# Working with Firewalls and VPCs

**Janani Ravi**
CO-FOUNDER, LOONYCORN

www.loonycorn.com

# Overview

Every VPC acts as a distributed firewall

All VPCs have two implied firewall rules

Auto mode VPCs have additional rules that are pre-created

Users can add and configure firewall rules and routes

# Firewall Rules

# Google VPC a.k.a. “Network”

A VPC network, often just called a network, is a global, private, isolated virtual network partition that provides managed network functionality on the GCP

# Google VPC a.k.a. “Network”

A VPC network, often just called a network, is a global, private, isolated virtual network partition that provides managed network functionality on the GCP

- Firewall rules restrict and regulate network traffic flows in a VPC

# Google VPC a.k.a. “Network”

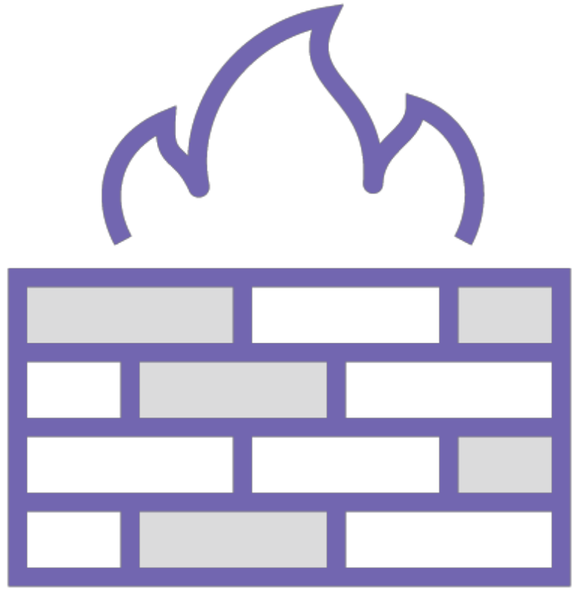
A VPC network, often just called a network, is a global, private, isolated virtual network partition that provides managed network functionality on the GCP

Under the hood, Google is routing traffic - that’s how VPCs can be global

# Google VPC a.k.a. “Network”

A VPC network, often just called a network, is a global, private, isolated virtual network partition that provides managed network functionality on the GCP

Routes, firewall rules, tags, IP addresses are all managed by the platform



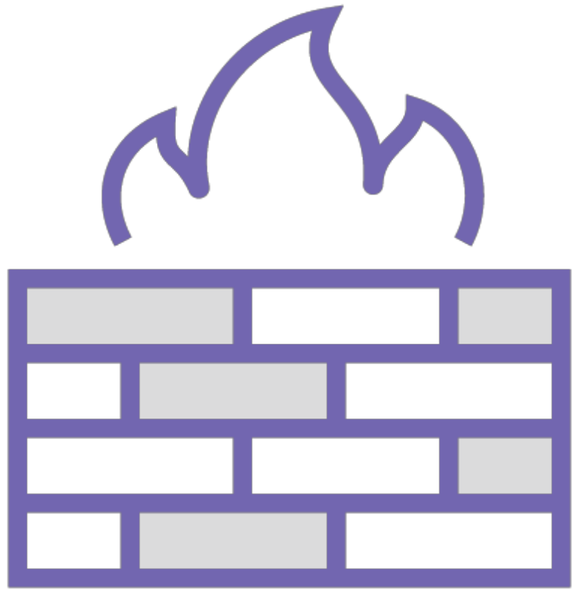
# Firewall Rules

**Every VPC is a distributed firewall**

**Firewall rules defined in VPC**

**Are applied on per-instance basis**

**Can also regulate internal traffic**



# Firewall Rules

**Every VPC has two permanent rules**

- Implied allow egress
- Implied deny ingress

**Can be overridden by more specific rules**

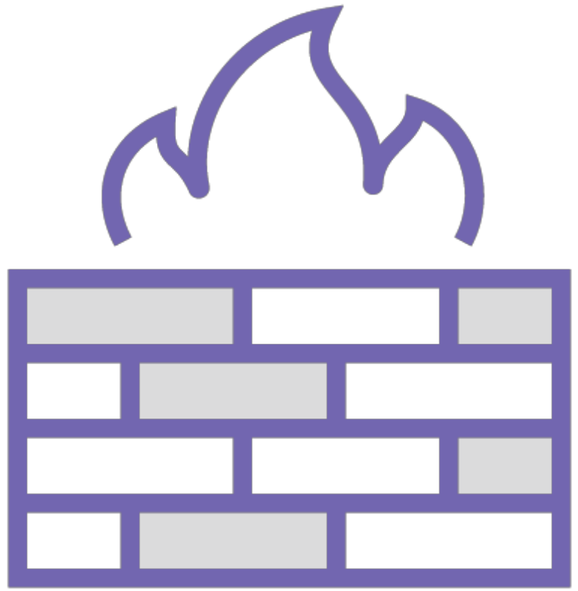
**In addition, default VPC has several rules**

# Always-blocked Traffic

**Protocols other than TCP, UDP, ICMP and IPIP**

**Egress traffic on TCP port 25 (SMTP)**

**Can not be unblocked by firewall rule**



# Firewall Rules

**Every firewall rule has several components**

- Priority (0 highest, 65535 lowest)
- Direction (ingress/egress)
- Action (allow/deny)
- Target
- Source or destination
- Protocol and port
- Enforcement status (enabled/disabled)


# Priority

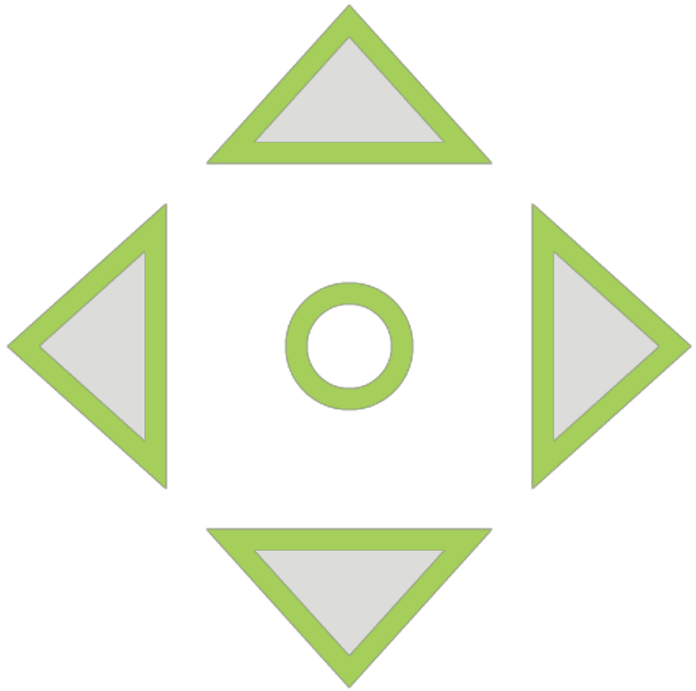
Integer from 0 to 65535 (inclusive)

Lower integer ~ higher priority

Used to resolve rule conflicts

Highest priority rule applicable to target wins

Specificity does not matter



# Direction

**Always defined from perspective of target**

- Ingress: Traffic coming into target from some source
- Egress: Traffic sent out by target to some destination

# Action

**Action to be taken when match found**

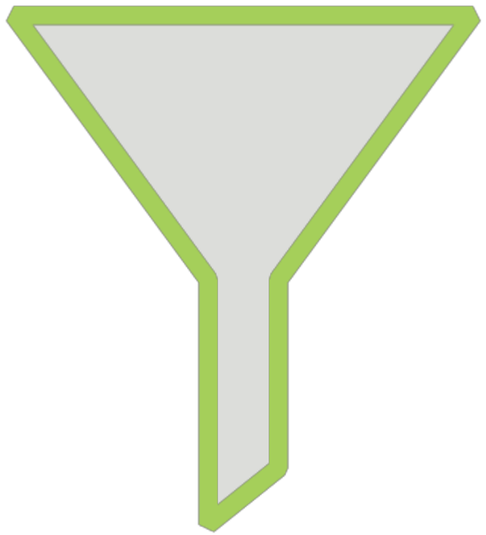
- Allow: Permit connection
- Deny: Block connection

**Rule can only specify one action**

# Target

**Three possible specifications**

- All instances in network
- Instances by target tag
- Instances by target service account



# Source or Destination Filter

**Can specify exactly one (not both)**

**For ingress rules: specify source**

**For egress rules: specify destination**

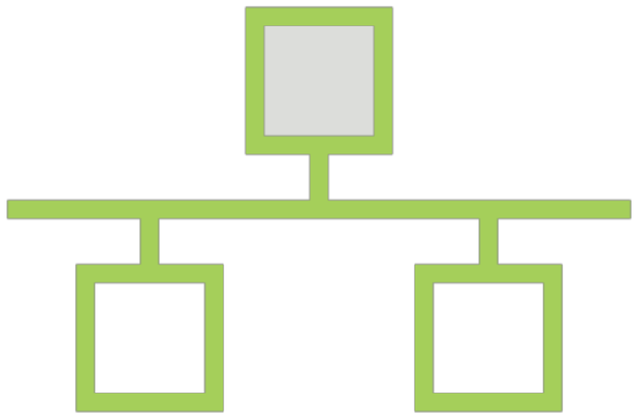
# Sources

- Any IP (0.0.0.0/0)
- Source IP ranges
- Source tags
- Source service accounts
- Some combinations

# Destination

**Any IP (0.0.0.0/0)**

**Destination IP ranges**



# Protocol and Port

**If both omitted - rule applies to all traffic**

**Protocol can be name or decimal number**

**If port omitted, applies to all ports**

**Can specify combinations**

- tcp:80
- tcp:20-22
- tcp:80; tcp:443

# Routes

# Networking Must-haves

| Objective | GCP Solution |
| --- | --- |
| Resources within a project need to communicate | Internal IP addresses |
| Resources on GCP need to communicate with outside world | External IP addresses |
| Traffic sent to an IP address needs to reach that address | Routes |
| Platform users need to be able to restrict traffic flows | Firewall rules |

# Networking Must-haves

| Objective | GCP Solution |
| --- | --- |
| Resources within a project need to communicate | Internal IP addresses |
| Resources on GCP need to communicate with outside world | External IP addresses |
| **Traffic sent to an IP address needs to reach that address** | **Routes** |
| Platform users need to be able to restrict traffic flows | Firewall rules |

# Routes

**Route: Path for network traffic**

**Can be blocked by firewall rule**

**Each VM instance has route controller**

**So knows all applicable routes**

# Routes

**Four types of routes**

- Default
- Subnet
- Static
- Dynamic

# Demo

**Creating firewall rules using the web console and the gcloud command line utility**

# Demo

**Testing the ICMP and SSH firewall rules**

# Demo

## Deleting firewall rules

# Demo

**Using network tags to apply firewall rules to specific VM instances**

# Demo

**Adding and deleting subnets in custom mode networks**

# Summary

Every VPC acts as a distributed firewall

All VPCs have two implied firewall rules

Auto mode VPCs have additional rules that are pre-created

Users can add and configure firewall rules and routes