AWS Shield

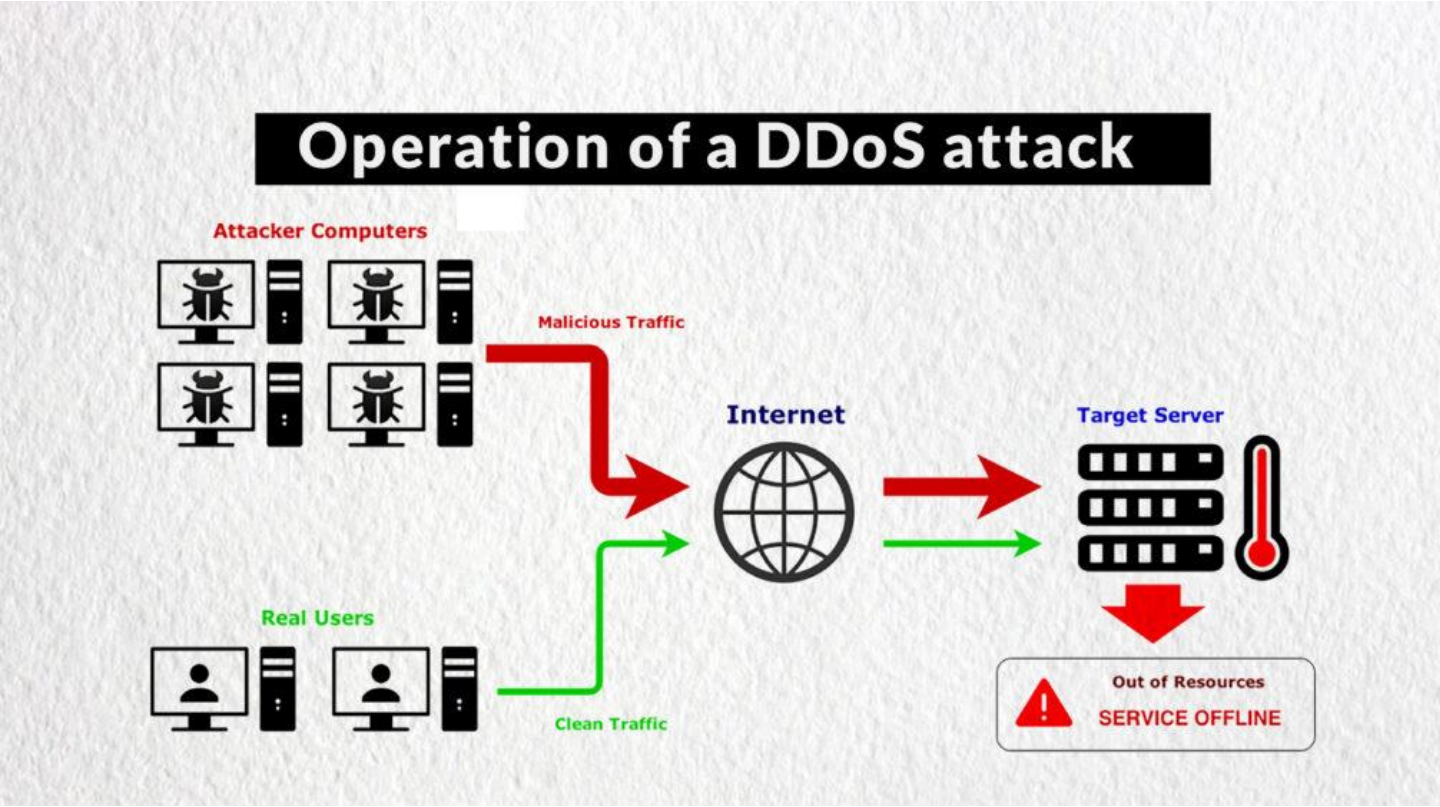
Protection against Distributed Denial of Service (DDoS) attacks is primarily essential for your internet-facing applications.

AWS is dedicated to providing you with the tools, best practices, and services you need to ensure high availability, security, and resiliency in your defence against bad actors on the internet.

What are DDoS Attacks?

The denial of service (DDoS) attack aims to overload IT resources where they cannot function properly. This form of attack is usually launched in one among the subsequent ways:

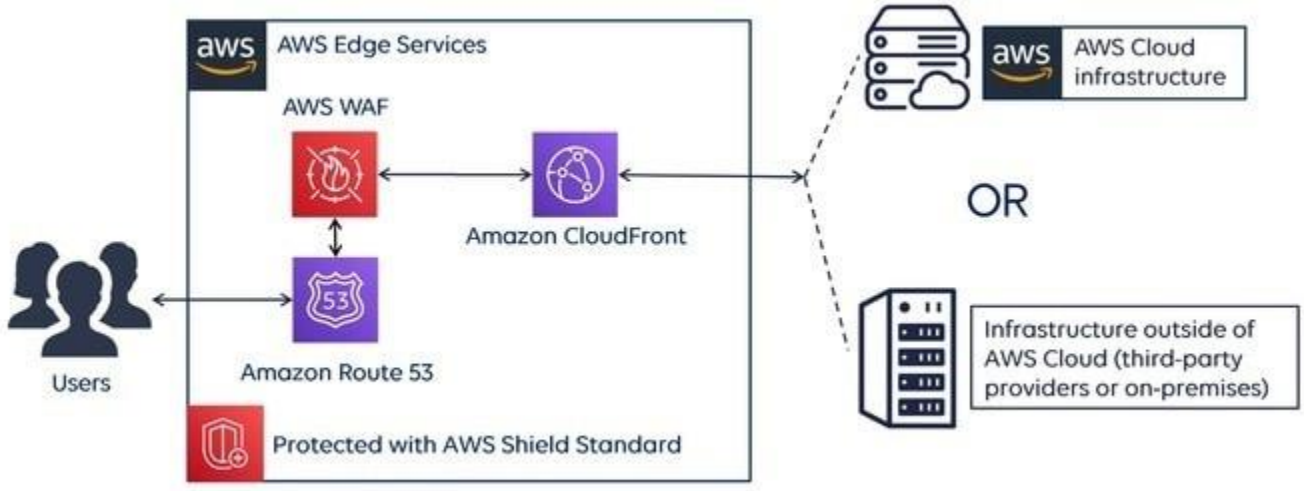
- The workload on cloud services is artificially increased with imitation messages or repeated communication requests.
- The network is overloaded with traffic, which reduces its responsiveness and cripples its performance.
- Multiple cloud service requests are sent to consume excessive memory and processing resources.



What is AWS Shield?

It is a managed Distributed Denial of Service (DDoS) protection service that safeguards applications running on Amazon Web Services (AWS). It delivers always-on monitoring and automatic inline mitigations that reduce application downtime and latency, eliminating the requirement for AWS

Support to benefit from DDoS protection.



Benefits of AWS Shield

1. **Seamless integration and deployment:** Your AWS resources come with Standard protection and are protected against the most common network and transport layer DDoS attacks. Using the AWS Management Console or APIs, you can easily enable Advanced protection for Elastic IP, Elastic Load Balancing (ELB), Amazon CloudFront, AWS Global Accelerator, or Amazon Route 53 resources you want to protect.
2. **Customizable protection:** Advanced gives you the freedom to choose which resources to safeguard for infrastructure (Layer 3 and 4). To protect against sophisticated application-layer assaults, you can use AWS WAF to define custom rules. These adaptable rules can be activated in a matter of seconds, allowing attacks to be promptly mitigated.
3. **Managed Protection and Attack Visibility:** With Standard, you always get on heuristics-based network flow monitoring and inline mitigation against frequently occurring network and transport layer DDoS attacks. The Advanced provides enhanced resource-specific detection and employs advanced mitigation and routing techniques for sophisticated or more significant attacks.
4. **Cost Efficient:** Standard is automatically enabled for all AWS customers at no additional cost. With Advanced, customers get AWS WAF and AWS Firewall Manager at no additional cost for using resources protected by AWS Shield Advanced as described on the Shield pricing.

Types of AWS Shield

1. AWS Standard Shield

- All AWS customers benefit from its automatic protection of it.
- It provides always-on network flow monitoring, which inspects incoming traffic to AWS and detects malicious traffic in real-time.
- It uses several techniques like deterministic packet filtering and priority-based traffic shaping to mitigate attacks without impact on your applications automatically.
- You get extensive availability protection with CloudFront and Route 53 against all known infrastructure attacks.
- You can also get a list of all the events that AWS Shield has detected and neutralised.

2. AWS Shield Advanced

- It provides enhanced detection, inspects network flows, and monitors application layer traffic to your Elastic IP address, Elastic Load Balancing, CloudFront, or Route 53 resources.
- It handles the majority of DDoS protection and mitigation responsibilities for **layer 3**, **layer 4**, and **layer seven** attacks.
- You have access to the 24×7 AWS DDoS Response Team.
- It gives automatic additional mitigation capacity to protect against more serious DDoS attacks.
- It is available globally on all CloudFront and Route 53 edge locations.
- With this, you will see the history of all incidents in the trailing 13 months.

What does AWS Shield protect against?

1. AWS Shield Standard protects your applications and websites against the following types of DDoS attacks:

- **State-Exhaustion Attacks (layer 4) – SYN Flood:** Consumes the TCP connection status tables found in various network infrastructure and security devices and application servers. The attacker connects to a server rapidly but does not complete the connection. These attacks can prohibit legitimate users from accessing data, leaving security systems vulnerable to data theft.
- **Volumetric Attacks (layer 3):** Referred to as network floods and include UDP floods (UDP reflection attacks) and ICMP floods. This type of attack occurs when a network is **overwhelmed by malicious traffic**, causing your applications or services to become unavailable.

2. AWS Shield Advanced protects your apps against the same attacks as the Standard version with some specific functions, but because it also includes AWS WAF, it protects against:

- **Application-Layer Attacks (layer 7) – HTTP floods, DNS query floods**: Comprised of popular requests (HTTP GETs and DNS queries) designed to consume application resources. An example is an attacker who continuously utilises a website functionality (submitting a contact form or any API requests) where he knows that it causes database and application processing.
- **Other Application-Layer Attacks:** SQL injection (SQLi), Cross-site scripting (XSS), Remote file inclusion (RFI) and other web application attacks and threats from the OWASP Top 10 publication.

AWS Shield Pricing

There is no charge for inbound data transfer on AWS, and you do not pay for DDoS attack traffic that AWS Shield mitigates.

Type	AWS Shield Standard	AWS Shield Advanced
Commitment	None	1 Year
Monthly Fee	None	$3000
Data Transfer Out (DTO) Usage Fees	None	Refer to the below DTO table

AWS Shield Standard

It is built into the AWS services that you can use for your web applications. There are **no additional costs for Standard**.

AWS Shield Advanced

It is a paid service that **adds extra** security to internet-facing applications. You'll pay **$3000** for every organisation that signs up for Advanced and commits to a one-year subscription. You will only have to pay the monthly cost once if your company has many AWS accounts.

Data transfer out to the public Internet	Amazon CloudFront	Elastic Load Balancing (ELB)	AWS Elastic IP	AWS Global Acceleration	Amazon Route 53
First 100 TB	$0.025	$0.05	$0.05	$0.05	No additional cost
Next 400 TB	$0.02	$0.04	$0.04	$0.04	No additional cost
Next 500 TB	$0.015	$0.03	$0.03	$0.03	No additional cost

Difference between AWS WAF and AWS Shield

These two services are part of the AWS Edge Services ecosystem and protect against DDoS attacks. The difference between both is that **AWS WAF (Web Application Firewall) protects the application layer,** whereas **AWS Shield protects the OSI model's infrastructure layers.**

Type	AWS Shield	AWS WAF
Protection Against	State-Exhaustion Attacks and Volumetric Attacks	HTTP Floods, DNS query floods, SQL injection, Cross-site scripting, Remote file inclusion
How it Works	Offers automatic DDoS protection against more common layer 3, the network layer, and layer 4, the transport layer attacks	Protects your web apps by filtering, monitoring, and blocking any malicious HTTP/S traffic (on layer 7) travelling to the web Application