Overview of VPC Service Controls

VPC Service Controls improves your ability to mitigate the risk of data exfiltration from Google Cloud services such as Cloud Storage and BigQuery. You can use VPC Service Controls to create perimeters that protect the resources and data of services that you explicitly specify.

Note: For more information about products and services that VPC Service Controls supports, refer to the Supported products (/vpc-service-controls/docs/supported-products) page.

VPC Service Controls secures your Google Cloud services by defining the following controls:

- 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` (/storage/docs/gsutil/commands/cp) or `bq mk` (/bigquery/docs/reference/bq-cli-reference#bq_mk).
- Data exchange between clients and resources separated by perimeters is secured by using ingress and egress rules.
- Context-aware access to resources is based on client attributes, such as identity type (service account or user), identity, device data, and network origin (IP address or VPC network). The following are examples of context-aware access:
    - Clients outside the perimeter that are on Google Cloud or on-premises are within authorized VPC networks and use Private Google Access to access resources within a perimeter.
    - Internet access to resources within a perimeter is restricted to a range of IPv4 and IPv6 addresses.

VPC Service Controls provides an extra layer of security defense for Google Cloud services that is independent of Identity and Access Management (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. We recommend using both VPC Service Controls and 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:

- **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.
- **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. VPC Service Controls prevents service operations such as a `gsutil cp` command copying to a public Cloud Storage bucket or a `bq mk` command copying to a permanent external BigQuery table.

  Google Cloud also provides a restricted virtual IP that is used integrated with VPC Service Controls. The restricted VIP also allows requests to be made to services supported by VPC Service Controls without exposing those requests to the internet.
- **Public exposure of private data caused by misconfigured IAM policies**: VPC Service Controls provides an extra layer of security by denying access from unauthorized networks, even if the data is exposed by misconfigured IAM policies.
- **Monitoring access to services**: Use VPC Service Controls in dry run mode (/vpc-service-controls/docs/dry-run-mode) to monitor requests to protected services without preventing access and to understand traffic requests to your projects. You can also create honeypot perimeters to identify unexpected or malicious attempts to probe accessible services.

You can use an organization access policy and configure VPC Service Controls for your entire Google Cloud organization, or use scoped policies (/access-context-manager/docs/scoped-policies) and configure VPC Service Controls for a folder or project in the organization. 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 goal of VPC Service Controls is to control the movement of data, rather than metadata, across a service perimeter through supported services. VPC Service Controls also manages access to metadata, but there might be scenarios in which metadata can be copied and accessed without VPC Service Controls policy checks.

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

Capabilities

VPC Service Controls lets you to define security policies that prevent access to Google-managed services outside of a trusted perimeter, block access to data from untrusted locations, and mitigate data exfiltration risks. You can use VPC Service Controls for the following use cases:

- Isolate Google Cloud 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 Google Cloud resources (#internet) from the internet
- Protect data exchange across perimeters and organizations (/vpc-service-controls/docs/secure-data-exchange) by using ingress and egress rules
- Allow context-aware access to resources (/vpc-service-controls/docs/context-aware-access) based on client attributes by using ingress rules

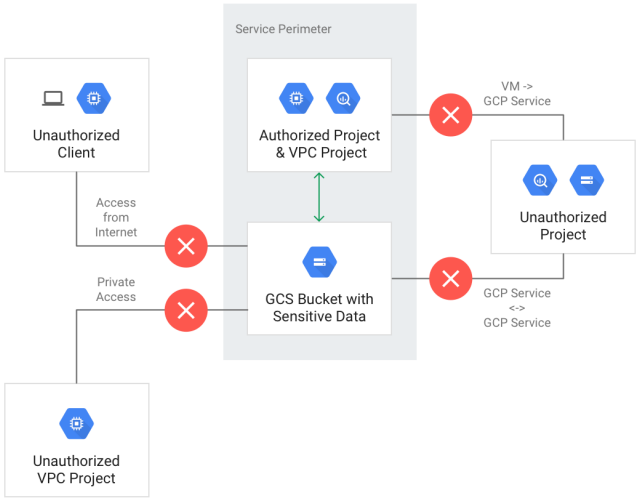
Isolate Google Cloud resources into service perimeters

A **service perimeter** creates a security boundary around Google Cloud resources. You can configure a perimeter to control communications from virtual machines (VMs) to a Google Cloud service (API), and between Google Cloud services. A perimeter allows free communication within the perimeter but, by default, blocks communication to Google Cloud services across the perimeter. The perimeter does not block access to any third-party API or services in the internet.

Here are some examples of VPC Service Controls creating a security boundary:

- A VM within a Virtual Private Cloud (VPC) network (/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, VPC Service Controls doesn't allow VMs within VPC networks that are outside the perimeter to access Cloud Storage buckets that are inside the perimeter.
- A copy operation between two Cloud Storage buckets succeeds if both buckets are in the same service perimeter, but if one of the buckets is outside the perimeter, the copy operation fails.
- VPC Service Controls doesn't allow a VM within a VPC network that is inside a service perimeter to access Cloud Storage buckets that are outside the perimeter.

The following diagram shows a service perimeter that allows communication between a VPC project and Cloud Storage bucket inside the perimeter but blocks all communication across the perimeter:

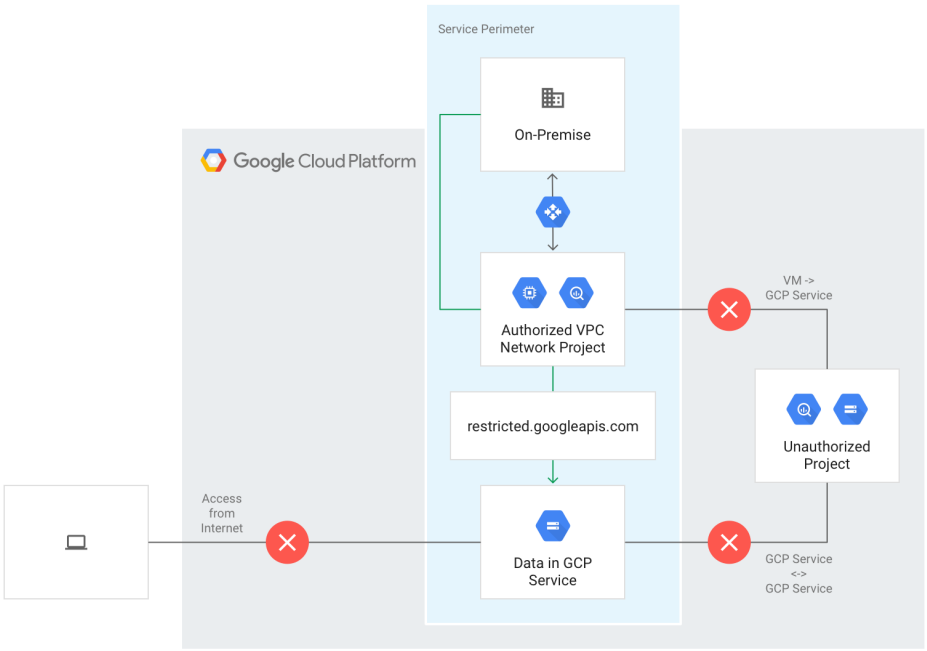


Extend perimeters to authorized VPN or Cloud Interconnect

You can configure private communication to Google Cloud resources from VPC networks that span hybrid environments with Private Google Access on-premises extensions (/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 necessary, you can continue to enable inspected and audited access to all Google APIs (for example, Gmail) over the internet.

The following diagram shows a service perimeter that extends to hybrid environments with Private Google Access:

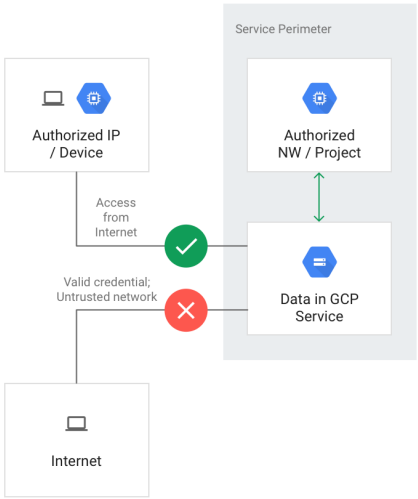


Control access to Google Cloud resources from the internet

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 various attributes, such as the source IP address. If requests made from the internet do not meet the criteria defined in the access level, the requests are denied.

To use the Google 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.

The following diagram shows a service perimeter that allows access from the internet to protected resources based on the configured access levels, such as IP address or device policy:



Unsupported Services

For more information on products and services that are supported by VPC Service Controls, refer to the Supported products (/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 (/vpc-service-controls/docs/use-access-levels) that includes the service account for that service and apply it to perimeters as needed (/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 service perimeter around resources of Google-managed services to control communication to and between those services

service perimeter

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

ingress rule

A rule that allows an API client that is outside the perimeter to access resources within a perimeter.

egress rule

A rule that allows 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.

service perimeter bridge

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

Note: Instead of using a perimeter bridge, we recommend using ingress and egress rules that provide more granular controls.

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 several 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. You can create access policies that are scoped to specific folders or projects alongside an access policy that can apply to the entire organization.

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.

What's next

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

Last updated 2022-09-28 UTC.