Configuring firewall rules

This page provides guidance for configuring Google Cloud firewall rules and your peer (https://cloud.google.com/vpn/docs/concepts/overview#peer-definition) network firewall rules.

When you configure Cloud VPN tunnels to connect to your peer network, you should review and modify firewall rules in both the Google Cloud and peer networks to make sure that they meet your needs. If your peer network is another Virtual Private Cloud network, then you configure Google Cloud firewall rules for both sides of the network connection.

Note: If your Cloud VPN tunnel uses dynamic (BGP) routing (https://cloud.google.com/vpn/docs/concepts/choosing-networks-routing#dynamic-routing), make sure you allow BGP traffic (#dynamic-rules) so that route information can be exchanged.

Google Cloud firewall rules

The implied allow egress (https://cloud.google.com/vpc/docs/firewalls#default_firewall_rules) rule allows instances and other resources in your Google Cloud network to make outgoing requests and receive established responses, but the implied deny ingress (https://cloud.google.com/vpc/docs/firewalls#default_firewall_rules) rule blocks all incoming traffic to your Google Cloud resources.

At minimum, you need to create firewall rules to allow ingress traffic from your peer network to Google Cloud. You may also need to create egress rules if you have created other egress rules to *deny* certain types of traffic.

You might want to configure a range broad enough to cover future IP address space if you add more subnets or expand existing ones in your VPC network.

If you are not familiar with how firewall rules work in Google Cloud, refer to the Firewalls Rules Overview (https://cloud.google.com/vpc/docs/firewalls) first.

Permissions required for this task

To perform this task, you must have been granted the following permissions **OR** the following IAM roles.

Roles

- `roles/compute.securityAdmin` (https://cloud.google.com/compute/docs/access/iam#compute.securityAdmin)

Example configurations

For multiple examples of restricting ingress or egress traffic, refer to the firewall configuration examples (https://cloud.google.com/vpc/docs/using-firewalls#configuration_examples) in the VPC documentation.

The following example creates a firewall rule that allows *all incoming TCP, UDP, and ICMP* traffic from your peer network to your Google Cloud network.

CONSOLE GCLOUD

1. Go to the VPN tunnels page in the Google Cloud Console.
   GO TO THE VPN TUNNELS PAGE (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/VPN/LIST?TAB=TUNNE
2. Click the VPN tunnel that you want to use.
3. In the VPN gateway section, click the name of VPC network. This directs you to the VPC network details page that contains the tunnel.
4. Select the **Firewall rules** tab.
5. Click **Add firewall rule**. Add a rule for TCP, UDP, and ICMP:
   - Name: `allow-tcp-udp-icmp`
   - Source filter: IP ranges.

- Source IP ranges: **Remote Network IP Range** value from when you created the tunnel. If you have more than one peer network range, enter each one. Press the **Tab** key between entries.
- Allowed protocols or ports: `tcp; udp; icmp`
- Target tags: Any valid tag or tags.

6. Click **Create**.
7. Create other firewall rules if necessary.

Alternatively, you can create rules from the Firewall rules page in the Google Cloud console.

1. Go to the FIREWALL RULES PAGE (HTTPS://CONSOLE.CLOUD.GOOGLE.COM/NETWORKING/FIREWALLS) page.
2. Click **Create firewall rule**.
3. Populate the following fields:
   - **Name:** `vpnrule1`
   - **VPC network:** `my-network`
   - **Source filter:** `IP ranges`.
   - **Source IP ranges:** The peer network's IP address ranges to accept from the peer VPN gateway.
   - **Allowed protocols and ports:** `tcp;udp;icmp`
4. Click **Create**.

Peer firewall rules

When configuring your peer firewall rules, consider the following:

- You should configure rules to allow egress and ingress traffic to and from the IP ranges used by the subnets in your Google Cloud network.
- You may choose to permit all protocols and ports, or you may restrict traffic to only the necessary set of protocols and ports to meet your needs.
- You must allow `ICMP` traffic if you need to be able to communicate among peer systems and instances or resources in Google Cloud using `ping`.
- Remember that on-premise firewall rules can be implemented by both your network devices (for example, security appliances, firewall devices, switches, routers, and

gateways) and in software running on your systems (such as firewall software included with an operating system). All firewalls “in the way” to Google Cloud must be configured appropriately to allow traffic.

- If your VPN tunnel uses dynamic (BGP) routing, make sure that you allow BGP traffic for the link-local IP addresses. Refer to the next section for more details.

Considerations for dynamic routing

Dynamic (BGP) routing exchanges route information using TCP port 179. Some VPN gateways allow this traffic automatically when you choose dynamic routing. If your gateway does not, you must configure it to allow incoming and outgoing traffic on TCP 179. All BGP IP addresses use the link-local `169.254.0.0/16` CIDR block.

If your peer VPN gateway is not directly connected to the Internet, make sure that it and peer routers, firewalls, and security appliances are configured to at least pass BGP traffic (TCP port 179) and ICMP traffic to your VPN gateway. ICMP is not required, but is useful to test connectivity between a Cloud Router and your VPN gateway. The range of IP addresses to which your peer firewall rule should apply must include the BGP IP address of the Cloud Router and the BGP IP address of your gateway.

What's next

- Learn about the basic concepts of Cloud VPN (https://cloud.google.com/vpn/docs/concepts/overview)
- See Advanced Configurations (https://cloud.google.com/vpn/docs/concepts/advanced) for information on high-availability, high-throughput scenarios, or multiple subnet scenarios.
- Create a custom Virtual Private Cloud network (https://cloud.google.com/vpc/docs/using-vpc#create-custom-network)
- Set up different types of Cloud VPN (https://cloud.google.com/vpn/docs/how-to/choosing-a-vpn)
- Maintain VPN tunnels and gateways (https://cloud.google.com/vpn/docs/how-to/maintaining-vpns)
- View logs and monitoring metrics (https://cloud.google.com/vpn/docs/how-to/viewing-logs-metrics)

- Get troubleshooting help (https://cloud.google.com/vpn/docs/support/troubleshooting)

Previous
← Creating Google Cloud to Google Cloud HA VPN gateways
(https://cloud.google.com/vpn/docs/how-to/creating-ha-vpn2)

Next
Configuring the peer VPN gateway →
(https://cloud.google.com/vpn/docs/how-to/configuring-peer-gateway)

Last updated December 4, 2019.