Google Cloud

Firewalls for network security

So far, you've learned that networking in the cloud is similar to traditional on-premises networking. The key difference is that cloud networks are software defined, meaning the cloud service provider (CSP) implements network devices using software. Firewalls, a powerful security control used to protect networks, are another virtualized networking component.

In this reading, you'll learn more about firewalls in the cloud, and their importance as a service.

Firewalls in the cloud

Firewalls in the cloud operate similarly to firewalls in an on-premises environment. Firewalls are a network security device that monitor traffic to or from networks. Firewalls can also restrict specific incoming and outgoing network traffic.

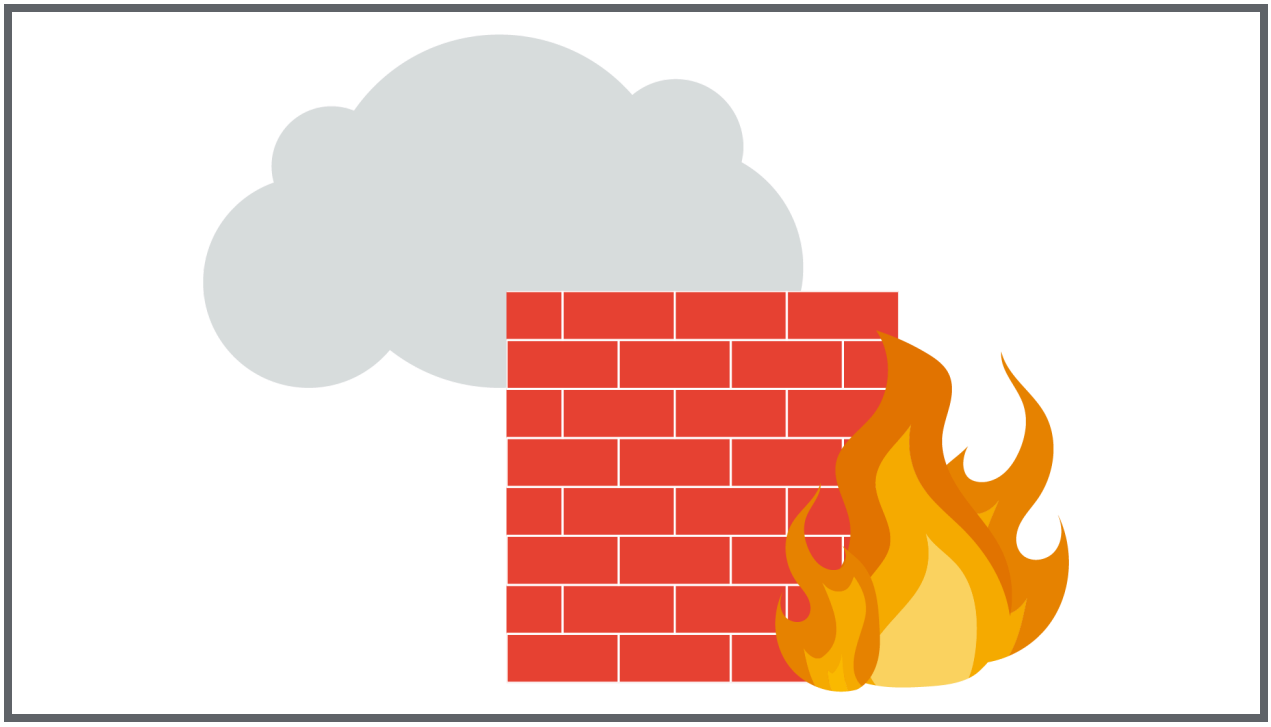
In the cloud, firewalls are software-based and hosted by CSPs. While the CSP is responsible for maintaining the software and physical infrastructure, the customer is responsible for configuring the firewall rules that filter incoming traffic.

Firewalls in the cloud are also scalable. As the cloud network grows, firewalls scale to match the increasing or decreasing demand. This means that despite needs changing, network resources will still be secured.

Firewall as a service

Firewall as a service (FWaaS) is a service model for cloud environments. Organizations can adopt FWaaS to help block unauthorized traffic on their network. For example, Google's Cloud Firewall is a FWaaS solution that protects resources from attacks both internally and externally.

In contrast to on-premises environments, cloud environments have more access points for network traffic. Consider a business that has hundreds of employees. These employees often have several devices, like laptops and mobile devices, that need to connect to the organization's network. This dramatic increase in connectivity opens the network to more vulnerabilities. FWaaS can protect these traffic access points, making it easier to control traffic and apply consistent security policies across employees.



Firewall best practices

Here are a few best practices you can apply when using firewalls:

- Always use the principle of least privilege. When creating firewall rules, only allow necessary traffic to traverse the network.
- Use hierarchical firewall policies, which will allow your organization to apply firewall policies to the organization and folder levels. Invoking hierarchical policy structure promotes consistency across organizational resources and the firewalls that protect them.
- If your organization isn't using their CSP's firewall service, choose a FWaaS solution developed by a company that tailors their product to the specific CSP's environment. There are many companies that provide FWaaS solutions to organizations.

Key takeaways

Whether operating on-premises or in the cloud, firewalls are an essential control to help secure networks. Adopting a cloud firewall is very similar to using a traditional hardware-based firewall. Firewalls in the cloud use a CSP's trusted architecture while giving organizations the control to configure firewall rules and policies. Cloud firewalls are also scalable, making them ideal for organization's with dynamic cloud networks and resources.

Resources for more information

These resources provide more information about firewalls in the cloud:

- This Google Cloud blog post compares cloud to on-premises networks and firewalls.
- This documentation about Google's Cloud Firewall provides more information about the service.