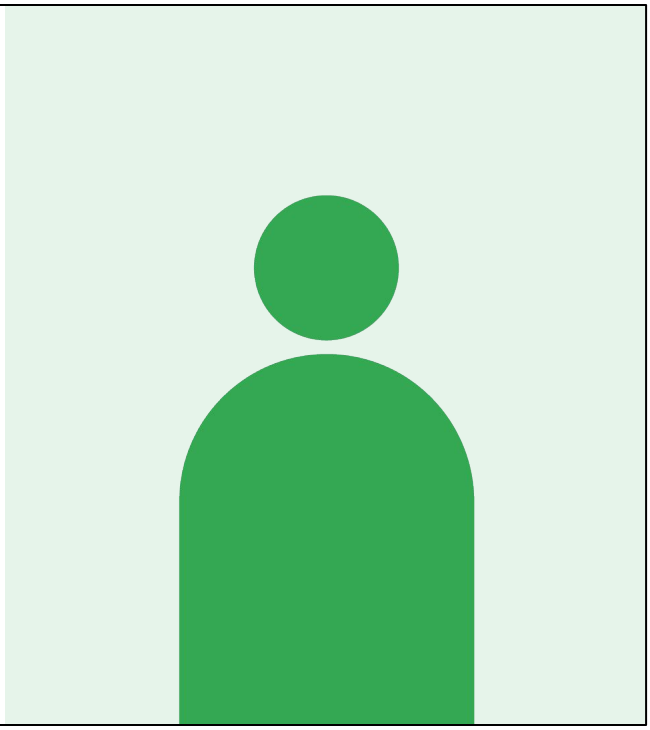
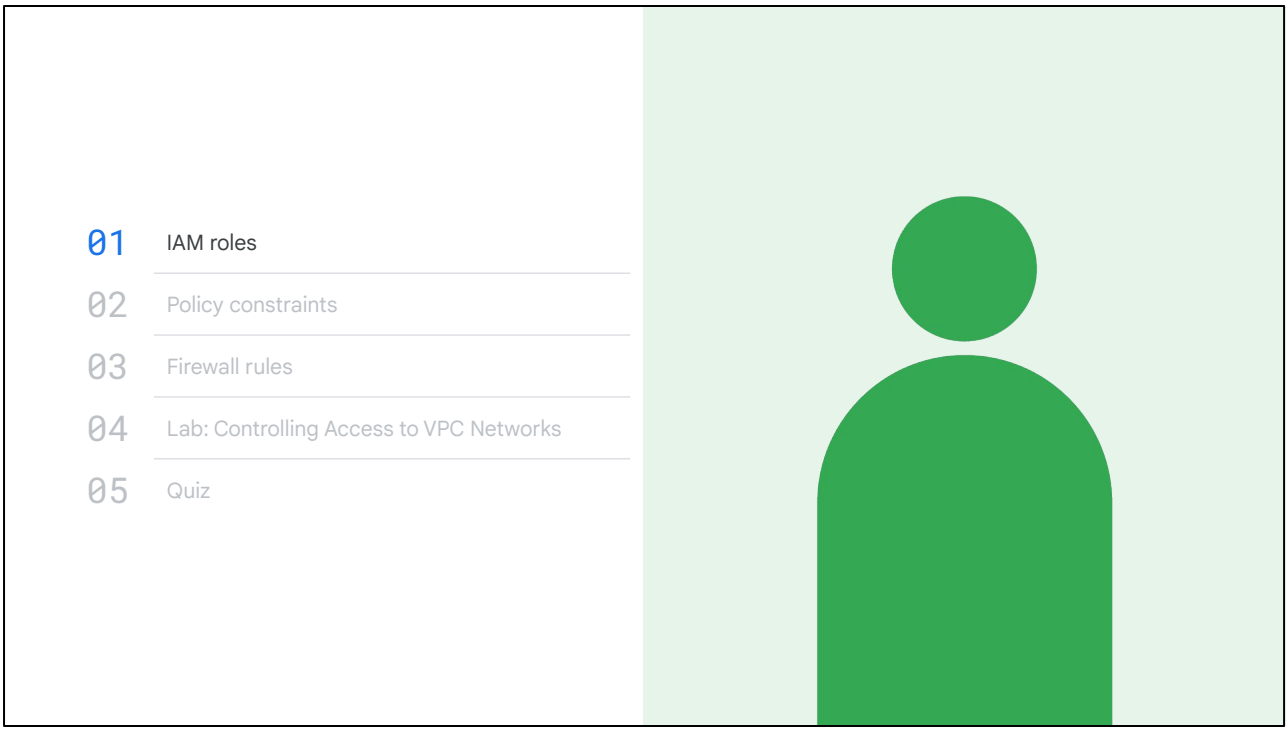
Networking in Google Cloud

Module 2: Controlling Access to VPC Networks



Welcome to the Controlling Access to VPC Networks module. This is the second module of the Networking in Google Cloud: Defining and Implementing Networks course.



In this module, we will cover the topics listed on the screen.

We will begin with an overview of IAM roles and how they affect access to Google Cloud resources. After that, we will discuss refining access by applying policy constraints. We will conclude with a brief discussion of firewall rules, a lab exercise, a short quiz.

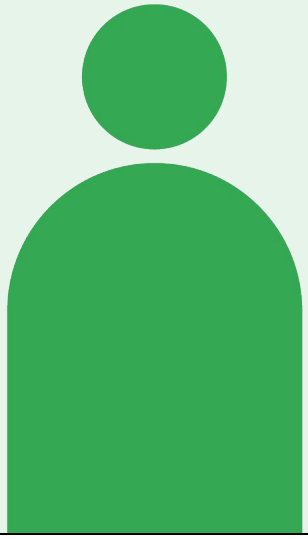
01 IAM roles

02 Policy constraints

03 Firewall rules

04 Lab: Controlling Access to VPC Networks

05 Quiz



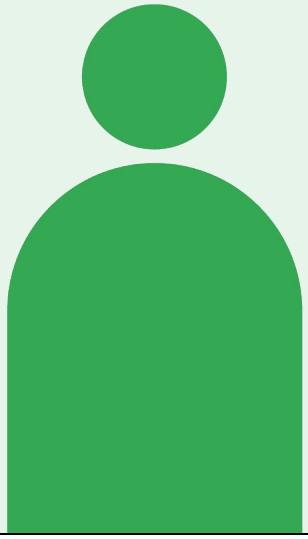
01 IAM roles

02 Policy constraints

03 Firewall rules

04 Lab: Controlling Access to VPC Networks

05 Quiz



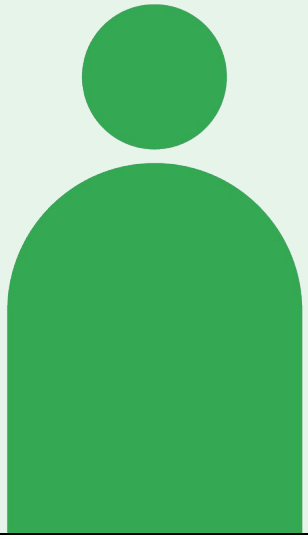
01 IAM roles

02 Policy constraints

03 Firewall rules

04 Lab: Controlling Access to VPC Networks

05 Quiz



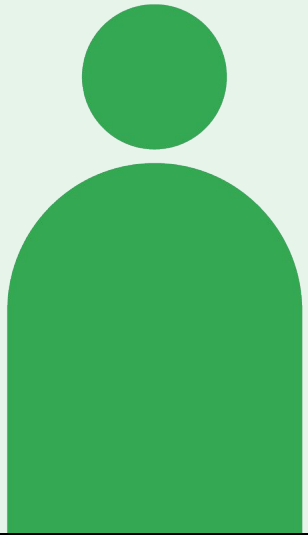
01 IAM roles

02 Policy constraints

03 Firewall rules

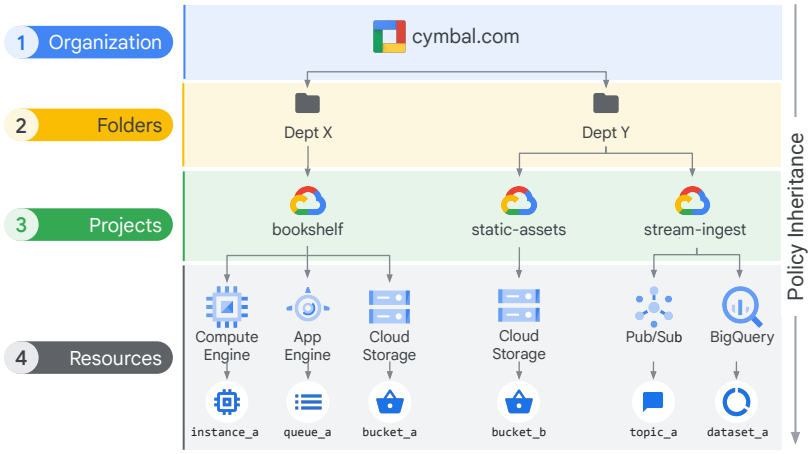
04 Lab: Controlling Access to VPC Networks

05 Quiz



Cloud IAM resource hierarchy

- A policy is set on a resource, and each policy contains a set of:
  - Roles.
  - Members
- Resources inherit policies from the parent.
- If the parent policy is less restrictive, it overrides a more restrictive resource policy.



In the diagram, you can see a sample Cloud IAM resource hierarchy. Let's use the diagram to review how Cloud IAM works.

Google Cloud resources are organized hierarchically as shown in this tree structure. The Organization node is the root node in this hierarchy, folders are the children of the organization, projects are the children of the folders, and the individual resources are the children of projects. Each resource has exactly one parent.

Cloud IAM allows you to set policies at all of these levels, where a policy contains a set of roles and members. Let's go through each of the levels from top to bottom, as resources inherit policies from their parent.

The organization resource represents your company. Cloud IAM roles granted at this level are inherited by all resources under the organization.

The folder resource could represent your department. Cloud IAM roles granted at this level are inherited by all resources that the folder contains.

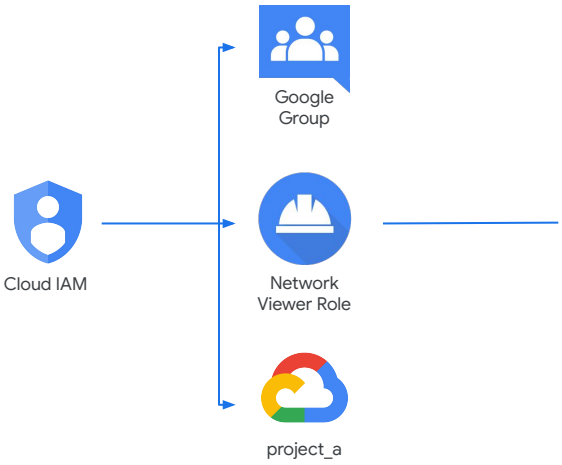
Projects represent a trust boundary within your company. Services within the same project have a default level of trust.

The Cloud IAM policy hierarchy always follows the same path as the Google Cloud resource hierarchy, meaning, if you change the resource hierarchy, the policy hierarchy also changes. For example, moving a project into a different organization

will update the project's Cloud IAM policy to inherit from the new organization's Cloud IAM policy.

Another thing to point out, is that child policies cannot restrict access granted at the parent level. For example, if someone grants you the Editor role for Department X and someone grants you the Viewer role at the bookshelf project level, then you still have the Editor role for that project. Therefore, it is a best practice is to follow the principle of least privilege. The principle applies to identities, roles, and resources. Always select the smallest scope that’s necessary to reduce your exposure to risk.

Predefined roles



List of Permissions

- ✓ compute.addresses.get
- ✓ compute.addresses.list
- ✓ compute.globalAddresses.get
- ✓ compute.globalAddresses.list
- ✓ commute.backendBuckets.get
- ✓ compute.backendBuckets.list
- ✓ compute.networks.list

...

In addition to the basic roles, Cloud IAM provides predefined roles that give granular access to specific Google Cloud resources and prevent unwanted access to other resources. These roles are collections of permissions.

Most of the time, to do any meaningful operations, you need more than one permission. For example, in this slide, a group of users is granted the Network Viewer role on project_a. This provides the users of that group a lot of permissions, of which some are illustrated on the right-hand side.

The permissions are classes and methods in the APIs. For example, compute.networks.list can be broken into the service, resource, and verb, meaning that this permission is used to list all of the VPC networks that project_a contains.

Grouping these permissions into roles, and having those roles represent abstract functions, makes them easier to manage. Also, users can have multiple roles, providing flexibility.

Custom roles

List of Permissions

- ✓ `Compute.firewalls.`
- ✓ `compute.sslCertificates.get`
- ✓ `compute.sslCertificates.list`

→ **Custom Role**

My Network Admin Role

Cloud IAM

In addition to the predefined roles, Cloud IAM also provides the ability to create customized Cloud IAM roles. You can create a custom Cloud IAM role with one or more permissions, and then grant that custom role to users who are part of your organization.

In essence, custom roles enable you to enforce the principle of least privilege, ensuring that the user and service accounts in your organization have only the permissions essential to performing their intended functions.

For example, you might want a user to create, modify, and delete firewall rules but have read-only permissions to SSL certificates. In this case, the Security Admin role provides too many permissions and the Network Admin role does not provide enough. So, you can select the corresponding permissions for firewall rules and SSL certificate as shown on the left-hand side along with any other permissions to create a new custom network admin role.

Cloud IAM provides a UI and API for creating and managing custom roles. For more information on custom roles, refer to Custom roles in the Google Cloud documentation.

Network-related IAM roles

Role Title	Description
Network Viewer	Read-only access to all networking resources
Network Admin	Permissions to create, modify, and delete networking resources, except for firewall rules and SSL certificates
Security Admin	Permissions to create, modify, and delete firewall rules and SSL certificates

Let's focus on predefined roles that provide granular access to VPC networking resources.

There is the Network Viewer role that provides read-only access to all networking resources. For example, if you have software that inspects your network configuration, you could grant that software's service account the Network Viewer role.

Next, the Network Admin role contains permissions to create, modify, and delete networking resources, except for firewall rules and SSL certificates. In other words, the network admin role allows read-only access to firewall rules, SSL certificates, and instances to view their ephemeral IP addresses.

The Security Admin role contains permissions to create, modify, and delete firewall rules and SSL certificates.

Now, there are other predefined roles for networking resources that relate to Shared VPC, which allows an organization to connect resources from multiple projects to a common VPC network. We will cover Shared VPC along with those other predefined roles in a later module of this course.

For more information on these roles, see Compute Engine IAM roles and permissions in the Google Cloud documentation.

Module agenda

01 IAM roles

02 Policy constraints

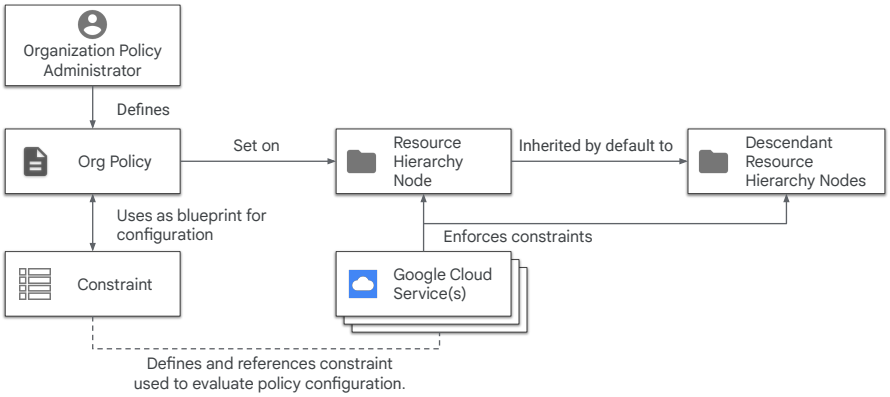
03 Firewall rules

04 Lab: Controlling Access to VPC Networks

05 Quiz

Next, we will discuss how policy constraints let you centrally manage access to Google Cloud resources, including VPC networks.

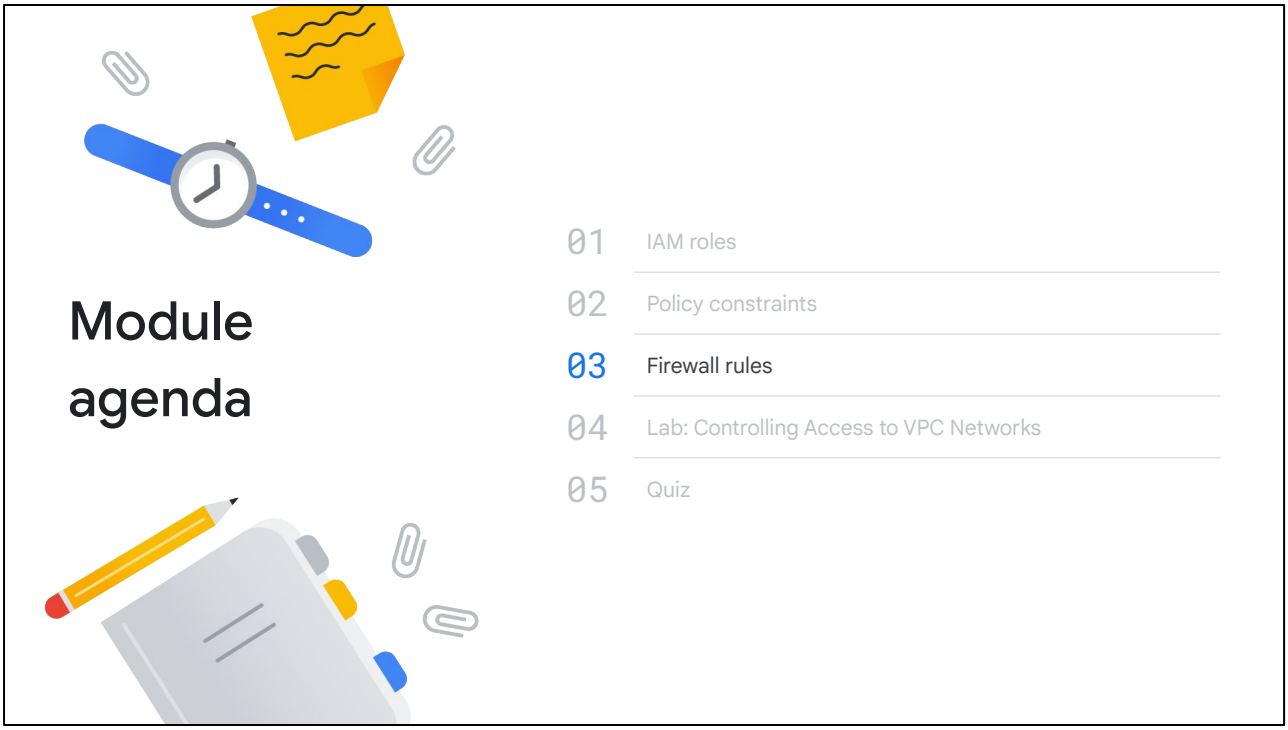
The Organization Policy Service gives you centralized and programmatic control over your cloud resources



Identity and Access Management focuses on who, and lets the administrator authorize who can take action on specific resources based on permissions. Organization Policy focuses on what, and lets the administrator set restrictions on specific resources to determine how they can be configured. The Organization Policy Service gives you centralized and programmatic control over your organization's cloud resources. As the organization policy administrator, you will be able to configure constraints across your entire resource hierarchy.

An organization policy is a configuration of restrictions. You, as the organization policy administrator, define an organization policy, and you set that organization policy on organizations, folders, and projects in order to enforce the restrictions on that resource and its descendants. In order to define an organization policy, you choose a constraint, which is a particular type of restriction against either a Google Cloud service or a group of Google Cloud services. You configure that constraint with your desired restrictions.

Descendants of the targeted resource hierarchy node inherit the organization policy. By applying an organization policy to the root organization node, you are able to effectively drive enforcement of that organization policy and configuration of restrictions across your organization.



Next, let's briefly discuss firewall rules and how they affect access to VPC networks and the internet.

Firewall rules protect your VM instances from unapproved connections

- 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.
- Deny all ingress and allow all egress rules are implied.

Google Cloud firewall rules protect your 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.

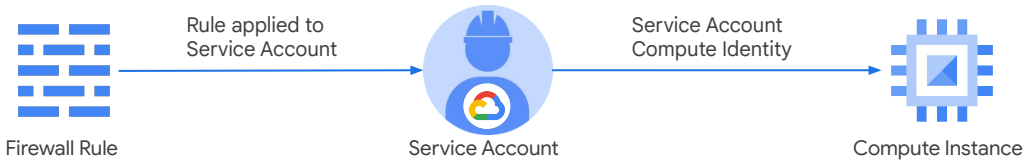
Although firewall rules are applied to the network as a whole, connections are allowed or denied at the instance level.

Let’s explore this concept more deeply by controlling access to specific target instances and from specific source instances, not by their IP range but by using network tags and service accounts.

Firewall rule parameters: Target and Source

Target:
- All instances in the network
- Specified target tags
- Specified service accounts

Source:
- IP ranges
- Subnets
- Source tags
- Service account



A firewall rule is composed of several parameters.

The target parameter of a firewall rule defines the instances to which the firewall rule is intended to apply. This parameter has three choices, as shown on this slide. “All instances in the network” specifies that the firewall rule applies to all instances in the network, which we explored in the previous module.

To provide more granularity, firewall rules can also be applied to only those VM instances that match specific service accounts or network tags, which are user-defined strings that you can apply to your VM instances.

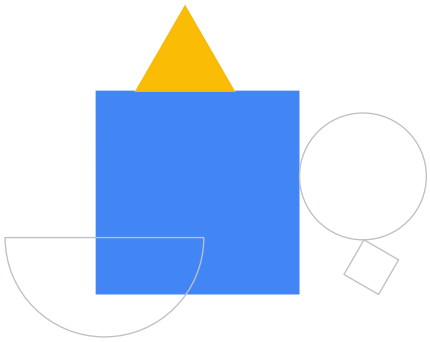
The source parameter of a firewall rule is intended for ingress traffic and defines the allowed sources of the traffic. Similar to the target parameter, firewall rules can be applied to traffic coming from VM instances that match a specific network tag or use a specific service account.

Because service accounts are controlled through Cloud IAM, they are considered more secure than tags.

For more information on filtering by service account versus network tag, refer to Filtering by service account versus network tag in the Google Cloud documentation.

Lab Intro

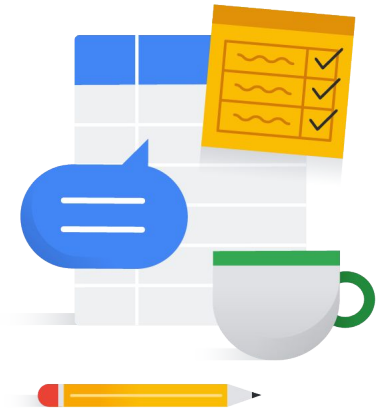
Controlling Access to VPC Networks



In this lab, you learn how to perform the following tasks:

- Create tagged firewall rules.
- Create a service account with IAM roles.
- Explore permissions for the Network Admin and Security Admin roles.

Debrief



In this module, you learned about controlling access to VPC networks using Cloud IAM. You saw a sample Cloud IAM resource hierarchy and were shown how IAM policies controlled access to the Google Cloud resources. You then saw how policy constraints and firewall rules can fine-tune resource access. You applied what you learned in a lab exercise and a quiz.