Logging and Monitoring

**Logging**

* VPC Service Controls logs all accesses that are denied because of security policy violations to Cloud Logging by default.
* The audit log records are securely stored in Google infrastructure and available for future analysis.

Ref: <https://cloud.google.com/vpc-service-controls/docs/audit-logging>

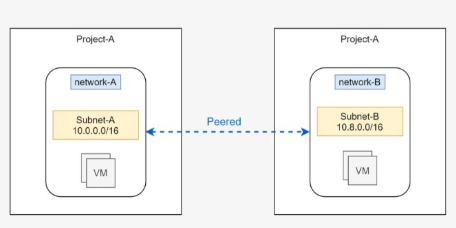
**Monitoring**

* Any and all violations are logged to cloud logging
* Log based alerts can be setup to get notified of
  + Violations
  + Changes to vpc perimeter config including creation of new perimeter, modification/deletion of existing perimeters

Ref: <https://cloud.google.com/logging/docs/alerting/log-based-alerts>

VPC Peering

If the perimeter is set up to protect vpc service, vpc peering is only allowed within the perimeter by default. That means if you have 2 vpcs in the same project, you can establish vpc peering between those 2 vpcs.



If they are in 2 different project and vpc peering should be allowed by creating an exception using egress and ingress policies

IAM

When you restrict IAM with a perimeter, only actions that use the IAM API are restricted. These actions include

* managing custom IAM roles
* managing workload identity pools
* managing service accounts and keys

Allow creation of custom iam roles, service accounts and keys can be restricted for an ip or ip range(cidr) or a user or a service account. Except the allowed ips or user or service account others can't perform any of the above actions.

This can be achieved using access level in access context manager