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

Service perimeter configuration

VPC Service Controls can be configured using the Google Cloud Console, the `gcloud` command-line tool (https://cloud.google.com/sdk/gcloud/reference/access-context-manager/), and the Access Context Manager APIs (https://cloud.google.com/access-context-manager/docs/apis).

Before you begin

- Read Overview of VPC Service Controls (https://cloud.google.com/vpc-service-controls/docs/overview)

Service perimeter configuration stages

To configure VPC Service Controls:

1. If you want to use the `gcloud` command-line tool (https://cloud.google.com/sdk/gcloud/reference/access-context-manager/) or the Access Context Manager APIs (https://cloud.google.com/access-context-manager/docs/apis) to create your service perimeters, create an access policy (https://cloud.google.com/access-context-manager/docs/create-access-policy).

★ **Note:** You do not have to manually create an access policy if you are using the Cloud Console to manage VPC Service Controls. An access policy will be created for your Organization automatically.

2. Secure GCP resources with service perimeters.

3. Set up private connectivity from a VPC network (optional).
4. Grant access from outside a service perimeter using access levels (optional).

Create an access policy

An access policy collects the service perimeters and access levels you create for your Organization. An Organization can only have one access policy.

When service perimeters are created and managed using the **VPC Service Controls** page of the Cloud Console, you do not need to create an access policy.

However, when using the `gcloud` command-line tool (https://cloud.google.com/sdk/gcloud/reference/access-context-manager/) or the Access Context Manager APIs (https://cloud.google.com/access-context-manager/docs/apis) to create and configure your service perimeters, you must first create an access policy (https://cloud.google.com/access-context-manager/docs/create-access-policy).

To learn more about Access Context Manager and access policies, read the overview of Access Context Manager (https://cloud.google.com/access-context-manager/docs/overview).

Secure GCP resources with service perimeters

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 (https://cloud.google.com/vpc-service-controls/docs/create-service-perimeters).

Note: If you're using Shared VPC (https://cloud.google.com/vpc/docs/shared-vpc), you must include the host project (https://cloud.google.com/vpc-service-controls/docs/troubleshooting#shared_vpc) in a service perimeter along with any projects that belong to the Shared VPC.

To learn more about how service perimeters work and what services VPC Service Controls can be used to secure, read the Overview of VPC Service Controls (https://cloud.google.com/vpc-service-controls/docs/overview).

Some services have limitations with how they can be used with VPC Service Controls (https://cloud.google.com/vpc-service-controls/docs/supported-products#service-limitations). If you encounter issues with your projects after setting up your service perimeters, read Troubleshooting (https://cloud.google.com/vpc-service-controls/docs/troubleshooting).

Set up private connectivity from a VPC network

To provide additional security for VPC networks that are protected by a service perimeter, we recommend using Private Google Access. This includes private connectivity from on-premises networks (https://cloud.google.com/vpc-service-controls/docs/private-connectivity).

To learn about configuring private connectivity, read Setting up private connectivity to Google APIs and services (https://cloud.google.com/vpc-service-controls/docs/set-up-private-connectivity).

Restricting access to Google Cloud resources to only private access from VPC networks means that access using interfaces such as the Cloud Console and the Stackdriver console will be denied. You can continue to use the `gcloud` command-line tool or API clients from VPC networks that share a service perimeter or perimeter bridge with the restricted resources.

Grant access from outside a service perimeter using access levels

Access levels can be used to allow requests from outside a service perimeter to resources protected by that perimeter.

Note: While access levels allow external requests, they do not permit protected projects to access resources outside the perimeter.

Using access levels, you can specify public IPv4 and IPv6 CIDR blocks, and individual user and service accounts that you want to permit to access resources protected by VPC Service Controls.

If you are restricting resources using private connectivity from VPC networks, you can re-enable using the Cloud Console to access protected services by adding a CIDR block to an access level that includes the public IP address of the host where the Cloud Console is being used. If you want to re-enable the Cloud Console for a specific user regardless of IP address, add that user account as a member to the access level.

Note: The Stackdriver console does not support using access levels. The Monitoring API should not be restricted if you want to use the Stackdriver console.

To learn about using access levels, read Creating an access level (https://cloud.google.com/access-context-manager/docs/create-access-level).

Sharing data across service perimeters

A project can only be included in one service perimeter. If you want to allow communication between two perimeters, create a service perimeter bridge (https://cloud.google.com/vpc-service-controls/docs/share-across-perimeters).

Perimeter bridges can be used to enable communication between projects in different service perimeters. A project can belong to more than one perimeter bridge.

To learn more about perimeter bridges, read Sharing across perimeters with bridges (https://cloud.google.com/vpc-service-controls/docs/share-across-perimeters).

Last updated December 4, 2019.