GOOGLE CLOUD PLATFORM

ROUTES AND FIREWALLS

FIREWALL RULES

- When you create a GCP firewall rule, you specify a VPC network and a set of components that define what the rule will do.
- The components enable you to target certain types of traffic, based on the traffic's protocol, ports, sources, and destinations.
- While firewall rules are defined at the network level, connections are allowed or denied on a per-instance basis.
- GCP firewall rules exist not only between your instances and other networks, but between individual instances within the same network.
- Every network has two implied firewall rules which permit outgoing connections and block incoming connections.

FIREWALL RULES

- Each firewall rule's action is either allow or deny. The rule applies to traffic as long as it is enforced.
- Each firewall rule applies to incoming (ingress) or outgoing (egress) traffic, not both.
- GCP firewall rules are stateful - firewall rules allow bidirectional communication once a session is established
- The maximum number of tracked connections in the firewall rule table depends on the number of stateful connections – 130k/vCPU
- **Always blocked traffic** GRE traffic, Protocols other than TCP, UDP, ICMP, and IPIP, Egress traffic on TCP port 25 (SMTP)
- **Always allowed traffic** DHCP, DNS resolution, instance metadata, NTP

FIREWALL RULE COMPONENTS

Priority: Integer from 0 to 65535, inclusive; default 1000

Action: Either allow or deny

Enforcement: Either enabled (default) or disabled

Target: The target parameter specifies the source/destination. Instances in the VPC network/service accounts/network tag

Source/destination: Any network or a specific range of IPv4 addresses; default is any (0.0.0.0/0).

Protocols and Ports: The protocol (such as TCP, UDP, or ICMP) and port

DEMO: LISTING FIREWALL RULES

Listing firewall rules for a VPC network

1. Go to the VPC networks page in the Google Cloud Platform Console.
2. Click the **Name** of a VPC network to go to its details page.
3. On the details page for the network, click the **Firewall rules** tab.

Listing firewall rules for a network interface of a VM instance

1. Go to the VM instances page in the Google Cloud Platform Console and find the instance to view.
2. In the instance's **more actions** menu (), select **View network details**.
3. If an instance has multiple network interfaces, select the network interface to view in the **Network interface details** section.
4. Click the **Firewall rules** tab to see all the rules that apply to the network interface, sorted by rule name.

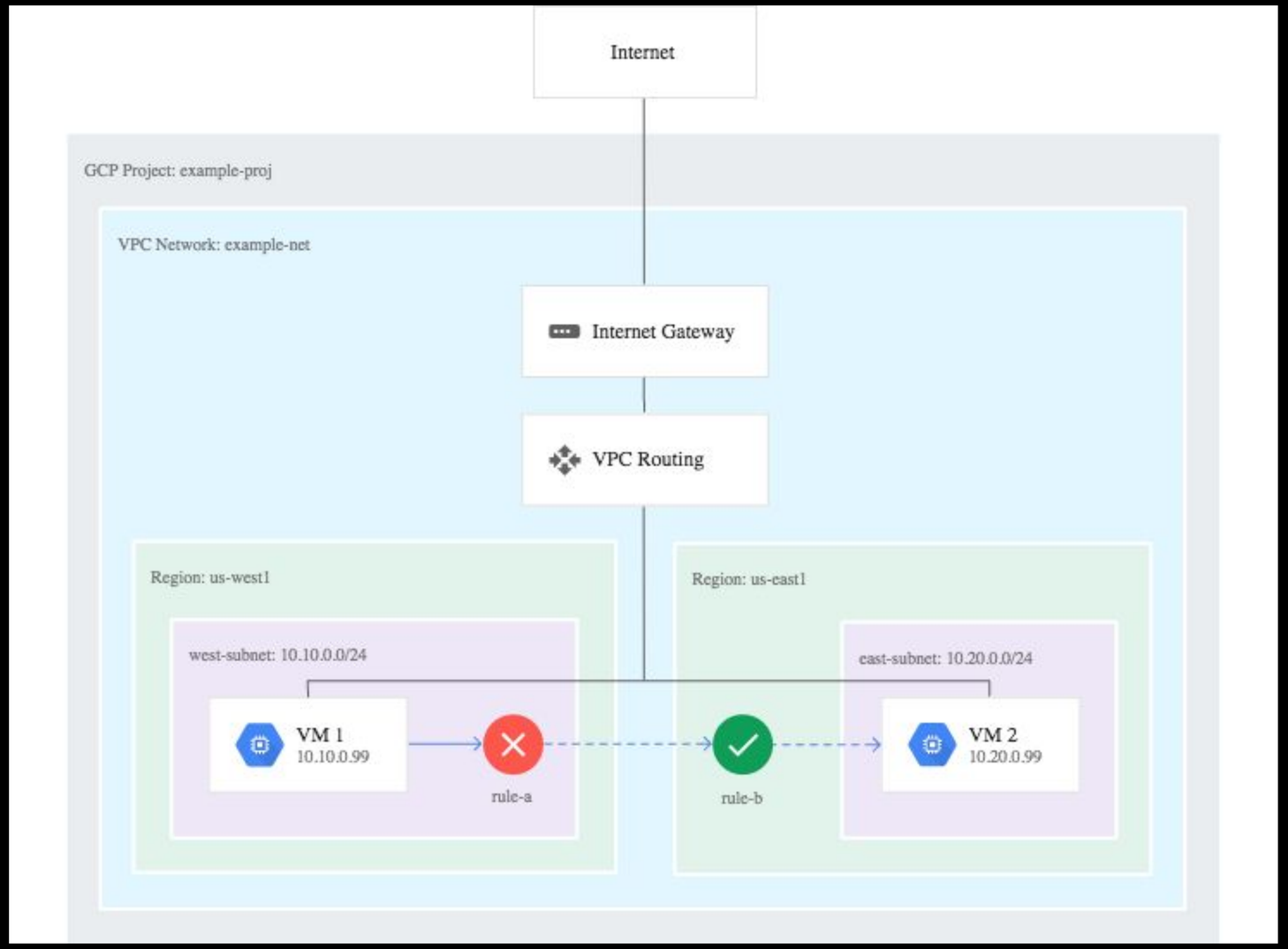
DEMO: CREATING FIREWALL RULES

1. Go to the Firewall rules page in the Google Cloud Platform Console
2. Click Create firewall rule
3. Enter a Name for the firewall rule
4. This name must be unique for the project
5. Specify the Network where the firewall rule will be implemented
6. Specify the Priority of the rule
7. The lower the number, the higher the priority
8. For the Direction of traffic, choose ingress or egress
9. For the Action on match, choose allow or deny
10. Specify the Targets of the rule
11. For an ingress rule, specify the Source filter
12. For an egress rule, specify the Destination filter
13. Define the Protocols and ports to which the rule will apply
14. Click Create.

FIREWALL RULES LOGGING

- *Firewall Rules Logging* allows you to audit, verify, and analyze the effects of your firewall rules.
- You can only enable firewall rule logging for rules in a VPC network and for TCP and UDP connections.
- You **cannot** enable firewall rule logging for the implied deny ingress and implied allow egress rules or for automatically-created default rules in the default network
- Connection logging limits are expressed as a maximum number of connections that can be logged in a five second interval – 500/vCPU

LOGGING EXAMPLE



- Rule A: An egress deny firewall rule has a target of all instances in the network, a destination of 10.20.0.99 (VM2), and applies to TCP port 80.
- Rule B: An ingress allow firewall rule has a target of all instances in the network, a source of 10.10.0.99 (VM1), and applies to TCP port 80.

FIREWALL LOG RECORD

- Suppose VM1 attempts to connect to VM2 on TCP port 80. The following firewall rules are logged:

1. A log entry for rule A from the perspective of VM1 is generated as VM1 attempts to connect to 10.20.0.99 (VM2).

2. Because rule A actually blocks the traffic, rule B is never considered, so there is no log entry for rule B from the perspective of VM2.

Field	Values
connection	src_ip=10.10.0.99, src_port=[EPHEMERAL_PORT], dest_ip=10.20.0.99, dest_port=80, protocol=tcp
disposition	DENIED
rule_details	Reference = "network:example-net/firewall:rule-a" priority = 10 action = DENY destination_range = 10.20.0.99/32 ip_port_info = tcp:80 direction = egress
instance	project_id="example-proj" instance_name=VM1 region=us-west1 zone=us-west1-a
vpc	project_id="example-proj" vpc_name=example-net subnetwork_name=west-subnet
remote_instance	project_id="example-proj" instance_name=VM2 region=us-east1 zone=us-east1-a
remote_vpc	project_id="example-proj" vpc_name=example-net subnetwork_name=east-subnet

ROUTING IN GCP

ROUTE TYPE	CATEGORY	DESTINATION	NEXT HOP	REMOVABLE
Default route	system-generated	0.0.0.0/0	default-internet-gateway	Yes
Subnet route	system-generated	Primary and secondary subnet IP ranges	VPC network, which forwards packets to VMs in its subnets	Subnet is deleted
Static route	custom	• IP range that does not partially or exactly overlap with any subnet IP range • IP range *broader* than a subnet IP range	• An instance by name • An instance by its IP address • A Cloud VPN tunnel	Yes
Dynamic route	custom	• IP range that does not partially or exactly overlap with any subnet IP range • IP range *broader* than a subnet IP range	IP address of the Cloud Router's BGP peer	Only by a Cloud Router if it no longer receives the route from its BGP peer

APPLICABILITY AND ORDER

Applicable routes

- System-generated routes apply to all instances in a VPC network.
- Custom static routes can apply to all instances or specific instances, depending on the tag attribute of the route.
- Dynamic routes apply to instances based on the dynamic routing mode of the VPC network – regional/global

Routing order

- Subnet routes are considered first
- If the packet does not fit in the destination for a subnet route, GCP looks for another route with the most specific destination.
- If more than one route has the same most specific destination, GCP considers the priority of the route
- If no applicable destination is found, GCP drops the packet

DEMO: INSPECT ROUTES

Listing routes for VPC networks

1. Go to the Routes page in the Google Cloud Platform Console.
   You can use the **Filter routes** text box to limit the routes shown. For example, you can type the name of a VPC network and press enter to show the routes for a specific network.
2. The **All** tab shows all types of routes. To view just custom dynamic routes, click the **Dynamic** tab

To view details for *system-generated and custom static routes*, including destinations and next hops:

1. Go to the Routes page in the Google Cloud Platform Console.
2. Click the name of a route.

DEMO: ROUTE ANALYSIS

To view the routes based on applicability and routing order, use route analysis:

1. Go to the VM instances page in the Google Cloud Platform Console and find the instance to view.
2. In the instance's **more actions** menu (), select **View network details**.
3. If an instance has multiple network interfaces, select the network interface to view in the **Network interface details** section.
4. In the **Network Analysis** section, select the **Route analysis** tab.
5. View the table, which is sorted from the most specific to least specific IP address range, to determine what route applies for a given destination range

DEMO: ADD STATIC ROUTE

1. Go to the Routes page in the Google Cloud Platform Console.
2. Click **Create route**.
3. Specify a **Name** and a **Description** for the route.
4. Select an existing **Network** where the route will apply.
5. Specify a **Destination IP range** to define the destination of the route.
6. Specify a **Priority** for the route. A priority is only used to to determine routing order if routes have equivalent destinations
7. To make the route applicable only to select instances with matching network tags, specify those in the **Instance tags** field. Leave the field blank to make the route applicable to all instances in the network.
8. Select a **Next hop** for the route:
    1. **Default internet gateway** creates a route to the Internet.
    2. **Specify an instance** allows you to select an instance by name. Traffic will be routed to that even if its IP address changes.
    3. **Specify IP address** allows you to enter an IP address of an *existing instance* in the VPC network.
    4. **Specify VPN tunnel** allows you to select an existing Cloud VPN tunnel as a next hop.
9. Click **Create**.