Private Google Access enables VM instances with only internal (private) IP addresses (no external IP addresses) to reach the public IP addresses of Google APIs and services (https://developers.google.com/apis-explorer/). The source IP address of the packet can be the primary internal IP address of the network interface or any alias IP address that is assigned to the interface.

In addition to Google APIs and services, Private Google Access also grants access to third-party services hosted in App Engine. This allows your VMs to talk to your App Engine-based services.

You enable Private Google Access at the subnet level. When enabled, instances in the subnet that only have private IP addresses can send traffic to Google APIs and services through the default route (`0.0.0.0/0`) with a next hop to the default Internet gateway.

Private Google Access allows access to certain Google Cloud services from VM instances with only internal IP addresses. For details about Private Google Access and other private access options, see Private Access Options for Services (/vpc/docs/private-access-options).

To view the eligible APIs and services that you can use with Private Google Access, see supported services (/vpc/docs/private-access-options#pga-supported) in the Private Google Access overview.

Project owners, editors, and IAM members with the Network Admin (/compute/docs/access/iam#compute.networkAdmin) role can create or update subnets and assign IP addresses.

For more information on roles, read the IAM roles (/compute/docs/access/iam) documentation.

Stackdriver Logging captures all API requests made from VM instances in subnets that have Private Google Access enabled. Log entries identify the source of the API request using the private IP of the instance.

You can configure daily usage and monthly rollup reports to be delivered to a Cloud Storage bucket. See the Viewing Usage Reports (/compute/docs/usage-export) page for details.

Private Google Access has the following requirements:

- Private Google Access does not automatically enable any API. You must enable the Google APIs (https://support.google.com/cloud/answer/6158841?hl=en) you need to use via the APIs & services page (https://console.cloud.google.com/apis/dashboard) in the Google Cloud Console separately.
- Private Google Access requires a VPC network (/vpc/docs/vpc). Both auto and custom mode VPC networks are supported. Legacy networks (/vpc/docs/legacy) are not supported.
- Private Google Access only applies to instances that only have internal IP addresses. Enabling or disabling Private Google Access has no effect on instances with external IP addresses (/compute/docs/ip-addresses/reserve-static-external-ip-address).
- You enable Private Google Access on a subnet-by-subnet basis, either when you create a subnet or by editing the subnet later on. When enabled for a subnet, Private Google Access applies to new and existing VM instances in that subnet that do not have external IP addresses.
- Private Google Access requires a route to the public IP addresses used by Google APIs and services. The default route usually provides this path. Refer to the routing (#ensuring_that_routing_is_properly_configured) section for additional details.

DNS resolution for domains associated with Google APIs or services, including `*.googleapis.com` and `gcr.io`, does not change when Private Google Access is enabled for a subnet. The DNS records for Google APIs and services always point to external IP addresses. The pool of external IP addresses they use is subject to change, but can be determined by querying `_spf.google.com` and the TXT records it references.

For example:

Private Google Access works in conjunction with an appropriate route (#ensuring_that_routing_is_properly_configured) to allow VM instances with only internal IP addresses to reach the external IP addresses of Google APIs and services. Although Private Google Access supports Google APIs and services that have external IPs from `_spf.google.com`, Private Google

Access doesn't support all external IPs from `_spf.google.com`. For example, the external IPs for `smtp.gmail.com` aren't supported.

Even though the IP addresses for Google APIs and services are public, the traffic path from instances that are using e Google Access to the Google APIs remains within Google's network.

Instead of using the standard set of public IP addresses, you can configure your DNS to map `*.googleapis.com` to a well-defined range. You do this by inserting a CNAME record that marks `*.googleapis.com` as an alias for one of these Google-provided domains:

Domain and VIPs	Supported services	Example usage

`restricted.googleapis.com`
`199.36.153.4/30`
	Enables API access to Google APIs and services that are supported by VPC Service Controls (/vpc-service-controls/docs/supported-products)
	.
	Blocks access to Google APIs and services that do not support VPC Service Controls (/vpc-service-controls/docs/overview). Does not support G Suite web applications or G Suite APIs.
		Use **`restricted.googleapis.com`** to make only the VPC Service Controls restricted services available to hosts in your VPC network or on-premises network.

`private.googleapis.com`
`199.36.153.8/30`
	Enables API access to most Google APIs and services regardless of whether they are supported by VPC Service Controls. Includes API access to Google Maps, Google Ads, Google Cloud platform, and most other Google APIs whose names end in **`googleapis.com`**. Does not support G Suite web applications.	Use **`private.googleapis.com`** when you must access Google APIs and services under the following circumstances:
		• You are not using VPC Service Controls.
		• You are using VPC Service Controls but also need to access services that are not supported by VPC Service Controls.

f you use or plan to use VPC Service Controls, Google recommends that you direct DNS requests for **`*.googleapis`** **`restricted.googleapis.com`** VIP unless you must also access Google APIs and services that are not supported b ervice Controls. Although you can access services that are supported by VPC Service Controls on both VIPs, only the `restricted.googleapis.com` domain provide additional mitigation for data exfiltration risks because they deny s to Google APIs and services that are not supported by VPC Service Controls.

In a typical VPC network the primary purpose of the default route is to provide Internet access to instances with external IP addresses.

However, Private Google Access uses the default route (/vpc/docs/vpc#system-generated-routes) to send traffic to the external IP addresses of Google APIs and services from instances in subnets where Private Google Access is enabled. Review the routes overview (/vpc/docs/routes) for information about how routing works in Google Cloud.

If you have replaced the default route with a custom static route having a destination of `0.0.0.0/0` and a next hop that's *not* the default Internet gateway, you must create a set of custom routes (#advanced_routing) to meet the routing requirement for Private Google Access. For example, you must create custom routes in the following situations:

- You have a custom static route to direct traffic destined to `0.0.0.0/0` to a Cloud VPN tunnel or to another instance, such as a NAT instance (/vpc/docs/special-configurations#natgateway)
- You use a Cloud Router to accept a custom dynamic route having a destination of `0.0.0.0/0`

You can create a set of custom static routes to send traffic to the external IP addresses of Google APIs and services. The next hop for each route in this set must be the `default Internet gateway`, but the destination for each is a unique IP address range from the set of ranges that are used by Google APIs and services. See DNS resolution for APIs and services (#dns_resolution) to determine those IP ranges.

n: The set of IP addresses associated with Google APIs and services can change without notice, so you must monito ges (#dns_resolution) and update your set of custom static routes accordingly.

Alternatively, you can use the `restricted.googleapis.com` (`199.36.153.4/30`) or `private.googleapis.com` (`199.36.153.8/30`) VIPs (virtual IP addresses) to create a single custom static route that you don't have to continuously monitor. These ranges are typically used with VPC

Service Controls and don't support all Google APIs and services. Refer to Domain names and VIPs (/vpc/docs/private-access-options#private-vips) for more information. You'll also need to create a Cloud DNS managed private zone for `googleapis.com` with an `A` record for the chosen VIP or VIP's domain name and a `CNAME` record for `*.googleapis.com` to the chosen domain name. For more information, Configuring Private Google Access for on-premises hosts (/vpc/docs/configure-private-google-access-hybrid).

If you want to use VPC Service Controls (/vpc-service-controls/docs/) in combination with Private Google Access, refer to Setting up private connectivity (/vpc-service-controls/docs/set-up-private-connectivity) in the VPC Service Controls documentation.

To determine whether a default route exists for a given network, use the Cloud Console or the `gcloud` command line tool:

If you can use a default route for Private Google Access and need to re-create it, create a replacement custom static route (/vpc/docs/using-routes#addingroute) with the following destination and next hop:

- Destination: `0.0.0.0/0`
- Next hop: **Default Internet gateway**

If you can't use a default route, you can create multiple custom static routes (/vpc/docs/using-routes#addingroute) to meet the routing requirement for Private Google Access, where each route has the following destination and next hop:

- Destination: one of the IP address ranges (#dns_resolution) that's used by Google APIs and services.
- Next hop: **Default Internet gateway**

In addition to meeting the routing requirements, firewall rules in your network must allow access from VMs to Google APIs and Google Cloud services.

For instances to use Private Google Access, you must allow egress traffic from the instances to the Google APIs and services. If you have a firewall rule that denies egress traffic, you can selectively apply that rule to other instances that do not need Private Google Access, or you can override that rule by creating a higher priority rule to allow traffic to Google APIs and services. If you choose to create a higher priority firewall rule to allow traffic to Private Google Access, consider the following options:

- Create a firewall rule that allows egress to the `0.0.0.0/0` address range, which indicates egress can go to any destination. Apply that rule only to instances that require Private Google Access by setting target tags on the firewall rule. Use a source tag or service account (/vpc/docs/firewalls#serviceaccounts) on the instances. Creating a rule that applies only to specific targets that do not have external IP addresses compensates for the broad destination range. Instances without external IP addresses cannot send packets outside of the VPC network. View Internet access requirements (/vpc/docs/vpc#internet_access_reqs) for details.
- If you allow Private Google Access traffic by creating multiple firewall rules to permit egress to specific destinations, you must periodically review and update those rules so they include all possible IP address ranges that are used by Google APIs and services. See the DNS resolution for APIs and services (#dns_resolution) section to determine those IP ranges.

on: IP ranges for Google APIs and services can change without notice, so creating firewall rules with specific destinat
ad to outages until you manually look up the Google API and service IP ranges and update your firewall rules.

By default, Private Google Access isn't enabled. You can enable it when you create a subnet, and you can enable or disable it by editing a subnet.

Follow these steps to enable Private Google Access:

Follow these steps to disable Private Google Access for an existing subnet:

Because Private Google Access is only relevant for instances *without* external IP addresses, you might need to modify running instances after you enable Private Google Access for a subnet. To remove an external IP address from an instance, see Unassigning a static external IP address (/compute/docs/ip-addresses/reserve-static-external-ip-address#unassign_ip) in the Compute Engine documentation.

For more information about instance IP addresses, see IP addresses (/compute/docs/ip-addresses/) in the Compute Engine documentation.

- To configure Private Google Access for on-premises hosts, see Configuring Private Google Access for on-premises hosts (/vpc/docs/configure-private-google-access-hybrid).