Anti-DDoS Solutions Available on the Market

Author: Graciela Martínez
Coordination and Revision: Communications Area
Edition: Communications Area
Department: Technology Area

September 2024

lacnic
www.lacnic.net

Multiple vendors and companies offer a variety of anti-DDoS solutions. Below is a list of some of the tools available on the market.

Commercial Solutions

Selecting the most suitable solution for each organization depends on various factors, including budget, required protection level, and existing infrastructure.

Cloudflare [1]:

Description: Cloudflare is one of the most popular DDoS mitigation solutions. It offers protection against both network and application targeted attacks, with a global infrastructure that disperses malicious traffic.

Features: DDoS protection, CDN (Content Delivery Network), WAF (Web Application Firewall), and secure DNS.

Advantages: Easy to implement, global scalability, real-time analysis, and cost-effective for sites of all sizes.

Akamai:

Description: This company is best known for its content delivery network but also offers robust DDoS mitigation capabilities through its Kona Site Defender Service.

Features: Network and application-level protection, traffic distribution across a global network, and advanced monitoring and analysis tools.

Advantages: Large distribution network, support for high traffic volumes, and high reliability.

https://www.akamai.com/

Amazon Web Services (AWS) Shield:

Description: AWS Shield is a DDoS mitigation solution built into the AWS infrastructure. There are two tiers of AWS Shield: Standard and Advanced.

Features: Protection against network and application targeted attacks, integration with other AWS services, and advanced monitoring and response capabilities.

Advantages: Native integration with AWS, automatic protection and scalability, detailed reporting options, and additional support with AWS Shield Advanced.

https://aws.amazon.com/en/shield/

Google Cloud Armor:

Description: Google Cloud Armor provides DDoS protection for applications hosted on Google Cloud, using Google's global infrastructure.

Features: Rules-based security policies, mitigation of network and application-level attacks, and protection against volumetric and application attacks.

Advantages: Native integration with Google Cloud, easy to configure and manage, and global scalability.

https://cloud.google.com/armor/docs?hl=es-419

Imperva Incapsula:

Description: Imperva Incapsula offers DDoS protection for web applications and cloud-based services.

Features: DDoS mitigation at network and application level, WAF, bot protection, and real-time monitoring and analysis capabilities.

Advantages: Comprehensive protection against various types of attacks, easy to deploy, and advanced configuration and customization options. https://www.imperva.com/

Arbor Networks (NETSCOUT):

Description: Arbor Networks is a security solution focusing on DDoS protection, used by both service providers and enterprises.

Features: Real-time attack detection and mitigation, global network-based intelligence, and detailed analyses.

Advantages: Extensive experience and reputation in DDoS mitigation, support for large infrastructures, and advanced analysis tools.

https://www.netscout.com/solutions/service-provider-ddos-protection

F5 Networks:

Description: F5 Networks provides DDoS mitigation solutions designed to protect applications and networks through its BIG-IP system.

Features: DDoS mitigation at network and application level, WAF, load balancing, and monitoring and analysis tools.

Advantages: Hybrid hardware and software approach, high reliability, and ability to handle large volumes of traffic.

https://www.f5.com/es_es

The solutions above are popular for their effectiveness and ability to handle large volumes of traffic, and also because they are easy to install and utilize.

Organizations should check with their security solution providers and ISPs, who often include DDoS mitigation services as a form of adding value to their connectivity service.

Open-Source Solutions

There are also several open-source tools used for DDoS attack mitigation. Examples include:

Haproxyr:

Description: HAProxy is a free, very fast, and reliable reverse-proxy offering high availability, load balancing, and proxying for TCP and HTTP-based applications.

Features: It is a load balancer and proxy that can help distribute traffic evenly across multiple servers.

Advantages: It can be useful for handling large volumes of traffic during a DDoS attack

https://github.com/haproxy

Gatekeeper:

Description: Gatekeeper is the first open-source DDoS protection system, used by network operators working for institutions, service and content providers, enterprise networks, etc.

Features: It is designed to scale to any peak bandwidth. Despite its geographically distributed architecture, the network policy that describes all decisions that have to be enforced on incoming traffic is centralized.

Advantages: Its ability to scale to any bandwidth allows it to withstand current and future DDoS attacks. Likewise, its centralized policy enables network operators to leverage distributed algorithms that would not be viable under very high latency (e.g. distributed databases) and to fight multiple multi-vector DDoS attacks at once.

https://github.com/AltraMayor/gatekeeper

FastNetMon:

Description: A high-performance DDoS detector/sensor built on top of multiple packet capture engines: NetFlow, IPFIX, sFlow, AF_PACKET.

Features: Detects hosts in the deployed network sending or receiving large volumes of traffic, packets/bytes/flows per second and performs a configurable action to handle that event. These configurable actions include notifying you, calling script, or making BGP announcements.

Advantages: It has multiple advantages, such as detecting DoS/DDoS in as little as 1-2 seconds, it scales up to terabits on a single server (sFlow, Netflow, IPFIX) or to 40G+ in mirror mode, thresholds can be configured per subnet, email notifications about detected attacks, and complete IPv6 support.

https://github.com/pavel-odintsov/fastnetmon/

Finally, it's worth noting that some ISPs and security providers also offer DDoS scrubbing services to their customers. These services consist of sending the organization clean traffic after absorbing the attack, as they are supposed to have the intelligence to detect and discard most types of DDoS attacks. To ensure effectiveness, they should be complemented with DNS and BGP solutions.