

How to Deploy a CloudGen Firewall with Multiple NICs in Google Cloud Using the Command Line

<https://campus.barracuda.com/doc/96026623/>

In some scenarios, an instance with multiple network interfaces in multiple VPC networks is required. Add the required number of network interfaces during deployment. The primary network interface is configured automatically; the additional network interfaces must be added manually to the CloudGen Firewall configuration. In Google Launcher, only the latest version is visible. The additional network interfaces must be added in the firewall configuration after deployment. The CloudGen Firewall images are available in the Google Cloud Launcher. These images can be deployed with the gcloud command-line tool included in the Google Cloud SDK.

- **Image project** - barracuda-release
- **Images available** - cudangfbyol-v711-056-hf843-hf844-20170926, cudangfbyol-v703-087-20170804, cudangfbyol-v710-371-20170804

Before You Begin

- Install the Google Cloud SDK. Alternatively, you can also use Google Cloud Shell.
- Gather information needed for deployment:
 - Name of the VPC network you plan to deploy to
 - Name of the subnet you plan to deploy to
 - Private IP address you want to assign to the new CGF instance
 - Availability zone you will deploy to

Step 1. Deploying a Multi-NIC Firewall Instance

To create an instance with multiple network interfaces, execute the `--network-interface` argument for each NIC, without adding IP addresses to avoid assigning public to each NIC.

```
gcloud compute instances create my-first-ngfirewall \
  --image-family barracuda-nextgen-firewall-f-series \
  --image-project barracuda-release \
  --project my-project \
  --machine-type n1-standard-1 \
  --network-interface network=default,subnet=default,private-network-
ip=10.128.0.10 \
  --network-interface no-address,network=second-vpc,subnet=default,private-
network-ip=10.129.0.20 \
  --can-ip-forward \
```

```
--tags ngfw \  
--zone us-central1-b
```

Step 2. Configure Additional Network Interfaces on the Firewall

Step 2.1 Add the Network Interfaces to the Firewall

Define the number of interfaces attached to the instance.

1. Go to **CONFIGURATION > Configuration Tree > Box > Network**.
2. Click **Lock**.
3. In the left menu, select **Interfaces**.
4. Double-click the entry in **Network Interface Cards**. The **Network Interface Configuration** window opens.
5. Change the **Number of Interfaces** to the number of interfaces attached to the firewall.
6. Click **Send Changes** and **Activate**.

Step 2.2. Add Routes for Each Network Interface

Add two directly attached routes and a gateway route for each network interface.

1. Go to **CONFIGURATION > Configuration Tree > Box > Network**.
2. Click **Lock**.
3. In the left menu, select **Routing**.
4. In the left menu, expand the **Configuration Mode** section and click **Switch to Advanced View**.
5. Create a new **directly attached route** for the 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 **Unclassified**.

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="Unclassified"/>	

6. 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 **Unclassified**.

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="Unclassified"/>	

7. 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 **Unclassified**.

Route Configuration

Target Network Address	10.78.1.0/24	
Route Type	gateway	
Interface Name	eth1	<input type="checkbox"/> Other
Gateway	10.78.1.1	
Route Metric		
Source Address		
Foreign IP Sufficient	no	
Trust Level	Unclassified	

8. Click **Send Changes** and **Activate**.

Step 2.3. 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**. The 'Failsafe Activation Succeeded' message is displayed after your new network configurations have been successfully activated.

Step 2.4. Add the IP Addresses as Box IPs

1. Go to **CONFIGURATION > Configuration Tree > Box > Network**.
2. In the left menu, select **IP Configuration**.
3. Click **Lock**.
4. In the **Additional IPv4 Addresses** table, add the private IP addresses.
5. Click **Send Changes** and **Activate**.

Next Steps

Verify that all client instances are routed via the CloudGen Firewall and that the Google firewall does not block any connections.

Figures

1. multinic_gce_01.png
2. multinic_gce_02.png
3. multinic_gce_03.png

© Barracuda Networks Inc., 2024 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.