

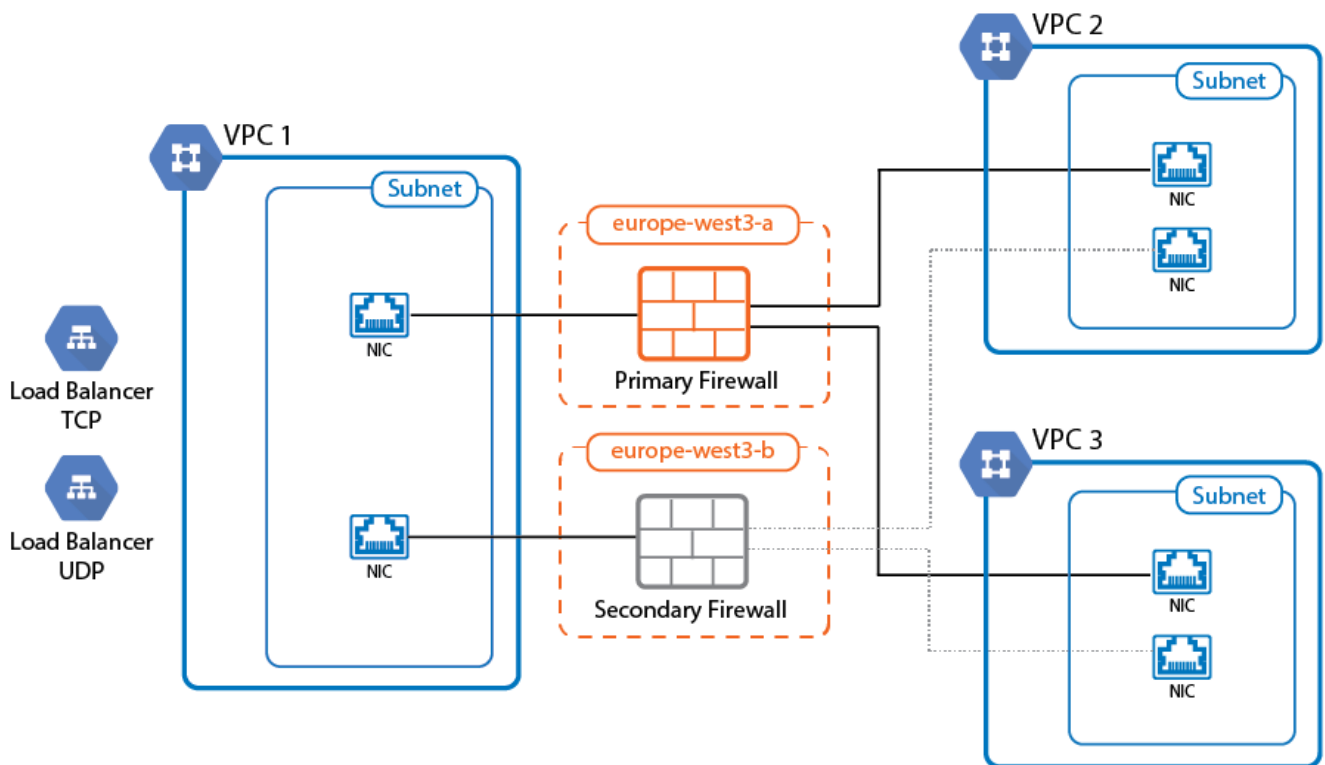
How to Configure a High Availability Cluster in Google Cloud

<https://campus.barracuda.com/doc/73007965/>

Running your NextGen Firewall in a High Availability cluster in the Google Cloud ensures that even in the event of a datacenter failure in the cloud the other firewall can take over and your applications will remain reachable. All VPC networks must be in the same region; however, the two firewall instances are deployed into two different zones inside this region. The firewall instances are configured with one network interface per VPC network. Routing table in the VPC networks are configured to use the firewall as the target for traffic to the Internet and to other VPC networks. This allows the firewall to act both as the default gateway for Internet-bound traffic and as a segmentation firewall to VPC-to-VPC traffic. The number of network interfaces is determined by the number of CPU cores of the selected instance types. For example: for three VPCs, you need an instance with 3 CPU cores or more.

To rewrite the routes using the firewall as the target, a script must be placed in the `/opt/phion/hooks/ha/` directory of each firewall. The script is executed every time the virtual server fails over and rewrites the routes to use the active firewall as the target.

To use the High Availability cluster with a single public IP address, add a TCP and/or UDP Google Network Load balancer. To use the load balancer, there must be a service on port 80 or 433 running on or behind the firewall because the Google legacy health check only allows HTTP and HTTPS health checks. Use the SSL VPN service or the Cloud landing page. Alternatively, it is also possible to probe a web service behind the firewall, but an outage of the web service would result in the firewall to be considered unhealthy.



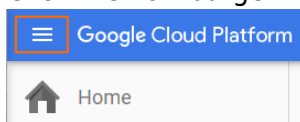
Before You Begin

- Download the Google Cloud Image from the Barracuda Networks Download Portal: <https://dlportal.barracudanetworks.com>.
- Create a custom service account and role for the High Availability cluster. For more information, see [How to Create a Custom Role and Service Account for the NextGen Firewall in the Google Cloud](#).
- Download the Google Cloud Takeover script needed for Step 18: [gcp-ha-takeover.sh](https://github.com/barracuda-networks/gcp-ha-takeover.sh)

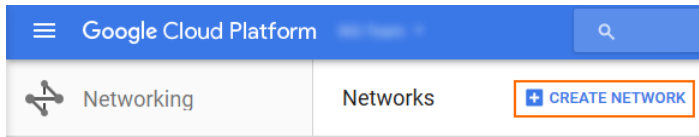
Step 1. Create the Hub VPC Network

Create the virtual private network where the two firewall instances will be running. Create a subnet for the firewall instances.

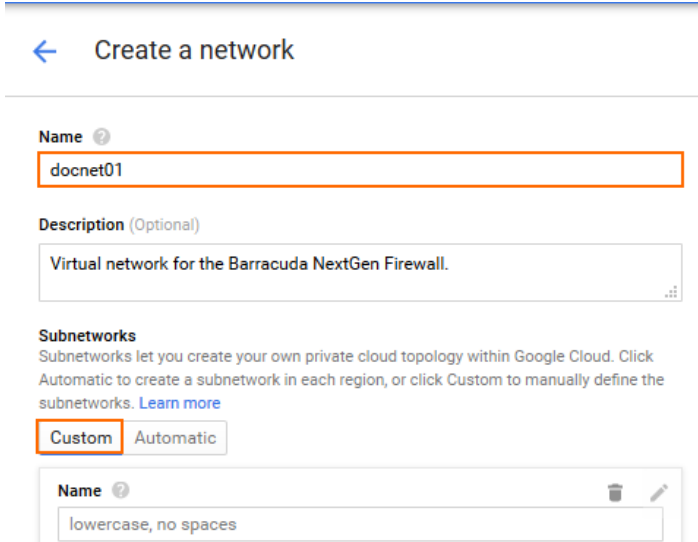
1. Log into the Google Cloud Platform. <https://console.cloud.google.com/>
2. Click the hamburger menu in the upper-left corner.



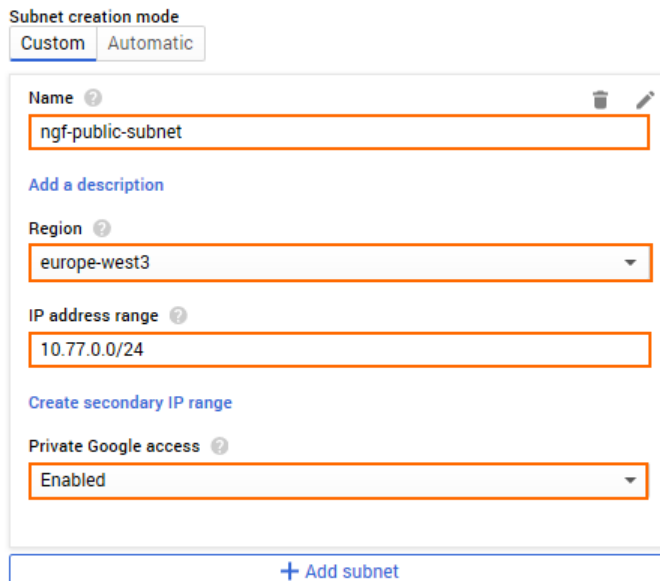
3. In the **Compute** section, click **Networking**.
4. In the main area, click **Create Network**.



5. Enter the **Name** and, in the **Subnetworks** section, click **Custom**.






 A screenshot of the 'Create a network' form. The 'Name' field contains 'docnet01'. The 'Description' field contains 'Virtual network for the Barracuda NextGen Firewall.'. In the 'Subnetworks' section, the 'Custom' option is selected. Below this, a 'Name' field for subnetworks is shown with the placeholder text 'lowercase, no spaces'.

6. Create the public subnet:
 - **Name** - Enter **ngf-public-subnet**
 - **Region** - Select your region. All virtual networks must be in the same region.
 - **IP address range** - Enter the network in CIDR format. Do not use a network that overlaps with your on-premises network.
 - **Private Google access** - Select **Enabled**.


 A screenshot of the 'Subnet creation mode' form. The 'Custom' option is selected. The 'Name' field contains 'ngf-public-subnet'. The 'Region' dropdown is set to 'europe-west3'. The 'IP address range' field contains '10.77.0.0/24'. The 'Private Google access' dropdown is set to 'Enabled'. A '+ Add subnet' button is at the bottom.

7. (optional) For each additional subnet in this virtual network, click **Add subnet**.
8. Click **Create**.

The VPC network for the firewall instances are now listed in the **VPC Networks** list.

 VPC network  VPC networks  External IP addresses  Firewall rules	VPC networks + CREATE VPC NETWORK REFRESH 				
	docnet01	3	Custom	1	Off
	europa-west3	ngf-public-subnet	10.77.0.0/24	10.77.0.1	
	europa-west3	private-subnet-01	10.77.1.0/24	10.77.1.1	
	europa-west3	private-subnet-02	10.77.2.0/24	10.77.2.1	

Step 2. Create Additional VPC Networks

Create additional virtual networks with subnets in the same region. The number of virtual networks may not exceed the number of CPU cores on the firewall instance. Verify that the networks of the VPC networks do not overlap.

The VPC networks are now listed in the **VPC Networks** list.

docnet01	3	Custom	1	Off
europa-west3	ngf-public-subnet	10.77.0.0/24	10.77.0.1	
europa-west3	private-subnet-01	10.77.1.0/24	10.77.1.1	
europa-west3	private-subnet-02	10.77.2.0/24	10.77.2.1	
docnet02	1	Custom	1	Off
europa-west3	docnet02-subnet02	10.78.1.0/24	10.78.1.1	
docnet03	1	Custom	1	Off
europa-west3	docnet03-subnet02	10.79.1.0/24	10.79.1.1	

Step 3. Create Google Firewall Rules


Google firewall rules must be configured for traffic to reach the firewall instances.

1. Go to <https://console.cloud.google.com>.
2. Click the hamburger menu in the upper-left corner.
3. In the **Compute** section, click **Networking**.
4. In the left menu, click **Firewall rules**.
5. In the main area, click **Create firewall rule**.


Firewall rules
[+ CREATE FIREWALL RULE](#) [DELETE](#)


6. Create a firewall rule to allow incoming traffic from the Internet to your firewall instances:
 - o **Name** – Enter the firewall rule name.


- **Network** – Select the network created in Step 1.
- **Priority** – Set a priority lower than 1000.
- **Direction of traffic** – Select **Ingress**.
- **Action on match** – Select **Allow**.
- **Targets** – Select **Specified target tags**.
- **Target tags** – Enter the tag `ngfha` that will be assigned to the firewall instances.
- **Source filter** – Select **IP ranges**.
- **Source IP ranges** – Enter `0.0.0.0/0`.
- **Protocols and ports** – Enter a semicolon-delimited, lower-case list of protocols and ports, or select **Allow all**.

Name 


Description (Optional)

Network 


Priority 
Priority can be 0 - 65535 [Check priority of other firewall rules](#)

Direction of traffic 


Ingress
 Egress


Action on match 


Allow
 Deny


Targets 


Target tags

Source filter 

Source IP ranges 

Second source filter 

Protocols and ports 

Allow all
 Specified protocols and ports

7. Click **Create**.

8. In each VPC network, create a firewall rule to allow traffic from selected subnets to the firewall:
- **Name** – Enter the firewall rule name.
 - **Network** – Select one of the VPC network created in Step 2. Select the VPC network created in Step 1 to allow traffic from private subnets in the hub VPC network to the firewall.
 - **Priority** – Set a priority lower than 1000.

- **Action on match** – Select **Allow**.
 - **Targets** – Select **Specified target tags**.
 - **Target tags** – Enter the tag `ngfha` that will be assigned to the firewall instances.
 - **Source filter** – Select **Subnetworks**.
 - **Subnetworks** – Select the subnets and click **OK**.
 - **Protocols and ports** – Enter a semicolon-delimited, lower-case list of protocols and ports, or select **Allow all**.
9. Click **Create**.

Traffic is now allowed to and from the firewall instances from the Internet and the additional VPC networks, as well as the private networks in the hub VPC network.

Step 4. Create a Storage Bucket and Upload the Image

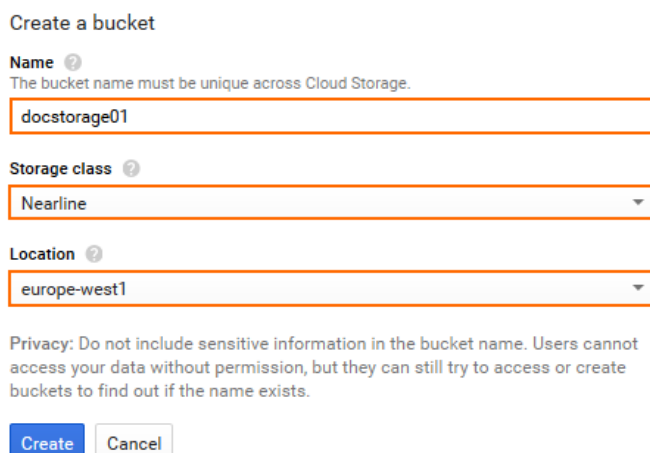
Upload the image to Google Cloud. If the upload through the browser does not work, you can instead use Google Cloud SDK to upload the image.

1. Go to <https://console.cloud.google.com>.
2. Click the hamburger menu in the upper left corner.
3. In the **Storage** section, click **Storage**.
4. In the main area, click **Create bucket**.



Browser CREATE BUCKET REFRESH DELETE

5. Create a storage bucket:
 - **Name** – Enter a unique name.
 - **Storage class** – Select a storage class depending on your preferences.
 - **Location** – Select the location matching the region you are deploying in.



Create a bucket

Name ⓘ
The bucket name must be unique across Cloud Storage.

Storage class ⓘ

Location ⓘ

Privacy: Do not include sensitive information in the bucket name. Users cannot access your data without permission, but they can still try to access or create buckets to find out if the name exists.

6. Click **Create**.
7. Click the storage bucket you just created.

Buckets

 Name docstorage01

8. Click **Upload Files** and select the firewall image you previously downloaded from the [Barracuda Download Portal](#).

Browser

9. The upload window is displayed in the lower-right corner.




The image is now listed in the file list of the storage bucket.

Browser

Buckets / docstorage01

Filter by prefix...

<input type="checkbox"/> Name	Size	Type	Last modified	Share publicly
<input type="checkbox"/>  gce-ng-7.0.1-056.VFxxx.tar.gz	1.79 GB	application/gzip	8/25/16, 9:59 AM	<input type="checkbox"/>

Step 5. Create a Compute Engine Image from the Uploaded Disk Image

To be able to deploy a firewall from the disk image uploaded in Step 3, you must create a Google Compute Engine image. The firewall is created with one dhcp interface. DHCP reservation can be done manually (static) or automatically by Google during deployment. Once assigned, the internal IP address does not change.

1. Go to <https://console.cloud.google.com>.
2. Click the hamburger menu in the upper-left corner.
3. In the **Compute** section, click **Compute Engine**.
4. In the left menu, click **Images**.
5. In the main area, click **Create Images**.

Images [+] CREATE IMAGE CREATE INSTANCE

6. Create an image using the disk image uploaded in Step 3.
 - o **Name** - Enter a name for the firewall image.
 - o **Encryption** - Select **Automatic (recommended)**.
 - o **Source** - Select **Cloud Storage file**.
 - o **Cloud Storage File** - Click **Browse** and select the disk image in the storage bucket created in Step 3.

[← Create an image](#)

Name ?

Family (Optional) ?

Description (Optional)

Encryption ?

Source ?

Cloud Storage file ?
 docstorage01/gce-ng-7.0.1-056.VFxxx.tar.gz Browse

Create Cancel

7. Click **Create**.

The firewall image is now listed in the **Images** list.

Images [+] CREATE IMAGE CREATE INSTANCE DEPRECATE DELETE

name:nextgen* Columns ▾ Labels

<input type="checkbox"/>	Name	Size	Created by	Family	Creation time
<input checked="" type="checkbox"/>	nextgen-firewall-f-701	80 GB	NG-Team		Aug 25, 2016, 10:42:30 AM

Step 6. Create Primary Firewall Instance

Launch the primary firewall instance into the public subnet of the hub VPC network. Add one network interface per additional VPC network. The number of CPU cores must be at least equal to the required

number of network interfaces.

1. Go to <https://console.cloud.google.com>.
2. Click the hamburger menu in the upper-left corner.
3. In the **Compute** section, click **Compute Engine**.
4. In the main area, click **Create instance**.

VM instances + CREATE INSTANCE

5. Enter a lowercase **Name** for the primary firewall instance.
6. Select the **Zone**. The zone must be in the same region as the public subnet in the network created in Step 1.
7. Select **Machine type**. Verify that the number of vCPUs matches the number of cores included in your F-Series Firewall license and the number of network interfaces used by the instance.

Name ?

Zone ?

Machine type
 8 GB memory Customize

8. In the **Boot disk** section, click **Change**.
9. Click the **Custom Images** tab.
10. Select the image you created in Step 5.
11. Select the **Boot disk type**:
 - **Standard persistent disk**
 - **SSD persistent disk**

Boot disk

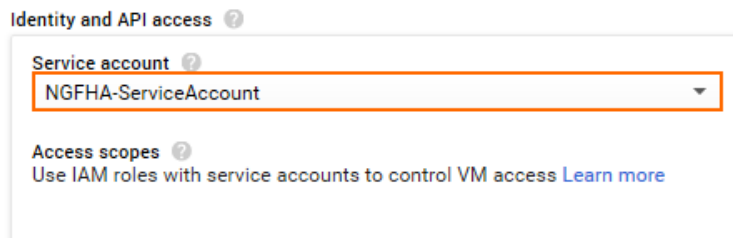
Select an image or snapshot to create a boot disk; or attach an existing disk

OS images Application images Custom images Snapshots Existing disks

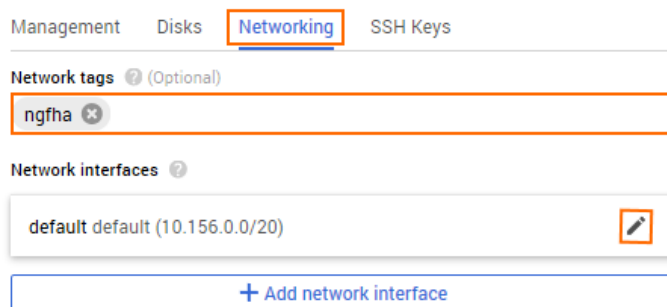
cusdangfbyol-v711-056-hf84-hf844-20170925
 The Barracuda NextGen Firewall F-Series is an enterprise-grade next-generation firewall that was purpose-built for efficient deployment and operation within dispersed, highly dynamic, and security-critical network environments.
 Created from NG-Team on Sep 25, 2017, 8:00:31 PM

Boot disk type ? Size (GB) ?

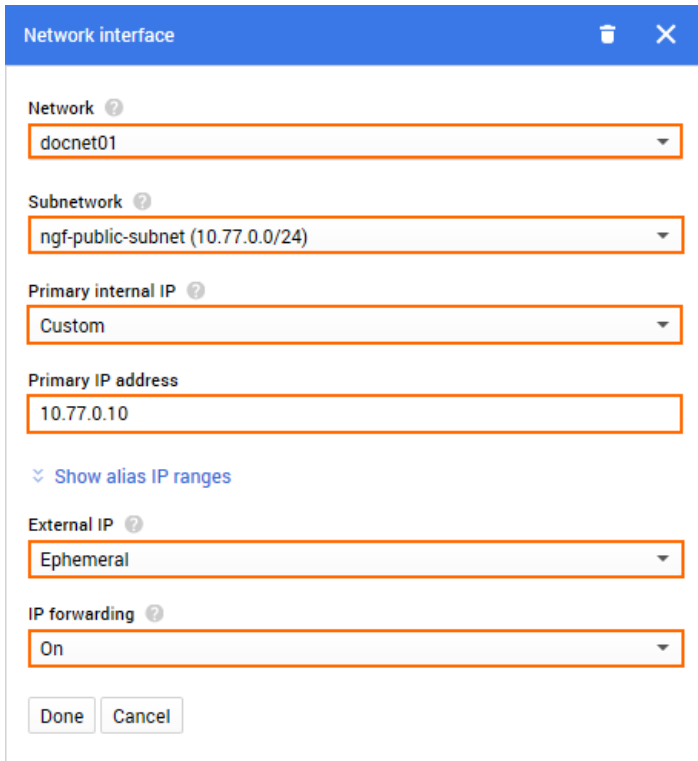
12. Click **Select**.
13. Select the dedicated **Service account** associated with the custom role created for the High Availability cluster. For more information, see [How to Create a Custom Role and Service Account for the NextGen Firewall in the Google Cloud](#).
14. In the **Access scopes** section, select **Allow full access to all Cloud APIs**.



15. Below the **Firewall** section, click **Management, disk, networking, SSH keys**.
16. Click on the **Networking** tab.
17. Add ngfha to the **Network tags**.
18. In the **Network Interfaces** section, click the edit icon for the **default** network interface.



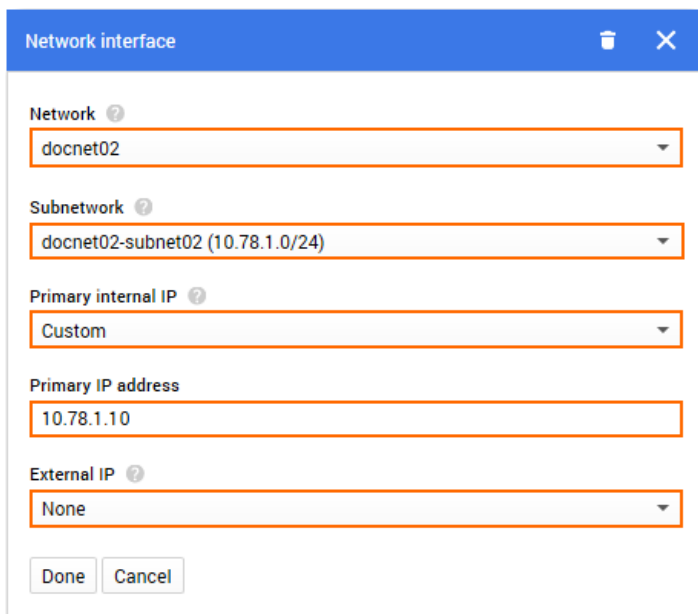
19. Configure the default network interface:
 - **Network** – Select the network created in Step 1.
 - **Subnetwork** – Select the public subnet created in Step 1.
 - **Internal IP** – Select **Custom**.
 - **Internal IP address** – Enter a free IP address in the subnet. The first IP address in the subnet is reserved for the gateway.
 - **External IP** – Select a reserved external IP address; otherwise, select **Ephemeral** to use a dynamic public IP address.
 - **IP forwarding** – Select **On**.



20. For each additional network interface, click **Add network interface**.




21. Configure the additional network interface:

- **Network** – Select one of the additional VPC networks created in Step 2.
- **Subnetwork** – Select a subnet in the VPC network that is in the same region as the firewall instance.
- **Internal IP** – Select **Custom**.
- **Internal IP address** – Enter a free IP address in the subnet. The first IP address in the subnet is reserved for the gateway.
- **External IP** – Select **None**.



22. Click **Done**. All network interfaces are now listed in the **Network interfaces** section.

Network interfaces 

docnet01 ngf-public-subnet (10.77.0.0/24)	
docnet02 docnet02-subnet02 (10.78.1.0/24)	
docnet03 docnet03-subnet02 (10.79.1.0/24)	

[+ Add network interface](#)

23. Click **Create**.

The primary firewall instance is now started.

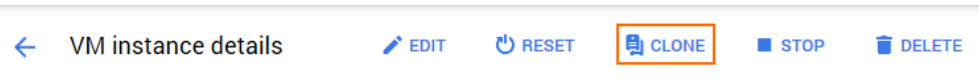
Step 7. Create the Secondary Firewall Instance


Deploy the secondary firewall of the High Availability cluster into the same subnet, but in a different zone. This ensures that one firewall of the cluster will always be running, even in case of a datacenter failure within the Google Cloud. To ease configuration clone the primary firewall and change the configuration to match the settings of the secondary firewall.

1. Go to <https://console.cloud.google.com>.
2. Click the hamburger menu in the upper-left corner.
3. In the **Compute** section, click **Compute Engine**.
4. Click on the primary firewall instance created in Step 4. The **VM instance details** page opens.


<input type="checkbox"/>	Name ^	Zone	Recommendation	Internal IP	External IP	Connect
<input checked="" type="checkbox"/>	doc-ngfha-01	europe-west3-b		10.77.0.10	35.198.187.69	SSH ▾ ⋮

5. Click **CLONE**.



 doc-ngfha-01

6. Enter the **Name** for the secondary firewall instance.
7. Select a **Zone**. Select different zones in the same region for the two firewalls in the High Availability cluster.



Name 

Zone 

8. Below the **Firewall** section, click **Management, disk, networking, SSH keys**.
9. Click the **Networking** tab
10. Add ngfha to the **Network tags**.
11. In the **Network Interfaces** section, click the edit icon for the **default** network interface
12. Click the edit icon for the first network interface:

- **Network** – Select the network created in Step 1.
 - **Subnetwork** – Select the public subnet created in Step 1.
 - **Internal IP** – Select **Custom**.
 - **Internal IP address** – Enter a free IP address in the subnet.
 - **External IP** – Select a reserved external IP address; otherwise, select **Ephemeral** to use a dynamic public IP address.
 - **IP forwarding** – Select **On**.
13. Click **Done**.
 14. Click the edit icon for the other network interfaces, and assign free custom internal IP addresses in the subnets.
 15. Click **Create**.

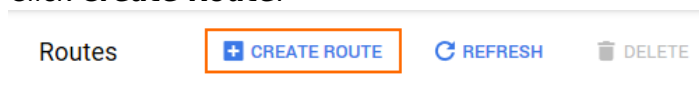
Both the primary and secondary firewalls of the High Availability cluster are now running.

<input type="checkbox"/> Name ^	Zone	Recommendation	Internal IP	External IP	Connect
<input type="checkbox"/>  doc-ngfha-01	europa-west3-a		10.77.0.10	35.198.187.69	SSH ▾ ⋮
<input type="checkbox"/>  doc-ngfha-02	europa-west3-b		10.77.0.11	35.198.120.230	SSH ▾ ⋮

Step 8. Configure Default Route for the VPC Networks to Use the Primary Firewall

For each VPC network, create a default route for the client instances to use the active firewall as the target.

1. Go to <https://console.cloud.google.com>.
2. Click the hamburger menu in the upper-left corner.
3. Click **VPC network**.
4. In the left menu, click **Routes**.
5. Click **Create Route**.



6. Configure the route:
 - **Name** – Enter a name for the route.
 - **Network** – Select the VPC network from the list.
 - **Destination IP range** – Enter 0.0.0.0/0.
 - **Priority** – Enter 100.
 - **Next hop** – Select **Specify an instance**.
 - **Next hop instance** – Select the active firewall.

Name [?]

Description (Optional)

Network [?]

Destination IP range [?]

Priority [?]

Instance tags (Optional) [?]

Next hop [?]

Next hop instance [?]

7. Click **Create**.

All traffic leaving the VPC is now being sent through the active firewall. If you have attached two additional VPC networks to the firewall, you should have at least two routes: one for each VPC network. If you also have private subnets in the hub VPC network, three routes must be created. The next hop is the IP address of the firewall's network interface in that VPC network subnet.

Step 9. Add Additional Network Interface to the Primary Firewall Configuration

Add and configure the additional network interfaces on the primary firewall.

1. Log into the primary firewall:
 - **IP Address** - The public IP address listed in the **External IP** column on the **VM Instances** page.
 - **User** - Enter root
 - **Password** - The name of the instance.
2. Go to **CONFIGURATION > Configuration Tree > Box > Network**.
3. Click **Lock**.
4. In the left menu, select **Interfaces**.
5. Double-click the entry in **Network Interface Cards**. The **Network Interface Configuration** window opens.
6. Change the **Number of Interfaces** to the number of interfaces attached to the firewall.
7. Click **Send Changes**.
8. In the left menu, select **Routing**.

9. In the left menu, expand the **Configuration Mode** section and click **Switch to Advanced**.
10. Create a new **directly attached route** for private IP address of the network interface:
 - **Target Network Address** - Enter the private IP address of the network interface with a /32 subnet mask E.g., 10.78.1.10/32
 - **Route Type** - Select **directly attached network**.
 - **Interface Name** - Select the network interface. E.g., eth1
 - **Foreign IP Sufficient** - Select **yes**.
 - **Trust Level** - Select **Trusted**.
 - **MTU** - Enter 1460.

Route Configuration

Target Network Address	<input type="text" value="10.78.1.10/32"/>	
Route Type	<input type="text" value="directly attached network"/>	
Interface Name	<input type="text" value="eth1"/> <input type="checkbox"/> Other	
Gateway	<input type="text"/>	
Route Metric	<input type="text"/>	
Source Address	<input type="text"/>	
Foreign IP Sufficient	<input type="text" value="yes"/>	
Trust Level	<input type="text" value="Trusted (added to Trusted-LAN for Firewall)"/>	
Default Gateway	<input type="text"/>	
MTU	<input type="text" value="1460"/>	

11. Create a new **directly attached route** for the default subnet gateway assigned by Google. The default gateway is always the first IP address in the subnet:
 - **Target Network Address** - Enter the first IP address in the subnet with /32 subnet mask. E.g., 10.78.1.1/32
 - **Route Type** - Select **directly attached network**.
 - **Interface Name** - Select the network interface. E.g., eth1
 - **Foreign IP Sufficient** - Select **yes**.
 - **Trust Level** - Select **Trusted**.
 - **MTU** - Enter 1460.

Route Configuration

Target Network Address	<input type="text" value="10.78.1.1/32"/>	
Route Type	<input type="text" value="directly attached network"/>	
Interface Name	<input type="text" value="eth1"/> <input type="checkbox"/> Other	
Gateway	<input type="text"/>	
Route Metric	<input type="text"/>	
Source Address	<input type="text"/>	
Foreign IP Sufficient	<input type="text" value="yes"/>	
Trust Level	<input type="text" value="Trusted (added to Trusted-LAN for Firewall)"/>	
Default Gateway	<input type="text"/>	
MTU	<input type="text" value="1460"/>	

12. Create a new **gateway route** for the subnet using the default subnet gateway:
 - **Target Network Address** - Enter the subnet in CIDR format. E.g., 10.78.1.0/24
 - **Route Type** - Select **gateway**.
 - **Gateway** - Enter the first IP address in the subnet. E.g., 10.78.1.1
 - **Trust Level** - Select **Trusted**.
 - **MTU** - Enter 1460.

Route Configuration

Target Network Address	10.78.1.0/24
Route Type	gateway
Interface Name	<input type="text"/> <input type="checkbox"/> Other
Gateway	10.78.1.1
Route Metric	<input type="text"/>
Source Address	<input type="text"/>
Foreign IP Sufficient	no
Trust Level	Trusted (added to Trusted-LAN for Firewall)
Default Gateway	<input type="text"/>
MTU	1460

13. Click **Send Changes** and **Activate**.

Step 10. Disable ICMP Gateway Monitoring For Additional Network Interfaces

Disable ICMP gateway monitoring for all additional network interfaces.

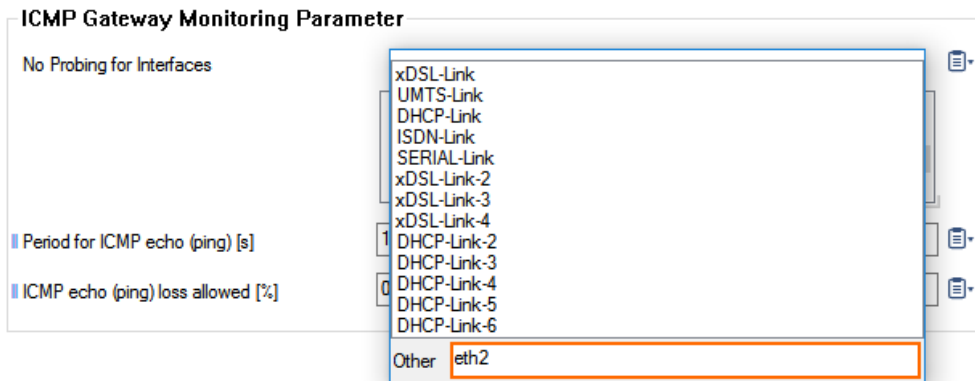
1. Log into the primary firewall.
2. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Control**.
3. Click **Lock**.
4. For each additional network interface click **+** to add an entry in the **No Probing for Interfaces** table,

ICMP Gateway Monitoring Parameter

No Probing for Interfaces

<input type="text"/>	<input type="button" value="+"/> <input type="button" value="X"/> <input type="button" value="copy"/>
DHCP-Link ISDN-Link SERIAL-Link	<input type="text"/>

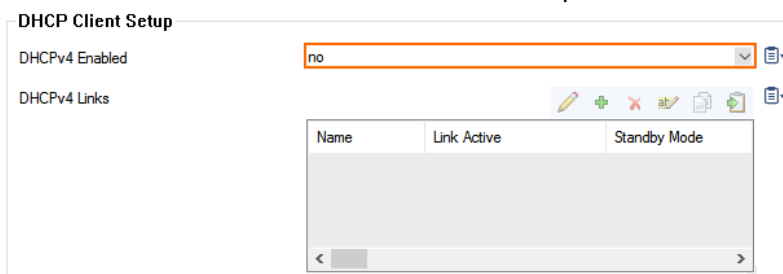
5. If the interface is not in the list enter it in the **Other** field.



6. Click **Send Changes** and **Activate**.

Step 11. Change Primary Firewall Configuration to Use Static Network Interface

1. Log into the primary firewall.
2. Go to **CONFIGURATION > Configuration Tree > Box > Network**.
3. In the left menu, expand the **Configuration Mode** section and click **Switch to Advanced**.
4. Click **Lock**.
5. in the left menu, click **xDSL/DHCP/ISDN**.
6. Delete the **DHCP01** entry in the **DHCP Links** list.
7. Select **No** from the **DHCPv4 Enabled** drop-down list.



8. In the left menu, click **IP Configuration**.
9. In the **Management IP and Network** section, reconfigure the management IP:
 - o **Interface Name** - Select **Other** and enter eth0.
 - o **Management IP** - Enter the private IP address of the primary firewall. Go to **CONTROL > Network**. The private IP address is assigned to the dhcp interface.
 - o **Associated Netmask** - Select **single-host**.
 - o **MTU** - Enter 1460.

Management IP and Network

Interface Name	eth0 <input type="checkbox"/> Other
Management IP (MIP)	10.77.0.10
Associated Netmask	single-host
Responds to Ping	yes
Use for NTPd	yes
Trust Level	Trusted (added to Trusted-LAN for Firewall)
MTU	1460

10. In the left menu, click **Routing**.

11. Create a new **directly attached route** for the default subnet gateway assigned by Google. The default gateway is always the first IP address in the subnet:

- **Target Network Address** - Enter the first IP address in the subnet with /32 subnet mask. E.g., 10.77.0.1/32
- **Route Type** - Select **directly attached network**.
- **Interface Name** - Select **Other** and enter eth0.
- **Foreign IP Sufficient** - Select **yes**.
- **Trust Level** - Select **Unclassified**.
- **MTU** - Enter 1460.

Route Configuration

Target Network Address	10.77.0.1/32
Route Type	directly attached network
Interface Name	eth0 <input type="checkbox"/> Other
Gateway	
Route Metric	
Source Address	
Foreign IP Sufficient	yes
Trust Level	Unclassified
Default Gateway	
MTU	1460

12. Click **OK**.

13. Click + in the **Routes** table and add the default route:

- **Target Network Address** - Enter 0.0.0.0/0.
- **Route Type** - Select **gateway**.
- **Gateway** - Enter the first IP address in the subnet. E.g., 10.77.0.1
- **Trust Level** - Select **Unclassified**.
- **MTU** - Enter 1460.

Route Configuration

Target Network Address	<input type="text" value="0.0.0.0/0"/>	
Route Type	<input type="text" value="gateway"/>	
Interface Name	<input type="text" value=""/> <input type="checkbox"/> Other	
Gateway	<input type="text" value="10.77.0.1"/>	
Route Metric	<input type="text"/>	
Source Address	<input type="text"/>	
Foreign IP Sufficient	<input type="text" value="no"/>	
Trust Level	<input type="text" value="Unclassified"/>	
Default Gateway	<input type="text"/>	
MTU	<input type="text" value="1460"/>	

14. Click **OK**.
15. Click **Send Changes** and **Activate**.

Open the **CONTROL > Network** page. Your interface and IP address are now static.

Step 12. Activate Network Changes

1. Go to **CONTROL > Box**.
2. In the left menu, expand the **Network** section and click **Activate new network configuration**.
3. Select **Failsafe**.

Step 13. Configure the DNS Server

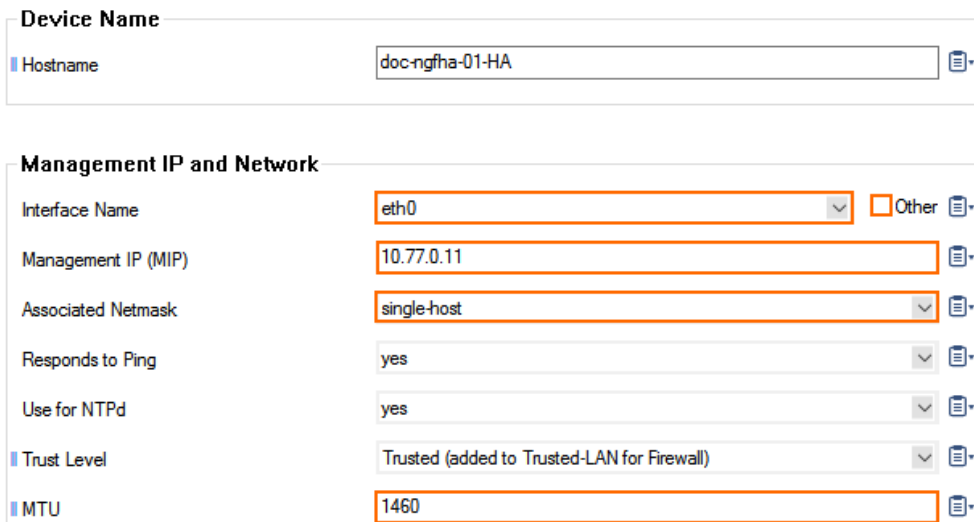
Add the first IP address of the subnet as the DNS server (e.g., 10.77.0.1). Do not use external DNS servers because, otherwise, it is not possible to resolve the internal Google metadata service used by the HA failover script.

For more information, see [How to Configure DNS Settings](#).

Step 14. Create DHA Cluster Configuration

Create the DHA cluster configuration for the secondary firewall and configure the routing configuration.

1. Log into the primary firewall.
2. Go to **CONFIGURATION > Configuration Tree > Box**.
3. Right-click **Box** and select **Create DHA box**. At the bottom of the **Config Tree**, the **HA Box** configuration node is added.
4. Go to **CONFIGURATION > Configuration Tree > HA Box > HA Network**.
5. In the left menu, expand the **Configuration Mode** section and click **Switch to Advanced**.
6. In the **Management IP and Network** section, reconfigure the management IP:
 - **Interface Name** - Select **Other** and enter eth0.
 - **Management IP** - Enter the private IP address of the secondary firewall. On the secondary firewall, go to **CONTROL > Network**. The private IP address is assigned to the dhcp interface.
 - **Associated Netmask** - Select **single-host**.
 - **MTU** - Enter 1460.



The screenshot shows the configuration interface for a Barracuda CloudGen Firewall. The 'Device Name' section has a 'Hostname' field with the value 'doc-ngfha-01-HA'. The 'Management IP and Network' section has several fields: 'Interface Name' is set to 'eth0' (with an 'Other' checkbox), 'Management IP (MIP)' is '10.77.0.11', 'Associated Netmask' is 'single-host', 'Responds to Ping' is 'yes', 'Use for NTPd' is 'yes', 'Trust Level' is 'Trusted (added to Trusted-LAN for Firewall)', and 'MTU' is '1460'. Each field has a copy icon to its right.

7. Edit the directly attached routes for the private IP addresses to match the secondary firewall custom internal IP address on that network interface.
8. Verify that the routing is configured analog to the primary firewall:
 - **For the hub VPC network** - One gateway route and on directly attached route.
 - **For each additional VPC network** - One gateway and two directly attached routes. The directly attached routes for the private IP addresses must be changed to match the custom internal IP addresses of the secondary firewall on that interface.

Main Routing Tables

IPv4 Routing Table

Name	Target Network Address	Route Type
docnet01DefaultRoute	0.0.0.0/0	gateway
docnet01GW	10.77.0.1/32	directly attach
docnet02Subnet	10.78.1.0/24	gateway
docnet02gw	10.78.1.1/32	directly attach
docnet02privateIP	10.78.1.11/32	directly attach
docnet03GW	10.79.1.1/32	directly attach
docnet03PrivateIP	10.79.1.11/32	directly attach
docnet03Subnet	10.79.1.0/24	gateway

9. Click **Send Changes** and **Activate**.

Step 15. Add the Private IPs to the Virtual Server IPs and Add the Secondary Firewall to the Virtual Server

Add the custom private IP addresses of both firewalls to the additional network interfaces to the virtual server IP addresses.

1. Log into the primary firewall
2. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > S1 > Server Properties**.
3. Click **Lock**.
4. From the **Backup Box** drop-down list, select **Other-Box**.
5. In the **Additional IP** table, add the private IP addresses for both firewalls.

Additional IP

Additional IP	Label	Reply to Ping	Descrip
10.78.1.10	IP3	1	
10.79.1.10	IP4	1	
10.78.1.11	IP5	1	
10.79.1.11	IP6	1	

6. Click **Send Changes** and **Activate**.

Step 16. Join the High Availability Cluster

Step 16.1 Export PAR File

1. On the primary firewall, create the PAR file:
2. Go to **CONFIGURATION > Configuration Tree > Box**.
3. From the **Config Tree**, right-click **Box** and select **Create PAR file for HA box**.
4. Save the PAR file to your local hard disk drive.

Step 16.2 Import the PAR File on the Secondary Firewall

1. Log in to the secondary firewall:
 - **IP Address** – The public IP address listed in the **External IP** column on the **VM Instances** page.
 - **User** – Enter root
 - **Password** – The name of the instance.
2. Go to **CONFIGURATION > Configuration Tree > Box**.
3. From the **Config Tree**, right-click **Box** and select **Restore from PAR file**.
4. Click **OK**.
5. Select the boxha.par file created in Step 15.1 and click **OK**.
6. Click **Activate**.

Step 16.3 Activate the Network Configuration on the Secondary Firewall

1. Go to **CONTROL > Box**.
2. Click **Trust**.
3. In the left menu, expand **Network** and click **Activate new network configuration**.
4. Select **Failsafe** as the activation mode.

Step 17. Activate and License the High Availability Cluster

Activate and license the High Availability cluster. Activate the secondary firewall first. Then, activate the primary firewall.

For more information, see [How to Activate and License a Standalone High Availability Cluster](#).

Step 18. Add High Availability Failover Script to Primary and Secondary Firewalls

To rewrite the default routes using the firewall as the default gateway to always use the active firewall in the High Availability cluster, copy the failover script to the `/opt/phion/hooks/ha/` on both firewalls. The script is executed automatically every time the virtual server fails over.

Step 18.1. Enable SSH Root Access

1. Log into the primary firewall.
2. Go to **CONFIGURATION > Configuration Tree > Box > Advanced Configuration > SSH**.
3. Click **Lock**.
4. In the left menu, select **Basic Setup**.
5. From the **Permit Root Login** drop-down list, select **key-only**.
6. Click **Send Changes** and **Activate**.

Step 18.2. Create the Failover Script on both Firewalls

Create this script on both firewalls.

1. Download the [gcp-ha-takeover.sh](#) script.
2. Log into the primary firewall via SSH.
3. Go to the
4. Copy the **gcp-ha-takeover.sh** script to the **/opt/phion/hooks/ha/** directory on the firewall
5. Make the script executable:

```
chmod +x /opt/phion/hooks/ha/gcp-ha-takeover.sh
```

6. Repeat on the secondary firewall.

Step 19. (optional) Add Google Network Load Balancer

To use only one public-facing IP address, it is also possible to use the Google Network Load Balancer in front of the High Availability cluster. To use the load balancer, a service on port 80 or 443 must be reachable for the health check of the load balancer. TCP and UDP services require separate load balancers. To use a service on the firewall for probing create an **App Redirect** rule redirecting HTTP traffic to the fwauth daemon running on 127.0.0.1:451.

For more information, see <https://cloud.google.com/compute/docs/load-balancing/network/>

Figures

1. google_cloud_ha_lb.png
2. gcc_networking01.png
3. gcc_networking02.png
4. gcc_networking03.png
5. gcc_networking04.png
6. gcc_networking05.png
7. gcc_networking06.png
8. gcc_firewall_rule01.png
9. gcc_google_fw_rule_01.png
10. gcc_storage01.png
11. gcc_storage02.png
12. gcc_storage03.png
13. gcc_storage04.png
14. gcc_storage05.png
15. gcc_storage06.png
16. gcc_create_image01.png
17. gcc_create_image02.png
18. gcc_create_image03.png
19. gcc_prim_fw01.png
20. gcc_prim_fw_02.png
21. gcc_prim_fw_03.png
22. gcc_prim_fw_04.png
23. gcc_prim_fw_05.png
24. gcc_prim_fw_06.png
25. gcc_prim_fw_07.png
26. gcc_prim_fw_08.png
27. gcc_secondary_fw_01.png
28. gcc_secondary_fw_02.png
29. gcc_secondary_fw_03.png
30. gcc_secondary_fw_04.png
31. gce_routes_01.png
32. gce_routes_02.png
33. gce_add_nic_01.png
34. gce_add_nic_02.png
35. gce_add_nic_03.png
36. gce_no_icmp_gateway_monitoring_01.png
37. gce_no_icmp_gateway_monitoring_02.png
38. gce_static_mip_01.png
39. gce_static_mip_02.png
40. gce_static_mip_03.png
41. gce_static_mip_04.png
42. gce_dha_01.png
43. gce_dha_02.png
44. gce-virtualserver_ips.png

© Barracuda Networks Inc., 2020 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.