How to Manually Upload and Deploy the F-Series Firewall in the Google Cloud

https://campus.barracuda.com/doc/53248285/

You can deploy the Barracuda NextGen Firewall F-Series to the Google Cloud as a gateway or remote connectivity device. The firewall is deployed into a dedicated subnet (public subnet) in the Google Cloud network, and the instances for your cloud-based applications are deployed into backend or private subnets of the network. Each subnet is automatically assigned a dedicated gateway IP address and default route that allow the instances to connect to the Internet via the default Google Cloud gateway. An additional tag-based Google Cloud route is introduced to use the firewall as the default gateway. This route is applied automatically to all backend instances with this tag. Google Cloud firewall rules must be created to allow traffic between the firewall and the backend instances, as well as from the Internet to the firewall. By default, the Google Cloud firewall blocks all traffic, even between two instances in a subnet. The firewall has only a single dhcp network interface with a private IP address. Assign a static or ephemeral (dynamic) external IP address to your firewall to be able to connect to the Google Cloud network, even from outside the network.

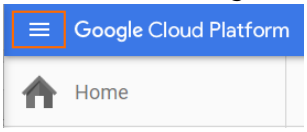
Before you begin

- Google Cloud account is required.
- Download the Google Cloud firewall image from the Barracuda Download portal.

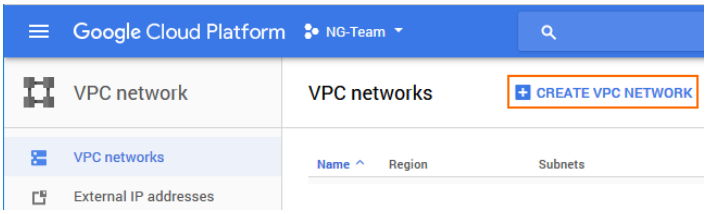
Step 1. Create a network in the Google Cloud

Create the virtual network you are deploying your firewall to.

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

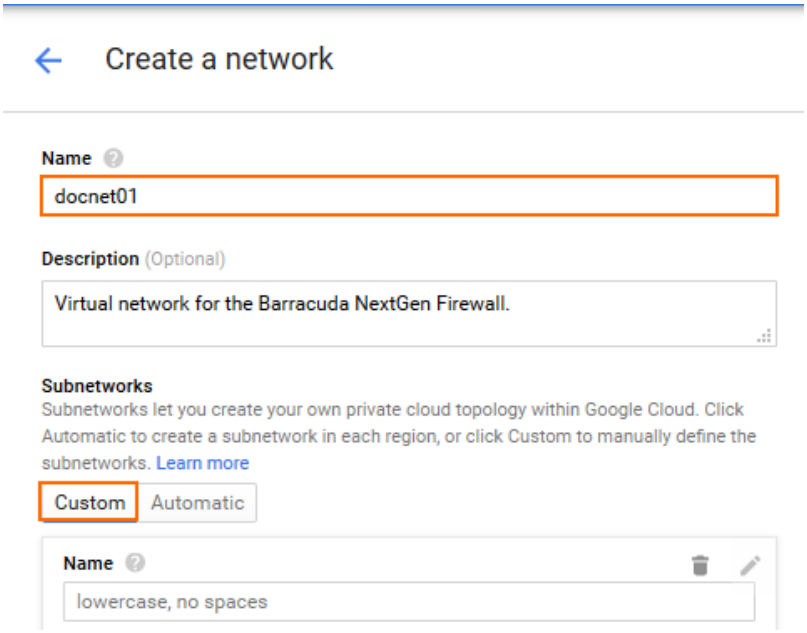


3. In the **Networking** section, click **VPC Network**.
4. In the main area, click **Create Network**.

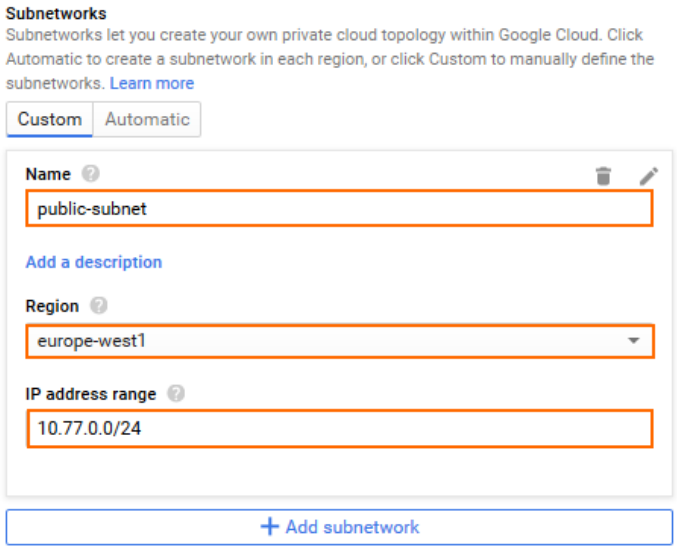


5. Enter the **Name**.

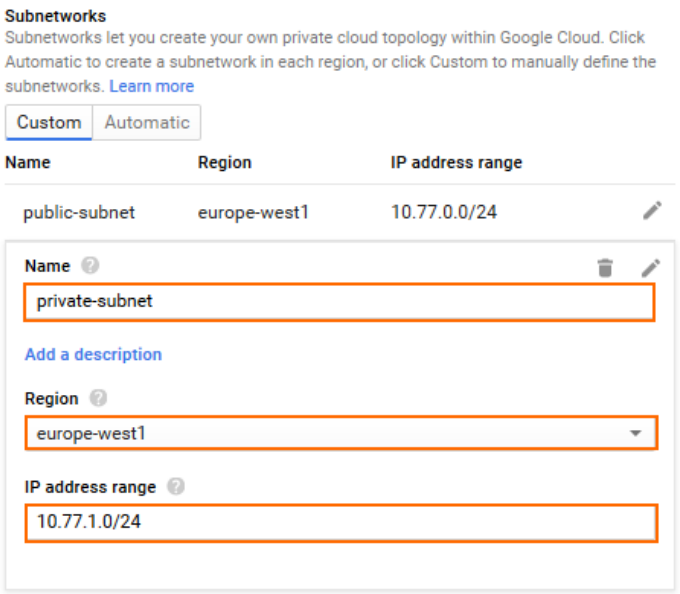
6. In the **Subnetworks** section, click **Custom**.



7. Create the public subnet:
   - **Name** – Enter **public-subnet**
   - **Region** – Select your region.
   - **IP address range** – Enter the network in CIDR format. If possible, do not use a network that overlaps with your on-premises network.

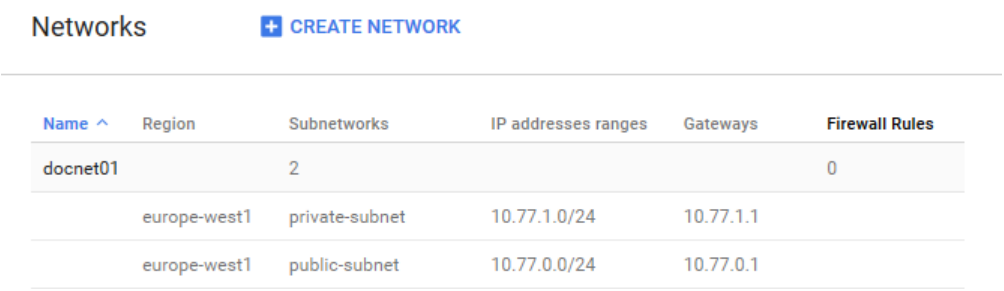


8. Click **Add subnetwork** and create the private subnet:
   - **Name** – Enter **private-subnet**
   - **Region** – Select your region.
   - **IP address range** – Enter the network in CIDR format. If possible, do not use a network that overlaps with your on-premises network.



9. Click **Create**.

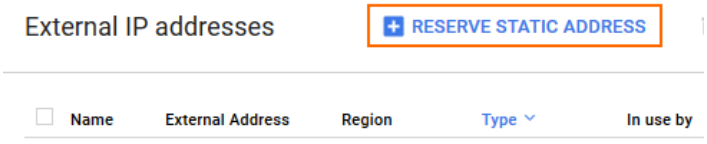
The network is now listed.



Step 2. Create an external IP address

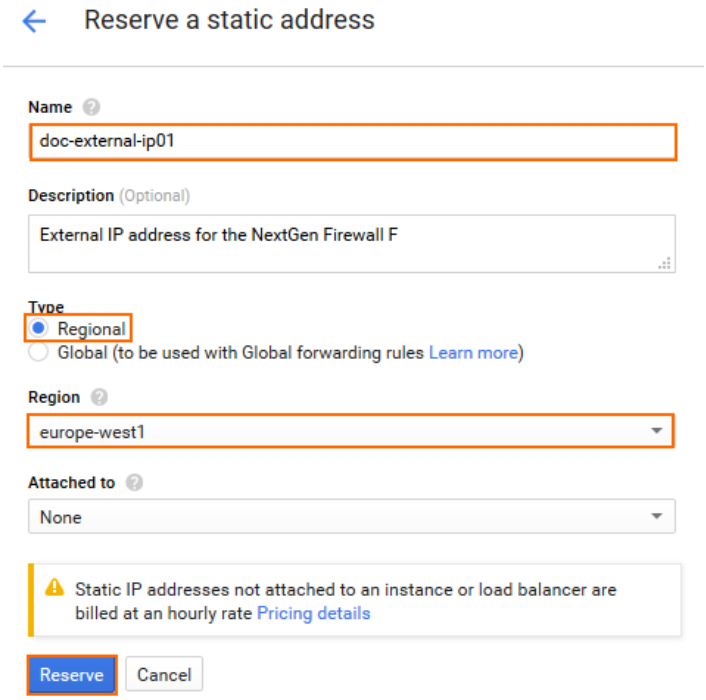
Create a static external IP address for your firewall. You can also skip this step and use an ephemeral IP address when creating the firewall instance.

1. Go to https://console.cloud.google.com.
2. Click the hamburger menu in the upper left corner.
3. In the **Networking** section, click **VPC Network**.
4. In the left menu, click **External IP addresses**.
5. In the main area, click **Reserve static address**.



6. Reserve a static address:

- **Name** – Enter a unique name for the external IP address.
- **Type** – Select **Regional**
- **Region** – Select the same region you selected for the public subnet of the network.



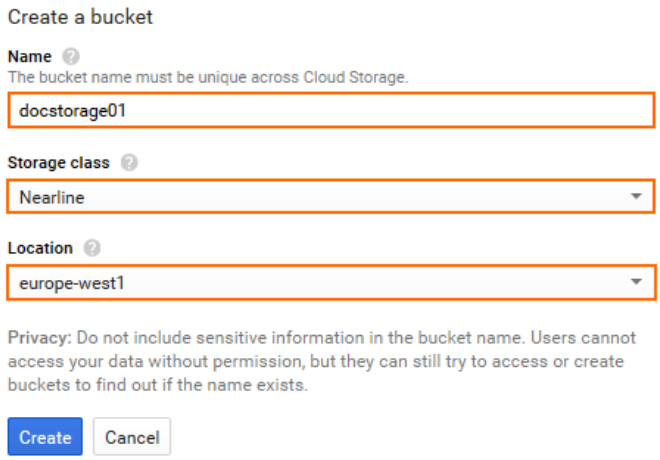
7. Click **Reserve**.

Step 3. 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 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**.

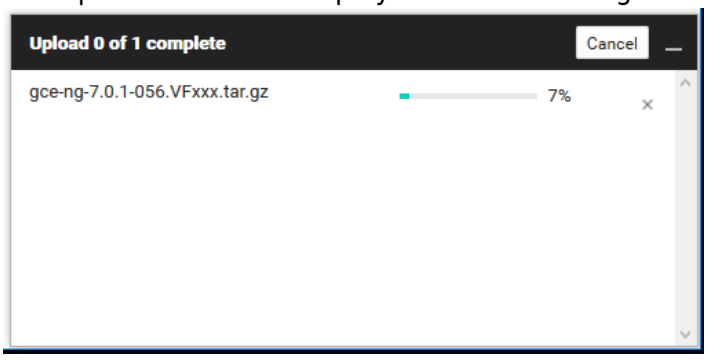
5. Create a storage bucket:
   - **Name** – Enter a unique name.
   - **Storage class** – Select a storage class depending on your preferences.
   - **Location** – Select the location matching the region you are deploying in.



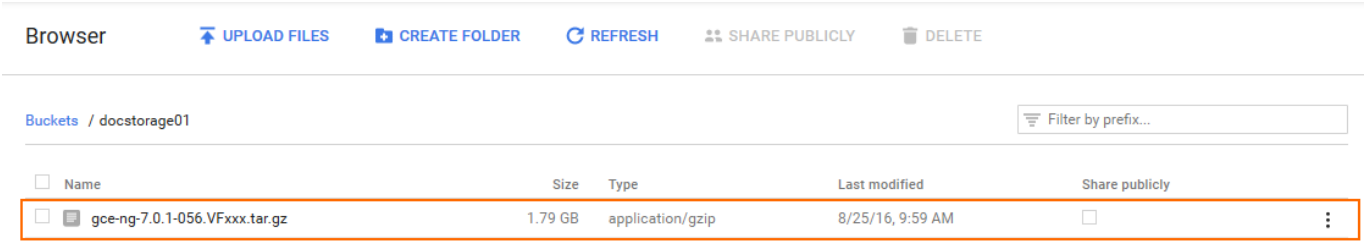
6. Click **Create**.
7. Click on the storage bucket you just created.

8. Click **Upload Files** and select the firewall image you previously downloaded from the Barracuda Download Portal.

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



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

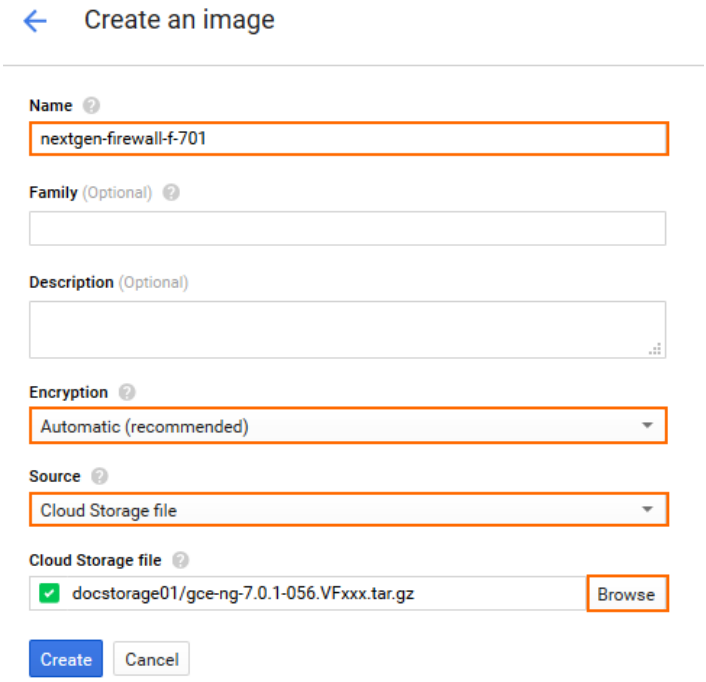


Step 4. Create a Compute Engine image from the uploaded disk image

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.

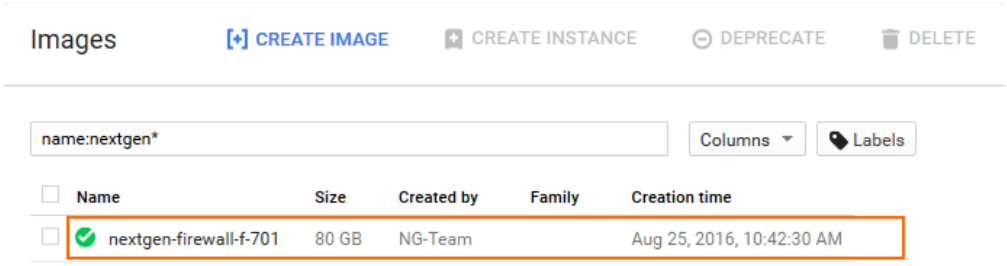
1. Go to https://console.cloud.google.com.
2. Click the hamburger menu in the upper left corner.
3. In the **Compute** section, click **Compute Engine**.
4. In the left menu, click **Images**.
5. In the main area, click **Create Images**.

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



7. Click **Create**.

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

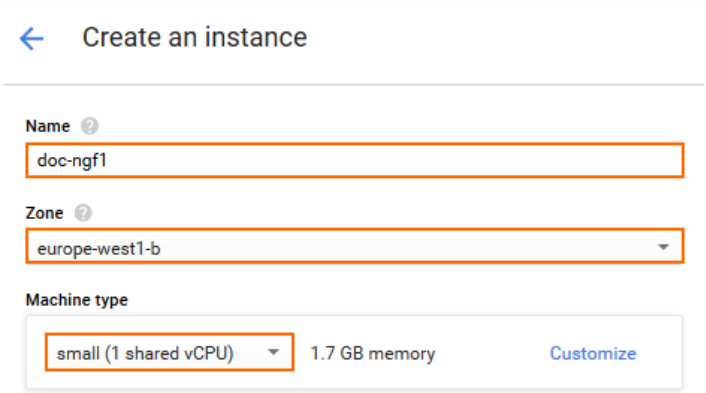


Step 5. Create the firewall instance

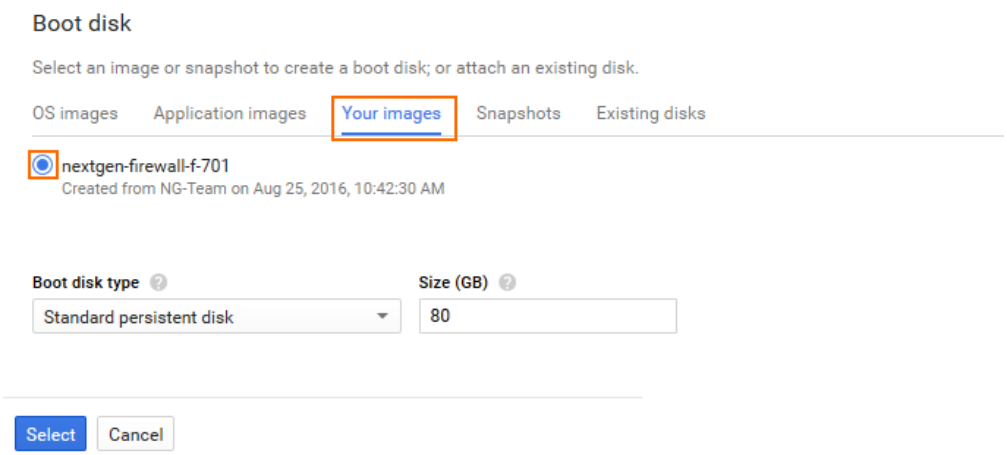
Create the firewall instance using the image created in step 4.

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**.

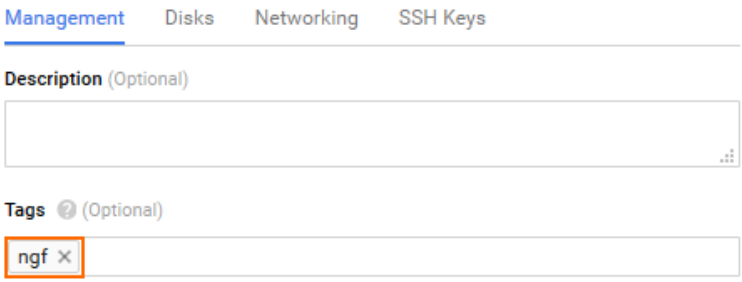
5. Enter a lowercase **Name** for the firewall instance.
   The name of the instance is set as the default password of the firewall instance.
6. Select the **Zone**. The zone must be in the same region as the public subnet in the network created in step 1.
7. Select **Machine type**. Verify that the number of vCPU matches the number of cores included in your F-Series Firewall license.



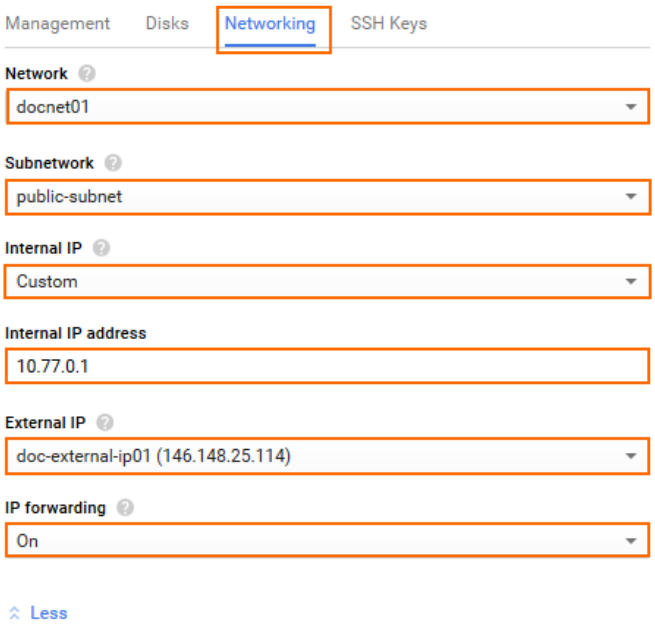
8. In the **Boot disk** section, click **Change**.
9. Click the **Your Images** tab.
10. Select the image you created in step 4.



11. Click **Select**.
12. Below the **Firewall** section, click **Management, disk, networking, SSH keys**.
13. Click on the **Management** tab, enter a **Tag** for the firewall, and press **ENTER**. This tag is later used to identify the firewall instance in the Google Cloud firewall rules and routes.



14. Click on the **Networking** tab and configure the following networking settings:
    - **Network** – Select the network created in step 1.
    - **Subnetwork** – Select the public subnet created in step 1.
    - **(optional) Internal IP** – To use a specific static internal IP address, select **Custom**.
    - **(Custom internal IP address only) Internal IP address** – Enter a free IP address in the public subnet. The first IP address in the subnet is reserved for the gateway.
    - **External IP** – Select the external IP address created in step 2, or else select **Ephemeral** to use a dynamic public IP address.
    - **IP forwarding** – Select **On.**



15. Click **Create**.

Step 6. (optional) Create instances in the private subnet

Deploy an instance into the private subnet. The backend instances must be tagged to be able to assign routes and firewall rules to them. Do not assign a public IP address to the backend instances.

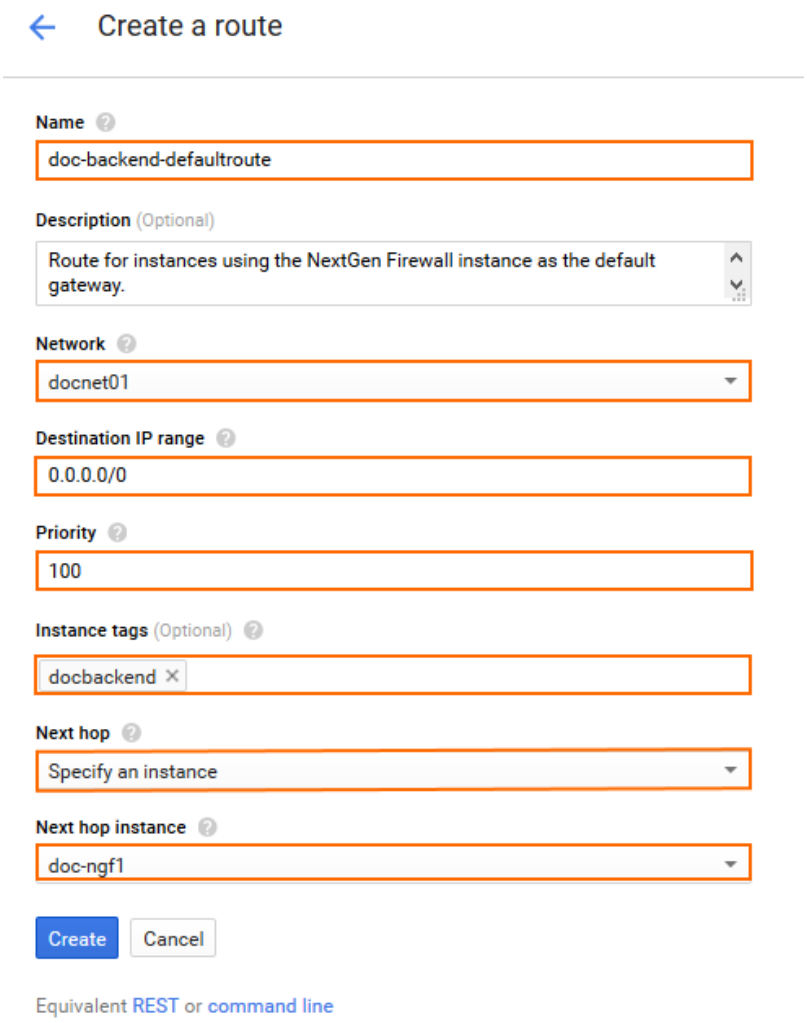
Step 7. Create default route for backend instances

A default route for each subnet with a metric of 1000 is created for each subnet. For the backend instances to use the firewall as the default gateway, create a default route with a metric lower than 1000. Configure the firewall instance as the next-hop, and add the tags identifying the backend instances. The route is automatically applied to all instances with the same tags as listed in the route.

1. Go to https://console.cloud.google.com.
2. Click the hamburger menu in the upper left corner.
3. In the **Networking** section, click **VPC Network**.
4. In the left menu, click **Routes**.

5. Click **Create route** to create the default route for the backend instances:
   - **Name** – Enter a name for the route.
   - **Network** – Select the network created in step 1.
   - **Destination IP range** – Enter `0.0.0.0/0`.

- **Priority** – Enter a priority lower than 1000. If two routes for the same destination exist, the route with the lower priority is used.
- **Instance tags** – Enter the tags used for each instance that should be routed over the NextGen Firewall.
- **Next hop** – Select **Specify and instance**.
- **Next hop instance** – Select the firewall instance created in step 4 from the list.



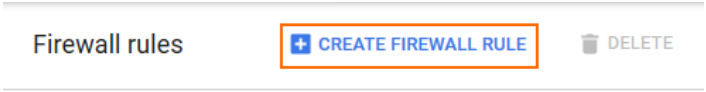
6. Click **Create**.

Step 8. Create a Google Cloud firewall rule

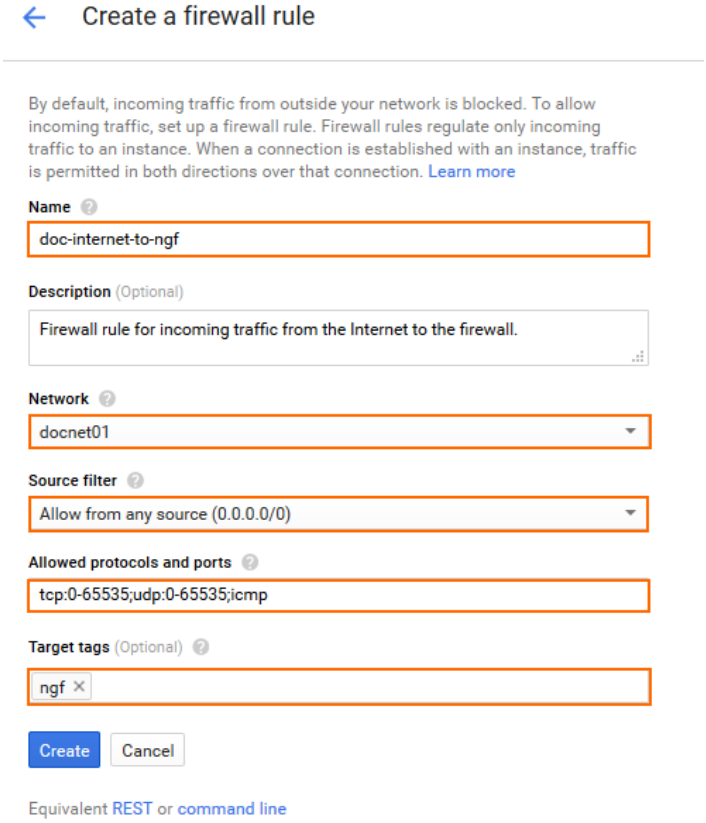
Create firewall rules to allow traffic into your virtual network and from the firewall to the backend instances. By default, all traffic is blocked.

1. Go to https://console.cloud.google.com.
2. Click the hamburger menu in the upper left corner.
3. In the **Networking** section, click **VPC Network**.
4. In the left menu, click **Firewall rules**.

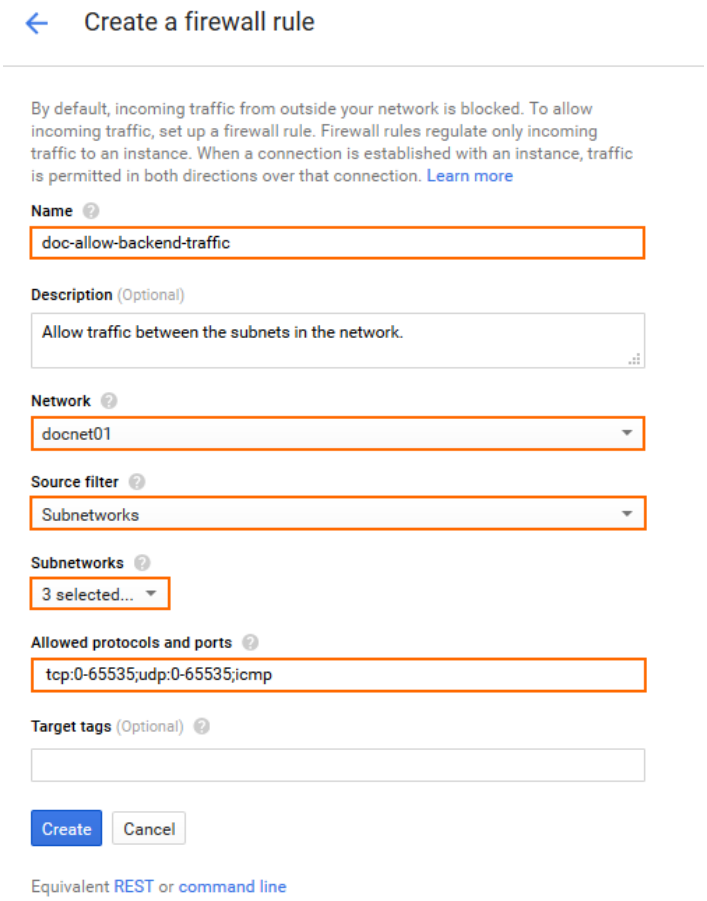
5. In the main area, click **Create firewall rule**.



6. Create a firewall rule to allow incoming traffic to your firewall Instances:
   - **Name** – Enter the firewall rule name.
   - **Network** – Select the network created in step 1.
   - **Source filter** – Select **Allow from any source (0.0.0.0/0)**.
   - **Allowed protocols and ports** – Enter a semicolon-delimited, lower-case list of protocols and ports in the following format. tcp:807 is required to be able to connect via NextGen Admin. E.g., Use `tcp:0-65535;udp:0-65535;icmp` to allow all TCP, UDP, and ICMP traffic to the firewall.
   - **Target tags** – Enter the tag assigned to the firewall in step 3.



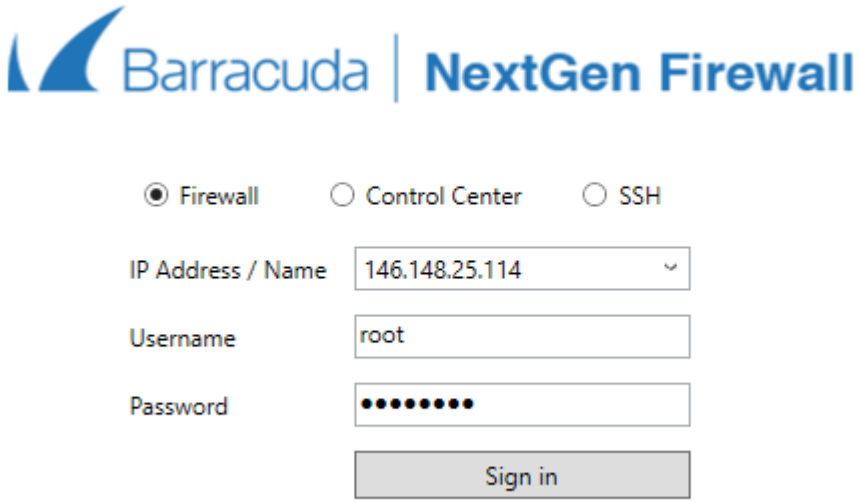
7. Create a firewall rule to allow all traffic from selected subnets to the firewall:
   - **Name** – Enter the firewall rule name.
   - **Network** – Select the network created in step 1.
   - **Source filter** – Select **Subnetworks**.
   - **Subnetworks** – Select the public subnet and all private subnets with instances that are using the firewall as the default gateway.
   - **Allowed protocols and ports** – Enter a semicolon-delimited, lower-case list of protocols and ports. E.g., `tcp:0-65535;udp:0-65535;icmp` to allow all TCP, UDP, and ICMP traffic between instances in these subnets.



8. Click **Create**.

You can now log in to your firewall instance running in the Google Cloud using NextGen Admin:

- **IP address** – Enter the external IP address created in step 2.
- **User** – Enter `root`
- **Password** – Enter the instance **Name**.



Serial console

The Google Cloud Platform allows to to enable and connect to the serial port of your firewall instance. This feature allows you to troubleshoot your F-Series Firewall in case of a misconfiguration in a web-based serial console.

For more information, see How to Access the Serial Console on the F-Series Firewall in the Google Cloud.

Next steps

- You can now license and start using your firewall. For more information, see Getting Started.

Figures