Data Sheet

FLASHBOX

DDoS PROTECTION: Volumetric DDoS Attacks

Protect and secure your business against DDoS attacks.

Definition of a Volumetric DDoS Attack

A DDoS (distributed-denial-of-service) attack is one of the most significant and popular kinds of cybersecurity threats, aimed at preventing or significantly slowing access to your network. There are three main kinds of DDoS attack: volumetric (or volume-based), protocol or application-layer attacks.

Volumetric attacks overwhelm the bandwidth capabilities of your network by sending a high volume of traffic or request packets, leading to denial of service. They are the most common type of DDoS because of the ease of generating a high volume of requests, and the potential of amplification techniques to scale the attack.

Volumetric attacks have also been on the rise due to the massive increase in unsecured Internet of Things (IoT) devices, which are leveraged into botnets to launch crippling volumetric DDoS attacks.

Common Volumetric Attack Types

User Datagram Protocol (UDP) Floods
UDP packets are used to flood random ports on a server, forcing it to repeatedly check for, and respond to non-existent applications.

ICMP, or Ping Floods
ICMP echo requests (also known as pings) are used to overwhelm a victim's network, forcing it to respond with an equal number of replies.

Domain Name Servers (DNS) Amplification
Target server IP addresses are spoofed and fake DNS requests are sent to open resolvers, which send responses at an amplified factor.

Mirai & Its Variants

The Mirai botnet
The self-propagating Mirai botnet was behind what was then the largest denial-of-service attack in history. DNS provider, Dyn, was knocked offline in October 2016, bringing down many popular sites, including Twitter, Netflix, CNN and many others across the U.S. and Europe.

Mirai has a scanner process that seeks out unsecured IoT devices to compromise, and ten attack vectors it can launch to coordinate a mass volumetric DDoS attack against any chosen target.

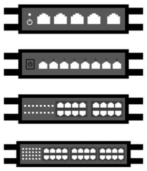
Mirai & Its Variants

The author made the source code for Mirai online back in 2016, and it has spawned a wave of Mirai copycats ever since.

Largest DDoS Attack Ever

In March 2018, GitHub was briefly knocked offline in the largest DDoS attack ever. At its peak, traffic reached 1.35 Terabits per second (Tbps). The attack was driven by memcached reflection; many vulnerable servers remain exposed.

“This attack was the largest attack seen to date by Akamai, more than twice the size of the September, 2016 attacks that announced the Mirai botnet and possibly the largest DDoS attack publicly disclosed. Because of memcached reflection capabilities, it is highly likely that this record attack will not be the biggest for long.” - Akamai



Mitigating Volumetric DDoS Attacks

Flashbox counters damaging volumetric attacks through its singular web application delivery and security protection platform. Our cloud protection service offers full integration with AWS, giving Flashbox access to a global network of scrubbing centers that scale when necessary to guarantee that your services can withstand large botnet threats and even the biggest volumetric attacks.

Our always-on cloud service and use of the latest monitoring technologies ensures sure that accurate, rapid filtering continues so that legitimate traffic will still reach your host servers, even when under attack.

Why Flashbox for your Comprehensive DDoS Protection?

With proactive monitoring, precise threat assessments and timely responses, Flashbox has only one mission: to keep your data safe and secure, 365/24/7. We offer four deployment options:

CLOUD PROTECTION

We offer two kinds of cloud protection: DNS redirect and BGP redirect. Whether you are relocating, rightsizing, upgrading, or outsourcing – we can help. As leading infrastructure experts, our team will engineer an agile and scalable data center and/or cloud solution.

ON PREMISES PROTECTION

The best on-premises DDoS protection solutions provide real-time, 365/24/7 threat detection and in-line mitigation. There is zero latency and all kinds of DDoS threat can be accurately diagnosed and removed.

HYBRID PROTECTION

We can help you secure the most comprehensive service, providing on-premises protection at the appliance level combined with cloud-based protection. Flashbox will help design a hybrid protection service that offers DDoS and web application protection at scale.

PROFESSIONAL PLANNING & MANAGEMENT SERVICES

This service is for customers who want Flashbox to manage their on-premises boxes, cloud-based protection solutions and/or their hybrid package. Our team has decades of security experience and will work with you to provide top-level security and professional services.

Key Benefits of Flashbox Protection

- Comprehensive DDoS Protection
- 365/24/7 Monitoring & Visibility
- Real-time Threat Detection
- Multivector Protection
- Timely Deployment
- Critical Expertise
- Fully Managed Services

FLASHBOX
NETWORKS

CORPORATE HEADQUARTERS

660 4th Street #621
San Francisco, CA 94107 USA

www.flashbox.net