🔥 **What is a Firewall in GCP?**

A firewall in GCP controls the network traffic going into (**ingress**) or out of (**egress**) your Virtual Machines (VMs).

Think of it like a security guard at your house:

* "Who can come in?"
* "Who can go out?"

GCP firewalls are applied at the **VPC level**, not at the VM level, and they are **stateful** (if you allow incoming traffic, the response is automatically allowed out).

🚪 **What is an Ingress Rule?**

**Ingress rule** controls **incoming traffic** to your VM from the internet or other resources.

**Example:** You want to allow HTTP traffic (port 80) from the internet to your web server VM.

**Ingress Rule:**

* Direction: Ingress
* Source IP: 0.0.0.0/0 (anyone)
* Protocol: TCP
* Port: 80

✅ Now your website is accessible from the internet.

🧳 **What is an Egress Rule?**

**Egress rule** controls **outgoing traffic** from your VM to the internet or other systems.

**Example:** You want to allow your VM to download updates from the internet.

**Egress Rule:**

* Direction: Egress
* Destination IP: 0.0.0.0/0 (anywhere)
* Protocol: TCP
* Port: 443 (HTTPS)

✅ Now your VM can reach the internet to download updates or connect to external APIs.

🧱 **Default Firewall Rules in GCP**

When you create a default VPC, GCP also creates some default firewall rules for you:

| **Rule Name** | **Direction** | **What It Does** |
| --- | --- | --- |
| default-allow-ssh | Ingress | Allows SSH (port 22) from anywhere |
| default-allow-rdp | Ingress | Allows RDP (port 3389) from anywhere |
| default-allow-icmp | Ingress | Allows ping (ICMP) from anywhere |
| default-allow-internal | Ingress | Allows all traffic within the VPC network |
| default-allow-egress | Egress | Allows all outbound traffic from the VMs |

🔐 **How to Create Custom Firewall Rule in GCP Console**

1. Go to **VPC network** → **Firewall rules**
2. Click **Create firewall rule**
3. Enter:
   * Name
   * Direction: Ingress or Egress
   * Targets: All instances in the network / specific tags
   * Source/Destination IP
   * Protocols and ports (TCP, UDP, ICMP, etc.)
4. Click **Create**

📌 **Example: Allow ICMP (Ping) only from internal subnet**

| **Field** | **Value** |
| --- | --- |
| Direction | Ingress |
| Source IP Ranges | 10.0.0.0/24 (your subnet) |
| Protocols/Ports | ICMP |
| Action | Allow |
| Target Tags | allow-icmp (VM must have this tag) |