VPC Service Controls (https://cloud.google.com/vpc-service-controls/)
Documentation (https://cloud.google.com/vpc-service-controls/docs/) Guides

Private Google Access with VPC Service Controls

Private Google Access offers private connectivity to hosts either in a VPC network or on-premises network that use private IP addresses to access Google APIs and services (https://developers.google.com/apis-explorer/#p/). You can extend a VPC Service Controls service perimeter to hosts in those networks to control access to protected resources.

For hosts in a VPC network, they must have a private IP address only (no public IP address) and be in a subnet with *Private Google Access* enabled.

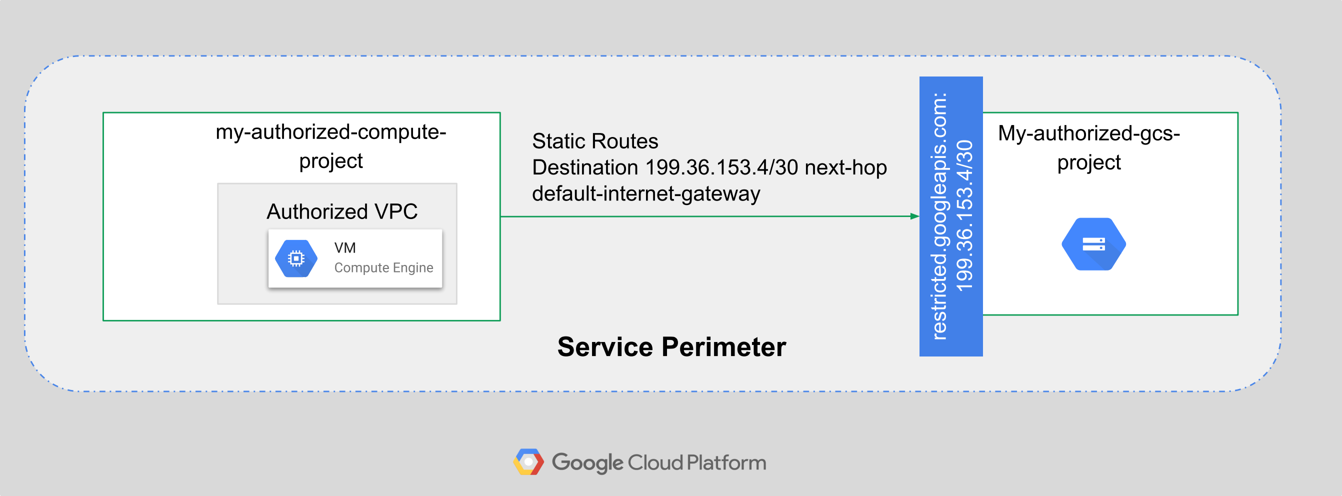
For on-premises hosts to reach restricted Google API services, requests to Google APIs must be sent through a VPC network, either through a Cloud VPN (https://cloud.google.com/vpn/docs) tunnel or Cloud Interconnect (https://cloud.google.com/interconnect/docs) connection.

In both cases, all requests to Google APIs and services must be sent to a virtual IP address (VIP) range `199.36.153.4/30` (`restricted.googleapis.com`). The IP address range is not announced to the Internet. Traffic sent to the VIP stays within Google's network only.

Note: If you require access to other Google APIs and services that aren't supported by VPC Service Controls, you can use `199.36.153.8/30` (`private.googleapis.com`). However, we recommend that you use `restricted.googleapis.com`, which integrates with VPC Service Controls and mitigates data exfiltration risks. In either case, VPC Service Controls service perimeters are always enforced on APIs and services that support VPC Service Controls.

VPC network example

In the following example, the service perimeter contains two projects: one that has an authorized VPC network and another with the protected Cloud Storage resource. In the VPC network, VM instances must be in a subnet with Private Google Access (https://cloud.google.com/vpc/docs/private-google-access#pga) enabled and only require access to VPC Service Controls restricted services. Queries to Google APIs and services from VM instances in the authorized VPC network resolve to `restricted.googleapis.com` and can access the protected resource.


my-authorized-compute-project
Authorized VPC
VM
Compute Engine
Static Routes
Destination 199.36.153.4/30 next-hop default-internet-gateway
restricted.googleapis.com:
199.36.153.4/30
My-authorized-gcs-project
Service Perimeter
Google Cloud Platform

(https://cloud.google.com/vpc-service-controls/images/pga-for-vpc-service-controls-1.svg)
Private Google Access with VPC Service Controls (click to enlarge)

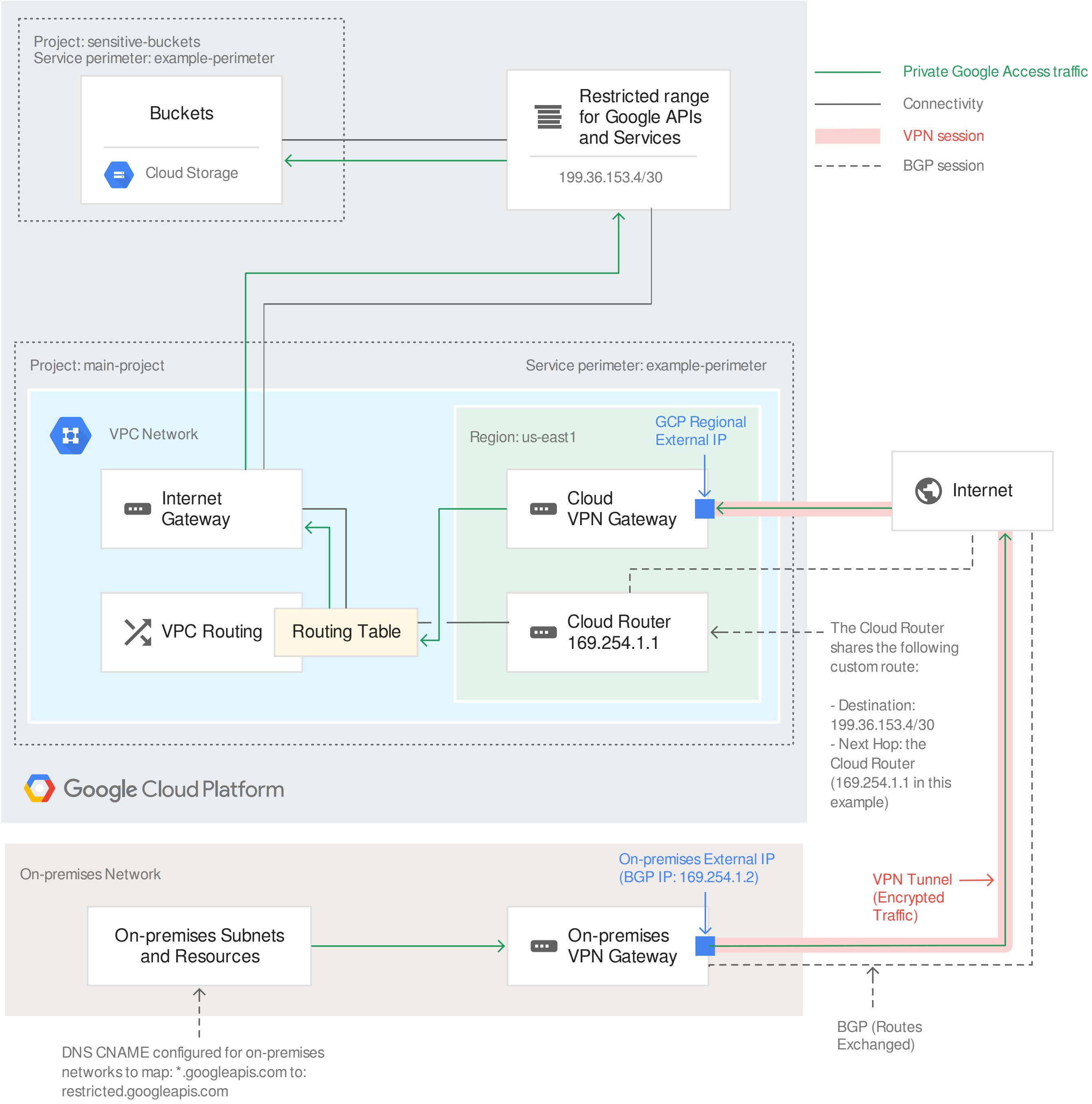
- DNS was configured in the VPC network to map `*.googleapis.com` requests to `restricted.googleapis.com`, which resolves to `199.36.153.4/30`.
- A custom static route was added to the VPC network that directs traffic with the destination `199.36.153.4/30` to the `default-internet-gateway` as the next hop. Even though `default-internet-gateway` is used as the next hop, traffic is routed privately through Google's network to the appropriate API or service.
- The VPC network was authorized to access the `My-authorized-gcs-project` because both projects are in the same service perimeter.

On-premises network example

You can use either static routing, by simply configuring a static route in the on-premises router, or by announcing the restricted Google API address range through border gateway protocol (BGP) from Cloud Router (https://cloud.google.com/compute/docs/cloudrouter).

To use Private Google Access for on-premises hosts with VPC Service Controls, set up private connectivity (https://cloud.google.com/vpc/docs/configure-private-google-access-hybrid) for on-premises hosts and then configure VPC Service Controls. Define a service perimeter for the project that contains the VPC network that's connected to your on-premises network.

In the following scenario, the storage buckets in project `sensitive-buckets` can only be accessed from VM instances in the project `main-project` and from connected on-premises applications. On-premises hosts can access storage buckets in the project `sensitive-buckets` because traffic goes through a VPC network that's inside the same service perimeter as `sensitive-buckets`.


Project: sensitive-buckets
Service perimeter: example-perimeter
Buckets
Cloud Storage
Restricted range for Google APIs and Services
199.36.153.4/30
Private Google Access traffic
Connectivity
VPN session
BGP session
Project: main-project
Service perimeter: example-perimeter
VPC Network
Region: us-east1
GCP Regional External IP
Internet Gateway
Cloud VPN Gateway
Internet
VPC Routing
Routing Table
Cloud Router 169.254.1.1
The Cloud Router shares the following custom route:
- Destination: 199.36.153.4/30
- Next Hop: the Cloud Router (169.254.1.1 in this example)
Google Cloud Platform
On-premises Network
On-premises External IP (BGP IP: 169.254.1.2)
On-premises Subnets and Resources
On-premises VPN Gateway
VPN Tunnel (Encrypted Traffic)
BGP (Routes Exchanged)
DNS CNAME configured for on-premises networks to map: *.googleapis.com to: restricted.googleapis.com

(https://cloud.google.com/vpc-service-controls/images/pga-hybrid-use-case1.svg)
Private Google Access for hybrid cloud use case (click to enlarge)

- The on-premises DNS configuration maps `*.googleapis.com` requests to `restricted.googleapis.com`, which resolves to the `199.36.153.4/30`.
- The Cloud Router was configured to advertise the `199.36.153.4/30` IP address range through the VPN tunnel. Traffic going to Google APIs is routed through the tunnel to the VPC network.

- A custom static route was added to the VPC network that directs traffic with the destination `199.36.153.4/30` to the `default-internet-gateway` as the next hop. Even though `default-internet-gateway` is used as the next hop, traffic is routed privately through Google's network to the appropriate API or service.
- The VPC network was authorized to access the `sensitive-buckets` projects, and on-premises hosts have the same access.
- On-premises hosts can't access other resources that are outside of the service perimeter.

The project that connects to your on-premises network must be a member of the service perimeter to reach restricted resources. On-premises access also works if the relevant projects are connected by a perimeter bridge.

What's next

- To configure private connectivity, refer to Setting up private connectivity (https://cloud.google.com/vpc-service-controls/docs/set-up-private-connectivity).

Last updated August 13, 2019.