Maidenhead Bridge

CSC GRE and Checkpoint FW

Enabling GRE tunnels to Zscaler for Checkpoint Customers

Configuration Guide – V 1.1

Table of Contents

1 Introduction....3
2 Network Diagram....3
3 CSC-GRE IP addressing....4
4 Traffic Flow, Ports and Protocol....5
4.1 Internal Side....5
4.2 External Side....5
5 Practical example:....6
5.1 Step 1: Configuring “Hosts” and “NAT” for local IPs....6
5.1.1 External Cluster IP....7
5.1.2 Egress Bypass IP....8
5.1.3 Csc-gre-a External Interface....9
5.1.4 Csc-gre-b External Interface....10
5.2 Step 2: Configuring “Hosts” for external IPs....11
5.2.1 Primary Zscaler Node (ZEN)....11
5.2.2 Secondary Zscaler Node (ZEN)....11
5.2.3 Google DNS 1....12
5.2.4 Google DNS 2....12
5.3 Step 3: Configuring “Policy” rules....13
5.3.1 Policy Rules explained:....14
6 Verifying that everything works....15
6.1 Cluster Active status....15
6.2 Cluster Stand By Status....16
7 Next Steps....17

1 Introduction

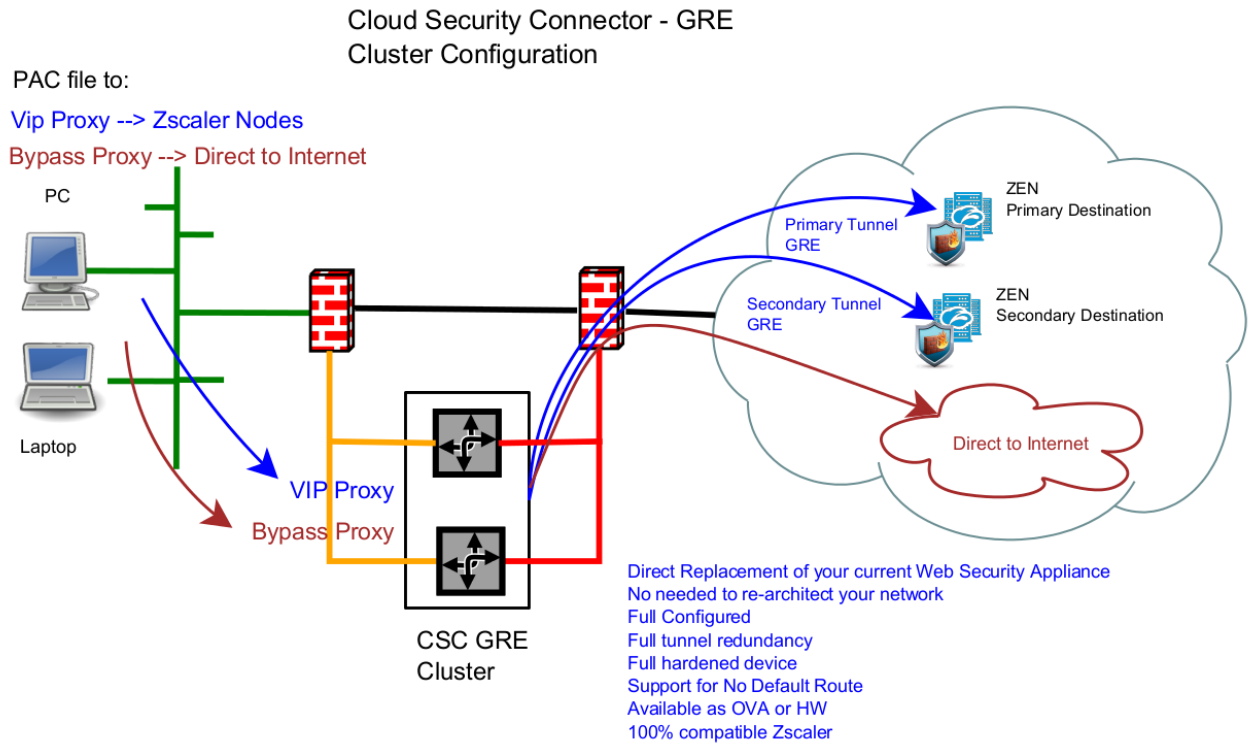
Checkpoint Firewalls are a clear market leader at the moment of writing this document and will remain for some time in the future.

When connecting companies with Checkpoint Firewall to Zscaler there is no way to provide redundancy and/or scalability up to 1 Gbps.

With the Cloud Security Connector – GRE you can solve this problem very easily. This Configuration Guide shows the Firewall rules required to achieve connectivity up to 1 Gbps to Zscaler with full local and remote redundancy.

2 Network Diagram

This is a typical scenario of a CSC GRE cluster behind firewalls:

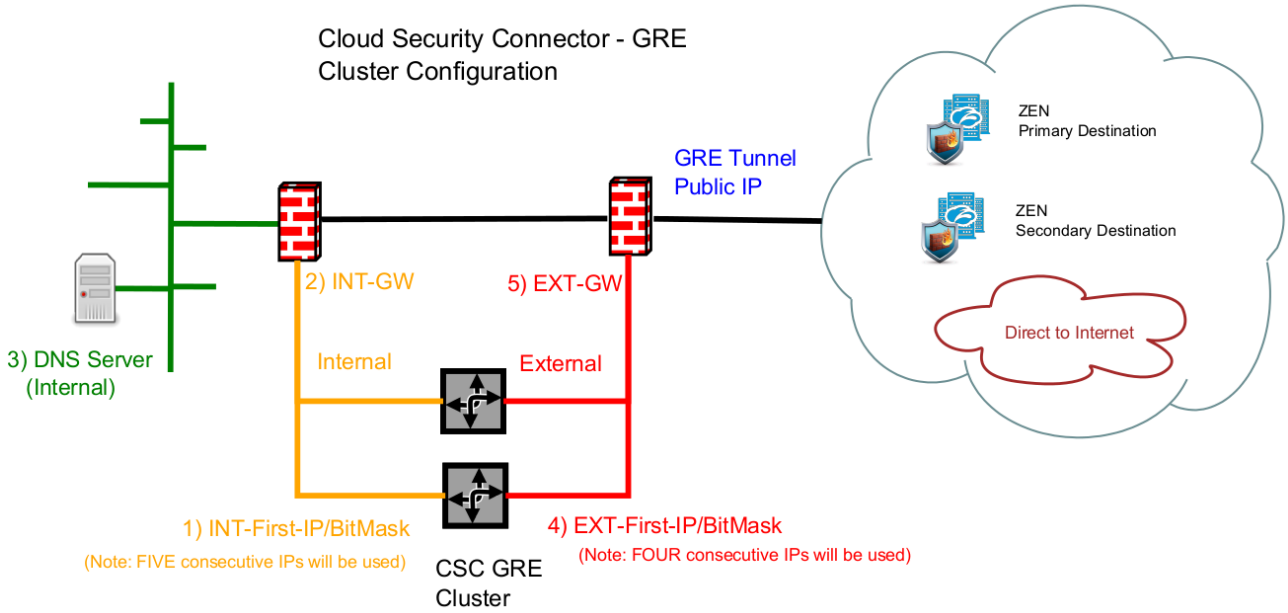


This network diagram shows the VIP proxy (traffic to Zscaler) and Bypass Proxy (traffic to internet directly) on the internal side.

On the external side we can see the GRE tunnels to Zscaler nodes and the traffic direct to internet via the proxy bypass.

3 CSC-GRE IP addressing

This diagram shows the information required when creating the CSC GRE.



Internal interface:

On the internal side the CSC GRE Cluster requires 5 IPs. We ask for the first one and the system will assign the other four. This is the order assigned to each IP (from first to fifth)

1. Internal Cluster IP
2. VIP proxy
3. Bypass Proxy
4. csc-gre-a Internal Interface
5. csc-gre-b Internal Interface

External Interface:

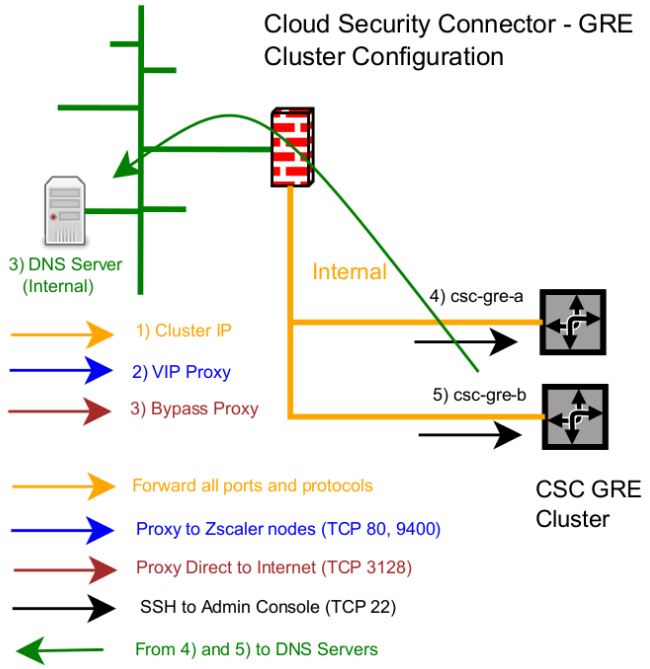
On the external side the CSC GRE Cluster requires 4 IPs. We ask for the first one and the system will assign the other three. This is the order assigned to each IP (from first to fourtth)

1. External Cluster IP
2. Egress Bypass IP
3. csc-gre-a External Interface
4. csc-gre-b External Interface

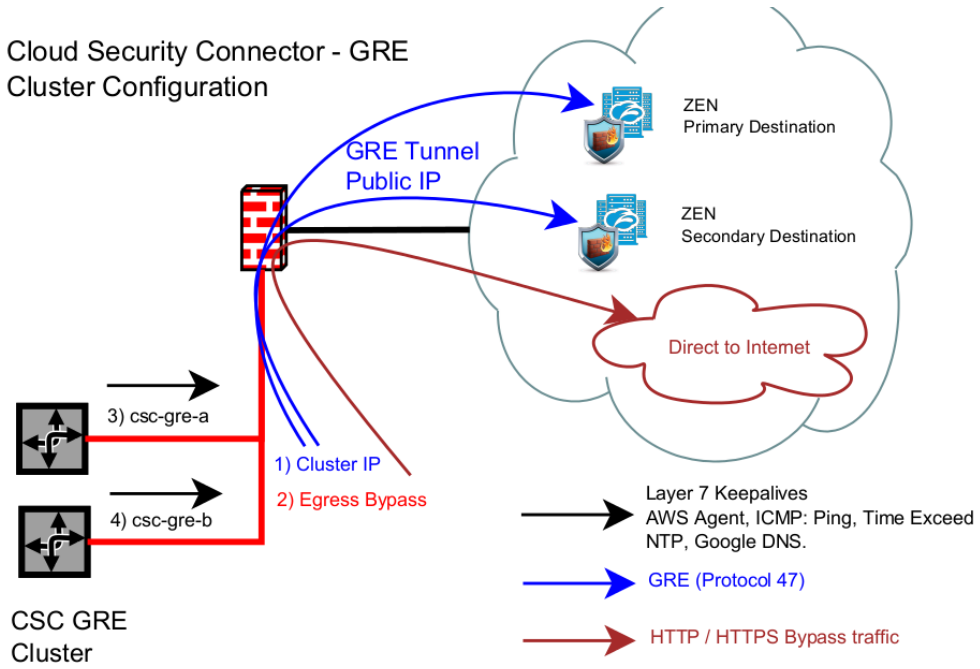
4 Traffic Flow, Ports and Protocol

4.1 Internal Side

The following graph shows the traffic on the internal side of the CSC:



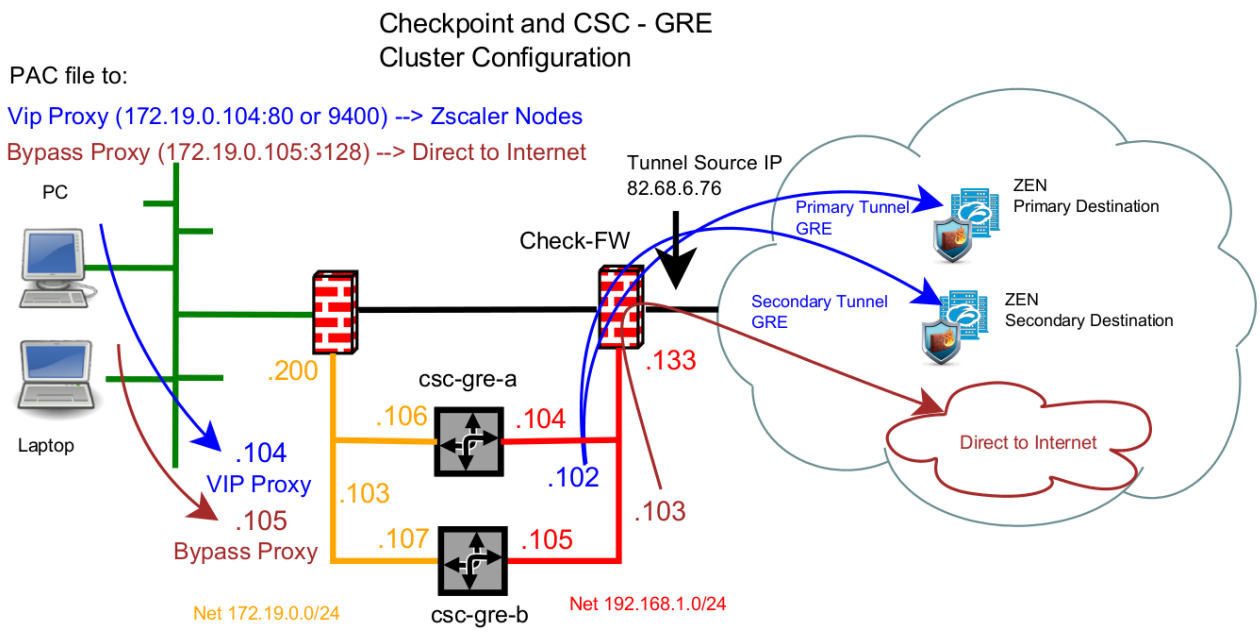
4.2 External Side



5 Practical example:

We are going to show how to configure Checkpoint Rules with a practical example. We are going to put focus on the EXTERNAL side.

This is the IP addressing of our example:



All the information required for Firewall Rules can be taken from the "Configuration and Status" menu of the CSCs GRE.

Here a detail of the information required:

```
INTERFACES INFORMATION
External Interface (eth0) IP: 192.168.1.105/24 | External Cluster IP: 192.168.1.102 | External Gateway: 192.168.1.133 is Alive
Internal Interface (eth1) IP: 172.19.0.107/24 | Internal Cluster IP: 172.19.0.103 | Internal Gateway: 172.19.0.200 is Alive
VIP Proxy: 172.19.0.104
Bypass Proxy:172.19.0.105  (--> Bypass Proxy Egress IP 192.168.1.103)

DNS INFORMATION
DNS Server (1) IP: 172.19.0.21 is Not reachable (ping failure)
DNS Server (2) IP: 172.19.0.22 is Not reachable (ping failure)
Google DNS 1: 8.8.8.8 is Alive
Google DNS 2: 8.8.4.4 is Alive

ZSCALER INFORMATION
Zscaler Cloud:  zscalerbeta
GRE tunnels egress Public IP: 82.68.6.76
Primary Tunnel:
                ZEN Public IP: 165.225.72.38
                Tunnel IPs (local/zen): 172.17.7.57 / 172.17.7.58
Secondary Tunnel:
                ZEN Public IP: 104.129.194.38
                Tunnel IPs (local/zen): 172.17.7.61 / 172.17.7.62
```

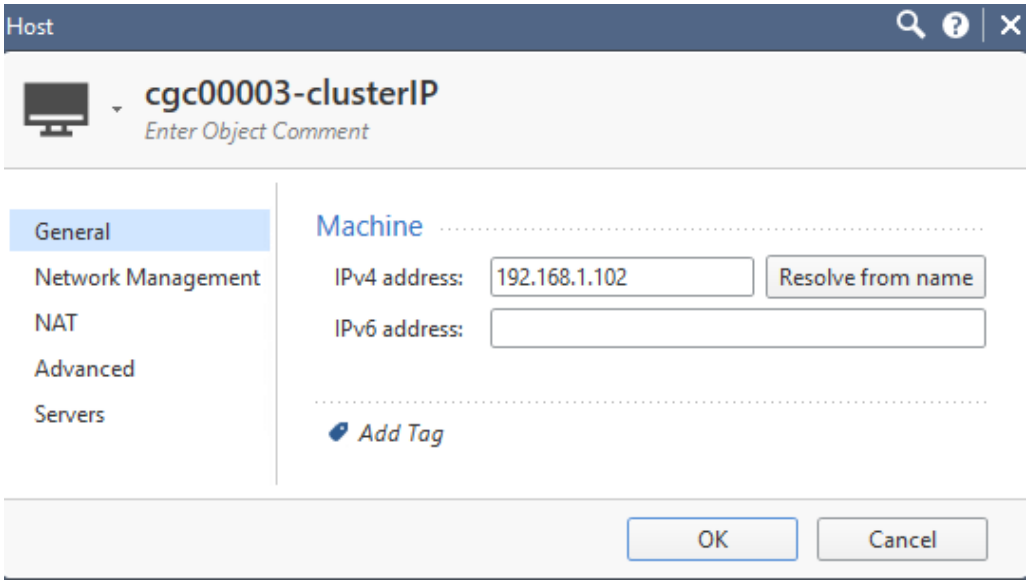
5.1 Step 1: Configuring "Hosts" and "NAT" for local IPs

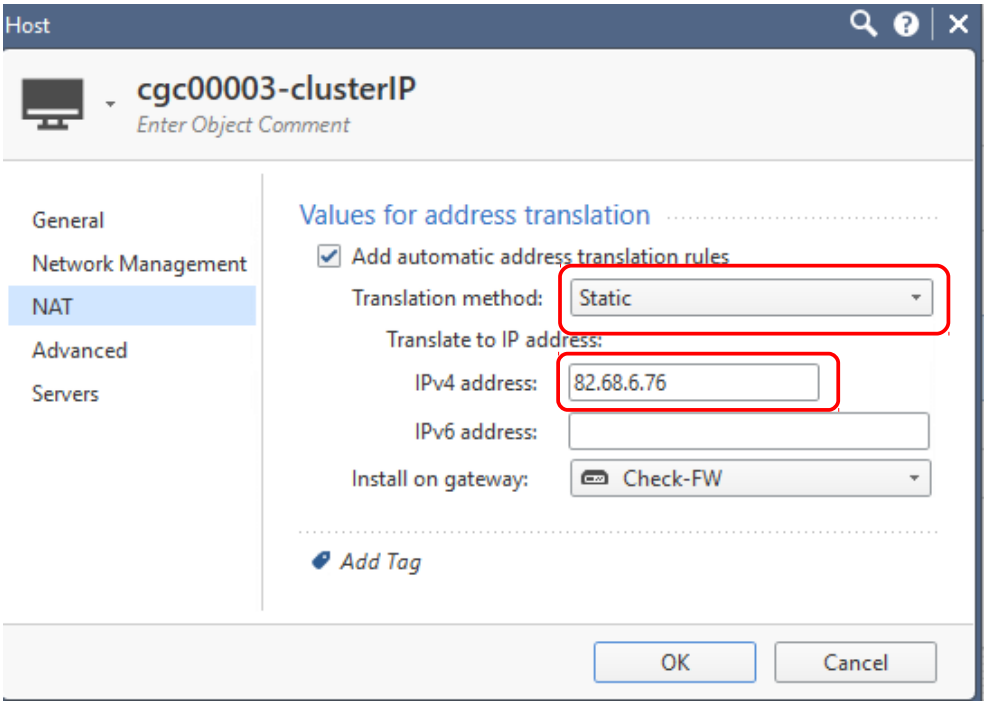
For each object with light green square in the previous image, we need to create a "Host" on the Checkpoint console. For each of this Hosts we need to create a NAT rule. The public IP for the NAT

rule in this example is 82.68.6.76 (called “GRE tunnels egress Public IP” on the Configuration and Status Menu).

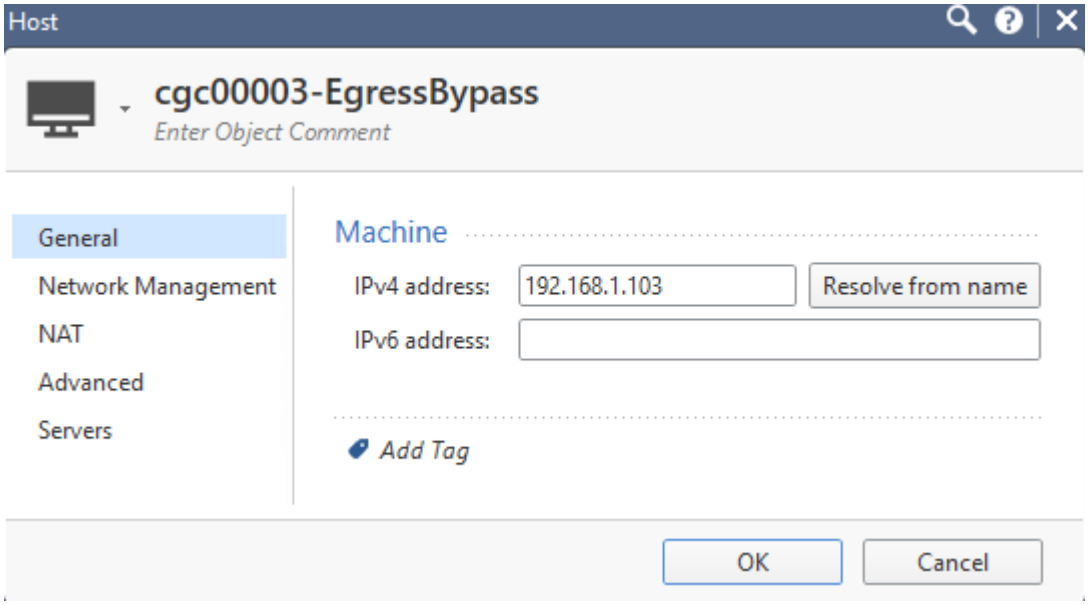
5.1.1 External Cluster IP

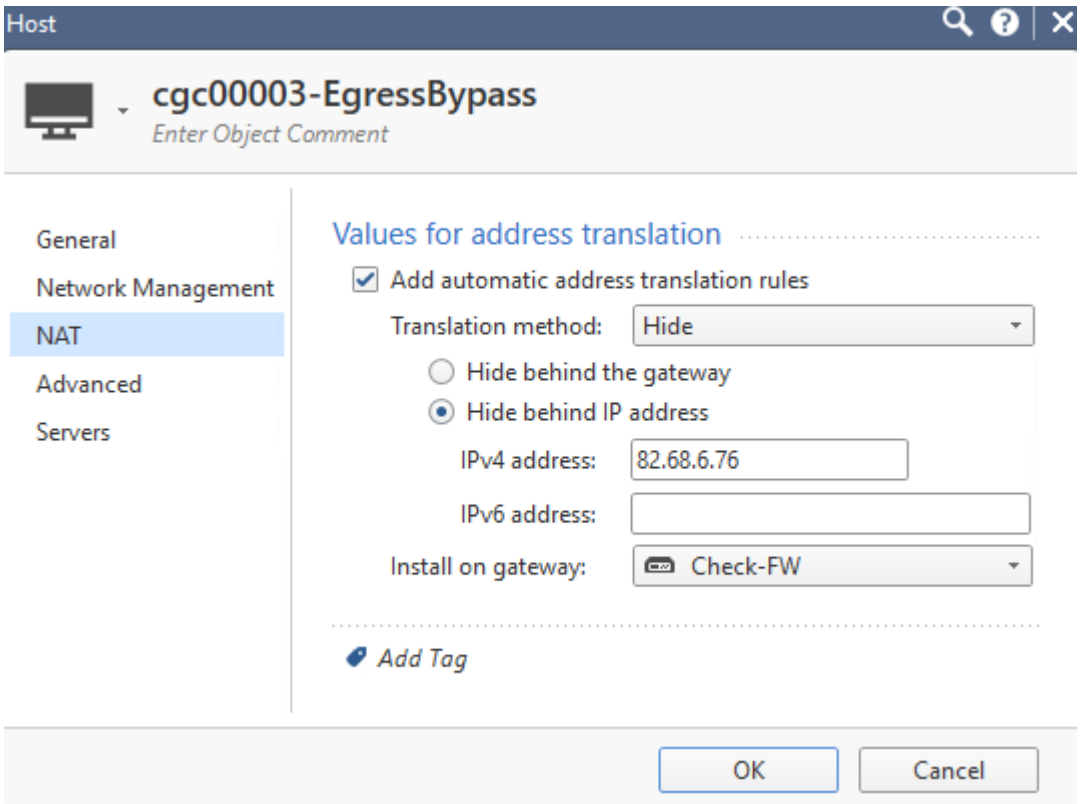
IMPORTANT: Please note that the GRE Tunnels are initiated from this IP and the NAT in this case must be STATIC (only in this case). Also, the “External Cluster IP” is the only one IP that is mandatory to NAT using the “GRE tunnels egress Public IP” in order to match with the Zscaler Location IP. Others local ips can be nated using other public IPs if you want.



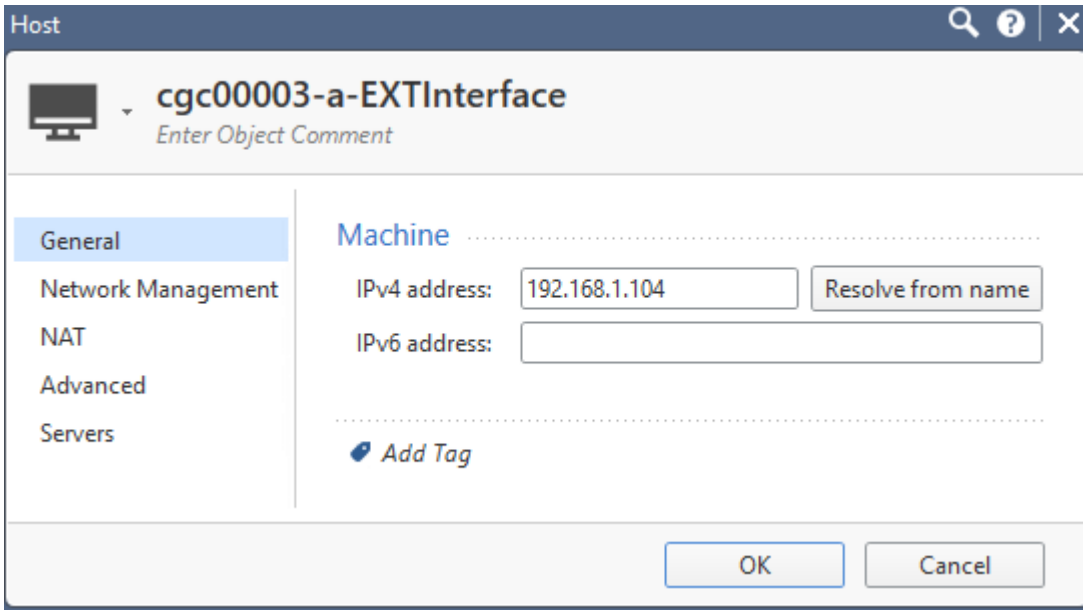


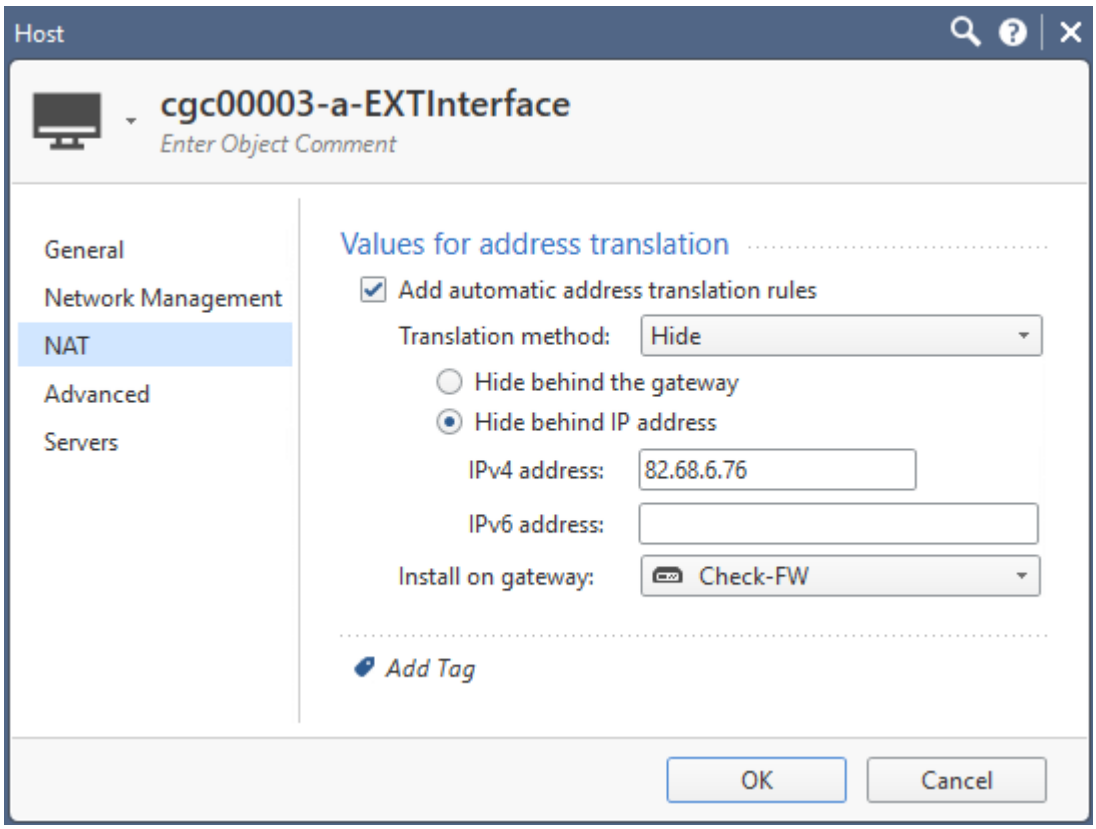
5.1.2 Egress Bypass IP



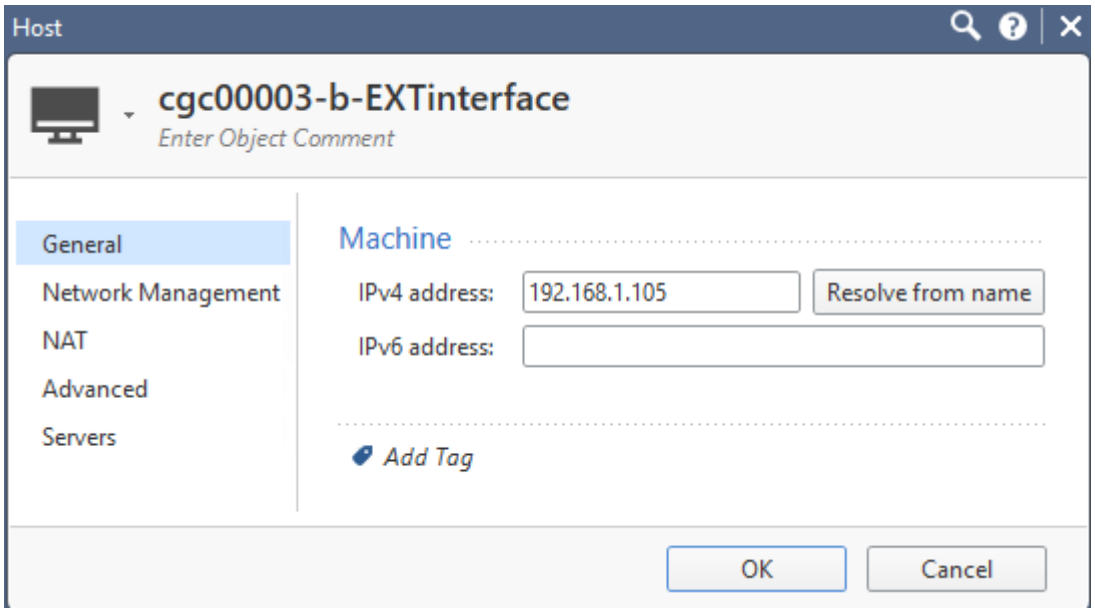


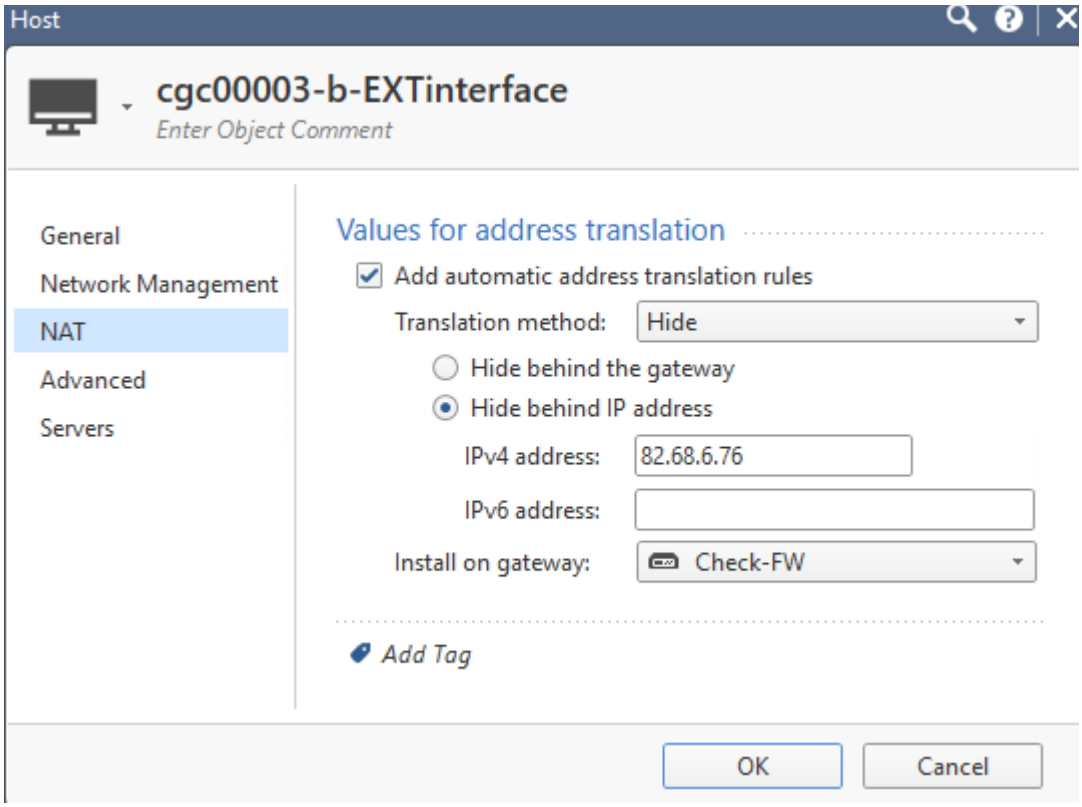
5.1.3 Csc-gre-a External Interface





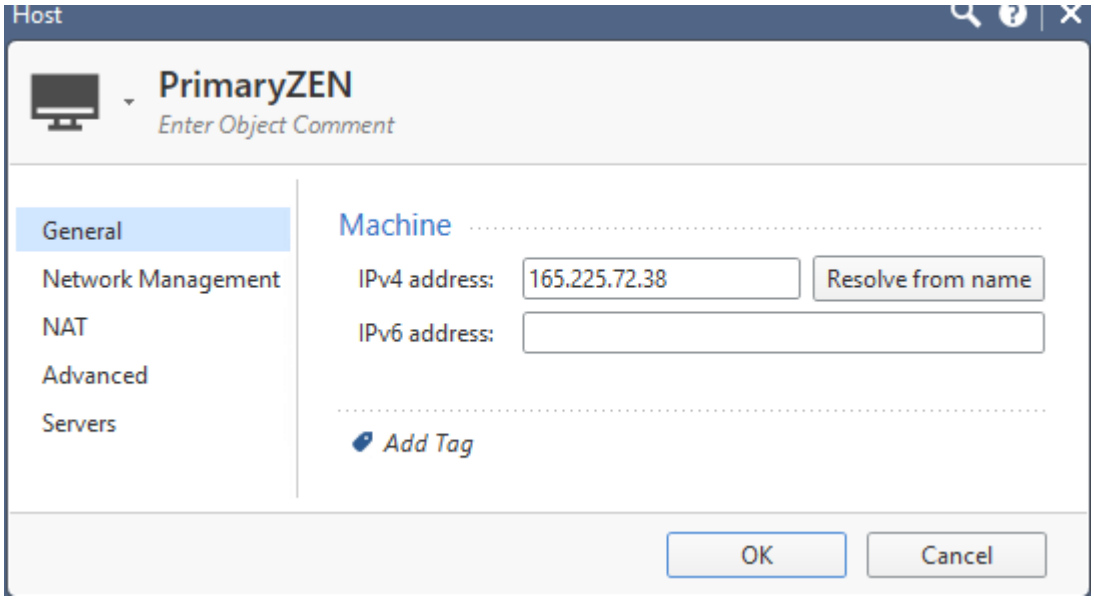
5.1.4 Csc-gre-b External Interface



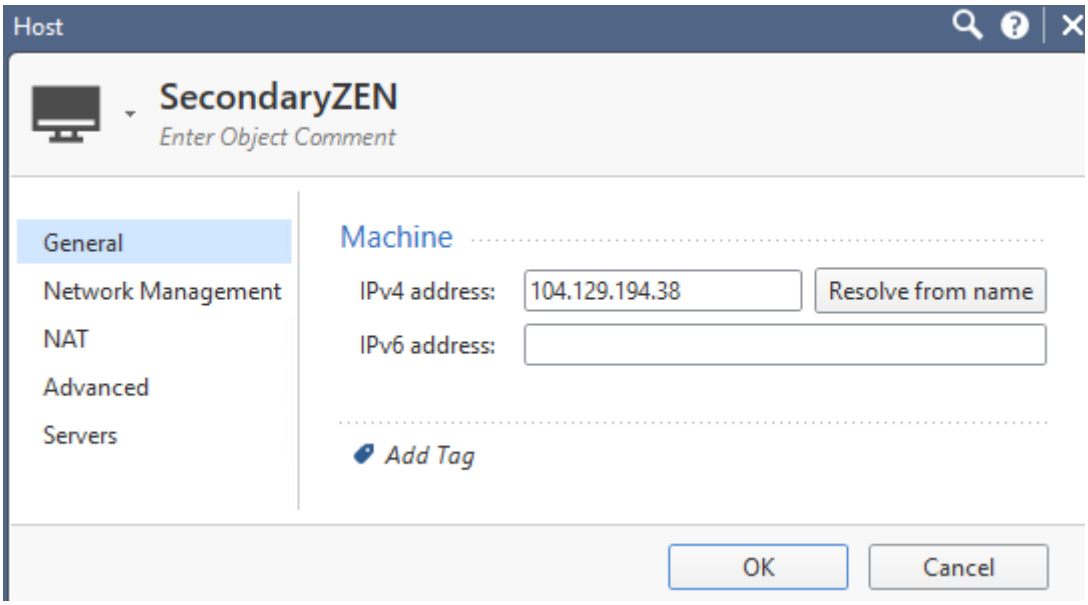


5.2 Step 2: Configuring “Hosts” for external IPs

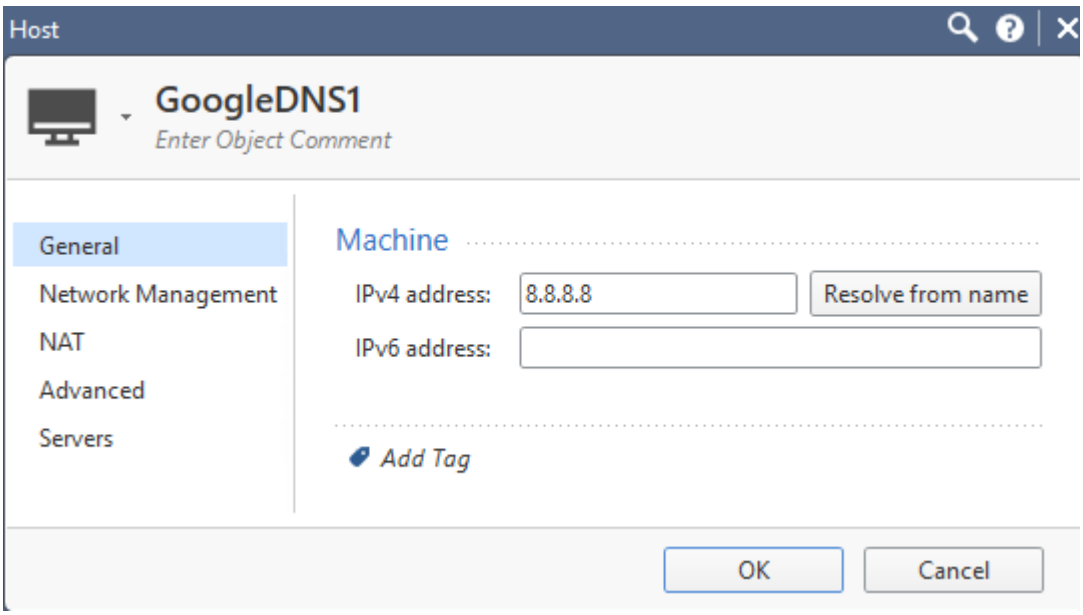
5.2.1 Primary Zscaler Node (ZEN)



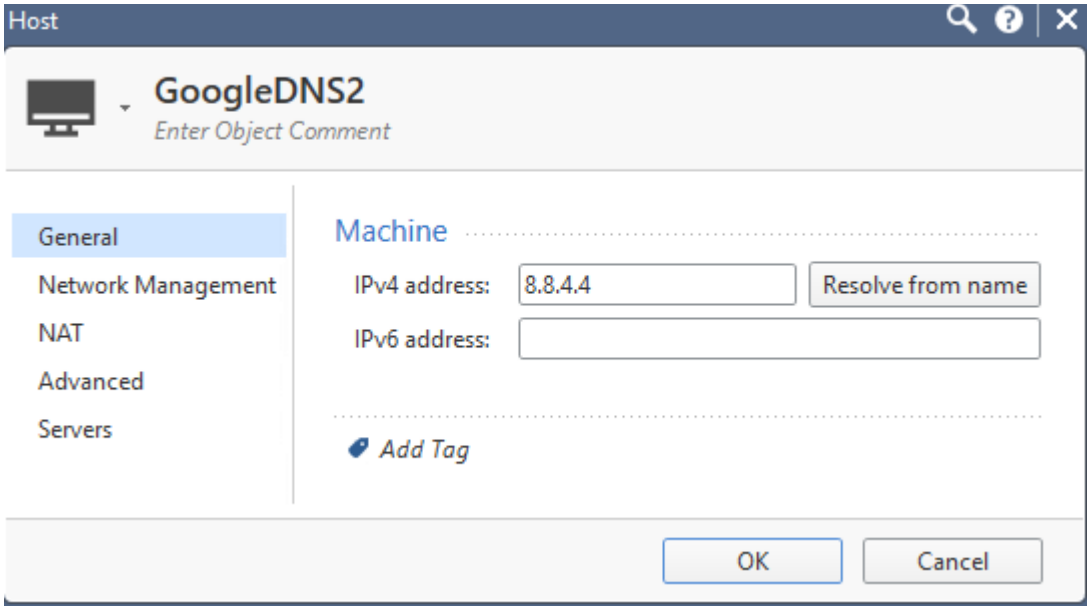
5.2.2 Secondary Zscaler Node (ZEN)



5.2.3 Google DNS 1



5.2.4 Google DNS 2



5.3 Step 3: Configuring “Policy” rules

No.	Name	Source	Destination	VPN	Services & Applications	Action
1	CSC Cluster IP	cgc00003-clusterIP	PrimaryZEN SecondaryZEN	Any	gre	Accept
2	CSC External Interfaces	cgc00003-b-EXTinterface cgc00003-a-EXTInterface	PrimaryZEN SecondaryZEN GoogleDNS1 GoogleDNS2	Any	http dns	Accept
3	CSC Egress Bypass	cgc00003-EgressBypass	Any	Any	https http HTTP_proxy tcp-high-ports	Accept
4	CSC AWS Agent (https), PAC Bypass (http)	cgc00003-a-EXTInterface cgc00003-b-EXTinterface	Any	Any	https http	Accept
5	MyTraceroute Direct	cgc00003-a-EXTInterface cgc00003-b-EXTinterface	Any	Any	echo-request	Accept
6	MyTraceroute Reverse	Any	cgc00003-a-EXTInterface cgc00003-b-EXTinterface	Any	time-exceeded echo-reply	Accept
7	NTP Direct	cgc00003-a-EXTInterface cgc00003-b-EXTinterface	Any	Any	ntp	Accept

5.3.1 Policy Rules explained:

Rule #	Name	Purpose
1	CSC Cluster IP	GRE tunnels from External Cluster IP to Primary ZEN and Secondary ZEN
2	CSC External Interfaces	Layer 7 Keepalives (HTTP) and DNS to Google from External interfaces of the CSCs
3	CSC Egress Bypass	Bypassed traffic from Egress Bypass IPs. Mandatory: HTTP and HTTPS Optional (but recommended): TCP High Ports
4	CSC AWS Agent PAC Bypass	Management from AWS (https) To reach Zscaler PAC file servers (http)
5	MyTraceRoute Direct	MyTraceRoute test
6	MyTraceRoute Direct	Idem before.
7	NTP	Network Time Protocol

6 Verifying that everything works

In order to check that everything work, go to the CSC, menu “Configuration and Status” on both CSCs: Cluster Active and Stand by. The values remarked are affected by the FW Rules created.

6.1 Cluster Active status

```
GENERAL INFORMATION
Company : Maidenhead Bridge
Location : Student60
CSC ID : cgc00003-b
CSC date: Wed 14 Feb 15:53:48 GMT 2018
Soft version : 2.1

INTERFACES INFORMATION
External Interface (eth0) IP: 192.168.1.105/24 | External Cluster IP: 192.168.1.102 | External Gateway: 192.168.1.133 is Alive
Internal Interface (eth1) IP: 172.19.0.107/24 | Internal Cluster IP: 172.19.0.103 | Internal Gateway: 172.19.0.200 is Alive
VIP Proxy: 172.19.0.104
Bypass Proxy:172.19.0.105  (--> Bypass Proxy Egress IP 192.168.1.103)

DNS INFORMATION
DNS Server (1) IP: 172.19.0.21 is Not reachable (ping failure)
DNS Server (2) IP: 172.19.0.22 is Not reachable (ping failure)
Google DNS 1: 8.8.8.8 is Alive
Google DNS 2: 8.8.4.4 is Alive        1

ZSCALER INFORMATION
Zscaler Cloud:  zscalerbeta
GRE tunnels egress Public IP: 82.68.6.76
Primary Tunnel:
                ZEN Public IP: 165.225.72.38
                Tunnel IPs (local/zen): 172.17.7.57 / 172.17.7.58
Secondary Tunnel:
                ZEN Public IP: 104.129.194.38
                Tunnel IPs (local/zen): 172.17.7.61 / 172.17.7.62

TUNNEL STATUS
Primary Tunnel (reachability):
                              Layer 7 Keepalive is: Alive
                              GRE ZEN Tunnel IP is: Alive        2
Secondary Tunnel (reachability):
                              Layer 7 Keepalive is: Alive
                              GRE ZEN Tunnel IP is: Alive        3

Tunnel Status: Primary tunnel is active since: Wed 14 Feb 05:48:20 GMT 2018        4

HTTP://IP.ZSCALER.COM PAGE STATUS
You are accessing this host via a Zscaler BETA proxy hosted at Frankfurt IV in the zscalerbeta.net cloud.        5
Your Gateway IP Address is 82.68.6.76

BYPASS PROXY - EGRESS INTERFACE STATUS
Bypass Proxy Egress Interface 192.168.1.103 can reach test page (http://pac.zscalerbeta.net)        6

CLUSTER STATUS
This CSC (cgc00003-b) is Cluster ACTIVE

AWS SSM AGENT
AWS SSM Agent is active (running) since Wed 2018-02-14 08:45:16 GMT; 7h ago        7
Registration values: {"ManagedInstanceID":"mi-0553bc37d2002047e","Region":"eu-west-1"}
```

Most of the tests are self explained, but here the detail:

1. Google DNS 1 and 2 are reachable.
2. Primary Tunnel Keepalive and GRE ZEN tunnel IP are alive
3. SecondaryTunnel Keepalive and GRE ZEN tunnel IP are alive
4. Primary Tunnel is active since:….
5. ip.zscaler.com page is reachable and shows the correct public IP

6. Bypass Proxy Egress IP can reach the Internet using the test page pac.<yourcloudname>.net
7. AWS SSM Agent can reach AWS Cloud. (if AWS agent was activated)

6.2 Cluster Stand By Status

Please, note that some tests are not performed here due to this is the stand by CSC.

```
GENERAL INFORMATION
Company : Maidenhead Bridge
Location : Student60
CSC ID : cgc00003-a
CSC date: Thu 15 Feb 07:10:49 GMT 2018
Soft version : 2.1

INTERFACES INFORMATION
External Interface (eth0) IP: 192.168.1.104/24 | External Cluster IP: 192.168.1.102 | External Gateway: 192.168.1.133 is Alive
Internal Interface (eth1) IP: 172.19.0.106/24 | Internal Cluster IP: 172.19.0.103 | Internal Gateway: 172.19.0.200 is Alive
VIP Proxy: 172.19.0.104
Bypass Proxy:172.19.0.105  (--> Bypass Proxy Egress IP 192.168.1.103)

DNS INFORMATION
DNS Server (1) IP: 172.19.0.21 is Not reachable (ping failure)
DNS Server (2) IP: 172.19.0.22 is Not reachable (ping failure)
Google DNS 1: 8.8.8.8 is Alive
Google DNS 2: 8.8.4.4 is Alive

ZSCALER INFORMATION
Zscaler Cloud:  zscalerbeta
GRE tunnels egress Public IP: 82.68.6.76
Primary Tunnel:
                ZEN Public IP: 165.225.72.38
                Tunnel IPs (local/zen): 172.17.7.57 / 172.17.7.58
Secondary Tunnel:
                ZEN Public IP: 104.129.194.38
                Tunnel IPs (local/zen): 172.17.7.61 / 172.17.7.62

TUNNEL STATUS
Primary Tunnel (reachability):
                              Layer 7 Keepalive is: Alive
                              GRE ZEN Tunnel IP is: Standby - This CSC (cgc00003-a) is Cluster Standby
Secondary Tunnel (reachability):
                              Layer 7 Keepalive is: Alive
                              GRE ZEN Tunnel IP is: Standby - This CSC (cgc00003-a) is Cluster Standby

Tunnel Status: No active tunnel since: Wed 14 Feb 06:39:51 GMT 2018

HTTP://IP.ZSCALER.COM PAGE STATUS
No test performed - This CSC (cgc00003-a) is Cluster Standby

BYPASS PROXY - EGRESS INTERFACE STATUS
No test performed - This CSC (cgc00003-a) is Cluster Standby

CLUSTER STATUS
This CSC (cgc00003-a) is Cluster STANDBY

AWS SSM AGENT
AWS SSM Agent is active (running) since Wed 2018-02-14 08:43:45 GMT; 22h ago
Registration values: {"ManagedInstanceID":"mi-043f6379dbab5a799","Region":"eu-west-1"}
```

Important: Note that the values remarked are leaving direct from the CSC interface when the CSC is Stand By.

1. Google DNS 1 and 2 are Alive.
2. Primary Tunnel Layer 7 keepalive is Alive.
3. Secondary Tunnel Layer 7 keepalive is Alive.
4. AWS SSM Agent can reach AWS Cloud (if AWS agent was activated).

7 Next Steps

If all test passed, the next step is to create the PAC file, to configure the bypasses and to start passing traffic through the CSC. Please, refer to the CSC Administration Guide for more details if needed. (Go to http://support.maidenheadbridge.com to obtain it)