VPC firewall rules to network firewall policy migration

Background
Firewall enforcement order
IAM-governed tags overview
- Benefits of network firewall policies with IAM-governed tags

IAM requirements and considerations
- Network firewall policy permissions and roles
- IAM-governed tags roles

IAM-governed tags bindings to instances
Global network firewall policies migration overview
- Migration from VPC firewall rules to network firewall policy
- Migration from VPC firewall rules containing network tags to a network firewall policy
- Migration from VPC firewall rules containing service accounts to a network firewall policy
- Migration from VPC firewall rules containing service accounts and network tags to a network firewall policy

FAQ

Background

Cloud Firewall is a fully-distributed, cloud-native, firewall service that delivers granular control without network re-architecting. Cloud Firewall is stateful and supports micro-segmentation by expressing firewall rules in terms of target VM instances.

As large enterprise customers adopt Google Cloud as their cloud platform and migrate services and workloads into the cloud, VPC firewall rules present challenges and limitations since they use network tags, which do not currently have strict IAM controls.

To address these limitations and challenges customers face, we have introduced network firewall policies (global and regional) with IAM-governed tags which complements our other firewall offerings.

In the global and regional network firewall policies, we offer rules defined on a per VPC-network basis, either for all regions of the network (global) or a single region (regional). Granular controls enforced at the virtual machine (VM) level using the new Identity and Access Management (IAM)-governed Tags deliver intra-subnet micro-segmentation with pervasive policy coverage that automatically applies to workloads wherever they are deployed, independent of the network architecture.

The combination of the new policy structures and IAM-governed Tags delivers a consistent firewall experience across the Google Cloud resource hierarchy. This simplifies operations, while also achieving more granular control to enable a more least-privilege, self-service DevOps environment for each group or app.

In addition, all future feature enhancements for Cloud Firewall will only be supported through the firewall policies. No new functionality will be added to the VPC firewall rules.

This document provides a guide for customers who want to migrate their firewall rules configuration from our traditional VPC firewall rules to our new network firewall policies. This document covers how to migrate and how to use the migration tool to effectively migrate firewall rules from VPC firewall rules to **global network firewall policies**.

Firewall enforcement order

With the introduction of network firewall policies, Google Cloud Firewall rules consists of the following components:

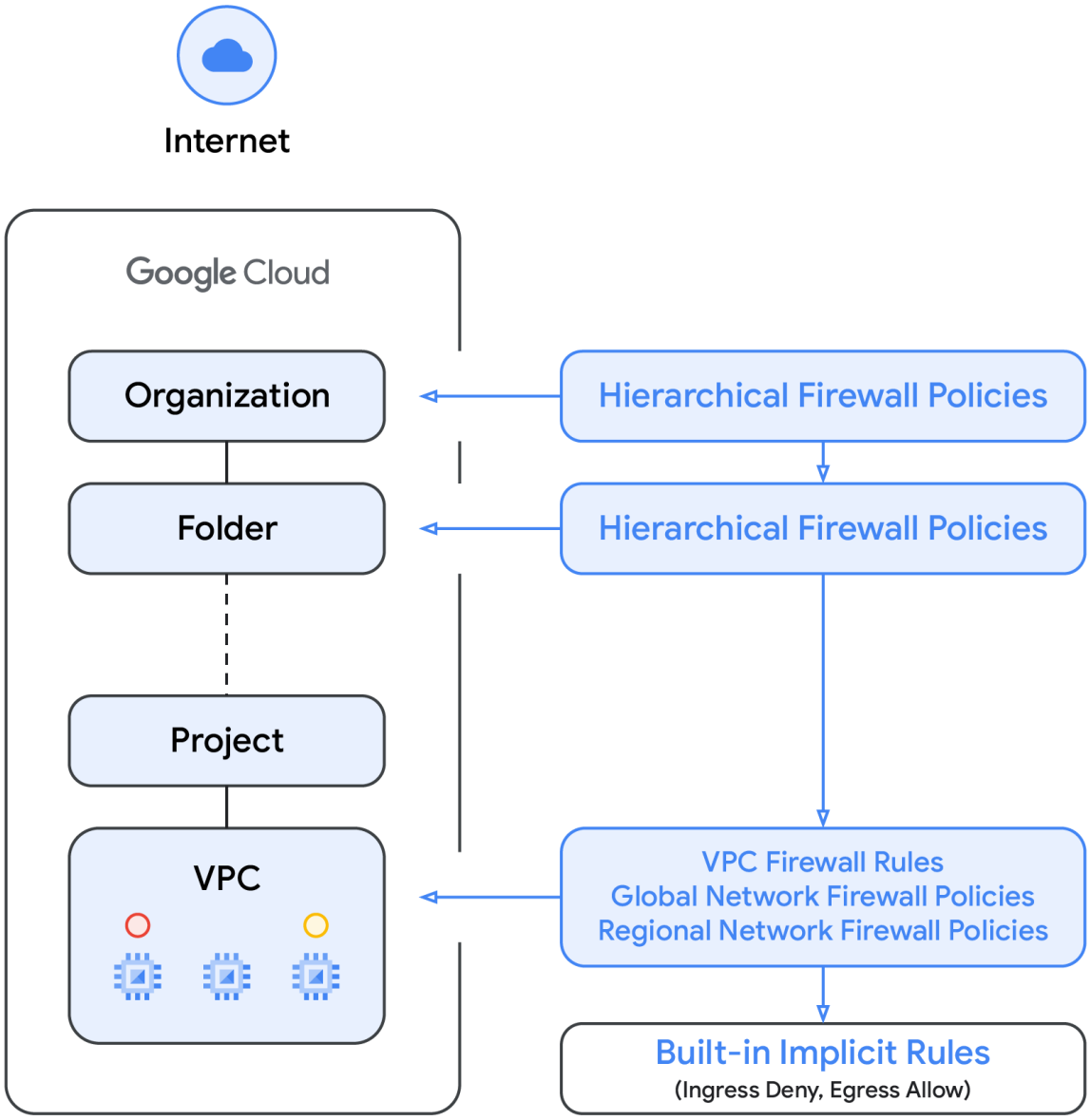
1. Hierarchical firewall policy
2. VPC firewall rules
3. Network firewall policy (global and regional)

Hierarchical firewall policies are supported at the organization and folder nodes within the resource hierarchy, whereas VPC firewall rules and network firewall policies get applied at the VPC level. A big difference between VPC firewall rules and network firewall policies is that VPC firewall rules can be applied only to a single VPC, whereas network firewall policies can get attached to a single VPC or group of VPCs, in addition to other benefits like batch update.

Finally, we also have the implied firewall rules that come with every VPC network:

- An egress rule whose action is allow, destination is 0.0.0.0/0 (and the equivalent for IPv6)
- An ingress rule whose action is deny, source is 0.0.0.0/0 (and the equivalent for IPv6)

By default, the enforcement sequence is shown in the following diagram:



Please note that the enforcement order between the VPC firewall rules and the global network firewall policy can be swapped. Customers can specify the enforcement order at any time with the ffollowing gcloud command:

```
gcloud compute networks update VPC_NETWORK \
    --network-firewall-policy-enforcement-order BEFORE_CLASSIC_FIREWALL
```

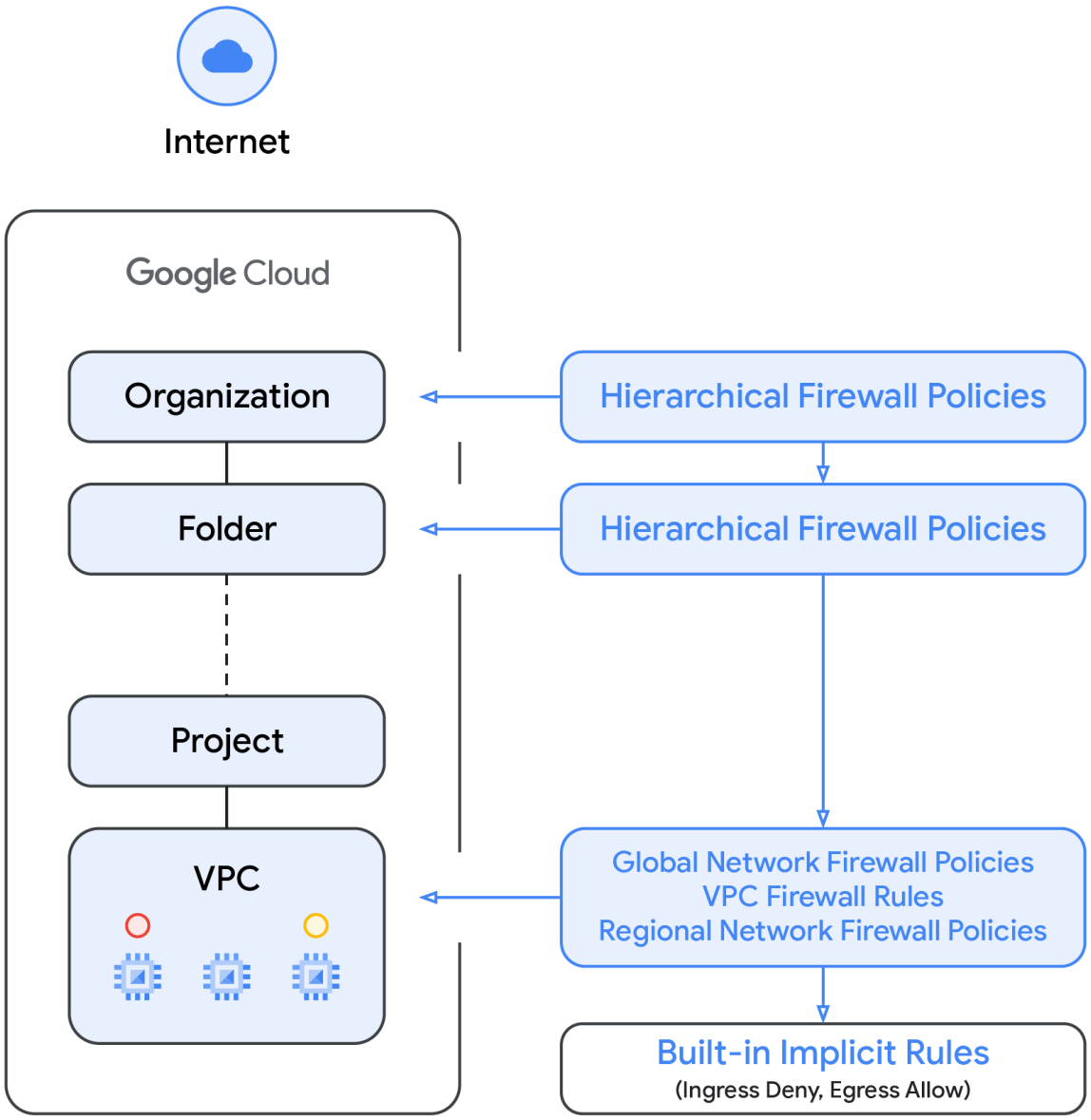
The new behavior can be verified by running the command below:

```
gcloud compute networks describe VPC_NETWORK
```

Expected output:

```
autoCreateSubnetworks: false
creationTimestamp: '2022-09-23T12:21:52.316-07:00'
firewallPolicy:
https://www.googleapis.com/compute/v1/projects/[PROJECT_ID]/global/firewallPolicies/[FI
REWALL_POLICY]
id: '6749205358365096383'
kind: compute#network
name: [VPC_NETWORK]
networkFirewallPolicyEnforcementOrder: BEFORE_CLASSIC_FIREWALL
...
```

If customers want to reverse the default sequence and evaluate the network firewall policy before the VPC firewall rules, the previous command will change the order, so the new effective sequence will be the following:



Once customers have migrated their VPC firewall rules to network firewall policies it is recommended to swap the evaluation order so network firewall policies take precedence over VPC firewall rules.

In case you want to check if the Global Network Firewall Policy or the VPC Firewall rules take precedence, you can use the following command to get the effective firewalls on compute instances:

```
gcloud compute instances network-interfaces get-effective-firewalls VM-NAME --zone=ZONE
```

While analyzing the output, please note the type network-firewall-policy means global network firewall policies whereas the type network-firewall means VPC firewall rules. Therefore, if the *type: network-firewall policy* is shown before *type: network-firewall* that means that global network firewall policies will be evaluated first.

Please note that automatically created VPC firewall rules by Google services such as GKE cluster creation will remain in VPC firewall rules until those teams migrate off VPC firewall rules in favor of the new network firewall policies.

For additional information and the latest details please refer to this link.

IAM-governed tags overview

The new IAM-governed Tags (also known as Tags) in network firewall policy rules are key-value pair resources defined at the organization level of the Google Cloud resource hierarchy. Each tag contains IAM access control that specifies granular permissions for that specific tag. IAM permissions, for instance, allow one to specify which principal can assign values to tags and which principal can attach tags to resources. Once an IAM-governed tag has been applied to a resource, rules in network firewall policies can use it to allow and deny traffic.

IAM-governed tags adhere to the GCP inheritance resource model, meaning tags and their values are passed down across the hierarchy from their parents. As a result, tags may be created in one place and then used by other folders and projects throughout the resource hierarchy. Visit this page for further details on tags and access restriction.

IAM-governed tags should not be confused with network tags, the latter are strings that can be added to GCE VMs; they are associated with the VM and vanish when the VM is decommissioned. VPC firewall rules may include network tags, but since they are not regarded as cloud resources, they are not subject to IAM access control. Another significant distinction is that IAM-governed tags are allocated to a specific network interface of a VM, whereas network tags are assigned at the VM level, meaning the network tag will be assigned to all the network interfaces in a VM. The table below provides more information on how IAM-governed tags and network tags differ from one another.

	IAM-governed tags for Firewall	Network tags
Defined	At the organization level	A text attribute of a VM
Parent	Organization	N/A
Access Control	Use the traditional IAM permissions and roles	No IAM control
Attachment	Tags attached to a VM's network interface in the target network for that Tag	VM (maps to primary IP ranges of the VM of all network interfaces of the VM)
Management	Centralized Tag management, support resource hierarchy	At the resource level (VM)
IP Range Coverage	Covers all IP ranges assigned to a VM interface, primary and secondary	Covers only the primary IP range for a VM interface.

For more details please refer to this link.

Benefits of network firewall policies with IAM-governed tags

As shown in the table above, IAM-governed tags provide centralized management and separation of duties between tags admin and network/compute admin. Although the compute service account was used by VPC firewall rules to identify the VM in firewall rules, this posed several constraints. For instance, a VM could only have one service account assigned to it, and that service account would be applicable to all of the VM's network interfaces. Using IAM-governed tags to create network policies gives the entire organization access to a wide range of firewall configuration choices. For instance, different IAM-Governed tags can be assigned to different network interfaces on a VM with multiple network interfaces in different VPCs, enabling users to apply different firewall rules on this VM in each VPC network.

Leveraging IAM-Governed Tags allow network administrators to build granular network policies with very little dependencies on the underlying compute identity and to modify these rules regardless of any service account changes, making the rules easy to read and manage.

IAM requirements and considerations

Network firewall policy permissions and roles

Similar to managing permissions for VPC firewalls, IAM roles need to be assigned to users and groups to manage and apply rules in network firewall policies. It is recommended to assign the network firewall applicable IAM roles to a Google Cloud Group rather than individuals, then add and remove users from that group. It is recommended to create a group for each persona in your organization, assign permissions based on the business requirements of each persona and continuously monitor and adjust these permissions. The IAM roles used by network firewall policies are listed here. These roles are used to grant permissions to create firewall policy, associate a policy to a network, modify and delete policies, view rules for a VPC and VM. You can use the Google managed roles for each action or you can create your own custom roles with fine grained permissions and then assign the custom roles to different groups.

IAM-governed tags roles

IAM-Governed tags let you define sources and targets in global and regional network firewall policies. Note that these tags are different from network tags as described in the previous section *IAM-governed tags overview*. IAM-governed tags are created at the organization level and they are scoped to a single VPC within a project. Unlike network tags, these tags have IAM access control which allows you to control who can define the tags and who can use the tags and associate them to VMs.

If you are using IAM-Governed tags as source and target in your firewall rules, then the following Tagging roles and permissions need to be defined in your organization. Add these roles or permissions to the group(s) that manages tags based on the group's business needs. Note that some of these permissions are already associated with existing roles such as Compute Admin who has the permissions to assign IAM-governed tags to VMs.

Task	Role	Permissions
Create and manage tags	Tag Administrator (tagAdmin)	• resourcemanager.tagKeys.create • resourcemanager.tagKeys.update • resourcemanager.tagKeys.delete • resourcemanager.tagKeys.list • resourcemanager.tagKeys.get • resourcemanager.tagKeys.getIamPolicy • resourcemanager.tagKeys.setIamPolicy • resourcemanager.tagValues.create • resourcemanager.tagValues.update • resourcemanager.tagValues.delete • resourcemanager.tagValues.list • resourcemanager.tagValues.get • resourcemanager.tagValues.getIamPolicy • resourcemanager.tagValues.setIamPolicy
Use a tag	Tag User role (tagUser)	• resourcemanager.tagValueBindings.create • resourcemanager.tagValueBindings.delete
Manage a tag on a VM	Multiple roles includes the permission required for this task, including Tag User and Compute Instance Admin	• compute.instances.createTagBinding • compute.instances.deleteTagBinding

Follow the principle of least-privilege and separation of duties when assigning roles and permission to principals. In many cases the group who define organizational wide tags do not need to have permissions to assign tags to VMs. To achieve tight access control it is recommended to leverage IAM Role Recommender which suggests, remove and replace roles that provide excess permissions to principals.

To add the tagAdmin role to a principal run the command below:

```
gcloud organizations add-iam-policy-binding ORGANIZATION_ID \
   --member=user:EMAIL_ADDRESS \
   --role=roles/resourcemanager.tagAdmin
```

For example, if the Google Group email address is tag_admin@my-org.com and organization id is 12345, the

command will be:

```
gcloud organizations add-iam-policy-binding 12345
    --member=user:tag_admin@my-org.com --role=roles/resourcemanager.tagAdmin
```

Use the command below to verify that the permissions were added:

```
gcloud organizations get-iam-policy ORGANIZATION_ID --flatten=bindings
--filter=bindings.role:roles/resourcemanager.tagAdmin
```

As **Tag Administrator** follow these steps to create and define new tags for your organization. Leverage the same naming convention for tags as you use for other resources in your organization. For example, if your naming convention includes the format <Business_Unit.Region.Group.Project> then Tags should also follow the same or similar naming conventions.

```
gcloud resource-manager tags keys create TAG_NAME \
   --parent organizations/ORGANIZATION_ID \
   --purpose GCE_FIREWALL \
   --purpose-data network=PROJECT_ID/VPC_NAME
```

For example:

```
gcloud resource-manager tags keys create TAG_KEY \
   --parent organizations/ORGANIZATION_ID --purpose GCE_FIREWALL \
   --purpose-data network=PROJECT_ID/VPC_NAME

Waiting for TagKey [TAG_KEY] to be created...done.
createTime: '2022-09-23T20:49:01.162228Z'
etag: PwvmFuHO4wK1y6c5Ut2n5w==
name: tagKeys/[TAG_KEY_ID]
namespacedName: [ORGANIZATION_ID]/[TAG_KEY]
parent: organizations/[ORGANIZATION_ID]
purpose: GCE_FIREWALL
purposeData:
  network:
https://www.googleapis.com/compute/v1/projects/[PROJECT_ID]/global/networks/[VPC_NAME]
shortName: [TAG_KEY]
updateTime: '2022-09-23T20:49:03.873776Z'
```

Then run the following command to list the Tag Keys:

```
gcloud resource-manager tags keys list --parent organizations/[ORGANIZATION_ID]
```

After tags have been created, as IAM Admin, assign the tagUser role to the principal that uses the tags and binds the tags to VMs. To add the tagUser role to a principal run the command below.

```
gcloud resource-manager tags values add-iam-policy-binding
ORGANIZATION_ID/TAG_KEY/TAG_VALUE \
--member=user:EMAIL_ADDRESS \
```

```
--role=roles/resourcemanager.tagUser
```

For example, if the user's email address is jhon@my-org.com, organization id is 12345 and the Tag is "App1=value1", the command will be:

```
gcloud resource-manager tags values add-iam-policy-binding
           12345/App1/value1
           --member 'user:jhon@my-org.com' --role 'roles/resourcemanager.tagUser'
```

To view Tag Values run the following command:

```
gcloud resource-manager tags values list --parent=[ORGANIZATION ID]/[TAG_KEY]
```

For example:

```
gcloud resource-manager tags values list --parent=[ORGANIZATION ID]/[TAG_KEY]

NAME                     SHORT_NAME  DESCRIPTION
tagValues/809928805379   App1        Tag for App 1
```

Then run the following command to list the IAM bindings:

```
gcloud resource-manager tags values get-iam-policy <RESOURCE NAME>
```

For example:

```
gcloud resource-manager tags values get-iam-policy tagValues/809928805379


bindings:
- members:
  - user:******a@google.com
  role: roles/resourcemanager.tagUser
etag: BwXpNrpv85A=
version: 1
```

Review the IAM roles required to create, associate, modify and view firewall rules for VM and VPC networks from this page.

IAM-governed tags bindings to instances

Ensure that Tags are attached to the workloads before the migration. To do that you need the right permissions as described above. To bind an IAM-governed tags to a VM, the principal who assigns the tag needs the compute.instances.createTagBinding and compute.instances.deleteTagBinding permission on the IAM-governed tag, these permissions are included in the roles/resourcemanager.tagUser role.

Note that if the principal who needs to assign the IAM-governed tag has the Compute.InstanceAdmin or ComputeAdmin role then the tagUser role is already included in these roles.

To bind a tag and list effective tags on a resource, run the command below:

```
gcloud resource-manager tags bindings create \
   --tag-value=MY_TAG \
   --parent=RESOURCE_ID
   --location=LOCATION
```

For example, if the tag value is TAG_KEY/TAG_VALUE and the instance to assign the tage is MY_INSTANCE, then command to bind a tag to an instance will be:

```
gcloud resource-manager tags bindings create \
  --location ZONE_ID \
  --tag-value ORGANIZATION_ID/[TAG_KEY]/[TAG_VALUE] \
  --parent \
//compute.googleapis.com/projects/PROJECT_ID/zones/$zone/instances/MY_INSTANCE
```

Use the command below to verify that the permissions were added:

```
gcloud resource-manager tags bindings list --location ZONE_ID --parent
//compute.googleapis.com/projects/PROJECT_ID/zones/ZONE_ID/instances/MY_INSTANCE
--effective
```

Expected output:

```
namespacedTagKey: [ORGANIZATION_ID]/[TAG_KEY]
namespacedTagValue: [ORGANIZATION_ID]/[TAG_KEY]/[TAG_VALUE]
tagKey: tagKeys/[TAG_KEY_ID]
tagValue: tagValues/[TAG_VALUE_ID]
```

For more details on how to bind Tags to instances please refer to this link.

Bulk binding of IAM-governed tags

If you have permission at each and instance, you can automate the tag binding process using `gcloud beta compute firewall-rules migrate`.

Mapping file

First, you should create the required Tags that will serve as replacement to the network tags. How to create secure tags is described in IAM-governed tags roles.

You can create a mapping file manually or you can use the export-tag-mapping option in the migration tool to prepare such a file (Migration from VPC firewall rules containing network tags to a network firewall policy). The file can also contain mapping for service accounts (see Migration from VPC firewall rules containing service accounts to a network firewall policy).

Once a file is created and the mapping between network tags and secure tags values is done the file should look like this:

```
{“network-tag-1”: “tagValues/xxxxx”, “network-tag-2”: “tagValues/zzzzz”
     “sa:seervice2@account.com”: “tagValues/yyyyy”}
```

Binding secure tags to VM instances

The following command binds secure tags to VM instances based on the providing mapping:

```
gcloud beta compute firewall-rules migrate --source-network=SOURCE_VPC_NETWORK
--bind-tags-to-instances --tag-mapping-file=//tmp/mapping.json
```

It finds all VM instances in the SOURCE_VPC_NETWORK network and binds secure tags to them based on the mapping defined in //tmp/mapping.json.

Global network firewall policies migration overview

Because VPC firewall rules apply to all regions of the VPC network, this guide shows you how to migrate VPC firewall rules to rules in a global network firewall policy.

Let’s discuss now how to effectively migrate from VPC firewall rules to network firewall policies. At a high level, what the migration tool does is to create a global network firewall policy and copy the existing VPC firewall rules into the global network firewall policy. Please note that the migration tool does not delete existing rules. Users can then attach the network firewall policy to a VPC and once it works as desired, VPC firewall rules can be removed. Ideally, the best way to verify it's working as intended is to enable logging on both VPC firewall rules and network firewall policy. Once only network firewall policy has hit counts and VPC firewall rules are shadowed, this provides a good indicator that the migration tool is working as intended.

If two or more firewall rules have the same priority, the migration tool will automatically update it to avoid collisions. Please review the priorities auto generated by the migration tool to make sure they are acceptable. This new assigned priority is created to ensure the relative sequence of the original rules are respected -- meaning if, for example, there are a few rules (4) with the same priority (1000), followed by a rule with priority 2000, the migration tool will set up a unique priority number allocation to respect the prior sequence (1000, 1001, 1002, 1003, 1004), and make sure the new priorities for these 4 rules are higher than that of all rules which as a priority lower than 1000.

To start the migration process you will need to run a gcloud command. There are a few arguments you need to enter; two of them are mandatory which are the source VPC network (SOURCE_VPC_NETWORK) and the target network firewall policy (TARGET_NETWORK_FIREWALL_POLICY).

Please note the Network Firewall Policy cannot exist, since the migration tool will create it.

```
gcloud compute firewall-rules migrate --source-network=SOURCE_VPC_NETWORK
     –target-firewall-policy=TARGET_NETWORK_FIREWALL_POLICY [OTHER_FLAGS]
```

Additionally, logging will be kept as is for any migration, meaning that if a VPC firewall rule has logging turned on, the migration tool will leave it on and in case it is off, it will keep it off.

Migration from VPC firewall rules to network firewall policy

If VPC firewall rules do not contain network tags or service accounts, it will be a straightforward migration process requiring a single command.

If that is the case you can go ahead and execute the following command indicating your source VPC Network and the target network firewall policy:

```
gcloud beta compute firewall-rules migrate --source-network=SOURCE_VPC_NETWORK
–target-firewall-policy=TARGET_NETWORK_FIREWALL_POLICY
```

This command will migrate all VPC firewall rules to a new network firewall policy, and once it is created, we recommend users first review that the migration was executed accurately before attaching it to a VPC network. Please note this command does not apply to firewall rules auto-generated by GKE.

Migration from VPC firewall rules containing network tags to a network firewall policy

In case that VPC firewall rules do contain network tags, there are a couple steps required. First, users should create the required Tags that will serve as replacement to those network tags, meaning that all network tags will require a Tags creation for the required mapping if the exact configuration needs to be maintained. For that, please review the prior section that covers IAM in detail on how to create these Tags and the required IAM credentials. Additionally, IAM binding can happen only after Tags have been created. For example, if there is a VPC firewall rule containing a network tag “sql-server”, a user could create a Tag key and value pair such as “vm-function:sql-server”.

The second step here is to leverage a json file to map the existing network tags to the new Tags. In case that the required mapping file is not provided, the migration will fail. Additionally, ensure that thoseTags are properly attached to your workloads.

Next, you can create a json file where you specify the mapping or have the migration tool look for existing network tags being used on your VPC Firewall rules to be associated with secure tags. You have the capability to export mappings:

```
gcloud beta compute firewall-rules migrate --source-network=SOURCE_VPC_NETWORK
     --export-tag-mapping --tag-mapping-file=//tmp/mapping.json
```

This command will export all network tags within your VPC Firewall rules and export them in a json file:

```
Looking for VPC Firewalls and Network Firewall Policies associated with VPC Network
     'SOURCE_VPC_NETWORK'.
Found x Network Firewall Policies associated with the VPC Network 'SOURCE_VPC_NETWORK'.
Found xx VPC Firewalls associated with the VPC Network 'SOURCE_VPC_NETWORK'.
Legacy tags were exported to '//tmp/mapping.json'
```

Next, you can edit the file */tmp/mapping.json* to create your required mapping. Make sure to use tagValues/integer syntax or else will fail:

Example:

```
{“network-tag-1”: null, “network-tag-2”: null, “network-tag-3”: null}
```

As you can see the three objects are network tags.

Next steps is to edit the file and ensure there is a correct mapping between network tags and tags and service accounts and tags. The edited file should look like this:

```
{“network-tag-1”: “tagValues/xxxxx”, “sql-server”: “tagValues/yyyyy”, “network-tag-3”:
     “tagValues/zzzzz”}
```

Last step here is to start the migration process attaching the json mapping file and once executed, this should complete the migration:

```
gcloud beta compute firewall-rules migrate
     --target-firewall-policy=TARGET_NETWORK_FIREWALL_POLICY
     --source-network=SOURCE_VPC_NETWORK --tag-mapping-file=//tmp/mapping.json
```

After this is completed, please review the newly created network firewall policy to ensure it is accurate and meets your expectations. Once this is done, you can attach the network firewall policy to the VPC and remove the VPC firewall rules. Please note you can also swap the rule evaluation order so that network firewall policies take precedence over VPC firewall rules.

Migration from VPC firewall rules containing service accounts to a network firewall policy

In the case that VPC firewall rules do contain service accounts, there are a couple of steps required. First, users should precreate the required Tags equivalent to those service accounts, meaning that all service accounts will require a Tags creation for a one to one mapping if the exact configuration needs to be maintained. For that, please review the prior section that covers IAM in detail on how to create these tags and the required IAM credentials. Additionally, IAM binding can happen only after tags have been created.

The second step here is to leverage a json file to map the existing service accounts to Tags. In case that the required mapping file is not provided, the migration will fail. Additionally, ensure that those Tags are properly attached to your workloads.

Next, you can create a json file where you specify the mapping or have the migration tool look for existing network tags being used on your VPC firewall rules to be associated with tags. You have the capability to export mappings:

```
gcloud beta compute firewall-rules migrate --source-network=SOURCE_VPC_NETWORK
     --export-tag-mapping --tag-mapping-file=//tmp/mapping.json
```

This command will export all network tags within your VPC firewall rules and export them in a json file:

```
Looking for VPC Firewalls and Network Firewall Policies associated with VPC Network
     'SOURCE_VPC_NETWORK'.
Found x Network Firewall Policies associated with the VPC Network 'SOURCE_VPC_NETWORK'.
Found xx VPC Firewalls associated with the VPC Network 'SOURCE_VPC_NETWORK'.
Legacy tags were exported to '//tmp/mapping.json'
```

Next, you can edit the file *//tmp/mapping.json* to create your required mapping. Make sure to use tagValues/integer syntax or else will fail:

Example:

```
{"sa:seervice1@account.com”: null, "sa:seervice2@account.com”: null,
     "sa:seervice3@account.com”: null}
```

As you can see the three objects are service accounts indicated by “*sa:*”.

Next steps is to edit the file and ensure there is a correct mapping between network tags and IAM-governed tags and service accounts and IAM-governed tags. The edited file should look like this:

```
{“sa:seervice1@account.com”: “tagValues/xxxxx”, “sa:seervice2@account.com”:
     “tagValues/yyyyy”, "sa:seervice3@account.com”: “tagValues/zzzzz”}
```

Last step here is to start the migration process attaching the json mapping file and once executed, this should complete the migration:

```
gcloud beta compute firewall-rules migrate
     --target-firewall-policy=TARGET_NETWORK_FIREWALL_POLICY
     --source-network=SOURCE_VPC_NETWORK --tag-mapping-file=//tmp/mapping.json
```

After this is completed, please review the newly created network firewall policy to ensure it is accurate and meets your expectations. Once this is done, you can attach the network firewall policy to the VPC and remove the VPC firewall rules. Please note you can also swap the rule evaluation order so that network firewall policies take precedence over VPC firewall rules.

Migration from VPC firewall rules containing service accounts and network tags to a network firewall policy

In case that VPC firewall rules contain a combination of service accounts and network tags, the same steps will apply here. First, users should create the required IAM-governed tags equivalent for their service accounts and network tags. All service accounts and network tags will require a tag creation, or a 1:1 mapping if the exact configuration needs to be maintained. For that, please review the prior section that covers IAM in detail on how to create these tags and the required IAM credentials. Additionally, IAM binding can happen only after tags have been created.

The second step here is to leverage a json file to map the existing service accounts and network tags to secure tags. In case that the required mapping file is not provided, the migration will fail. Additionally, ensure that those secure tags are attached to your workloads.

Next, you can create a json file where you specify the mapping or have the migration tool look for existing network tags being used on your VPC firewall rules to be associated with tags. You have the capability to export mappings:

```
gcloud beta compute firewall-rules migrate --source-network=SOURCE_VPC_NETWORK
     --export-tag-mapping --tag-mapping-file=//tmp/mapping.json
```

This command will export all network tags within your VPC Firewall rules and export them in a json file:

```
Looking for VPC Firewalls and Network Firewall Policies associated with VPC Network
     'SOURCE_VPC_NETWORK'.
Found x Network Firewall Policies associated with the VPC Network 'SOURCE_VPC_NETWORK'.
Found xx VPC Firewalls associated with the VPC Network 'SOURCE_VPC_NETWORK'.
Legacy tags were exported to '//tmp/mapping.json'
```

Next, you can edit the file *//tmp/mapping.json* to create your required mapping. Make sure to use tagValues/integer syntax or else will fail:

Example:

```
{“network-tag-1”: null, “network-tag-2”: null, "sa:seervice@account.com”: null}
```

As you can see the first two objects are network tags and the last one is a service account indicated by “*sa:*”.

Next steps is to edit the file and ensure there is a correct mapping between network tags and tags and service accounts and tags. The edited file should look like this:

```
{“network-tag-1”: “tagValues/xxxxx”, “sql-server”: “tagValues/yyyyy”,
     "sa:seervice@account.com”: “tagValues/zzzzz”}
```

Last step here is to start the migration process attaching the json mapping file and once executed, this should complete the migration:

```
gcloud beta compute firewall-rules migrate
     --target-firewall-policy=TARGET_NETWORK_FIREWALL_POLICY
     --source-network=SOURCE_VPC_NETWORK --tag-mapping-file=//tmp/mapping.json
```

After this is completed, please review the newly created network firewall policy to ensure it is accurate and meets your expectations. Once this is done, you can attach the network firewall policy to the VPC and remove the VPC firewall rules. Please note you can also swap the rule evaluation order to network firewall policies take precedence over VPC firewall rules.

FAQ

1. **What happens if I have many VPC firewall rules with the same priority?**

   We will examine the rules and separate them between deny and allow rules. Deny rules will be given higher (smaller) priority numbers versus allow rules. For several allow rules or several deny rules with the same priority number, the system will randomly pick a non-conflict number that does not overlap with rules outside of this group, while still respecting their relative position in the firewall set. Example:

   Priority: VPC firewall rule name
   1000: vpc-fw-rule-1
   1000: vpc-fw-rule-2
   1000: vpc-fw-rule-3
   1000: vpc-fw-rule-4

   The migration tool will update rules priorities to avoid collisions. Here is the result after executing the migration tool:

   new-priority: old-priority: rule-name
   1000: 1000: vpc-fw-rule-1
   1001: 1000: vpc-fw-rule-2
   1002: 1000: vpc-fw-rule-3
   1003: 1000: vpc-fw-rule-4

2. **If firewall rules within a VPC can't be migrated because some rules contain Service Accounts or Network Tags, what would happen if I try to migrate?**

   We will migrate all the rules we can, and the rules that are not compatible with the migration tool or if the tag mapping file has not been specified will not not be migrated. Since the newly created network firewall policy is not attached to a VPC it is the responsibility of the user to check what rules were migrated and which ones need to be manually added before the new network firewall policy can be attached to the VPC.

3. **Can the migration tool migrate VPC firewall rules and a network firewall policy to a new network firewall policy?**

   Absolutely, the migration tool was designed with this aspect in mind. If a VPC contains VPC firewall rules and also a network firewall policy attached, we will migrate all the compatible VPC firewall rules as well as the network firewall policy rules to the new network firewall policy. It is the responsibility of the user to then make sure this has been migrated properly before attaching it to the VPC.

4. **Does migration change firewall enforcement order?**

No. Independent of migration, the firewall enforcement order is relevant. By default VPC firewall rules are evaluated before rules in network firewall policies. For example, if you have a VPC firewall rule with priority of 2000 and a rule with priority 1000 in a global network firewall policy attached to the same VPC network, and the firewall enforcement order evaluates VPC firewalls first, the VPC firewall rule is evaluated before the rule in the network firewall policy, regardless of the priority numbers. To change firewall enforcement order such that rules in network firewall policies are evaluated before VPC firewall rules check this link.

5. **Unsupported scenarios by Tags**

   Managed Instance Groups, Google Kubernetes Engine do not support Tags association.

6. **How can I view and troubleshoot IAM permissions**

   Policy Analyzer lets you find out which principal, such as users or groups, have access to resources based on IAM policies. With Policy Analyzer you can find who has access to a resource and what actions the principles can execute on the resource. For example, you can find which users or groups can create an IAM-governed tag and what permission a specific group has on a resource.

7. **Can I add multiple IAM-governed Tags to the same instance?**

   Yes, however even though one TagKey can have multiple TagValues, an instance can have multiple TagValues only if using separate TagKeys. For example, tagkey1/tagvalue1 and tagkey2/tagvalue2 are required instead of tagkey/tagvalue1 and tagkey/tagvalue2.

8. **Can I use source or target IAM-governed Tags to define sources or targets in a network other than the VPC network to which the network firewall policy applies??**

   In general, no, except for resources in a network connected using VPC network peering. Source tags and target tags can refer to instances in the same VPC network as the firewall policy or instances in any peered VPC networks. Resources in networks connected using Cloud VPN or Cloud Interconnect cannot be identified by IAM-governed tags.

9. **Can I explicitly bind a IAM-governed Tag to a network interface? Are VMs with multiple NICs supported?**

   Yes – an IAM governed tag implicitly identifies a network interface (NIC) of a VM bound to that tag. This is because each VM NIC must be in a unique VPC network, and because an IAM-governed tag is associated with only one VPC network. Firewall rules in a network policy of a different VPC network can refer to a different NIC of a VM by using a target or source IAM-governed tag for that other network.

10. **How can I see IAM-governed Tags bound to my instance using the short name and not the IDs?**

    Use gcloud/API to list effective tags on a resource (Preview).

11. **As a Project Admin, what are the permissions required to use IAM-governed Tags and bind it to a VM?**

To manage Resource Manager Tags on a VM, it's required to have permissions to use the specific tag and to manage the tag on a specific VM. See IAM Permissions Reference to list all Identity and Access Management (IAM) permissions and the predefined roles that grant them.

12. Can all Tags created in resource manager be used in Network Firewall Policies?

No. Tags must have the purpose field as “GCE_FIREWALL” before this tag can be referenced with firewall rules. Each of these tags must have a single target network and the tag can only be used to be associated with network interfaces in that VPC. Cloud Firewall only supports tags associated with VM interfaces today. Support for tags associated with higher level nodes, e.g. project, will be added in the future.