Welcome to the Protecting against Distributed Denial of Service Attacks (or DDoS): Techniques and Best Practices module.

Module overview

How DDoS attacks work

Google Cloud mitigations

Types of complementary partner products

Distributed Denial of Service Attacks are a major concern today. They can have a huge - and potentially fatal - impact on businesses if the business is not adequately prepared.

We will start this module with a quick discussion on how DDoS attacks work.

And then we will review some DDoS mitigation techniques that are provided by Google Cloud.

Then we will finish up with a review of complementary partner products and a lab where you will get a chance to see some DDoS mitigations in action.

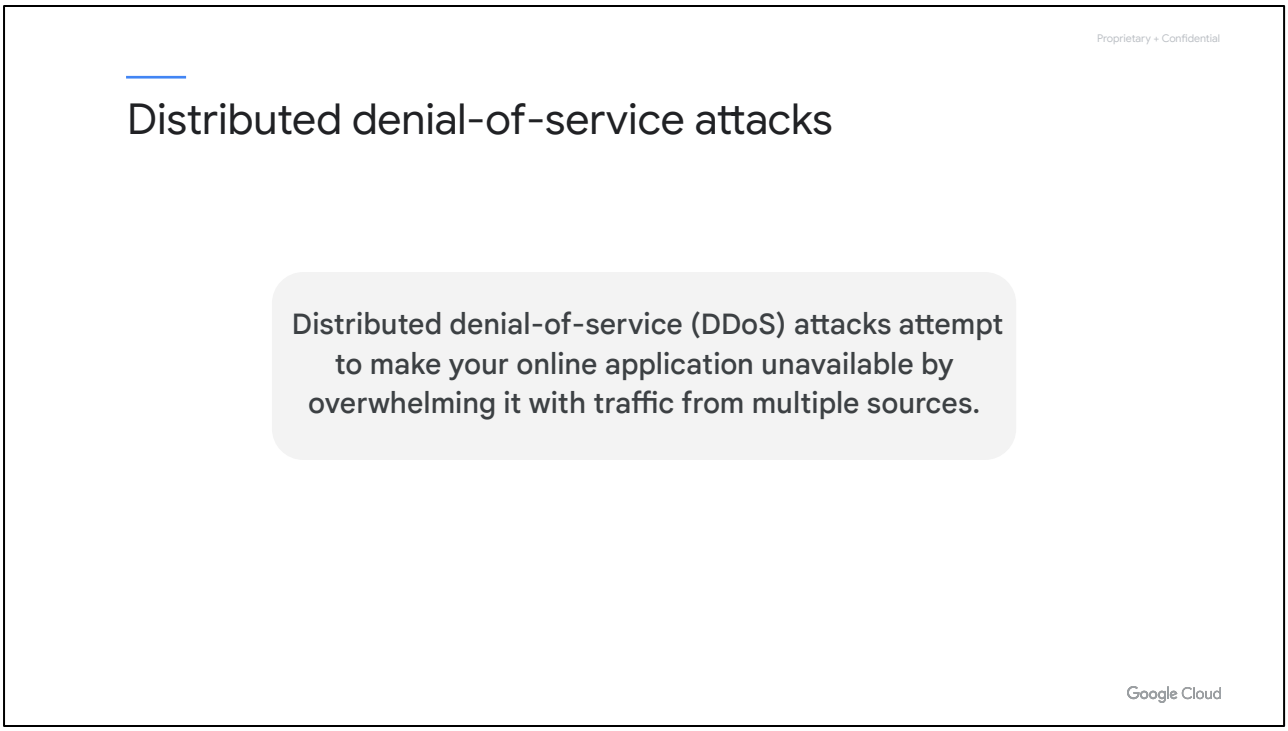
Protecting against Distributed Denial of Service Attacks (DDoS)

How DDoS attacks work

Google Cloud mitigations

Types of complementary partner products

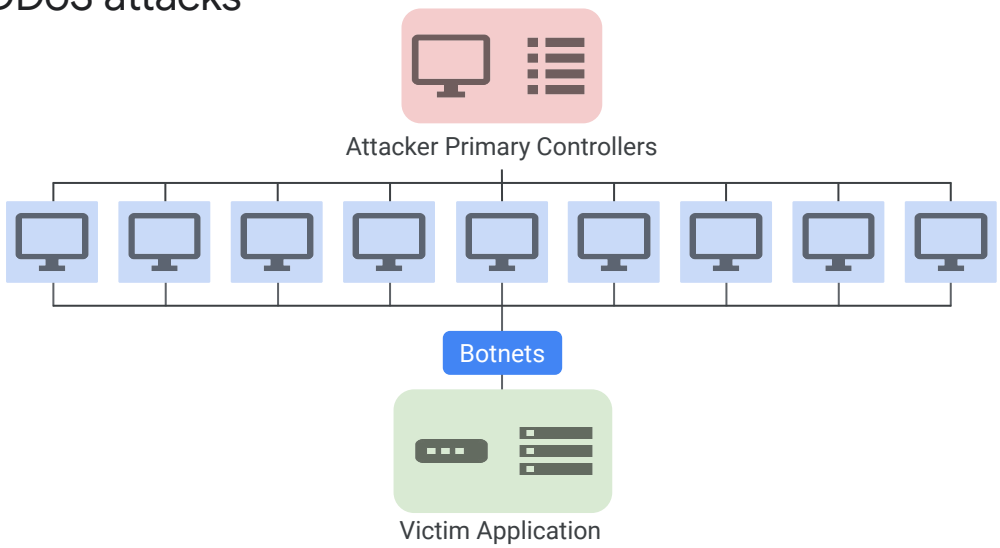
OK, let's get started with how DDoS attacks work.



A distributed denial-of-service (or DDoS) attack is a malicious attempt to disrupt normal traffic of a targeted server, service or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic from multiple sources.

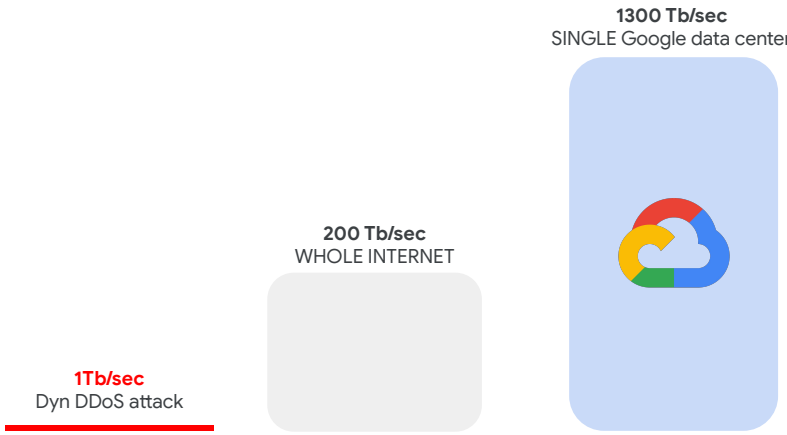
Essentially, it is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. DDoS attacks can come from individuals, cybercriminal groups, or can even be state-sponsored.

DDoS attacks



In the diagram, attackers build networks of infected computers, known as 'botnets', by spreading malicious software through emails, websites and social media. Once infected, these machines can be controlled remotely, without their owners' knowledge and they are then used like an army to launch an attack against any target. Some botnets are millions of machines strong.

Denial of service (DoS)



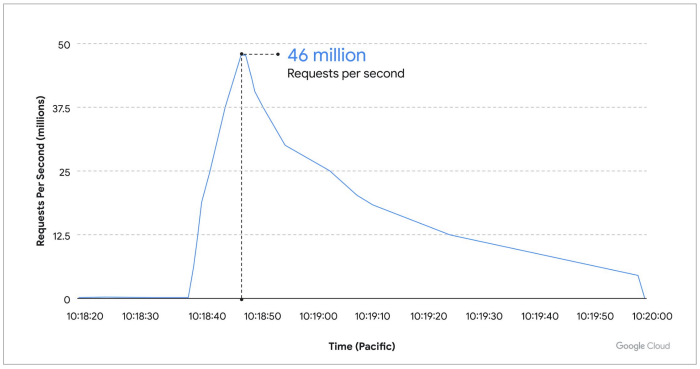
For context, a large attack in 2017 had a strength of around one terabit per second.

For reference, the whole internet has a bisection bandwidth of 200 terabits per second.

Now when you compare this to a single Google Data Center, which has a bisection bandwidth of 1,300 terabits per second, you can see, we have internal capacity many times that of any traffic load we can anticipate. This means that when there is an attack, we have time to isolate it and address it.

DDoS attacks are growing in frequency and size

- The largest Layer 7 DDoS attack at 46 million requests per second.
  - *76% larger than the previously reported record.*
  - Originated from 5,256 source IPs from 132 countries.
- Cloud Armor blocked the attack ensuring the service stayed online and continued serving their end-users.



Google Cloud

Over the past few years, Google has observed that distributed denial-of-service (DDoS) attacks are increasing in frequency and growing in size exponentially.

On June 1, 2022, a Google Cloud Armor customer was targeted with a series of HTTPS DDoS attacks which peaked at 46 million requests per second. This is the largest Layer 7 DDoS reported to date—at least 76% larger than the previously reported record.

To give a sense of the scale of the attack, that is like receiving all the daily requests to Wikipedia (one of the top 10 trafficked websites in the world) in just 10 seconds.

Cloud Armor blocked the attack ensuring the customer's service stayed online and continued serving their end-users.

For more details of this attack, read this blog:
Link:
https://cloud.google.com/blog/products/identity-security/how-google-cloud-blocked-largest-layer-7-ddos-attack-at-46-million-rps

Protecting against Distributed Denial of Service Attacks (DDoS)

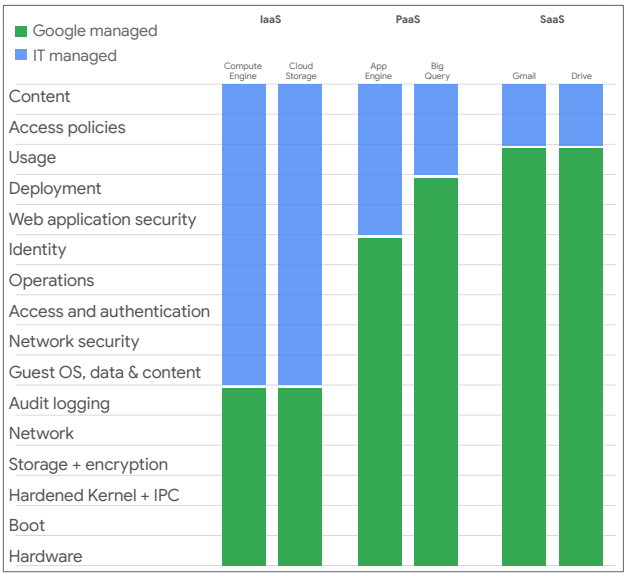
How DDoS attacks work

Google Cloud mitigations

Types of complementary partner products

Now let's review some DDoS mitigation techniques that are provided by Google Cloud.

DDoS prevention is a shared responsibility between you and Google



When you build an application on your on-premises infrastructure, you're responsible for the entire stack's security: from the physical security of the hardware and the premises in which they are housed, through the encryption of the data on the disk, the integrity of your network, and all the way up to securing the content stored in those applications.

When you move an application to Google Cloud, Google handles many of the lower layers of security. Because of its scale, Google can deliver a higher level of security at these layers than most of our customers could afford to do on their own.

Successful DDoS mitigation strategies have many layers

Load balancing	Using proxy-based load balancing to distribute load across resources
Attack surface	Reducing the attack surface on by reducing externally facing resources
Internal traffic	Isolating internal traffic from the outside world by restricting access
API management	Monitor and manage APIs to spot and throttle DDoS attacks
CDN Offloading	Offloading static content to a CDN to minimize impact
Specialized DDoS protection	Deploying applications that specifically provide deeper DDoS protection

Creating secure applications requires a multi-faceted approach which has been customized to fit your business' needs, vulnerabilities, and resources. Properly understanding the different options available when facing a DDoS attack can help your organization create a plan to minimize the impact.

Let's look at these generalized strategies in more detail and discuss how Google Cloud helps you implement them.

DDoS prevention on Google Cloud

- Leverage Google's load balancer.
- Reduce attack surface in VPCs.
- Isolate internal traffic.
- Use Cloud CDN.
- Use API management and monitoring.
- Leverage Google Cloud Armor.

In this lesson, you will learn more about:

- Leveraging Google's load balancer.
- Reducing the network attack surface.
- Isolating internal traffic.
- Using Cloud CDN.
- Using API management and monitoring.
- Leveraging the Google Cloud Armor defense service.

Leveraging Google's load balancer

Cloud Load Balancing provides built-in defense against infrastructure DDoS attacks.

- No additional configuration is required to activate this DDoS defense.

- Leverages Google's central DoS mitigation service.
  - If the system detects an attack, it can configure load balancers to drop or throttle traffic.

Google Cloud's load balancer provides built-in defense against infrastructure DDoS attacks - and no additional configuration is needed. Placing a load balancer in front of your services will filter known-bad traffic streams before they reach your resources. Google Cloud offers load balancing at layer 4 (the transport layer, such as TCP or UDP) and layer 7 (the application layer, generally HTTP or HTTPS.) The layer 4 load balancers automatically protect against things like UDP floods and TCP SYN floods. The layer 7 load balancers provide layer 4 protections plus protection from connection-based attacks like Slowloris.

Google Cloud load balancers leverage Google's global DoS mitigation service. If the system detects an attack, it will automatically configure the load balancers to drop or throttle traffic.

Reducing attack surface

Attack surface definition:

Sum of the different points where an unauthorized user can try to enter data to or extract data from an environment.

- Isolate machines within VPCs.
- Set up firewall rules to block unused ports.
- Use firewall rules to block unwanted sources.
- Use firewall tags and service accounts to control targets.

An attack surface of a software environment is the sum of the different points where an unauthorized user can try to enter data to or extract data from an environment. Keeping the attack surface as small as possible is a basic security measure.

Reduce attack surface means reducing how much exposure your VMs have to the Internet. You should host Compute Engine resources that require network communication on the same VPC network. If the resources aren't related and don't require network communication among themselves, consider hosting them on different VPC networks. For most applications implemented in Google Cloud, Google also recommends creating separate subnets within a network for each tier of an application (for example, web front end, services layer, and database back end.) That is because subnetting is a convenient way to implement inter-network firewall restrictions.

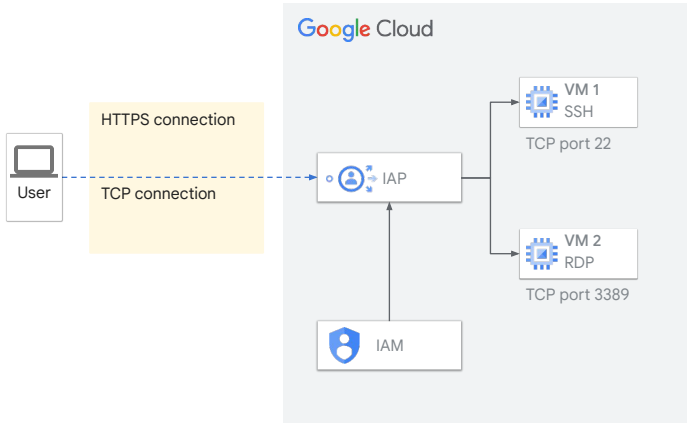
You can control individual ingress and egress traffic for compute resources using firewall rules.

Be sure you are blocking both unused ports as well as unwanted sources.

Remember, you can use firewall tags and service accounts to help control which targets to use for firewall rules.

Restricting public access to internal traffic

- Don't give machines public IPs unnecessarily.
- Use Identity-Aware Proxy or bastion hosts to limit machines exposed to the internet.
- Use internal load balancers for internal services.



It is also important to ensure you restrict external traffic within your VPCs. Virtual machines should not be given public IP addresses unnecessarily.

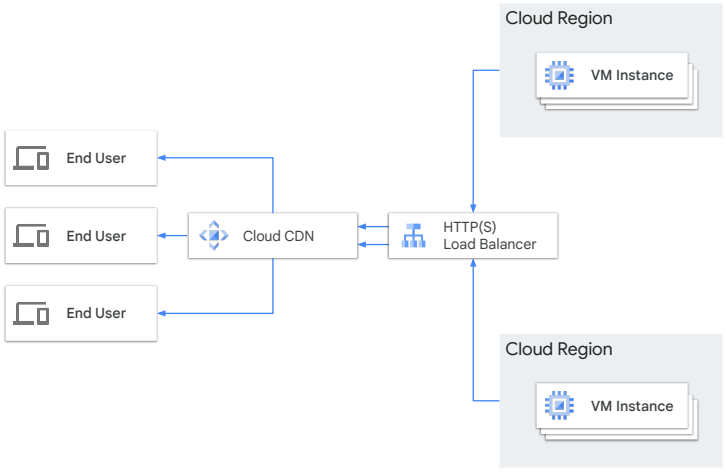
Even if you need to connect to the VM from the internet, leveraging solutions like Identity-Aware Proxy or bastion hosts can help restrict the internal traffic. These solutions are covered in the **Securing Compute Engine** module of the **Security Best Practices in Google Cloud** course.

You can also connect your on-premise network with your VPC network using VPN IPsec Tunnels or Dedicated Interconnect.

Using Cloud CDN

Caches content between your users and your servers.

- Requests for cached content are routed to POPs.
- Google's massive infrastructure can absorb attacks.



Google's Cloud Content Delivery Network (or CDN) is used to cache web content at over 90 edge locations, or points of presence (POPs), around the globe.

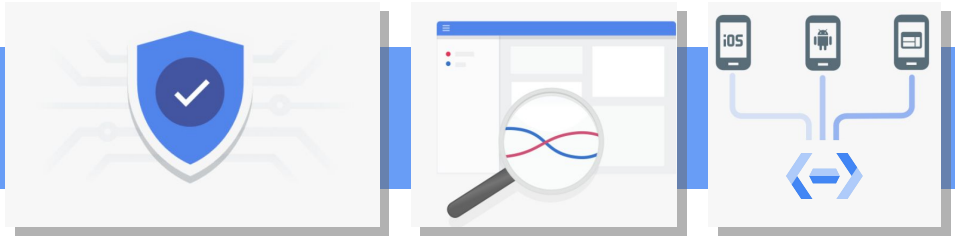
Cloud CDN provides very similar protection as Google's load balancers. In addition, requests for your content are routed to Google's POPs (points of presence) rather than directly to your resources.

Thus, Google Cloud's resilient network infrastructure absorbs the brunt of attacks.

This also naturally reduces the load on your resources even when there are no attacks.

API management and monitoring

- Create an API gateway to manage your backend services.
  - Throttle requests to limit requests from clients.
  - Control access to APIs from a single location.
  - Monitor API usage.
- Can use Cloud Endpoints or Apigee to create API gateways.



For IT, network and DevOps teams, allowing access to backend services is often required to facilitate interactions between applications, services, customers and business partners.

This access can also introduce vulnerabilities and challenges.

Putting an API gateway, or API management, in front of your backend services can help prevent denial of service attacks by:

- Throttling requests to limit the number of requests per client.
- Controlling access to API from a single centralized location.
- Adding the ability to monitor and track all API usage.

In Google Cloud, there are two options for implementing API management: Cloud Endpoints or Apigee.

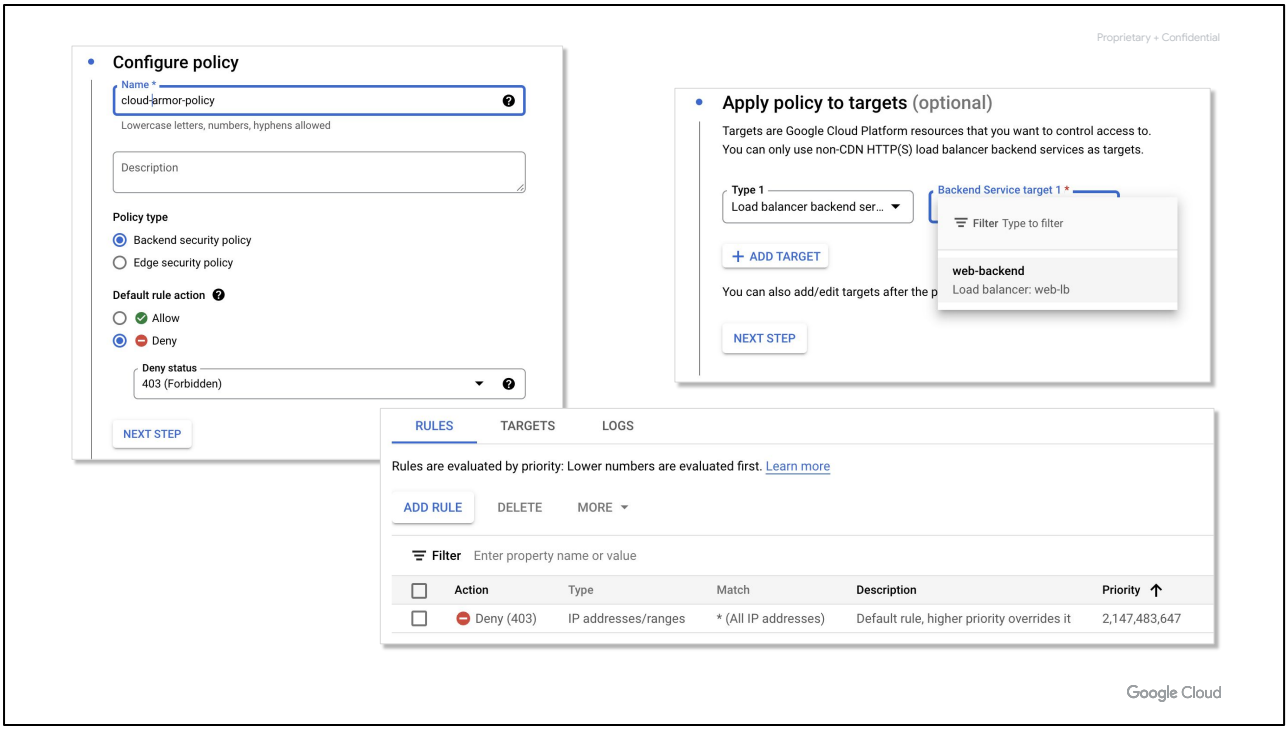
Google Cloud Armor

- Google Cloud Armor protection is delivered at the edge of Google's network and blocks attacks close to their source.
- Enables IP blocklist/allowlist security policies.

Google Cloud Armor is a DDoS and application defense service. It delivers defense at scale against infrastructure and web application Distributed Denial of Service (DDoS) attacks using Google's global infrastructure and security systems.

Similar to CDNs, Google Cloud Armor protection is delivered at the edge of Google's network and can block attacks close to their source, before they have a chance of affecting your applications. Google Cloud Armor works with the Global HTTP(S) Load Balancer to provide built-in defenses against infrastructure DDoS attacks.

Additionally, Google Cloud Armor enables you to customize your defenses and mitigate multivector attacks, such as enforcing access control to allow or restrict user traffic based on IPv4 and IPv6 addresses or CIDRs. Google Cloud Armor also works with security offerings from security partners, enabling you to build a comprehensive security model for your services.



Google Cloud Armor defense is customized using a security policy which can contain one or more rules.

Rules tell your security policy what to do (the action), when to do it (the condition) and where to apply the rule (the target).

Google Cloud Armor also provides several predefined rules to defend against cross-site scripting (XSS) and SQL injection (SQLi) application-aware attacks.

Other Google Cloud Armor Features

- Supports variety of load balancers:
  - Global external HTTP(S)
  - Global external HTTP(S) (classic)
  - External TCP proxy
  - External SSL proxy
- Supports:
  - Rate limiting
  - Adaptive protection
  - Google Cloud Armor bot management with reCAPTCHA Enterprise
  - Custom rules language

Google Cloud Armor also provides the following features:

- **Variety of load balancer support:** Google Cloud Armor now supports TCP Proxy load balancers and SSL proxy load balancers in General Availability, in addition to Global external HTTP(S) and Global external HTTP(S) (classic) load balancers.
- **Rate limiting:** rate-based rules help you protect your applications from a large volume of requests that flood your instances and block access for legitimate users.
- **Adaptive protection:** helps you protect your Google Cloud applications, websites, and services against L7 distributed denial-of-service (DDoS) attacks such as HTTP floods and other high-frequency layer 7 (application-level) malicious activity.
- **Cloud Armor bot management with reCAPTCHA Enterprise:** help you evaluate and act on incoming requests that might be from automated clients.
- **Custom rules language:** enables you to define prioritized rules with configurable match conditions and actions in a security policy.

For the latest Google Cloud Armor updates, check out the Google Cloud Armor release notes.

- **Link:** cloud.google.com/armor/docs/release-notes

To explore Google Cloud Armor's features further, check out the **Securing your Network with Cloud Armor** quest.

- **Link:** https://www.cloudskillsboost.google/quests/254

Protecting against Distributed Denial of Service Attacks (DDoS)

How DDoS attacks work

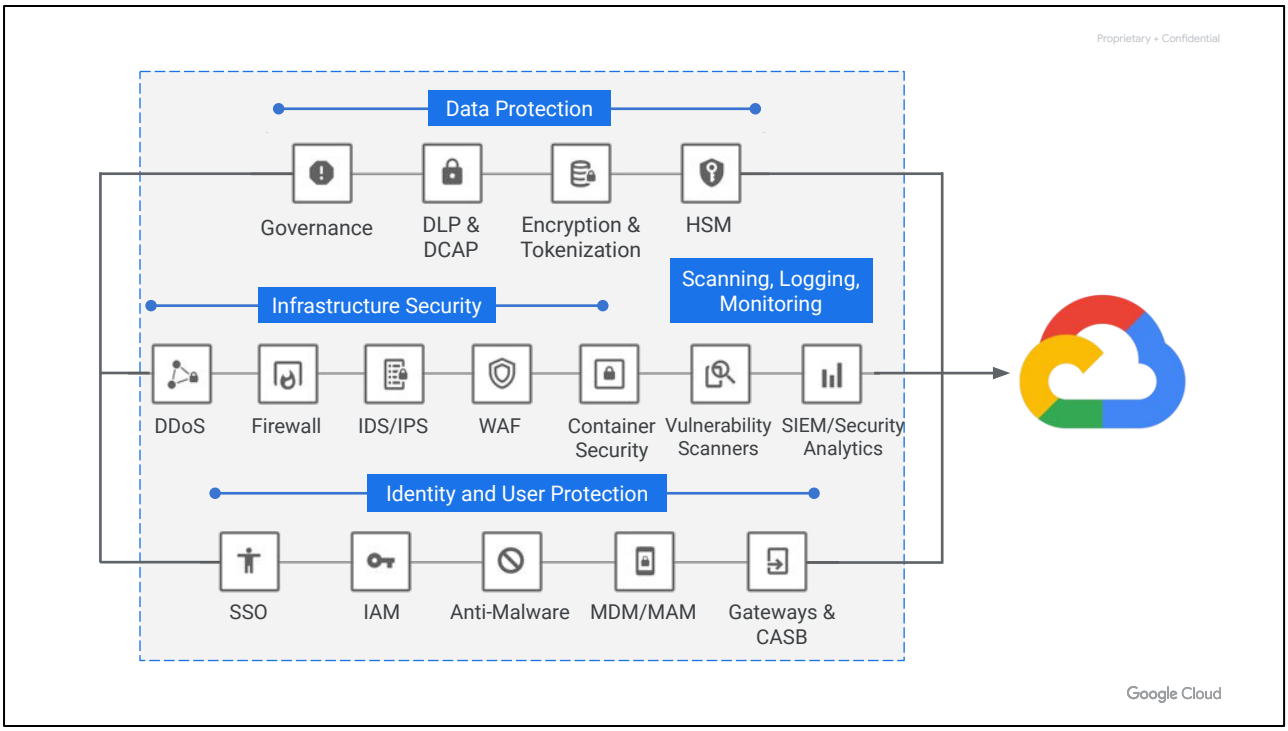
Google Cloud mitigations

Types of complementary partner products

As you have seen, here at Google we offer some of the best in class platform security, but we did not stop there.

Google also partners with a number of security-centric firms.

In this section, we will review some of the complementary partner products.



There are several different categories of security in our security ecosystem:

Data protection - which includes things like

- Governance
- Data Loss Prevention
- Data-Centric Audit and Protection
- Encryption
- Hardware security modules

Infrastructure protection - which includes:

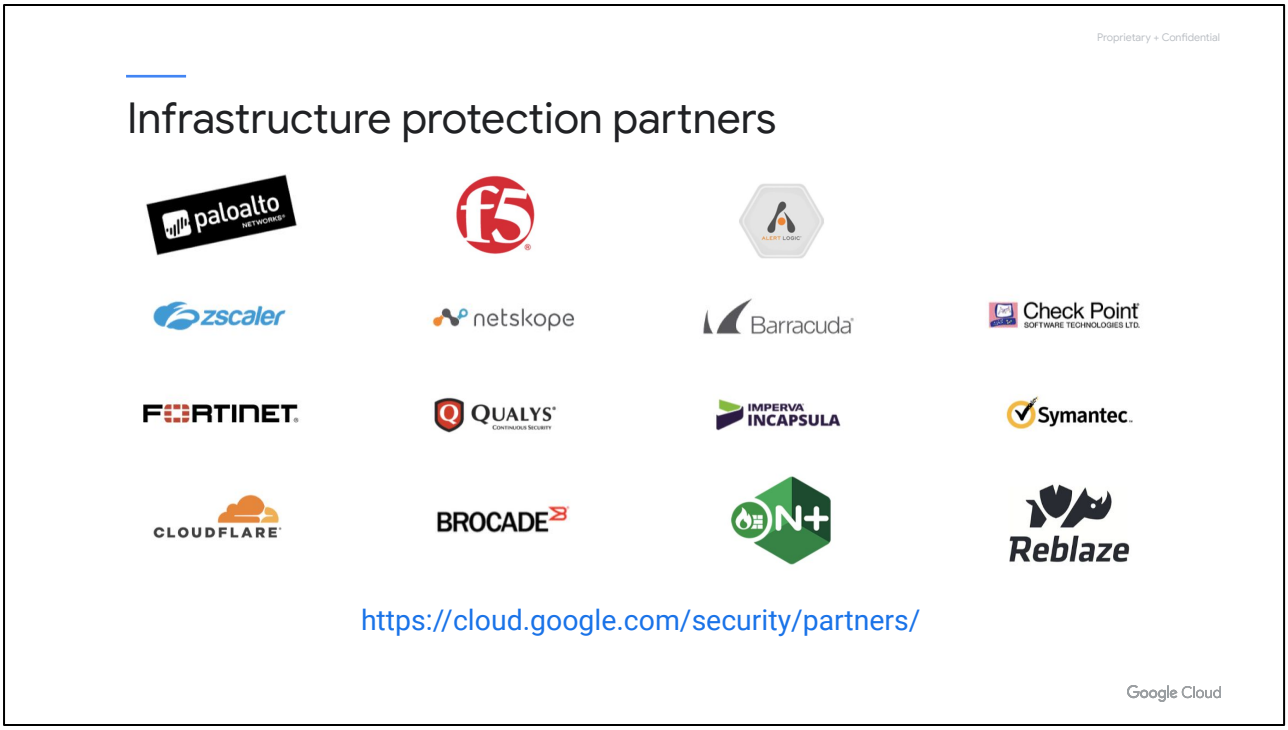
- DDoS protection
- Network and application firewalls
- Intrusion detection and prevention
- Container security

Scanning, Logging and monitoring, which includes a vulnerability scanner and security and information management tools.

Identify and user protection, which includes:

- Single sign on
- Identity and access management,
- Anti-malware,
- Mobile device and application management
- Cloud Access Security Brokers

Configuration, vulnerability, risk, and compliance protection, across all areas of your infrastructure.



Infrastructure Protection helps protect your cloud infrastructure and applications from cyber-attacks. There are many industry leaders that provide services that can be leveraged from Google Cloud covering a wide range of solutions, including:

- Next generation firewalls
- Web application firewalls
- Web proxies and cloud gateways
- Server Endpoint protection
- Distributed Denial of Service
- And Container Security

Data protection partners

https://cloud.google.com/security/partners/

Data protection partners can help protect your data from unauthorized access, as well as internal and external threats through encryption, key management, and policy-driven data loss prevention controls.

Logging and monitoring partners

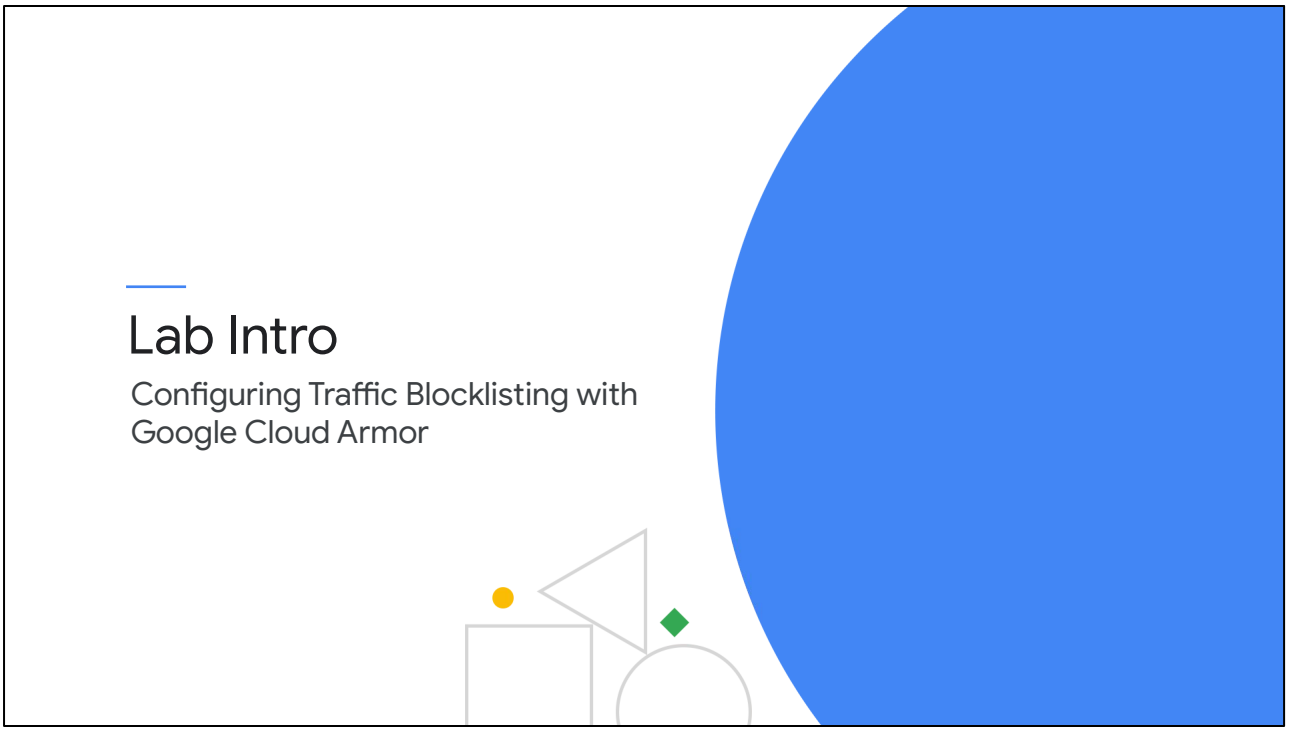
https://cloud.google.com/security/partners/

Logging and monitoring partners help enable visibility and auditability of user and system activities in your infrastructure, while providing policy-driven alerting and reporting.

Configuration, vulnerability, risk, and compliance

https://cloud.google.com/security/partners/

Configuration, vulnerability, risk and compliance partners can facilitate the visualization and inspection of your network and application deployments for vulnerabilities, security and compliance risks, and be able to assist with remediation.



Next, you will see Google Cloud Armor in action. In this lab, you will perform the following tasks:

- Configure an HTTP Load Balancer for a simple web application,
- And use Google Cloud Armor to blocklist an IP address and restrict access to an HTTP Load Balancer

Module review

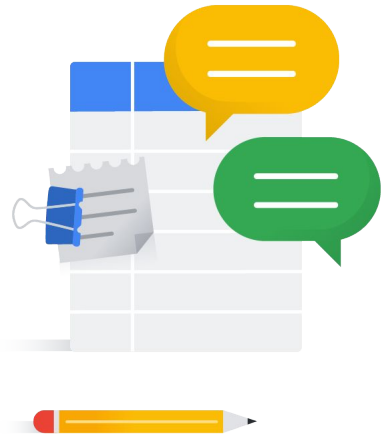
- DDoS attacks overwhelm a server with a flood of traffic to disrupt services.
- DDos attacks often use servers and computers infected with malware.
- DDoS mitigation requires a multi-layered approach designed to absorb attacks, reduce risk, isolate sensitive traffic, and monitor systems for signs of malicious behavior.

- Google Cloud provides tools to execute these strategies, including load balancing, VPCs for isolation, Cloud Endpoint or Apigee to create API management gateways, Cloud CDN for serving content from the edge to the outside, and Google Cloud Armor for at-scale defense of your applications and operations.
- Third-party options are also available that complement Google Cloud products. Different categories of third-party security in the ecosystem include infrastructure protection partners, data protection partners, monitoring and logging partners and vulnerability, risk and compliance partners. A more detailed, current list can be seen at: https://cloud.google.com/security/partners.

The next module covers another important security topic: content-related vulnerabilities.

Module review

- Google Cloud provides tools for all of these uses:
  - Google Cloud load balancing.
  - VPCs that control traffic via firewall rules and isolate sensitive servers.
  - Cloud Endpoint or Apigee as API management gateways.
  - Cloud CDN for content service outside Google Cloud.
  - Google Cloud Armor for application and system defense at scale.
- Third-party options are also available that complement Google Cloud products.



- Google Cloud provides tools to execute these strategies, including load balancing, VPCs for isolation, Cloud Endpoint or Apigee to create API management gateways, Cloud CDN for serving content from the edge to the outside, and Google Cloud Armor for at-scale defense of your applications and operations.
- Third-party options are also available that complement Google Cloud products. Different categories of third-party security in the ecosystem include infrastructure protection partners, data protection partners, monitoring and logging partners and vulnerability, risk and compliance partners. A more detailed, current list can be seen at: https://cloud.google.com/security/partners.

The next module covers another important security topic: content-related vulnerabilities.