AWS Shield

09 December 2023 16:56

AWS Shield is a managed Distributed Denial of Service (DDoS) protection service provided by Amazon Web Services (AWS). It helps protect AWS applications from various types of DDoS attacks by detecting and mitigating them in real time. Here are some common use cases for AWS Shield:

1. DDoS Protection:
   - *Volumetric Attacks:* Shield protects against large-scale volumetric attacks that attempt to overwhelm a network's bandwidth by flooding it with traffic.
   - *Application Layer Attacks:* It safeguards against more sophisticated application layer attacks, which target specific aspects of an application or service.

2. High Availability:
   - By protecting against DDoS attacks, AWS Shield helps ensure high availability for your applications and services. Downtime due to DDoS attacks can be costly, and Shield helps minimize such risks.

3. Web Application Firewall (WAF) Integration:
   - AWS Shield can be integrated with AWS WAF, providing a comprehensive security solution. WAF helps protect web applications from common web exploits and vulnerabilities, while Shield focuses on DDoS protection.

4. Automatic and Manual DDoS Mitigation:
   - AWS Shield provides both automatic and manual DDoS mitigation options. Automatic mitigation helps protect against common and well-known attack patterns, while manual mitigation allows for more fine-tuned control when needed.

5. Global Threat Environment Monitoring:
   - AWS Shield continuously monitors the global threat landscape to identify emerging DDoS attack patterns. This enables proactive protection against evolving threats.

6. Cost Savings:
   - Shield can help reduce the cost associated with DDoS attacks. By mitigating attacks and preventing downtime, businesses can avoid revenue losses and expenses related to recovering from an attack.

7. Incident Response and Reporting:
   - AWS Shield provides detailed reports on DDoS attacks, including attack traffic details and mitigation outcomes. This information is valuable for incident response, forensic analysis, and improving overall security posture.

8. Integration with AWS Services:
   - Shield seamlessly integrates with other AWS services, providing a holistic security approach. This includes integration with AWS CloudFront, AWS Route 53, and other services commonly used for delivering applications.

9. Customizable Protection:
   - AWS Shield allows you to customize DDoS protection based on your specific needs

   and application requirements. You can configure settings to match your application's traffic patterns, and you have the flexibility to adjust mitigation strategies as needed.

10. Continuous Monitoring and Learning:
    - AWS Shield leverages machine learning algorithms to continuously adapt and improve its ability to detect and mitigate new and evolving DDoS attack vectors. This helps in staying ahead of emerging threats.

11. Multi-Layered Defense:
    - AWS Shield provides a multi-layered defense strategy, combining network-level and application-level protections. This ensures comprehensive coverage against a wide range of DDoS attack techniques.

12. Protection for Different Workloads:
    - Whether you are running web applications, APIs, or other types of workloads on AWS, Shield is designed to provide protection across various types of applications and services.

13. Visibility and Control:
    - AWS Shield provides visibility into ongoing attacks through real-time monitoring and reporting. This visibility allows you to make informed decisions and take necessary actions to mitigate the impact of DDoS attacks.

14. Advanced Threat Intelligence:
    - AWS Shield benefits from threat intelligence gathered by AWS from a diverse set of customers and global network traffic. This collective intelligence enhances the service's ability to identify and mitigate sophisticated DDoS attacks.

In summary, AWS Shield is a versatile and comprehensive service that helps organizations defend against DDoS attacks, ensuring the availability, reliability, and security of their applications and services on the AWS platform. Its integration with other AWS services and adaptability to different workloads make it a valuable component of a robust security architecture in the cloud.

What types of attacks can AWS Shield Standard help protect me from

- AWS Shield Standard is designed to protect against common and most frequently observed Distributed Denial of Service (DDoS) attacks. Here are some types of DDoS attacks that AWS Shield Standard can help protect you from:

- **Volumetric Attacks:**

- Traffic Flooding: Shield defends against large-scale volumetric attacks that flood your network with a high volume of traffic, aiming to overwhelm your infrastructure's bandwidth.

- **Application Layer Attacks:**
  - HTTP/HTTPS Floods: These attacks target the application layer by overwhelming web servers with a large number of HTTP/HTTPS requests, attempting to exhaust server resources.
  - Slowloris and RUDY Attacks: These are types of low-and-slow attacks that aim to keep many connections to the target web server open for as long as possible, exhausting server resources over time.

- **State-Exhaustion Attacks:**
  - SYN/ACK Floods: Shield helps protect against attacks that exploit the TCP handshake process, overwhelming a server with a large number of SYN or ACK packets, exhausting server resources.
  - UDP Reflection Attacks: Shield mitigates attacks that involve sending a large number of UDP packets to a network, with the source address spoofed to appear as if they are coming from the target.

- **DNS Query Floods:**
  - Shield provides protection against DDoS attacks that target the Domain Name System (DNS) infrastructure by flooding it with a high volume of DNS queries, making it difficult for legitimate requests to be processed.

- **Amplification Attacks:**
  - DNS Amplification: Shield helps prevent attacks that use DNS servers to amplify the volume of attack traffic, making it more challenging to mitigate.

- **Application-Layer Protocol Anomalies:**
  - Shield is capable of identifying and mitigating anomalies in application-layer protocols, such as malformed or invalid requests, to prevent them from affecting the targeted application.