Welcome to the Configuring Virtual Private Cloud for Isolation and Security module, part of the Security in Google Cloud course.

Agenda

VPC Firewalls

Load Balancing and SSL Policies

Interconnect and Peering Options

Best Practices for VPC Networks

Lab: Configuring VPC Firewalls

VPC Flow Logs

Lab: Configuring and Using VPC Flow Logs in Cloud Logging

Quiz and Module Review

Google Cloud

A Virtual Private Cloud (or VPC) is a global, private, isolated virtual network partition that provides managed networking functionality for your Google Cloud resources.

In this module, we will discuss many VPC related security concepts including VPC firewalls, load balancing SSL policies, network interconnect and peering options, VPC network best practices and VPC flow logs. You will also have the opportunity to practice what you've learned, by completing the **Configuring VPC Firewalls** and **Configuring** and **Using and Viewing VPC Flow Logs in Cloud Logging** labs.

Agenda

VPC Firewalls

Load Balancing and SSL Policies

Interconnect and Peering Options

Best Practices for VPC Networks

Lab: Configuring VPC Firewalls

VPC Flow Logs

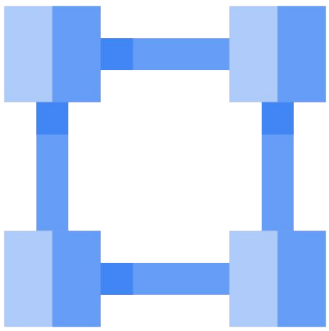
Lab: Configuring and Using VPC Flow Logs in Cloud Logging

Quiz and Module Review

Google Cloud

Let’s get started by learning more about VPC firewalls.

Virtual Private Cloud (VPC)

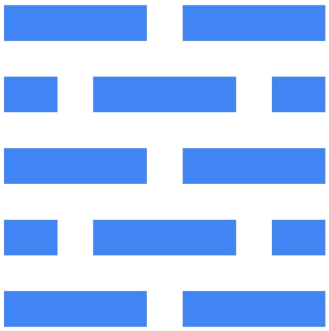


Google Cloud

A VPC network on Google Cloud lets you create and control your own private, logically isolated network, where you can deploy your Google compute resources (Compute Engine instances, Google Kubernetes Engine instances, and so on). Each VPC network in your project provides private communication among your Google Cloud compute resources.

You can control individual ingress and egress traffic for compute resources using firewall rules. You can also connect your on-premises network with your VPC network using VPN IPsec Tunnels or Dedicated Interconnect.

Firewall rules protect VM instances from unapproved connections

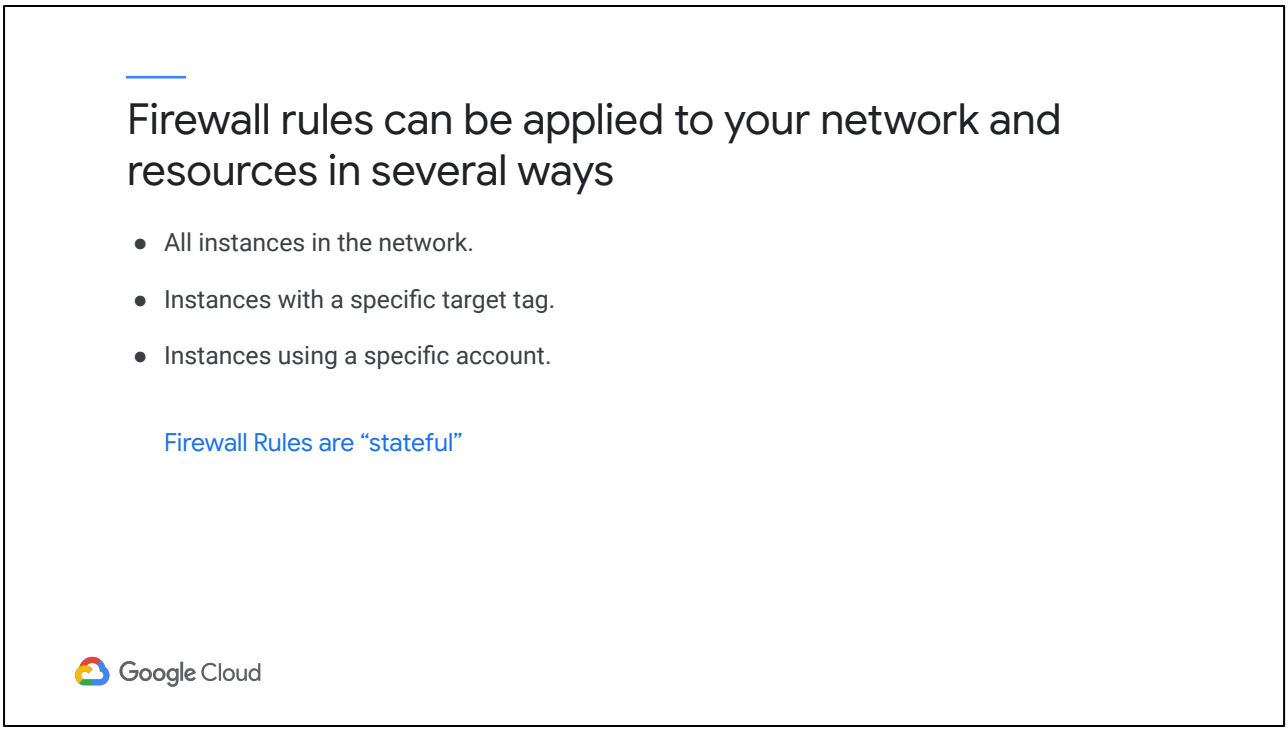


Google Cloud

Google Cloud firewall rules let you allow or deny traffic to and from your VM instances based on a configuration you specify and can be applied to both inbound (ingress) and outbound (egress) traffic.

Google Cloud firewall rules provide effective protection and traffic control regardless of the operating system your instances use. Google Cloud firewall rules are defined for the VPC network as a whole, and since VPC networks can be global in Google Cloud, firewall rules are also global.

Every VPC network functions as a distributed firewall. While firewall rules are defined at the network level, connections are allowed or denied on a per-instance basis. You can think of the Google Cloud firewall rules as existing not only between your instances and other networks, but between individual instances within the same network.



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 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.

Firewall rules

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 apply to specific protocols only, or combinations of protocols and ports only.
action	Allow or deny
priority	0–65535. The order in which rules are evaluated; the first matching rule is applied.

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. The source can be an IP address or range, a source tag or a source service account. The destination parameter is only applicable to egress rules and can only be an IP address or range.
- **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 2 implied firewall rules

1. Allow all outgoing traffic:

   An egress rule, action is allow, destination is 0.0.0.0/0, and lowest priority (65535)

2. Block all incoming traffic:

   An ingress rule, action is deny, source is 0.0.0.0/0, and lowest priority (65535)

Google Cloud

Every VPC network has two permanent implied firewall rules. These rules always exist in every VPC network, but will not be shown in the Cloud Console.The first permits all outgoing connections to any IP address

The second implied rule blocks all incoming traffic. Both of these rules apply to all instances in the network, and have the lowest possible priority which allows them to be easily overridden by a higher priority firewall rule.

Default VPCs have additional allow rules

- `default-allow-internal`
- `default-allow-ssh`
- `default-allow-rdp`
- `default-allow-icmp`
- All with the second lowest priority (65534)
- These rules should be deleted or modified as needed

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 blocked

- There is some traffic that is always blocked.
- Firewall rules cannot be used to unblock this traffic.

There is some network traffic that is always blocked on VPC networks. This traffic cannot be unblocked with firewall rules.

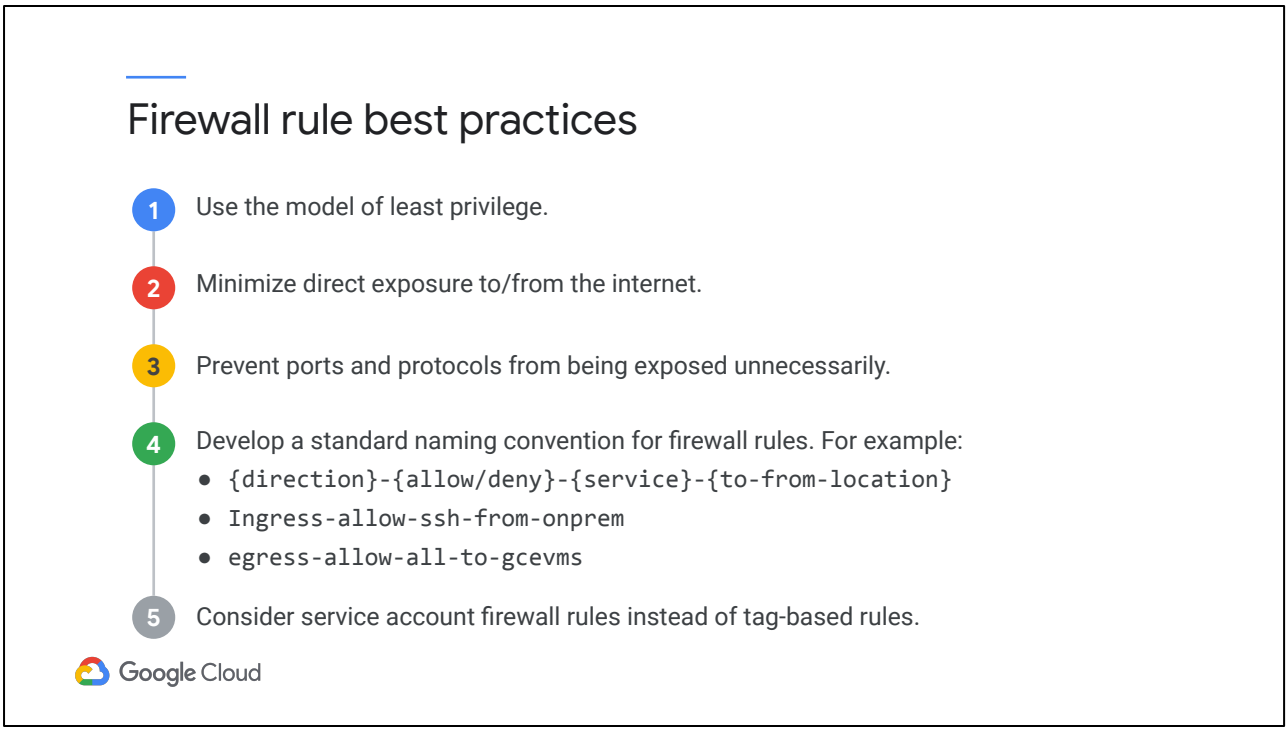
Some VPC network traffic is always blocked

Blocked traffic	Applies to
GRE traffic	all sources, all destinations, including among instances using internal IP addresses, unless explicitly allowed through protocol forwarding
Protocols other than TCP, UDP, ICMP, ESP, AH, SCTP, and IPIP	Traffic between: • instances and the internet • instances if they are addressed with external IP addresses • instances if a load balancer with an external IP address is involved
Egress traffic on TCP port 25 (SMTP)	Traffic from: • instances to the internet • instances to other instances addressed by external IP addresses
Egress traffic on TCP port 465 or 587 (SMTP over SSL/TLS)	Traffic from: • instances to the internet, except for traffic destined for known Google SMTP servers • instances to other instances addressed by external IP addresses

Google Cloud

Here is a list of traffic that is always blocked:

- All GRE traffic, unless explicitly allowed through protocol forwarding
- Protocols other than TCP, UDP, ICMP, ESP, AH, SCTP, and IPIP:
  - Between instances and the Internet
  - Between instances if they are addressed with external IP addresses
  - Between instances if a load balancer with an external IP address is involved
- Egress traffic on TCP port 25 (which is SMTP traffic) to the Internet or any instance external IP address
- Egress traffic on TCP port 465 or 587 (which is SMTP over TLS) to the Internet or any instance external IP address except to known Google SMTP servers.



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.

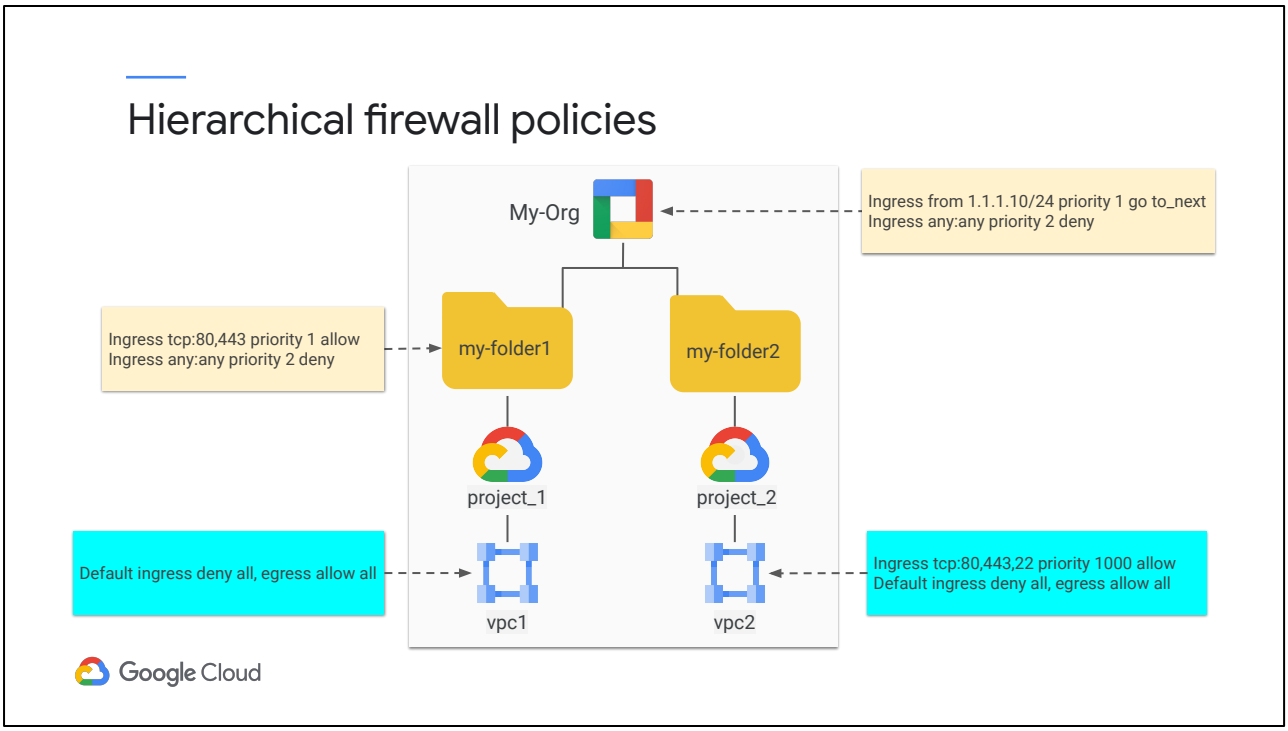
3. To prevent ports and protocols from being exposed accidentally, create a firewall rule with the lowest priority that blocks all outbound traffic for all protocols and ports. This rule will override the implied egress rule that allows all outbound traffic and instead lock down your Compute Engine instances 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

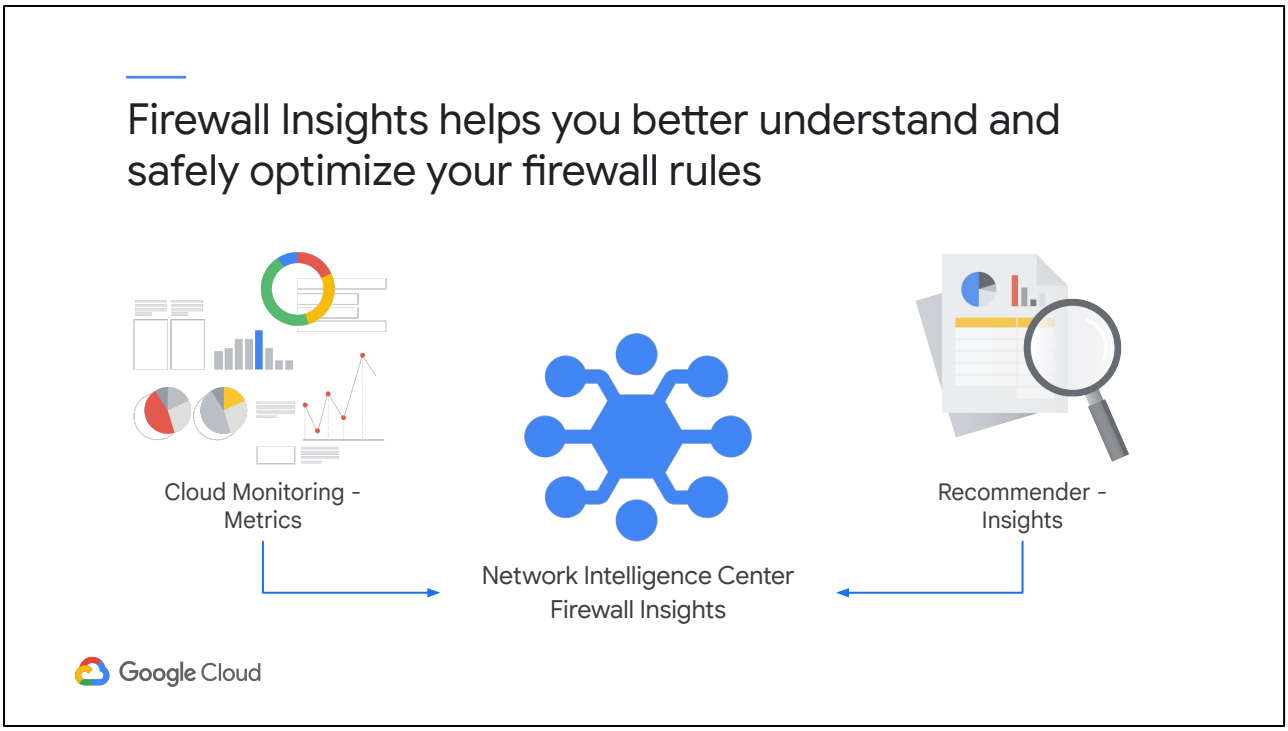
Examples using this formation would be ingress-allow-ssh-from-onprem and egress-allow-all-to-gcevms.

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 Admin role, but users requires explicit IAM rights to use a service account.



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. In addition, hierarchical firewall policy rules can delegate evaluation to lower-level policies or VPC network firewall rules with a goto_next action. Lower-level rules cannot override a rule from a higher place in the resource hierarchy. This lets organization-wide admins manage critical firewall rules in one place.

By default, all hierarchical firewall policy rules apply to all VMs in all projects under the organization or folder where the policy is associated. However, you can restrict which VMs get a given rule by specifying a target network or target service account. The levels of the hierarchy at which firewall rules can now be applied are represented in the diagram, shown here. The yellow boxes near the top represent hierarchical firewall policies, while the blue boxes at the bottom represent VPC firewall rules.



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.

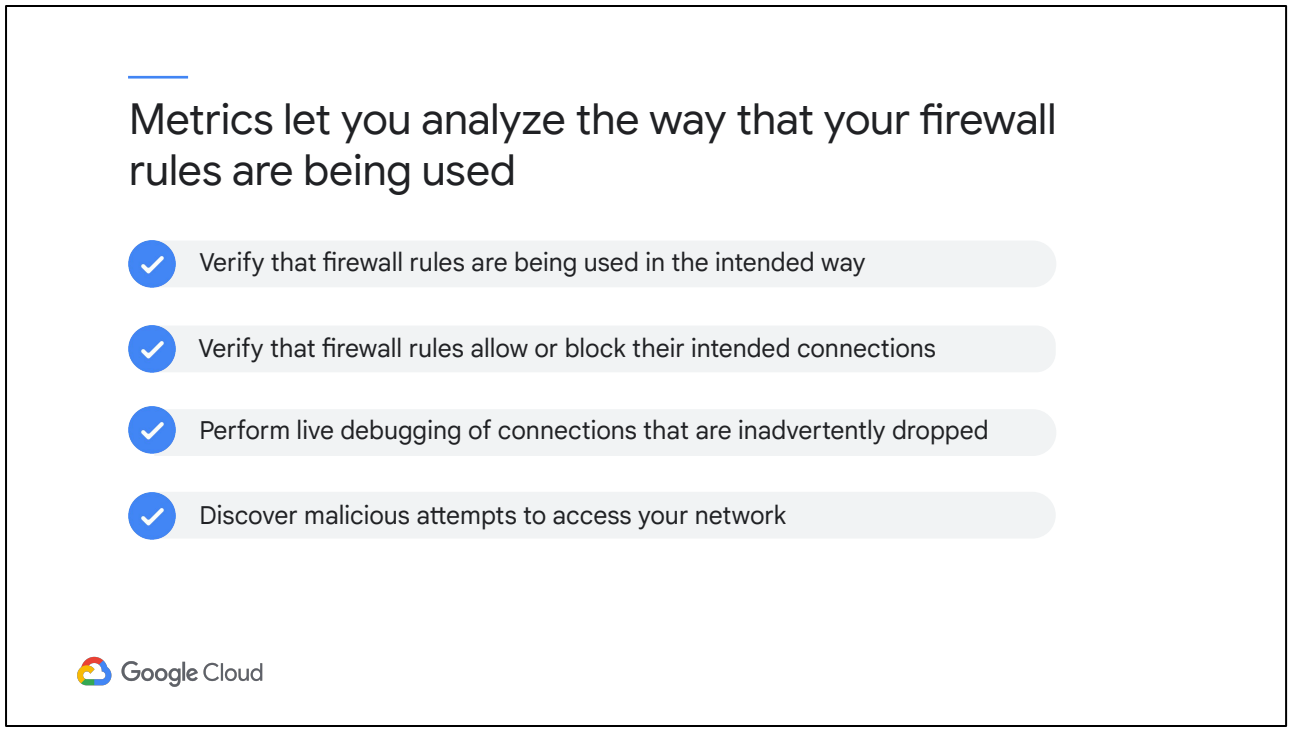
Cloud Monitoring collects measurements to help you understand how your applications and system services are performing. A collection of these measurements is generically called a metric. The applications and system services being monitored are called monitored resources. Measurements might include the 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.

Using Cloud Monitoring for metrics:

https://cloud.google.com/monitoring/api/v3/metrics

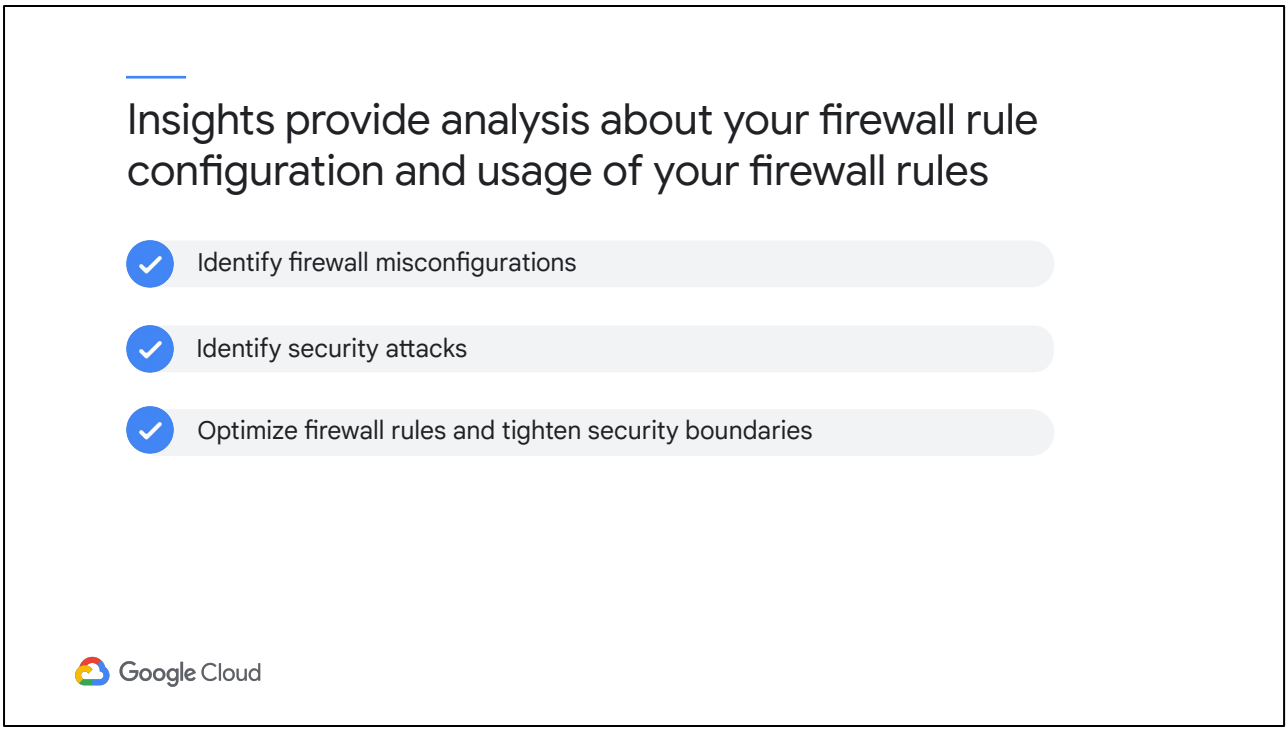
Using Recommender for insights:
https://cloud.google.com/recommender/docs/insights/using-insights



Firewall Insights metrics let you analyze the way that your firewall rules are being used. Firewall Insights metrics are available through Cloud Monitoring and the Google Cloud Console. Metrics are derived through Firewall Rules Logging.

With Firewall Insights metrics, you can perform the following tasks:

- Verify that firewall rules are being used in the intended way.
- Over specified time periods, verify that firewall rules allow or block their intended connections.
- Perform live debugging of connections that are inadvertently dropped because of firewall rules.
- Discover malicious attempts to access your network, in part by getting alerts about significant changes in the hit counts of firewall rules.



Insights provide analysis about your firewall rule configuration and usage of your firewall rules. They use the `google.compute.firewall.Insight` insight type.

With insights, you can perform the following tasks:

- Identify firewall misconfigurations.
- Identify security attacks.
- Optimize firewall rules and tighten security boundaries by identifying overly permissive allow rules and reviewing predictions about their future usage. Please note that at the time of writing, these capabilities are in preview.

Agenda

VPC Firewalls

Load Balancing and SSL Policies

Interconnect and Peering Options

Best Practices for VPC Networks

Lab: Configuring VPC Firewalls

VPC Flow Logs

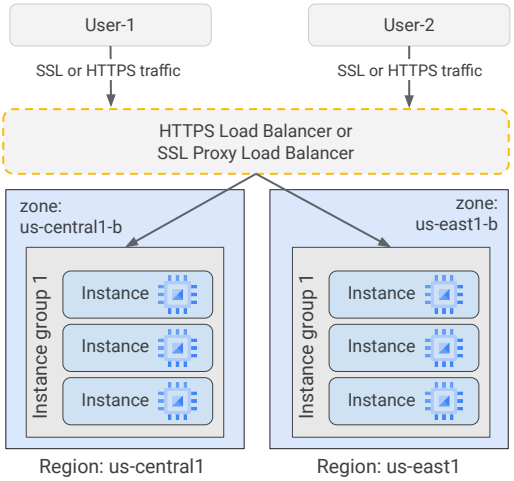
Lab: Configuring and Using VPC Flow Logs in Cloud Logging

Quiz and Module Review

Google Cloud

Google Cloud load balancers support SSL for encryption in transit. In this course, the term “SSL” refers to both the SSL and TLS protocols. In this section we will review the SSL capabilities in the Google Cloud load balancer.

Google Cloud load balancers



Google Cloud

Google Cloud load balancers support HTTPS or SSL Proxy for encryption in transit. These load balancers require at least one signed SSL certificate installed on the target HTTPS proxy for the load balancer.

You can use Google-managed or self-managed SSL certificates. The client SSL session terminates at the load balancer.

Google Cloud Load Balancing terminates user SSL connections at the load balancing layer, then balances the connections across your instances using the SSL or TCP protocols. Cloud SSL proxy is intended for non-HTTPS traffic. For HTTPS traffic, HTTPS load balancing is recommended instead.

Defining an SSL policy

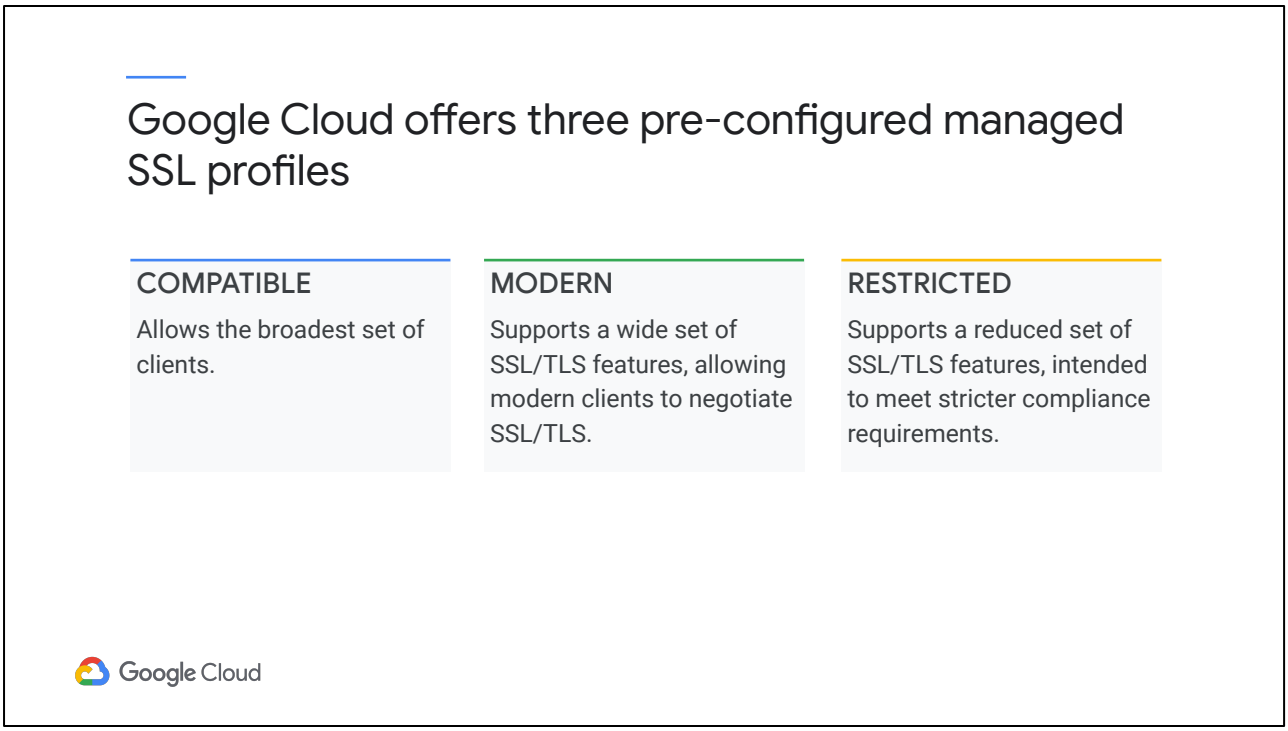
SSL policies specify:

- The minimum TLS version clients can connect with: TLS 1.0, 1.1, or 1.2.
- A profile of SSL policy features.

An SSL policy gives you the ability to control the features of SSL that your SSL proxy or HTTPS load balancer negotiates with clients.

An SSL policy specifies a minimum TLS version and a profile. The TLS versions currently supported are TLS 1.0, 1.1, and 1.2.

SSL 3 or earlier is not supported by the Google Cloud load balancer or SSL proxy. The profile selects a set of SSL features to enable in the load balancer.

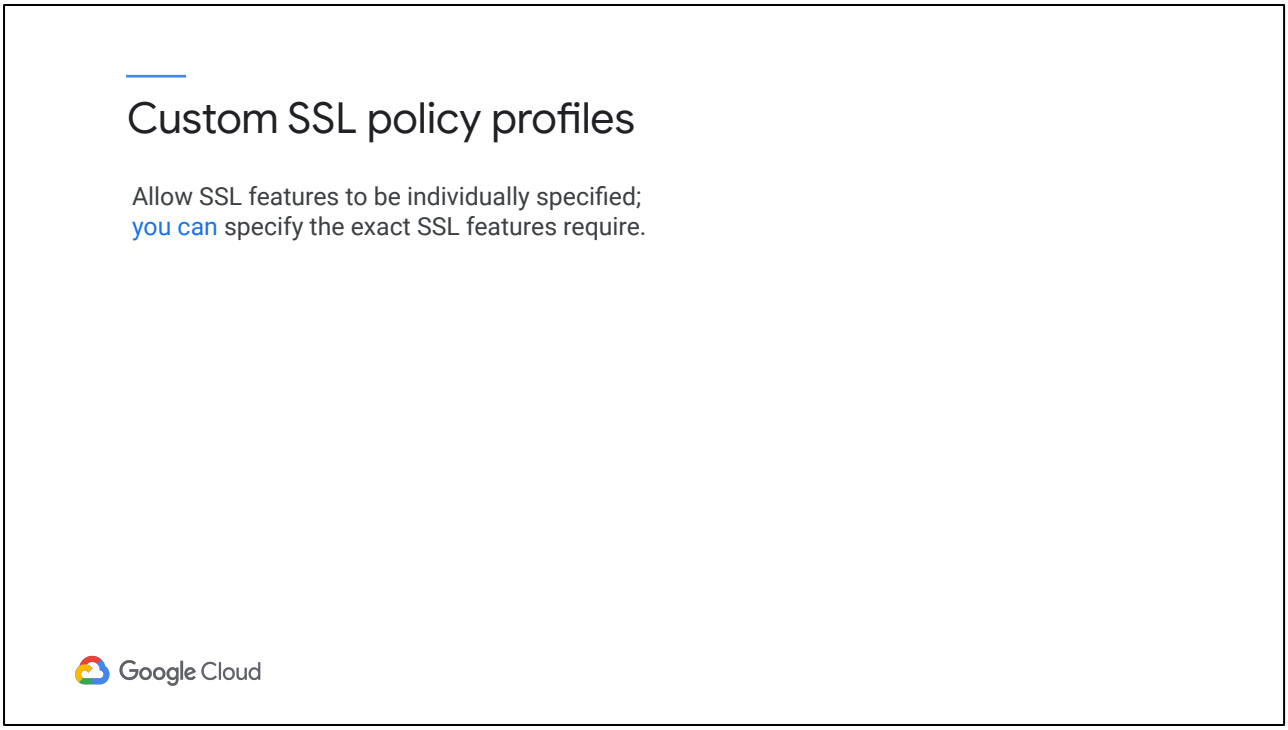


There are 3 pre-configured Google-managed profiles that allow you to specify the level of compatibility appropriate for your application. A fourth custom profile allows you to select SSL features individually.

The specific settings in any of the pre-configured profiles are managed by Google and will be adjusted over time as required.

The three Google-managed profiles are:

- COMPATIBLE: This profile allows the broadest set of clients, including those which support out-of-date SSL features
- MODERN: Supports a wide set of SSL features, allowing modern clients to negotiate SSL.
- RESTRICTED: Supports a reduced set of SSL features, intended to meet stricter compliance requirements



Custom SSL Policy profiles can also be created. They let you select the exact set of SSL features you would like to support. But the features will need to be managed as requirements or available features change

If no SSL policy at all is set, a default SSL profiles is applied that is equivalent to an SSL policy that is using the COMPATIBLE profile.

Agenda

VPC Firewalls

Load Balancing and SSL Policies

Interconnect and Peering Options

Best Practices for VPC Networks

Lab: Configuring VPC Firewalls

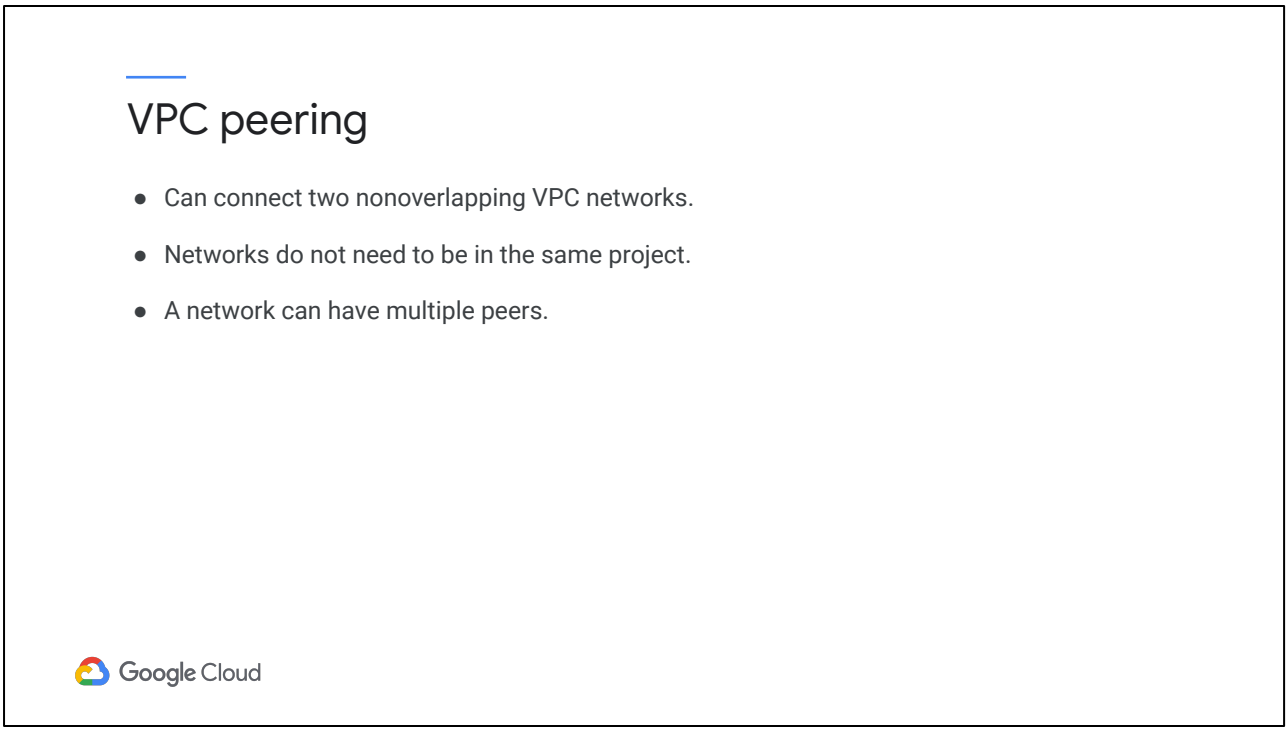
VPC Flow Logs

Lab: Configuring and Using VPC Flow Logs in Cloud Logging

Quiz and Module Review

Google Cloud

Next, we will address Interconnect and VPC peering options.



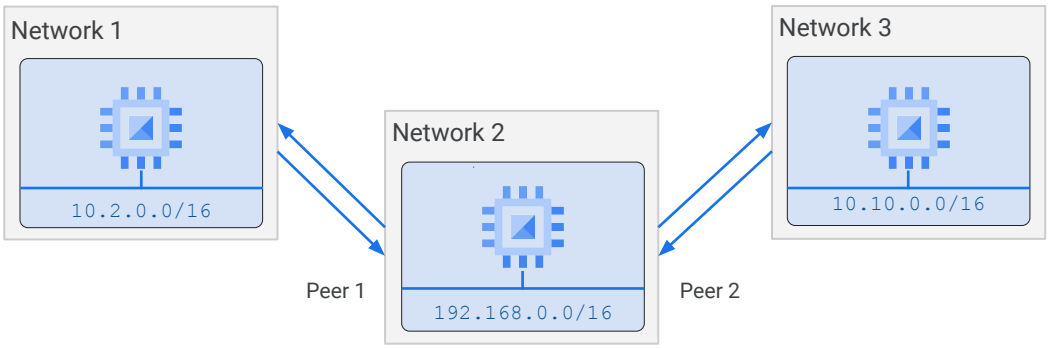
VPC peering allows you to create connectivity across two nonoverlapping VPC networks. VPC peering enables the resources in these VPCs to communicate across private RFC1918 space, reducing exposure to attack.

Peered networks do not need to be in the same project, or even in the same organization. The network firewall rules and routes are independently managed by the project that each respective VPC belongs to. These firewall rules are not imported across the peered networks, you need to configure rules in each of the peered VPCs to control traffic across the peered VPCs.

Currently, a network can have up to 25 directly-peered networks. These networks can be connected in a series or a hub-spoke-style, as long as subnets do not overlap.

VPC Network Peering does not provide granular route controls to filter out which subnet CIDRs are reachable across peered networks. You must use firewall rules to filter traffic if such filtering is needed.

Once networks have peered, every internal, private IP is accessible across the peered networks



Google Cloud

VPC Network Peering gives you several advantages over using external IP addresses or VPNs to connect networks, including:

- Decreased network latency. Public IP networking suffers higher latency than private networking.
- Increased network security. Service owners do not need to have their services exposed to the public Internet and deal with its associated risks.
- Lower network cost. Google cloud charges egress bandwidth pricing for networks using external IPs to communicate even if the traffic is within the same zone. If however, the networks are peered they can use internal IPs to communicate and save on those egress costs. Regular network pricing still applies to all traffic.

Shared VPCs

- Make a VPC network shareable across several projects in your organization.
- Require a host project.

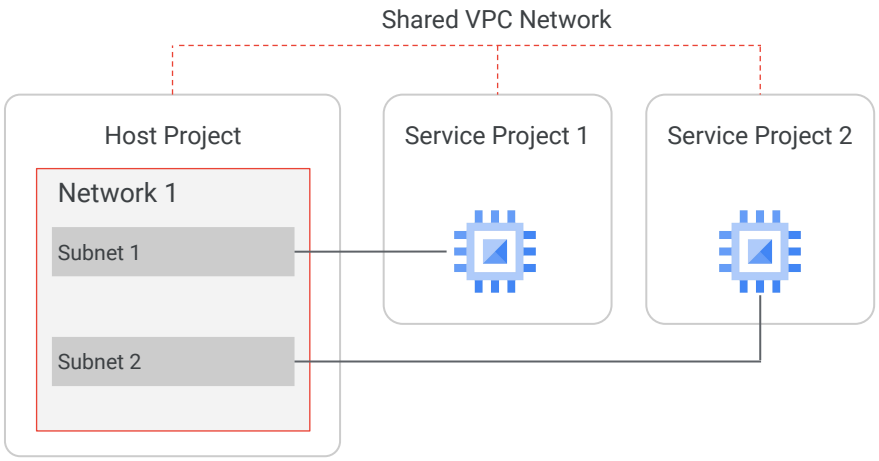
Google Cloud

Shared VPCs allow an organization to connect resources from multiple projects to a common VPC network, so they can communicate with each other securely and efficiently using internal IPs.

When you use Shared VPC, you designate a project as a host project and attach one or more other service projects to it.

The VPC networks in the host project are called Shared VPC networks.

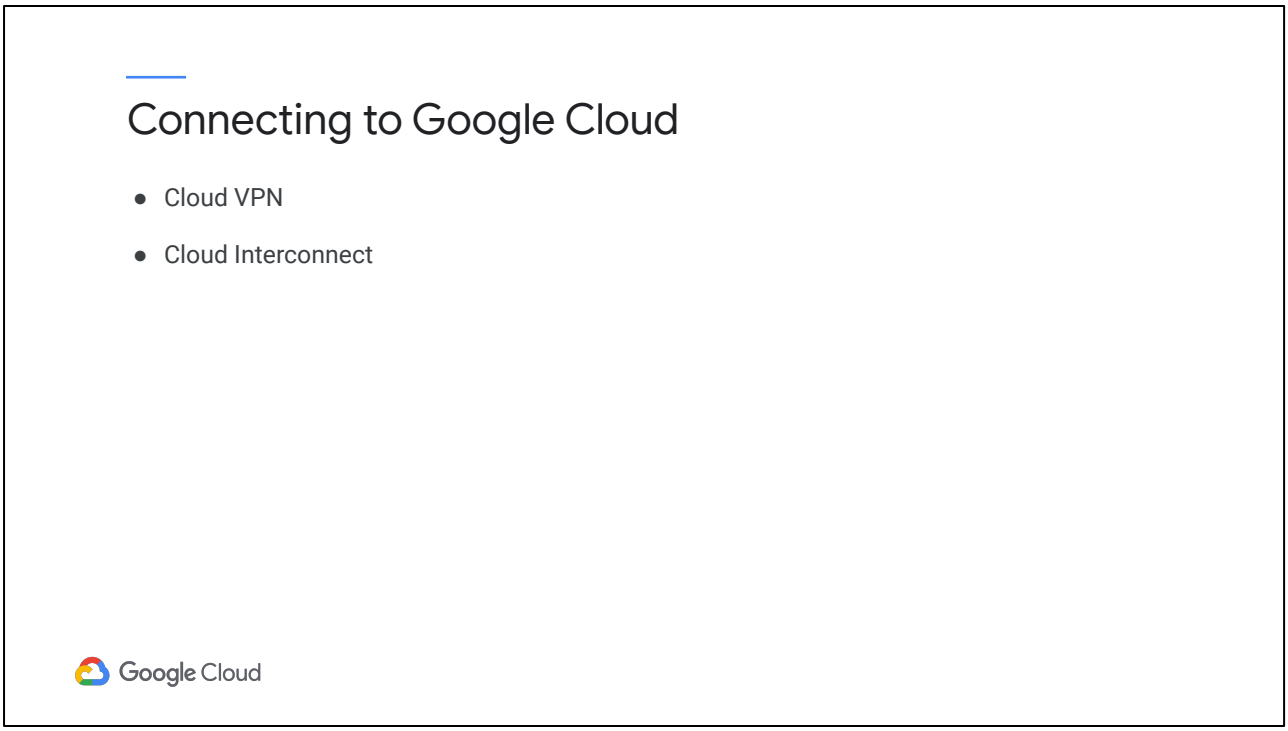
Shared VPCs



Google Cloud

The diagram shows a host project sharing its VPC network with two service projects. It is sharing Subnet_1 with one project and Subnet_2 with another project.

Shared VPC connects projects within the same organization. Participating host and service projects cannot belong to different organizations.

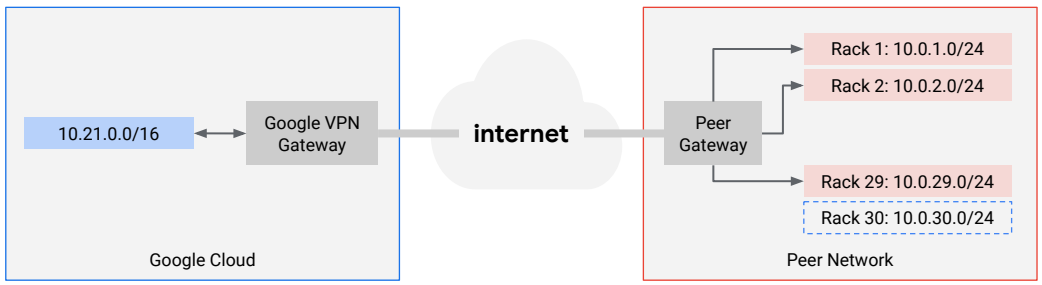


What about connecting from your local on-prem network to your cloud VPC network?

Secure connections to public cloud providers are a concern for all organizations, and some organizations may want to securely extend their data center network into Google Cloud projects. This can be accomplished through Cloud VPN or Cloud Interconnect.

Cloud VPN

- Securely connects your on-premises network to your Cloud VPC network.
- Supports site-to-site VPN



Google Cloud

Google offers IPSec-based managed VPNs to connect your on-premise corporate network or data center network, or other cloud service providers. Cloud VPN uses the IPSec protocol connection to provide end-to-end encryption between the two networks, and supports IKEv1 and IKEv2 using a shared secret (IKE pre-shared key).

Cloud VPN traffic will either traverses the public Internet or can use a direct peering link to Google's network.

Each Cloud VPN tunnel can support up to 3 Gbps when the traffic is traversing a direct peering link, or 1.5 Gbps when it's traversing the public internet.

VPN with static routes

With static routing, updating the tunnel requires:

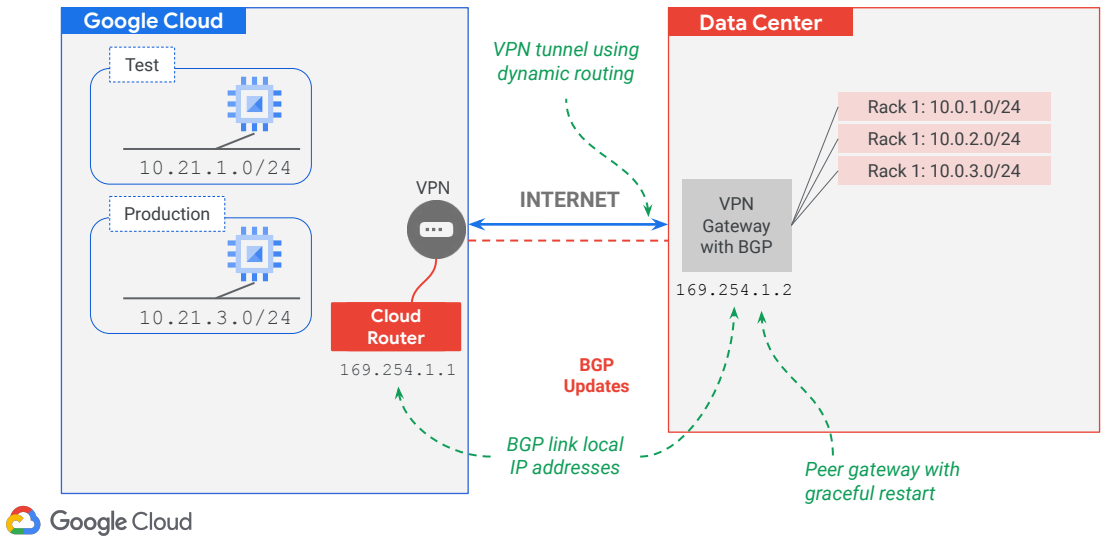
- The addition of static routes to Google Cloud.
- Restarting the VPN tunnel to include the new subnet.

Google Cloud

When using VPNs with static routes, each update to the network requires a manual addition of the the static routes and the network to be rebooted.

This would be required whenever a new subnet is added to either the VPC network or the on-prem corporate network.

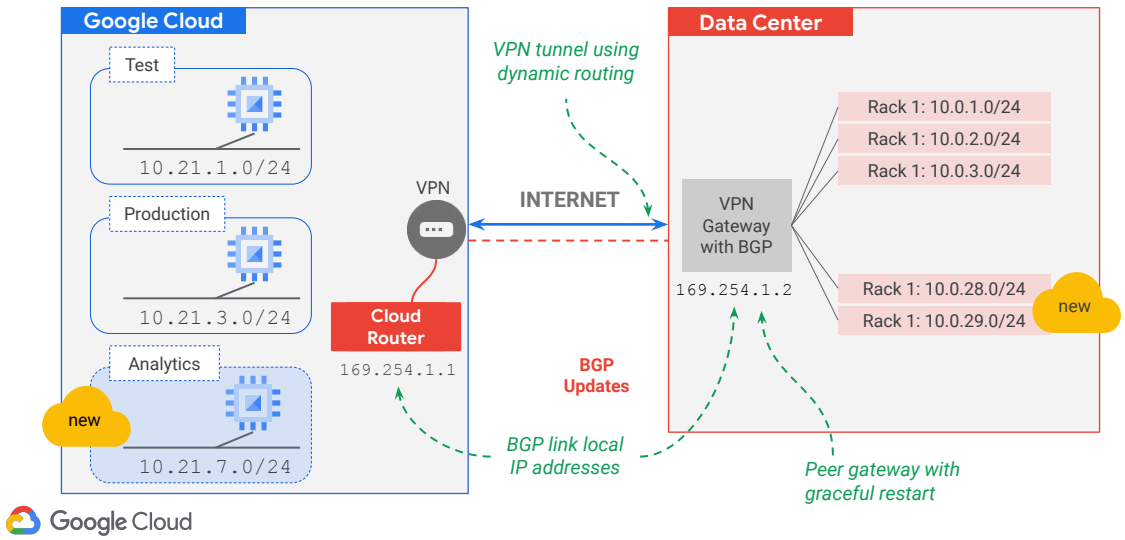
Dynamic routing with Cloud Router



Google Cloud

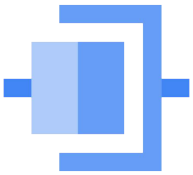
A Cloud Router enables you to dynamically exchange routes between your VPC network and on-premises networks by using Border Gateway Protocol (BGP). Changes to the network topology no longer have to be managed with static routes.

Dynamic routing with Cloud Router



New subnets added in Google Cloud or added in the on-prem network are discovered and shared, enabling connectivity between the two peers for both entire networks. The Cloud Router automatically learns new subnets in your VPC network and announces them to your on-premises network.

Cloud Interconnect offers two options for connecting on-premises network to Google Cloud



Dedicated Interconnect

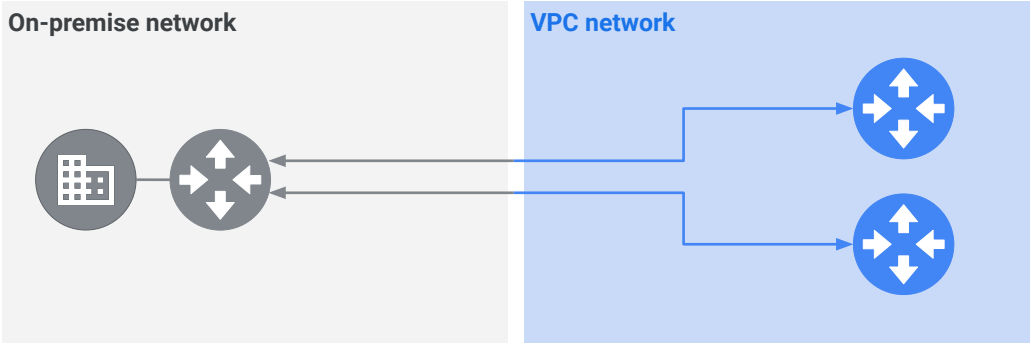
Partner Interconnect

Google Cloud

In addition to IPSec VPN connections, there are two other options for connecting on-premises network to Google Cloud: Dedicated Interconnect and Partner Interconnect.

These provide low latency, highly available, dedicated connections to enable you to reliably transfer data between your on-premises and VPC networks. Also, Cloud Interconnect connections provide RFC 1918 communication, which means internal (private) IP addresses are directly accessible from both networks.

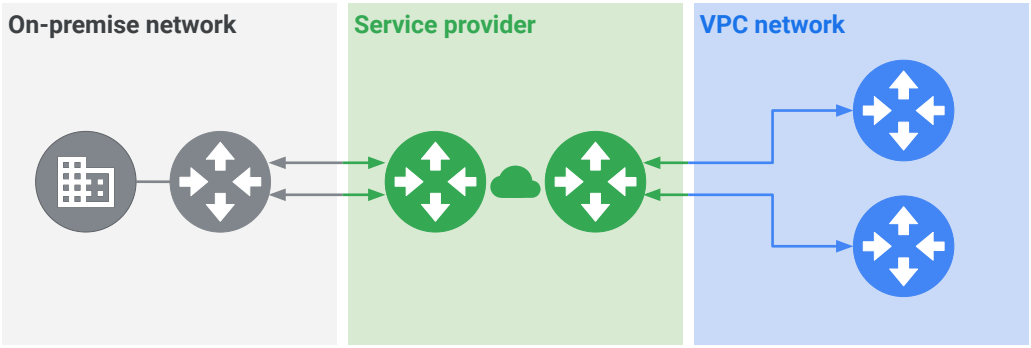
Dedicated Interconnect



Google Cloud

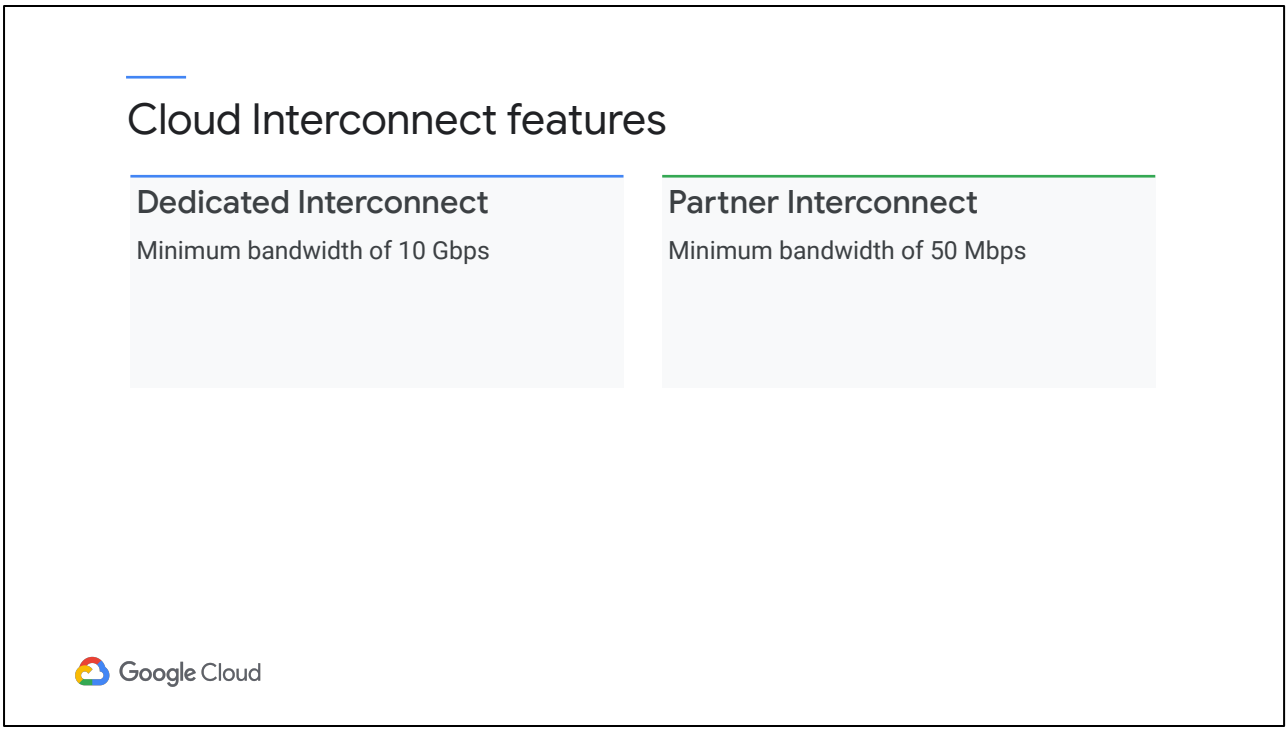
Dedicated interconnect provides a direct physical connection between your on-premises network and Google Cloud VPC networks.

Partner Interconnect



Google Cloud

Partner Interconnect provides connectivity between your on-premises network and Google Cloud VPC networks through a supported service provider.



When choosing an interconnect type, there are several features that need to be evaluated.

Dedicated interconnect has a minimum bandwidth of 10 Gbps. If you don't require 10 Gbps connections, Partner Interconnect starts at only 50 Mbps and provides a variety of capacity options

If more than 10 Gbps bandwidth is needed, multiple interconnects can be provisioned.

Cloud Interconnect setup

Dedicated Interconnect

- Requires routing equipment in a colocation facility that supports the regions that you want to connect to.
- Traffic flows directly between networks, not through the public internet.

Partner Interconnect

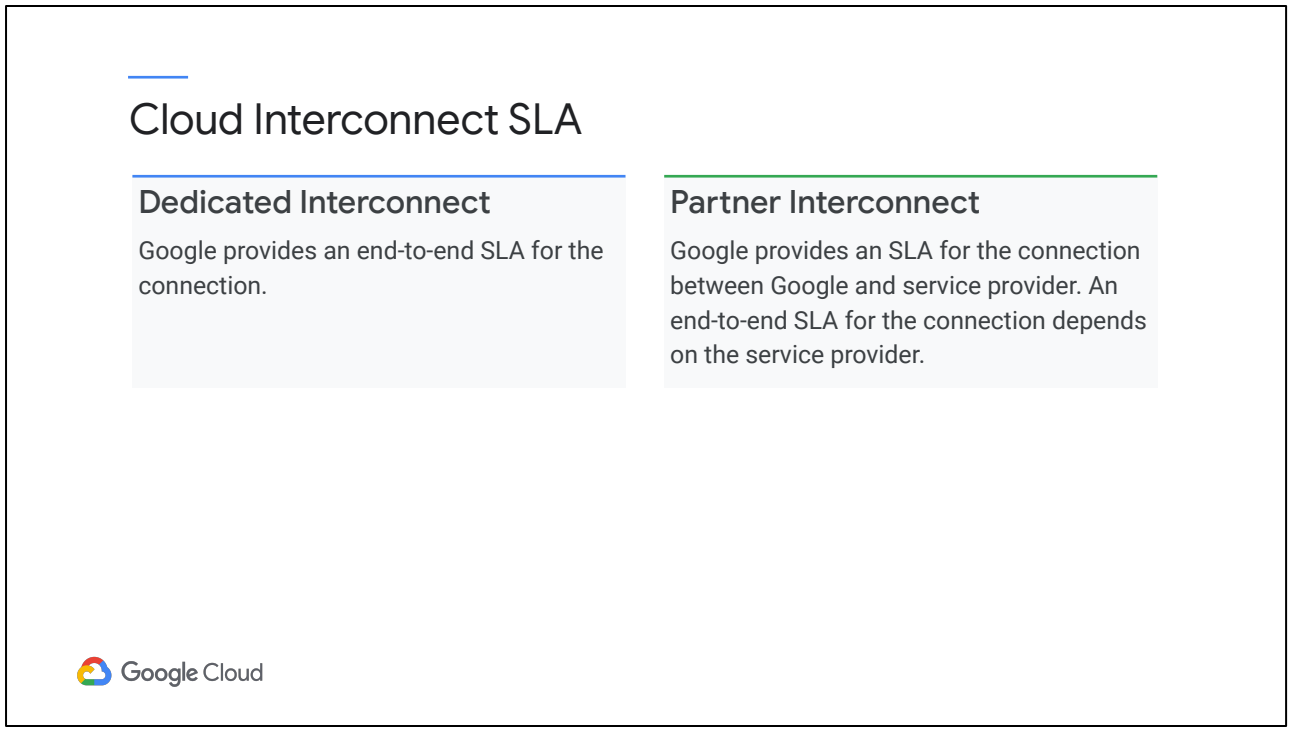
- Use any supported service provider to connect to Google.
- Traffic flows through a service provider, not through the public internet.

Google Cloud

Dedicated Interconnect requires routing equipment in a colocation facility that supports the Google Cloud regions that you want to connect to.

In this case, all traffic flows directly between your on-prem network and your VPC network. Nothing travels on the public Internet.

For users that can't physically meet Google's network in a colocation facility, you can use Partner Interconnect to connect to a variety of service providers to reach your VPC networks. All traffic flows through the service provider’s network, and nothing travels on the public Internet.



The service level agreement is slightly different depending on the interconnect type.

For Dedicated Interconnect, Google provides an end-to-end SLA for the connection.

For Partner Interconnect, Google provides an SLA for the connection between Google and service provider. An end-to-end SLA for the connection depends on the service provider.

Agenda

VPC Firewalls

Load Balancing and SSL Policies

Interconnect and Peering Options

Best Practices for VPC Networks

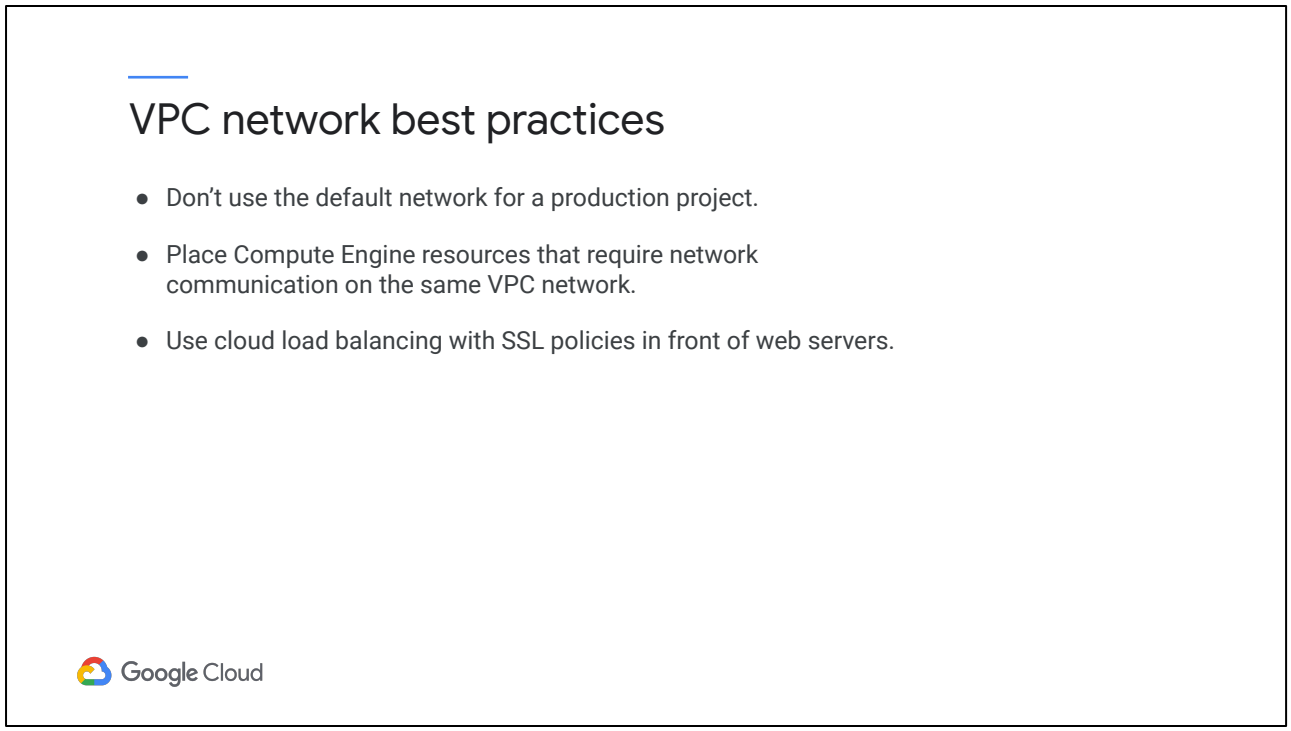
Lab: Configuring VPC Firewalls

VPC Flow Logs

Lab: Configuring and Using VPC Flow Logs in Cloud Logging

Quiz and Module Review

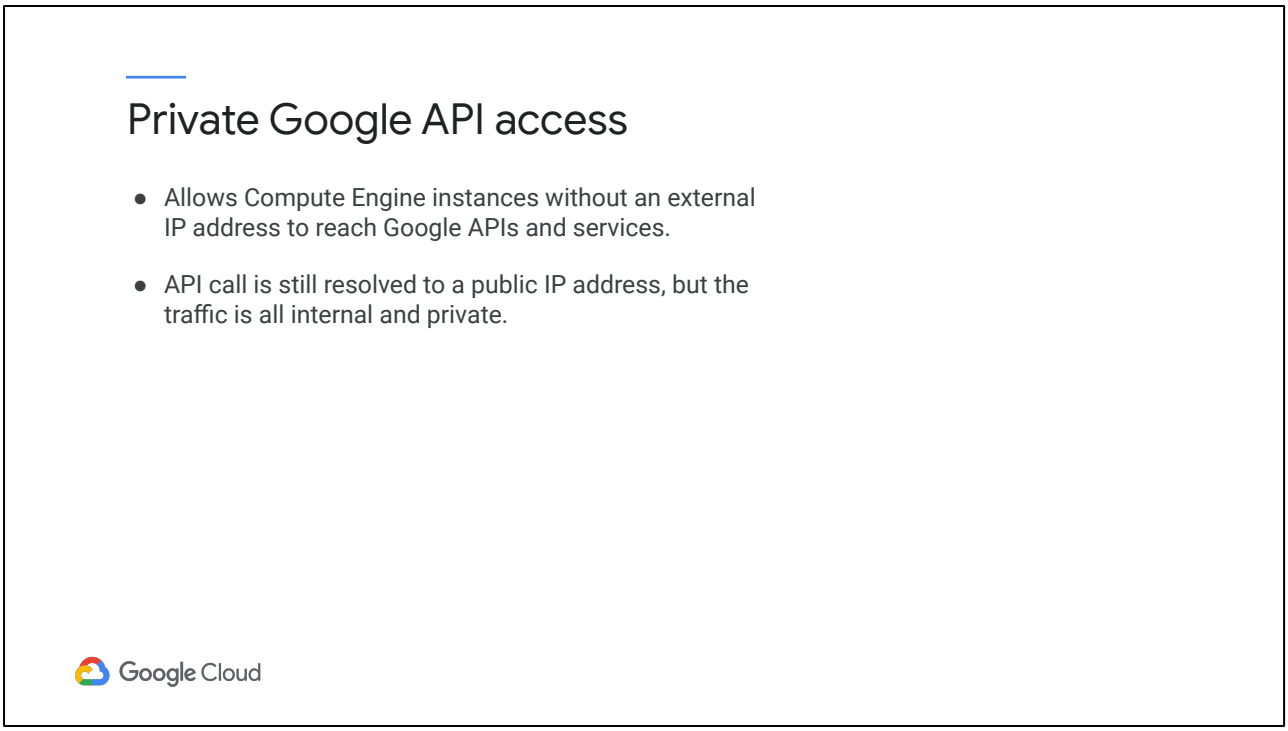
Using “best practices” for your VPC networking helps.



As we discussed earlier, the default network automatically has several firewall rules that are not desirable for production systems. While these default firewall rules can be modified, it is often best to not use the default network for a project. Instead, create a new network with the regions, IP address ranges, and firewall rules that your organization needs, then delete the default network so it’s not accidentally used.

Place Compute Engine resources that require network communication on the same VPC network. Create separate subnets within a network for each tier of an application.For example: web front end, services layer, and database back end.

Use a cloud load balancer with SSL policies in front of web servers. Placing a load balancer in front of all web servers provides many benefits, including a global anycast IP address and built in DDoS protection and mitigation. Using SSL policies allows you to control the SSL encryption being used for the encryption in transit.



Private Google API Access enables Compute Engine instances on a VPC subnet to reach Google APIs and services using an internal IP address rather than an external IP address.

Previously, you had to provide a public path for your internal Compute Engine instances (for example, an external IP address or a NAT gateway) to allow the instances to access Google APIs.

With Private Google Access, an API call is resolved to a public IP address, but the traffic is all internal and private. Network address translation is in Google's infrastructure and is transparent to the user.

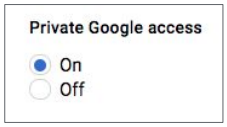
If Private Google Access is not enabled, an organization requires an external IP address to communicate with Google APIs. Although the communication is encrypted, this IP address can increase an organization’s risk by unnecessarily exposing its network to the internet. The Cloud and Developer APIs and services that can be reached include, but are not limited to, the following:

- BigQuery
- Cloud Bigtable
- Container Registry
- Dataproc
- Datastore
- Pub/Sub

- Cloud Spanner
- Cloud Storage

Private Google API access

- Is enabled/disabled on VPC subnets.
  - Disabled by default
- Subnet must still have a route to the default-internet-gateway set.



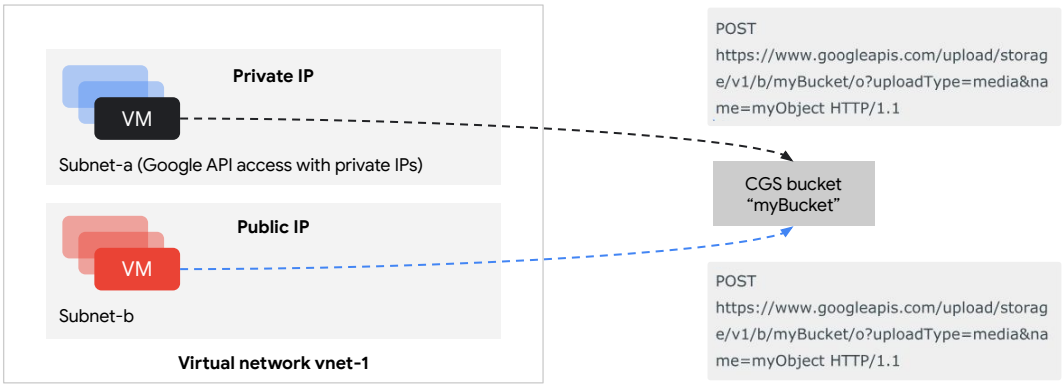
Name	Destination IP ranges	Priority	Instance tags	Next hop
default-route-1a75685f7b26cbcd	0.0.0.0/0	1000	None	Default internet gateway

Google Cloud

Private Google API access is enabled on Google VPC subnets. By default, newly created subnetworks don't have this feature enabled. You add this feature to your projects when you create a subnetwork or by modifying an existing subnetwork.

You must also ensure that any Compute Engine instance that accesses a Google API has a matching default-internet-gateway route set in its VPC network. All VPCs have a default-internet-gateway route, unless the route has been manually deleted.

Private Google API access example



Google Cloud

This diagram shows how a VPC network with two subnetworks, subnet-a and subnet-b, might implement Private Google Access. In this example, you want VM instances in subnet-a to have only internal (private) IP addresses and you also want those VMs to have access to the Cloud Storage bucket called myBucket in the diagram.

To accomplish this, you must ensure that there is a default route with next-hop default-internet-gateway in the VPC network. Then, on subnet-a, enable the Private Google access.

The VM instance without an external IP in subnet-a can now access the Cloud Storage bucket as long as the credentials used for the request have the IAM permissions for this bucket.

VPC Service Controls helps mitigate many security risks without sacrificing performance

- Unauthorized access using stolen credentials.
- Data exfiltration and compromised code.
- Public exposure of private data.

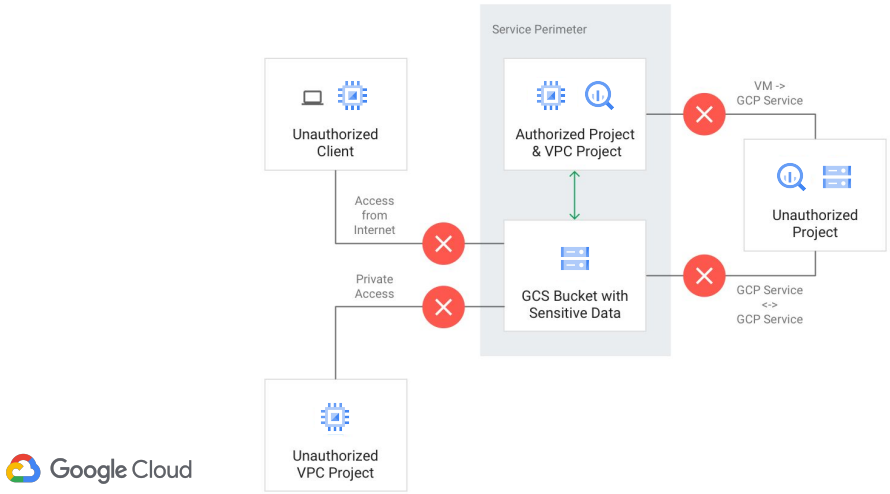
Google Cloud

VPC Service Controls improve your ability to reduce the risk of data exfiltration from your Google-managed services like Cloud Storage and BigQuery. VPC Service Controls create security perimeters around your Google-managed resources and allow you to control the movement of data across that perimeter.

VPC Service Controls

- Protect resources within a perimeter so they can only be privately accessed from clients within authorized VPC networks using Private Google Access with either Google Cloud or on-premises.
- Ensure clients within a perimeter that have private access to resources do not have access to unauthorized (potentially public) resources outside the perimeter.
- Prevent data from being copied to unauthorized resources outside the perimeter using service operations.
- Restrict Internet access to resources within a perimeter using allowlisted IPv4 and IPv6 ranges.

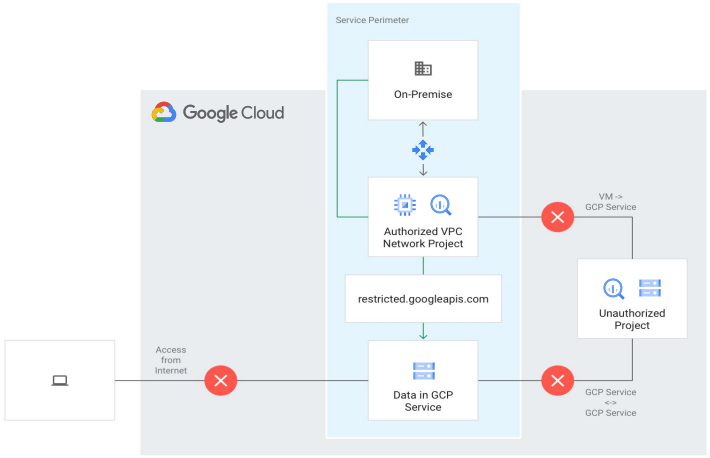
Prevent access to your Google-managed services outside of a trusted perimeter



VPC Service Controls provide an additional layer of security defense for Google Cloud services that is independent of IAM. While IAM enables granular *identity-based access control*, VPC Service Controls enables broader *context-based perimeter security*, including controlling data egress across the perimeter.

It is recommended that both VPC Service Controls and IAM be used for defense in depth.

Extend communication from your cloud resources to an on-premises environment

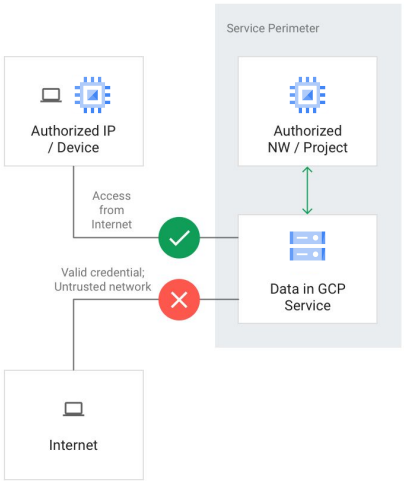


Google Cloud

Private Google Access on-premises extensions allow private communication between VPC networks that span hybrid cloud environments. VPC networks must be part of a service perimeter for VMs on that network to privately access managed Google Cloud resources within that service perimeter.

VMs with private IPs on a VPC network that is part of a service perimeter cannot access managed resources outside the service perimeter. For example, a VM within a VPC network that is part of a service perimeter can privately access a Cloud Storage bucket in the same service perimeter, but the VM will be denied access to Cloud Storage buckets that are outside of it.

Restrict access to your resources from the Internet by creating custom attribute-based access levels



Google Cloud

Access from the internet to managed resources within a service perimeter is denied by default. You can enable access based on the context of the request by creating access levels that control access based on a number of attributes, such as the source IP address.

Requests made from the internet are denied if they do not meet the criteria defined in the access level.

Cloud Console can be used to access resources within a perimeter, but you must configure an access level that allows access from one or more IPv4 and IPv6 ranges (or to specific user accounts.)

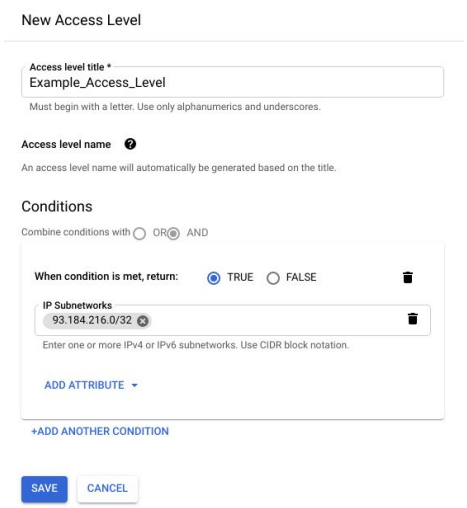
VPC Service Controls can be configured using any of three Google Cloud tools

- Cloud Console
- `gcloud` command-line tool
- Access Context Manager APIs

Google Cloud

The first two tools in this list - the Google Console and the gcloud command-line tool - are likely to already be familiar to you. Let's take a brief look at the third tool on this list, the Access Context Manager, which may not be as familiar to many Google Cloud users as the first two are...

Access Context Manager defines fine-grained attribute based controls for projects and resources



Google Cloud

So, what is Access Context Manager? Access Context Manager is a tool with an API that allows Google Cloud organization administrators to define fine-grained, attribute based access control for projects and resources in Google Cloud.

Administrators first define an access policy, which is an organization-wide container for organizing access levels and service perimeters, that includes the necessary requirements for requests to be allowed.

Requirements may include:

- Device type and operating system
- IP address
- User identity

Access Context Manager isn't responsible for policy enforcement. Its purpose is to describe the desired rules. Access policy is configured and enforced across various points, including through VPC Service Controls.

Access Context Manager reduces the size of your privileged network using defined access attributes

- Access Policies
- Access Levels
  - IP address
  - Device type
  - User identity

Google Cloud

What is an Access Policy?

An access policy acts as a container for access levels, and as such, a single access policy can contain multiple access levels. When using Access Context Manager to manage your Access Policies, you can create policies that are attached to a project - say, for quota purposes - but such policies are not restricted to just that project and can also be used elsewhere in your organization.

An access level is a set of attributes (such as IP address, device type and User identity) that are assigned to requests based on their origin. Using this information, when requests come in, you can decide what level of access to grant. Access levels are customizable; "High_Trust," "Medium_Trust," and “Low_Trust” are examples. You can specify multiple access levels as part of an access policy.

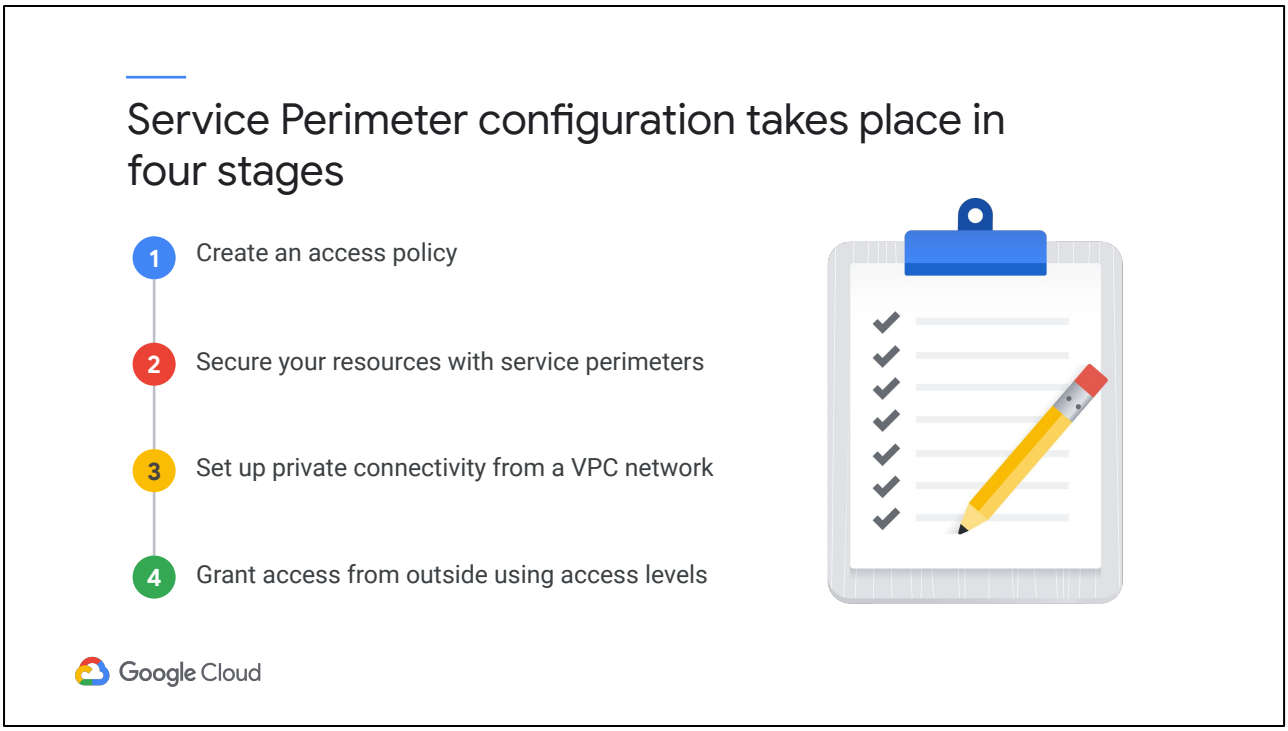
Now, let’s look a bit more closely at these assignable attributes.

The first attribute is IP address, which means you can grant a certain access level based upon the IP address of the originating request. The range of IPs to allow is specified in the form of a Classless Inter-Domain Routing (CIDR) block, which allows for an easily recognizable, simple, and fine-grained control over the IPs allowed. A single access level can contain one or multiple IP ranges.

Access Context Manager uses Endpoint Verification to gather information regarding user devices, including operating system and version. You can then grant an access level based on this data; for example, you might decide to grant a more permissive access level to devices running the latest version of the primary operating system deployed at your company.

In some instances, you may wish to grant an access level to specific entities - in this case, the identity of the requester determines whether the condition is met. This scenario is often often used in conjunction with Service Accounts and VPC Service Controls; for example, to enable a Cloud Function to access data protected by VPC Service Controls. Identity-only access levels can only be created and managed with the gcloud command line tool, not via the Google Cloud Console. Now that we have an understanding of the tools that can be used to set up VPC Service Control access policies, let’s go over the steps required to do so...

Now that we have a better understanding of the tools that can be used to set up access policies, let’s go over the steps required to actually configure and enable VPC service controls.



The four stages of a typical VPC service perimeter configuration are:

- Create an access policy.
- Secure your Cloud resources with service perimeters.
- Set up private connectivity from a VPC network.
- Grant access from the outside using access levels.

Let's look at each of these stages in more detail.

An access policy (one per Organization) collects the service perimeters and access levels you have created. When service perimeters are created and managed using the VPC Service Controls page of the Cloud Console, you do not need to manually create an access policy.
However, when using the gcloud command-line tool or the Access Context Manager APIs to create and configure your service perimeters, you must first create an access policy.

Service perimeters are used to protect services used by projects in your Organization, after you have identified the projects and services you want to protect. If you are using a Shared VPC, you must include the host project in the service perimeter along with any projects that belong to the Shared VPC.

Use Private Google Access to provide additional security for VPC networks that are protected by a service perimeter. Restricting access to Google Cloud resources to only private access from VPC networks means that access using interfaces such as

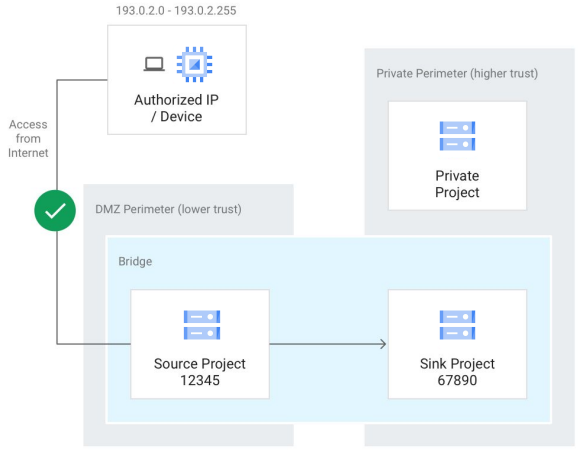
the Cloud Console and the the Google Cloud operations suite console will be denied. You can continue to use the gcloud command-line tool or API clients from VPC networks that share a service perimeter or perimeter bridge with the restricted resources.

Access levels can be used to allow requests from outside a service perimeter to resources which are protected by that perimeter, but do not permit protected projects to access resources from outside the perimeter.

Access levels protected by VPC Service Controls can be set to accept access requests from public IPv4 and IPv6 CIDR blocks, or individual user and service accounts. If you are restricting resources using private connectivity from VPC networks, you can re-enable access by using the Cloud Console to add a CIDR block to an access level that includes the public IP address of the host where the Cloud Console is being used.

If you want to re-enable the Cloud Console for a specific user regardless of IP address, add that user account as a member to the access level.

VPC Service Controls can also allow communication between two perimeters using a service perimeter bridge



Google Cloud

Can VPC Service Controls be used in a hybrid cloud environment? Yes, they can!

Perimeter bridges can be used to enable communication between projects in different service perimeters. Keep in mind that a project can belong to more than one perimeter *bridge* but can only be included in one service perimeter.

Agenda

VPC Firewalls

Load Balancing and SSL Policies

Interconnect and Peering Options

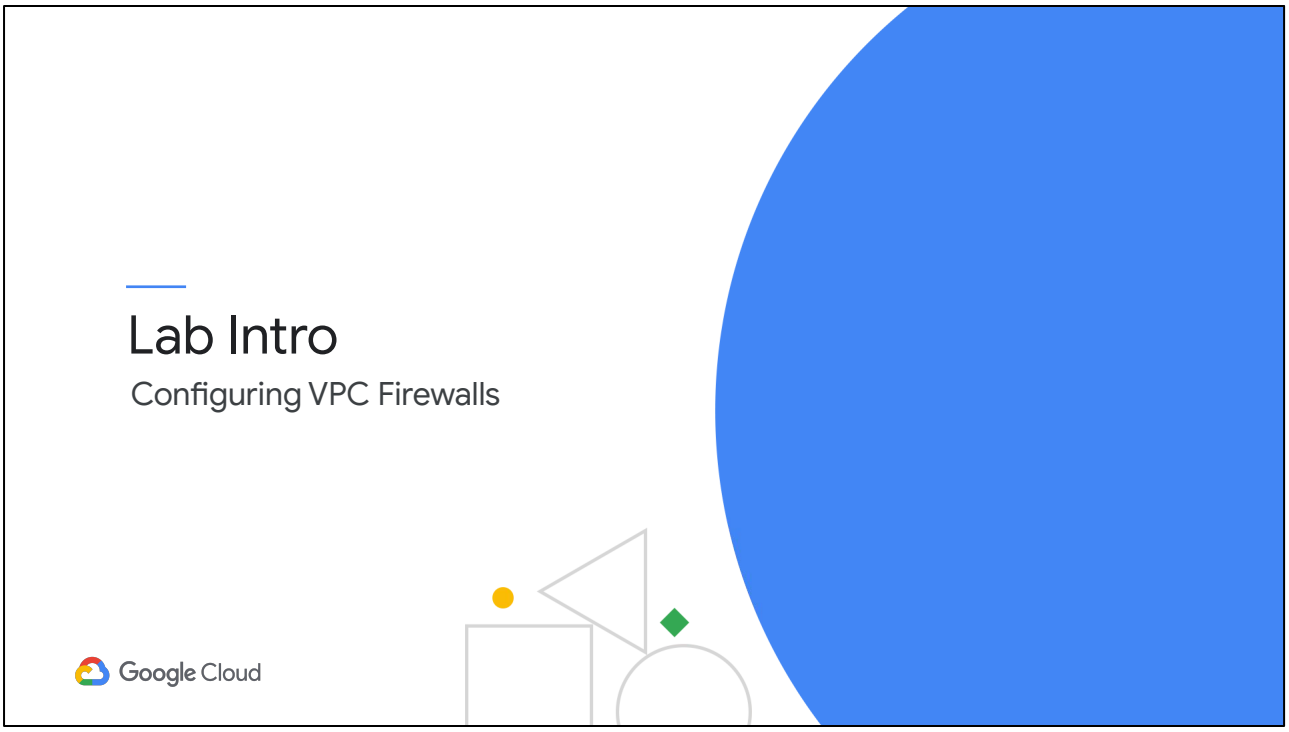
Best Practices for VPC Networks

Lab: Configuring VPC Firewalls

VPC Flow Logs

Lab: Configuring and Using VPC Flow Logs in Cloud Logging

Quiz and Module Review



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

- Create an auto-mode network, a custom-mode network, and associated subnetworks
- Investigate firewall rules in the default network and then delete the default network
- Learn how to use features of Firewall rules for more precise and flexible control of connections

Agenda

VPC Firewalls

Load Balancing and SSL Policies

Interconnect and Peering Options

Best Practices for VPC Networks

Lab: Configuring VPC Firewalls

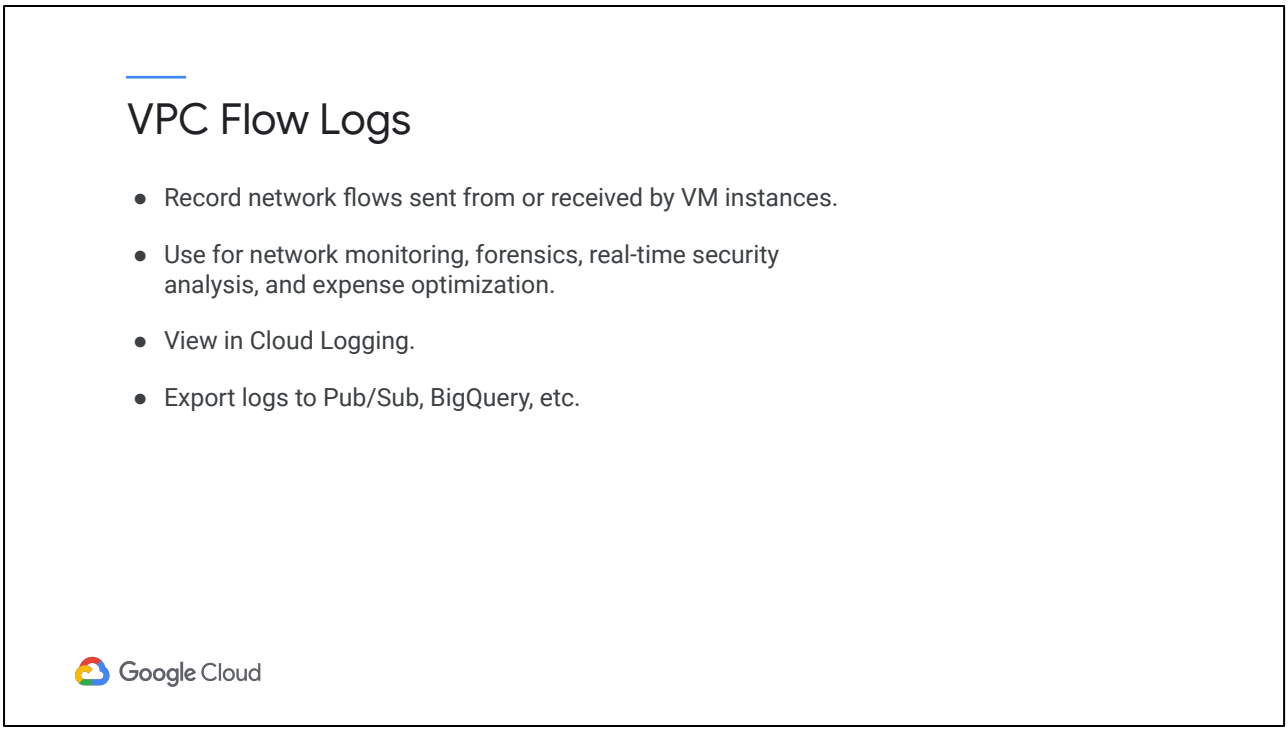
VPC Flow Logs

Lab: Configuring and Using VPC Flow Logs in Cloud Logging

Quiz and Module Review

Google Cloud

Now let's have a look at VPC Flow Logs.



VPC Flow Logs record network flows sent from or received by VM instances. VPC flow logs will only include traffic seen by a VM, For example if outbound traffic was blocked by an egress rule, it will be seen and logged, but inbound traffic blocked by an ingress rule, not reaching a VM, will not be seen and not logged.

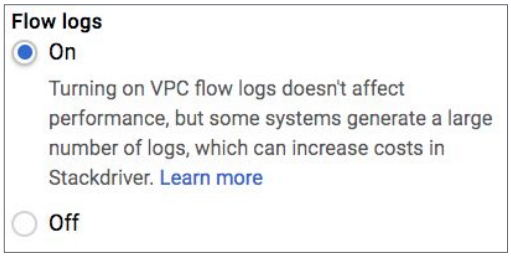
These logs can be used to monitor network traffic to and from your VMs, forensics, real-time security analysis, and expense optimization.

You can view flow logs in Cloud Logging - formerly known as Stackdriver Logging - and you can export logs to any destination that Cloud Logging export supports - Pub/Sub, BigQuery, etc.

Flow logs are aggregated by connection, at 5-second intervals, from Compute Engine VMs and exported in real time. By subscribing to Pub/Sub, you can analyze flow logs using real-time streaming APIs.

VPC Flow Logs

- Is enabled on VPC subnets
  - Disabled by default



- No performance penalty

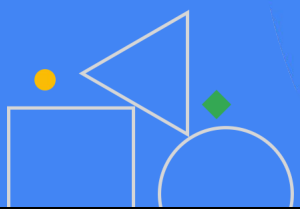
Google Cloud

You can enable or disable VPC Flow Logs per VPC network subnet. When you enable VPC Flow Logs, you enable for all VMs in a subnet.

VPC Flow Logs is natively built into the networking stack of the VPC network infrastructure. There is no extra delay and no performance penalty in routing the logged IP packets to their destination, but some systems generate a large number of logs, which can increase costs in Cloud Logging.

Demo

Securing Projects with VPC Service Controls



Now I’m going to show you a quick demo that goes over how to secure projects to prevent data exfiltration by creating a service perimeter.

Agenda

VPC Firewalls

Load Balancing and SSL Policies

Interconnect and Peering Options

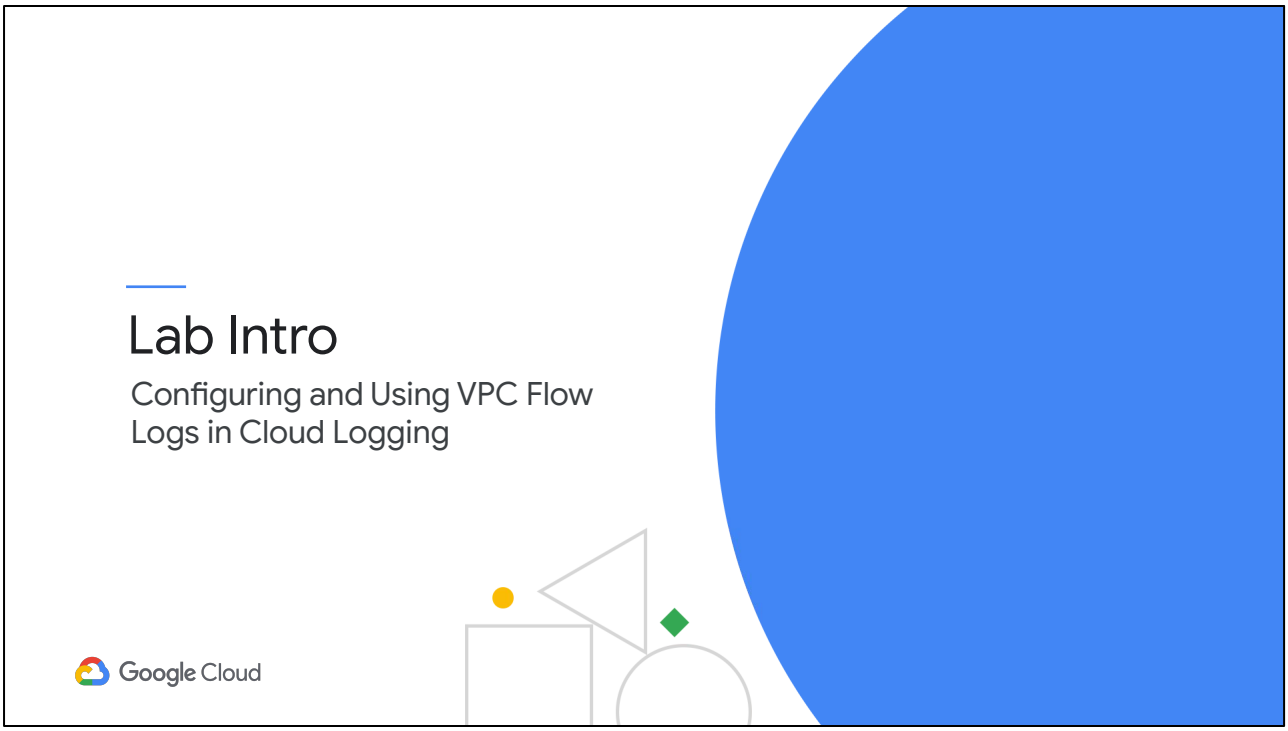
Best Practices for VPC Networks

Lab: Configuring VPC Firewalls

VPC Flow Logs

Lab: Configuring and Using VPC Flow Logs in Cloud Logging

Quiz and Module Review



In this lab, you learn how to work with VPC flow logs. You will enable VPC flow logging and then use Cloud Logging to access the logs. You will filter logs for specific subnets, VMs, ports, or protocols. You will also perform network monitoring, forensics, and real-time security analysis. When finished, you will disable VPC flow logging.

Agenda

VPC Firewalls

Load Balancing and SSL Policies

Interconnect and Peering Options

Best Practices for VPC Networks

Lab: Configuring VPC Firewalls

VPC Flow Logs

Lab: Configuring and Using VPC Flow Logs in Cloud Logging

Quiz and Module Review

Quiz #1

Question

Which TWO of the following statements about VPCs is TRUE?

A. Every VPC network functions as a distributed firewall where firewall rules are defined at the network level.

B. Google Cloud firewall allow rules by default only affect traffic flowing in one direction.

C. A connection is considered active if it has at least one packet sent over a one hour period.

D. VPC firewall rules in Google Cloud are global in scope.

Quiz #1

Answer

Which TWO of the following statements about VPCs is TRUE?

A. Every VPC network functions as a distributed firewall where firewall rules are defined at the network level.

B. Google Cloud firewall allow rules by default only affect traffic flowing in one direction.

C. A connection is considered active if it has at least one packet sent over a one hour period.

D. VPC firewall rules in Google Cloud are global in scope.

Google Cloud

A. Since VPC networks can be global in Google Cloud, firewall rules are also global.
D. Google Cloud firewall rules exist not only between your instances and other networks, but also between individual instances within the same network.

Quiz #2

Question

Which THREE of the following are firewall rule parameters?

A. Action
B. Direction
C. IP Address
D. Organization
E. Project
F. Source
G. Timestamp

Quiz #2

Answer

Which THREE of the following are firewall rule parameters?

A. Action
B. Direction
C. IP Address
D. Organization
E. Project
F. Source
G. Timestamp

Google Cloud

A. An action, represented by either allow or deny, determines whether a rule permits or blocks traffic.
B. Direction can be either egress or ingress.
C. However, the source parameter is only applicable to ingress rules.

Quiz #3

Question

Which ONE of the following statements is TRUE when discussing the SSL capabilities of the Google Cloud load balancer?

A. You must use one of the 3 pre-configured “Google-managed profiles” to specify the level of compatibility appropriate for your application.

B. Google Cloud load balancers require, and will only accept, a Google-managed SSL Cert.

C. The Google-managed profile, COMPATIBLE, allows clients which support out-of-date SSL features.

D. If no SSL policy is set, the SSL policy is automatically set to the most constrained policy, which is RESTRICTED.

Quiz #3

Answer

Which ONE of the following statements is TRUE when discussing the SSL capabilities of the Google Cloud load balancer?

A. You must use one of the 3 pre-configured “Google-managed profiles” to specify the level of compatibility appropriate for your application.

B. Google Cloud load balancers require, and will only accept, a Google-managed SSL Cert.

C. The Google-managed profile, COMPATIBLE, allows clients which support out-of-date SSL features.

D. If no SSL policy is set, the SSL policy is automatically set to the most constrained policy, which is RESTRICTED.

Google Cloud

C. The other two profiles, MODERN and RESTRICTED allow you to restrict SSL usage to clients with modern capabilities, or to restrict SSL access even further to meet compliance requirements.

Module Review

- Ensure firewall rules use the model of least privilege.
  - Minimize direct exposure to/from the internet.
  - Prevent ports and protocols from being exposed unnecessarily.
- SSL policies specify the minimum TLS version clients can connect with and a profile of SSL policy features.
- VPC peering allows you to create connectivity across two nonoverlapping VPC networks.
- Shared VPC allows an organization to connect resources from multiple projects to a common VPC network.
- Cloud Interconnect offers options for connecting on-premises network to Google Cloud.
- VPC flow logs are used for network monitoring, forensics, real-time security analysis, and expense optimization.


Google Cloud