Cloud access control in action

Throughout your cloud cybersecurity journey, you've learned that cloud access control is an essential element of cybersecurity. It ensures only authenticated and authorized individuals can access data and resources. In this reading, first, you'll learn more about cloud access control policies, roles and permissions, identity and access management (IAM), Virtual Private Cloud (VPC) networks, and firewalls. Next you'll learn how IAM helps you control who gets access to the data and resources in your cloud. Finally, you'll get examples of what happens in cloud access control failures.

VPCs and access control in action - IAM

As a cloud security professional, you'll use Identity Access Management, or IAM, to grant predefined roles to users based on what access they need. Basic roles existed in Google Cloud before today's more fine-grained model—including predefined and custom roles—was introduced. You can use basic roles in certain scenarios—like a sandbox environment. While basic roles and IAM predefined roles are available, it's recommended you use predefined roles whenever possible. In exceptional cases, where using a predefined role might not be sufficient, you may need to grant the correct permissions using one of the basic roles or create a custom role.

The original basic roles include:

- **Owner role:** A user with this role has all viewer and editor permissions. This user also has permissions to change settings, delete projects, and manage access control.
- **Editor:** A user with this role has all the privileges the viewer role has, along with the ability to create, modify, and delete resources.
- **Viewer:** A user with this role only has read permission and cannot change resources.
- **Browser** provides access to browse Google Cloud resources.

Now, consider a scenario where you work for an organization and use Google's Compute Engine. You have IAM policies in place that allow your organization to grant access to a specific subset of resources based on a user's scope and business needs.

You use IAM policies—instead of the **viewer, editor** and **owner** basic roles—because predefined roles have specific scope and service to only grant user access to the services they are responsible to manage.

You also use IAM policies to give IAM administrators the ability to grant access to team members who need that specific access. Suppose you have a networking team that manages

all the networking resources except for firewalls and SSL certificates, which the security team manages. You'd grant the networking team the **compute.networkAdmin** predefined role and grant the security team the **compute.securityAdmin** role. Or, if you have a combined team that manages both security and networking, grant the team both predefined roles. The Compute Network Admin role allows read-only access to firewall rules, SSL certificates, and instances (to view their ephemeral IP addresses). The Compute Security Admin Role allows users to create and modify firewall rules and SSL certificates.

VPCs and access control in action using organization policies

Organization policies are policies that go across an entire cloud resource hierarchy and restrict allowed configurations.

For example, in Compute Engine you can turn off:

- Interactive access to the serial console
- External IP addresses for VM instances

To set the organization policies, you need to be granted with the correct policy admin role. Along with the IAM and organization policies you've explored so far, cloud providers have other access management solutions. For this example, we'll discuss Google's Access Context Manager, but most providers have their own solutions.

Access levels describe what the requirements are for requests to be honored. Some examples include:

- The device type and operating system
- The IP address
- User identity

Context Manager describes desired rules and allows administrators in an organization to define fine-grained access control for projects and resources based on attributes. Each cloud provider offers access controls that can rely on different attributes, (e.g. the ones listed in the previous access level examples or attributes used in organization policies or IAM permissions). Often different attributes and access controls are combined with each other.

Poor access control and access control failures

Poor access control and access control failures also lead to vulnerabilities. Here's an example. An attacker group bypasses poorly configured Multi-Factor Authentication, or MFA. They do this by using alternate single-factor protocols for an email service that's cloud-based and still allowed. The group used social engineering and obtained password reset messages that were

sent to single-factor authentication email accounts. In this case, MFA was not enabled in the email service, so the attacker gained access to a super admin account.

When you use MFA, it's critical to disable any less-secure methods. In this example, an ineffective method—single factor authentication—was set up in the email account. Since MFA was not enabled everywhere, including in the email service, it did not prevent the attackers from getting elevated privileges and allowed them to do serious damage in the cloud environment.

Remember, always enable MFA in any password request situation and always use authentication with other complementary mechanisms.

Pro tip: Always deny access by default except when dealing with public resources.

VPC firewalls

You can use VPC firewalls to allow or deny connections between types of resources in your VPC network. For example, VPC firewalls enable you to deny or allow connections to or from virtual machine (VM) instances that are in your VPC network. Once they're enabled, firewall rules are enforced based on priority. This is true regardless of the VM operating system and configuration, and whether they've started up or not.

Here are some best practices for firewall rules:

- Use least-privilege and only allow the specific traffic you need while blocking everything else.
- Block traffic that should never be allowed at an organization or folder level by using hierarchical firewall rules.
- Restrict any "allow" rules to specific VMs by specifying the service accounts the VMs are running under.
- If you need to create rules based on IP addresses, minimize the number of these rules and also keep the IP range included in the rules as small as possible.

Cloud providers give you methods to identify network interfaces or instances where firewall rules apply. In the case of Compute Engine from Google, targets identify network interfaces.

Here are a few ways you can define these targets.

- Default target instances: includes all instances in the VPC network
- Target network tag instances: the firewall rule only applies to specific network instances that use a matching network tag
- Target service account instances: the firewall rule only applies to network instances that use a specific service account

Putting it all together

Organization policies, firewall rules, and IAM permissions work together to provide different access control levels. That way, you can perform actions like assigning roles and configuring access. When you add firewalls that can allow or deny connections between types of resources in your network, you have a lot of protection from unauthorized access.

Key takeaways

MFA is a necessary strategy to prevent access to an organization's network resources exploitation. It reduces the risk of compromised passwords because users have to pass two levels of authentication. If you use MFA, you can prevent attackers from exploiting single-factor authentication and gaining access to a superuser account.

You can also grant roles to users and only allow them access to what they need based on their roles. Organizational policies can be implemented across your whole cloud resource hierarchy to restrict allowed configurations.

Be careful when setting up access control. For example, using MFA will give you more secure access control than single-factor authentication. However, combining less-secure authentication, like single-factor authentication with strong authentication, will be ineffective.

Firewalls are an effective way to allow or deny connections between types of resources in your VPC network.