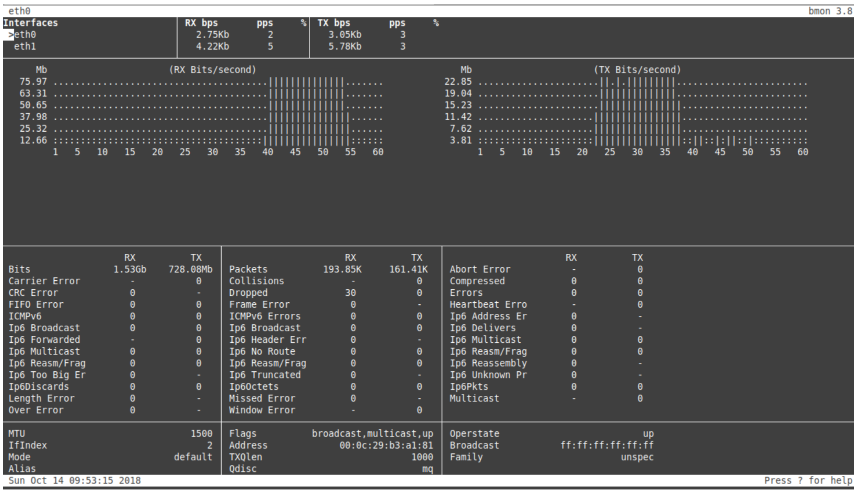
The following image shows in BLUE the Configuration information and in RED the statuses.



```
Selection: 1

GENERAL INFORMATION
Company : Maidenhead Bridge
Location : CSCMux01
CSC ID : cmg00001
CSC date: Sun 14 Oct 09:23:44 BST 2018
Soft version : 1.0

INTERFACES INFORMATION
CSC1: Ext. Interface (eth0) IP: 192.168.1.170/24 | Ext. Bypass Proxy 192.168.1.171 | Ext. GW 192.168.1.240 is Alive
CSC2: Ext. Interface (eth0) IP: 192.168.1.172/24 | Ext. Bypass Proxy 192.168.1.173 | Ext. GW 192.168.1.240 is Alive
CSC3: Ext. Interface (eth0) IP: 192.168.1.174/24 | Ext. Bypass Proxy 192.168.1.175 | Ext. GW 192.168.1.240 is Alive
Internal Interface (eth1) IP: 172.19.0.170/24 | Internal Gateway: 172.19.0.200 is Alive
VIP Proxy: 172.19.0.171
Bypass Proxy:172.19.0.172:3128

DNS INFORMATION
DNS Server (1) IP: 172.19.0.133 is Alive
DNS Server (2) IP: 172.19.0.134 is Alive

ZSCALER INFORMATION
Zscaler Cloud:  zscalerthree

LOAD BALANCING STATUS
Last change: Sun 14 Oct 08:42:46 BST 2018
(UP)   CSC1 is active.
(UP)   CSC2 is active.
(UP)   CSC3 is active.

CSC TUNNEL STATUS
CSC1 Primary tunnel is active since: Sun 14 Oct 08:43:24 BST 2018
CSC2 Primary tunnel is active since: Sun 14 Oct 08:43:17 BST 2018
CSC3 Primary tunnel is active since: Sun 14 Oct 08:43:10 BST 2018

AWS SSM AGENT
AWS SSM Agent is active (running) since Sun 2018-10-14 08:40:27 BST; 43min ago
Registration values: {"ManagedInstanceID":"mi-0e5e3f99c21cf36e8","Region":"eu-west-1"}

Press ANY KEY to continue
```

9.1.2 Show Interfaces Traffic

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



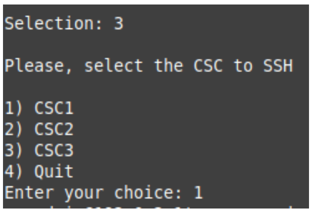
```
 eth0                                                                                                  bmon 3.8
Interfaces                      RX bps       pps     %  TX bps       pps     %
 >eth0                            2.75Kb       2        3.05Kb       3
  eth1                            4.22Kb       5        5.78Kb       3

      Mb                      (RX Bits/second)                                Mb                      (TX Bits/second)
   75.97 .......................................||||||||||||||.......       22.85 ......................||.|.|||||||||........................
   63.31 .......................................||||||||||||||.......       19.04 ......................||||||||||||||........................
   50.65 .......................................||||||||||||||.......       15.23 ......................|||||||||||||||.......................
   37.98 .......................................|||||||||||||||......       11.42 .....................||||||||||||||||.......................
   25.32 .......................................|||||||||||||||......        7.62 .....................||||||||||||||||.......................
   12.66 ::::::::::::::::::::::::::::::::::::::||||||||||||||||::::::        3.81 :::::::::::::::::::::||||||||||||||||::||::|:||::|::::::::::
         1   5   10   15   20   25   30   35   40   45   50   55   60              1   5   10   15   20   25   30   35   40   45   50   55   60

                        RX          TX                           RX          TX                           RX          TX
 Bits               1.53Gb    728.08Mb   Packets             193.85K     161.41K   Abort Error              -           0
 Carrier Error           -           0   Collisions                -           0   Compressed               0           0
 CRC Error               0           -   Dropped                  30           0   Errors                   0           0
 FIFO Error              0           0   Frame Error               0           -   Heartbeat Erro           -           0
 ICMPv6                  0           0   ICMPv6 Errors             0           0   Ip6 Address Er           0           -
 Ip6 Broadcast           0           0   Ip6 Broadcast             0           0   Ip6 Delivers             0           -
 Ip6 Forwarded           -           0   Ip6 Header Err            0           -   Ip6 Multicast            0           0
 Ip6 Multicast           0           0   Ip6 No Route              0           0   Ip6 Reasm/Frag           0           0
 Ip6 Reasm/Frag          0           0   Ip6 Reasm/Frag            0           0   Ip6 Reassembly           0           -
 Ip6 Too Big Er          0           -   Ip6 Truncated             0           -   Ip6 Unknown Pr           0           -
 Ip6Discards             0           0   Ip6Octets                 0           0   Ip6Pkts                  0           0
 Length Error            0           -   Missed Error              0           -   Multicast                -           0
 Over Error              0           -   Window Error              -           0

 MTU                              1500   Flags       broadcast,multicast,up   Operstate                        up
 IfIndex                             2   Address          00:0c:29:b3:a1:81   Broadcast         ff:ff:ff:ff:ff:ff
 Mode                          default   TXQlen                        1000   Family                       unspec
 Alias                                   Qdisc                           mq
 Sun Oct 14 09:53:15 2018                                                                               Press ? for help
```

IMPORTANT:

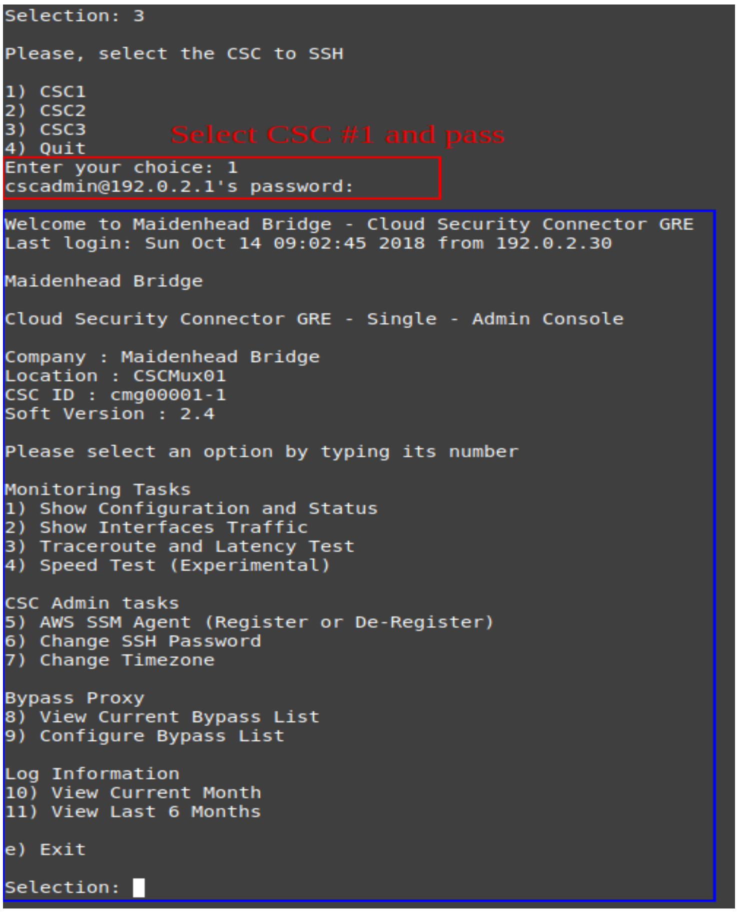
- Press “q” to quit
- Press “?” for help

9.1.3 SSH to balanced CSCs

Allows to get access to each balanced CSCs:



```
Selection: 3

Please, select the CSC to SSH

1) CSC1
2) CSC2
3) CSC3
4) Quit
Enter your choice: 1
```



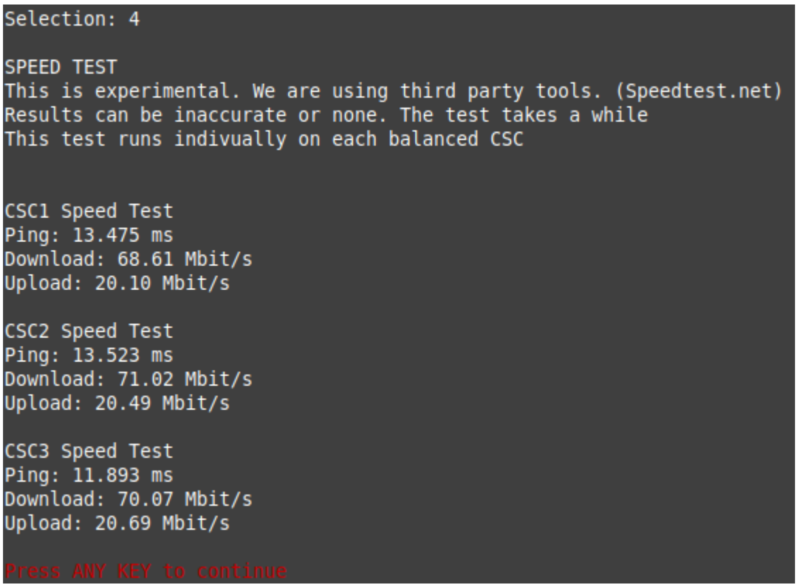
Select CSC #1 and pass

```
Selection: 3

Please, select the CSC to SSH

1) CSC1
2) CSC2
3) CSC3
4) Quit
Enter your choice: 1
cscadmin@192.0.2.1's password:
Welcome to Maidenhead Bridge - Cloud Security Connector GRE
Last login: Sun Oct 14 09:02:45 2018 from 192.0.2.30

Maidenhead Bridge

Cloud Security Connector GRE - Single - Admin Console

Company : Maidenhead Bridge
Location : CSCMux01
CSC ID : cmg00001-1
Soft Version : 2.4

Please select an option by typing its number

Monitoring Tasks
1) Show Configuration and Status
2) Show Interfaces Traffic
3) Traceroute and Latency Test
4) Speed Test (Experimental)

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

Bypass Proxy
8) View Current Bypass List
9) Configure Bypass List

Log Information
10) View Current Month
11) View Last 6 Months

e) Exit

Selection: 
```

9.1.4 Speed Test

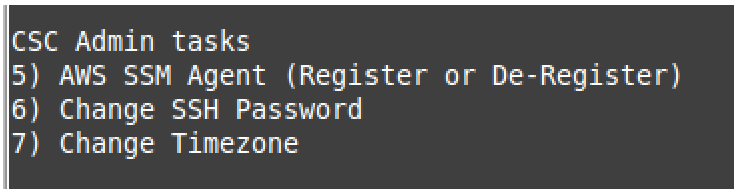
The CSC runs the Speedtest.net (same test that you can run from the Web Page) on each of the balanced CSC. This function is experimental due to we need to rely on third party tools.

With this tool, you can check the quality of each GRE tunnel individually.



```
Selection: 4

SPEED TEST
This is experimental. We are using third party tools. (Speedtest.net)
Results can be inaccurate or none. The test takes a while
This test runs indivually on each balanced CSC


CSC1 Speed Test
Ping: 13.475 ms
Download: 68.61 Mbit/s
Upload: 20.10 Mbit/s

CSC2 Speed Test
Ping: 13.523 ms
Download: 71.02 Mbit/s
Upload: 20.49 Mbit/s

CSC3 Speed Test
Ping: 11.893 ms
Download: 70.07 Mbit/s
Upload: 20.69 Mbit/s

Press ANY KEY to continue
```

9.2 CSC Admin Tasks



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

5. AWS SSM Agent (Register or De-Register)

6. Change SSH Password: Allows to change the password of the CSC.

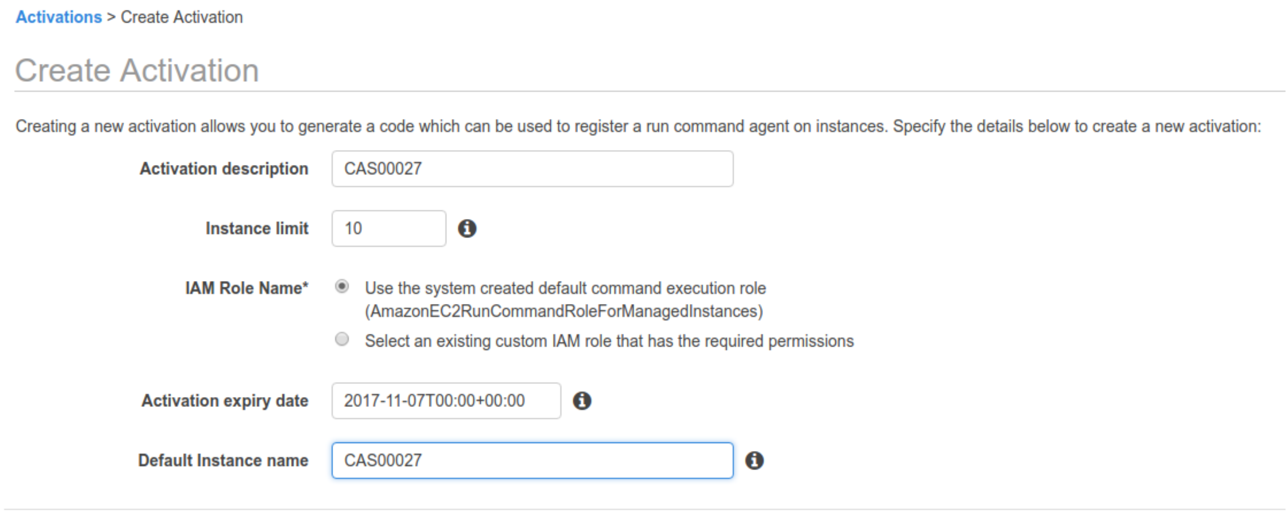
7. Change Timezone: In case if needed, you can select your Timezone here.

9.2.1 AWS SSM Agent (Register / De-Register)

One of the main functionalities added after version 2.0 is that the CSC GRE can be integrated with the Amazon Cloud (AWS). The CSC 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. AWS allows to manage for free up to 1000 managed instances.

The steps required to add the CSC are two:



Create Activation

Creating a new activation allows you to generate 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

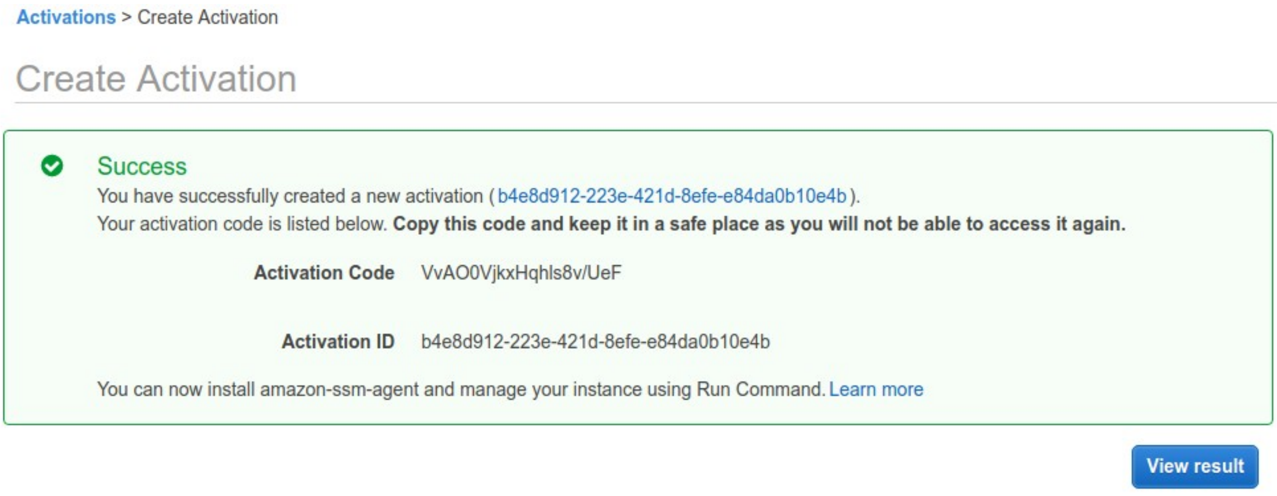
Activation expiry date 2017-11-07T00:00+00:00

Default Instance name CAS00027

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 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.**

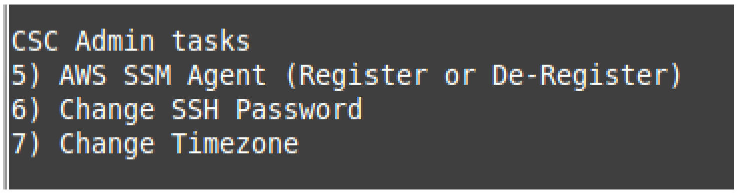
Activation Code VvAO0VjkxHqhls8v/UeF

Activation ID b4e8d912-223e-421d-8efe-e84da0b10e4b

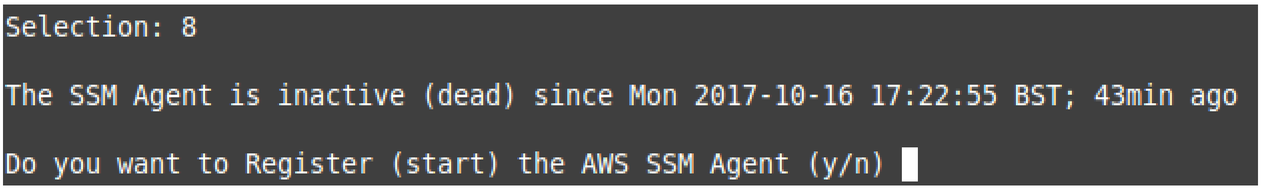
You can now install amazon-ssm-agent and manage your instance using Run Command. Learn more

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 “5) AWS SSM Agent (Register or De-Register)”



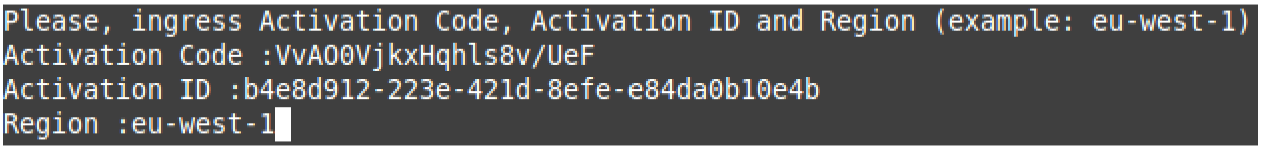
```
CSC Admin tasks
5) AWS SSM Agent (Register or De-Register)
6) Change SSH Password
7) Change Timezone
```



```
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)
```

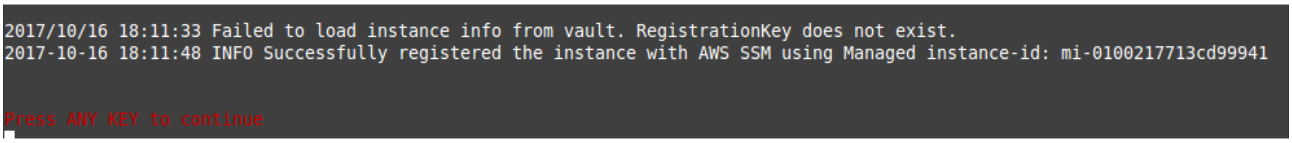
Ingress "y"

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
```

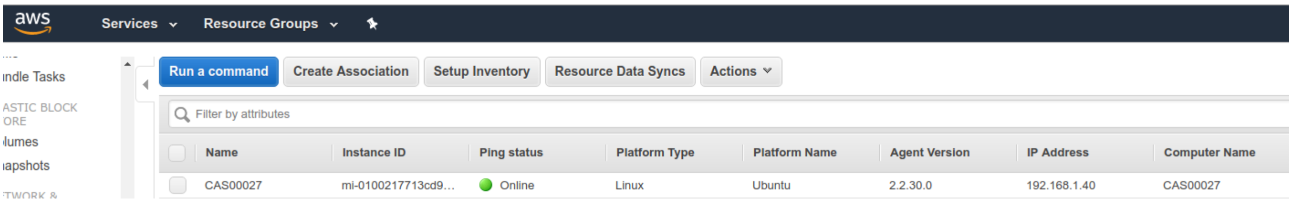
If the AWS SSM agent is registered successfully you will receive the following message:



```
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).

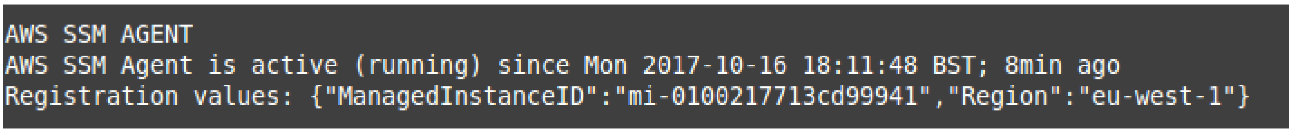
Go to your EC2 Console (SYSTEMS MANAGER SHARED RESOURCES > Managed Instances) and you will be able to see your CSC registered as an instance:



☐	Name	Instance ID	Ping status	Platform Type	Platform Name	Agent Version	IP Address	Computer Name
☐	CAS00027	mi-0100217713cd9...	● Online	Linux	Ubuntu	2.2.30.0	192.168.1.40	CAS00027

9.2.1.1 *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"}
```

IMPORTANT: Go to Appendix B to learn how to "Run Commands" from the AWS console to *monitoring the CSC and Update Bypass Lists.*

9.2.2 Change SSH Password

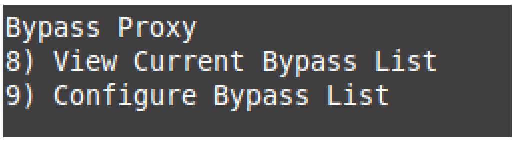
From this menu, you can change the SSH Password of the Admin Console.

9.2.3 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.

9.3 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
8) View Current Bypass List
9) 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:

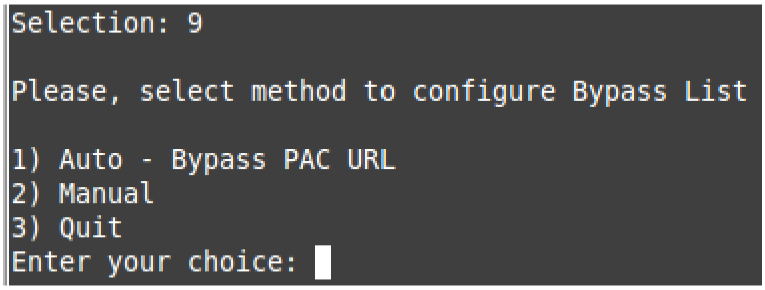
CSC	PAC file
Www.example.com	Www.example.com
.example.com	*.example.com
Important! Be careful not to create an "Open Proxy" setting something like ".com" that will allow to pass all domains ending on ".com"	

9.3.1 View Current Bypass List

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

9.3.2 Configure Bypass List

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



```
Selection: 9

Please, select method to configure Bypass List

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

9.3.2.1 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.

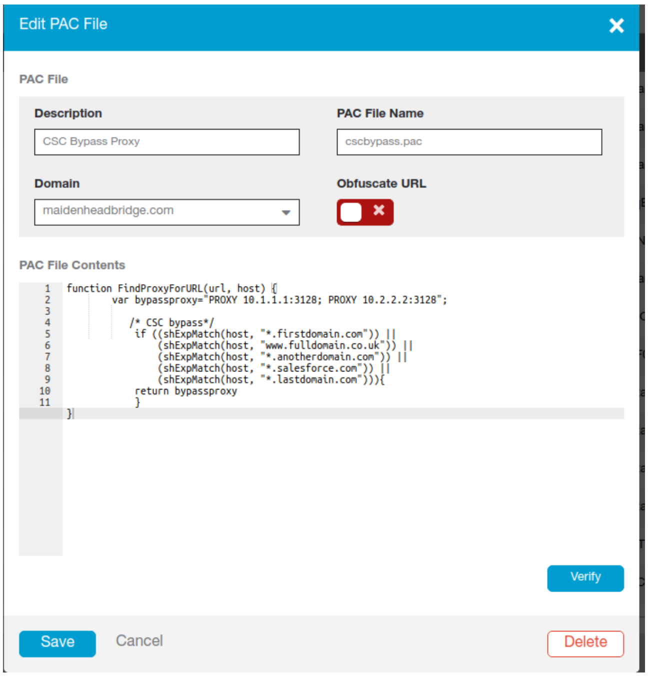
Example of "Bypass PAC file"

```
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:



Description: CSC Bypass Proxy

PAC File Name: cscbypass.pac

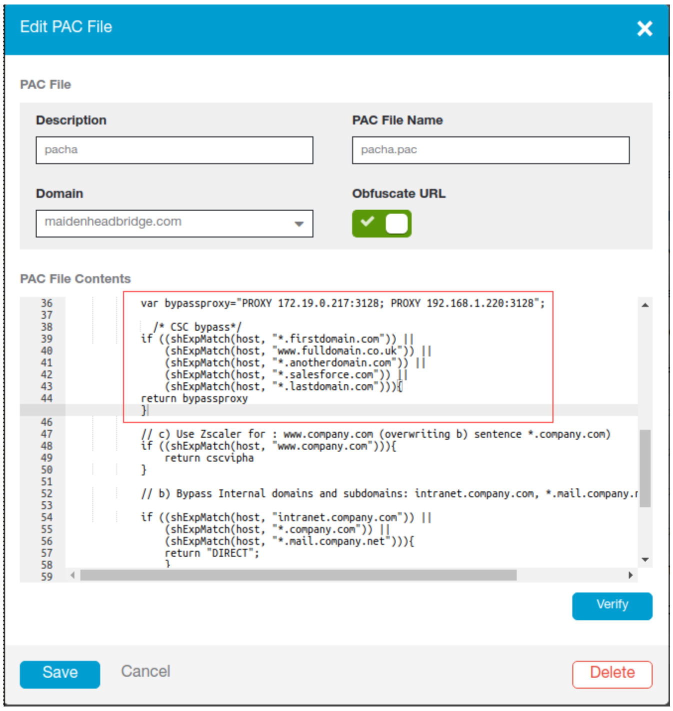
Domain: maidenheadbridge.com

Obfuscate URL: ☒

PAC File Contents

```
function FindProxyForURL(url, host) {
        var bypassproxy="PROXY 10.1.1.1:3128; PROXY 10.2.2.2:3128";

           /* 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
             }
}
```

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



Description: pacha

PAC File Name: pacha.pac

Domain: maidenheadbridge.com

Obfuscate URL: ✓

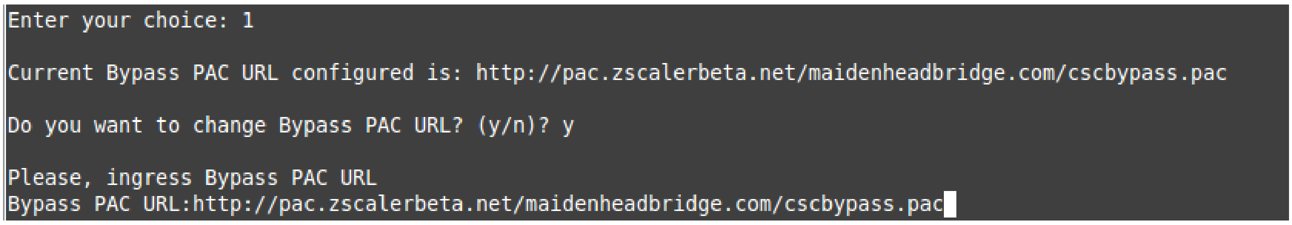
PAC File Contents

```
        var bypassproxy="PROXY 172.19.0.217:3128; PROXY 192.168.1.220:3128";

          /* 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
        }

        // c) Use Zscaler for : www.company.com (overwriting b) sentence *.company.com)
        if ((shExpMatch(host, "www.company.com"))){
            return cscvipha
        }

        // b) Bypass Internal domains and subdomains: intranet.company.com, *.mail.company.r

        if ((shExpMatch(host, "intranet.company.com")) ||
            (shExpMatch(host, "*.company.com")) ||
            (shExpMatch(host, "*.mail.company.net"))){
            return "DIRECT";
            }
```

Important: Proxy Bypass is reachable only on port TCP 3128

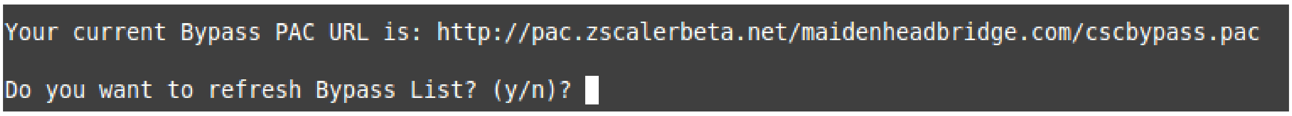
Configuration Steps:

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

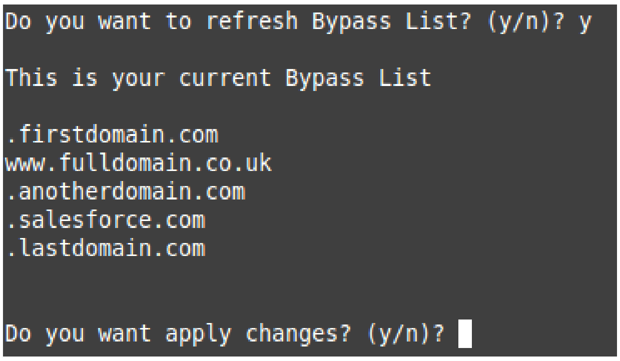


```
Enter your choice: 1

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:

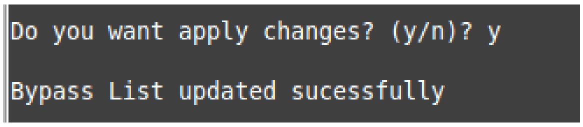


```
Your current Bypass PAC URL is: http://pac.zscalerbeta.net/maidenheadbridge.com/cscbypass.pac

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



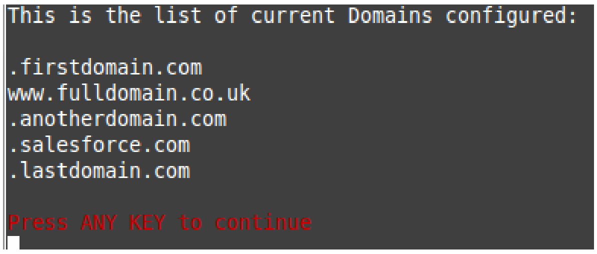
```
Do you want to refresh Bypass List? (y/n)? y

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)



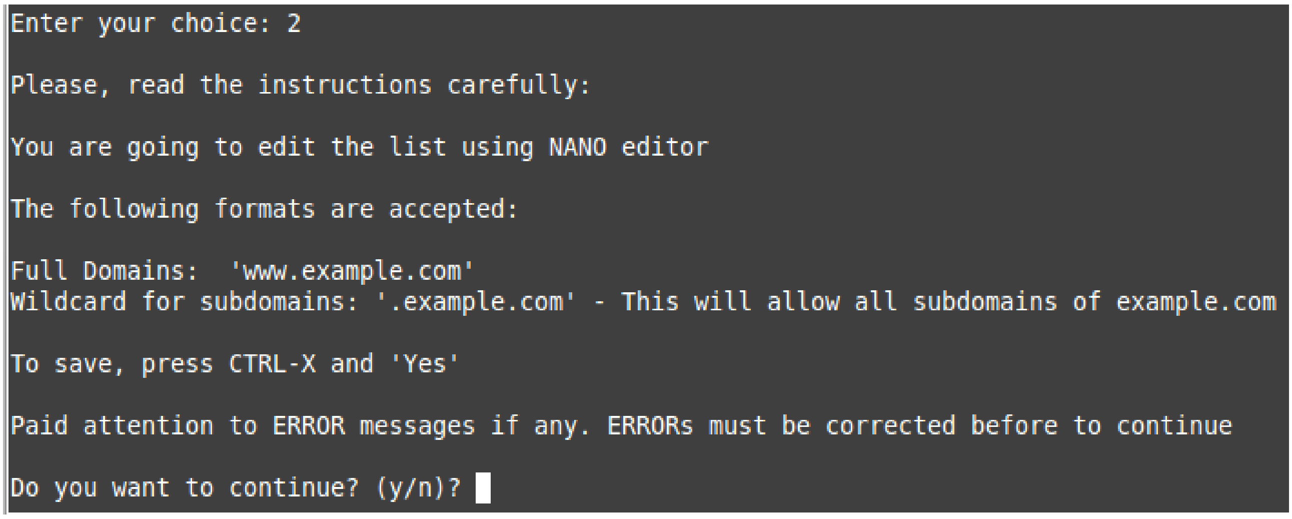
```
This is the list of current Domains configured:

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

Press ANY KEY to continue
```

IMPORTANT: Go to Appendix B to learn how to Update Bypass List from AWS

9.3.2.2 2) Manual

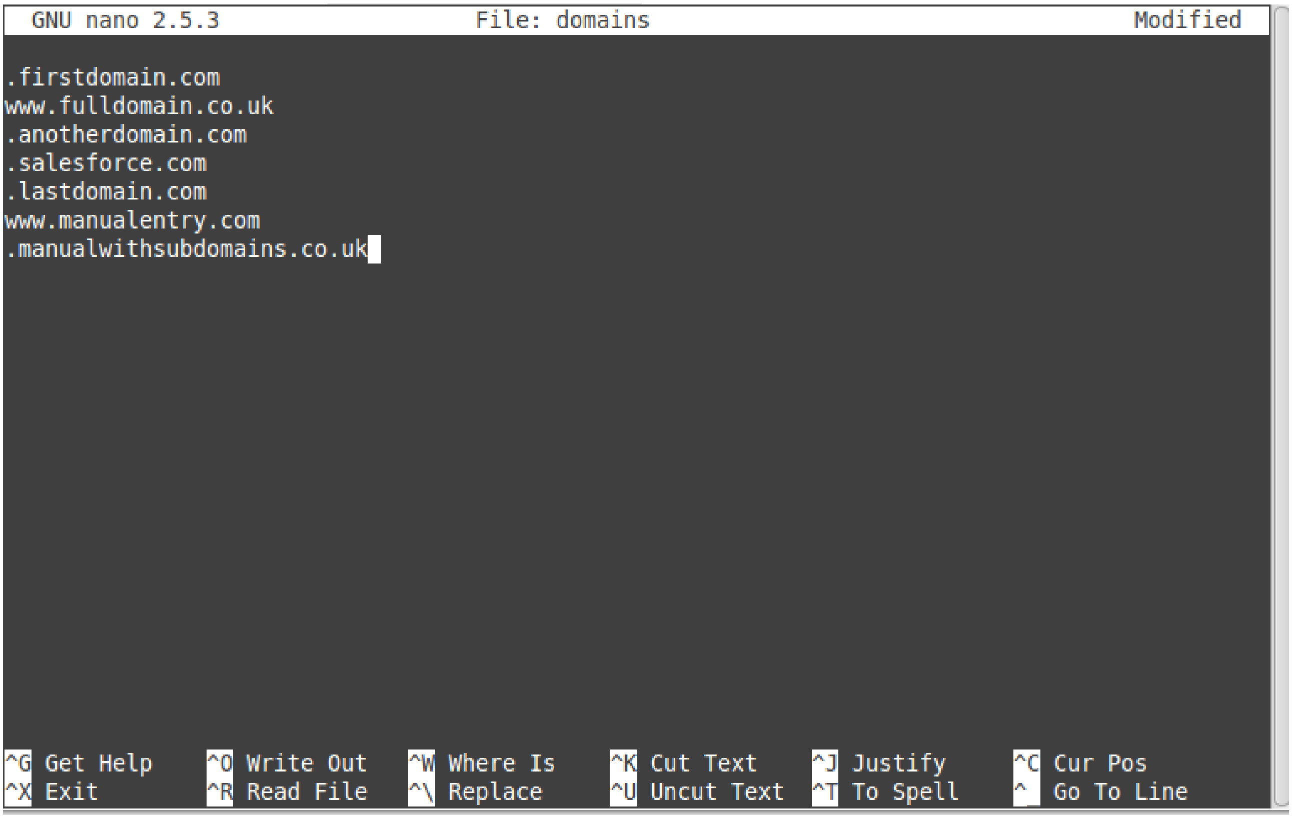
If you want to update manually your bypass list, follow this steps

1. Select Option 2)



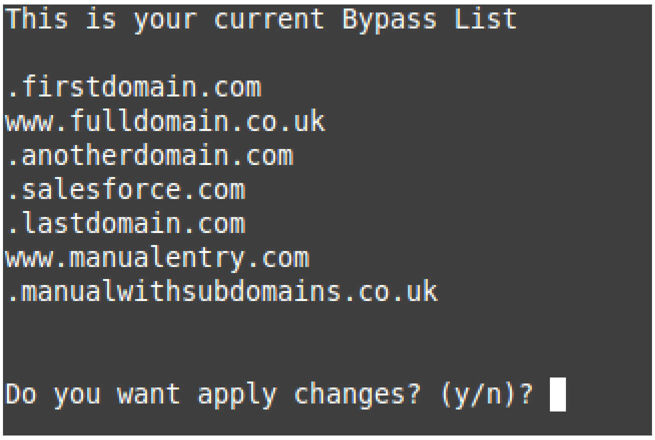
```
Enter your choice: 2

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”



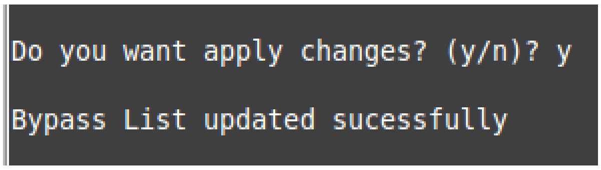
```
.firstdomain.com
www.fulldomain.co.uk
.anotherdomain.com
.salesforce.com
.lastdomain.com
www.manualentry.com
.manualwithsubdomains.co.uk
```

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:

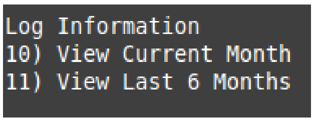


```
Do you want apply changes? (y/n)? y

Bypass List updated sucessfully
```

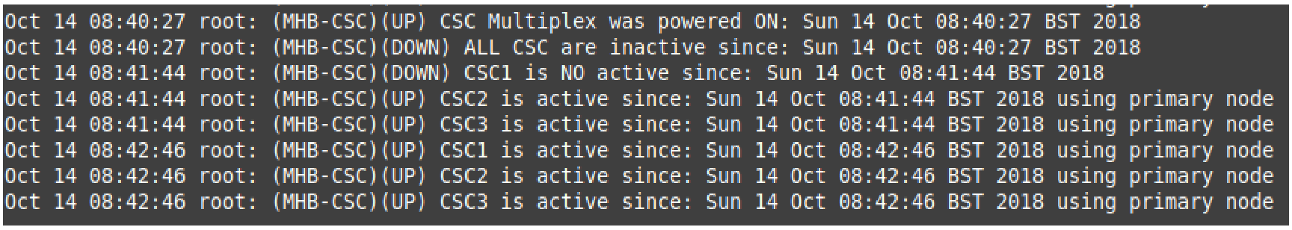
9.4 Log Information

This section shows the logs on the CSC Multiplex GRE.

It is possible to view the current month and the last 6 months logs.



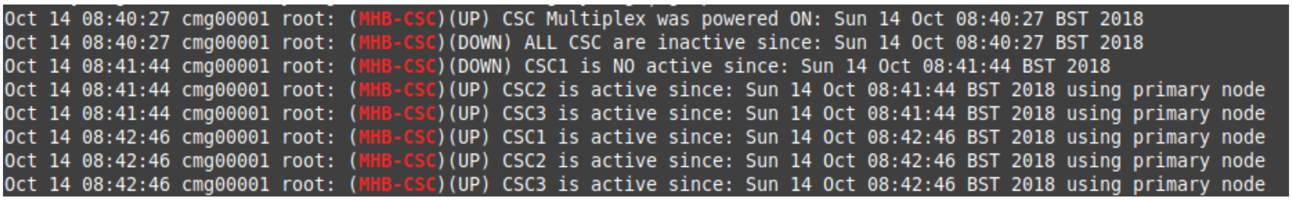
```
Log Information
10) View Current Month
11) View Last 6 Months
```



```
Oct 14 08:40:27 root: (MHB-CSC)(UP) CSC Multiplex was powered ON: Sun 14 Oct 08:40:27 BST 2018
Oct 14 08:40:27 root: (MHB-CSC)(DOWN) ALL CSC are inactive since: Sun 14 Oct 08:40:27 BST 2018
Oct 14 08:41:44 root: (MHB-CSC)(DOWN) CSC1 is NO active since: Sun 14 Oct 08:41:44 BST 2018
Oct 14 08:41:44 root: (MHB-CSC)(UP) CSC2 is active since: Sun 14 Oct 08:41:44 BST 2018 using primary node
Oct 14 08:41:44 root: (MHB-CSC)(UP) CSC3 is active since: Sun 14 Oct 08:41:44 BST 2018 using primary node
Oct 14 08:42:46 root: (MHB-CSC)(UP) CSC1 is active since: Sun 14 Oct 08:42:46 BST 2018 using primary node
Oct 14 08:42:46 root: (MHB-CSC)(UP) CSC2 is active since: Sun 14 Oct 08:42:46 BST 2018 using primary node
Oct 14 08:42:46 root: (MHB-CSC)(UP) CSC3 is active since: Sun 14 Oct 08:42:46 BST 2018 using primary node
```

9.4.1 SysLog Server information example:

This example show the initial Power On of a CSC Multiplex GRE .



```
Oct 14 08:40:27 cmg00001 root: (MHB-CSC)(UP) CSC Multiplex was powered ON: Sun 14 Oct 08:40:27 BST 2018
Oct 14 08:40:27 cmg00001 root: (MHB-CSC)(DOWN) ALL CSC are inactive since: Sun 14 Oct 08:40:27 BST 2018
Oct 14 08:41:44 cmg00001 root: (MHB-CSC)(DOWN) CSC1 is NO active since: Sun 14 Oct 08:41:44 BST 2018
Oct 14 08:41:44 cmg00001 root: (MHB-CSC)(UP) CSC2 is active since: Sun 14 Oct 08:41:44 BST 2018 using primary node
Oct 14 08:41:44 cmg00001 root: (MHB-CSC)(UP) CSC3 is active since: Sun 14 Oct 08:41:44 BST 2018 using primary node
Oct 14 08:42:46 cmg00001 root: (MHB-CSC)(UP) CSC1 is active since: Sun 14 Oct 08:42:46 BST 2018 using primary node
Oct 14 08:42:46 cmg00001 root: (MHB-CSC)(UP) CSC2 is active since: Sun 14 Oct 08:42:46 BST 2018 using primary node
Oct 14 08:42:46 cmg00001 root: (MHB-CSC)(UP) CSC3 is active since: Sun 14 Oct 08:42:46 BST 2018 using primary node
```

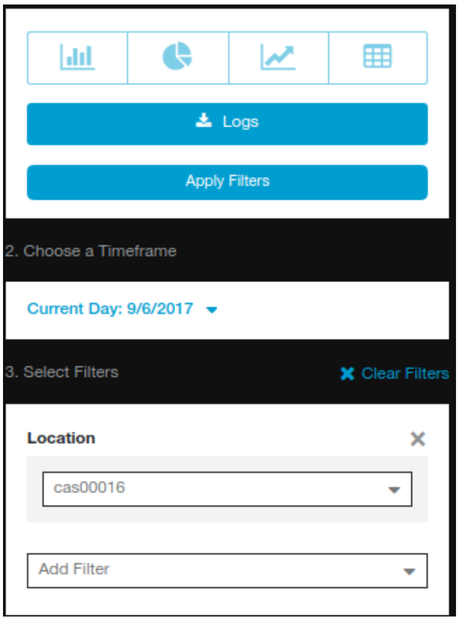
10 Checking full visibility of the transaction on the Zscaler GUI

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

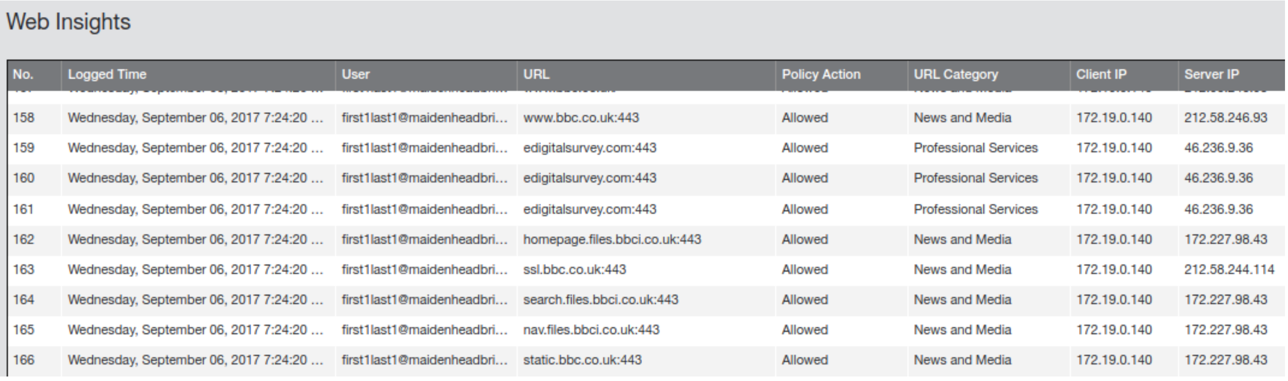
Click Logs and Filter by Location [cas00016 in this example is the name of the Location]



Current Day: 9/6/2017

Location: cas00016

Apply Filters:

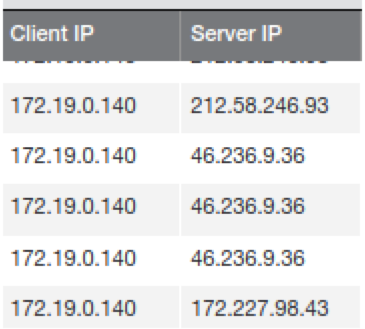


Web Insights

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:



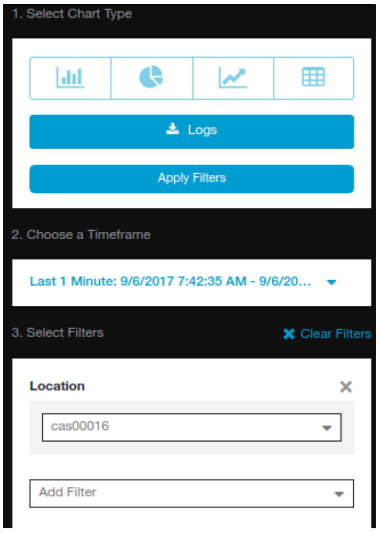
Client IP	Server IP
172.19.0.140	212.58.246.93
172.19.0.140	46.236.9.36
172.19.0.140	46.236.9.36
172.19.0.140	46.236.9.36
172.19.0.140	172.227.98.43

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

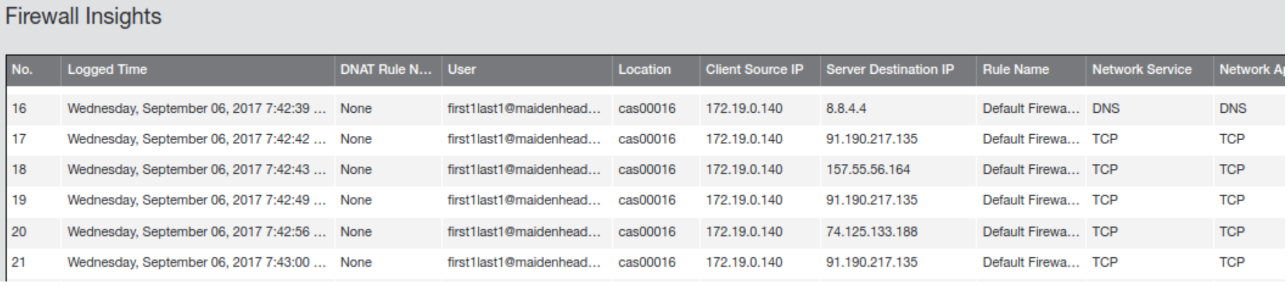
Click Logs and Filter by Location [cas00016 in this example is the name of the Location]



Last 1 Minute: 9/6/2017 7:42:35 AM - 9/6/20…

Location: cas00016

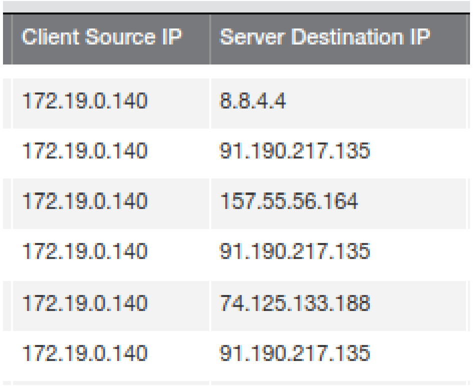
Apply Filters



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. ***GRE NAT and firewall rules in general. GRE is not TCP. GRE is a protocol like TCP (number 47). In order to do NAT you will probably required to do a STATIC SOURCE NAT and to allow protocol 47 in both directions.***
2. ***Are Vmware interfaces are properly mapped?***
3. ***Are the configuration values correct? Check all values again using “Configuration and Status” menu.***

11.2 Proxy Bypass

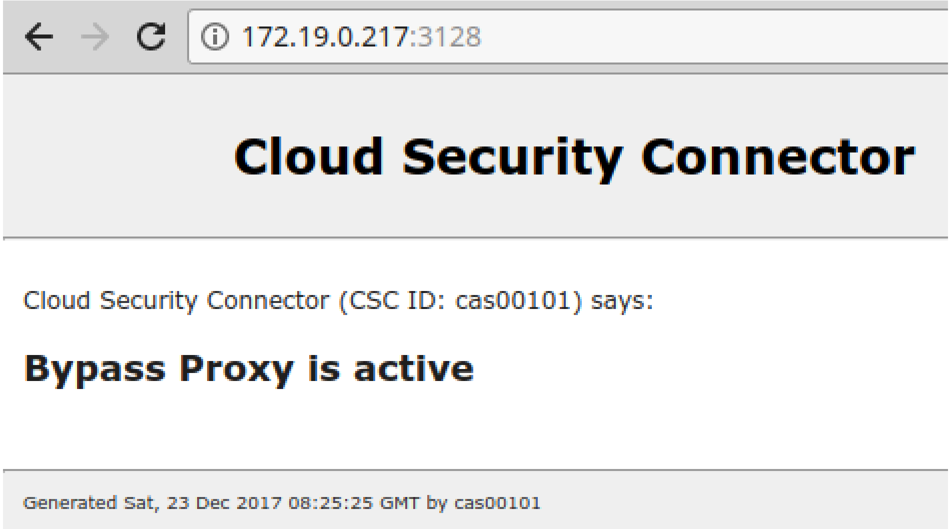
11.2.1 How to check if the Proxy Bypass is active?

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:



Cloud Security Connector

Cloud Security Connector (CSC ID: cas00101) says:

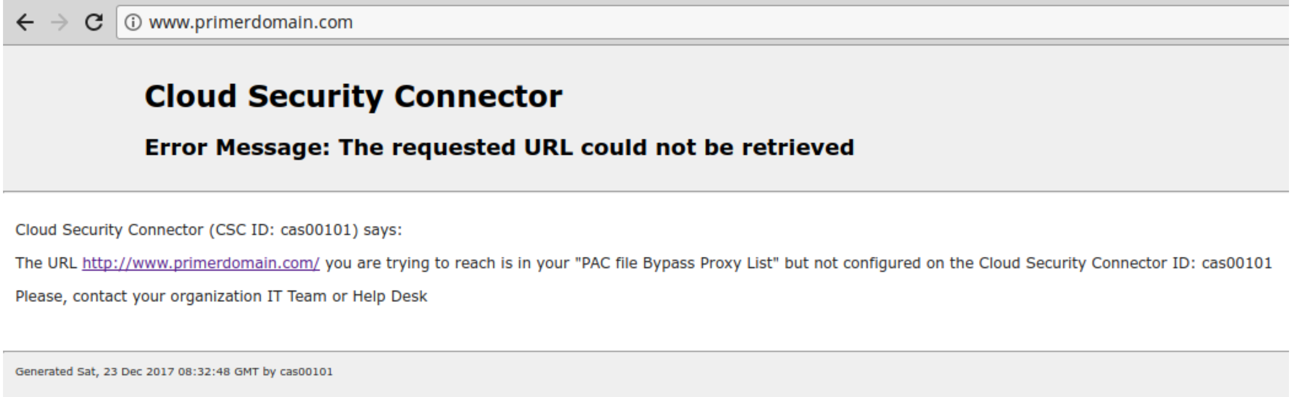
Bypass Proxy is active

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:



Cloud Security Connector

Error Message: The requested URL could not be retrieved

Cloud Security Connector (CSC ID: cas00101) says:

The URL http://www.primerdomain.com/ 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

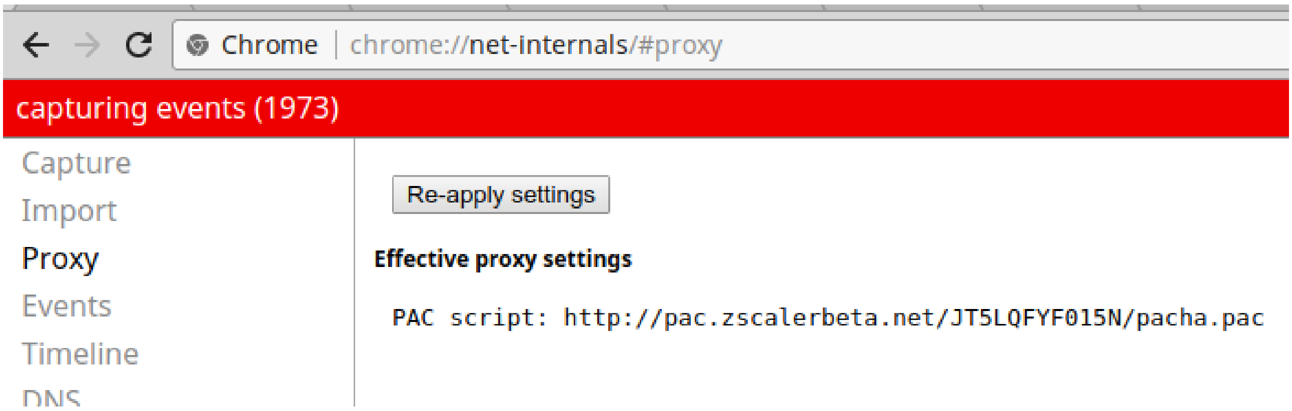
Please, for all this test use “Google Chrome”

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:



Effective proxy settings

```
PAC script: http://pac.zscalerbeta.net/JT5LQFYF015N/pacha.pac
```

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

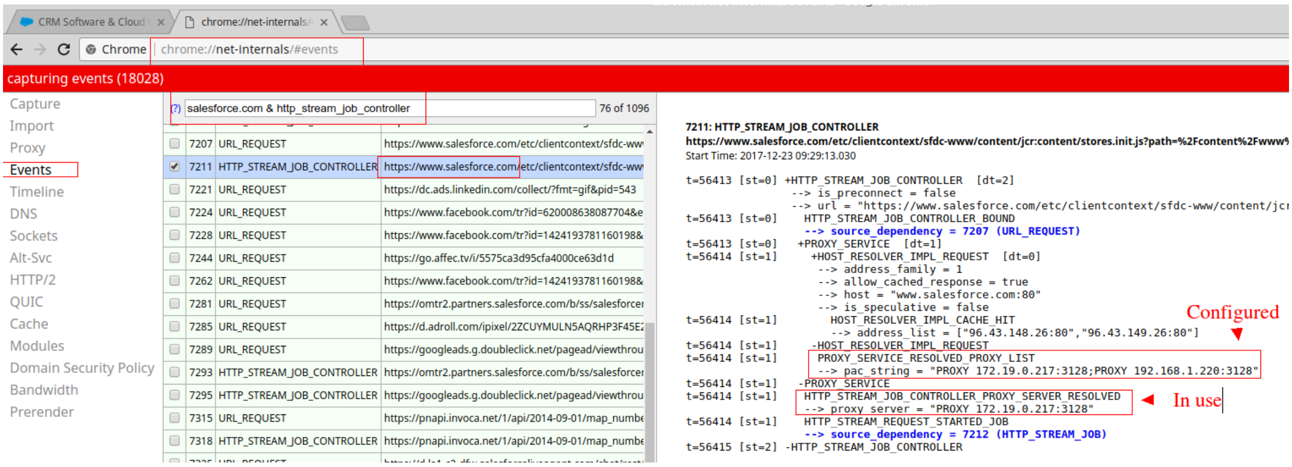
Using Google Chrome, do the following steps:

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")



☐	7207	URL_REQUEST	https://www.salesforce.com/etc/clientcontext/sfdc-ww
☑	7211	HTTP_STREAM_JOB_CONTROLLER	https://www.salesforce.com/etc/clientcontext/sfdc-ww
☐	7221	URL_REQUEST	https://dc.ads.linkedin.com/collect/?fmt=gif&pid=543
☐	7224	URL_REQUEST	https://www.facebook.com/tr?id=620008638087704&e
☐	7228	URL_REQUEST	https://www.facebook.com/tr?id=1424193781160198&
☐	7244	URL_REQUEST	https://go.affec.tv/i/5575ca3d95cfa4000ce63d1d
☐	7262	URL_REQUEST	https://www.facebook.com/tr?id=1424193781160198&
☐	7281	URL_REQUEST	https://omtr2.partners.salesforce.com/b/ss/salesforce
☐	7285	URL_REQUEST	https://d.adroll.com/ipixel/2ZCUYMULN5AQRHP3F45E
☐	7289	URL_REQUEST	https://googleads.g.doubleclick.net/pagead/viewthrou
☐	7293	HTTP_STREAM_JOB_CONTROLLER	https://omtr2.partners.salesforce.com/b/ss/salesforce
☐	7295	HTTP_STREAM_JOB_CONTROLLER	https://googleads.g.doubleclick.net/pagead/viewthrou
☐	7315	URL_REQUEST	https://pnapi.invoca.net/1/api/2014-09-01/map_numbe
☐	7318	HTTP_STREAM_JOB_CONTROLLER	https://pnapi.invoca.net/1/api/2014-09-01/map_numbe

7211: HTTP_STREAM_JOB_CONTROLLER
https://www.salesforce.com/etc/clientcontext/sfdc-www/content/jcr:content/stores.init.js?path=%2Fcontent%2Fwww
Start Time: 2017-12-23 09:29:13.030

```
t=56413 [st=0] +HTTP_STREAM_JOB_CONTROLLER  [dt=2]
                --> is_preconnect = false
                --> url = "https://www.salesforce.com/etc/clientcontext/sfdc-www/content/jc
t=56413 [st=0]    HTTP_STREAM_JOB_CONTROLLER_BOUND
                  --> source_dependency = 7207 (URL_REQUEST)
t=56413 [st=0]   +PROXY_SERVICE  [dt=1]
t=56414 [st=1]     +HOST_RESOLVER_IMPL_REQUEST  [dt=0]
                    --> address_family = 1
                    --> allow_cached_response = true
                    --> host = "www.salesforce.com:80"
                    --> is_speculative = false
t=56414 [st=1]        HOST_RESOLVER_IMPL_CACHE_HIT
                      --> address_list = ["96.43.148.26:80","96.43.149.26:80"]
t=56414 [st=1]     -HOST_RESOLVER_IMPL_REQUEST
t=56414 [st=1]      PROXY_SERVICE_RESOLVED_PROXY_LIST
                    --> pac_string = "PROXY 172.19.0.217:3128;PROXY 192.168.1.220:3128"
t=56414 [st=1]   -PROXY_SERVICE
t=56414 [st=1]    HTTP_STREAM_JOB_CONTROLLER_PROXY_SERVER_RESOLVED
                  --> proxy_server = "PROXY 172.19.0.217:3128"
t=56414 [st=1]    HTTP_STREAM_REQUEST_STARTED_JOB
                  --> source_dependency = 7212 (HTTP_STREAM_JOB)
t=56415 [st=2] -HTTP_STREAM_JOB_CONTROLLER
```

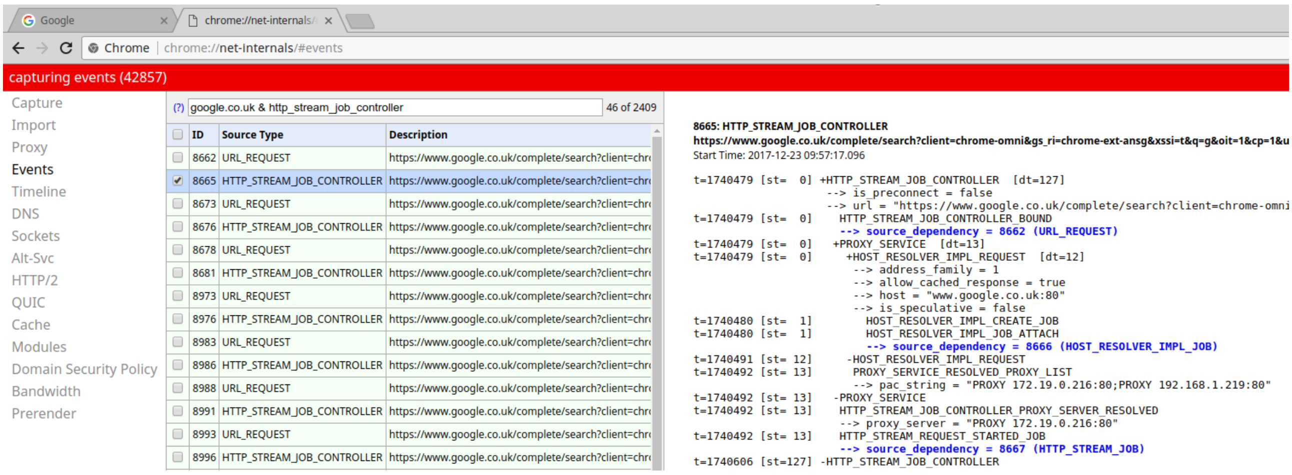
In this example, www.salesforce.com is using the Bypass proxy:

```
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”



☐	ID	Source Type	Description
☐	8662	URL_REQUEST	https://www.google.co.uk/complete/search?client=chr
☑	8665	HTTP_STREAM_JOB_CONTROLLER	https://www.google.co.uk/complete/search?client=chr
☐	8673	URL_REQUEST	https://www.google.co.uk/complete/search?client=chr
☐	8676	HTTP_STREAM_JOB_CONTROLLER	https://www.google.co.uk/complete/search?client=chr
☐	8678	URL_REQUEST	https://www.google.co.uk/complete/search?client=chr
☐	8681	HTTP_STREAM_JOB_CONTROLLER	https://www.google.co.uk/complete/search?client=chr
☐	8973	URL_REQUEST	https://www.google.co.uk/complete/search?client=chr
☐	8976	HTTP_STREAM_JOB_CONTROLLER	https://www.google.co.uk/complete/search?client=chr
☐	8983	URL_REQUEST	https://www.google.co.uk/complete/search?client=chr
☐	8986	HTTP_STREAM_JOB_CONTROLLER	https://www.google.co.uk/complete/search?client=chr
☐	8988	URL_REQUEST	https://www.google.co.uk/complete/search?client=chr
☐	8991	HTTP_STREAM_JOB_CONTROLLER	https://www.google.co.uk/complete/search?client=chr
☐	8993	URL_REQUEST	https://www.google.co.uk/complete/search?client=chr
☐	8996	HTTP_STREAM_JOB_CONTROLLER	https://www.google.co.uk/complete/search?client=chr

8665: HTTP_STREAM_JOB_CONTROLLER
https://www.google.co.uk/complete/search?client=chrome-omni&gs_ri=chrome-ext-ansg&xssi=t&q=g&oit=1&cp=1&u
Start Time: 2017-12-23 09:57:17.096

```
t=1740479 [st=  0] +HTTP_STREAM_JOB_CONTROLLER  [dt=127]
                    --> is_preconnect = false
                    --> url = "https://www.google.co.uk/complete/search?client=chrome-omni
t=1740479 [st=  0]    HTTP_STREAM_JOB_CONTROLLER_BOUND
                      --> source_dependency = 8662 (URL_REQUEST)
t=1740479 [st=  0]   +PROXY_SERVICE  [dt=13]
t=1740479 [st=  0]     +HOST_RESOLVER_IMPL_REQUEST  [dt=12]
                        --> address_family = 1
                        --> allow_cached_response = true
                        --> host = "www.google.co.uk:80"
                        --> is_speculative = false
t=1740480 [st=  1]        HOST_RESOLVER_IMPL_CREATE_JOB
t=1740480 [st=  1]        HOST_RESOLVER_IMPL_JOB_ATTACH
                          --> source_dependency = 8666 (HOST_RESOLVER_IMPL_JOB)
t=1740491 [st= 12]     -HOST_RESOLVER_IMPL_REQUEST
t=1740492 [st= 13]      PROXY_SERVICE_RESOLVED_PROXY_LIST
                        --> pac_string = "PROXY 172.19.0.216:80;PROXY 192.168.1.219:80"
t=1740492 [st= 13]   -PROXY_SERVICE
t=1740492 [st= 13]    HTTP_STREAM_JOB_CONTROLLER_PROXY_SERVER_RESOLVED
                      --> proxy_server = "PROXY 172.19.0.216:80"
t=1740492 [st= 13]    HTTP_STREAM_REQUEST_STARTED_JOB
                      --> source_dependency = 8667 (HTTP_STREAM_JOB)
t=1740606 [st=127] -HTTP_STREAM_JOB_CONTROLLER
```

In this case:

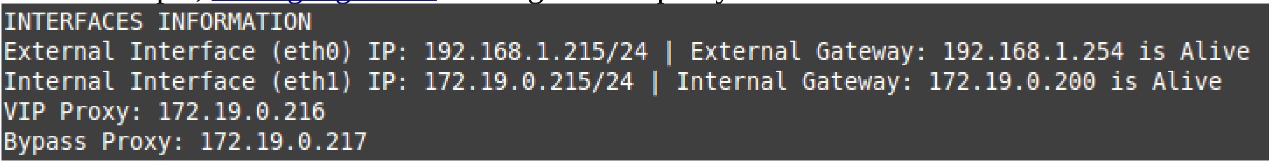
- PROXY_SERVICE_RESOLVED_PROXY_LIST

  --> 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, 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 – PAC File Example

Click here to obtain a PAC file example that will help to redirect traffic to Zscaler and to do Local Bypasses or Direct bypasses to Internet.

14 Appendix B – “Run Commands” from AWS to monitor the CSC

When you have your CSC registered on AWS as “managed instance” you can execute the “Monitoring Tasks” and also to “Update Bypass List”. This is particular important if you have several CSC and you want to update all in one task.

14.1 Documents

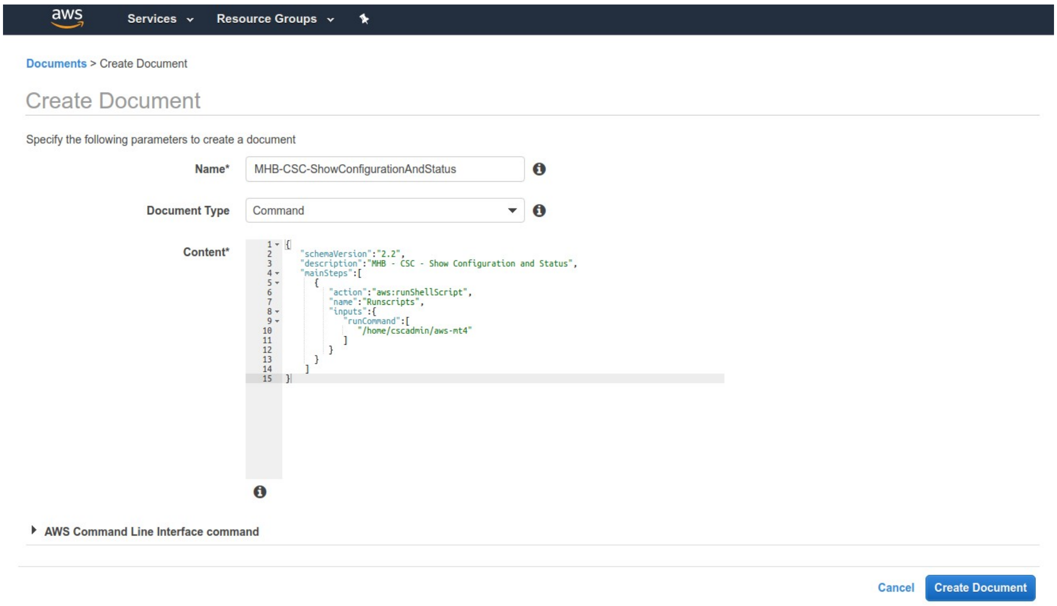
To execute “Run Commands” you need to have “Documents”. “Documents” contains a series of commands to execute. For simplicity purposes, we provide the “Documents” required for the operations of the CSC.

To obtain the Documents required you can open a ticket to http://support.maidenheadbridge.com (indicating your AWS Account ID) or to create them manually Copying/Pasting the information that follows.

14.1.1 Creating a Document

From EC2 Console > Systems Manager Shared Resources > Documents → Click “Create Document”

Put the “Name” , “Document Type” = Command and fill “Content”



Specify the following parameters to create a document

Name*: MHB-CSC-ShowConfigurationAndStatus

Document Type: Command

Content*

```
{
   "schemaVersion":"2.2",
   "description":"MHB - CSC - Show Configuration and Status",
   "mainSteps":[
      {
         "action":"aws:runShellScript",
         "name":"Runscripts",
         "inputs":{
            "runCommand":[
               "/home/cscadmin/aws-mt4"
            ]
         }
      }
   ]
}
```

Click “Create Document”

14.1.2 List of Documents

Please, create the “Documents” using this values:

Name	MHB-CSC-ShowConfigurationAndStatus
Content	

```
{
  "schemaVersion":"2.2",
  "description":"MHB - CSC - Show Configuration and Status",
  "mainSteps":[
    {
      "action":"aws:runShellScript",
      "name":"Runscripts",
      "inputs":{
        "runCommand":[
          "/home/cscadmin/aws-mt4"
        ]
      }
    }
   ]
}
```

Name	MHB-CSC-SpeedTest
Content	

```
{
  "schemaVersion":"2.2",
  "description":"MHB - CSC - Speed Test",
  "mainSteps":[
    {
      "action":"aws:runShellScript",
      "name":"Runscripts",
      "inputs":{
        "runCommand":[
          "/home/cscadmin/aws-mt7"
        ]
      }
    }
   ]
}
```

Name	MHB-CSC-TraceRouteAndLatencyTest

Content

```
{
  "schemaVersion":"2.2",
  "description":"MHB - CSC - TraceRoute and Latency Test",
  "mainSteps":[
    {
      "action":"aws:runShellScript",
      "name":"Runscripts",
      "inputs":{
        "runCommand":[
          "/home/cscadmin/aws-mt6"
        ]
      }
    }
  ]
}
```

Name	MHB-CSC-UpdateBypassList

Content

```
{
  "schemaVersion":"2.2",
  "description":"MHB - CSC - Update Bypass List",
  "mainSteps":[
    {
      "action":"aws:runShellScript",
      "name":"Runscripts",
      "inputs":{
        "runCommand":[
          "/home/cscadmin/aws-bp-refresh-list"
        ]
      }
    }
  ]
}
```

14.1.3 Run Commands

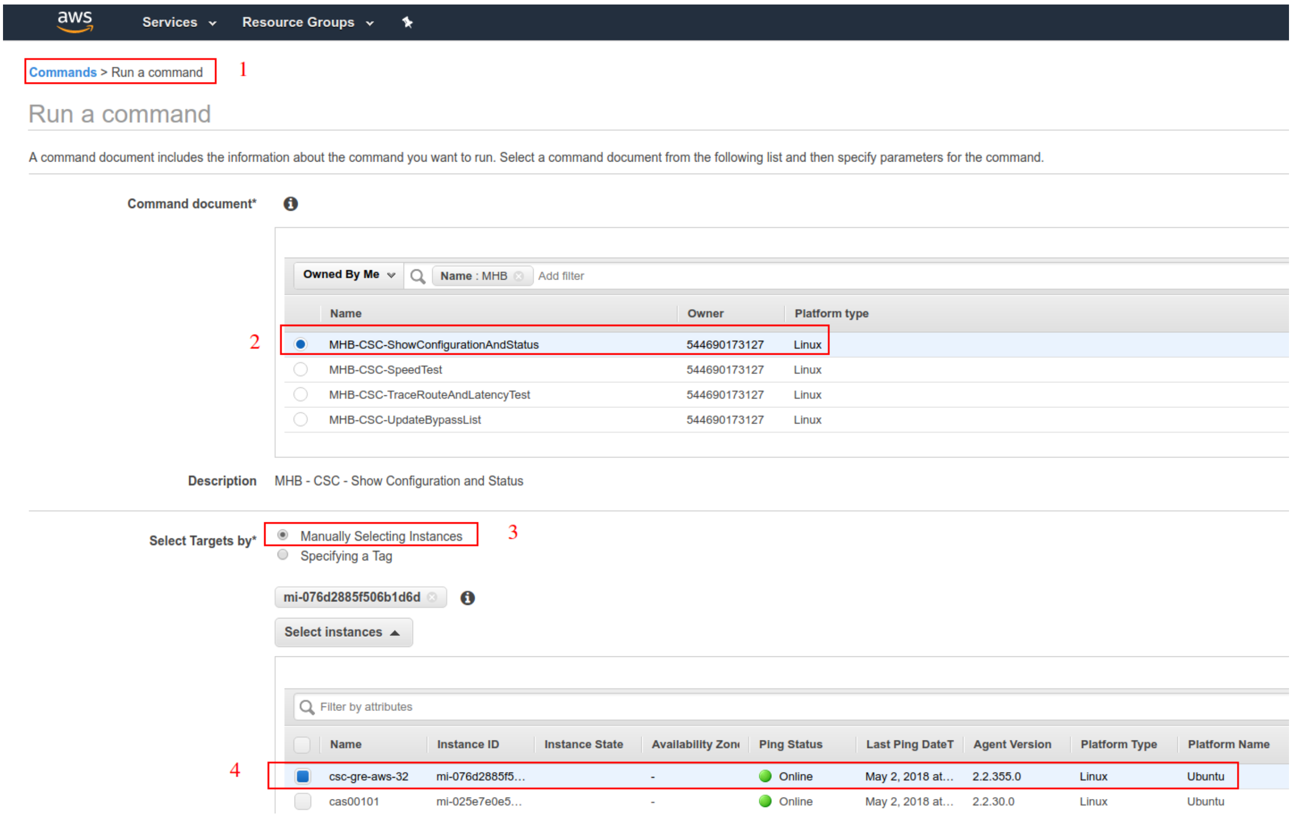
After you created the Documents, you are ready to Run Commands on the CSC.

You can see the results of the operation on the “Output” section or to store the results on a S3 Buckets for further inspection.

> *Note: The “Output” Section allows only 2500 characters. The Traceroute and Latency Test uses more than 2500. We recommend to store this command on a S3 bucket directly.*

To Run Commands go to: Systems Manager Services > Run Command

Here an example of Running: MHB-CSC-ShowConfigurationAndStatus



Commands > Run a command

Run a command

A command document includes the information about the command you want to run. Select a command document from the following list and then specify parameters for the command.

Command document*

	Name	Owner	Platform type
●	MHB-CSC-ShowConfigurationAndStatus	544690173127	Linux
○	MHB-CSC-SpeedTest	544690173127	Linux
○	MHB-CSC-TraceRouteAndLatencyTest	544690173127	Linux
○	MHB-CSC-UpdateBypassList	544690173127	Linux

Description MHB - CSC - Show Configuration and Status

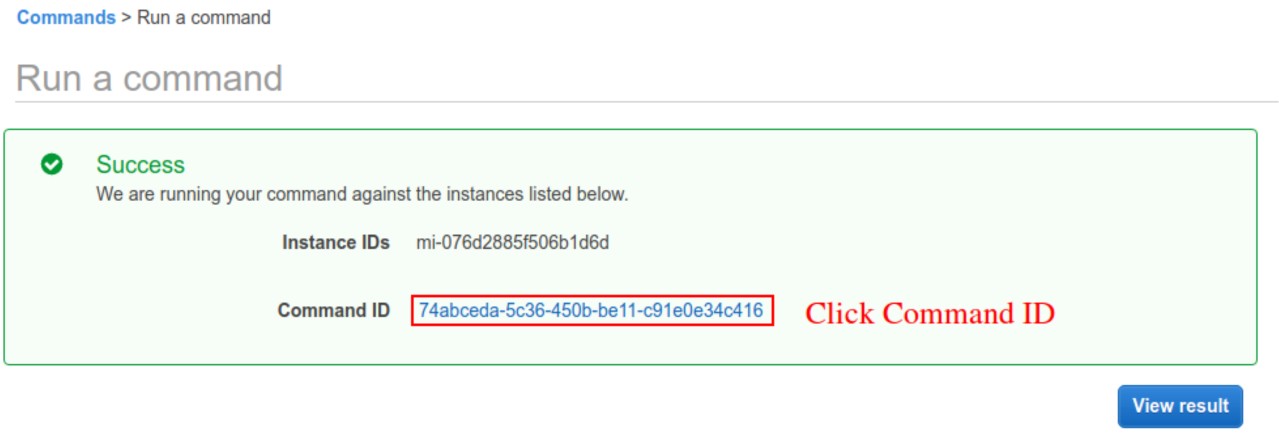
Select Targets by*
● Manually Selecting Instances
○ Specifying a Tag

mi-076d2885f506b1d6d

	Name	Instance ID	Instance State	Availability Zone	Ping Status	Last Ping DateT	Agent Version	Platform Type	Platform Name
☑	csc-gre-aws-32	mi-076d2885f5…		-	Online	May 2, 2018 at…	2.2.355.0	Linux	Ubuntu
☐	cas00101	mi-025e7e0e5…		-	Online	May 2, 2018 at…	2.2.30.0	Linux	Ubuntu

1. Run a Command
2. Select the Document created
3. Select the Instances
4. We are selecting only one instance, but you can select as much as you want.
5. Click Run

Next Screen is:



Commands > Run a command

Run a command

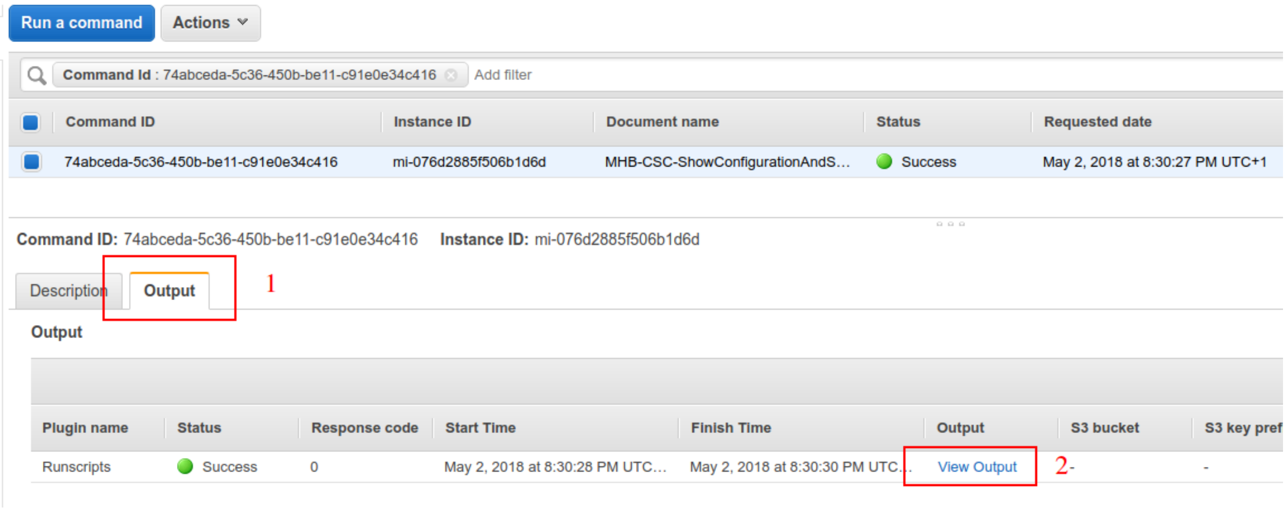
Success
We are running your command against the instances listed below.

Instance IDs mi-076d2885f506b1d6d

Command ID 74abceda-5c36-450b-be11-c91e0e34c416

Click Command ID

Click “Command ID”



Command Id : 74abceda-5c36-450b-be11-c91e0e34c416

☐	Command ID	Instance ID	Document name	Status	Requested date
☐	74abceda-5c36-450b-be11-c91e0e34c416	mi-076d2885f506b1d6d	MHB-CSC-ShowConfigurationAndS…	● Success	May 2, 2018 at 8:30:27 PM UTC+1

Command ID: 74abceda-5c36-450b-be11-c91e0e34c416 **Instance ID:** mi-076d2885f506b1d6d

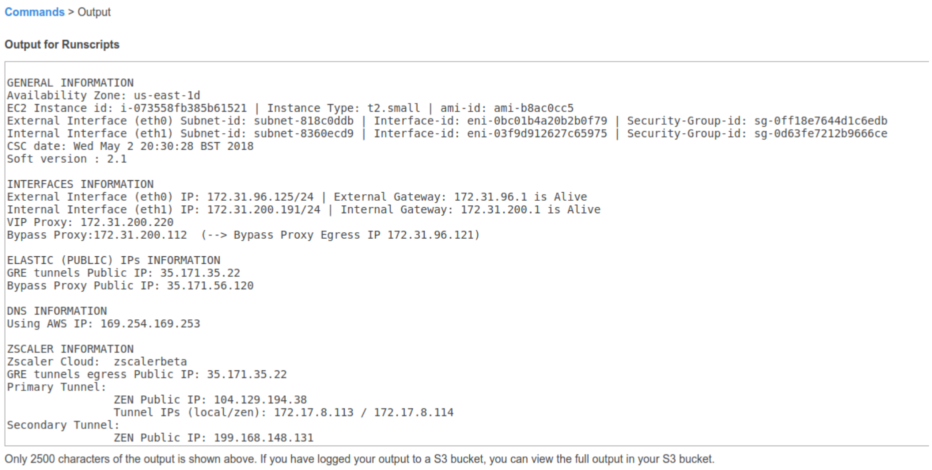
Output

Output

Plugin name	Status	Response code	Start Time	Finish Time	Output	S3 bucket	S3 key pref
Runscripts	● Success	0	May 2, 2018 at 8:30:28 PM UTC…	May 2, 2018 at 8:30:30 PM UTC…	View Output		-

1. Select “Output”
2. Click “View Output”

and you will be able to see the result of the Run Command:



Commands > Output

Output for Runscripts

```
GENERAL INFORMATION
Availability Zone: us-east-1d
EC2 Instance id: i-073558fb385b61521 | Instance Type: t2.small | ami-id: ami-b8ac0cc5
External Interface (eth0) Subnet-id: subnet-818c0ddb | Interface-id: eni-0bc01b4a20b2b0f79 | Security-Group-id: sg-0ff18e7644d1c6edb
Internal Interface (eth1) Subnet-id: subnet-8360ecd9 | Interface-id: eni-03f9d912627c65975 | Security-Group-id: sg-0d63fe7212b9666ce
CSC date: Wed May 2 20:30:28 BST 2018
Soft version : 2.1

INTERFACES INFORMATION
External Interface (eth0) IP: 172.31.96.125/24 | External Gateway: 172.31.96.1 is Alive
Internal Interface (eth1) IP: 172.31.200.191/24 | Internal Gateway: 172.31.200.1 is Alive
VIP Proxy: 172.31.200.220
Bypass Proxy:172.31.200.112  (--> Bypass Proxy Egress IP 172.31.96.121)

ELASTIC (PUBLIC) IPs INFORMATION
GRE tunnels Public IP: 35.171.35.22
Bypass Proxy Public IP: 35.171.56.120

DNS INFORMATION
Using AWS IP: 169.254.169.253

ZSCALER INFORMATION
Zscaler Cloud:  zscalerbeta
GRE tunnels egress Public IP: 35.171.35.22
Primary Tunnel:
                ZEN Public IP: 104.129.194.38
                Tunnel IPs (local/zen): 172.17.8.113 / 172.17.8.114
Secondary Tunnel:
                ZEN Public IP: 199.168.148.131
```

Only 2500 characters of the output is shown above. If you have logged your output to a S3 bucket, you can view the full output in your S3 bucket.