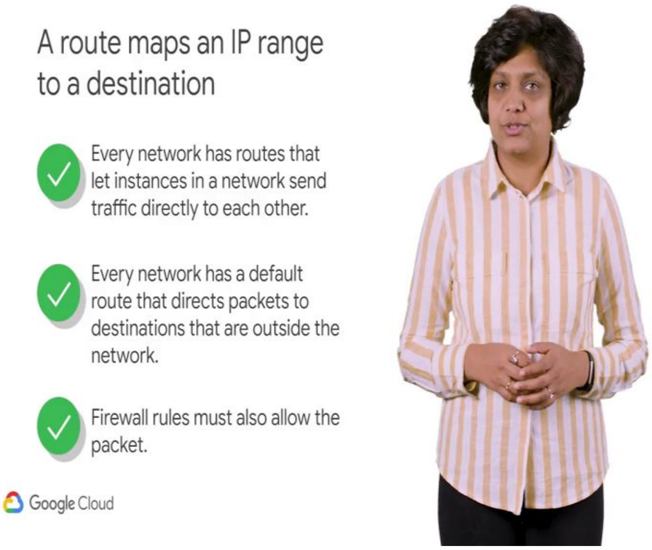
# Google Cloud Computing Foundation Course
Priyanka Vergardia
Google Cloud

## Lecture-56
## Routes and Firewall Rules in the Cloud

**(Refer Slide Time: 00:07)**



A route maps an IP range to a destination

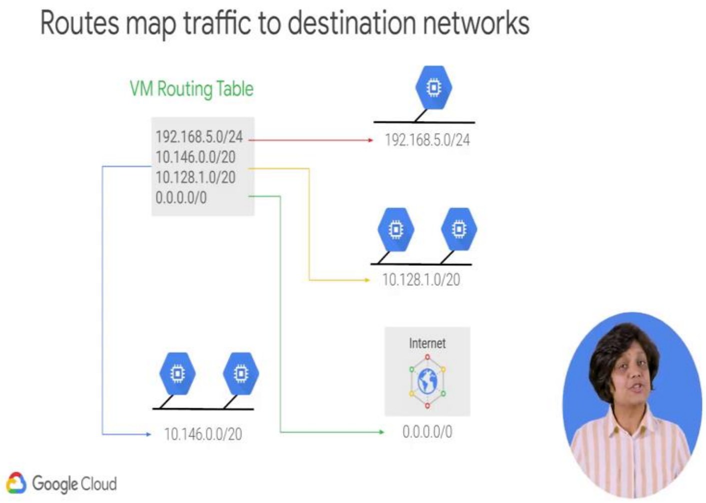
- ✓ Every network has routes that let instances in a network send traffic directly to each other.
- ✓ Every network has a default route that directs packets to destinations that are outside the network.
- ✓ Firewall rules must also allow the packet.

Google Cloud

In this topic you will consider routes and how firewall rules allow traffic to flow within a VPC. By default every Network has routes that let instances inner networks send traffic directly to each other even across subnets. In addition every network has a default route that directs packets to destinations that are outside the network. Although these routes cover most normal routing needs you can also create special routes that override these routes.

Just creating a route does not ensure that packets will be received by the specified next-hop. Firewall rules must also allow the packet. The default network has a pre-configured firewall rules that allow all instances in the network to talk with each other. Manually created networks do not have such rules. So, you must create them as you will experience in the first lab.

**(Refer Slide Time: 00:56)**


Routes map traffic to destination networks

VM Routing Table

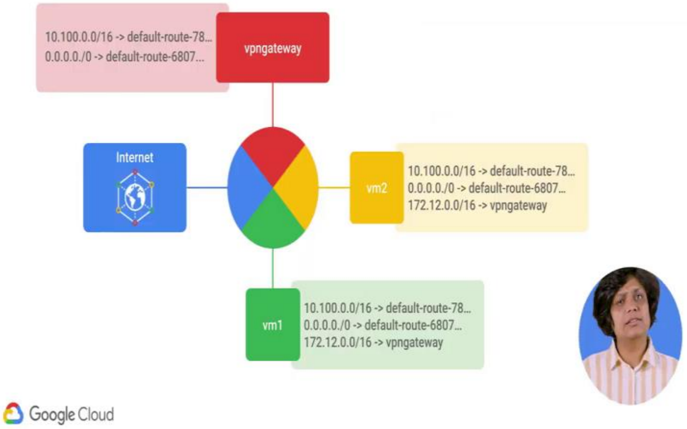
192.168.5.0/24
10.146.0.0/20
10.128.1.0/20
0.0.0.0/0

Routes match packets by destination IP addresses however no traffic will flow without also matching a firewall rule. A route is created when a network is created enabling traffic delivery from anywhere. Also a router is created when a subnet is created. This is what enables VMs on the same network to communicate. This diagram shows a simplified routing table but you will look at this in more detail next. Each route in the routes collection can apply to one or more instances a round applies to an instance if the network and instance tags match.

If the network matches and there are no instance tags specified the route applies to all instances in that network. Compute engine then uses the routes collection to create individual read-only routing tables for each instance.

**(Refer Slide Time: 01:51)**

## Instance routing tables

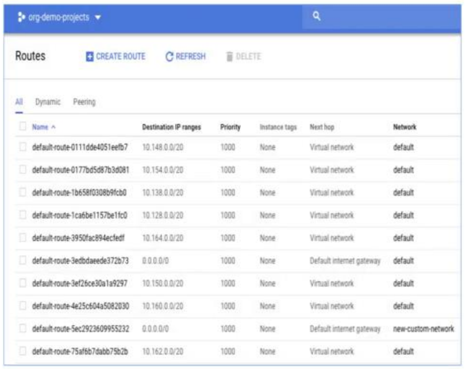

10.100.0.0/16 -> default-route-78...
0.0.0.0./0 -> default-route-6807...
vpngateway
Internet
vm2
10.100.0.0/16 -> default-route-78...
0.0.0.0./0 -> default-route-6807...
172.12.0.0/16 -> vpngateway
vm1
10.100.0.0/16 -> default-route-78...
0.0.0.0./0 -> default-route-6807...
172.12.0.0/16 -> vpngateway

Google Cloud

This diagram shows a massively scalable were sure router at the core of each network. Every virtual machine instance in the network is directly connected to this router and all packets leaving a virtual machine instance our first handled at this layer before they are forwarded to their next hub. The virtual work router selects the next hop for a packet by consulting the routing table for that instance.

**(Refer Slide Time: 02:19)**

## Routes define the paths network traffic takes from a VM instance to other destinations

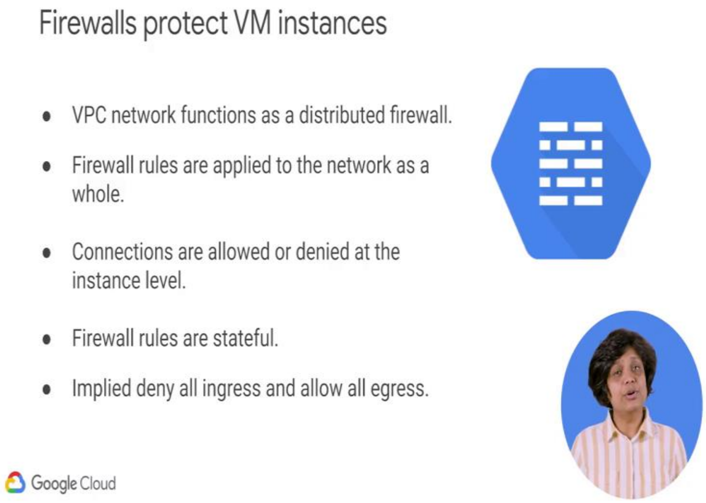


| Name ^ | Destination IP ranges | Priority | Instance tags | Next hop | Network |
|---|---|---|---|---|---|
| default-route-0111dde4051eefb7 | 10.148.0.0/20 | 1000 | None | Virtual network | default |
| default-route-0177bd5d87b3d081 | 10.154.0.0/20 | 1000 | None | Virtual network | default |
| default-route-1b658f0308b9fcb0 | 10.138.0.0/20 | 1000 | None | Virtual network | default |
| default-route-1ca6be1157be1fc0 | 10.128.0.0/20 | 1000 | None | Virtual network | default |
| default-route-3950fac894ecfedf | 10.164.0.0/20 | 1000 | None | Virtual network | default |
| default-route-3edbdaeede372b73 | 0.0.0.0/0 | 1000 | None | Default internet gateway | default |
| default-route-3ef26ce30a1a9297 | 10.150.0.0/20 | 1000 | None | Virtual network | default |
| default-route-4e25c604a5082030 | 10.160.0.0/20 | 1000 | None | Virtual network | default |
| default-route-5ec2923609955232 | 0.0.0.0/0 | 1000 | None | Default internet gateway | new-custom-network |
| default-route-75af6b7dabb75b2b | 10.162.0.0/20 | 1000 | None | Virtual network | default |

Google Cloud

Every route consists of a destination and a neck stop. Traffic whose destination IP is within the destination range is sent to the next hop for delivery.

**(Refer Slide Time: 02:30)**



Firewalls protect VM instances

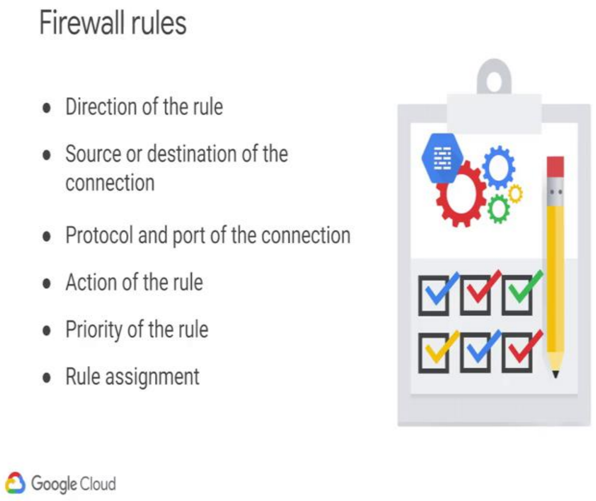
- VPC network functions as a distributed firewall.
- Firewall rules are applied to the network as a whole.
- Connections are allowed or denied at the instance level.
- Firewall rules are stateful.
- Implied deny all ingress and allow all egress.

Google Cloud

GCP firewall rules protect virtual machine instances from unapproved connections both inbound and outbound known as ingress and egress respectively. Essentially every VPC network functions as a distributed firewall. Although firewall rules are applied to the network as a whole connections are allowed or denied at the instance level. You can think of the firewall as existing not only between your instances and other networks but between individual instances within the same network.

GCP firewall rules are stateful this means that if a connection is allowed between the source and a target or a target and a destination all subsequent traffic in either direction will be allowed in other words firewall rules allow bi-directional communication once the session established. Also if for some reason all firewall rules in a network are deleted there is still an implied deny all ingress rule and an implied allow all egress rule for the network.

**(Refer Slide Time: 03:38)**



Firewall rules

- Direction of the rule
- Source or destination of the connection
- Protocol and port of the connection
- Action of the rule
- Priority of the rule
- Rule assignment

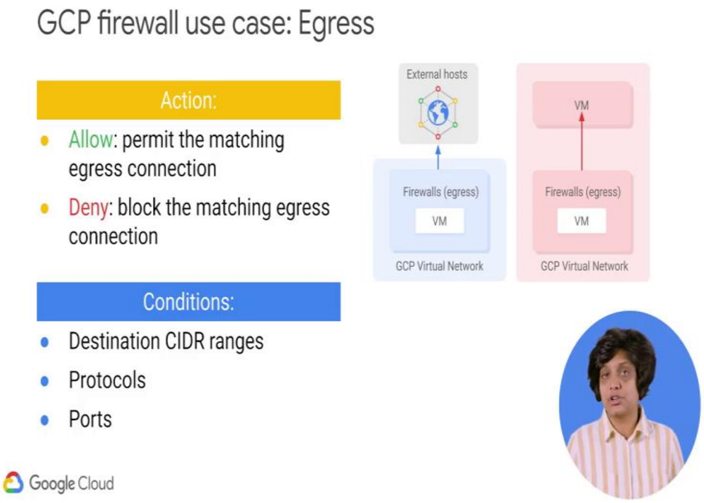
Google Cloud

You should express your desired firewall configuration as a set of firewall rules. Conceptually a firewall rule is composed of certain parameters. The direction of the rule inbound connection are matched against ingress rules only and outbound connections are matched against egress rules only. For the ingress direction sources can be specified as part of the rule with IP addresses source tags or a source service account.

For the egress direction destination can be specified as part of the rule with one or more ranges of IP addresses. The protocol and port of the connection where any rule can be restricted to apply to specific protocols only or specific company of protocols and ports only. The action of the rule which is to allow or deny packets that match the direction protocol port and source or destination of the rule the priority of the rule which governs the order in which the rules are evaluated the first matching rule is applied.

And lastly the rule assignment by default all rules are assigned to all instances but you can assign certain rules to certain instances only. Let us look at some GCP firewall use cases for both egress and ingress.

**(Refer Slide Time: 05:01)**



GCP firewall use case: Egress

Action:

- Allow: permit the matching egress connection
- Deny: block the matching egress connection

Conditions:

- Destination CIDR ranges
- Protocols
- Ports

Egress firewall rules control outgoing connections that originated inside your GCP Network. Egress allow rules allow outbound connections that match specific protocol ports and IP addresses. Egress deny rules prevent instances from initiating connections that match non-permitted port protocol and IP range combinations. For egress firewall rules destinations to which a rule applies may be specified using IP CIDR ranges.

Specifically you can use just nation range to protect from undesired connections initiated by a VM instance towards an external destination. For example an external host you can also use just nation ranges to protect from undesired connections initiated by a VM instance towards specific GCP CIDR ranges.

**(Refer Slide Time: 05:56)**

For example a VM in a specific subnet ingress firewall rules protect against incoming connections to the instance from any source. Ingress allow rules allow specific protocol ports and IP addresses to connect in. The firewall prevents instances from receiving connections on non permitted ports or protocols. Rules can be restricted to only affect particular sources. Source CIDR ranges can be used to protect an instance from undesired connections coming either from external network or from GCP IP ranges.

This diagram illustrates a we am receiving a connection from an external address and another VM receiving connection from a VM in the same network you control ingress connections from VM instance by constructing inbound connection conditions using a source CIDR arranges protocols or ports.