Overview of VPC Service Controls

VPC Service Controls improves your ability to mitigate the risk of data exfiltration from Google-managed services like Cloud Storage and BigQuery. With VPC Service Controls, you can configure security perimeters around the resources of your Google-managed services and control the movement of data across the perimeter boundary.

Note: For more information on products and services that are supported by VPC Service Controls, refer to the Supported products (https://cloud.google.com/vpc-service-controls/docs/supported-products) page.

For all Google-managed services secured with VPC Service Controls, you can ensure that:

- Resources within a perimeter can only be privately accessed from clients within authorized VPC networks using Private Google Access with either Google Cloud or on-premises.
- Clients within a perimeter that have private access to resources do not have access to unauthorized (potentially public) resources outside the perimeter.
- Data cannot be copied to unauthorized resources outside the perimeter using service operations such as `gsutil cp` (https://cloud.google.com/storage/docs/gsutil/commands/cp) or `bq mk` (https://cloud.google.com/bigquery/docs/reference/bq-cli-reference#bq_mk).
- When enabled, internet access to resources within a perimeter is restricted using whitelisted IPv4 and IPv6 ranges.

VPC Service Controls provides an additional layer of security defense for Google Cloud services that is independent of Cloud Identity and Access Management (Cloud IAM). While Cloud IAM enables granular *identity-based access control*, VPC Service Controls enables broader *context-*

based perimeter security, including controlling data egress across the perimeter. We recommend using both VPC Service Controls and Cloud IAM for defense in depth.

Security benefits of VPC Service Controls

VPC Service Controls helps mitigate the following security risks without sacrificing the performance advantages of direct private access to Google Cloud resources:

1. **Access from unauthorized networks using stolen credentials**: By allowing private access only from authorized VPC networks, VPC Service Controls protects against theft of OAuth credentials or service account credentials.
2. **Data exfiltration by malicious insiders or compromised code:** VPC Service Controls complements network egress controls by preventing clients within those networks from accessing the resources of Google-managed services outside the perimeter.

   VPC Service Controls also prevents reading data from or copying data to a resource outside the perimeter using service operations such as copying to a public Cloud Storage bucket using the `gsutil cp` command or to a permanent external BigQuery table using the `bq mk` command.

   The restricted VIPs feature can be used to prevent access from a trusted network to storage services that are not integrated with VPC Service Controls.
3. **Public exposure of private data caused by misconfigured Cloud IAM policies**: VPC Service Controls provides an additional layer of security by denying access from unauthorized networks, even if the data is exposed by misconfigured Cloud IAM policies.

   By assigning the Access Context Manager Policy Admin role for Cloud IAM, VPC Service Controls can be configured by a user who is not the Cloud IAM policy administrator.

VPC Service Controls is configured for your Google Cloud organization to create a broad, uniform policy that applies consistently to all protected resources within the perimeter. You retain the flexibility to process, transform, and copy data within the perimeter. The security controls automatically apply to all new resources created within a perimeter.

VPC Service Controls and metadata

VPC Service Controls is not designed to enforce comprehensive controls on metadata movement.

In this context, "data" is defined as content stored in a Google Cloud resource. For example, the contents of a Cloud Storage object. "Metadata" is defined as the attributes of the resource or its parent. For example, Cloud Storage bucket names.

The primary design goal of this release of VPC Service Controls is to control the movement of data, rather than metadata, across a service perimeter via supported services. While in most cases VPC Service Controls also controls access to metadata, there may be scenarios in which metadata can be copied and accessed without VPC Service Controls policy checks.

We recommend that you rely on Cloud IAM (https://cloud.google.com/iam/docs), including the use of custom roles (https://cloud.google.com/iam/docs/understanding-custom-roles), to ensure appropriate control over access to metadata.

Capabilities

VPC Service Controls provides these benefits by enabling you to define security policies that prevent access to Google-managed services outside of a trusted perimeter, blocking access to data from untrusted locations and mitigating data exfiltration risks. With this release of VPC Service Controls, you are able to:

- Isolate GCP resources and VPC networks (#isolate) into service perimeters
- Extend perimeters to on-premises networks (#hybrid_access) to authorized VPN or Cloud Interconnect
- Control access to GCP resources (#internet) from the internet

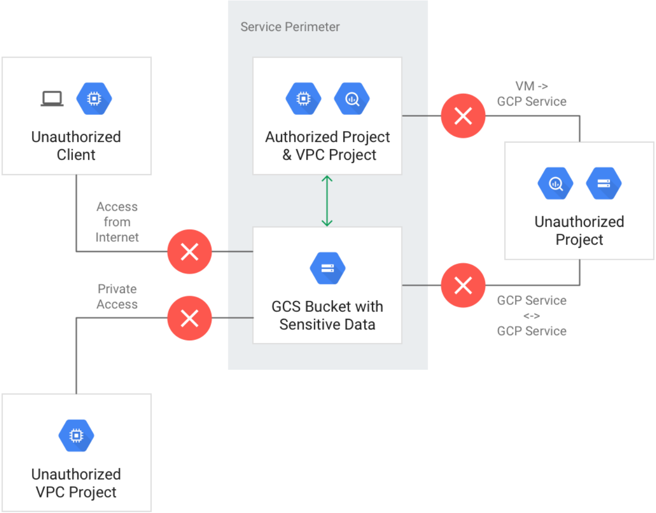
Isolate GCP resources into service perimeters

A **service perimeter** creates a security boundary around Google Cloud resources. You can configure a service perimeter to control communications from virtual machines (VMs) to a Google Cloud service (API), and between Google Cloud services. A service perimeter allows free communication within the perimeter but, by default, blocks all communication across the perimeter.

For example:

- A VM within a Virtual Private Cloud (VPC) network (https://cloud.google.com/vpc/docs/vpc) that is part of a service perimeter can read from or write to a Cloud Storage bucket in the same perimeter. However, any attempt to access the bucket from VPC networks that are not inside the perimeter is denied.

- A copy operation between two Cloud Storage buckets will succeed if both buckets are in the same service perimeter, but will fail if one of the buckets is outside the perimeter.
- A VM within a VPC network that is part of a service perimeter can privately access any Cloud Storage buckets in the same perimeter. However, the VM will be denied access to Cloud Storage buckets that are outside the perimeter.

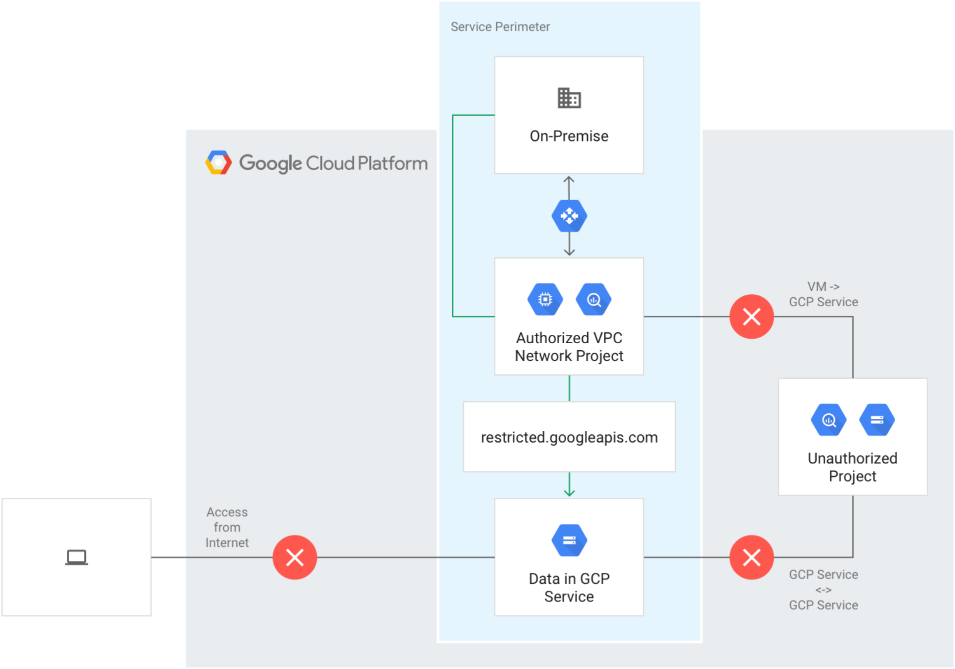


Extend perimeters to authorized VPN or Cloud Interconnect

You can configure private communication to Google Cloud resources from VPC networks that span hybrid environments with Private Google Access on-premises extensions (https://cloud.google.com/vpc-service-controls/docs/private-connectivity). A VPC network 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. If required, you can continue to enable inspected and audited access to all Google APIs (for example, Gmail) over the internet.

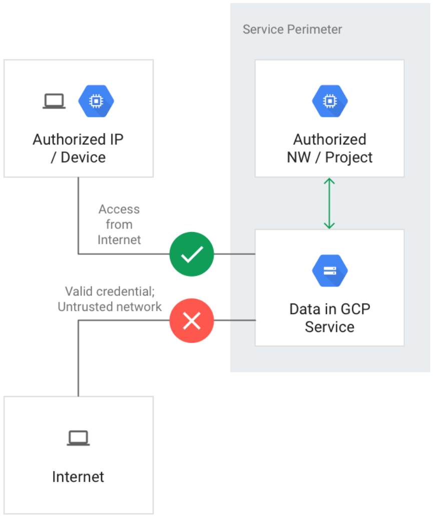
For example, a VM within a VPC network that is part of a service perimeter can privately access a Cloud Storage bucket in the same service perimeter. However, the VM will be denied access to Cloud Storage buckets that are outside the service perimeter.



Control access to GCP resources from the internet

Access from the internet to managed resources within a service perimeter is denied by default. Optionally, you can enable access based on the context of the request. To do so, you can create **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.

To use the Cloud Console to access resources within a perimeter, you must configure an access level that allows access from one or more IPv4 and IPv6 ranges, or to specific user accounts.



Unsupported Services

For more information on products and services that are supported by VPC Service Controls, refer to the Supported products (https://cloud.google.com/vpc-service-controls/docs/supported-products) page.

Warning: While it may be possible to enable unsupported services to access the data of supported products and services, we recommend that you do not. Unexpected issues might occur when attempting to access a supported service using an unsupported service, especially within the same project.

Unsupported services may not function at all when enabled in a project protected by VPC Service Controls, especially when low-level storage services like Cloud Storage or Pub/Sub are restricted. We recommend deploying unsupported services in projects outside perimeters. To allow these services to access data in resources within a perimeter, create an access level (https://cloud.google.com/vpc-service-controls/docs/use-access-levels) that includes the service account for that service and apply it to perimeters as needed (https://cloud.google.com/vpc-service-controls/docs/manage-service-perimeters#add-access-level).

Attempting to restrict an unsupported service using the `gcloud` command-line tool or the Access Context Manager API will result in an error.

Cross-project access to data of supported services will be blocked by VPC Service Controls. Additionally, the restricted VIP can be used to block the ability of workloads to call unsupported services.

Terminology

In this topic, you have learned about several new concepts introduced by VPC Service Controls:

VPC Service Controls

Technology that enables you to define a security perimeter around resources of Google-managed services to control communication to and between those services

restricted VIP

The restricted VIP provides a private network route for products and APIs supported by VPC Service Controls in order to make data and resources used by those products inaccessible from the internet. `restricted.googleapis.com` resolves to `199.36.153.4/30`. This IP address range is not announced to the internet.

service perimeter

A security perimeter around Google-managed resources. Allows free communication within the perimeter but, by default, blocks all communication across the perimeter.

service perimeter bridge

A perimeter bridge allows projects in different security perimeters to communicate. Perimeter bridges are bidirectional, allowing projects from each service perimeter equal access within the scope of the bridge.

Access Context Manager

A context-aware request classification service that can map a request to an access level based on specified attributes of the client, such as the source IP address.

access level

A classification of requests over the internet based on a number of attributes, such as source IP range, client device, geolocation, and others. A service perimeter can be configured to grant access from the internet based on the access level associated with a request. Access levels are determined by the Access Context Manager service.

access policy

A Google Cloud resource object that defines service perimeters. There can be only one access policy object in an organization, and it is a child of the Organization resource.

What's next

- Learn about service perimeter configuration (https://cloud.google.com/vpc-service-controls/docs/service-perimeters).
- Review the known service limitations (https://cloud.google.com/vpc-service-controls/docs/supported-products#service-limitations).

Last updated December 4, 2019.