Making the most of a single IPv4 address

By default each project is permitted a single *public* IPv4 address due to the world-wide shortage of IPv4 addresses but it is possible to work around this limitation. Projects do not have a quota for a floating IP initially, but can request one as laid out in the Requesting, Allocating and Associating Floating IPs section in our Guide.

Below we lay out the ability to create and use a proxy instance to route your traffic to different instances using a single IPv4 address.

Proxy instance

If offering a public service such as a web application is required, setting up a proxy host instance will permit inbound traffic directed at the public IPv4 address to be redirected to an appropriate instance based on the port number requested. For example, all traffic for port 80 will be directed to an instance running apache and ports 2200 can be set up to forward ssh traffic to the internal instance allowing terminal access.

The following is a tutorial that will step through building a proxy instance and an internal web server. For comprehensive steps, refer also to the Basic Guide

1. Create a security group for the proxy instance. The security group will need to allow access to the instance itself, and ports that are to be forwarded to internal groups. Name the group **Proxy**:

```
Rule: Custom TCP Rule:
Open Port: Port
Port: 22
Remote: CIDR
CIDR: 0.0.0.0/0


Rule: Custom TCP Rule:
Open Port: Port
Port: 2200
Remote: CIDR
CIDR: 0.0.0.0/0


Rule: Custom TCP Rule:
Open Port: Port
Port: 80
Remote: CIDR
CIDR: 0.0.0.0/0
```

2. Create a security group for the internal instances named **Internal**:

```
Rule: Custom TCP Rule:
Open Port: Port Range
From Port: 1
To Port: 65535
Remote: Security Group
Security Group: Proxy
```

3. Launch the proxy instance:

   Image: Ubuntu 18.04
   Flavor: m1.tiny
   Security groups: default, Proxy
   Key pair: pre-generated

   The proxy instance must be provisioned from the Ubuntu 18.04 image, as it contains pre-built scripts that enable proxy functionality.

   We suggest adding the default security group to both instances as the default group has egress rules that permit outbound access to the wide world you normally expect. If you do not wish to use the default security group, you will need to add the egress rules. Please Networking#EgressRulesandSecurityGroups for instructions.

4. Launch internal instance:

Image: Ubuntu 18.04
Flavor: m1.small
Security Groups: default, Internal
Key pair: pre-generated

5. Allocate and associate a floating IP to the proxy instance.
6. Log-in to the proxy instance.
7. Add the following lines to `/etc/rac-iptables.sh` to permit network address translation (NAT) forwarding to the internal instance. You must be root to modify `rac-iptables.sh`:

```
iptables -t nat -A PREROUTING -p tcp --dport 2200 -j DNAT --to-destination
<private_ip_internal_instance>:22
iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination <private_ip_internal_instance>:
80
```

8. Run `/usr/local/bin/proxyServer` to enable IP forwarding, enable the rules added in step 7 to run at boot.

   If you receive an error about rc.local not existing run the following snippet:

```
cat <<EOF | tee /etc/rc.local
bash /etc/rac-iptables.sh
exit 0
EOF
```

9. If you have not already, load these rules immediately by running:

```
sudo /etc/rac-iptables.sh
```

10. Log-in to the internal instance via the proxy instance. Make sure you specify port 2200, else you will only ssh to the proxy:

```
 $ ssh -p 2200 -i /path/to/<private_key> ubuntu@<floating_ip>
```

11. Install apache on the internal instance:

```
$ sudo apt-get update && sudo apt-get install -y apache2
```

You can now browse to the default apache page using the floating IP address. Just as the ssh session is forwarded to the internal instance via the rules specified in step 7 above, the browser will connect to port 80 on the proxy instance and be forwarded to port 80 of the internal instance.

Using this framework, you can build as many instances as allowed by your Rapid Access Cloud project and need only a single floating IP. What's more, some measure of security is gained, as the Security Group rule created in step 2 means access to internal instances is allowed only from the proxy instance.

RAC VPN

Alternatively, you can use the Rapid Access Cloud VPN to access your instances without requiring a public IPv4 address.