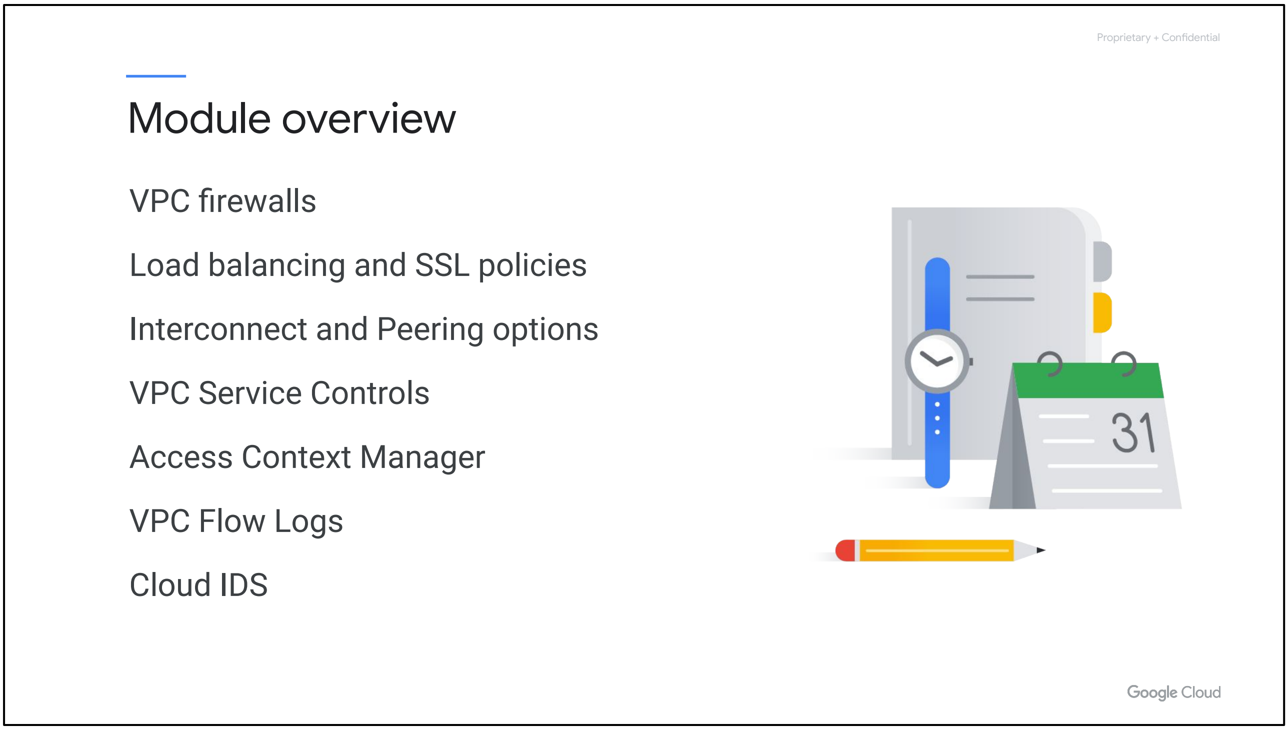
Configuring Virtual Private Cloud for Isolation and Security

Welcome to module 4 of Managing Security in Google Cloud: **Configuring Virtual Private Cloud for Isolation and Security**.



Module overview

VPC firewalls

Load balancing and SSL policies

Interconnect and Peering options

VPC Service Controls

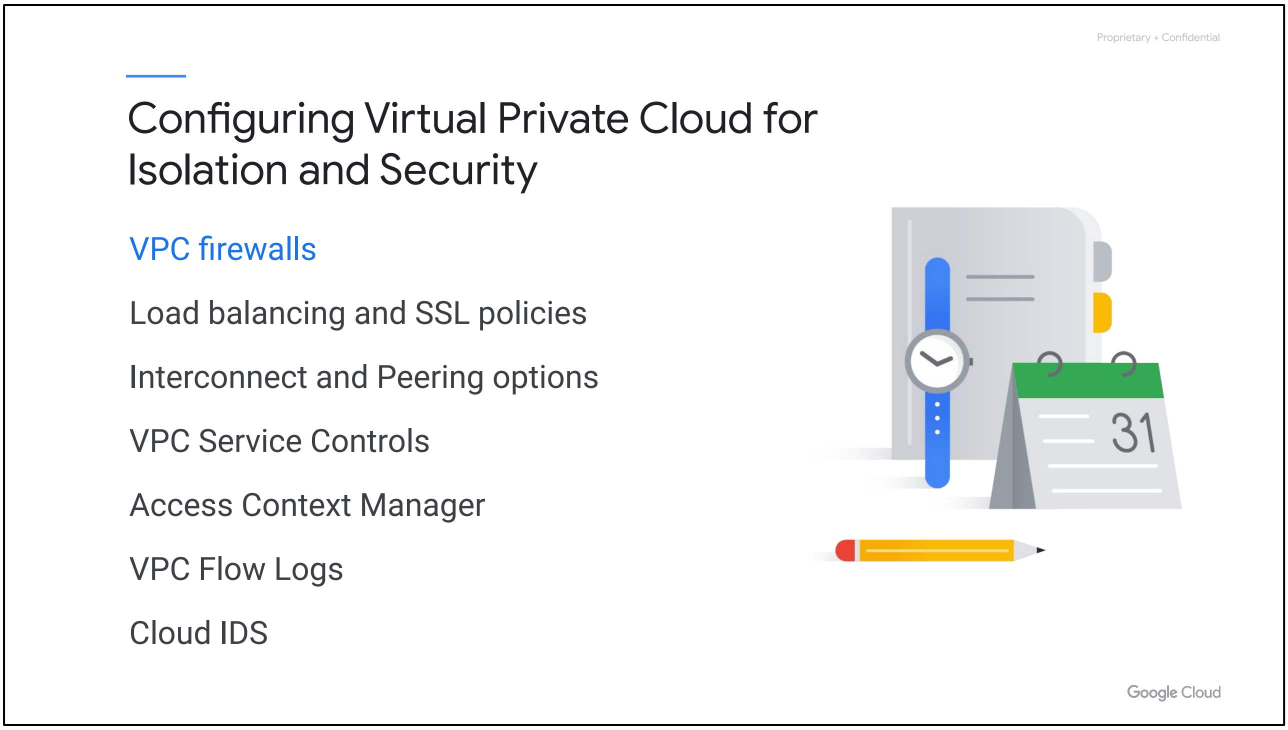
Access Context Manager

VPC Flow Logs

Cloud IDS

In this module, we will discuss many VPC related security concepts including VPC firewalls, load balancing SSL policies, network interconnect and peering options, VPC service controls, and access context manager, VPC flow logs, and Cloud IDS.

You will also have the opportunity to practice what you’ve learned, by completing the **Configuring VPC Firewalls**, **Configuring and Using and Viewing VPC Flow Logs in Cloud Logging**, and **Getting Started with Cloud IDS** labs.



Configuring Virtual Private Cloud for Isolation and Security

VPC firewalls

Load balancing and SSL policies

Interconnect and Peering options

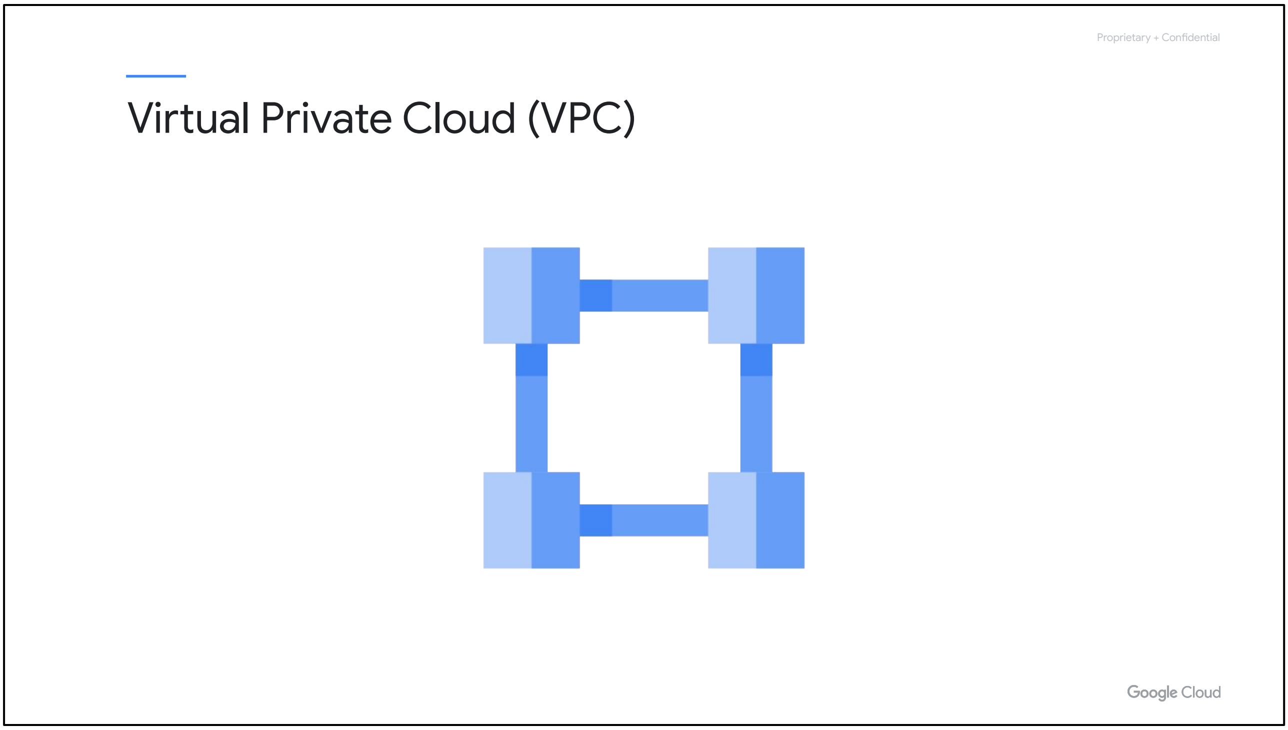
VPC Service Controls

Access Context Manager

VPC Flow Logs

Cloud IDS

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



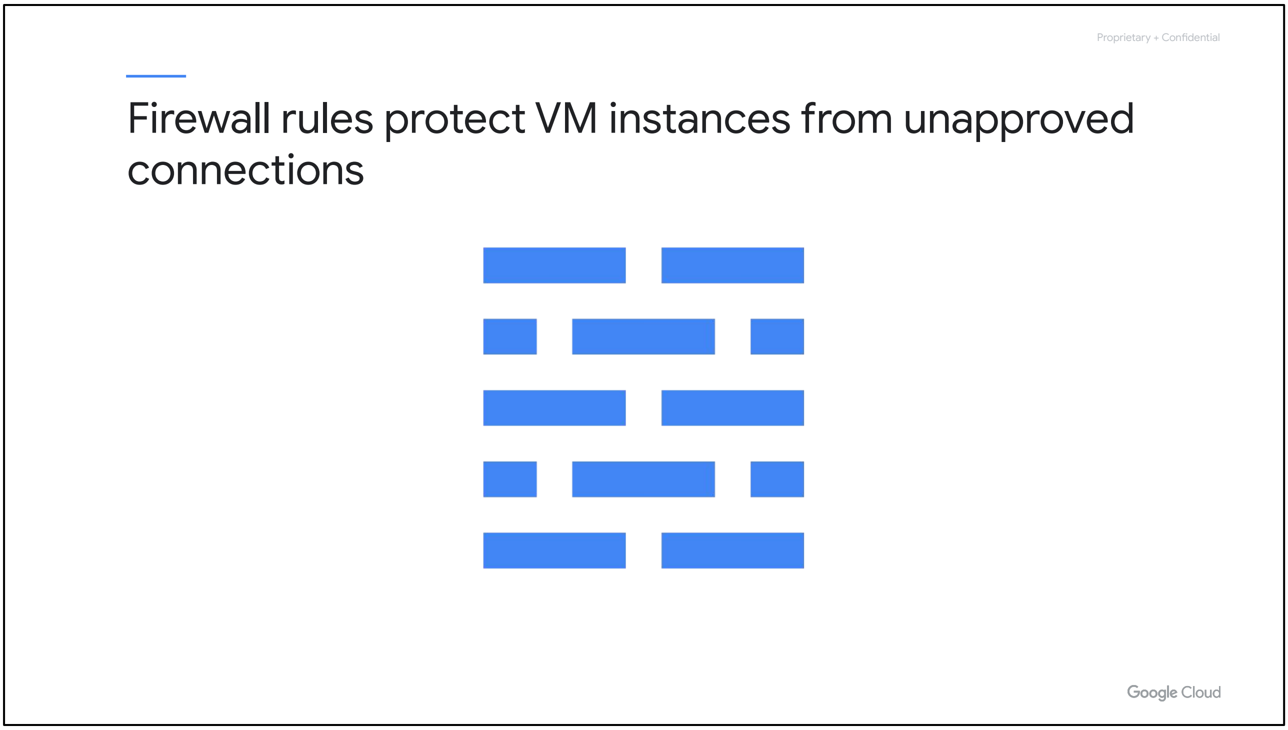
Virtual Private Cloud (VPC)

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.

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.



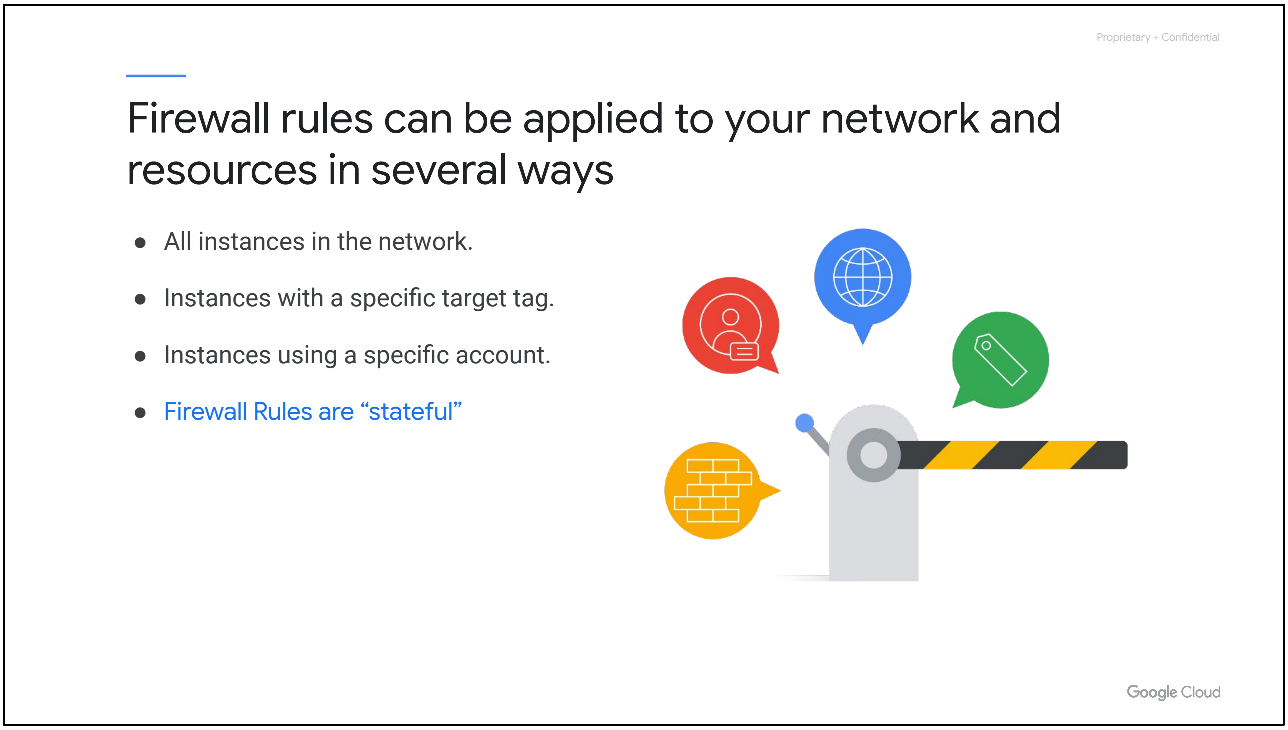
Firewall rules protect VM instances from unapproved connections

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.



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 account.
- Firewall Rules are “stateful”

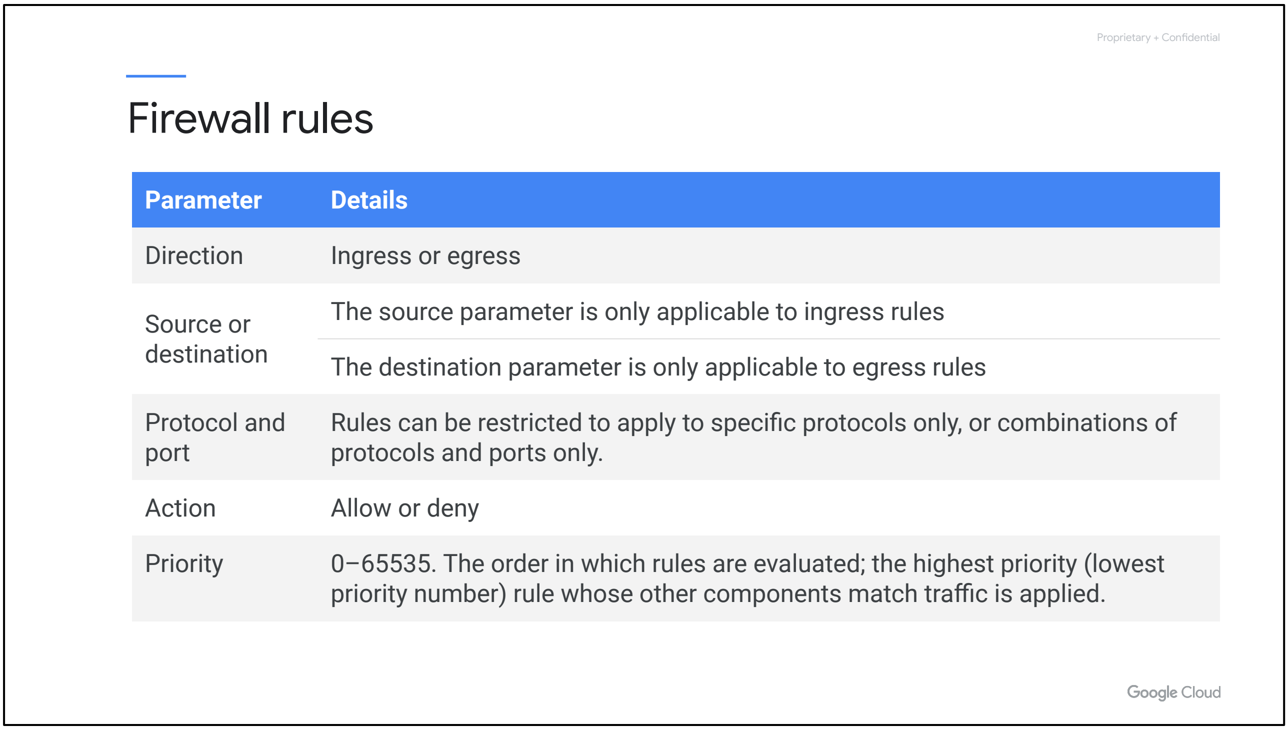
Applying rules to all instances in the network means the rule will apply to every instance running in that VPC network without having to tag or mark the instances in any other way.

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.



Proprietary + Confidential

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 highest priority (lowest priority number) rule whose other components match traffic is applied.

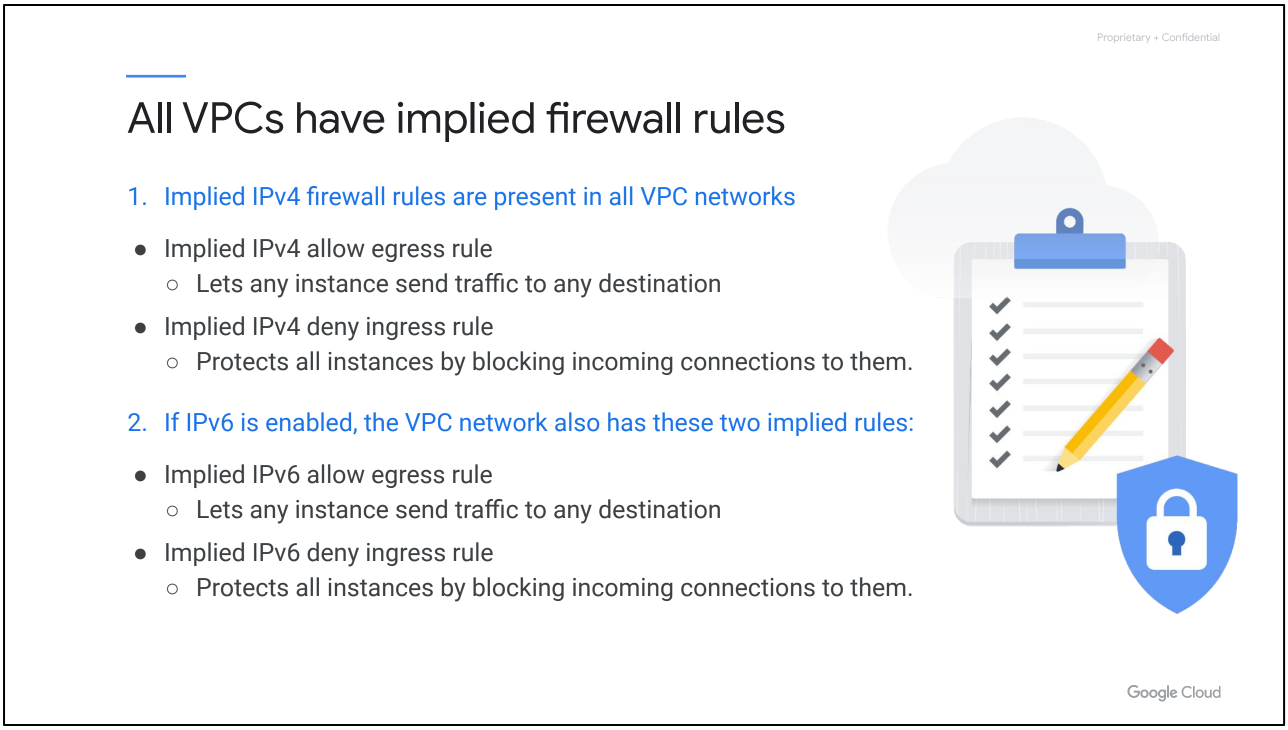
Google Cloud

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 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.



Proprietary + Confidential

All VPCs have implied firewall rules

1. 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.

2. 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.

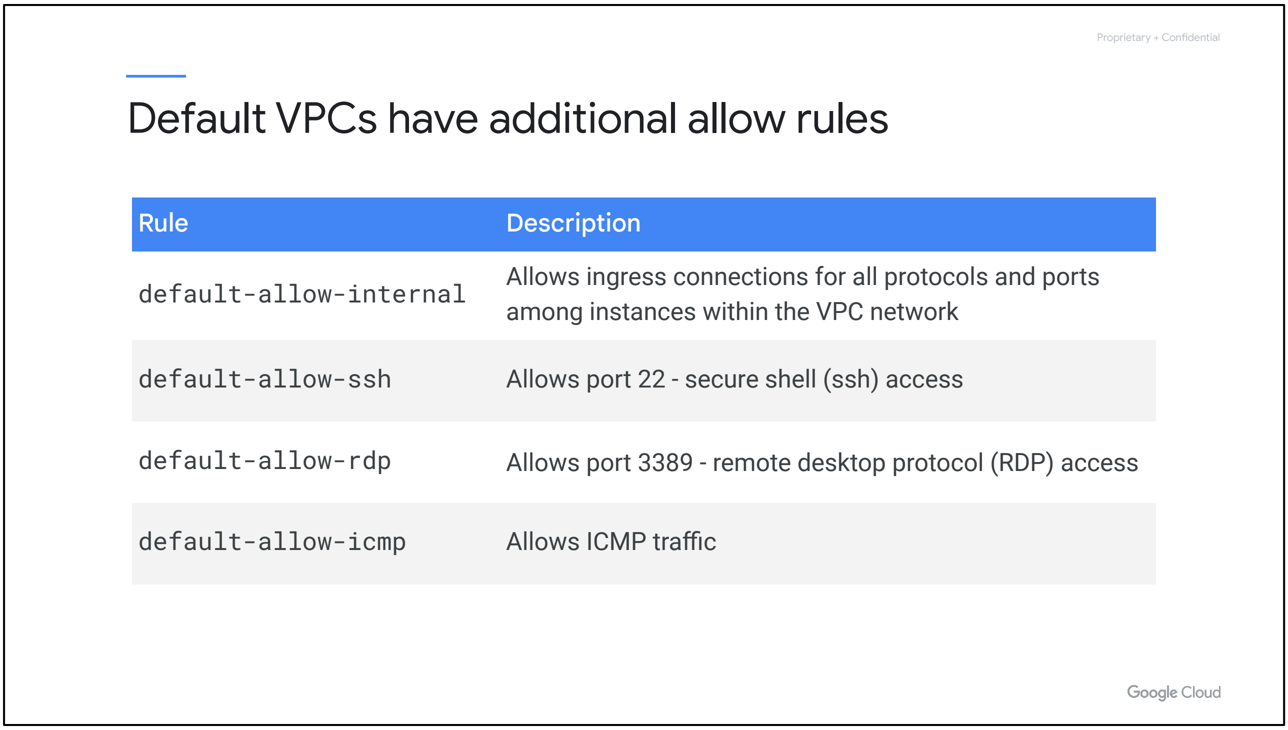
- **Implied IPv6 deny ingress rule.** An ingress rule whose action is deny, source

- 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

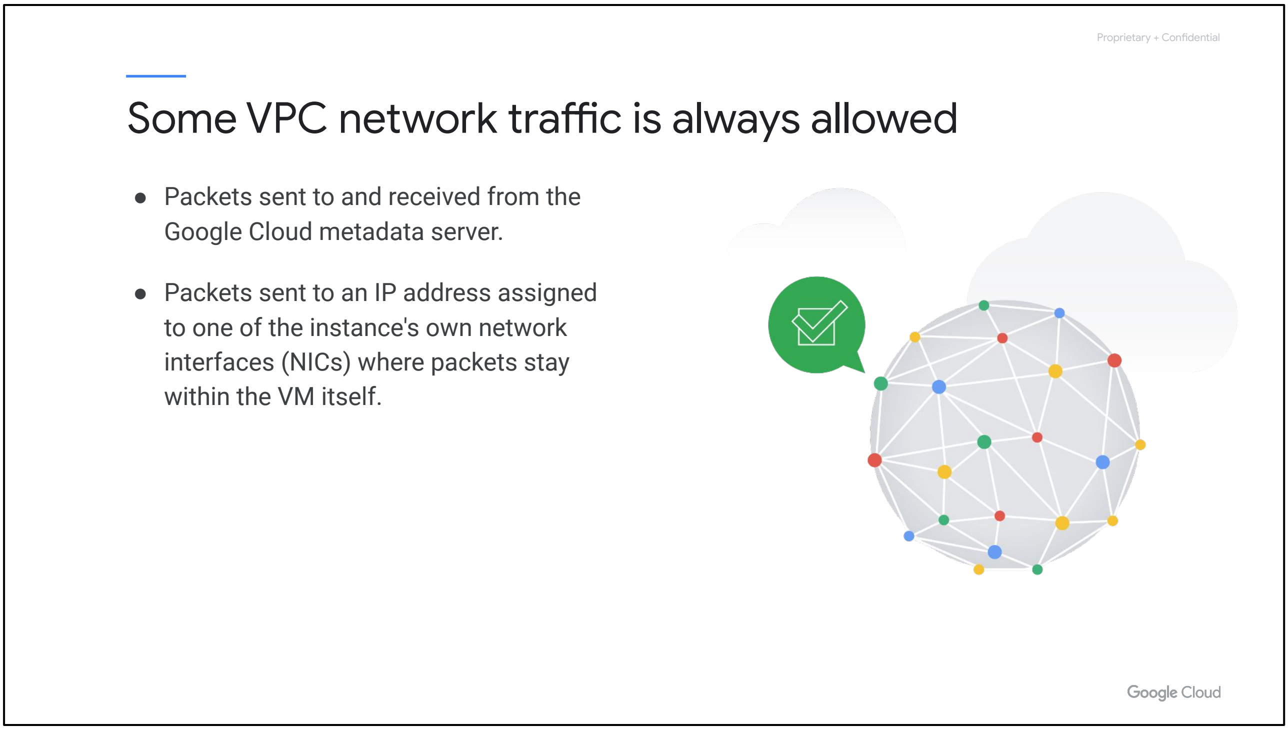
Google Cloud

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.



Proprietary + Confidential

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

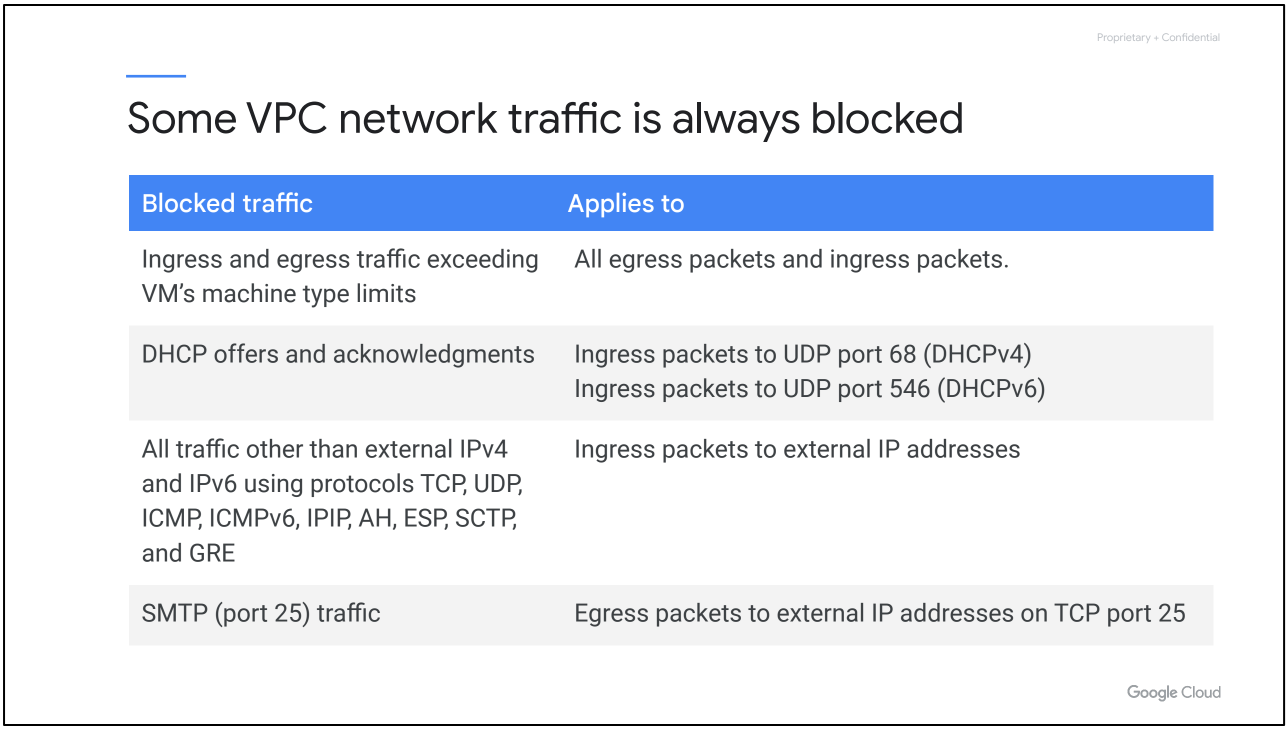
Some network traffic is always allowed.

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

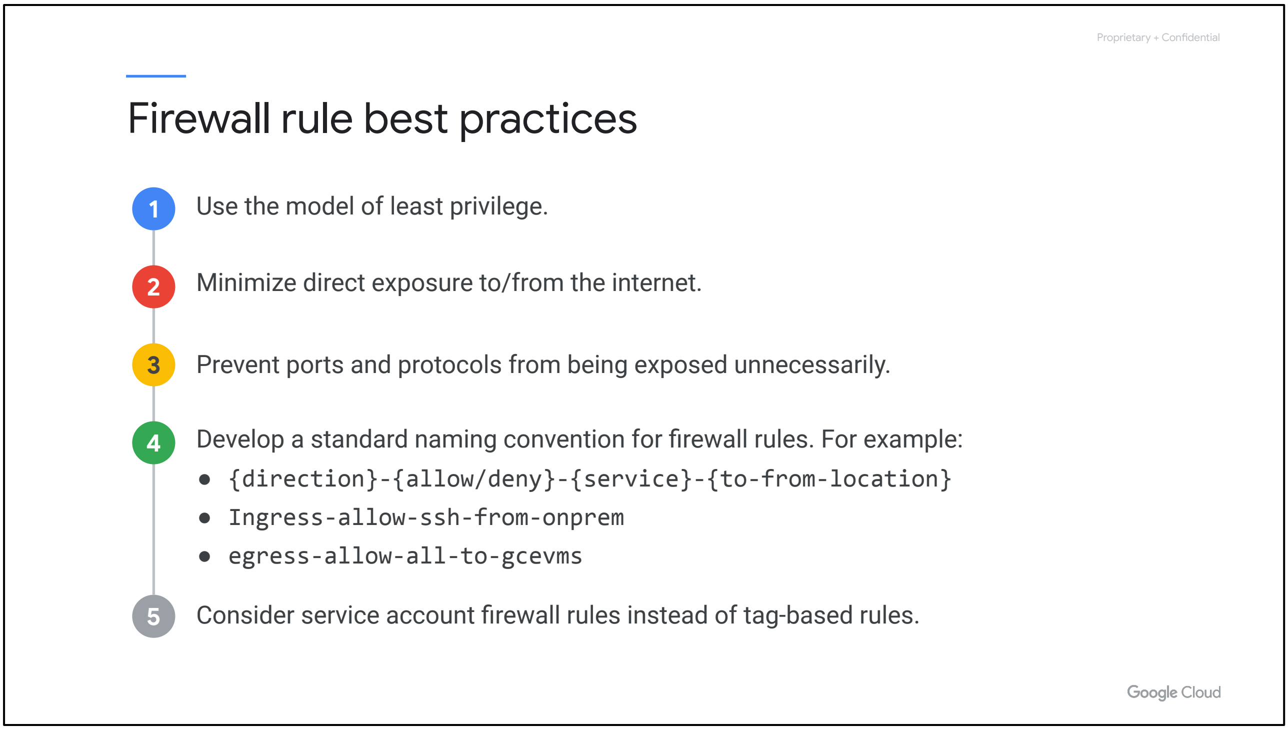
Blocked traffic	Applies to
Ingress and egress traffic exceeding VM's machine type limits	All egress packets and ingress packets.
DHCP offers and acknowledgments	Ingress packets to UDP port 68 (DHCPv4) Ingress packets to UDP port 546 (DHCPv6)
All traffic other than external IPv4 and IPv6 using protocols TCP, UDP, ICMP, ICMPv6, IPIP, AH, ESP, SCTP, and GRE	Ingress packets to external IP addresses
SMTP (port 25) traffic	Egress packets to external IP addresses on TCP port 25

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

- Google Cloud accounts for bandwidth per VM instance, for each network interface (NIC) or IP address. A VM's machine type defines its maximum possible egress rate; however, you can only achieve that maximum possible egress rate in specific situations. Google Cloud protects each VM by limiting ingress traffic delivered to an external IP address associated with the VM.
- 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.
- By default, Google Cloud blocks egress packets sent to TCP destination port 25 of an external IP address (including an external IP address of another Google Cloud resource). However, this traffic is not blocked in projects owned by select Google Cloud customers.

Check out the link in the speaker notes for more information on blocked traffic.

- **Link:** cloud.google.com/vpc/docs/firewalls#blockedtraffic



Proprietary + Confidential

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.

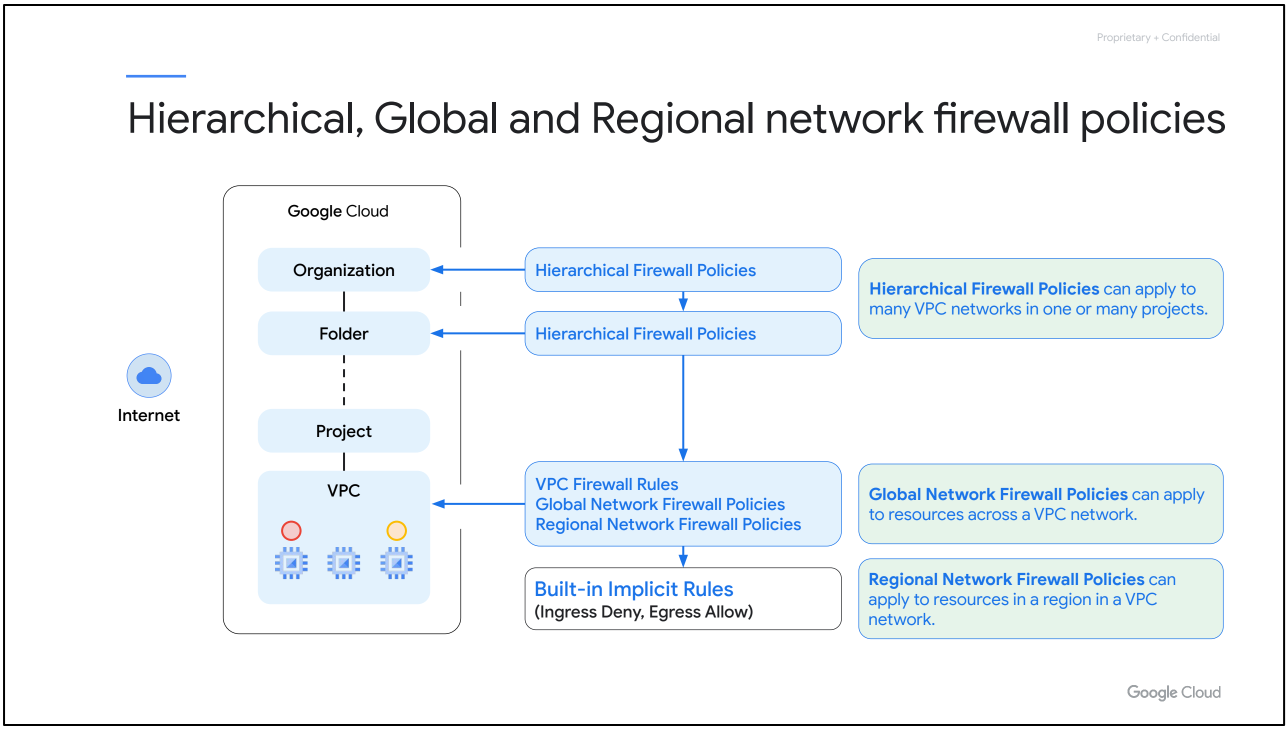
3. To prevent ports and protocols from being exposed accidentally, create a firewall rule with the lowest priority that blocks all outbound traffic for all protocols and ports. This rule will override the implied egress rule that allows all outbound traffic and instead lock down your Compute Engine instances 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 Admin role, but users require explicit IAM rights to use a service account.



Proprietary + Confidential

Hierarchical, Global and Regional network firewall policies

Google Cloud

Organization

Folder

Project

VPC

Internet

Hierarchical Firewall Policies

Hierarchical Firewall Policies

VPC Firewall Rules
Global Network Firewall Policies
Regional Network Firewall Policies

Built-in Implicit Rules
(Ingress Deny, Egress Allow)

Hierarchical Firewall Policies can apply to many VPC networks in one or many projects.

Global Network Firewall Policies can apply to resources across a VPC network.

Regional Network Firewall Policies can apply to resources in a region in a VPC network.

Google Cloud

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.

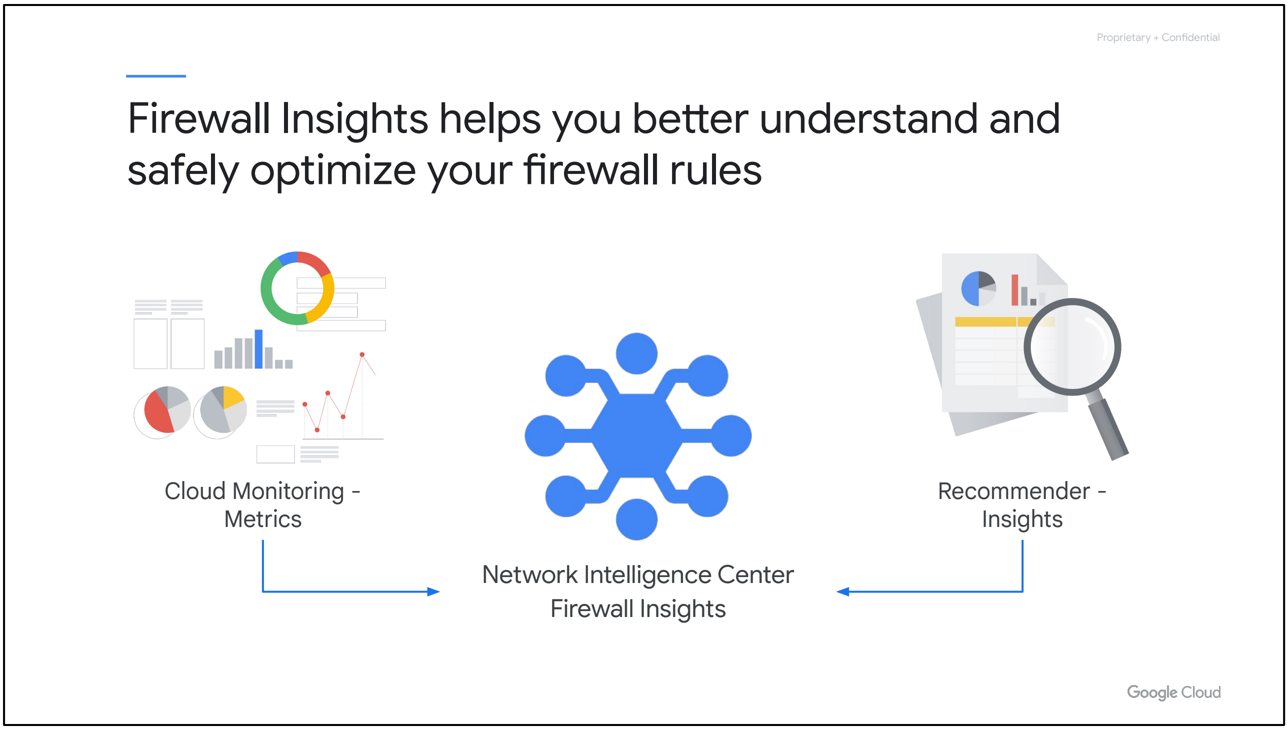
Global and regional network firewall policies improve upon the previous VPC firewall rules structure.

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.



Proprietary + Confidential

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.

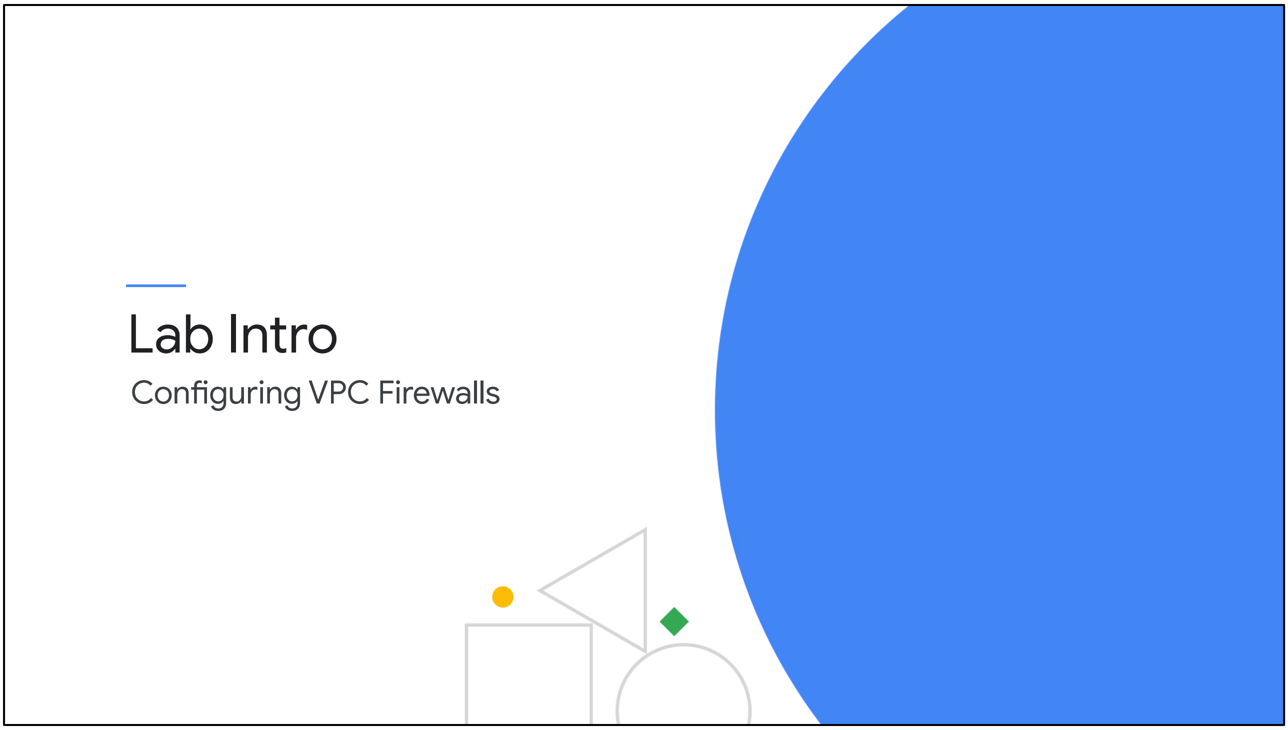
Firewall Insights uses Cloud Monitoring metrics and Recommender insights.

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

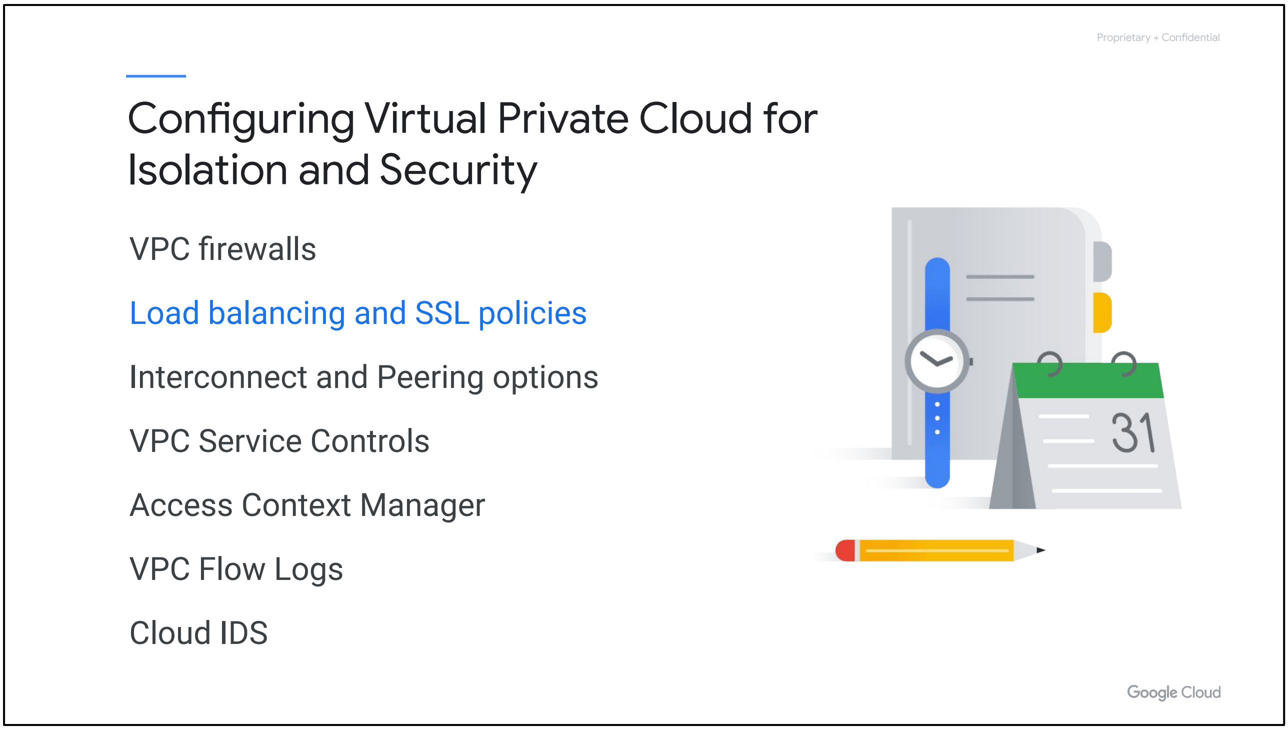


Lab Intro

Configuring VPC Firewalls

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
- And learn how to use features of Firewall rules for more precise and flexible control of connections



Proprietary + Confidential

Configuring Virtual Private Cloud for Isolation and Security

VPC firewalls

Load balancing and SSL policies

Interconnect and Peering options

VPC Service Controls

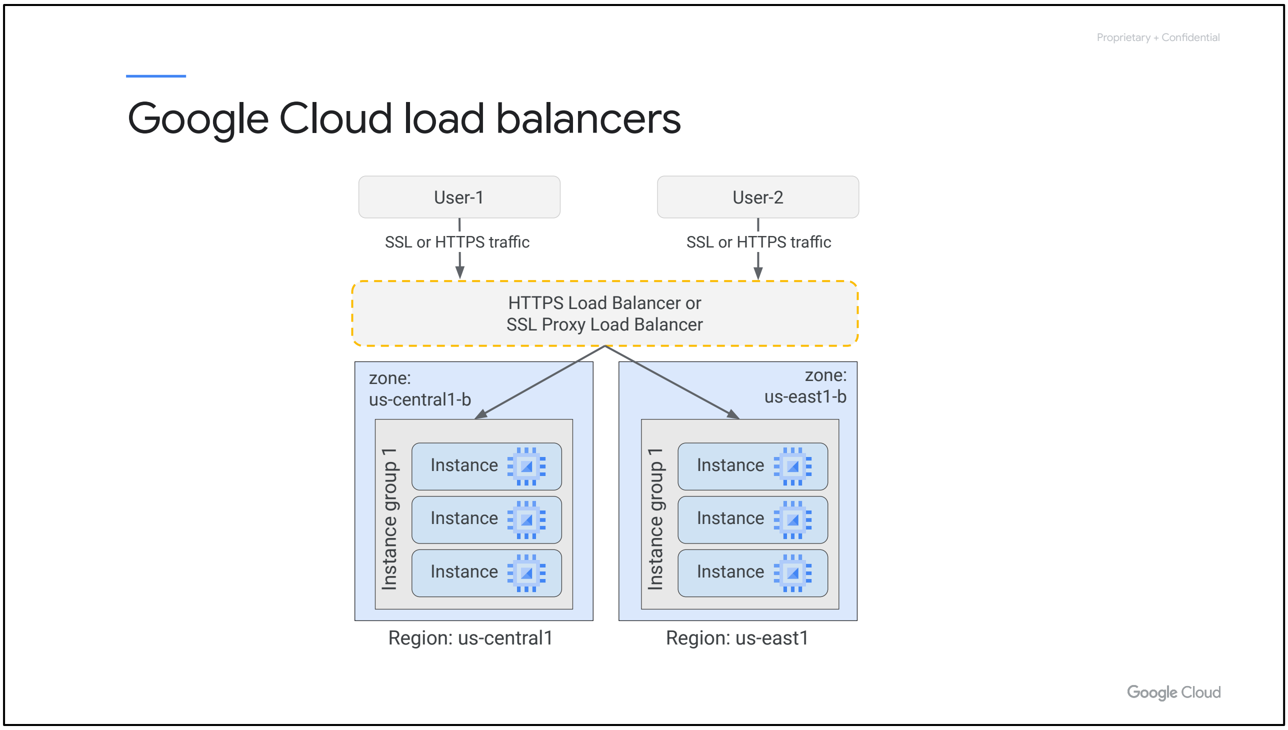
Access Context Manager

VPC Flow Logs

Cloud IDS

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.



Proprietary + Confidential

Google Cloud load balancers

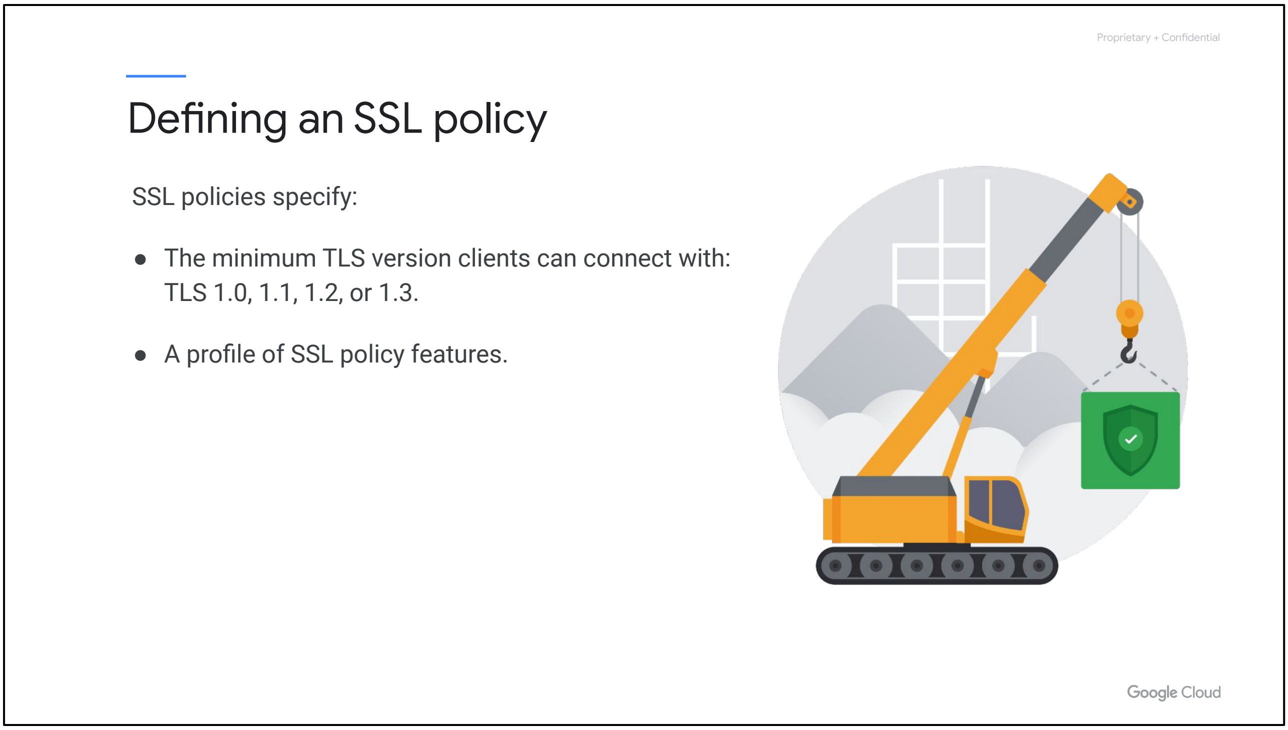
Google Cloud

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.

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.



Defining an SSL policy

SSL policies specify:

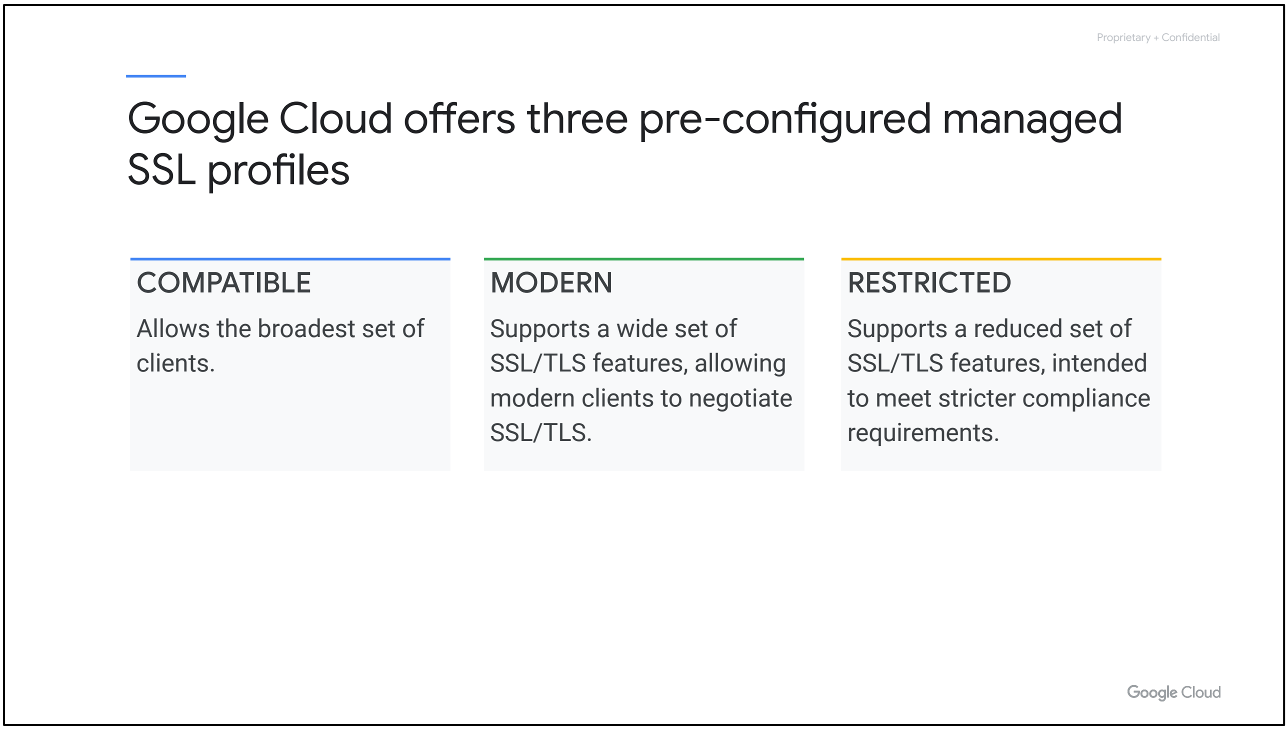
- The minimum TLS version clients can connect with: TLS 1.0, 1.1, 1.2, or 1.3.
- A profile of SSL policy features.

Google Cloud

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, 1.2, and 1.3.

Using SSL policies allows you to control the SSL encryption being used for the encryption in transit.



Google Cloud offers three pre-configured managed SSL profiles

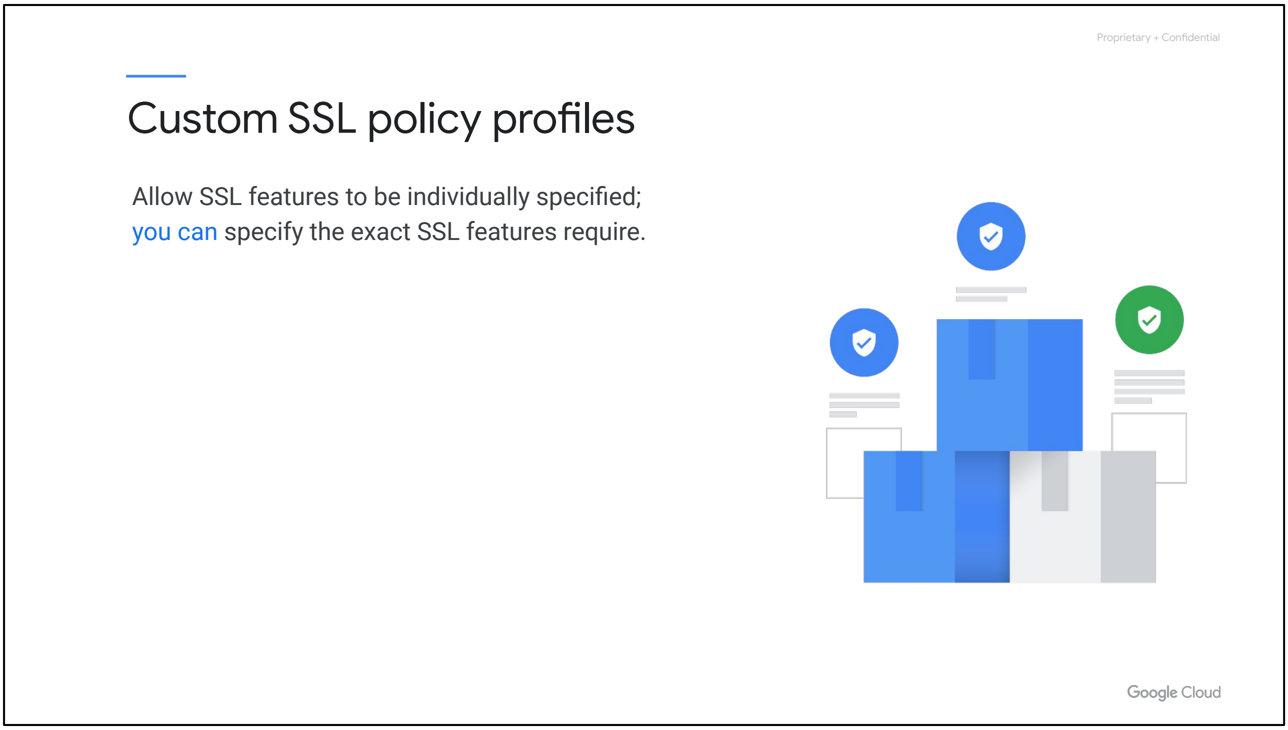
COMPATIBLE	MODERN	RESTRICTED
Allows the broadest set of clients.	Supports a wide set of SSL/TLS features, allowing modern clients to negotiate SSL/TLS.	Supports a reduced set of SSL/TLS features, intended to meet stricter compliance requirements.

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



Proprietary + Confidential

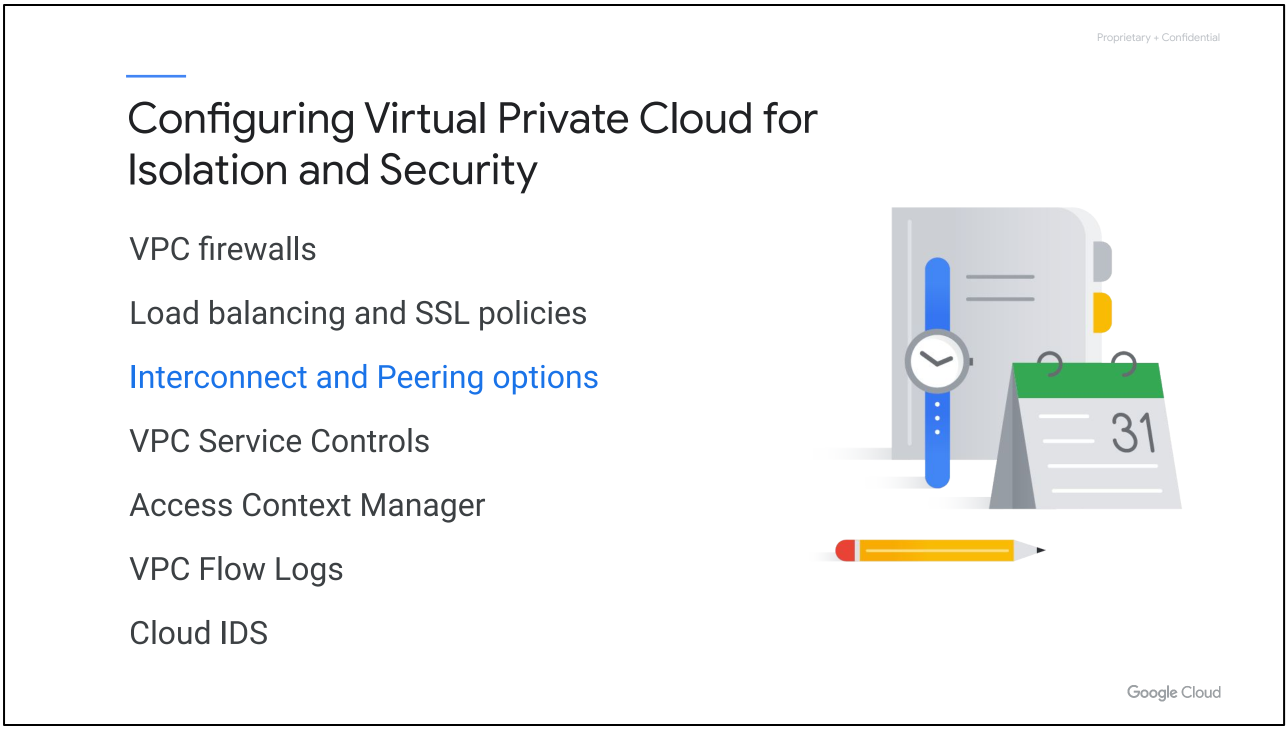
Custom SSL policy profiles

Allow SSL features to be individually specified; you can specify the exact SSL features require.

Google Cloud

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 as available features change.

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



Proprietary + Confidential

Configuring Virtual Private Cloud for Isolation and Security

VPC firewalls

Load balancing and SSL policies

Interconnect and Peering options

VPC Service Controls

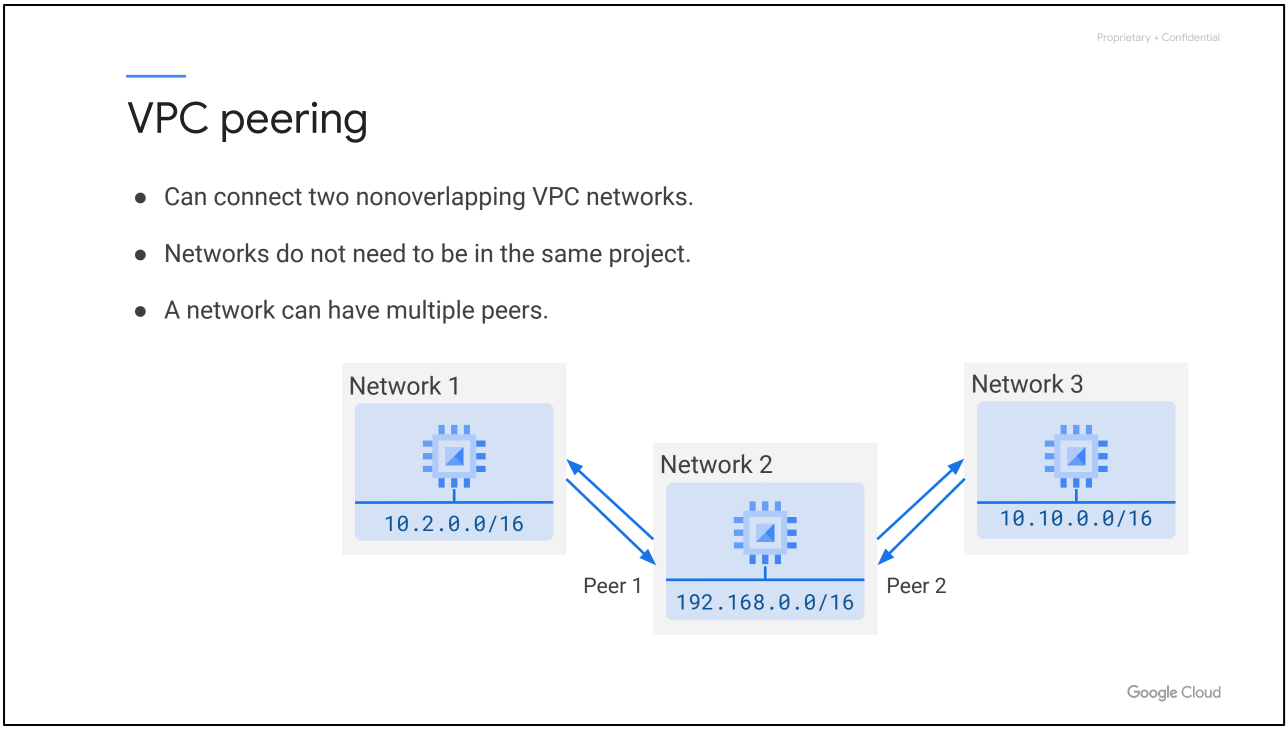
Access Context Manager

VPC Flow Logs

Cloud IDS

Google Cloud

Next, we'll address Interconnect and VPC peering options.



VPC peering

- Can connect two nonoverlapping VPC networks.
- Networks do not need to be in the same project.
- A network can have multiple peers.

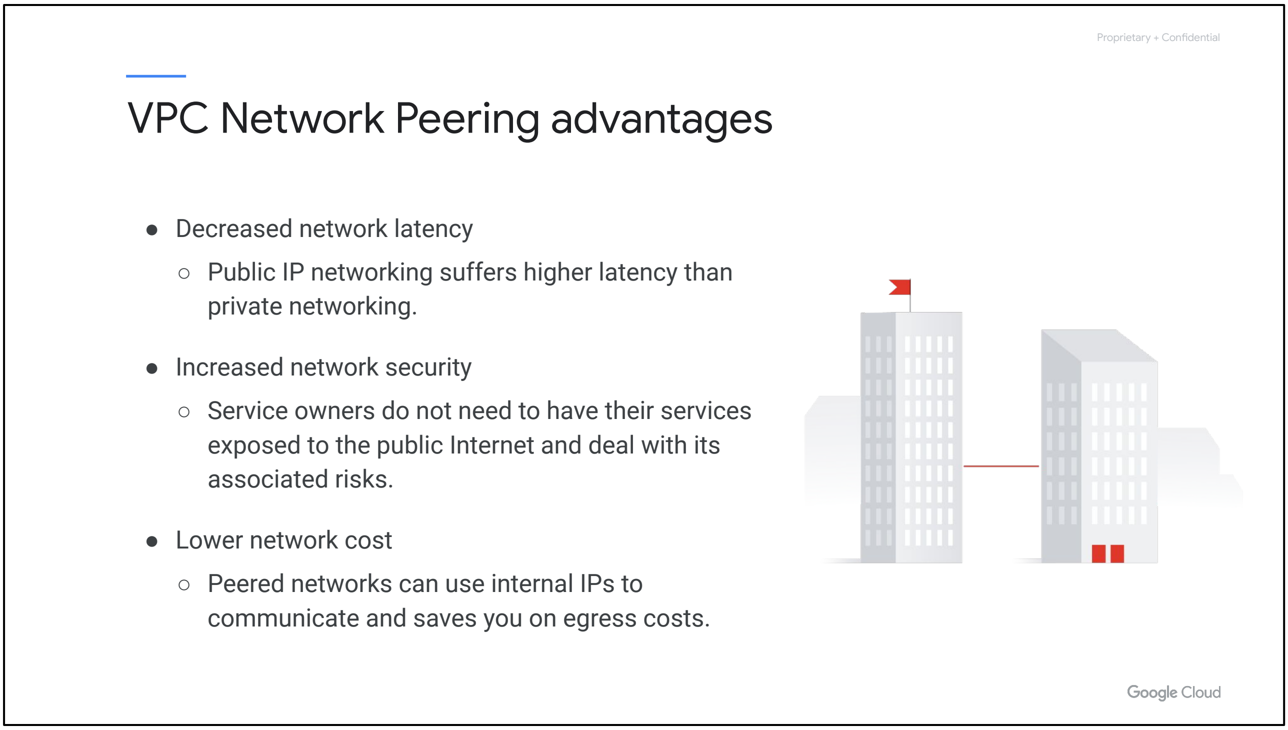
Google Cloud

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.



Proprietary + Confidential

VPC Network Peering advantages

- 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
  - Peered networks can use internal IPs to communicate and saves you on egress costs.

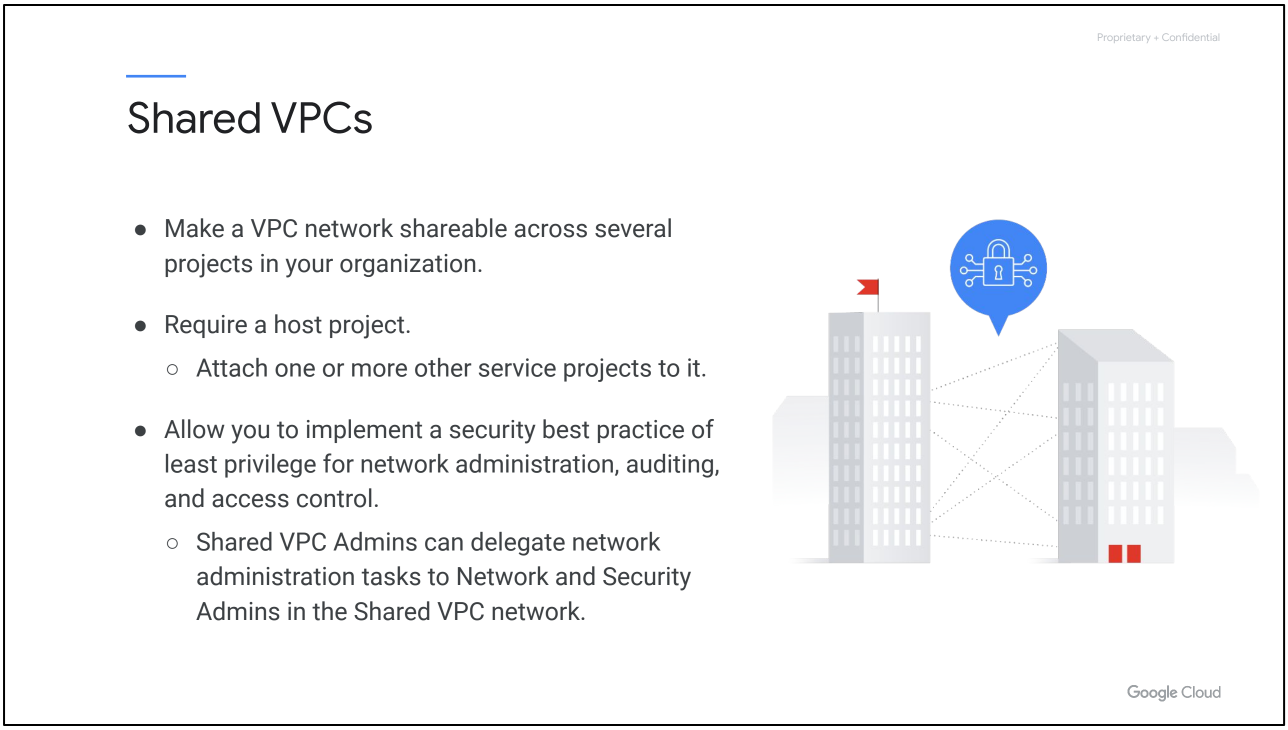
Google Cloud

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.

- And 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 the networks are peered however, they can use internal IPs to communicate and save on those egress costs. Regular network pricing still applies to all traffic.



Shared VPCs

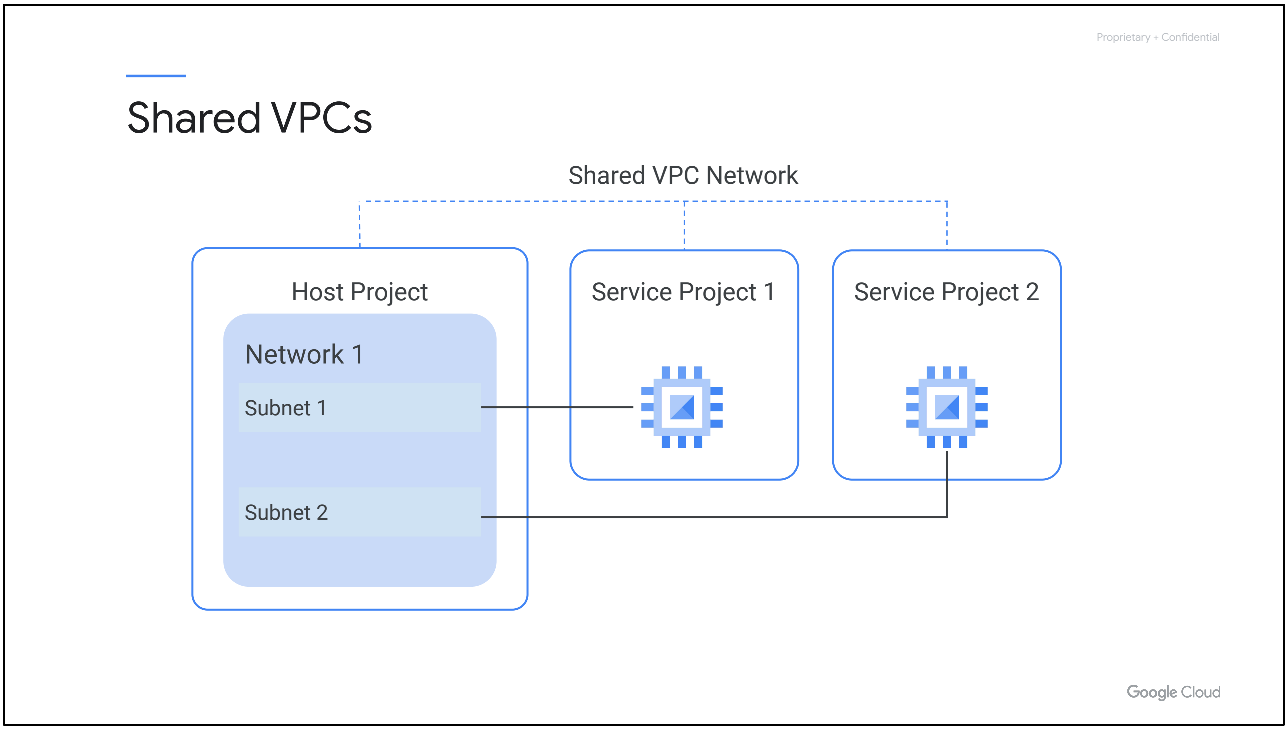
- Make a VPC network shareable across several projects in your organization.
- Require a host project.
  - Attach one or more other service projects to it.
- Allow you to implement a security best practice of least privilege for network administration, auditing, and access control.
  - Shared VPC Admins can delegate network administration tasks to Network and Security Admins in the Shared VPC network.

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 allow you to implement a security best practice of least privilege for network administration, auditing, and access control. Shared VPC Admins can delegate network administration tasks to Network and Security Admins in the Shared VPC network without allowing Service Project Admins to make network-impacting changes.



Proprietary + Confidential

Shared VPCs

Shared VPC Network

Host Project

Network 1

Subnet 1

Subnet 2

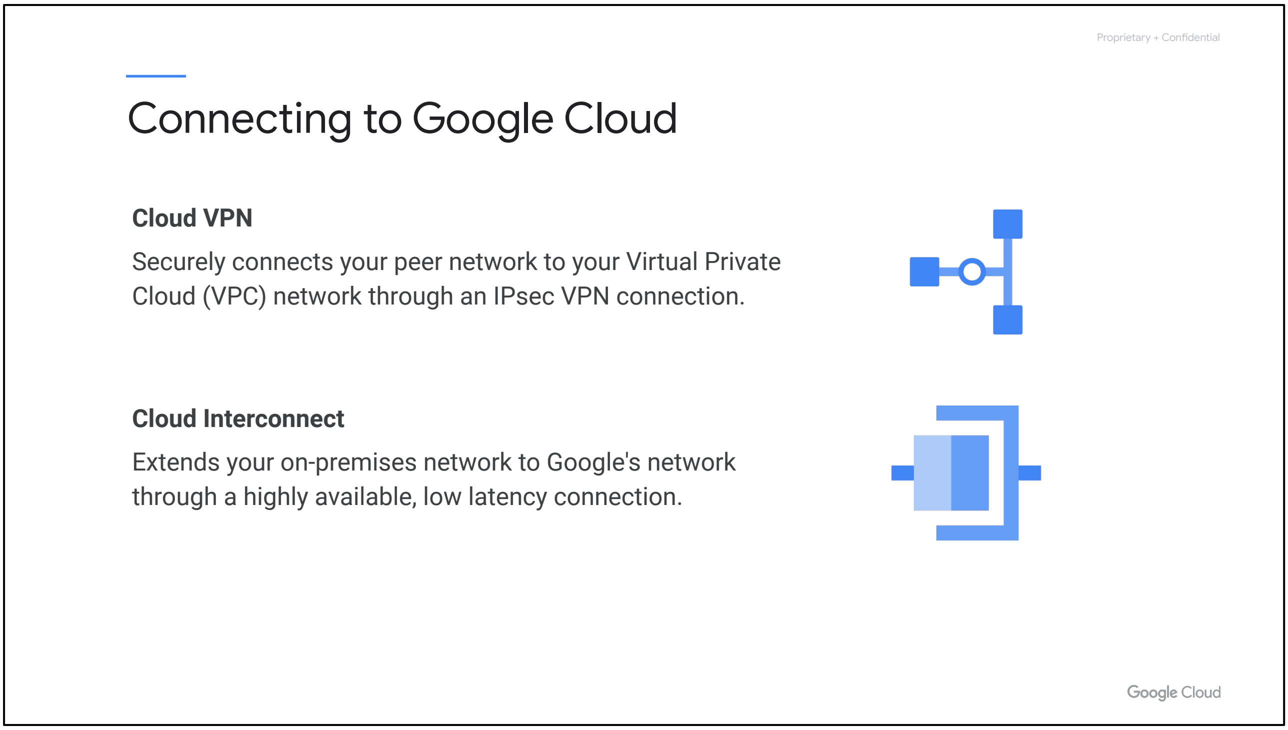
Service Project 1

Service Project 2

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.



Proprietary + Confidential

Connecting to Google Cloud

Cloud VPN

Securely connects your peer network to your Virtual Private Cloud (VPC) network through an IPsec VPN connection.

Cloud Interconnect

Extends your on-premises network to Google's network through a highly available, low latency connection.

Google Cloud

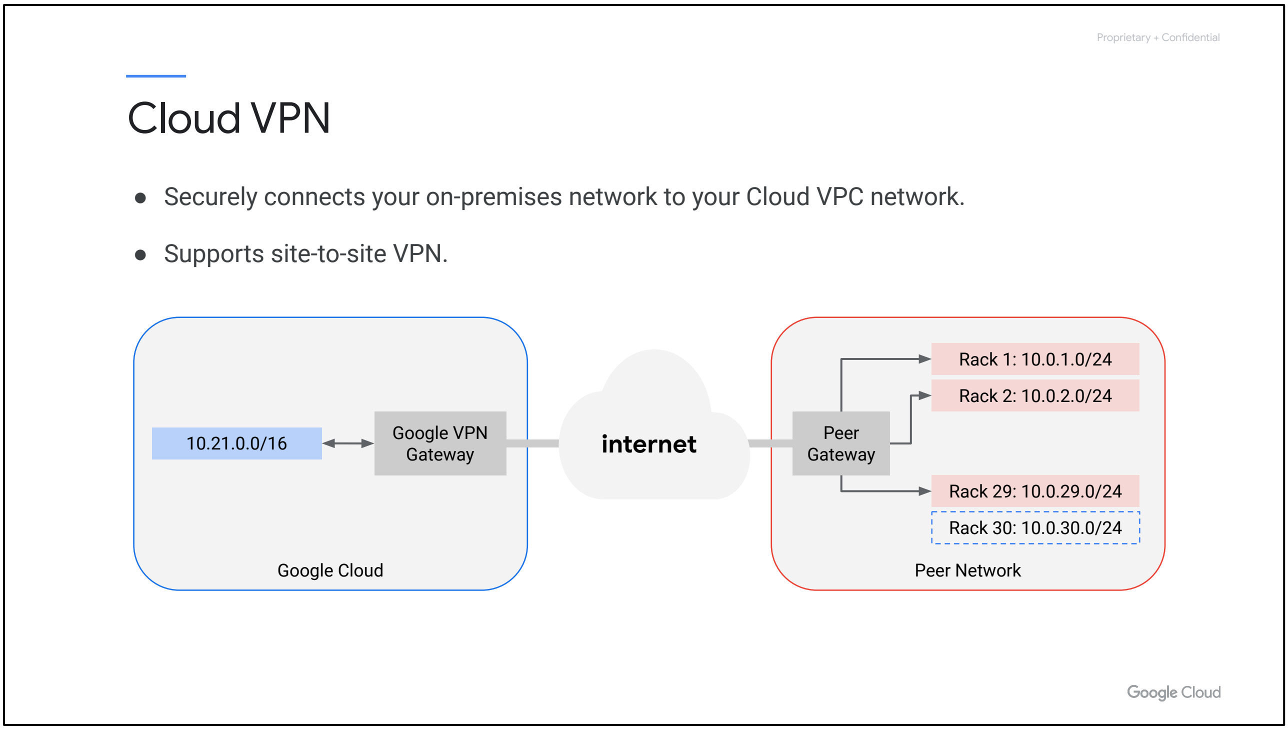
What about connecting from your local on-prem network to your cloud VPC network?

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 peer network to your Virtual Private Cloud (VPC) network through an IPsec VPN connection.

Cloud Interconnect extends your on-premises network to Google's network through a highly available, low latency connection.

We’ll talk about these in more detail now.



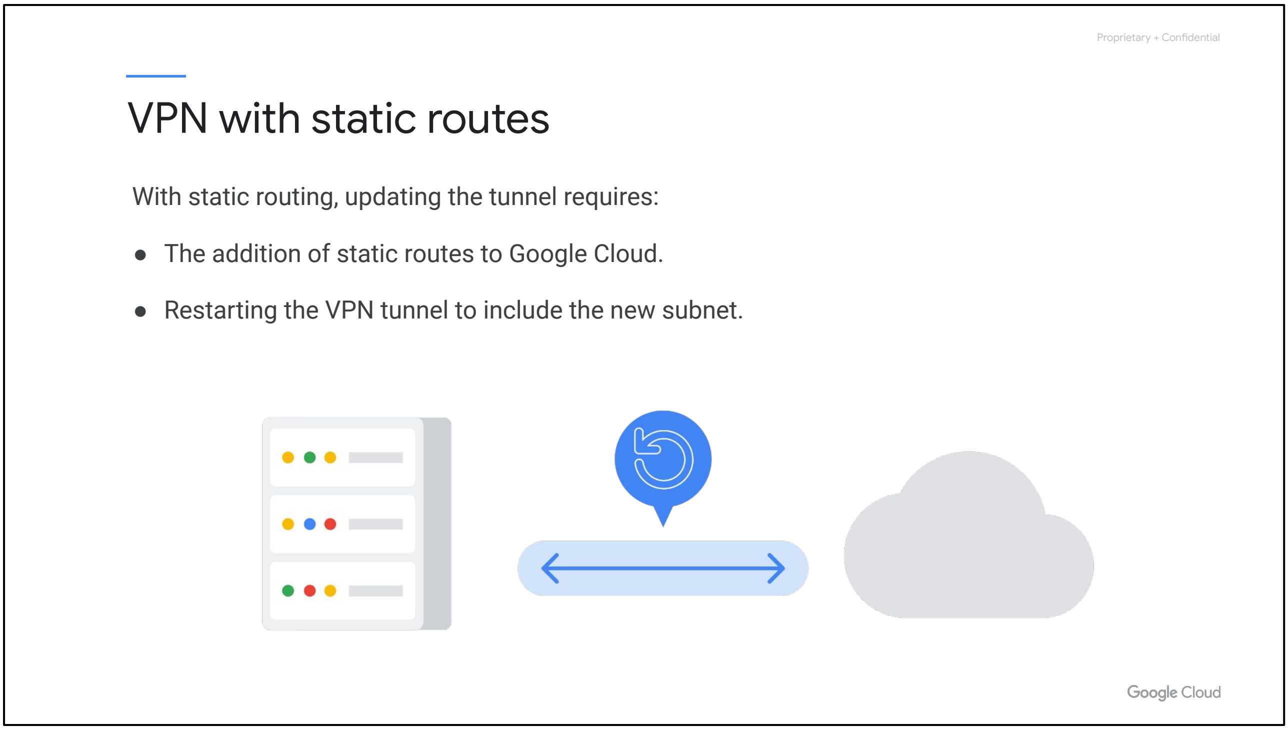
Cloud VPN

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

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 traverse 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.



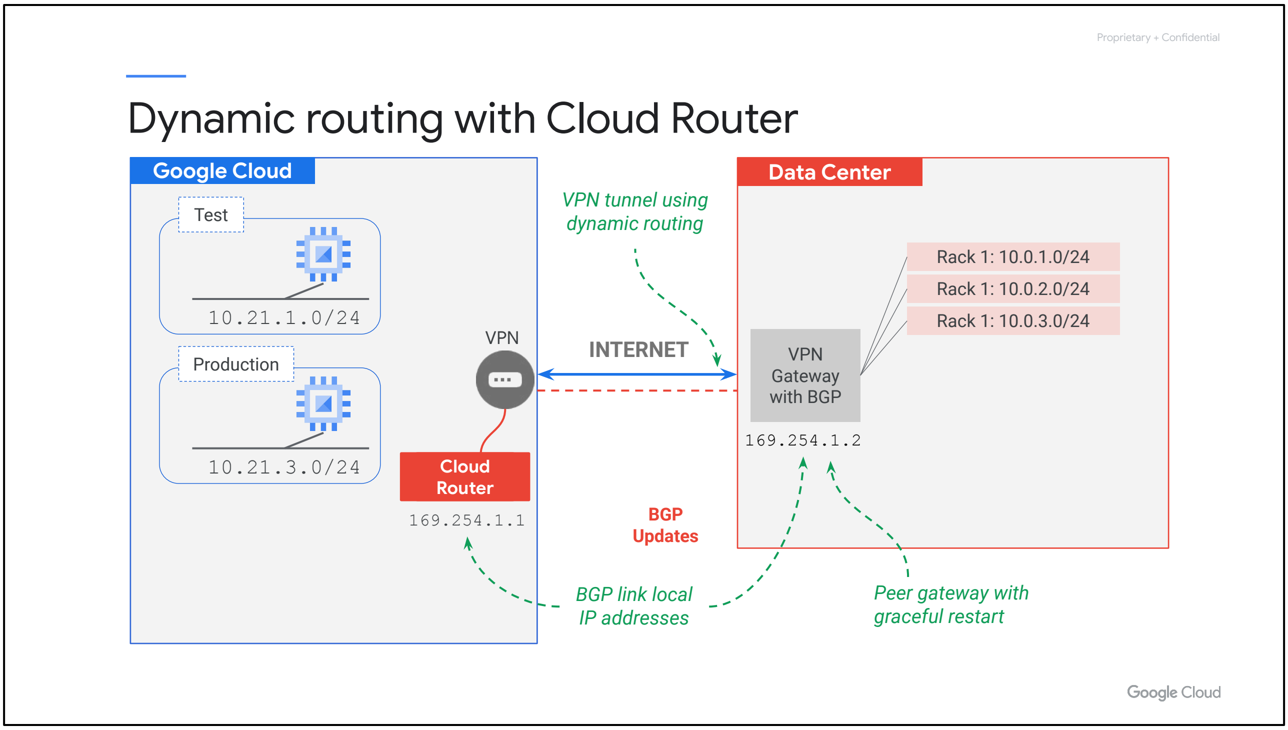
VPN with static routes

With static routing, updating the tunnel requires:

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

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

Test

10.21.1.0/24

Production

10.21.3.0/24

VPN

Cloud Router

169.254.1.1

VPN tunnel using dynamic routing

INTERNET

BGP Updates

BGP link local IP addresses

Data Center

Rack 1: 10.0.1.0/24

Rack 1: 10.0.2.0/24

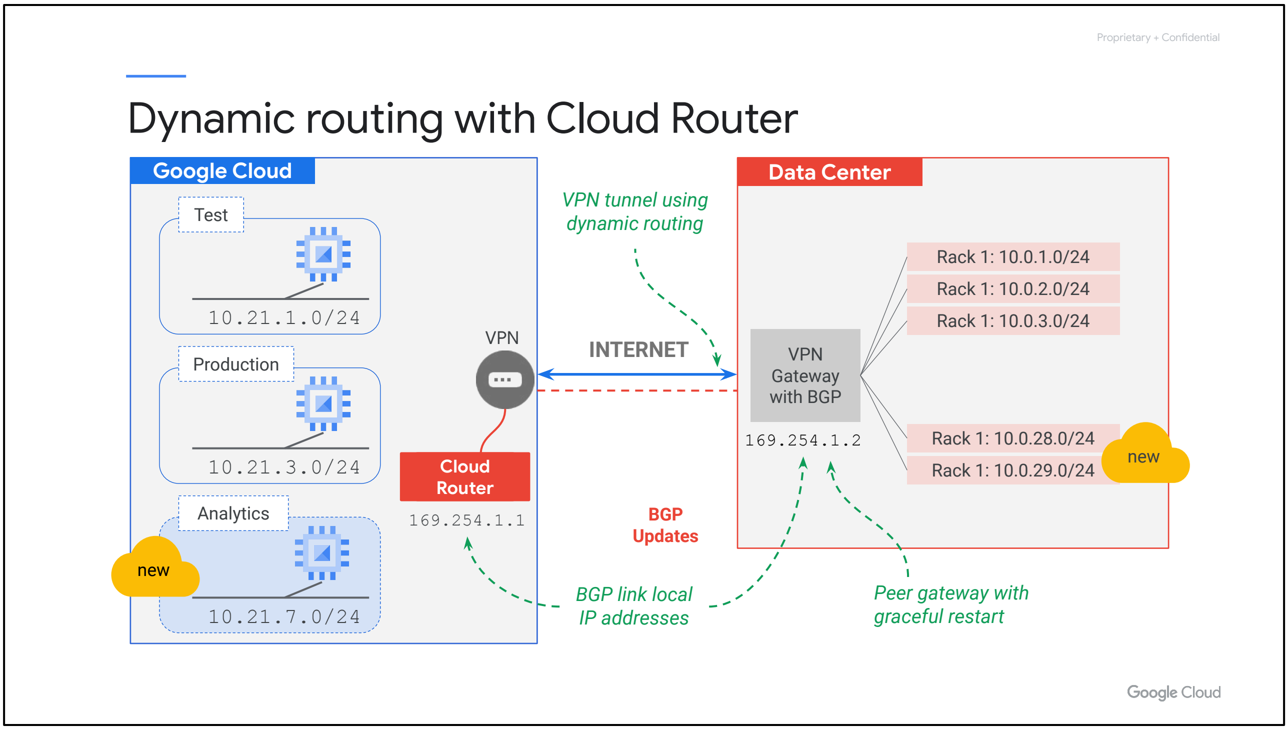
Rack 1: 10.0.3.0/24

VPN Gateway with BGP

169.254.1.2

Peer gateway with graceful restart

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.



Proprietary + Confidential

Dynamic routing with Cloud Router

Google Cloud

Test

10.21.1.0/24

Production

10.21.3.0/24

Analytics

10.21.7.0/24

new

VPN

Cloud Router

169.254.1.1

VPN tunnel using dynamic routing

INTERNET

BGP Updates

BGP link local IP addresses

Data Center

VPN Gateway with BGP

169.254.1.2

Rack 1: 10.0.1.0/24
Rack 1: 10.0.2.0/24
Rack 1: 10.0.3.0/24
Rack 1: 10.0.28.0/24
Rack 1: 10.0.29.0/24

new

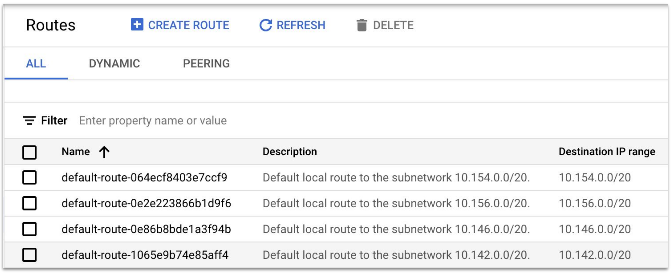
Peer gateway with graceful restart

Google Cloud

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.

Proprietary + Confidential

Google Cloud routes



Routes ⊞ CREATE ROUTE ⟳ REFRESH 🗑 DELETE

ALL DYNAMIC PEERING

Filter Enter property name or value

□	Name ↑	Description	Destination IP range
□	default-route-064ecf8403e7ccf9	Default local route to the subnetwork 10.154.0.0/20.	10.154.0.0/20
□	default-route-0e2e223866b1d9f6	Default local route to the subnetwork 10.156.0.0/20.	10.156.0.0/20
□	default-route-0e86b8bde1a3f94b	Default local route to the subnetwork 10.146.0.0/20.	10.146.0.0/20
□	default-route-1065e9b74e85aff4	Default local route to the subnetwork 10.142.0.0/20.	10.142.0.0/20

- Define paths network traffic take from a VM to other destinations.
  - Can be inside VPC or outside of it.
- Routes created when a network or subnet is created.
- Consists of single destination prefix and next hop.

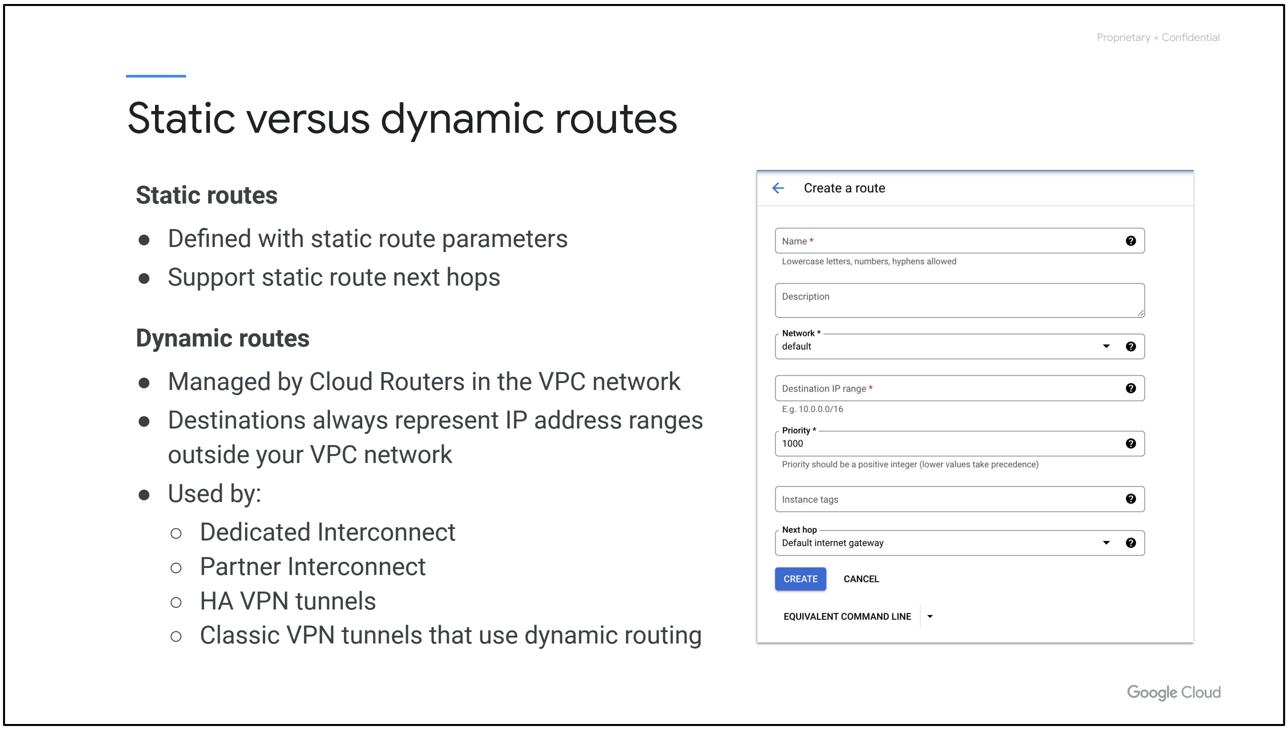
Google Cloud

Before diving more into Cloud VPN, let’s take a moment to discuss Google Cloud routes and the difference between dynamic and static routes.

Google Cloud routes define the paths that network traffic takes from a virtual machine (VM) instance to other destinations. These destinations can be inside your Google Cloud Virtual Private Cloud (VPC) network (for example, in another VM) or outside it.

A route is created when a network or subnet is created, enabling traffic delivery from anywhere. This is what enables VMs on the same network to communicate.

In a VPC network, a route consists of a single destination prefix in CIDR format and a single next hop. When an instance in a VPC network sends a packet, Google Cloud delivers the packet to the route's next hop if the packet's destination address is within the route's destination range.



Static versus dynamic routes

Static routes

- Defined with static route parameters
- Support static route next hops

Dynamic routes

- Managed by Cloud Routers in the VPC network
- Destinations always represent IP address ranges outside your VPC network
- Used by:
  - Dedicated Interconnect
  - Partner Interconnect
  - HA VPN tunnels
  - Classic VPN tunnels that use dynamic routing

Create a route

Name *
Lowercase letters, numbers, hyphens allowed

Description

Network *: default

Destination IP range *
E.g. 10.0.0.0/16

Priority *: 1000
Priority should be a positive integer (lower values take precedence)

Instance tags

Next hop: Default internet gateway

CREATE CANCEL

EQUIVALENT COMMAND LINE

Static routes are defined using static route parameters and support static route next hops.

You can create static routes manually using the Google Cloud console, gcloud compute routes create, or the routes.insert API.

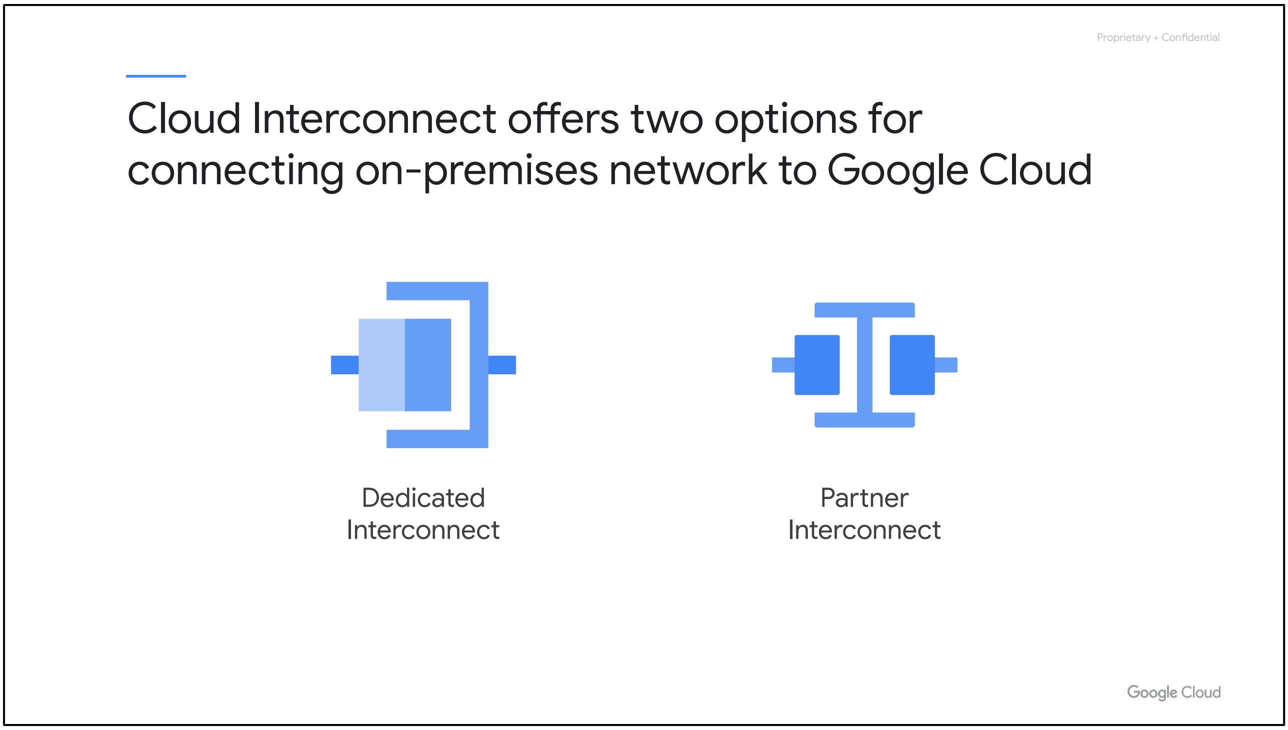
Dynamic routes are managed by Cloud Routers in the VPC network. Their destinations always represent IP address ranges outside your VPC network, received from a BGP peer. Dynamic routes are used by:

- Dedicated Interconnect
- Partner Interconnect
- HA VPN tunnels
- Classic VPN tunnels that use dynamic routing

One key benefit of using dynamic routers allows you to discover topology changes and route traffic accordingly so users don't sense disruptions.

For more information on routes and the difference between static and dynamic routes, check out the link in the speaker notes of this module:

- **Link:** cloud.google.com/vpc/docs/routes



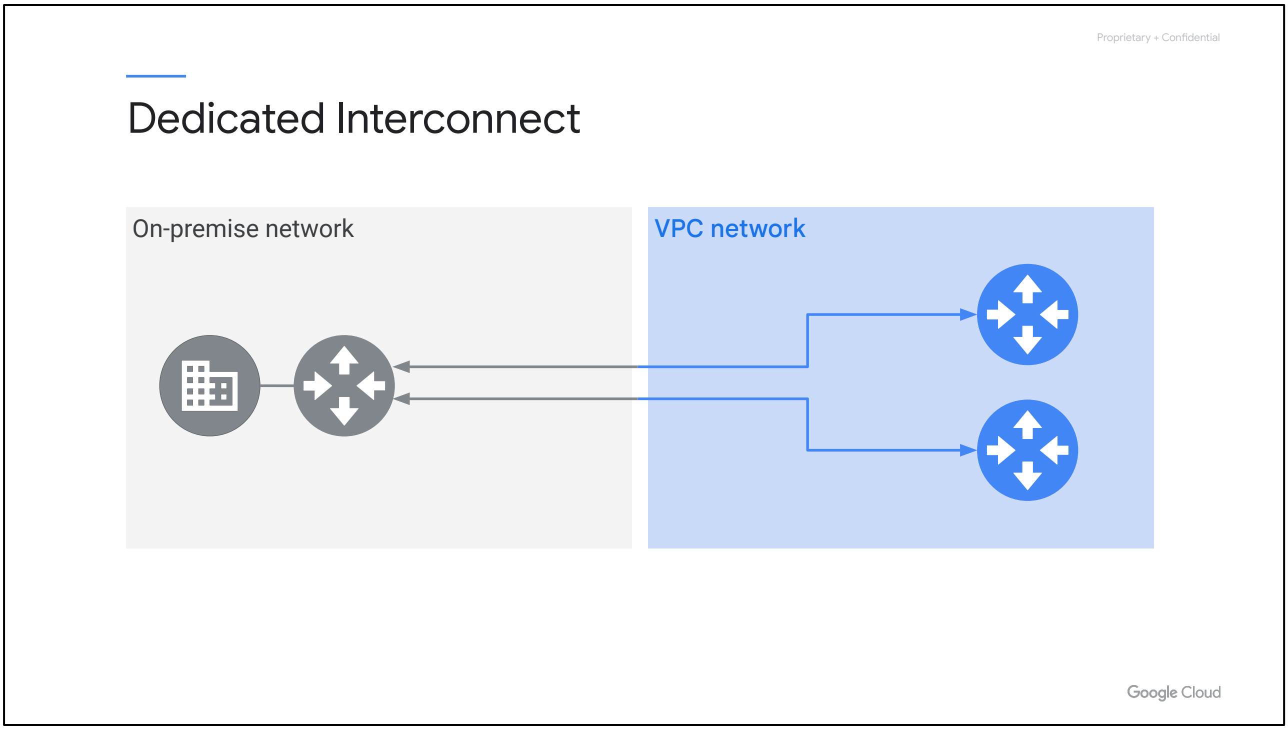
Cloud Interconnect offers two options for connecting on-premises network to Google Cloud

Dedicated Interconnect

Partner Interconnect

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.

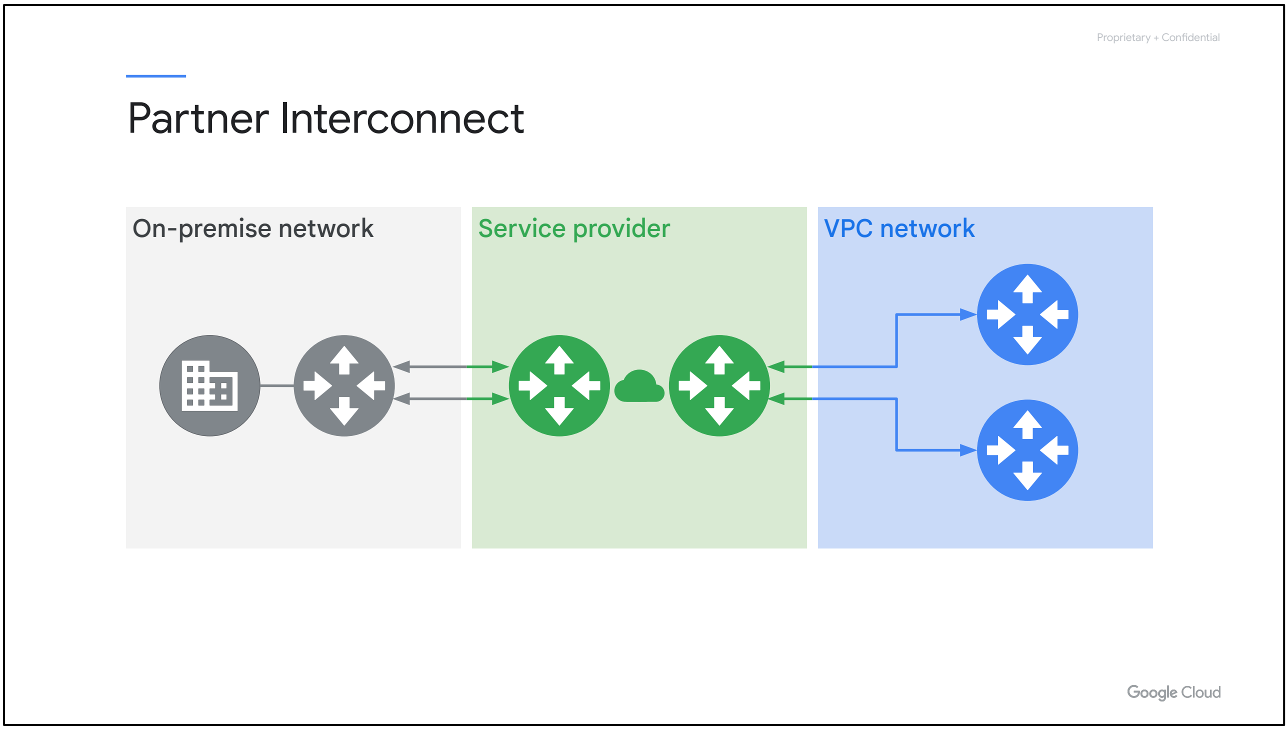


Dedicated Interconnect

On-premise network

VPC network

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



Proprietary + Confidential

Partner Interconnect

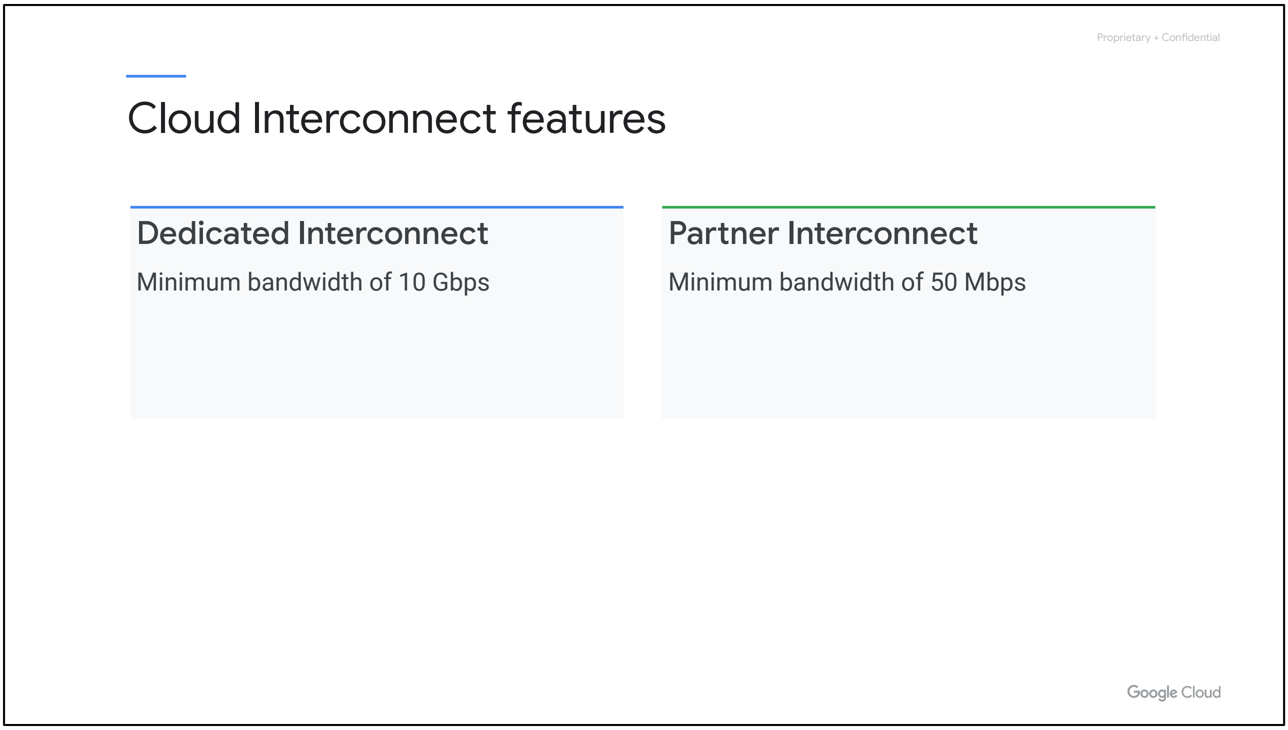
On-premise network

Service provider

VPC network

Google Cloud

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



Cloud Interconnect features

Dedicated Interconnect

Minimum bandwidth of 10 Gbps

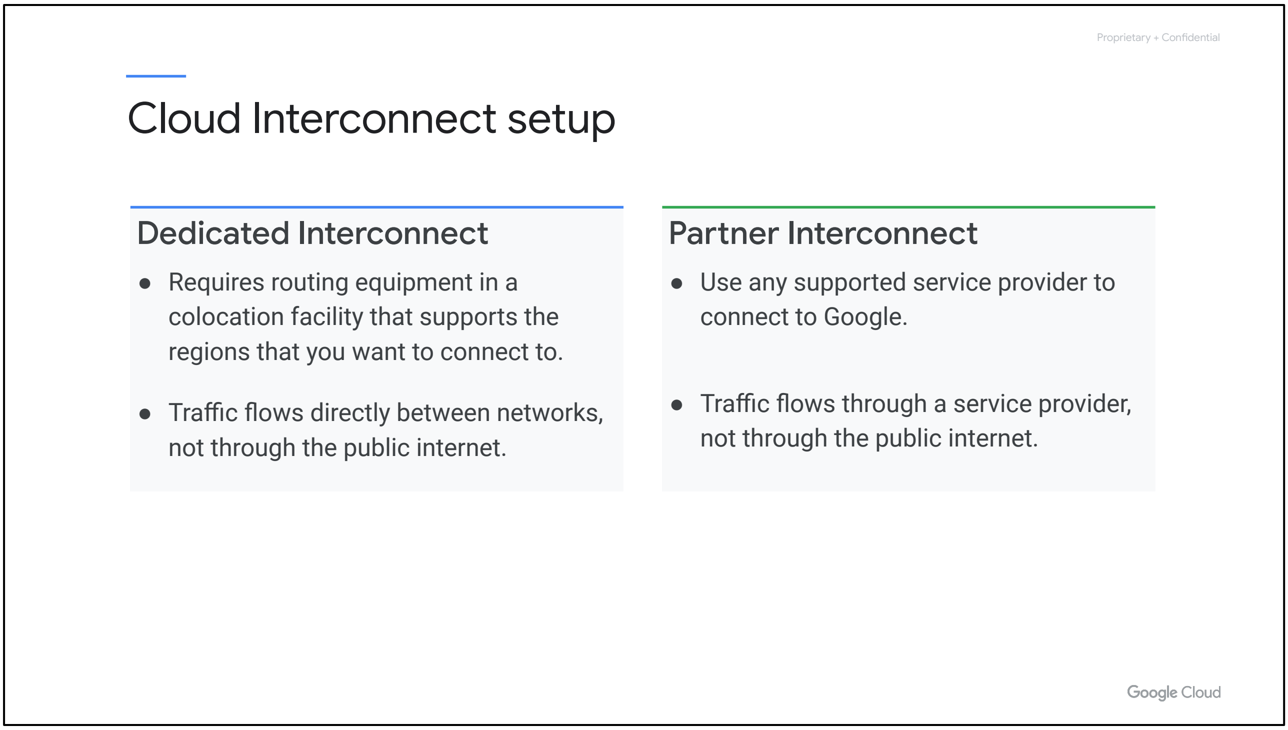
Partner Interconnect

Minimum bandwidth of 50 Mbps

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.

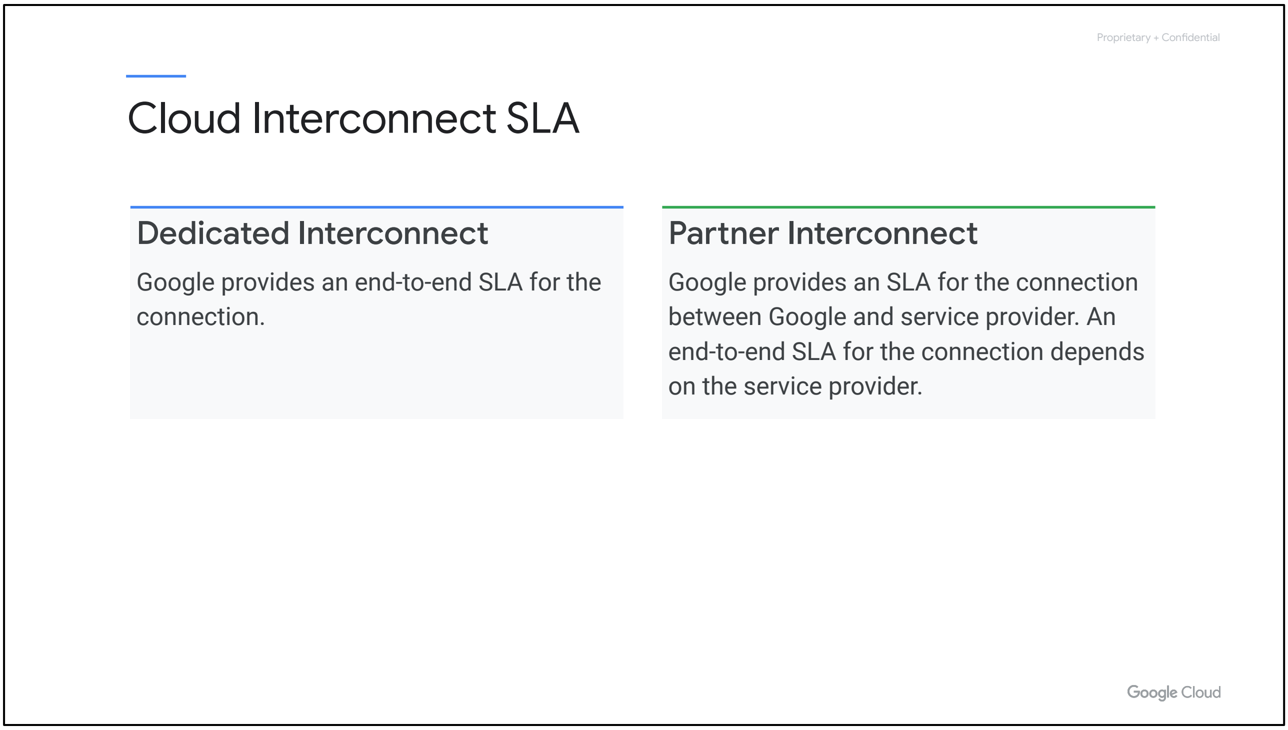
Partner Interconnect

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

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-premises 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.



Cloud Interconnect SLA

Dedicated Interconnect

Google provides an end-to-end SLA for the connection.

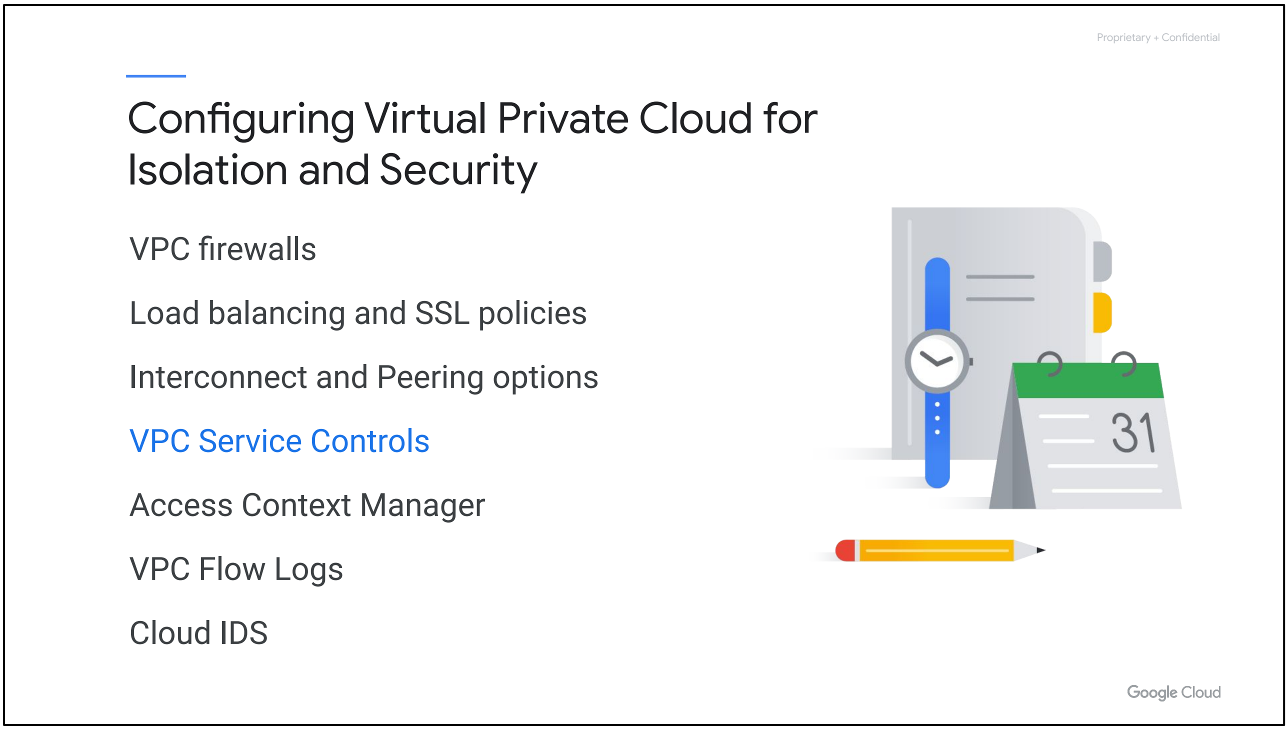
Partner Interconnect

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.

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.



Configuring Virtual Private Cloud for Isolation and Security

VPC firewalls

Load balancing and SSL policies

Interconnect and Peering options

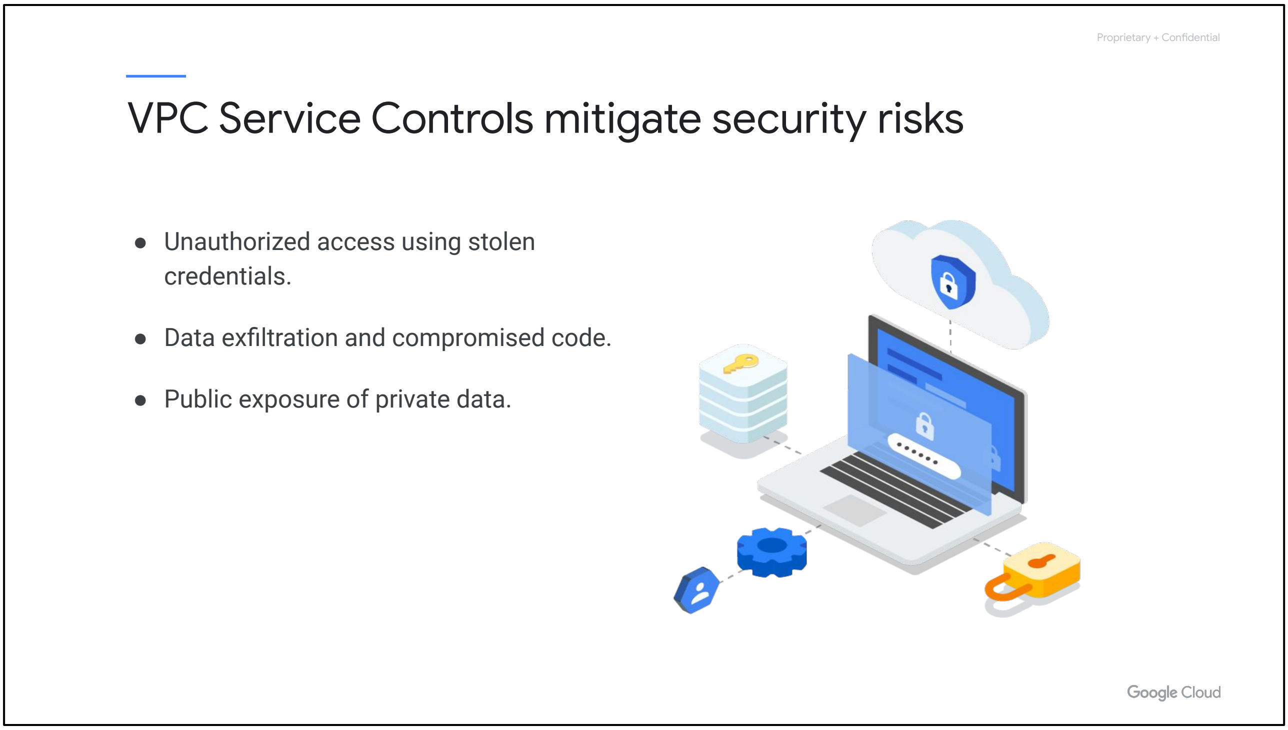
VPC Service Controls

Access Context Manager

VPC Flow Logs

Cloud IDS

Now let’s talk about VPC service controls.



Proprietary + Confidential

VPC Service Controls mitigate security risks

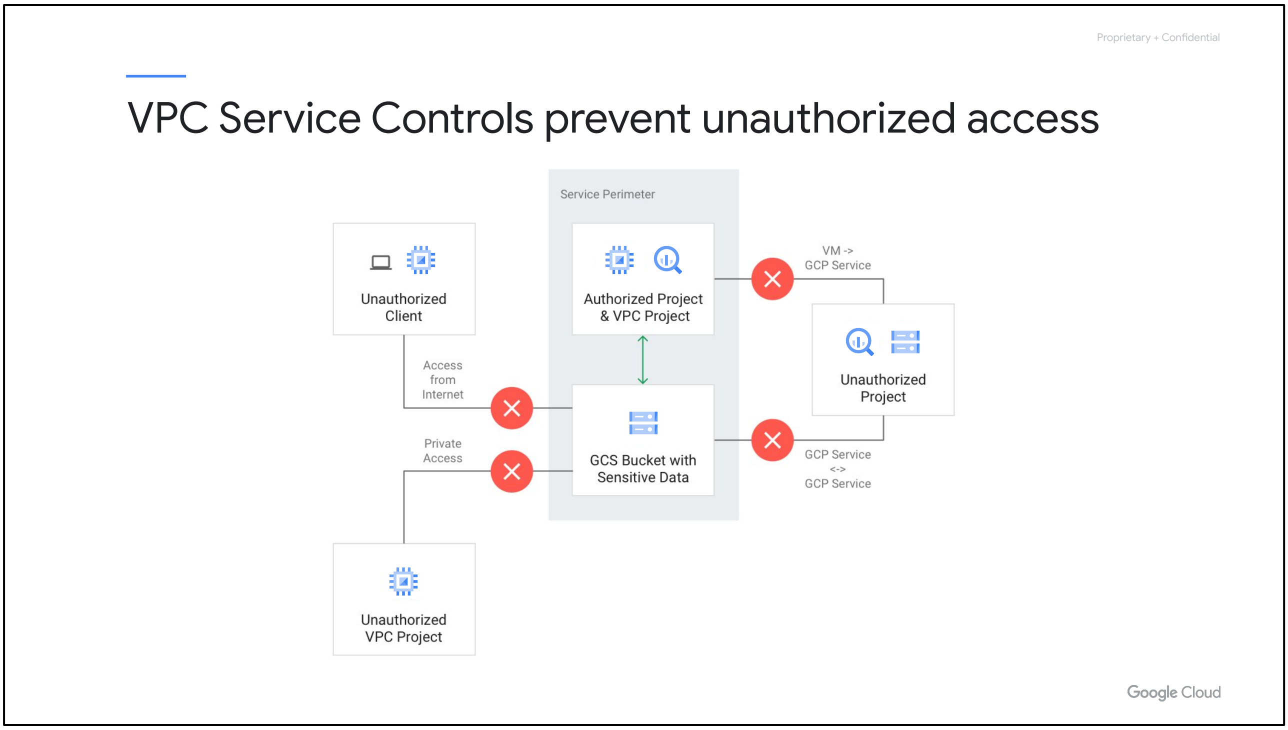
- Unauthorized access using stolen credentials.
- Data exfiltration and compromised code.
- Public exposure of private data.

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.



Proprietary + Confidential

VPC Service Controls prevent unauthorized access

Service Perimeter

Unauthorized Client

Authorized Project & VPC Project

VM -> GCP Service

Unauthorized Project

Access from Internet

GCS Bucket with Sensitive Data

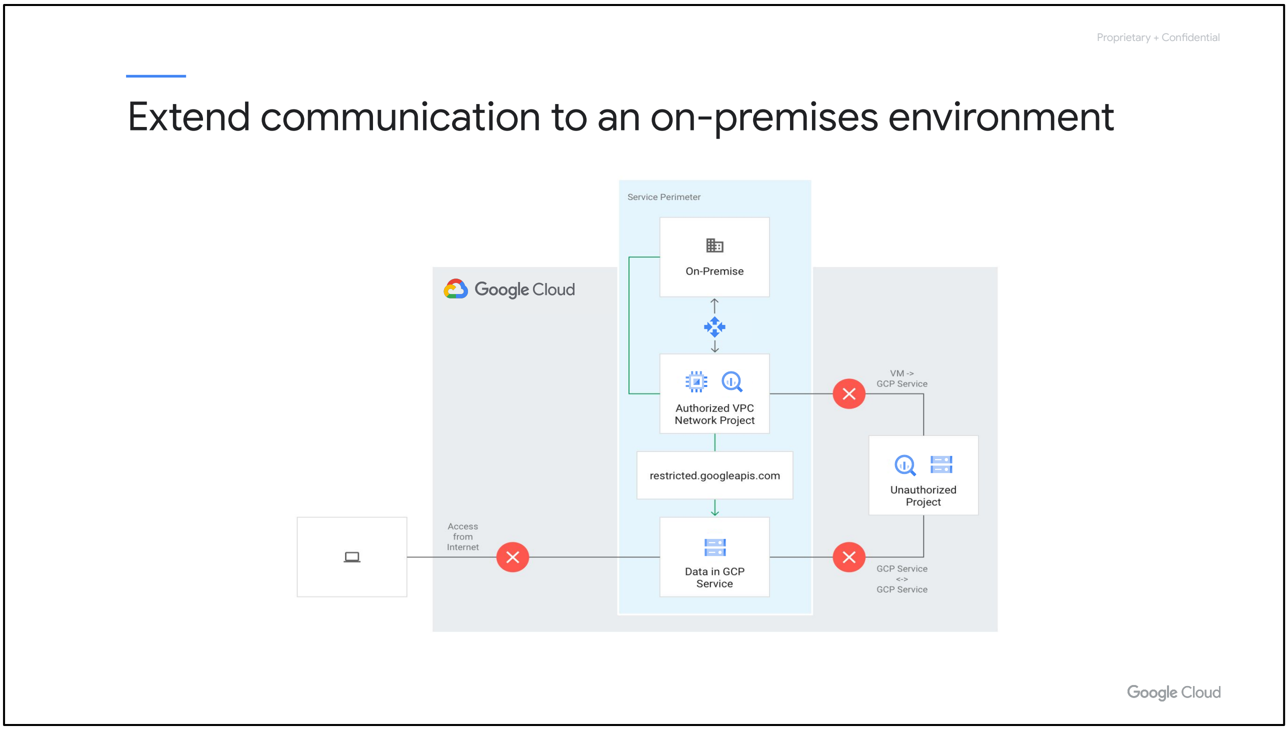
Private Access

GCP Service <-> GCP Service

Unauthorized VPC Project

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.



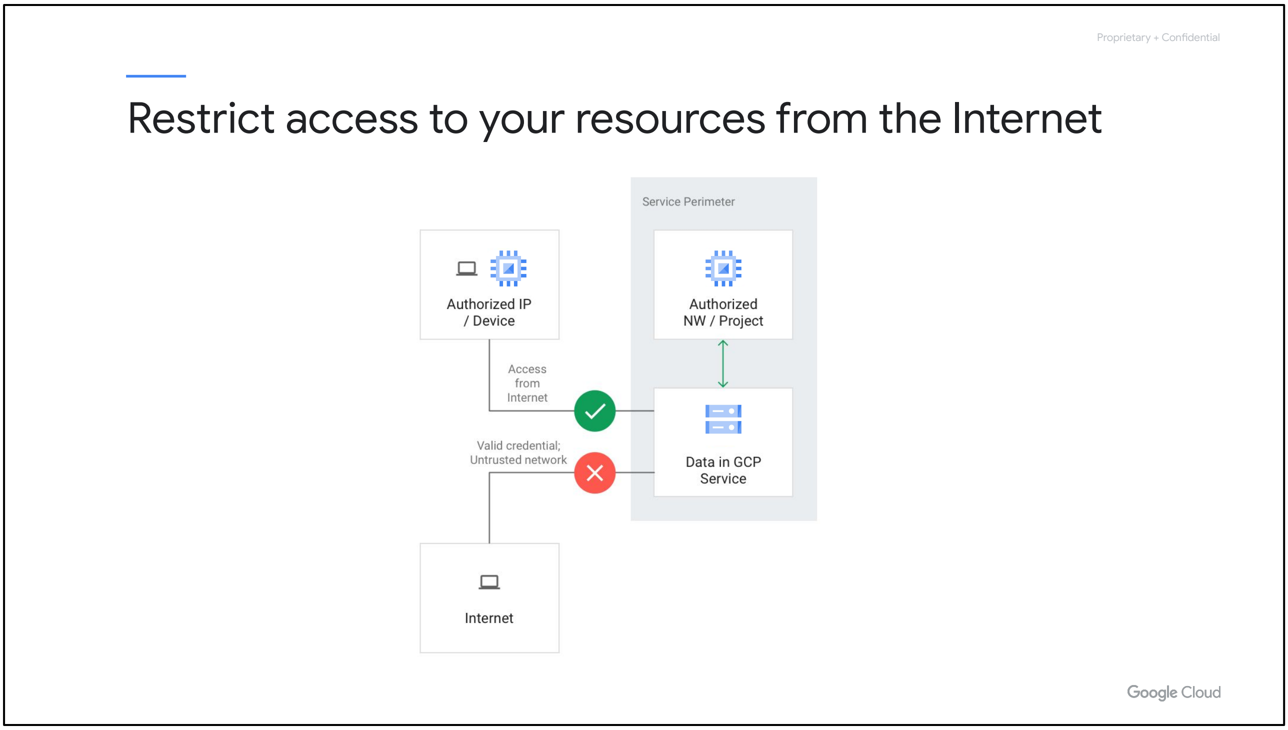
Proprietary + Confidential

Extend communication 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.



Proprietary + Confidential

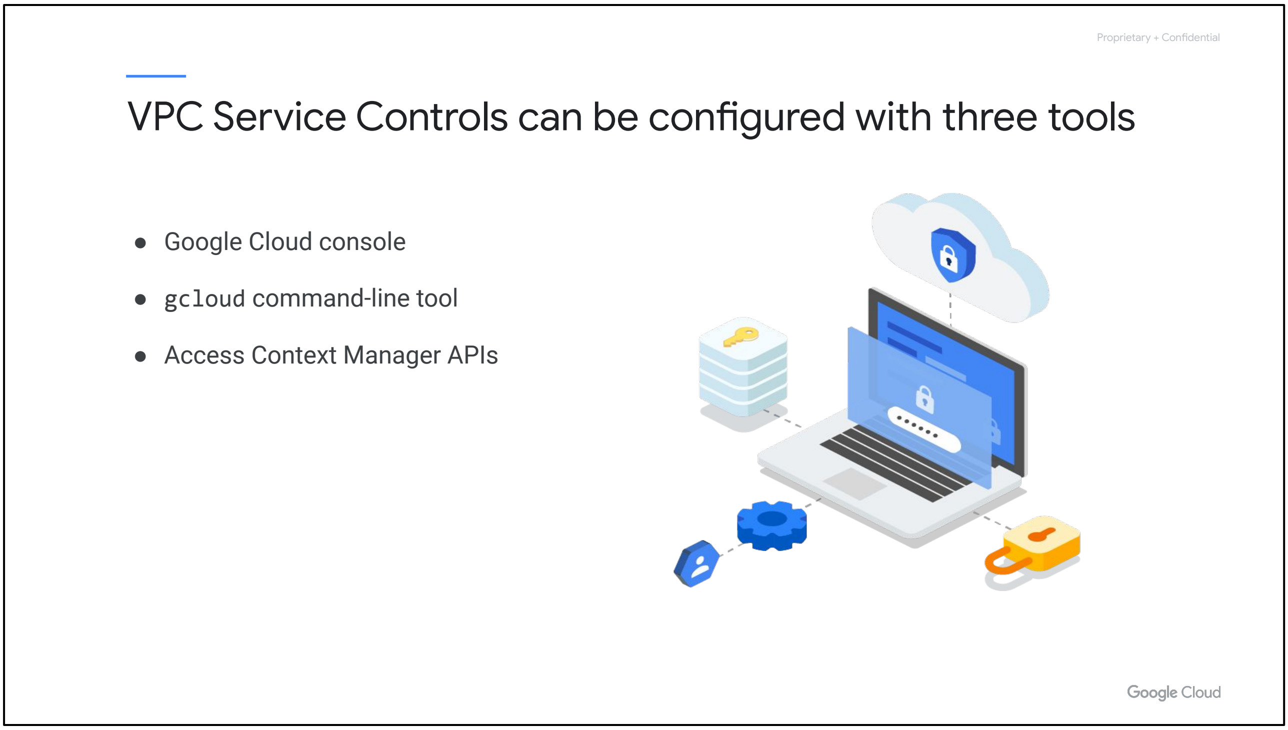
Restrict access to your resources from the Internet

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.)



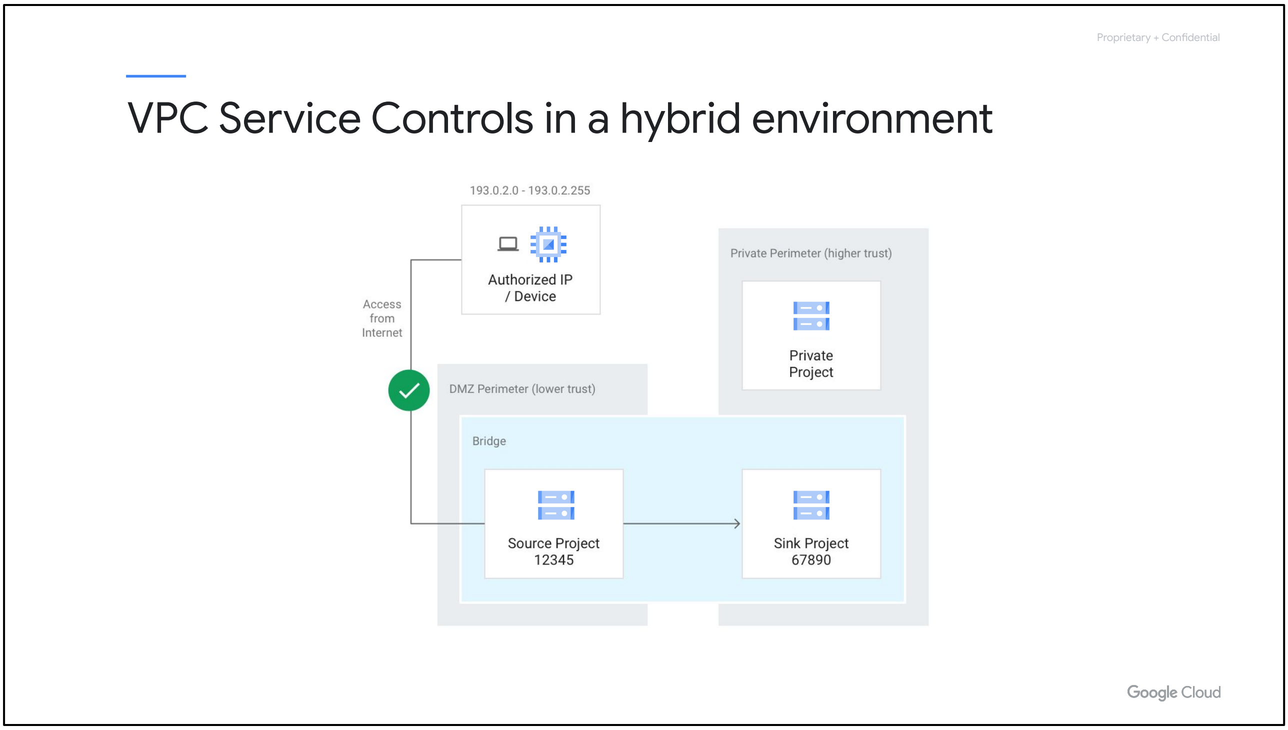
Proprietary + Confidential

VPC Service Controls can be configured with three tools

- Google 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.



Proprietary + Confidential

VPC Service Controls in a hybrid environment

193.0.2.0 - 193.0.2.255

Authorized IP / Device

Access from Internet

DMZ Perimeter (lower trust)

Private Perimeter (higher trust)

Private Project

Bridge

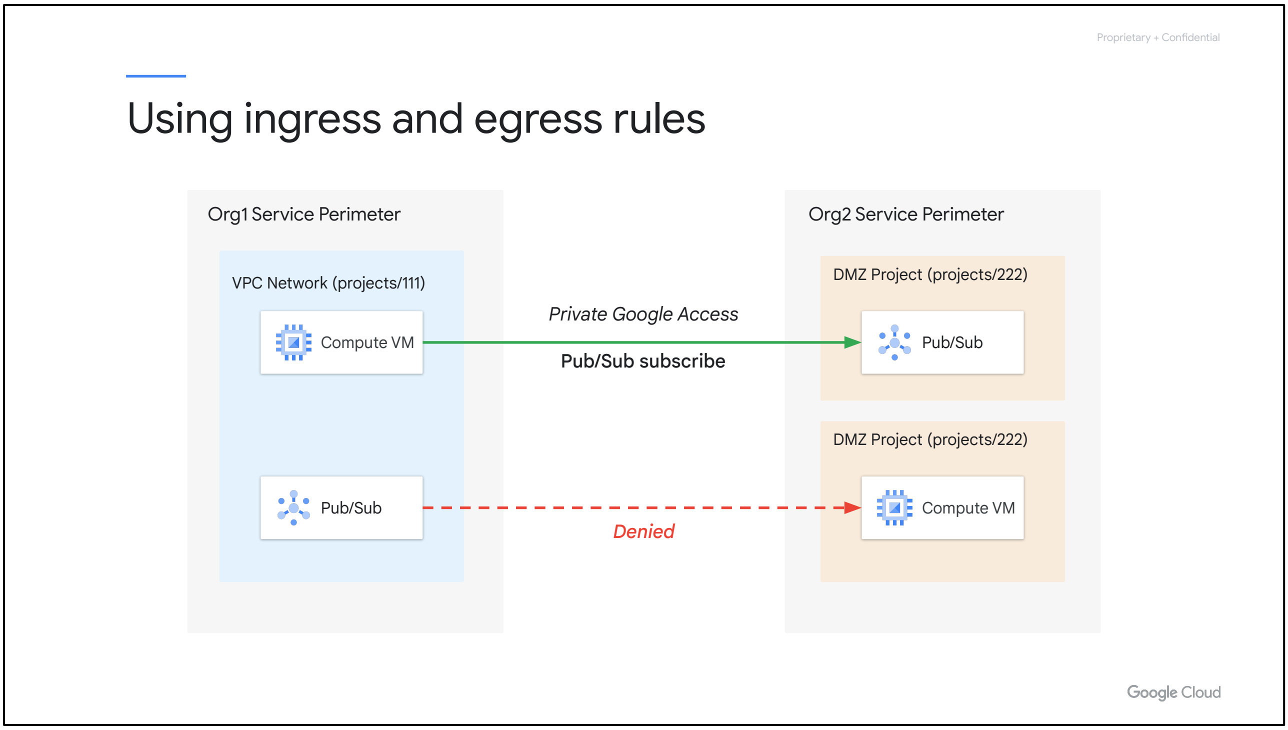
Source Project 12345

Sink Project 67890

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.

NOTE: Instead of using a perimeter bridge, we recommend using ingress and egress rules that provide more granular controls. Let's discuss these next.



Proprietary + Confidential

Using ingress and egress rules

Org1 Service Perimeter

VPC Network (projects/111)

Compute VM

Pub/Sub

Org2 Service Perimeter

DMZ Project (projects/222)

Pub/Sub

DMZ Project (projects/222)

Compute VM

Private Google Access

Pub/Sub subscribe

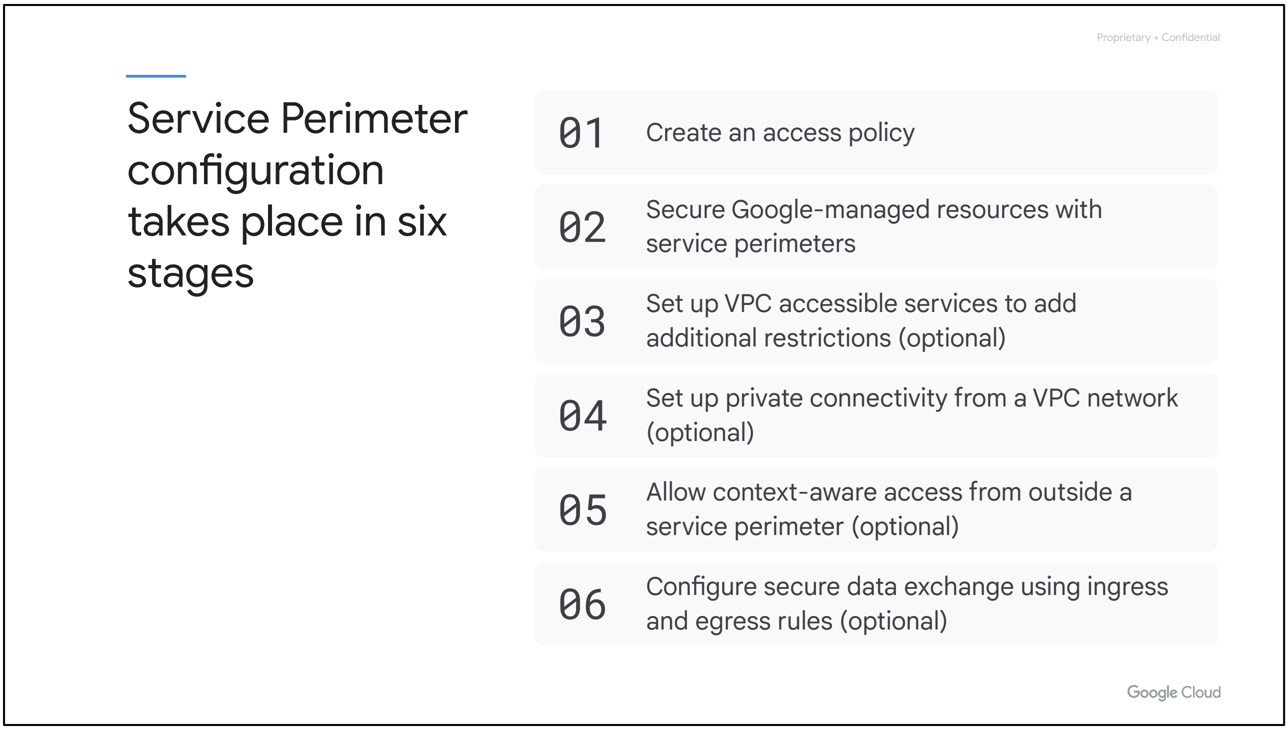
Denied

Google Cloud

VPC Service Controls use ingress and egress rules to allow access to and from the resources and clients protected by service perimeters.

- **Ingress rules** allow an API client that is outside the perimeter to access resources within a perimeter.
- **Egress rules** allow an API client or resource that is inside the perimeter to access Google Cloud resources outside the perimeter. The perimeter does not block access to any third-party API or services in the internet.

The diagram shows two organizations, Org1 and Org2, which use VPC Service Controls and share data by using a Pub/Sub topic. To enable data exchange, Org1 must define an egress rule that allows the subscription and save the file as org1egress.yaml. Org2 must define a corresponding ingress rule allowing the subscription and save the file as org2ingress.yaml.



Proprietary + Confidential

Service Perimeter configuration takes place in six stages

01 Create an access policy

02 Secure Google-managed resources with service perimeters

03 Set up VPC accessible services to add additional restrictions (optional)

04 Set up private connectivity from a VPC network (optional)

05 Allow context-aware access from outside a service perimeter (optional)

06 Configure secure data exchange using ingress and egress rules (optional)

Google Cloud

Let’s go over the steps required to actually configure and enable VPC service controls.

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

- Create an access policy.
- Secure Google-managed resources with service perimeters.
- Set up VPC accessible services to add additional restrictions to how services can be used inside your perimeters (optional).
- Set up private connectivity from a VPC network (optional).
- Allow context-aware access from outside a service perimeter using ingress rules (optional).
- Configure secure data exchange using ingress and egress rules (optional).

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

An access policy collects the service perimeters and access levels you create for your organization. An organization can have one access policy for the entire organization and multiple scoped access policies for the folders and projects.

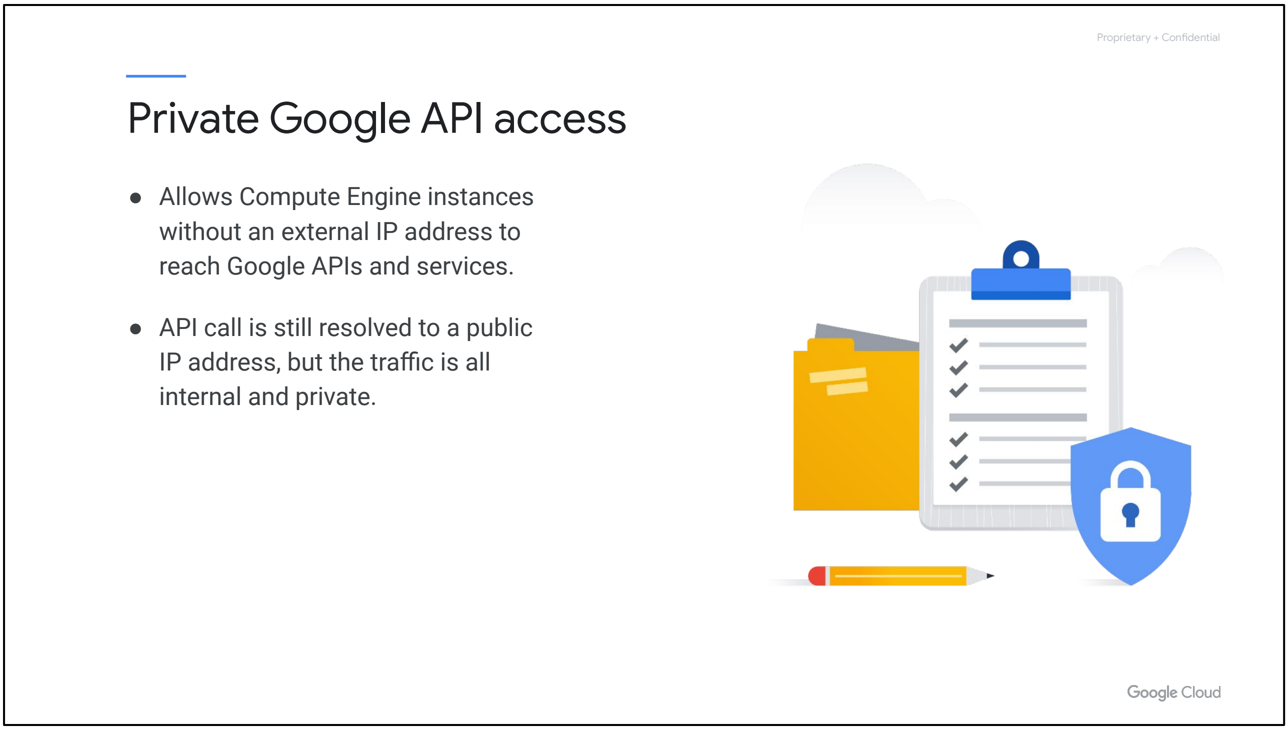
Service perimeters are used to protect services used by projects in your organization. After identifying the projects and services you want to protect, create one or more service perimeters.

When you enable VPC accessible services for a perimeter, access from network endpoints inside your perimeter is limited to a set of services that you specify.

To provide additional security for VPC networks and on-premises hosts that are protected by a service perimeter, we recommend using Private Google Access. For more information, see private connectivity from on-premises networks.

You can allow context-aware access to resources restricted by a perimeter based on client attributes. You can specify client attributes, such as identity type (service account or user), identity, device data, and network origin (IP address or VPC network).

You can include your project only in one service perimeter. If you want to allow communication across the perimeter boundary, set up ingress and egress rules.



Proprietary + Confidential

Private Google API access

- Allows Compute Engine instances without an external IP address to reach Google APIs and services.
- API call is still resolved to a public IP address, but the traffic is all internal and private.

Google Cloud

One more feature we want to touch on before diving into Access Context Manager is Private Google API access.

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.

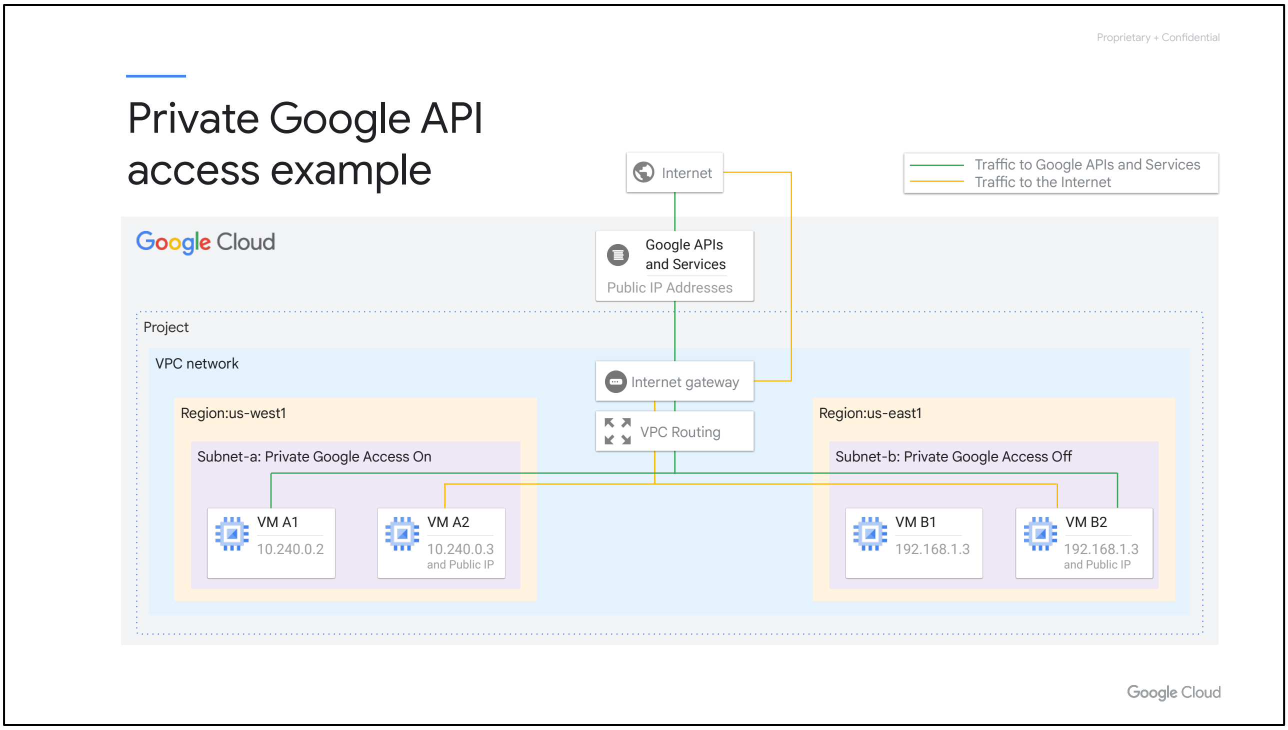
Previously, you had to provide a public path for your internal Compute Engine instances (for example, an external IP address or a NAT gateway) to allow the instances to access Google APIs.

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:

- BigQuery
- Cloud Bigtable
- Container Registry

- Dataproc
- Datastore
- Pub/Sub
- Cloud Spanner, and finally,
- Cloud Storage



Proprietary + Confidential

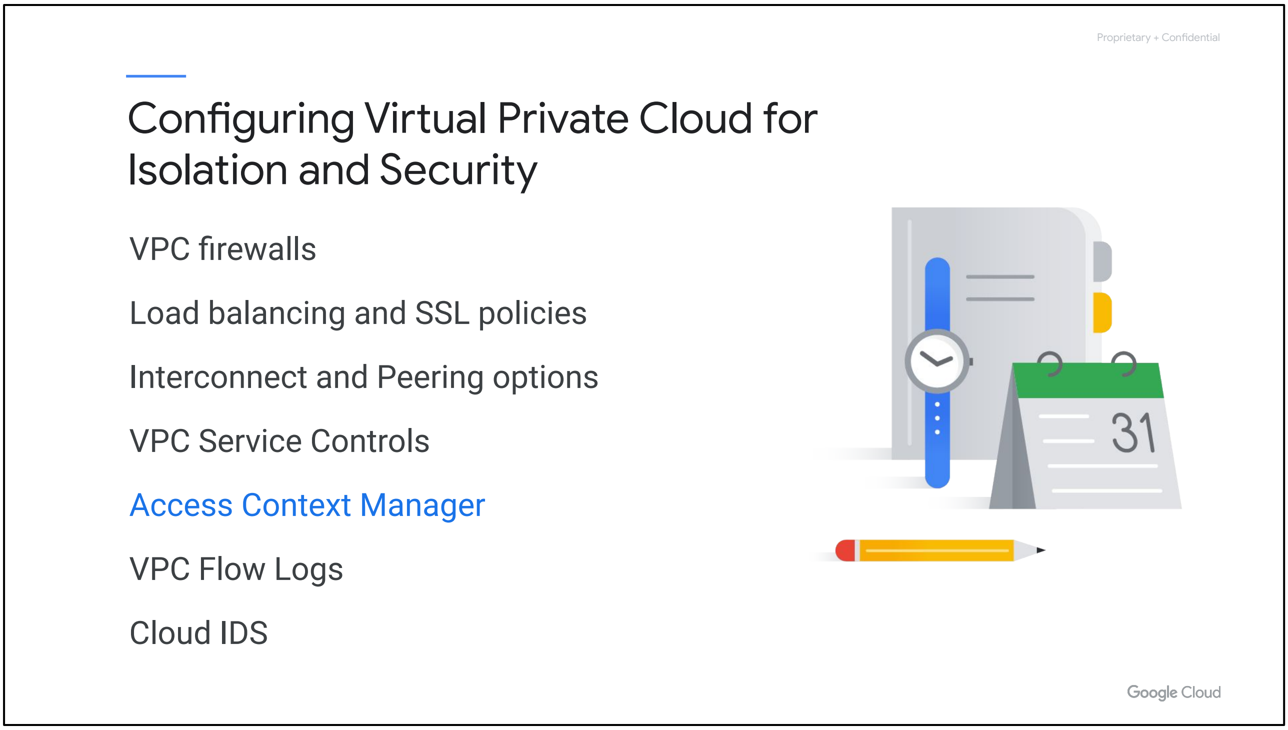
Private Google API access example

Google Cloud

The following diagram illustrates an implementation of Private Google Access.

The VPC network has been configured to meet the DNS, routing, and firewall network requirements for Google APIs and services. Private Google Access has been enabled on subnet-a, but not on subnet-b.

- VM A1 can access Google APIs and services, including Cloud Storage, because its network interface is located in subnet-a, which has Private Google Access enabled. Private Google Access applies to the instance because it only has an internal IP address.
    a. Private Google Access does not apply to instances with external IP addresses.
- VM B1 **cannot** access Google APIs and services because it only has an internal IP address and Private Google Access is disabled for subnet-b.
- VM A2 and VM B2 can both access Google APIs and services, including Cloud Storage, because they each have external IP addresses. Private Google Access has no effect on whether or not these instances can access Google APIs and services because both have external IP addresses.



Configuring Virtual Private Cloud for Isolation and Security

VPC firewalls

Load balancing and SSL policies

Interconnect and Peering options

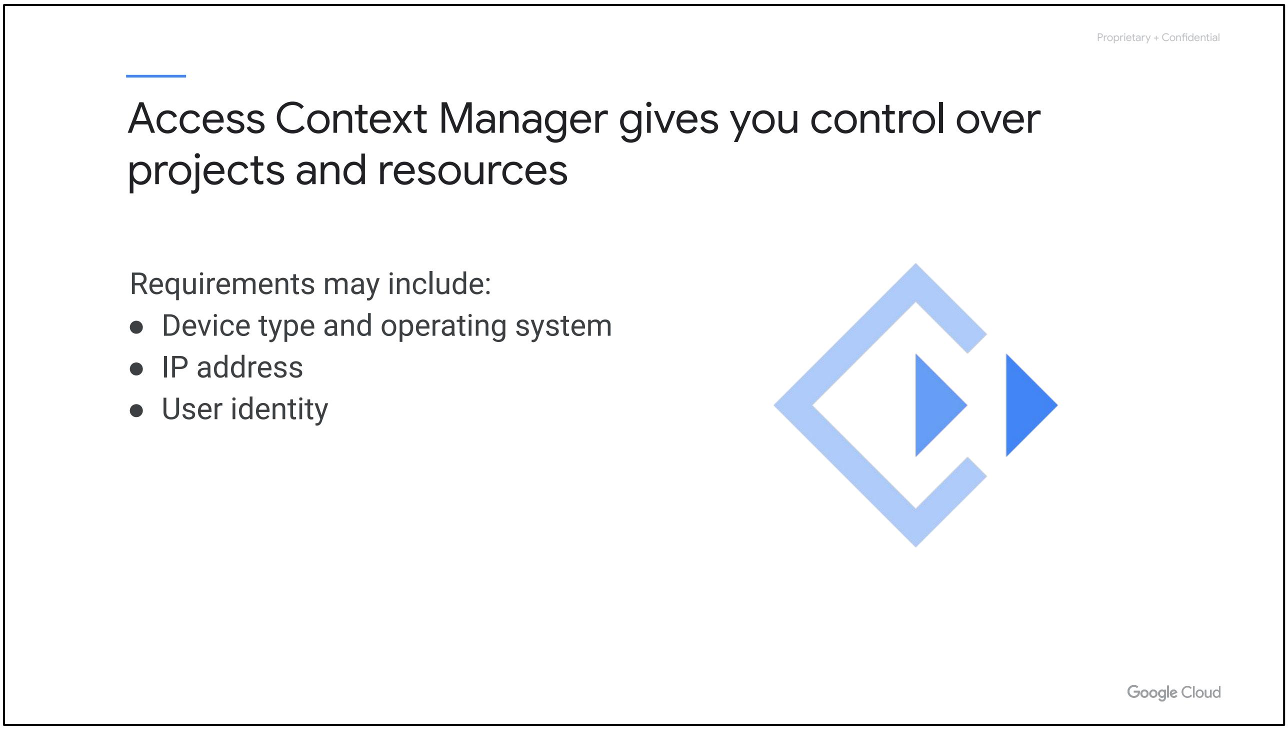
VPC Service Controls

Access Context Manager

VPC Flow Logs

Cloud IDS

Now let’s talk about Access Context Manager.



Proprietary + Confidential

Access Context Manager gives you control over projects and resources

Requirements may include:

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

Google Cloud

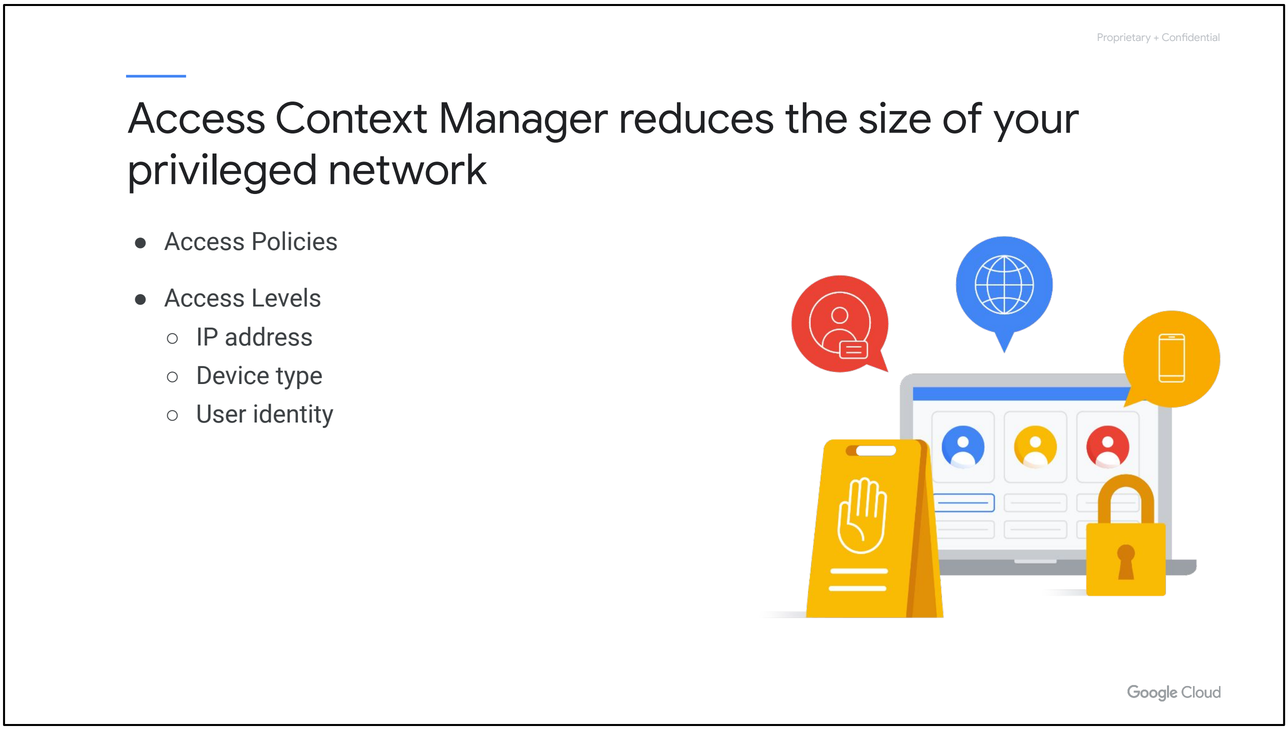
So, what is Access Context Manager? Access Context Manager is a tool with an API that allows Google Cloud organization administrators to define fine-grained, attribute based access control for projects and resources in Google Cloud.

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

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

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.

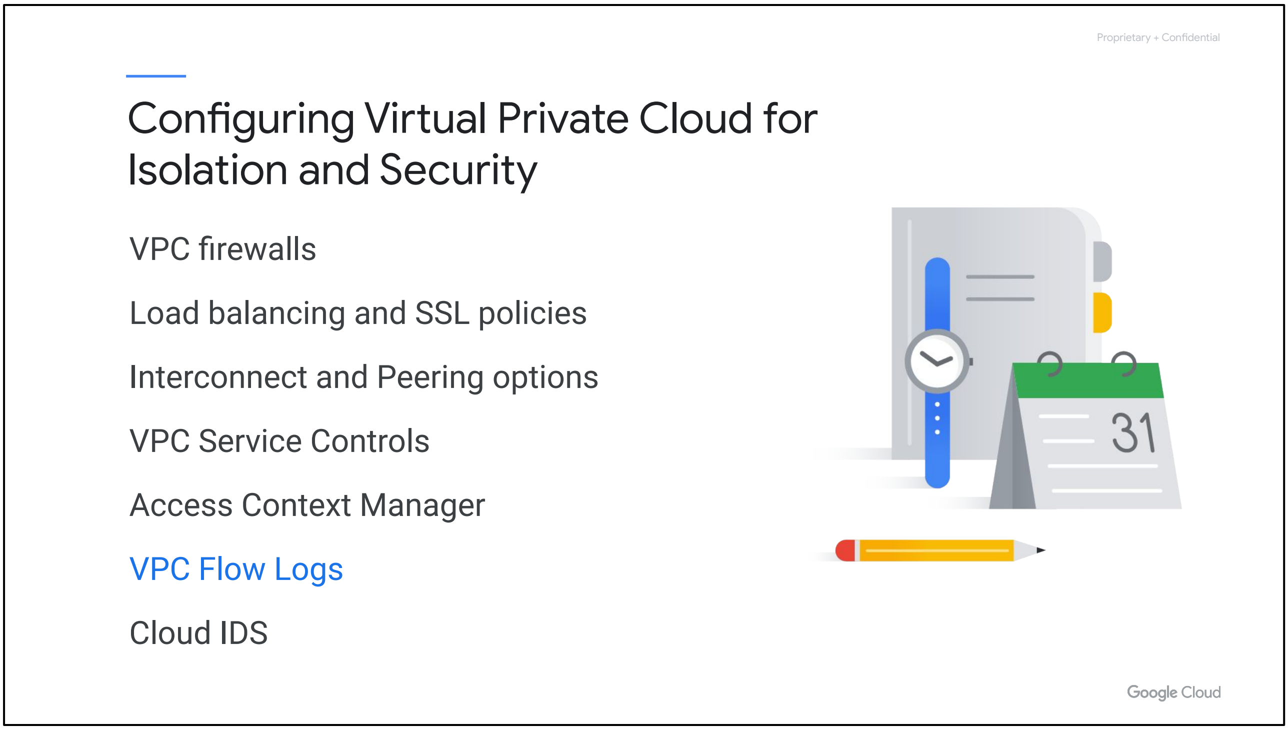
An access level is a set of attributes (such as IP address, device type and User identity) that are assigned to requests based on their origin. Using this information, when requests come in, you can decide what level of access to grant. Access levels are customizable; "High_Trust," "Medium_Trust," and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



Configuring Virtual Private Cloud for Isolation and Security

VPC firewalls

Load balancing and SSL policies

Interconnect and Peering options

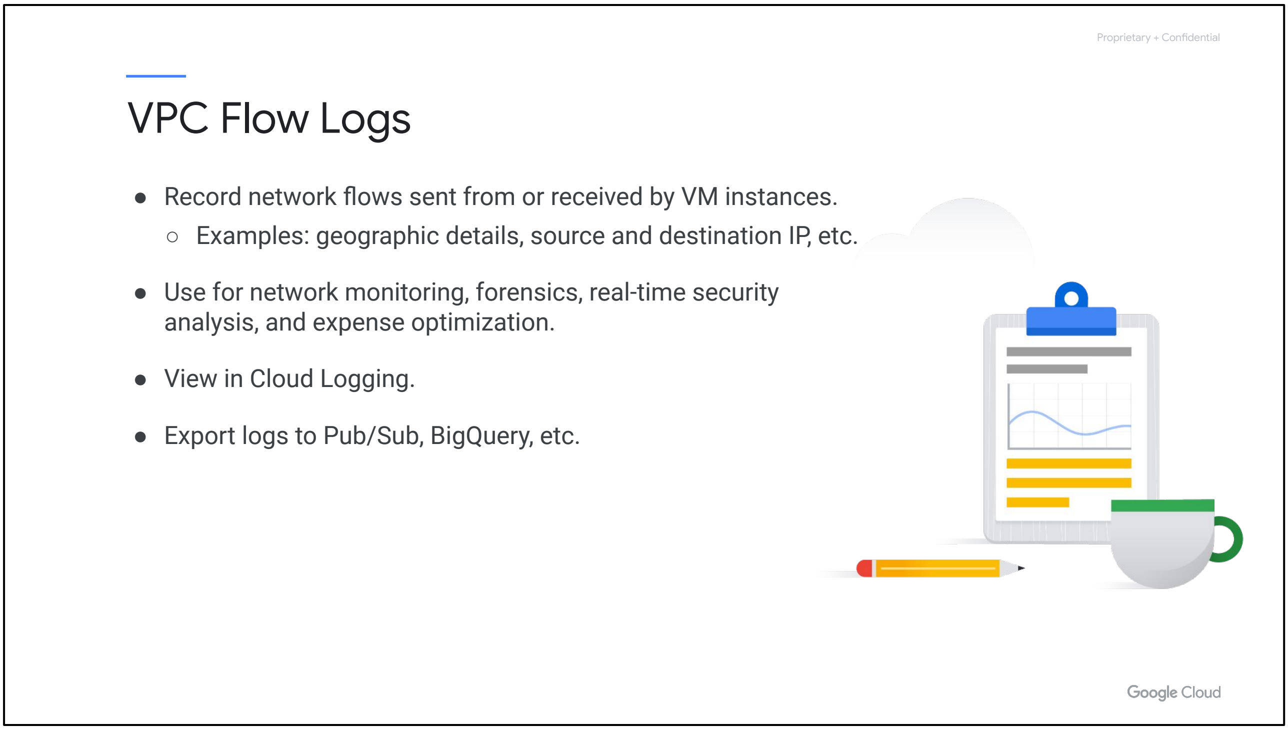
VPC Service Controls

Access Context Manager

VPC Flow Logs

Cloud IDS

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



VPC Flow Logs

- Record network flows sent from or received by VM instances.
  - Examples: geographic details, source and destination IP, etc.
- Use for network monitoring, forensics, real-time security analysis, and expense optimization.
- View in Cloud Logging.
- Export logs to Pub/Sub, BigQuery, etc.

VPC Flow Logs record network flows sent from or received by VM instances. Examples include geographic details, source and destination IP, etc.

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.

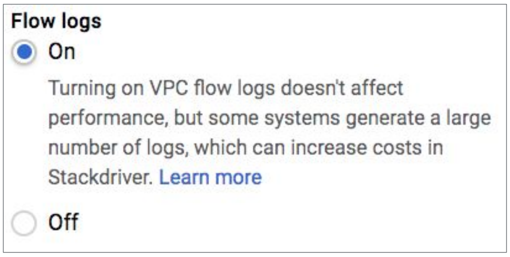
These logs can be used to monitor network traffic to and from your VMs, forensics, real-time security analysis, and expense optimization.

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



Flow logs

● On

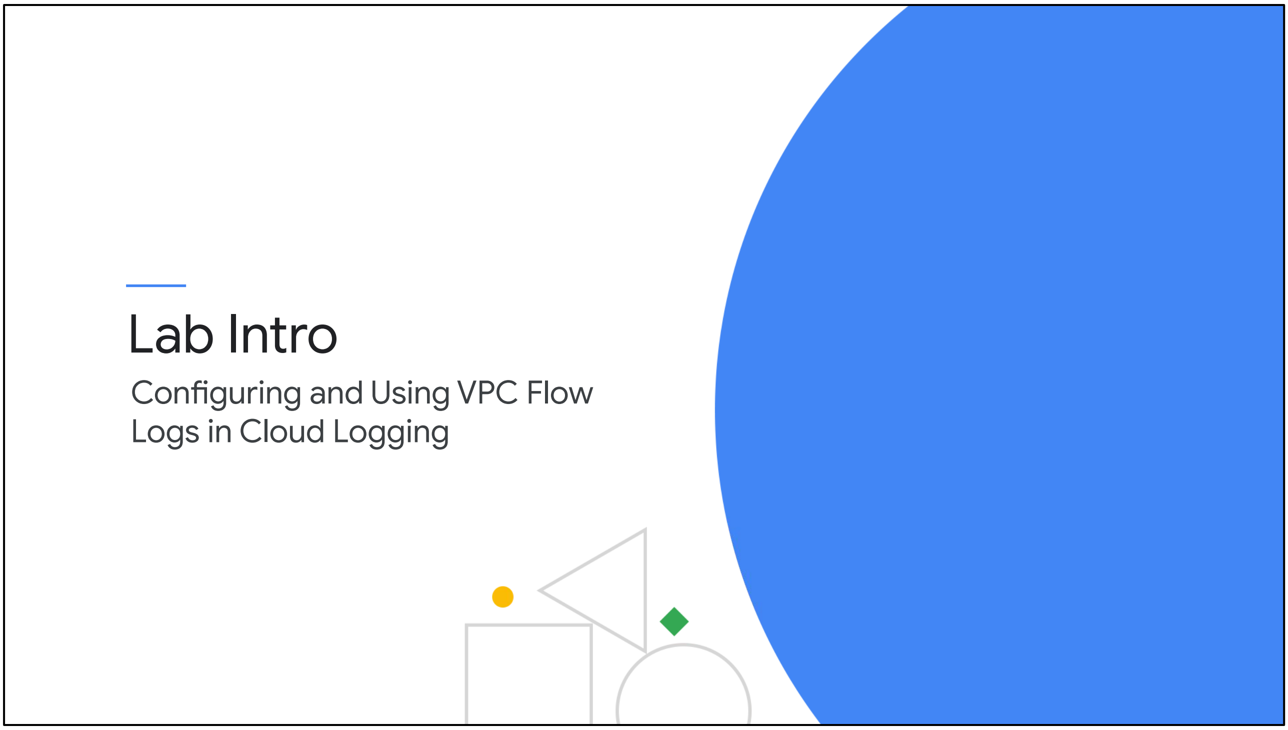
Turning on VPC flow logs doesn't affect performance, but some systems generate a large number of logs, which can increase costs in Stackdriver. Learn more

○ Off

- No performance penalty

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

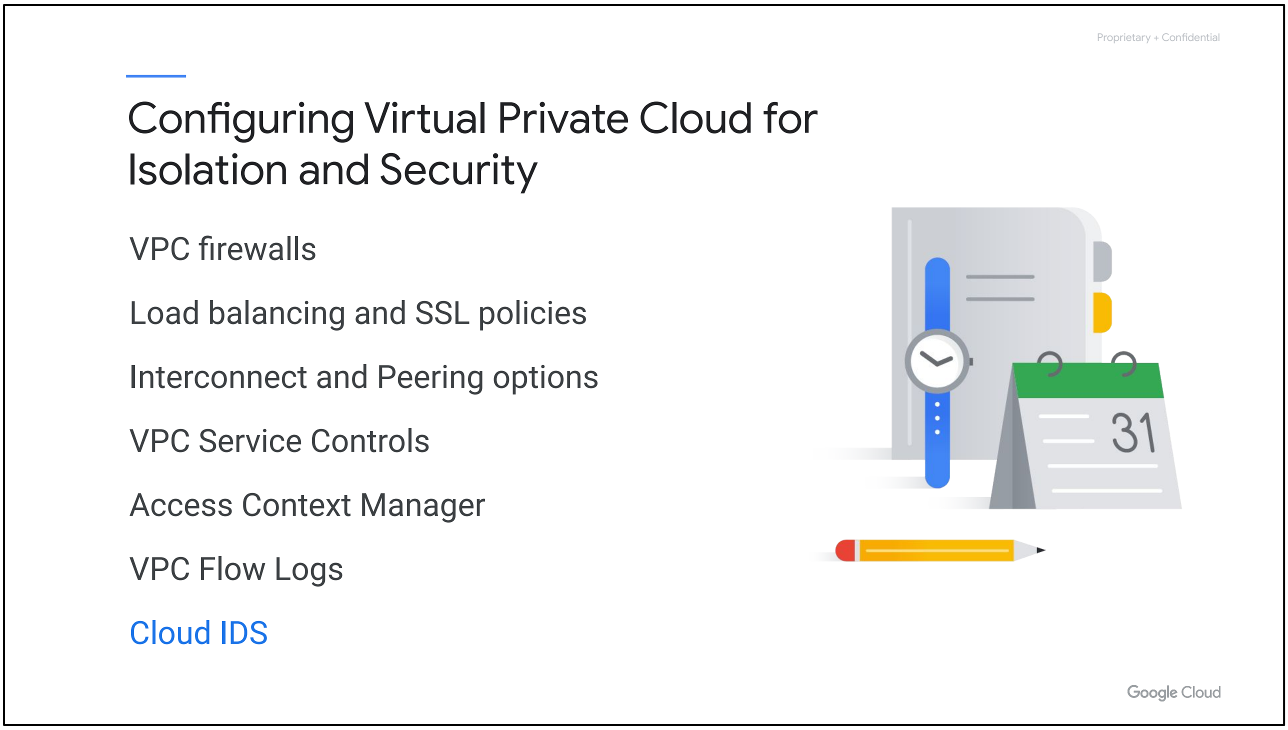
VPC Flow Logs is natively built into the networking stack of the VPC network infrastructure. There is no extra delay and no performance penalty in routing the logged IP packets to their destination, but some systems generate a large number of logs, which can increase costs in Cloud Logging.



Lab Intro

Configuring and Using VPC Flow Logs in Cloud Logging

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.



Configuring Virtual Private Cloud for Isolation and Security

VPC firewalls

Load balancing and SSL policies

Interconnect and Peering options

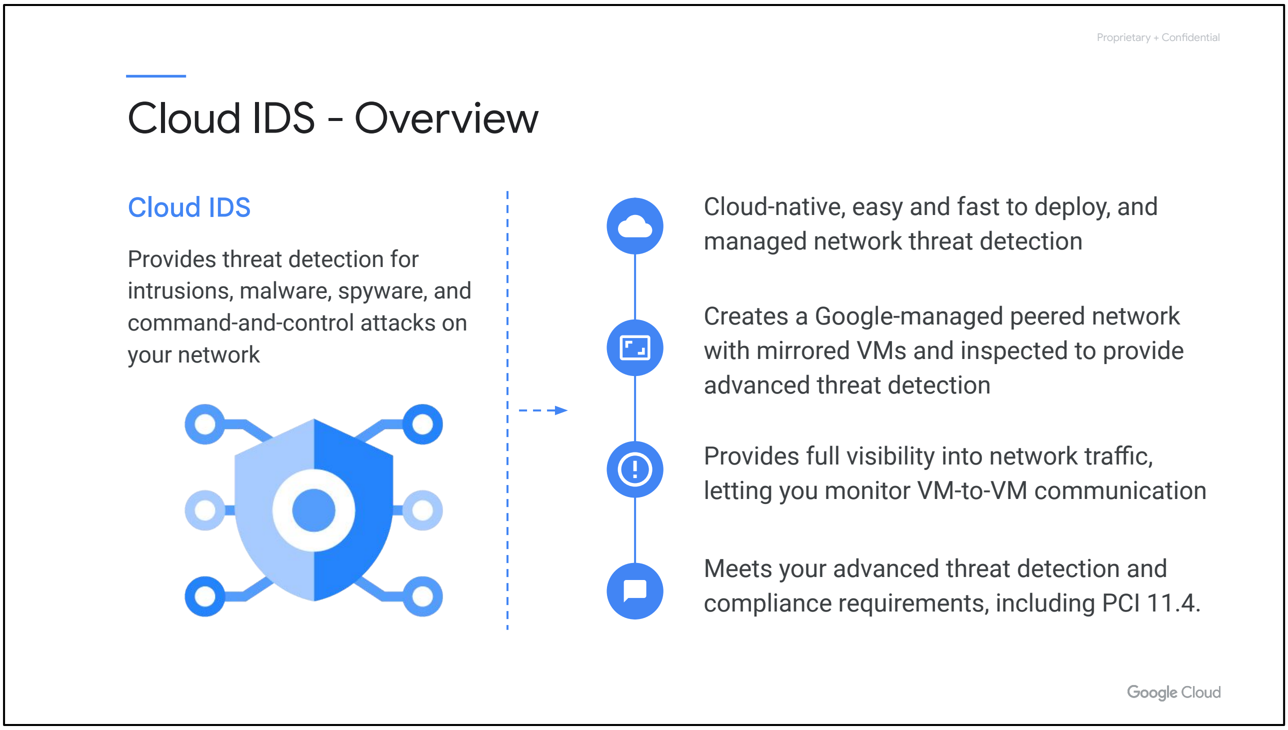
VPC Service Controls

Access Context Manager

VPC Flow Logs

Cloud IDS

Now let’s talk a little bit about Cloud IDS.



Cloud IDS - Overview

Cloud IDS

Provides threat detection for intrusions, malware, spyware, and command-and-control attacks on your network

- Cloud-native, easy and fast to deploy, and managed network threat detection
- Creates a Google-managed peered network with mirrored VMs and inspected 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

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

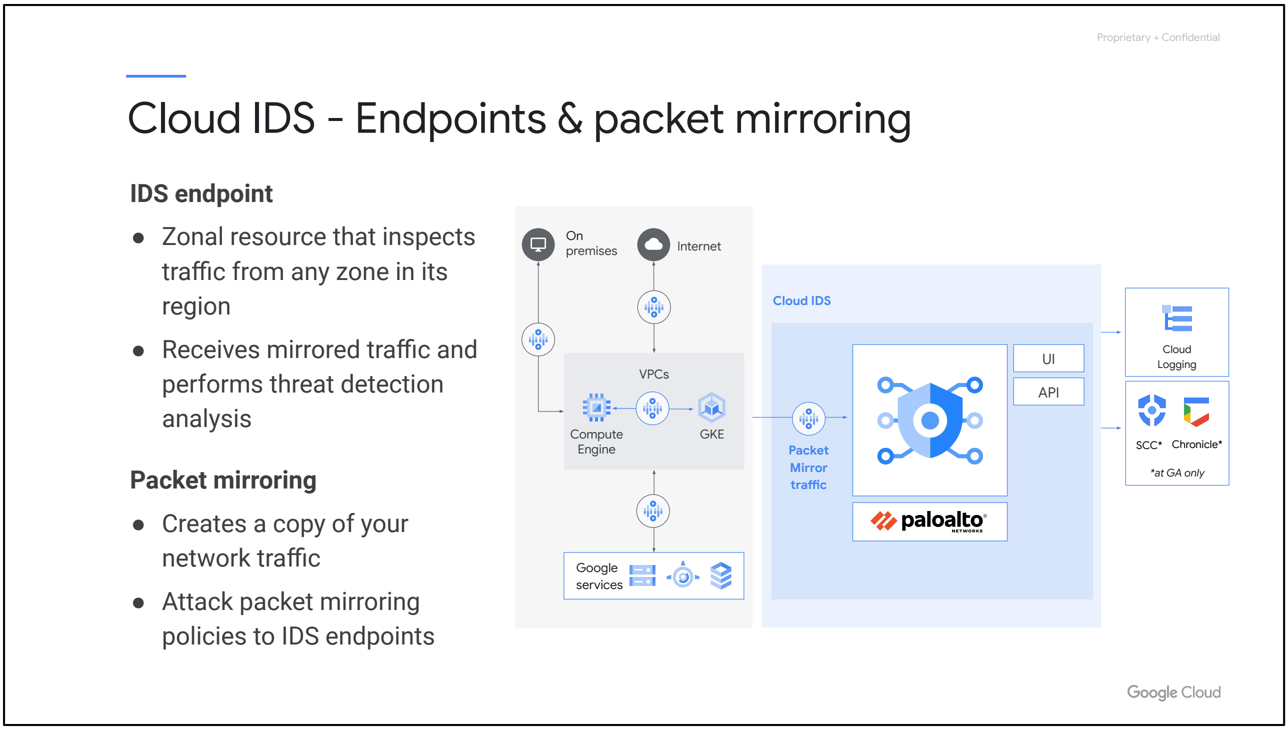
Cloud IDS is an intrusion detection service that provides threat detection for intrusions, malware, spyware, and command-and-control attacks on your network.

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.

Not only does Cloud IDS give you immediate indications when attackers are attempting to breach your network, the service can also be used for compliance validation, like PCI 11.

Cloud IDS also 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 & 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
- Attack 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.

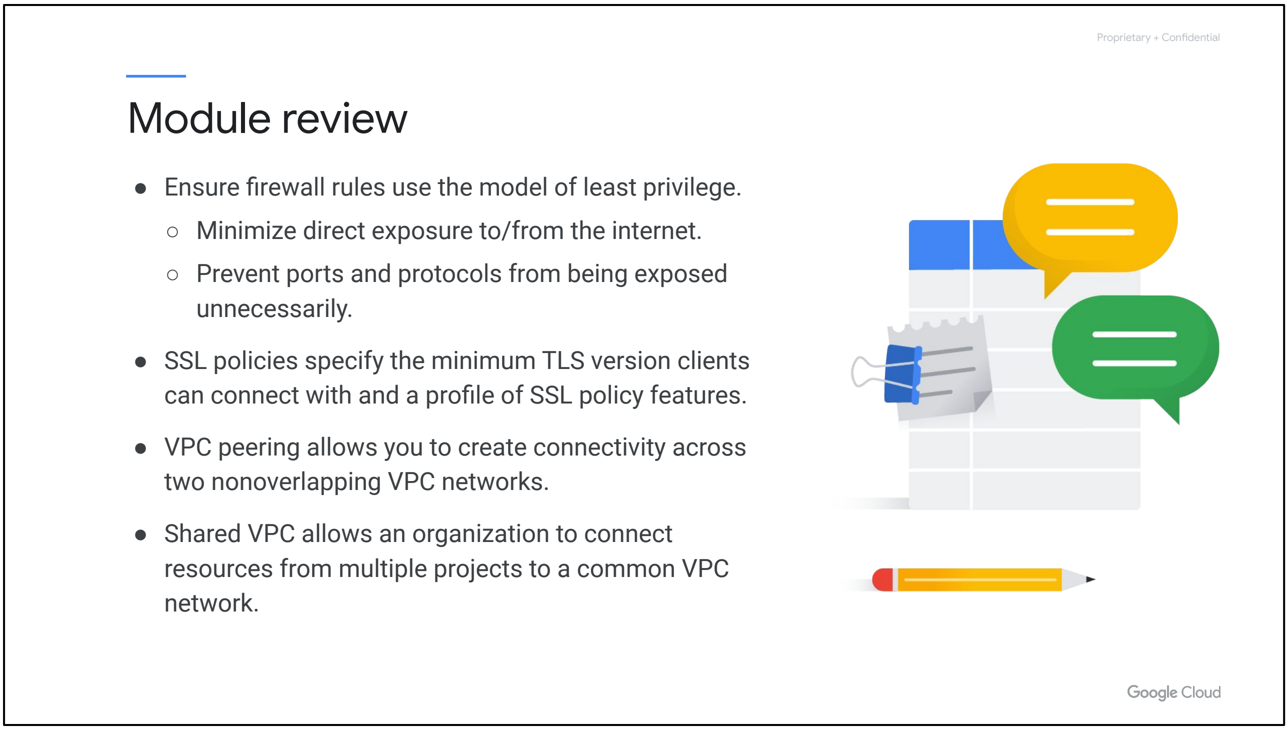
These policies send mirrored traffic to a single IDS endpoint for inspection. The packet mirroring logic sends all traffic from individual VMs to Google-managed IDS VMs: for example, all traffic mirrored from VM1 and VM2 will always be sent to IDS-VM1.

Lab Intro

Getting Started with Cloud IDS

In this lab, you deploy Cloud IDS (Intrusion Detection System), a next-generation advanced intrusion detection service that provides threat detection for intrusions, malware, spyware and command-and-control attacks.

You will simulate multiple attacks and view the threat details in the Cloud Console.



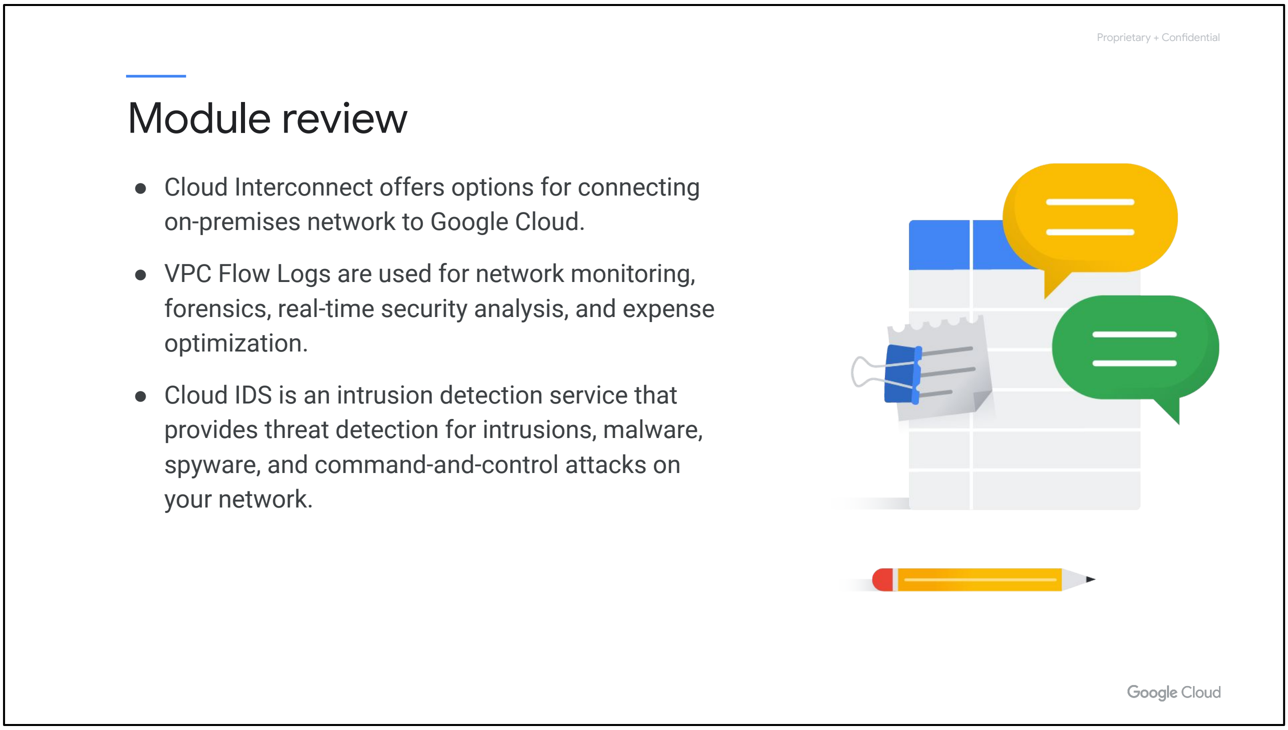
Module review

- 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.

Google Cloud

To recap:

- 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.



Proprietary + Confidential

Module review

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