

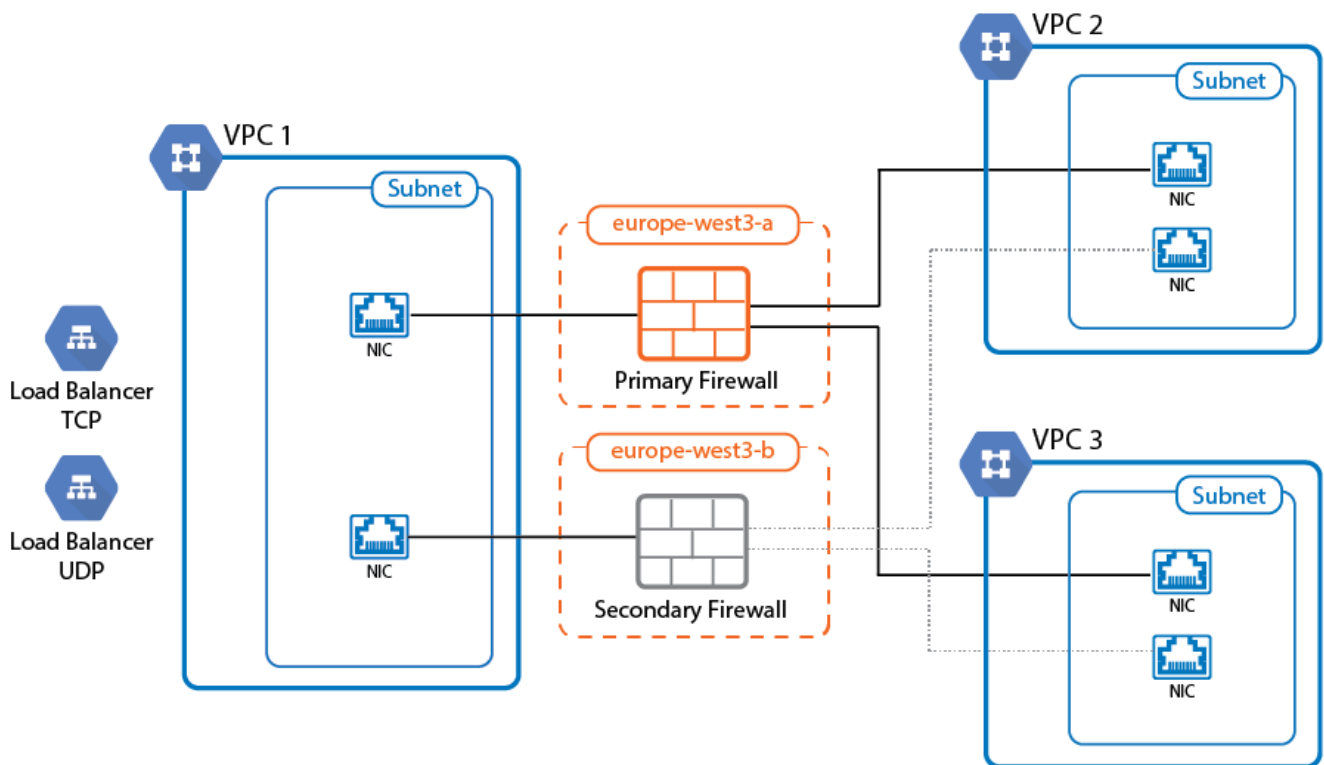
## How to Configure a High Availability Cluster in Google Cloud

<https://campus.barracuda.com/doc/25153/>

Running your CloudGen Firewall in a High Availability cluster in the Google Cloud ensures that even in the event of a data center 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 service 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 CloudGen 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)

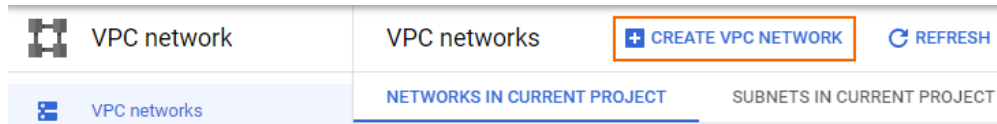
## Step 1. Create the Hub VPC Network

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

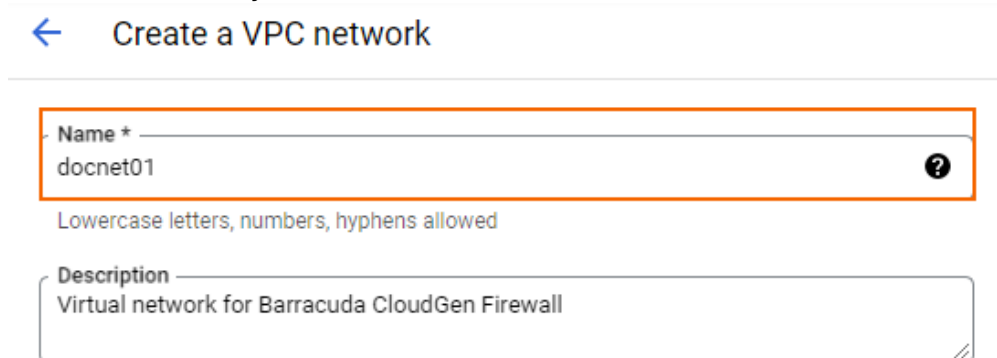
1. Log into the Google Cloud Platform. <https://console.cloud.google.com/>
2. Create a new project or select your project.
3. Click the hamburger menu in the upper-left corner.



- In the **VPC network** section, select **VPC networks**.
- Click **CREATE VPC NETWORK**.




- Enter a **Name** for your network.



- In the **Subnets** section, select **Custom**.

## Subnets

Subnets let you create your own private cloud topology within Google Cloud. Click **Automatic** to create a subnet in each region, or click **Custom** to manually define the subnets. [Learn more](#)

Subnet creation mode 

- Custom
- Automatic

- Create the public subnet:
  - Name** - Enter `cgf-public-subnet`
  - Region** - Select your region. All virtual networks must be in the same region.
  - IPv4 range** - Enter the network in CIDR format. Do not use a network that overlaps with your on-premises network.
  - Private Google Access** - Select the radio button.

**Name \***  
cgf-public-subnet

Lowercase letters, numbers, hyphens allowed

**Description**

**Region \***  
europe-west3

**IP stack type**

IPv4 (single-stack)

IPv4 and IPv6 (dual-stack) ?

**IPv4 range \***  
10.77.0.0/24

E.g. 10.0.0.0/24

[CREATE SECONDARY IPV4 RANGE](#)

**Private Google Access** ?

On

Off

9. (optional) For each additional subnet in this virtual network, click **ADD SUBNET**.
10. Click **CREATE**.

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

VPC network		VPC networks							
		NETWORKS IN CURRENT PROJECT				SUBNETS IN CURRENT PROJECT			
VPC networks		VPC networks							
IP addresses		Filter Enter property name or value							
Bring your own IP		<b>Name ↑</b>	<b>Subnets</b>	<b>MTU ?</b>	<b>Mode</b>	<b>Internal IP ranges</b>	<b>Gateways</b>	<b>Firewall rules</b>	<b>Global dynamic</b>
Firewall		<a href="#">alena-vpc</a>	38	1460	Auto			3	Off
Routes		<a href="#">alena-wan-demo-vpc</a>	2	1460	Custom			1	Off
VPC network peering		<a href="#">anna-pvt-net</a>	2	1460	Custom			10	Off
Shared VPC		<a href="#">default</a>	36	1460	Auto			20	Off
Serverless VPC access		<a href="#">docnet01</a>	1	1460	Custom			0	Off

## 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.

### 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 **VPC network** section, select **Firewall**.
4. Click **CREATE FIREWALL RULE**.



5. Create a firewall rule to allow incoming traffic from the Internet to your firewall instances:
  - o **Name** - Enter the firewall rule name.
  - o **Network** - Select the network created in Step 1.
  - o **Priority** - Set a priority lower than 1000.

#### ← Create a firewall rule

Firewall rules control incoming or outgoing traffic to an instance. By default, incoming traffic from outside your network is blocked. [Learn more](#)

Name \*  
cgf-allow-all-inbound

Lowercase letters, numbers, hyphens allowed

Description

#### Logs

Turning on firewall logs can generate a large number of logs which can increase costs in Cloud Logging. [Learn more](#)

- On  
 Off

Network \*  
docnet01


Priority \*  
900

CHECK PRIORITY OF OTHER FIREWALL RULES

Priority can be 0 - 65535


- o **Direction of traffic** - Select **Ingress**.

- **Action on match** - Select **Allow**.
- **Targets** - Select **Specified target tags**.
- **Target tags** - Enter the tag `cgfha` that will be assigned to the firewall instances.
- **Source filter** - Select **IPv4 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**.

Direction of traffic 


Ingress

Egress


Action on match 


Allow


Deny

Targets 


Specified target tags


Target tags \* 


cgfha 

Source filter 


IPv4 ranges

Source IPv4 ranges \* 

0.0.0.0/0 

Second source filter 

None

Protocols and ports 

Allow all

Specified protocols and ports

6. Click **CREATE**.

7. 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 `cgfha` 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**.
8. 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.

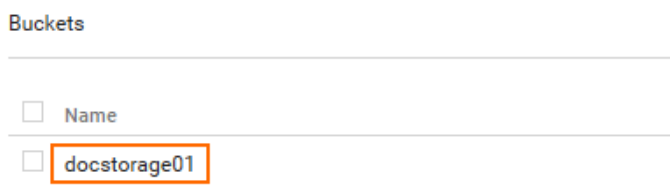
## Step 4. Create a Storage Bucket and Upload the Disk Image

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

1. Go to <https://console.cloud.google.com>.
2. Click the hamburger menu in the upper-left corner.

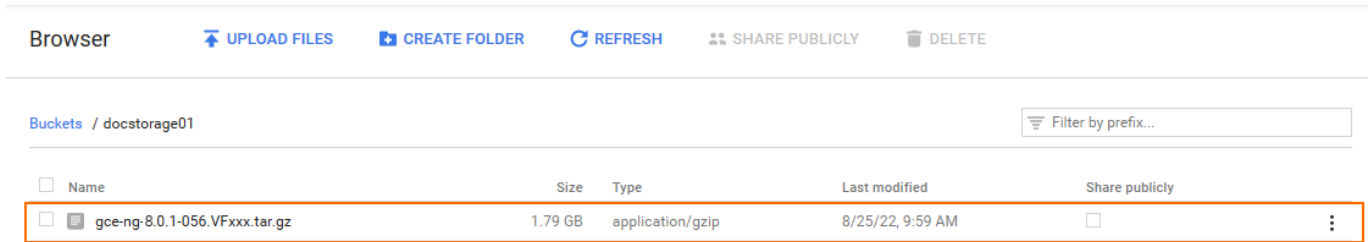


3. In the **Cloud Storage** section, click **Buckets**.
4. In the main area, click **CREATE**.
5. Create a storage bucket:
  - **Name** – Enter a unique name.
  - **Region** – Select the location matching the region you are deploying in.
  - **Storage class** – Select a storage class depending on your preferences.
6. Click **CREATE**. The storage bucket is now listed in the **Buckets** list.
7. Click the storage bucket you just created.



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

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



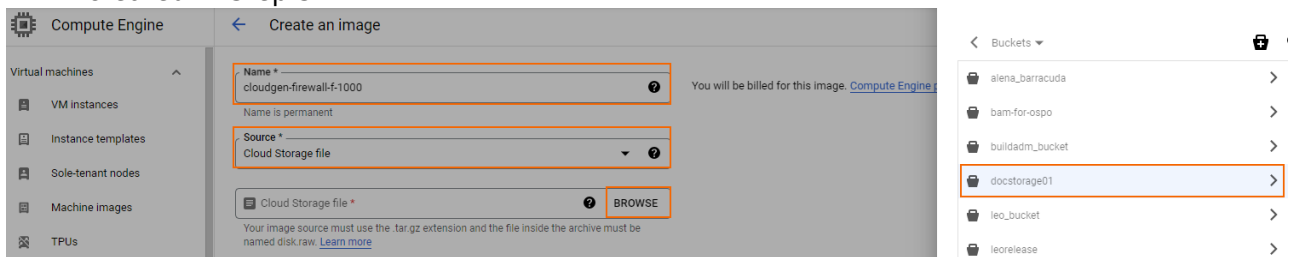
### Step 5. Create a Compute Engine Image from the Uploaded Disk Image

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 Engine** section, select **Images**.
4. In the main area, click **CREATE IMAGE**.



5. Create an image using the disk image uploaded in Step 3.
  - o **Name** - Enter a name for the firewall image.
  - 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.



6. Click **CREATE**.

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

Images [\[+\] CREATE IMAGE](#) [\[+\] CREATE INSTANCE](#) [\[⊖\] DEPRECATE](#) [\[🗑️\] DELETE](#)

name:cloudgen\* [Columns](#) [Labels](#)

<input type="checkbox"/>	Name	Size	Created by	Family	Creation time
<input checked="" type="checkbox"/>	cloudgen firewall-f-701	80 GB	NG-Team		Aug 25, 2022, 10:42:30 AM

## Step 6. Create the 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 Engine** section, click **VM instances**.
4. In the main area, click **CREATE INSTANCE**.

VM instances [\[+\] CREATE INSTANCE](#)

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

**Name \***  
doc-cgfha-01

**Labels** ?  
+ ADD LABELS

**Region \***  
europe-west3 (Frankfurt) ?  
Region is permanent

**Zone \***  
europe-west3-c ?  
Zone is permanent

## Machine configuration

### Machine family

GENERAL-PURPOSE COMPUTE-OPTIMIZED MEMORY-OPTIMIZED GPU

Machine types for common workloads, optimized for cost and flexibility

**Series**  
E2  
CPU platform selection based on availability

**Machine type**  
e2-highcpu-16 (16 vCPU, 16 GB memory)

8. In the **Boot disk** section, click **Change**.
9. Click the **CUSTOM IMAGES** tab.
10. Select the disk image you created in Step 5.
11. Select the **Boot disk type**.

ENABLE

**Container** ?  
Deploy a container image to this VM instance  
DEPLOY CONTAINER

**Boot disk** ?

Name	doc-cgfha
Type	New bal...
Size	10 GB
License type	Free
Image	Debia...

CHANGE

Select an image or snapshot to create a boot disk; or attach an existing disk. Can't find what you're looking for? Explore hundreds of VM solutions in [Marketplace](#)

PUBLIC IMAGES CUSTOM IMAGES SNAPSHOTS ARCHIVE SNAPSHOTS

Source project for images \*  
ng-team ? CHANGE

Show deprecated images

**Image \***  
cudacgcbbyol-v721-129-20180515  
Created on May 15, 2018, 2:39:04 AM

**Boot disk type \***  
Standard persistent disk

COMPARE DISK TYPES

Size (GB) \*  
250

12. Click **SELECT**.
13. Select the dedicated **Service account** associated with the custom role that was created for the High Availability cluster. For more information, see [How to Create a Custom Role and Service Account for the CloudGen Firewall in the Google Cloud](#).

14. In the **Access scopes** section, select **Allow full access to all Cloud APIs**.

Identity and API access ?

Service account ?

CGFHA-ServiceAccount ▼

Access scopes ?

Use IAM roles with service accounts to control VM access [Learn more](#)

15. Below the **Firewall** section, scroll down and expand **Advanced options**.
16. Expand **Networking**.
17. Add cgfha to the **Network tags**.

Advanced options ^

Networking ^

Hostname and network interfaces

Network tags ?

cgfha ?

Hostname ?

Set a custom hostname for this instance or leave it default. Choice is permanent

18. Select **Enable** for **IP forwarding**.
19. In the **Network interfaces** section, edit the **default** network interface,
20. Edit the first network interface:
- **Network** – Select the network created in Step 1.
  - **Subnetwork** – Select the public subnet created in Step 1.
  - **Primary Internal IP** – Select **Ephemeral (Custom)**. Enter a free IP address in the subnet. The first IP address in the subnet is reserved for the gateway.
  - **External IPv4 address** – Select a reserved external IP address. To use a dynamic public IP address, select **Ephemeral**.
21. For each additional network interface, click **ADD NETWORK INTERFACE**.
22. 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.
  - **Primary Internal IP** – Select **Ephemeral (Custom)**. Enter a free IP address in the subnet. The first IP address in the subnet is reserved for the gateway.
  - **External IPv4 address** – Select **None**.
23. Click **DONE**. All network interfaces are now listed in the **Network interfaces** section.



24. Click **CREATE**.

The primary firewall instance is now started.

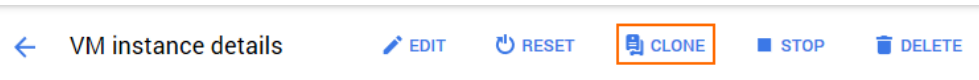
## Step 7. Create the Secondary Firewall Instance


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 data center 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 Engine** section, select **VM instances**.
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-cgffa-01	europe-west3-b		10.77.0.10	35.198.187.69	SSH ▾ ⋮

5. Click **CLONE**.



 doc-ngffa-01

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

**Name \***  
doc-cgfh-02

**Labels** ?  
+ ADD LABELS

**Region \***  
europe-west3 (Frankfurt) ?  
Region is permanent

**Zone \***  
europe-west3-b ?  
Zone is permanent

8. Scroll down and expand **Advanced options**.
9. Expand **Networking**.
10. Add cgfha to the **Network tags**.

**Advanced options** ^



**Networking** ^  
Hostname and network interfaces

**Network tags**  
cgfha ?

Hostname ?  
Set a custom hostname for this instance or leave it default. Choice is permanent

11. Select **Enable** for **IP forwarding**.
12. In the **Network Interfaces** section, click the edit icon for the **default** network interface,
13. Click the edit icon for the first network interface:
  - o **Network** – Select the network created in Step 1.
  - o **Subnetwork** – Select the public subnet created in Step 1.
  - o **Primary Internal IP** – Select **Ephemeral (Custom)**. Enter a free IP address in the subnet.
  - o **External IPv4 address** – Select a reserved external IP address. To use a dynamic public IP address, select **Ephemeral**.
14. Click **DONE**.
15. Click the edit icon for the other network interfaces, and assign free custom internal IP addresses in the subnets.
16. 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	europe-west3-a		10.77.0.10	35.198.187.69	SSH ▾ ⋮
<input type="checkbox"/>  doc-ngfha-02	europe-west3-b		10.77.0.11	35.198.120.230	SSH ▾ ⋮

---

## Step 8. Configure a 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**.



Routes **CREATE ROUTE** REFRESH DELETE

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 \***  
docnet02-default-route-cgf

Lowercase letters, numbers, hyphens allowed

**Description**  
Default route for docnet02 using the firewall as the target

**Network \***  
docnet02

**Destination IP range \***  
0.0.0.0/0

E.g. 10.0.0.0/16

**Priority \***  
100

Priority should be a positive integer (lower values take precedence)

Instance tags

**Next hop**  
Specify an instance

doc-cgfha-01

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 an Additional Network Interface to the Primary Firewall Configuration

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

- 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 password located in **VM instances > your VM instance > Custom metadata**.

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 **OK**.
8. Click **Send Changes**.
9. In the left menu, select **Advanced Routing**.
10. In the left menu, expand the **Configuration Mode** section and click **Switch to Advanced**.
11. Click + in the **IPv4 Routing Table** to create a new direct 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** - Select the network interface. E.g., eth1
  - **Foreign IP Sufficient** - Select **yes**.
  - **Trust Level** - Select **Trusted**.
  - **MTU** - Enter 1460.

**IPv4 Route Configuration**

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


12. Click + in the **IPv4 Routing Table** to create a new direct 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.


**IPv4 Route Configuration**


Target Network Address	<input checked="" type="checkbox"/> 10.78.1.1/32	
Gateway	<input type="text"/>	
Route Metric	<input type="text"/>	
Route Type	<input checked="" type="checkbox"/> directly attached network	
Interface	<input checked="" type="checkbox"/> eth1 <input type="checkbox"/> Other	
Source Address	<input type="text"/>	
Foreign IP Sufficient	<input checked="" type="checkbox"/> yes	
Trust Level	<input checked="" type="checkbox"/> Trusted (added to Trusted-LAN for Firewall)	
Default Gateway	<input type="text"/>	
MTU	<input checked="" type="checkbox"/> 1460	
Advertise Route	<input type="text" value="no"/>	
Reachable IPs		
Re-Reachable Command	<input type="text"/>	


13. Click + in the **IPv4 Routing Table** to 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.


**IPv4 Route Configuration**


Target Network Address  10.78.1.0/24 


Gateway  10.78.1.1 


Route Metric  


Route Type  


Interface   Other 


Source Address  








Foreign IP Sufficient  


Trust Level  Trusted (added to Trusted-LAN for Firewall) 

Default Gateway  

MTU  1460 

Advertise Route  

Reachable IPs       

Re-Reachable Command  




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

## Step 10. Disable ICMP Gateway Monitoring for Additional Network Interfaces

Disable ICMP gateway monitoring for all additional network interfaces.

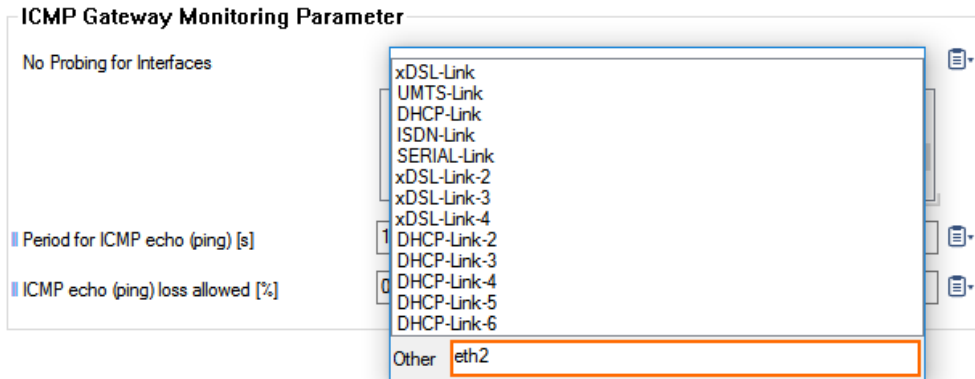
1. Log into the primary firewall.
2. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Control**.
3. Click **Lock**.
4. For each additional network interface click **+** to add an entry in the **No Probing for Interfaces** table,

**ICMP Gateway Monitoring Parameter**

No Probing for Interfaces   

DHCP-Link  
ISDN-Link  
SERIAL-Link

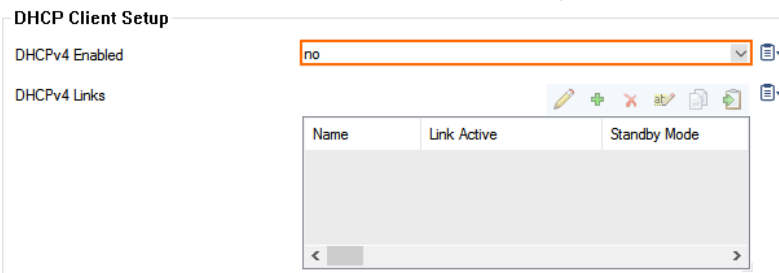
5. If the interface is not in the list, enter it in the **Other** field.



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

## Step 11. Change the Primary Firewall Configuration to Use the 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**.
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 Network and IPs** 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 Network and IPs**

Interface	<input checked="" type="checkbox"/> eth0	<input checked="" type="checkbox"/> Other	
Management IP	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 **Advanced Routing**.

11. Click + in the **IPv4 Routing Table** to create a new direct attached route for the default subnet gateway assigned by Google. The default gateway is always the first IP address in the subnet:

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

**IPv4 Route Configuration**

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

12. Click **OK**.

13. Click + in the **IPv4 Routing Table** and add the default route:

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

**IPv4 Route Configuration**

Target Network Address	<input type="text" value="0.0.0.0/0"/>	
Gateway	<input checked="" type="checkbox"/> <input type="text" value="10.77.0.1"/>	
Route Metric	<input type="text"/>	
Route Type	<input checked="" type="checkbox"/> <input type="text" value="gateway"/>	
Interface	<input type="text"/> <input type="checkbox"/> Other	
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 checked="" type="checkbox"/> <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 the 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. Configure the Management IP and Network on the Primary Firewall

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. In the left menu click **IP Configuration**.
5. In the **Management IP and Network** section, reconfigure the management IP:
  - o **Interface** - Select **Other** and enter eth0.
  - o **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.
  - o **Associated Netmask** - Select **single-host**.
  - o **MTU** - Enter 1460.

**Management Network and IPs**

Interface	<input checked="" type="checkbox"/> eth0	<input checked="" type="checkbox"/> Other	
Management IP	<input checked="" type="checkbox"/> 10.77.0.11		
Associated Netmask	<input checked="" type="checkbox"/> single-host		
Responds to Ping	yes		
Use for NTPd	yes		
Trust Level	Trusted (added to Trusted-LAN for Firewall)		
MTU	<input checked="" type="checkbox"/> 1460		

6. Edit the directly attached routes for the private IP addresses to match the secondary firewall custom internal IP address on that network interface.
7. In the left menu, click **Advanced Routing**.
8. Verify that the routing is configured analog to the primary firewall:
  - o For the hub VPC network - One gateway route and one directly attached route.
  - o 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 Shared IPs

---

Add the custom private IP addresses of both firewalls to the additional network interfaces to the shared IP addresses, e.g., 10.78.1.10, 10.78.1.11, 10.79.1.10 and 10.79.1.11.

1. Log into the primary firewall
2. Go to **CONFIGURATION > Configuration Tree > Box > Network**.
3. Click **Lock**.
4. In the left menu, click **IP Configuration**.
5. In the **Shared Networks and IPs** section, double-click on the entry of the network where the IP address is attached to, or click **+** to create a new entry.
6. The **Shared Network and IPs** window opens.
  1. In the **Shared IPs in this Network** section, click **+**.
    - **IP Address** – Enter the IP address.
    - **Alias for this IP**– Select **None**.
    - **Responds to Ping**– Select **yes**.
    - Click **OK** to save this settings.
  2. Click **OK** to save this settings.
7. Click **Send Changes** and **Activate**.
8. Go to **CONTROL > Box**.
9. In the left menu, expand the **Network** section and click **Activate new network configuration**.
10. Select **Failsafe**.

## Step 16. Create a High Availability Cluster

---

Create a high availability cluster on your primary firewall and join it with the secondary firewall.

For more information, see [How to Set Up a High Availability Cluster](#).

## 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. (optional) Add the 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. start\_menu.png
3. new\_vpc.png
4. net\_name.png
5. custom\_net.png
6. edit\_subnet.png
7. net\_list.png
8. start\_menu.png
9. create\_rule.png
10. create\_rule\_01.png
11. create\_rule\_02.png
12. start\_menu.png
13. gcc\_storage03.png
14. gcc\_storage06.png
15. gcc\_create\_image01.png
16. browse\_img.png
17. gcc\_create\_image03.png
18. gcc\_prim\_fw01.png
19. create\_inst.png
20. boot\_disk.png
21. gcc\_prim.png
22. adv\_net.png
23. gcc\_prim\_fw\_08.png
24. gcc\_secondary\_fw\_01.png
25. gcc\_secondary\_fw\_02.png
26. sec\_inst.png
27. adv\_net.png
28. gcc\_secondary\_fw\_04.png
29. gce\_routes\_01.png
30. create\_route.png
31. direct\_attached\_route1.png
32. direct\_attached\_route2.png
33. gw\_route.png
34. gce\_no\_icmp\_gateway\_monitoring\_01.png
35. gce\_no\_icmp\_gateway\_monitoring\_02.png
36. gce\_static\_mip\_01.png
37. mip\_ha\_google\_cloud.png
38. add\_route2.png
39. default\_route.png
40. mip\_google\_ha.png
41. gce\_dha\_02.png

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.