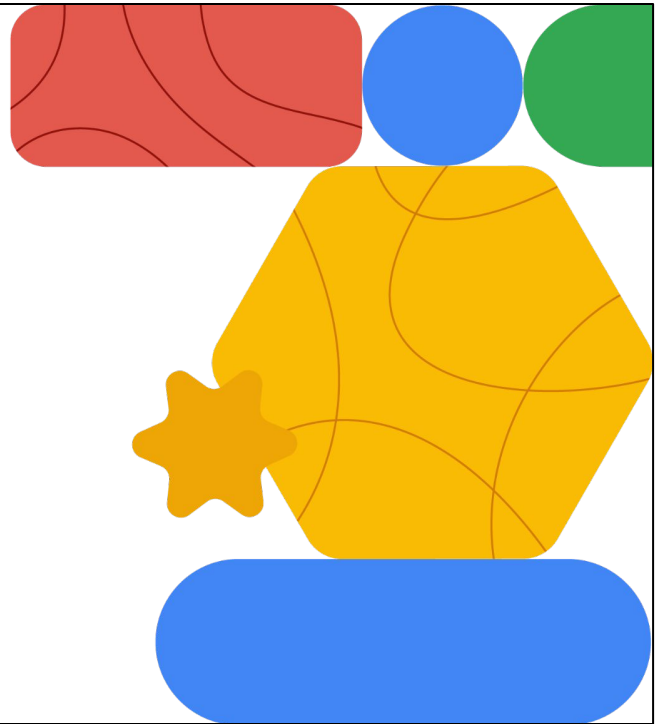# Networking in Google Cloud

**Controlling access to
VPC Networks**

Welcome to the Controlling access to VPC Networks module.

Today's agenda

Google Cloud

In this module, we'll cover some ways to restrict access to your VPC networks.

We'll begin with an overview of the IAM (Identity Access Management) resource hierarchy and policy constraints.

We will then cover firewall rules and how they further control access to your VPC networks. You will then use what you learned in a lab exercise, Controlling Access to VPC Networks, followed by a brief quiz.

We will begin with IAM roles.
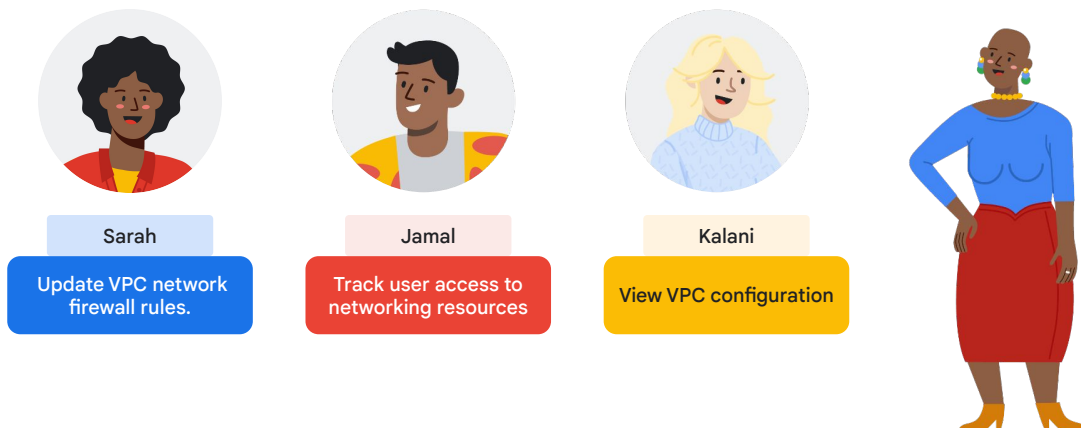
Karen, a cloud network administrator, is tasked with ensuring that principles of least privilege are maintained when granting access to cloud network engineers.
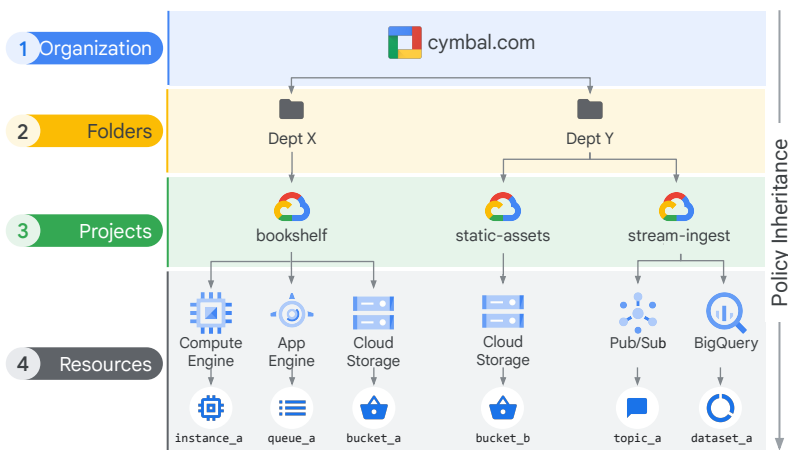- Sarah is tasked with updating VPC network firewall rules.
- Jamal is tasked with tracking user access to cloud networking resources.
- Kalani must be able to view VPC network configurations.

How can Karen grant everyone the access that they need?

To answer this question, let us explore IAM first.

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.
- A less restrictive parent policy will override a more restrictive child resource policy.
- A deny policy can be used to further restrict access.

1 Organization — cymbal.com

2 Folders — Dept X, Dept Y

3 Projects — bookshelf, static-assets, stream-ingest

4 Resources

| Compute Engine | App Engine | Cloud Storage | Cloud Storage | Pub/Sub | BigQuery |
| instance_a | queue_a | bucket_a | bucket_b | topic_a | dataset_a |

Policy Inheritance

Google Cloud

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

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. IAM roles granted at this level are inherited by all resources under the organization.

The folder resource could represent your department. 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 IAM policy hierarchy always follows the same path as the Google Cloud resource hierarchy. This means that, if you change the resource hierarchy, the policy hierarchy also changes. For example, moving a project into a different organization will update
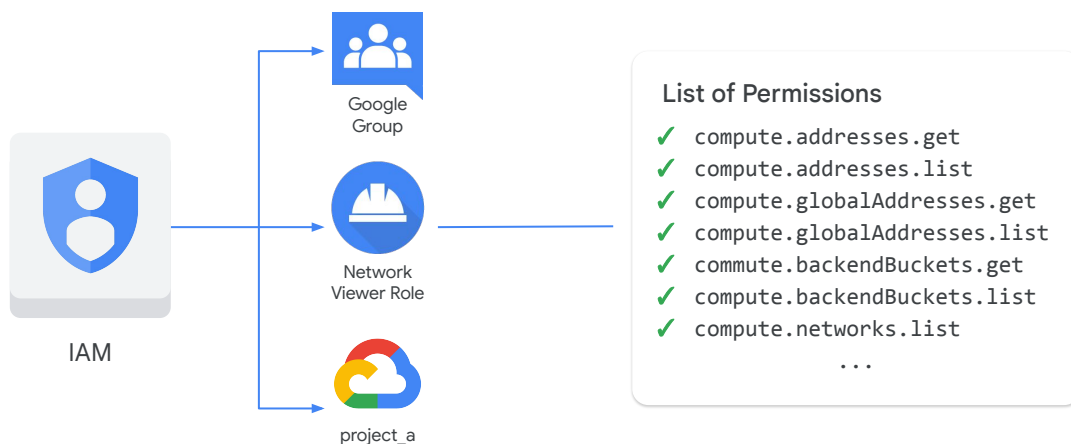
the project's IAM policy to inherit from the new organization's IAM policy.

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.

NOTE: Deny policies take precedence over access policies. They provide more granular control. Deny policies were recently introduced so you can define *deny rules* that prevent certain principals from using certain permissions, regardless of the roles they're granted. Each project, folder, and organization can have up to 5 deny policies attached to it.
Reference: https://cloud.google.com/iam/docs/deny-overview

Predefined roles

Google Group

Network Viewer Role

project_a

IAM

List of Permissions

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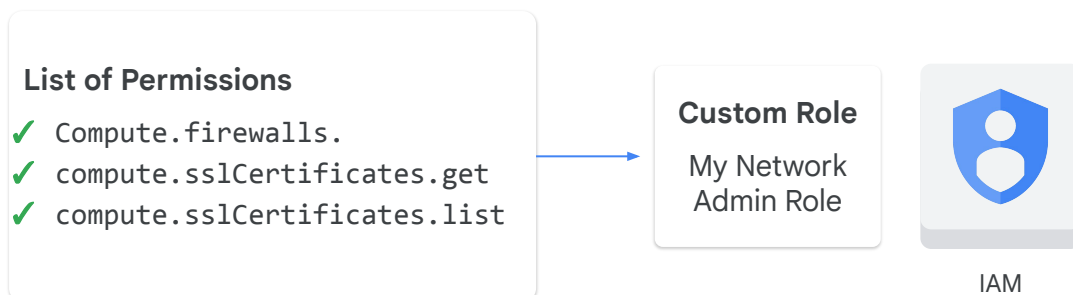✓ `compute.networks.list`
      `...`

Google Cloud

In addition to the basic roles, 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. Some are illustrated on the right 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

IAM

In addition to the predefined roles, IAM also provides the ability to create customized IAM roles. You can create a custom 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 administrator role provides too many permissions and the network administrator role does not provide enough. So, you can select the corresponding permissions for firewall rules and SSL certificates as shown on the left side along with any other permissions to create a new custom network administrator role.

IAM provides a UI and an 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 administrator	Permission to create, modify, and delete networking resources, except for firewall rules and SSL certificates
Security administrator	Permission 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 administrator role contains permissions to create, modify, and delete networking resources, except for firewall rules and SSL certificates. In other words, the network administrator role allows read-only access to firewall rules, SSL certificates, and instances to view their ephemeral IP addresses.
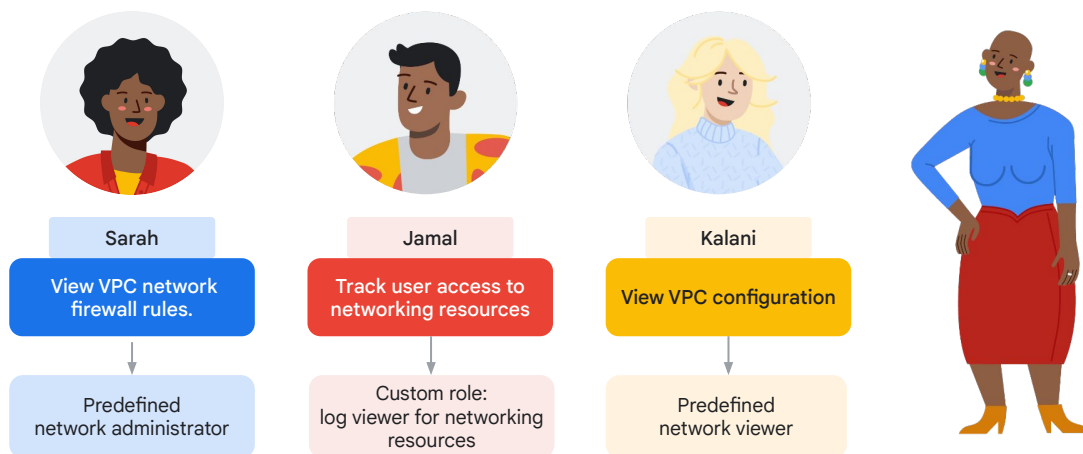
The security administrator role contains permissions to create, modify, and delete firewall rules and SSL certificates.

Now, there are other predefined roles for networking resources that relate to Shared VPC, which allow 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.

Use case: Granting access

Sarah

View VPC network firewall rules.

↓

Predefined network administrator

Jamal

Track user access to networking resources

↓

Custom role: log viewer for networking resources

Kalani

View VPC configuration

↓

Predefined network viewer

Going back to the use case.

Karen uses IAM to ensure the network engineers have just enough access to do their jobs. If a predefined role exists that provides just the access that a cloud network engineer needs, she adds the engineer to it. If no predefined role exists with sufficient permissions, Karen creates a custom role with just enough permissions for the network engineer job responsibilities and then adds the engineer to it.

Today's agenda

Google Cloud

Firewall rules can be applied to your network and resources in several ways

- All instances in the network.
- Instances with a specific target tag.
- Instances using a specific service account.
- Firewall rules are "stateful."
- To apply firewall rules to multiple VPC networks in an organization, use firewall policies.
- Firewall policies use tags to identify and group resources for firewall rules.
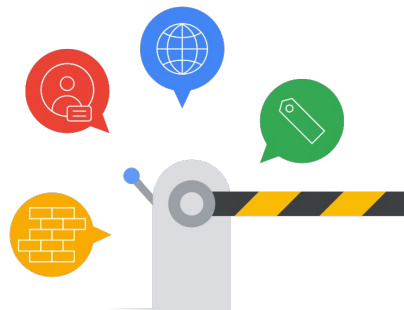
Google Cloud

Applying rules to all instances in the network means the rule will apply to every instance running in that VPC network without having to tag or mark the instances in any other way.

Applying rules to instances tagged with a specified target tag requires any instance needing the firewall rule to be "tagged" with the firewall rule target tag.

Lastly, applying firewall rules to specific service accounts will apply those rules to both new instances created and associated with the service account and existing instances if you change their service accounts.

Note that changing the service account associated with an instance requires that you stop and restart it for the change to take effect.

Google Cloud firewalls are stateful, which means that, for each initiated connection tracked by allow rules in one direction, the return traffic is automatically allowed regardless of any other rules in place. In other words, firewall rules allow bidirectional communication once a session is established. The connection is considered active if at least one packet is sent every 10 minutes.

To apply firewall rules to multiple VPC networks in an organization, use firewall policies. Network firewall policies use tags. Tags are key-value pairs defined at the organization level that provide a flexible way to identify and group resources for firewall rules with granular control through IAM permissions.

Firewall rule parameters

Parameter	Details
Direction	Ingress or egress
Source or destination	The source parameter is only applicable to ingress rules.
	The destination parameter is only applicable to egress rules.
Protocol and port	Rules can be restricted to specific protocols only, or combinations of protocols and ports only.
Action	Allow or deny
Priority	0–65535. A lower number indicates a higher priority.

Google Cloud

A firewall rule is composed of many settings that are specified by the following five parameters:

- **Direction:** rules can be applied depending on the connection direction, values can be ingress or egress.
- **Source or destination:** the source parameter is only applicable to ingress rules and the destination parameter is only applicable to egress rules. Firewall targets can be applied to all instances in a network, source tags, and service accounts, and can be further filtered by IP addresses or ranges.
- **Protocol and port:** the protocol, such as TCP, UDP, or ICMP and port number. You can specify a protocol, a protocol and one or more ports, a combination of protocols and ports, or nothing. If the protocol is not set, the firewall rule applies to all protocols.
- **Action:** an action can be set to either allow or deny, and will determine if the rule permits or blocks traffic.
- **Priority:** a numerical value from zero to 65,535, which is used to determine the order the rules are evaluated. Rules are evaluated starting from zero, so a lower number indicates a higher priority. If you do not specify a priority when creating a rule, it is assigned a priority of 1000.

When evaluating rules, the first rule that matches is the one that will be applied.

If two rules have the same priority, the rule with a deny action overrides a rule with an allow action.
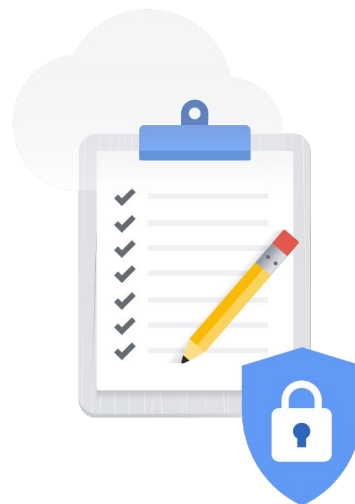
All VPCs have implied firewall rules

Implied IPv4 firewall rules are present in all VPC networks
- Implied IPv4 allow egress rule: Lets any instance send traffic to any destination.
- Implied IPv4 deny ingress rule: Protects all instances by blocking incoming connections to them.

If IPv6 is enabled, the VPC network also has these two implied rules:
- Implied IPv6 allow egress rule: Lets any instance send traffic to any destination.
- Implied IPv6 deny ingress rule: Protects all instances by blocking incoming connections to them.

Google Cloud

Implied IPv4 firewall rules are present in all VPC networks, regardless of how the networks are created, and whether they are auto mode or custom mode VPC networks. The default network has the same implied rules.

- **Implied IPv4 allow egress rule.** An egress rule whose action is allow, destination is 0.0.0.0/0, and priority is the lowest possible (65535) lets any instance send traffic to any destination, except for traffic blocked by Google Cloud.

- **Implied IPv4 deny ingress rule.** An ingress rule whose action is deny, source is 0.0.0.0/0, and priority is the lowest possible (65535) protects all instances by blocking incoming connections to them. A higher priority rule might allow incoming access.

If IPv6 is enabled, the VPC network also has these two implied rules:

- **Implied IPv6 allow egress rule.** An egress rule whose action is allow, destination is ::/0, and priority is the lowest possible (65535) lets any instance send traffic to any destination, except for traffic blocked by Google Cloud. A higher priority firewall rule may restrict outbound access. Internet access is allowed if no other firewall rules deny outbound traffic and if the instance has an external IP address.

- **Implied IPv6 deny ingress rule.** An ingress rule whose action is deny, source

- is ::/0, and priority is the lowest possible (65535) protects all instances by blocking incoming connections to them. A higher priority rule might allow incoming access.

The implied rules *cannot* be removed, but they have the lowest possible priorities.

For more information on implied rules check out the link in the speaker notes.
- **Link:** cloud.google.com/vpc/docs/firewalls#default_firewall_rules

Default VPCs have additional allow rules

Rule	Description
default-allow-internal	Allows ingress connections for all protocols and ports among instances within the VPC network.
default-allow-ssh	Allows port 22 - secure shell (ssh) access.
default-allow-rdp	Allows port 3389 - remote desktop protocol (RDP) access.
default-allow-icmp	Allows ICMP traffic.

Google Cloud

In Google Cloud, all projects get a default VPC created automatically. In addition to the implied rules, the default VPC network is pre-populated with firewall rules that allow incoming, or ingress, traffic to instances.The first rule is default-allow-internal, which allows ingress connections for all protocols and ports among instances within the VPC network. It effectively permits incoming connections to VM instances from others in the same network.

The other three rules in the default network are default-allow-ssh, default-allow-rdp and default-allow-icmp.These rules allow port 22, secure shell (ssh), port 3389, remote desktop protocol (RDP), and ICMP traffic respectively, from any source IP address to any instance in the VPC network.

All of these rules have the second-to-lowest priority of 65534.

As you may have noticed some of these rules can be a little dangerous. These rules can (and should) be deleted or modified as necessary.

Some VPC network traffic is always allowed

✅ Packets sent to and received from the Google Cloud metadata server.

✅ Packets sent to an IP address assigned to one of the instance's own network interfaces (NICs) where packets stay within the VM itself.

Google Cloud

Some network traffic is always allowed.

For VM instances, VPC firewall rules, and hierarchical firewall policies do not apply to:

- Packets sent to and received from the Google Cloud metadata server,

- And packets sent to an IP address assigned to one of the instance's own network interfaces (NICs) where packets stay within the VM itself. IP addresses assigned to an instance's NIC include:

    - The primary internal IPv4 address of the NIC.
    - Any internal IPv4 address from an alias IP range of the NIC.
    - If IPv6 is configured on the subnet, any of the IPv6 addresses assigned to the NIC.
    - An internal or external IPv4 address associated with a forwarding rule for load balancing or protocol forwarding if the instance is a backend for the load balancer or is a target instance for protocol forwarding.
    - Loopback addresses.
    - And addresses configured as part of networking overlay software you run within the instance itself.

Check out the link in the speaker notes for more information on blocked traffic.
- **Link:** cloud.google.com/vpc/docs/firewalls#alwaysallowed

Some VPC network traffic is always blocked

Blocked traffic	Applies to
DHCP offers and acknowledgments	Ingress packets to UDP port 68 (DHCPv4) Ingress packets to UDP port 546 (DHCPv6)
All traffic other than external IPv4 and IPv6 using protocols TCP, UDP, ICMP, ICMPv6, IPIP, AH, ESP, SCTP, and GRE	Ingress packets to external IP addresses

Google Cloud

There is some network traffic that is always blocked on VPC networks.

- Google Cloud blocks incoming DHCP offers and acknowledgments from all sources except for DHCP packets coming from the metadata server.
- External IPv4 and IPv6 addresses only accept TCP, UDP, ICMP, ICMPv6, IPIP, AH, ESP, SCTP, and GRE packets.

Check out the link in the speaker notes for more information on blocked traffic.
- **Link:** cloud.google.com/vpc/docs/firewalls#blockedtraffic

Firewall rule best practices

1 Use the model of least privilege.

2 Minimize direct exposure to/from the internet.

3 Prevent ports and protocols from being exposed unnecessarily.

4 Develop a standard naming convention for firewall rules. For example:
- {direction}-{allow/deny}-{service}-{to-from-location}
- Ingress-allow-ssh-from-onprem
- egress-allow-all-to-gcevms

5 Consider service account firewall rules instead of tag-based rules.

Google Cloud

There are a few firewall rule best practices to help secure instances running in Compute Engine.

1. Keep your firewall rules in line with the model of least privilege. Create rules to explicitly allow only traffic necessary for your applications to communicate.

2. It is always best to minimize direct exposure to the internet. To do this, avoid having "allow" firewall rules defined with the source or destination range set to 0.0.0.0/0.

3. To prevent ports and protocols from being exposed accidentally, create a firewall rule with the lowest priority that blocks all outbound traffic for all protocols and ports. This rule will override the implied egress rule that allows all outbound traffic and instead lock down your Compute Engine instances from making connections. You should then create higher-priority firewall rules for specific Compute Engine instances to open required ports and protocols. This helps prevent ports and protocols from being exposed unnecessarily.

4. Another best practice is to adopt a standard naming convention for firewall rules. The exact format is not critically important, just create a standard and be consistent. An example of a naming convention would be to include the following information in your firewall rules:
   - The direction, which is ingress or egress allow or deny indicating the rule's action.

- The service or protocol name.
- The word "from" or "to" and then a short description of the source or destination.

Examples using this formation would be ingress-allow-ssh-from-onprem and egress-allow-all-to-gcevms.

1. When applying firewall rules, you should consider using service account firewall rules instead of tag-based rules. The reason for this is that tag-based firewall rules can be applied by any user who has the Compute Engine instance administrator role, but users require explicit IAM rights to use a service account.

Hierarchical, global, and regional network firewall policies
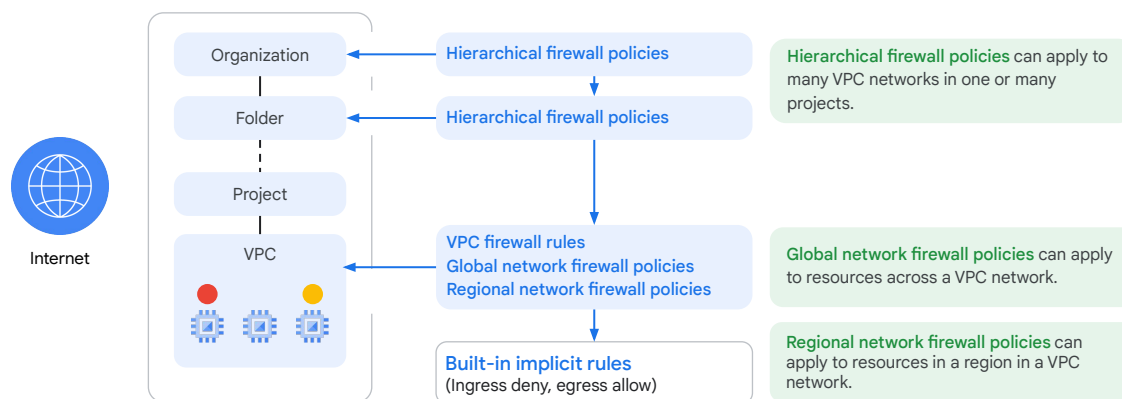
Hierarchical firewall policies let you create and enforce a consistent firewall policy across your organization. You can assign hierarchical firewall policies to the organization as a whole or to individual folders. These policies contain rules that can explicitly deny or allow connections, as do Virtual Private Cloud (VPC) firewall rules.

Global and regional network firewall policies improve upon the previous VPC firewall rules structure.

Similar to hierarchical firewall policies, these network firewall policy structures act as a container for firewall rules. Rules defined in a network firewall policy are enforced once the policy is associated with a VPC network, enabling simultaneous batch updates to multiple rules in the same policy.

The same network firewall policy can be associated with more than one VPC network, and each VPC network can only have one global network firewall policy and one regional firewall policy per region associated with it. Both global network firewall policies and regional network firewall policies support IAM-governed tags, and all Cloud firewall enhancements moving forward will be delivered on the new network firewall policy constructs.

A global network firewall policy provides a global firewall configuration structure to match the global nature of Google Cloud VPC networks. It applies to workloads deployed in all Google Cloud regions in the VPC network.

A regional network firewall policy provides a regional firewall configuration structure for Google Cloud firewalls that can only be used in a single target region. When using regional network firewall policies, users can designate a target region for a firewall policy. The firewall configuration data will be applied to workloads only in that specific region and will not be propagated to any other Google Cloud regions.

Firewall Insights helps you better understand and safely optimize your firewall rules

Cloud Monitoring: Metrics

Network Intelligence Center Firewall Insights

Recommender: Insights
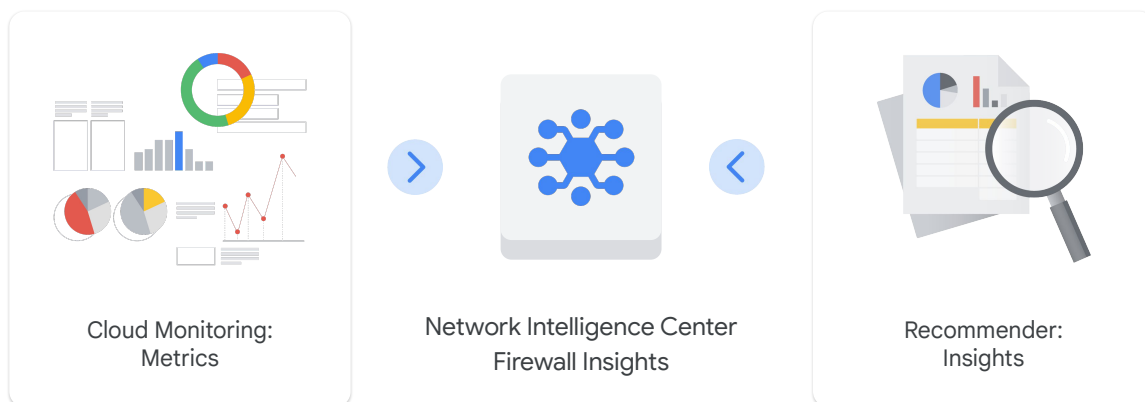
Google Cloud

Firewall Insights, a component product of Network Intelligence Center, produces metrics and insights that let you make better decisions about your firewall rules. It provides data about how your firewall rules are being used, exposes misconfigurations, and identifies rules that could be made more strict.

Firewall Insights uses Cloud Monitoring metrics and Recommender insights.

Cloud Monitoring collects measurements to help you understand how your applications and system services are performing. A collection of these measurements is generically called a metric. The applications and system services being monitored are called monitored resources. Measurements might include the latency of requests to a service, the amount of disk space available on a machine, the number of tables in your SQL database, the number of widgets sold, and so forth. Resources might include virtual machines, database instances, disks, and so forth.

Recommender is a service that provides recommendations and insights for using resources on Google Cloud. These recommendations and insights are per-product or per-service, and are generated based on heuristic methods, machine learning, and current resource usage. You can use insights independently from recommendations. Each insight has a specific insight type. Insight types are specific to a single Google Cloud product and resource type. A single product can have multiple insight types, where each provides a different type of insight for a different resource.

- **Link:** Using Cloud Monitoring for metrics:

- https://cloud.google.com/monitoring/api/v3/metrics
- **Link:** Using Recommender for insights:
  https://cloud.google.com/recommender/docs/insights/using-insights

Use case: Apply firewall rules hierarchically

Requirements:

A firewall solution that can be applied at multiple levels

Solution:

Cloud Firewall

Organization firewall policy

Folder firewall policy

VPC firewall rules

Network firewall policy

Built-in implicit rules
(ingress deny, egress allow)

Google Cloud

Cymbal has recently migrated its on-premises networks to Google Cloud. Kwan, a network engineer, is tasked with securing the Cymbal VPC networks. The firewall solution from the on-premises network works, but Kwan wants a flexible solution that can be applied at multiple levels of the Cymbal cloud infrastructure hierarchy. What should Kwan use?

Solution: Kwan should use Cloud Firewall. Cloud Firewall includes hierarchical firewall policies that can be applied at the organization, folder, project or VPC level. It also includes global and regional network firewall policies.

Today's agenda

Google Cloud

Next, in a lab exercise, you'll control access to VPC networks.

Lab

Configuring VPC Firewalls
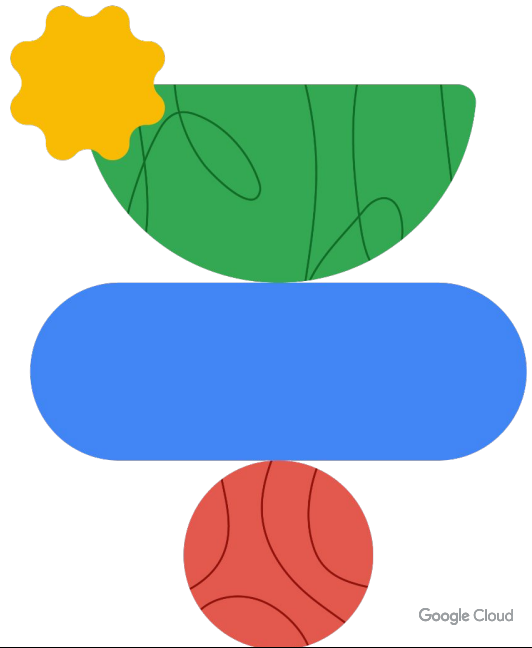
In this lab, you investigate Virtual Private Cloud (VPC) networks and create firewall rules to allow and deny access to a network and instances.
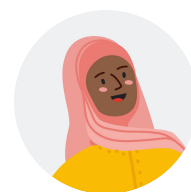
Today's agenda

Google Cloud

Let's talk briefly about another Google Cloud security offering—Cloud IDS.

Use case: Detect network-based threats

Problem:

- Unauthorized access attempts
- Execution of malicious software
- Covert monitoring tools, and command-and-control attacks

Solution: Cloud IDS

- Cloud IDS is a network security service offered by Google Cloud.
- It provides improved visibility into network and system vulnerabilities.
- It has threat detection capabilities.

Google Cloud

Quinn, a network engineer at Cymbal Corporation, is looking for a way to improve the security of the company's cloud infrastructure. Cymbal has observed a concerning rise in cyberattacks targeting sensitive customer and financial data. These attacks range from unauthorized access attempts to the delivery and execution of malicious software. Additionally, covert monitoring tools and command-and-control attacks attempting to establish communication channels between compromised systems and external servers have been detected. Such threats pose a substantial risk to Cymbal's reputation, customer trust, and regulatory compliance, underscoring the urgent need for advanced security measures.

Solution

To mitigate these escalating cyber threats, Cymbal has implemented Google Cloud IDS. Cloud IDS is a network security service offered by Google Cloud that provides real-time detection of intrusions, malware, spyware, and command-and-control attacks. With comprehensive monitoring of both internal and external traffic, Cloud IDS offers Cymbal improved visibility into their network and system vulnerabilities. The scalability of the service allows Cymbal to adapt their threat detection capabilities as their infrastructure expands. As a fully managed service, Cloud IDS simplifies security management, enabling Cymbal's IT team to focus on other priorities while ensuring the safeguarding of their critical assets.

Cloud IDS: Overview

It provides threat detection for intrusions, malware, spyware, and command-and-control attacks on your network.

→

Creates a Google-managed peered network with mirrored VMs.

Inspects traffic from mirrored VMs to provide advanced threat detection.

Provides full visibility into network traffic, letting you monitor VM-to-VM communication.

Meets your advanced threat detection and compliance requirements, including PCI 11.4.

Google Cloud

Cloud IDS is an intrusion detection service that provides threat detection for intrusions, malware, spyware, and command-and-control attacks on your network.

Cloud IDS works by creating a Google-managed peered network with mirrored VMs. Traffic in the peered network is mirrored, and then inspected by Palo Alto Networks threat protection technologies to provide advanced threat detection.

Cloud IDS provides full visibility into network traffic, including both north-south and east-west traffic, letting you monitor VM-to-VM communication to detect lateral movement.

Cloud IDS gives you immediate indications when attackers are attempting to breach your network, and the service can also be used for compliance validation, like PCI 11.

In addition, Cloud IDS automatically updates all signatures without any user intervention, enabling users to focus on analyzing and resolving threats without managing or updating signatures.
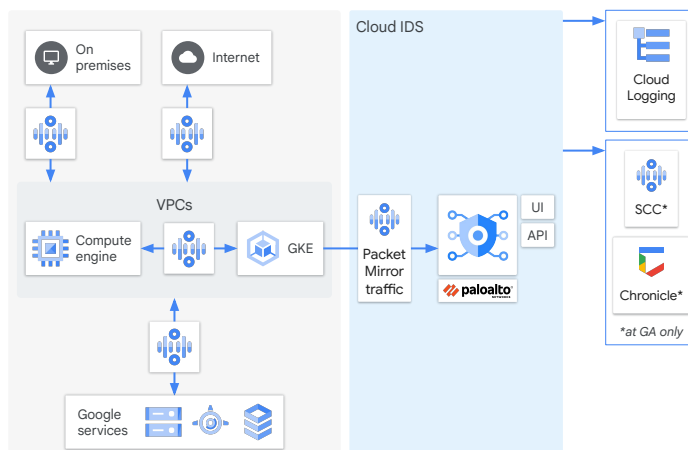
Cloud IDS: Endpoints and packet mirroring

IDS endpoint
- Zonal resource that inspects traffic from any zone in its region.
- Receives mirrored traffic and performs threat detection analysis.

Packet mirroring
- Creates a copy of your network traffic.
- Attaches packet mirroring policies to IDS endpoints.

Google Cloud

To better understand Cloud IDS, it's important to understand how the service uses endpoints and packet mirroring.

Cloud IDS uses a resource known as an *IDS endpoint*, a zonal resource that can inspect traffic from any zone in its region. Each IDS endpoint receives mirrored traffic and performs threat detection analysis.

Cloud IDS uses Google Cloud packet mirroring, which creates a copy of your network traffic. After creating an IDS endpoint, you must attach one or more *packet mirroring policies* to it.

These policies send mirrored traffic to a single IDS endpoint for inspection. The packet mirroring logic sends all traffic from individual VMs to Google-managed IDS VMs. For example, all traffic mirrored from VM1 and VM2 will always be sent to IDS-VM1.
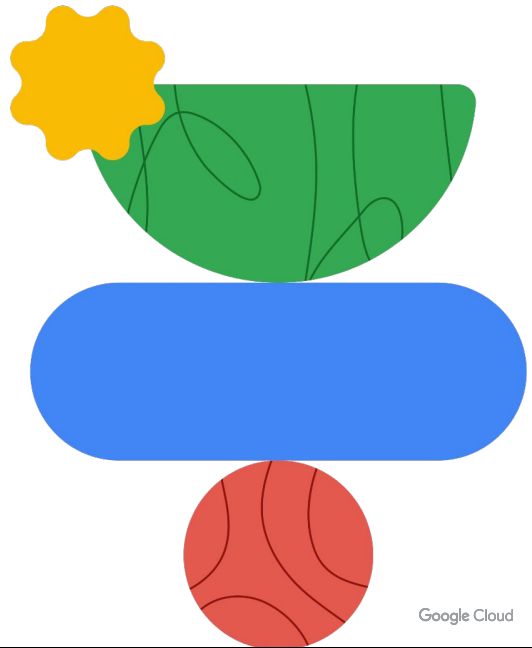
Today's agenda

Google Cloud

Lab intro

Getting Started with Cloud IDS

In this lab, you deploy Cloud Intrusion Detection System (Cloud IDS), a next-generation advanced intrusion detection service that provides threat detection for intrusions, malware, spyware, and command-and-control attacks. You simulate multiple attacks and view the threat details in the Google Cloud console.
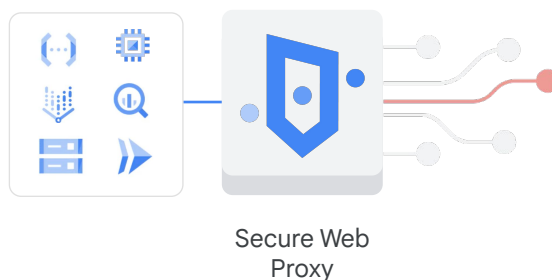
Today's agenda

Google Cloud

Restrict access to trusted external web services

- ✓ Secure Web Proxy enhances the security of outbound web traffic from different sources.

- ✓ Secure Web Proxy acts as a gateway to filter traffic based on configurable policies.

Secure Web Proxy

Secure Web Proxy is a Google Cloud service designed to enhance the security of outbound web traffic (HTTP/S) from various sources, including virtual machines, containers, serverless environments, and workloads outside of Google Cloud. It acts as a gateway, filtering traffic based on configurable policies that leverage cloud identities and web applications. This enables organizations to enforce granular control over web access, improving overall security posture while maintaining flexibility and ease of use.

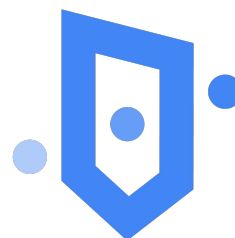# Common use cases

Cloud migration
Simplifies the transition to Google Cloud by maintaining your current security policies for outbound web traffic.

Egress control
Granular policies (Identity and URL centric) for web traffic to Internet.

Incident forensics
Investigate security events and incidents of any kind related to web traffic and internet via comprehensive logging.

Google Cloud

Secure Web Proxy provides the following benefits:

- **Streamlined Cloud migration:** Secure Web Proxy simplifies your transition to Google Cloud by maintaining your current security policies for outbound web traffic. This eliminates the need for third-party tools or manual configuration adjustments.

- **Controlled access to external services:** By allowing you to define granular access policies, Secure Web Proxy enhances the security of your network. You can establish specific identities for workloads or applications and then apply policies to various web locations.

- **Monitored access to untrusted websites:** Secure Web Proxy identifies and logs any traffic that deviates from your established policies, providing you with valuable insights. This allows you to monitor internet usage, uncover potential threats, and respond proactively to safeguard your network.

Let's explore the last one on the list.

Use case: Restrict access to trusted external web services

- Secure Web Proxy allows you to create very specific rules for outgoing web traffic from your cloud environment.
- Secure Web Proxy can significantly increase the security of your network.
- Secure Web Proxy is a proactive approach to cyber security.
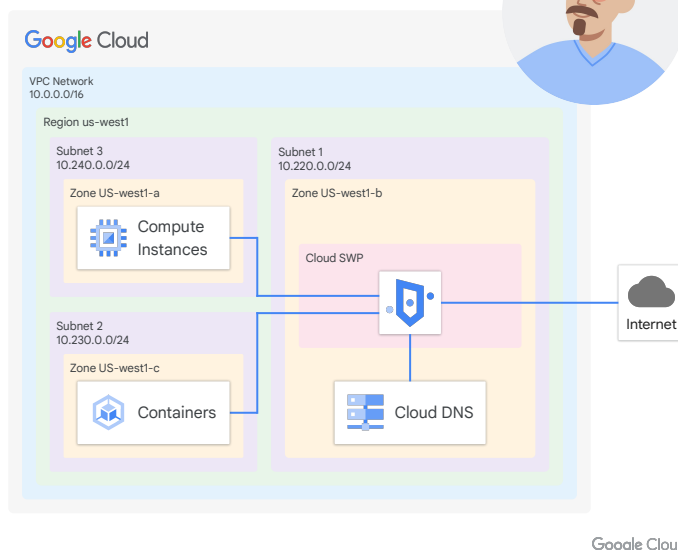
Kwan, a network engineer at Cymbal Corporation, is staring down a growing network infrastructure headache. Kwan needs a unified, automated solution that simplifies network management across both on-premises and cloud environments, while providing granular security and cost control.

Secure Web Proxy lets you apply granular access policies to your egress web traffic so that you can secure your network. This allows you to programmatically restrict cloud workload access to only trusted external web services.

Secure Web Proxy enables you to create very specific rules for outgoing web traffic from your cloud environment. This means you can define exactly which external websites and services your cloud workloads are allowed to access.

By doing this, you can significantly increase the security of your network. You're essentially creating an allowlist of approved web destinations, preventing your systems from communicating with potentially harmful or unauthorized websites.

This programmatic restriction ensures that your cloud workloads interact only with the specific external web services you trust, minimizing the risk of data breaches, malware infections, and other security threats. It's a proactive approach to cybersecurity that helps you maintain control over your network traffic and safeguard your valuable assets.

Today's agenda

01   IAM roles

02   Firewall rules

03   Lab: Configuring VPC Firewalls

04   Cloud IDS

05   Lab: Getting Started with Cloud IDS

06   Secure Web Proxy

07   Quiz

Google Cloud

Quiz | Question 1

Question

Which IAM role includes permissions to create, modify, and delete networking resources, except for firewall rules and SSL certificates?

A.   Network administrator

B.   Network viewer

C.   Security administrator

D.   Security viewer

Google Cloud

Quiz | Question 2

Question

Which type of IAM member belongs to an application or virtual machine instead of an individual end user?

A.   Google account

B.   Service account

C.   Google group

D.   Cloud Identity domain

Let's ask Gemini ✦

> How do I optimize IAM permissions?

> Create a gcloud command to give the developer Google group access to view my Google Cloud project.

This concludes the module. Before we wrap up, let's explore some useful Gemini prompts that can help you with related questions. The slide displays a few sample prompts to get you started.

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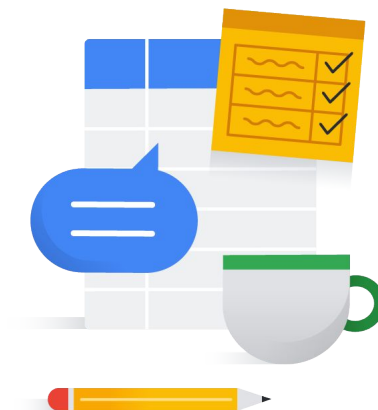
In this module, you learned about controlling access to VPC networks using IAM. You saw a sample IAM resource hierarchy and were shown how IAM policies controlled access to the Google Cloud resources. You then saw how policy constraints and firewall rules can fine-tune resource access. We also covered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

Thank you.

THANK YOU