Data Sheet

FLASHBOX

DDoS PROTECTION: Protocol Attacks

Protect and secure your business against DDoS attacks.

Definition of a Protocol DoS Attack

A DoS (denial-of-service) attack is one of the most significant and popular kinds of cybersecurity threat, aimed at preventing or significantly slowing access to your network. There are three main kinds of DDoS attack: protocol, also known as exhaustion-state attacks, volumetric or application-layer attacks.

Protocol (layer 4) attacks are aimed at exploiting server resources, or other kinds of intermediate critical infrastructure, such as load balancers and firewalls. They are a form of DoS, involving overwhelming a network host with requests from multiple locations. They target a weakness in how a protocol operates, hence their name.

Protocol or state-exhaustion attack types include SYN floods, ping of death, smurf DDoS and fragmented packet attacks. Attack magnitude is measured in Packets per second (Pps).

Protocol attacks account for around 20% of all recorded DDoS attacks. They are often used in combination with other kinds of attack vectors to compromise a single target, and can be highly effective.

What are Multi-Vector Approaches?

Increasing numbers of DDoS attacks use a multi-vector approach, combining different kinds of DDoS attack. This kind of approach is appealing to an attacker as it can lead to the most significant damage to an enterprise or organization. This tactic can increase the chances of success by either simultaneously targeting several different types of network resources, or using one attack vector as a smokescreen while another more powerful vector is deployed as the main weapon. According to Imperva Incapsula, 81% of attacks are multi-vector.

Common Protocol Attack Types

SYN Floods

SYN Floods exploit weaknesses in the TCP connection sequence, also known as the three-way handshake. An attacker sends a large volume of TCP requests to a target's system, intending to exhaust server resources.

Smurf Attack

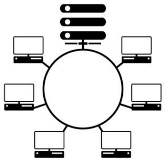
A Smurf attack exploits vulnerabilities in the Internet Protocol (IP) and Internet Control Message Protocols (ICMP), ultimately rendering computer networks inoperable. When combined with IP broadcasting, the Smurf attack can be catastrophic.

Ping of Death

The Ping of Death manipulates IP protocols by overwhelming a targeted system with oversized or malicious pings. It was highly used in the past and has largely been patched, however, many websites still block ICMP (ping) messages to prevent any future iterations of this kind of DDoS.

“The right security service can help shut down a Smurf or other DDoS attack before it begins. The Smurf Attack sounds cute but poses real risks if servers are overwhelmed.” - Kaspersky Lab

Mitigating Protocol DDoS Attacks



Flashbox counters protocol or state-exhaustion attacks through its cloud and/or on-premises solutions by blocking bad traffic before it ever reaches your site. Our services leverage cutting-edge traffic analysis algorithms that enable rapid differentiation between legitimate and bad traffic.

ISP grade edge routers filter out and isolate identifiable malicious packets, such as SYN floods. Furthermore, Flashbox’s cloud-based BGP routing means that when an attack occurs, traffic is rerouted through our global scrubbing centers using BGP announcements. Flashbox temporarily acts as the ISP, allowing it to inspect and filter all incoming traffic, only forwarding legitimate requests via GRE tunneling.

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 comprehensive 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 Flashbox team will engineer an agile and scalable custom data center and/or cloud solution that grows with your business.

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