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

Allowing access to protected resources from outside a perimeter

You can use **access levels** to grant controlled access to protected Google Cloud resources in service perimeters from outside a perimeter.

An access level defines a set of attributes that must be met before a request is honored. Access levels can consider various criteria, such as IP address and user identity.

Note: Some attributes, such as device policy attributes, are not currently supported by VPC Service Controls.

For a detailed overview of access levels, read the Access Context Manager overview (https://cloud.google.com/access-context-manager/docs/overview).

Limitations of using access levels with VPC Service Controls

When using access levels with VPC Service Controls, certain limitations apply:

- Access levels only allow requests from *outside* a perimeter for the resources of a protected service *inside* a perimeter.

  You cannot use access levels to allow requests from a protected service *inside* a perimeter for resources *outside* the perimeter. If you need a protected service to make requests for resources outside the perimeter, try using perimeter bridges (https://cloud.google.com/vpc-service-controls/docs/share-across-perimeters).

- Requests for a protected resource in a perimeter that originate from *another* perimeter will always be denied, even if an access level would normally allow the external request. For

more information, read about <u>requests between perimeters</u>
 (https://cloud.google.com/vpc-service-controls/docs/troubleshooting#requests-between-perimeters)
.

Using access levels

Access levels are created and managed using Access Context Manager.

Creating an access level

To create an access level, read about <u>creating an access level</u>
 (https://cloud.google.com/access-context-manager/docs/create-access-level) in the Access Context
Manager documentation.

The following examples explain how to create an access level using different conditions:

- <u>IP address</u>
   (https://cloud.google.com/access-context-manager/docs/create-access-level#corporate-network-
  example)

- <u>User and service accounts</u>
   (https://cloud.google.com/access-context-manager/docs/create-access-level#members-example)
  (members)

Adding access levels to service perimeters

You can add access levels to a service perimeter when creating the perimeter, or to an existing
perimeter:

- Read about <u>adding access levels when you create a perimeter</u>
     (https://cloud.google.com/vpc-service-controls/docs/create-service-perimeters#external-access)

- Read about <u>adding access levels to an existing perimeter</u>
     (https://cloud.google.com/vpc-service-controls/docs/manage-service-perimeters#add-access-level)

Managing access levels

To manage your access levels, read about managing access levels
(https://cloud.google.com/access-context-manager/docs/managing-access-levels). This documentation
explains how to list, modify, and delete existing access levels.